



Citrix SD-WAN 11.4

Machine translated content

Disclaimer

このコンテンツの正式なバージョンは英語で提供されています。Cloud Software Group ドキュメントのコンテンツの一部は、お客様の利便性のみを目的として機械翻訳されています。Cloud Software Group は機械翻訳されたコンテンツを管理していないため、誤り、不正確な情報、不適切な用語が含まれる場合があります。英語の原文から他言語への翻訳について、精度、信頼性、適合性、正確性、またはお使いの Cloud Software Group 製品またはサービスと機械翻訳されたコンテンツとの整合性に関する保証、該当するライセンス契約書またはサービス利用規約、あるいは Cloud Software Group とのその他すべての契約に基づき提供される保証、および製品またはサービスのドキュメントとの一致に関する保証は、明示的か黙示的かを問わず、かかるドキュメントの機械翻訳された範囲には適用されないものとします。機械翻訳されたコンテンツの使用に起因する損害または問題について、Cloud Software Group は責任を負わないものとします。

Contents

Citrix SD-WAN 11.4.0a リリースのリリースノート	11
Citrix SD-WAN 11.0 SE ネットワークの問題のトラブルシューティング	23
Citrix SD-WAN 11.4.1 リリースのリリースノート	24
Citrix SD-WAN 11.4.2a リリースのリリースノート	29
Citrix SD-WAN 11.4.2b リリースのリリースノート	35
Citrix SD-WAN 11.4.3a リリースのリリースノート	41
Citrix SD-WAN 11.4.4 リリースのリリースノート	47
SD-WAN アプライアンスの新しいユーザーインターフェイス	49
システム要件	78
SD-WAN プラットフォームモデルとソフトウェアパッケージ	80
アップグレード・パス	84
仮想 WAN 展開で仮想 WAN ソフトウェアを 9.3.5 にアップグレードする	85
稼働中の仮想 WAN 展開で 11.4 にアップグレードする	89
仮想 WAN 展開を動作させずに 11.4 にアップグレードする	95
Citrix SD-WAN アプライアンスソフトウェアの再イメージ化	101
ローカル変更管理を使用した部分的なソフトウェアのアップグレード	103
USB で Premium 版変換に WANOP	106
Standard Edition から Premium Edition への変換	109
USB イメージ再作成ユーティリティ	110
Citrix SD-WAN ライセンスオプション	113
ローカルライセンス	115
リモートライセンス	115
一元化されたライセンス	117

ライセンスの管理	121
ライセンスの有効期限	122
構成	122
初期設定	124
Web インターフェイス (UI) レイアウトの概要	125
アプライアンスハードウェアの設定	132
管理 IP アドレスの設定	133
日付と時刻の設定	140
セッションのタイムアウト	142
アラームの設定	144
ロールバックの構成	146
マスター制御ノードの設定	149
MCN の概要	150
MCN コンソールに切り替える	151
MCN を構成する	154
仮想 WAN セキュリティと暗号化の有効化と構成 (オプション)	175
セカンダリ MCN の設定	176
MCN 設定の管理	178
ブランチノードのセットアップ	188
ブランチノードの構成	190
ブランチサイトのクローン (オプション)	206
ブランチ構成の監査	208
MCN サイトとクライアントサイト間の仮想パスサービスの構成	208
MCN 設定のデプロイ	217

MCN 変更管理の実行	217
ブランチへの構成のデプロイ	219
ワンタッチスタート	224
クライアントアプライアンスのネットワークへの接続	226
クライアントへの SD-WAN アプライアンスパッケージのインストール	227
CloudInit を使用して、 OpenStack での Citrix SD-WAN Standard Edition のデプロイ	233
210 SE LTE アプライアンスでの LTE 機能の構成	243
110-LTE-WiFi アプライアンスでの LTE 機能の構成	258
外付け USB LTE モデムの構成	271
デプロイ	275
チェックリストと展開方法	276
ベストプラクティス	277
ゲートウェイモード	283
インラインモード	297
仮想インラインモード	303
SD-WAN ネットワークの構築	319
Premium (エンタープライズ) エディションでのみ WAN 最適化	320
2 ボックスモード	323
高可用性	333
光ファイバ Y ケーブルを使用したエッジモードの高可用性の有効化	341
ゼロタッチ	344
オンプレミスのゼロタッチ	365
AWS	365
Azure	376

単一リージョンの展開	394
マルチリージョンの展開	396
Citrix Virtual Apps and Desktops のワークロードの構成ガイド	401
ドメイン・ネーム・システム	413
DHCP サーバと DHCP リレー	419
DHCP サーバと DHCP リレーの設定	420
DHCP クライアントによる WAN リンク IP アドレスの学習	424
ダイナミック PAC ファイルのカスタマイズ	429
GRE トンネル	433
MCN サイトの GRE トンネルの設定（任意）	434
ブランチサイトの GRE トンネルの設定	436
帯域内およびバックアップ管理	437
インターネットアクセス	447
統合ファイアウォールを使用したブランチでの直接インターネットブレイクアウト	448
Secure Web Gateway による直接インターネットアクセス	451
バックホールインターネット	452
ヘアピンモード	454
ホストされたファイアウォール	456
Palo Alto Networks SD-WAN 1100 プラットフォーム上のファイアウォール統合	457
SD-WAN 1100 プラットフォームでの Check Point ファイアウォールの統合	480
リンク集約グループ	496
リンク状態の伝播	501
メータリングおよびスタンバイ WAN リンク	502
Office 365 の最適化	514

Citrix Cloud および Cloud サービスの最適化	526
Citrix SD-WAN アプライアンスのオンプレミス構成用の Citrix SD-WAN オーケストレータ	531
PPPoE セッション	540
サービス品質	549
クラス	550
IP アドレスとポート番号による規則	552
アプリケーション名による規則	559
ルールグループを追加して MOS を有効にする	565
アプリケーション分類	566
QoS 公平性 (RED)	580
MPLS キュー	582
レポート	591
アプリケーション QoE	592
HDX QoE	595
複数のネットフローコレクタ	597
ルート統計情報	599
ルーティング	602
SD-WAN オーバーレイルーティング	603
ルーティングドメイン	627
ルーティングドメインの構成	628
ルートの設定	630
CLI を使用してルーティングにアクセスする	631
動的ルーティング	631
OSPF	641

BGP	651
iBGP	658
eBGP	659
アプリケーションルート	659
ルートフィルタリング	664
ルート集約	669
プロトコルプリファレンス	672
マルチキャストルーティング	673
仮想パスルートコストの構成	677
仮想ルータ冗長プロトコルの設定	680
ネットワークオブジェクトの構成	685
LAN セグメンテーションのルーティングサポート	688
ルーティング間ドメインサービス	688
ECMP 負荷分散	694
セキュアなピアリング	698
DC サイトのスタンドアロン SD-WAN SE および WANOP アプライアンスから PE アプライアンスへの自動 セキュアピアリング	700
DC サイトおよびブランチサイトの PE アプライアンスから、自動セキュアピアリングが開始されます	705
スタンドアロンの SD-WAN SE および WANOP アプライアンスを使用して、 DC サイトおよびブランチの PE アプライアンスから自動セキュアピアリングを開始	710
DC サイトおよびブランチ PE アプライアンスの PE アプライアンスから、手動によるセキュアピアリングを開始	715
DC サイトの PE アプライアンスから、ブランチスタンドアロン SD-WAN SE および WANOP アプライア ンスへの手動セキュアピアリング	718
ドメイン参加と代理ユーザーの作成	722
セキュリティ	727

IPsec トンネル終了	727
Citrix SD-WAN と AWS トランジットゲートウェイとの統合	728
仮想パスおよびダイナミックパスの IPsec トンネルを構成する方法	740
SD-WAN とサードパーティデバイス間の IPsec トンネルを構成する方法	741
IKE 証明書を追加する方法	749
IPsec トンネルの設定を表示する方法	750
IPsec の監視とログ	752
IPsec 非仮想パスルートの適格性	755
IPsec ヌル暗号化	756
FIPS 準拠	757
Citrix SD-WAN Secure Web Gateway	761
GRE トンネルと IPsec トンネルを使用した Zscaler 統合	762
Citrix SD-WAN での Forcepoint を使用したファイアウォールトラフィックリダイレクトのサポート	773
IPsec トンネルを使用した Palo Alto 統合	777
ステートフルファイアウォールと NAT のサポート	783
グローバルファイアウォールの設定	785
ファイアウォールの詳細設定	786
ゾーン	788
ポリシー	791
ネットワークアドレス変換 (NAT)	796
静的 NAT	797
ダイナミック NAT	805
仮想 WAN サービスの構成	812
ファイアウォールセグメンテーションの構成	814

証明書認証	820
AppFlow と IPFIX	824
SNMP	834
管理インターフェース	838
NDP ルータアドバタイズメントおよびプレフィクス委任グループ	843
WAN の最適化	846
Citrix SD-WAN Premium Edition	847
最適化を有効化し、デフォルトの機能設定を構成する	848
最適化のデフォルトチューニング設定の構成	852
最適化の既定のアプリケーション分類子の構成	853
最適化のデフォルトサービスクラスを構成する	856
ブランチサイトの最適化を構成する	862
SSL プロファイルの設定	863
Citrix WAN 最適化クライアントプラグイン	867
ハードウェアとソフトウェアの要件	868
WANOP プラグインの仕組み	869
プラグインで使用するためのアプライアンスのデプロイ	876
プラグイン MSI ファイルをカスタマイズする	880
Windows システムにプラグインを展開する	886
WANOP プラグイン GUI コマンド	891
WANOP プラグインの更新	895
WANOP プラグインのトラブルシューティング	895
SMB 3.1.1 接続	896
ハウツー記事	898

インターフェイスグループ	898
仮想 IP アドレス ID の設定	899
アクセスインターフェイスの設定	900
仮想 IP アドレスの構成	900
GRE トンネルの設定	901
ブランチ間通信用の動的パスを設定する	902
監視とトラブルシューティング	905
仮想 WAN の監視	906
統計情報の表示	907
フロー情報の表示	909
レポートの表示	914
ファイアウォールの統計情報の表示	920
診断	923
パス・マッピングと帯域幅の使用率の向上	938
管理 IP のトラブルシューティング	943
セッションベースの HTTP 通知	944
アクティブ帯域幅テスト	950
適応型帯域幅検出	952
ベストプラクティス	954
セキュリティ	954
ルーティング	963
QoS	963
WAN リンク	964
よくあるご質問	965

Citrix SD-WAN 11.4.0a リリースのリリースノート

November 17, 2022

このリリースノートドキュメントでは、Citrix SD-WAN リリース 11.4.0a に存在する機能強化と変更、修正された問題と既知の問題について説明します。

注

- セキュリティ関連のアドバイザリの一覧については、Citrix セキュリティ情報を参照してください。
- Citrix SD-WAN 11.4.0a リリースは、<https://support.citrix.com/article/CTX319135> に記載されているセキュリティの脆弱性を修正し、リリース 11.4.0 を置き換えます。リリース 11.4.0 で利用可能だった機能強化およびバグ修正に加えて、リリース 11.4.0a には次のバグ修正が含まれています-SDWANHELP-2106、SDWANHELP-2078、SDWANHELP-2066、NSSDW-35630、NSSDW-35596、および NSSDW-34670。
- Citrix SD-WAN 11.4.0 リリースは、Citrix SD-WAN Center と SD-WAN 構成エディターを完全にサポートする最後のメインラインリリースです。Citrix SD-WAN Center と SD-WAN 構成エディターはどちらも廃止されました。非推奨化は、製品/機能が段階的に廃止されることを事前に通知するものですが、現在提供されており、完全にサポートされています。次の Citrix SD-WAN リリースファミリでは、Citrix SD-WAN Center と SD-WAN 構成エディターは削除され、サポートされなくなります。その代わりに、Citrix ではすべての構成要件に Citrix SD-WAN Orchestrator を使用することをお勧めします。Citrix SD-WAN Orchestrator は、Citrix SD-WAN Center および SD-WAN 構成エディターを使用して現在実行されているすべての構成をサポートします。詳細については、「[Citrix SD-WAN Orchestrator サービス](#)」および「[オンプレミス向け SD-WAN オーケストレータ](#)」を参照してください。

新機能

リリース 11.4.0a で利用可能な機能強化と変更点。

構成と管理

フォールバック構成の WAN ポート用の静的 IP アドレス用の NITRO レスト API

Citrix SD-WAN 11.4.0 リリース以降では、NITRO REST API を使用して、フォールバック構成で WAN ポートの静的 IP アドレスを構成できます。既存のフォールバック設定 API に新しいパラメーターが追加されます。

[NSSDW-33255]

Citrix SD-WAN の新しい UI の機能強化

Citrix SD-WAN の新規 UI には、次の機能強化が含まれています。

- Citrix SD-WAN の新規 UI の外観は、Citrix の再ブランディングに従って、新しい色とフォントを反映するように変更されます。
- 新しい UI は、クライアントとして構成されているすべての Citrix SD-WAN アプライアンスで、デフォルトで有効になります。

注:

Citrix SD-WAN アプライアンスを MCN としてプロビジョニングすると、レガシー UI にリダイレクトされます。

- LACP LAG インターフェイスの詳細を表示できます。
- DNS プロキシ統計の監視
- SLAAC WAN リンクのモニタリング

[NSSDW-30842、NSSDW-28818、NSSDW-32030]

SNMP

次の SNMP MIB が追加されます。

- アプライアンス統計
 - アプライアンスで使用された CPU の割合
 - アプライアンスで使用された RAM のパーセンテージ
- WAN リンク統計テーブル
 - WAN リンクの LAN から WAN への最大物理レート (Kbps)
 - WAN リンクの WAN から LAN への最大物理レート (Kbps)
 - WAN リンクの LAN から WAN への許可レート (Kbps)
 - WAN リンクの WAN から LAN への許可レート (Kbps)

[NSSDW-30592]

帯域内管理

帯域内管理では、高可用性デバイスのペアがサポートされます。高可用性ペアのアプライアンスは、インバンドアクセスを使用して相互に通信します。

[NSSDW-24534]

IPv6 インターネットおよびイントラネットサービスのスタティック NAT ポリシー

Citrix SD-WAN バージョン 11.3.1 を実行しているアプライアンスをバージョン 11.4.0 にアップグレードするときには、IPv6 インターネット/イントラネットサービスの既存の静的 NAT ポリシーを手動で更新する必要があります。

[NSSDW-33726]

その他

エッジセキュリティコンポーネントのパッチアップグレードサポート

Citrix SD-WAN Advanced Edition (AE) は、エッジセキュリティサブシステムのアップグレードを可能にするパッチアップグレードメカニズムをサポートしています。

エッジセキュリティが有効な既存のリリースから、エッジセキュリティコンポーネントの新しいバージョンを含む上位リリースにアップグレードすると、サブシステムの更新のパリティのみがダウンロードされ、アップグレードされます。

[NSSDW-26721]

SD-WAN Center ダッシュボード

Citrix SD-WAN Center ダッシュボードでは、最大 300 サイトを構成すると、マルチリージョンの概要ダッシュボードが表示されます。

[NSSDW-21753]

ネットワーク

クラス

Citrix SD-WAN は、仮想パスおよび動的仮想パスでトラフィックフローを持つクラスのみを表示します。クラスが表示され、値として 0 が表示されている場合は、以前にフローしていたトラフィックが停止したことを意味します。ただし、クラスがまったく表示されない場合は、仮想パスサービスの状態がリセットされたため（ソフトウェアのアップグレードや再起動など）、そのクラスのトラフィックフローがまったくないことを意味します。

[NSSDW-33974]

IPFIX の IPv6 サポート

Citrix SD-WAN は、IPFIX 用の IPv6 アドレスをサポートしています。Citrix SD-WAN は、テンプレート 615 および 616 を使用して、IPv6 IPFIX フローデータをエクスポートします。アプリケーションフロー情報 (**IPFIX**) を選択して、テンプレート 615 に従ってデータセットをエクスポートできます。フローデータのエクスポートで問題が発生した場合は、テンプレート **616** に従ってデータをエクスポートする基本プロパティ (**IPFIX**) を選択します。

[NSSDW-29153]

DNS プロキシおよび DNS トランスペアレントフォワーダの IPv6 サポート

Citrix SD-WAN は、****DNS** プロキシおよび **DNS** 透過転送を構成するための **IPv6** アドレスをサポートしています
******。DNS プロキシまたは DNS 透過転送を定義するには、次の IPv6 DNS サービスタイプを使用します。

- **StaticV6**: 静的 IPv6 DNS サーバーの IP アドレスを設定できます。内部、ISP、グーグル、またはその他のオープンソースの DNS サービスを作成できます。StaticV6 DNS サービスは、グローバルレベルおよびサイトレベルで構成できます。

- **dynamicV6**: ダイナミック IPv6 DNS サーバーの IP アドレスを設定できます。DynamicV6 DNS サービスは、サイトレベルでのみ構成できます。サイトごとに許可される DynamicV6 サービスは 1 つだけです。

[NSSDW-29151]

ECMP 負荷分散

Equal Cost Multi-Path (ECMP; 等価コストマルチパス) グループを使用すると、同じコスト、宛先、サービスタイプを持つ複数のルートをグループ化できます。ECMP 負荷分散により、次のことが保証されます

- 複数の等価コスト接続でのトラフィックの分散。
- 利用可能な帯域幅の最適な使用。
- ルートが到達不能になった場合、他の ECMP メンバールートへのトラフィックのダイナミック転送。
- ECMP は、IPsec/GRE トンネルでスタティックルートをサポートします。
- ECMP グループは、仮想パスおよびイントラネットサービス経路で形成できます。

[NSSDW-1238]

プラットフォームとシステム

Citrix Hypervisor 8.2

Citrix SD-WAN は、11.4.0 以降の Citrix Hypervisor 8.2 でサポートされています。

[NSSDW-32037]

Office 365 のカテゴリ

Citrix SD-WAN 11.4.0 では、[Office **365** を許可する] カテゴリと [最適化] カテゴリをより細かく分類し、ネットワークに依存する Office 365 トラフィックのパフォーマンスを改善するための選択的なブッキングを可能にします。ネットワークに依存するトラフィックを、クラウドの SD-WAN (クラウドダイレクトまたは Azure 上の SD-WAN VPX)、または自宅の SD-WAN デバイスから近くのある SD-WAN に、より信頼性の高いインターネット接続で転送することで、QoS と優れた接続復元性を実現します。トラフィックを最寄りのトラフィックにステアリングする場合と比べて、QoS と優れた接続復元性を実現します。Office 365 フロントドア、レイテンシーの増加を犠牲に。QoS を備えた予約済み SD-WAN ソリューションは、VoIP ドロップアウトと切断を減らし、ジッタを減らし、Microsoft Teams のメディア品質平均オピニオンスコアを向上させます。

最適化カテゴリは、次のサブカテゴリに分類されます。

- Teams リアルタイム
- Exchange Online
- SharePoint 最適化

[許可] カテゴリは、次のサブカテゴリに分類されます。

- Teams TCP フォールバック
- メールを交換する

- SharePoint 許可
- Office365 共通

[NSSDW-27324]

高可用性と高スループットを備えた SD-WAN SE の Google Cloud Platform サポート

Google Cloud Platform (GCP) で SD-WAN SE インスタンスを高可用性に設定できるようになりました。GCP 上の SD-WAN インスタンスは、1 Gbps のより高いスループットもサポートします。

[NSSDW-17179]

有線 802.1X 認証

有線 802.1X は、LAN リソースにアクセスする前にクライアントの認証を要求する認証メカニズムです。Citrix SD-WAN Orchestrator サービスは、LAN インターフェイスでの有線 802.1X 認証の構成をサポートします。

Citrix SD-WAN ネットワークでは、クライアントは認証要求を Citrix SD-WAN アプライアンスに送信し、LAN リソースにアクセスします。Citrix SD-WAN アプライアンスはオーセンティケーターとして機能し、認証要求を認証サーバーに送信します。Citrix SD-WAN Orchestrator サービスは、認証サーバーとして構成される RADIUS サーバーのみをサポートします。

[NSSDW-1921]

解決された問題

リリース 11.4.0a で対処された問題。

構成と管理

いくつかのネットワークオブジェクトを追加した後、設定の監査とエクスポートが失敗しました。問題は修正されました。

[SDWANHELP-2041]

許可されたメモリリソースに制限があるため、Citrix SD-WAN アプライアンスから Citrix SD-WAN Center への大規模なネットワーク構成のインポートに失敗しました。問題は修正されました。

[SDWANHELP-2034]

Citrix SD-WAN の電子メール通知により、認証コマンドに余分な **CR** '文字が追加され、SMTP セッションが終了します。

[SDWANHELP-2028]

大規模ネットワークのデータベースアーカイブ中、MCN アプライアンス上の統計レコードが数分間、統計データベーステーブルに挿入されませんでした。

[SDWANHELP-1872]

インターフェイスの変更中、VRRP は古いインターフェイスデータを使用することがあり、その結果、コアダンプが発生する可能性があります。

[SDWANHELP-1867]

ファイアウォール仮想マシンがシャットダウン状態の場合、ローカル GUI でホストされたファイアウォール設定が読み込まれません。

[SDWANHELP-1839]

仮想 IP アドレスの構成中に、バックアップ管理ネットワークを **[なし]** として選択することはできません。

[SDWANHELP-1824]

[パブリック **IPv4** アドレス] フィールドが、構成エディターの **[基本]** セクションの下にグレー表示されました。

[SDWANHELP-1780]

ブランチオフィスの WAN リンクでパブリック IP アドレスの学習が有効になっている間、RCN は新しいパブリック IP アドレスを学習せず、次の場合にデッドパスになる可能性があります。

- ブランチと RCN の間に設定バージョンの不一致があります
- ブランチ WAN リンクのパブリック IP アドレスが変更されました

[SDWANHELP-1580]

アプライアンス管理ポートが DHCPv4 で構成されている場合、静的 IPv4 アドレスへの切り替えは失敗します。

[NSSDW-35630]

アプライアンスに DHCP IPv4 アドレスと DHCP IPv6 アドレスの両方が設定されていて、ネットワークに DHCP IPv6 サーバのみが設定されている場合、アプライアンスは DHCP IPv4 アドレスを待機し続けるため、IPv6 アドレスも割り当てられません。

[NSSDW-33741]

リージョナルコントロールノード (RCN) ネットワーク用に作成された自動生成されたサマリールートには、65534 ではなく 30,000 のコストが割り当てられます。

[NSSDW-32629]

Citrix SD-WAN Center からプッシュしたときに、アプライアンス設定が Citrix SD-WAN に適用されない。

[NSSDW-32257]

レガシー UI から外部モデムの有効化と無効化が機能しない。

[NSSDW-32221]

構成中に監査エラーが発生すると、すべての WAN リンクに同じ IP タイプのアクセスインターフェイスが設定されていない限り、ユーザーはサイト上でインターネットサービスを構成できなくなります。

[NSSDW-32185]

DHCP クライアントとして設定された WAN リンクは、仮想パスの障害につながります。この問題は、WAN リンクの名前が変更され、変更管理の影響を受けた場合に発生します。

[NSSDW-32110]

ライセンス

Citrix SD-WAN 110 および 210 プラットフォームでは、管理ポートがデータポートとして構成されている場合、新しいバージョンへのアップグレード後にホスト **ID** が変更されることがあります。この問題が発生した場合、SD-WAN アプライアンスは猶予ライセンスを使用します。

[SDWANHELP-186]

その他

複数の HA インターフェイスを使用してサイトのクローンを作成する場合、2 番目の HA インターフェイスの IP アドレスはクローンされません。

[SDWANHELP-2005]

Citrix SD-WAN Center の GUI ログが過剰なディスク容量を消費するため、アップグレードと STS 障害が発生します。

[SDWANHELP-1960]

フルスクリーンモードでブラウザで Citrix SD-WAN Center 11.3.0 ログインページを表示すると、Citrix ロゴと製品名が正しく表示されません。

[SDWANHELP-1910]

ネットワーク管理者ロールには、ネットワーク管理者ロールの定義に従って許可されてはならないセキュリティ管理者ロール固有のアクティビティを実行するアクセス権があります。

[SDWANHELP-1906]

Citrix SD-WAN Center での大規模なネットワーク構成（構成ファイルサイズが 16MB を超えている場合）** のインポートとエクスポートが失敗しました **。

[SDWANHELP-1787]

Citrix SD-WAN センターの電子メール通知では、認証コマンドに余分な **CR** 文字が追加され、SMTP セッションが終了します。

[SDWANHELP-1736]

Qualys セキュリティスキャナーツールにより、Citrix SD-WAN アプライアンスのサービスの 1 つが大量のメモリを消費し、アプライアンスの応答不能と再起動につながりました。問題は修正されました。

[SDWANHELP-1530]

Edge Security のウイルス対策およびマルウェア対策コンポーネントの内部ライセンスの有効期限が切れると、Citrix SD-WAN はウイルスとマルウェアの検出を停止します。

[NSSDW-35596]

再認証を実行すると、Wi-Fi クライアントレポートにアップロードおよびダウンロードデータの負の値が表示されません。

[NSSDW-31903]

11.2.1 または 11.2.2 ソフトウェアに付属する SD-WAN アプライアンスをオンプレミスの Citrix SD-WAN Orchestrator で管理するには、SD-WAN アプライアンスソフトウェアを 11.3.0 バージョンにアップグレードする必要があります。

[NSSDW-31612]

ネットワーク

Citrix SD-WAN 11.3.1 にアップグレードした後、最大伝送ユニット (MTU) サイズが 1492 バイトに設定されていると、MSS (最大セグメントサイズ) クランプが PPPoE で失敗します。

[SDWANHELP-2048]

帯域内管理が有効で、データプレーンを介して RADIUS サーバにアクセスできる場合、Wi-Fi WPA2-エンタープライズ認証が失敗します。

[SDWANHELP-2032]

アプリケーションルーティング、QoS、または DNS 機能のアプリケーション ID 関連エントリは、FPC (FPC) ハッシュテーブルに定期的に追加されます。エージドアウトエントリがテーブルから削除されると、場合によっては、Citrix SD-WAN アプライアンスがクラッシュする可能性があります。

[SDWANHELP-1980]

LAN 側またはローカルサービスで受信したパケットが LAN GRE 経由で送信されると、SD-WAN サービスがクラッシュします。

[SDWANHELP-1846]

パス MTU 検出の場合、パス MTU プローブイベントは、タイマーキックオフ中に処理のためにキューに入れられます。セグメンテーションの失敗は、実際の実行を試みたときにプロブイベントが有効でない場合に発生します。

[SDWANHELP-1754]

デフォルト以外のルーティングドメイン内のインターネットサービスルートおよびパスの適格性が設定されている場合、パスがダウンし、所定のルーティングドメインが設定されていないリモートサイトでは、インターネットルートは到達不能としてマークされません。

[SDWANHELP-1400]

サマリールートを含む Citrix SD-WAN 構成がロードされると、アプライアンスが継続的にリロードされることがあります。

[NSSDW-34670]

アプライアンスにサマリールートとして設定されたスタティックルートがあり、動的に学習された別の同じプレフィックスルートがある場合、サマリールートはルートを集計していません。

[NSSDW-34355]

インポートフィルタを追加して、以前にインポートした OSPF/BGP ルートを削除するとサービスクラッシュが発生する可能性があります。

[NSSDW-34207]

SLAAC がルータから IP とゲートウェイアドレスを学習すると、現在のアドレスが期限切れになるまで、ゲートウェイが変更されたり、ネットワークセグメントが変更されたりしても、SD-WAN アプライアンスの再起動後であっても、SLAAC は IP を再学習しません。これにより、ポートの移動時にアドレスの取得が遅れる可能性があります。

[NSSDW-33807]

SLAAC がルータから IP アドレスとゲートウェイアドレスを学習すると、ゲートウェイが変更されても（現在のアドレスが期限切れになるまで）、SLAAC はゲートウェイを再学習しません。

例：

- ブランチアプライアンスは、ゲートウェイ 1 から IP とゲートウェイを学習します。
- ネットワーク管理者は、ゲートウェイ 1 を新しいゲートウェイ 2 に置き換えることにします。管理者は、ゲートウェイ 2 を Gateway-1 と同じ設定し、ルータアダプタイズメントから Gateway-1 が送信したのと同じプレフィックス情報を送信します。ただし、ゲートウェイ 2 の送信元アドレスはゲートウェイ 1 とは異なります。
- ブランチアプライアンスは、ゲートウェイ 2 の IP を自動的に学習しません。（現在のアドレスがタイムアウトしない限り）

[NSSDW-33802]

構成を更新すると、プレフィックス委任 LAN 仮想ネットワークインターフェイスでホストされている DHCP サーバーが起動しない場合があります。プレフィックス委任は、Citrix SD-WAN 11.3.1 リリースではサポートされていません。

[NSSDW-33664]

プロキシ NDP を使用してインターネットまたはイントラネットサービスでスタティック NAT を有効にすると、ネットワーク内の他のホストが所有および使用するアドレスに対して SD-WAN が NDP に応答することがあります。

[NSSDW-33653]

アンダーレイサイトの診断帯域幅テストは、Citrix SD-WAN 11.3.1 リリースではサポートされていません。

[NSSDW-33597]

IPv6 アクセスインターフェイスを備える WAN リンクでインターネットサービスを有効にすると、構成の更新後にサービスが中断されることがあります。

[NSSDW-32212]

Wi-Fi 機能は、Citrix SD-WAN 11.3 リリースでは、高可用性 (HA) をサポートしていません。

[NSSDW-32197]

インターネット負荷分散が有効になっているインターネットサービスで IPv4 と IPv6 の両方で使用すると、ダイナミック NAT が正しく機能しないか、または構成の更新中にサービスが中断されることがあります。

[NSSDW-32139]

LTE インターフェイスの DHCPv4 および DHCPv6 モードでは、設定の更新後に SD-WAN デバイスの IP アドレスが失われることがあります。

[NSSDW-31998]

プラットフォームとシステム

Citrix SD-WAN 4000 アプライアンスを 11.3.0、11.3.1、または 11.4.0 にアップグレードすると、競合状態が原因で SD-WAN サービスが失敗することがあります。

[SDWANHELP-2016]

フィルタポリシールールの検証は、設定の更新中に実行され、新しく作成されたルールと変更されたルールを区別します。「match_type」の比較チェックがないため、インターネットへの接続の大部分は「O_DENIED」としてファイアウォールによってブロックされています。回避策は、デフォルトのルールを「拒否」から「ドロップ」に変更することです。

[SDWANHELP-2078]

HDX レポートが有効で、Citrix SD-WAN アプライアンスを介して HDX トラフィックが実行されている場合、Citrix SD-WAN アプライアンスがコアダンプを監視することがあります。

[SDWANHELP-1957]

CLI を使用してファイアウォール NAT 情報をダンプすると、アプライアンスがクラッシュします。

[SDWANHELP-1901]

トランスペアレントな DSN 転送が有効の場合、大きな DNS 応答パケットの処理によって、適切な境界条件チェックが行われなために、スタックオーバーフローが発生する可能性があります。使用例の 1 つは、Office 365 の既定のカテゴリの分類を有効にするために、クラウドサービスが DNS から IP を学習する必要がある場合です。

[SDWANHELP-1891]

ファイアウォールルールは、信頼できないインターフェイスで受信した ICMP ping 要求を許可しますが、ping 応答をドロップするため、SD-WAN サービスがクラッシュします。

[SDWANHELP-1865]

Citrix SD-WAN デバイスを 11.2.2 バージョンにアップグレードすると、SD-WAN デバイスから送信された VRRP アドバタイズメントパケットサイズが正しくないため、複数の **VRRP** デバイスがマスターとして機能します。

[SDWANHELP-1804]

ダイナミック仮想パス（DVP）の作成中に、プロトコルメッセージが予期しない IP タイプオブサービス（TOS）値で到着すると、コアダンプが発生する可能性があります。

[SDWANHELP-1783]

同じサブネットに 2 つの仮想 IP アドレス（1 つのプライベート、もう 1 つは非プライベート）が作成されると、同じサブネットに対して 2 つのルートが作成され、サブネットがリモートサイトにアドバタイズされないという問題が発生します。

[SDWANHELP-1739]

GRE トンネルの到達可能性が UP から Down に変更された場合、GRE トンネル適格である GRE トンネルルートは、到達可能性ステータスの変更によって更新されません。

[SDWANHELP-1623]

コマンドラインインターフェイス（CLI）を使用して開始された SSH セッションでは、ハードコードされたアイドルタイムアウト値は 120 分でした。タイムアウト期間の長い時間は、SSH セッションがタイムアウトしていないかのように見えます。この問題は、SSH タイムアウト値（5 ～9999 分）を設定するための新しい設定を GUI に追加して修正されています。

[SDWANHELP-162]

Azure HA 展開では、セカンダリアクセスインターフェイスが WAN リンク上に構成されている場合、SD-WAN パスは起動しません。

[SDWANHELP-1578]

パケットデータプロトコル（PDP）が IPv4 および（または）IPv6 で有効になっている場合、一部のキャリアは IPv6 データセッションだけを許可します。

[SDWANHELP-177]

既知の問題

リリース 11.4.0a に存在する問題。

構成と管理

規則の設定に使用されたアプリケーションが非推奨の場合、アップグレード後に GUI は異なるアプリケーションで同じ規則を表示します。

[NSSDW-34618]

帯域外管理インターフェイスが接続されている場合は、アプライアンス UI からのみ DNS 設定を更新できます。

帯域内管理が構成されている場合、アプライアンス UI を使用して更新された DNS 設定は有効になりません。DNS 設定は、Citrix SD-WAN Orchestrator サービスの UI からのみ更新できます。

[NSSDW-33932]

新しくプロビジョニングされた仮想マシンを最初にダウングレードしてから、仮想マシンがプロビジョニングされたバージョンにアップグレードすると、VPX ブランチはシングルサイトモードになります。

回避策:

影響を受けるブランチでローカル変更管理を実行します。

[NSSDW-29513]

その他

Citrix SD-WAN Center で新しいローカルユーザーを追加すると、黄色のバナーが表示され、** ファイアウォール アクセスが有効から無効に変更されたことを示すメッセージが表示されます **。

[SDWANHELP-1737]

WPA3 失敗した認証は、サイトレベルのアラートでは報告されません。

[NSSDW-32053]

ネットワーク

SD-WAN サイトでのルートテーブルの頻繁な変更と、設定の更新またはダイナミックルートの削除により、リモート サイトでルート同期の問題が発生する可能性があります。

[SDWANHELP-2043]

ファイアウォールのダイナミック NAT ポリシーまたはポートフォワーディングルールに対して設定を変更すると、コアダンプが発生する可能性があります。

[NSSDW-34603]

プラットフォームとシステム

次のプラットフォームでは、HDX レポートが有効になっているときに、接続を HDX に分類して統計レポートを開始した後に解析エラーが発生すると、新しい HDX 接続があるときにアプライアンスがクラッシュします。

- Citrix SD-WAN 2100
- Citrix SD-WAN 4100

- Citrix SD-WAN 5100
- Citrix SD-WAN 6100

[SDWANHELP-182]

Citrix SD-WAN 110 SE ネットワークの問題のトラブルシューティング

November 8, 2021

このセクションでは、Citrix SD-WAN 110 SE アプライアンスのネットワーク接続の問題と、トラブルシューティング手順について説明します。

現象

Citrix SD-WAN 110 SE アプライアンスは、次の条件下でネットワーク接続を確立できません。

- アプライアンスは SD-WAN Orchestrator によって管理されるか、ゼロタッチ展開（ZTD）によって起動されます。
- アプライアンスは工場出荷時の状態であり、ZTD/SD-WAN オークストレータエージェントはインストールされていません。
- アプライアンスの時間（CMOS またはハードウェア）が実際の時間より前です。
- アプライアンスの時間は、ZTD/SD-WAN Orchestrator エージェントのダウンロード/インストールの前に、NTP デモンによって逆方向に設定されます。

回避方法

初期インストール後（またはユニットを工場出荷時の設定にリセットした後）、SD-WAN 110 をインストールするエンドユーザーは、アプライアンスが組織ネットワークに正常に接続されていることを確認する必要があります。エンドユーザーは、ネットワーク接続を確認するために、アプライアンスと一緒に組織固有の指示（VoIP 電話機のダイヤルトーンなど）を提供する必要があります。アプライアンスがネットワークに接続しない場合、エンドユーザーは下記の指示に従うことができます。

1. アプライアンスの電源を入れたままにして、30 分以上待ちます。
2. 電源ボタン（1～2 秒）を短く押してシャットダウンします。
3. アプライアンスのライトが暗くなったら、もう一度電源ボタンを押してアプライアンスの電源を入れ直します。
SD-WAN 110 アプライアンスが再起動し、ネットワークに接続します。

Citrix SD-WAN 11.4.1 リリースのリリースノート

November 8, 2021

このリリースノートでは、Citrix SD-WAN リリース 11.4.1 における機能強化と変更、修正および既知の問題について説明します。

メモ

このリリースノートには、セキュリティ関連の修正は含まれていません。セキュリティに関する修正とアドバイスの一覧については、Citrix セキュリティ情報を参照してください。

新機能

リリース 11.4.1 で使用可能な機能強化と変更。

構成と管理

DHCP サーバ

仮想インターフェイスごとに 1 つのリレーエージェントがスポンサーされ、リレーエージェントごとに合計 16 の DHCP サーバを設定できます。サイトには最大 16 のリレーエージェントを設定できます。

[NSSDW-34083]

DHCP クライアントメッセージでオプション 12 として使用されるホスト名

Citrix SD-WAN リリース 11.4.1 以降では、ホスト名はサイト名と同じです。管理インターフェイスが DHCP クライアントとして動作している場合、ホスト名はオプション 12 として DHCP クライアントメッセージで使用されます。Citrix SD-WAN リリース 11.2.3 以降、リリース 11.4.1 までは、ホスト名は **sdwan** として設定されていました。

[NSSDW-32523]

プラットフォームとシステム

AT コマンド

LTE をサポートする Citrix SD-WAN プラットフォームモデルは、AT コマンドの実行をサポートします。AT コマンドは、LTE モデムの設定とステータスのモニタリングとトラブルシューティングに役立ちます。

[NSSDW-35671]

シェルコマンドへのアクセス

`shell` コマンドは、CBVWSSH スタティックアカウントのログインクレデンシャルの入力を求められることなく、SD-WAN CLI コンソールで直接実行できます。この機能は、CBVWSSH アカウントのハードコードされたパスワードを削除し、より安全な方法を使用して置き換えるため、SD-WAN アプライアンスのセキュリティを強化します。この機能は、管理者アカウントユーザーに対してのみサポートされています。

[NSSDW-34942]

参考資料-アプリケーション署名ライブラリ

DPI アプリケーション署名ライブラリが更新されました。

[NSSDW-34527]

解決された問題

リリース 11.4.1 で解決された問題。

構成と管理

Citrix SD-WAN Center では、すべての属性がフェッチされ、選択した時間間隔が 1 時間を超えると、パスおよび仮想パスのレポート API が失敗します。

[SDWANHELP-2231]

まれなシナリオでは、Citrix SD-WAN アプライアンスが内部プロセスの問題により管理アクセスを失うことがあります。

[SDWANHELP-2179]

LTE インターフェイスを使用してサイトのクローンを作成する場合、UI は LTE WAN リンクアクセスインターフェイスの静的 IP アドレスを入力する必要があります。監査時には、設定が正しくないと見なされ、次の監査エラーが表示されます。

EC601、EC343、EC346

[SDWANHELP-2177]

Citrix SD-WAN Center から構成をエクスポートするたびに、**tmp** フォルダー内の一時ファイルがクリーンアップされませんでした。

[SDWANHELP-2057]

Citrix SD-WAN UI は、[構成] > [仮想 **WAN**] > [構成の表示] > [パス] にパス構成を完全に表示しません。一部のパスだけが表示され、他のパスは非表示になります。

[SDWANHELP-2050]

AppFlow が有効な HDX セットアップで TCP オプションを追加すると、TCP 接続が確立されません。

[SDWANHELP-1741]

アプライアンス管理ポートが DHCPv4 で構成されている場合、静的 IPv4 アドレスへの切り替えは失敗します。

[NSSDW-35630]

この問題は、ユーザーがモデムを無効にしており、動作モードが **Lower Power** に切り替わる前にモデムを再度有効にしたい場合に発生します。

修正は、有効化/無効化操作を実行する前に、ユーザーに警告し、現在の **Operating Mode** を表示することです。

[NSSDW-25067]

インストールとアップグレード

MPLS WAN リンクが WAN リンクテンプレートを使用するように設定され、イントラネット/インターネットサービスに対して有効になっている場合、設定のコンパイル中に予期しない監査エラー EC14203 が発生します。

Citrix SD-WAN 11.3.1 以前のリリースでは、WAN リンク許可レートが、WAN リンクテンプレートを使用して MPLS WAN リンクを構成しているときに、WAN リンクを使用するすべてのサービスに必要な最小予約帯域幅よりも低い値に設定されている場合、エラーがスローされないことがあります。Citrix SD-WAN 11.3.2 以降のリリースにアップグレードすると、エラーが表示されます。アップグレードを実行する前に、正しい WAN リンク許可レートを設定し、設定をアクティブにします。

[SDWANHELP-2134]

その他

Citrix SD-WAN Center 監視 REST API は、WAN リンク統計がクエリされるときに機能しません。

[SDWANHELP-2274]

新しい構成が Citrix SD-WAN Center にインポートされると、Zscaler 構成はインポートされません。

[SDWANHELP-2137]

Edge Security のウイルス対策コンポーネントおよびマルウェア対策コンポーネントの内部ライセンスの有効期限が切れると、Citrix SD-WAN はウイルスとマルウェアの検出を停止します。

[NSSDW-35596]

ネットワーク

GRE フローに IPv4 送信元 IP アドレスと IPv6 宛先 IP アドレスがある場合、IPv4 GRE トンネルトラフィックは [**モニタリング**] > [フロー (**Flows**)] で IPv6 トンネルとして誤って分類され、ブロックされる可能性があります。

[SDWANHELP-2214]

Citrix SD-WAN 11.3.1 にアップグレードした後、最大伝送ユニット（MTU）サイズが 1492 バイトに設定されていると、MSS（最大セグメントサイズ）クランプが PPPoE で失敗します。

[SDWANHELP-2048]

SD-WAN サイトでのルートテーブルの頻繁な変更と、設定の更新またはダイナミックルートの削除により、リモートサイトでルート同期の問題が発生する可能性があります。

[SDWANHELP-2043]

Citrix SD-WAN アプライアンスが新しいポートの検出に失敗すると、WAN リンクパスの状態が **DEAD** に移行します。

[SDWANHELP-1998]

まれに、ルーティングテーブルにルート変更があると、Citrix SD-WAN サービスがリロードされます。

[NSSDW-36289]

CRL 処理が有効になっている場合、サードパーティの暗号化ライブラリのメモリの問題により、コアダンプが発生する可能性があります。

[NSSDW-35679]

サマリールートを含む Citrix SD-WAN 構成がロードされると、アプライアンスが継続的にリロードされることがあります。

[NSSDW-34670]

次のシナリオでは、2 つのサイト間のスタティック仮想パスを削除しても、削除されたスタティック仮想パスを経由して学習されたルートは削除されません。

- 静的仮想パスは、設定変更の一部として削除されます。
- 新しい Geo-MCN をクライアントにすると、古い Geo MCN とブランチ間の静的仮想パスは削除されます。

[NSSDW-34655]

プラットフォームとシステム

動的仮想パス（DVP）が起動している間に STS バンドルが生成されると、Citrix Virtual WAN サービスが再起動することがあります。

[SDWANHELP-2123]

Citrix SD-WAN 4000 アプライアンスを 11.3.0、11.3.1、または 11.4.0 にアップグレードすると、競合状態が原因で SD-WAN サービスが失敗することがあります。

[SDWANHELP-2106]

レガシー UI ダッシュボードの [システムステータス] セクションには、サイト名に [完了] 文字列が含まれていると、次のエラーメッセージが表示されます。

Unable to obtain system data because the system is busy. Click Refresh to retry.

[SDWANHELP-2098]

フィルタポリシー ルールの検証は、設定の更新中に実行され、新しく作成されたルールと変更されたルールを区別します。**match_type** の比較チェックがないため、インターネットへの接続のほとんどは **O_DENIED** としてファイアウォールによってブロックされています。

[SDWANHELP-2078]

アプリケーションルートのリアルタイム統計情報が SD-WAN Orchestrator または SD-WAN ブランチデバイスから取得されると、デバイスの接続が失われ、クラッシュが観察されます。これは、アプリケーションルートが 16 を超える場合にのみ発生します（自動生成されたアプリケーションルートを含む）。

[SDWANHELP-2066]

既知の問題

リリース 11.4.1 に存在する問題。

構成と管理

[モニタリング (**Monitoring**)] > [フロー (**Flows**)] ページに表示されている列を切り替えるオプションは、期待どおりに機能していません列を選択またはフィルタリングしても、次のメッセージが表示されます。

Please select at least one column.

[SDWANHELP-2272]

その他

Zscaler 構成変更管理プロセスのタイムアウト期間は 2 時間です。設定エラーが発生すると、プロセス全体が 2 時間停止します。

[SDWANHELP-2249]

WPA3 失敗した認証は、サイトレベルのアラートでは報告されません。

[NSSDW-32053]

ネットワーク

まれに、ブランチサイトに静的パブリック IP アドレスを持つ WAN リンクの 1 つがある場合、ダイナミック仮想パスの形成は失敗します。

回避策: ブランチサイトの仮想 WAN サービスを静的パブリック IP アドレスで再起動します。

[NSSDW-36429]

Citrix SD-WAN BGP 構成で、ルーティングドメインのルーター ID が変更されると、SD-WAN 動的ルーティングプロトコルが再起動することがあります。

[NSSDW-35657]

ファイアウォールのダイナミック NAT ポリシーまたはポートフォワーディングルールに対して設定を変更すると、コアダンプが発生する可能性があります。

[NSSDW-34603]

プラットフォームとシステム

LTE モデムは、QMI プロキシプロセスが機能していない状態のままで継続的に再起動します。

回避策: アプライアンスを再起動します。

[SDWANHELP-2270]

Citrix SD-WAN 11.4.2a リリースのリリースノート

February 8, 2022

このリリースノートドキュメントでは、Citrix SD-WAN リリース Build 11.4.2a に存在する機能強化と変更、修正された問題と既知の問題について説明します。

メモ

- セキュリティに関する修正とアドバイスの一覧については、Citrix セキュリティ情報を参照してください。
- Citrix SD-WAN 11.4.2a リリースは <https://support.citrix.com/article/CTX330728> で説明されているセキュリティの脆弱性に対処し、リリース 11.4.2 に代わるものです。リリース 11.4.2 で利用可能だった機能強化とバグ修正に加えて、リリース 11.4.2a には SDWANHELP-2480 および SDWANHELP-2456 のバグ修正が含まれています。

新機能

ビルド 11.4.2a で利用できる機能強化と変更。

その他

帯域内管理

Citrix SD-WAN 11.4.2a リリース以降、SD-WAN アプライアンスでインバンド管理を構成し、インバンド管理ポートを介して Citrix SD-WAN Orchestrator サービスへの接続を確立する必要があります。そうしないと、管理ポートが接続されておらず、インバンド IP アドレスも構成されていないと、アプライアンスは Citrix SD-WAN Orchestrator サービスへの接続を失います。

[NSSDW-37174]

LTE インターフェイス

Citrix SD-WAN Orchestrator サービスを使用して、LTE インターフェイスベースの WAN リンクをプライベートイントラネット WAN リンクとして構成できるようになりました。この機能強化により、LTE インターフェイスをパブリックインターネット WAN リンクまたはプライベートイントラネット WAN リンクとして柔軟に構成できます。

[NSSDW-37064]

オーケストレータ接続ステータス

SD-WAN ダッシュボードの [新しい UI] には、次の Orchestrator 接続ステータスが表示されます。

- オンラインステート
- サービス状態
- DNS 状態
- ローカルゲートウェイの状態
- 失敗した理由
- 接続経由

[NSSDW-36434]

プラットフォームとシステム

ドメインとアプリケーション

ドメイン名ベースのアプリケーションで、Citrix SD-WAN Orchestrator サービスで構成可能なポートとプロトコルがサポートされるようになりました。[**Configure Port**] チェックボックスをオンにすると、必要に応じて任意のポートまたはポート範囲を編集、追加、または削除できます。また、プロトコルを [TCP]、[UDP]、または [任意] に変更または選択できます。以前は ([**Configure Port**] チェックボックスをオフにして)、アプリケーションの下にグループ化されたドメインでは、ポート 80 と 443、およびプロトコル **Any** のみがサポートされていました。

[NSSDW-29930]

解決された問題

ビルド 11.4.2a で対処された問題。

その他

ドメイン名ベースのアプリケーションの DNS 学習エントリにより、最初のパケット分類テーブルが上限に達すると、アプライアンスがクラッシュします。

[SDWANHELP-2480]

フローの数が常に多く、アプライアンスの最大フローキャパシティ制限を超えている場合、フローマッピングの変更によりデータベースが再起動することがあります。

[SDWANHELP-2456]

HA 制御パスなど、VLAN タグ付きの暗号化されていないパスの場合、一部の SD-WAN 制御パケットが不正なイーサネットヘッダーで送信され、パスが不安定になったり、使用不能になったりしていました。

[SDWANHELP-2384]

ブランチなしでスタンドアロン RCN をデプロイすると、監査エラー ID が表示される。

[SDWANHELP-2381]

Citrix SD-WAN Orchestrator サービスからインターネットサービスの ICMP プローブを有効にすると、インターネット WAN リンクがダウンすると、次のアプライアンスで SD-WAN サービスが再起動されます。

- Citrix SD-WAN 2100
- Citrix SD-WAN 4100
- Citrix SD-WAN 5100
- Citrix SD-WAN 6100

[SDWANHELP-2378]

Citrix SD-WAN Center ダッシュボードに情報が読み込まれません。

[SDWANHELP-2373]

変更管理プロセスを通じて MCN からネットワークアプライアンスに変更をプッシュしている間、アプライアンスの SD-WAN サービスは約 2 分間アプライアンスの切断を再開しました。

[SDWANHELP-2366]

Citrix SD-WAN 5100 モデルの LAG グループを構成できません。

[SDWANHELP-2339]

PE をサポートする Citrix SD-WAN アプライアンスモデルで PAC ファイルをダウンロードできません。

[SDWANHELP-2336]

パス暗号化がオフになっていると、パスで高い MTU と損失が観察されます。

[SDWANHELP-2327]

SD-WAN Orchestrator HA セットアップで、アプライアンスソフトウェアを 11.3.0 より前のバージョンから 11.4.1、11.3.2 以下にアップグレードすると、スタンバイアプライアンスがクラッシュします。

[SDWANHELP-2315]

他のリモートサイトとの仮想パスが無効で、WAN リンクがスタンバイモードに設定され、ハートビートが無効になっているサイトでは、パケット損失が徐々に増加しています。

[SDWANHELP-2276]

[モニタリング (**Monitoring**)] > [フロー (**Flows**)] ページに表示されている列を切り替えるオプションは、期待どおりに機能していません列を選択またはフィルタリングしても、次のメッセージが表示されます。

列を少なくとも 1 つ選択してください。

[SDWANHELP-2272]

LTE モデムは、QMI プロキシプロセスが機能していない状態のままで継続的に再起動します。

[SDWANHELP-2270]

TACACS+ 認証を使用して SD-WAN への SSH 接続が確立されると、同じユーザに対する複数の認証要求が送信され、過剰なロギングが発生します。

[SDWANHELP-2087]

SMTP サーバー名が FQDN として設定されている場合、電子メール通知は送信できません。この問題は、DNS サーバに次のものが含まれている場合に発生します。

- FQDN の少なくとも 2 つの IPv4 A レコード。
- 少なくとも 1 つの FQDN の IPv6 AAAA レコード。

[SDWANHELP-2027]

まれに、ルーティングテーブルにルート変更があると、Citrix SD-WAN サービスがリロードされます。

[NSSDW-36289]

CRL 処理が有効になっている場合、サードパーティの暗号化ライブラリのメモリの問題により、コアダンプが発生する可能性があります。

[NSSDW-35679]

Edge Security のウイルス対策コンポーネントおよびマルウェア対策コンポーネントの内部ライセンスの有効期限が切れると、Citrix SD-WAN はウイルスとマルウェアの検出を停止します。

[NSSDW-35596]

サマリールートを含む Citrix SD-WAN 構成がロードされると、アプライアンスが継続的にリロードされることがあります。

[NSSDW-34670]

アプライアンスにサマリールートとして設定されたスタティックルートがあり、動的に学習された別の同じプレフィックスルートがある場合、サマリールートはルートを集計していません。

[NSSDW-34355]

ネットワーク上の DNS プロキシに重複する名前が使用されている場合、Citrix SD-WAN UI にエラーが表示される。

[NSSDW-33842]

SLAAC がルータから IP とゲートウェイアドレスを学習すると、現在のアドレスが期限切れになるまで、ゲートウェイが変更されたり、ネットワークセグメントが変更されたりしても、SD-WAN アプライアンスの再起動後であっても、SLAAC は IP を再学習しません。これにより、ポートの移動時にアドレスの取得が遅れる可能性があります。

[NSSDW-33807]

SLAAC がルータから IP アドレスとゲートウェイアドレスを学習すると、ゲートウェイが変更されても（現在のアドレスが期限切れになるまで）、SLAAC はゲートウェイを再学習しません。

例：

- ブランチアプライアンスは、ゲートウェイ 1 から IP とゲートウェイを学習します。
- ネットワーク管理者は、ゲートウェイ 1 を新しいゲートウェイ 2 に置き換えることにします。管理者は、ゲートウェイ 2 を Gateway-1 と同じ設定し、ルータアダプタイズメントから Gateway-1 が送信したのと同じプレフィクス情報を送信します。ただし、ゲートウェイ 2 の送信元アドレスはゲートウェイ 1 とは異なります。
- ブランチアプライアンスは、ゲートウェイ 2 の IP を自動的に学習しません。（現在のアドレスがタイムアウトしない限り）

[NSSDW-33802]

リージョナルコントロールノード（RCN）ネットワーク用に作成された自動生成されたサマリールートには、65534 ではなく 30,000 のコストが割り当てられます。

[NSSDW-32629]

Citrix SD-WAN Center からプッシュしたときに、アプライアンス設定が Citrix SD-WAN に適用されない。

[NSSDW-32257]

既知の問題

リリース 11.4.2a に存在する問題。

その他

SD-WAN WANOP UI の [**ICA** 接続] ページにエラーが表示され、ページには接続がないと表示されます。

[SDWANHELP-2431]

SNMP サービスにアウトオブバンドポートを使用するアプライアンスがインバンドポートに切り替わると、アプライアンスのすべての管理サービスはインバンドポートを介してインターネットに接続します。アウトオブバンドポートに送信された SNMP 要求は失敗します。

回避策：アウトオブバンドポートで障害が発生した場合にインバンドポートに要求を送信するように、外部 SNMP サービスを設定します。

[SDWANHELP-2358]

VMware ハイパーバイザーに Citrix SD-WAN VPX をインストールできません。Citrix SD-WAN VPX は、AMD Opteron (tm) またはそれ以前のバージョンの AMD プロセッサではサポートされていません。Citrix SD-WAN は AMD EPYC プロセッサでのみ認定され、推奨されています。

[SDWANHELP-2309]

UI の [Monitoring classes] テーブルに表示されるトラフィックレートは、リアルタイム、インタラクティブハイ、インタラクティブ中、およびインタラクティブ低クラスタイプのトラフィックが同時に開始されると、約 150 Kbps 低くなります。

[NSSDW-37568]

管理ポートで構成された DNS が無効または到達できない場合、インバンドが DNS プロキシとインターネットサービスで構成されていても、DNS 解決エラーのためにアプライアンスは SD-WAN Orchestrator サービスに接続できません。

回避策：管理ポートで有効な DNS を構成するか、DNS をクリアして、デフォルトで構成された DNS (9.9.9.9) を使用するようにします。

[NSSDW-37467]

MCN で管理されている Citrix SD-WAN アプライアンスでは、新しい UI ダッシュボードの Orchestrator の接続状態が「不良/不明」と表示されます。

[NSSDW-37462]

LTE ドングルまたは管理ポートによって提供された DNS に到達できない場合、ネットワークが接続のためにインバンド管理に切り替えられても、Citrix SD-WAN Orchestrator サービスの接続が失敗します。

[NSSDW-37428]

まれに、ブランチサイトに静的パブリック IP アドレスを持つ WAN リンクの 1 つがある場合、ダイナミック仮想パスの形成は失敗します。

回避策：

静的パブリック IP アドレスを使用して、ブランチサイトで Virtual WAN サービスを再起動します。

[NSSDW-36429]

Citrix SD-WAN BGP 構成で、ルーティングドメインのルーター ID が変更されると、SD-WAN 動的ルーティングプロトコルが再起動することがあります。

[NSSDW-35657]

ファイアウォールのダイナミック NAT ポリシーまたはポートフォワーディングルールに対して設定を変更すると、コアダンプが発生する可能性があります。

[NSSDW-34603]

WPA3 失敗した認証は、サイトレベルのアラートでは報告されません。

[NSSDW-32053]

Citrix SD-WAN 11.4.2b リリースのリリースノート

June 8, 2022

このリリースノートのドキュメントでは、Citrix SD-WAN リリースビルド 11.4.2b に存在する機能強化と変更、修正された既知の問題について説明します。

メモ

- このリリースノートには、セキュリティ関連の修正は含まれていません。セキュリティに関する修正とアドバイスの一覧については、Citrix セキュリティ情報を参照してください。
- リリース 11.4.2a で利用可能だった機能強化とバグ修正に加えて、リリース 11.4.2b には次のバグ修正、SDWANHELP-2594 が含まれています。

新機能

ビルド 11.4.2b で使用できる機能強化と変更。

LTE インターフェイス

Citrix SD-WAN Orchestrator サービスを使用して、LTE インターフェイスベースの WAN リンクをプライベートイントラネット WAN リンクとして構成できるようになりました。この拡張により、LTE インターフェイスをパブリックインターネット WAN リンクまたはプライベートイントラネット WAN リンクとして柔軟に構成できます。

[NSSDW-37064]

オーケストレータ接続ステータス

SD-WAN の新しい UI ダッシュボードには、次のオーケストレータ接続ステータスが表示されます。

- オンラインステート
- サービス状態
- DNS 状態

- ローカルゲートウェイの状態
- 失敗した理由
- 接続経由

[NSSDW-36434]

アプライアンスの設定

Citrix SD-WAN Orchestrator サービスには、管理ネットワークの優先順位を構成するオプションが導入されています。ネットワークの管理インターフェイスとして [インバンド] または [アウトオブバンド] を選択できます。このオプションは、SD-WAN アプライアンスが 11.4.2 以降のソフトウェアバージョンを実行している場合にのみ使用できます。

[NSSDW-35774]

オンプレミス向けの SD-WAN Orchestrator との IPv6 管理接続のサポートは、Citrix SD-WAN ソフトウェアバージョン 11.4.2 以降から利用できます。

[NSSDW-35647]

プラットフォームとシステム

ドメイン名ベースのアプリケーションで、Citrix SD-WAN Orchestrator サービスで構成可能なポートとプロトコルがサポートされるようになりました。[**Configure Port**] チェックボックスをオンにすると、必要に応じて任意のポートまたはポート範囲を編集、追加、または削除できます。また、プロトコルを [TCP]、[UDP]、または [任意] に変更または選択できます。以前は (また、[ポートを設定] チェックボックスがオフの場合)、アプリケーションの下にグループ化されたドメインでは、ポート 80 と 443、およびプロトコル **Any** のみがサポートされていました。

[NSSDW-29930]

解決された問題

ビルド 11.4.2b で対処される問題。

サイトまたは WAN リンクの設定変更時に拡張展開を行う場合、ルーティングエンジンを再起動すると、BGP セッションがフラップします。

[SDWANHELP-2594]

ドメイン名ベースのアプリケーションの DNS 学習エントリにより、最初のパケット分類テーブルが上限に達すると、アプライアンスがクラッシュします。

[SDWANHELP-2480]

フローの数が常に多く、アプライアンスの最大フローキャパシティ制限を超えている場合、フローマッピングの変更によってデータパスが再起動することがあります。

[SDWANHELP-2456]

HA 制御パスなど、VLAN タグ付きの暗号化されていないパスの場合、一部の SD-WAN 制御パケットが不正なイーサネットヘッダーで送信され、パスが不安定になったり、使用不能になったりしていました。

[SDWANHELP-2384]

ブランチなしでスタンドアロン RCN をデプロイすると、監査エラー ID が表示される。

[SDWANHELP-2381]

インターネットサービスの ICMP プローブが Citrix SD-WAN Orchestrator サービスから有効になっている場合、次のアプライアンスでインターネット WAN リンクがダウンすると、SD-WAN サービスが再起動されます。

- Citrix SD-WAN 2100
- Citrix SD-WAN 4100
- Citrix SD-WAN 5100
- Citrix SD-WAN 6100

[SDWANHELP-2378]

Citrix SD-WAN Center ダッシュボードに情報が読み込まれません。

[SDWANHELP-2373]

変更管理プロセスを通じて MCN からネットワークアプライアンスに変更をプッシュしている間、アプライアンスの SD-WAN サービスは約 2 分間アプライアンスの切断を再開しました。

[SDWANHELP-2366]

Citrix SD-WAN 5100 モデルの LAG グループを構成できません。

[SDWANHELP-2339]

PE をサポートする Citrix SD-WAN アプライアンスモデルで PAC ファイルをダウンロードできません。

[SDWANHELP-2336]

パス暗号化がオフになっていると、パスで高い MTU と損失が観察されます。

[SDWANHELP-2327]

SD-WAN Orchestrator HA セットアップで、アプライアンスソフトウェアが 11.3.0 より前のバージョンからバージョン 11.4.1、11.3.2 以下にアップグレードされると、スタンバイアプライアンスがクラッシュします。

[SDWANHELP-2315]

他のリモートサイトとの仮想パスが無効で、WAN リンクがスタンバイモードに設定され、ハートビートが無効になっているサイトでは、パケット損失が徐々に増加しています。

[SDWANHELP-2276]

[**モニタリング (Monitoring)**] > [フロー (**Flows**)] ページに表示されている列を切り替えるオプションは、期待どおりに機能していません列を選択またはフィルタリングしても、次のメッセージが表示されます。

列を少なくとも 1 つ選択してください。

[SDWANHELP-2272]

LTE モデムは、QMI プロキシプロセスが機能していない状態のままで継続的に再起動します。

[SDWANHELP-2270]

TACACS+ 認証を使用して SD-WAN への SSH 接続が確立されると、同じユーザに対する複数の認証要求が送信され、過剰なロギングが発生します。

[SDWANHELP-2087]

SMTP サーバー名が FQDN として設定されている場合、電子メール通知は送信できません。この問題は、DNS サーバに次のものが含まれている場合に発生します。

- FQDN の少なくとも 2 つの IPv4 A レコード。
- 少なくとも 1 つの FQDN の IPv6 AAAA レコード。

[SDWANHELP-2027]

Citrix SD-WAN 11.4.2 リリースでは、オンプレミス用 Citrix SD-WAN Orchestrator から署名付き CSR 証明書をアップロードすると、拡張子が.der のファイルに対して失敗します。

[NSSDW-37813]

LTE ドングルまたは管理ポートによって提供された DNS に到達できない場合、ネットワークが接続のためにインバンド管理に切り替えられても、Citrix SD-WAN Orchestrator サービスの接続が失敗します。

[NSSDW-37428]

帯域内管理

Citrix SD-WAN 11.4.2 リリース以降、SD-WAN アプライアンスでインバンド管理を構成し、インバンド管理ポートを介して Citrix SD-WAN Orchestrator サービスへの接続を確立する必要があります。そうしないと、管理ポートが接続されておらず、インバンド IP アドレスも構成されていないと、アプライアンスは Citrix SD-WAN Orchestrator サービスへの接続を失います。

[NSSDW-37174]

DHCP サーバーが DVP および HA 構成で新しいアドレスを割り当てると、Citrix SD-WAN サービスがクラッシュすることがあります。

[NSSDW-36513]

ネットワーク上の DNS プロキシに重複する名前が使用されている場合、Citrix SD-WAN UI にエラーが表示される。

[NSSDW-33842]

プラットフォームとシステム

カスタム SNMP コミュニティストリングを初めて追加しても、既存のコミュニティストリング設定は削除されません。

[SDWANHELP-2561]

既知の問題

リリース 11.4.2b に存在する問題。

その他

部分的なサイトアップグレードを無効にした後にネットワーク全体を新しいソフトウェアバージョンにアップグレードすると、一部のサイトが古いバージョンに自動的に修正されて戻される可能性があります。

回避策: 別の変更管理がトリガーされると、ダウングレードされたサイトは予想されるソフトウェアバージョンにアップグレードされます。

[SDWANHELP-2586]

レガシー GUI は CGI セッションファイルを一時ディレクトリに残します。これらの CGI セッションは起動時にクリーンアップされるため、Citrix SD-WAN サービスの実行が妨げられる可能性があります。

回避策: 電源ボタンを 4 秒以上押してアプライアンスを再起動し、ボックスの電源を再びオンにするか、電源ケーブルを抜いて数秒後に接続し直します。

[SDWANHELP-2567]

Citrix SD-WAN LTE サービスは、LTE モデムのトランザクションタイムアウトエラーが原因でハングすることがあります。

回避策: アプライアンスを再起動します。

[SDWANHELP-2565]

Citrix SD-WAN UI のまれな競合状態が原因で、誤った DB インデックスで統計が要求されると、t2_app がクラッシュします。

[SDWANHELP-2548]

Citrix SD-WAN 1100 上のパロアルト VM (VM-50 モデル) に割り当てられたメモリは、5.5 GB に増加します。

[SDWANHELP-2534]

ICA 分類で発生する可能性があったメモリリークが修正されました。

[SDWANHELP-2527]

Citrix SD-WAN サービスは、インターネット負荷分散構成の Advanced Edition (AE) プラットフォームでクラッシュすることがあります。

回避策: インターネットサービスをプライマリモードとセカンダリモードで構成します。

[SDWANHELP-2521]

Citrix SD-WAN アプライアンスは、管理ポートで必要なトラフィックのみを許可します。これにより、有効になっている場合、ユーザーは miRIC 管理 GUI にアクセスできなくなります。

[SDWANHELP-2479]

プレフィックス付きの **IP** アドレスを入力しようとする、ファイアウォールフィルタポリシーの送信元/宛先 IP フィールドの検証に失敗していました。

[SDWANHELP-2471]

SNMP サービスに帯域外ポートを使用するアプライアンスが帯域内ポートに切り替わると、アプライアンスのすべての管理サービスが帯域内ポートを介してインターネットに接続します。アウトオブバンドポートに送信される SNMP 要求は失敗します。

回避策: アウトオブバンドポートで障害が発生した場合にインバンドポートに要求を送信するように、外部 SNMP サービスを設定します。

[SDWANHELP-2358]

Citrix SD-WAN 11.4.2 リリースでは、オンプレミス用 Citrix SD-WAN Orchestrator から署名付き CSR 証明書をアップロードすると、拡張子が .der のファイルに対して失敗します。

回避策: この問題は、.pem ファイルには適用されません。 .pem 署名付き CSR を使用します。

[NSSDW-37813]

UI の [Monitoring classes] テーブルに表示されるトラフィックレートは、リアルタイム、インタラクティブハイ、インタラクティブ中、およびインタラクティブ低クラスタイプのトラフィックが同時に開始されると、約 150 Kbps 低くなります。

[NSSDW-37568]

MCN で管理されている Citrix SD-WAN アプライアンスでは、新しい UI ダッシュボードの Orchestrator の接続状態が「不良/不明」と表示されます。

[NSSDW-37462]

LTE ドングルまたは管理ポートによって提供された DNS に到達できない場合、ネットワークが接続のためにインバンド管理に切り替えられても、Citrix SD-WAN Orchestrator サービスの接続が失敗します。

[NSSDW-37428]

まれに、ブランチサイトに静的パブリック IP アドレスを持つ WAN リンクの 1 つがある場合、ダイナミック仮想パスの形成は失敗します。

回避策: 静的パブリック IP アドレスを使用して、ブランチサイトで Virtual WAN サービスを再起動します。

[NSSDW-36429]

Citrix SD-WAN BGP 構成で、ルーティングドメインのルーター ID が変更されると、SD-WAN 動的ルーティングプロトコルが再起動することがあります。

[NSSDW-35657]

ファイアウォールのダイナミック NAT ポリシーまたはポートフォワーディングルールに対して設定を変更すると、コアダンプが発生する可能性があります。

[NSSDW-34603]

WPA3 失敗した認証は、サイトレベルのアラートでは報告されません。

[NSSDW-32053]

プラットフォームとシステム

カスタム SNMP コミュニティストリングを初めて追加しても、既存のコミュニティストリング設定は削除されません。

回避策: SNMP v1/v2 を無効にしてから有効にして、既存のコミュニティストリングをクリアします。

[SDWANHELP-2561]

Citrix SD-WAN 11.4.3a リリースのリリースノート

June 8, 2022

このリリースノートドキュメントでは、Citrix SD-WAN リリース Build 11.4.3a に存在する機能強化と変更、修正された問題と既知の問題について説明します。

注

Citrix SD-WAN 11.4.3a リリースは、<https://support.citrix.com/article/CTX370550> で説明されているセキュリティの脆弱性に対処し、リリース 11.4.3 を置き換えます。

新機能

ビルド 11.4.3a で利用できる機能強化と変更。

DHCP ログの強化

Citrix SD-WAN アプライアンスは、IP アドレスの DHCP サーバーログを生成できます。エンドポイントに IP アドレスが割り当てられるたびに、ログが生成されます。ログには、IP アドレス割り当てのタイムスタンプ、リース期間、MAC アドレス、クライアント ID などの詳細が含まれます。

[NSSDW-36840]

ハードウェア監視サポート: 電源、ディスク、ヘルスステータスなどのハードウェアコンポーネントを監視し、**CLI** コマンド **hw_mon** を使用してステータスを確認できます。重大なハードウェアイベントは、Citrix SD-WAN イベントに記録されます。

[NSSDW-36660]

NAT ログの機能強化

Citrix SD-WAN 11.4.3 リリース以降、静的および動的 NAT ログが拡張され、変換された IP アドレスと変換された IP ポートに関連する情報が表示されます。新しく導入されたフィールドは次のとおりです。

翻訳された IP アドレス

- **natsrc** -変換されたソース IP アドレス
- **natdest** -変換された宛先 IP アドレス

NAT タイプ

- **snat** -snat が 1 の場合、接続はソース NAT 変換を通過していることを意味します。
- **dnat** -dnat が 1 の場合、接続は宛先 NAT 変換を通過していることを意味します。

翻訳済みポート

- **natsport** -変換された送信元ポートアドレス
- **natdport** -変換された宛先ポートアドレス

[NSSDW-34602]

解決された問題

ビルド 11.4.3a で対処された問題。

サイトまたは WAN リンクの設定変更時に拡張展開を行う場合、ルーティングエンジンを再起動すると、BGP セッションがフラップします。

[SDWANHELP-2594]

レガシー GUI は CGI セッションファイルを一時ディレクトリに残します。これらの CGI セッションは起動時にクリーンアップされるため、Citrix SD-WAN サービスの実行が妨げられる可能性があります。

[SDWANHELP-2567]

Citrix SD-WAN LTE サービスは、LTE モデムのトランザクションタイムアウトエラーが原因でハングすることがあります。

[SDWANHELP-2565]

動的ルールを追加する際に、考えられるメモリリークの問題が修正されました。

[SDWANHELP-2563]

Citrix SD-WAN UI のまれな競合状態が原因で、誤った DB インデックスで統計が要求されると、t2_app がクラッシュします。

[SDWANHELP-2548]

Citrix SD-WAN 1100 上のパロアルト VM (VM-50 モデル) に割り当てられたメモリは、5.5 GB に増加します。

[SDWANHELP-2534]

ICA 分類で発生する可能性があったメモリリークが修正されました。

[SDWANHELP-2527]

ドメイン名ベースのアプリケーションの DNS 学習エントリにより、最初のパケット分類テーブルが上限に達すると、アプライアンスがクラッシュします。

[SDWANHELP-2480]

Citrix SD-WAN アプライアンスは、管理ポートで必要なトラフィックのみを許可します。これにより、有効になっている場合、ユーザーは miRIC 管理 GUI にアクセスできなくなります。

[SDWANHELP-2479]

プレフィックス付きの **IP** アドレスを入力しようとすると、ファイアウォールフィルタポリシーの送信元/宛先 IP フィールドの検証に失敗していました。

[SDWANHELP-2471]

フローの数が常に多く、アプライアンスの最大フローキャパシティ制限を超えている場合、フローマッピングの変更によってデータパスが再起動することがあります。

[SDWANHELP-2456]

管理ポートがダウン/アップすると、Syslog サーバへの通信のソース IP は 169.254.200.2 になります

[SDWANHELP-2450]

Citrix SD-WAN Center ダッシュボードに情報が読み込まれません。

[SDWANHELP-2373]

スタティックルートは、配信サービスとして GRE トンネルをサポートします。最初にスタティックルートを適切に削除せずに GRE トンネルを削除すると、GRE トンネル配信サービスを使用するルートに問題が発生します。

この修正により、GRE トンネルが削除されると、配信サービスとして GRE トンネルを使用して設定されたルートが自動的に削除されます。

[NSSDW-37846]

Citrix SD-WAN 11.4.2 リリースでは、オンプレミス用 Citrix SD-WAN Orchestrator から署名付き CSR 証明書をアップロードすると、拡張子が.der のファイルに対して失敗します。

[NSSDW-37813]

AT&T 3G ネットワークの日没は 2022 年 2 月に予定されています。Citrix SD-WAN 110 LTE モデムは音声中心に設定されており、AT&T の 3G サンセット後は VoLTE をサポートしません。

[NSSDW-37736]

LTE ドングルまたは管理ポートによって提供される DNS に到達できない場合、Citrix SD-WAN Orchestrator サービスの接続が失敗します。ネットワークが接続のためにインバンド管理に切り替わったとしても。

[NSSDW-37428]

帯域内管理

Citrix SD-WAN 11.4.2 リリース以降、SD-WAN アプライアンスでインバンド管理を構成し、インバンド管理ポートを介して Citrix SD-WAN Orchestrator サービスへの接続を確立する必要があります。そうしないと、管理ポートが接続されておらず、インバンド IP アドレスも構成されていないと、アプライアンスは Citrix SD-WAN Orchestrator サービスへの接続を失います。

[NSSDW-37174]

DHCP サーバーが DVP および HA 構成で新しいアドレスを割り当てると、Citrix SD-WAN サービスがクラッシュすることがあります。

[NSSDW-36513]

まれに、ルーティングテーブルにルート変更があると、Citrix SD-WAN サービスがリロードされます。

[NSSDW-36289]

CRL 処理が有効になっている場合、サードパーティの暗号化ライブラリのメモリの問題により、コアダンプが発生する可能性があります。

[NSSDW-35679]

Edge Security のウイルス対策コンポーネントおよびマルウェア対策コンポーネントの内部ライセンスの有効期限が切れると、Citrix SD-WAN はウイルスとマルウェアの検出を停止します。

[NSSDW-35596]

サマリールートを含む Citrix SD-WAN 構成がロードされると、アプライアンスが継続的にリロードされることがあります。

[NSSDW-34670]

アプライアンスにサマリールートとして設定されたスタティックルートがあり、動的に学習された別の同じプレフィックスルートがある場合、サマリールートはルートを要約していません。

[NSSDW-34355]

Citrix SD-WAN では、モバイルブロードバンドデバイスでは DHCP のみが許可されます。これは、データプランに静的 IP が割り当てられているお客様には機能しません。

[NSSDW-33971]

SLAAC がルータから IP とゲートウェイアドレスを学習すると、現在のアドレスが期限切れになるまで、ゲートウェイが変更されたり、ネットワークセグメントが変更されたりしても、SD-WAN アプライアンスの再起動後であっても、SLAAC は IP を再学習しません。これにより、ポートの移動時にアドレスの取得が遅れる可能性があります。

[NSSDW-33807]

SLAAC がルータから IP アドレスとゲートウェイアドレスを学習すると、ゲートウェイが変更されても（現在のアドレスが期限切れになるまで）、SLAAC はゲートウェイを再学習しません。

例：

- ブランチアプライアンスは、ゲートウェイ 1 から IP とゲートウェイを学習します。
- ネットワーク管理者は、ゲートウェイ 1 を新しいゲートウェイ 2 に置き換えることにします。管理者は、ゲートウェイ 2 を Gateway-1 と同じ設定し、ルータアドバタイズメントから Gateway-1 が送信したのと同じブリフィクス情報を送信します。ただし、ゲートウェイ 2 の送信元アドレスはゲートウェイ 1 とは異なります。
- ブランチアプライアンスは、ゲートウェイ 2 の IP を自動的に学習しません。（現在のアドレスがタイムアウトしない限り）

[NSSDW-33802]

地域制御ノード (RCN) ネットワーク用に作成された自動生成されたサマリールートには、65534 ではなく 30,000 のコストが割り当てられます。

[NSSDW-32629]

Citrix SD-WAN Center からプッシュしたときに、アプライアンス設定が Citrix SD-WAN に適用されない。

[NSSDW-32257]

WPA3 失敗した認証は、サイトレベルのアラートでは報告されません。

[NSSDW-32053]

再認証を実行すると、Wi-Fi クライアントレポートにアップロードおよびダウンロードデータの負の値が表示されません。

[NSSDW-31903]

プラットフォームとシステム

カスタム SNMP コミュニティストリングを初めて追加しても、既存のコミュニティストリング設定は削除されません。

[SDWANHELP-2561]

既知の問題

リリース 11.4.3a に存在する問題。

部分的なサイトアップグレードを無効にした後にネットワーク全体を新しいソフトウェアバージョンにアップグレードすると、一部のサイトが古いバージョンに自動的に修正されて戻される可能性があります。

回避策: 別の変更管理がトリガーされると、ダウングレードされたサイトは予想されるソフトウェアバージョンにアップグレードされます。

[SDWANHELP-2586]

Citrix SD-WAN サービスは、インターネット負荷分散構成の Advanced Edition (AE) プラットフォームでクラッシュすることがあります。

回避策: インターネットサービスをプライマリモードとセカンダリモードで構成します。

[SDWANHELP-2521]

SNMP サービスに帯域外ポートを使用するアプライアンスが帯域内ポートに切り替えると、アプライアンスのすべての管理サービスが帯域内ポートを介してインターネットに接続します。アウトオブバンドポートに送信される SNMP 要求は失敗します。

回避策: アウトオブバンドポートで障害が発生した場合にインバンドポートに要求を送信するように、外部 SNMP サービスを設定します。

[SDWANHELP-2358]

VPX では、有効なライセンスがなければ、デーモンは自動的に再起動されます。この場合、デーモンがクラッシュすることがあります。デーモンが自動的に正常に起動するため、ユーザーへの影響はありません。

[NSSDW-37981]

UI の [Monitoring classes] テーブルに表示されるトラフィックレートは、リアルタイム、インタラクティブハイ、インタラクティブ中、およびインタラクティブ低クラスタイプのトラフィックが同時に開始されると、約 150 Kbps 低くなります。

[NSSDW-37568]

MCN で管理されている Citrix SD-WAN アプライアンスでは、新しい UI ダッシュボードの Orchestrator の接続状態が「不良/不明」と表示されます。

[NSSDW-37462]

まれに、ブランチサイトに静的パブリック IP アドレスを持つ WAN リンクの 1 つがある場合、ダイナミック仮想パスの形成は失敗します。

回避方法:

静的パブリック IP アドレスを使用して、ブランチサイトで Virtual WAN サービスを再起動します。

[NSSDW-36429]

Citrix SD-WAN BGP 構成で、ルーティングドメインのルーター ID が変更されると、SD-WAN 動的ルーティングプロトコルが再起動することがあります。

[NSSDW-35657]

ファイアウォールのダイナミック NAT ポリシーまたはポートフォワーディングルールに対して設定を変更すると、コアダンプが発生する可能性があります。

[NSSDW-34603]

ユーザーが内蔵モデムのステータスを表示することを選択すると、レガシー UI には外付けモデムのステータスも表示されます。

[NSSDW-32219]

Citrix SD-WAN 11.4.4 リリースのリリースノート

June 18, 2024

このリリースノートドキュメントでは、Citrix SD-WAN リリース Build 11.4.4 の拡張と変更、修正された問題と既知の問題について説明します。

注

Citrix SD-WAN 11.4.4 リリースは、<https://support.citrix.com/article/CTX617071>で説明されているセキュリティの脆弱性に対処しています。

新機能

ビルド 11.4.4 で利用できる機能強化と変更点。

デフォルトのタイムアウト時間は **5** 分に設定されています

Citrix SD-WAN アプライアンスのデフォルトの GUI/CLI セッションタイムアウト期間は 5 分に設定されています。この設定により、Citrix SD-WAN アプライアンスへの不正アクセスのリスクが軽減されます。

[NSSDW-36840]

解決された問題

ビルド 11.4.4 で対処されている問題。

Citrix SD-WAN アプライアンスは、データセンターのトラフィックをルーティングするために誤った GRE トンネルを使用することがあります。

[SDWANHELP-2488]

場合によっては、2つの支店間のトラフィックフローに遅延が発生することがあります。この問題は、Dynamic Virtual Path (DVP) がブランチ間通信で有効になっていて、一方のブランチが DVP を使用し、もう一方のブランチが MCN を使用してトラフィックをルーティングする場合に発生します。

[SDWANHELP-2637, SDWANHELP-2749]

場合によっては、Net Flow と AppFlow が複数の WAN リンクで有効になっていると、Citrix SD-WAN アプライアンスが突然再起動することがあります。

[SDWANHELP-2745]

場合によっては、統計の開始日と終了日が正しくないため、Citrix SD-WAN Center データベースの自動クリーンアップが停止することがあります。

[SDWANHELP-2751]

高負荷時に構成の更新が行われると、Citrix SD-WAN アプライアンスが突然再起動することがあります。

[SDWANHELP-2760]

Citrix SD-WAN Center ダッシュボードの「サイト QoE」セクションは、選択した日付範囲を検証できないため、統計を読み込めません。

[SDWANHELP-2772]

稼働時間が1か月以上前の場合、Citrix SD-WAN ダッシュボードには正確な稼働時間データが表示されません。

[SDWANHELP-2856]

インターネットサービス用に NAT ポリシーが設定されている場合、「firewall_dynamic_nat_policy」オブジェクトを変更するための Citrix SD-WAN ファイアウォールの REST API 呼び出しは機能しません。

[SDWANHELP-2862]

ユーザーが Citrix SD-WAN Center を使用して Citrix Cloud に初めてログオンすると、Citrix SD-WAN Center の [構成] > [ゼロタッチ展開] ページにアクセスできなくなります。

[SDWANHELP-2923]

既知の問題

リリース 11.4.4 に存在する問題。

場合によっては、DPDK ライブラリの問題が原因で Citrix SD-WAN 2100 アプライアンスがクラッシュすることがあります。この問題は、Citrix SD-WAN アプライアンスがリンクアグリゲーショングループ (LAG) で構成され、LACP が有効になっている場合に発生します。

回避策: LACP を使用して LAG を無効にします。

[NSSDW-38568]

SD-WAN アプライアンスの新しいユーザーインターフェイス

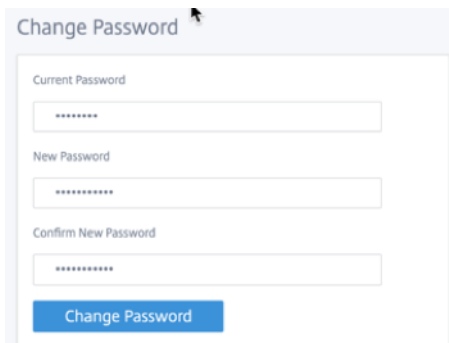
February 8, 2022

SD-WAN アプライアンスに新しいユーザーインターフェイス (UI) が導入されました。新しい UI は、最新の UI テクノロジを使用して構築されます。新しい UI デザインにより、セキュリティが向上し、ルックアンドフィールが改善され、よりパフォーマンス、安全、応答性が高まります。しかし、新しい UI では、レガシー UI の各機能のフローとページレイアウトが保持されています。

Citrix SD-WAN 11.4 リリース以降、クライアントとして構成されているすべての Citrix SD-WAN アプライアンスで、新しい UI がデフォルトで有効になります。

注

- MCN として Citrix SD-WAN アプライアンスをプロビジョニングすると、レガシー UI にリダイレクトされます。
- 管理者ロールを持つすべてのローカルユーザとリモート管理者ユーザは、新しいユーザーインターフェイスにアクセスできます。リモートユーザーアカウントは、RADIUS または TACACS + 認証サーバーを介して認証されます。SD-WAN アプライアンスの Provisioning 中に、デフォルトの admin ユーザーアカウントパスワードを変更する必要があります。デフォルトのパスワードは SD-WAN アプライアンスのシリアル番号であり、デバイスにログオンした後に初めて変更することが義務付けられています。



レガシー UI は下位互換性を保つために維持され、非推奨です。レガシー UI には、URL **[https: ///cgi-bin/login.cgi](https://cgi-bin/login.cgi)** を使用してアクセスできます。< ip-address > ユーザ **admin** のユーザ名とパスワードは、(新規/レガシー) 両方のユーザインターフェイスで同じままであり、最初のログイン手順はどちらのインターフェイスでも実行できます。新しい UI の将来のバージョンでは、追加のユーザーがサポートされる予定です。

Citrix SD-WAN の新しいユーザーインターフェイス

新しい UI は、Google Chrome (バージョン 81)、Mozilla Firefox、Microsoft Edge (バージョン 81+)、Legacy Microsoft Edge (バージョン 44+) のブラウザを使用してアクセスすることができます。

注:

Microsoft Internet Explorer、Apple Safari、およびその他のブラウザはサポートされていません。

新しい UI ページにアクセスするには、次の手順に従います。

1. 新しいブラウザタブを開き、**https:// <management-ip>** に移動し、SD-WAN アプライアンスの新しい UI にアクセスします。IPv6 アドレスにアクセスする場合は、**https://<[IPv6 address]>** と入力します。

例: **https://[fd73:xxxx:yyyy:26::9]**

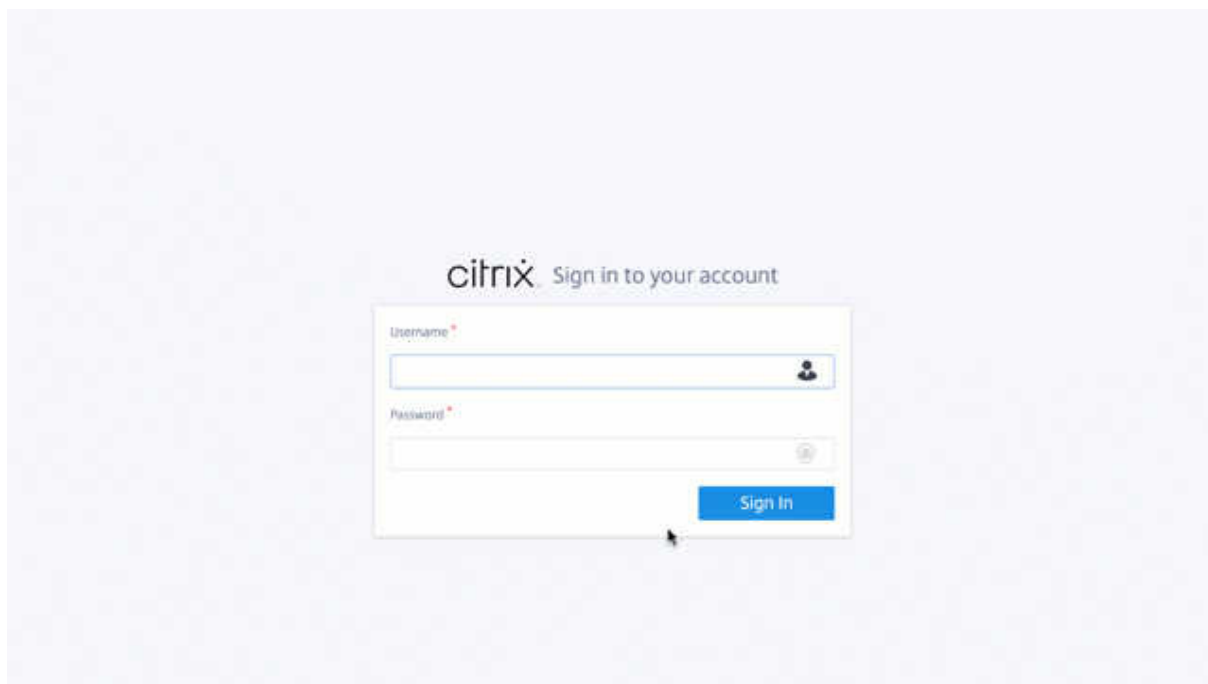
注:

インバンド管理が有効になっているシナリオでは、インターフェイスの IP アドレス **<management-ip>

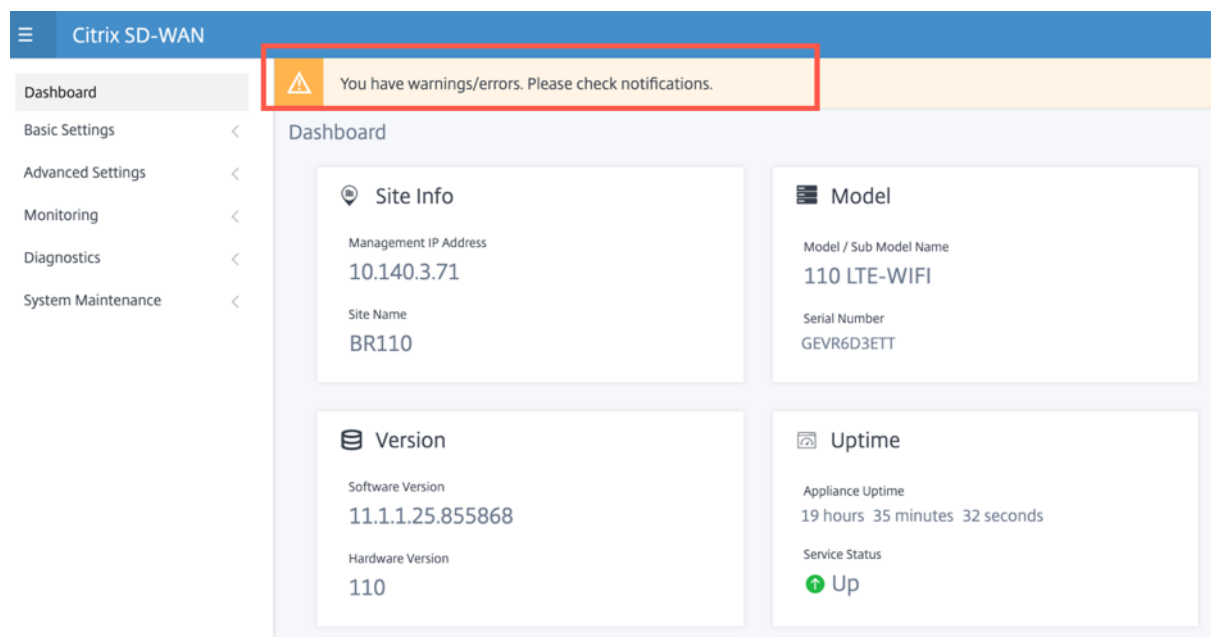
をで指定して、新しい UI にアクセスできます。インバンド管理は、IP サービスに使用できるように有効になっている複数の信頼できるインターフェイスで有効にできます。管理 IP とインバンド仮想 IP を使用して UI にアクセスできます。

1. ユーザー名とパスワードを入力します。[サインイン] をクリックします。

Citrix SD-WAN ユーザーインターフェイスのページが表示されます。

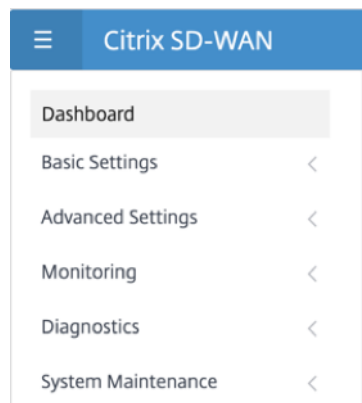


正常にログインすると、ナビゲーションパネルが左側にあることがわかります。また、警告やエラーがある場合は、ダッシュボードに通知バナーが表示されます。



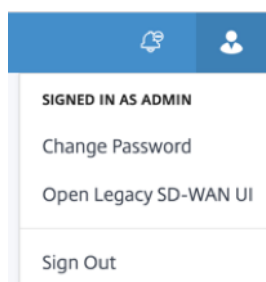
ナビゲーション

左側のナビゲーションサイドバーは、ハンバーガーアイコンをクリックすると非表示にしたり、表示させたりすることができます。左上隅のハンバーガーアイコンには、ダッシュボード、基本/詳細設定、監視、および管理関連のオプションへのリンクが表示されます。



メニューバー

右上隅のユーザーメニューには、ログオンしたユーザーの詳細が表示されます。[レガシー **SD-WAN UI** を開く] オプションをクリックすると、新しいブラウザタブでレガシーユーザインターフェイスを開くことができます。通知を表示するには、ベルアイコンをクリックします。

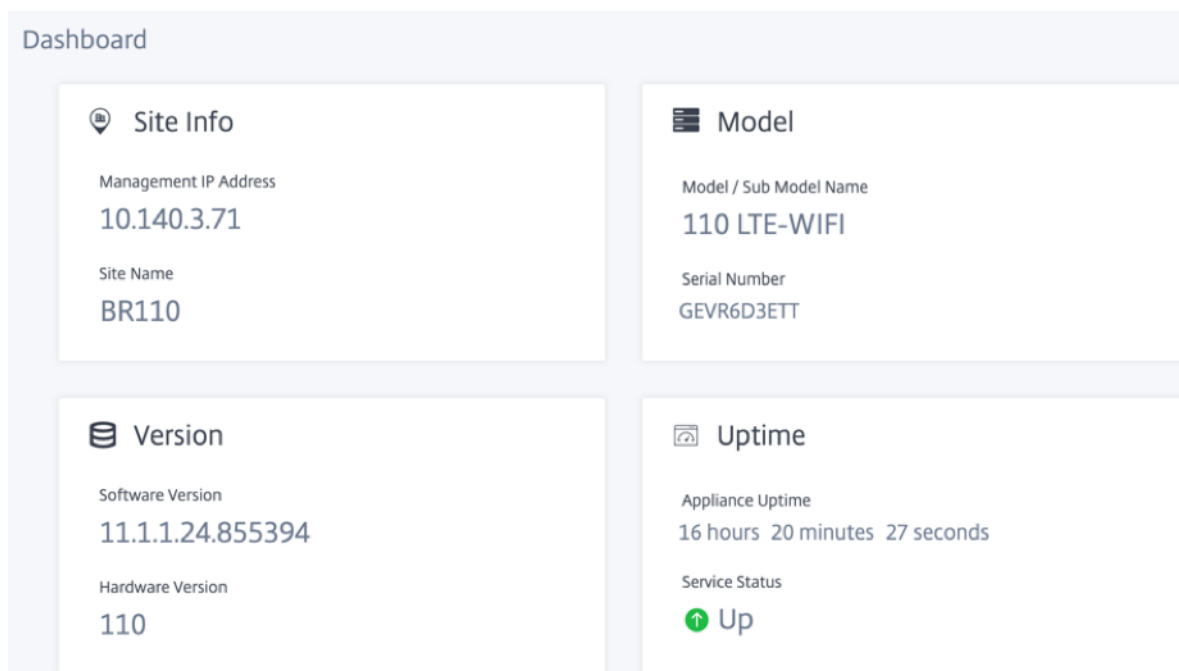


ダッシュボード

[**Dashboard**] ページには、SD-WAN アプライアンスの次の基本情報がタイルビューとして表示されます。

- [**S**ite]: 管理 **IP** アドレス と サイト 名とともにサイト情報を表示します。
- 「モデル」 (Model)- ** モデル/サブモデル名とシリアル番号を表示します **。
- [**V**ersion]: ソフトウェア および ハードウェア のバージョンを表示します。
- 稼働時間 - アプライアンスの稼働時間、**Citrix** 仮想 **WAN** サービスのステータス、**Orchestrator** 接続状態を表示します。
- **High Availability**: ローカルおよびピアアプライアンスの **HA** ステータスと、最後に受信した高可用性アップデート時刻を表示します。
- 従量制課金リンク-メータリングが有効になっているリンクの使用状況と請求の詳細を表示します。
- オーケストレータ接続 -Citrix SD-WAN Orchestrator サービスによるアプライアンスの接続ステータスを表示します。次のステータス情報が表示されます。
 - オンライン状態-アプライアンスと Citrix SD-WAN Orchestrator サービス間の接続ステータスを示します。アプライアンスから Citrix SD-WAN Orchestrator サービスに定期的にハートビート信号が送信され、接続状態が「良好」または「悪い」として識別されます。
 - サービス状態-ダウンロード、ホーム、ロギング、統計情報など、必要なすべての SD-WAN Orchestrator サービスへのアプライアンスの https 到達可能性を示します。サービスの状態が悪い場合は、接続が確立されているものの、すべてまたは一部のサービスにアクセスできないことを意味します。到達不能なサービス名が表示されます。
 - **DNS** 状態-FQDN の DNS 解決ステータスを示します。DNS の状態が悪い場合は、いずれかの FQDN の DNS 解決が失敗していることを意味します。未解決の FQDN の名前が表示されます。
 - [ローカルゲートウェイの状態]-デフォルトゲートウェイのステータスを示します。アウトオブバンド接続の場合、ゲートウェイの状態はデフォルトゲートウェイに ping を実行することで判断されます。インバンド接続の場合、ゲートウェイの状態は、インバンドイーサネットインターフェイスの IP アドレスに ping を実行することで判断されます。
 - 接続経由-アプライアンスが Citrix SD-WAN Orchestrator サービスに到達する方法を示します。デフォルト設定であるアウトオブバンド経由、またはインバンド管理が設定されている場合はインバンド経由のいずれか。

- 失敗した理由:SD-WAN Orchestrator サービスへの接続中に失敗した理由。



基本設定

SD-WAN アプライアンスの基本設定には、次のエンティティ構成が含まれます。新しい UI には、各エンティティを個別に設定するための個別のページが用意されています。

- 管理と DNS
- インターフェイス設定
- LACP LAG グループ
- 日時
- RADIUS サーバ
- TACACS+ サーバ

管理と DNS

[管理と **DNS**] ページから、管理インターフェイスの IP アドレスと DNS 設定を構成できます。詳細については、「[管理 IP アドレスの構成](#)」を参照してください。

管理インターフェイスの許可リストは、管理インターフェイスへのアクセス許可を持つ IP アドレスまたは IP ドメインの承認リストです。空のリストを指定すると、すべてのネットワークから管理インターフェイスにアクセスできます。IP アドレスを追加すると、信頼できるネットワークだけが管理 IP アドレスにアクセスできるようになります。

許可リストに IPv4 アドレスを追加または削除するには、IPv4 アドレスのみを使用して SD-WAN アプライアンス管理インターフェイスにアクセスする必要があります。同様に、許可リストに IPv6 アドレスを追加または削除するに

は、IPv6 アドレスのみを使用して SD-WAN アプライアンス管理インターフェイスにアクセスする必要があります

The screenshot shows the Citrix SD-WAN Management Interface. The left sidebar contains a menu with the following items: Dashboard, Basic Settings (expanded), Management & DNS (selected), Interface Settings, Date & Time, Advanced Settings, Monitoring, Diagnostics, and System Maintenance. The main content area is titled 'Network Adapters' and contains three sections:

- Management Interface IP**: Includes a checkbox for 'Enable DHCP' (checked), and input fields for 'IP Address' (192.168.1.1), 'Subnet Mask' (255.255.255.0), and 'Gateway IP Address' (192.168.1.1).
- DNS Settings**: Includes input fields for 'Primary DNS' and 'Secondary DNS', and a 'Clear' button.
- Current DNS**: Displays the current 'Primary DNS' (192.168.1.1) and 'Secondary DNS' (192.168.1.1).

A 'Save' button is located at the bottom of the page.

設定するアプライアンスの **IP** アドレス、サブネットマスク、および **Gateway IP** アドレスを入力します。[**DNS 設定**] セクションで、プライマリおよびセカンダリの DNS サーバの詳細を指定し、[保存] をクリックします。

インターフェイス設定

インターフェイス設定ページには、イーサネットポートの設定データが表示されます。ダウンしているポートは、MAC アドレスに対して赤いドットで示されます。

☰

Citrix SD-WAN

Dashboard

Basic Settings ▼

Management & DNS

Interface Settings

Date & Time

Advanced Settings <

Monitoring <

Diagnostics <

System Maintenance <

Ethernet Interface Settings

Interface		MAC Address	Autonegotiate	Speed	Duplex
1/4-MGMT	●	08:35:71:11:bf:1f	<input checked="" type="checkbox"/>	100Mb/s ▼	Full ▼
1/1	●	08:35:71:11:bf:1c	<input checked="" type="checkbox"/>	Unknown ▼	Half ▼
1/2	●	08:35:71:11:bf:1d	<input checked="" type="checkbox"/>	1000Mb/s ▼	Full ▼
1/3	●	08:35:71:11:bf:1e	<input type="checkbox"/>	100Mb/s ▼	Full ▼
LAG0	●	Device not configured	<input checked="" type="checkbox"/>	Unknown ▼	Unknown ▼
LAG1	●	Device not configured	<input checked="" type="checkbox"/>	Unknown ▼	Unknown ▼

Save

LACP LAG グループ

リンク集約グループ（LAG）機能を使用すると、SD-WAN アプライアンス上の 2 つ以上のポートをグループ化して、1 つのポートとして連携させることができます。これにより、可用性の向上、リンクの冗長性、およびパフォーマンスの向上が保証されます。

以前は、LAG ではアクティブ-バックアップ・モードのみがサポートされていました。Citrix SD-WAN 11.3 リリース以降では、802.3AD リンクアグリゲーション制御プロトコル（LACP）プロトコルベースのネゴシエーションがサポートされています。LACP は標準プロトコルであり、LAG 用のより多くの機能を提供します。

アクティブバックアップモードでは、いつでも 1 つのポートだけがアクティブになり、他のポートはバックアップモードになります。アクティブサポートおよびバックアップサポートは、LAG 機能についてデータプレーン開発キット (DPDK) パッケージに依存しています。

LACP を使用すると、すべてのポートで同時にトラフィックを送信できます。利点として、リンク冗長メカニズムとともに帯域幅を増やすことができます。LACP 実装では、アクティブ-アクティブモードがサポートされています。アクティブ-バックアップモードでは、SD-WAN UI からフル LACP アクティブ/アクティブモードを選択することもできます。

LAG 機能は、次の DPDK でサポートされているプラットフォームでのみ使用できます。

- Citrix SD-WAN 110 SE
- Citrix SD-WAN 210 SE
- Citrix SD-WAN 410 SE
- Citrix SD-WAN 1100 SE/PE
- Citrix SD-WAN 2100 SE/PE
- Citrix SD-WAN 4100、および 5100 SE

- Citrix SD-WAN 6100 SE

注

LAG 機能は、VPX/VPXL プラットフォームではサポートされていません。

Citrix SD-WAN アプライアンスの各 LAG にグループ化された最大 4 つのポートを持つ最大 4 つの LAG を作成できます。

Citrix SD-WAN 210 および 410 アプライアンスの場合、最大 3 つの LAG を、Citrix SD-WAN 110 アプライアンスの場合は、最大 2 つの LAG を作成できます。

LAG は、[レガシー UI](#) または [SD-WAN Orchestrator](#) のみを使用して作成できます。新しい UI では、作成された LAG の詳細のみを表示できます。

LAG の詳細を表示するには、[基本設定] > [LACP LAG グループ] に移動します。

アクティブポートとパートナーポートの現在のステート、システム、ポートプライオリティの詳細など、LACP LAG の詳細を表示できます。

LACP LAG							
LAG0							
NAME	SELECTION	STATE	SYSTEM PRIORI...	PORT PRIORITY	PARTNER STATE	PARTNER SYST...	PARTNER PORT ...
1/1	Selected	ACT AGG SY...	65535	65280	AGG SYNC C...	128	128
1/4	Selected	ACT AGG SY...	65535	65280	AGG SYNC C...	128	128
LAG1							
NAME	SELECTION	STATE	SYSTEM PRIORI...	PORT PRIORITY	PARTNER STATE	PARTNER SYST...	PARTNER PORT ...
1/7	N/A	Inactive	N/A	N/A	N/A	N/A	N/A
1/8	N/A	Inactive	N/A	N/A	N/A	N/A	N/A

日時

[日付と時刻の設定 (Date and Time)] 設定ページから、アプライアンスで日付と時刻を設定する必要があります。詳細については、「[日付と時刻の設定](#)」を参照してください。

Dashboard

Basic Settings

Management & DNS

Interface Settings

Date & Time

Advanced Settings

Monitoring

Diagnostics

System Maintenance

Date/Time Settings

If the Appliance date/time is turned back due to NTP or manual changes, reporting artifacts may occur.

NTP Settings

☒ Use NTP Server

Server Address

0.pool.ntp.org:1.pool.ntp.org:2.pool.ntp.org:3.pool.ntp.org

Save

Date/Time Settings

May 6, 2020 1:55 PM

Save

Timezone Settings

After changing the timezone setting, a reboot will be necessary for the timezone changes to take full effect. Until then, some logs will continue to use the actual timezone setting in effect at the time of the last reboot, even though events timestamps may reflect the new setting.

Timezone

UTC

Save

RADIUS サーバ

SD-WAN アプライアンスを構成して、1 つ以上の RADIUS サーバでユーザーアクセスを認証できます。

RADIUS サーバを構成するには、次の手順を実行します。

1. [**RADIUS** を有効にする] チェックボックスをオンにします。
2. サーバの **IP** アドレスと認証ポートを入力します ******。最大 3 つのサーバ IP アドレスを構成できます。

注:

IPv6 アドレスを構成するには、RADIUS サーバにも IPv6 アドレスが設定されていることを確認してください。

3. サーバキーを入力し、確定します。
4. タイムアウト値を秒単位で入力します。
5. [保存] をクリックします。

RADIUS サーバ接続をテストすることもできます。 ****** ユーザ名とパスワードを入力します。 [Verify] ****** をクリックします。

RADIUS Server

Server Settings

☒ Enable RADIUS

Server 1 IP Address *

Authentication Port

Server 2 IP Address

Authentication Port

Server 3 IP Address

Authentication Port

Server Key

Confirm Server Key

Timeout(seconds)

Test RADIUS Server Connection

User Name

Password

TACACS+ サーバ

TACACS+ サーバを認証用に設定できます。RADIUS 認証と同様に、TACACS+ は秘密キー、IP アドレス、およびポート番号を使用します。デフォルトのポート番号は 49 です。

TACACS+ サーバを設定するには、次の手順を実行します。

1. [**TACACS+** を有効にする] チェックボックスをオンにします。

2. サーバの **IP** アドレスと認証ポートを入力します ******。最大 3 つのサーバ IP アドレスを構成できます。

注:

IPv6 アドレスを設定するには、TACACS+ サーバにも IPv6 アドレスが設定されていることを確認します。

3. [認証タイプ] として [**PAP**] または [**ASCII**] を選択します。

- PAP: パスワード認証プロトコル (PAP) を使用して、強力な共有秘密を TACACS+ サーバに割り当てることにより、ユーザ認証を強化します。
- [ASCII]: ASCII 文字セットを使用して、TACACS+ サーバに強力な共有秘密を割り当てることにより、ユーザ認証を強化します。

4. サーバキーを入力し、確定します。

5. タイムアウト値を秒単位で入力します。

6. [保存] をクリックします。

TACACS+ サーバ接続をテストすることもできます。 ****** ユーザ名とパスワードを入力します。 [Verify] ****** をクリックします。

TACACS+ Server

Settings

☒ Enable TACACS+

Server 1 IP Address *	Authentication Port
<input type="text"/>	<input type="text" value="49"/>
Server 2 IP Address	Authentication Port
<input type="text"/>	<input type="text"/>
Server 3 IP Address	Authentication Port
<input type="text"/>	<input type="text"/>

Authentication Type ☐ PAP ☒ ASCII

Server Key

Confirm Server Key

Timeout(seconds)

Save

Test TACACS+ Server Connection

User Name

Password

Verify

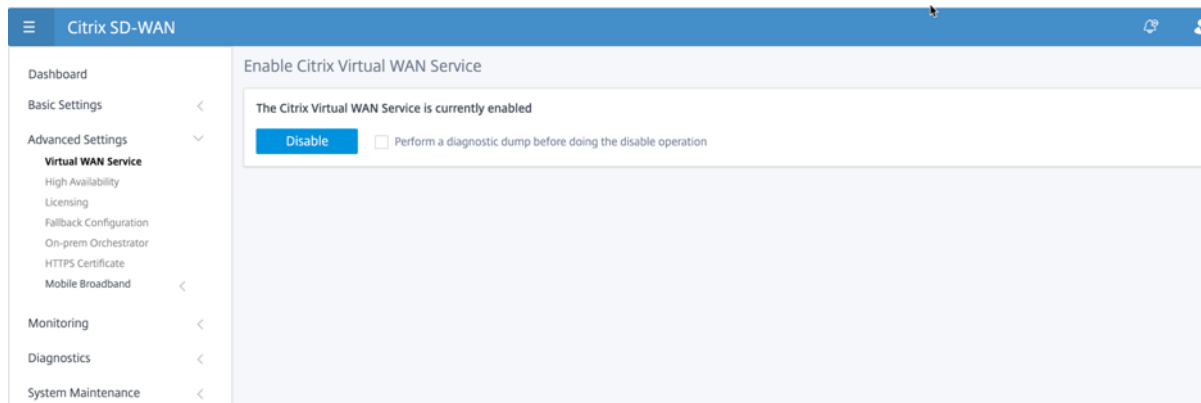
詳細設定

SD-WAN アプライアンスの詳細設定には、次のエンティティ構成が含まれます。

- Citrix 仮想 WAN サービス
- 高可用性
- モバイルブロードバンド
- ライセンス
- フォールバック構成
- HTTPS 証明書
- オンプレミス・オーケストレーター

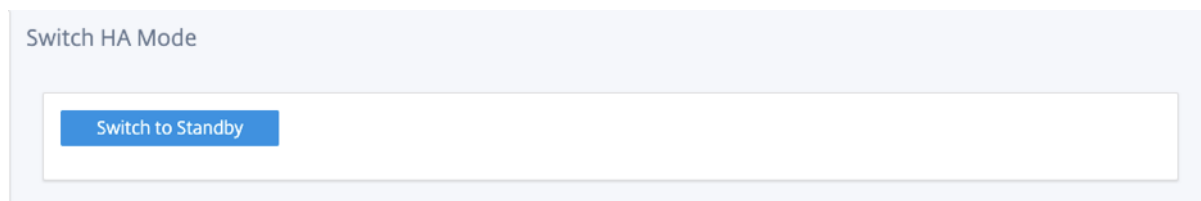
Citrix 仮想 WAN サービス

[Citrix 仮想 WAN サービス] ページでは、Citrix 仮想 WAN サービスを有効または無効にできます。詳細については、[仮想 WAN サービスの構成](#)を参照してください。



高可用性

[高可用性 (HA)] ページから、SD-WAN 高可用性 (HA) セットアップのアクティブ状態とスタンバイ状態を切り替えることができます。高可用性ステータスは、ダッシュボードで使用できます（高可用性が設定されている場合）。詳細については、「[高可用性モード](#)」を参照してください。



モバイルブロードバンド

Citrix SD-WAN 210 SE LTE および 110 LTE Wi-Fi アプライアンスなどの Citrix SD-WAN アプライアンスには、内蔵 LTE モデムが搭載されています。外部 3G/4G USB モデムは、以下の Citrix SD-WAN アプライアンスでも接続できます。

- Citrix SD-WAN 210 SE
- Citrix SD-WAN 210 SE LTE
- Citrix SD-WAN 110 SE
- Citrix SD-WAN 110 LTE Wi-Fi SE

サポートされている外部 USB モデムは、CDC イーサネット、MBIM、および NCM の 3 種類です。

レガシー GUI を使用した LTE の設定の詳細については、次のトピックを参照してください。

- [210 SE LTE アプライアンスでの LTE 機能の構成](#)

- [110-LTE-WiFi アプライアンスでの LTE 機能の構成](#)
- [外付け USB LTE モデムの構成](#)

内蔵 LTE モデムの場合は、Citrix SD-WAN アプライアンスの SIM カードスロットに SIM カードを挿入します。アンテナを Citrix SD-WAN アプライアンスに固定します。詳細については、[LTE アンテナの取り付けとアプライアンスの電源投入を参照してください](#)。

注:

Citrix SD-WAN 110-LTE-WiFi アプライアンスには、2 つの標準 (2FF) SIM スロットがあります。マイクロ (3FF) およびナノ (4FF) サイズの SIM を使用するには、SIM アダプタを使用します。小さい SIM をアダプタにスナップします。アダプタは、フィールド交換可能ユニット (FRU) として Citrix から入手するか、SIM プロバイダから入手できます。内部 LTE モデム用の SIM のホットスワップは、Citrix SD-WAN 110-LTE-WiFi アプライアンスでのみサポートされています。

外部 LTE モデムの関連事項:

- サポートされている USB LTE ドングルを使用してください。対応ドングルのハードウェアモデルは Verizon USB730L と AT&T USB800 である。
- SIM カードが USB LTE ドングルに挿入されていることを確認します。CDC イーサネット LTE ドングルには静的 IP アドレスがあらかじめ設定されているため、SIM カードが挿入されていないと、設定が妨げられ、接続障害や断続的な接続が発生します。
- CDC イーサネット LTE ドングルを SD-WAN アプライアンスに挿入する前に、外部 USB スティックを Windows/Linux マシンに接続し、適切な APN およびモバイルデータローミング構成でインターネットが正常に動作していることを確認します。USB ドングルの接続モードがデフォルト値の **【手動】** から **【自動】** に変更されていることを確認します。

注

- Citrix SD-WAN アプライアンスは、一度に 1 つの USB LTE ドングルしかサポートしません。複数の USB ドングルが接続されている場合は、すべてのドングルを外し、1 つのドングルだけを接続します。
- Citrix SD-WAN アプライアンスは、USB モデムのユーザー名とパスワードをサポートしていません。セッティング時に、モデムのユーザー名とパスワード機能が無効になっていることを確認します。
- 外部 MBIM ドングルの抜き差しやリブートは、内部 LTE モデムデータセッションに影響を与えます。これは予想される動作です。
- 外部 LTE モデムを接続すると、SD-WAN アプライアンスで認識されるまでに約 3 分かかります。

モバイルブロードバンドの状態を表示するには、モデムの種類を選択します。

Dashboard
Basic Settings
Advanced Settings
Virtual WAN Service
High Availability
Mobile Broadband
Status
Operations
Licensing
Fallback Configuration
HTTPS Certificate
On-prem Orchestrator
Monitoring
Diagnostics
System Maintenance

Mobile Broadband Status

Modem Type
Status Of

Internal Modem
Device

Status	
Active SIM	SIM Two
Data Service Capability	non-simultaneous-cs-ps
ESN	0
Expected Data Format	802-3
Hardware Revision	10000
IMEI	867698040416771
MEID	86769804041677
MSISDN	
Manufacturer	QUALCOMM INCORPORATED
Max RX Channel Rate (bps)	100000000
Max TX Channel Rate (bps)	50000000
Model	QUECTEL Mobile Broadband Module
Networks	gsm,umts,lte
Operating Mode	online
Operating Mode HW Restricted	0
PRL Only Preference	0
PRL Version	0
Revision	EG25GGBR07A07M2G
SIM Capability	supported
Software Version	EG25GGBR07A07M2G
Type	110-WIFI-LTE

以下は、いくつかの有用なステータス情報です。

- **モデムの種類:** モデムの種類として [外部] または [内部] を選択します。内蔵モデムは、[モバイルブロードバンド] > [ステータス] ページにステータスを表示します。SIM 設定、APN 設定、モデムの有効化/無効化、モデムの再起動、SIM の更新などのその他のすべてのセクションは、[モバイルブロードバンド] > [操作] ページにあります。
- **アクティブ SIM:** アクティブになることができる SIM はいつでも、1 つのみです。現在アクティブな SIM を表示します。
- **動作モード:** モデムの状態を表示します。
- **SIM 機能:** SIM がサポートされているかどうかが表示されます。
- **Model:** モバイルブロードバンドモジュール名を表示します。

[外付けモデム] を選択すると、外部モデムのステータスが表示されます。ただし、外部モデムが設定されていない場合は、このデバイスで [選択されたモデムが構成されていません] という警告メッセージが表示されます。

CDC イーサネット外部モデムのデバイスの詳細

Mobile Broadband Status	
Modem Type	Status Of
External Modem	Device
Status	
Product ID	9030
Vendor ID	3410
Manufacturer	Novatel Wireless
Product	Mifi USB730L

MBIM および NCM 外部モデムのデバイスの詳細 [**Modem Mode**] フィールドには、外付けドングルの種類が表示されます。

Mobile Broadband Status	
Modem Type	Status Of
External Modem	Device
Status	
Active SIM	SIM One
Data Service Capability	none
ESN	
Expected Data Format	unknown
Hardware Revision	
IMEI	866785032748294
MEID	
MSISDN	
Manufacturer	
Max RX Channel Rate (bps)	150000000
Max TX Channel Rate (bps)	150000000
Model	CL2E3372HM
Modem Mode	MBIM
Networks	gprs, edge, umts, hsdpa, hsupa, lte, custom
Operating Mode	online
Operating Mode HW Restricted	0
PRL Only Preference	0
PRL Version	0
Revision	
SIM Capability	not-supported
Software Version	
Product ID	157c
Vendor ID	12d1
Manufacturer	HUAWEI_MOBILE
Product	HUAWEI_MOBILE

SIM の詳細は、MBIM および NCM 外部モデムについてのみ表示されます。

Mobile Broadband Status

Modem Type		Status Of
External Modem		SIM One
Status		
APN	internet	
APN Autodetect	Searching	
Application State	unknown	
Application Type	unknown	
Authentication	None	
Card State	present	
Connection Status	connected	
Home Network	Idea	
ICCID	89911100001445614166	
IMSI	404446068985937	
Address	10.2.250.171	
Gateway	10.2.250.169	
MTU	1500	
Netmask	255.255.255.248	
Primary DNS	112.110.241.1	
Secondary DNS	112.110.249.1	
Data Session	Not Available	
Enabled		
MCC	404	
MNC	44	
PIN Retries	0	
PIN State	disabled	
PUK Retries	0	
Radio Interface	lte	
Roaming Status	on	
Signal Strength	Excellent	
Username		

モバイルブロードバンド動作 内部モデムと外部モデムでサポートされる操作:

操作	内蔵モデム	外部モデム-CDC イーサネット	外部モデム-MBIM および NCM
SIM プリファレンス	はい-デュアル SIM をサポートするアプライアンスの場合	いいえ	いいえ
SIM ピン	はい	いいえ	いいえ

操作	内蔵モデム	外部モデム-CDC イーサネット	外部モデム-MBIM および NCM
APN 設定	はい	いいえ	はい
ネットワーク設定	はい	いいえ	いいえ
ローミング	はい	いいえ	いいえ
ファームウェアの管理	はい	いいえ	いいえ
モデムの有効化/無効化	はい	いいえ	はい
モデムの再起動	はい	いいえ	いいえ
SIM のリフレッシュ	はい	いいえ	いいえ

SIM プリファレンス Citrix SD-WAN 110-LTE-WiFi アプライアンスにデュアル SIM を挿入できます。一度に 1 つの SIM だけがアクティブになります。**SIM** プリファレンスを選択します。

- **SIM One** 優先: SIM が 2 つ挿入されている場合、LTE モデムは起動時に SIM One を使用します（使用可能な場合）。LTE モデムが起動して実行されると、その時点で使用可能な SIM（SIM One または SIM Two）が使用され、SIM がアクティブになるまで使用され続けます。
- **SIM Two** 推奨: SIM が 2 台挿入されている場合、LTE モデムは SIMTwo を使用します（利用可能な場合）。LTE モデムが起動して実行されると、その時点で使用可能な SIM（SIM One または SIM Two）が使用され、SIM がアクティブになるまで使用され続けます。
- **SIM One:** 両方の SIM スロットの SIM 状態に関係なく、SIM One のみが使用されます。SIM One は常にアクティブです。
- **SIM Two:** 両方の SIM スロットの SIM 状態に関係なく、SIM Two のみが使用されます。SIM Two は常にアクティブです。

注:

Citrix SD-WAN 210-SE LTE Wi-Fi アプライアンスには、SIM カードスロットが 1 つしかないため、[SIM 設定] オプションは使用できません。

SIM Preference

Preferred SIM

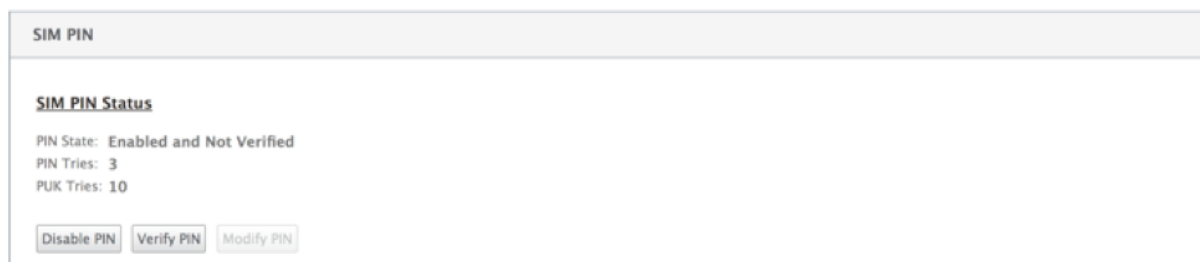
SIM Two

Apply

SIM ピン

PIN でロックされている SIM カードを挿入した場合、SIM ステータスは [有効] および [未確認] 状態になります。SIM PIN で認証されるまで、SIM カードは使用できません。SIM PIN は通信事業者から入手できます。

SIM PIN 操作を実行するには、[詳細設定] > [モバイルブロードバンド] > [操作] > [SIM PIN ステータス] に移動します。



次の操作を実行できます。

- **SIM PIN** を確認します。[確認] をクリックします。配送業者が提供した SIM PIN を入力し、[確認] をクリックします。ステータスが [有効] および [確認済み] に変わります。
- **SIM PIN** を有効にする: SIM PIN が無効になっている SIM の SIM PIN を有効にできます。[有効にする] をクリックします。通信事業者から提供された SIM PIN を入力し、[有効] をクリックします。SIM PIN の状態が [有効] および [未確認] に変わると、PIN が検証されず、PIN が検証されるまで LTE 関連の操作を実行できなくなります。[Verify] をクリックします。配送業者が提供した SIM PIN を入力し、[確認] をクリックします。
- **SIM PIN** を無効にする: SIM PIN が有効で検証された SIM の SIM の PIN 機能を無効にすることができます。[無効化] をクリックします。SIM PIN を入力し、[無効] をクリックします。
- **SIM PIN** の変更: PIN が [有効] および [確認済み] 状態になると、PIN を変更できます。[修正] をクリックします。通信事業者から提供された SIM PIN を入力します。新しい SIM PIN を入力し、確認します。[修正] をクリックします。
- **SIM** ブロック解除-SIM PIN を忘れた場合は、キャリアから取得した SIM PUK を使用して SIM PIN をリセットできます。SIM のブロックを解除するには、[ブロック解除] をクリックします。キャリアから取得した SIM PIN と SIM PUK を入力し、[ブロック解除] をクリックします。

注:

SIM カードは、SIM のブロックを解除しながら、10 回の PUK の試行に失敗すると、永久にブロックされます。新しい SIM カードについては、通信事業者のサービスプロバイダーにお問い合わせください。

APN 設定

1. APN 設定を構成するには、[詳細設定] > [モバイルブロードバンド] > [オペレーション] の順に選択し、[APN 設定] セクションに移動します。

注

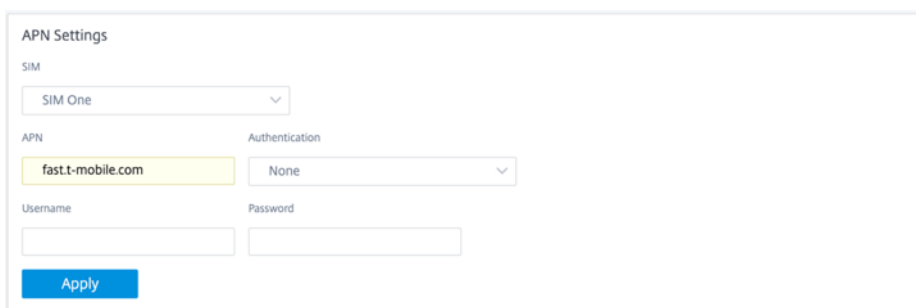
キャリアから APN 情報を入手します。

2. SIM カードを選択し、通信事業者から提供された **APN**、ユーザー名、パスワード、認証を入力します。PAP、CHAP、PAPCHAP 認証プロトコルから選択できます。通信事業者が認証タイプを提供していない場合は、[なし] に設定します。

(注

) これらのフィールドはすべてオプションです。

3. [適用] をクリックします。



APN Settings

SIM

SIM One

APN

fast.t-mobile.com

Authentication

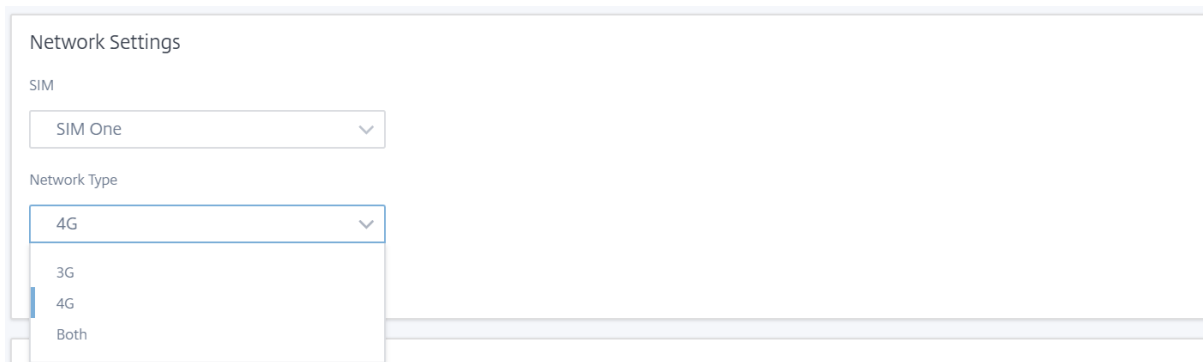
None

Username

Password

Apply

ネットワーク設定 内部 LTE モデムをサポートする Citrix SD-WAN アプライアンスのモバイルネットワークを選択できます。サポートされるネットワークは、3G、4G、またはその両方です。



Network Settings

SIM

SIM One

Network Type

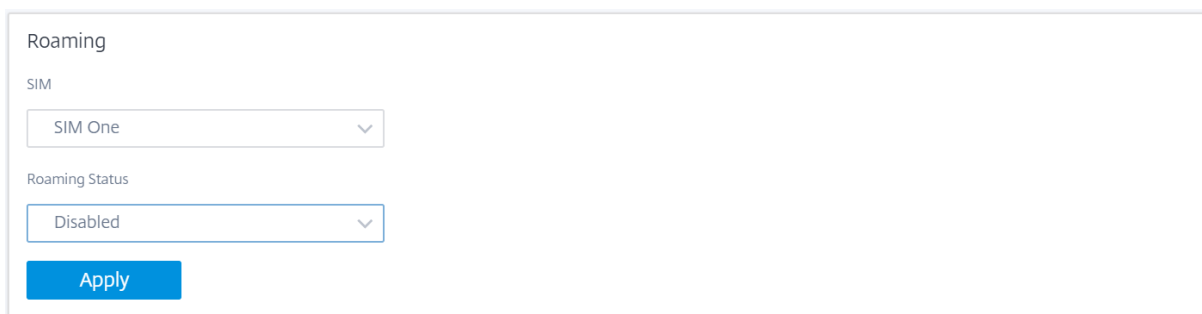
4G

3G

4G

Both

ローミング ローミングオプションは、LTE アプライアンスではデフォルトで有効になっています。無効にすることもできます。



Roaming

SIM

SIM One

Roaming Status

Disabled

Apply

ファームウェアの管理

LTE 対応のすべてのアプライアンスには、使用可能なファームウェアのセットがあります。既存のファームウェアのリストから選択するか、ファームウェアをアップロードして適用することができます。使用するファームウェアが不明な場合は、[**AUTO-SIM**] オプションを選択します。AUTO-SIM オプションを使用すると、LTE モデムは、挿入された SIM カードに基づいて最も一致するファームウェアを選択することができます。

モデムの有効化/無効化 LTE 機能を使用する意図に応じて、モデムを有効/無効にします。デフォルトでは、LTE モデムは有効になっています。



Enable/Disable Modem

Enable

モデムの再起動 モデムをリブートします。再起動操作が完了するまで、最大で 7 分かかる場合があります。



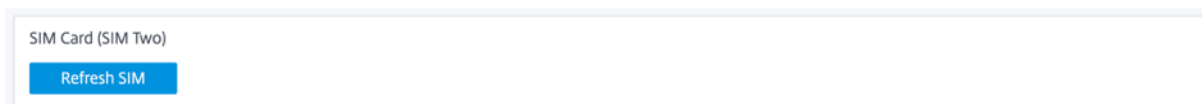
Reboot Modem

Reboot

SIM のリフレッシュ SIM カードが **LTE-WiFi** モデムで正しく検出されない場合は、[**SIM を更新**] オプションを使用します。

注:

[SIM の更新] 操作は、アクティブな SIM に対してのみ適用されます。



SIM Card (SIM Two)

Refresh SIM

Citrix SD-WAN Center を使用して、ネットワーク内のすべての LTE サイトをリモートで表示および管理できます。詳細については、[リモート LTE サイト管理を参照してください](#)。

LTE 構成の詳細については、[110-LTE-WiFi アプライアンスの LTE 機能の構成および 210 SE LTE アプライアンスの LTE 機能の構成を参照してください。](#)

外部 LTE モデムの設定については、[外部 USB LTE モデムの設定を参照してください。](#)

ライセンス

[ライセンス] ページには、サーバーの場所、モデル、ライセンスタイプなどのライセンスの詳細が表示されます。

Citrix SD-WAN	
Dashboard	Licensing
Basic Settings	
Advanced Settings	
Virtual WAN Service	
High Availability	
Mobile Broadband	
Status	
Operations	
Licensing	
Fallback Configuration	
HTTPS Certificate	
On-prem Orchestrator	
Monitoring	
Diagnostics	
System Maintenance	

Status	
Maximum Bandwidth (MAXBW)	50 Mbps
License Server Location	Local
License Expiration Date	Wed Dec 2 00:00:00 2020
License Type	Eval
Local License Server HostID	02357111bf1f
Maintenance Expiration Date	Tue Dec 1 00:00:00 2020
State	Licensed
Model	110VW-050

注：

SD-WAN Center からライセンスをインストールおよび適用する場合は、有効にする SD-WAN アプライアンス Edition が特定のアプライアンスでサポートされ、正しいソフトウェアバージョンが使用できることを確認してください。

デフォルト/フォールバック構成

[デフォルト/フォールバック構成] ページには、保存されているフォールバック構成データが表示されます。フォールバック構成が無効になっている場合は、[フォールバック構成の有効化] スイッチをオンにすることで、フォールバック構成を有効に できます。

The screenshot displays the 'Fallback Configuration' page in the Citrix SD-WAN 11.4 interface. The left sidebar contains navigation links: Dashboard, Basic Settings, Advanced Settings (with sub-links for Virtual WAN Service, High Availability, Mobile Broadband, Status, Operations, and Licensing), Fallback Configuration (with sub-links for HTTPS Certificate and On-prem Orchestrator), Monitoring, Diagnostics, and System Maintenance. The main content area is titled 'Fallback Configuration' and includes a description: 'The fallback configuration provides basic network functionality when a critical failure occurs and the system can no longer function.' Below this, there is a toggle for 'Enable Fallback Configuration' (currently enabled) and a 'Reset' button. The 'WAN Settings' section states: 'WAN settings are currently not configurable. WAN ports are configured as independent WAN Links using DHCP client and monitor the Quad9 DNS service to determine WAN connectivity.' The 'LAN Settings' section includes fields for 'VLAN ID' (0) and 'IP Address' (192.168.0.1/24), a checkbox for 'Enable DHCP Server', 'DHCP Start' (192.168.0.50) and 'DHCP End' (192.168.0.250) ranges, a checked 'Dynamic DNS Servers' checkbox, 'DNS Server' (9.9.9.9) and 'Alt DNS Server' (149.112.112.112) fields, and an unchecked 'Internet Access' checkbox. The 'Port Settings' section features a table with columns 'Port' and 'Mode'. The 'Mode' column has radio buttons for 'WAN', 'LAN', and 'Disabled', followed by an input field for the IP address. The rows are: 1/1 (LAN selected, empty IP), 1/2 (WAN selected, 9.9.9.9), 1/3 (Disabled selected, empty IP), 1/4-MGMT (Disabled selected, empty IP), LTE-1 (WAN selected, 9.9.9.9), and LTE-E1 (WAN selected, 9.9.9.9). At the bottom, there is a section for 'Unassigned Port Bypass Mode' with a dropdown menu set to 'Fail to Block'.

注

LTE インターフェイスは、スタティック IP アドレスでは設定できません。

詳細については、「[デフォルト/フォールバック設定](#)」を参照してください。

HTTPS 証明書

セキュリティで保護された接続を確立するには、HTTPS 証明書が必要です。[[HTTPS 証明書](#)] ページには、既にインストールされている HTTPS 証明書の詳細が表示されます。詳細については、「[HTTPS 証明書](#)」を参照してください。

HTTPS Certificate

Installed Certificate

Issuer		Issued To	
Country:	US	Country:	US
State/Province:	California	State/Province:	California
Locality:	San Jose	Locality:	San Jose
Organization:	Citrix Systems, Inc.	Organization:	Citrix Systems, Inc.
Organizational Unit:	Engineering	Organizational Unit:	Engineering
Common Name:	Citrix	Common Name:	Citrix
Email:	support@citrix.com	Email:	support@citrix.com

Certificate Details

Certificate Fingerprint:	9D:FA:53:C0:55:0C:28:6C:E3:FB:24:60:60:D2:82:C0:17:00:34:88
Start Date:	Apr 16 12:15:31 2020 GMT
End Date:	Apr 14 12:15:31 2030 GMT
Serial Number:	F227B6ABF41CC86D

Upload Certificate

Upload the certificate that secures the Management HTTPS connection to this Virtual WAN appliance. Uploading and installing the HTTPS Certificate will cause the HTTP server to restart, invalidating all connected sessions.
NOTE: For best results: when the operation is complete close the browser window and reconnect to the appliance.

Upload Certificate

Click to select or drag n drop file here.
 Allowed file types are .crt

Upload Key

Click to select or drag n drop file here.
 Allowed file types are .key

Regenerate Certificate

Regenerate the certificate that secures the Management HTTPS connection to this Virtual WAN appliance. Regenerating the HTTPS Certificate will cause the HTTP server to restart, invalidating all connected sessions.
NOTE: For best results: when the operation is complete close the browser window and reconnect to the appliance.

オンプレミス・オーケストレーター

Citrix オンプレミス SD-WAN Orchestrator は、Citrix SD-WAN Orchestrator サービスのオンプレミスソフトウェアバージョンです。Citrix On-Prem SD-WAN Orchestrator は、Citrix パートナーが複数の顧客を一元管理できる単一の管理プラットフォームを提供し、適切な役割ベースのアクセス制御を使用して複数の顧客を一元管理できるようにします。

Orchestrator の接続を有効にし、オンプレミス SD-WAN オーケストレータの ID を指定することで、Citrix SD-WAN アプライアンスと Citrix オンプレミス SD-WAN オーケストレータ間の接続を確立できます。

注

- **SD-WAN** アプライアンスでのオンプレミス **SD-WAN Orchestrator** 構成機能は、Citrix オンプレミス SD-WAN Orchestrator イネーブラです。SD-WAN アプライアンス上の Citrix オンプレミス SD-WAN

オーケストレータ構成機能は、現在使用できません。将来のリリースを対象としています。

- SD-WAN アプライアンス上でオンプレミスの **SD-WAN Orchestrator** 構成機能が **SD-WAN** アプライアンス上で構成されている場合、ゼロタッチ展開は機能しません。

Orchestrator 接続を有効にするには、次の手順に従います。

1. アプライアンスの GUI で、[詳細設定] > [オンプレミス **Orchestrator**] > [ID] に移動します。
2. [オンプレミ **SD-WAN Orchestrator** 接続を有効にする] チェックボックスをオンにします。

The screenshot shows the 'On-Prem SD-WAN Orchestrator Identity' configuration page in the Citrix SD-WAN GUI. The left sidebar contains navigation options: Dashboard, Basic Settings, Advanced Settings (with sub-items like Citrix Virtual WAN Service, High Availability, Mobile Broadband, Licensing, Fallback Configuration, HTTPS Certificate, On-prem Orchestrator Identity, and Certificate), Monitoring, Diagnostics, and System Maintenance. The main content area has a title 'On-Prem SD-WAN Orchestrator Identity' and a note: 'Note: This section is applicable only to On-prem SD-WAN Orchestrator managed networks, and not Cloud Orchestrator or SD-WAN Center managed networks. This is to enable appliances to join an On-prem SD-WAN Orchestrator managed network, in cases where the connectivity options at the appliance end do not allow for automated zero touch provisioning. Configure the On-Prem SD-WAN Orchestrator identity by providing a valid IP address and clicking "Apply" to enable your appliance to connect to the On-Prem SD-WAN Orchestrator.' Below the note are two checked checkboxes: 'Enable On-Prem SD-WAN Orchestrator connectivity' and 'Advanced Configuration'. There are three rows of input fields: 'On-prem SD-WAN Orchestrator IP', 'Download Management Service IP', and 'Statistics Management Service IP' in the first row; 'On-prem SD-WAN Orchestrator Domain', 'Download Management Service Domain', and 'Statistics Management Service Domain' in the second row. The 'On-prem SD-WAN Orchestrator Domain' field contains the text 'sdwanzt.citrixnetworkapi.net'. An 'Apply' button is at the bottom.

3. 構成用に、オンプレミス SD-WAN Orchestrator の IP アドレスまたはドメイン、またはその両方（IP アドレスとドメイン）を入力します。

ドメインのみを構成する場合は、ローカル DNS サーバーに DNS レコードを追加し、SD-WAN アプライアンスに DNS サーバーの IP アドレスを構成する必要があります。構成するには、[構成] > [ネットワークアダプタ] > [IP アドレス] に移動します。

たとえば、オンプレミスの SD-WAN Orchestrator ドメインが citrix.com として構成されている場合、DNS サーバに、以下の FQDN およびオンプレミスの SD-WAN オーケストレータの IP アドレス用の DNS レコードを作成する必要があります。

- download.citrix.com
- sdwanzt.citrix.com
- sdwan-home.citrix.com

詳細設定の場合：

たとえば、オンプレミス Orchestrator ドメインが **citrix.com** として構成されている場合、ダウンロード管理サービスドメインは **download.citrix.com** として構成され、統計管理サービスドメインは **statistics.citrix.com** として構成されます。次に、以下の FQDN および対応する IP アドレスの DNS サーバーに DNS レコードを作成する必要があります。

- download.citrix.com
- sdwanzt.citrix.com
- statistics.citrix.com

On-Prem Orchestrator では、大規模なネットワークのスケラビリティを向上させるため、ダウンロードや独立したサーバインスタンスでの統計などのサービスの実行がサポートされる場合があります。詳細構成を選択し、ダウンロード管理サービスと統計管理サービスを構成できます。

[詳細設定] チェックボックスをオンにして、次の詳細を入力します。

- ダウンロード管理サービス **IP/ドメイン**: SD-WAN ソフトウェアおよび構成のダウンロードの側面を独立したサーバインスタンスにオフロードするのに役立つ IP アドレス/ドメインを提供し、大規模ネットワークのスケラビリティを向上させます。
- 統計管理サービス **IP/ドメイン**: SD-WAN 統計情報の収集と管理をデバイスから独立したサーバインスタンスへオフロードできる IP アドレス/ドメインを提供し、大規模ネットワークのスケラビリティを向上させます。

4. [適用] をクリックします。

SD-WAN アプライアンスまたはオンプレミスの SD-WAN Orchestrator 証明書を再生成、ダウンロード、アップロードするには、[詳細設定] > [オンプレミス **Orchestrator**] > [証明書] に移動します。

オンプレミス **Orchestrator** 認証タイプが無効の場合、アプライアンスは、認証なし、一方向認証、または双方向認証モードのいずれかを使用して **、オンプレミス Orchestrator に接続できます。

オンプレミス **Orchestrator** 認証タイプが有効になっている場合、アプライアンスは双方向認証を介してオンプレミス **Orchestrator** にのみ接続できます。

オンプレミスの Orchestrator の認証タイプを有効状態から無効にすると、一方向認証モードの既存のアプライアンスは切断状態になります。接続するには、アプライアンスの認証タイプを [双方向認証] に変更し、SD-WAN アプライアンス証明書を On-Prem Orchestrator にアップロードする必要があります。

注

- 生成される証明書は X509 自己署名証明書です。
- 証明書の有効期限が切れたり、侵害されたりした場合は、証明書を再生成する必要があります。
- 証明書の有効期間は 10 年です。
- フィンガープリント、開始日、終了日などの証明書の詳細を表示できます。
- お客様は、On-Prem Orchestrator と SD-WAN アプライアンスの間で証明書が再生成され、交換されることを確認する必要があります。これにより、On-Prem Orchestrator とのアプライアンスの接続が切断されるのを防ぐことができます。

5. [認証タイプ] を選択します。次に、SD-WAN アプライアンスとオンプレミスの SD-WAN Orchestrator 接続間でサポートされる認証タイプを示します。

- 認証なし—オンプレミスの SD-WAN Orchestrator と SD-WAN アプライアンスの間の認証は行われません。また、SD-WAN アプライアンスまたはオンプレミスの SD-WAN Orchestrator 証明書を使用する必要はありません。ただし、MPLS などのセキュアなネットワークがある場合は、このオプションを使用できます。

Secure Connectivity

No Authentication – Insecure connection. Use this option if you have a secure network. For eg: MPLS

One-way Authentication – On-prem Orchestrator certificates have to be uploaded to all the appliances. Appliance will trust On-prem Orchestrator using the uploaded certificates.

Two-way Authentication – On-prem Orchestrator and Appliance certificates have to be exchanged. Appliance and On-prem Orchestrator will trust each other using the exchanged certificates.

Authentication Type

No Authentication

Apply

- 一方向認証—一方向認証の種類を選択する場合は、オンプレミスの Orchestrator 証明書をアップロードする必要があります。オンプレミスオーケストレータからオンプレミスオーケストレータをダウンロードし、[アップロード] をクリックします。SD-WAN アプライアンスは、アップロードされた証明書をを使用して、オンプレミス Orchestrator を信頼します。

Secure Connectivity

No Authentication – Insecure connection. Use this option if you have a secure network. For eg: MPLS

One-way Authentication – On-prem Orchestrator certificates have to be uploaded to all the appliances. Appliance will trust On-prem Orchestrator using the uploaded certificates.

Two-way Authentication – On-prem Orchestrator and Appliance certificates have to be exchanged. Appliance and On-prem Orchestrator will trust each other using the exchanged certificates.

Authentication Type

One-Way Authentication

Apply

On-prem SD-WAN Orchestrator Certificate

Certificate Details:

Certificate Fingerprint:	0D:37:24:A6:99:B6:D4:8F:CB:55:C1:3C:AB:42:9E:7F:19:EB:23:53
Start Date:	May 21 13:34:50 2020 GMT
End Date:	May 19 13:34:50 2030 GMT

Click here to select the file or drag and drop the selected file.
Allowed file type is .pem

Upload

- 双方向認証—オンプレミスの Orchestrator とアプライアンス証明書は、相互に交換する必要があります。双方向認証の場合は、オンプレミスの Orchestrator で SD-WAN アプライアンス証明書を再生成し、ダウンロードし、アップロードする必要があります。SD-WAN アプライアンスと On-Prem Orchestrator は、交換された証明書をを使用して相互に信頼します。

Secure Connectivity

No Authentication – Insecure connection. Use this option if you have a secure network. For eg: MPLS
 One-way Authentication – On-prem Orchestrator certificates have to be uploaded to all the appliances. Appliance will trust On-prem Orchestrator using the uploaded certificates.
 Two-way Authentication – On-prem Orchestrator and Appliance certificates have to be exchanged. Appliance and On-prem Orchestrator will trust each other using the exchanged certificates.

Authentication Type
 Two-Way Authentication

Apply

On-prem SD-WAN Orchestrator Certificate

Certificate Details:

Certificate Fingerprint:	0D:37:24:A6:99:B6:D4:8F:C8:55:C1:3C:AB:42:9E:7F:19:EB:23:53
Start Date:	May 21 13:34:50 2020 GMT
End Date:	May 19 13:34:50 2030 GMT

Click here to select the file or drag and drop the selected file.
 Allowed file type is .pem

Upload

SD-WAN Appliance Certificate

Certificate Details:

Certificate Fingerprint:	FC:36:3C:E5:EF:C2:F8:ED:48:20:0C:28:6C:5D:BA:82:55:CE:04:DD
Start Date:	Jul 21 06:07:08 2020 GMT
End Date:	Jul 19 06:07:08 2030 GMT

Regenerate Download

注:

一方向認証または双方向認証のみを使用することをお勧めします。認証がない場合は、セキュリティで保護された DNS サーバーを選択する必要があります。

オンプレミス SD-WAN Orchestrator 接続を無効にするには、[オンプレミス **SD-WAN Orchestrator** 接続を有効にする] をオフにして、[適用] をクリックします。オンプレミスオーケストレーター管理ネットワークを Cloud Orchestrator または MCN 管理ネットワークに変換するには、オンプレミス SD-WAN Orchestrator 接続を無効にし、構成をリセットする必要があります。設定をリセットするには、[構成] > [システムメンテナンス] > [構成のリセット] に移動します。

アップグレードとダウングレード

- SD-WAN アプライアンスを 11.1.1/11.2.0/10.2.7 から 11.2.1 ソフトウェアバージョンにアップグレードした後、アプライアンス証明書とオンプレミス Orchestrator 証明書の両方を交換する必要があります。
- SD-WAN アプライアンスを 11.2.1 から 11.1.1/11.2.0/10.2.7 ソフトウェアバージョンにダウングレードした後、Citrix SD-WAN アプライアンス UI で ID 設定を再度適用する必要があります。オンプレミスの SD-WAN Orchestrator 構成または SD-WAN アプライアンスの接続に関連する問題がある場合は、オンプレ

ミスの SD-WAN Orchestrator 接続を無効にしてから、オンプレミスの SD-WAN Orchestrator 接続を再度有効にします。

10.2.7/11.1.1/11.11.2.0 ソフトウェアを実行している SD-WAN アプライアンスを管理するには、オンプレミスの SD-WAN SD-WAN Orchestrator 認証タイプを無効にする必要があります。

監視

[監視] セクションでは、アドレス解決プロトコル (**ARP**)、ルート、イーサネット、イーサネット **MAC** 統計情報、および **DHCP** クライアント **WAN** リンク、**SLAAC WAN** リンク、**DHCP** サーバ/リレー、ファイアウォール接続、フロー、および **DNS** 統計を表示できます。

- **ARP**、ルート、イーサネット、およびイーサネット **MAC** 統計情報: ARP、ルート、イーサネット、およびイーサネット MAC の統計情報を表示できます。統計情報を使用して、トラフィックまたはインターフェイスエラーを確認できます。詳細については、[統計情報の表示を参照してください](#)。
- **DHCP** クライアント **WAN** リンク: [DHCP クライアント WAN リンク] ページには、学習した IP のステータスが表示されます。IP の更新を要求できます。これにより、リース時間が更新されます。[**Release Renew**] を選択することもできます。これにより、新しいリースで新しい IP アドレスが発行されます。詳細については、「[DHCP クライアント WAN リンクの監視](#)」を参照してください。
- **SLAAC WAN** リンク: [SLAAC WAN リンク] ページには、SLAAC が仮想インターフェイスに割り当てる IPv6 アドレスの詳細が表示されます。また、[**Release Rnew**] を選択して、SLAAC が新しい IP アドレス、または新しいリースを持つ同じ IP アドレスを IPv6 クライアントに割り当てられるようにすることもできます。
- **DHCP** サーバ/リレー: SD-WAN アプライアンスを DHCP サーバまたは DHCP リレーエージェントとして使用できます。
 - DHCP サーバ機能を使用すると、SD-WAN アプライアンスの LAN/WAN インターフェイスと同じネットワーク上のデバイスは、SD-WAN アプライアンスから IP 設定を取得できます。
 - DHCP リレー機能を使用すると、SD-WAN アプライアンスは DHCP クライアントとサーバ間で DHCP パケットを転送できます。

詳細については、「[DHCP サーバ](#)」および「[DHCP リレー](#)」を参照してください。

- ファイアウォール接続: [ファイアウォール接続] ページには、ファイアウォール接続の統計情報が表示されます。ファイアウォールポリシーが、各アプリケーションのトラフィックに対してどのように動作しているかを確認できます。詳細については、[ファイアウォールの統計情報の表示を参照してください](#)。
- フロー: [フロー (**Flows**)] セクションでは、仮想 WAN フロー情報を表示するための基本的な手順について説明します。詳細については、[フロー情報の表示を参照してください](#)。
- **DNS** プロキシ統計: このページには、構成された DNS プロキシの詳細が表示されます。[更新] をクリックして、現在のデータを取得します。詳細については、「[ドメインネームシステム](#)」を参照してください。

診断

[診断] セクションには、接続の問題をテストおよび調査するためのオプションが用意されています。詳細については、「[診断](#)」を参照してください。

注:

Citrix SD-WAN 110 アプライアンスの場合、一度に存在できる診断パッケージは 1 つのみです。Citrix SD-WAN 210 アプライアンスでは、最大 5 つの診断パッケージを使用できます。

システムメンテナンス

[システムメンテナンス] セクションを使用して、メンテナンス作業を実行します。[システムメンテナンス] ページには、次のオプションがあります。

- ファイルの削除: ログファイル、バックアップファイル、およびアーカイブされたデータベースを削除できます。ドロップダウンメニューから削除するファイルを選択し、「削除」ボタンをクリックします。
- システムの再起動: 仮想 WAN サービスを再起動するか、システムを再起動できます。
- ローカル変更管理: ローカル変更管理 プロセスでは、新しいアプライアンスパッケージをこの個別のアプライアンスにアップロードできます。
- 構成のリセット: 構成をリセットできます。このオプションでは、このアプライアンスのユーザーデータ、ログ、履歴、およびローカル構成データが消去されます。
- 工場出荷時のリセット: 出荷時のリセット オプションを使用して、SD-WAN アプライアンスを出荷時のバージョンにリセットします。

(注

) これらの機能はすべて、既存の [SD-WAN](#) ドキュメントで詳しく説明されています。

サポートされていないプラットフォーム

新しい UI は、次の SD-WAN アプライアンスをサポートしていません。

- Citrix SD-WAN 1000 SE/PE
- Citrix SD-WAN 2000 SE/PE
- Citrix SD-WAN 4000 SE

システム要件

May 10, 2021

ハードウェア要件

SD-WAN アプライアンスのインストール手順については、[SD-WAN アプライアンスの設定](#)を参照してください。

ファームウェアの要件

仮想 WAN 環境のすべての Citrix SD-WAN アプライアンスモデルでは、同じ Citrix SD-WAN ファームウェアリリースを実行する必要があります。

注

以前のソフトウェアバージョンを実行しているアプライアンスは、SD-WAN リリース 11.4 を実行しているアプライアンスへの仮想パス接続を確立できません。詳細については、Citrix サポートチームにお問い合わせください。

ソフトウェア要件

ライセンス要件の詳細については、[ライセンス](#)を参照してください。

ブラウザの要件

ブラウザで Cookie を有効にし、JavaScript をインストールして有効にする必要があります。

SD-WAN 管理 Web インターフェイスは、次のブラウザでサポートされています。

- Mozilla Firefox 49+
- Google Chrome 51+
- Microsoft Internet Explorer 11+
- Microsoft Edge 13+
- Safari 9+

サポートされているブラウザでは、Cookie を有効にし、JavaScript をインストールして有効にする必要があります。

Hypervisor

Citrix SD-WAN SE/PE VPX は、次のハイパーバイザーで構成できます。

- VMware ESXi サーバ（バージョン 5.5.0 以降）
- Citrix Hypervisor 6.5 以降です。
- Microsoft Hyper-V 2012 R2 以降。
- Linux KVM

クラウドプラットフォーム

Citrix SD-WAN SE/PE VPX は、次のクラウドプラットフォームで構成できます。

- Microsoft Azure
- Amazon Web Services
- Google Cloud Platform

SD-WAN プラットフォームモデルとソフトウェアパッケージ

September 26, 2023

このセクションでは、Citrix SD-WAN ソフトウェアパッケージのダウンロードについて説明します。

注

ソフトウェアをダウンロードする前に、Citrix SD-WAN ソフトウェアライセンスを取得して登録する必要があります。詳しくは、「[ライセンス](#)」を参照してください。

SD-WAN アプライアンスパッケージには、特定の SD-WAN 構成パッケージにバンドルされた特定のアプライアンスモデル用の SD-WAN ソフトウェアパッケージが含まれます。この 2 つのパッケージは、マスターコントロールノード (MCN) で実行されている管理 **Web** インターフェイスの変更管理ウィザードを使用してバンドルされ、クライアントに配布されます。

これが初期インストールの場合は、SD-WAN ネットワークに存在する各クライアントアプライアンスで、適切なアプライアンスパッケージを手動でアップロード、ステージングおよびアクティブ化する必要があります。既存の SD-WAN 展開の設定を更新する場合、クライアントへの仮想パスが動作可能になると、MCN は既存の各クライアントで適切なアプライアンスパッケージを自動的に配布し、アクティブ化します。

ソフトウェアパッケージをダウンロードする

アプライアンスモデルごとに異なる Citrix SD-WAN ソフトウェアパッケージがあります。ネットワークに含めるアプライアンスモデルごとに、適切なソフトウェアパッケージをダウンロードする必要があります。

Citrix SD-WAN ソフトウェアパッケージをダウンロードするには、[製品のダウンロードの URL にアクセスします](#)。ソフトウェアのダウンロード手順は、このサイトに記載されています。

Citrix SD-WAN ソフトウェアパッケージ

サポートされている SD-WAN アプライアンスモデルごとに異なる Citrix SD-WAN ソフトウェアパッケージがあります。ネットワークに組み込む予定のアプライアンスモデルごとに、適切なパッケージを入手する必要があります。

サポートされる **SD-WAN** アプライアンスモデル

Citrix SD-WAN アプライアンスには、主に次の 3 つのカテゴリがあります。

- SD-WAN アプライアンスハードウェアモデル
 - WANOP、Standard Edition、Premium Edition
- SD-WAN VPX 仮想アプライアンス (SD-WAN VPX)
 - Standard Edition と WANOP Edition

注

SD-WAN 環境内のすべての SD-WAN アプライアンスモデルで、同じ SD-WAN ファームウェアリリースを実行する必要があります。詳細については、Citrix SD-WAN カスタマーサポートにお問い合わせください。

SD-WAN アプライアンスの詳細については、製品ダウンロードサイトの [SD-WAN 製品プラットフォーム Edition のデータシート](#)を参照してください。

SD-WAN 標準 Edition のハードウェアアプライアンス

サポートされている SD-WAN Standard Edition ハードウェアアプライアンスモデルは次のとおりです。

SD-WAN SE プラットフォームモデル	役割
110-SE/110-LTE-WiFi/110-WiFi-SE	小規模ブランチアプライアンス
210-SE/210-SE LTE	小規模ブランチアプライアンス
410-SE	小規模ブランチアプライアンス
1000-SE	小規模ブランチアプライアンス
1100-SE	大規模なブランチアプライアンス
2000-SE	大規模なブランチアプライアンス
2100-SE	大規模なブランチアプライアンス
4100-SE	データセンター-マスターコントロールノード (MCN) アプライアンス
5100-SE	データセンター-マスターコントロールノード (MCN) アプライアンス
6100-SE	データセンター-マスターコントロールノード (MCN) アプライアンス

SD-WAN WAN Optimization ハードウェアアプライアンス (**SD-WAN WANOP**)

サポートされている SD-WAN WAN 最適化 (WANOP) アプライアンスモデルは次のとおりです。

SD-WAN WANOP プラットフォームモデル	役割
WANOP 4100	データ・センター・アプライアンス
WANOP 5100	データ・センター・アプライアンス

SD-WAN VPX 仮想アプライアンス (**SD-WAN VPX-SE**)

以下は、サポートされている SD-WAN VPX 仮想アプライアンス (VPX-SE) モデルです。

SD-WAN VPX-SE プラットフォームモデル	役割
VPX 20-SE	MCN またはクライアントアプライアンス、小規模ブランチ
VPX 50SE	MCN またはクライアントアプライアンス、小規模ブランチ
VPX 100-SE	MCN またはクライアントアプライアンス、小規模ブランチ
VPX 200-SE	MCN またはクライアントアプライアンス、小規模ブランチ
VPX 500-SE	MCN またはクライアントアプライアンス、小規模ブランチ
VPX 1000-SE	MCN またはクライアントアプライアンス、小規模ブランチ

詳しくは、「Citrix SD-WAN 仮想 VPX [Standard Edition の前提条件](#)」を参照してください。

SD-WAN WANOP 仮想アプライアンス (**SD-WAN VPX-WANOP**)

以下は、サポートされている SD-WAN WANOP 仮想アプライアンス (VPX-WANOP) モデルです。

SD-WAN VPX WANOP プラットフォームモデル	役割
WANOP VPX-2	小規模ブランチアプライアンス
WANOP VPX-6	小規模ブランチアプライアンス
WANOP VPX-10	小規模ブランチアプライアンス

SD-WAN VPX WANOP プラットフォームモデル	役割
WANOP VPX-20	小規模ブランチアプライアンス
WANOP VPX-50	大規模なブランチアプライアンス
WANOP VPX-100	大規模なブランチアプライアンス
WANOP VPX-200	大規模なブランチアプライアンス

重要

リリースバージョン 10.1 では、Enterprise プラットフォーム Edition は「Premium Edition」にリブランドされています。

SD-WAN Premium Edition ハードウェアアプライアンス (SD-WAN PE)

サポートされている SD-WAN Premium (Enterprise) Edition アプライアンス (SD-WAN PE) モデルは次のとおりです。

SD-WAN EE プラットフォームモデル	役割
1000-PE	大規模なブランチ、データセンターのアプライアンス
1100-PE	大規模なブランチ、データセンターのアプライアンス
2000-PE	大規模なブランチ、データセンターのアプライアンス
2100-PE	大規模なブランチ、データセンターのアプライアンス
5100-PE	大規模なブランチ、データセンターのアプライアンス
6100-PE	大規模なブランチ、データセンターのアプライアンス

サポートされていない機能

次の機能は、Citrix SD-WAN 1000 SE/PE、Citrix SD-WAN 2000 SE/PE、および Citrix SD-WAN 4000 SE アプライアンスではサポートされていません。

- [IPv6](#)
- [SD-WAN アプライアンスの新しい UI](#)
- [外付け LTE USB モデム](#)
- [インバンド管理](#)
- [データインターフェイスとして使用される管理ポート](#)
- [DNS プロキシサービス](#)

- [802.1x サポート](#)
- [フォールバック構成](#)
- [Day-0/Day-N の設定](#)
- [ダイナミックルータ ID](#)
- [アドバンス Edition](#)
- [Wi-Fi](#)
- [LTE](#)
- [クラウドダイレクトサービス](#)
- [ECMP 負荷分散](#)
- [LACP ラグ](#)

アップグレード・パス

November 8, 2021

次の表は、以前のバージョンからアップグレードできるすべての Citrix SD-WAN ソフトウェアのバージョンの詳細を示しています。

SD-WAN	11.1	11.0	10.2	10.1	10	9.3.5	9.3.4	9.3	9.2
SD-WAN 11.0	✓								
SD-WAN 10.2	✓	✓							
SD-WAN 10.1	✓	✓	✓						
SD-WAN 10	✓	✓	✓	✓					
SD-WAN 9.3.5	✓	✓	✓	✓	✓				
SD-WAN 9.3.4	—	—	—	—	—	✓			
SD-WAN 9.3	—	—	—	—	—	✓	✓		
SD-WAN 9.2	—	—	—	—	—	✓	✓	✓	
SD-WAN 9.1	—	—	—	—	—	✓	✓	✓	✓

アップグレードパスの情報は、『[Citrix アップグレードガイド](#)』にも記載されています。

注

- Citrix SD-WAN リリース 9.3.x からアップグレードする場合は、メジャーリリースにアップグレードする前に 10.2.8 にアップグレードすることをお勧めします。

- ソフトウェアアップグレードの実行中は、アクティブ化する前に、接続されているすべてのサイトへのステージングが完了していることを確認してください。不完全な無視（Ignore Complete）を有効にしてステージングが完了する前にアクティベーションが行われた場合、ステージングがまだ進行中のサイトの MCN で仮想パスが表示されないことがあります。ネットワークをリカバリするには、それらのサイトのローカル変更管理を手動で実行する必要があります。
- Citrix SD-WAN リリース 11.0.0 以降、SD-WAN ソフトウェアの基盤となる OS/カーネルが新しいバージョンにアップグレードされます。アップグレードプロセス中に自動再起動を実行する必要があります。その結果、各アプライアンスのアップグレードに予想される時間が約 100 秒増加します。さらに、新しい OS を含めることで、各ブランチアプライアンスに転送されるアップグレードパッケージのサイズが約 90 MB 増加します。

仮想 WAN 展開で仮想 WAN ソフトウェアを 9.3.5 にアップグレードする

May 10, 2021

注:

MCN からブランチサイトへの仮想パスを確立して、9.3.4 以降のビルドを実行中の仮想 WAN 構成を作成します。

- MCN アプライアンスで、[構成] > [仮想 WAN] > [変更管理] に移動します。
- シトリックスのダウンロードページから Virtual WAN ネットワークのすべてのサイトの *cb-vw-
<ApplianceModel>-9.3.5.23.tar.gz* ファイルを取得します。
- <ApplianceModel> アップグレードを実行する必要がある構成ファイルで定義されたブランチの *cb-vw-
9.3.5.23.tar.gz* ファイルをアップロードします。MCN アプライアンスの SD-WAN Web インターフェイスで変更管理を実行し、変更管理プロセスを完了します。

Site Appliance	Model	State	Software	Currently Active	Currently Staged	Traffic Interruption	Download Package
MCN/OSite-Appliance	CB1000	active	8.1.0.95.472519	15:54 on 6/29/17		Loc Chg Mgt	active / none
Branch/OSite-Appliance	CB2000	active	8.1.0.95.472519	15:54 on 6/29/17		Loc Chg Mgt	active / none
Branch/400-Appliance	CB400	active	8.1.0.95.472519	15:54 on 6/29/17		Loc Chg Mgt	active / none
Branch/VW-Appliance	CBVFX	active	8.1.0.95.472519	15:54 on 6/29/17	8.1.0.95.472519	Loc Chg Mgt	active / none
VFX/loc/Branch-Appliance	CBVFX	active	8.1.0.95.472519	15:54 on 6/29/17	8.1.0.95.472519	Loc Chg Mgt	active / none

- [次へ] をクリックして、さらに進みます。

The screenshots illustrate the 'Upload and Verify Files' process in the Citrix SD-WAN 11.4 interface. The first screenshot shows the 'Upload and Verify Files' dialog with a file selected. The second screenshot shows the 'Verification Results' dialog indicating success. The third screenshot shows the 'License' dialog with the 'I accept the End User License Agreement' checkbox checked.

Configuration File Names: Active - Config_8_1_0_1k_MCN_2k_ven_esi_cb400_branch.cfg Staged -

Site Appliance	Model	State	Currently Active		Currently Staged		Traffic Interruption		Download Package
			Software	Config	Software	Config	Expected	Actual	
MCN1Site-Appliance	CB1000		8.1.0.95.472519	1554 on 6/29/17			Loc Chg Mgt		active / none
Branch2Site-Appliance	CB2000		8.1.0.95.472519	1554 on 6/29/17			Loc Chg Mgt		active / none
Branch400-Appliance	CB400		8.1.0.95.472519	1554 on 6/29/17			Loc Chg Mgt		active / none
BranchVPX-Appliance	CBVPX		8.1.0.95.472519	1554 on 6/29/17	8.1.0.95.472519		Loc Chg Mgt		active / none
VPX_Esi_Branch-Appliance	CBVPX		8.1.0.95.472519	1554 on 6/29/17	8.1.0.95.472519		Loc Chg Mgt		active / none

Verification Results

Status: Validation Success

This Configuration is valid. (version 1498754288)

Files created:

- Config_8_1_0_1k_MCN_2k_ven_esi_cb400_branch.xml
- Config_8_1_0_1k_MCN_2k_ven_esi_cb400_branch.xml.lst
- config_id_file.lst

License

CITRIX LICENSE AGREEMENT

This is a legal agreement ("AGREEMENT") between the end-user customer ("you"), and the providing Citrix entity (the applicable providing entity is hereinafter referred to as "CITRIX"). Your location of receipt of Citrix product (hereinafter "PRODUCT") and software maintenance (hereinafter "MAINTENANCE") determines the providing entity hereunder. Citrix Systems, Inc., a Delaware corporation, licenses the PRODUCT and provides MAINTENANCE in the Americas. Citrix Systems International GmbH, a Swiss company wholly owned by Citrix Systems, Inc., licenses the PRODUCT and provides MAINTENANCE in Europe, the Middle East, and Africa. Citrix Systems Asia Pacific Pty Ltd, licenses the PRODUCT and provides MAINTENANCE in Asia and the Pacific (excluding Japan). Citrix Systems Japan KK licenses the PRODUCT and provides MAINTENANCE in Japan. BY INSTALLING AND/OR USING THE PRODUCT, YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, DO NOT INSTALL AND/OR USE THE PRODUCT. Nothing contained in any purchase order or any other document submitted by you shall in any way modify or add to the terms and conditions contained in this AGREEMENT.

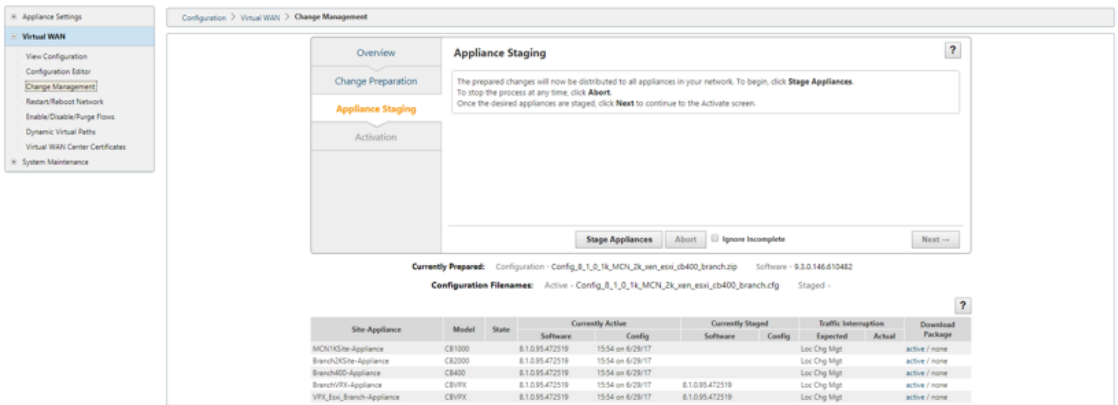
1. PRODUCT LICENSES.

a. End User Licenses. The PRODUCT is made available by CITRIX under the license models identified at <http://www.citrix.com/buy/licensing/product.html>. Notwithstanding anything set forth in this AGREEMENT or at the referenced website, your use of Open Source Software shall in all ways be exclusively governed by the open source license indicated as applicable to the code at <http://www.citrix.com/buy/licensing/open-source.html>. "Open Source Software" means those portions of the PRODUCT that are made available by CITRIX under an open source license (e.g., a version of a GNU General Public License).

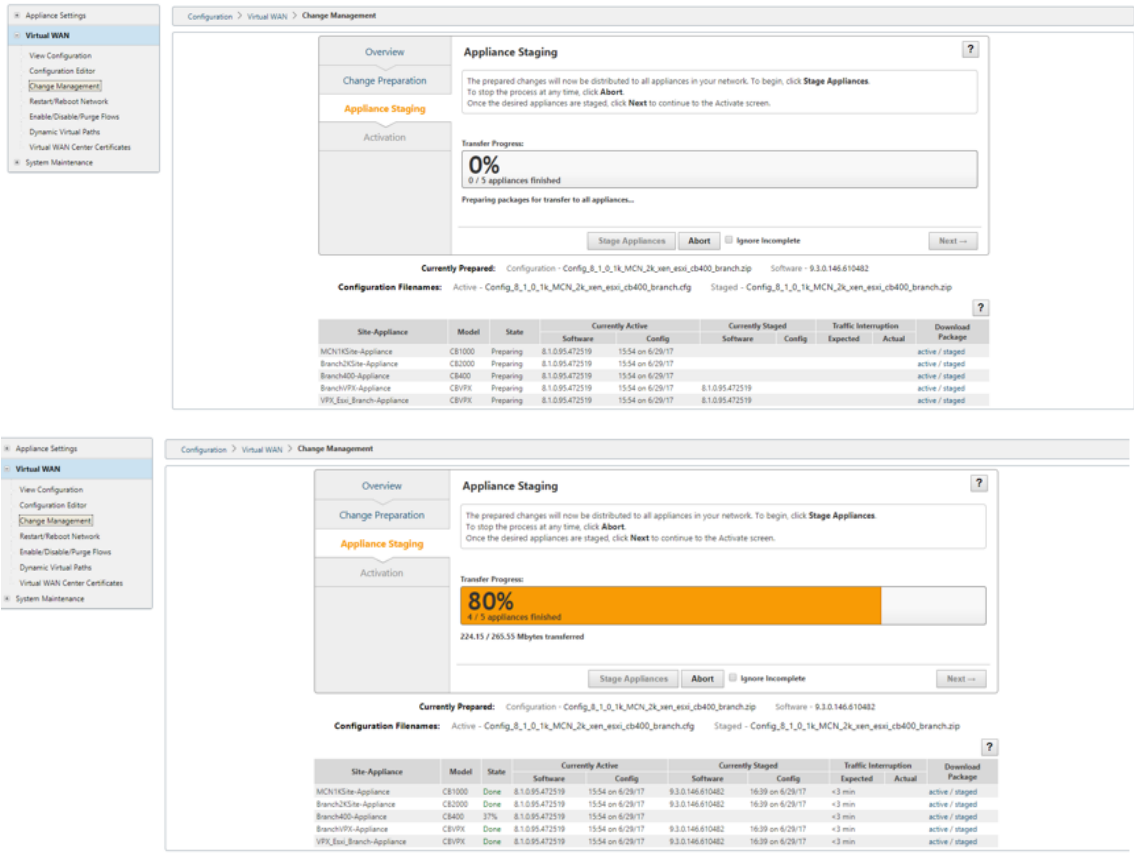
You must accept the license terms before installing the new package.

☒ I accept the End User License Agreement.

5. ライセンス契約に同意すると、アプライアンスのステージングに移動します。アプライアンスをステージングするには、アプライアンスのステージングをクリックします。



6. 「転送の進行状況」ステータスは、アプライアンスにソフトウェア・パッケージを準備およびステージングの一部として表示されます。



7. 転送の進行状況が 100% と表示されたら、[次へ] をクリックして続行します。

Appliance Staging

The prepared changes will now be distributed to all appliances in your network. To begin, click **Stage Appliances**. To stop the process at any time, click **Abort**. Once the desired appliances are staged, click **Next** to continue to the Activate screen.

Transfer Progress: 100%

Appliance Staging complete. You may now proceed to Activation.

Currently Prepared: Configuration - Config_8_1_0_1k_MCN_2k_xen_essl_cb400_branch.zip Software - 9.3.0.146.610482

Configuration Filenames: Active - Config_8_1_0_1k_MCN_2k_xen_essl_cb400_branch.cfg Staged - Config_8_1_0_1k_MCN_2k_xen_essl_cb400_branch.zip

Site Appliance	Model	State	Currently Active		Currently Staged		Traffic Interruption		Download Package
			Software	Config	Software	Config	Expected	Actual	
MCN1KSite-Appliance	CB1000	Done	8.1.0.95.472519	15:54 on 6/29/17	9.3.0.146.610482	16:39 on 6/29/17	<3 min		active / staged
Branch2KSite-Appliance	CB2000	Done	8.1.0.95.472519	15:54 on 6/29/17	9.3.0.146.610482	16:39 on 6/29/17	<3 min		active / staged
Branch400-Appliance	CB400	Done	8.1.0.95.472519	15:54 on 6/29/17	9.3.0.146.610482	16:39 on 6/29/17	<3 min		active / staged
BranchVPX-Appliance	CBVPX	Done	8.1.0.95.472519	15:54 on 6/29/17	9.3.0.146.610482	16:39 on 6/29/17	<3 min		active / staged
VPX_Essl_Branch-Appliance	CBVPX	Done	8.1.0.95.472519	15:54 on 6/29/17	9.3.0.146.610482	16:39 on 6/29/17	<3 min		active / staged

8. [アクティブ化] ページで、[ステージングのアクティブ化] をクリックしてアクティブ化を開始します。

Activate

You may now activate the changes that have been distributed across your network. Each appliance will apply the changes and restart the Virtual WAN Service.

Note: A reboot or loss of power during this operation may result in an incomplete installation which could require manual installation to resolve. Click **Activate Staged** to begin.

Activate Staged in: 10 seconds

Currently Prepared: Configuration - Config_8_1_0_1k_MCN_2k_xen_essl_cb400_branch.zip Software - 9.3.0.146.610482

Configuration Filenames: Active - Config_8_1_0_1k_MCN_2k_xen_essl_cb400_branch.cfg Staged - Config_8_1_0_1k_MCN_2k_xen_essl_cb400_branch.zip

Site Appliance	Model	State	Currently Active		Currently Staged		Traffic Interruption		Download Package
			Software	Config	Software	Config	Expected	Actual	
MCN1KSite-Appliance	CB1000	Done	8.1.0.95.472519	15:54 on 6/29/17	9.3.0.146.610482	16:39 on 6/29/17	<3 min		active / staged
Branch2KSite-Appliance	CB2000	Done	8.1.0.95.472519	15:54 on 6/29/17	9.3.0.146.610482	16:39 on 6/29/17	<3 min		active / staged
Branch400-Appliance	CB400	Done	8.1.0.95.472519	15:54 on 6/29/17	9.3.0.146.610482	16:39 on 6/29/17	<3 min		active / staged
BranchVPX-Appliance	CBVPX	Done	8.1.0.95.472519	15:54 on 6/29/17	9.3.0.146.610482	16:39 on 6/29/17	<3 min		active / staged
VPX_Essl_Branch-Appliance	CBVPX	Done	8.1.0.95.472519	15:54 on 6/29/17	9.3.0.146.610482	16:39 on 6/29/17	<3 min		active / staged

Activate

You may now activate the changes that have been distributed across your network. Each appliance will apply the changes and restart the Virtual WAN Service.

Note: A reboot or loss of power during this operation may result in an incomplete installation which could require manual installation to resolve. Click **Activate Staged** to begin.

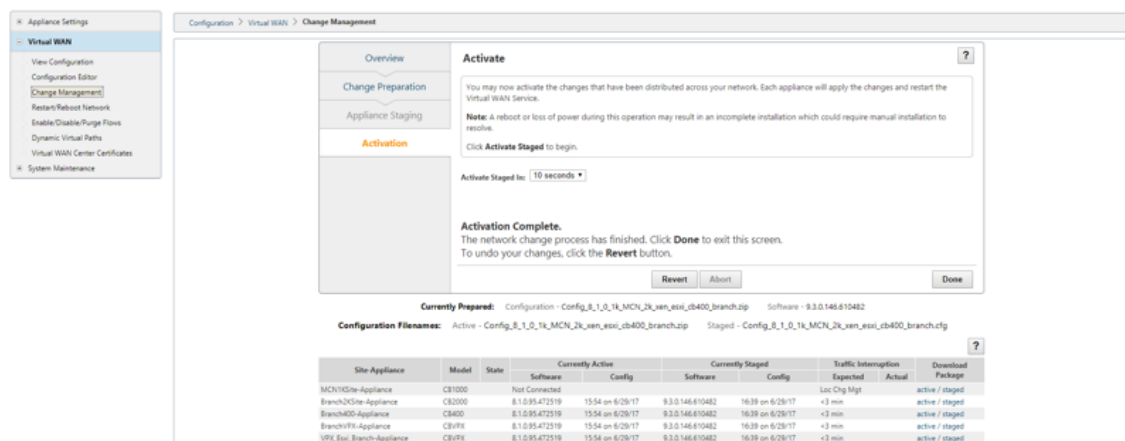
Activate Staged in: 10 seconds

Currently Prepared: Configuration - Config_8_1_0_1k_MCN_2k_xen_essl_cb400_branch.zip Software - 9.3.0.146.610482

Configuration Filenames: Active - Config_8_1_0_1k_MCN_2k_xen_essl_cb400_branch.cfg Staged - Config_8_1_0_1k_MCN_2k_xen_essl_cb400_branch.zip

Site Appliance	Model	State	Currently Active		Currently Staged		Traffic Interruption		Download Package
			Software	Config	Software	Config	Expected	Actual	
MCN1KSite-Appliance	CB1000	Done	8.1.0.95.472519	15:54 on 6/29/17	9.3.0.146.610482	16:39 on 6/29/17	<3 min		active / staged
Branch2KSite-Appliance	CB2000	Done	8.1.0.95.472519	15:54 on 6/29/17	9.3.0.146.610482	16:39 on 6/29/17	<3 min		active / staged
Branch400-Appliance	CB400	Done	8.1.0.95.472519	15:54 on 6/29/17	9.3.0.146.610482	16:39 on 6/29/17	<3 min		active / staged
BranchVPX-Appliance	CBVPX	Done	8.1.0.95.472519	15:54 on 6/29/17	9.3.0.146.610482	16:39 on 6/29/17	<3 min		active / staged
VPX_Essl_Branch-Appliance	CBVPX	Done	8.1.0.95.472519	15:54 on 6/29/17	9.3.0.146.610482	16:39 on 6/29/17	<3 min		active / staged

9. 180 秒のアクティベーションカウントダウンが完了したら、[完了] をクリックします。



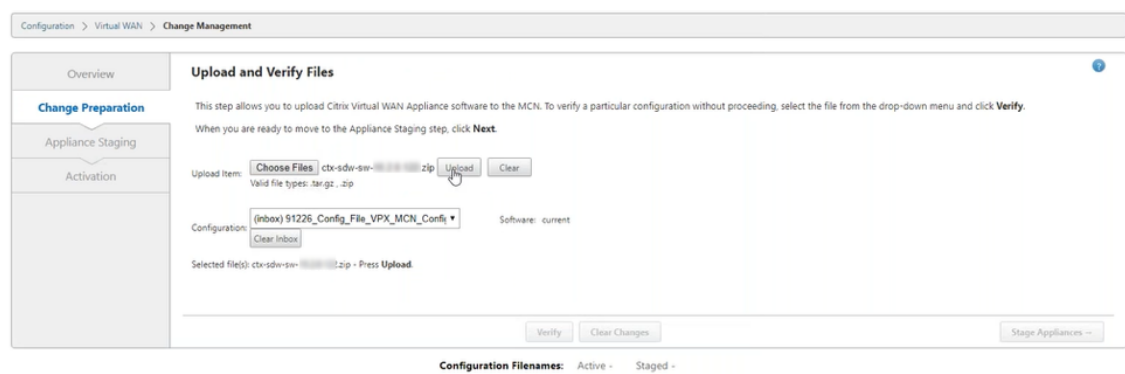
稼働中の仮想 WAN 展開で 11.4 にアップグレードする

November 8, 2021

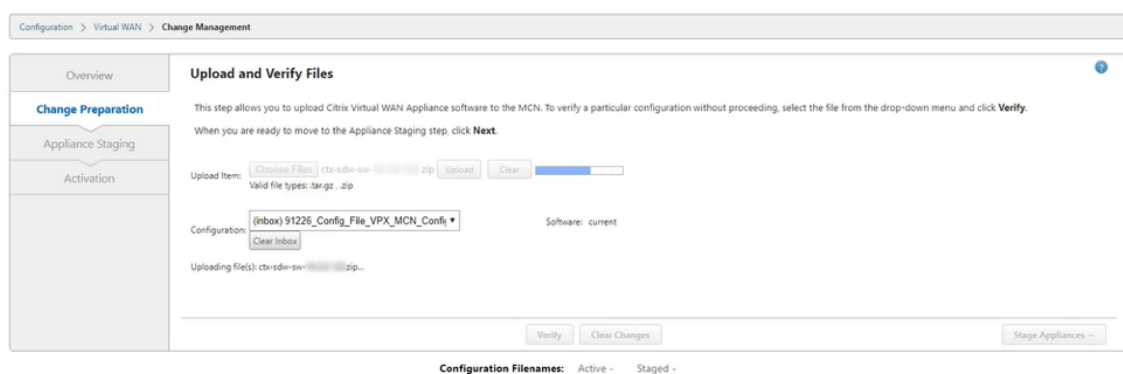
1. 「変更管理」>「変更準備」ページで、「ファイルを選択」をクリックし、*ctx-sdw-sw-11.4.0.x.zip* ソフトウェアパッケージファイルを選択します。[アップロード] をクリックします。

注:

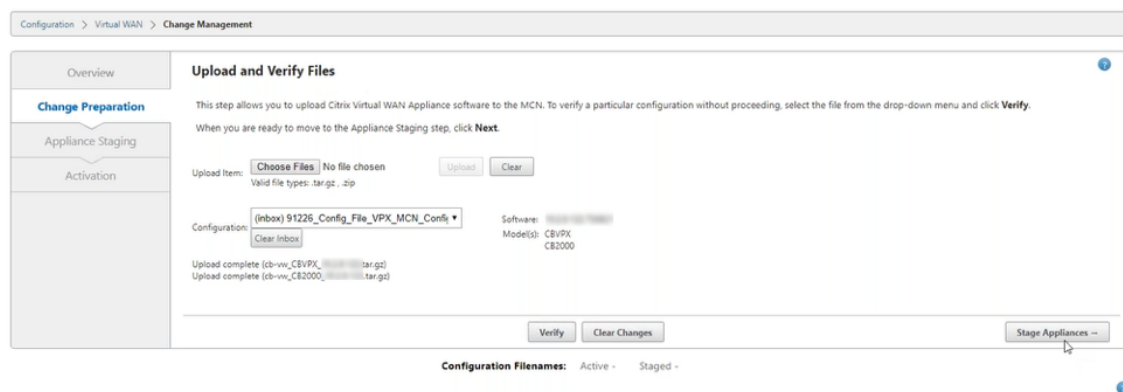
Citrix SD-WAN リリース 11.4 ソフトウェアパッケージは、[ダウンロード] ページからダウンロードできます。



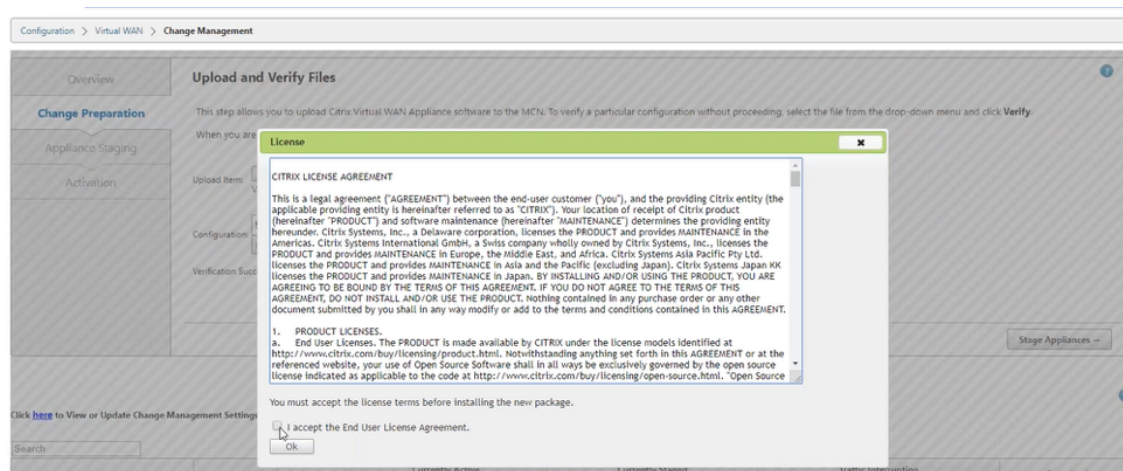
進行状況バーが表示され、現在のアップロードの進行状況が表示されます。



2. アップロードプロセスが成功すると、関連するアプライアンスモデルが表示されます。アプライアンスは、構成ファイルに基づいてアップグレードされます。



3. [アプライアンスのステージング] をクリックして、設定ファイルの検証を続行します。ユーザー同意の [使用許諾契約] ページが表示されます。「エンドユーザー使用許諾契約書に同意します」をクリックし、「OK」をクリックします。



4. アプライアンスのステージングプロセスが開始されます。変更は、ネットワーク上のすべてのアプライアンスに配布されます。転送の進行状況バーが表示され、サイト詳細テーブルが更新されます。

Overview

Change Preparation

Appliance Staging

Activation

Appliance Staging

The prepared changes will now be distributed to all appliances in your network.
To stop the process at any time, click **Abort**.
Once the desired appliances are staged, click **Next** to continue to the Activate screen.

Transfer Progress:

0%

0 / 3 appliances finished

Prepare Packages (0 / 3 packages prepared)

Stage Packages

Done

Abort

Ignore Incomplete

Next --

Currently Prepared: Configuration - 91226_Config_File_VPX_MCN_Config_test.zip Software -

Configuration Filenames: Active - Staged -

[Click here to View or Update Change Management Settings.](#)

Search

Site-Appliance	Model	State	Currently Active		Currently Staged		Traffic Interruption		Download Package
			Software	Config	Software	Config	Expected	Actual	
CB2k8Branch-Branch	CB2000	Preparing	Not Connected				Loc Chg Mgt		none / staged
CBVPX8Branch-Branch	CBVPX	Preparing	Not Connected				Loc Chg Mgt		none / staged
CBVPX_MCN-Appliance	CBVPX	Preparing	Not Connected				Loc Chg Mgt		none / staged

Activate windows

5. 転送の進行状況が 100% 完了したら、[次へ] をクリックしてアクティベーションに進みます。

Overview

Change Preparation

Appliance Staging

Activation

Appliance Staging

The prepared changes will now be distributed to all appliances in your network.
To stop the process at any time, click **Abort**.
Once the desired appliances are staged, click **Next** to continue to the Activate screen.

Transfer Progress:

100%

Appliance Staging complete. You may now proceed to Activation.

Prepare Packages

Stage Packages

Done

Abort

Ignore Incomplete

Next --

Currently Prepared: Configuration - Multir_dvp9_ipsecFIPS.zip Software - Current Running

Configuration Filenames: Active - Multir_dvp9_ipsecFIPS.zip Staged - Multir_dvp9_ipsecFIPS.zip

[Click here to View or Update Change Management Settings.](#)

Global Multi-Region Summary

Search

Region	Total Sites	Not Connected	Preparing/Staging	Staged	Failed
Default_Region	4	0	0	4	0
APAC_r1	2	0	0	2	0
AMEA_r1	23	0	0	23	0

Region - Default_Region Details

Show 25 entries

Search

Customize

Refresh

Site-Appliance	Model	State	Currently Active		Currently Staged		Traffic Interruption		Download Package
			Software	Config	Software	Config	Expected	Actual	
MCN1-MCN1-CB4100	CB4100	<div></div>		12:56 on 2/23/18	<div></div>	11:56 on 2/23/18	<1 sec	371 ms	active / staged
APAC_RCN-APAC_RCN-CB1000	CB1000	<div></div>		12:56 on 2/23/18	<div></div>	11:56 on 2/23/18	<1 sec	269 ms	active / staged
BR1-BR1-CBVPXL	CBVPXL	<div></div>		12:56 on 2/23/18	<div></div>	11:56 on 2/23/18	<1 sec	304 ms	active / staged
RCN01-2000-RCN01-2000	CB2000	<div></div>		12:56 on 2/23/18	<div></div>	11:56 on 2/23/18	<1 min	183 ms	active / staged

Previous

1

Next

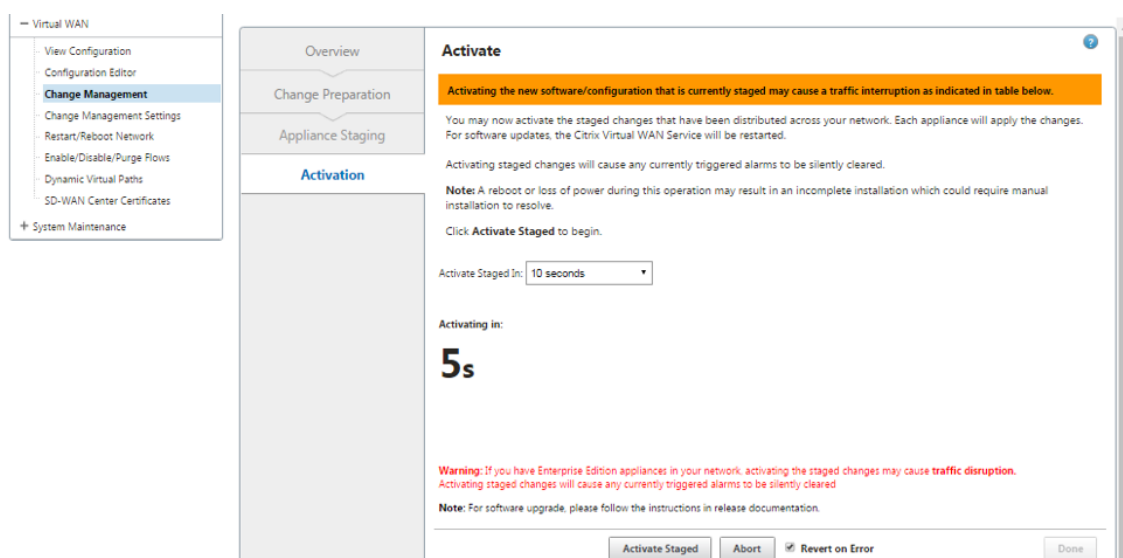
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

91

サマリーテーブルに表示されるソフトウェアパッケージ設定のさまざまな状態は、次のことを示しています。

- 準備中 - アプライアンスに転送するアップデートパッケージを準備するローカル処理。
- リージョンパッケージの準備 - RCN に転送する更新パッケージを準備するローカル処理。(RCN がネットワークの一部である場合に適用されます)。
- **Percentage** - アプライアンスに転送されたパッケージの割合。
- アンパック - アップデートパッケージを適用するためのリモートアプライアンス処理。
- リージョンを転送中 - パッケージは RCN に転送されています。(RCN がネットワークの一部である場合に適用されます)。
- **Failed** - リモートで不完全な転送が検出されました。
- キャンセル - ステージアプライアンスの間に「不完全を無視」がチェックされたときにユーザーによってキャンセルされました
- 不要 - 準備済みステージングパッケージには、このサイトアプライアンス名が含まれていません。
- 未接続 - ローカルはリモートのアクティブなパッケージ情報を見ることができません。

6. ステージングされたソフトウェアをアクティブ化するには、[Activate Staged] をクリックします。



7. カウントダウン後、アクティブ化が完了したことを示すメッセージが表示されます。[完了] をクリックします。

View Configuration

Configuration Editor

Change Management

Change Management Settings

Restart/Reboot Network

Enable/Disable/Purge Flows

Dynamic Virtual Paths

SD-WAN Center Certificates

System Maintenance

Overview

Change Preparation

Appliance Staging

Activation

Activate

Activating the new software/configuration that is currently staged may cause a traffic interruption as indicated in table below.

You may now activate the staged changes that have been distributed across your network. Each appliance will apply the changes. For software updates, the Citrix Virtual WAN Service will be restarted.

Activating staged changes will cause any currently triggered alarms to be silently cleared.

Note: A reboot or loss of power during this operation may result in an incomplete installation which could require manual installation to resolve.

Click **Activate Staged** to begin.

Activate Staged In: 10 seconds

Activation Complete.

The network change process has finished. Click **Done** to exit this screen.

To undo your changes, click the **Revert** button.

Revert

Abort

Done

Currently Prepared:

Configuration - Multir_dvp9_ipsecFIPS.zip

Software - Current Running

Configuration Filenames:

Active - Multir_dvp9_ipsecFIPS.zip

Staged - Multir_dvp9_ipsecFIPS.zip

Click [here](#) to View or Update Change Management Settings.

Global Multi-Region Summary

Search

Region	Total Sites	Not Connected	Preparing/Staging	Staged	Failed
Default_Region	4	0	0	0	0
AMEA_r1	23	0	0	0	0
APAC_r1	2	0	0	0	0

Region - Default_Region Details

Show 25 entries

Search

Customize

Refresh

Site-Appliance	Model	State	Currently Active		Currently Staged		Traffic Interruption		Download Package
			Software	Config	Software	Config	Expected	Actual	
MCN1-MCN1-CB4100	CB4100	Done		13:15 on 2/23/18		13:43 on 2/23/18	0 sec		active / staged
APAC_RCN-APAC_RCN-CB1000	CB1000	Done		13:15 on 2/23/18		13:43 on 2/23/18	0 sec		active / staged
BR1-BR1-CBV9XL	CBV9XL	Done		13:15 on 2/23/18		13:43 on 2/23/18	0 sec		active / staged
RCN01-2000-RCN01-2000	CB2000	Done		13:15 on 2/23/18		13:43 on 2/23/18	0 sec		active / staged

Previous 1 Next

8. 「変更管理」 ページに移動して、転送ステータスを表示します。

Configuration > Virtual WAN > Change Management

Details

Active Configuration:
MCN2k_BlackWidowConnect
ed_v1_New_BR210LTE_2100_Gateway
mode_v7.db

Staged Configuration:
MCN2k_BlackWidowConnect
ed_v1_New_BR210LTE_2100_Gateway
mode_v7.db

Prepared Configuration:
MCN2k_BlackWidowConnect
ed_v1_New_BR210LTE_2100_Gateway
mode_v7.db

Overview

Change Preparation

Appliance Staging

Activation

Step 1
Upload Files to MCN

Step 2
Transfer Files to Clients

Step 3
Activate Change

Clicking the **Activate Staged** button will skip to the Appliance Staging step, where you may switch to a previously-staged appliance package (if present).

Activate Staged

Begin →

Global Multi-Region Summary

Search

Region	Total Sites	Not Connected	Connected	Traffic Impacted	No Traffic Impact	Staging		
						In Progress	Completed	Failed
Default_Region	4	0	4	4	0	0	2	0
region2	2	1	1	0	2	0	1	0
region1	4	1	3	2	2	0	1	0

Region - region1 Details of Traffic Impacted Sites

Customize

Refresh

Show 25 entries

Search

Site-Appliance	Model	State	Currently Active		Currently Staged		Traffic Interruption		Download Package
			Software	Config	Software	Config	Expected	Actual	
R1-Site1-BLR-R1-Site1-BLR-CBVPX	VPX		10.2.8.116.790218	11:34 on 12/10/18	10.2.8.117.790218	6:30 on 12/10/18	<3 min	194 ms	active / staged
R1-Site1-BLR-New_HA_Appliance	VPX		10.2.8.116.790218	11:34 on 12/10/18	10.2.8.117.790218	6:30 on 12/10/18	<3 min	192 ms	active / staged

Previous

1

Next

複数リージョンのサマリーテーブルには、次の詳細が表示されます。

- リージョン-リージョンの名前
- サイト合計 -リージョン内のサイトの合計数。
- NotConnected** -リージョン内で接続されていないサイトの総数。
- Connected** -リージョン内で接続されているサイトの総数。
- 影響を受けたトラフィック -リージョン内でトラフィックが影響を受けるサイトの総数。
- トラフィックへの影響なし -リージョン内でトラフィックが影響を受けていないサイトの総数。
- Staging In Progress** -ローカル処理がリージョン内で転送用の更新パッケージを準備しようとしているサイトの総数。
- ステージング完了: リージョン内でステージングが完了したサイトの合計数。
- ステージング失敗 -リージョン内で不完全な転送が削除されたサイトの総数。

Global Multi-Region Summary

Search

Region	Total Sites	Not Connected	Connected	Traffic Impacted	No Traffic Impact	Staging		
						In Progress	Completed	Failed
Default_Region	4	0	4	4	0	0	2	0
region2	2	1	1	0	2	0	1	0
region1	4	1	3	2	2	0	1	0

グローバルマルチリージョン概要テーブルエントリリンクをクリックして、リージョン固有の設定レポートをフィルタリングします。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

94

Region - Default Region Details of Connected Sites

Show 25 entries Search

Customize Refresh

Site-Appliance	Model	State	Currently Active		Currently Staged		Traffic Interruption		Download Package
			Software	Config	Software	Config	Expected	Actual	
MCN-NY-MCN-NY-CB2000	2000		10.2.2.117.75002/18	11:34 on 12/10/18	10.2.2.117.75002/18	6:30 on 12/10/18	<3 min	82 s	active / staged
Def-Site1-SC-Def-Site1-SC-CBVPX	VPX		10.2.2.117.75002/18	11:34 on 12/10/18	10.2.2.117.75002/18	6:30 on 12/10/18	<3 min	209 s	active / staged
R1-RCN-MUM-R1-RCN-MUM-CBVPX	VPX	Done(auto)	10.2.2.117.75002/18	11:34 on 12/10/18	10.2.2.117.75002/18	6:30 on 12/10/18	<3 min	195 s	active / staged
R2-RCN-SA-R2-RCN-SA-CBVPX	VPX	Done(auto)	10.2.2.117.75002/18	11:34 on 12/10/18	10.2.2.117.75002/18	6:30 on 12/10/18	<3 min	199 s	active / staged

Previous 1 Next

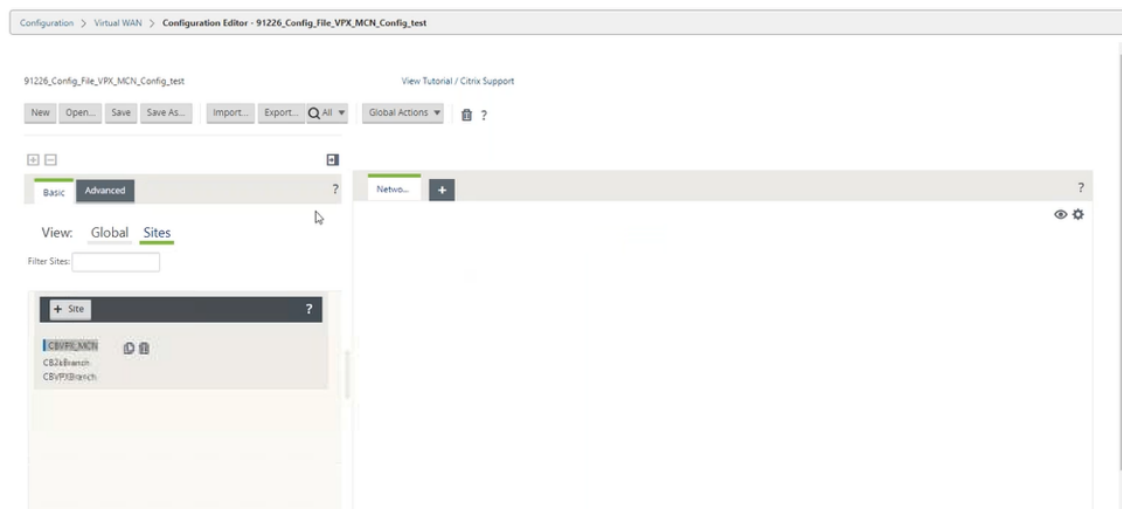
マルチリージョン展開の場合、各 RCN で [変更管理の設定] ページに移動し、依存コンポーネントのインストールをスケジュールします。デフォルトでは、MCN/RCN は、ブランチでのソフトウェアの可用性に基づいて、毎日 21:20:00 にスケジュールインストールを試みるよう割り当てます。詳細については、「[変更管理の設定](#)」を参照してください。

仮想 WAN 展開を動作させずに 11.4 にアップグレードする

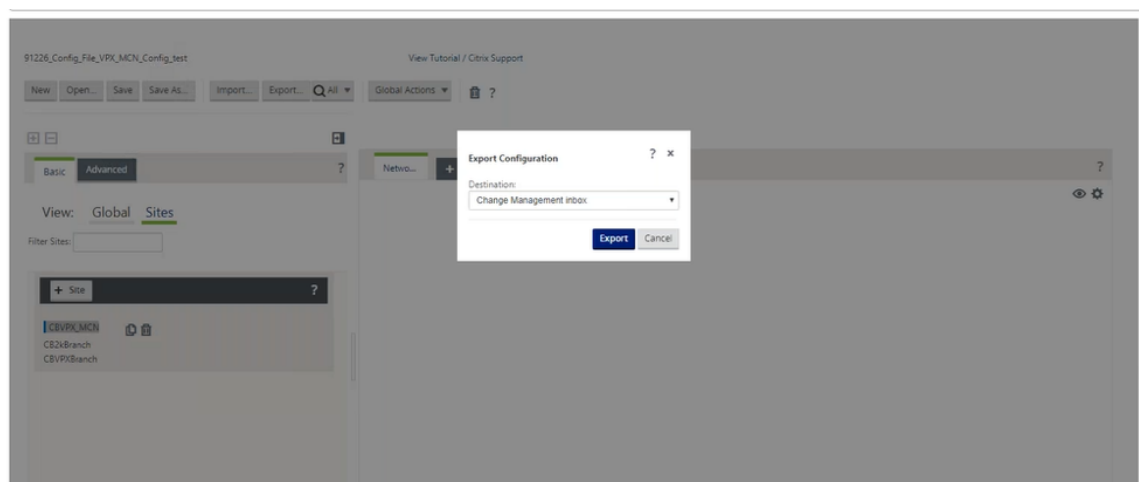
November 8, 2021

注：最新の 11.4 機能を設定するには、MCN アプライアンスを 11.4 ソフトウェアに再接続します。詳しくは、「[Citrix SD-WAN アプライアンスソフトウェアのイメージの再設定](#)」を参照してください。

1. 構成 エディタを使用して構成 を準備し、有効な名前前で構成を保存します。詳細については、「[構成](#)」トピックを参照してください。



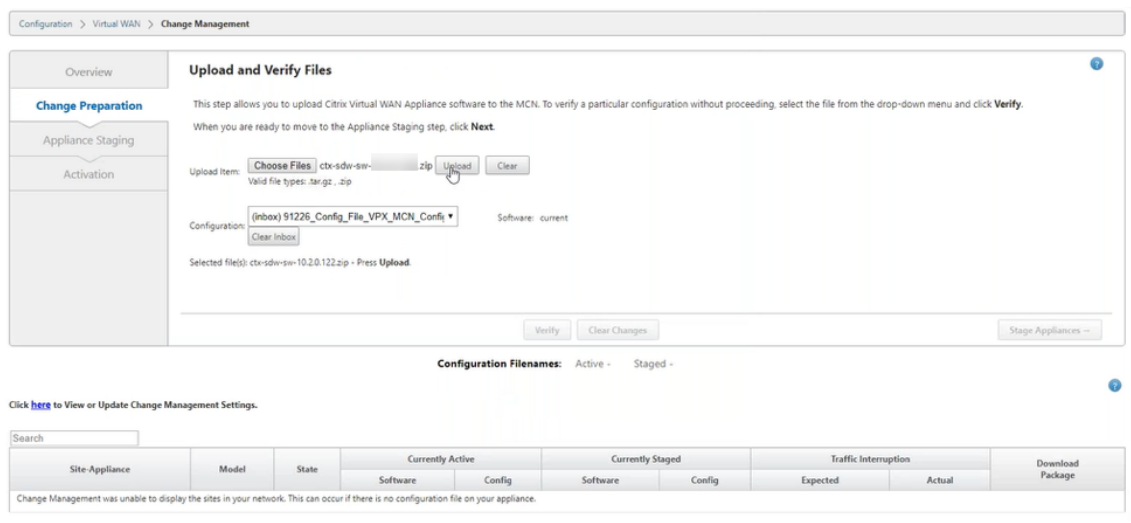
2. 保存した構成を変更管理にエクスポートします。[エクスポート] をクリックし、宛先として [変更管理の受信トレイ] を選択します。[エクスポート] をクリックします。



3. 「変更管理」>「変更準備」ページで、「ファイルを選択」をクリックし、*ctx-sdw-sw-11.4.0.x.zip* ソフトウェアパッケージファイルを選択します。[アップロード] をクリックします。

注:

Citrix SD-WAN リリース 11.4 ソフトウェアパッケージは、[\[ダウンロード\]](#) ページからダウンロードできます。



進行状況バーが表示され、現在のアップロードの進行状況が表示されます。

Configuration > Virtual WAN > Change Management

Overview

Change Preparation

Appliance Staging

Activation

Upload and Verify Files

This step allows you to upload Citrix Virtual WAN Appliance software to the MCN. To verify a particular configuration without proceeding, select the file from the drop-down menu and click **Verify**. When you are ready to move to the Appliance Staging step, click **Next**.

Upload Item: cti-sdw-sw-...zip

Valid file types: tar.gz, .zip

Configuration: (inbox) 91226_Config_File_VPX_MCN_Config Software: current

Uploading file(s): cti-sdw-sw-...zip...

Configuration Filenames: Active - Staged -

Click [here](#) to View or Update Change Management Settings.

Site-Appliance	Model	State	Currently Active		Currently Staged		Traffic Interruption		Download Package
			Software	Config	Software	Config	Expected	Actual	
Change Management was unable to display the sites in your network. This can occur if there is no configuration file on your appliance.									

4. アップロードプロセスが成功すると、各ブランチプラットフォームモデルに関する情報を含む構成ファイルに基づいてアップグレードされる関連モデルが表示されます。

Configuration > Virtual WAN > Change Management

Overview

Change Preparation

Appliance Staging

Activation

Upload and Verify Files

This step allows you to upload Citrix Virtual WAN Appliance software to the MCN. To verify a particular configuration without proceeding, select the file from the drop-down menu and click **Verify**. When you are ready to move to the Appliance Staging step, click **Next**.

Upload Item: No file chosen

Valid file types: tar.gz, .zip

Configuration: (inbox) 91226_Config_File_VPX_MCN_Config Software:

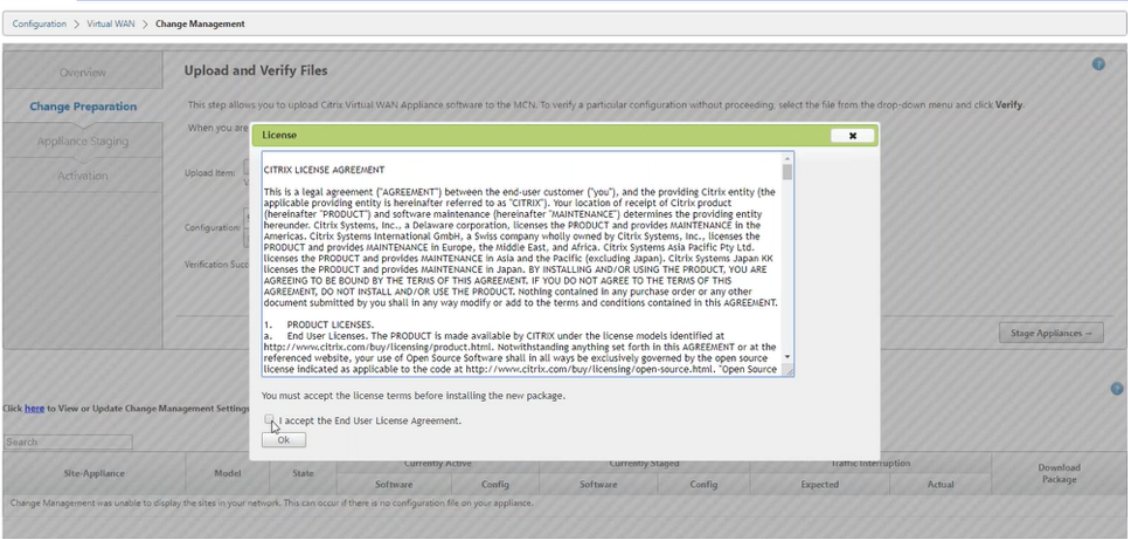
Upload complete (cb-vw-CBVPX-...tar.gz)
Upload complete (cb-vw-CB2000-...tar.gz)

Configuration Filenames: Active - Staged -

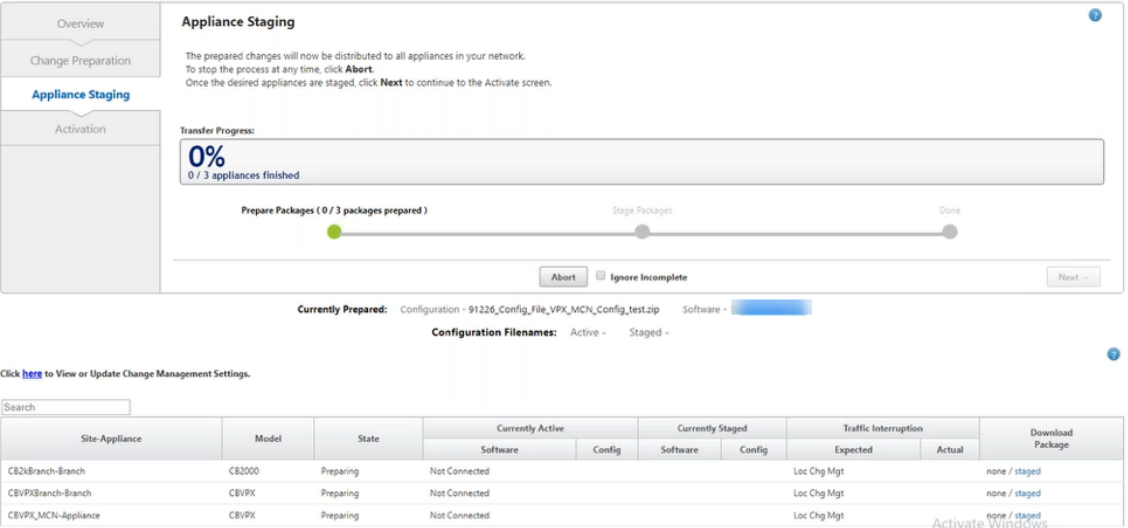
Click [here](#) to View or Update Change Management Settings.

Site-Appliance	Model	State	Currently Active		Currently Staged		Traffic Interruption		Download Package
			Software	Config	Software	Config	Expected	Actual	
Change Management was unable to display the sites in your network. This can occur if there is no configuration file on your appliance.									

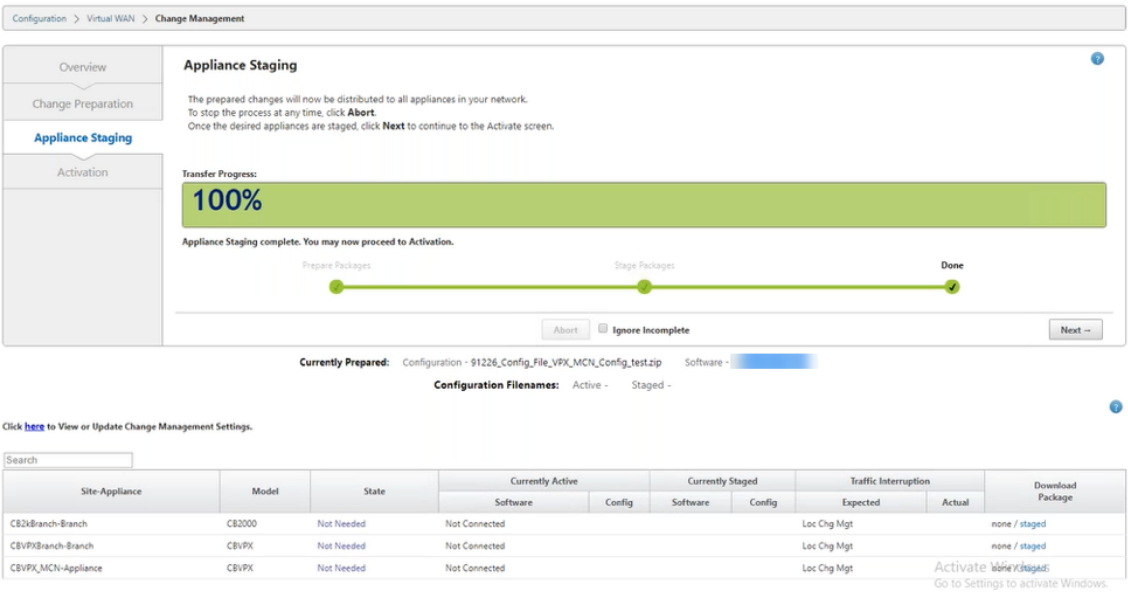
5. [アプライアンスのステージング] をクリックして、設定ファイルの検証を続行します。ユーザー同意の [使用許諾契約] ページが表示されます。「エンドユーザー使用許諾契約書に同意します」をクリックし、「OK」をクリックします。



6. アプライアンスのステージングプロセスが開始され、ネットワーク上のすべてのアプライアンスに変更が配信されます。転送の進行状況バーが表示され、サイト詳細テーブルが更新されます。

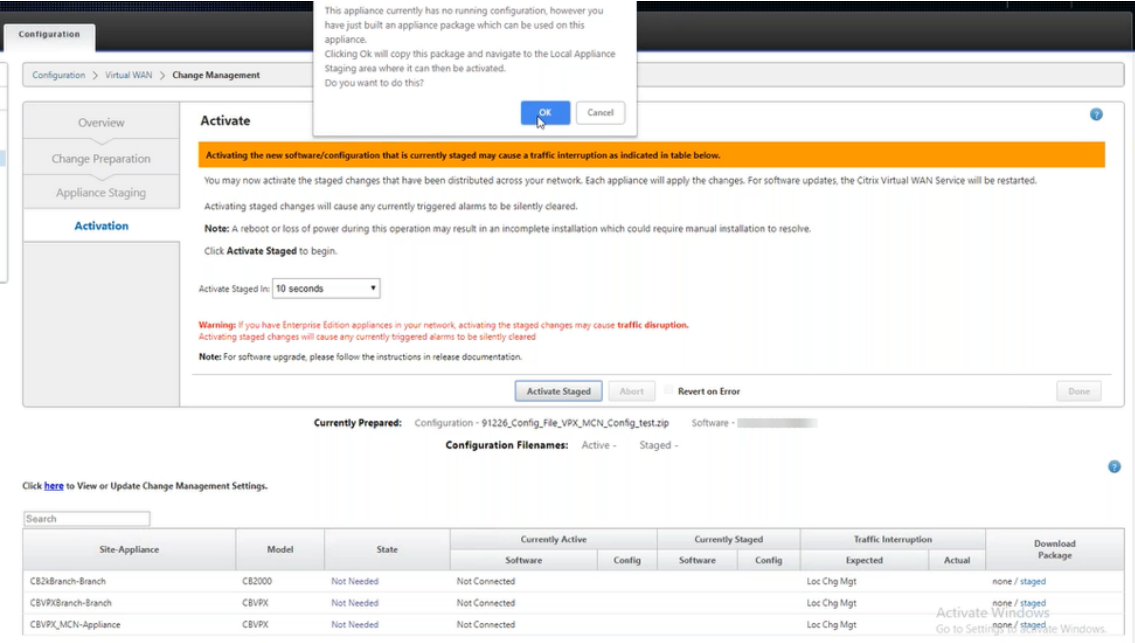


7. 転送の進行状況が 100% 完了したら、[次へ] をクリックしてアクティベーションに進みます。

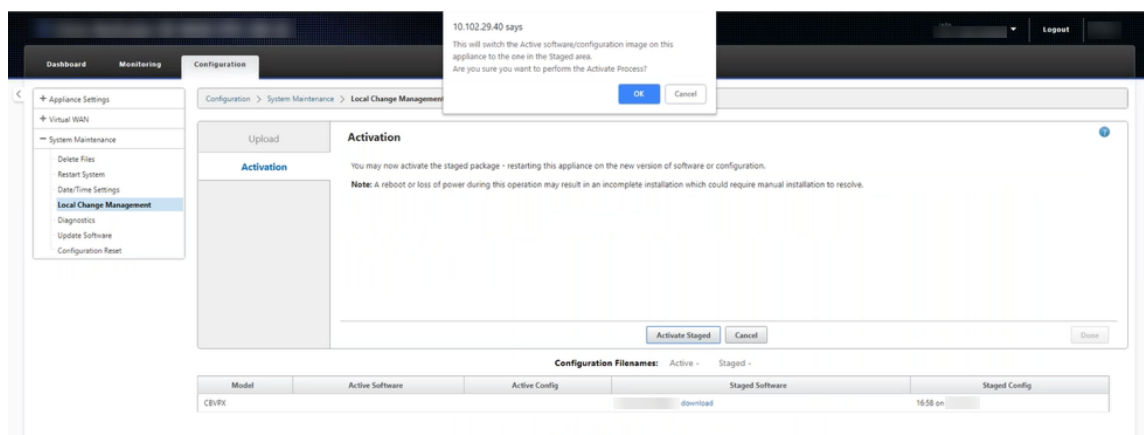


8. [ステージングを有効化] をクリックします。アプライアンスが初めてステージングされるときに、ユーザー承認のポップアップメッセージが表示されます。

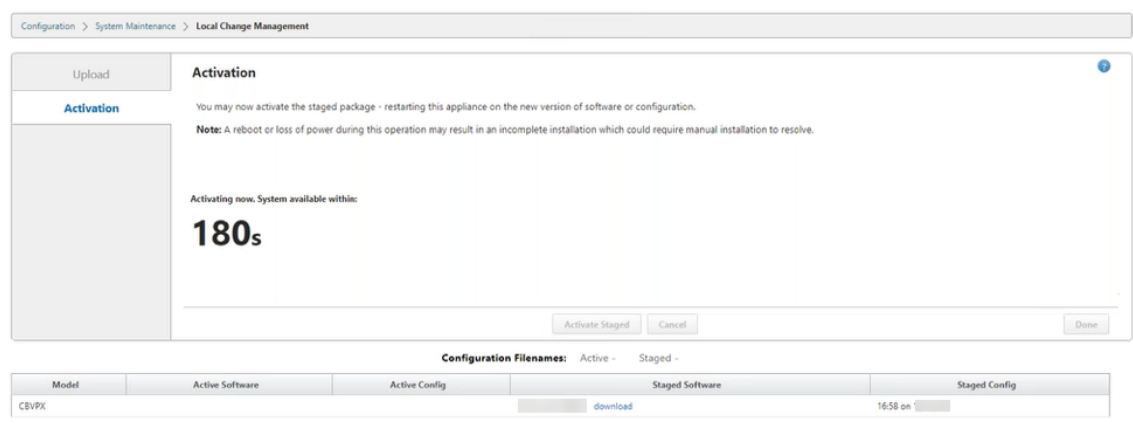
ローカルアプライアンスをアクティブ化するための [ローカル変更管理] ページにリダイレクトされます。「OK」をクリックして続行します。



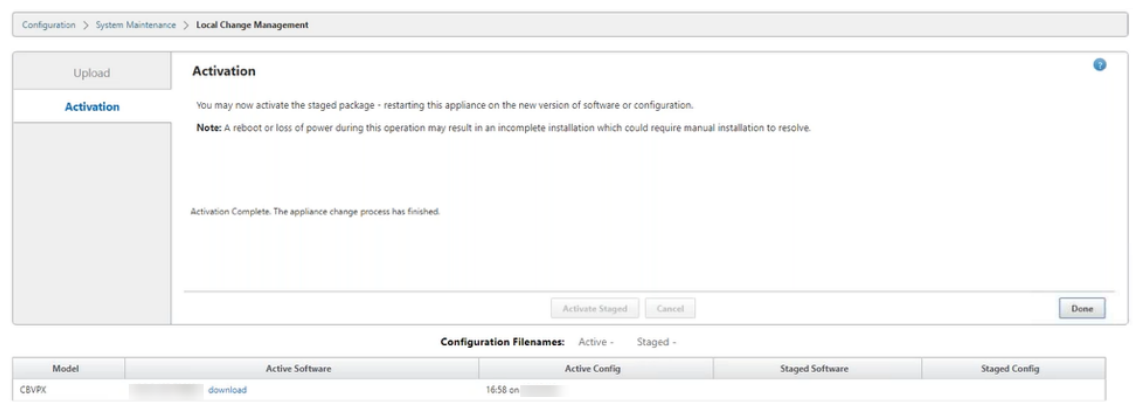
9. [ローカル変更管理でステージングをアクティブ化] をクリックします。アクティベーション確認メッセージが表示されます。[OK] をクリックします。



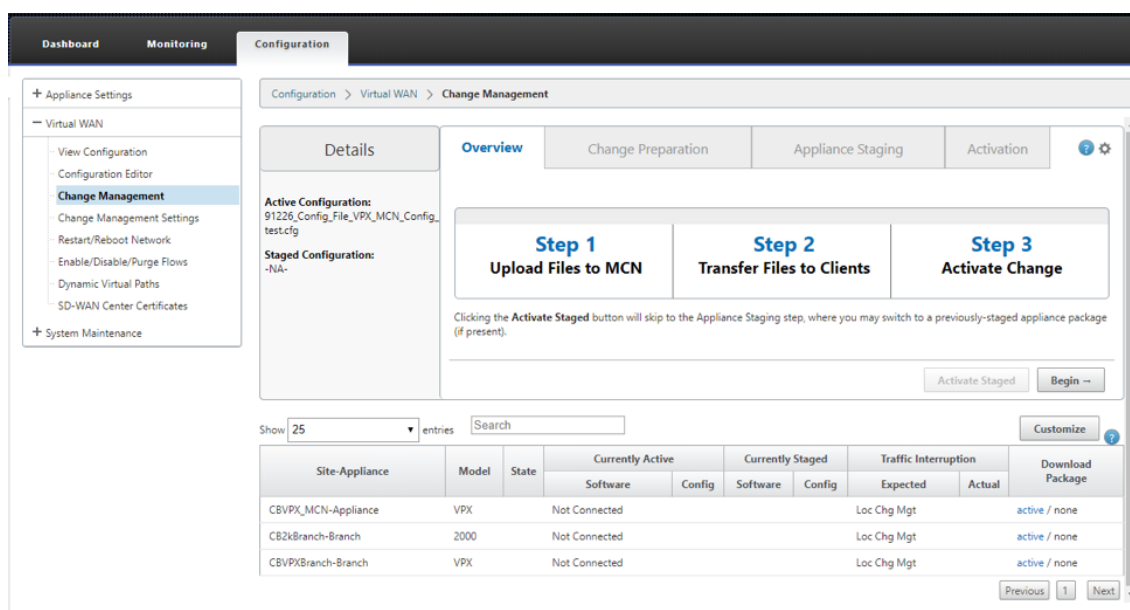
アクティベーションは 180 秒のカウントダウンタイマーから始まります。



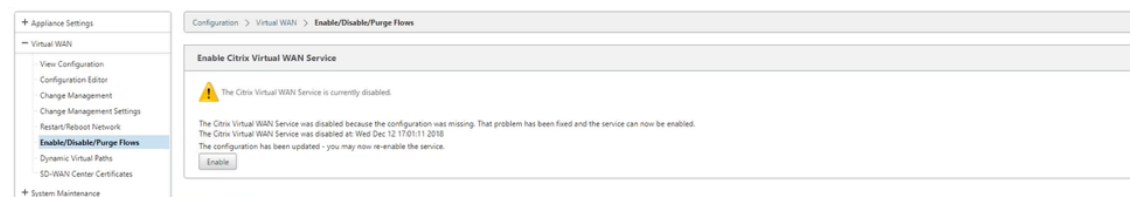
10. カウントダウン後、アクティブ化が完了したことを示すメッセージが表示されます。[**Done**] をクリックすると、アプライアンスが再起動します。



11. アプライアンスが再起動したら、[**Change Management**] ページに移動し、仮想 WAN ソフトウェアアップグレードのみでネットワークにブートストラップする必要がある各ブランチのローカル変更管理パッケージをダウンロードします。



12. アプライアンスで SD-WAN サービスを有効にします。仮想 **WAN** > 有効/無効/ページフローにナビゲートし、『**Enable**』をクリックして下さい。



ネットワークに新しいサイトをさらに構成して追加するには、「[ブランチノードの設定](#)」トピックの手順に従います。

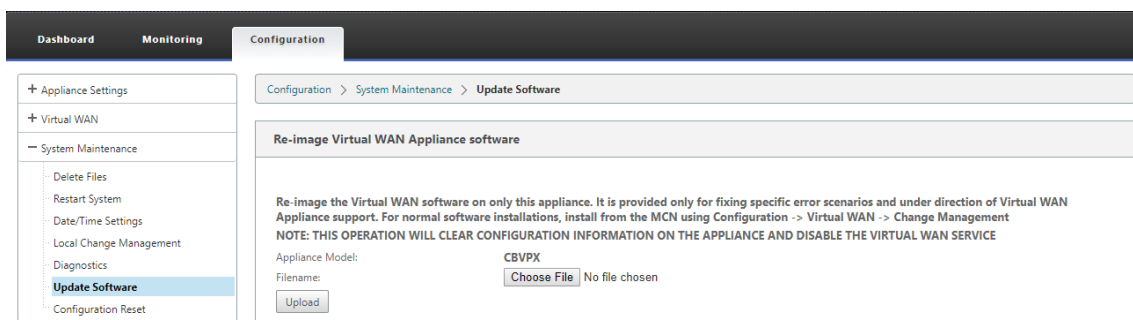
Citrix SD-WAN アプライアンスソフトウェアの再イメージ化

May 10, 2021

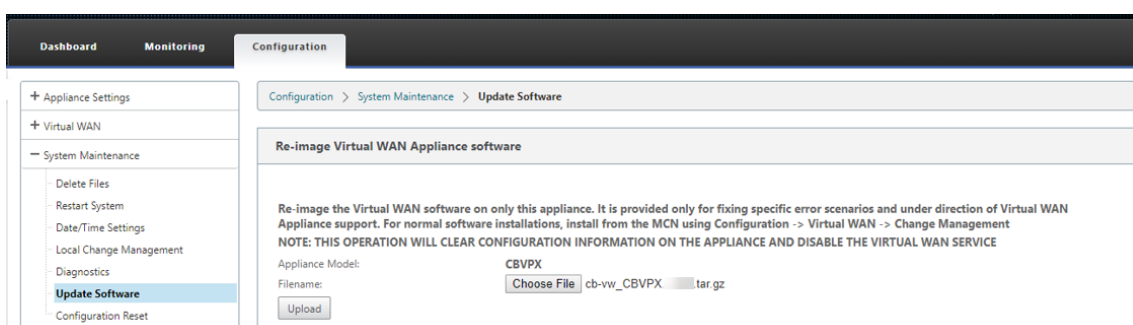
必要な Citrix SD-WAN ソフトウェアバージョンとプラットフォームの .tar.gz ファイルを [シトリックスのダウンロード](#) ポータルからダウンロードします。

Citrix SD-WAN アプライアンスソフトウェアのイメージを再作成するには

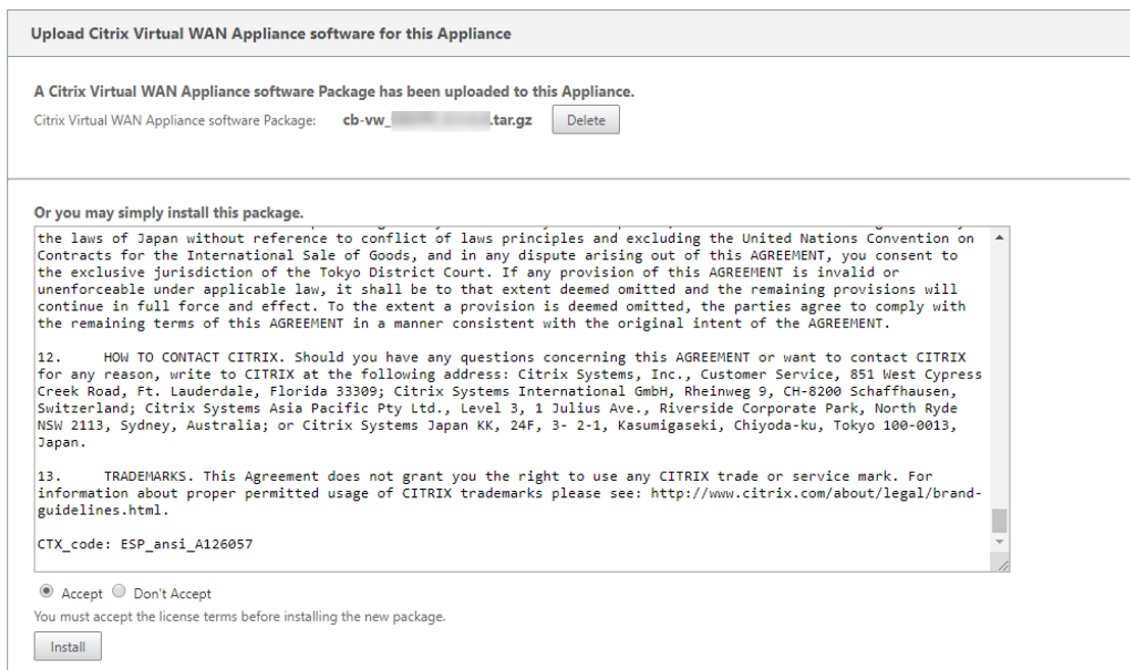
1. SD-WAN アプライアンスの GUI で、[構成] > [システムメンテナンス] > [ソフトウェアの更新] に移動します。



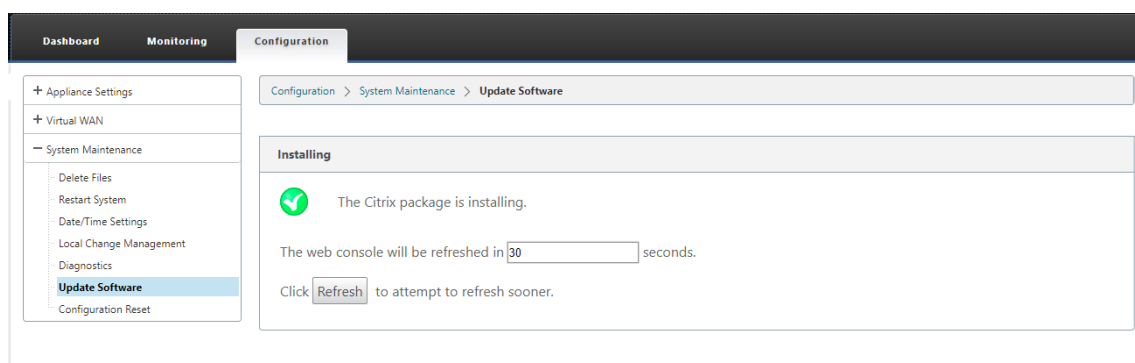
2. [ファイルの選択] をクリックし、ダウンロードした Citrix SD-WAN アプライアンスソフトウェアを選択します。[アップロード] をクリックします。



3. ライセンス条項を読み、同意します。[同意する] をクリックし、[インストール] をクリックします。



ソフトウェアの更新には約 35 秒かかり、その後アプライアンスが再起動します。



ローカル変更管理を使用した部分的なソフトウェアのアップグレード

May 10, 2021

重要

デフォルトでは、[部分的なソフトウェアアップグレード] オプションは無効になっています。

[ローカル変更管理] オプションを使用すると、クライアントサイトのサブセットに新しい SD-WAN ソフトウェアリリースバージョンをインストールできます。これは、部分的なソフトウェアアップグレード機能によって実現されます。この機能により、ネットワーク管理者は、すべてのサイトを同時にアップグレードすることなく、ネットワーク上のサイト上のソフトウェアを選択的にアップグレードできます。この機能の特定のユースケースは、管理者が新しいソフトウェアを少数のブランチサイトでテストしてから、ネットワーク内のすべてのサイトにインストールすることです。

前提条件と要件

部分的なソフトウェアアップグレードを実行する前に、次の要件を確認してください。

1. アクティブな SD-WAN バージョン 10.0 以降のソフトウェアがある。[部分的なソフトウェアアップグレードを有効にする] チェックボックスをクリックします。このチェックボックスをオフにすると、MCN アプライアンスで現在実行されているソフトウェアが、アクティブな仮想パスが実行されているブランチに適用されます。

Configuration > Virtual WAN > Change Management Settings

Enable/Disable Partial Software Upgrade

☐ Enable Partial Software Upgrade Apply

Scheduling Information

Show entries Search

Edit Selected Refresh

<input type="checkbox"/>	Site Name	Scheduling Information	Status	Edit
<input type="checkbox"/>	RCN3BR2	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)	...	
<input type="checkbox"/>	RCNDefaultBR2VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)	!	
<input type="checkbox"/>	RCNDefaultBR1VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)	...	
<input type="checkbox"/>	RCN3BR2(HA-Secondary)	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)	✗	
<input type="checkbox"/>	MCNVPXHA	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)	✓	
<input type="checkbox"/>	MCNVPXHA(HA-Secondary)	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)	✓	
<input type="checkbox"/>	GeoMCNVPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)	●	
<input type="checkbox"/>	RCN1BR11000	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)	●	
<input type="checkbox"/>	RCN1BR2VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)	●	
<input type="checkbox"/>	RCN1RCN	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)	●	

Showing 1 to 10 of 17 entries Previous 1 2 Next

Configuration > Virtual WAN > Change Management Settings

Enable/Disable Partial Software Upgrade

☒ Enable Partial Software Upgrade Apply

Scheduling Information

Show entries

Help

Enable/Disable Partial Software Upgrade

- Use this section to control the Partial Software Upgrade feature of change management.
- Enable Partial Software Upgrade to allow sites in the network to be selectively upgraded
- Disable Partial Software Upgrade to turn off the feature and synchronize all sites in the network with the MCN. This may cause network disruption while synchronization is in progress.

Close

Showing 1 to 4 of 17 entries

2. MCN 変更管理 プロセスを使用して、アクティブなソフトウェアと同じメジャーバージョン番号で、アクティブな構成と同じ構成で新しいバージョンのソフトウェアをステージングします。
3. 新しいソフトウェアは、アクティブなソフトウェアと同じメジャーバージョンである必要があります。マイナーバージョンは、異なるソフトウェアバージョンにすることができます。
4. まず、MCN からすべてのサイトで新しいソフトウェアをステージングする必要があります。「変更管理の 段階的ステップの有効化」で停止します。

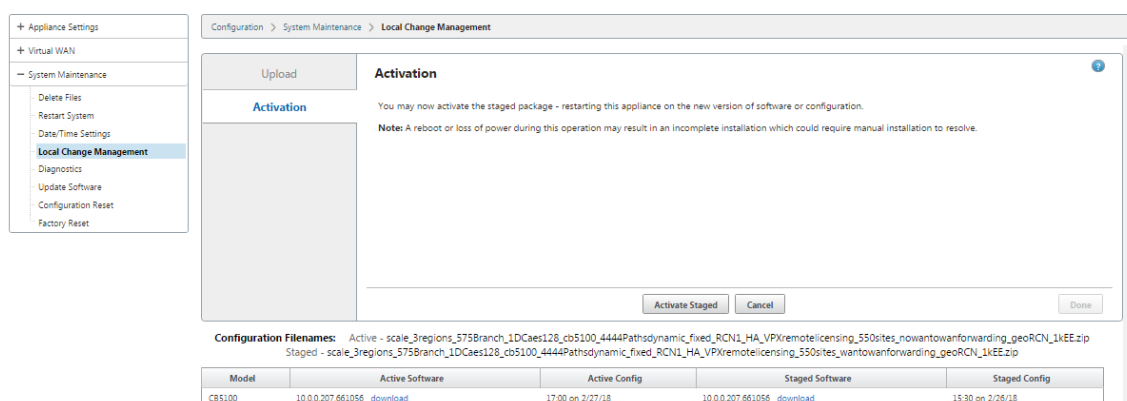
アクティブサイトと部分サイトの構成では、MCN サイトとブランチサイトでソフトウェアが同一である必要があります。部分的にアップグレードされたサイトでは、別の機能セットを有効にすることはできません。個々のサイトに進み、ローカル変更管理を実行します。高可用性の展開については、以下の手順を参照してください。

SD-WAN ソフトウェアの部分的なアップグレードを実行するには、次の手順を実行します。

ブランチノードで部分的な SD-WAN ソフトウェアアップグレードを実行できるシナリオには、高可用性モードと非高可用性モードの 2 つがあります。

高可用性モードを使用せずにブランチノードをアップグレードする

1. Citrix SD-WAN Web 管理インターフェイスで、サイトの一部アップグレードプロセスでアップグレードする必要があるブランチサイトに移動します。
2. [ローカル変更管理] を開きます。[次へ] をクリックします。
3. [ステージングを有効化] をクリックします。各ブランチサイトには、新しいソフトウェアバージョンがインストールされます。



高可用性モードでのブランチノードのアップグレード

1. SD-WAN Web 管理インターフェイスで、ブランチサイトに移動します。ブランチサイトは、部分的なサイトアップグレードによってアップグレードする必要があります。
2. スタンバイアプライアンスのサービスを無効にします。
3. プライマリアプライアンスで、ローカル変更管理を開きます。
4. [ステージングを有効化] をクリックします。このアプライアンスは、新しいソフトウェアバージョンでインストールされます。
5. スタンバイアプライアンスで、ローカル変更管理を開きます。

6. [ステージングを有効化] をクリックします。これで、スタンバイアプライアンスが新しいソフトウェアバージョンでインストールされます。
7. プライマリアプライアンスとスタンバイアプライアンスがアクティベーションプロセスを完了したら、スタンバイアプライアンスでサービスを有効にします。

ネットワークのアップグレード

ネットワークを同期する準備ができたなら、MCN ネットワーク変更管理画面に移動し、[ステージングのアクティブ化] をクリックします。

USB で Premium 版変換に WANOP

May 10, 2021

注

SD-WAN 1000 および 2000 WANOP アプライアンスのみ、SD-WAN Premium エディションアプライアンスに変換できます。

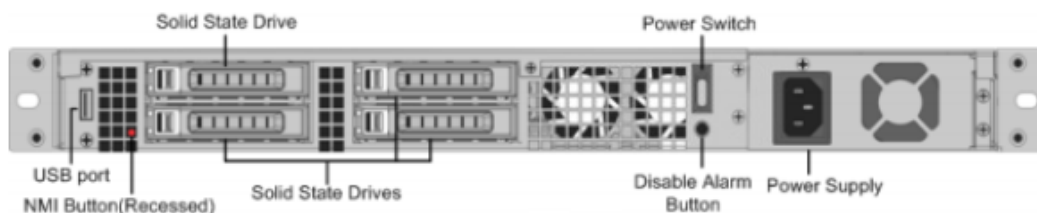
はじめに

- 1000 WS ではなく、1000 アプライアンスのみを変換していることを確認します。1000 WS アプライアンスは、SD-WAN Premium (エンタープライズ) エディションアプライアンスへの変換をサポートしていません。
- 既存の *Dom-0-root/nsroot* にログインするためのデフォルトの認証情報があることを確認します。

アップグレード手順

変換手順は、次の手順を含む 2 段階のプロセスです。

- 付属の USB スティックを Citrix SD-WAN アプライアンスに挿入します。
- シリアルコンソールが接続されていることを確認し、変換プロセスを続行します。



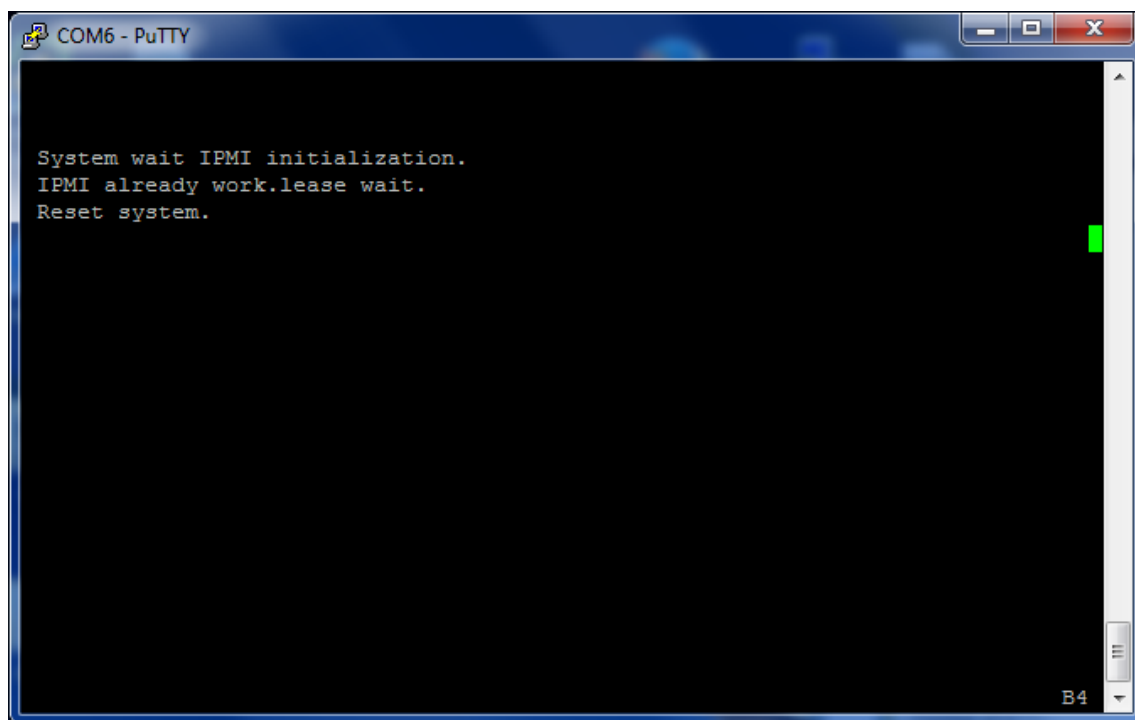
USB スティックで変換する方法

USB スティックを使用してアプライアンスをアップグレードするには:

1. 付属の USB スティックを Citrix SD-WAN アプライアンスに挿入します。
2. アプライアンスのシリアルコンソールに接続します。
3. アプライアンスを再起動します。
4. 起動プロセス中に、カーソルが画面上を移動しているのを確認したら、次の操作を行います。
 - a) [**Esc**] キーを押したままにします。
 - b) **Shift** キーを押したままにします。
 - c) 数字 **1** キーを押します (SHIFT+1=!) キーを押し、すべてのキーを放します。
 - d) カーソルの移動を停止するまで、手順 a、b、c を繰り返します。

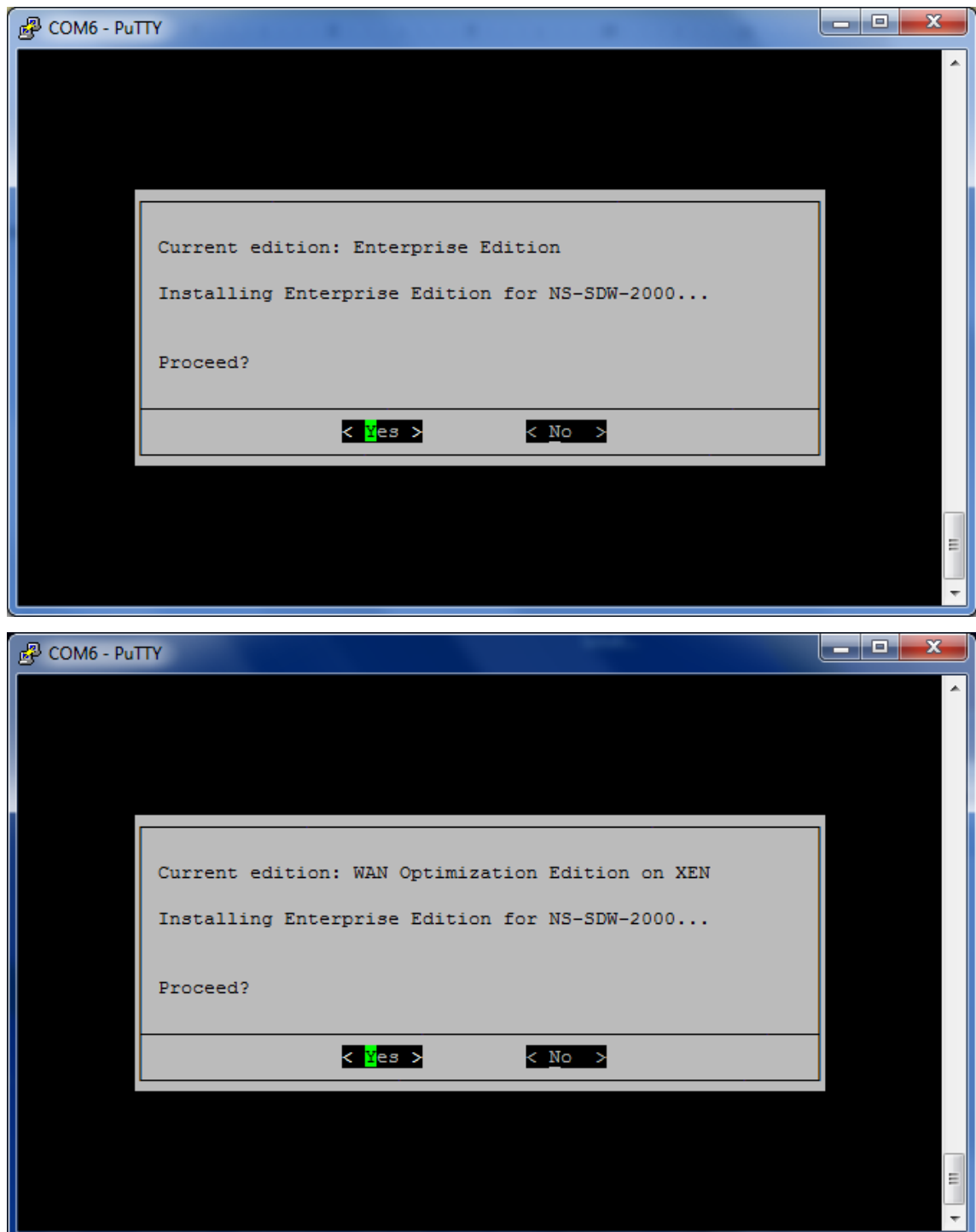
注

上記の手順は、アプライアンスの再起動プロセス中に実行する必要があります。キーストロークは、手順 4 で説明したように、BIOS のポストステージ中に発生します。



5. BIOS がロードされたら、外付け USB ドライブ (PNY USB 2.0 FD 1100 など) を選択してアプライアンスを起動します。外付け USB ドライブは、注文済みの場合は Citrix から出荷されます。

プラットフォームが 1000 や 2000 など、複数のエディションをサポートしている場合は、使用するプラットフォーム・エディションを選択する必要があります。そのため、確認する前に Premium (エンタープライズ) エディションを選択してください。



6. プロンプトが表示されたら、**Enterprise Edition** ソフトウェアアップグレードオプションを選択します。
7. アップグレードプロセスは 20~30 分で完了します。1~2 分後にシステムがリブートし、ログインプロンプ

トが表示されます。1000 プラットフォームエディションでは、内部 USB ドライブ自体の更新には約 30 分かかるため、アップグレードプロセスは約 1 時間です。

8. 手順が完了したら、USB メモリを取り外します。



参照ドキュメント

- Citrix SD-WAN 製品のライセンスについては、以下のサポートリンクを参照してください。 <http://support.citrix.com/article/ctx131110>。
- Citrix SD-WAN に関するドキュメントおよびリリースノートについては、「」を参照してください。 <http://support.citrix.com/article/ctx131110>。

Standard Edition から Premium Edition への変換

May 10, 2021

重要

リリースバージョン 10.1 では、プラットフォーム版「Enterprise」は「Premium」という用語にリブランドされています。

Standard Edition から Premium (Enterprise) Edition へのプラットフォーム変換を実行するには、次の手順に従います。

1. 設定をローカルにエクスポートします。

2. 「変更管理」ページから アクティブパッケージ をダウンロードします。
3. ダウンロードしたパッケージを使用して、[システムメンテナンス] > [ソフトウェアの更新] > [仮想 WAN アプライアンスソフトウェアのイメージを再作成] からアプライアンスをアップグレードします。
4. [ファイルを選択] をクリックして、`CB-VW_CB1000_X.x.x.tar.gz` ファイルを指定します。x.x.x.x は SD-WAN ソフトウェアリリースバージョンです。
5. [アップロード] をクリックします。[同意する] を選択し、[インストール] をクリックして続行します。
6. Premium (エンタープライズ) エディションライセンスをインストールします。
7. 上記の手順 2 でダウンロードしたアクティブパッケージを使用して、アプライアンス上で ローカル変更管理 を実行します。

WAN 最適化プロビジョニングの条件を次に示します。

1. サイトロールが MCN の場合、WAN 最適化プロビジョニングは以下だけ実行されます。
 - ソフトウェアのアップグレードは、.zip パッケージ (SSUP) を使用して行われます
 - ライセンスは PE
 - 仮想 WAN サービスが有効になっている
2. サイトロールが [クライアント] の場合、WAN 最適化プロビジョニングは次の場合にのみ実行されます。
 - ソフトウェアのアップグレードは、.zip パッケージ (SSUP) を使用して行われます
 - 仮想 WAN サービスが有効になっている
 - ライセンスは PE
 - 仮想バスは MCN で形成される
3. WAN 最適化を即座にプロビジョニングするには、対応するサイトの [管理設定の変更] ページで [メンテナンスウィンドウ] の値を 0 に設定します。

USB イメージ再作成ユーティリティ

May 10, 2021

SD-WAN USB 再イメージユーティリティを使用すると、起動可能な USB メモリからクリーンな工場出荷時のイメージをインストールして、ハードウェアを再利用することができます。Citrix では、SD-WAN ソフトウェアイメージがブリロードされた USB スティックフィールド交換可能ユニット (FRU) を提供しています。USB FRU を使用して、アプライアンスに必要なサポート対象エディション (SE/PE/AE) に再イメージします。使用するアプライアンスのライセンス/構成によって、アプライアンスのエディションが決まります。

次の表に、使用可能な USB FRU イメージの詳細と、SD-WAN アプライアンスでサポートされているエディションを示します。

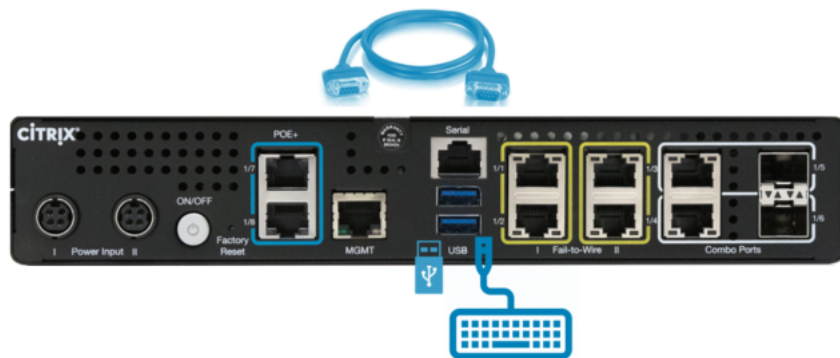
アプライアンス	USB FRU イメージ	サポートされているエディション
Citrix SD-WAN 110	11.1.1.39	SE
Citrix SD-WAN 210	10.2.7.17	SE, AE
Citrix SD-WAN 410	10.2.3.32	SE
Citrix SD-WAN 1100	10.2.7.17	SE, PE, AE
Citrix SD-WAN 2100	10.2.7.17	SE, PE
Citrix SD-WAN 4100	10.2.7.17	SE
Citrix SD-WAN 5100	10.2.7.17	SE, PE
Citrix SD-WAN 6100	10.2.7.17	SE, PE

USB イメージの再作成を実行するには、次の手順に従います。

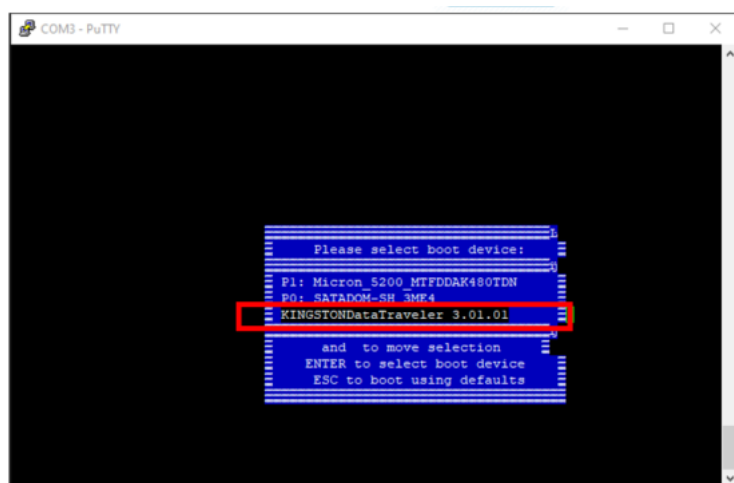
1. Citrix が提供する USB スティックをアプライアンスの USB ポートの 1 つに挿入します。
2. USB キーボードを別の USB ポートに接続します。

ヒント

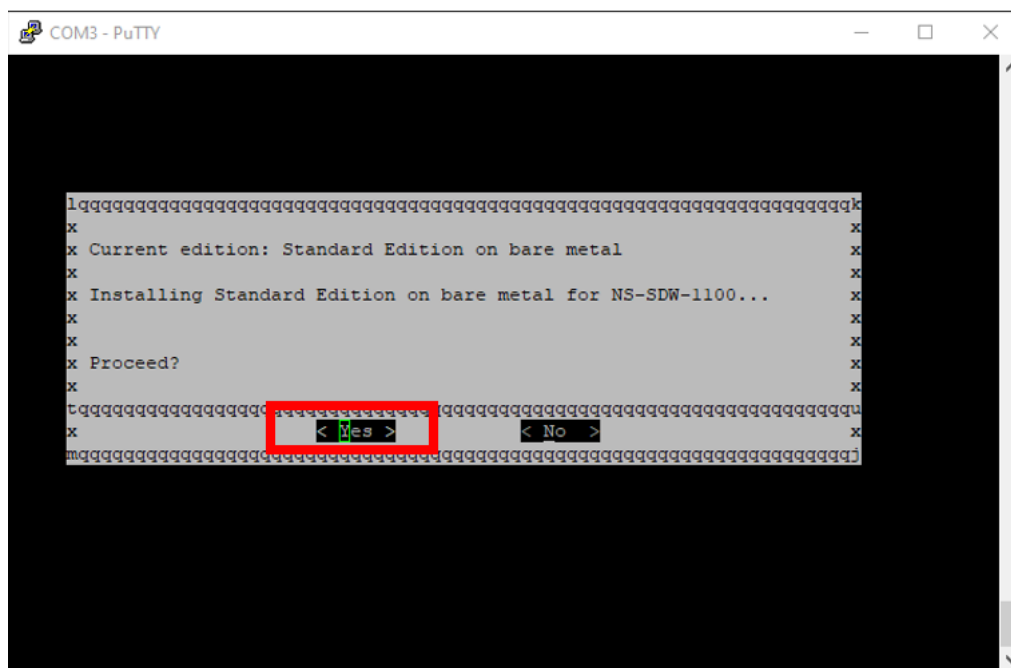
アプライアンスに 1 つの USB ポートがある場合は、USB スプリッタを使用して USB スティックと USB キーボードの両方を接続します。



3. 管理者としてシリアルコンソールにログインし、CLI を使用して `reboot` アプライアンスコマンドを発行します。
4. 起動時に、USB 接続キーボードの **F11** キーまたはシリアルコンソール接続で **SHIFT+ESC+1** キーを押して連続的に押します。
5. ブートデバイスメニューから USB ドライブを選択し、Enter キーを押します。



6. プラットフォームでサポートされているエディションに応じて、インストールを続行するための許可を要求する画面が表示されます。[はい] を選択します。



注

PE および AE の再イメージ化の場合、適切な OS および PE/AE ライセンスのインストールが完了するまで、アプライアンスは GUI に Standard Edition として表示される場合があります。

インストールの完了には 30 分かかります。イメージ再作成プロセス中は、アプライアンスの電源を切らないでください。数回再起動することがあります。

7. 工場出荷時のイメージでは、DHCP がデフォルトで有効になっています。すべてのプラットフォームのデフォルトの管理 IP アドレスは 192.168.100.1 です。SD-WAN GUI にアクセスする場合に使用します。

次のコマンドを発行して、シリアルコンソールから管理 IP を手動で設定することもできます。

コマンド `'management_ip'` を発行します。

コマンドを発行する `'インターフェイス 192.168.100.1 255.255.255.0 192.168.100.254'`

コマンド「適用」を発行します。

8. デフォルトでは、ソフトウェアは SE にアップグレードされます。アプライアンスがサポートするエディションに応じて、必要に応じて PE または AE ライセンスをインストールします。

注

AE 機能を設定および管理できるのは、SD-WAN Orchestrator だけです。詳しくは、「[Edge セキュリティ](#)」を参照してください。

Citrix SD-WAN ライセンスオプション

May 10, 2021

4 つの Citrix SD-WAN Edition には、それぞれ異なる SD-WAN 機能のセットまたはサブセットがあります。インストールするライセンスの種類によって、Platform Edition (Standard Edition、WANOP Edition、Premium Edition、Advanced Edition) が決まります。

注

ライセンスをインストールして適用するときは、特定のアプライアンスが有効にする SD-WAN アプライアンスエディションをサポートしていること、および適切なソフトウェアバージョンが利用可能であることを確認してください。

Citrix SD-WAN プラットフォームソフトウェアのサポート

次の表は、使用可能な SD-WAN ソフトウェアの各バージョンでサポートされる Citrix SD-WAN プラットフォームを示しています。

注

リリースバージョン 10.2 では、エンタープライズプラットフォームエディションはプレミアムエディションにリブランドされています。

バージョン	WAN Optimization Edition			
	Standard Edition	Premium Edition	Advanced Edition	
リリース 7.x	はい	いいえ	いいえ	いいえ

バージョン	WAN Optimization			
	Edition	Standard Edition	Premium Edition	Advanced Edition
リリース 8.x	いいえ	はい	いいえ	いいえ
リリース 9.0、9.1、9.2、9.3	はい	はい	はい	いいえ
リリース 10.0、10.1、10.2	はい	はい	はい	いいえ
リリース 11.0、11.1	はい	はい	はい	いいえ
リリース 11.2	はい	はい	はい	はい
リリース 11.3	はい	はい	はい	はい

Citrix SD-WAN リリース 11.3 でサポートされているすべてのアプライアンスモデルを表示するには、[Citrix SD-WAN のデータシート](#)を参照してください。

ソフトウェアをダウンロードする前に、Citrix SD-WAN ソフトウェアライセンスを取得して登録する必要があります。SD-WAN ソフトウェアライセンスの取得方法については、Citrix カスタマーサポートにお問い合わせください。アプライアンスにライセンスファイルをアップロードおよびインストールする手順については、[SD-WAN ソフトウェアライセンスファイルのアップロードとインストール](#)のセクションを参照してください。ライセンスをインストールする前に、アプライアンスのハードウェアをセットアップし、アプライアンスの日付と時刻を設定する必要があります。

SD-WAN プラットフォームエディションのライセンスを Provisioning するライセンス手順では、次のトピックについて説明します。

- サポートされる SD-WAN ライセンスモデル: ローカル、リモート、および集中型。
- SD-WAN アプライアンスのリモートライセンスサーバのサポート
- リモートライセンスサーバを使用するための前提条件。

注

2020 年 11 月 4 日より、「Citrix ライセンスの返却と変更」プロセスに変更が加えられています。この新しいプロセスでは、Citrix.com の [ライセンスの管理] ポータルおよび Partner Central の [マイライセンスツール] を使用して、ライセンスを返却または変更することはできません。

詳細およびユースケースのリストについては、「[KB 記事 CTX285157](#)」を参照してください。

ローカルライセンス

May 10, 2021

ローカルライセンスでは、ネットワーク内の各アプライアンスにログインし、ライセンスファイルをアップロードする必要があります。ZTD サービスを使用している場合、アプライアンスは猶予ライセンスのみで使用するようになります。アクティブなネットワーク接続用のライセンスファイルをアップロードする必要があります。ライセンスファイルは、個々のアプライアンスのホスト ID に基づいて生成されます。

SD-WAN アプライアンスのライセンスをインストールおよび構成するには、SD-WAN Web 管理インターフェイスを使用します。

XenServer/ESXI/Hyper-V プラットフォームに展開された SD-WAN アプライアンスのライセンスをインポートする：

1. SD-WAN Web 管理インターフェイスで、[構成] > [アプライアンスの設定] > [ライセンス] に移動します。
2. [ローカル] を選択し、ライセンスをアップロードします。[アップロードとインストール] をクリックします。
3. [設定の適用] をクリックして、変更を保存します。

License Configuration

☒ Local ☐ Remote

Upload License for this Appliance

Filename: No file chosen

Licenses Uploaded

Filename: CCB_4100VW-2000_SSERVER_Retail.lic

リモートライセンス

May 10, 2021

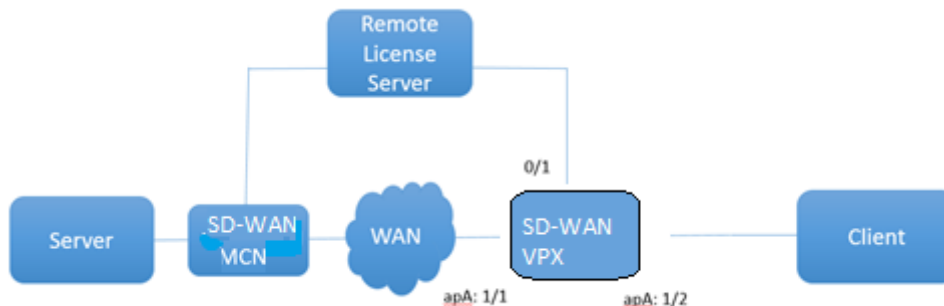
SD-WAN アプライアンスのリモートライセンスサーバーを使用するための前提条件

- NTP は、ライセンスサーバと SD-WAN の両方に対して構成する必要があります（日付と時刻は同期している必要があります）。

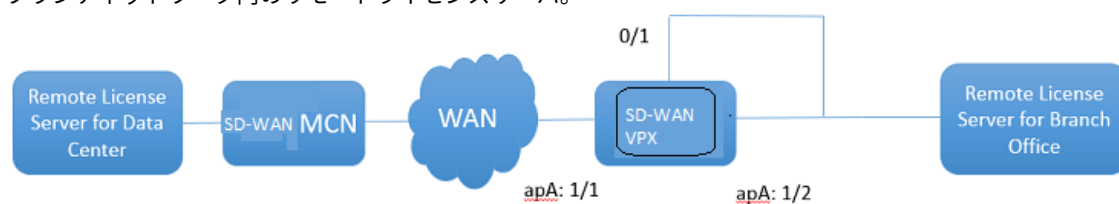
- 最新のライセンスサーバーバージョンを使用することをお勧めします。
 - リリース 9.1、9.2: 11.13.1 L.S
 - Release 10.0, 10.1, 10.2, 11.0, 11.0.1, 11.0.2:11.14.1 L.S
 - リリース 11.0.3, 11.1, 11.2:11.16.3 L.S

ユースケース:

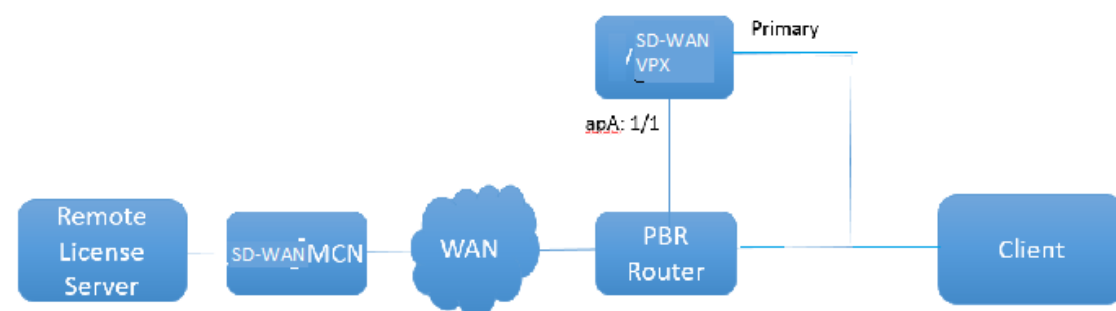
1. Data/APA ポートを使用せずに管理ネットワーク経由で到達可能なリモートライセンスサーバ。



2. ブランチネットワーク内のリモートライセンスサーバ。



3. SD-WAN VPX-SE-支社における PBR の導入。



リモートライセンス:

1. SD-WAN Web 管理インターフェイスで、[構成] > [アプライアンスの設定] > [ライセンス] に移動します。
2. [リモート] を選択し、[リモートサーバー] の IP アドレスの詳細を入力します。

3. ドロップダウンメニューから目的のアプライアンス モデル を選択します。リモートライセンスサーバーのデフォルトポートは 27000 です。

重要

- SD-WAN センターを使用して SD-WAN アプライアンスのリモートライセンスをインストールする場合は、SD-WAN Web 管理インターフェイスの構成エディターのグローバル設定で、SD-WAN MCN アプライアンスの集中ライセンスを有効にします。
- Citrix SD-WAN Center では、IPv6 アドレスはサポートされていません。

一元化されたライセンス

May 10, 2021

多数のネットワークノードでネットワーク展開が拡大するにつれて、アプライアンスの管理とライセンス管理が煩雑になります。SD-WAN アプライアンスの効率的なオンボーディングと簡単なネットワーク運用のために、このプロセスを簡素化するために、SD-WAN ネットワークの一元的なライセンスモデルが導入されました。

新しい集中型ライセンスモデルでは、SD-WAN Center Web 管理インターフェイス（SD-WAN アプライアンス管理およびレポートポータル）によって、アプライアンスにログインしなくても、ネットワーク上の個々の SD-WAN アプライアンスにライセンスサービスが提供されます。

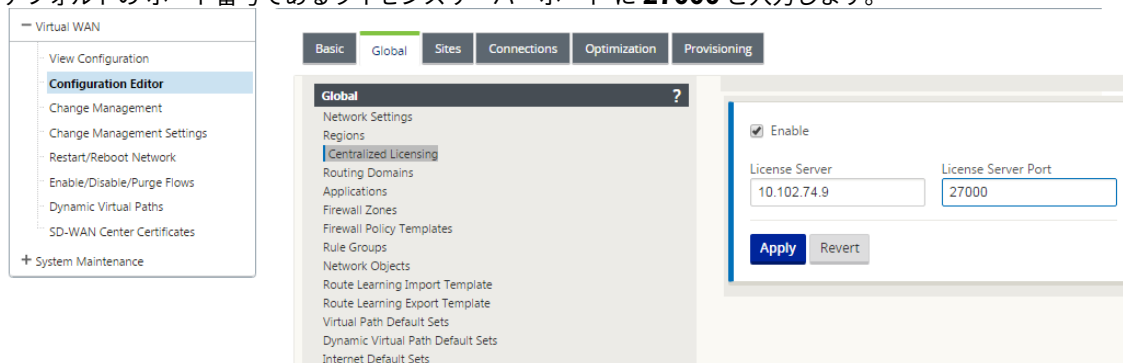
SD-WAN Center IP アドレスは、SD-WAN アプライアンス GUI の [グローバル] > [集中型ライセンス] の下で提供されます。この IP アドレスは、構成パッケージまたは更新によって個々のアプライアンスに伝播されます。IP アド

レスが変更されたら、変更管理プロセスを実行して、アプライアンスをプッシュする必要があります。グローバル設定は、ローカルサイト設定によって上書きできます。

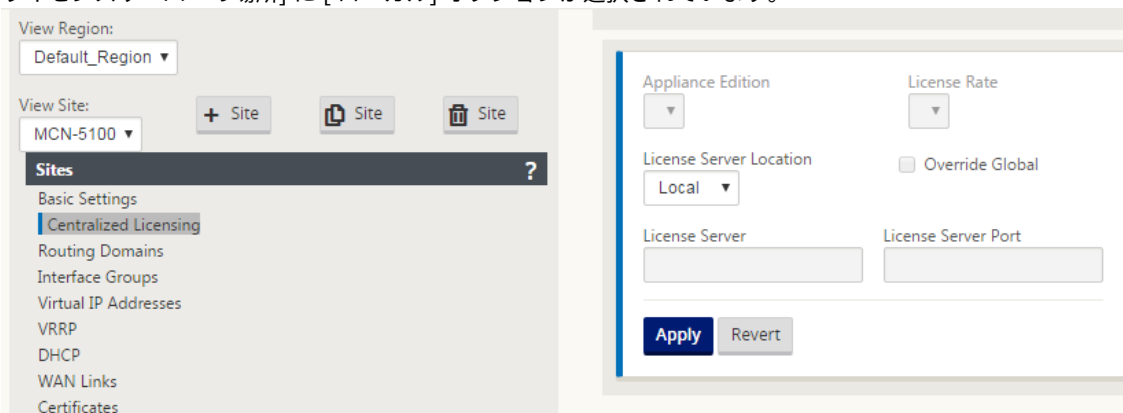
ライセンス帯域幅は、アプライアンスモデルでサイト設定用に選択できます。WAN リンク帯域幅は、選択したライセンスに対して監査されます。

SD-WAN アプライアンスの GUI で集中ライセンスを有効にするには、次の手順を実行します。

1. [構成] > [仮想 **WAN**] > [構成エディタ] に移動します。既存の仮想 WAN 構成パッケージを開くか、構成パッケージを作成します。構成パッケージが開きます。
2. 「グローバル」タブに移動します。[集中型ライセンス]を選択します。[有効]をクリックします。
3. SD-WAN ライセンスをダウンロードして管理できるライセンスサーバーの IP アドレスを入力します。SD-WAN MCN またはブランチアプライアンスの構成パッケージが SD-WAN Center からライセンスをダウンロードできるように、SD-WAN Center 管理 IP アドレスを指定します。
4. デフォルトのポート番号であるライセンスサーバーポートに **27000** と入力します。



5. [適用] をクリックします。
6. 「サイト」タブにナビゲートします。中央ライセンスを管理する地域とサイトに応じて、[サイトの表示]で [MCN] または [ブランチサイト] を選択します。
7. [集中型ライセンス] を選択します。中央のライセンスオプションビューが表示されます。デフォルトでは、[ライセンスサーバーの場所] に [ローカル] オプションが選択されています。



8. ドロップダウンメニューをクリックし、[**Central**] を選択して、ライセンスサーバーのデフォルトの場所を変更します。グローバル設定で中央ライセンスを有効にしたときに、ライセンスサーバに提供した IP アドレスとポート情報が表示されます。たとえば、ライセンスサーバは、ネットワーク内のアプライアンスを管理する SD-WAN Center の IP アドレスを指定できます。

The screenshot shows a configuration window with the following fields and values:

Field	Value
Appliance Edition	SE ▼
License Rate	4000 ▼
License Server Location	Central ▼
License Server	10.102.74.9
License Server Port	27000

Buttons: Apply, Revert

9. インストールするアプライアンスに応じて、アプライアンスのエディションとライセンスレートを選択します
**。[** 適用] をクリックします。

The screenshot shows the same configuration window as before, but with the 'Appliance Edition' dropdown menu open, displaying the following options:

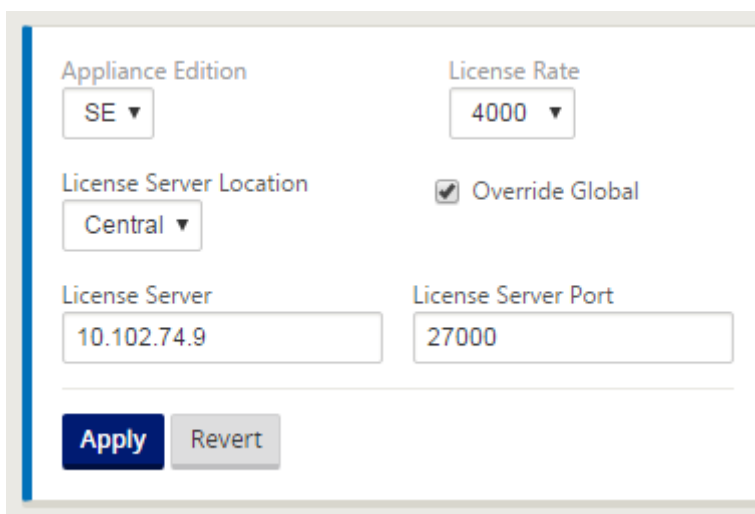
- SE ▼
- SE
- EE
- Central ▼

The 'License Rate' field now shows 'AUTO ▼'.

Buttons: Apply, Revert

注記: 構成の「グローバル」(Global) 設定で指定されているライセンスサーバー情報を上書きすることもできます。

10. グローバル設定をオーバーライドするには、[グローバルをオーバーライド] を選択します。新しいライセンスサーバーの IP アドレスを構成します。デフォルトのライセンスサーバーのポート番号 (27000) を保持します。[適用] をクリックします。



Appliance Edition	License Rate
SE ▼	4000 ▼
License Server Location	<input checked="" type="checkbox"/> Override Global
Central ▼	
License Server	License Server Port
10.102.74.9	27000
<input type="button" value="Apply"/> <input type="button" value="Revert"/>	

構成したライセンスサーバーから、特定の SD-WAN アプライアンス構成パッケージ用に構成されたブランチサイトおよび MCN サイト内のすべてのノードのライセンスを管理できるようになりました。

ライセンスサーバーは SD-WAN Center 管理ポータルであり、ネットワーク構成から取得したライセンスを変更管理プロセスでサイトから取得します。

帯域幅割り当てに基づくライセンス:

各アプライアンスは、構成された帯域幅以上の帯域幅レベルのライセンスを選択できます。構成された帯域幅ライセンスが利用できない場合、アプライアンスが次に高い帯域幅ライセンスを選択する機能が追加されます。この機能は、中央ライセンスサーバー機能とリモートライセンスサーバー機能の両方で有効です。たとえば、次のようになります:

- 410 ~200 Mbps のライセンスが 3 つある場合 410 アプライアンスに関連付けられているすべての帯域幅割り当てに同じライセンスを使用します。サイト A (20 Mbps)、サイト B (50 Mbps)、およびサイト C (200 Mbps) は、すべて 410 ~200 Mbps のライセンスを使用する必要があります。
- 410 ~20 Mbps のライセンスと 410 ~200 Mbps のライセンスのそれぞれが 1 つある場合サイト A は 50 Mbps を消費するように構成され、サイト A は 410 ~200 Mbps のライセンスを使用できます。

ライセンスの猶予期間:

ライセンスファイルまたはライセンス構成がアプライアンスから削除されたときの猶予期間は 30 日間です。猶予アラートは、Syslog と電子メールでサポートされます。

注

選択したライセンスレートが設定された WAN リンクレートと一致しない場合、ライセンスイベントに関する次のメッセージがアプライアンス GUI に表示されます。

メッセージ: 設定されている許可レート (LAN から WAN へ) NNN (Kbps) の合計は、ライセンスレート (NNN (Kbps) の 2 倍を超えてはなりません。

重大度: 警告

イベント: Syslog、電子メール

ライセンスの管理

May 10, 2021

Citrix SD-WAN アプライアンスのライセンスは、リモートライセンスサービスと通信してライセンスをチェックすることによって管理されます。アプライアンスにライセンスが付与されている場合、ネットワーク操作は中断なく続行されます。アプライアンスにライセンスが付与されていない場合は、猶予ライセンスモードが開始されます。

SD-WAN アプライアンスのライセンス管理プロセス

1. 各サイトは、Web 管理インターフェイスを使用してリモートサーバーまたは SD-WAN Center と通信します。この通信は、接続を監視するハートビートメカニズムと、ライセンスのステータスを検証するチェックアウトメカニズムを介して行われます。
2. ハートビートは TCP 接続を介してライセンスサーバに 10 ～20 分ごとに送信され、接続を確認します。
3. 2 つの連続したハートビートが失われた後、アプライアンスは猶予モードになります。チェックアウト方法によって、ライセンスのステータスが決まります。このステータスは、SD-WAN Center からアプライアンスに送信される「Real」、「Grace」、または「Denied」です。アプライアンスがライセンスのステータスを確認するために SD-WAN Center に到達するたびに、新しいライセンスをチェックインおよびチェックアウトします。SD-WAN Center が 2 回の心拍を受信しない場合、SD-WAN Center はサイトに割り当てられたライセンスをプールに解放します。猶予期間は 30 日なので、2 つのハートビートが失われた後、アプライアンスは猶予期間に入ります。これらの 30 日間、通信を復元する必要があります。復元されると、アプライアンスは通常の動作モードに戻ります。通信が復元されない場合、アプライアンスはライセンスなし状態になり、ライセンスなし/ライセンスの有効期限の手順に従います。

MCN アプライアンスのアウトオブボックスライセンス (OOB):

- MCN アプライアンスには最初の猶予期間がありません。出番するにはライセンスが必要です。

クライアントアプライアンスのアウトオブボックスライセンス (OOB):

- クライアントノードには、ZTD 機能の有無にかかわらず 30 日間の猶予期間が与えられます。
- アプライアンスは、30 日間有効な OOB ライセンスファイルを使用して有効になっています。
- ライセンスファイルをアップロードするか、集中ライセンスサーバーを介してライセンスを取得するには 30 日間かかります。
- アプライアンスがライセンスされている場合、アプライアンスは正常に機能し、ネットワークの一部になります。
- アプライアンスのライセンスが 30 日以内にない場合は、ライセンスの有効期限の手順に従います。

アプライアンスをリセットして再び OOB ライセンスを取得する唯一の方法は、「工場出荷時へのリセット」を実行することです。

ライセンスの有効期限

May 10, 2021

SD-WAN アプライアンスは 30 日間の猶予期間に入り、ライセンスの有効期限が切れた後にライセンスをアップロードする必要があります。

猶予期間中は、すべての操作が正常に機能します。ライセンスが期限内にアップロードされていない場合 (有効期限から 30 日後)、Virtual WAN サービスは無効になります。

集中型ライセンスには、猶予期間、ライセンスなし、ライセンス、通信ステータス、および障害の機能を追跡するログファイルがあります。

SD-WAN アプライアンス GUI の診断では、SD-WAN Center の他のサイトへの MCN 接続テスト機能を使用できます。これは、各アプライアンスがライセンスサーバーに到達できるかどうかをテストするために使用できます。サイト、ライセンスの状態、ステータステーブルは、ライセンスの管理と追跡に使用できます。

猶予期間:

1. アウトオブボックスクライアントノードには、30 日間の猶予期間が提供されます。通知は、アプライアンスが Out-of-Box モードであり、有効なライセンスが必要であることを示します。このオプションでは、猶予ライセンスファイルが使用されます。
2. ライセンスの有効期限: ライセンスの有効期限が切れると、30 日間の猶予期間が提供されます。通知は、猶予期間の理由がライセンスの有効期限であり、更新が必要であることを示します。
3. SD-WAN Center との通信の喪失: 2 回の心拍喪失後、アプライアンスは 30 日間猶予モードに入ります。通知は、猶予期間の理由が通信障害であることを示します。

構成

November 8, 2021

SD-WAN ソフトウェアとライセンスをインストールしたら、SD-WAN アプライアンス設定を構成して、ネットワークと配置の管理を開始できます。

SD-WAN アプライアンスの設定には、次のものが含まれます。

MCN の構成: MCN は、初期システム構成とその後の構成変更の配布ポイントとして機能します。ほとんどのアップグレード手順は、MCN の管理 Web インターフェイスから実行します。仮想 WAN に存在できるアクティブな MCN

は 1 つだけです。

デフォルトでは、アプライアンスにはクライアントの役割が事前に割り当てられています。アプライアンスを MCN として確立するには、まず MCN サイトを追加して構成し、指定した MCN アプライアンス上で構成と適切なソフトウェアパッケージをステージングしてアクティブ化する必要があります。

ブランチの設定: ブランチサイトを追加する手順は、MCN サイトの作成と構成に似ています。ただし、構成手順と設定の一部は、ブランチサイトでは若干異なります。さらに、最初のブランチサイトを追加したら、同じアプライアンスモデルを持つサイトのクローン作成（複製）機能を使用して、それらのサイトの追加と構成のプロセスを合理化できます。MCN サイトの作成と同様に、ブランチサイトをセットアップするには、MCN アプライアンスの管理 Web インターフェイスの構成エディタを使用する必要があります。設定エディタは、インターフェイスが **MCN** コンソールモードに設定されている場合にのみ使用できます。

MCN とブランチサイト間の仮想パスを構成する:MCN と各クライアント（ブランチ）サイト間の仮想パスサービスを構成します。これを行うには、設定エディタの **[** 接続]** セクションの設定ツリーにある設定フォームと設定を使用します ******。

WAN 最適化の有効化と構成: このセクションでは、仮想 WAN で SD-WAN Premium (Enterprise) Edition WAN 最適化機能を有効化および構成する手順について説明します。これを行うには、MCN の Web 管理インターフェイスの **[構成エディター]** の **[最適化]** セクションフォームを使用します。

注:

Citrix SD-WAN Orchestrator サービスは IPv6 アドレスをサポートしていません。

Citrix SD-WAN アプライアンスの次の機能は、Citrix SD-WAN 11.3 リリースからの IPv6 アドレスをサポートします。

- 管理平面フィーチャ
 - 管理インターフェイス
 - RADIUS サーバー
 - TACACS+ サーバ
 - SMTP サーバー
 - Syslog サーバー
 - HTTP サーバ
 - DNS サーバー
 - アプリフロー/IPFIX
 - SNMP
 - リモートライセンス
 - 一元化されたライセンス
 - NTP サーバー
 - 許可リスト
 - SD-WAN アプライアンス用の新しいユーザーインターフェイス
 - 診断

注:

管理 IPv6 アドレスを使用して上記の機能を構成した後、[アプライアンスの設定] > [ネットワークアダプタ] で IPv6 プロトコルを無効にすると、機能が期待どおりに動作しません。

- データ平面フィーチャ
 - スタティックルーティング
 - [IPv6 WAN リンクを介したインターネットサービス](#)
 - [IPv6 WAN リンクを介したイントラネットサービス](#)
 - ルータアダプタイズメント
 - DHCP クライアント
 - DHCP サーバ/リレー
 - [アプリケーション QoS](#)
 - ファイアウォール
 - 帯域内管理
 - [高可用性](#)
 - [IP ルール](#)
 - [IPv6 は LTE リンクでサポートされています](#)

メモ

- IPv6 アドレスは、Citrix SD-WAN 1000 SE/PE、Citrix SD-WAN 2000 SE/PE、および Citrix SD-WAN 4000 SE アプライアンスではサポートされていません。
- IPv6 アドレスは、次の構成ではサポートされていません。
 - Dynamic Routing (OSPF/BGP)
 - Virtual Router redundancy protocol
 - Premium edition or Two-Box support
 - Cloud direct
 - VNF/3rd Party Firewall
 - Netflow
 - Header compression for IPv6 packets
 - Application Routing
 - Office-365 support
 - Prefix delegation group

初期設定

September 26, 2023

これらの手順は、SD-WAN に追加するアプライアンスごとに完了する必要があります。したがって、このプロセスでは、ネットワーク全体でサイト管理者との調整が必要になり、アプライアンスが適切なタイミングで準備され、展開の準備が整っていることを確認する必要があります。ただし、マスター制御ノード（MCN）を構成してデプロイすると、いつでもクライアントアプライアンス（クライアントノード）を SD-WAN に追加できます。

仮想 WAN に追加するアプライアンスごとに、次の操作を行う必要があります。

1. SD-WAN アプライアンスハードウェアと、展開する SD-WAN VPX 仮想アプライアンス（SD-WAN VPX-VW）を設定します。
2. アプライアンスの管理 IP アドレスを設定し、接続を確認します。
3. アプライアンスの日付と時刻を設定します。
4. コンソールセッションの タイムアウト しきい値を高い値または最大値に設定します。

警告

コンソールセッションがタイムアウトになったり、構成を保存する前に管理 Web Interface からログアウトした場合、保存されていない構成の変更はすべて失われます。その後、システムに再度ログインし、設定手順を最初から繰り返す必要があります。そのため、構成パッケージを作成または変更したり、その他の複雑なタスクを実行したりするときは、コンソールセッションの タイムアウト 間隔を高い値に設定することを強くお勧めします。

5. アプライアンスにソフトウェアライセンスファイルをアップロードしてインストールします。

SD-WAN 仮想アプライアンス（SD-WAN VPX）のインストール手順については、次のセクションを参照してください。

- 「[SD-WAN VPX について](#)」を参照してください。
- 「[ESXi での SD-WAN VPX-SE のインストールとデプロイ](#)」を参照してください。

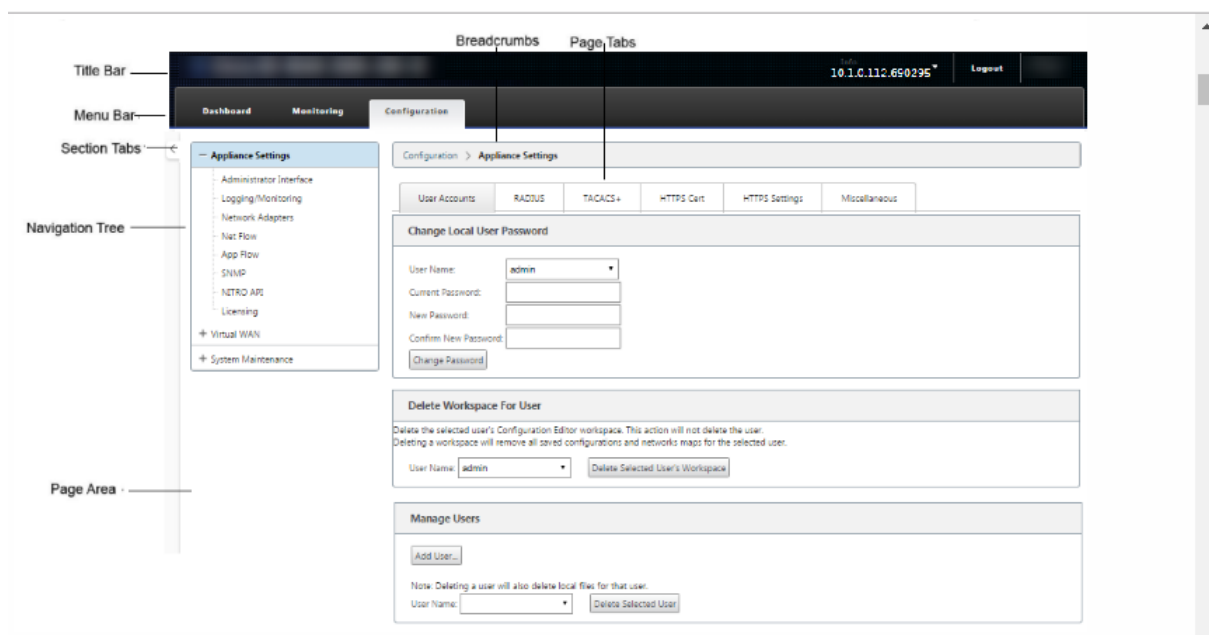
Web インターフェイス (UI) レイアウトの概要

May 10, 2021

このセクションでは、基本的なナビゲーション手順と、SD-WAN Web 管理インターフェイスページ階層のナビゲーションロードマップについて説明します。また、構成エディタ および 変更管理ウィザードの特定のナビゲーション手順についても説明します。

基本的なナビゲーション

以下の図は、Web 管理インタフェースの基本的なナビゲーション要素と、それらを識別するために使用される用語の概要を示しています。



基本的なナビゲーション要素は次のとおりです。

- **タイトル・バー**：アプライアンスのモデル番号、アプライアンスのホスト IP アドレス、アプライアンス上で現在実行されているソフトウェア・パッケージのバージョン、および現在のログイン・セッションのユーザー名が表示されます。タイトルバーには、セッションを終了するための [ログアウト] ボタンもあります。
- **メイン・メニュー・バー**：すべての管理 Web Interface 画面のタイトル・バーの下に表示されるバーです。これには、選択したセクションのナビゲーション・ツリーおよびページを表示するためのセクション・タブが含まれます。
- **セクションタブ**：セクションタブは、ページ上部のメインメニューバーにあります。これらは、Web 管理インタフェースのページおよびフォームの最上位カテゴリです。各セクションには、そのセクションのページ階層を移動するための独自のナビゲーションツリーがあります。セクションタブをクリックして、そのセクションのナビゲーション・ツリーを表示します。
- **ナビゲーション・ツリー**：ナビゲーション・ツリーは、メイン・メニュー・バーの下に左ペインにあります。これにより、セクションのナビゲーションツリーが表示されます。セクションタブをクリックして、そのセクションのナビゲーションツリーを表示します。ナビゲーションツリーには、次の表示オプションとナビゲーションオプションが用意されています。
 - セクション・タブをクリックすると、そのセクションのナビゲーション・ツリーおよびページ階層が表示されます。
 - ツリー内の分岐の横にある [+] (プラス記号) をクリックすると、その分岐トピックで使用可能なページが表示されます。
 - ページ名をクリックすると、そのページがページ領域に表示されます。
 - ブランチ項目の横にある 「-」 (マイナス記号) をクリックして、ブランチを閉じます。

- **ブレッডクラム** -これは、現在のページへのナビゲーションパスを表示します。ブレッডクラムは、ページ領域の上部、メインメニューバーのすぐ下にあります。アクティブなナビゲーションリンクは青いフォントで表示されます。現在のページの名前は、黒の太字フォントで表示されます。
- **ページ領域** -これは、選択したページのページ表示と作業領域です。ナビゲーションツリーでアイテムを選択すると、そのアイテムのデフォルトページが表示されます。
- **ページタブ** -一部のページには、そのトピックまたは設定フォームの子ページを表示するためのタブが含まれています。これらは、ページ領域の上部、ブレッডクラム表示のすぐ下にあります。「変更管理」ウィザードと同様に、タブはページ領域の左ペイン、ナビゲーション・ツリーとページの作業領域の間にあります。
- **ページ領域のサイズ変更** -一部のページでは、ページ領域 (またはそのセクション) の幅を拡大または縮小して、テーブルまたはフォーム内のフィールドの数を増やすことができます。この場合、ページ領域ペイン、フォーム、またはテーブルの右枠にグレーの縦のサイズ変更バーが表示されます。カーソルが双方向矢印に変わるまで、サイズ変更バーの上にカーソルを移動します。次に、バーをクリックして右または左にドラッグし、領域の幅を拡大または縮小します。

ページでサイズ変更バーを使用できない場合は、ブラウザの右端をクリックしてドラッグし、ページ全体を表示できます。

Web 管理インターフェイスのダッシュボード

[ダッシュボード] セクションタブをクリックして、ローカルアプライアンスの基本情報を表示します。

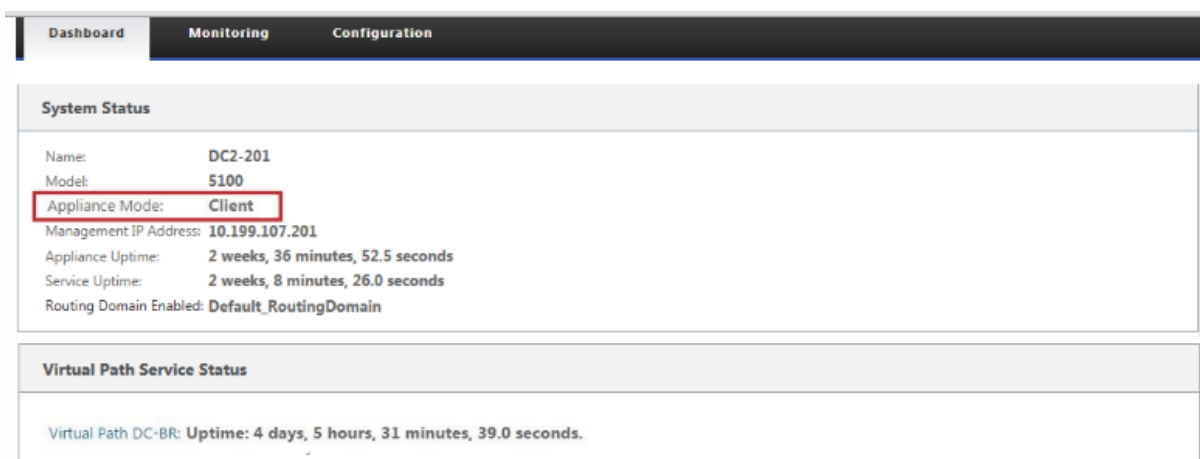
[ダッシュボード] ページには、アプライアンスの次の基本情報が表示されます。

- システムステータス
- 仮想パスサービスのステータス
- ローカルアプライアンスソフトウェアパッケージのバージョン情報

次の図は、マスターコントロールノード (MCN) アプライアンスのダッシュボード表示の例を示しています。



次の図は、クライアントアプライアンスの Dashboard ディスプレイの例を示しています。



構成エディタ

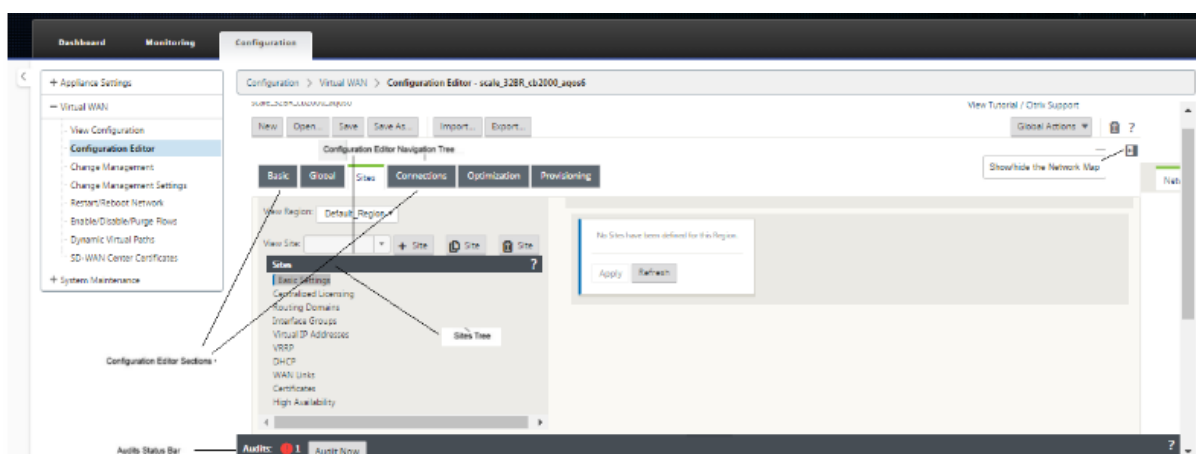
構成エディタを使用すると、仮想 WAN アプライアンスサイト、接続、最適化、Provisioning の追加と構成、仮想 WAN 構成の作成と定義を行うことができます。

構成エディタは、Web 管理インターフェイスが MCN コンソールモードの場合にだけ使用できます。デフォルトでは、新しいアプライアンスの Web Interface がクライアントモードに設定されています。構成エディタにアクセスする前に、モード設定を MCN コンソールに変更する必要があります。手順については、「[管理 Web インターフェイスを MCN コンソールモードに切り替える。]」を参照してください。 (/en-us/citrix-sd-wan/current-release/configuration/set-up-master-control-node/switch-to-mcn-console.html)

構成エディタに移動するには、次の操作を行います。

1. MCN アプライアンスの Web 管理インターフェイスにログインします。1. [構成] タブを選択します。1. ナビゲーションツリーで、ツリーの [Virtual WAN] ブランチの横にある [+] をクリックします。これにより、仮想 WAN カテゴリで使用できるページが表示されます。1. ツリーの [仮想 WAN] ブランチで、[構成エディタ] を選択します。

次の図は、構成エディターの基本的なナビゲーションとページ要素、およびそれらを識別するために使用される用語を示しています。



次に、このガイドで参照されている 構成エディターの 主要なナビゲーション要素について説明します。

- 構成エディターのメニュー・バー—ページ領域の上部、ブレッドクラム・リンクのすぐ下にあります。メニューバーには、構成エディターの 操作のための主要なアクティビティボタンがあります。さらに、メニューバーの右端には、構成エディタの チュートリアルを開始するための「チュートリアルの表示」リンクボタンがあります。このチュートリアルでは、構成エディタの 表示の各要素について、一連のバブルの説明を順を追って説明します。
- 構成エディターのセクションツリー—これは、構成エディターの ページ領域の左ペインにある濃い灰色のバーのスタックです。各グレーのバーは、トップレベルのセクションを表します。セクション名をクリックすると、そのセクションのサブブランチが表示されます。
- 「セクション」(Sections Tree branch)—セクションツリーでセクション名をクリックすると、セクションブランチが開きます。各セクションブランチには、構成カテゴリとフォームのサブブランチが 1 つ以上含まれ、さらに子ブランチとフォームを含めることができます。
- サイトツリー—構成 エディタで現在開いている構成に追加されているサイトノードが表示されます。セクションツリーで、サイト名をクリックすると、そのサイトのブランチが開きます。ブランチを閉じるには、サイトををクリックします。サイト・ツリーおよび構成フォームのナビゲートおよび使用方法の詳細については、次のセクションを参照してください。
 - マスター・コントロール・ノード (MCN) サイトの設定
 - ブランチサイトの追加と構成
- 監査ステータスバー—これは、「構成エディタ」ページの下部にある濃いグレーのバーで、「管理 Web Interface」画面の幅全体にわたって表示されます。監査 ステータスバーは、構成エディタ が開いている場合にのみ使用できます。ステータスバーの左端にある監査アラートアイコン（赤い点またはゴールデンロッドデルタ）は、現在開いている構成に 1 つ以上のエラーが存在することを示します。ステータスバーをクリックすると、その構成のすべての未解決の監査アラートの完全なリストが表示されます。

変更管理ウィザード

変更管理 ウィザードでは、マスターコントロールノード (MCN) アプライアンスとクライアントアプライアンスで Virtual WAN ソフトウェアと構成をアップロード、ダウンロード、ステージング、アクティブ化するプロセスをガイドします。変更管理 ウィザードには、次の 2 つのバージョンがあります。1 つは、Virtual WAN システム全体 (「グローバル」) の変更管理用で、もう 1 つはローカル変更管理用です。

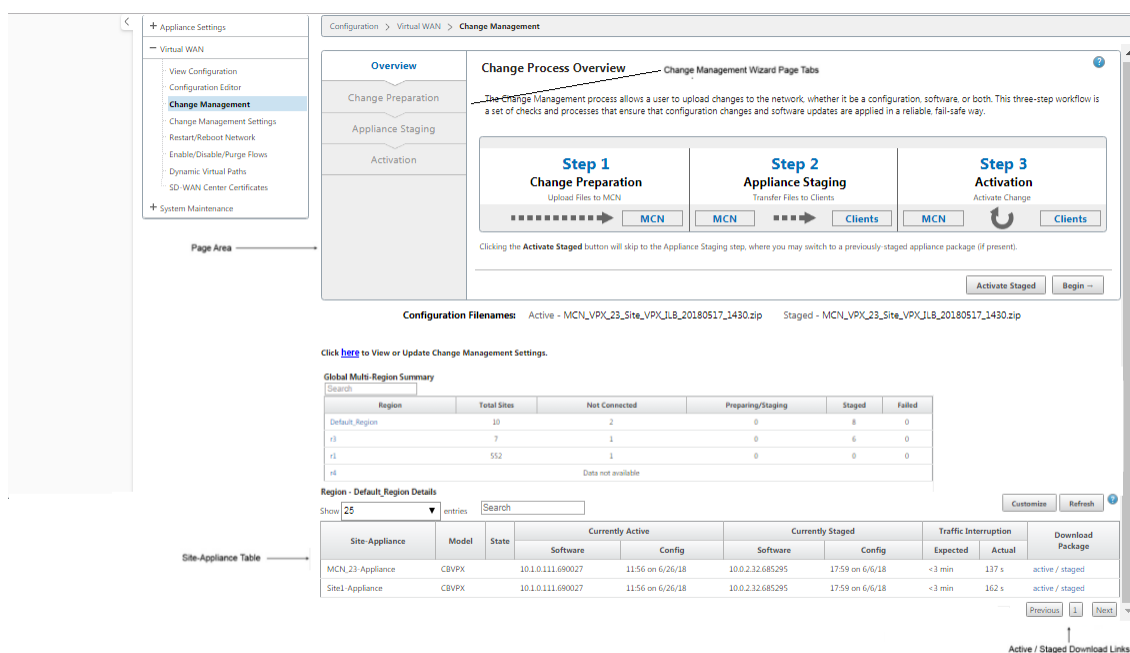
- **MCN (グローバル) 変更管理ウィザード**—**MCN** グローバル変更管理 ウィザードはプライマリ (メイン) バージョンであり、MCN アプライアンス Web 管理インターフェイスでのみ使用できます。これを使用して、ネットワーク内の仮想 WAN アプライアンスの種類ごとに展開する仮想 WAN アプライアンスパッケージを生成します。また、ウィザードを使用して、仮想 WAN にすでにデプロイされているアプライアンスに構成の変更を自動的に反映することもできます。基本的な操作手順については、以下の「MCN グローバル変更管理ウィザードの使用」の項を参照してください。MCN グローバル 変更管理 ウィザードを使用してアプライアンス・パッケージを作成する手順については、[MCN での仮想 WAN アプライアンスパッケージの準備](#)を参照してください。
- **ローカル変更管理ウィザード**—ローカル変更管理 ウィザードは、MCN とすべてのクライアントノードアプライアンスの両方で実行されている Web 管理インターフェイスで使用できます。これを使用して、仮想 WAN に追加するローカルアプライアンス上で適切な仮想 WAN アプライアンスパッケージをアップロード、ステージングおよびアクティブ化します。また、このウィザードを使用して、更新されたアプライアンスパッケージをローカル MCN、またはネットワークにすでに展開されている個々のローカル仮想 WAN アプライアンスにアップロードすることもできます。

MCN グローバル変更管理ウィザードの使用

MCN グローバル 変更管理 ウィザードを開くには、次の操作を行います。

1. MCN アプライアンスの Web 管理インターフェイスにログインします。
2. [構成] タブを選択します。ナビゲーションツリーで、ツリーの [**Virtual WAN**] ブランチの横にある [+] をクリックします。
3. 仮想 **WAN** ブランチ。「変更管理」を選択します。

次の図に示すように、変更管理 ウィザードの最初のページである「変更プロセスの概要」ページが表示されます。



4. ウィザードを開始するには、[開始] をクリックします。

ウィザードを使用してアプライアンスで SD-WAN ソフトウェアをアップロード、ステージングおよびアクティブ化するための詳細な手順については、次のセクションを参照してください。

- [MCN での仮想 WAN アプライアンスパッケージの準備](#)
- [クライアントへの仮想 WAN アプライアンスパッケージのインストール](#)

変更管理 ウィザードには、次のナビゲーション要素があります。

- ページ領域 - 変更管理 ウィザードの各ページのフォーム、テーブル、アクティビティボタンが表示されます。
- 変更管理ウィザードのページ・タブページ・タブは、ウィザードの各ページのページ領域の左ペインにあります。タブは、ウィザードプロセスで対応する手順が実行された順に一覧表示されます。タブがアクティブになっている場合、タブをクリックしてウィザードの前のページに戻ることができます。タブがアクティブな場合、名前は青いフォントで表示されます。グレーのフォントは、非アクティブなタブを示します。すべての依存関係（前の手順）がエラーなしで実行されるまで、タブは非アクティブです。
- **Appliance-Site** テーブル：ほとんどのウィザードページでは、ウィザードページ領域の下部にあります。この表には、構成済みの各アプライアンス・サイトに関する情報と、そのアプライアンス・モデルおよびサイトのアクティブまたはステージングされたアプライアンス・パッケージをダウンロードするためのリンクが含まれています。このコンテキストのパッケージは、そのアプライアンスモデルに対応する適切な SD-WAN ソフトウェアパッケージと、指定された構成パッケージを含む Zip ファイルバンドルです。表の上にある **Configuration Filenames** セクションには、ローカルアプライアンス上で現在アクティブでステージングされているパッケージのパッケージ名が表示されます。
- アクティブ/ステージングされたダウンロードリンク：これらは、**Appliance-Site** テーブルの各エントリの [**Download Package**] フィールド（右端の列）にあります。エントリ内のリンクをクリックして、そのアプ

ライセンスサイトのアクティブなパッケージまたはステージングされたパッケージをダウンロードします。

- 開始—「開始」をクリックして、変更管理 ウィザードプロセスを開始し、「変更の準備」タブページに進みます。
- **[Activate Staged]**—これが初期展開ではなく、現在ステージングされている構成をアクティブ化する場合は、**Activation** ステップに直接進むことができます。**[Activate Staged]** をクリックして、[Activation] ページに直接進み、現在ステージングされている構成のアクティブ化を開始します。

アプライアンスハードウェアの設定

May 10, 2021

Citrix SD-WAN アプライアンスのハードウェア（物理アプライアンス）をセットアップするには、次の手順に従います。

1. シャーシをセットアップします。

Citrix SD-WAN アプライアンスは、標準ラックにインストールできます。デスクトップに設置する場合は、シャーシを平らな場所に置きます。適切な換気のために、アプライアンスの側面と背面に最低 2 インチの隙間があることを確認してください。

2. 電源を接続します。

- a) 電源スイッチが [Off] に設定されていることを確認します。
- b) 電源コードをアプライアンスと AC コンセントに差し込みます。
- c) アプライアンスの前面にある電源ボタンを押します。

3. 電源を接続します。

- a) 電源スイッチが [Off] に設定されていることを確認します。
- b) 電源コードをアプライアンスと AC コンセントに差し込みます。
- c) アプライアンスの前面にある電源ボタンを押します。

4. アプライアンスの管理ポートをパーソナル・コンピュータに接続します。

アプライアンスの管理 IP アドレスを設定して、次の手順を完了する準備として、アプライアンスを PC に接続する必要があります。

注

アプライアンスを接続する前に、PC でイーサネットポートが有効になっていることを確認します。イーサネット・ケーブルを使用して、SD-WAN アプライアンス管理ポートをパーソナル・コンピュータのデフォルトのイーサネット・ポートに接続します。

SD-WAN VPX-SE 管理ポート

SD-WAN VPX-SE 仮想アプライアンスは仮想マシンであるため、物理的な管理ポートはありません。ただし、VPX 仮想マシンの作成時に SD-WAN VPX-SE の管理 IP アドレスを設定しなかった場合は、「[SD-WAN VPX-SE の管理 IP アドレスの設定](#)」の項で説明されているように、ここで設定する必要があります。

SD-WAN VPX-SE 仮想アプライアンスは仮想マシンであるため、物理的な管理ポートはありません。ただし、VPX 仮想マシンの作成時に SD-WAN VPX-SE の管理 IP アドレスを設定しなかった場合は、「[SD-WAN VPX-SE の管理 IP アドレスの設定](#)」の項で説明されているように、ここで設定する必要があります。

管理 IP アドレスの設定

September 26, 2023

SD-WAN アプライアンスへのリモートアクセスを有効にするには、アプライアンスに一意の管理 IP アドレスを指定する必要があります。そのためには、まずアプライアンスを PC に接続する必要があります。その後、PC でブラウザを開き、アプライアンスの管理 Web インターフェイスに直接接続し、そのアプライアンスの管理 IP アドレスを設定できます。管理 IP アドレスは、アプライアンスごとに一意である必要があります。

Citrix SD-WAN アプライアンスは、IPv4 プロトコルと IPv6 プロトコルの両方をサポートします。IPv4、IPv6、またはその両方（デュアルスタック）を設定できます。IPv4 プロトコルと IPv6 プロトコルの両方を構成すると、IPv4 プロトコルが IPv6 プロトコルよりも優先されます。

メモ

- 機能固有の設定で IPv4 または IPv6 アドレスを設定するには、同じプロトコルが有効になっていて、管理インターフェイスプロトコルとして設定されていることを確認してください。たとえば、SMTP サーバの IPv6 アドレスを設定する場合は、IPv6 アドレスが管理インターフェイスアドレスとして設定されていることを確認します。
- リンクローカルアドレス（「fe80」で始まる IPv6 アドレス）は使用できません。
- IPv6 アドレスを設定するには、IPv6 アドレスをアドバタイズするルータがネットワーク内に必要です。

ハードウェア SD-WAN アプライアンスと VPX 仮想アプライアンス（Citrix SD-WAN VPX-SE）の管理 IP アドレスを設定する手順は、異なります。各タイプのアプライアンスのアドレスを構成する手順については、以下を参照してください。

- SD-WAN VPX** 仮想アプライアンス—「[SD-WAN VPX-SE の管理 IP アドレスの設定](#)」および「[SD-WAN VPX-SE と SD-WAN WANOP VPX インストールの違い](#)」セクションを参照してください。

ハードウェア SD-WAN アプライアンスの管理 IP アドレスを構成するには、次の手順を実行します。

注

ネットワークに追加するハードウェアアプライアンスごとに、次のプロセスを繰り返す必要があります。

1. ハードウェア SD-WAN アプライアンスを構成する場合は、アプライアンスを物理的に PC に接続します。

- イーサネットケーブルの一方の端をアプライアンスの管理ポートに接続し、もう一方の端を PC のデフォルトのイーサネットポートに接続します。

注

アプライアンスへの接続に使用している PC で、イーサネットポートが有効になっていることを確認します。

2. アプライアンスの管理 IP アドレスの設定に使用している PC の現在の Ethernet ポート設定を記録します。

アプライアンスの管理 IP アドレスを設定する前に、PC のイーサネットポート設定を変更する必要があります。管理 IP アドレスの構成後に復元できるように、元の設定を必ず記録してください。

3. PC の IP アドレスを変更します。

PC で、ネットワークインターフェイスの設定を開き、PC の IP アドレスを次のように変更します。

- 192.168.100.50

4. PC の [サブネットマスク] 設定を次のように変更します。

- 255.255.0.0

5. PC でブラウザを開き、アプライアンスのデフォルトの IP アドレスを入力します。ブラウザのアドレス行に次の IP アドレスを入力します。

- 192.168.100.1

注

SD-WAN アプライアンスに接続する場合は、Google Chrome ブラウザを使用することをお勧めします。

管理 Web インターフェイスのブラウザ証明書の警告を無視します。

これにより、接続されたアプライアンスで SD-WAN 管理 Web インターフェイスのログイン画面が開きます。

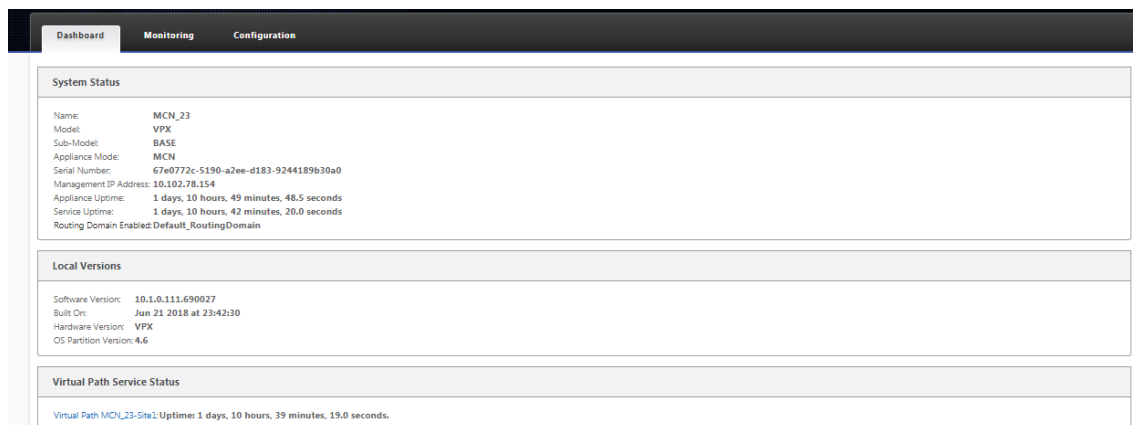
6. 管理者のユーザー名とパスワードを入力し、[ログイン] をクリックします。

- デフォルトの管理者ユーザー名: *admin*
- デフォルトの管理者パスワード: *password*

注

デフォルトのパスワードを変更することをお勧めします。パスワード回復には設定のリセットが必要になる場合があるため、必ず安全な場所にパスワードを記録してください。

管理 Web インターフェイスにログインすると、次に示すように [**Dashboard**] ページが表示されます。



アプライアンスの管理 Web インターフェイスに初めてログインすると、ダッシュボードにアラートアイコン（ゴールデンロッドデルタ）と、SD-WAN サービスが無効になっており、ライセンスがインストールされていないことを示すアラートメッセージが表示されます。現時点では、このアラートは無視できます。このアラートは、ライセンスをインストールし、アプライアンスの構成および展開プロセスを完了した後に解決されます。

7. メインメニューバーで、[構成] セクションタブを選択します。

これにより、画面の左ペインに [構成] ナビゲーションツリーが表示されます。[構成] ナビゲーションツリーには、次の 3 つの主要なブランチがあります。

- アプライアンスの設定
- 仮想 WAN
- システムメンテナンス

「構成」タブを選択すると、「アプライアンスの設定」ブランチが自動的に開き、次の図に示すように、「管理者インタフェース」ページがデフォルトで事前に選択されています。

The screenshot shows the Citrix SD-WAN 11.4 Administrator Interface. The top navigation bar includes 'Dashboard', 'Monitoring', and 'Configuration'. The left sidebar shows a tree structure under 'Appliance Settings' with 'Administrator Interface' selected. The main content area has a breadcrumb trail 'Configuration > Appliance Settings > Administrator Interface' and a tabbed interface with 'User Accounts', 'RADIUS', 'TACACS+', 'HTTPS Cert', 'HTTPS Settings', and 'Miscellaneous'. The 'User Accounts' tab is active, displaying three sections: 'Change Local User Password' (with fields for User Name: admin, Current Password, New Password, and Confirm New Password), 'Delete Workspace For User' (with a User Name dropdown set to admin and a 'Delete Selected User's Workspace' button), and 'Manage Users' (with an 'Add User...' button, a note about deleting local files, and a 'Delete Selected User' button).

8. ナビゲーション・ツリーの「アプライアンスの設定」 ブランチで、「ネットワーク・アダプタ」を選択します。これにより、[ネットワークアダプタ] 設定ページが表示され、次の図に示すように、[IP アドレス] タブが既定で事前に選択されています。

The screenshot shows the Citrix SD-WAN 11.4 Configuration page, specifically the Network Adapters tab. The left sidebar contains a navigation menu with options like Appliance Settings, Administrator Interface, Logging/Monitoring, Network Adapters (selected), Net Flow, App Flow, SNMP, NITRO API, Licensing, Virtual WAN, and System Maintenance. The main content area is divided into several sections:

- Management Interface IP:** Includes tabs for IP Address, Ethernet, and Mobile Broadband. Under the IP Address tab, there are sections for DHCP (with an 'Enable DHCP' checkbox) and Manual (with fields for IP Address: 10.102.78.154, Subnet Mask: 255.255.255.0, and Gateway IP Address: 10.102.78.1). Buttons for 'Change Settings' and 'Clear Settings' are present.
- DNS Settings:** Includes fields for Primary DNS and Secondary DNS, with 'Change Settings' and 'Clear Settings' buttons.
- Management Interface Whitelist:** Includes a text area for 'Allowed Network' with a 'Remove' button, and an 'Add Network(s):' field with a 'Change Settings' button.
- Management Interface DHCP Server:** Includes a status indicator (stopped), an 'Enable DHCP Server' checkbox, and fields for Lease Time (minutes), Domain Name, Start IP Address, and End IP Address, with a 'Change Settings' button.
- Management Interface DHCP Relay:** Includes an 'Enable DHCP Relay' checkbox and a 'DHCP Server IP Address' field, with a 'Change Settings' button.

9. [IP アドレス] タブで、次のいずれかを有効にします。

- IPv4 プロトコル:** IPv4 アドレスを有効にするには、[**IPv4** を有効にする] チェックボックスをオンにします。動的ホスト制御プロトコル (DHCP) は、ネットワーク上の各デバイスに IP アドレスおよびその他のネットワーク設定パラメータを動的に割り当てます。IP アドレスを動的に割り当てするには、[**DHCP** を有効にする] を選択します。IP アドレスを手動で構成するには、次の詳細を入力します。
 - IP アドレス
 - サブネット マスク
 - Gateway IP アドレス
- IPv6 プロトコル:** IPv6 アドレスを有効にするには、[**IPv6** を有効にする] チェックボックスをオンにします。IPv6 アドレスを手動で構成するか、DHCP または SLAAC を有効にして IP アドレスを自動的に割り当てることができます。

手動で構成するには、次の詳細を入力します。

- IP アドレス
- 前

SLAAC を構成するには、[**SLAAC**] チェックボックスをオンにします。SLAAC は、ネットワーク上の各デバイスに IPv6 アドレスを自動的に割り当てます。SLAAC を使用すると、IPv6 クライアントは、ローカルで利用可能な情報と近隣探索プロトコル (NDP) を介してルータによってアドバタイズされる情報の組み合わせを使用して、独自のアドレスを生成できます。

DHCP を構成するには、[**DHCP**] チェックボックスをオンにします。ステートレス DHCP を有効にするには、[**SLAAC**] と [**DHCP**] の両方のチェックボックスをオンにします。

- **IPv4** プロトコルと **IPv6** プロトコルの両方: **IPv4** プロトコルと **IPv6** プロトコルの両方を有効にするには、**IPv6** を有効にするチェックボックスと **IPv4** を有効にするの両方のチェックボックスを選択します。このようなシナリオでは、SD-WAN アプライアンスには、1 つの IPv4 管理 IP アドレスと IPv6 管理アドレスが 1 つあります。

メモ

- 管理 IP アドレスは、アプライアンスごとに一意である必要があります。
- [IP アドレス] タブの [管理インターフェイス **DHCP** サーバー] および [**DHCP** リレー] セクションは、管理インターフェイスで IPv4 プロトコルが有効になっている場合にのみ適用できます。
- 管理インターフェイスが DHCP クライアントとして動作する場合、ホスト名はオプション 12 として DHCP クライアントメッセージで使用されます。Citrix SD-WAN リリース 11.2.3 以降、リリース 11.4.1 までは、ホスト名は **sdwan** として設定されていました。Citrix SD-WAN リリース 11.4.1 以降では、ホスト名はサイト名と同じです。
サイト名が初めて変更または構成された場合、構成の更新が完了して仮想 WAN サービスが起動するまで、古いサイト名または **sdwan** が DHCP クライアントメッセージのホスト名として使用されます。構成の更新が完了し、仮想 WAN サービスが起動すると、後続の DHCP クライアントメッセージは新しいサイト名を使用します。

10. [設定の変更] をクリックします。確認ダイアログボックスが表示され、これらの設定を変更することを確認するメッセージが表示されます。

11. [OK] をクリックします。

12. PC のネットワークインターフェイスの設定を元の設定に戻します。

注

PC の IP アドレスを変更すると、アプライアンスへの接続が自動的に切断され、管理 Web インターフェイス上のログインセッションが終了します。

13. アプライアンスを PC から切断し、アプライアンスをネットワークルーターまたはスイッチに接続します。イーサネットケーブルを PC から取り外しますが、アプライアンスからは取り外さないでください。ケーブルの自由な端をネットワークルーターまたはスイッチに接続します。

これで、SD-WAN アプライアンスがネットワークに接続され、ネットワーク上で利用可能になりました。

14. 接続をテストします。ネットワークに接続されている PC で、ブラウザを開き、アプライアンスに構成した管理 IP アドレスを次の形式で入力します。

IPv4 アドレスの場合: <https://<IPv4 address>>

例: <https://10.10.2.3>

IPv6 アドレスの場合: [https://<\[IPv6 address\]>](https://<[IPv6 address]>)

例: [https://\[fd73:xxxx:yyyy:26::9\]](https://[fd73:xxxx:yyyy:26::9])

接続に成功すると、構成したアプライアンスの SD-WAN 管理 Web インターフェイスの [ログイン] 画面が表示されます。

ヒント

接続を確認したら、管理 Web インターフェイスからログアウトしないでください。これを使用して、以降のセクションで概説されている残りのタスクを完了します。

これで、SD-WAN アプライアンスの管理 IP アドレスが設定され、ネットワーク上の任意の場所からアプライアンスに接続できるようになります。

管理インターフェイスの許可リスト

許可リストとは、管理インターフェイスへのアクセス許可を持つ IP アドレスまたは IP ドメインの承認リストです。空のリストを指定すると、すべてのネットワークから管理インターフェイスにアクセスできます。IP アドレスを追加すると、信頼できるネットワークだけが管理 IP アドレスにアクセスできるようになります。

許可リストに IPv4 アドレスを追加または削除するには、IPv4 アドレスのみを使用して SD-WAN アプライアンス管理インターフェイスにアクセスする必要があります。同様に、許可リストに IPv6 アドレスを追加または削除するには、IPv6 アドレスのみを使用して SD-WAN アプライアンス管理インターフェイスにアクセスする必要があります。

Management Interface Whitelist
An empty Whitelist allows Management Interface to be accessed from all networks. V4 networks can be added/removed only from a V4 network. V6 networks can be added/removed only from a V6 network.
Add Network(s): <input type="text"/>
<input type="button" value="Change Settings"/>

日付と時刻の設定

May 10, 2021

アプライアンスに SD-WAN ソフトウェア・ライセンスをインストールする前に、アプライアンスに日付と時刻を設定する必要があります。

注

- ネットワークに追加するアプライアンスごとに、このプロセスを繰り返す必要があります。
- 現在の時刻が手動または NTP サーバを使用して変更され、新しく設定された時刻がセッションのタイムアウトタイマーよりも長い場合、UI セッションはログアウトされます。

日付と時刻を設定するには、次の操作を行います。

1. 構成しているアプライアンスの管理 Web Interface にログインします。
2. メインメニューバーで、[構成] タブを選択します。
これにより、画面の左ペインに [構成] ナビゲーションツリーが表示されます。
3. ナビゲーションツリーで [システムメンテナンス] ブランチを開きます。
4. [システムメンテナンス] ブランチで、[日付/時刻の設定] を選択します。これにより、次のように [日付/時刻の設定] ページが表示されます。

5. ページの下部にある [**Time Zone**] フィールドのドロップダウンメニューからタイムゾーン を選択します。

注

タイムゾーンの設定を変更する必要がある場合は、日付と時刻を設定する前に変更する必要があります。変更しないと、入力したとおりに設定が維持されません。

6. [タイムゾーンの変更] をクリックします。これにより、タイムゾーンが更新され、それに応じて現在の日付と時刻の設定が再計算されます。この手順の前に正しい日付と時刻を設定すると、設定が正しくなくなります。タイムゾーンの更新が完了すると、成功の警告アイコン（緑色のチェックマーク）とステータスメッセージがページの上部セクションに表示されます。
7. (任意) NTP サーバサービスを有効にします。
 - a) [**NTP** サーバを使用] を選択します。
 - b) [Server Address] フィールドに サーバアドレスを入力します。
 - c) [設定の変更] をクリックします。

更新が完了すると、成功の警告アイコン（緑のチェックマーク）とステータスメッセージが表示されます。
8. 「日付」フィールドのドロップダウンメニューから月、日、年を選択します。
9. [**Time**] フィールドのドロップダウンメニューから時、分、および秒を選択します。
10. [日付を変更] をクリックします。

注:

これにより、日付と時刻の設定が更新されますが、成功の警告アイコンやステータスメッセージは表示されません。

次の手順では、コンソールセッションの タイムアウト しきい値を最大値に設定します。この手順はオプションですが、推奨されます。これにより、設定作業中にセッションが途中で終了するのを防ぎ、その結果、作業が失われる可能性があります。コンソールセッションの タイムアウト 値を設定する手順は、次のセクションで説明します。タイムアウトしきい値をリセットしない場合は、「[SD-WAN ソフトウェアライセンスファイルのアップロードとインストール](#)」セクションに直接進んでください。

警告

コンソールセッションがタイムアウトになったり、構成を保存する前に管理 Web Interface からログアウトした場合、保存されていない構成の変更はすべて失われます。システムに再度ログインし、最初から設定手順を繰り返します。

セッションのタイムアウト

May 10, 2021

コンソールセッションがタイムアウトになったり、構成を保存する前に管理 Web Interface からログアウトした場合、保存されていない構成の変更はすべて失われます。その後、システムに再度ログインし、設定手順を最初から繰り返す必要があります。そのため、構成パッケージを作成または変更する場合や、その他の複雑なタスクを実行する場合は、コンソールセッションのタイムアウト間隔を高い値に設定することをお勧めします。デフォルトは 60 分です。最大値は 9,999 分です。セキュリティ上の理由から、これらのタスクを完了した後、しきい値を下限値にリセットする必要があります。

コンソールセッションの タイムアウト 間隔をリセットするには、次の手順を実行します。

1. [構成] タブを選択し、ナビゲーション・ツリーで [アプライアンスの設定] ブランチを選択します。

これにより、「アプライアンスの設定」ページが表示され、デフォルトで「ユーザー・アカウント」タブが事前に選択されています。

Configuration > Appliance Settings

User Accounts RADIUS TACACS+ HTTPS Cert **Miscellaneous**

Change Local User Password

User Name: admin

Current Password:

New Password:

Confirm New Password:

Change Password

Delete Workspace For User

2. [その他] タブ (右端隅) を選択します。

「その他」タブ・ページが表示されます。

Configuration > Appliance Settings

User Accounts RADIUS TACACS+ HTTPS Cert Miscellaneous

Change Web Console Timeout

Timeout: 60 Enter the new timeout value in minutes (1-9999).

Change Timeout

Switch to Client Console

Switch the mode of the Web Console to enable configuration of Client functionality.

Switch Console

3. コンソールの [タイムアウト] 値を入力します。

[**Web** コンソールの **** タイムアウト の変更 ****] セクションの [タイムアウト] フィールドに、最大値 9999 まで大きい値 (分単位) を入力します。デフォルトは 60 で、初期設定セッションでは非常に短すぎます。

注


セキュリティ上の理由から、設定と展開の完了後に、この値をより低い間隔にリセットしてください。

4. [タイムアウトの変更] をクリックします。

これにより、セッションの タイムアウト 間隔がリセットされ、操作が完了すると成功メッセージが表示されます。

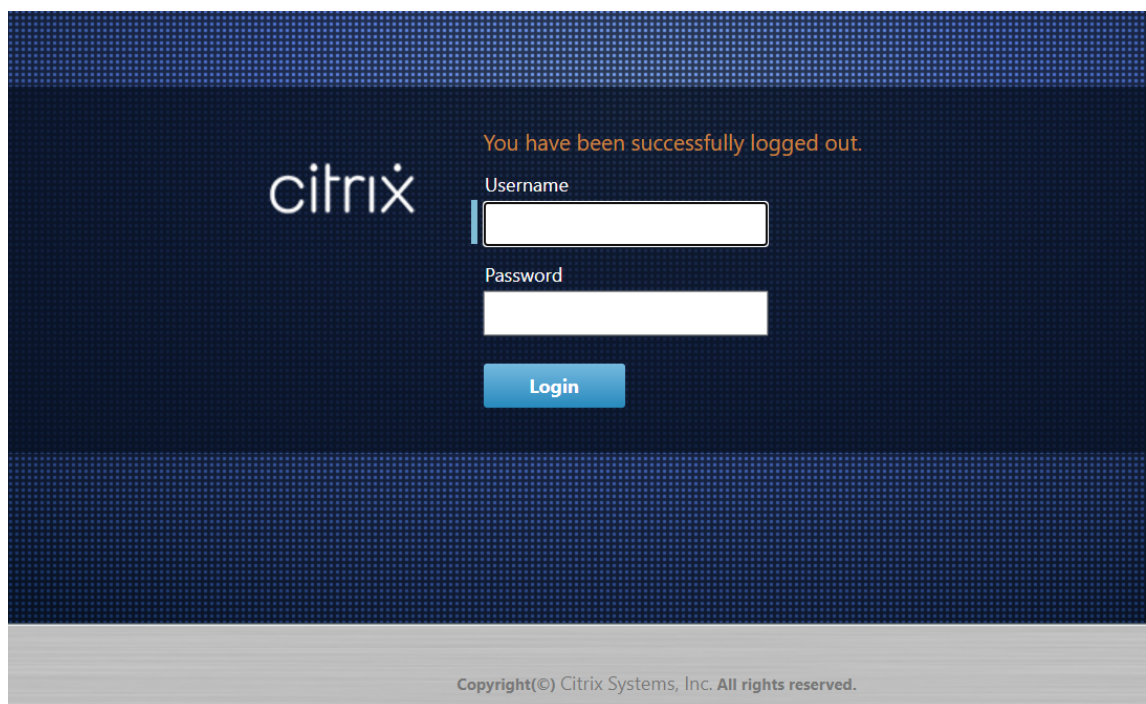
Configuration > Appliance Settings

Timeout Change Success

 Your timeout has been changed.

You will be automatically logged out in seconds.

短い間隔（数秒）後、セッションは終了し、管理 Web Interface から自動的にログアウトされます。[ログイン] ページが表示されます。



The image shows the Citrix login page. It has a dark blue background with a grid pattern. The Citrix logo is on the left. On the right, there is a message "You have been successfully logged out." in orange. Below the message are input fields for "Username" and "Password", and a blue "Login" button. At the bottom, there is a copyright notice: "Copyright(©) Citrix Systems, Inc. All rights reserved."

5. 管理者のユーザー名 (*admin*) とパスワード (パスワード) を入力し、「ログイン」をクリックします。

次のステップでは、SD-WAN ソフトウェアライセンスファイルをアプライアンスにアップロードしてインストールします。

アラームの設定

May 10, 2021

SD-WAN アプライアンスを設定して、ネットワークと優先順位に基づいてアラーム状態を特定し、アラートを生成し、電子メール、syslog、または SNMP トラップ経由で通知を受信できるようになりました。

アラームは、イベントタイプ、トリガー状態、クリア状態、重大度で構成されたアラートです。

アラーム設定を構成するには：

1. SD-WAN Web 管理インターフェイスで、[構成] > [アプライアンスの設定] > [ログ/モニタリング] の順に選択し、[アラームオプション] をクリックします。
2. [Add Alarm] をクリックして、新しいアラームを追加します。

Configuration > Appliance Settings > Logging/Monitoring

Log Options Alert Options Alarm Options Syslog Server

Alarm Configuration

Add Alarm

Event Type	Trigger State	Trigger Duration (sec)	Clear State	Clear Duration (sec)	Severity	Email	Syslog	SNMP
PATH	DEAD	0	GOOD	0	EMERGENCY	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
VIRTUAL PATH	DEAD	0	GOOD	0	CRITICAL	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
WAN LINK	DEAD	0	GOOD	0	ERROR	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Apply Settings

3. 次のフィールドの値を選択または入力します。

- **イベントタイプ:** SD-WAN アプライアンスは、ネットワーク内の特定のサブシステムまたはオブジェクトに対してアラームをトリガーできます。これらはイベントタイプと呼ばれます。使用可能なイベントタイプは、SERVICE、VIRTUAL_PATH、WANLINK、PATH、DYNAMIC_VIRTUAL_PATH、WAN_LINK_CONGESTION、USAGE_CONGESTION、FAN、POWER_SUPPLY、PROXY_ARP、ETHERNET、DISCOVERED_MTU、GRE_TUNNEL、IPSEC_TUNNEL です。
- **トリガー状態:** イベントタイプのアラームをトリガーするイベント状態。使用可能なトリガー状態オプションは、選択したイベントタイプによって異なります。
- **トリガー期間:** 秒単位の期間。アプライアンスがアラームをトリガーする速度を決定します。即時アラートを受信するには「0」を入力するか、15～7200 秒の値を入力します。Trigger Duration 期間内に同じオブジェクトでさらにイベントが発生すると、アラームはトリガーされません。イベントが Trigger Duration 期間よりも長く持続する場合のみ、より多くのアラームがトリガーされます。
- **Clear State:** アラームがトリガーされた後に、イベントタイプのアラームをクリアするイベント状態。使用可能な Clear State オプションは、選択したトリガー状態によって異なります。
- **[Clear Duration]:** アラームをクリアするまでの待機時間を秒単位で指定します。「0」と入力してアラームをただちにクリアするか、15-7200 秒の値を入力します。指定された時間内に同じオブジェクトで別のクリア状態イベントが発生した場合、アラームはクリアされません。
- **重大度:** アラームの緊急度を決定するユーザー定義フィールド。重大度は、アラームがトリガーまたはクリアされたときに送信されるアラートと、トリガーされたアラームの概要に表示されます。
- **Email:** イベントタイプのアラームトリガーとクリアアラートが電子メールで送信されます。
- **Syslog:** イベントタイプのアラームトリガーおよびクリアアラートが Syslog 経由で送信されます。
- **SNMP:** イベントタイプのアラームトリガーおよびクリアアラートは、SNMP トラップを介して送信されます。

- 必要に応じて、引き続きアラームを追加します。
- [設定の適用] をクリックします。

トリガーされたアラームの表示

トリガーされたすべてのアラームの概要を表示するには、次の手順を実行します。

SD-WAN Web 管理インターフェイスで、[構成] > [システムメンテナンス] > [診断] > [アラーム] に移動します。

トリガーされたすべてのアラームのリストが表示されます。

The screenshot shows the 'Alarms' section of the SD-WAN Web Management Interface. The left sidebar contains 'System Maintenance' and 'Diagnostics' (highlighted). The main content area has tabs for 'Ping', 'Traceroute', 'Packet Capture', 'Path Bandwidth', 'System Info', 'Diagnostic Data', 'Events', 'Alarms' (selected), and 'Diagnostics Tool'. Below the tabs, there's a 'Triggered Alarms Summary' section with a filter dropdown set to 'Any column' and a 'Show 100 entries' dropdown. A table lists 11 triggered alarms. The table has columns: Severity, Event Type, Object Name, Trigger State, Trigger Duration (sec), Clear State, Clear Duration (sec), and Clear Action. The alarms include various path and virtual path events with states like 'DEAD' or 'GOOD'.

Severity	Event Type	Object Name	Trigger State	Trigger Duration (sec)	Clear State	Clear Duration (sec)	Clear Action
EMERGENCY	PATH	Client-1-WL-1-3G->MCN-WL-1-MPLS	DEAD	0	GOOD	0	[Clear]
EMERGENCY	PATH	Client-1-WL-1-MPLS->MCN-WL-1-MPLS	DEAD	0	GOOD	0	[Clear]
CRITICAL	VIRTUAL_PATH	MCN-DC/Client-1	DEAD	0	GOOD	0	[Clear]
EMERGENCY	PATH	MCN-WL-1-MPLS->Client-1-WL-1-3G	DEAD	0	GOOD	0	[Clear]
EMERGENCY	PATH	MCN-WL-1-MPLS->Client-1-WL-1-MPLS	DEAD	0	GOOD	0	[Clear]
EMERGENCY	PATH	Client-2-WL-1-MPLS->MCN-WL-1-MPLS	DEAD	0	GOOD	0	[Clear]
EMERGENCY	PATH	Client-2-WL-1-3G->MCN-WL-1-MPLS	DEAD	0	GOOD	0	[Clear]
CRITICAL	VIRTUAL_PATH	MCN-DC/Client-2	DEAD	0	GOOD	0	[Clear]
EMERGENCY	PATH	MCN-WL-1-MPLS->Client-2-WL-1-3G	DEAD	0	GOOD	0	[Clear]
EMERGENCY	PATH	MCN-WL-1-MPLS->Client-2-WL-1-MPLS	DEAD	0	GOOD	0	[Clear]
ERROR	WAN_LINK	MCN-WL-1-MPLS	DEAD	0	GOOD	0	[Clear]

トリガーされたアラームのクリア

トリガーされたアラームを手動でクリアするには、次の手順を実行します。

- SD-WAN Web 管理インターフェイスで、[構成] > [システムメンテナンス] > [診断] > [アラーム] に移動します。
- [**Clear Action**] カラムで、クリアするアラームを選択します。
- [チェック済みアラームをクリア] をクリックします。または、[**Clear All Alarms**] をクリックして、すべてのアラームをクリアします。

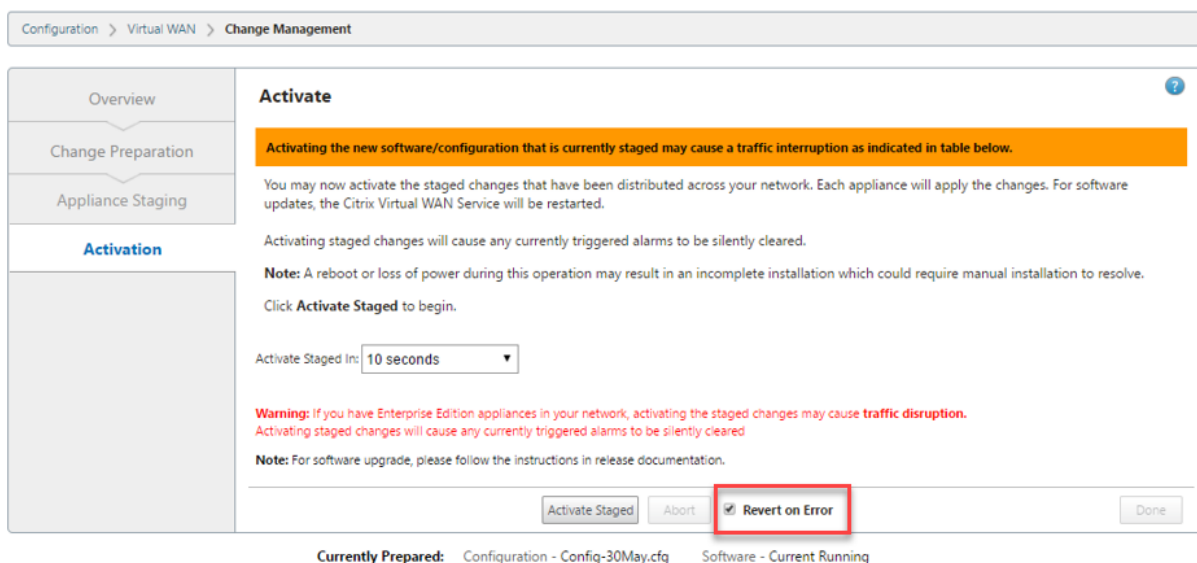
ロールバックの構成

May 10, 2021

構成ロールバック機能を使用すると、変更管理システムは、以前にアクティブだったソフトウェア/構成に戻すことにより、次のソフトウェア/構成エラーを検出してリカバリできます。

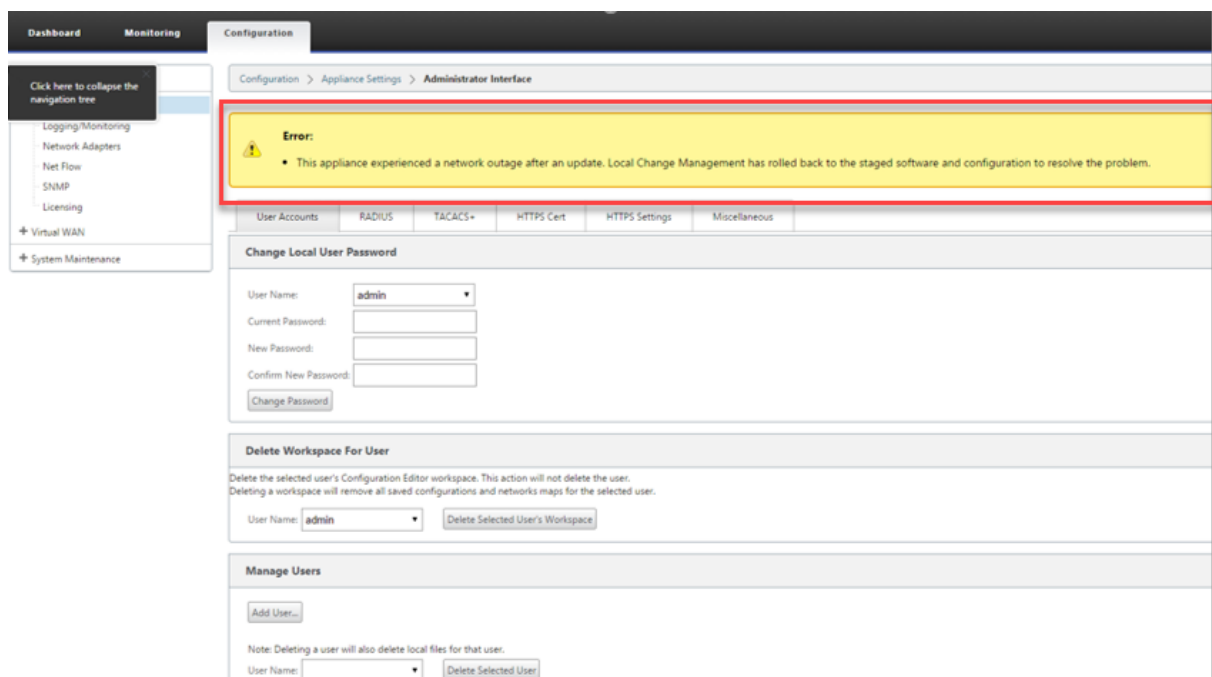
- ソフトウェアのアップグレード後、Virtual Path は停止し、ソフトウェアのクラッシュが発生するとサービスが無効になります。
- 構成を変更した後、Virtual Path はソフトウェアクラッシュなしで停止します。
- MCN アプライアンス自体の構成によって MCN サイトでネットワークの問題が発生した場合、システム停止は検出されず、それ自体をロールバックしません。ただし、ネットワーク内の他のすべてのクライアントは、MCN に接続できなかったため、自身をロールバックします。

構成ロールバック機能はデフォルトで有効になっています。この機能を無効にするには、変更管理ウィザードの [** アクティブ化] タブの [エラー時に元に戻す **] オプションをオフにします。



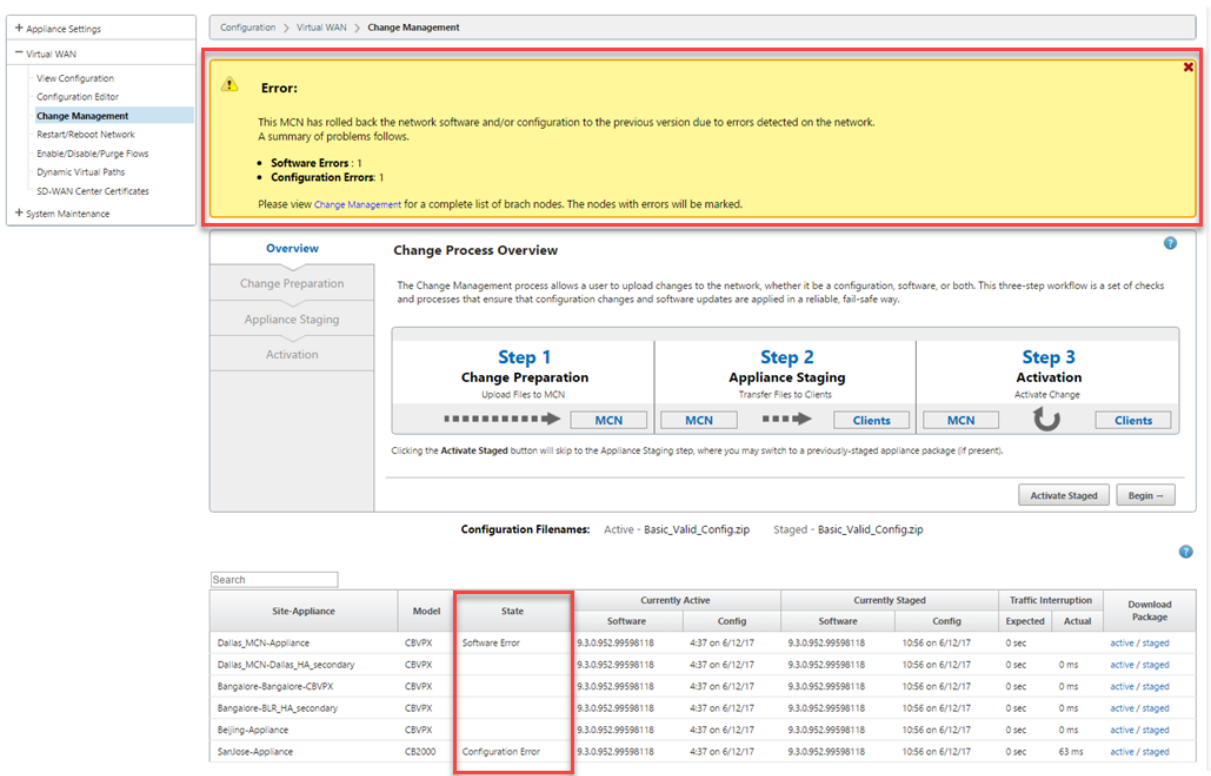
MCN からステージングされたパッケージをアクティブ化中にクライアント上でシステム構成エラーが発生した場合は、クライアントは以前のソフトウェア構成に戻り、次のスクリーンショットに示すように、エラーメッセージが表示されます。

アプライアンスのクラッシュが検出された場合、クライアントは SOFTWARE_UPDATE オブジェクトのクリティカル重大度イベントを生成し、ネットワーク障害が検出された場合は CONFIG_UPDATE オブジェクトのクリティカル重大度イベントを生成します。



「エラー時に元に戻す」が有効な場合、クライアントアプライアンスは自身を約 30 分間監視します。ソフトウェアが 30 分以内にクラッシュした場合、またはネットワークが 30 分間ダウンしている場合（MCN への仮想パスを確立できない場合）、ロールバックがトリガーされます。

次のスクリーンショットに示すように、MCN では、エラーメッセージが表示されます。クライアントがネットワークに再参加すると、検出されたエラーの種類が報告されます。エラー数の要約カウントがエラーメッセージに表示されます。



MCN の [**Change Management**] ウィンドウには、サイト・アプライアンスの状態が表示され、そのサイトでソフトウェアエラーまたは構成エラーが発生したかどうかを示されます。

マスター制御ノードの設定

May 10, 2021

SD-WAN マスターコントロールノード (**MCN**) は、仮想 WAN のヘッドエンドアプライアンスです。通常、これはエンタープライズデータセンターに導入された 4000 または 5100 の仮想 WAN アプライアンスです。MCN は、初期システム設定とその後の設定変更の配布ポイントとして機能します。また、ほとんどのアップグレード手順は、MCN の管理 Web インターフェイスを通じて行います。仮想 WAN に存在できるアクティブな MCN は 1 つだけです。

デフォルトでは、アプライアンスにはクライアントの役割が事前に割り当てられています。アプライアンスを MCN として確立するには、まず MCN サイトを追加して構成し、指定した MCN アプライアンス上で構成と適切なソフトウェアパッケージをステージングしてアクティブ化する必要があります。

MCN サイト展開の補足情報

次のサポート技術情報サポート資料をお勧めします。

- 仮想 WAN PBR モードの展開手順 ([CTX201577](#))

<http://support.citrix.com/article/CTX201577>

- 仮想 WAN ゲートウェイモードの展開手順 (CTX201576)

<http://support.citrix.com/article/CTX201576>

MCN サイト構成手順の概要

MCN サイトを追加および設定する手順は、次のとおりです。

1. 管理 Web インターフェイスを **MCN** コンソール モードに切り替えます。
2. MCN サイトを追加します。
3. MCN サイトの仮想インターフェイスグループを設定します。
4. MCN サイトの仮想 IP アドレスを設定します。
5. (任意) サイトの LAN GRE トンネルを設定します。
6. MCN サイトの WAN リンクを設定します。
7. MCN サイトのアクセスインターフェイスを設定します。
8. MCN サイトのルートを設定します。
9. (任意) MCN サイトの高可用性を設定します。
10. (任意) 仮想 WAN のセキュリティと暗号化を設定します。
11. MCN サイト構成に名前を付けて保存します。

これらの各タスクの手順については、次のセクションで説明します。

MCN の概要

May 10, 2021

マスターコントロールノード (**MCN**) は、仮想 WAN のマスター Controller として機能する中央の仮想 WAN アプリアンスであり、クライアントノードの中央管理ポイントです。すべての構成アクティビティ、およびアプリアンスパッケージの準備、およびクライアントへの配布は MCN で実行されます。また、特定の仮想 WAN モニタリング情報は MCN 上でのみ使用できます。MCN は

Virtual WAN 全体を監視できますが、クライアントノードはローカルイントラネットのみを監視でき、接続先のクライアントに関する情報も監視できます。

MCN の主な目的は、企業のサイト間通信のために、仮想 WAN 上に配置された 1 つ以上のクライアントノードで仮想パスを確立して利用することです。MCN は、複数のクライアントノードを管理し、仮想パスを持つことができます。複数の MCN を設定できますが、一度にアクティブにできるのは 1 つだけです。

以下の図は、Virtual WAN Edition 展開における MCN（データセンター）アプライアンスとクライアント（ブランチノード）アプライアンスの基本的な役割とコンテキストを示しています。



MCN コンソールに切り替える

May 10, 2021

MCN サイトを追加および構成するには、まず MCN ロールに昇格するアプライアンスの管理 Web インターフェイスにログインし、管理 Web インターフェイスを **MCN** コンソール モードに切り替える必要があります。**MCN** コンソール モードでは、現在接続している管理 Web インターフェイスの構成エディタにアクセスできます。その後、構成エディタを使用して MCN サイトを追加および構成できます。

注

MCN コンソール モードに切り替えると、管理 Web インターフェイスモードの動作モードだけが変更され、アプライアンス自体のアクティブロールは変更されません。アプライアンスを MCN のロールに昇格するには、最初に MCN サイトを追加して設定し、指定した MCN アプライアンス上で構成とソフトウェアパッケージをアクティブ化する必要があります。

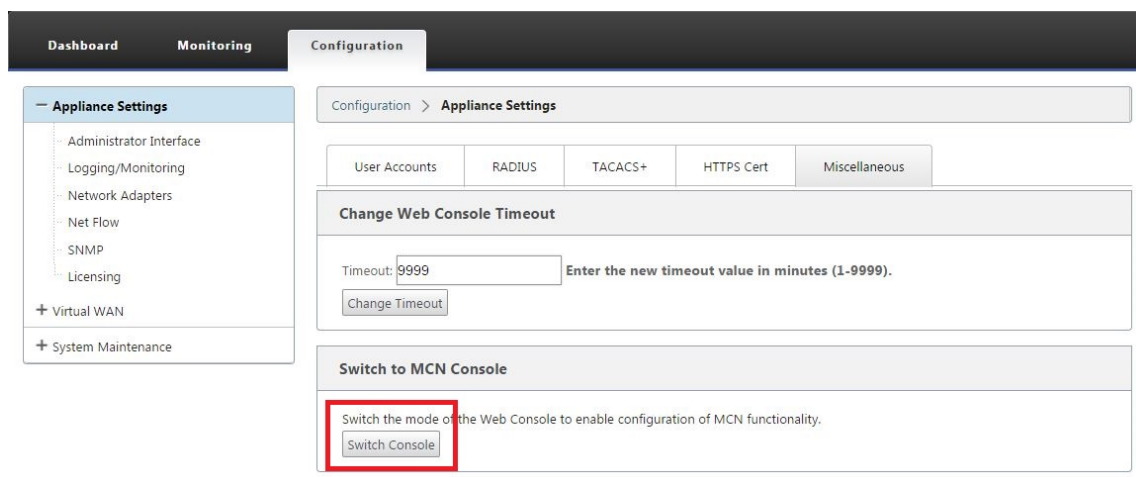
管理 Web インターフェイスを **MCN** コンソール モードに切り替えるには、次の手順を実行します。

1. MCN として設定するアプライアンスの管理 Web インターフェイスにログインします。
2. 管理 Web Interface のメイン画面のメインメニューバーにある「構成」をクリックします（ページ上部にある青いバー）。
3. ナビゲーション・ツリー（左ペイン）で、アプライアンスの設定 ブランチを開き、管理者インタフェースをクリックします。

これにより、中央のペインに [管理者インタフェース] ページが表示されます。

4. 「その他」タブを選択します。

[その他の管理 設定] ページが表示されます。



[その他] タブページの下部には、[クライアント] > [MCN コンソール に切り替える] セクションがあります。このセクションでは、アプライアンスのコンソールモードを切り替えるための **[Switch Console]** ボタンについて説明します。

セクション見出しは、次のように現在のコンソールモードを示します。

- クライアントコンソール モード（デフォルト）の場合、セクションの見出しは **MCN** コンソールに切り替えるです。
- **MCN** コンソール モードの場合、セクションの見出しは [クライアントコンソールに切り替え] です。

デフォルトでは、新しいアプライアンスは クライアント・コンソール・モード に設定されています。

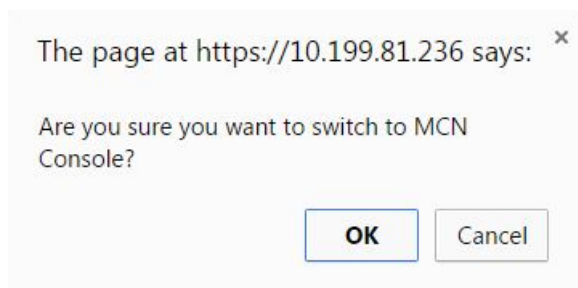
MCN コンソール モードでは、ナビゲーションツリーの **[構成エディタ]** ブランチが有効になります。構成エディタ は MCN アプライアンスでのみ使用できます。

注

次の手順に進む前に、アプライアンスがデフォルト (**Client Console** モード) に設定されていることを確認します。セクションの見出しは、**MCN** コンソールに切り替えます。

5. スイッチ・モード をクリックして、アプライアンス・モードを **MCN** コンソール・モード に設定します。

MCN モードに切り替えるかどうかを確認するダイアログボックスが表示されます。




6. **[OK]** をクリックします。

これにより、コンソールモードが **MCN** コンソール モードに切り替わり、現在のセッションが終了します。成功メッセージと、セッションが終了するまでの残り秒数を示すカウントダウンステータスが表示されます。

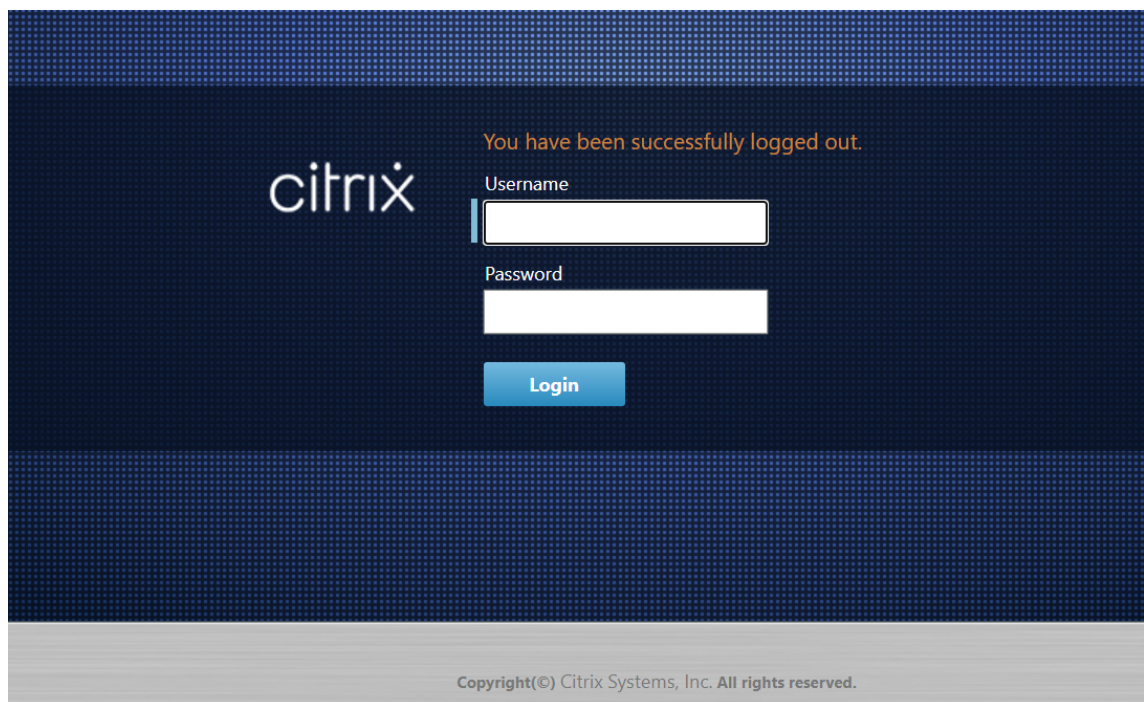
Configuration > Appliance Settings

Switch Console Success

 Your console has been switched.

You will be automatically logged out in seconds.

カウントダウンが完了すると、セッションが終了し、ログインページが表示されます。



The login page features a dark blue background with a subtle dot pattern. On the left is the Citrix logo. On the right, a message states 'You have been successfully logged out.' Below this are input fields for 'Username' and 'Password', followed by a blue 'Login' button. At the bottom, a copyright notice reads 'Copyright(©) Citrix Systems, Inc. All rights reserved.'

7. 管理者のユーザー名とパスワードを入力し、[ログイン]をクリックします。

- デフォルトの管理者ユーザー名: *admin*
- デフォルトの管理者パスワード: パスワード

ログイン後、ダッシュボードが表示され、アプライアンスが MCN モードであることを示します。

The screenshot displays the Citrix SD-WAN 11.4 web interface. At the top, there are three tabs: **Dashboard**, **Monitoring**, and **Configuration**. The **Configuration** tab is selected. Below the tabs, there are three main sections:

- System Status**:
 - Name: **MCN_23**
 - Model: **VPX**
 - Sub-Model: **BASE**
 - Appliance Mode: **MCN**
 - Serial Number: **67e0772c-5190-a2ee-d183-9244189b30a0**
 - Management IP Address: **10.102.78.154**
 - Appliance Uptime: **1 days, 10 hours, 49 minutes, 48.5 seconds**
 - Service Uptime: **1 days, 10 hours, 42 minutes, 20.0 seconds**
 - Routing Domain Enabled: **Default_RoutingDomain**
- Local Versions**:
 - Software Version: **10.1.0.111.690027**
 - Built On: **Jun 21 2018 at 23:42:30**
 - Hardware Version: **VPX**
 - OS Partition Version: **4.6**
- Virtual Path Service Status**:
 - Virtual Path MCN_23-Site1: Uptime: **1 days, 10 hours, 39 minutes, 19.0 seconds.**

次の手順では、新しい構成を開き、MCN サイトを [サイト] テーブルに追加し、新しい MCN サイトの構成を開始します。

MCN を構成する

May 10, 2021

最初のステップは、新しい構成パッケージを開き、MCN サイトを新しい構成に追加します。

注

構成エディタは、**MCN** コンソール モードでのみ使用できます。ナビゲーションツリーの [Virtual WAN] ブランチで [**Configuration Editor**] オプションが使用できない場合は、コンソールモードの変更手順については、[管理 Web インターフェイスの MCN コンソールモードへの切り替え](#)を参照してください。

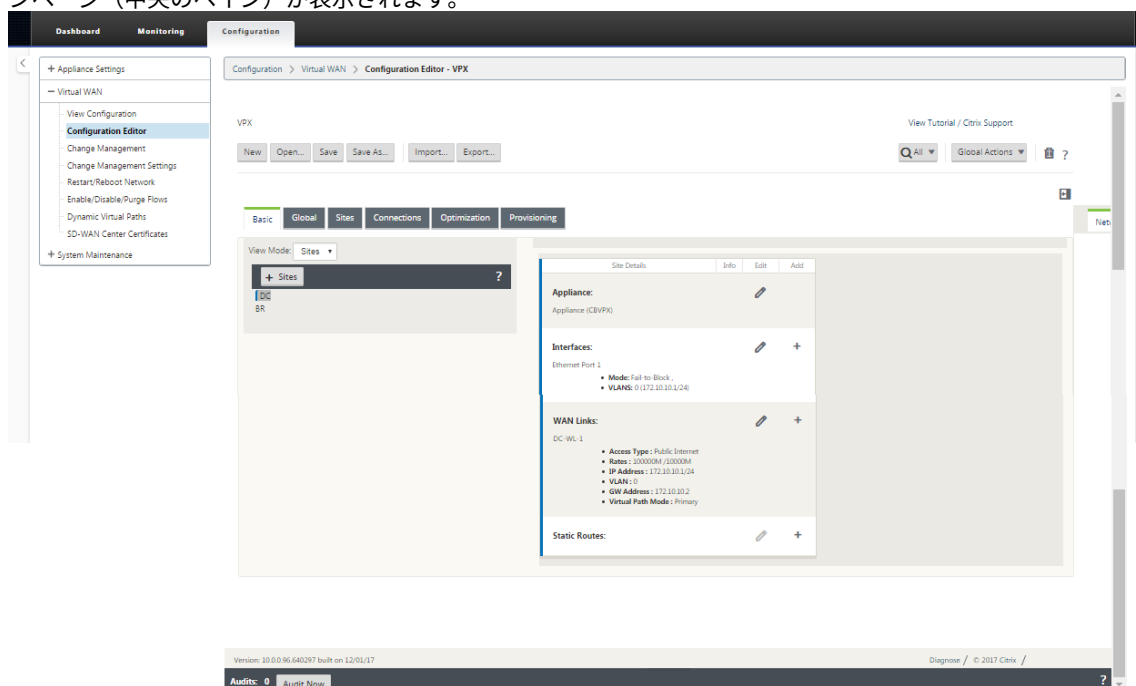
構成パッケージは頻繁に保存するか、構成内の重要なポイントに保存することをお勧めします。手順については、「[MCN サイト設定の命名、保存、およびバックアップ](#)」セクションに記載されています。

警告

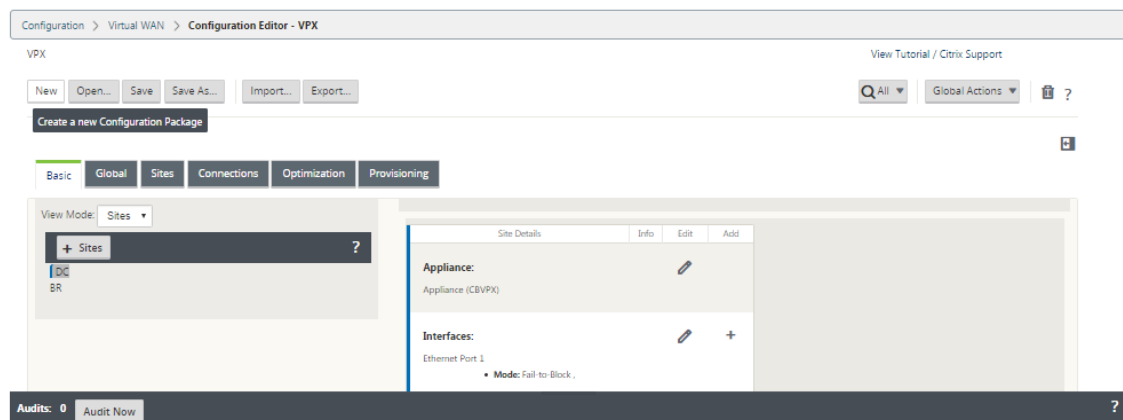
コンソールセッションがタイムアウトになったり、構成を保存する前に管理 Web Interface からログアウトした場合、保存されていない構成の変更はすべて失われます。その後、システムに再度ログインし、設定手順を最初から繰り返す必要があります。そのため、構成パッケージを作成または変更したり、その他の複雑なタスクを実行したりするときは、コンソールセッションのタイムアウト間隔を高い値に設定することをお勧めします。デフォルトは 60 分です。最大値は 9,999 分です。セキュリティ上の理由から、これらのタスクを完了した後、しきい値を下限値にリセットする必要があります。手順については、「[コンソール・セッションのタイムアウト間隔の設定（オプション）](#)」を参照してください。

MCN アプライアンスサイトを追加して構成を開始するには、次の手順を実行します。

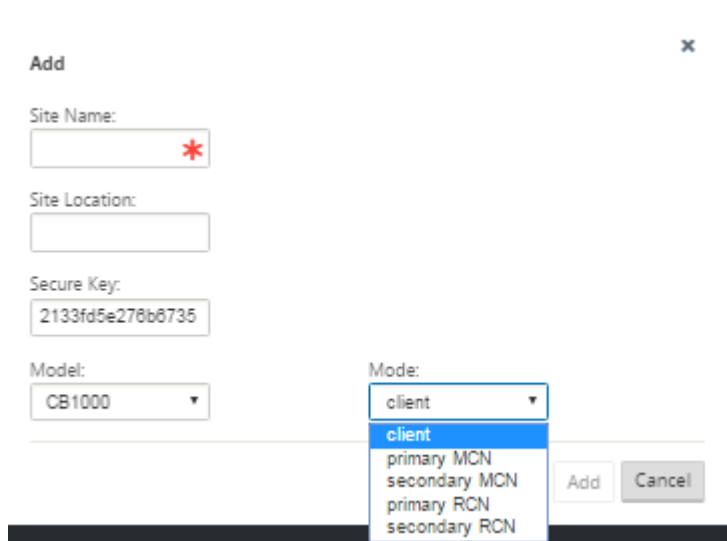
1. ナビゲーションツリーで、[仮想 **WAN**] > [構成エディタ] に移動します。これにより、構成エディタのメインページ（中央のペイン）が表示されます。



2. 「新規」(**New**) をクリックして、新しい構成の定義を開始します。[新しい 構成設定] ページが表示されます。



3. ** サイト バーの [+ S** ites] をクリックして、MCN サイトの追加と構成を開始します。[サイトの追加] ダイアログボックスが表示されます。



4. サイト情報を入力します。

以下を実行します：

1. サイト名とセキュアキーを入力します。
2. アプライアンスの モデルを選択します。
3. モードを選択します。
4. モードとして プライマリ **MCN** を選択します。

注

モデル・オプション・メニューには、サポートされているアプライアンス・モデルの汎用モデル名がリストされます。一般名には、Standard Edition モデルのサフィックスは含まれませんが、対応する SD-WAN アプライアンスモデルに対応しています。この SD-WAN アプライアンスモデルに対応するモデル番号を選択します。(たとえば、これが SD-WAN 4000-SE アプライアンスの場合は 4000 を選択します)。

エントリにはスペースを含めることはできません。また、Linux 形式である必要があります。

サイトを追加するには、次の手順に従います。

1. [追加] をクリックしてサイトを追加します。これにより、新しいサイトが [サイト] ツリーに追加され、新しいサイトの [基本設定] 構成フォームが表示されます。

[適用] をクリックすると、追加のアクションが必要であることを示す監査警告が表示されます。赤い点または金色のデルタアイコンは、表示されるセクションにエラーを示します。これらの警告を使用して、エラーや不足している構成情報を識別できます。監査警告アイコンの上にカーソルを置くと、そのセクションのエラーの簡単な説明が表示されます。暗いグレーの 監査 ステータスバー（ページ下部）をクリックして、未解決の監査警告をすべて一覧表示することもできます。設定時にサイトレベルで設定可能なホスト ARP タイマー（ms）が追加されます。現在のデフォルト値は 1,000 ミリ秒です。設定可能な範囲は 1,000 ミリ秒から 18,000 ミリ秒です。ホスト ARP タイマーの設定は、管理ポートには適用されません。

2. 新しいサイトの基本設定を入力するか、デフォルトをそのまま使用します。ゲートウェイや One-ARM などの Citrix SD-WAN 展開では、ARP 要求を頻繁に受信すると、トラフィックフローに影響するアクセスポイントが過負荷になります。ARP タイマーを設定して、特定のインターバル時間で ARP 要求を送信できるようになりました。時間間隔は秒単位で設定されます。ARP の間隔は、Citrix SD-WAN アプライアンス GUI の [基本設定] タブでデータセンターサイトを構成するときに設定できます。

3. (オプション、推奨) 進行中の構成を保存します。

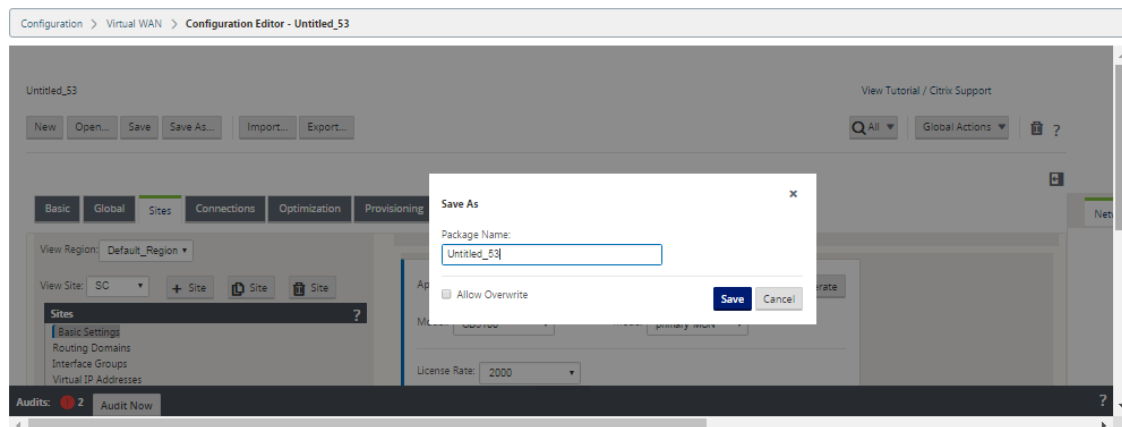
1 つのセッションで設定を完了できない場合は、いつでも保存できるため、後で再び設定を完了できます。構成は、ローカルアプライアンスの Workspace に保存されます。保存した構成での作業を再開するには、構成エディタのメニューバー（ページ上部）の「開く」をクリックします。これにより、変更する構成を選択するためのダイアログボックスが表示されます。

注

余分な予防策として、間違った構成パッケージを上書きしないように、[保存]ではなく[名前を付けて保存]を使用することをお勧めします。

現在の構成パッケージを保存するには、次の手順を実行します。

1. [名前を付けて保存] をクリックします（[構成エディタ] の中央ペインの上部にある）。[名前を付けて保存] ダイアログボックスが表示されます。



2. 構成パッケージ名を入力します。構成を既存のパッケージに保存する場合は、保存する前に [上書きを許可] を選択してください。
3. [保存] をクリックします。

MCN のインターフェイスグループの設定方法

新しい MCN サイトを追加した後、次の手順では、サイトの仮想インターフェイスグループを作成して設定します。

次に、仮想インターフェイスグループの設定に関する注意事項をいくつか示します。

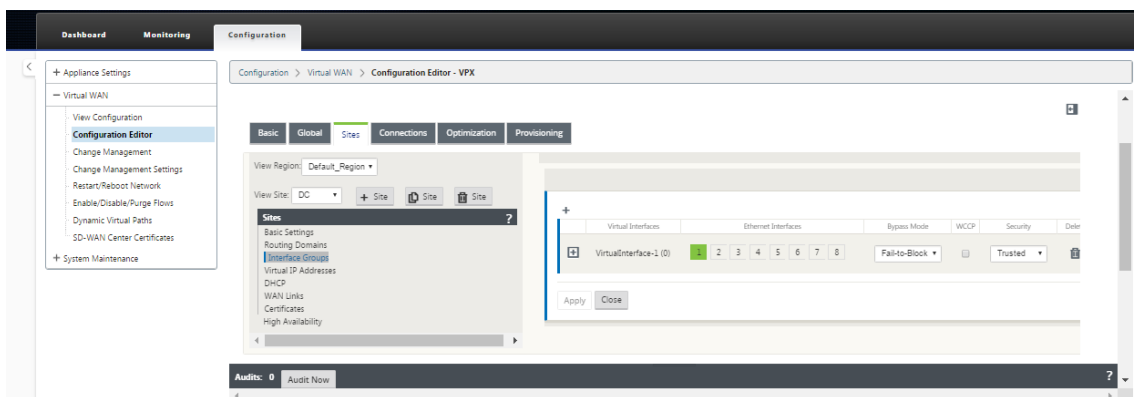
- グループに最も適した論理名を使用します。
- 信頼できるネットワークは、ファイアウォールの背後に保護されるネットワークです。
- 仮想インターフェイスは、インターフェイスを Fail to Wire (FTW) ペアに関連付けます。
- 単一の WAN インターフェイスを FTW ペアにすることはできません。
- IPv6 アドレスは 11.1.0 リリースで導入され、信頼できないインターフェイスでのみサポートされています。信頼できないインターフェイスはルーティング不可能で、仮想パストラフィックに使用されます。

注

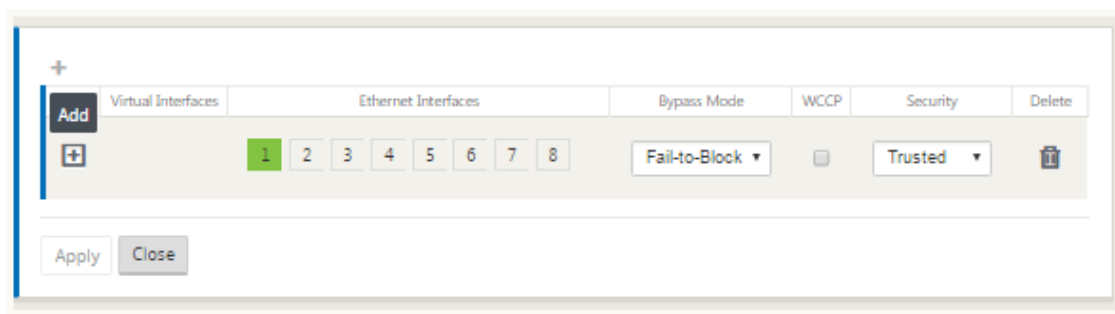
仮想インターフェイスグループの設定に関する注意事項および詳細については、「仮想ルーティングおよび転送」の項を参照してください。

新しい MCN サイトに仮想インターフェイスグループを追加するには、次の手順を実行します。

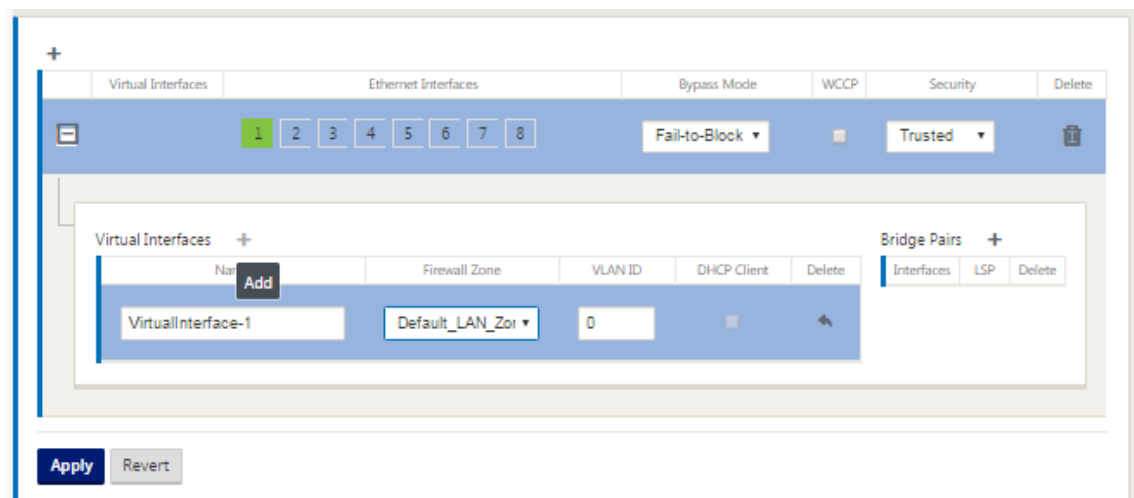
1. 構成エディタの [サイト] ビューで、[サイトの表示] ドロップダウンメニューからサイトを 選択します。これにより、選択したサイトの構成ビューが開きます。



2. [+] をクリックして、仮想インターフェイスグループを追加します。これにより、新しい空の Virtual インターフェイスグループエントリがテーブルに追加され、編集用に開きます。



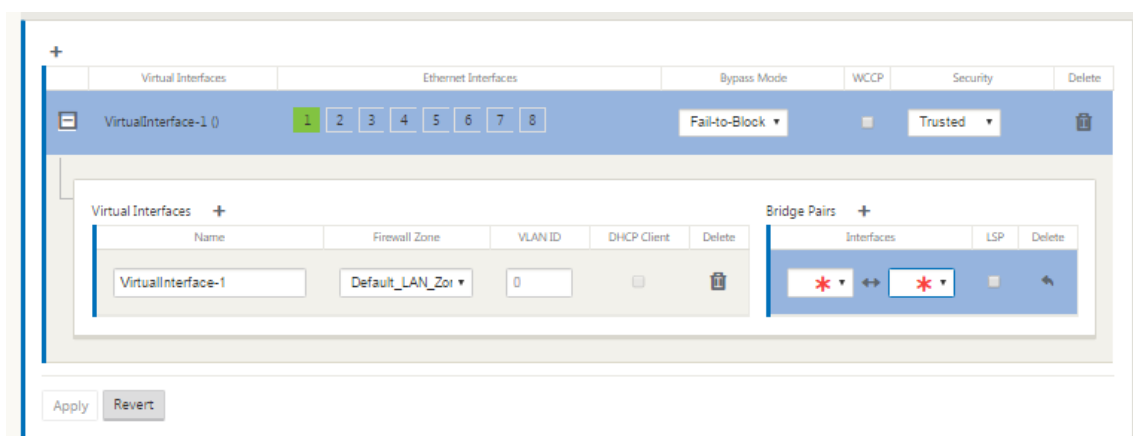
3. [仮想インターフェイス] の右側にある [+] をクリックします。これにより、新しい空のグループエントリがテーブルに追加され、編集用に開きます。



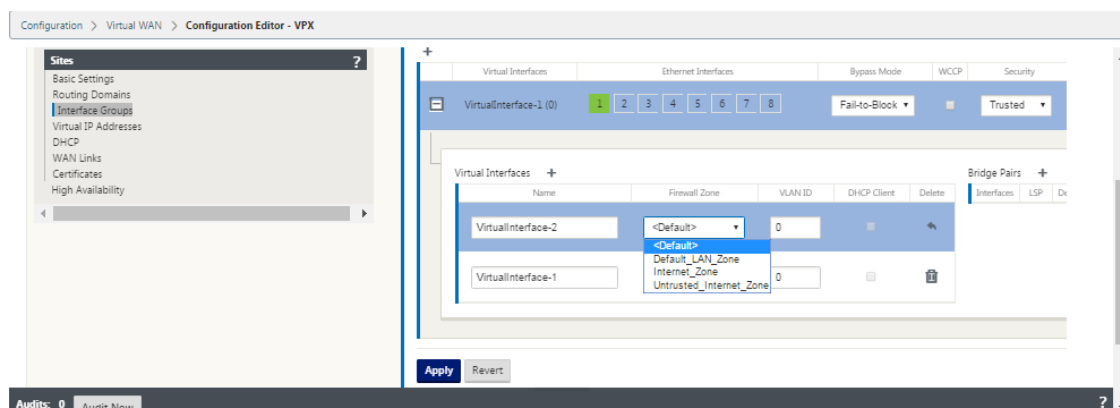
4. グループに含める イーサネットインターフェイスを 選択します。[**Ethernet Interfaces**] で、そのインターフェイスを含める/除外するインターフェイスをクリックします。グループに含めるインターフェイスはいくつでも選択できます。



5. ドロップダウンメニューから [バイパスモード] を選択します (デフォルトなし)。バイパスモード は、アプリケーションまたはサービスの障害または再起動が発生した場合に、仮想インターフェイスグループ内のブリッジペアインターフェイスの動作を指定します。オプションは、[配線失敗] または [ブロック失敗] です。
6. ドロップダウンメニューから [セキュリティレベル] を選択します。仮想インターフェイスグループのネットワークセグメントのセキュリティレベルを指定します。オプションは、[信頼済み] または [信頼できない] です。信頼できるセグメントはファイアウォールで保護されます (デフォルトは Trusted です)。
7. 追加した仮想インターフェイスの左端にある [+] をクリックします。[仮想インターフェイス] テーブルが表示されます。



8. [仮想インターフェイス] の右側にある [+] をクリックします。これにより、名前、ファイアウォールゾーン、**VLAN ID**、ダイレクトブロードキャスト、クライアントモード、ステートレスアドレス自動設定 (**SLAAC**) が表示されます。



9. この仮想インターフェイスグループの名前と **VLAN ID** を入力します。

- **Name** —この仮想インターフェイスが参照される名前です。
- ファイアウォールゾーン - ドロップダウンメニューからファイアウォールゾーンを選択します。
- **VLAN ID** : これは、仮想インターフェイスとの間で送受信されるトラフィックを識別およびマーキングするための ID です。ネイティブ/タグなしトラフィックには、0（ゼロ）の ID を使用します。
- 「クライアントモード」 - ドロップダウンメニューからクライアントモードを選択します。
- ダイレクトブロードキャスト - 仮想インターフェイスで、このチェックボックスを有効にすると、ダイレクトブロードキャストパケットを仮想 IP サブネットに転送できます。
- **SLAAC** —仮想インターフェイスで ステートレスアドレス自動設定（**SLAAC**）チェックボックスを有効にすると、接続されたルータからグローバル IPv6 アドレスを自動的に取得できます。**SLAAC** をオンにした仮想インターフェイスでは、設定された仮想 IP アドレスは必要ありません。

注

SLAAC は、信頼できないインターフェイスのブランチサイトでのみ有効にできます。

SLAAC の IP アドレスを解放または更新することができます。

10. [ブリッジペア] の右側にある [+] をクリックします。これにより、新しい **Bridge Pairs** エントリが追加され、編集用が開きます。
11. ペアリングするイーサネットインターフェイスをドロップダウンメニューから選択します。さらにペアを追加するには、[ブリッジペア] の横にある [+] をもう一度クリックします。
12. [適用] をクリックします。これにより、設定が適用され、新しい仮想インターフェイスグループがテーブルに追加されます。この段階では、新しい仮想インターフェイスグループエントリの右側に、黄色の Delta Audit Alert アイコンが表示されます。これは、サイトの仮想 IP アドレス (VIP) をまだ構成していないためです。現時点では、このアラートは、サイトの仮想 IP を正しく構成すると自動的に解決されるため、無視できます。
13. さらに仮想インターフェイスグループを追加するには、[Interface Groups] ブランチの右側にある [+] をクリックし、上記の手順に進みます。

MCN の仮想 IP アドレスを設定する方法

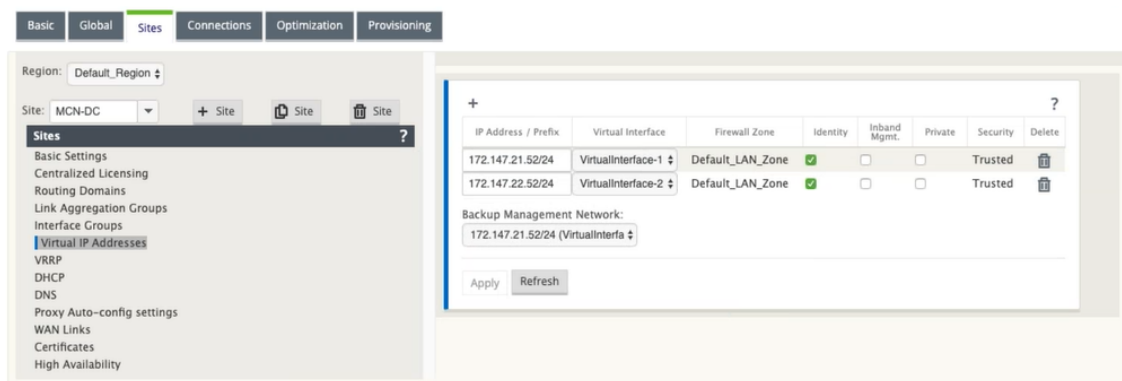
次の手順では、サイトの仮想 IP アドレスを構成し、適切なグループに割り当てます。

1. 新しい MCN サイトの [サイト] ビューで、[仮想 IP アドレス] の左にある [+] をクリックします。これにより、新しいサイトの 仮想 IP アドレス テーブルが表示されます。
2. [仮想 IP アドレス] の右側にある [+] をクリックして、アドレスを追加します。これにより、新しい仮想 IP アドレスを追加および構成するためのフォームが開きます。
3. IP アドレス / プレフィックス 情報を入力し、アドレスが関連付けられている 仮想インターフェイスを 選択します。仮想 IP アドレスには、完全なホストアドレスとネットマスクを含める必要があります。
4. [ファイアウォールゾーン]、[ID]、[プライベート]、[セキュリティ] など、仮想 IP アドレスの設定を選択します。
5. [Inband Mgmt] を選択すると、仮想 IP アドレスが Web UI や SSH などの管理サービスに接続できるようになります。

注:

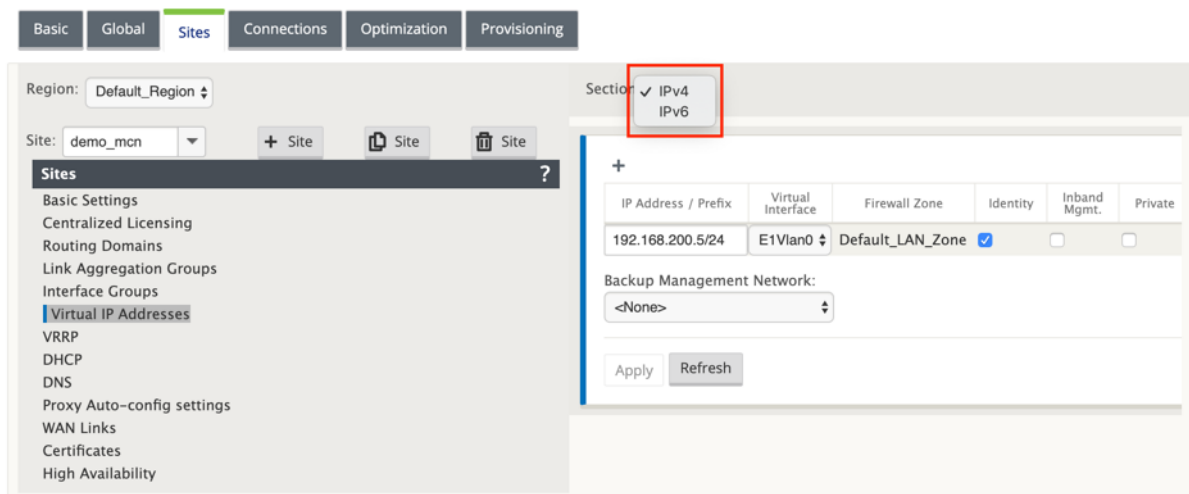
インターフェイスは、セキュリティタイプ「信頼済み」および「ID」が有効である必要があります。

6. バックアップ管理ネットワークとして仮想 IP を選択します。これにより、管理ポートにデフォルト Gateway が設定されていない場合に、管理に仮想 IP アドレスを使用できます。



7. [適用] をクリックします。これにより、アドレス情報がサイトに追加され、サイトの 仮想 IP アドレス テーブルに含められます。
8. さらに仮想 IP アドレスを追加するには、[仮想 IP アドレス] の右側にある [+] をクリックし、上記の手順を実行します。

11.1.0 以降のリリースでは、[仮想 IP アドレス] の下に ****IPv4** アドレスと **IPv6** アドレスの **** 2 つ**のサブセクションを使用できます。



制限事項

- IPv4 と IPv6 の両方のアクセスインターフェイスが同じ WAN リンクに設定されている場合、パスのペアは 1 つだけ作成されます。
- IPv6 パスがダウンした場合、同じ WAN リンクの IPv4 へのフォールバックは発生しません。
- IPv6 アドレスの追跡は、11.1.0 リリースではサポートされていません。
- IPv6 は、仮想パス経由の SD-WAN デバイス間の通信でのみサポートされます。インターネットサービスおよびイントラネットサービスはサポートされていません。11.1.0 リリースでは、管理プレーンのサポートはありません。
- 11.1.0 リリースでは、210 デバイス上の LTE リンクでは IPv6 はサポートされません。
- DHCPv6 クライアントおよびサーバは IPv6 ではサポートされていません。自動アドレス指定用に SLAAC を設定できます。

新しく作成された信頼できないインターフェイスの仮想 IP アドレスを追加する必要があります。または、SLAAC がブランチサイトである場合は、SLAAC を有効にできます。仮想 IP アドレスを追加するには

1. [セクション] ドロップダウンメニューから [IPv6] を選択します。
2. 次のフィールドを定義します。
3. [IP Address/Prefix]: 完全なホストアドレスとネットマスクを指定します。
4. [Virtual Interface]: ドロップダウンメニューから、関連付けられた仮想インターフェイスの 1 つを選択します。
5. ファイアウォールゾーン: 仮想インターフェイスのファイアウォールゾーン。
6. [Link Local] (オプション) -[Link Local] チェックボックスをオンにすると、この IPv6 仮想 IP アドレスを仮想インターフェイスのリンクローカルアドレスとして使用できます。

注:

[Link Local] チェックボックスが有効になっていない場合、アプライアンスはリンク・ローカル・アドレスを自動的に生成して割り当てます。

IP Address / Prefix	Virtual Interface	Firewall Zone	Link Local	Private	Security	Delete
2607:f0d0:2001:0...	E2Vlan0	Untrusted_Internet_Zone	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Untrusted	

Apply Refresh

メモ

近隣探索プロトコル（NDP）は IPv6 でサポートされています。

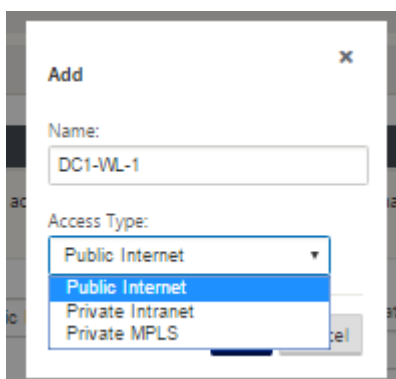
IPv4 と IPv6 の両方のアクセスインターフェイスがローカルサイトとリモートサイトで定義されている場合、パスは IPv6 アドレスのみを使用して形成されます。

MCN の WAN リンクの設定方法

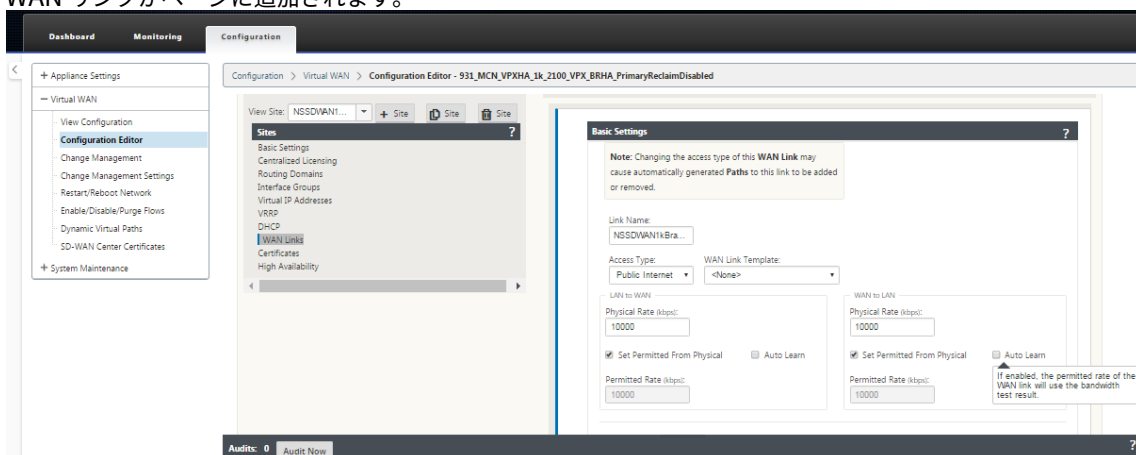
次のステップでは、サイトの WAN リンクを構成します。

1. 新しい MCN サイトの [サイト] ビューで、[**WAN リンク**] ラベルをクリックします。

2. [**WAN リンク**] の右側にある [Add Link] をクリックして、新しい WAN リンクを追加します。[追加] ダイアログボックスが表示されます。

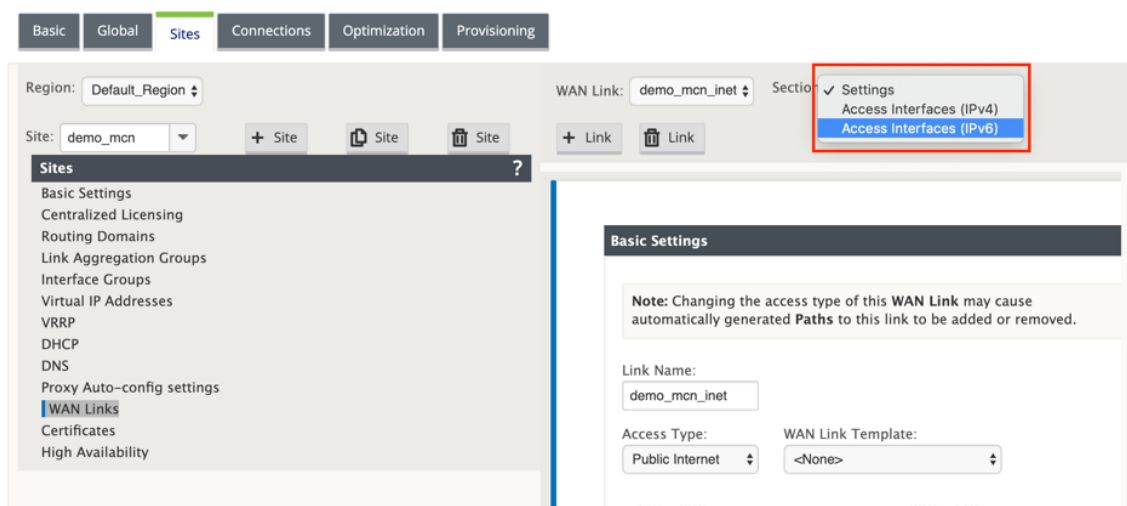


3. (オプション) デフォルトを使用しない場合は、WAN リンクの名前を入力します。デフォルトはサイト名で、次のサフィックス「WL-」が付加されます。<number> ここで、<number> はこのサイトの WAN リンクの数をも 1 ずつ増やします。
4. ドロップダウンメニューから「アクセスタイプ」を選択します。オプションは、[パブリックインターネット]、[プライベートイントラネット]、または [プライベート **MPLS**] です。
5. [追加] をクリックします。これにより、[WAN リンクの基本設定] 設定ページが表示され、新しい未設定の WAN リンクがページに追加されます。



IPv4 と IPv6 の両方のアクセスインターフェイスが同じ WAN リンクに対して構成されている場合、2 つのサイト間の IPv6 パスのみが形成されます。

1. [設定] ドロップダウンメニューから [アクセスインターフェイス (**IPv6**)] を選択します。



2. 次のフィールドを定義します。

- 「名前」 — アクセスインターフェース名を指定します。
- **[Virtual Interface]** : ルーティングドメインを選択したら、ドロップダウンメニューから関連する仮想インターフェースのいずれかを選択します。
- **[IP Address]** : SD-WAN 上のアクセスインターフェースエンドポイントに静的 IP アドレスを指定します。
- **[Gateway IP アドレス]** — ゲートウェイルータの IP アドレスを指定します。

メモ

仮想アプライアンスが SLAAC モードを使用するように構成されている場合は、IP アドレスと Gateway IP アドレスを設定できません。

- **Virtual Path Mode** : ドロップダウンメニューから仮想パスモードを選択して、この WAN リンク上の仮想パストラフィックのプライオリティを決定します。
- **Gateway MAC アドレスバインダー** [ゲートウェイ MAC アドレスバインド] チェックボックスが有効な場合、インターネットまたはイントラネットサービスで受信されるパケットの送信元 MAC アドレスは、ゲートウェイ MAC アドレスと一致する必要があります。



WAN リンクに対して IPv6 インターフェイスが作成されたら、このインターフェイスを使用してインターネットサービスプロバイダ (ISP) と通信できます。

メモ

最初の IPv6 ソリューションは仮想パス接続のみであるため、LAN 側の IPv6 パケットを送信できません。

帯域幅消費の自動学習

自動学習は、システムの起動時に実行され、正常な結果が観察されるまで 5 分ごとに繰り返されます。自動学習は、設定エディタから WAN リンク設定の変更が行われた後にも実行されます。

テストは手動で実行することも、SD-WAN GUI でスケジュールすることもできます。テストが成功し、自動学習が有効になっている場合、これらのテストの結果は、許可されたレートにも適用されます。

大規模なネットワークで自動学習を使用する場合、config change が再起動すると、すべてのサイトが MCN で同時にテストを実行し、帯域幅の使用率が高くなり、結果が不正確になります。帯域幅テストは、1 日 1～2 回（通常はトラフィック量が少ない場合）にスケジュールすることをお勧めします。

注

WAN リンク帯域幅の自動検出は、ブランチにのみ適用され、MCN/RCN には適用されません。

1. 新しい WAN リンクのリンクの詳細を入力します。LAN から WAN、WAN から **LAN** への設定を構成します。いくつかのガイドラインは次のとおりです。

- 一部のインターネットリンクは非対称である場合があります。
- 許可された速度を誤って設定すると、そのリンクのパフォーマンスに悪影響を及ぼす可能性があります。
- 認定レートを超えるバースト速度は使用しないでください。
- インターネット WAN リンクの場合は、必ずパブリック IP アドレスを追加してください。

2. グレーの [詳細設定] セクションバーをクリックします。リンクの [詳細設定] フォームが開きます。

3. リンクの **【詳細設定】** を入力します。

- **[Provider ID]**: (オプション) 同じサービスプロバイダーに接続されている WAN リンクを指定するための一意の ID 番号 1 ~100 を入力します。仮想 WAN は、重複パケットを送信するときにプロバイダー ID を使用してパスを区別します。
- **[Frame Cost (bytes)]**: 各パケットに追加するヘッダー/トレーラーのサイズ (バイト単位) を入力します。たとえば、追加されたイーサネット IPG または AAL5 トレーラーのバイト単位のサイズ。
- **輻輳しきい値**: 輻輳しきい値 (マイクロ秒単位) を入力します。このしきい値は、WAN リンクがパケット転送を抑制し、それ以上の輻輳を回避します。
- **[MTU Size (bytes)]**: フレームコストを含まない、最大の raw パケットサイズ (バイト単位) を入力します。

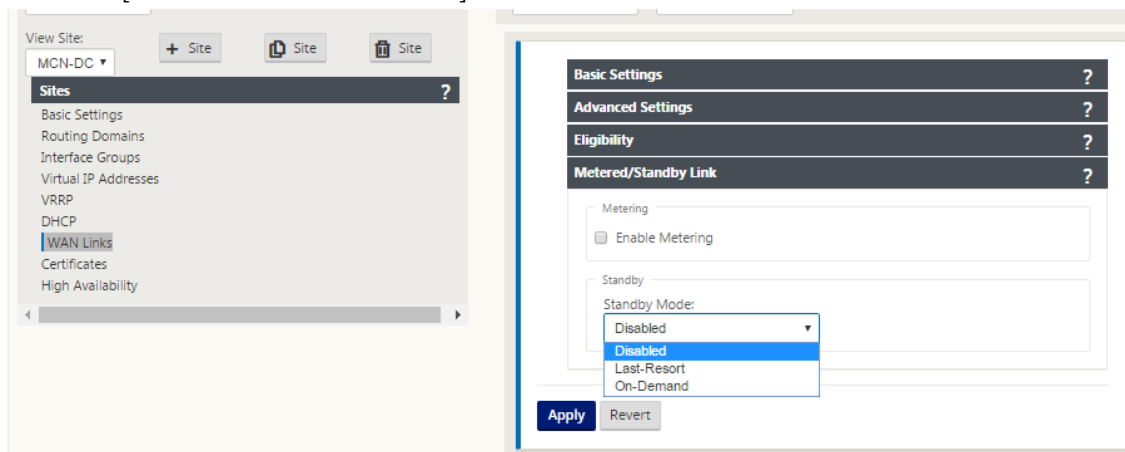
4. グレーの「適格」セクション・バーをクリックします。リンクの **【適格設定】** フォームが開きます。

5. リンクの「適格」設定を選択します。

6. グレーの **【従量制課金リンク】** セクションバーをクリックします。リンクの **【従量制課金リンク設定】** フォームが開きます。

7. (オプション) このリンクの **メータリング** を有効にするには、**【メータリングを有効にする】** を選択します。こ

れにより、[メータリング設定を有効にする] フィールドが表示されます。



Metering

☒ Enable Metering ☒ Disable if Data Cap reached

Data Cap (MB): Billing Cycle: Starting From:

Standby

Standby Mode:

Heartbeat Interval

Caution: It takes at least 4 times the heartbeat interval to detect connectivity failure.

Active Heartbeat Interval:

8. リンクのメータリング設定を構成します。以下のコマンドを実行します。

- 「データ上限 (MB)」—リンクに対するデータ上限割り当てをメガバイト単位で入力します。
- 「請求 サイクル」—ドロップダウンメニューから「月次」または「週次」を選択します。
- 開始日—請求サイクルの開始日を入力します。
- 「Set **Last Resort**」—他のすべての使用可能なリンクに障害が発生した場合に、このリンクを最後の手段のリンクとして有効にする場合に選択します。通常の WAN 条件下では、仮想 WAN は、リンクステータスを確認するために、従量制課金リンクを介して最小限のトラフィックだけを送信します。ただし、障害が発生した場合、SD-WAN は本番トラフィックを転送するための最後の手段として、アクティブな従量制課金リンクを使用できます。

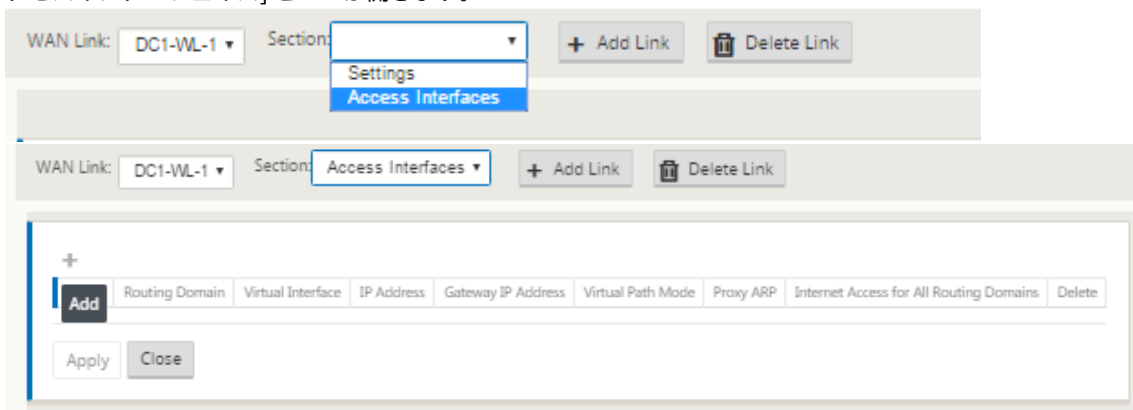
[適用] をクリックします。これにより、指定した設定が新しい WAN リンクに適用されます。

次のステップでは、新しい WAN リンクのアクセスインターフェイスを設定します。アクセスインターフェイスは、特定の WAN リンクのインターフェイスとしてまとめて定義された、仮想インターフェイス、WAN エンドポイント

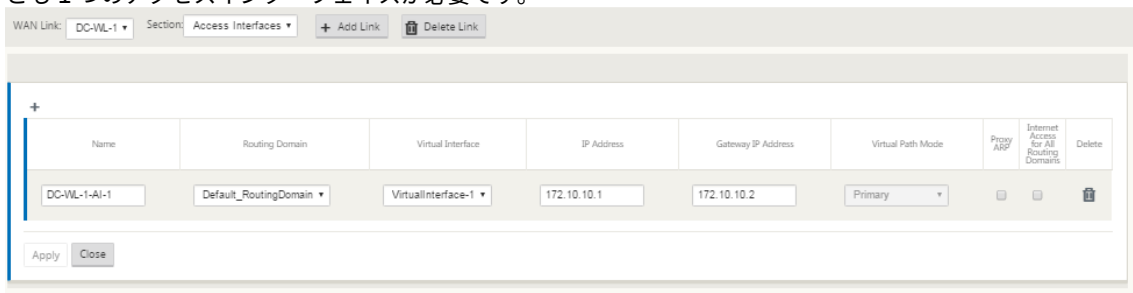
IP アドレス、ゲートウェイ IP アドレス、および仮想パスモードで構成されます。各 WAN リンクには、少なくとも 1 つのアクセスインターフェイスが必要です。

アクセスインターフェイスの設定方法

1. リンクの [WAN リンク] 設定ページで [アクセスインターフェイス] を選択します。これにより、サイトの [アクセスインターフェイス] ビューが開きます。



2. [+] をクリックして、インターフェイスを追加します。これにより、テーブルに空白のエントリが追加され、編集用に開かれます。リンクの [アクセスインターフェイス] 設定を入力します。各 WAN リンクには、少なくとも 1 つのアクセスインターフェイスが必要です。



3. 以下のコマンドを実行します。

- [Name]: このアクセスインターフェイスが参照される名前です。新しいアクセスインターフェイスの名前を入力するか、デフォルトをそのまま使用します。デフォルトでは、
WAN_Link_name-AI-number: という命名規則が使用されます。WAN_link_name はこのインターフェイスに関連付ける WAN リンクの名前で、number はこのリンクに現在設定されているアクセスインターフェイスの数を 1 ずつ増やしたものです。

注

名前が切り捨てられた場合は、フィールドにカーソルを置き、クリックしたままマウスを右または左に回転すると、切り捨てられた部分が表示されます。

- 仮想インターフェイス: このアクセスインターフェイスが使用する仮想インターフェイスです。このブランチサイト用に構成された Virtual Interfaces のドロップダウンメニューからエントリを選択します。

- ルーティングドメイン - アクセスインターフェイス用に選択するルーティングドメイン。
- **IP アドレス**—アプライアンスから WAN へのアクセスインターフェイスエンドポイントの IP アドレスです。
- **Gateway IP** アドレス—ゲートウェイルータの IP アドレスです。
- **Virtual Path Mode** : この WAN リンク上の仮想パストラフィックのプライオリティを指定します。オプションは、[プライマリ]、[セカンダリ]、または[除外]です。[除外]に設定すると、このアクセスインターフェイスはインターネットおよびイントラネットトラフィックにのみ使用されます。
- **[Proxy ARP]**: 有効にするチェックボックスをオンにします。有効にすると、Gateway に到達できない場合に、仮想 WAN アプライアンスはゲートウェイ IP アドレスの ARP 要求に応答します。

1. [適用] をクリックします。

これで、新しい WAN リンクの設定が完了しました。これらの手順を繰り返して、サイトの WAN リンクを追加および構成します。

次のステップでは、サイトのルートを追加および構成します。

MCN のルートを設定する方法

サイトのルートを追加および構成するには、次の手順を実行します。

1. 新しい MCN サイトの [接続] ビューをクリックし、[ルート] を選択します。これにより、サイトの [ルート] ビューが表示されます。
2. ルートを追加するには、[ルート] の右側にある [+] をクリックします。これにより、編集用の [ルート] ダイアログボックスが開きます。

The screenshot shows a dialog box titled "Add" with a close button (X) and a help button (?). It contains the following fields and options:

- Network IP Address**: A text input field with a red asterisk (*) indicating it is required.
- Cost**: A text input field containing the value "5".
- Service Type**: A dropdown menu currently showing "Local".
- Gateway IP Address**: A text input field with a red asterisk (*) indicating it is required.
- Export Route**: A checked checkbox.
- Summary Route**: An unchecked checkbox.
- Eligibility Based On Path**: An unchecked checkbox.
- Path:**: A dropdown menu currently showing "<None>".
- Eligibility Based On Gateway**: An unchecked checkbox.
- Buttons**: "Add" and "Cancel" buttons at the bottom right.

3. 新しいルートのルート設定情報を入力します。以下のコマンドを実行します。

- 「ネットワーク **IP** アドレス」—ネットワーク **IP** アドレスを入力します。
- **Cost**—このルートのルートプライオリティを決定するために、1～15 の重みを入力します。低コストのルートは、高コストのルートよりも優先されます。デフォルト値は 5 です。
- **[Service Type]**—このフィールドのドロップダウンメニューからルートのサービスタイプを選択します。
 - 仮想パス—このサービスは、仮想パスを通過するトラフィックを管理します。仮想パスは、2 つの WAN リンク間の論理リンクです。これは、2 つの SD-WAN ノード間で高いサービス・レベル通信を提供するために結合された WAN パスの集合で構成されます。これは、変化するアプリケーションの需要と WAN の状態に常に測定し、適応することによって達成されます。SD-WAN アプライアンスは、パス単位でネットワークを測定します。仮想パスは、スタティック（常に存在）またはダイナミック（2 つの SD-WAN アプライアンス間のトラフィックが設定されたしきい値に達した場合のみ存在）のいずれかになります。
 - インターネット—このサービスは、エンタープライズサイトとパブリックインターネット上のサイト間のトラフィックを管理します。このタイプのトラフィックはカプセル化されません。輻輳時には、SD-WAN は、仮想パスに対するレート制限によるインターネットトラフィックと、管理者が確立した SD-WAN 構成に従ってイントラネットトラフィックによって、帯域幅を積極的に管理します。
 - イントラネット—このサービスは、仮想パス経由の送信用に定義されていないエンタープライズイントラネットトラフィックを管理します。インターネットトラフィックと同様に、カプセル化されていないままであり、SD-WAN は、輻輳時にこのトラフィックを他のサービスタイプと比較してレート制限することで、帯域幅を管理します。特定の条件下では、仮想パスでイントラネットフォールバック用に構成されている場合、通常は仮想パスで移動するトラフィックは、ネットワークの信頼性を維持するために、代わりにイントラネットトラフィックとして扱われることがあります。
 - パススルー—このサービスは、仮想 WAN を通過するトラフィックを管理します。パススルーサービスに送信されるトラフィックには、ブロードキャスト、ARP、その他の非 IPv4 トラフィック、および Virtual WAN アプライアンスのローカルサブネット、構成済みサブネット、またはネットワーク管理者が適用したルール上のトラフィックが含まれます。このトラフィックは、SD-WAN によって遅延、シェーピング、または変更されません。したがって、SD-WAN アプライアンスが他のサービスで使用するように構成されている WAN リンク上で、パススルートラフィックが実質的なリソースを消費しないようにする必要があります。
 - ローカル：このサービスは、他のサービスと一致しないサイトへのローカルな IP トラフィックを管理します。SD-WAN は、ローカルルートを送信元および宛先とするトラフィックを無視します。
 - **GRE** トンネル：このサービスは、GRE トンネル宛ての IP トラフィックを管理し、サイトで設定された LAN GRE トンネルと一致します。GRE トンネル機能を使用すると、LAN 上の GRE トンネルを終了するように SD-WAN アプライアンスを設定できます。サービスタイプ GRE Tunnel のルートの場合、Gateway はローカル GRE トンネルのトンネルサブネットの 1 つに存在する必要があります。
 - **LAN IPsec** トンネル—このサービスは、IPsec トンネル宛の IP トラフィックを管理します。
 - インタールーティング—このサービスは、サイト内のルーティングドメイン間または異なるサイト間のルートリークを可能にします。これにより、エッジルータがルートリークを処理する必要がなくなります。
- 「ゲートウェイ **IP** アドレス」—このルートの ゲートウェイ **IP** アドレスを入力します。
- 適格性 -パスに基づく（チェックボックス）：（オプション）有効にすると、選択したパスがダウンしても、ルー

トはトラフィックを受信しません。

- 「パス」 (Path) ルートの適格性を判断するために使用するパスを指定します。

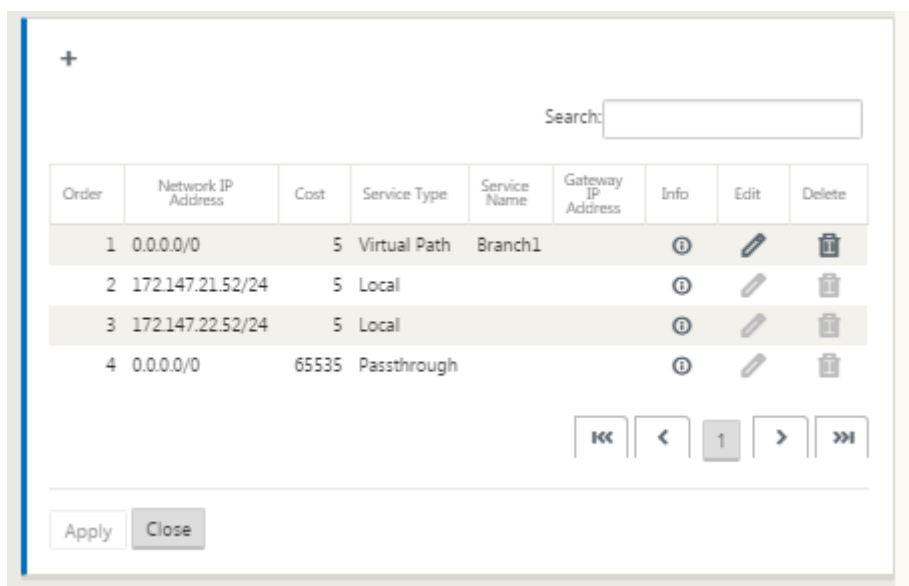
「サービスタイプ」に応じて、次の設定が表示されます。

サービスの種類	サービスタイプ設定
仮想パス	[Next Hop Site]: 仮想パスパケットの送信先となるリモートサイトを示します。
インターネット	ルートのエクスポート: ルートを他の接続されたサイトにエクスポートするには、有効/無効にします。パスに基づく適格性
イントラネット	エクスポートルート、イントラネットサービス、パスに基づく適格性、トンネルに基づく適格性
パススルー	パスに基づく適格性
ローカル	エクスポートルート、サマリールート、パスに基づく適格性
GRE トンネル	エクスポートルート、パスに基づく適格性、ゲートウェイに基づく適格性
IPSec トンネル	エクスポートルート、パスに基づく適格性、IPSec トンネル、トンネルに基づく適格性
破棄	エクスポートルート、サマリールート
インタールーティング	インタールーティングドメインサービス

1. [適用] をクリックします。

注

[適用] をクリックすると、追加のアクションが必要であることを示す監査警告が表示されることがあります。赤い点または金色のデルタアイコンは、表示されるセクションにエラーを示します。これらの警告を使用して、エラーや不足している構成情報を識別できます。監査警告アイコンの上にカーソルを置くと、そのセクションのエラーの簡単な説明が表示されます。暗いグレーの 監査 ステータスバー (ページ下部) をクリックして、すべての監査警告の一覧を表示することもできます。



Order	Network IP Address	Cost	Service Type	Service Name	Gateway IP Address	Info	Edit	Delete
1	0.0.0.0/0	5	Virtual Path	Branch1				
2	172.147.21.52/24	5	Local					
3	172.147.22.52/24	5	Local					
4	0.0.0.0/0	65535	Passthrough					

設定済みのルートを次のように編集することもできます。

Edit

Network IP Address: 0.0.0.0/0 Cost: 5 Service Type: Virtual Path Gateway IP Address:

Next Hop Site:

Branch1 ▼

☒ Eligibility Based On Path

Path:

Branch1-WL-1->MCN-DC-WL-1 ▼

Apply

Cancel

サイトのルートを追加するには、[ルート] ブランチの右側にある [***] をクリックし、上記の手順を実行します。
**

これで、新しい MCN サイトのプライマリ設定情報の入力が完了しました。次の 2 つのセクションでは、オプションの手順について説明します。

- [MCN サイトの高可用性 \(HA\) の設定 \(オプション\)。](#)
- [仮想 WAN セキュリティおよび暗号化の有効化と設定 \(オプション\)。](#)

これらの機能を今すぐ設定したくない場合は、[MCN サイト設定の命名、保存、およびバックアップ] に進みます。 (</en-us/citrix-sd-wan/current-release/configuration/set-up-master-control-node/manage-mcn-configuration.html>)

仮想 WAN セキュリティと暗号化の有効化と構成 (オプション)

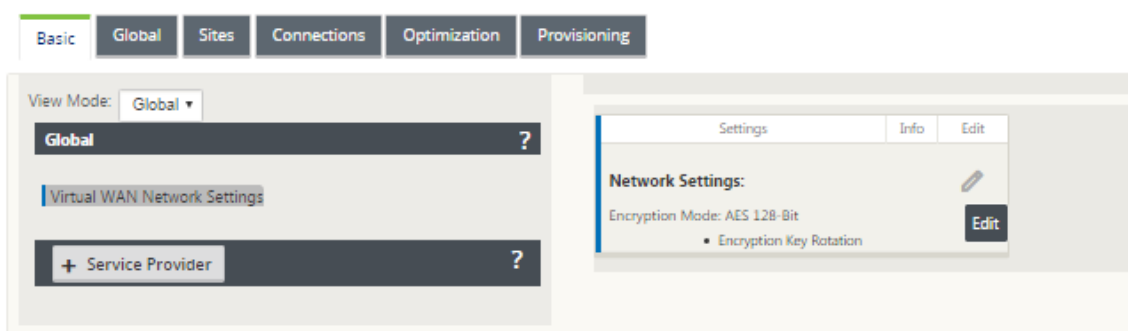
May 10, 2021

仮想 WAN のセキュリティと暗号化を有効にして構成するには、次の手順を実行します。

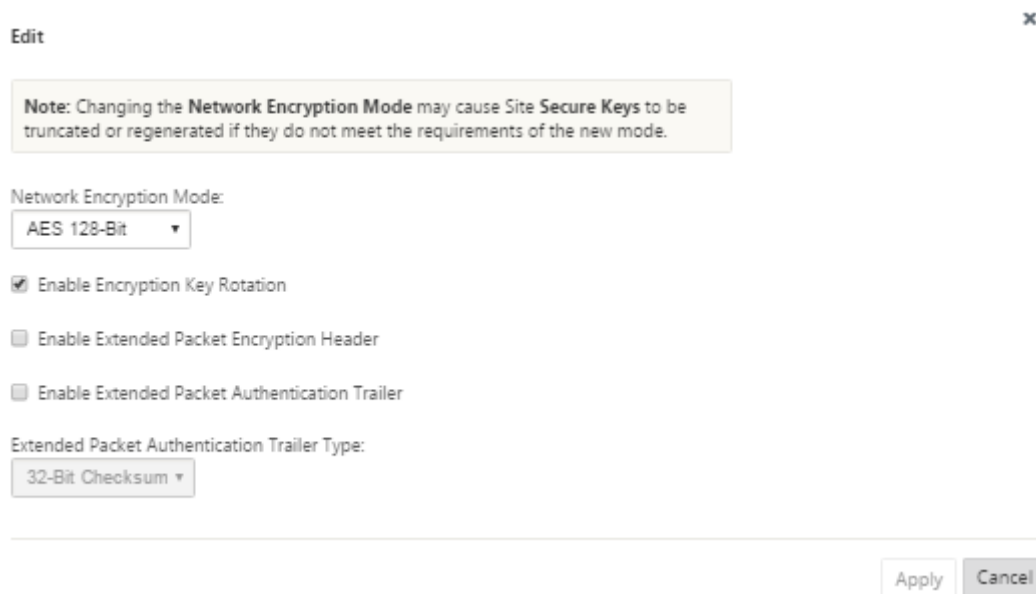
注

仮想 WAN セキュリティと暗号化の有効化はオプションです。

1. 構成エディタの「基本」タブに移動し、「表示 モードから グローバル」を選択します。[仮想ネットワーク設定] 構成フォームが表示されます。



2. [編集] (鉛筆アイコン) をクリックして、フォームの編集を有効にします。



3. グローバルセキュリティ設定を入力します。使用できるオプションは、次のとおりです。

- ネットワーク暗号化モード暗号化パスに使用される暗号化アルゴリズムです。ドロップダウンメニューから [AE **S** 128 ビット] または [AES ******256 ビット ******] のいずれかを選択します。

- 暗号化キーのローテーションを有効にする：有効にすると、暗号化キーは 10 ～15 分間隔でローテーションされます。
- **Enable Extended Packet Encryption Header**: 有効にすると、暗号化トラフィックの先頭に 16 バイトの暗号化カウンタが付加され、初期化ベクトルとして機能し、パケット暗号化をランダム化します。
- 拡張パケット認証トレーラーを有効にする：有効にすると、暗号化されたトラフィックの内容に認証コードが追加され、メッセージが変更されずに配信されることを確認します。
- 拡張パケット認証トレーラタイプ: これは、パケットの内容を検証するために使用されるトレーラのタイプです。ドロップダウンメニューから [**32 ビットチェックサム**] または [**SHA-256**] のいずれかを選択します。

4. [**Apply**] をクリックして、設定を構成に適用します。

これで、MCN サイトの構成は完了です。次のステップでは、次のセクションで説明するように、新しい MCN サイト設定に名前を付けて保存します（オプションですが、推奨）。

警告

コンソールセッションがタイムアウトになったり、構成を保存する前に管理 Web Interface からログアウトした場合、保存されていない構成の変更はすべて失われます。その後、システムに再度ログインし、設定手順を最初から繰り返す必要があります。そのため、構成パッケージを頻繁に保存するか、構成内の重要なポイントに保存することをお勧めします。

セカンダリ MCN の設定

November 8, 2021

MCN 冗長性をサポートするために、サイトをセカンダリ MCN として設定できます。セカンダリ MCN は、プライマリ MCN の健全性を継続的に監視します。プライマリ MCN に障害が発生すると、セカンダリ MCN が MCN の役割を引き継ぎます。セカンダリ MCN を作成するには、[モード] オプションで新しいサイトを追加するときに、セカンダリ MCN を選択します。仮想インターフェイス、仮想 IP、WAN リンク、およびその他の設定を手動で設定できます。同様に、セカンダリ RCN を設定することもできます。

注

セカンダリ MCN 設定と高可用性設定を混同しないでください。セカンダリ MCN 構成では、異なる地理的な場所にあるブランチ/クライアントサイトがセカンダリ MCN として構成され、ディザスタリカバリが可能になります。HA 構成では、フォールトトレランスを確保するために、2 つのアプライアンスを同じサブネットまたは地理的な場所で構成します。高可用性構成の構成については、「[高可用性展開](#)」を参照してください。

セカンダリ MCN のアプライアンスモデルは、使用状況、帯域幅要件、およびサポートされるサイト数に基づいて選択できます。

プライマリ MCN からセカンダリ MCN への切り替えは、プライマリ MCN が非アクティブ状態の 15 秒後に発生します。セカンダリ MCN のプライマリ再要求は設定できません。プライマリ再要求は、プライマリアプライアンスが再びオンになり、ホールドタイマーが期限切れになると、自動的に実行されます。

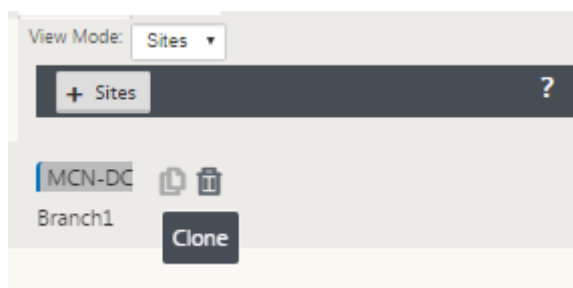
セカンダリ MCN を設定する最善の方法は、MCN 設定のほとんどを保持するため、既存の MCN のクローンを作成することです。サイトのクローンが作成されると、サイトの構成設定セット全体がコピーされ、単一のフォーム画面に表示されます。その後、要件に従って設定をすばやく簡単に変更できます。

注

MCN をクローンして、セカンダリ MCN またはブランチサイトを作成できます。設定できるセカンダリ MCN は 1 つだけです。

MCN サイトのクローンを作成し、セカンダリ **MCN** を作成するには

1. 構成エディタで、[基本] > [サイト] に移動し、MCN サイトのクローンアイコンをクリックします。



2. 新しいサイトの構成パラメータ設定を入力します。

Clone

Please review the following fields and make the appropriate changes for the new Site.

Site Name:
MCN-DC

Appliance Name:
Appliance

Mode:
secondary MCN

Secure Key:
250bcca02112f3b6

Routing Domains

Name	Enable	Default
Default_RoutingDomain	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Virtual Interfaces

Name	VLAN ID	DHCP
VirtualInterface-1	0	<input type="checkbox"/>
VirtualInterface-2	0	<input type="checkbox"/>

Virtual IP Addresses

Include	Virtual Interface	Virtual IP Address/Prefix
<input checked="" type="checkbox"/>	VirtualInterface-1	172.147.21.52/24
<input checked="" type="checkbox"/>	VirtualInterface-2	172.147.22.52/24

Local Routes

Include	Network Address	Routing Domain	Gateway
---------	-----------------	----------------	---------

WAN Links

Include Link	WAN Link	Access Type
<input checked="" type="checkbox"/>	MCN-DC-WL-1	

Access Interfaces

Include Interface	Access Interface	Virtual Interface	Virtual IP Address	Gateway
<input checked="" type="checkbox"/>	MCN-DC-WL-1-...	VirtualInterface-1	172.147.21.52	172.147.21.1

| ☒ | MCN-DC-WL-2 | | | |

GRE Tunnels

Include	Name	Source IP	Destination IP	Tunnel IP / Prefix
---------	------	-----------	----------------	--------------------

Clone

Cancel

注:

Audit Alert アイコン（赤いドット）が付いた強調表示されたフィールドは、現在の設定とは異なる値を持つ必要がある必須パラメータ設定を示します。

- 3. [モード] フィールドで、セカンダリ **MCN** を選択します。すべての監査アラートを解決します。
- 4. [クローン] をクリックして、セカンダリ MCN サイトを作成します。

MCN 設定の管理

May 10, 2021

次のステップは、新しい設定に名前を付けて保存することです。これは、設定パッケージとしても見られます。このステップは、設定のこの時点ではオプションですが、推奨されています。構成パッケージは、ローカルアプライアン

スの Workspace に保存されます。その後、管理 Web インターフェイスからログアウトし、後で構成プロセスを続行します。ただし、ログアウトした場合は、再開時に保存した設定を再度開く必要があります。保存した設定を開く手順を以下に示します。

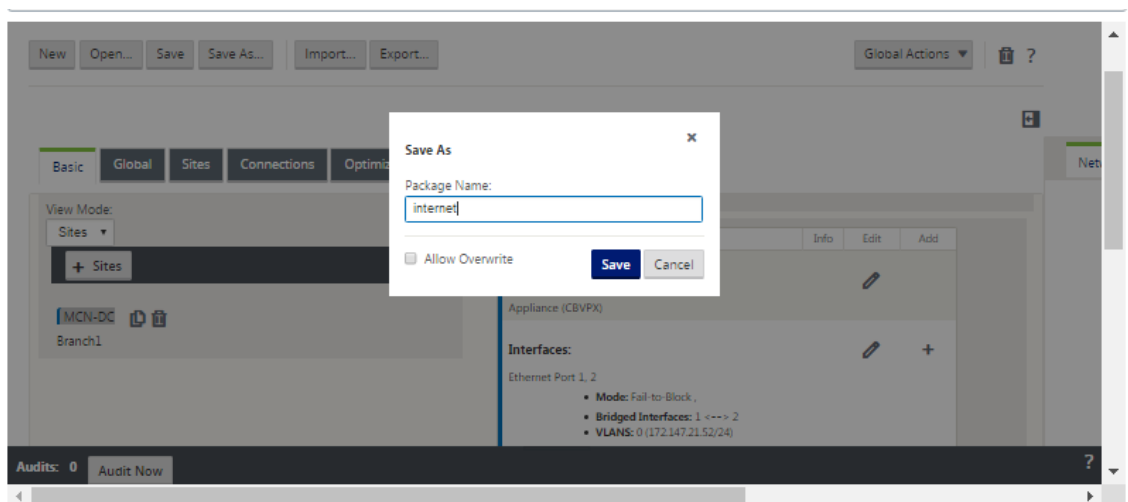
警告

Console セッションがタイムアウトになったり、構成を保存する前に Management Web Interface からログアウトした場合、保存されていない構成の変更はすべて失われます。システムに再度ログインし、最初から設定手順を繰り返す必要があります。そのため、構成パッケージを頻繁に保存するか、構成内の重要なポイントに保存することをお勧めします。

ヒント:

追加の予防策として、誤った構成パッケージを上書きしないように、[保存] ではなく [名前を付けて保存] を使用することをお勧めします。

1. [名前を付けて保存] をクリックします ([構成エディタ] の中央ペインの上部にある)。[名前を付けて保存] ダイアログボックスが表示されます。



2. 構成パッケージ名を入力します。

注

構成を既存の構成パッケージに保存する場合は、保存する前に [上書きを許可] を選択してください。

3. [保存] をクリックします。

注

構成ファイルを保存したら、管理 Web Interface からログアウトして、後で構成プロセスを続行できます。ただし、ログアウトした場合は、再開時に保存した設定を再度開く必要があります。手順については、「[保存した構成パッケージの構成エディタへのロード](#)」の項を参照してください。

これで、MCN サイトの構成が完了し、新しい SD-WAN 構成パッケージが作成されました。これで、ブランチサイトを追加および構成する準備が整いました。手順については、ブランチサイトのセットアップ

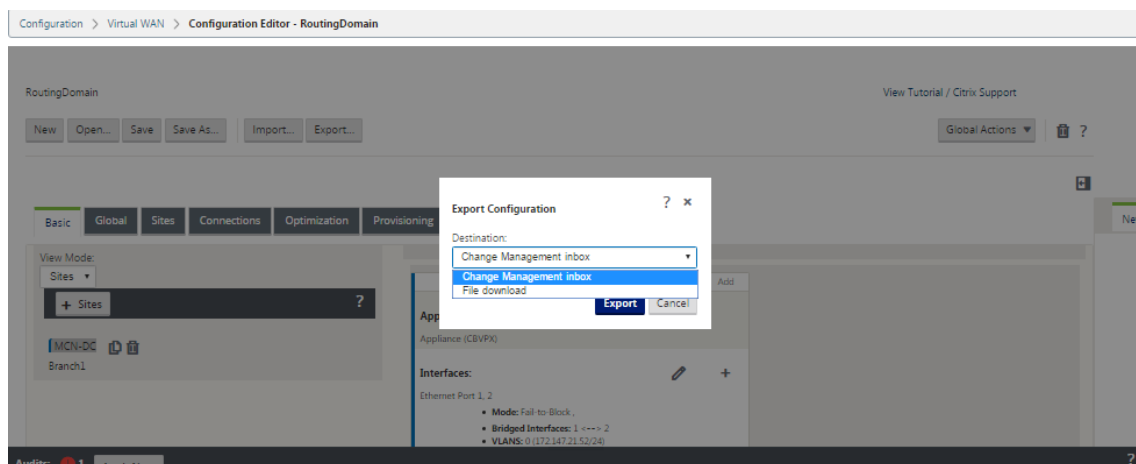
ブ] (</en-us/citrix-sd-wan/current-release/configuration/setup-branch-nodes.html>) を参照してください。

構成パッケージのバックアップコピーのエクスポート

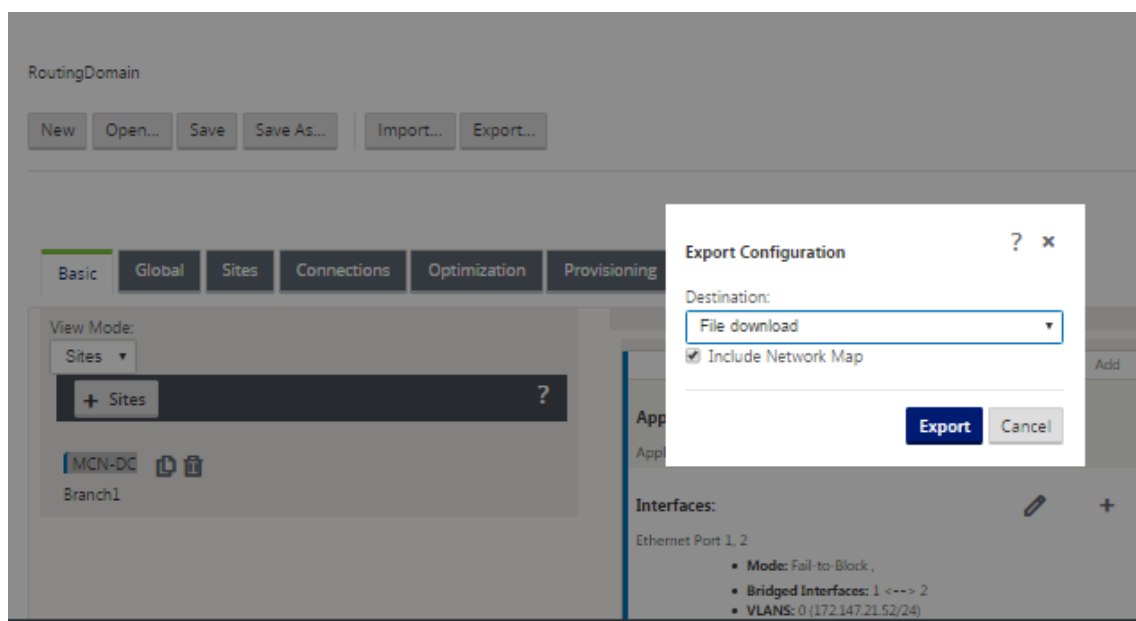
進行中の構成をアプライアンス Workspace に保存するだけでなく、定期的にローカル PC に構成をバックアップすることをお勧めします。

現在の構成パッケージを PC にエクスポートするには、次の手順を実行します。

1. [エクスポート] をクリックします。[設定のエクスポート] ダイアログボックスが表示されます。



2. [宛先:] ドロップダウンメニューから [ファイル] [ダウンロード] を選択します。これにより、既定で選択されている [ネットワークマップを含める] オプションが表示されます。



3. デフォルトを受け入れ、[エクスポート]をクリックします。これには、構成パッケージにネットワークマップ情報が含まれ、構成を保存する名前と場所を指定するためのファイルブラウザが開きます。
4. PCの保存場所に移動し、[保存]をクリックします。これにより、構成パッケージがPCに保存されます。

注

バックアップされた構成パッケージを復元するには、**Import** 操作を使用して、PC からパッケージをインポートし、構成エディターにロードします。その後、インポートしたパッケージを管理 Web インターフェイス Workspace に保存して、将来使用できるようにすることができます。

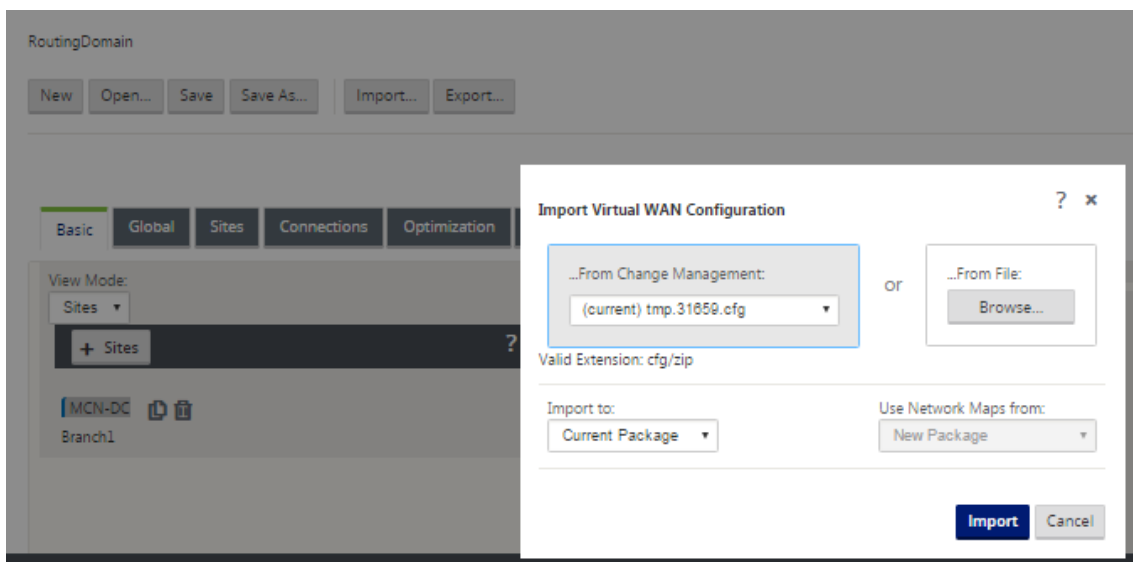
バックアップされた構成パッケージのインポート

場合によっては、以前のバージョンの構成パッケージに戻したいことがあります。以前のバージョンのコピーをローカル PC に保存した場合は、そのコピーを Configuration Editor にインポートし、編集用に開くことができます。これが初期展開でない場合は、現在の MCN のグローバル変更管理受信ボックスから既存の構成パッケージをインポートすることもできます。これらの両方の手順の手順を以下に示します。

構成パッケージをインポートするには、次の手順を実行します。

1. 構成エディタを開きます。
2. 構成エディターのメニューバーで、「インポート」をクリックします。

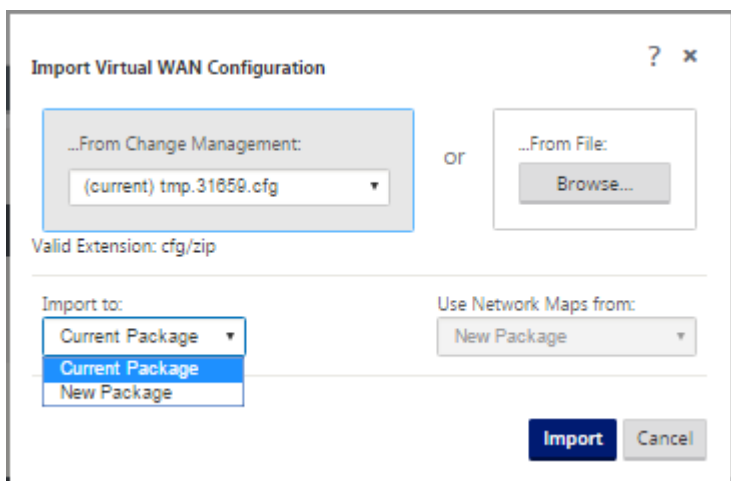
[仮想 **WAN** 構成のインポート] ダイアログボックスが表示されます。



3. パッケージのインポート元となる場所を選択します。
 - 変更管理から構成パッケージをインポートするには、「変更管理から」ドロップダウンメニュー（左上）からパッケージを選択します。

- ローカル PC から構成パッケージをインポートするには、[参照] をクリックして、ローカル PC でファイルブラウザを開きます。ファイルを選択し、[**OK**] をクリックします。

- インポート先を選択します (該当する場合)。構成パッケージがすでに 構成エディタで開いている場合は、「インポート先:」ドロップダウンメニューが表示されます。

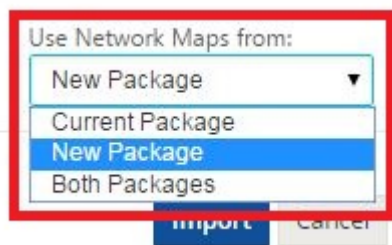


次のいずれかのオプションを選択します:

「現在のパッケージ」—現在開かれている構成パッケージの内容を、インポートされたパッケージの内容に置き換え、開かれているパッケージの名前を保持するには、これを選択します。ただし、変更されたパッケージを明示的に保存するまで、現在のパッケージの保存バージョンの内容は上書きされません。[名前を付けて保存] を使用してパッケージを保存する場合は、[上書きを許可] を選択して、前のバージョンの上書きを有効にします。

- 「新規パッケージ」(New Package)—新しい空白の構成パッケージを開き、インポートされたパッケージの内容をこのパッケージに移入するには、これを選択します。新しいパッケージには、インポートされたパッケージと同じ名前が自動的に付けられます。

- 含めるネットワークマップを指定します (該当する場合)。構成パッケージが 構成エディタで既に開かれている場合は、[使用元ネットワークマップ:] ドロップダウンメニューを使用できます。



次のいずれかのオプションを選択します:

- [Current Package]—これで、パッケージに現在設定されているネットワークマップが Configuration Editor で利用可能になったままになり、インポートされたパッケージからネットワークマップはすべて

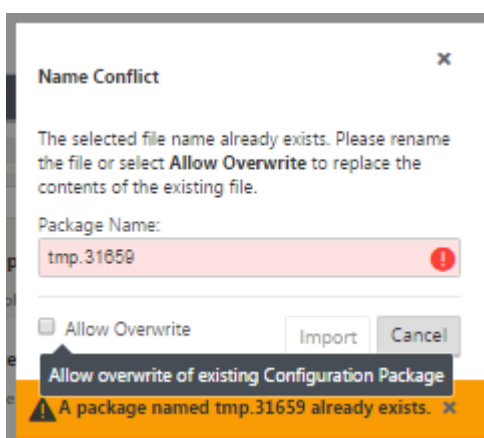
破棄されます。

- **[New Package]** —現在開いているパッケージに現在設定されているネットワークマップが、インポートされたパッケージのネットワークマップ (存在する場合) に置き換えられます。
- **Both Packages** —現在のパッケージ とインポートされたパッケージの両方からすべてのネットワークマップが含まれます。

6. **[インポート]** をクリックします。インポートされたファイルは、仕様に従って 構成エディタにロードされます。

注

Workspace に同じ名前のパッケージが存在する場合は、「名前の競合」(**Name Conflict**) ダイアログボックスが表示されます。



インポートしたパッケージに使用する名前を指定するには、次のいずれかの操作を行います。

- 「パッケージ名」(**Package Name**) フィールドに別の名前を入力して、新しいパッケージの名前を変更し、「インポート」(**Import**) ボタンを有効にします。インポートされたパッケージは、指定された名前で 構成エディタ にロードされます。パッケージ名は Workspace に保存されますが、パッケージを明示的に保存するまで、パッケージの内容はワークスペースに保存されます。
- **[Allow Overwrite]** を選択して、既存の名前を保持し、保存したパッケージの内容の上書きを有効にすることを確認します。ただし、変更されたパッケージを明示的に保存するまで、現在のパッケージの保存バージョンの内容は上書きされません。

これにより、[名前の競合] ダイアログボックスの [インポート] ボタンも有効になります。[インポート] をクリックして、インポート操作を完了します。

保存された構成パッケージをロードする

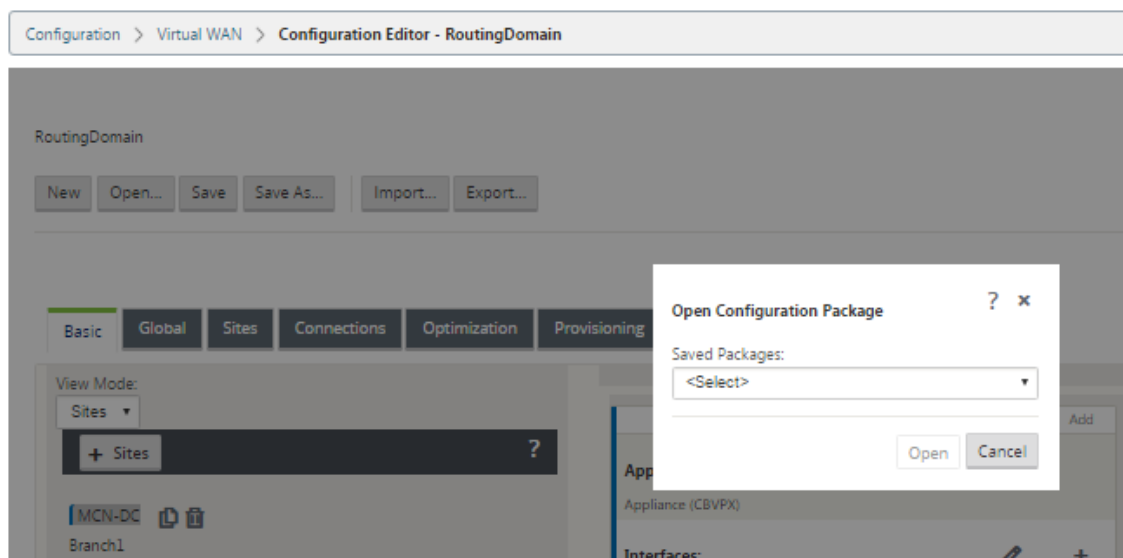
保存した構成パッケージの作業を再開するには、まずパッケージを開き、構成エディタにロードする必要があります。

保存した構成パッケージをロードするには、次の手順を実行します。

1. 管理 Web インターフェイスにログインし直して、構成エディタに移動します。これにより、新しいセッションの [構成エディター] のメインページが開きます。

管理 Web インターフェイスにログインし直した場合、構成エディタ は最初に新しいセッション用に開かれ、構成パッケージはロードされません。新しい構成を開始（新規）、保存された既存の構成を開く（開く）、またはインポート（インポート）してから、以前にローカル PC にバックアップした構成 を開く（開く）ことができます。

2. [開く] をクリックします。[構成パッケージを開く] ダイアログボックスが表示されます。



3. 「保存されたパッケージ」ドロップダウンメニューから開くパッケージ を選択します。

注

構成エディタを開いた場合、Workspace に保存した構成の数によっては、「保存済みパッケージ」(**Saved Packages**) メニューが表示されるまでに数秒または 1、2 分かかる場合があります。その場合は、暫定的に [保存済みパッケージ] メニューフィールドに [保存済みパッケージなし] というメッセージが表示されることがあります。このような場合は、[キャンセル] をクリックしてダイアログボックスを閉じ、しばらく待ってから、もう一度 [開く] をクリックしてダイアログボックスを再度開きます。

4. [開く] をクリックします。

注

これにより、指定した構成パッケージが開き、編集のために 構成エディタ にロードされます。これは、選択した構成をローカルアプライアンスにステージングしたりアクティブ化したりしません。

サイト名の変更

構成エディタで MCN サイトの名前を変更する場合は、サイトの名前を変更した設定を MCN および SD-WAN ネットワークに適用する必要があります。MCN の役割と、高可用性が有効か無効かによって、サイト名を変更するときの

SD-WAN ネットワーク設定には次のシナリオが適用されます。

- MCN
- 高可用性の MCN
- GEO
- 高可用性の GEO
- RCN
- 高可用性を備えた RCN

MCN サイトの名前変更

MCN の名前を変更した後、名前を変更したサイトで新しい設定をロードする必要があります。

名前を変更したサイトの新しい構成をアップロードするには、次の手順に従います。

1. MCN から、新しい構成でネットワークをステージングします。
2. 名前を変更した MCN のステージング構成パッケージをダウンロードします。
3. MCN の「ローカル変更管理」ページにナビゲートします。
 - a) 先にダウンロードしたパッケージをアップロードします。
 - b) 処理が完了したら、[次へ] をクリックします。
 - c) [アクティブ化] をクリックします。

注

ステップ 3 (c) が完了すると、変更管理プロセスによって、ネットワーク内のアプライアンス (ノード) 用のステージングされたソフトウェアが自動的にアクティブ化されます。

高可用性による MCN サイト名の変更

高可用性が有効になっている MCN の名前を変更したら、新しい設定をロードする必要があります。

1. MCN から、新しい構成でネットワークをステージします。
2. アクティブ MCN アプライアンスと高可用性 MCN アプライアンスのステージング構成パッケージを新しい名前でダウンロードします。
3. スタンバイ MCN アプライアンスでサービスを無効にします。
4. アクティブな MCN の [ローカル変更管理] ページにナビゲートします。
 - a) 先にダウンロードしたパッケージをアップロードします。
 - b) 処理が完了したら、[次へ] をクリックします。
 - c) [アクティブ化] をクリックします。
 - d) 高可用性が無効になっているスタンバイ MCN アプライアンスについて、ステップ i、ii、iii、iv を繰り返します。

- e) スタンバイ MCN アプライアンス上でサービスを有効にします。

注

ステップ 4 (c) が完了すると、変更管理プロセスによって、ネットワーク内のアプライアンスのステージングされたソフトウェアが自動的にアクティブ化されます。

GEO サイトの名前を変更する

名前を変更した GEO サイトの新しい構成をアップロードするには:

1. MCN から、名前が変更された GEO サイトを含む新しい構成を持つステージネットワーク。
2. MCN から、名前を変更した GEO サイトのステージング構成パッケージをダウンロードします。
3. **MCN** で、[ネットワーク用に ステージングされたアクティブ化] を選択します。これにより、名前を変更したサイトが無効になり、サイトが使用できなくなります。
4. GEO サイトの「ローカル変更管理」ページにナビゲートします。
 - a) 先にダウンロードしたパッケージをアップロードします。
 - b) パッケージの処理が完了したら、[次へ] をクリックします。
 - c) [アクティブ化] をクリックします。

高可用性で **GEO** サイトの名前を変更する

名前を変更した GEO サイトを高可用性で有効にした新しい設定をアップロードするには、次の手順を実行します。

1. MCN から、名前が変更された GEO サイトを含む新しい構成を持つステージネットワーク。
2. MCN から、名前が変更された GEO サイトを持つアクティブアプライアンスと高可用性アプライアンスの両方のステージング構成パッケージをダウンロードします。
3. **MCN** で、ネットワークの [ステージングの有効化] を選択します。これにより、名前を変更したサイトが無効になり、サイトが使用できなくなります。
4. アクティブな GEO アプライアンスに移動します。
 - a) 「ローカル変更管理」ページに移動します。
 - b) 先にダウンロードしたパッケージをアップロードします。
 - c) パッケージの処理が完了したら、[次へ] をクリックします。
 - d) [アクティブ化] をクリックします。
 - e) スタンバイアプライアンスに対して、手順 a、b、c、d を繰り返します。

RCN サイトの名前変更

RCN サイトの名前を変更して新しい設定をアップロードするには、次の手順に従います。

1. MCN から、名前が変更された RCN サイトを含む新しい構成を持つステージネットワーク。
2. MCN から、名前を変更した RCN サイトのステージングパッケージをダウンロードします。
3. **MCN** で、[ネットワーク用に ステージングされたアクティブ化] を選択します。これにより、名前が変更された RCN サイトが無効になり、MCN でリージョンサイトが使用できなくなります。リージョンの RCN サイトとブランチは相互に通信しますが、ステップ 4 が完了するまで、リージョンは MCN と通信できません (名前が変更されていない GEO RCN が無い限り)。
4. RCN の「ローカル変更管理」ページにナビゲートします。
 - a) 先にダウンロードしたパッケージをアップロードします。
 - b) パッケージ処理が完了したら、[次へ] をクリックします。
 - c) [アクティブ化] をクリックします。

注

リージョンのステージングは、ステップ 4 (c) が完了するまで行われなため、リージョンのブランチが使用可能になるまでに時間がかかります。RCN の変更管理プロセスは、リージョンのステージングを管理します。

高可用性による RCN サイト名の変更

名前を変更した RCN サイトを高可用性で有効にした新しい設定をアップロードします。

1. MCN から、名前が変更された RCN サイトを含む新しい構成を持つステージネットワーク。
2. MCN から、RCN サイトの名前を変更したアクティブアプライアンスと高可用性アプライアンスの両方のステージングパッケージをダウンロードします。これにより、名前が変更された RCN サイトが無効になり、MCN でリージョンサイトが使用できなくなります。リージョンの RCN サイトとブランチは相互に通信しますが、ステップ 4 が完了するまで、リージョンは MCN と通信できません (名前が変更されていない GEO RCN が無い限り)。
3. **MCN** で、ネットワークの [ステージをアクティブ化] を選択します。
4. スタンバイ RCN アプライアンスでサービスを無効にします。
5. アクティブな RCN の「ローカル変更管理」ページにナビゲートします。
 - a) 先にダウンロードしたパッケージをアップロードします。
 - b) パッケージの処理が完了したら、[次へ] をクリックします。
 - c) [アクティブ化] をクリックします。
 - d) 無効になっているスタンバイ RCN アプライアンスに対して、手順 a、b、c を繰り返します。

6. スタンバイ RCN アプライアンスでサービスを有効にします。

GEO RCN サイトの名前を変更する

名前が変更された GEO RCN サイトを使用して新しい設定をアップロードするには:

1. MCN から、名前を変更した GEO RCN サイトを持つ新しい構成を持つステージネットワーク。
2. MCN から、名前を変更した GEO RCN サイトのステージングパッケージをダウンロードします。
3. **MCN** で、[ネットワーク用に ステージングされたアクティブ化] を選択します。これにより、名前を変更したサイトが無効になり、サイトが使用できなくなります。プライマリ RCN がオンラインの場合、GEO RCN サイトの名前を変更しても、リージョンはネットワークに接続されたままになります。
4. GEO RCN の「ローカル変更管理」ページにナビゲートします。
 - a) 先にダウンロードしたパッケージをアップロードします。
 - b) パッケージの処理が完了したら、[次へ] をクリックします。
 - c) [アクティブ化] をクリックします。

GEO RCN サイトを高可用性で名前変更する

1. MCN から、名前を変更した GEO RCN サイトを持つ新しい構成を持つステージネットワーク。
2. MCN から、名前が変更された GEO RCN サイトのアクティブアプライアンスと高可用性アプライアンスの両方のステージングパッケージをダウンロードします。
3. **MCN** で、[ネットワーク用に ステージングされたアクティブ化] を選択します。これにより、名前を変更したサイトが無効になり、サイトが使用できなくなります。プライマリ RCN がオンラインの場合、GEO RCN サイトの名前を変更しても、リージョンはネットワークに接続されたままになります。
4. アクティブな GEO RCN の「ローカル変更管理」ページにナビゲートします。
 - a) 先にダウンロードしたパッケージをアップロードします。
 - b) パッケージの処理が完了したら、[次へ] をクリックします。
 - c) [アクティブ化] をクリックします。
 - d) スタンバイアプライアンスに対して手順 a、b and c を繰り返します。

ブランチノードのセットアップ

May 10, 2021

この章では、ブランチサイトを追加および構成する手順について説明します。ブランチサイトを追加する手順は、MCN サイトを作成および設定する場合とよく似ています。ただし、構成手順と設定の一部は、ブランチサイトでは若干異なります。さらに、最初のブランチサイトを追加したら、同じアプライアンスモデルを持つサイトについては、クローン（複製）機能を使用して、これらのサイトを追加および構成するプロセスを合理化できます。

ブランチサイトをセットアップするために MCN サイトを作成する場合と同様に、MCN アプライアンスの管理 Web インターフェイスで **Configuration Editor** を使用する必要があります。構成エディタは、インターフェイスが **MCN** コンソール モードに設定されている場合にのみ使用できます。

補足的なブランチサイトの展開情報

このガイドに加えて、以下の Knowledge Base サポート記事も推奨されます。

- 仮想 WAN PBR モードの展開手順 ([CTX201577](http://support.citrix.com/article/CTX201577))
<http://support.citrix.com/article/CTX201577>
- 仮想 WAN ゲートウェイモードの展開手順 ([CTX201576](http://support.citrix.com/article/CTX201576))
<http://support.citrix.com/article/CTX201576>

ブランチサイト構成手順の概要

このプロセスを完了するための手順は次のとおりです。

1. ブランチサイトを追加します。
2. ブランチサイトの仮想インターフェイスグループを設定します。
3. ブランチサイトの仮想 IP アドレスを構成します。
4. (任意) ブランチサイトの LAN GRE トンネルを設定します。
5. ブランチサイトの WAN リンクを構成します。
6. ブランチサイトのルートを設定します。
7. (オプション) ブランチサイトの高可用性を設定します。
8. (オプション) 新しいブランチサイトのクローンを作成し、追加のサイトを作成および構成します。

注

サイトのクローン作成は任意です。仮想 WAN アプライアンスモデルは、オリジナルサイトとクローンサイトの両方で同じである必要があります。クローンの指定されたアプライアンスモデルを変更することはできません。アプライアンスモデルがサイトで異なる場合は、サイトを手動で追加する必要があります。

9. 構成監査アラートを解決します。

10. 完了した設定を保存します。

ブランチノードの構成

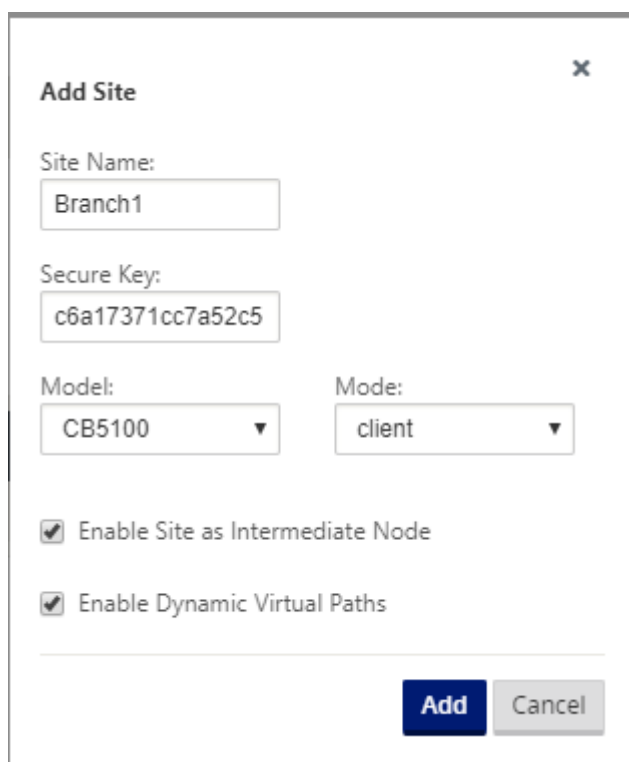
May 10, 2021

新しいブランチサイトを [Sites] テーブルに追加し、サイトの構成を開始するには、次の手順を実行します。

注

新しい構成パッケージを作成して保存した後で MCN からログアウトした場合、続行する前に、再度ログインして設定を再度開く必要があります。これを行うには、構成エディターの メニューバー (ページ上部) の「開く」をクリックします。これにより、変更する構成を選択するためのダイアログボックスが表示されます。

1. 構成エディタで続行し、サイト バーの [追加] をクリックして、新しいブランチサイトの追加と構成を開始します。[サイトの追加] ダイアログボックスが表示されます。



2. 次のサイト情報を入力します。

注

エントリにはスペースを含めることはできません。また、Linux 形式である必要があります。

- 「サイト名」— サイトの名前を入力します。
- アプライアンス名— アプライアンスに割り当てる名前を入力します。

- セキュアキー—これは、SD-WAN アプライアンスの暗号化とメンバーシップの検証に使用される 8 ～ 32 桁の 16 進キーです。デフォルトでは、このフィールドには自動的に生成されたセキュリティキーがあらかじめ入力されています。デフォルトをそのまま使用するか、カスタムキーの 16 進形式を入力します。
 - モデル：ドロップダウンメニューからアプライアンス・モデルを選択します。
 - モード：モードとしてクライアントを選択します。
3. [追加] をクリックしてサイトを追加します。新しいサイトが [サイト] ツリーに追加され、サイトの [基本設定] 構成フォームが開きます。

The screenshot displays the 'Basic Settings' configuration form for a new site. On the left, a 'View Site:' dropdown menu is set to 'Branch', and a 'Sites' sidebar lists various configuration options: Basic Settings (selected), Routing Domains, Interface Groups, Virtual IP Addresses, VRRP, DHCP, WAN Links, Certificates, and High Availability. The main form contains the following fields and controls:

- Site Name:** A text field containing 'Branch'.
- Appliance Name:** A text field containing 'Branch-CB1000'.
- Secure Key:** A text field containing '005a85b2611f305c', with a 'Regenerate' button to its right.
- Model:** A dropdown menu set to 'CB1000'.
- Mode:** A dropdown menu set to 'client'.
- Site Location:** A text field containing 'SC'.
- Default Direct Route Cost:** A text field containing '5'.
- Gateway ARP Timer (ms):** A text field containing '1000'.
- Enable Source MAC Learning:** An unchecked checkbox.
- Buttons:** 'Apply' and 'Close' buttons at the bottom.

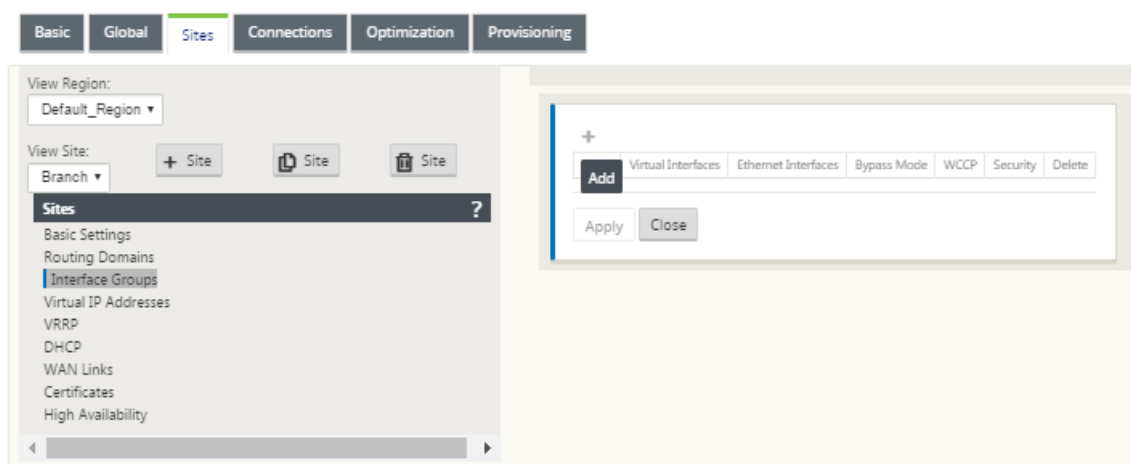
4. サイトの基本設定を入力し、[適用] をクリックします。

次のステップでは、新しいブランチサイトのインターフェイスグループを追加および設定します。

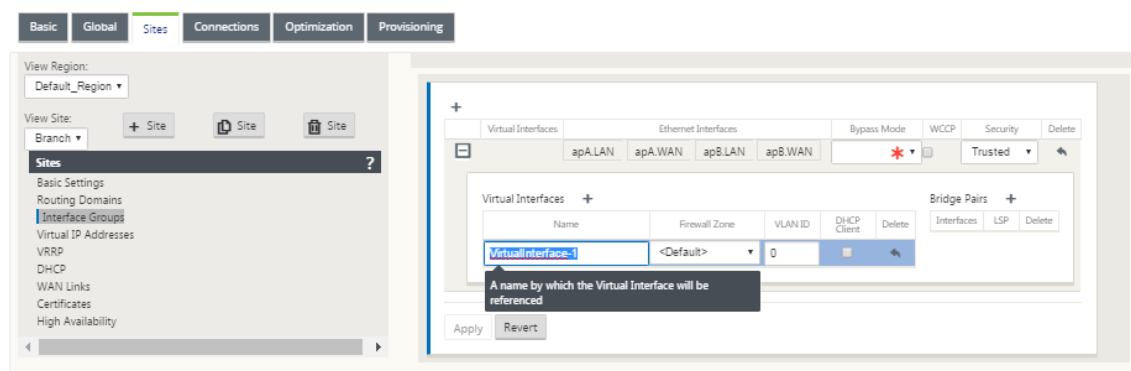
ブランチのインターフェイスグループの設定方法

インターフェイスグループを新しいブランチサイトに追加するには、次の手順を実行します。

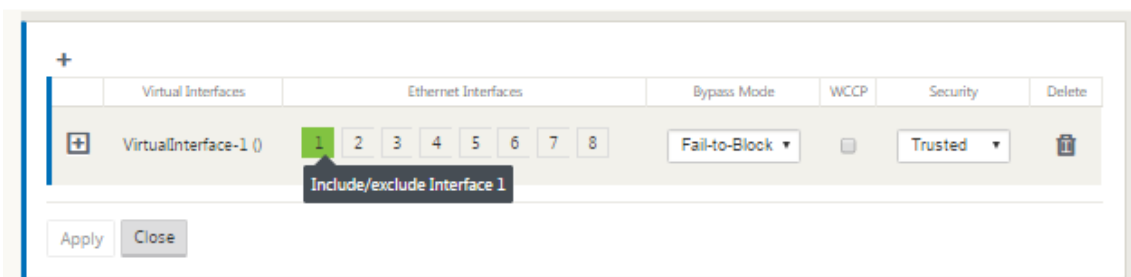
1. 構成エディタの [サイト] ビューで、[サイト] ドロップダウンメニューからブランチサイトを選択します。これにより、選択したサイトの構成ビューが開きます。



2. [+] をクリックして、仮想インターフェイスグループを追加します。新しい空の Virtual インターフェイスグループエントリがテーブルに追加され、編集用に開きます。
3. [仮想インターフェイス] の右側にある [+] をクリックします。新しい空のグループエントリがテーブルに追加され、編集のために開きます。



4. グループに含める イーサネットインターフェイスを 選択します。
[**Ethernet Interfaces**] で、そのインターフェイスを含める/除外するインターフェイスをクリックします。グループに含めるインターフェイスはいくつでも選択できます。



5. ドロップダウンメニューから [バイパスモード] を選択します（デフォルトなし）。

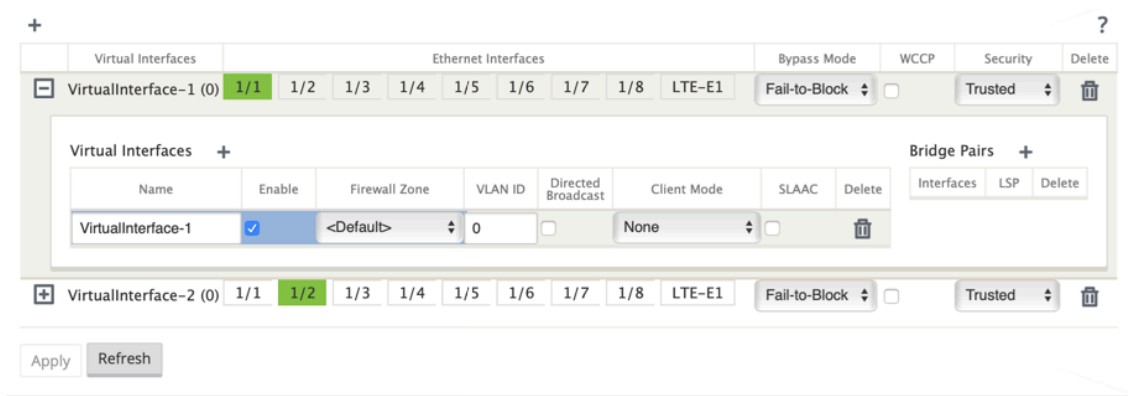
バイパスモード は、アプライアンスまたはサービスの障害または再起動が発生した場合に、仮想インターフェイスグループ内のブリッジペアインターフェイスの動作を指定します。オプションは、[配線失敗] または [ブ

ロック失敗] です。

6. ドロップダウンメニューから [セキュリティレベル] を選択します。

仮想インターフェイスグループのネットワークセグメントのセキュリティレベルを指定します。オプションは、[信頼済み] または [信頼できない] です。信頼できるセグメントはファイアウォールで保護されます（デフォルトは Trusted です）。

7. 追加した仮想インターフェイスの左端にある [+] をクリックします。[仮想インターフェイス] テーブルが表示されます。



8. [仮想インターフェイス] の右側にある [+] をクリックします。名前、ファイアウォールゾーン、**VLAN ID** ID が表示されます。

9. この仮想インターフェイスグループの名前と **VLAN ID** を入力します。

- **[Name]**: この仮想インターフェイスが参照される名前。
- **[Enable]**: デフォルトでは、すべての仮想インターフェイスに対して **[Enable]** チェックボックスがオンになっています。仮想インターフェイスを無効にする場合は、**[Enable]** チェックボックスをオフにします。

注

- 仮想インターフェイスを無効にするオプションは、WAN リンクアクセスインターフェイスで使用されていない場合にのみ使用できます。仮想インターフェイスが WAN リンクアクセスインターフェイスで使用されている場合、チェックボックスは読み取り専用で、デフォルトでオンになっています。
- 有効になっている仮想インターフェイスとともに、他の機能を設定する際に、**[WAN リンクのアクセスインターフェイス]** の下を除き、無効化された仮想インターフェイスも表示されます。無効にした仮想インターフェイスを選択した場合でも、仮想インターフェイスは考慮されず、ネットワーク設定には影響しません。

- ファイアウォールゾーン - ドロップダウンメニューからファイアウォールゾーンを選択します。
- **VLAN ID**: 仮想インターフェイスとの間で送受信されるトラフィックを識別およびマーキングするための ID。ネイティブ/タグなしトラフィックには、0（ゼロ）の ID を使用します。

10. [ブリッジペア] の右側にある [+] をクリックします。新しい **Bridge Pairs** エントリが追加され、編集用に開きます。
11. ペアリングするイーサネットインターフェイスをドロップダウンメニューから選択します。さらにペアを追加するには、[ブリッジペア] の横にある [+] をもう一度クリックします。
12. [適用] をクリックします。設定が適用され、テーブルの新しい仮想インターフェイスグループに追加されます。

注

この段階では、新しい仮想インターフェイスグループエントリの右側に、黄色の Delta Audit Alert アイコンが表示されます。これは、サイトの仮想 IP アドレス (VIP) をまだ構成していないためです。現時点では、このアラートは、サイトの仮想 IP を正しく構成すると自動的に解決されるため、無視できます。

13. さらに仮想インターフェイスグループを追加するには、[インターフェイスグループ] ブランチの右側にある [+] をクリックし、上記の手順を実行します。

ブランチサイトの仮想 IP アドレスを構成する方法

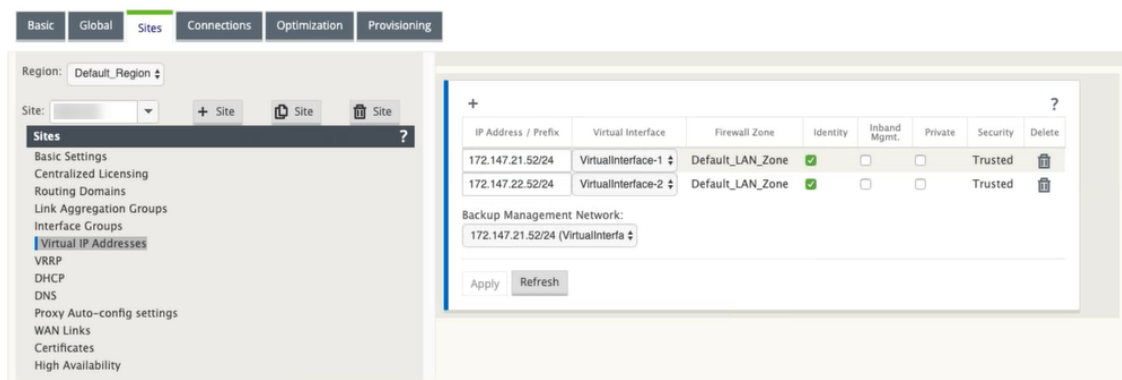
次の手順では、サイトの仮想 IP アドレスを構成し、適切なグループに割り当てます。

1. 新しいブランチサイトの [サイト] ビューで、[仮想 IP アドレス] の左にある [+] をクリックします。これにより、新しいサイトの仮想 IP アドレス テーブルが表示されます。
2. [仮想 IP アドレス] の右側にある [+] をクリックして、アドレスを追加します。新しい仮想 IP アドレスを追加および設定するためのフォームが表示されます。
3. IP アドレス / プレフィックス 情報を入力し、アドレスが関連付けられている仮想インターフェイスを選択します。仮想 IP アドレスには、完全なホストアドレスとネットマスクを含める必要があります。
4. [ファイアウォールゾーン]、[ID]、[プライベート]、[セキュリティ] など、仮想 IP アドレスの設定を選択します。
5. [Inband Mgmt] を選択すると、仮想 IP アドレスが Web UI や SSH などの管理サービスに接続できるようになります。

注:

インターフェイスは、セキュリティタイプが **Trusted** で **Identity** を有効にする必要があります。

6. バックアップ管理ネットワークとして仮想 IP を選択します。これにより、管理ポートにデフォルト Gateway が設定されていない場合に、管理に仮想 IP アドレスを使用できます。

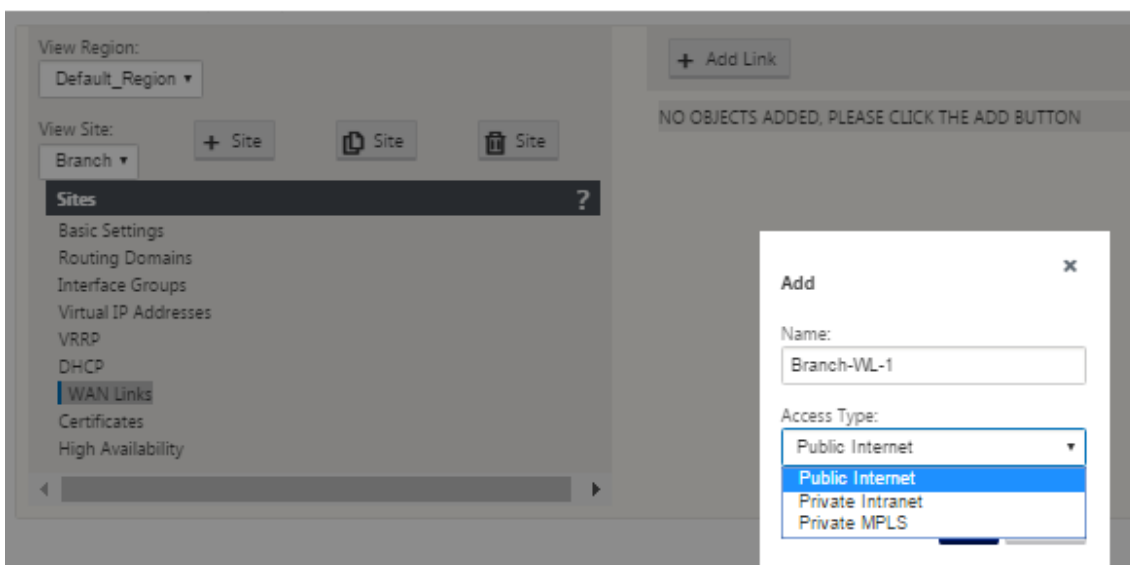


7. [適用] をクリックします。サイトへのアドレス情報が追加され、サイトの 仮想 **IP** アドレス テーブルに含まれます。
8. さらに仮想 IP アドレスを追加するには、[仮想 **IP** アドレス] の右側にある [+] をクリックし、上記の手順を実行します。

ブランチの **WAN** リンクを構成する方法

次のステップでは、サイトの WAN リンクを構成します。

1. 新しいブランチ サイト の [サイト] ビューで、[**WAN** リンク] ラベルをクリックします。
2. [**WAN** リンク] の右側にある [Add Link] をクリックして、新しい WAN リンクを追加します。[追加] ダイアログボックスが表示されます。



3. (オプション) デフォルトを使用しない場合は、WAN リンクの名前を入力します。

デフォルトはサイト名で、次のサフィックスを付加します。

-WL-<number>

ここで <number>、はこのサイトの WAN リンクの数 を 1 ずつ増やします。

4. ドロップダウンメニューから「アクセスタイプ」を選択します。

オプションは、[パブリックインターネット]、[プライベートイントラネット]、または [プライベート マルチプロトコルラベルスイッチング] です。

5. [追加] をクリックします。[**WAN** リンク の基本設定] 設定ページが表示され、新しい未設定の WAN リンクがページに追加されます。

6. 新しい WAN リンクのリンクの詳細を入力します。LAN から WAN、WAN から **LAN** への設定を構成します。

いくつかのガイドラインは次のとおりです。

- 一部のインターネットリンクは非対称である場合があります。許可された速度を誤って設定すると、そのリンクのパフォーマンスに悪影響を及ぼす可能性があります。
- 認定レートを超えるバースト速度は使用しないでください。
- インターネット WAN リンクの場合は、必ずパブリック IP アドレスを追加してください。

7. グレーの [詳細設定] セクションバーをクリックします。リンクの [詳細設定] フォームが開きます。

8. リンクの【詳細設定】を入力します。

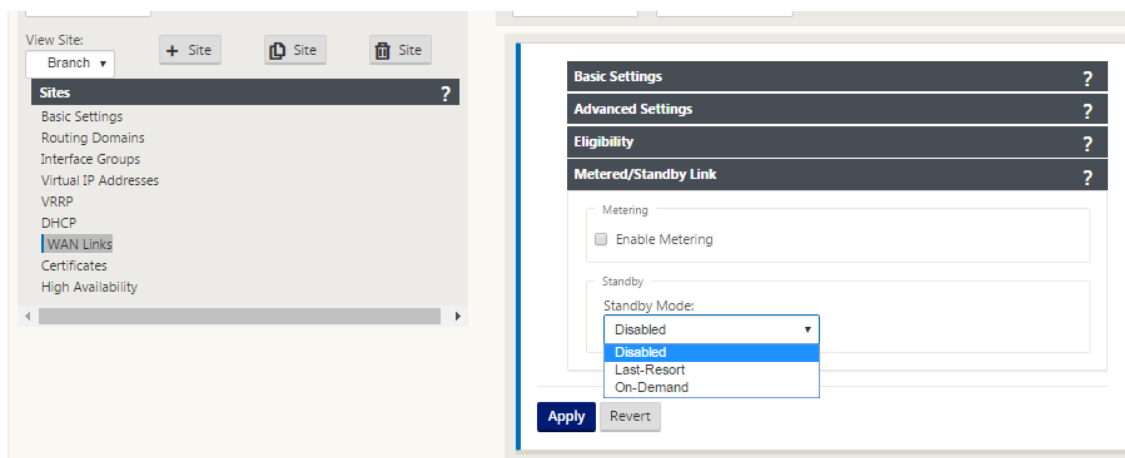
- **[Provider ID]**: (オプション) 一意の ID 番号 1~100 を入力し、同じサービスプロバイダーに接続されている WAN リンクを指定します。仮想 WAN は、重複パケットを送信するときにプロバイダー ID を使用してパスを区別します。
- **フレームコスト (バイト)**: 各パケットに追加するヘッダー/トレーラーのサイズ (バイト単位) を入力します。たとえば、追加されたイーサネット IPG または AAL5 トレーラーのバイト単位のサイズ。
- **輻輳しきい値**: 輻輳しきい値 (マイクロ秒) を入力します。このしきい値は、WAN リンクがパケット転送を抑制し、それ以上の輻輳を回避します。
- **[MTU Size (bytes)]**: フレームコストを含まない、最大の raw パケットサイズ (バイト単位) を入力します。

9. グレーの「適格」セクション・バーをクリックします。リンクの【適格 設定】フォームが開きます。

10. リンクの「適格」設定を選択します。

11. グレーの【従量制課金リンク】セクションバーをクリックします。リンクの【従量制課金リンク 設定】フォームが開きます。

12. (オプション) このリンクのメータリングを有効にするには、[メータリングを有効にする]を選択します。これにより、[メータリング設定を有効にする]フィールドが表示されます。



The screenshot shows the Citrix SD-WAN configuration interface. On the left, the 'View Site:' menu is open, showing 'WAN Links' selected. On the right, the 'Metered/Standby Link' settings panel is displayed. The 'Basic Settings' tab is active, showing the 'Enable Metering' checkbox checked. The 'Standby Mode' dropdown menu is open, showing 'Disabled' selected. The 'Apply' button is visible at the bottom of the panel.

Metering

☒ Enable Metering ☒ Disable if Data Cap reached

Data Cap (MB): Billing Cycle: Starting From:

Standby

Standby Mode:

Heartbeat Interval

Caution: It takes at least 4 times the heartbeat interval to detect connectivity failure.

Active Heartbeat Interval:

13. リンクのメータリング設定を構成します。次のように入力します：

- 「データ上限 **(MB)**」—リンクに対するデータ上限割り当てを MB 単位で入力します。
- [請求サイクル]—ドロップダウンメニューから [毎月] または [毎週] を選択します。
- [開始日]—請求サイクルの開始日を入力します。
- [最後のレポートを設定]：他のすべての利用可能なリンクに障害が発生した場合に、このリンクをラストリゾートリンクとして有効にするには、このオプションを選択します。通常の WAN 条件下では、仮想 WAN は、リンクステータスを確認するために、従量制課金リンクを介して最小限のトラフィックだけを送信します。ただし、障害が発生した場合、SD-WAN は本番トラフィックを転送するための最後の手段として、アクティブな従量制課金リンクを使用できます。

14. [適用] をクリックします。これにより、指定した設定が新しい WAN リンクに適用されます。

次のステップでは、新しい WAN リンクのアクセスインターフェイスを設定します。アクセスインターフェイス

スは、特定の WAN リンクのインターフェイスとしてまとめて定義された、仮想インターフェイス、WAN エンドポイント IP アドレス、ゲートウェイ IP アドレス、および仮想パスモードで構成されます。各 WAN リンクには、少なくとも 1 つのアクセスインターフェイスが必要です。

注

リモート帯域幅を考慮して共有を自動プロビジョニングするオプションが追加され、WAN リンクが設定されます。[リモート帯域幅を使用して Provisioning を設定] オプションを使用すると、大規模なネットワークと多様な帯域幅構成を持つユーザーは、データセンターサイトの帯域幅プロビジョニングを動的に管理できます。

15. リンクの [WAN リンク] 設定ページで [アクセスインターフェイス] を選択します。これにより、サイトの [アクセスインターフェイス] ビューが開きます。

The screenshot shows the 'WAN Link' configuration page. The 'WAN Link' dropdown is set to 'Branch-WL-1'. The 'Section' dropdown is open, showing 'Settings' and 'Access Interfaces' (highlighted in blue). There are '+ Add Link' and 'Delete Link' buttons. Below the dropdowns, there is a table with columns: Routing Domain, Virtual Interface, IP Address, Gateway IP Address, Virtual Path Mode, Proxy ARP, Internet Access for All Routing Domains, and Delete. An 'Add' button is next to the table. At the bottom, there are 'Apply' and 'Close' buttons.

16. [+] をクリックして、インターフェイスを追加します。テーブルに空白のエントリが追加され、編集のために開きます。リンクの [アクセスインターフェイス] 設定を入力します。

注

各 WAN リンクには、少なくとも 1 つのアクセスインターフェイスが必要です。

The screenshot shows the 'WAN Link' configuration page. The 'WAN Link' dropdown is set to 'Branch-WL-1'. The 'Section' dropdown is set to 'Access Interfaces'. There are '+ Add Link' and 'Delete Link' buttons. Below the dropdowns, there is a table with columns: Name, Virtual Interface, IP Address, Gateway IP Address, Virtual Path Mode, Proxy ARP, Internet Access for All Routing Domains, and Delete. The table contains one entry: 'Branch-WL-1' (Name), 'VirtualInterface-1' (Virtual Interface), '172.10.10.1' (IP Address), '172.10.10.2' (Gateway IP Address), 'Primary' (Virtual Path Mode), and checkboxes for 'Proxy ARP' and 'Internet Access for All Routing Domains'. At the bottom, there are 'Apply' and 'Close' buttons.

17. 次のように入力します：

- 名前: これは、このアクセスインターフェイスが参照される名前です。新しいアクセスインターフェイスの名前を入力するか、デフォルトをそのまま使用します。デフォルトでは、次の命名規則が使用されます。

WAN_link_name-AI-number

WAN_LINK_name は、このインターフェイスに関連付ける WAN リンクの名前です。数字は、このリンクに現在設定されているアクセスインターフェイスの数で、1 ずつ増加します。

注

名前が切り捨てられた場合は、フィールドにカーソルを置き、クリックしたままマウスを右または左に回転すると、切り捨てられた部分が表示されます。

- 仮想インターフェイス—このアクセスインターフェイスが使用する仮想インターフェイス。このブランチサイト用に構成された Virtual Interfaces のドロップダウンメニューからエントリを選択します。
- IP アドレス—アプライアンスから WAN へのアクセスインターフェイスエンドポイントの IP アドレス。
- Gateway IP アドレス—ゲートウェイルータの IP アドレスです。
- 仮想パスモード: この WAN リンク上の仮想パストラフィックのプライオリティ。オプションは、[プライマリ]、[セカンダリ]、または [除外] です。[除外] に設定すると、このアクセスインターフェイスはインターネットおよびイントラネットトラフィックにのみ使用されます。
- [Proxy ARP]: 有効にするチェックボックスをオンにします。有効にすると、Gateway に到達できない場合に、仮想 WAN アプライアンスはゲートウェイ IP アドレスの ARP 要求に応答します。

18. [適用] をクリックします。

これで、新しい WAN リンクの設定が完了しました。この手順を繰り返して、サイトに追加の WAN リンクを追加および構成します。

次のステップでは、サイトのルートを追加および構成します。

ブランチのルートを構成する方法

サイトのルートを追加および構成するには、次の手順を実行します。

- 新しいブランチサイトの [接続] ビューをクリックし、[ルート] を選択します。これにより、サイトの [ルート] ビューが表示されます。
- ルートを追加するには、[ルート] の右側にある [+] をクリックします。これにより、編集用の [ルート] ダイアログボックスが開きます。

Add

Network IP Address * Cost Service Type Gateway IP Address *

☒ Export Route

☐ Summary Route

☐ Eligibility Based On Path

Path:

☐ Eligibility Based On Gateway

3. 新しいルートのルート設定情報を入力します。

- 「ネットワーク **IP** アドレス」—ネットワーク IP アドレスを入力します。
- **Cost**: このルートのルートプライオリティを決定するために、1～15 の重みを入力します。低コストのルートは、高コストのルートよりも優先されます。デフォルト値は 5 です。
- **[Service Type]**—このフィールドのドロップダウンメニューからルートのサービスタイプを選択します。使用できるオプションは、次のとおりです。
 - 仮想パス—このサービスは、仮想パスを通過するトラフィックを管理します。仮想パスは、2 つの WAN リンク間の論理リンクです。これは、2 つの SD-WAN ノード間で高いサービス・レベル通信を提供するために結合された WAN パスの集合で構成されます。これは、変化するアプリケーション需要と WAN 条件を常に測定し、適応させることによって行われます。SD-WAN アプライアンスは、パス単位でネットワークを測定します。仮想パスは、スタティック（常に存在）またはダイナミック（2 つの SD-WAN アプライアンス間のトラフィックが設定されたしきい値に達した場合のみ存在）のいずれかになります。
 - インターネット—このサービスは、エンタープライズサイトとパブリックインターネット上のサイト間のトラフィックを管理します。このタイプのトラフィックはカプセル化されません。輻輳時には、SD-WAN は、仮想パスに対するレート制限によるインターネットトラフィックと、管理者が確立した SD-WAN 構成に従ってイントラネットトラフィックによって、帯域幅を積極的に管理します。
 - イントラネット—このサービスは、仮想パス経由の送信用に定義されていないエンタープライズイントラネットトラフィックを管理します。インターネットトラフィックと同様に、カプセル化されていないままであり、SD-WAN は、輻輳時にこのトラフィックを他のサービスタイプと比較してレート制限することで、帯域幅を管理します。特定の条件下では、仮想パス上のイントラネットフォールバック用に構成されている場合、通常は仮想パスとともに移動するトラフィックは、代わり

にイントラネットトラフィックとして扱われ、ネットワークの信頼性を維持できます。

- **パススルー**—このサービスは、仮想 WAN を通過するトラフィックを管理します。パススルーサービスに送信されるトラフィックには、ブロードキャスト、ARP、その他の非 IPv4 トラフィック、および Virtual WAN アプライアンスのローカルサブネット、構成済みサブネット、またはネットワーク管理者が適用したルール上のトラフィックが含まれます。このトラフィックは、SD-WAN によって遅延、シェーピング、または変更されません。したがって、SD-WAN アプライアンスが他のサービスで使用するように構成されている WAN リンク上で、パススルートラフィックが実質的なリソースを消費しないようにする必要があります。
 - **ローカル**：このサービスは、他のサービスと一致しないサイトへのローカルな IP トラフィックを管理します。SD-WAN は、ローカルルートを送信元および宛先とするトラフィックを無視します。
 - **GRE トンネル**：このサービスは、GRE トンネル宛の IP トラフィックを管理し、サイトで設定された LAN GRE トンネルと一致します。GRE トンネル機能を使用すると、LAN 上の GRE トンネルを終了するように SD-WAN アプライアンスを設定できます。サービスタイプ GRE Tunnel のルートの場合、Gateway はローカル GRE トンネルのトンネルサブネットの 1 つに存在する必要があります。
 - **LAN IPsec トンネル**—このサービスは、IPsec トンネル宛の IP トラフィックを管理します。
 - **インタールーティング** -このサービスは、サイト内のルーティングドメイン間または異なるサイト間のルートリークを可能にします。これにより、エッジルータがルートリークを処理する必要がなくなります。
- 「ゲートウェイ **IP** アドレス」—このルートのゲートウェイ IP アドレスを入力します。
 - [パスに基づく適格性] (チェックボックス)：(オプション) 有効の場合、選択したパスがダウンしているときにルートはトラフィックを受信しません。
 - 「パス」 (Path) —ルートの適格性を判断するために使用するパスを指定します。

4. [適用] をクリックします。

注

[適用] をクリックすると、追加のアクションが必要であることを示す監査警告が表示されることがあります。赤い点または金色のデルタアイコンは、表示されるセクションにエラーを示します。これらの警告を使用して、エラーや不足している構成情報を識別できます。監査警告アイコンの上にカーソルを置くと、そのセクションのエラーの簡単な説明が表示されます。暗いグレーの 監査 ステータスバー (ページ下部) をクリックして、すべての監査警告の一覧を表示することもできます。

Order	Network IP Address	Cost	Service Type	Service Name	Gateway IP Address	Info	Edit	Delete
1	0.0.0.0/0	5	Virtual Path	Branch1		ⓘ	✎	🗑
2	172.147.21.52/24	5	Local			ⓘ	✎	🗑
3	172.147.22.52/24	5	Local			ⓘ	✎	🗑
4	0.0.0.0/0	65535	Passthrough			ⓘ	✎	🗑

Navigation: ⏪ ⏩ 1 ⏪ ⏩

Buttons: Apply Close

以下に示すように、設定済みのルートを編集することもできます。

Edit ? x

Network IP Address: 172.147.61.0/24 Cost: 5 Service Type: Intranet Gateway IP Address:

☐ Export Route

Intranet Service: Intranet

☒ Eligibility Based On Path

Path: Branch1-WL-2->MCN-DC-WL-1

☐ Eligibility Based On Tunnel

Apply Cancel

これで、クライアントサイトの構成に必要な手順が完了しました。また、展開の次のフェーズに進む前に、完了するように選択できる、追加のオプションの手順もいくつかあります。これらの手順のリストと手順へのリンクを以下に示します。これらの機能を今すぐ設定したくない場合は、直接 [MCN での SD-WAN アプライアンスパッケージの準備] に進みます。(/en-us/citrix-sd-wan/current-release/configuration/installing-virtual-wan-appliance-packages-clients.html)

オプションの手順は次のとおりです。

- 高可用性の構成—高可用性は、1 つのサイトの 2 つの Virtual WAN アプライアンスが冗長性のためにアクティブ/スタンバイパートナーシップ容量でサービスを提供する構成です。このサイトに高可用性を実装していない場合は、この手順を省略できます。手順については、[ブランチサイトの高可用性（高可用性）の設

定（オプション）。]を参照してください。(/en-us/citrix-sd-wan/current-release/configuration/setup-branch-nodes/ha-for-a-branch-node.html)

- 新しいブランチサイトのクローン—構成したブランチサイトのクローンを作成し、別のサイトを追加するためのテンプレートとして使用することもできます。元のサイトとクローンのアプライアンスモデルは、同じである必要があります。手順については、「[ブランチ・サイトのクローン作成（オプション）](#)」を参照してください。
- **WAN Optimization** の構成—Citrix SD-WAN 仮想 WAN ライセンスに **WAN Optimization** 機能が含まれている場合は、これらの機能を有効にして構成に追加できます。これを行うには、構成エディタの「最適化」セクションを完了し、変更した構成を保存する必要があります。

構成の保存

次のステップでは、完了した サイト 構成を保存します。構成は、ローカルアプライアンスの Workspace に保存されます。

警告

コンソールセッションがタイムアウトになったり、構成を保存する前に管理 Web Interface からログアウトした場合、保存されていない構成の変更はすべて失われます。その後、システムに再度ログインし、設定手順を最初から繰り返す必要があります。そのため、構成パッケージを頻繁に保存するか、構成内の重要なポイントに保存することをお勧めします。

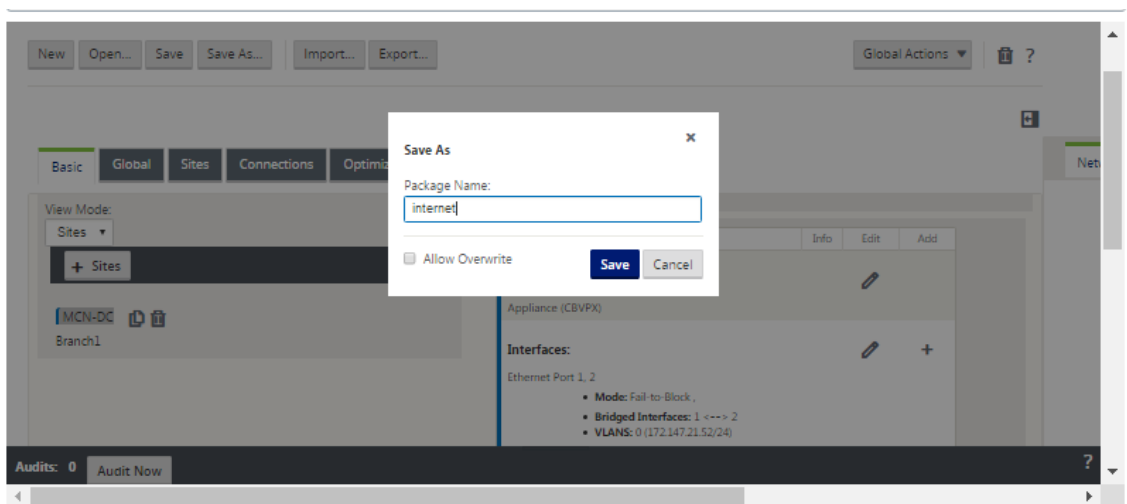
注

余分な予防策として、間違った構成パッケージを上書きしないように、[保存]ではなく[名前を付けて保存]を使用することをお勧めします。

構成ファイルを保存した後、管理 Web Interface からログアウトし、後で構成プロセスを続行するオプションがあります。ただし、ログアウトした場合は、再開時に保存した設定を再度開く必要があります。手順については、「**MCN** の設定」のセクションを参照してください。[保存した構成パッケージの構成エディタへのロード](#)。

現在の構成パッケージを保存するには、次の手順を実行します。

1. [名前を付けて保存] をクリックします（[構成エディタ]の中央ペインの上部にある）。[名前を付けて保存] ダイアログボックスが表示されます。



2. 構成パッケージ名を入力します。[保存] をクリックします。

注

構成を既存の構成パッケージに保存する場合は、保存する前に [上書きを許可] を選択してください。

次の手順では、MCN とクライアントサイト間の仮想パスと仮想パスサービスを構成します。手順については、[MCN サイトとクライアントサイト間の仮想パスサービスの設定](#)を参照してください。

ブランチサイトの名前変更

ブランチサイトの名前を変更したら、新しい構成パッケージをネットワークにアップロードする必要があります。

1. MCN から、名前が変更されたブランチサイトを含む新しい構成を持つステージネットワーク。
2. 名前を変更したブランチサイトのステージングパッケージをダウンロードします。
3. **MCN** で、[ステージングされたネットワークのアクティブ化] を選択します。これにより、名前を変更したサイトが無効になり、サイトが使用できなくなります。
4. ブランチの「ローカル変更管理」ページにナビゲートします。
5. 先にダウンロードしたパッケージをアップロードします。[次へ] をクリックし、[アクティブ化] をクリックします。

高可用性を使用したブランチサイトの名前の変更

高可用性が有効なブランチサイトの名前を変更した後に新しい設定をアップロードするには、次の手順に従います。

1. MCN から、名前が変更されたブランチサイトを含む新しい構成でネットワークをステージングします。
2. ブランチサイトの名前を変更したアクティブアプライアンスと高可用性アプライアンスの両方のステージングパッケージをダウンロードします。

3. **MCN** で、[ネットワーク用に ステージングされたアクティブ化] を選択します。これにより、名前を変更したサイトが無効になり、サイトが使用できなくなります。
4. ブランチでアクティブなアプライアンスにナビゲートします。[ローカル変更管理] ページに移動します。
5. 先にダウンロードしたパッケージをアップロードします。[次へ] をクリックし、[アクティブ化] をクリックします。
6. スタンバイアプライアンスに対して、手順 4 (a) と 4 (b) を繰り返します。

ブランチサイトのクローン（オプション）

May 10, 2021

このセクションでは、新しいブランチサイトをクローンして、ブランチサイトを追加するための部分的なテンプレートとして使用する方法について説明します。

注

サイトのクローン作成は任意です。仮想 WAN アプライアンスモデルは、オリジナルサイトとクローンサイトの両方で同じである必要があります。クローンの指定されたアプライアンスモデルを変更することはできません。アプライアンスモデルがサイトで異なる場合は、前のセクションで説明したように、手動でサイトを追加する必要があります。

サイトのクローンを作成すると、ブランチノードの追加および構成プロセスが合理化されます。サイトのクローンが作成されると、サイトの構成設定セット全体がコピーされ、単一のフォームページに表示されます。その後、新しいサイトの要件に従って設定を変更できます。元の設定の一部は、必要に応じて保持できます。ただし、ほとんどの設定はサイトごとに一意である必要があります。

サイトのクローンを作成するには、次の操作を行います。

1. 構成エディタの [サイト] ツリー（中央のペイン）で、複製するブランチサイトをクリックします。
これにより、サイトツリーでその サイト ブランチが開き、「クローン」ボタン（ダブルページアイコン）と「削除」ボタン（ゴミ箱アイコン）が表示されます。
2. ツリー内のブランチサイト名の右側にある [クローン] アイコンをクリックします。
これにより、クローンサイトの 構成ページが開きます。

Clone

Please review the following fields and make the appropriate changes for the new Site.

Site Name:
BR1

Appliance Name:
Appliance

Mode:
client

Secure Key:
ada97484370f0d1

Region:
r1

Routing Domains

Name	Enable	Default
Default_RoutingDomain	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Virtual Interfaces

Name	VLAN ID	DHCP
VirtualInterface-1	0	<input type="checkbox"/>
VirtualInterface-2	0	<input type="checkbox"/>

Virtual IP Addresses

Include	Virtual Interface	Virtual IP Address/Prefix
<input checked="" type="checkbox"/>	VirtualInterface-1	172.110.0.5/24
<input checked="" type="checkbox"/>	VirtualInterface-2	192.110.0.5/24

Local Routes

Include | Network Address | Routing Domain | Gateway

WAN Links

Include Link	WAN Link	Access Type										
<input checked="" type="checkbox"/>	BR1-WL-1											
<div><div>Access Interfaces</div><table><thead><tr><th>Include Interface</th><th>Access Interface</th><th>Virtual Interface</th><th>Virtual IP Address</th><th>Gateway</th></tr></thead><tbody><tr><td><input checked="" type="checkbox"/></td><td>BR1-WL-1-AI-1</td><td>VirtualInterface-1</td><td>172.110.0.5</td><td>172.110.0.1</td></tr></tbody></table></div>			Include Interface	Access Interface	Virtual Interface	Virtual IP Address	Gateway	<input checked="" type="checkbox"/>	BR1-WL-1-AI-1	VirtualInterface-1	172.110.0.5	172.110.0.1
Include Interface	Access Interface	Virtual Interface	Virtual IP Address	Gateway								
<input checked="" type="checkbox"/>	BR1-WL-1-AI-1	VirtualInterface-1	172.110.0.5	172.110.0.1								
<input checked="" type="checkbox"/>	BR1-WL-2											
<div><div>Access Interfaces</div><table><thead><tr><th>Include Interface</th><th>Access Interface</th><th>Virtual Interface</th><th>Virtual IP Address</th><th>Gateway</th></tr></thead><tbody><tr><td><input checked="" type="checkbox"/></td><td>BR1-WL-2-AI-1</td><td>VirtualInterface-2</td><td>192.110.0.5</td><td>192.110.0.1</td></tr></tbody></table></div>			Include Interface	Access Interface	Virtual Interface	Virtual IP Address	Gateway	<input checked="" type="checkbox"/>	BR1-WL-2-AI-1	VirtualInterface-2	192.110.0.5	192.110.0.1
Include Interface	Access Interface	Virtual Interface	Virtual IP Address	Gateway								
<input checked="" type="checkbox"/>	BR1-WL-2-AI-1	VirtualInterface-2	192.110.0.5	192.110.0.1								

GRE Tunnels

Include | Name | Source IP | Destination IP | Tunnel IP / Prefix

3. 新しいサイトの構成パラメータ設定を入力します。

Audit Alert アイコン（赤いドット）が付いたピンク色のフィールドは、必要なパラメータ設定を示し、元のクローンサイトの設定とは異なる値を指定する必要があります。通常、この値は一意である必要があります。

ヒント

クローン作成プロセスをさらに合理化するには、クローンに名前を付ける際に、一貫した事前定義された命名規則を使用します。

4. すべての監査アラートを解決します。

エラーを診断するには、[**Audit Alert**] アイコン（赤い点またはゴールデンロッドのデルタ）にカーソルを合わせて、特定のアラートのバブルヘルプを表示します。

5. 「クローン」（右端隅）をクリックしてサイトを作成し、「サイト」（Sites）テーブルに追加します。

注

[クローン] ボタンは、必要な値をすべて入力するまで使用できず、新しいサイト構成にエラーがない状態になります。

6. （オプション）設定への変更を保存します。

注

余分な予防策として、間違った構成パッケージを上書きしないように、[保存]ではなく[名前を付けて保存]を使用することをお勧めします。既存の構成に保存する前に、[上書きを許可]を選択してください。そうしないと、変更は保存されません。

追加する各ブランチサイトについて、この時点までの手順を繰り返します。

すべてのサイトの追加が完了したら、次の手順では、監査アラートの構成を確認し、必要に応じて修正または追加を行います。

ブランチ構成の監査

May 10, 2021

項目の横にある Audit Alert アイコン (赤い点または金色のデルタ) は、その項目の構成エラーまたはパラメータ情報が不足していることを示します。アイコンの横にある数字は、そのアラートに関連するエラーの数を示します。特定のアラートのバブル・ヘルプを表示するには、アラート・アイコンにカーソルを合わせます。これにより、そのアラートによってフラグ付けされた特定のエラーの簡単な説明が表示されます。構成内のすべての監査アラートを解決する必要があります。そうしないと、展開プロセスの後半で、構成パッケージの検証、ステージングおよびアクティブ化ができなくなります。

すべての監査アラート (存在する場合) を解決すると、構成の「サイト」フェーズが完了します。次のステップでは、完成した サイト 構成を保存します。

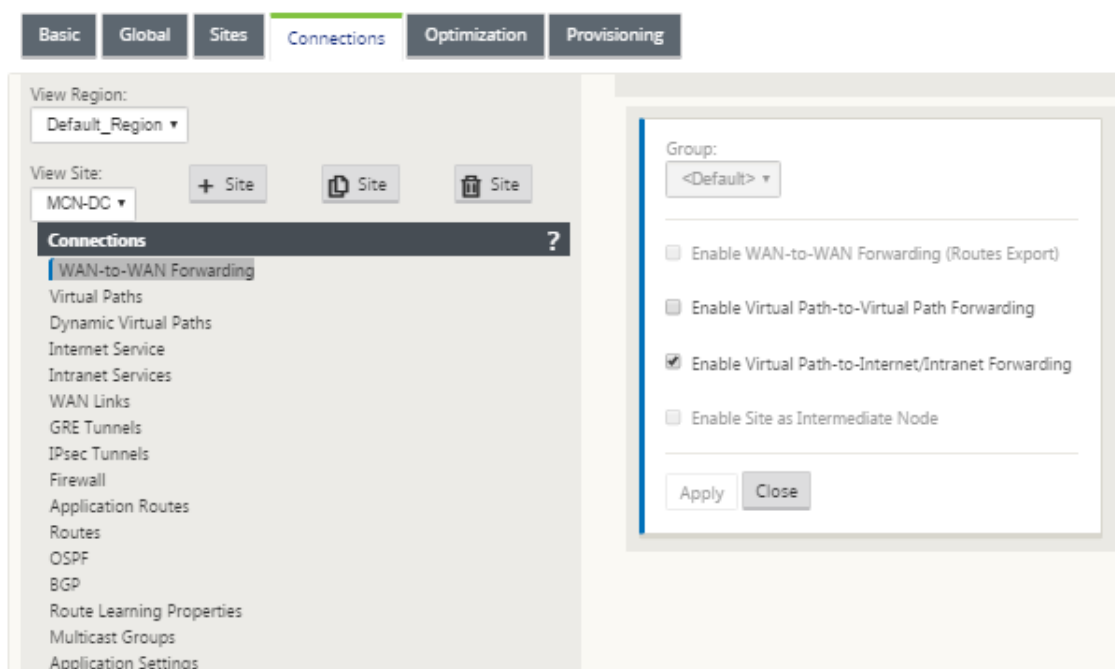
MCN サイトとクライアントサイト間の仮想パスサービスの構成

May 10, 2021

次の手順では、MCN と各クライアント (ブランチ) サイト間の仮想パスサービスを構成します。これを行うには、構成 エディタ の「接続」セクション構成ツリーにある構成フォームと設定を使用します。

MCN とクライアントサイト間の仮想パスサービスを構成するには、次の手順を実行します。

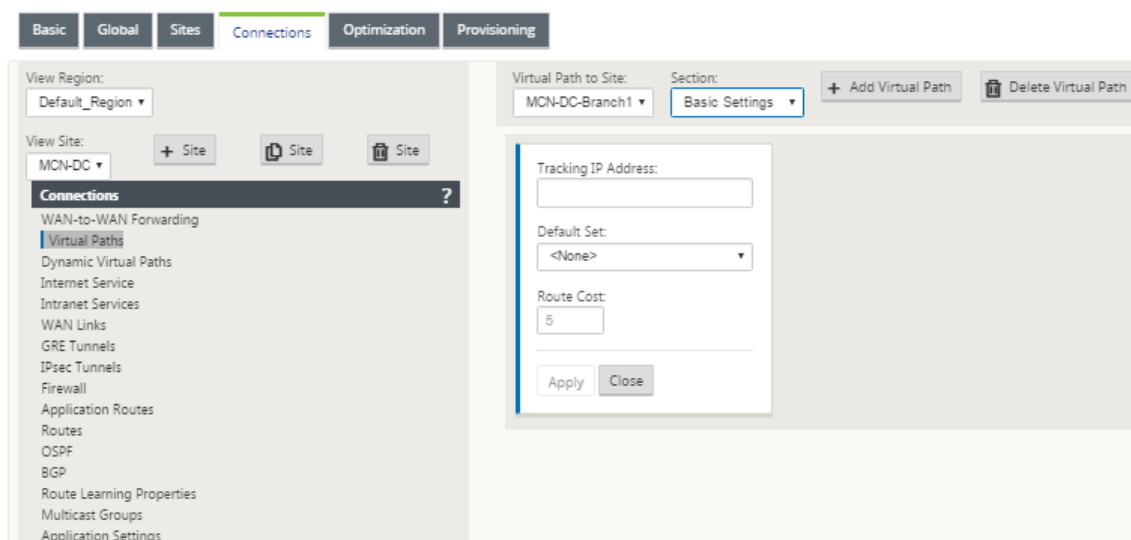
1. 構成エディタで続行し、[接続] タブをクリックします。[接続] セクションの設定ツリーが表示されます。
2. [接続] セクションページの [サイトの表示] ドロップダウンメニューを選択します。これにより、接続 構成で MCN サイトが開きます。



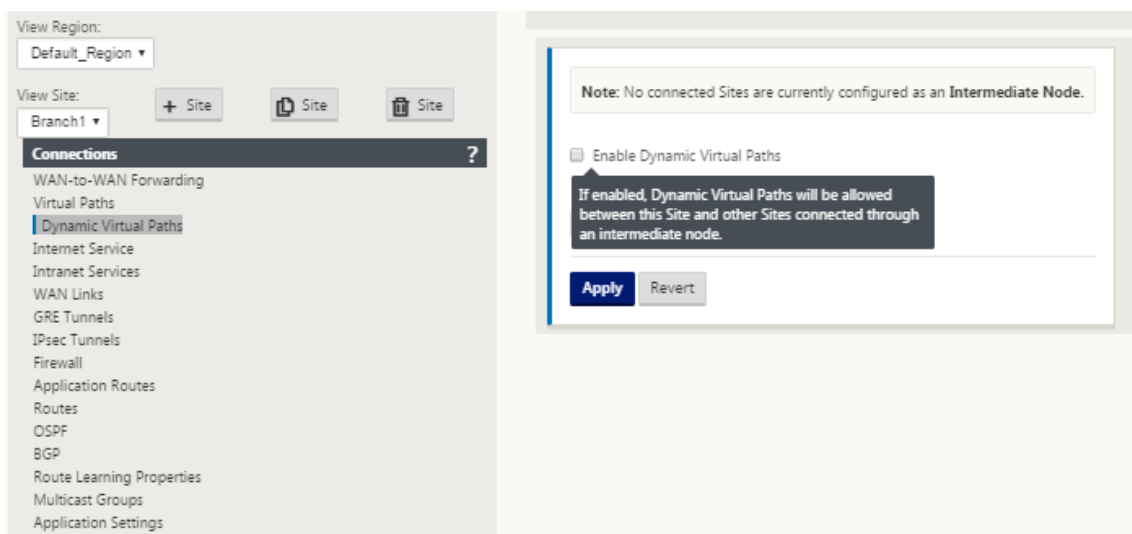
注

WAN から WAN への転送グループは、リージョン内でのみサポートされ、リージョン間ではサポートされません。リージョンを使用すると、WAN から WAN への転送グループに依存する代わりに、ネットワークを分離できます。

3. [仮想パス] をクリックします。これにより、MCN サイトの [仮想パス構成] セクション (子ブランチ) が開きます。このセクションでは、MCN と各仮想 WAN クライアントサイト間の仮想パスサービスを構成するための設定とフォームについて説明します。次の図は、MCN サイトの [仮想パス] セクションの例を示しています。



次の図は、ブランチサイトの 動的仮想パス セクションの例を示しています。



[動的仮想パス] セクションでは、次の項目を設定できます。

- 動的 仮想パス：（オプション）このセクションの設定では、動的仮想パスの有効化と無効化、およびサイトの動的仮想パスの最大許容値を設定できます。動的仮想パスは、構成されたしきい値に基づいて、サイト間で直接確立される仮想パスです。しきい値は、通常、これらのサイト間で発生するトラフィックの量に基づきます。動的仮想パスは、指定されたしきい値に達した後にのみ動作します。動的仮想パスは通常の動作では必要ないため、このセクションの設定は任意です。
- <MCN_Site_Name>_<Branch_Site_Name>：この仮想パスが必要なため、システムは最初に **MCN** とクライアントサイト間に静的な仮想パスを自動的に追加します。パスの名前は次の形式を使用します。

<MCN_Site_Name>_<Branch_Site_Name>

各項目の意味は次の通りです：

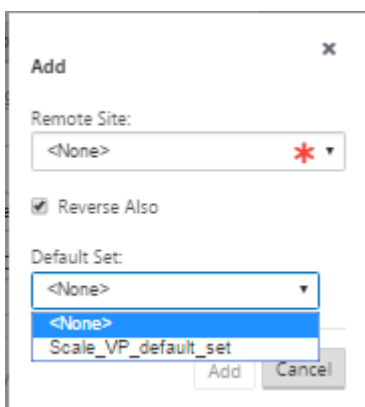
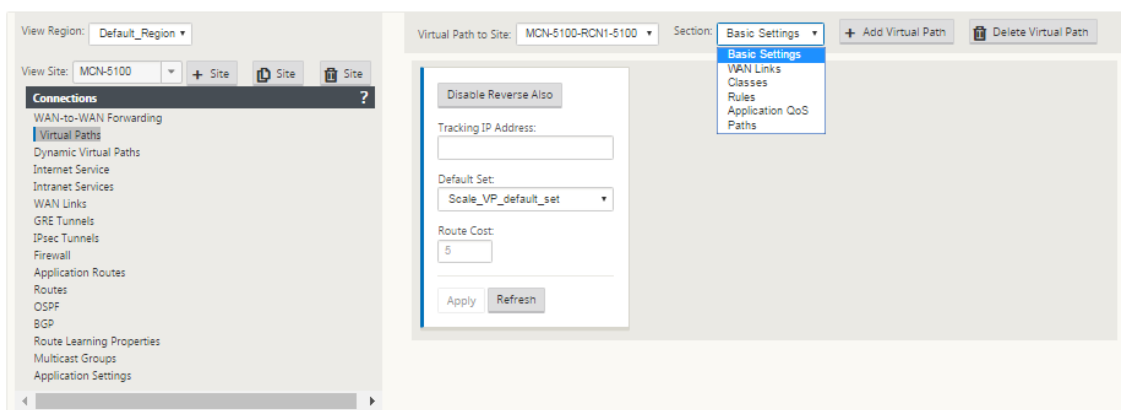
MCN_Site_name は、この仮想 WAN の MCN の名前です。

Branch_Site_Name は、現在の構成パッケージで識別されるクライアントサイトの名前です。

ユーザーが構成可能なデフォルト設定は、[接続] 構成ツリーの [仮想パス] > [デフォルトセット] セクションで定義されているように、最初は静的な仮想パスに適用されます。ただし、定義済みの デフォルトセットをカスタマイズしたり、追加したり、特定のサイトと仮想パスの構成をカスタマイズしたりできます。

注

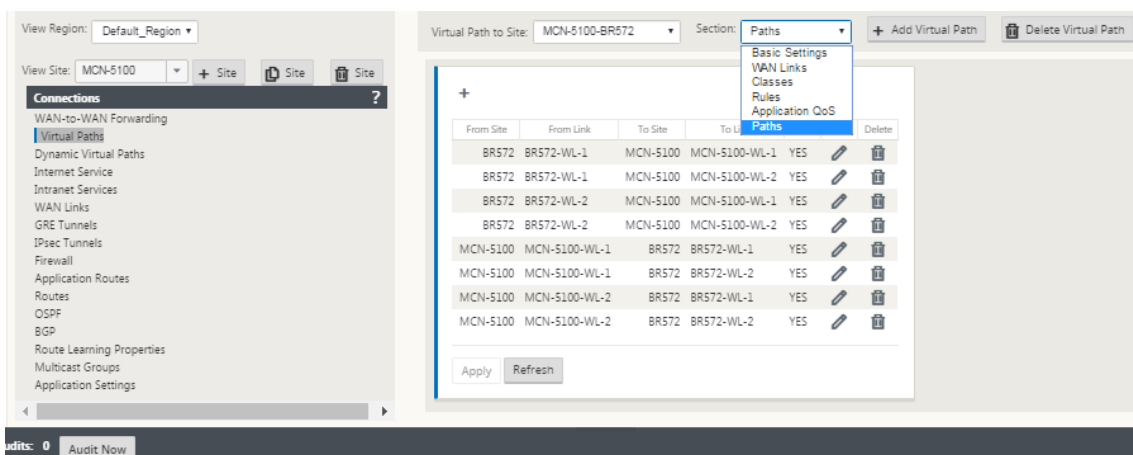
サイトの静的仮想パスを追加するには、手動で追加する必要があります。静的仮想パスを手動で追加する手順は、次の手順に記載されています。



4. [仮想パス] セクションの静的仮想パスの名前の横にある [+ ** 仮想パスの追加 **] をクリックします。これにより、スタティック仮想パスの設定が増えることが明らかになります。
 - a) リモート・サイト：このセクションでは、リモート・サイトの観点から 仮想パスの 設定を表示および構成できます。この特定の仮想パスの必要に応じて、クラス または 規則 を表示、カスタマイズ、および追加できます。必要に応じて、仮想パスをリモートサイトに追加することもできます。
 - b) **Reverse Aso-** 有効にすると、クラスとルールは両方のサイトで仮想パスでミラーリングされます。
 - c) **Default Set**：サイト上の仮想パスのルールとクラスを設定するために使用される仮想パスのデフォルト・セットの名前。

次の図は、MCN 静的仮想パスブランチと子ブランチの例を示しています。

5. [断面] ドロップダウンメニューから [パス] を選択します。



6. [パス] テーブルの上の [+] (追加) をクリックします。

[**Add Path**] ダイアログボックス (設定フォーム) が表示されます。

Add Path

From Site: MCN_DC-01_K

From WAN Link: MCN_DC-01_K

To Site: BR-01_K

To WAN Link: BR-01_K-WL-1

☒ Reverse Also

Add **Cancel**

7. 新しい仮想パスのソース・サイトとデスティネーション・サイト情報を指定します。

8. 使用可能なドロップダウンメニューから次の項目を指定します。

注

サイトの WAN リンクの構成方法に応じて、一部のフィールドは読み取り専用です。設定可能なフィールドには、使用可能な選択項目のドロップダウンメニューが表示されます。

- **[From Site]**: 仮想パスのソース・サイトです。必須の静的仮想パスの場合、これはデフォルトで MCN サイトとして設定されます。
- **From WAN Link**: 仮想パスの発信元の WAN リンクです。
- **[宛先]**: 仮想パスのデスティネーション・サイトです。
- 宛先 **WAN** リンク—仮想パスの宛先 WAN リンクです。

9. [追加] をクリックします。

これにより、構成済みの仮想パスが、[接続] > [仮想パス] ツリーの MCN および関連付けられたクライアントサイトの両方に追加されます。これにより、仮想パス（この場合は MCN）の [From Site] の [パス設定] 構成フォームも自動的に開きます。

From Site	From Link	To Site	To Link	Auto	Edit	Delete
BR572	BR572-WL-1	MCN-5100	MCN-5100-WL-1	YES		
BR572	BR572-WL-1	MCN-5100	MCN-5100-WL-2	YES		
BR572	BR572-WL-2	MCN-5100	MCN-5100-WL-1	YES		
BR572	BR572-WL-2	MCN-5100	MCN-5100-WL-2	YES		
MCN-5100	MCN-5100-WL-1	BR572	BR572-WL-1	YES		
MCN-5100	MCN-5100-WL-1	BR572	BR572-WL-2	YES		
MCN-5100	MCN-5100-WL-2	BR572	BR572-WL-1	YES		
MCN-5100	MCN-5100-WL-2	BR572	BR572-WL-2	YES		

Apply Refresh

10. [MCN からクライアントへの仮想パス] ラベルの右側にある [編集]（鉛筆のアイコン）をクリックします。これにより、編集用の仮想パスサービス構成フォームが開きます。

11. 仮想パスの設定を構成するか、デフォルトをそのまま使用します。

パス 構成フォームには、次の設定が含まれています。

- [サイト] セクションから：
 - サイト：仮想パスのソース・サイトです。必須の静的仮想パスの場合、これはデフォルトで MCN サイトとして設定されます。
 - **WAN** リンク：仮想パスの発信元の WAN リンクです。
- 「サイト」セクション：
 - サイト：仮想パスのデスティネーション・サイトです。
 - **WAN** リンク：仮想パスの宛先 WAN リンクです。
- リバース：この仮想パスに対して「リバース」を使用可能にするには、このチェックボックスを選択します。有効にすると、システムは元のパスに対して設定されたものと同じ WAN リンクを使用して、構成されたパスの反対方向に仮想パスを自動的に構築します。
- [IP DSCP タグ付け] ドロップダウンメニューからタグを選択します。これは、この仮想パスを通過するトラフィックの IP ヘッダーに設定する DSCP タグを指定します。
- **Enable Encryption** —この仮想パスに沿って送信されるパケットの暗号化を有効にするには、このチェックボックスを選択します。

- 不良損失に敏感です。ドロップダウンメニューから設定を選択します。使用できるオプションは、次のとおりです：

- **[Enable]**: (デフォルト) 有効にすると、パスが失われたために **BAD** とマークされ、パススコアリングのペナルティが発生します。
- **Disable** :
Bad Loss Sensitive を無効にすると、帯域幅の損失が許容できない場合に便利です。
- **[Custom]**: パスを BAD としてマークするのに必要な経過時間の経過に伴う損失の割合を指定するには、**[Custom]** を選択します。このオプションを選択すると、さらに次の設定が表示されます。
 - ★ **Percent Loss (%)**: パスが BAD とマークされるまでの損失しきい値の割合を指定します。指定した時間内に測定されます。デフォルトでは、パーセンテージは最後に受信した 200 個のケットに基づきます。
 - ★ **[Over Time (ms)]**: パケット損失を測定する期間 (ミリ秒単位) を指定します。このフィールドのドロップダウンメニューから、100 ~2000 のオプションを選択します。
- 無音期間 (**ms**): パスの状態が **GOOD** から **BAD** に移行するまでの期間 (ミリ秒単位) を指定します。

デフォルトは 150 ミリ秒です。このフィールドのドロップダウンメニューから 150 ~1000 のオプションを選択します。

- パス保護期間 (ミリ秒): パスが BAD から GOOD に移行するまでの待機時間 (ミリ秒) を指定します。このフィールドのドロップダウンメニューから 500 ~6000 のオプションを選択します。デフォルトは 10,000 ミリ秒です。
- 「不安定性の感受性」—有効にするには、このチェックボックスを選択します。有効の場合、パススコアリングアルゴリズムでは、パス状態が **BAD** とその他の遅延スパイクによる遅延ペナルティが考慮されます。
- **[Tracking IP Address]**: 仮想パスに仮想 IP アドレスを入力します。この仮想 IP アドレスを入力すると、パスの状態を確認できます。
- 逆トラッキング **IP** アドレス: 仮想パスに対して
逆方向も 有効になっている場合は、ping 可能なパスに仮想 IP アドレスを入力します。このアドレスを入力すると、逆方向パスの状態を確認できます。

12. **[適用]** をクリックします。これにより、MCN とクライアント サイト間の **2** つの新しい **From Site** および **To Site** の仮想パスが **[Paths]** テーブルに追加されたことがわかります。

Edit ✕

Convert to Static Path

Convert Path, AND all other Paths associated by WAN Link, Generated by an Autopath Group, to a Static Path. This action cannot be undone

MCN-5100

WAN Link:

BR572-WL-1

BR572

WAN Link:

MCN-5100-WL-1

☒ Reverse Also
 ☒ Enable Encryption

IP DSCP Tagging:

Any ▼

Bad Loss Sensitive:

Enable (Default) ▼

Silence Period (ms):

DEFAULT ▼

Path Probation Period (ms):

10000 (Default) ▼

☒ Instability Sensitive

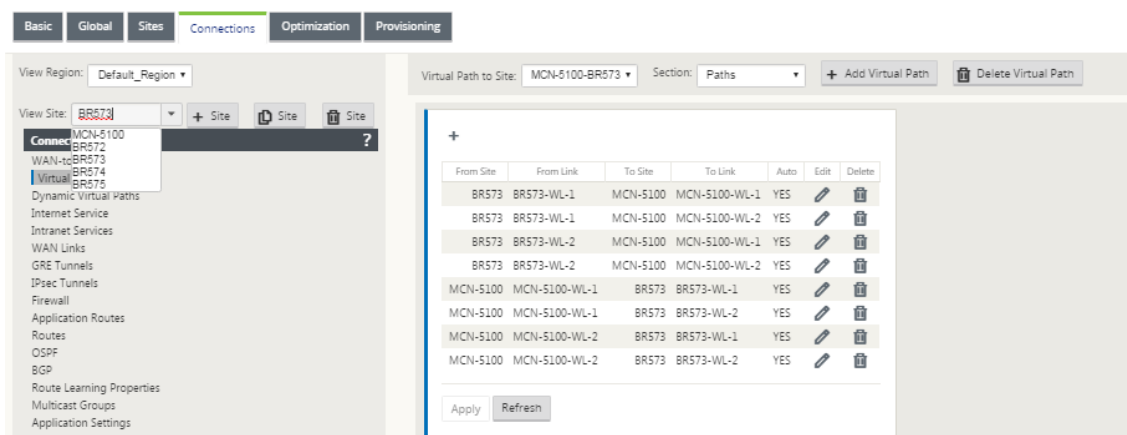
Tracking IP Address:

Reverse Tracking IP Address:

13. MCN に接続するブランチごとに、上記の手順を繰り返します。

次に、クライアントサイトの仮想パス構成をカスタマイズしたり、クライアント間のパスを追加および構成したりできます。手順については、以下の残りの手順で説明します。

14. [サイトの 表示] ドロップダウンメニューからクライアントサイトブランチを選択します。接続 ツリーでクライアントサイトブランチの構成が開きます。

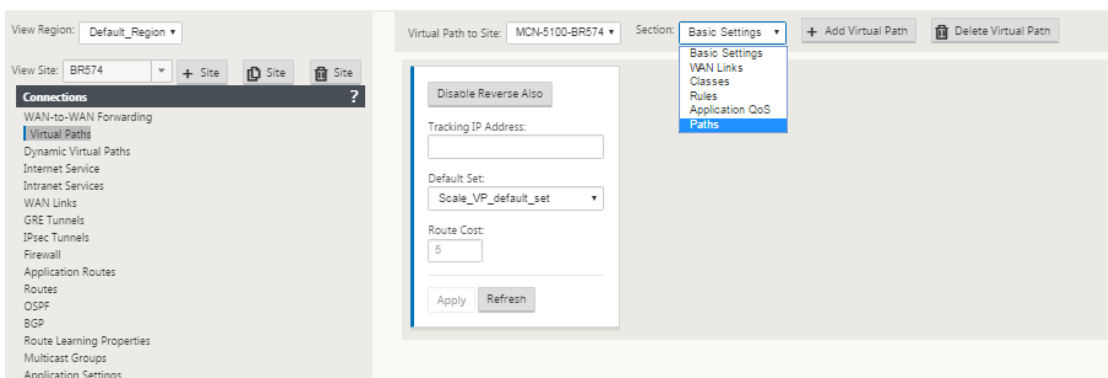


15. 構成するクライアントサイトの仮想パスの [パス設定] 構成フォームに移動します。

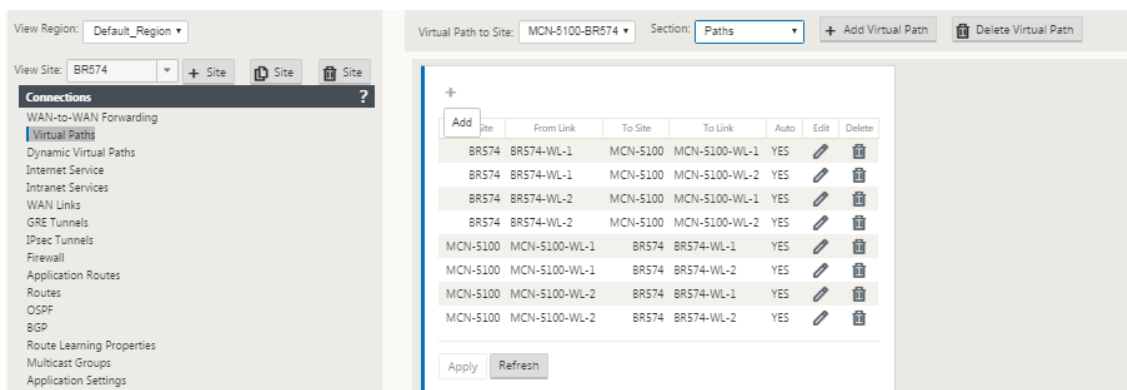
クライアントサイトの [パス設定] フォームに移動するには、次の操作を行います。

16. クライアントサイトのブランチページの [セクション] タブから [パス] を選択します。

次の図は、前の手順で追加された新しいサイトからのパスのパス設定フォームの例を示しています。



17. カスタマイズする各パスの設定を構成します。MCN サイトの仮想パスを構成するのと同じ手順に従います。



これで、クライアントサイトと MCN 間の仮想パスの基本構成は完了です。

注

構成エディタの「接続」セクションまたは「プロビジョニング」セクションでその他の設定を構成する方法については、管理 Web インタフェースのオンライン・ヘルプを参照してください。これらの設定を現在設定したくない場合は、以下に示す適切な手順に進むことができます。

次の手順は、展開用にアクティブ化した SD-WAN エディションライセンスによって異なります。

- **SD-WAN** プレミアム（エンタープライズ）エディション—プレミアム（エンタープライズ）エディションには、WAN 最適化機能のフルセットが含まれています。サイトに WAN Optimization を設定する場合は、[WAN Optimization の有効化と設定](#) トピックに進んでください。それ以外の場合は、直接 [クライアントへの SD-WAN アプライアンスパッケージのインストール] に進むことができます (/en-us/citrix-sd-wan/current-release/configuration/installing-virtual-wan-appliance-packages-clients.html)
- **SD-WAN** エディション—このエディションには、WAN Optimization 機能は含まれません。これで、直接 [クライアントへの SD-WAN アプライアンスパッケージのインストール] に進むことができます (/en-us/citrix-sd-wan/current-release/configuration/installing-virtual-wan-appliance-packages-clients.html)

MCN 設定のデプロイ

May 10, 2021

次の手順では、SD-WAN アプライアンスパッケージをクライアントノードに配布できるように準備します。これには、次の 2 つの手順が含まれます。

1. 構成パッケージを変更管理にエクスポートします。

アプライアンス・パッケージを生成する前に、構成 エディタから **MCN** 上のグローバル変更管理ステージング受信トレイに完成した構成 パッケージをエクスポートする必要があります。手順については、「[変更管理の実行](#)」セクションに記載されています。

2. アプライアンス・パッケージを生成およびステージングします。

新しい構成パッケージ を変更管理 受信トレイに追加したら、アプライアンスパッケージを生成してステージングできます。これを行うには、MCN 上の 管理 **Web** インターフェイスで [変更 管理] ウィザードを使用します。手順については、セクションを参照してください。[構成をブランチに配備します](#)。

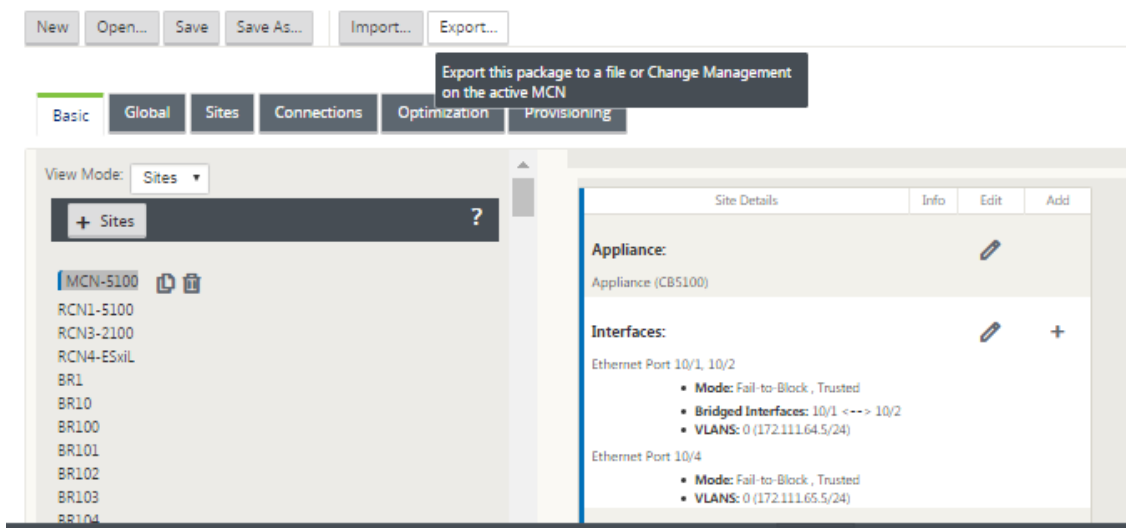
MCN 変更管理の実行

May 10, 2021

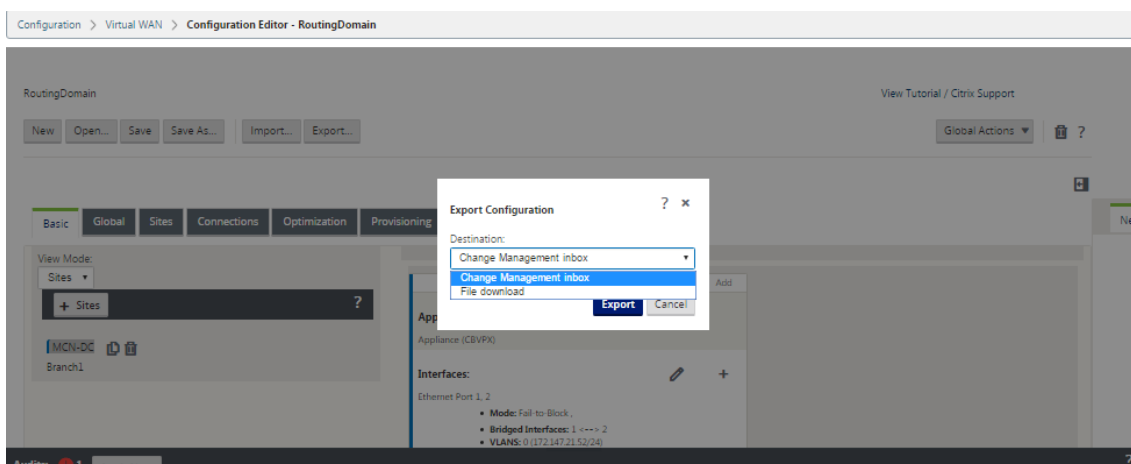
アプライアンス・パッケージを生成する前に、完成した構成パッケージを管理 Web Interface 変更管理 システムにエクスポートする必要があります。

構成パッケージ を変更管理にエクスポートするには、次の手順を実行します。

1. [構成エディタ] ページで、[エクスポート] (ページ上部にある) をクリックします。



これにより、[設定のエクスポート] ダイアログボックスが開きます。



2. エクスポート先として「変更管理の 受信トレイ」を選択します。[Destination] フィールドのドロップダウンメニューを使用して、選択を行います。
3. [エクスポート] をクリックします。

エクスポート操作が完了すると、ページの上部に緑色の成功ステータスメッセージが表示されます。

ヒント

成功メッセージにある青い「変更管理」リンクをクリックすると、変更 管理 ウィザードの「変更準備 - ファイルのアップロードと確認」ページ (2 ページ) に直接移動できます。構成プロセスの次のステップを実行するに

は、このページに移動する必要があります。ただし、成功メッセージは数秒間しか表示されません。その後、ナビゲーションツリーを使用してウィザードを開き、このページに進んでください。手順は次のセクションで説明します。

これで、SD-WAN ソフトウェアパッケージを MCN アプライアンスにアップロードし、クライアントノードに配布するアプライアンスパッケージを準備する準備が整いました。

ブランチへの構成のデプロイ

May 10, 2021

構成エディタを使用して構成を準備し、構成パッケージを変更管理の受信ボックスにエクスポートしたら、次の手順で SD-WAN アプライアンスパッケージをクライアントノードに配布できるように準備します。MCN 上の管理 **Web** インターフェイスで、変更 管理ウィザードを使用します。

SD-WAN アプライアンスモデルごとに異なる SD-WAN ソフトウェアパッケージがあります。アプライアンス・パッケージは、展開する構成パッケージにバンドルされた、特定のモデルのソフトウェア・パッケージで構成されます。したがって、ネットワーク内のアプライアンス・モデルごとに異なるアプライアンス・パッケージを用意し、生成する必要があります。

注

必要な SD-WAN ソフトウェアパッケージをネットワークに接続されている PC にまだダウンロードしていない場合は、ここでダウンロードできます。ソフトウェアの取得とダウンロードについては、「[SD-WAN ソフトウェアパッケージの取得](#)」を参照してください。

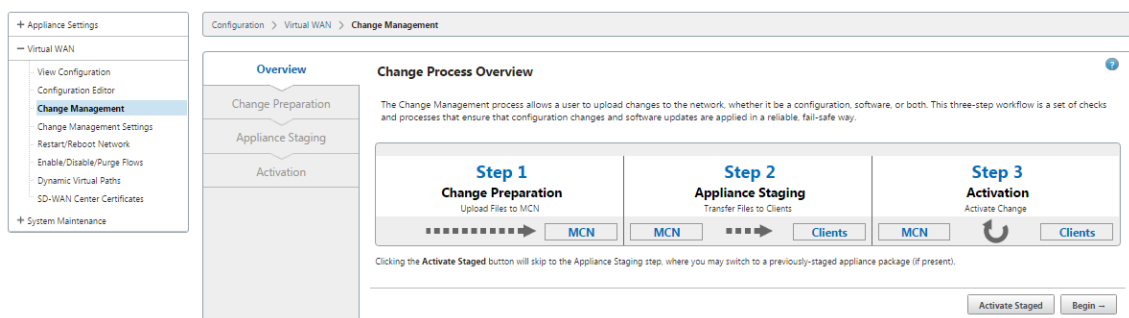
パッケージと設定を MCN にアップロードしてインストールするには、次の手順を実行します。

1. MCN アプライアンスの管理 Web インターフェイスにログインします。

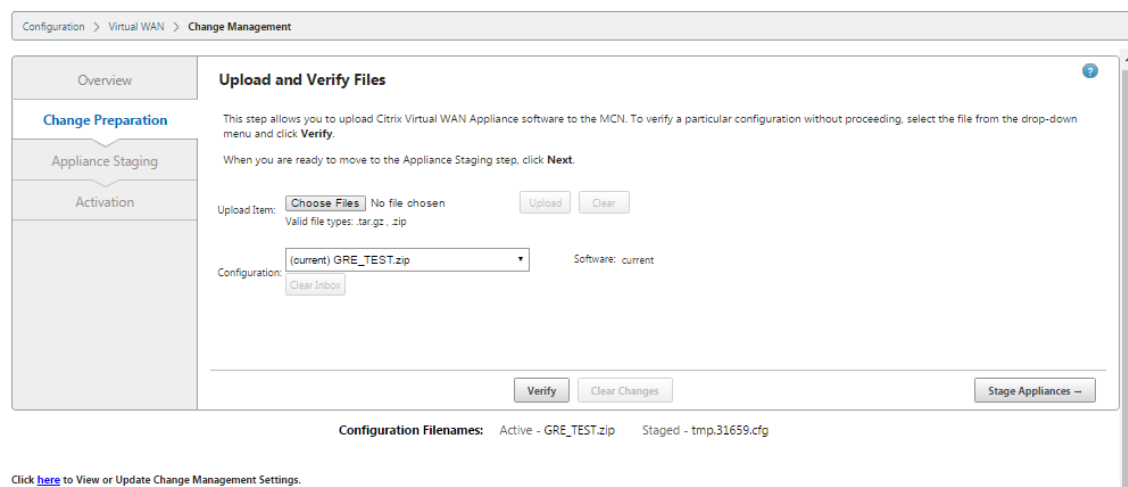
注

接続された PC に以前にダウンロードしたソフトウェアパッケージをアップロードしています。便宜上、この同じ PC を使用して MCN に再度接続することもできます。

2. [構成] タブを選択します。
3. 左側のペインで、[仮想 **WAN**] セクションを開き、[変更管理] を選択します。変更管理 ウィザードの最初のページである「変更プロセスの概要」ページが表示されます。



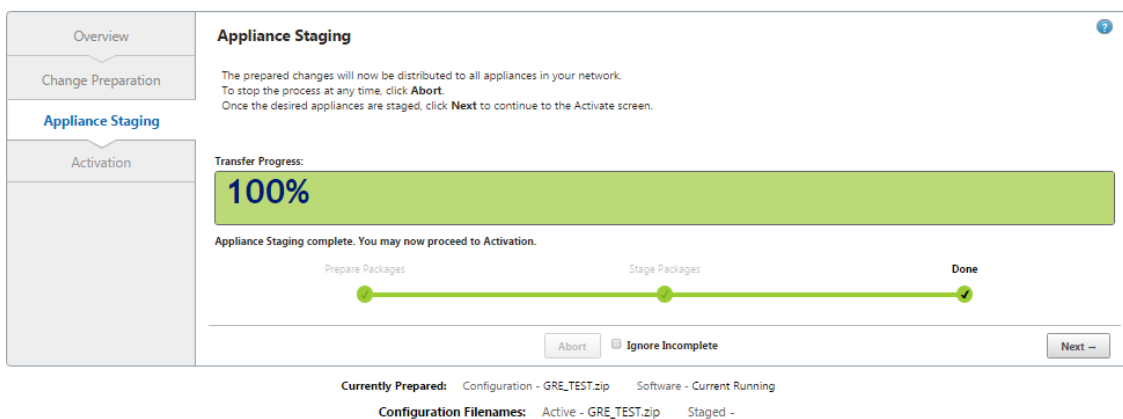
4. [開始] をクリックします。指定した構成およびソフトウェアパッケージが表示されることをアップロードおよび確認するための [**Change Preparation**] ページです。



5. ネットワークに必要な各 SD-WAN ソフトウェアパッケージをアップロードします。
展開する SD-WAN ソフトウェアパッケージごとに、次の手順を実行します。
- 「アイテムのアップロード」フィールドの横にある「ファイルを選択」をクリックします。アップロードする SD-WAN ソフトウェアパッケージを選択するためのファイルブラウザが開きます。
 - SD-WAN ソフトウェアパッケージを選択し、[**OK**] をクリックします。
 - 以前にローカル PC にダウンロードした SD-WAN ソフトウェアパッケージに移動し、アップロードするパッケージを選択します。
 - [**アップロード**] をクリックします。
 - ネットワークに必要な各 SD-WAN ソフトウェアパッケージについて、手順 (i) ~ (iii) を繰り返します。
6. 「構成」フィールドのドロップダウンメニューで、変更管理にエクスポートした新しい構成パッケージを選択します。
7. アプライアンスのステージをクリックします。アプライアンスのステージングでは、次のアクションが開始されます。
- 選択したソフトウェアパッケージと設定を MCN に転送します。

- 選択した構成で識別される各アプライアンス・モデルに対して、アプライアンス・パッケージを生成します。
- 新しいアプライアンス・パッケージを、サイト・アプライアンス・テーブルで使用可能なパッケージのリストに追加します。
- 新しい設定と適切なソフトウェアパッケージを MCN にステージングします。

8. [次へ] をクリックします。「アプライアンスのステージング」ページに進みます。



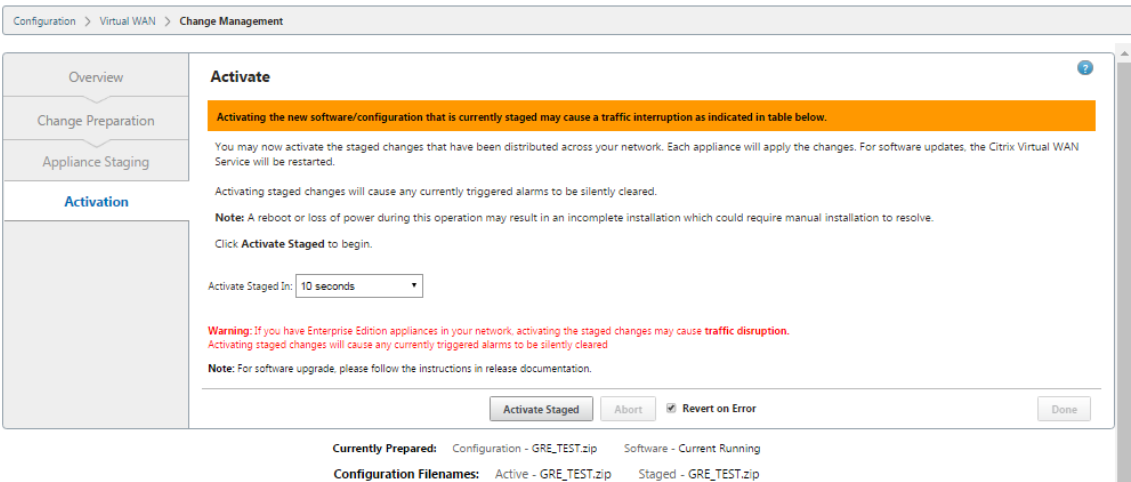
ステージング操作が完了すると、Site-Appliance** テーブルに、新しくステージングされたアプライアンス・パッケージ情報が入力されます。

注

これが初期展開の場合、MCN のみが更新され、ステージングされます。既存の展開を更新していて、展開されたサイト間で仮想パスがすでに機能している場合は、展開されたクライアントノードに適切なアプライアンスパッケージが配布され、それらのノードでステージングが開始されます。ただし、既存の Virtual WAN 展開に新しいクライアント・ノードを追加する場合は、この手順の残りの手順で説明するように、新しいクライアントごとに適切な Appliance パッケージを手動でアップロード、ステージングおよびアクティブ化する必要があります。

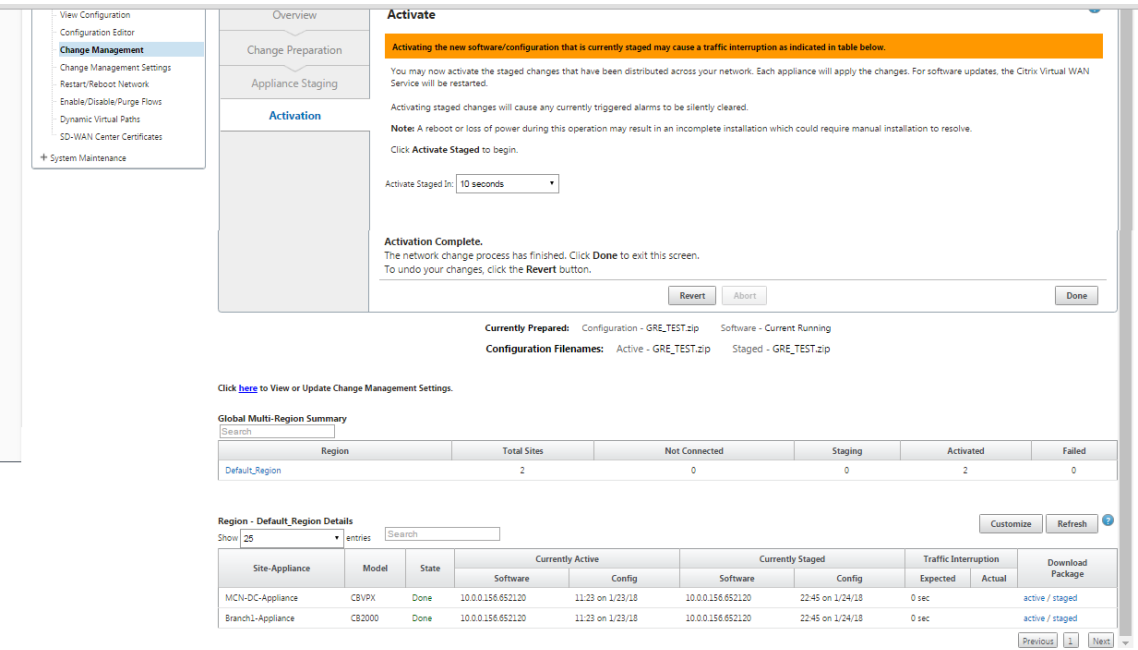
[変更管理] ページでサイトが接続されていないと表示される場合は、ステージングプロセス中に失敗としてマークされ、進行状況バーは 100% まで完了します。接続されていないサイトがオンラインに戻り、接続されると、MCN はそれを自動修正します。

9. エラーが発生したときに以前のアプリケーションパッケージに戻すには、[エラー時に元に戻す] を選択します。詳細については、「構成のロールバック」を参照してください。
10. [ステージングを有効化] をクリックします。



この時点の結果と次のステップは、これが初期構成であるか、既存の構成を更新または置き換えるかによって、次のように異なります。

- 既存の配置の設定を更新または変更する場合。
 - これが初期構成でない場合は、MCN アプライアンスの新しい構成と適切なアプライアンスパッケージがアクティブになります。その後、適切なアプライアンスパッケージが SD-WAN 内の各クライアントに配布され、自動的にアクティブ化されます。この処理が完了するまで数秒かかることがあります。



アクティベーションが完了すると、[アクティベーション完了] ステータスメッセージが表示され、[完了] ボタンが有効になります。さらに、表の上にある [Configuration Filenames] ステータス行 (Configuration Filenames) の [Active] フィールドに、新しくアクティブ化されたパッケージの名前が表示されるようになりました。

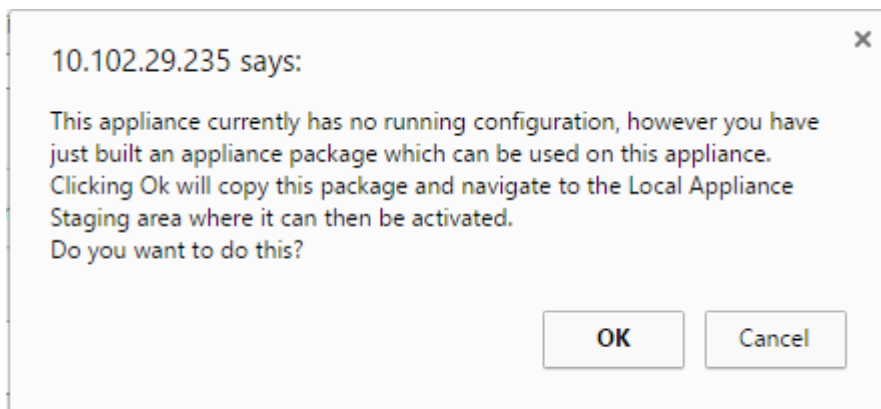
11. [** 完了] をクリックし、次のいずれかの操作に進みます。

- SD-WAN に新しいノードを追加しない場合は、SD-WAN 内の新しいアプライアンス・パッケージの準備、配布、アクティベーションが完了します。[仮想 WAN サービスの有効化](#)に直接進むことができます。
- SD-WAN に新しいクライアントノードを追加する場合は、
「[クライアントアプライアンスのネットワークへの接続](#)」を参照してください。

-初期構成をアクティブ化する場合、新しい構成パッケージはこの時点ではアクティブ化されず、さらに実行する必要がある手順があります。次の手順では、構成パッケージをローカルアプライアンスのステージング領域にコピーし、MCN 上で構成パッケージをステージングおよびアクティブ化するための準備を行います。

以下を実行します：

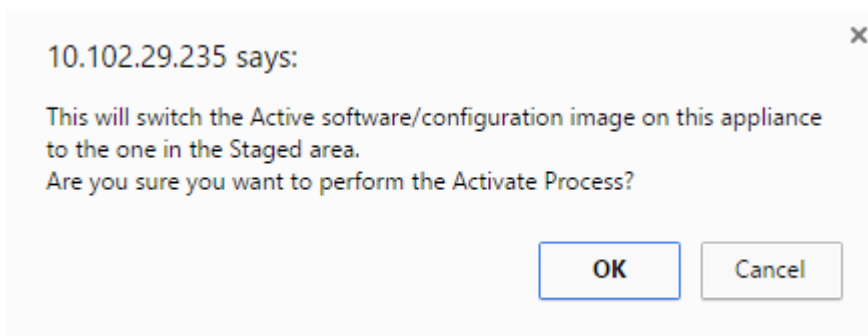
12. [ステージのアクティブ化] をクリックすると、次のメッセージが表示されます。

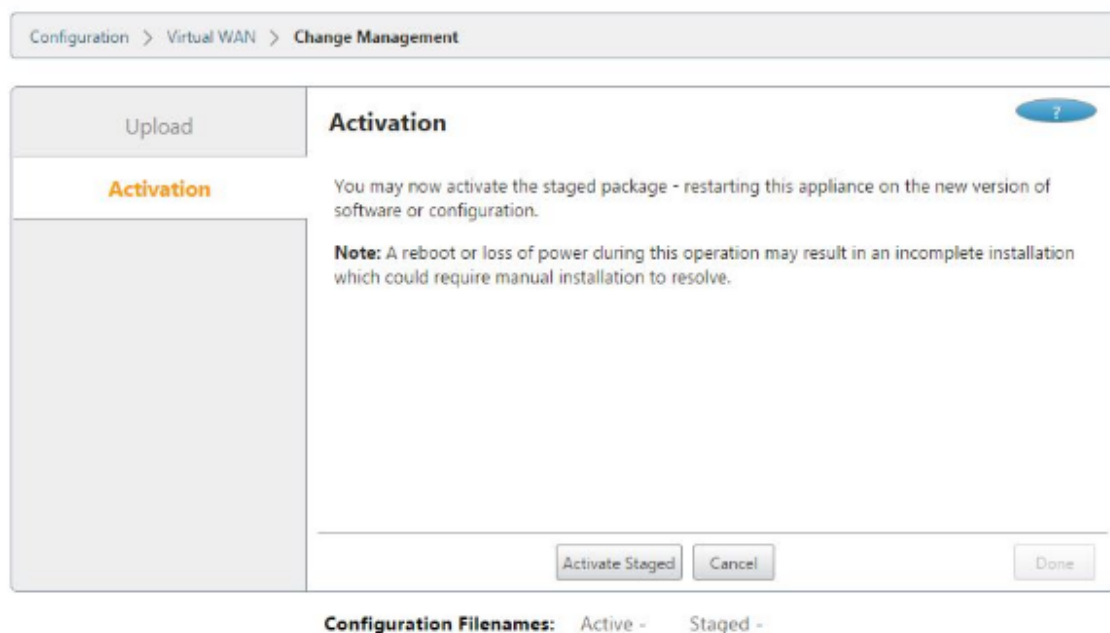


13. [**OK**] をクリックします。

14. [ステージングされたアクティブ化] をクリックします。

これにより、アクティベーション操作の確認を求めるダイアログボックスが表示されます。





15. **[OK]** をクリックします。

これにより、ステージングされた構成パッケージのアクティブ化が開始されます。この処理には数秒かかります。この間、進捗状況メッセージが表示されます。

アクティベーションが完了すると、アクティベーションが完了したことを示すステータスメッセージが表示され、**[完了]** ボタンが有効になります。

16. **[完了]** をクリックします。これにより、**[管理 Web Interface Dashboard]** ページに進み、アクティブ化の結果を表示できます。

これで、MCN での SD-WAN アプライアンスパッケージの準備が完了しました。クライアントアプライアンスをネットワークに接続する (</en-us/citrix-sd-wan/current-release/configuration/connecting-client-appliances-to-network.html>) に進みます。

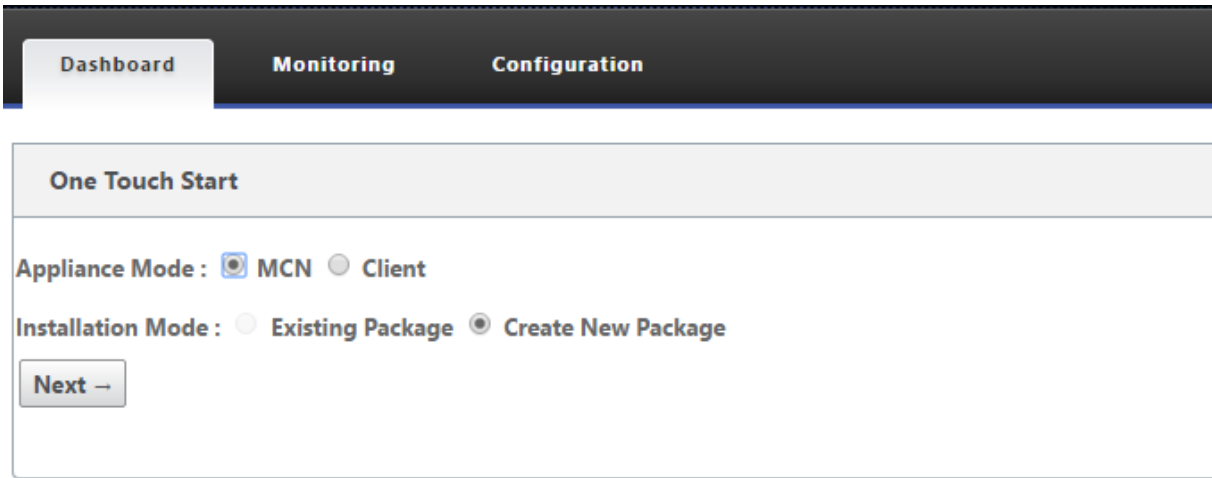
ヒント

変更管理 ウィザードでは、サイト・アプライアンスのテーブルを検索できます。これにより、複数のサイトがある大規模なネットワーク上のサイトを検索し、必要な段階的な構成をダウンロードできます。エラー状態を検索することもできます。たとえば、「失敗」や「未接続」などです。これにより、その状態にあるすべてのサイトのリストが表示されます。

ワンタッチスタート

May 10, 2021

タッチスタートにより、初回起動時に SD-WAN アプライアンスをクライアントとして簡単かつ迅速に構成できます。アプライアンスを初めて起動すると、ワンタッチ起動オプションが表示されます。



Dashboard Monitoring Configuration

One Touch Start

Appliance Mode : ☒ MCN ☐ Client

Installation Mode : ☐ Existing Package ☒ Create New Package

Next ->

注

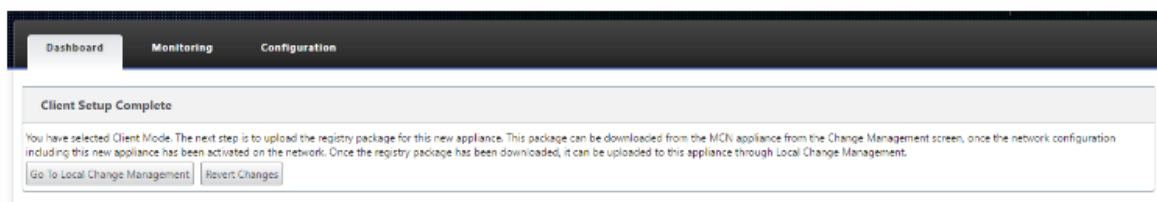
SD-WAN アプライアンスを MCN として設定するには、構成 エディタを使用して構成を作成するか、既存の構成をインポートします。詳細については、「[MCN での SD-WAN アプライアンスパッケージの準備](#)」を参照してください。

既存の構成ファイルを使用して SD-WAN アプライアンスをクライアントとして設定するには、次の手順を実行します。

1. アプライアンスモードとして [クライアント] を選択します。
2. [既存のパッケージ インストールモード] を選択します。管理者は、MCN の既存のパッケージを利用するために MCN の設定を定期的に保存する必要があります。
3. [ファイルの選択] をクリックして、ローカルコンピュータから構成パッケージを選択します。
4. [アップロードとインストール] をクリックします。

ローカル変更管理を使用して SD-WAN アプライアンスをクライアントとして設定するには、以下の手順に従ってください。

1. アプライアンスモードとして [クライアント] を選択します。
2. [**Create New Package**] を選択して、ローカル変更管理を使用してこのアプライアンスの構成パッケージをアップロードします。パッケージは、変更管理画面から MCN アプライアンスからダウンロードできます。
3. [次へ] をクリックします。
4. [ローカル変更管理に移動] をクリックします。



トピッククライアントへの SD-WAN アプライアンスパッケージのインストールの手順に従います。

クライアントアプライアンスのネットワークへの接続

November 8, 2021

最初の展開の場合、または既存の SD-WAN にクライアントノードを追加する場合は、ブランチサイト管理者がクライアントアプライアンスをそれぞれのブランチサイトのネットワークに接続するための次のステップです。これは、適切な SD-WAN アプライアンスパッケージをクライアントにアップロードおよびアクティブ化する準備です。各ブランチサイト管理者に接続して、これらの手順を開始および調整してください。

サイトアプライアンスを SD-WAN に接続するには、サイト管理者は次の操作を行う必要があります。

1. まだクライアントアプライアンスをセットアップしていない場合は、クライアントアプライアンスをセットアップします。

SD-WAN に追加するアプライアンスごとに、次の操作を行います。

- a) SD-WAN アプライアンスハードウェアと、展開する SD-WAN VPX 仮想アプライアンス (SD-WAN VPX-SE) をセットアップします。
 - b) アプライアンスの管理 IP アドレスを設定し、接続を確認します。
 - c) アプライアンスの日付と時刻を設定します。コンソールセッションタイムアウトしきい値を高い値または最大値に設定します。
 - d) アプライアンスにソフトウェアライセンスファイルをアップロードしてインストールします。
2. アプライアンスをブランチサイトの LAN に接続します。イーサネットケーブルの一端を SD-WAN アプライアンスの LAN 用に設定されたポートに接続します。次に、ケーブルのもう一方の端を LAN スイッチに接続します。
 3. アプライアンスを WAN に接続します。イーサネットケーブルの一端を SD-WAN アプライアンスの WAN 用に設定されたポートに接続します。次に、ケーブルのもう一方の端を WAN ルータに接続します。

次のステップは、ブランチサイト管理者がそれぞれのクライアントに適切な SD-WAN アプライアンスパッケージをインストールしてアクティブ化することです。

シェルコマンドへのアクセス

SD-WAN 11.4.1 リリース以降、管理者アカウントユーザは、CBVWSSH スタティックアカウントのログインクレデンシャルの入力を求められることなく、SD-WAN CLI コンソールから直接シェルコマンドを実行できます。この機能は、CBVWSSH アカウントのハードコードされたパスワードを削除し、より安全な方法を使用して置き換えるため、SD-WAN アプライアンスのセキュリティを強化します。シェルコマンドを実行するには、SD-WAN CLI コンソールにログインし、`shell`と入力します。

注

- この機能は、管理者アカウントユーザーに対してのみサポートされています。ネットワーク管理者、セキュリティ管理者、または Viewer アカウントユーザーにはサポートされていません。
- この機能は、トラブルシューティングのみを目的としています。`shell`コマンドによって行われたシステム固有の変更は、Citrix によって監視されます。

アップグレード

SD-WAN アプライアンスを 11.4.1 バージョンにアップグレードすると、デフォルトの管理者アカウントのパスワードが CBVWSSH アカウントと同期されます。CBVWSSH アカウントとデフォルト管理者アカウント間のこの同期は、管理者アカウントを編集または更新するたびに行われます。

ダウングレード

SD-WAN アプライアンスを 11.4.1 から古いバージョンにダウングレードすると、デフォルトの管理者アカウントのパスワードとリセットオプションが表示されます。ただし、新しいパスワードは CBVWSSH アカウントと同期されません。したがって、ダウングレード後も `shell` コマンドにアクセスできるようにするには、アプライアンスをダウングレードする前に現在のパスワードを覚えておく必要があります。

クライアントへの **SD-WAN** アプライアンスパッケージのインストール

May 10, 2021

アプライアンスパッケージを準備し、MCN を接続し、ブランチサイト管理者がそれぞれのクライアントアプライアンスを LAN および WAN に接続したら、次のステップは、各クライアントで適切な SD-WAN アプライアンスパッケージをアップロードしてアクティブ化することです。変更管理ウィザードの指示に従って、このプロセスを実行します。

クライアントアプライアンスにソフトウェアと構成をインストールしてアクティブ化するには、次の手順に従います。

1. 接続されている PC でブラウザを開き、MCN アプライアンスの管理 Web インターフェイスにログオンします。

ブラウザアドレスフィールドに MCN の管理 IP アドレスを入力します。これにより、MCN アプライアンスの管理 Web インターフェイス ダッシュボード ページが表示されます。

2. [構成] タブを選択します。左側のナビゲーションペインで、[**Virtual WAN**] を選択し、[変更管理] を選択します。

これにより、「変更プロセスの概要」ページ（「変更管理」ウィザードの最初のページ）が表示されます。

Configuration > Virtual WAN > Change Management

Overview
Change Preparation
Appliance Staging
Activation

Activate

Activating the new software/configuration that is currently staged may cause a traffic interruption as indicated in table below.

You may now activate the staged changes that have been distributed across your network. Each appliance will apply the changes. For software updates, the Citrix Virtual WAN Service will be restarted.

Activating staged changes will cause any currently triggered alarms to be silently cleared.

Notes: A reboot or loss of power during this operation may result in an incomplete installation which could require manual installation to resolve.

Click **Activate Staged** to begin.

Activate Staged In: 10 seconds

Warning: If you have Enterprise Edition appliances in your network, activating the staged changes may cause traffic disruption. Activating staged changes will cause any currently triggered alarms to be silently cleared.

Note: For software upgrade, please follow the instructions in release documentation.

Currently Prepared: Configuration - scale_3regions_575Branch_1DCaes128_cb5100_4444Pathdynamic_fixed_RCN1_HA_VPXremotelicensing_550sites_wantowanforwarding_geoRCN_1kEE.zip Software - Current Running

Configuration Filenames: Active - scale_3regions_575Branch_1DCaes128_cb5100_4444Pathdynamic_fixed_RCN1_HA_VPXremotelicensing_550sites_wantowanforwarding_geoRCN_1kEE.zip Staged - scale_3regions_575Branch_1DCaes128_cb5100_4444Pathdynamic_fixed_RCN1_HA_VPXremotelicensing_550sites_wantowanforwarding_geoRCN_1kEE.zip

Click [here](#) to View or Update Change Management Settings.

Global Multi-Region Summary

Region	Total Sites	Not Connected	Preparing/Staging	Staged	Failed
Default Region	10	2	0	8	0
r1	552	4	4	547	0
r3	8	2	1	5	0
r4	Data not available				

Region - Default Region Details

Show 25 entries

Site-Appliance	Model	State	Currently Active		Currently Staged		Traffic Interruption		Download Package
			Software	Config	Software	Config	Expected	Actual	
MCN-S100-Appliance	CB5100	Done	10.0.0.184.657939	13:18 on 2/14/18	10.0.0.184.657939	14:58 on 2/14/18	0 sec		active / staged
BR572-Appliance	CBVPX	Done	10.0.0.184.657939	13:18 on 2/14/18	10.0.0.184.657939	14:58 on 2/14/18	0 sec		active / staged
BR573-Appliance	CBVPX	Done	10.0.0.184.657939	13:18 on 2/14/18	10.0.0.184.657939	14:58 on 2/14/18	0 sec		active / staged
BR574-Appliance	CBVPX	Done	10.0.0.184.657939	13:18 on 2/14/18	10.0.0.184.657939	14:58 on 2/14/18	0 sec		active / staged
BR575-Appliance	CBVPX	Done	10.0.0.184.657939	13:18 on 2/14/18	10.0.0.184.657939	14:58 on 2/14/18	0 sec		active / staged
RCN1-S100-Appliance	CB5100	Transferring Region	10.0.0.184.657939	13:18 on 2/14/18	10.0.0.184.657939	14:58 on 2/14/18	0 sec		active / staged
RCN1-S100-RCN1_HA-Appliance	CB5100	Done	10.0.0.184.657939	13:18 on 2/14/18	10.0.0.184.657939	14:58 on 2/14/18	0 sec		active / staged
RCN3-2100-Appliance	CB2100	Done	10.0.0.184.657939	13:18 on 2/14/18	10.0.0.184.657939	14:58 on 2/14/18	0 sec		active / staged
RCN3Geo-2100-Appliance	CB2100	Cancelled	Not Connected					Loc Chg Mgt	active / staged
RCN4-ES10-Appliance	CBVPXL	Cancelled	Not Connected					Loc Chg Mgt	active / staged

このページの下部には、個々のサイトとアプライアンスを一覧表示する表が表示されます。「パッケージのダウンロード」列の表の右端には、アクティブ（使用可能な場合）およびステージングされたパッケージへのリンクがあります。

Traffic Interruption		Download Package
Expected	Actual	
0 sec		active / staged
Loc Chg Mgt		active / staged

注

これが初期インストールの場合、アクティブ リンクはまだ利用できず、プレーンテキストマーカー **none** に置き換えられます。

3. ダウンロードするパッケージの [**Staged**] リンクをクリックします。

[**Site-Appliance**] テーブルで、サイト・アプライアンスのエントリを探し、そのエントリの [**Download Package**] 列にある [**Staged**] リンクをクリックします。(ローカル PC 上の) ダウンロード場所を選択するためのファイルブラウザが表示されます。

4. ダウンロード場所を選択し、[**OK**] をクリックします。
5. (オプション) ダウンロードが完了したら、MCN 管理 Web インターフェイスからログアウトします。
6. ブラウザを開き、アプライアンス・パッケージの.zip ファイルをアップロードするクライアントの IP アドレスを入力します。

注

管理 Web インターフェイスのブラウザ証明書の警告は無視してください。

これにより、クライアントアプライアンスの [Citrix SD-WAN 管理 Web インターフェイスのログイン] 画面が開きます。



7. 管理者のユーザー名とパスワードを入力し、[ログイン]をクリックします。デフォルトの管理者ユーザー名は *admin* です。デフォルトのパスワードは *password* です。

これにより、クライアントアプライアンスの [管理 Web インターフェイス ダッシュボード] ページが表示されます。

System Status

Name:	MCN-5100
Model:	5100
Appliance Mode:	MCN
Serial Number:	4H30GNCNP00
Management IP Address:	10.199.107.201
Appliance Uptime:	1 weeks, 4 minutes, 45.3 seconds
Service Uptime:	1 days, 1 hours, 1 minutes, 42.0 seconds
Routing Domain Enabled:	Default_RoutingDomain

Local Versions

Software Version:	10.0.0.184.657939
Built On:	Feb 13 2018 at 17:32:49
Hardware Version:	5100
OS Partition Version:	4.6

Virtual Path Service Status

Virtual Path MCN-5100-BR572:	Uptime: 1 hours, 55 minutes, 42.0 seconds.
Virtual Path MCN-5100-BR573:	Uptime: 1 hours, 55 minutes, 44.0 seconds.
Virtual Path MCN-5100-BR574:	Uptime: 1 hours, 55 minutes, 23.0 seconds.
Virtual Path MCN-5100-BR575:	Uptime: 1 hours, 55 minutes, 41.0 seconds.
Virtual Path MCN-5100-RCN1-5100:	Uptime: 21 hours, 40 minutes, 32.0 seconds.
Virtual Path MCN-5100-RCN3-5100:	Uptime: 1 hours, 54 minutes, 49.0 seconds.
Virtual Path 'MCN-5100-RCN4-ES4L' is currently dead.	
Virtual Path 'MCN-5100-RCN3Geo-2100' is currently dead.	

注

これが初期インストールの場合、またはこのアプライアンスで仮想 WAN サービスを一時的に無効にした場合は、仮想 WAN サービスが非アクティブまたは無効であることを示すステータスメッセージと共に、金色の監査アラートアイコンが表示されます。現時点では、このアラートは無視できます。アラートは、インストールが完了した後、手動でサービスを開始するまで [ダッシュボード] ページに残ります。

8. [構成] タブを選択します。
9. ナビゲーション・ツリー（左ペイン）で「システムメンテナンス」ブランチを開き、「ローカル変更管理」を選択します。

アプライアンスパッケージをアップロードするための「ローカルアプライアンスの変更プロセスのアップロード」ページが表示されます。

Configuration > System Maintenance > Local Change Management

Upload

Local Appliance Change Process

The Local Change Management process allows a user to upload a new appliance package to this individual appliance. This two-step workflow is a set of checks and processes that ensure that configuration changes and software updates are applied to the appliance in a reliable, fail-safe way.

Note: This process does not update any other appliances on the network. For that purpose, use the Configuration -> Virtual WAN -> Change Management screen on the MCN.

Upload Item: [Choose File](#) No file chosen
Valid file types: ".zip"

[Upload](#)

[Next](#)

Configuration Filenames: Active - scale_3regions_575Branch_1DCaes128_cb5100_4444Pathdynamic_fixed_RCNI_HA_VPXremotelicensing_550sites_wantowanforwarding_geoRCN_1kEE.zip Staged - scale_3regions_575Branch_1DCaes128_cb5100_4444Pathdynamic_fixed_RCNI_HA_VPXremotelicensing_550sites_wantowanforwarding_geoRCN_1kEE.zip

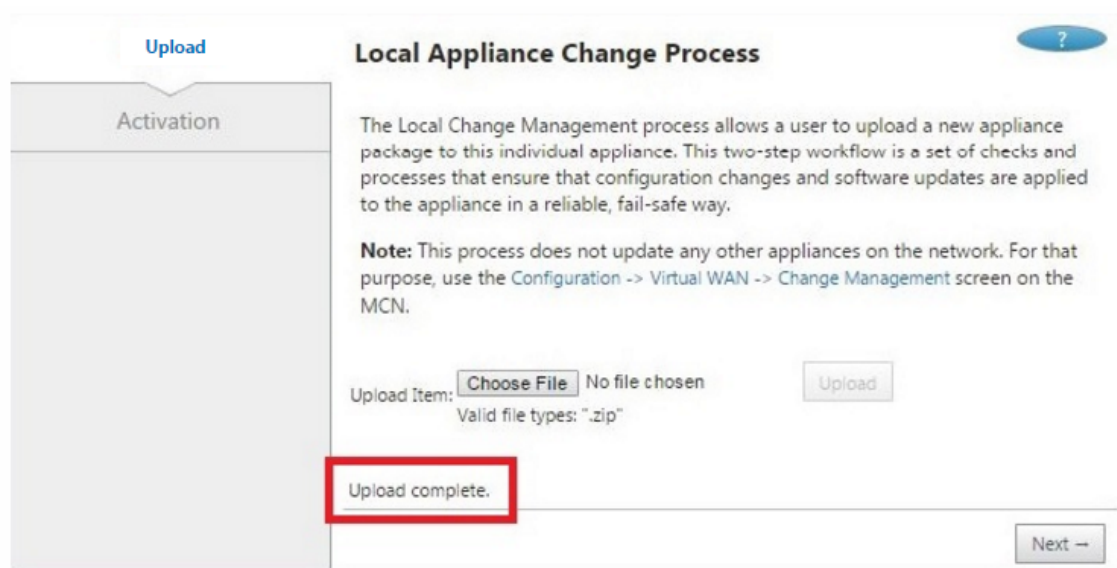
Model	Active Software	Active Config	Staged Software	Staged Config
CB5100	10.0.0.184.657939 download	13:18 on 2/14/18	10.0.0.184.657939 download	14:58 on 2/14/18

10. 「商品をアップロード」ラベルの横にある「ファイルを選択」をクリックします。

これにより、クライアントにアップロードするアプライアンス・パッケージを選択するためのファイル・ブラウザが開きます。

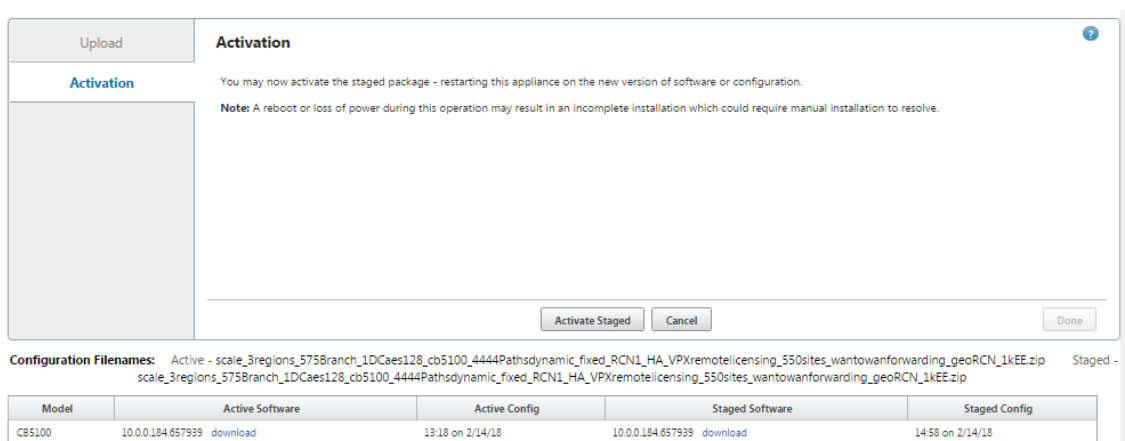
11. MCN からダウンロードした SD-WAN アプライアンスパッケージの zip ファイルに移動して選択し、[OK] をクリックします。
12. [アップロード] をクリックします。

アップロード処理が完了するまで数秒かかります。完了すると、アップロードが完了したことを示すステータスメッセージ（ページの左中央）が表示されます。



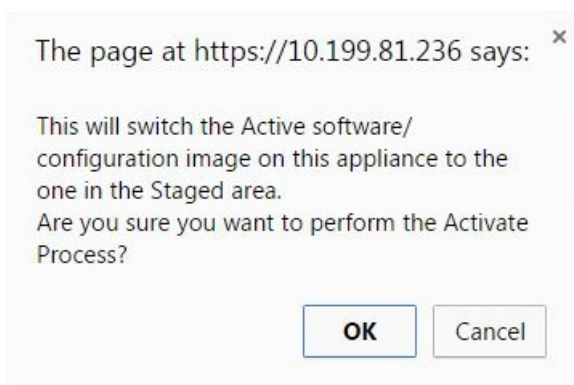
13. [次へ] をクリックします。

指定したソフトウェアパッケージがアップロードされ、[ローカル変更管理の アクティブ化] ページが表示されます。



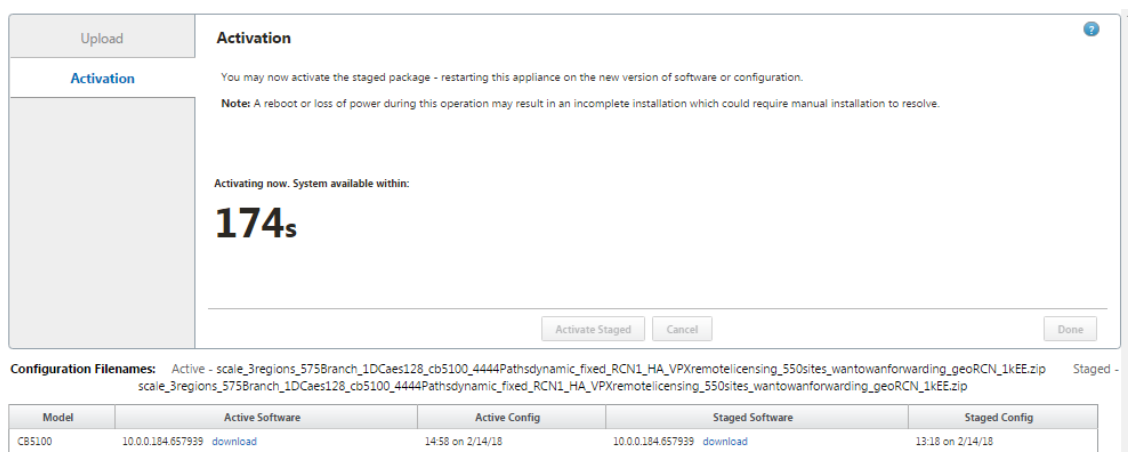
14. [ステージングを有効化] をクリックします。

これにより、アクティブ化操作の確認を求めるダイアログボックスが表示されます。

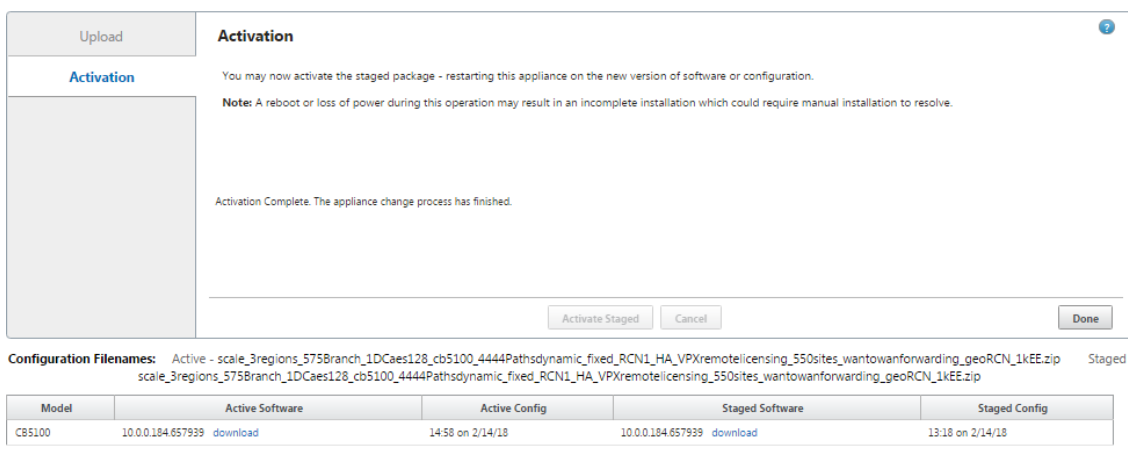


15. **[OK]** をクリックします。

これにより、新しくインストールされたパッケージがアクティブになり、初期展開でない場合は、クライアントアプライアンスで仮想 WAN サービスが起動します。この処理には数秒かかります。この間、進捗状況メッセージが表示されます。



アクティベーションが完了すると、アクティベーションが完了したことを示すステータスメッセージが表示され、**[完了]** ボタンが使用可能になります。

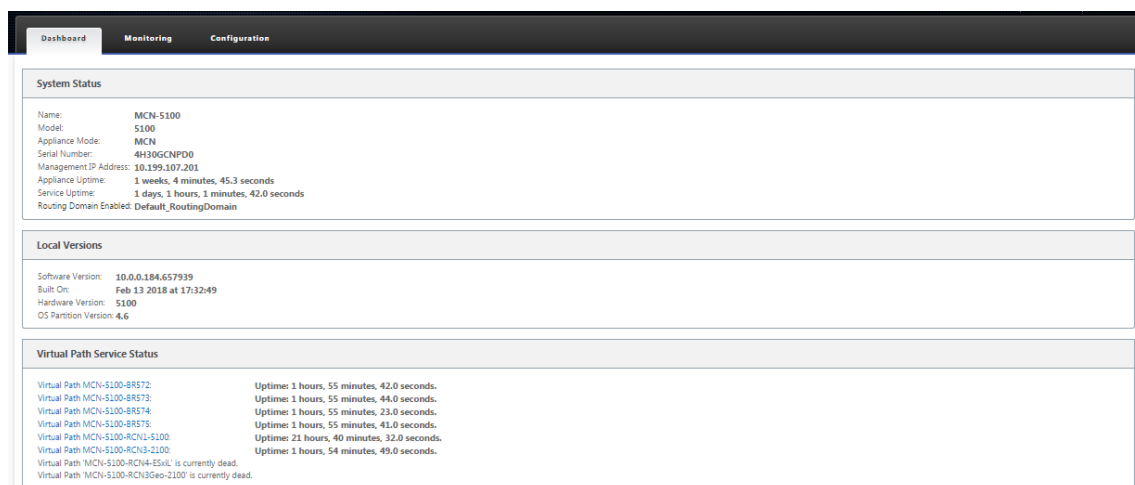


16. **[完了]** をクリックしてウィザードを終了し、アクティベーション結果を表示します。

アクティベーションが完了したら、[アクティベーション] ページの [** 完了] をクリックして、[管理 Web Interface ダッシュボード] ページに戻ります。 **

これが初期展開でない場合、このページには、現在アクティブなバージョンのソフトウェアパッケージ、OS パーティション、および仮想パスのステータスに関する更新された情報が表示されます。これが初期インストールの場合、「監査アラート」アイコンと、Virtual WAN サービスが非アクティブまたは無効であることを示すステータスメッセージが表示されます。この場合、[仮想 WAN サービスの有効化](#)の説明に従って、サービスを手動で有効にする必要があります。

次の図は、アラート・アイコンとステータス・メッセージを表示するクライアントの ダッシュボード・ページのサンプルを示しています。



SD-WAN の初期展開を完了するための最後の手順は、仮想 WAN サービスを有効にすることです。手順については、「[仮想 WAN サービスの有効化](#)」セクションに記載されています。

CloudInit を使用して、OpenStack での Citrix SD-WAN Standard Edition のデプロイ

May 10, 2021

OpenStack 環境に Citrix SD-WAN Standard Edition (SE) を展開できるようになりました。このためには、Citrix SD-WAN イメージが構成ドライブ機能をサポートしている必要があります。

メモ

構成ドライブ機能をサポートする Citrix イメージを作成します。

構成ドライブ機能では、管理ネットワーク経由で Citrix Orchestrator との通信を確立するために、次のパラメーター構成がサポートされます。

- 管理 IPv4 アドレス
- 管理 Gateway
- Name-server1
- Name-server2
- シリアル番号-認証 に使用され、新しいインスタンスに再使用する必要があります。クラウドで渡されたシリアル番号は、VPX インスタンスで自動生成されたトライアル番号を上書きする必要があります。

注

- シリアル番号を再利用するために、OpenStack 上で実行される SD-WAN に init スクリプトが組み込まれ、/etc/default/family のシリアル番号を変更します。
- Orchestrator には、SD-WAN アプライアンスが機能する一意のシリアル番号が必要です。

Cloudinit スクリプトは、設定ドライブを備えた OpenStack での SD-WAN デプロイメントのコンテキスト化をサポートします。

コンテキスト化の過程で、インフラストラクチャはコンテキストを仮想マシンで使用可能にし、仮想マシンはコンテキストを解釈します。コンテキスト化では、仮想マシンは特定のサービスを開始したり、ユーザーを作成したり、ネットワークと構成パラメータを設定したりできます。

OpenStack の SD-WAN インスタンスの場合、ユーザーからの管理 IP、DNS、およびシリアル番号に必要な入力。Cloudinit スクリプトはこれらの入力を解析し、指定された情報を使用してインスタンスをプロビジョニングします。

OpenStack クラウド環境でインスタンスを起動する場合、Citrix SD-WAN アプライアンスは、起動時のインスタンスの自動構成をサポートするために、ユーザーデータと CloudInit という 2 つのテクノロジーをサポートする必要があります。

OpenStack 環境で SD-WAN SE を Provisioning するには、次の手順を実行します。

前提条件

[イメージ] に移動し、[イメージを作成] をクリックします。

- イメージ名 -イメージ名を指定します。
- 「画像の説明」 -画像の説明を追加します。
- ファイル -ローカルドライブから kvm.qcow2 イメージファイルを参照して選択します。
- フォーマットドロップダウンリストから QCOW2 -QEMU エミュレータのディスクフォーマットを選択します。

[**Create Image**] をクリックします。

ネットワークポートとネットワークポートの両方が最初に作成され、定義済みである必要があります。ネットワーク・ポートを作成するには、次の手順に従います。

1. [ネットワーク] で [ネットワーク] を選択し、[ポート] タブに移動します。
2. [ポートの作成] をクリックし、必要な詳細を入力し、[作成] をクリックします。

Create Port ✕

Info

Security Groups

Name

Description:

You can create a port for the network. If you specify device ID to be attached, the device specified will be attached to the port created.

☒ **Enable Admin State**

Device ID ?

Device Owner ?

Specify IP address or subnet ?

Fixed IP Address ▼

Fixed IP Address * ?

MAC Address ?

☒ **Port Security** ?

VNIC Type ?

Normal ▼

Cancel

Create

[固定 IP アドレス] を選択した場合は、新しいポートのサブネット IP アドレスを指定する必要があります。

Project
API Access
Compute
Volumes
Network
Network Technology
Networks
Routers
Security Groups
Floating IPs
Trunks
Object Store
Admin

Project / Network / Networks / public
public
Edit Network
Overview Subnets Ports
Filter Create Port Delete Ports
Displaying 12 items

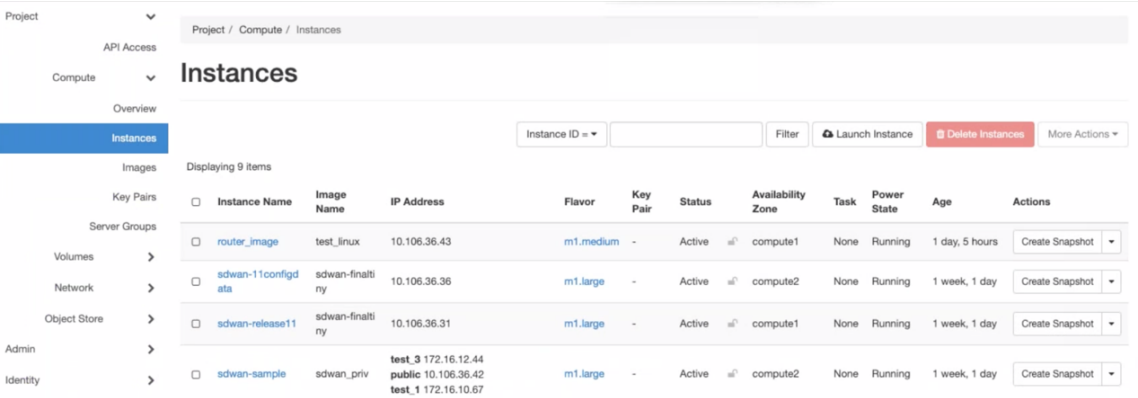
Name	Fixed IPs	MAC Address	Attached Device	Status	Admin State	Actions
Mgt-Port	10.106.36.41	fa:16:3e:24:8a:8c	Detached	Down	UP	Edit Port
(0b1273e8-1205)	10.106.36.31	fa:16:3e:c4:bc:eb	compute:compute1	Active	UP	Edit Port
test1	10.106.36.36	fa:16:3e:52:2d:8b	compute:compute2	Active	UP	Edit Port
tiny_mgmt	10.106.36.44	fa:16:3e:8d:83:04	Detached	Down	UP	Edit Port

ポートが作成され、どのデバイスにも接続されていないので、現在のステータスは [Detached] と表示されま

す。

OpenStack インスタンスを作成して、config-drive を有効にし、user_data を渡します。

3. OpenStack にログインし、インスタンスを設定します。



4. kvm.qcow2.gz ファイルをダウンロードし、解凍します。

5. [インスタンス] に移動し、[インスタンスの起動] をクリックします。

注:

[Inst ances] に戻り、[Launch Instance] をクリックするか、イメージを作成したら [Images] 画面から [Launch] をクリックします。

<input type="checkbox"/>	>	admin	sdwan-finaltiny	Image	Active	Public	No	QCOW2	1.33 GB	Launch
<input type="checkbox"/>	>	admin	sdwan_mtu_check	Image	Active	Public	No	QCOW2	1.32 GB	Launch
<input type="checkbox"/>	>	admin	sdwan_priv	Image	Active	Public	No	QCOW2	1.29 GB	Launch

6. [詳細] タブで、次の情報を入力します。

- 「インスタンス名」ーインスタンスのホスト名を指定します。
- [Des cription] ーインスタンスの説明を追加します。
- [Av ailability Zone] ーインスタンスをデプロイするアベイラビリティゾーンをドロップダウンリストから選択します。
- 「カウント」ーインスタンス数を入力します。この数を増やすと、同じ設定で複数のインスタンスを作成できます。[次へ] をクリックします。

Launch Instance

Details

Source *

Flavour *

Networks *

Network Ports

Security Groups

Key Pair

Configuration

Server Groups

Scheduler Hints

Metadata

Please provide the initial hostname for the instance, the availability zone where it will be deployed, and the instance count. Increase the Count to create multiple instances with the same settings.

Instance Name *

sdwan-openstack

Description

Availability Zone

Any Availability Zone

Count *

1

Total Instances (30 Max)

40%

11 Current Usage

1 Added

18 Remaining

✕ Cancel

< Back

Next >

Launch Instance

7. [ソース] タブで、[新しいボリュームの作成] で [いいえ] を選択し、[次へ] をクリックします。インスタンスソースは、インスタンスの作成に使用されるテンプレートです。

Launch Instance

Details

Source *

Flavour *

Networks *

Network Ports

Security Groups

Key Pair

Configuration

Server Groups

Scheduler Hints

Metadata

Instance source is the template used to create an instance. You can use an image, a snapshot of an instance (image snapshot), a volume or a volume snapshot (if enabled). You can also choose to use persistent storage by creating a new volume.

Select Boot Source

Image

Create New Volume

Yes

No

Allocated

Name	Updated	Size	Type	Visibility
Select an item from Available items below				

▼ Available 10

Select one

Q Click here for filters or full text search.

Name	Updated	Size	Type	Visibility	
➤ cirros	8/7/19 9:25 PM	12.65 MB	qcow2	Public	↑
➤ sdwan-finaltiny	11/7/19 10:42 AM	1.33 GB	qcow2	Public	↑
➤ sdwan_mtu_check	8/19/19 1:34 PM	1.32 GB	qcow2	Public	↑
➤ sdwan_priv	11/5/19 10:34 AM	1.29 GB	qcow2	Public	↑
➤ SDWAN_VPX_IMG_NEW	8/8/19 8:31 PM	1.31 GB	qcow2	Public	↑
➤ test_branch_1	10/4/19 10:07 AM	1.72 GB	qcow2	Public	↑
➤ test_brnach_2	10/4/19 10:08 AM	1.72 GB	qcow2	Public	↑
➤ test_dynamips	10/4/19 10:06 AM	1.72 GB	qcow2	Public	↑
➤ test_linux	10/4/19 10:07 AM	1.72 GB	qcow2	Public	↑
➤ test_mcn	10/4/19 10:08 AM	1.72 GB	qcow2	Public	↑

✕ Cancel

< Back

Next >

Launch Instance

8. インスタンスの [フレーバー] を選択し、[次へ] をクリックします。インスタンスに選択したフレーバーによって、インスタンスのコンピューティング、ストレージ、およびメモリ容量が管理されます。

メモ

選択するフレーバーには、作成しようとしているインスタンスのタイプをサポートするのに十分なリソースが割り当てられている必要があります。インスタンスに十分なリソースを提供していないフレーバーが、使用可能なテーブルで黄色の警告アイコンで識別されます。

管理者は、フレーバーの作成と管理を担当します。割り当てる矢印 (右側) をクリックします。

Launch Instance

Details

Source *

Flavour

Networks *

Network Ports

Security Groups

Key Pair

Configuration

Server Groups

Scheduler Hints

Metadata

Flavours manage the sizing for the compute, memory and storage capacity of the instance.

Allocated

Name	VCPUS	RAM	Total Disk	Root Disk	Ephemeral Disk	Public
> m1.large	4	8 GB	80 GB	80 GB	0 GB	Yes

Available 4

Select one

Q Click here for filters or full text search.

Name	VCPUS	RAM	Total Disk	Root Disk	Ephemeral Disk	Public
> m1.tiny	1	512 MB	1 GB	1 GB	0 GB	Yes
> m1.small	1	2 GB	20 GB	20 GB	0 GB	Yes
> m1.medium	2	4 GB	40 GB	40 GB	0 GB	Yes
> m1.xlarge	8	16 GB	160 GB	160 GB	0 GB	Yes

Cancel

< Back

Next >

Launch Instance

9. ネットワークを選択し、[**Next**] をクリックします。ネットワークは、インスタンスの通信チャンネルを提供します。

メモ

アドミニストレータがプロバイダのネットワークを作成し、これらのネットワークはデータセンター内の既存の物理ネットワークにマップされます。同様に、プロジェクトネットワークはユーザによって作成され、これらのネットワークは完全に分離され、プロジェクト固有です。

Launch Instance

Details

Source *

Flavour

Networks

Network Ports

Security Groups

Key Pair

Configuration

Server Groups

Scheduler Hints

Metadata

Networks provide the communication channels for instances in the cloud.

▼ Allocated 1

Select networks from those listed below.

	Network	Subnets Associated	Shared	Admin State	Status	
1	public	public_subnet	Yes	Up	Active	▼

▼ Available 30

Select at least one network

Q

Click here for filters or full text search.

×

	Network	Subnets Associated	Shared	Admin State	Status	
>	08c39ca9-c86e-4e80-8dd2-5b775497069c	09408ac1-6dfb-4381-bd2b-34c128f5280c	No	Up	Active	↑
>	0ce9e8b1-ad5d-4210-87dc-62917c827c17	76268f54-7faf-45ff-ae2a-b97fb72e3d6b	No	Up	Active	↑
>	26a6e41d-6f64-4f6b-b510-810938d9a669	c81c3a0e-e84e-46b1-9e29-3300b8e7323c	No	Up	Active	↑
>	272165f0-443b-4f81-9358-38a9e2ea0fa3	373b775b-9576-484d-abd8-9011362284da	No	Up	Active	↑
>	test_4	subnet_4	No	Up	Active	↑
>	8b69e4a3-c47a-4821-bb17-09aca96a4fe9	ab3c53f6-ca4b-4958-aedf-7c444b21c257	No	Up	Active	↑
>	test_1	subnet_1	No	Up	Active	↑
>	Hw_provider3_vlan20	provider3_subnet	No	Up	Active	↑
>	f1d4edbe-8272-400c-bba1-c350864eecd	366f5024-cf0a-4648-8053-c3fe946df958	No	Up	Active	↑
>	f3158a09-c8dc-421a-9e8f-04814860b955	736e9da4-7526-4072-aa93-666071df24f8	No	Up	Active	↑
>	test_3	subnet_3	No	Up	Active	↑
>	network_ipv6	subnetwork_ipv6 ipv4_subnet	No	Up	Active	↑

✕ Cancel

< Back

Next >

Launch Instance

10. インスタンスのネットワークポートを選択し、[**Next**] をクリックします。ネットワークポートは、インスタンスへの追加の通信チャネルを提供します。

メモ

ネットワークの代わりにポートを選択することも、両方のポートを混在させることもできます。

Launch Instance

Details

Source *

Flavour

Networks

Network Ports

Security Groups

Key Pair

Configuration

Server Groups

Scheduler Hints

Metadata

Ports provide extra communication channels to your instances. You can select ports instead of networks or a mix of both.

▼ Allocated 1

1

tiny_mgmt

10.106.36.44 on subnet public_subnet

Up

Down

↓

▼ Available 31

Filter

Name	IP	Admin State	Status	
> 3865f021-d8df-40a9-964a-7bb7f3728353	192.168.234.239 on subnet	Up	Down	↑
> 3f7888d2-dd2b-487d-ad88-6cf3261ebf8b	192.168.234.113 on subnet	Up	Down	↑
> 7847377d-6f82-4a7f-9e8d-26703bfc7b0b	192.168.234.240 on subnet	Up	Down	↑
> 2bd26300-4af2-4503-8ec8-728ad5967c5f	192.168.237.88 on subnet	Up	Down	↑
> 6ca1aeab-4b38-41f3-86cc-8973a3bfc3bd	192.168.240.223 on subnet	Up	Down	↑
> 9dc0d02b-7933-4689-92a3-18c3177c7c0d	192.168.240.251 on subnet	Up	Down	↑
> c378ba39-0c61-4e35-8a2c-0419fa8c2989	192.168.240.4 on subnet	Up	Down	↑
> 958ad235-94b0-4ccd-8f07-88539bc5b584	172.16.22.1 on subnet	Up	Down	↑
> Mgt-Port	10.106.36.41 on subnet public_subnet	Up	Down	↑

✕ Cancel

< Back

Next >

Launch Instance

11. [構成] に移動し、[ファイルの選択] をクリックします。user_data ファイルの 管理 IP、DNS、およびシリアル番号 情報を表示できます。
12. [構成ドライブ] チェックボックスを有効にします。構成ドライブを有効にすると、ユーザーメタデータをイメージ内に配置できます。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

242

Launch Instance

You can customise your instance after it has launched using the options available here. "Customisation Script" is analogous to "User Data" in other systems.

Load Customisation Script from a file

Choose file No file chosen

Customisation Script (Modified) Content size: 213 bytes of 16.00 KB

```
#config
management_ip
address 10.106.36.43
netmask 255.255.255.0
gateway 10.106.36.1
dns
```

Disk Partition

Automatic

☒ Configuration Drive

✕ Cancel < Back Next > Launch Instance

13. [インスタンスの起動] をクリックします。

210 SE LTE アプライアンスでの LTE 機能の構成

September 26, 2023

LTE 接続を使用して、Citrix SD-WAN 210-SE LTE アプライアンスをネットワークに接続できます。このトピックでは、モバイルブロードバンド設定の構成、LTE 用のデータセンターおよびブランチアプライアンスの構成などについて詳しく説明します。Citrix SD-WAN 210-SE LTE ハードウェアプラットフォームの詳細については、「[Citrix SD-WAN 210Standard Edition アプライアンス](#)」を参照してください。

注

LTE 接続は、SIM キャリアまたはサービスプロバイダーのネットワークによって異なります。

Citrix SD-WAN 210-SE LTE の使用を開始する

1. Citrix SD-WAN 210-SE LTE の SIM カードスロットに SIM カードを挿入します。

注:

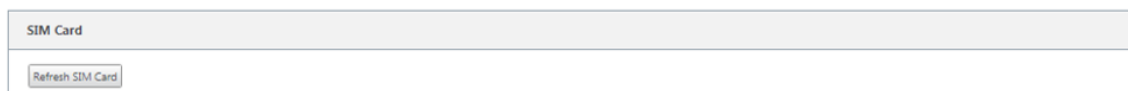
標準または 2FF SIM カード (15x25 mm) のみがサポートされています。

2. アンテナを Citrix SD-WAN 210-SE LTE アプライアンスに固定します。詳細については、「[LTE アンテナの取り付け](#)」を参照してください。

3. アプライアンスの電源を入れます。

注

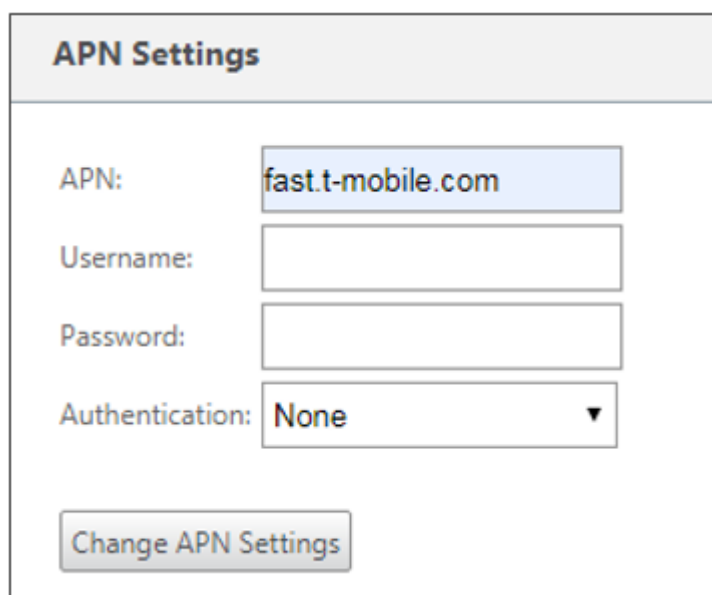
すでに電源が入って起動しているアプライアンスに SIM を挿入した場合は、[構成] > [アプライアンスの設定] > [ネットワークアダプタ] > [モバイルブロードバンド] > [SIM カード] に移動し、[SIM カードの更新] をクリックします。



4. APN 設定を構成します。SD-WAN GUI で設定 > アプライアンス設定 > ネットワークアダプタ > モバイルブロードバンド > **APN** 設定にナビゲートして下さい。

注:

APN 情報をキャリアから入手します。

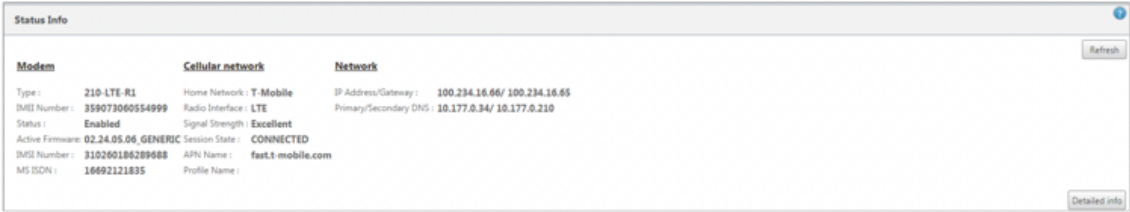


5. 通信事業者から提供された **APN**、ユーザー名、パスワード、認証を入力します。PAP、CHAP、PAPCHAP 認証プロトコルから選択できます。通信事業者が認証タイプを提供していない場合は、[なし] に設定します。

6. [**APN** 設定の変更] をクリックします。

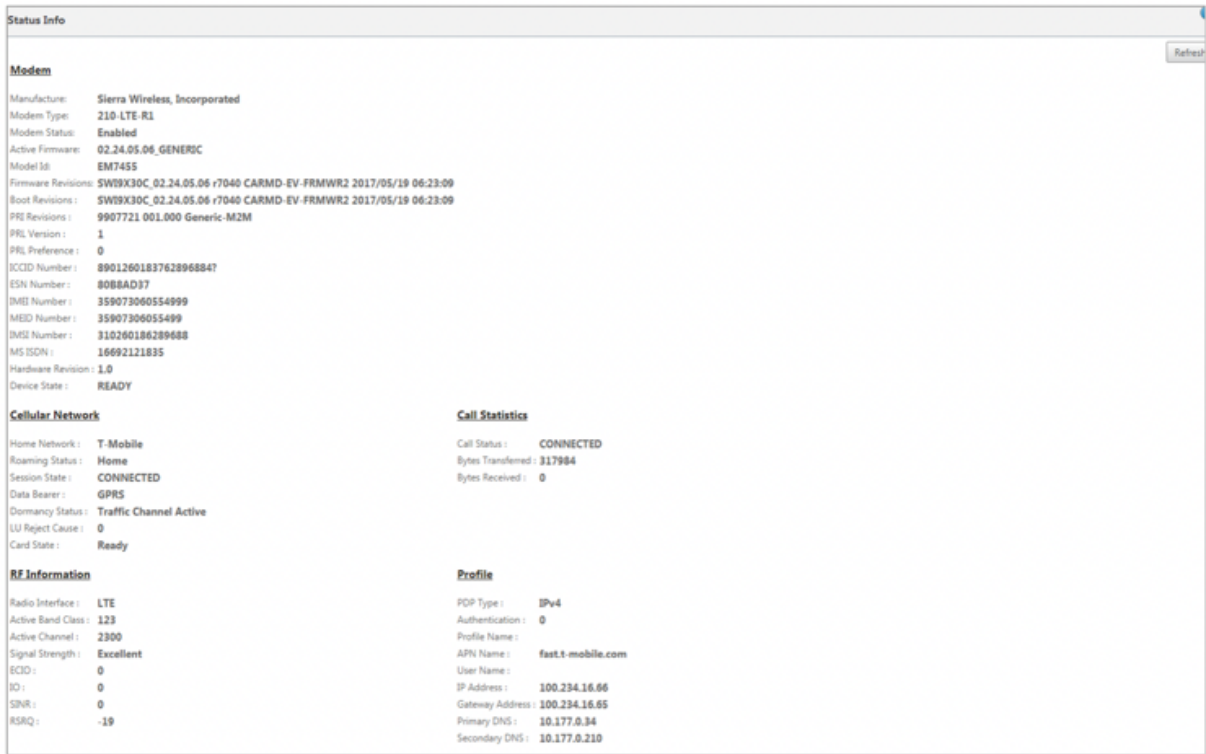
7. SD-WAN アプライアンス GUI で、設定 > アプライアンス設定 > ネットワークアダプタ > モバイルブロードバンドにナビゲートして下さい。

モバイルブロードバンド設定のステータス情報を表示できます。



以下は、いくつかの有用なステータス情報です。

- 動作モード：モデムの状態を表示します。
- アクティブ **SIM**：アクティブになることができる SIM はいつでも、1 つのみです。現在アクティブになっている SIM を表示した。
- カードの状態：Present は SIM が正しく挿入されていることを示します。
- 信号強度：信号強度の品質-優秀、良好、公正、不良、または信号なし。
- ホームネットワーク：挿入された SIM のキャリア。
- **APN** 名:LTE モデムが使用するアクセスポイント名。
- セッション状態：Connected は、デバイスがネットワークに参加したことを示します。セッション状態が切断されている場合は、データプランが有効になっているかどうかでアカウントがアクティベートされているかどうかを通信事業者に確認してください。



SIM ピン

PIN でロックされている SIM カードを挿入した場合、SIM ステータスは「有効」で、「未確認」** 状態になります。SIM PIN で認証されるまで、SIM カードは使用できません。SIM PIN は通信事業者から入手できます。

SIM PIN 操作を実行するには、[構成] > [アプライアンスの設定] > [ネットワークアダプタ] > [モバイルブロードバンド] > [SIM PIN] に移動します。

The screenshot shows the 'SIM PIN' configuration page. Under the 'SIM PIN Status' section, the 'PIN State' is 'Enabled and Not Verified', 'PIN Tries' is 3, and 'PUK Tries' is 10. There are three buttons: 'Disable PIN', 'Verify PIN', and 'Modify PIN'.

PIN を確認をクリックします。通信事業者から提供された SIM PIN を入力し、[**PIN の確認**] をクリックします。

The screenshot shows a dialog box for verifying the SIM PIN. It has a title bar with a close button. Inside, there is a label 'SIM PIN:' followed by a text input field. Below the input field is a 'Verify PIN' button.

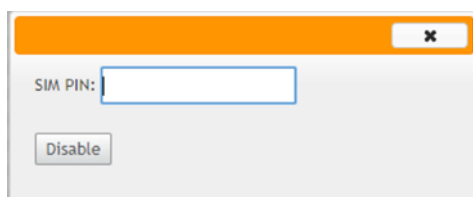
ステータスが [有効] および [確認済み] に変わります。

The screenshot shows the 'SIM PIN' configuration page after verification. The 'PIN State' is now 'Enabled and Verified', 'PIN Tries Remaining' is 3, and 'PUK Tries Remaining' is 10. The 'Verify PIN' button is now highlighted in blue.

SIM PIN を無効にする

SIM PIN が有効で確認されている SIM の SIM PIN 機能を無効にすることができます。

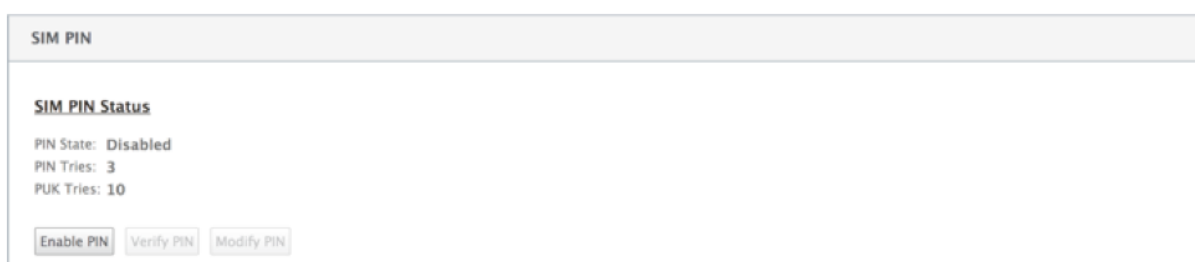
The screenshot shows the 'SIM PIN' configuration page after disabling the PIN. The 'PIN State' is 'Enabled and Verified', 'PIN Tries Remaining' is 3, and 'PUK Tries Remaining' is 10. The 'Disable PIN' button is now highlighted in blue.

A small dialog box with an orange header bar containing a close button (X). Below the header, there is a text input field labeled "SIM PIN:". Below the input field is a button labeled "Disable".

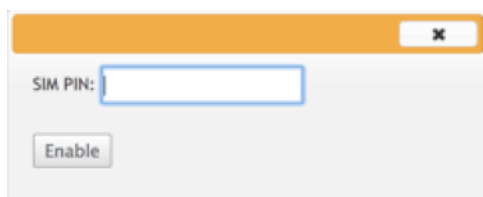
PIN を無効にするをクリックします。**SIM PIN** を入力して、[無効にする] をクリックします。

SIM PIN を有効にする

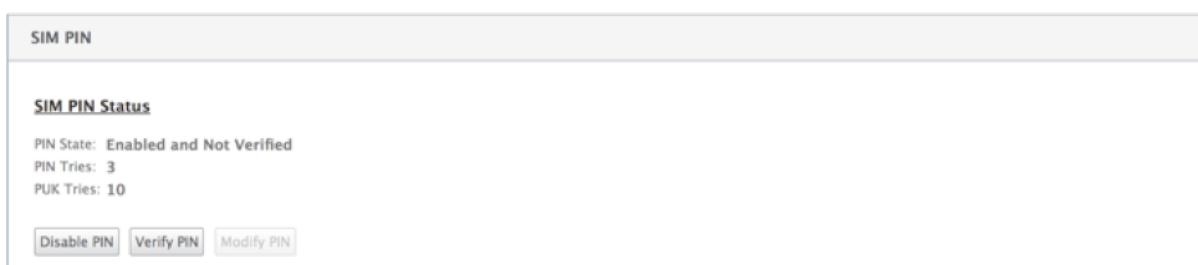
SIM PIN は、無効になっている SIM に対して有効にすることができます。

A panel titled "SIM PIN" with a sub-header "SIM PIN Status". Below the sub-header, the status is shown as "PIN State: Disabled", "PIN Tries: 3", and "PUK Tries: 10". At the bottom, there are three buttons: "Enable PIN", "Verify PIN", and "Modify PIN".

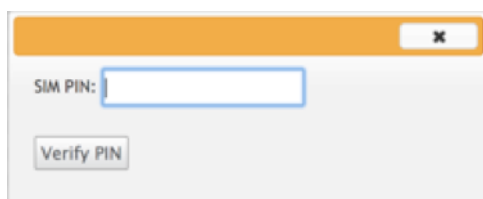
PIN を有効にするをクリックします。通信事業者から提供された SIM PIN を入力し、[有効] をクリックします。

A small dialog box with an orange header bar containing a close button (X). Below the header, there is a text input field labeled "SIM PIN:". Below the input field is a button labeled "Enable".

SIM PIN の状態が [有効] および [未確認] に変わると、PIN が検証されず、PIN が検証されるまで LTE 関連の操作を実行できなくなります。

A panel titled "SIM PIN" with a sub-header "SIM PIN Status". Below the sub-header, the status is shown as "PIN State: Enabled and Not Verified", "PIN Tries: 3", and "PUK Tries: 10". At the bottom, there are three buttons: "Disable PIN", "Verify PIN", and "Modify PIN".

PIN を確認をクリックします。通信事業者から提供された SIM PIN を入力し、[**PIN** の確認] をクリックします。

A small dialog box with an orange header bar containing a close button (X). Below the header, there is a text input field labeled "SIM PIN:". Below the input field is a button labeled "Verify PIN".

SIM PIN の変更

PIN が有効で確認済みの状態になったら、PIN の変更を選択できます。

The screenshot shows the 'SIM PIN' section of the interface. It has a title bar 'SIM PIN' and a sub-header 'SIM PIN Status'. Below this, it displays the following information: 'PIN State: Enabled and Verified', 'PIN Tries Remaining: 3', and 'PUK Tries Remaining: 10'. At the bottom, there are three buttons: 'Disable PIN', 'Verify PIN', and 'Modify PIN'. The 'Modify PIN' button is highlighted with a blue border.

PIN の変更をクリックします。通信事業者から提供された SIM PIN を入力します。新しい SIM PIN を入力し、確認します。**PIN** の変更をクリックします。

The screenshot shows a dialog box for modifying the SIM PIN. It has a title bar with a close button. Inside, there are three input fields: 'Old SIM PIN:', 'New SIM PIN:', and 'Confirm New SIM PIN:'. Below these fields is a button labeled 'Modify PIN'.

SIM のブロック解除

SIM PIN を忘れた場合、通信事業者から取得した SIM PUK を使用して SIM PIN をリセットすることができます。

The screenshot shows the 'Status Info' section of the interface. It has tabs for 'IP Address', 'Ethernet', and 'Mobile Broadband'. The 'Mobile Broadband' tab is selected. Below the tabs, it displays the following information: 'This SIM Card is Blocked. Please contact the carrier service for a PUK code to unblock the SIM card.', 'PIN State: Blocked', 'PIN Tries: 3', and 'PUK Tries: 10'. At the bottom, there is a button labeled 'Unblock'.

SIM のブロックを解除するには、[ブロック解除] をクリックします。キャリアから取得した **SIM PIN** と **SIM PUK** を入力し、[ブロック解除] をクリックします。

The screenshot shows a dialog box for unblocking the SIM. It has a title bar with a close button. Inside, there are two input fields: 'SIM PIN:' and 'SIM PUK:'. Below these fields is a button labeled 'Unblock'.

注:

SIM カードは、SIM のブロックを解除しながら、PUK の 10 回の試行に失敗して永久にブロックされます。新しい SIM カードについては、通信事業者のサービスプロバイダーにお問い合わせください。



Configuration > Appliance Settings > Network Adapters

IP Address Ethernet Mobile Broadband

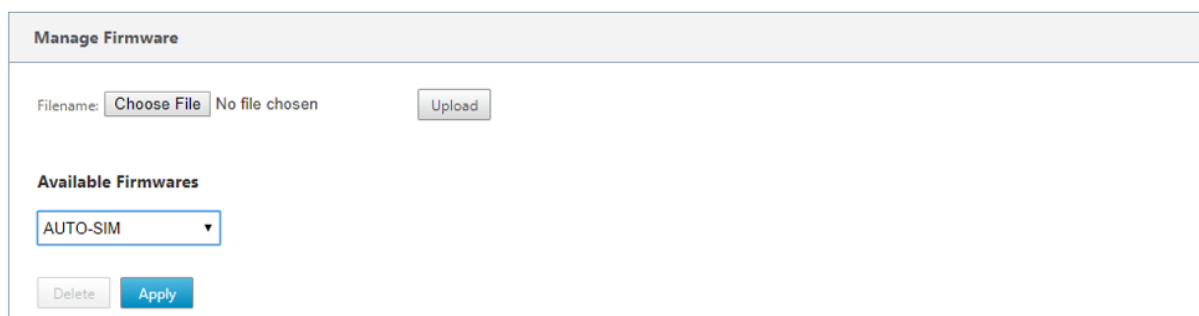
Status Info

This SIM Card is Permanently Blocked. Please contact the carrier service for a new SIM card.

ファームウェアの管理

LTE が有効になっているすべてのアプライアンスには、使用可能なファームウェアのセットがあります。既存のファームウェアのリストから選択するか、ファームウェアをアップロードして適用することができます。

使用するファームウェアが不明な場合は、AUTO-SIM オプションを選択して、LTE モデムが挿入された SIM カードに基づいて最も一致するファームウェアを選択できるようにします。



Manage Firmware

Filename: Choose File No file chosen Upload

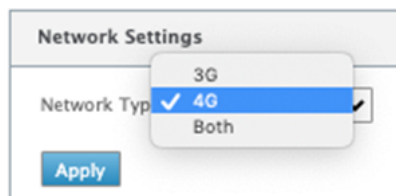
Available Firmwares

AUTO-SIM

Delete Apply

ネットワーク設定

内部 LTE モデムをサポートする Citrix SD-WAN アプライアンスのモバイルネットワークを選択できます。サポートされるネットワークは、3G、4G、またはその両方です。



Network Settings

Network Type 3G 4G Both

Apply

ローミング

ローミングオプションは、LTE アプライアンスではデフォルトで有効になっています。無効にすることもできます。

A screenshot of the 'Roaming' configuration panel. It has a title bar 'Roaming'. Below it, there is a label 'Roaming:' followed by a dropdown menu currently showing 'Disabled'. At the bottom of the panel is a blue 'Apply' button.

モデムの有効化/無効化

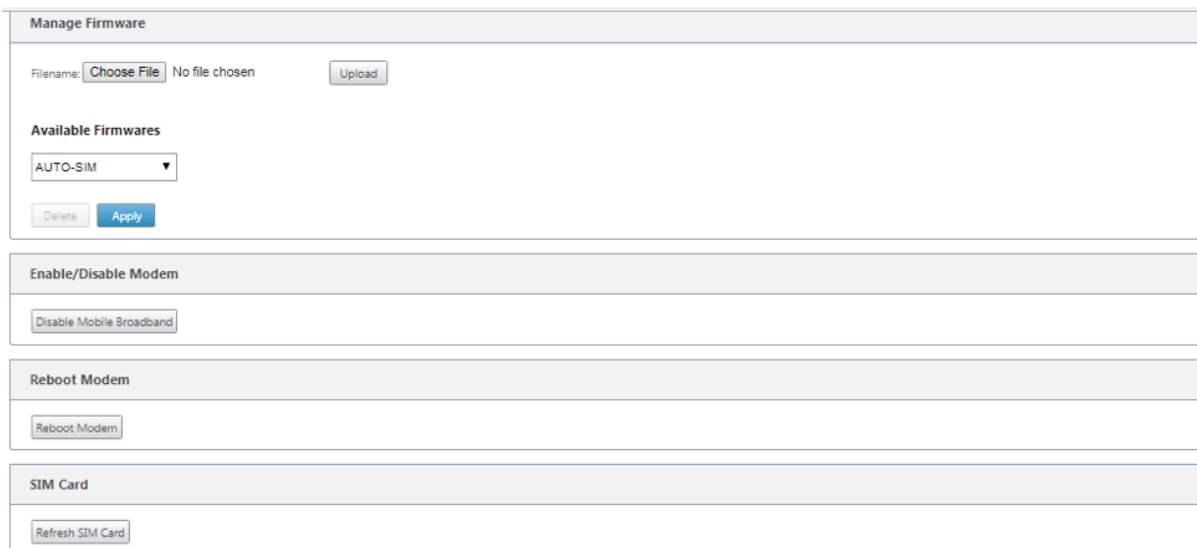
LTE 機能を使用する目的に応じて、モデムを有効または無効にします。デフォルトでは、LTE モデムは有効になっています。

モデムの再起動

モデムをリブートします。再起動操作が完了するまで、最大 3～5 分かかる場合があります。

SIM のリフレッシュ

このオプションは、SIM カードをホットスワップして 210-SE LTE モデムで新しい SIM カードを検出する場合に使用します。

A screenshot of the LTE management interface. It contains four sections: 1. 'Manage Firmware' with a file upload area (Filename: Choose File, No file chosen, Upload button) and an 'Available Firmwares' dropdown (currently showing AUTO-SIM) with Delete and Apply buttons. 2. 'Enable/Disable Modem' with a 'Disable Mobile Broadband' button. 3. 'Reboot Modem' with a 'Reboot Modem' button. 4. 'SIM Card' with a 'Refresh SIM Card' button.

Citrix SD-WAN Center を使用して、ネットワーク内のすべての LTE サイトをリモートで表示および管理できます。詳細については、[リモート LTE サイト管理を参照してください](#)。

CLI を使用した LTE 機能の設定

CLI を使用して 210-SE LTE モデムを設定するには。

- 1. Citrix SD-WAN アプライアンスコンソールにログインします。
- 2. プロンプトで、CLI インターフェイスにアクセスするためのユーザー名とパスワードを入力します。
- 3. プロンプトで、コマンド **lte** を入力します。>**help** と入力します。これにより、設定に使用できる LTE コマンドのリストが表示されます。

```
site210>lte
lte>help
status                # Show status
show                  # Show settings
disable               # Disable LTE modem
enable                # Enable LTE modem
apn <apn> [<user name> [<password> [<PAP|CHAP|PAPCHAP>]]] # Set APN
sim-power <off|on|reset> # Off, on, reset SIM card power
sim-pin <show>         # SIM card pin status
sim-pin <verify|disable|enable> <sim pin> # Verify/Disable/Enable SIM card PIN
sim-pin <modify> <old pin> <new pin> # Modify SIM card PIN
sim-pin <unblock> <sim puk> <sim pin> # Unblock SIM card PIN
reboot                # Reboot modem
ping                  # Check if modem manager ready
list-fw               # List available firmware
apply-fw <fw>        # Apply the specified firmware
```

次の表に、**LTE** コマンドの説明を示します。

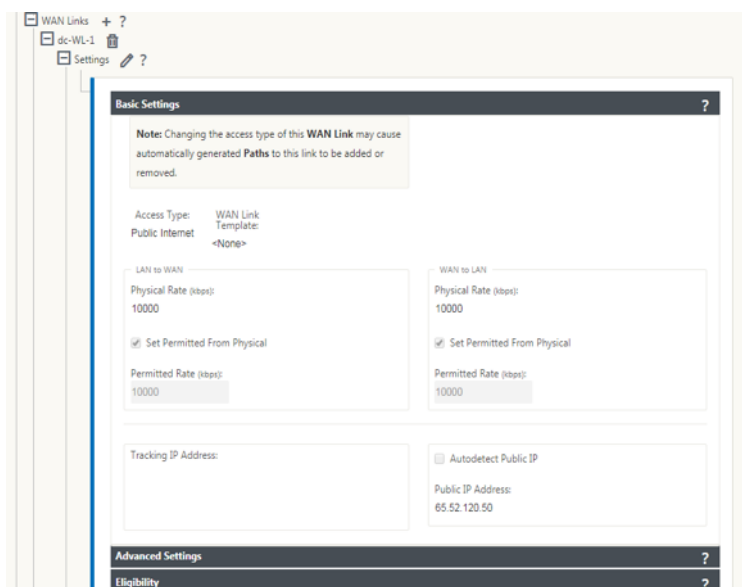
コマンド	説明
ヘルプ {lte>help}	使用可能な LTE コマンドとパラメータをリストします
ステータス {lte>status}	LTE 接続ステータスを表示します。
{lte>show} を表示	LTE 設定を表示します。
{lte>Disable} を無効にする	LTE モデムを無効にします。
{lte>Enable} を有効にする	LTE モデムを有効にします。
APN {lte>apn}	APN 設定情報を設定します。
SIM 電源オフ、オン、リセット> {lte>sim-電源オフ、オン、リセット}	SIM カードの電源を切る、SIM カードの電源を入れ、SIM カードを更新する
SIM PIN {lte>sim-pin}	SIM カードの電源を切る、SIM カードの電源を入れ、SIM カードを更新する
再起動 {lte>reboot}	LTE モデムを再起動します
Ping {lte>ping}	LTE モデムの PING
list-FW {lte>list-FW}	R1 または R2 LTE モデムで使用可能なファームウェアの一覧を表示します。
Apply-fw {lte>apply-fw}	キャリア固有のファームウェアを適用

LTE 用の MCN の設定

210-LTE アプライアンスを MCN として設定することはできません。ただし、MCN が LTE ブランチアプライアンスと連携するには、MCN アプライアンスで次の設定を実行します。

MCN を設定するには、次の手順を実行します。

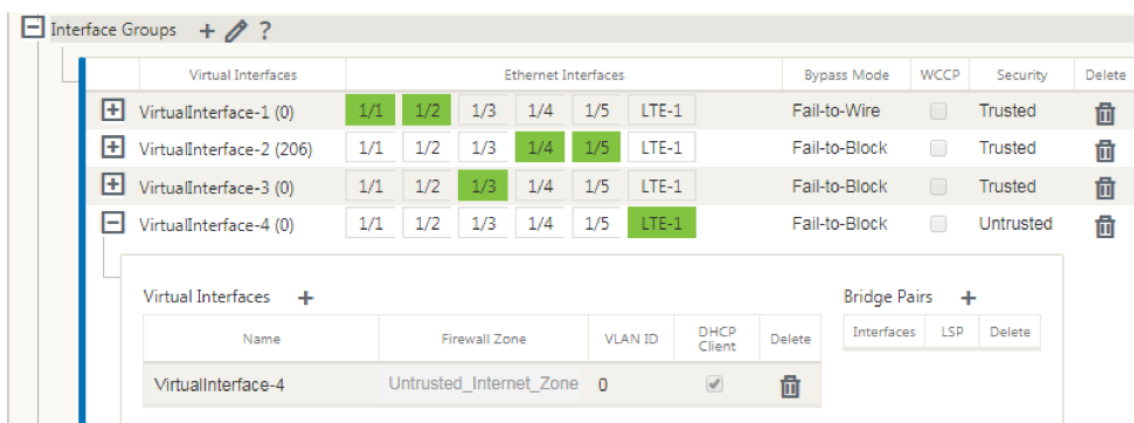
1. SD-WAN アプライアンスの GUI にログインします。[構成エディタ] に移動します。MCN サイトの設定を完了します。「[MCN の設定](#)」を参照してください。
2. WAN リンク設定の一部として、ルーティング可能なパブリック IP アドレスを指定してください。クライアントアプライアンスのパブリック IP アドレスを設定する必要はありません。



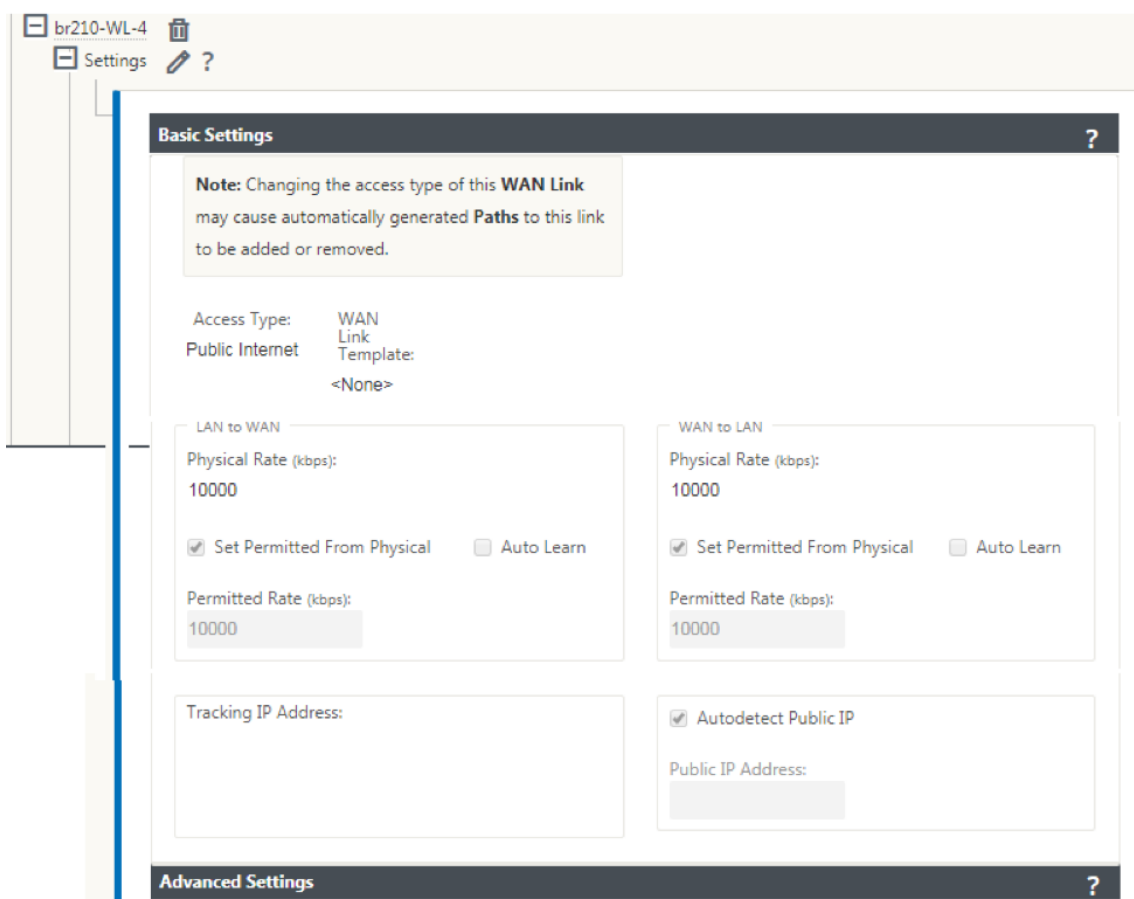
LTE のブランチを構成する

210-SE LTE アプライアンスをブランチサイトとして設定するには、次の手順を実行します。

1. SD-WAN アプライアンス GUI で、設定エディタに移動します。[ブランチの設定を参照してください](#)。
 - インターフェイスグループを作成します。
 - 次の項目を選択して、最大 1 つの仮想インターフェイスと 1 つのインターフェイスグループを作成し、LTE アダプタで WAN リンクを設定します。
 - イーサネットインターフェイス—LTE 1
 - セキュリティ：信頼できない（デフォルト）
 - DHCP クライアント：有効（デフォルト）



2. LTE インターフェイス用に作成された仮想インターフェイスを使用して WAN リンクを設定する場合は、WAN リンク設定の **AutoDetect Public IP** を有効にします。



3. デフォルトでは、LTE インターフェイスを使用して WAN リンクを設定しようとすると、WAN リンクは従量制リンクおよびラストリゾートスタンバイモードとしてマークされます。必要に応じて、これらのデフォルト設定を変更できます。

Advanced Settings	?
Eligibility	?
Metered/Standby Link	?
Metering	
<input checked="" type="checkbox"/> Enable Metering	
Data Cap (MB):	Billing Cycle:
0	Monthly ▼
Starting From: MM/DD/YYYY	
Standby	
Standby Mode:	Priority:
Last-Resort ▼	1 ▼

WAN リンクのアクセスインターフェイスの IP アドレスおよび Gateway アドレスは、DHCP を介してキャリアから情報を受信するため、設定する必要はありません。

Name	Virtual Interface	IP Address	Gateway IP Address	Virtual Path Mode	Proxy ARP	Delete
br-WL-1-AI-1	V2 ▼			Primary ▼	<input type="checkbox"/>	

Apply Revert

- 210-SE LTE アプライアンスに必要なブランチ設定の残りの部分を完了します。[ブランチの設定を参照してください](#)。
- SD-WAN ソフトウェアをアップロードして、変更管理を実行します。[変更管理の手順を参照してください](#)。
- ローカル変更管理プロセスを通じて構成をアクティブ化します。変更管理を実行すると、構成がアクティブ化され、必要な構成が適用されます。

LTE 経由のゼロタッチ展開

LTE 経由のゼロタッチ導入サービスを実現するための前提条件

- 210-SE LTE アプライアンス用のアンテナと SIM カードを取り付けます。
- SIM カードに有効なデータプランがあることを確認します。
- 管理ポートが接続されていないことを確認します。
 - 管理ポートが接続されている場合は、管理ポートを切断し、アプライアンスを再起動します。

- 管理インターフェイスで固定 IP アドレスが設定されている場合は、DHCP を使用して管理インターフェイスを設定し、設定を適用してから、管理ポートを切断し、アプライアンスを再起動する必要があります。

4. 210-SE アプライアンスの設定に、LTE インターフェイス用に定義されたインターネットサービスがあることを確認します。

アプライアンスの電源がオンになると、ゼロタッチ展開サービスは LTE ポートを使用して、管理ポートが接続されていない場合にのみ、最新の SD-WAN ソフトウェアおよび SD-WAN 構成を取得します。

SD-WAN センター GUI を使用して、210-SE LTE アプライアンスをゼロタッチ展開サービス用に展開および設定できます。

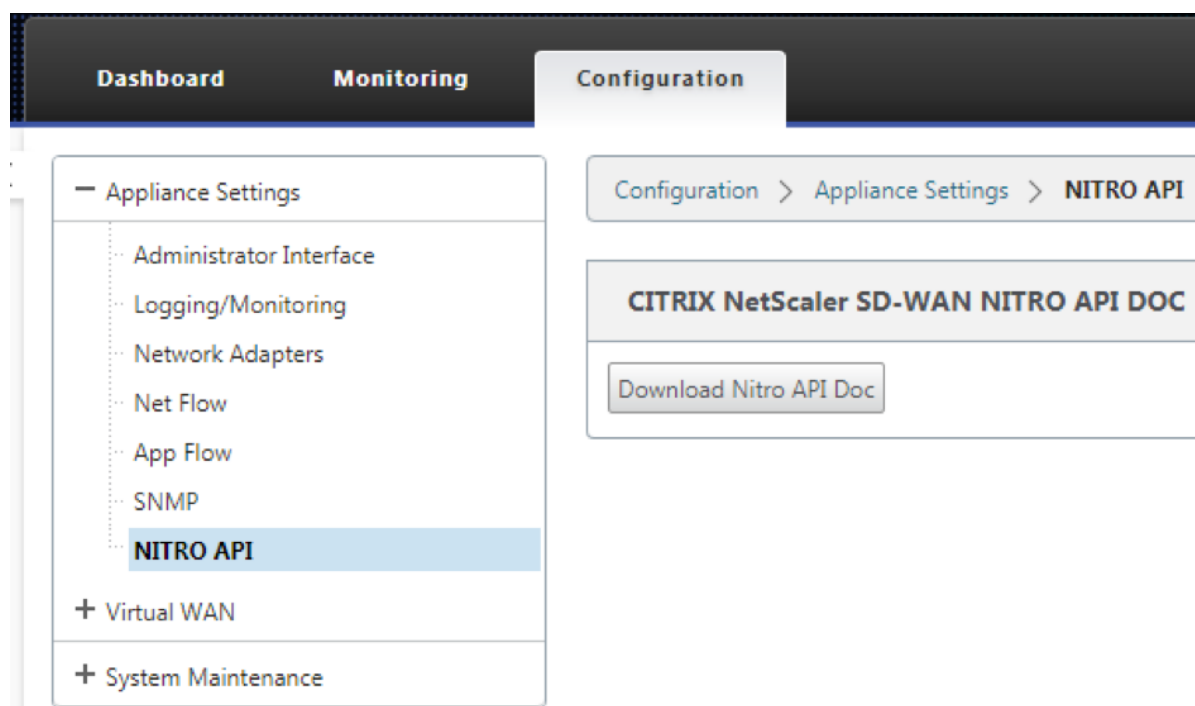
SD-WAN Center を使用した 210-SE LTE アプライアンスの展開と設定の詳細については、[ゼロタッチ展開手順を参照してください](#)。

210-SE LTE アプライアンスの管理インターフェイスを介したゼロタッチ導入サービス

管理ポートを接続し、他のすべての非 LTE [プラットフォームでサポートされている標準のゼロタッチ展開手順を使用します](#)。

LTE REST API

LTE REST API の詳細については、SD-WAN GUI に移動し、[構成] > [アプライアンスの設定] > [NITRO API] の順に移動します。[**Nitro API** ドキュメントのダウンロード] をクリックします。SIM PIN 機能用の REST API は、Citrix SD-WAN 11.0 で導入されています。



AT コマンド

AT コマンドは、LTE モデムの設定とステータスのモニタリングとトラブルシューティングに役立ちます。**AT** は **AtTension** の略称。すべてのコマンドラインが **at** で始まるので、AT コマンドと呼ばれます。LTE をサポートする Citrix SD-WAN プラットフォームモデルは、AT コマンドの実行をサポートします。AT コマンドはモデム固有であるため、AT コマンドのリストはプラットフォームによって異なります。

AT コマンドを実行するには、次の手順に従います。

1. Citrix SD-WAN アプライアンスコンソールにログインします。
2. プロンプトで、CLI インターフェイスにアクセスするためのユーザー名とパスワードを入力します。
3. プロンプトで「**lte**」と入力します。
4. **at** と入力し、AT コマンドを入力します。

以下はその例です：

- **at at+cpin** —SIM ステータス情報を提供します。

```
lte> at at+cpin?
Running at+cpin? command
AT command state: success
+CPIN: READY
OK
success
```

- で! **gstatus** -LTE モデムのステータス情報を提供します。

```
lte> at at!gstatus?
Running at!gstatus? command
AT command state: success
!GSTATUS:
Current Time: 1279298           Temperature: 62
Reset Counter: 1               Mode: ONLINE
System mode: LTE               PS state: Attached
LTE band: B5                   LTE bw: 10 MHz
LTE Rx chan: 2559             LTE Tx chan: 20559
LTE CA state: NOT ASSIGNED
EMM state: Registered          Normal Service
RRC state: RRC Connected
IMS reg state: Full Srv        IMS mode: Normal
PCC RxM RSSI: -73              RSRP (dBm): -112
PCC RxD RSSI: -73              RSRP (dBm): -107
Tx Power: --                   TAC: 1F00 (7936)
RSRQ (dB): -17.3               Cell ID: 00798912 (7964946)
SINR (dB): 0.2
OK
Success
```

- で! **impref?** -モデムのファームウェアとネットワークキャリア情報を提供します。

```
lte> at at!impref?
Running at!impref? command
AT command state: success
!IMPREF:
preferred fw version: 00.00.00.00
preferred carrier name: AUTO-SIM
preferred config name: AUTO-SIM_000.000_000
preferred subpri index: 000
current fw version: 02.33.03.00
current carrier name: VERIZON
current config name: VERIZON_002.079_001
current subpri index: 000
OK
success
```


110-LTE-WiFi アプライアンスでの LTE 機能の構成

November 8, 2021

LTE 接続を使用して、Citrix SD-WAN 110-LTE-WiFi アプライアンスをネットワークに接続できます。このトピックでは、モバイルブロードバンド設定の構成、LTE 用のデータセンターおよびブランチアプライアンスの構成などについて詳しく説明します。Citrix 110-LTE-WiFi ハードウェアプラットフォームについて詳しくは、「[Citrix SD-WAN 110 Standard Edition アプライアンス](#)」を参照してください。

注

LTE 接続は、SIM キャリアまたはサービスプロバイダーのネットワークによって異なります。

Citrix SD-WAN 110-LTE-WiFi の使用を開始する

1. アプライアンスの電源を入れ、Citrix SD-WAN 110-LTE-WiFi アプライアンスの SIM カードスロットに SIM カードを挿入します。

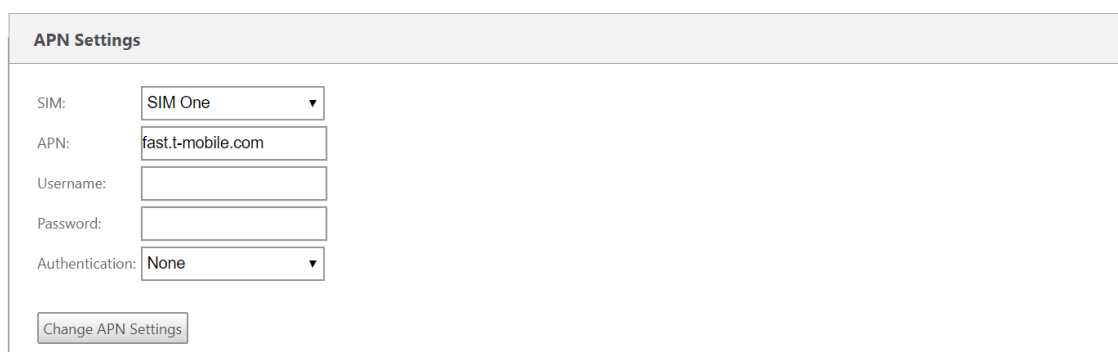
注

Citrix SD-WAN 110-LTE-WiFi アプライアンスは、2 つの標準を持っています (2FF) SIM スロット。マイクロ (3FF) およびナノ (4FF) サイズの SIM を使用するには、SIM アダプタを使用します。小さい SIM をアダプタにスナップします。アダプタは、フィールド交換可能ユニット (FRU) として Citrix から入手するか、SIM プロバイダから入手できます。

2. アンテナを Citrix SD-WAN 110-LTE-WiFi アプライアンスに固定します。詳細については、「[LTE アンテナの取り付け](#)」を参照してください。
3. アプライアンスの電源を入れます。
4. APN 設定を構成します。SD-WAN GUI で設定 > アプライアンス設定 > ネットワークアダプタ > モバイルブロードバンド > **APN** 設定にナビゲートして下さい。

注

キャリアから APN 情報を入手します。



APN Settings	
SIM:	<input type="text" value="SIM One"/>
APN:	<input type="text" value="fast.t-mobile.com"/>
Username:	<input type="text"/>
Password:	<input type="password"/>
Authentication:	<input type="text" value="None"/>
<input type="button" value="Change APN Settings"/>	

5. SIM カードを選択し、通信事業者から提供された **APN**、ユーザー名、パスワード、認証を入力します。PAP、CHAP、PAPCHAP 認証プロトコルから選択できます。通信事業者が認証タイプを提供していない場合は、[なし] に設定します。

注

これらのフィールドはすべてオプションです。

6. [**APN 設定の変更**] をクリックします。
7. SD-WAN アプライアンスの GUI で、[構成] > [アプライアンスの設定] > [ネットワークアダプタ] > [モバイルブロードバンド] に移動します。

モバイルブロードバンド設定のステータス情報を表示できます。

Modem	Cellular network	Network
Operating Mode: online	Home Network: airtel	IP Address/Gateway: 100.105.88.189/100.105.88.190
IMEI Number: 867698040397609	Radio Interface: lte	Primary/Secondary DNS: 125.22.47.102/59.144.144.106
Active SIM: SIM One	Signal Strength: Excellent	
IMSI Number: 404450986042323	Session State: connected	
ICCID Number: 8991000902637718627f	APN Name: absent	
Card State (SIM One): present	Card State (SIM Two): absent	

以下は、いくつかの有用なステータス情報です。

- 動作モード: モデムの状態を表示します。
- アクティブ **SIM**: アクティブになることができる SIM はいつでも、1 つのみです。現在アクティブになっている SIM を表示した。
- カードの状態: Present は SIM が正しく挿入されていることを示します。
- 信号強度: 信号強度の品質-優秀、良好、公正、不良、または信号なし。
- ホームネットワーク: 挿入された SIM のキャリア。
- APN** 名: LTE モデムが使用するアクセスポイント名。
- セッション状態: Connected は、デバイスがネットワークに参加したことを示します。セッション状態が切断されている場合は、アカウントが有効になっていて、データプランが有効になっていれば、通信事業者に確認してください。

SIM プリファレンス

Citrix SD-WAN 110-LTE-WiFi アプライアンスに 2 つの SIM を挿入できます。一度に 1 つの SIM だけがアクティブになります。 **SIM** プリファレンスを選択します。

- **SIM One** 推奨: 2 つの SIM が挿入されている場合、起動時に LTE モデムは SIM One を使用します (使用可能な場合)。LTE モデムが起動して実行されると、その時点で使用可能な SIM (SIM 1 または SIM 2) が使用されます。SIM がアクティブになるまで使用し続けます。
- **SIM Two** 推奨: SIM が 2 台挿入されている場合、LTE モデムは SIMTwo を使用します (利用可能な場合)。LTE モデムが起動して実行されると、その時点で使用可能な SIM (SIM 1 または SIM 2) が使用されます。SIM がアクティブになるまで使用し続けます。
- **SIM One:** 両方の SIM スロットの SIM 状態に関係なく、SIM One のみが使用されます。SIM One は常にアクティブです。
- **SIM Two:** 両方の SIM スロットの SIM 状態に関係なく、SIM Two のみが使用されます。SIM Two は常にアクティブです。

SIM Preference

Preferred SIM: SIM One preferred ▼

Apply

SIM ピン

PIN でロックされている SIM カードを挿入した場合、SIM ステータスは 有効化-検証されていない 状態になります。SIM PIN で認証されるまで、SIM カードは使用できません。SIM PIN は通信事業者から入手できます。

注

SIM PIN 操作は、アクティブな SIM にのみ適用されます。

SIM PIN 操作を実行するには、[構成] > [アプライアンスの設定] > [ネットワークアダプタ] > [モバイルブロードバンド] > **[SIM PIN]** に移動します。

SIM PIN

SIM PIN Status

PIN State: enabled-not-verified

PIN Retries Remaining: 3

PUK Retries Remaining: 10

Disable PIN
Verify PIN
Modify PIN
Unblock

PIN を確認をクリックします。通信事業者から提供された SIM PIN を入力し、**[PIN の確認]** をクリックします。

×

SIM PIN:

Verify PIN

ステータスは [有効化検証済み] に変わります。

SIM PIN
<p><u>SIM PIN Status</u></p> <p>PIN State: enabled-verified PIN Retries Remaining: 3 PUK Retries Remaining: 10</p> <p><input type="button" value="Disable PIN"/> <input type="button" value="Verify PIN"/> <input type="button" value="Modify PIN"/> <input type="button" value="Unblock"/></p>

SIM PIN を無効にする

SIM PIN が有効で確認されている SIM の SIM PIN 機能を無効にすることができます。

SIM PIN
<p><u>SIM PIN Status</u></p> <p>PIN State: enabled-verified PIN Retries Remaining: 3 PUK Retries Remaining: 10</p> <p><input type="button" value="Disable PIN"/> <input type="button" value="Verify PIN"/> <input type="button" value="Modify PIN"/> <input type="button" value="Unblock"/></p>

PIN を無効にするをクリックします。**SIM PIN** を入力して、[無効にする]をクリックします。

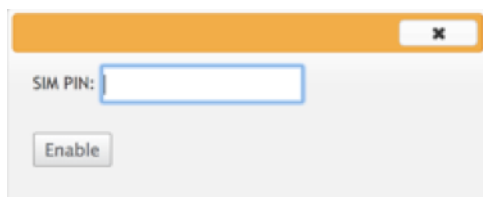
SIM PIN
<p><u>SIM PIN Status</u></p> <p>PIN State: disabled PIN Retries Remaining: 3 PUK Retries Remaining: 10</p> <p><input type="button" value="Enable PIN"/> <input type="button" value="Verify PIN"/> <input type="button" value="Modify PIN"/> <input type="button" value="Unblock"/></p>

SIM PIN を有効にする

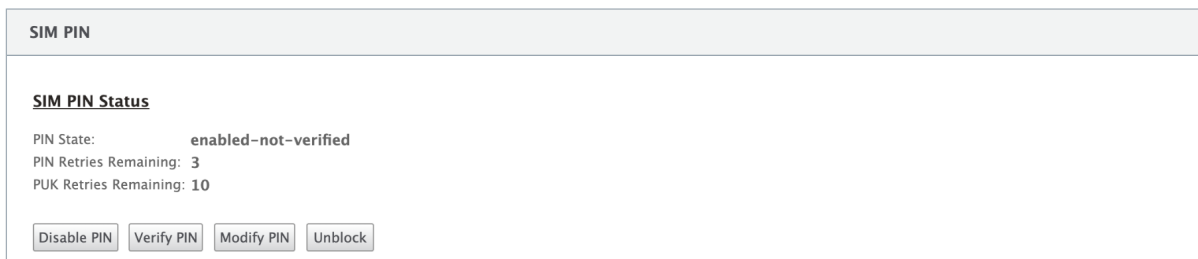
SIM PIN は、無効になっている SIM に対して有効にすることができます。

SIM PIN
<p><u>SIM PIN Status</u></p> <p>PIN State: disabled PIN Retries Remaining: 3 PUK Retries Remaining: 10</p> <p><input type="button" value="Enable PIN"/> <input type="button" value="Verify PIN"/> <input type="button" value="Modify PIN"/> <input type="button" value="Unblock"/></p>

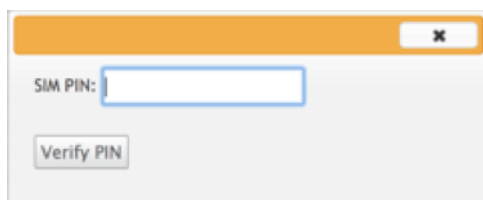
PIN を有効にするをクリックします。通信事業者から提供された SIM PIN を入力し、[有効]をクリックします。

A small dialog box with an orange header bar containing a close button (X). The main area is light gray and contains the text "SIM PIN:" followed by a text input field. Below the input field is a button labeled "Enable".

SIM PIN の状態が **enabled-not-verified** に変わった場合は、PIN が検証されず、PIN が検証されるまで LTE 関連の操作を実行できないことを意味します。

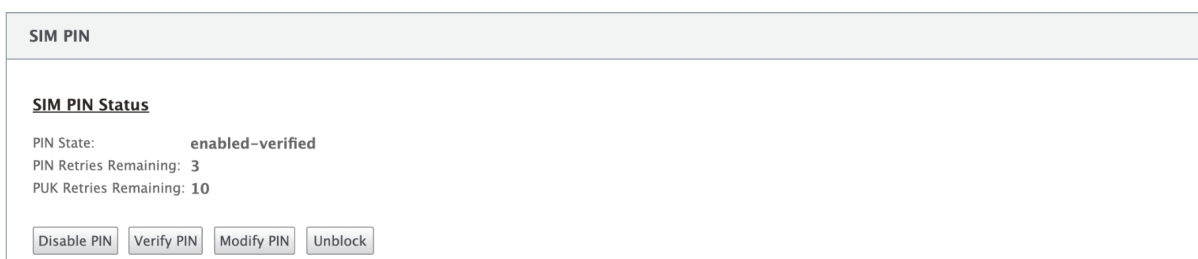
A panel titled "SIM PIN" with a light gray background. Below the title is a section header "SIM PIN Status". Under this header, the following text is displayed: "PIN State: enabled-not-verified", "PIN Retries Remaining: 3", and "PUK Retries Remaining: 10". At the bottom of the panel are four buttons: "Disable PIN", "Verify PIN", "Modify PIN", and "Unblock".

PIN を確認をクリックします。通信事業者から提供された SIM PIN を入力し、[**PIN の確認**] をクリックします。

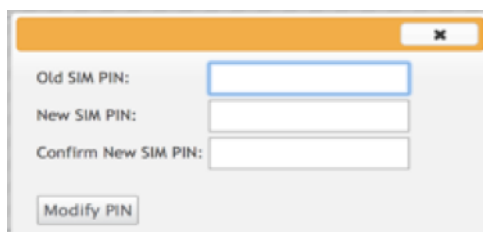
A small dialog box with an orange header bar containing a close button (X). The main area is light gray and contains the text "SIM PIN:" followed by a text input field. Below the input field is a button labeled "Verify PIN".

SIM PIN の変更

PIN が有効検証済み状態になったら、PIN の変更を選択できます。

A panel titled "SIM PIN" with a light gray background. Below the title is a section header "SIM PIN Status". Under this header, the following text is displayed: "PIN State: enabled-verified", "PIN Retries Remaining: 3", and "PUK Retries Remaining: 10". At the bottom of the panel are four buttons: "Disable PIN", "Verify PIN", "Modify PIN", and "Unblock".

PIN の変更をクリックします。通信事業者から提供された SIM PIN を入力します。新しい SIM PIN を入力し、確認します。**PIN** の変更をクリックします。

A dialog box with an orange header bar containing a close button (X). The main area is light gray and contains three text input fields labeled "Old SIM PIN:", "New SIM PIN:", and "Confirm New SIM PIN:". Below the input fields is a button labeled "Modify PIN".

SIM のブロック解除

SIM PIN を忘れた場合、通信事業者から取得した SIM PUK を使用して SIM PIN をリセットすることができます。

The screenshot shows the 'Mobile Broadband' tab selected. Under 'Status Info', a message states: 'This SIM Card is Blocked. Please contact the carrier service for a PUK code to unblock the SIM card.' Below this, the status is 'PIN State: Blocked', 'PIN Tries: 3', and 'PUK Tries: 10'. An 'Unblock' button is visible at the bottom.

SIM のブロックを解除するには、[ブロック解除] をクリックします。選択した **SIM PIN** を入力します。キャリアから入手した **SIM PUK** を入力し、[ブロック解除] をクリックします。

The dialog box has two input fields: 'SIM PIN:' and 'SIM PUK:'. An 'Unblock' button is at the bottom.

注：

SIM カードは、SIM のブロックを解除しながら、PUK の 10 回の試行に失敗して永久にブロックされます。新しい SIM カードについては、通信事業者に連絡する必要があります。

The screenshot shows the 'Network Adapters' tab. Under 'Status Info', a message states: 'This SIM Card is Permanently Blocked. Please contact the carrier service for a new SIM card.'

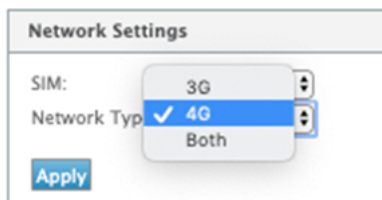
ネットワーク設定

内部 LTE モデムをサポートする Citrix SD-WAN アプライアンス上のモバイルネットワークを選択できます。サポートされるネットワークは、3G、4G、またはその両方です。

The 'Network Settings' dialog box shows 'SIM:' and 'Network Type:' fields. The 'Network Type' dropdown menu is open, showing options: '3G', '4G' (selected with a checkmark), and 'Both'. An 'Apply' button is at the bottom.

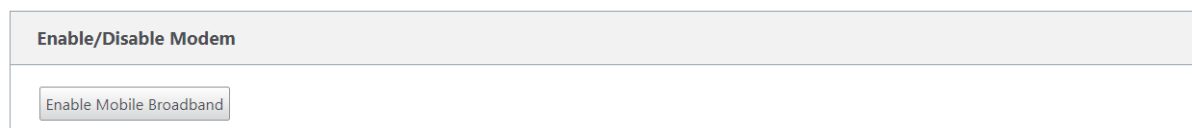
ローミング

ローミングオプションは、LTE アプライアンスではデフォルトで有効になっています。無効にすることもできます。



モデムの有効化/無効化

LTE 機能を使用する意図に応じて、モデムを有効/無効にします。デフォルトでは、LTE モデムは有効になっています。



モデムの再起動

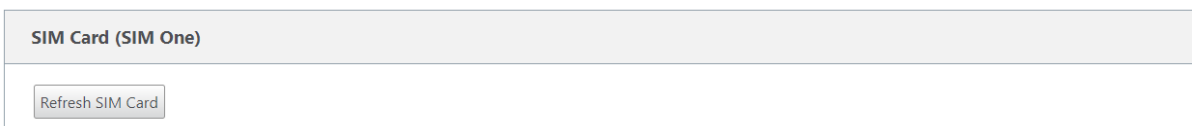
モデムをリブートします。再起動操作が完了するまで、最大で 7 分かかる場合があります。

SIM のリフレッシュ

このオプションは、110-LTE-WiFi モデムによって SIM カードが正しく検出されない場合に使用します。

注

[SIM の更新] 操作は、アクティブな SIM に対してのみ適用されます。



Citrix SD-WAN Center を使用して、ネットワーク内のすべての LTE サイトをリモートで表示および管理できます。詳細については、[リモート LTE サイト管理を参照してください](#)。

CLI を使用した LTE 機能の設定

CLI を使用して 110-LTE-WiFi モデムを設定します。

1. Citrix SD-WAN アプライアンスコンソールにログインします。
2. プロンプトで、CLI インターフェイスにアクセスするためのユーザー名とパスワードを入力します。
3. プロンプトで、コマンド **lte** を入力します。>**help** と入力します。これにより、設定に使用できる LTE コマンドのリストが表示されます。

```
lte> help
Usage
?|help                                # Print this message
status [default|verbose]             # Show status
show                                  # Show configuration
select [1|2] [1|2]                   # Show or choose modem and/or sim to work
enable                                # Enable the selected modem
disable                              # Disable the selected modem
apn <apn> [<username> [<password> [<NONE|PAP|CHAP|PAPCHAP>]]] # Set APN
sim-prefer <prefer|use> <1|2>        # Prefer to use or use SIM one or two
sim-power <show|off|on|reset>        # Show, off, on, reset SIM card power
sim-pin <show>                       # SIM card pin status
sim-pin <verify|disable|enable> <sim pin> # Verify/Disable/Enable SIM card PIN
sim-pin <modify> <old pin> <new pin>  # Modify SIM card PIN
sim-pin <unlock> <sim puk> <sim pin>  # Unblock SIM card PIN
reboot                               # Reboot modem
list-fw                              # List available firmware
upload-fw <fw file>                 # Upload firmware file
apply-fw <fw> [keep-AUTO-SIM]        # Apply firmware
delete-fw <fw>                     # Delete firmware
session <show|stop|start>           # Show/stop/start data session
exit|quit                            # Exit LTE CLI
```

次の表に、**LTE** コマンドの説明を示します。

コマンド	説明
ヘルプ {lte>help}	使用可能な LTE コマンドとパラメータをリストします
ステータス {lte>status}	LTE 接続ステータスを表示します。
{lte>show} を表示	LTE 設定を表示します。
{lte>Disable} を無効にする	LTE モデムを無効にします。
{lte>Enable} を有効にする	LTE モデムを有効にします。
APN {lte>apn}	APN 設定情報を設定します。
SIM 電源オフ、オン、リセット > {lte>sim-電源オフ、オン、リセット}	SIM カードの電源を切る、SIM カードの電源を入れ、SIM カードをリフレッシュする
[1 2] [1 2] {lte>select [1 2] [1 2]} を選択	LTE モデム用の SIM を選択します。
SIM-prefer {lte>sim-prefer}	優先する SIM または使用する SIM を選択します。
SIM PIN {lte>sim-pin}	SIM PIN 関連の操作
再起動 {lte>reboot}	LTE モデムを再起動します

注

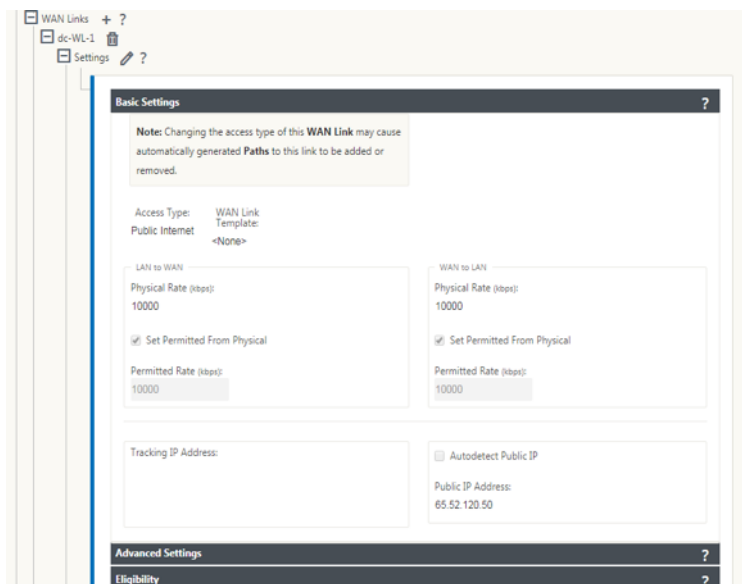
ファームウェア関連の操作は、110-LTE-WiFi アプライアンスではサポートされていません。

LTE 用の MCN の設定

110-LTE-WiFi アプライアンスを MCN として構成することはできません。ただし、MCN が LTE ブランチアプライアンスと連携するには、MCN アプライアンスで次の設定を実行します。

MCN を設定するには、次の手順を実行します。

1. SD-WAN アプライアンスの GUI にログインします。[構成エディタ] に移動します。MCN サイトの設定を完了します。[MCN の設定を参照してください](#)。
2. WAN リンク設定の一部として、ルーティング可能なパブリック IP アドレスを指定してください。クライアントアプライアンスのパブリック IP アドレスを設定する必要はありません。



LTE のブランチを構成する

110-LTE-WiFi アプライアンスをブランチサイトとして設定するには：

1. SD-WAN アプライアンス GUI で、設定エディタに移動します。[ブランチの設定を参照してください](#)。
 - インターフェイスグループを作成します。
 - 次の項目を選択して、最大 1 つの仮想インターフェイスと 1 つのインターフェイスグループを作成し、LTE アダプタで WAN リンクを設定します。
 - イーサネットインターフェイス-LTE 1
 - セキュリティ：信頼できない（デフォルト）

- DHCP クライアント：有効（デフォルト）

The screenshot shows the configuration page for Virtual Interfaces and Ethernet Interfaces. The top section lists four interfaces: E1_1_LAN (0), E1_2_WAN1 (0), E1_3_WAN2 (0), and ELTE-1Vlan0 (0). Each interface has columns for Virtual Interfaces, Ethernet Interfaces, Bypass Mode, WCCP, Security, and a Delete button. The bottom section shows the configuration for the selected interface, ELTE-1Vlan0, including Firewall Zone, VLAN ID, Directed Broadcast, Client Mode, SLAAC, and a Delete button. The Client Mode is set to DHCP.

Virtual Interfaces	Ethernet Interfaces	Bypass Mode	WCCP	Security	Delete
E1_1_LAN (0)	1/1 1/2 1/3 LTE-1	Fail-to-Wire	<input type="checkbox"/>	Trusted	
E1_2_WAN1 (0)	1/1 1/2 1/3 LTE-1	Fail-to-Block	<input type="checkbox"/>	Untrusted	
E1_3_WAN2 (0)	1/1 1/2 1/3 LTE-1	Fail-to-Block	<input type="checkbox"/>	Trusted	
ELTE-1Vlan0 (0)	1/1 1/2 1/3 LTE-1	Fail-to-Block	<input type="checkbox"/>	Untrusted	

Name	Firewall Zone	VLAN ID	Directed Broadcast	Client Mode	SLAAC	Delete
ELTE-1Vlan0	Untrusted_Intern	0	<input type="checkbox"/>	DHCP	<input type="checkbox"/>	

Apply Revert

2. LTE インターフェイス用に作成された仮想インターフェイスを使用して WAN リンクを設定する場合は、WAN リンク設定の **AutoDetect Public IP** を有効にします。

The screenshot shows the Basic Settings for a WAN Link. The Access Type is set to WAN Link Template. The Physical Rate (kbps) is 10000. The Permitted Rate (kbps) is 10000. The Autodetect Public IP checkbox is checked.

Note: Changing the access type of this WAN Link may cause automatically generated Paths to this link to be added or removed.

Access Type: WAN Link Template: <None>

LAN to WAN

Physical Rate (kbps): 10000

☒ Set Permitted From Physical ☐ Auto Learn

Permitted Rate (kbps): 10000

WAN to LAN

Physical Rate (kbps): 10000

☒ Set Permitted From Physical ☐ Auto Learn

Permitted Rate (kbps): 10000

Tracking IP Address:

☒ Autodetect Public IP

Public IP Address:

3. デフォルトでは、LTE インターフェイスを使用して WAN リンクを設定しようとすると、WAN リンクは従量制リンクおよびラストリゾートスタンバイモードとしてマークされます。必要に応じて、これらのデフォルト

設定を変更できます。

Advanced Settings	?
Eligibility	?
Metered/Standby Link	?
<p>Metering</p> <p><input checked="" type="checkbox"/> Enable Metering</p> <p>Data Cap (MB): <input type="text" value="0"/> Billing Cycle: <input type="text" value="Monthly"/> Starting From: <input type="text" value="MM/DD/YYYY"/></p>	
<p>Standby</p> <p>Standby Mode: <input type="text" value="Last-Resort"/> Priority: <input type="text" value="1"/></p>	

WAN リンクのアクセスインターフェイスの IP アドレスおよび Gateway アドレスは、DHCP を介してキャリアから情報を受信するため、設定する必要はありません。

Name	Virtual Interface	IP Address	Gateway IP Address	Virtual Path Mode	Proxy ARP	Delete
br-WL-1-AI-1	V2			Primary	<input type="checkbox"/>	

Apply Revert

4. 110-LTE-WiFi アプライアンスに必要なブランチ設定の残りの部分を完了します。[ブランチの設定を参照してください。](#)
5. SD-WAN ソフトウェアをアップロードして、変更管理を実行します。[変更管理の手順を参照してください。](#)
6. ローカル変更管理プロセスを通じて構成をアクティブ化します。変更管理を実行すると、構成がアクティブ化され、必要な構成が適用されます。

LTE 経由のゼロタッチ展開

SD-WAN 110 SE アプライアンスは、管理ポートとデータポートを介して、SD-WAN アプライアンスの day-0 Provisioning と day-n 管理の両方をサポートします。

LTE 経由のゼロタッチ導入サービスを有効にする前提条件：

1. アンテナを取り付け、アプライアンスの電源を入れ、SIM カードを挿入します。
2. SIM カードに有効なデータプランがあることを確認します。
3. 管理/データポートが接続されていないことを確認します。

- 管理/データポートが接続されている場合は、管理/データポートを切断します。
- 管理/データインターフェイスにスタティック IP アドレスが設定されている場合は、DHCP を使用して管理/データインターフェイスを設定し、設定を適用してから、管理/データポートを切断する必要があります。

4. 110-LTE-WiFi アプライアンスの設定で、LTE インターフェイスに対してインターネットサービスが定義されていることを確認します。

アプライアンスの電源がオンになると、ゼロタッチ展開サービスは LTE ポートを使用して、最新の SD-WAN ソフトウェアと SD-WAN 構成を取得します。

SD-WAN Center GUI を使用して、110-LTE-WiFi アプライアンスをゼロタッチ展開サービス用に展開および設定できます。

SD-WAN Center を使用した 110-LTE-WiFi アプライアンスのデプロイと設定の詳細については、[ゼロタッチデプロイメント手順を参照してください](#)。

110-SE LTE アプライアンスの管理/データインターフェースを介したゼロタッチ導入サービス

管理/データポートをインターネットに接続し、他のすべての非 LTE [プラットフォームでサポートされている標準のゼロタッチ展開手順を使用します](#)。

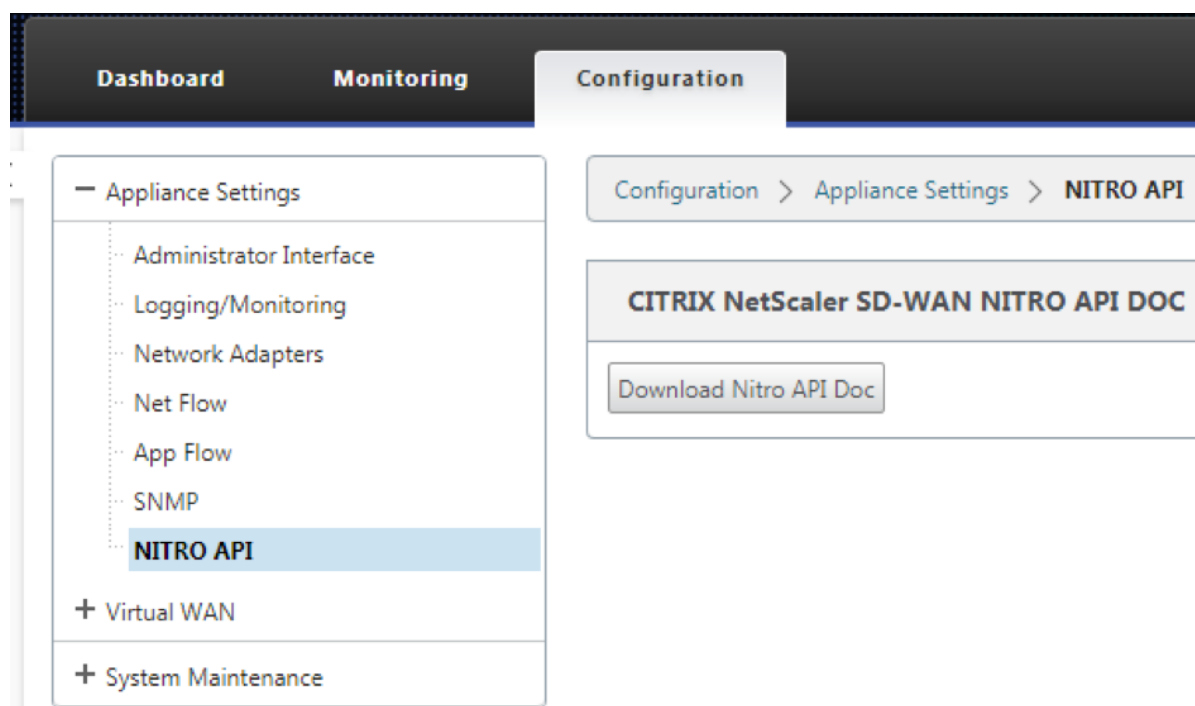
サポートされていないプラットフォーム

Day-0 プロビジョニングと Day-N 管理は、次の SD-WAN アプライアンスではサポートされていません。

- Citrix SD-WAN 1000 SE/PE
- Citrix SD-WAN 2000 SE/PE
- Citrix SD-WAN 4000 SE

LTE REST API

LTE REST API の詳細については、SD-WAN GUI に移動し、[構成] > [アプライアンスの設定] > [NITRO API] の順に移動します。[**Nitro API** ドキュメントのダウンロード] をクリックします。SIM PIN 機能用の REST API は、Citrix SD-WAN 11.0 で導入されています。



AT コマンド

AT コマンドは、LTE モデムの設定とステータスのモニタリングとトラブルシューティングに役立ちます。**AT** は **AtTension** の略称。すべてのコマンドラインが **at** で始まるので、AT コマンドと呼ばれます。LTE をサポートする Citrix SD-WAN プラットフォームモデルは、AT コマンドの実行をサポートします。AT コマンドはモデム固有であるため、AT コマンドのリストはプラットフォームによって異なります。

AT コマンドを実行するには、次の手順に従います。

1. Citrix SD-WAN アプライアンスコンソールにログインします。
2. プロンプトで、CLI インターフェイスにアクセスするためのユーザー名とパスワードを入力します。
3. プロンプトで「**lte**」と入力します。
4. **at** と入力し、AT コマンドを入力します。

以下はその例です：

- **at at+cpin** —SIM ステータス情報を提供します。

```
lte> at at+cpin?  
Running at+cpin? command  
AT command state: success  
+CPIN: READY  
OK  
success
```

外付け **USB LTE** モデムの構成

November 8, 2021

一部の Citrix SD-WAN アプライアンスでは、外部 3G/4G USB モデムを接続できます。アプライアンスは、3G/4G ネットワークと他の接続を使用して、帯域幅を集約して回復力を提供する仮想ネットワークを形成します。他のインターフェイスで接続障害が発生した場合、トラフィックは USB LTE モデムを介して自動的にリダイレクトされます。次のアプライアンスは、外部 USB モデムをサポートしています。

- Citrix SD-WAN 210 SE/AE
- Citrix SD-WAN 210 SE LTE
- Citrix SD-WAN 110 SE
- Citrix SD-WAN 110 Wi-Fi SE
- Citrix SD-WAN 110 LTE Wi-Fi SE
- Citrix SD-WAN 1100 SE/PE/AE
- Citrix SD-WAN 2100 SE/PE

[Citrix SD-WAN 210 SE LTE および CitrixSD-WAN 110 LTE Wi-Fi SE アプライアンス](#)には LTE モデムが内蔵されている。これらのアプライアンスでは、アクティブデュアル LTE がサポートされています。

次のアプライアンスは、外付け USB モデムをサポートしていません。

- Citrix SD-WAN 1000 SE/PE
- Citrix SD-WAN 2000 SE/PE
- Citrix SD-WAN 4000 SE

サポートされている外部 USB モデムは、CDC イーサネット、MBIM、および NCM の 3 種類です。**MBIM** モデムおよび **NCM USB** モデムでは、**APN** 設定およびモデムの有効/無効を設定できます。モバイルブロードバンド操作は、CDC イーサネット USB モデムではサポートされていません。

注

モデムタイプが MBIM の外部 LTE ドングルは、Citrix SD-WAN 2100 プラットフォームでは動作しません。

USB モデムの接続

ワイヤレスキャリアのガイドラインに従って、USB モデムを有効にしてテストします。

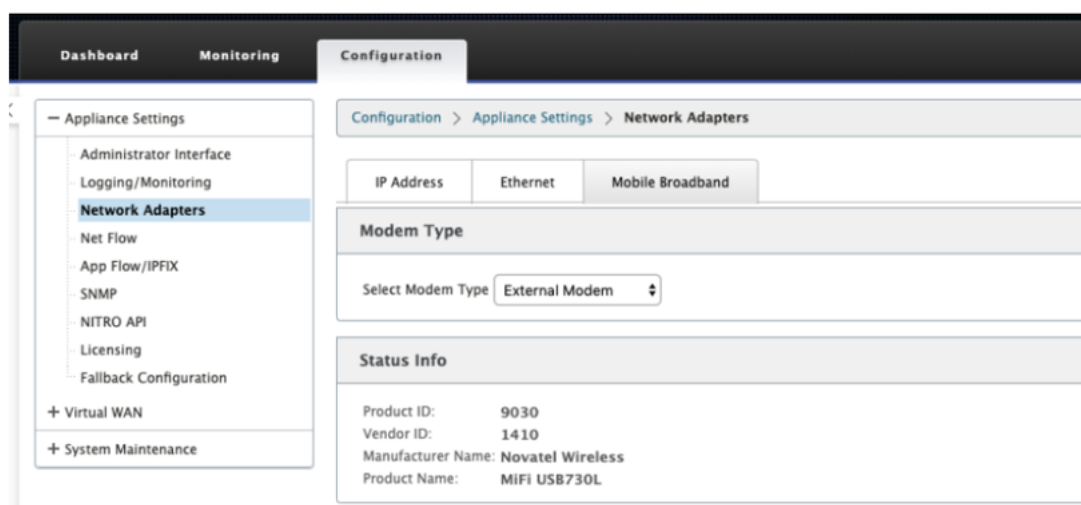
外部 LTE モデムの関連事項:

- サポートされている USB LTE ドングルを使用してください。対応ドングルのハードウェアモデルは Verizon USB730L と AT&T USB800 である。
- SIM カードが USB LTE ドングルに挿入されていることを確認します。CDC イーサネット LTE ドングルには静的 IP アドレスがあらかじめ設定されているため、SIM カードが挿入されていないと、設定が妨げられ、接続障害や断続的な接続が発生します。
- CDC イーサネット LTE ドングルを SD-WAN アプライアンスに挿入する前に、外部 USB スティックを Windows/Linux マシンに接続し、適切な APN およびモバイルデータローミング構成でインターネットが正常に動作していることを確認します。USB ドングルの接続モードがデフォルト値の [手動] から [自動] に変更されていることを確認します。

注

- Citrix SD-WAN アプライアンスは、一度に 1 つの USB LTE ドングルしかサポートしません。複数の USB ドングルが接続されている場合は、すべてのドングルを外し、1 つのドングルだけを接続します。
- Citrix SD-WAN アプライアンスは、USB モデムのユーザー名とパスワードをサポートしていません。セットアップ時に、モデムのユーザー名とパスワード機能が無効になっていることを確認します。
- 外部 MBIM ドングルの抜き差しやリブートは、内部 LTE モデムデータセッションに影響を与えます。これは予想される動作です。
- 外部 LTE モデムを接続すると、SD-WAN アプライアンスで認識されるまでに約 3 分かかります。

外部モデムの詳細を表示するには、アプライアンス UI で「構成」>「アプライアンスの設定」>「ネットワークアダプタ」>「モバイルブロードバンド」に移動します。モデムの種類として [外部モデム] を選択します。



注:

LTE USB ドングルのモデル番号は [ステータス情報] セクションに表示されません。

モバイルブロードバンド動作

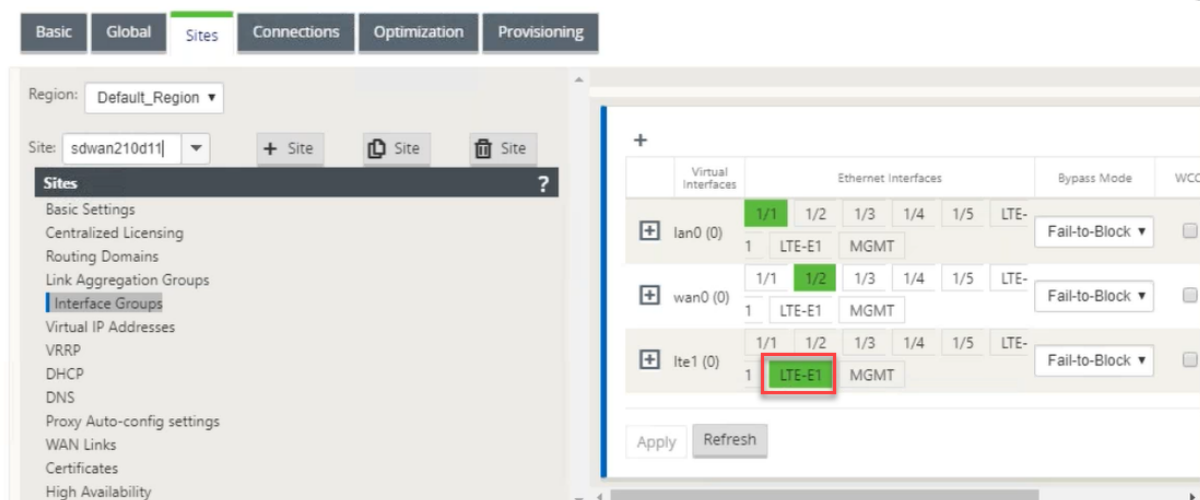
CDC イーサネットおよび MBIM /NCM 外部モデムでサポートされている動作

操作	外部モデム-CDC イーサネット	外部モデム-MBIM および NCM
SIM プリファレンス	いいえ	いいえ
SIM ピン	いいえ	いいえ
APN 設定	いいえ	はい
ネットワーク設定	いいえ	いいえ
ローミング	いいえ	いいえ
ファームウェアの管理	いいえ	いいえ
モデムの有効化/無効化	いいえ	はい
モデムの再起動	いいえ	いいえ
SIM のリフレッシュ	いいえ	いいえ

Citrix SD-WAN Center を使用して、ネットワーク内のすべての LTE サイトをリモートで表示および管理できます。詳細については、[リモート LTE サイト管理を参照してください](#)。

外部 **USB** モデムの設定

外部 USB モデムを構成するには、構成エディタで [サイト] に移動し、サイトを選択して、[インターフェイスグループ] をクリックします。外部 USB モデムインターフェイス LTE-E1 を設定できます。LTE のブランチの設定の詳細については、LTE の [ブランチの設定を参照してください](#)。



LTE 経路のゼロタッチ展開

USB LTE モデムを介したゼロタッチ導入サービスを有効にする前提条件:

- Citrix SD-WAN アプライアンスに USB モデムを挿入します。詳細については、「USB モデムの接続」を参照してください。
- USB モデムの SIM カードにデータプランがアクティブになっていることを確認します。
- 管理/データポートが接続されていないことを確認します。管理ポート/データポートが接続されている場合は、接続を解除します。
- アプライアンスの設定に、LTE インターフェイス用に定義されたインターネットサービスがあることを確認します。

アプライアンスの電源がオンになると、ゼロタッチ展開サービスは LTE-E1 ポートを使用して、最新の SD-WAN ソフトウェアと構成を取得します。

SD-WAN Center GUI を使用して、ゼロタッチ展開サービス用にアプライアンスをデプロイおよび構成します。詳細については、「[ゼロタッチ展開](#)」を参照してください。

SD-WAN Orchestrator によるゼロタッチ展開の詳細については、[ゼロタッチ展開を参照してください](#)。

サポートされている USB モデム

以下のモデムは、Citrix SD-WAN アプライアンスと互換性があります。

注:

Citrix は、ワイヤレスキャリアのファームウェアアップデートを制御しません。したがって、新しいモデムファームウェアと Citrix SD-WAN ソフトウェアの互換性は保証されません。お客様がモデムのファームウェアアップデートを制御している。ファームウェア更新プログラムをネットワーク全体にプッシュする前に、単一のサ

イトでテストすることをお勧めします。

リージョン	ワイヤレスキャリア/メーカー	USB モデム	サポートされている モデムタイプ	インターフェイス
米国	Verizon	グローバルモデム USB730L	cdc_ether	4G のみ
米国	AT&T	AT&T グローバルモ デム USB800	cdc_ether	4G のみ

AT コマンド

AT コマンドは、LTE モデムの設定とステータスのモニタリングとトラブルシューティングに役立ちます。**AT** は **ATtension** の略称。すべてのコマンドラインが **at** で始まるので、AT コマンドと呼ばれます。LTE をサポートする Citrix SD-WAN プラットフォームモデルは、AT コマンドの実行をサポートします。AT コマンドはモデム固有であるため、AT コマンドのリストはプラットフォームによって異なります。

AT コマンドを実行するには、次の手順に従います。

- 1. Citrix SD-WAN アプライアンスコンソールにログインします。
- 2. プロンプトで、CLI インターフェイスにアクセスするためのユーザー名とパスワードを入力します。
- 3. プロンプトで「**lte**」と入力します。
- 4. **at** と入力し、AT コマンドを入力します。

以下はその例です：

at at+cpin —SIM ステータス情報を提供します。

```
lte> at at+cpin?
Running at+cpin? command
AT command state: success
+CPIN: READY
OK
success
```

デプロイ

May 10, 2021

Citrix SD-WAN アプライアンスを使用して実装されるユースケースシナリオを次に示します。

- [ゲートウェイモードでの SD-WAN の導入](#)
- [インラインモード](#)
- [PBR モードでの SD-WAN の導入（仮想インラインモード）](#)
- [ブランチ間通信の動的パス](#)
- [WAN から WAN への転送](#)
- [SD-WAN ネットワークの構築](#)
- [LAN セグメンテーションのルーティング](#)
- [Premium Edition アプライアンスを利用して WAN 最適化サービスのみを提供する](#)
- [2 ボックスモード](#)
- [ゼロタッチ展開](#)
- [単一リージョン展開](#)
- [複数リージョン展開](#)
- [高可用性](#)

チェックリストと展開方法

August 30, 2022

インストールを開始する前に、まず『Citrix Virtual WAN 展開計画ガイド』を読んでおくことを強くお勧めします。この記事では、Virtual WAN の重要な概念と機能について説明し、展開を計画するためのガイドラインを示します。

展開の準備

SD-WAN Standard Edition と Premium（Enterprise）Edition を展開する手順と手順を次に示します。

デプロイのユースケースの一部を表示するには、「[デプロイ](#)」を参照してください。

1. Citrix SD-WAN 展開情報を収集します。
2. Citrix SD-WAN アプライアンスをセットアップします。
 - SD-WAN 展開に追加するハードウェアアプライアンスごとに、次のタスクを完了する必要があります。
 - アプライアンスのハードウェアを設定します。

- アプライアンスの管理 IP アドレスを設定し、接続を確認します。
- アプライアンスの日付と時刻を設定します。
- (任意) コンソールセッションタイムアウト間隔を高い値または最大値に設定します。

3. アプライアンスにソフトウェアライセンスファイルをアップロードしてインストールします。

インストールと構成のチェックリスト

展開する各 SD-WAN サイトについて、次の情報を収集します。

- ご使用の製品のライセンス情報
- デプロイする各アプライアンスの必要なネットワーク IP アドレス:
 - 管理 IP アドレス
 - 仮想 IP アドレス
 - サイト名
 - アプライアンス名 (サイトごとに 1 つ)
 - SD-WAN アプライアンスモデル (デプロイする各アプライアンス用)
 - 展開モード (MCN またはクライアント)
 - トポロジ
 - Gateway MPLS
 - GRE トンネル情報
 - ルート
 - VLAN
 - 各回線の各サイトでの帯域幅

ベストプラクティス

May 10, 2021

この記事では、Citrix SD-WAN ソリューションの導入のベストプラクティスについて説明します。以下の Citrix SD-WAN 展開モードの一般的なガイダンス、利点、ユースケースについて説明します。

Edge/Gateway モード

推奨事項

ゲートウェイモードの展開に関する推奨事項を次に示します。

1. ゲートウェイモードは、ルータの統合が実行され、お客様が SD-WAN をエッジデバイス終端接続にできる状態にある SD-WAN 支店に最適です。
2. プロジェクトをゼロから構築すると、優れたネットワークアーキテクチャを綿密な設計でレンダリングすることができます。

注:

ゲートウェイモードは、インフラストラクチャが一部の中断を伴う既存のプロジェクトに対して、データセンター側で使用できます。

アドバンテージ/ユースケース

ゲートウェイモード展開の利点と使用例を次に示します。

1. 顧客支社でのルータ/ファイアウォール/ネットワーク要素の統合に最適な使用例
2. DHCP によるシンプルで簡単な LAN ホスト管理。
 - SD-WAN をネクストホップにして、データポート用のすべての LAN ホストに DHCP ベースの IP アドレスリングを提供できるようにします。
3. すべての接続は SD-WAN エッジ/ゲートウェイで終了し、管理が容易になります。
4. SD-WAN はエッジルーティングの焦点であり、すべてのトラフィックを操舵します。帯域幅/容量のアカウントティングを含め、ブレイクアウト、バックホール、またはオーバーレイにエッジ上で決定が行われます。
5. LAN ホストとしてのすべての LAN サブネットホストは、SD-WAN LAN VIP をネクストホップとして使用できます。SD-WAN LAN がコアスイッチに接続されている場合は、ダイナミックルーティングを実行して、すべての LAN サブネットを可視化できます。
6. 高可用性 (HA) のための優れた柔軟性-サイトがアクティブ/スタンバイモードで動作するように、Gateway モードに対する厳格な推奨事項。また、SD-WAN デバイスがダウンした場合のトラフィックのブラックホールを防ぐのに役立ちます。
 - ブランチで使用可能なスイッチ-パラレル高可用性は、Gateway モードで動作します。
 - ブランチでは使用できないスイッチ-SD-WAN は、SD-WAN エッジ高可用性モード（フェールツーワイヤ高可用性モード）でも動作できます。このモードでは、2 つの SD-WAN ボックスがデジジチェーン接続され、フェールツーワイヤポートを使用してコンバージド高可用性ペアとして機能します。

7. インターネットを **UNTRUSTED** インターフェイスとして定義できます。これにより、ブレイクアウト用のダイナミック NAT が自動的に作成され、接続元 NAT によって応答が SD-WAN に戻されます。
8. 4980 上の ICMP/ARP/UDP 制御パケットだけが許可されるという点では、信頼できないインターフェイスに対するセキュリティ上の考慮事項は当然暗黙的に示されています。

注意事項

ゲートウェイモードで注意する必要がある情報は、次のとおりです。

- 慎重な設計とネットワークアーキテクチャ -ゲートウェイモードでは、ブランチ/エッジネットワーク全体が SD-WAN にあるため、慎重な設計とネットワークに関する考慮事項が必要になる場合があります。ブロックするもの、ルーティングするもの、ネットワーク LAN の方法、WAN の終端方法など。
- デバイスの障害 -エッジモードでは、Failto Wire 機能を使用できません。デバイスがダウンすると、ブランチ全体がダウンします。
- セキュリティポスター -ルーティングはエッジで管理されるため、ファイアウォール、ブレイクアウト/バックホールの考慮事項などのセキュリティ姿勢は極めて重要であり、お客様との認識が必要です。
- 高可用性: Fail-to-Wire の高可用性には、ポートアベイラビリティに関する考慮事項がいくつか必要であり、配置によっては設計が難しい場合があります。

– SD-WAN 110 は、フェイル・トゥ・ワイヤ・ポートを持たないため、オプションではありません。

たとえば、2 つの WAN リンクを動作させる必要がある場合は、LAN インターフェイスを含む高可用性インターフェイス用の専用ポートを含む 5 つのポートが必要です。

インライン・モード: フェイル・トゥ・ワイヤ/フェイル・トゥ・ブロック

推奨事項

インラインモード展開の推奨事項を次に示します。

1. インラインモードは、既存のインフラストラクチャを変更せず、SD-WAN が LAN セグメントに対して透過的にインラインに配置されているブランチに最適です。
2. また、データセンターのワークロードがデバイスのダウン/クラッシュによってブラックホールにならないようにすることが非常に重要であるため、データセンターでは、インライン・フェイル・トゥ・ワイヤまたはインライン・パラレル高可用性を採用することもできます。

利点とユースケース

インラインモード展開の利点と使用例を次に示します。

1. したがって、MPLS ルータを維持することは素晴らしい機能です。Fail-to-Wire 対応デバイスにより、ボックスがダウンした場合にインフラストラクチャをアンダーレイにシームレスにフェイルオーバーできます。
 - デバイスが Fail-to-WAN (SD-WAN 210 以上) をサポートしている場合、これにより、SD-WAN がクラッシュまたはダウンしたときに、1 つの SD-WAN をハードウェアにインラインで配置して、カスタマーエッジルータへの LAN トラフィックをバイパスできます。
 - お客様の LAN/イントラネットに自然な拡張をもたらす MPLS リンクが存在する場合、Fail-to-Wire ブリッジ-pair ポートが最良の選択肢 (Fail-to-Wire 対応ペア) であり、デバイスがクラッシュまたはダウンしたときに LAN トラフィックがカスタマーエッジルータにハードウェアがバイパスされます (次のホップ)。
2. ネットワークはシンプルです。
3. SD-WAN は、インラインモードを介してすべてのトラフィックを認識するため、適切な帯域幅/キャパシティアカウンティングの最適なシナリオです。
4. L2 セグメントの IP のみを必要とするため、統合要件はほとんどありません。LAN セグメントは、LAN インターフェイスに腕があるためよく知られています。コアスイッチに接続する場合は、ダイナミックルーティングを実行して、すべての LAN サブネットを可視化することもできます。
5. お客様の期待は、SD-WAN が新しいネットワークノードとして既存のインフラストラクチャに溶け込む必要があることです (他に何も変わりません)。
6. プロキシ **ARP** : インラインモードでは、ゲートウェイがダウンした場合、またはネクストホップへの SD-WAN インターフェイスがダウンした場合、SD-WAN が ARP 要求を LAN ネクストホップにプロキシすることが祝福されます。
 - 一般に、複数の WAN 接続 (MPLS/インターネット) を持つブリッジペア (Fail-to-Block または Fail-to-Wire) を使用するインラインモードでは、LAN ホストをネクストホップ Gateway に接続するブリッジペアインターフェイスに対してプロキシ ARP を有効にすることを推奨します。
 - 何らかの理由で、ネクストホップがダウンしているか、ネクストホップへの SD-WAN インターフェイスがダウンして Gateway に到達不能になっている場合、SD-WAN は ARP 要求のプロキシとして機能し、LAN ホストはパケットをシームレスに送信し、仮想パスを維持する残りの WAN 接続を使用できます。
7. 高可用性: Failto-Wire がオプションでない場合、デバイスを並列高可用性 (アクティブ/スタンバイ用の共通の LAN および WAN インターフェイス) デバイスに配置して、冗長性を実現できます。
 - SD-WAN 110 のように、アプライアンスが Fail-to-Wire をサポートしていない場合は、プライマリがダウンした場合に、スタンバイデバイスを起動できるインライン並列高可用性を実現する必要があります。

注意事項

インラインモードで注意する必要がある情報は次のとおりです。

- SD-WAN (LAN と WAN 側) に 2 つのアームを持つ配管ネットワーク, ネットワークは 2 つのアームで配管する必要があるため、いくつかのダウンタイムを必要とします。
- Failto Wire が使用されている場合、セキュリティが侵害されないように、信頼ゾーン内のカスタマーエッジルータ/ファイアウォールの背後にあることを確認する必要があります。
- MPLS QoS は、以前の QoS ポリシーが送信元 IP アドレスまたは DSCP ベースに依存していた可能性があるため、この点では少し変化します。これは、オーバーレイのためにマスクされるためです。
- SD-WAN の QoS がトラフィックの優先順位付けを処理し、優先順位の高いアプリケーションをすぐに他のクラスを送信するように、適切に設計された SD-WAN 固有の予約帯域幅を使用して MPLS ルータを再利用するように注意する必要があります (ただし、MPLS ルータ上の SD-WAN 用に予約された帯域幅)。MPLS キューは、自動パスグループに 1 つの DSCP が設定された代替または MPLS で、これを処理できます。
- カスタマーエッジルータでリンクが終端しているためにインターネットインターフェイスが信頼されている場合は、インターネットサービスを使用するには、アプライアンスからのインターネットブレイクアウトを有効にする排他的なダイナミック NAT ルールを作成する必要があります。
- インターネットリンクが WAN 接続だけであり、カスタマーエッジルータで終端している場合でも、カスタマーエッジルータが既存のアンダーレイインフラストラクチャを介してパケットを操縦するための予防措置を講じている場合は、接続をバイパスしても問題ありません。
 - インターネット接続のあるブリッジペア経由で LAN トラフィックをバイパスする流れや、アプライアンスがダウンしているときの流れを考慮する必要があります。これは機密性の高い企業イントラネットトラフィックであるため、障害発生前夜には、その処理方法を知っている必要があります。

仮想インライン/ワンアームモード

推奨事項

仮想インラインモードの展開に関する推奨事項を次に示します。

1. 仮想インラインモードは、SD-WAN ネットワーク配管を並列処理しながら、データセンターが既存のインフラストラクチャを使用して既存のワークロードを処理できるため、データセンターのネットワークに最適です。
2. SD-WAN はワンアームインターフェイスにあり、VIP の SLA トラッキングで管理されます。トラッキングが停止すると、トラフィックは既存のアンダーレイインフラストラクチャを介してルーティングを再開します。
3. ブランチは仮想インラインモードでデプロイすることもできますが、インライン/ゲートウェイのデプロイの方が優勢です。

利点とユースケース

仮想インラインモード展開の利点/使用例を次に示します。

1. データセンターで SD-WAN をネットワーク化するための最も簡単に推奨される方法

- 仮想インラインモードでは、ヘッドエンドコアルータと SD-WAN の並列ネットワークプログラミングが可能になります。
- 仮想インラインモードを使用すると、LAN トラフィックを迂回するために PBR を簡単に定義でき、SD-WAN を通過し、オーバーレイのメリットを得ることができます。

2. SD-WAN に障害が発生した場合、基盤となるインフラストラクチャへのシームレスなフェイルオーバー、および通常の条件下では SD-WAN へのシームレスな転送により、オーバーレイのメリットが得られます。

3. ** ネットワークと統合のシンプルな要件 **。ヘッドエンドルータから仮想インラインの SD-WAN へのシングルワンアームインターフェイス。

4. インポート専用モード（何もエクスポートしない）でダイナミックルーティングを簡単に展開でき、LAN サブネットをリモートの SD-WAN ピアアプライアンスに送信できます。

5. 物理的なを選択する方法を示すために、ルータ上で PBR を簡単に定義できます（WAN VIP ごとに 1 つ）。

注意事項

仮想インラインモードで注意する必要がある情報は次のとおりです。

- 定義された WAN リンクの SD-WAN 論理 VIP を適切な物理インターフェイスに明確にマッピングするには、適切な注意が必要です（そうしないと、WAN メトリック評価および WAN パスの選択で望ましくない問題が発生する可能性があります）。
- すべてのトラフィックが SD-WAN を介して転送されるか、特定のトラフィックだけ転送されるかを知るために、設計上の適切な考慮事項が必要です。
- つまり、SD-WAN は、SD-WAN の容量が他の非 SD-WAN トラフィックによって使用されないように、インターフェイス上で設定する必要がある帯域幅の一部分だけ専用にする必要があります。
 - SD-WAN WAN リンク容量が正しく定義されていないと、帯域幅アカウンティングの問題や輻輳の問題が発生することがあります。
- ダイナミックルーティングは、SD-WAN がデータセンターおよびブランチオフィスの VIP をヘッドエンドにエクスポートし、ルーティングが SD-WAN に対して影響される場合、オーバーレイパケットがループを開始し、望ましくない結果を引き起こすような設計が不適切に行われている場合、いくつかの問題を引き起こす可能性があります。
- ダイナミックルーティングは、学習対象とアドバタイズ対象のすべての潜在的な要因を考慮して適切に管理する必要があります。
- ワンアームの物理インターフェイスがボトルネックになることがあります。これらの回線では、アップロード/ダウンロードの両方に対応し、SD-WAN からの LAN と LAN から WAN/WAN から LAN へのトラフィックとしても機能するため、設計上の考慮事項が必要です。

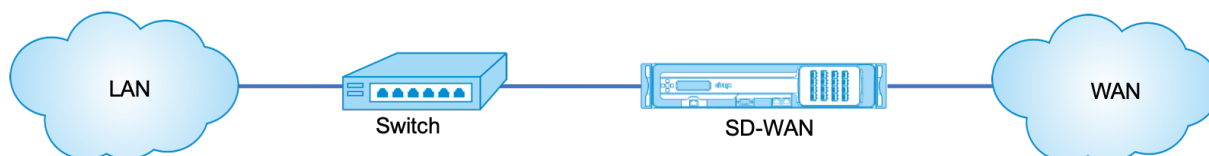
- 過剰な LAN から LAN へのトラフィックは、設計時に注意すべき点である可能性があります。
- ダイナミックルーティングを使用しない場合、すべての LAN サブネットを管理する場合は、適切な注意が必要です。そうしないと、望ましくないルーティングの問題が発生する可能性があります。
- 仮想インラインの SD-WAN にデフォルトルート (0.0.0.0/0) を定義して、ヘッドエンドルータを指すようにすると、ルーティングループの問題が発生する可能性があります。このような状況では、仮想パスがダウンした場合、データセンター LAN からのトラフィック（トラフィックのモニタリングなど）がヘッドエンドにループバックされ、SD-WAN に戻され、望ましくないルーティングの問題が発生します（仮想パスがダウンしている場合、リモートブランチサブネットは到達可能になりません。デフォルトルートは HIT になり、ループの問題が発生します）。

ゲートウェイモード

May 10, 2021

Gateway モードでは、SD-WAN アプライアンスが物理的にパスに配置されます（ツーマーム配置）。SD-WAN アプライアンスをそのサイトの LAN ネットワーク全体のデフォルトゲートウェイにするには、既存のネットワークインフラストラクチャを変更する必要があります。新しいネットワークとルータの交換に使用されるゲートウェイモード。ゲートウェイモードでは、SD-WAN アプライアンスが次のようになります。

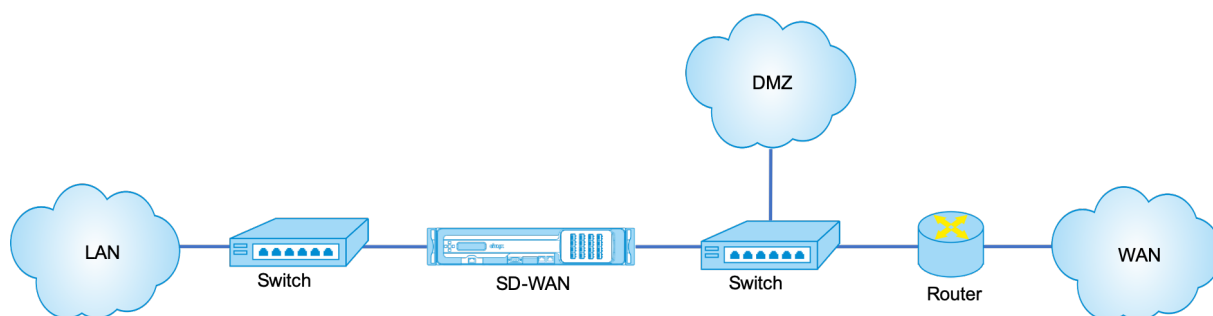
- WAN との間で送受信されるすべてのトラフィックを表示するには
- ローカルルーティングを実行するには



注

ゲートウェイモードで展開された SD-WAN は、レイヤ 3 デバイスとして機能し、フェールツーワイヤを実行できません。関連するすべてのインターフェイスが **Fail-to-Block** 用に設定されます。アプライアンスに障害が発生すると、サイトのデフォルト Gateway も失敗し、アプライアンスとデフォルト Gateway が復元されるまで停止します。

インラインモードでは、SD-WAN アプライアンスはイーサネットブリッジのように見えます。SD-WAN アプライアンスモデルのほとんどは、インラインモード用の フェールツーワイヤ（イーサネットバイパス）機能を備えています。電源が故障すると、リレーが閉じ、入力ポートと出力ポートが電氣的に接続され、イーサネット信号がポート間で通過できるようになります。Fail-to-Wire モードでは、SD-WAN アプライアンスは 2 つのポートを接続するクロスオーバーケーブルのように見えます。すでに定義されたネットワークに統合するために使用されるインラインモード。

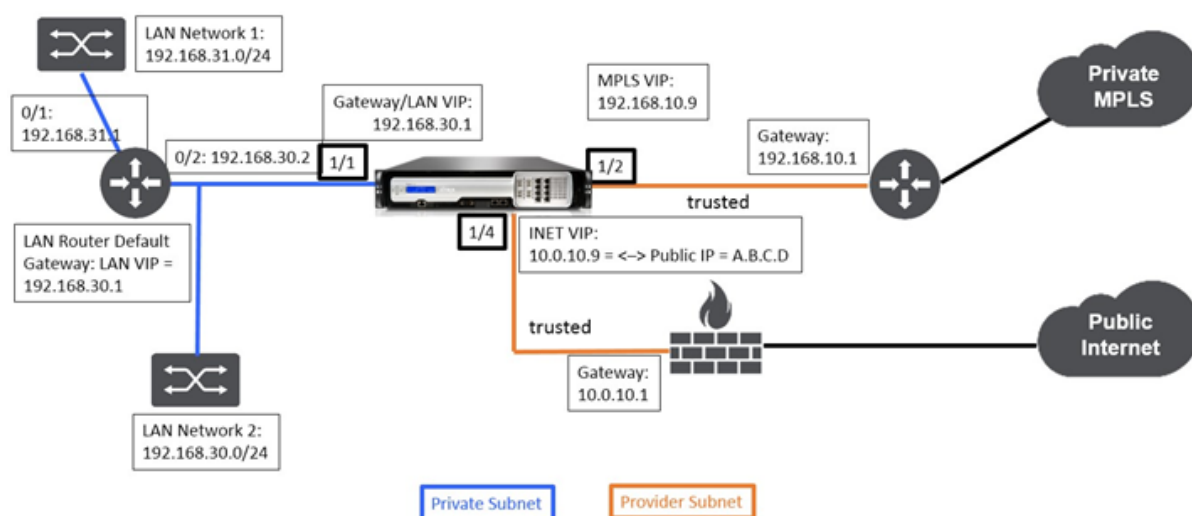


この記事では、ネットワーク設定のサンプルで SD-WAN アプライアンスをゲートウェイモードで構成する手順を順を追って説明します。インライン展開は、ブランチ側で設定を完了するためにも説明されています。Inline デバイスが削除されても、ネットワークは引き続き機能しますが、Gateway デバイスが削除されるとすべてのアクセスが失われます。

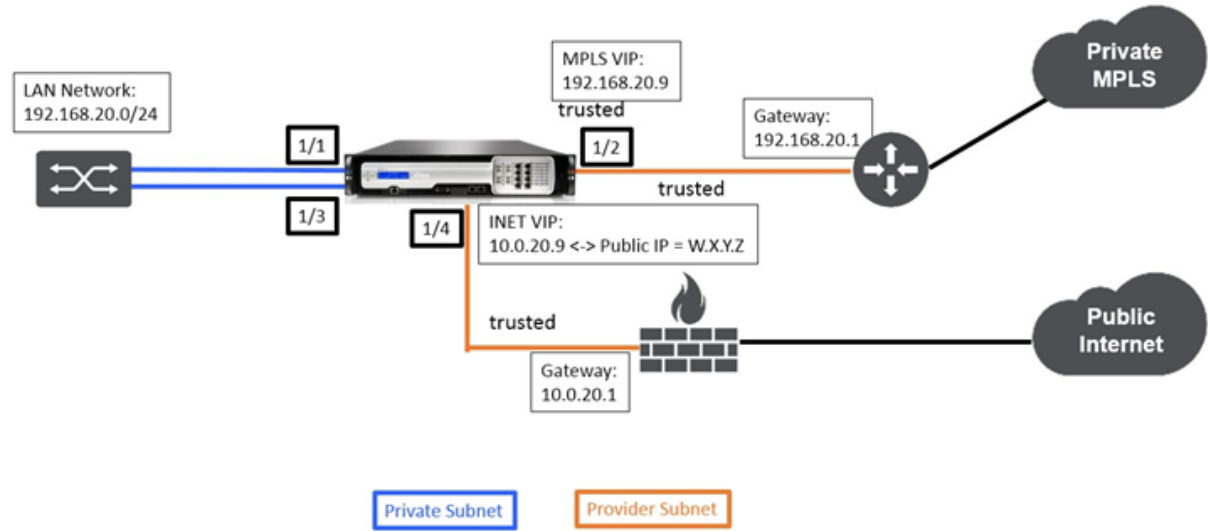
トポロジ

次の図は、SD-WAN ネットワークでサポートされるトポロジを示しています。

Gateway 導入におけるデータセンター



インライン展開でのブランチ



導入の要件

構成を構築する際に役立つように、展開の要件と関連情報を以下に説明します。

サイト名	データセンターサイト	ブランチサイト
アプライアンス名	A_DC1	A_BR1
管理 IP	172.30.2.10/24	172.30.2.20/24
セキュリティキー	もしあれば	もしあれば
モデル/エディション	4000	2000
モード	Gateway	インライン
トポロジ	2 x WAN パス	2 x WAN パス
VIP アドレス	192.168.10.9/24 –MPLS, 10.0.10.9/24 –インターネット (Public IP –A.B.C.D), 192.168.30.1/24-LAN	192.168.20.9/24-MPLS, 10.0.20.9/24 –インターネット (パ ブリック IP –W.X.Y.Z)
Gateway MPLS	192.168.10.1	192.168.20.1
ゲートウェイ・インターネット	10.0.10.1	10.0.20.1
リンク速度	MPLS –100 Mbps, インターネット –20 Mbps	MPLS –10 Mbps, インターネット –2 Mbps

サイト名	データセンターサイト	ブランチサイト
Route	ネットワーク IP アドレス-192.168.31.0/24、サービス IP-ローカル、ゲートウェイ IP アドレス-192.168.30.2	もしあれば
VLAN	もしあれば	もしあれば

構成の前提条件

- SD-WAN アプライアンスをマスターコントロールノードとして有効にします。
- 構成は SD-WAN アプライアンスのマスターコントロールノード (MCN) でのみ行われます。

アプライアンスをマスター・コントロール・ノードとして有効にするには:

1. SD-WAN Web 管理インターフェイスで、[構成] > [アプライアンスの設定] > [管理者インターフェイス] > [その他] タブ > [スイッチコンソール] に移動します。

注

[クライアントコンソールに切り替え]が表示されている場合、アプライアンスはすでに MCN モードになっています。SD-WAN ネットワークには、アクティブな MCN が 1 つだけ存在する必要があります。

2. [構成] > [仮想 WAN] > [構成エディター] の順に選択して、構成を開始します。[New] をクリックして、設定を開始します。

データセンターサイト Gateway モードの設定

データセンターサイトゲートウェイの展開を構成するための高レベルの構成手順を次に示します。

1. DC サイトを作成します。
2. 接続されたイーサネットインターフェイスに基づいてインターフェイスグループを設定します。
3. 各仮想インターフェイスの仮想 IP アドレスを作成します。
4. インターネットおよび MPLS リンクを使用して、バースト速度ではなく、物理レートに基づいて WAN リンクを設定します。
5. LAN インフラストラクチャにさらにサブネットがある場合は、Routes を設定します。

DC サイトを作成するには

1. [構成エディタ]>[サイト]に移動し、[+ 追加] ボタンをクリックします。
2. 以下に示すようにフィールドに入力します。
3. 変更するように指示されない限り、デフォルト設定を保持します。

Add [X]

Site Name:

Region:

Site Location:

Secure Key:

Model:

Mode:

Add **Cancel**

View Site: + Site [Site] [Site]

Sites ?

- Basic Settings
- Centralized Licensing
- Routing Domains
- Interface Groups
- Virtual IP Addresses
- VRRP
- DHCP
- WAN Links
- Certificates
- High Availability

Site Name:

Appliance Name: Secure Key: **Regenerate**

Model: Mode:

Site Location:

Default Direct Route Cost:

Gateway ARP Timer (ms):

☐ Enable Source MAC Learning

Apply **Revert**

接続されたイーサネットインターフェイスに基づいてインターフェイスグループを設定するには

1. 構成エディタで、[サイト]>[サイトの表示]>[**[サイト名]**]>[インタフェースグループ]に移動します。
[+] をクリックして、使用するインターフェイスを追加します。ゲートウェイモードでは、各インターフェイスグループに 1 つのイーサネットインターフェイスが割り当てられます。

- 仮想インターフェイスごとに 1 つのイーサネット/物理インターフェイスだけが使用されるため、バイパスモードは **Failto Block** に設定されます。ブリッジペアはありません。
- この例では、3 つのインターフェイスグループが作成されます。1 つが LAN に面し、もう 2 つは各 WAN リンクに面しています。上記の「DC ゲートウェイモード」トポロジのサンプルを参照し、次に示すように [Interface Groups] フィールドに入力します。

The screenshot displays the configuration page for three virtual interfaces. At the top, a navigation bar includes tabs for Virtual Interfaces, Ethernet Interfaces, Bypass Mode, WCCP, Security, and Delete. Below this, three configuration panels are shown, each for a different virtual interface.

- VirtualInterface-1 (0):** The 'Virtual Interfaces' table shows a single entry 'DC-LAN-1-1' with 'Firewall Zone' set to 'Default_LAN_Zon' and 'VLAN ID' set to '0'. The 'Bridge Pairs' section shows two interfaces connected by a bidirectional arrow.
- VirtualInterface-2 (0):** The 'Virtual Interfaces' table shows a single entry 'INET_DC-WAN-1-4' with 'Firewall Zone' set to '<Default>' and 'VLAN ID' set to '0'. The 'Bridge Pairs' section shows two interfaces connected by a bidirectional arrow.
- VirtualInterface-3 (0):** The 'Virtual Interfaces' table shows a single entry 'MPLS-DC-WAN-1-2' with 'Firewall Zone' set to '<Default>' and 'VLAN ID' set to '0'. The 'Bridge Pairs' section shows two interfaces connected by a bidirectional arrow.

At the bottom of the configuration area, there are 'Apply' and 'Revert' buttons.

仮想インターフェイスごとに仮想 IP (VIP) アドレスを作成するには

- WAN リンクごとに適切なサブネットに VIP を作成します。VIP は、仮想 WAN 環境内の 2 つの SD-WAN アプライアンス間の通信に使用されます。
- LAN ネットワークのゲートウェイアドレスとして使用する仮想 IP アドレスを作成します。

The screenshot displays a table of virtual IP addresses. The table has columns for IP Address / Prefix, Virtual Interface, Firewall Zone, Identity, Private, Security, and Delete. Below the table, there are 'Apply' and 'Refresh' buttons.

IP Address / Prefix	Virtual Interface	Firewall Zone	Identity	Private	Security	Delete
10.0.10.9/24	INET_DC-WAN-1-4 (0)	Default_LAN_Zone	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Trusted	
192.168.10.9/24	MPLS-DC-WAN-1-2 (0)	Default_LAN_Zone	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Trusted	
192.168.30.1/24	DC-LAN-1-1 (0)	Default_LAN_Zone	<input type="checkbox"/>	<input type="checkbox"/>	Trusted	

インターネットリンクを使用して、バースト速度ではなく、物理レートに基づいて WAN リンクを設定するには、次の手順を実行します。

1. [**WAN リンク**] に移動し、[**+ リンクの追加**] ボタンをクリックして、インターネットリンクの WAN リンクを追加します。
2. 以下に示すように、提供されたパブリック IP アドレスなど、インターネットリンクの詳細を入力します。自動検出パブリック **IP** は、MCN として設定された SD-WAN アプライアンスでは選択できません。
3. セクションのドロップダウンメニューから [**Access Interfaces**] に移動し、[**+ 追加**] ボタンをクリックして、インターネットリンクに固有のインターフェイスの詳細を追加します。
4. 以下に示すように、IP アドレスと Gateway アドレスのアクセスインターフェイスを設定します。

WAN Link: BR571-WL-1 Section: Settings + Add Link Delete Link

Basic Settings ?

Note: Changing the access type of this WAN Link may cause automatically generated Paths to this link to be added or removed.

Link Name: BR571-WL-1

Access Type: Public Internet WAN Link Template: <None>

LAN to WAN

Physical Rate (kbps): 10000

☒ Set Permitted From Physical ☐ Auto Learn

Permitted Rate (kbps): 10000

WAN to LAN

Physical Rate (kbps): 10000

☒ Set Permitted From Physical ☐ Auto Learn

Tracking IP Address:

☐ Autodetect Public IP

Public IP Address:

Name	Virtual Interface	IP Address	Gateway IP Address	Virtual Path Mode	Priority	ARP	Delete
SJC_DC-INET-AI-1	INET_DC-WAN-1-4	10.0.10.9	10.0.10.1	Primary			

MPLS リンクを作成するには

1. [**WAN リンク**] に移動し、[**+**] ボタンをクリックして、MPLS リンクの WAN リンクを追加します。

- 2. 次に示すように、MPLS リンクの詳細を入力します。
- 3. [**Access Interfaces**] に移動し、[+] ボタンをクリックして、MPLS リンクに固有のインターフェイス詳細を追加します。
- 4. 以下に示すように、IP アドレスと Gateway アドレスのアクセスインターフェイスを設定します。

Basic Settings ?

Note: Changing the access type of this WAN Link may cause automatically generated Paths to this link to be added or removed.

Link Name:

BR571-WL-1

Access Type:

Private MPLS

WAN Link Template:

<None>

LAN to WAN

Physical Rate (kbps):

10000

☒ Set Permitted From Physical

Permitted Rate (kbps):

10000

WAN to LAN

Physical Rate (kbps):

10000

☒ Set Permitted From Physical

Permitted Rate (kbps):

10000

Name	Virtual Interface	IP Address	Gateway IP Address	Virtual Path Mode	Poizy ARP	Delete
SJC_DC-MPLS-...	MPLS-DC-WAN-1-2	192.168.10.9	192.168.10.1	Primary	<input type="checkbox"/>	

ルートを設定するには

ルートは、上記の設定に基づいて自動作成されます。上記の DC LAN サンプルトポロジには、**192.168.31.0/24** という追加の LAN サブネットがあります。このサブネットのルートを作成する必要があります。ゲートウェイ IP アドレスは、次に示すように DC LAN VIP と同じサブネット内に存在する必要があります。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

290

+

Search

Order	Network IP Address	Cost	Service Type	Service Name	Gateway IP Address	Info	Edit	Delete
1	192.168.31.0/24	5	Local		192.168.30.2			
2	192.175.58.0/24	5	Virtual Path	BR571				
3	192.175.59.0/24	5	Virtual Path	BR572				
4	192.175.60.0/24	5	Virtual Path	BR573				
5	192.175.61.0/24	5	Virtual Path	BR574				
6	192.175.62.0/24	5	Virtual Path	BR575				
7	172.111.64.5/24	5	Local					
8	172.111.65.5/24	5	Local					
9	0.0.0.0/0	65535	Passthrough					

⏪

⏩

1

⏪

⏩

ブランチサイトのインライン展開設定

次に、インライン展開用にブランチサイトを構成するための高レベルの構成手順を示します。

- 1. ブランチサイトを作成します。
- 2. 接続されたイーサネットインターフェイスに基づいてインターフェイスグループを設定します。
- 3. 各仮想インターフェイスの仮想 IP アドレスを作成します。
- 4. インターネットおよび MPLS リンクを使用して、バースト速度ではなく、物理レートに基づいて WAN リンクを設定します。
- 5. LAN インフラストラクチャにさらにサブネットがある場合は、Routes を設定します。

ブランチサイトを作成するには

- 1. [構成エディタ] > [サイト] に移動し、[+] [追加] ボタンをクリックします。
- 2. 以下に示すようにフィールドに入力します。
- 3. 変更するように指示されない限り、デフォルト設定を保持します。

Add

Site Name:

BR_Site

Secure Key:

dd40529b4c910e...

Model:

210

Sub Model:

BASE

Mode:

client

Site Location:

Add

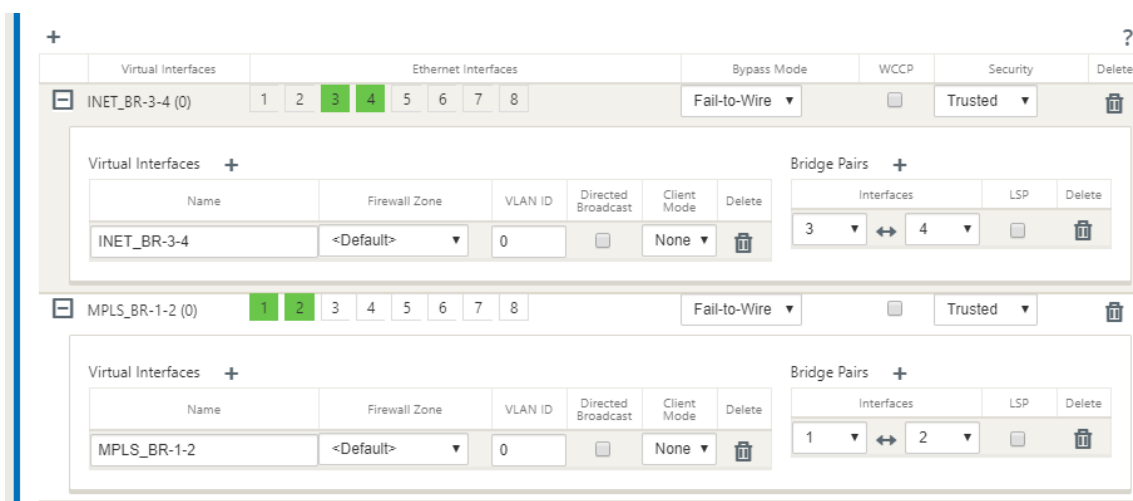
Cancel

The screenshot shows the Citrix SD-WAN 11.4 configuration interface. At the top, there are tabs: Basic, Global, Sites (selected), Connections, Optimization, and Provisioning. Below the tabs, there's a 'Region' dropdown set to 'Default_Region'. Under 'Site:', there's a dropdown set to 'BR_Site' and buttons for '+ Site', 'Site' (with a copy icon), and 'Site' (with a delete icon). A 'Sites' sidebar on the left lists various configuration options: Basic Settings (selected), Centralized Licensing, Routing Domains, Link Aggregation Groups, Interface Groups, Virtual IP Addresses, VRRP, DHCP, DNS, Proxy Auto-config settings, WAN Links, Certificates, and High Availability. The main configuration area on the right for 'BR_Site' includes:

- Site Name: BR_Site
- Appliance Name: BR_Site-210
- Secure Key: dd40529b4c910e... with a 'Regenerate' button
- Model: 210
- Sub Model: BASE
- Mode: client
- Site Location: (empty field)
- Default Direct Route Cost: 5
- Gateway ARP Timer (ms): 1000
- Host ARP Timer (ms): 1000
- ☐ Enable Source MAC Learning
- Buttons: Apply, Refresh

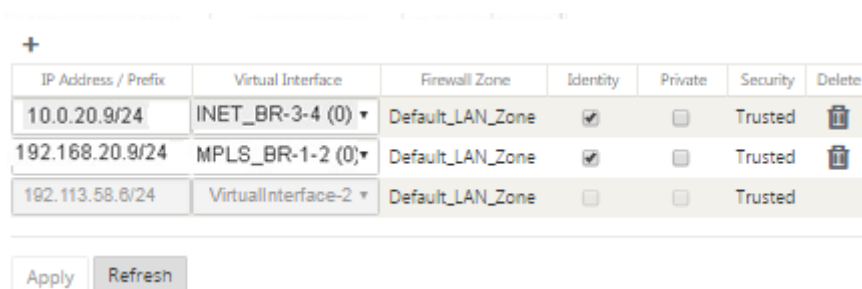
接続されたイーサネットインターフェイスに基づいてインターフェイスグループを設定するには

1. 構成エディタで、[サイト] > [サイトの表示] > [**[クライアントサイト名]**] > [インターフェイスグループ] に移動します。[+] をクリックして、使用するインターフェイスを追加します。インラインモードの場合、各インターフェイスグループには 2 つのイーサネットインターフェイスが割り当てられます。
2. バイパスモードは **fail-to-wire** に設定され、ブリッジペアは 2 つのイーサネットインターフェイスを使用し作成されます。
3. 上記の「リモートサイトインラインモード」トポロジのサンプルを参照し、次に示すように [Interface Groups] フィールドに入力します。



仮想インターフェイスごとに仮想 **IP (VIP)** アドレスを作成するには

1. 各 WAN リンクの適切なサブネット上に仮想 IP アドレスを作成します。VIP は、仮想 WAN 環境内の 2 つの SD-WAN アプライアンス間の通信に使用されます。



インターネットリンクを使用して、バースト速度ではなく、物理レートに基づいて WAN リンクを設定するには、次の手順を実行します。

1. [**WAN** リンク] に移動し、[+] ボタンをクリックして、インターネットリンクの WAN リンクを追加します。
2. 以下に示すように、自動検出パブリック IP アドレスなど、インターネットリンクの詳細を入力します。
3. [**Access Interfaces**] に移動し、[+] ボタンをクリックして、インターネットリンクに固有のインターフェイス詳細を追加します。
4. 以下に示すように、IP アドレスと Gateway のアクセスインターフェイスを設定します。

WAN Link: BR571-WL-1

Section: Settings

+ Add Link

Delete Link

Basic Settings

Note: Changing the access type of this WAN Link may cause automatically generated Paths to this link to be added or removed.

Link Name:
BR571-WL-1

Access Type:
Public Internet

WAN Link Template:
<None>

LAN to WAN

Physical Rate (kbps):
10000

☒ Set Permitted From Physical

☐ Auto Learn

Permitted Rate (kbps):
10000

WAN to LAN

Physical Rate (kbps):
10000

☒ Set Permitted From Physical

☐ Auto Learn

Permitted Rate (kbps):
10000

Tracking IP Address:

☐ Autodetect Public IP

Public IP Address:

Name	Virtual Interface	IP Address	Gateway IP Address	Virtual Path Mode	Proxy ARP	Delete
SJC_BR-INET-AI-1	INET_BR-3-4	10.0.20.9	10.0.20.1	Primary	<input checked="" type="checkbox"/>	

MPLS リンクを作成するには

1. [WAN リンク] に移動し、[+] ボタンをクリックして、MPLS リンクの WAN リンクを追加します。
2. 次に示すように、MPLS リンクの詳細を入力します。
3. [Access Interfaces] に移動し、[+] ボタンをクリックして、MPLS リンクに固有のインターフェースの詳細を追加します。
4. 以下に示すように、IP アドレスと Gateway のアクセスインターフェースを設定します。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

295

Basic Settings

Note: Changing the access type of this WAN Link may cause automatically generated Paths to this link to be added or removed.

Link Name:

BR571-WL-1

Access Type:

Private MPLS

WAN Link Template:

<None>

LAN to WAN

Physical Rate (kbps):

10000

☒ Set Permitted From Physical

Permitted Rate (kbps):

10000

WAN to LAN

Physical Rate (kbps):

10000

☒ Set Permitted From Physical

Permitted Rate (kbps):

10000

Name	Virtual Interface	IP Address	Gateway IP Address	Virtual Path Mode	Proxy ARP	Delete
SJC_BR-MPLS-...	MPLS_BR-1-2	192.168.20.9	192.168.20.1	Primary	<input checked="" type="checkbox"/>	

ルートを設定するには

ルートは、上記の設定に基づいて自動作成されます。このリモートブランチオフィスに固有のサブネットが増える場合は、それらのバックエンドサブネットに到達するためにトラフィックを誘導する Gateway を特定する特定のルートを追加する必要があります。

+

Search:

Order	Network IP Address	Cost	Service Type	Service Name	Gateway IP Address	Info	Edit	Delete
1	10.0.20.9/24	5	Local					
2	192.168.20.9/24	5	Local	BR571				
3	192.175.59.0/24	5	Virtual Path	BR572				
4	192.175.60.0/24	5	Virtual Path	BR573				
5	192.175.61.0/24	5	Virtual Path	BR574				
6	192.175.62.0/24	5	Virtual Path	BR575				
7	172.111.64.5/24	5	Local					
8	172.111.65.5/24	5						
9	0.0.0.0/0	65535	Passthrough					

⏪

⏩

1

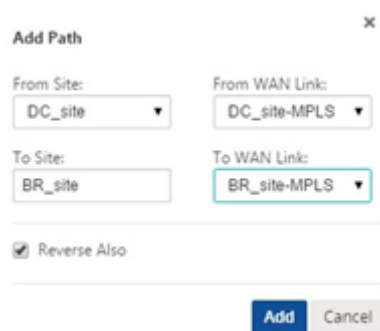
⏪

⏩

監査エラーを解決する

DC サイトとブランチサイトの構成が完了すると、DC サイトと BR サイトの両方で監査エラーを解決するように警告が表示されます。

デフォルトでは、アクセスタイプ [パブリックインターネット] として定義された WAN リンクのパスが生成されます。アクセスタイプが [プライベートインターネット] の WAN リンクでは、自動パスグループ機能を使用するか、手動でパスを有効にする必要があります。MPLS リンクのパスは、緑の四角形にある [Add operator] をクリックして有効にすることができます。



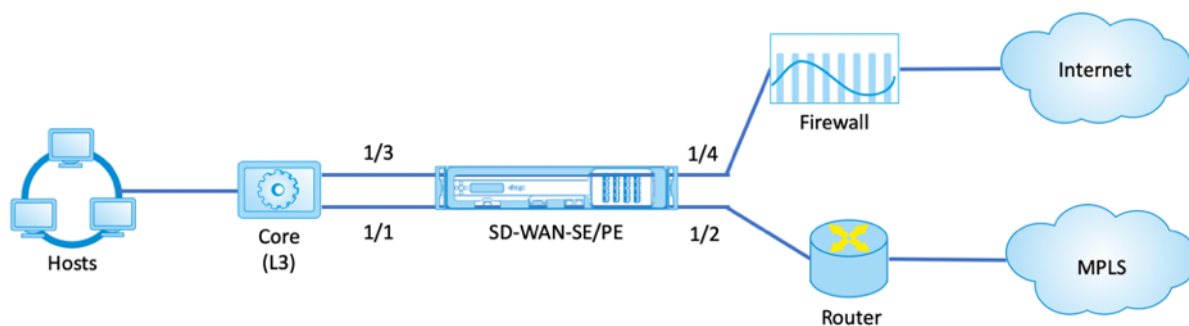
上記の手順をすべて完了したら、[SD-WAN アプライアンスパッケージの準備](#)に進みます。

インラインモード

May 10, 2021

この記事では、インライン展開モードでブランチを構成する方法について詳しく説明します。このモードでは、SD-WAN アプライアンスはイーサネットブリッジのように見えます。SD-WAN アプライアンスモデルのほとんどは、インラインモード用の配線接続（イーサネットバイパス）機能を備えています。電源が故障すると、リレーが閉じ、入力ポートと出力ポートが電氣的に接続され、イーサネット信号がポート間で通過できるようになります。Fail-to-Wire モードでは、SD-WAN アプライアンスは 2 つのポートを接続するクロスオーバーケーブルのように見えます。

次の図では、インターフェイス 1/1 および 1/2 はハードウェアバイパスペアであり、コアとエッジ MPLS ルータを接続するフェールツーワイヤです。インターフェイス 1/3 および 1/4 はハードウェアバイパスペアでもあり、コアをエッジファイアウォールに接続するフェールツーワイヤリングを行います。



ブランチサイトのインライン展開設定

次に、インライン展開用にブランチサイトを構成するための高レベルの構成手順を示します。

1. ブランチサイトを作成します。
2. 接続されたイーサネットインターフェイスに基づいてインターフェイスグループを設定します。
3. 各仮想インターフェイスの仮想 IP アドレスを作成します。
4. インターネットおよび MPLS リンクを使用して、バースト速度ではなく、物理レートに基づいて WAN リンクを設定します。
5. LAN インフラストラクチャにさらにサブネットがある場合は、Routes を設定します。

ブランチサイトを作成するには

1. [構成エディタ] > [サイト] に移動し、[+ 追加] ボタンをクリックします。
2. 変更するように指示されない限り、デフォルト設定を保持します。

Region: Default_Region

Site: BR_Site + Site Site Delete Site

Sites

- Basic Settings
- Centralized Licensing
- Routing Domains
- Link Aggregation Groups
- Interface Groups
- Virtual IP Addresses
- VRRP
- DHCP
- DNS
- Proxy Auto-config settings
- WAN Links
- Certificates
- High Availability

Site Name: BR_Site

Appliance Name: BR_Site-210 Secure Key: dd40529b4c910e... Regenerate

Model: 210 Sub Model: BASE

Mode: client Site Location:

Default Direct Route Cost: 5

Gateway ARP Timer (ms): 1000

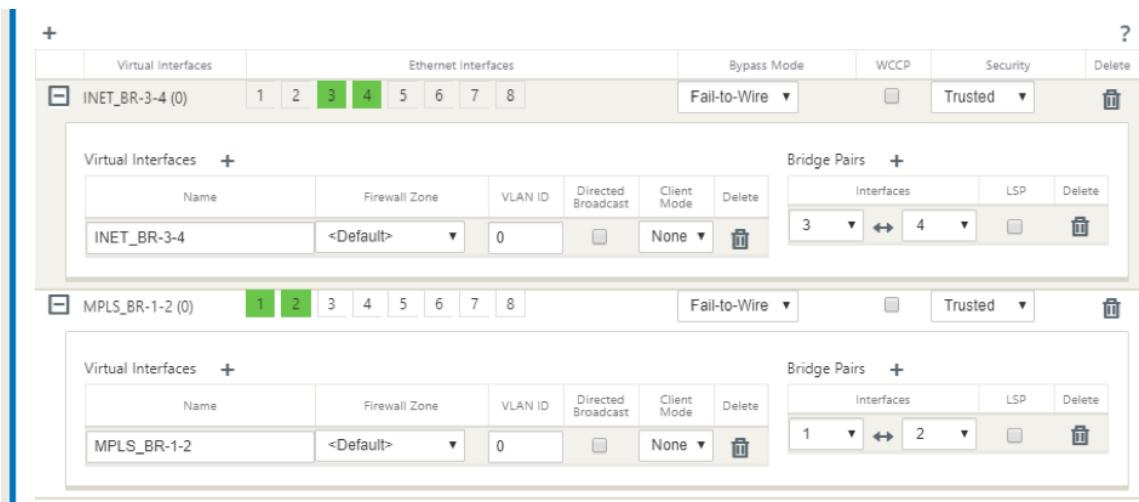
Host ARP Timer (ms): 1000

☐ Enable Source MAC Learning

Apply Refresh

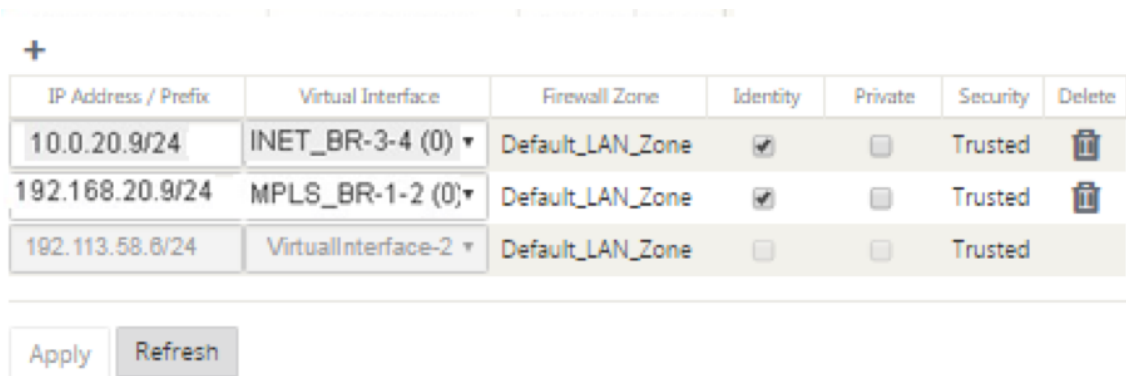
接続されたイーサネットインターフェイスに基づいてインターフェイスグループを設定するには

1. 構成エディタで、[サイト] > [サイトの表示] > [[クライアントサイト名]] > [インターフェイスグループ] に移動します。[+] をクリックして、使用するインターフェイスを追加します。インラインモードの場合、各インターフェイスグループには 2 つのイーサネットインターフェイスが割り当てられます。
2. バイパスモードは **fail-to-wire** に設定され、ブリッジペアは 2 つのイーサネットインターフェイスを使用し作成されます。
3. 上記のサンプルトポロジを参照し、次に示すように [Interface Groups] フィールドに入力します。



仮想インターフェイスごとに仮想 **IP (VIP)** アドレスを作成するには

1. 各 WAN リンクの適切なサブネット上に仮想 IP アドレスを作成します。VIP は、仮想 WAN 環境内の 2 つの SD-WAN アプライアンス間の通信に使用されます。



インターネットリンクを使用してバースト速度ではなく、物理レートに基づいて **WAN** リンクを設定するには

1. [**WAN** リンク] に移動し、[+] ボタンをクリックして、インターネットリンクの WAN リンクを追加します。
2. 以下に示すように、自動検出パブリック IP アドレスなど、インターネットリンクの詳細を入力します。
3. [**Access Interfaces**] に移動し、[+] ボタンをクリックして、インターネットリンクに固有のインターフェイスの詳細を追加します。
4. 以下に示すように、IP アドレスと Gateway のアクセスインターフェースを設定します。

WAN Link: BR571-WL-1

Section: Settings

+ Add Link

Delete Link

Basic Settings

Note: Changing the access type of this WAN Link may cause automatically generated Paths to this link to be added or removed.

Link Name:
BR571-WL-1

Access Type:
Public Internet

WAN Link Template:
<None>

LAN to WAN

Physical Rate (kbps):
10000

☒ Set Permitted From Physical

☐ Auto Learn

Permitted Rate (kbps):
10000

WAN to LAN

Physical Rate (kbps):
10000

☒ Set Permitted From Physical

☐ Auto Learn

Permitted Rate (kbps):
10000

Tracking IP Address:

☐ Autodetect Public IP

Public IP Address:

Name	Virtual Interface	IP Address	Gateway IP Address	Virtual Path Mode	Proxy ARP	Delete
SJC_BR-INET-AI-1	INET_BR-3-4	10.0.20.9	10.0.20.1	Primary	<input checked="" type="checkbox"/>	

MPLS リンクを作成するには

1. [WAN リンク] に移動し、[+] ボタンをクリックして、MPLS リンクの WAN リンクを追加します。
2. 次に示すように、MPLS リンクの詳細を入力します。
3. [アクセスインターフェイス] に移動し、[+] ボタンをクリックして、MPLS リンクに固有のインターフェイスの詳細を追加します。
4. 以下に示すように、IP アドレスと Gateway のアクセスインタフェースを設定します。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

301

Basic Settings

Note: Changing the access type of this WAN Link may cause automatically generated Paths to this link to be added or removed.

Link Name:

BR571-WL-1

Access Type:

Private MPLS

WAN Link Template:

<None>

LAN to WAN

Physical Rate (kbps):

10000

☒ Set Permitted From Physical

Permitted Rate (kbps):

10000

WAN to LAN

Physical Rate (kbps):

10000

☒ Set Permitted From Physical

Permitted Rate (kbps):

10000

Name	Virtual Interface	IP Address	Gateway IP Address	Virtual Path Mode	Proxy/ARP	Delete
SJC_BR-MPLS-...	MPLS_BR-1-2	192.168.20.9	192.168.20.1	Primary	<input checked="" type="checkbox"/>	

ルートを設定するには

ルートは、上記の設定に基づいて自動作成されます。このリモートブランチオフィスに固有のサブネットがさらに存在する場合は、それらのバックエンドサブネットに到達するためにトラフィックを誘導する Gateway を特定する特定のルートを追加する必要があります。

Search:

Order	Network IP Address	Cost	Service Type	Service Name	Gateway IP Address	Info	Edit	Delete
1	10.0.20.9/24	5	Local					
2	192.168.20.9/24	5	Local	BR571				
3	192.175.59.0/24	5	Virtual Path	BR572				
4	192.175.60.0/24	5	Virtual Path	BR573				
5	192.175.61.0/24	5	Virtual Path	BR574				
6	192.175.62.0/24	5	Virtual Path	BR575				
7	172.111.64.5/24	5	Local					
8	172.111.65.5/24	5						
9	0.0.0.0/0	65535	Passthrough					

仮想インラインモード

November 8, 2021

仮想インラインモードでは、ルータは PBR、OSPF、BGP などのルーティングプロトコルを使用して、着信および発信 WAN トラフィックをアプライアンスにリダイレクトし、アプライアンスは処理されたパケットをルータに転送します。

次の資料では、2 つの SD-WAN (SD-WAN SE) アプライアンスを構成する手順について説明します。

- 仮想インラインモードのデータセンターアプライアンス
- インラインモードのブランチアプライアンス
- ルーティングプロトコルは、コアシッチで設定するか、ルータでさらにアップストリームで設定する必要があります。ルータは SD-WAN アプライアンスの健全性を監視し、障害が発生した場合にアプライアンスをバイパスできるようにする必要があります。
- 仮想インラインモードでは、SD-WAN アプライアンスは物理的にパス外（ワンアーム展開）になります。つまり、バイパスモードが Fail-to-Block (FTB) に設定された単一のイーサネットインターフェイス（例：インターフェイス 1/5）のみが使用されます。

Citrix SD-WAN アプライアンスは、トラフィックを適切な Gateway に渡すように構成する必要があります。仮想パス用のトラフィックは SD-WAN アプライアンスに向けられ、カプセル化され、適切な WAN リンクに送信されます。

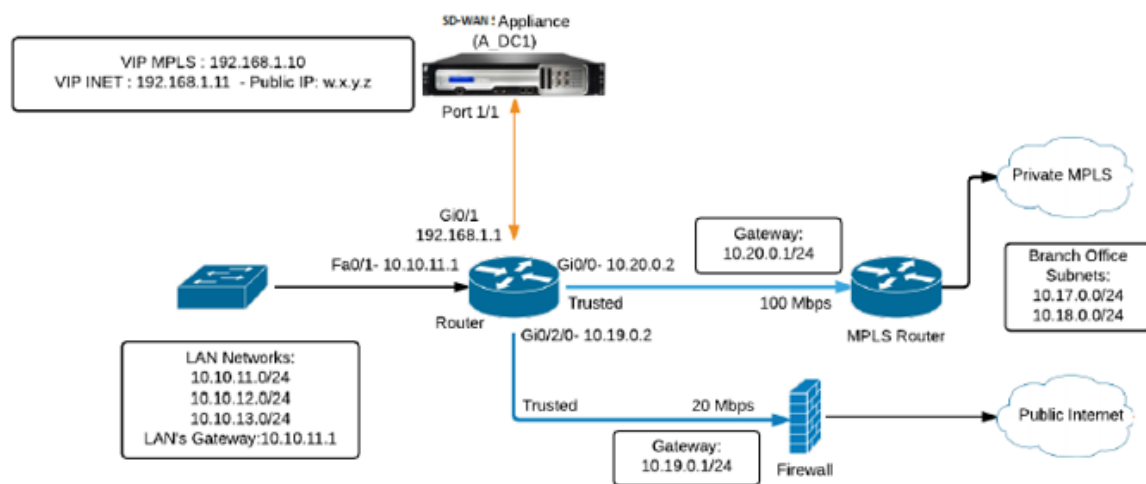
情報を収集する

仮想インラインモードの設定に必要な次の情報を収集します。

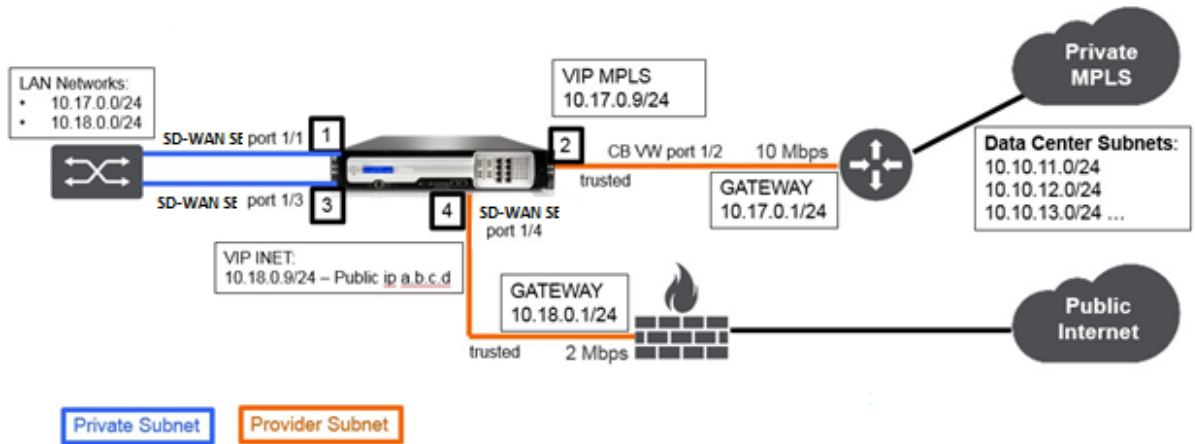
- 以下を含む、ローカルサイトとリモートサイトの正確なネットワーク図
 - ローカルおよびリモートの WAN リンクおよび両方向の帯域幅、サブネット、各リンク、ルート、VLAN からの仮想 IP アドレスおよびゲートウェイ。
- デプロイメントテーブル

次に、ネットワークダイアグラムと配置テーブルの例を示します。

データセンターのトポロジー-仮想インラインモード



ブランチトポロジインラインモード



サイト名	データ・センター・サイト	ブランチサイト
アプライアンス名	SJC-DC	SJC-BR
管理 IP	172.30.2.10/24	172.30.2.20/24
セキュリティキー	もしあれば	もしあれば
モデル/ Edition	4000	2000
Mode	仮想インラインモード	インライン
トポロジ	2 x WAN パス	2 x WAN パス
VIP アドレス	192.168.1.10/24 –MPLS, 192.168.2.10/24 –インターネット, パブリック IP w.x.y.z	10.17.0.9/24-MPLS, 10.18.0.9/24 –インターネット, パ ブリック IP a.b.c.d
Gateway MPLS	10.20.0.1	10.17.0.1
Gateway・インターネット	10.19.0.1	10.18.0.1
リンク速度	MPLS –100 Mbps, インターネット –20 Mbps	MPLS –10 Mbps, インターネット –2 Mbps

サイト名	データ・センター・サイト	ブランチサイト
Route	物理インターフェイスのいずれかを介して LAN サブネット (10.10.11.0/24、10.10.12.0/24、10.10.13.0/24、など) に到達する方法について、SD-WAN SE アプライアンスのルートを追加する必要があります。Gi0/1-192.168.1.1、構成 > 仮想 WAN > 設定エディタ > SJC_DC\ > ルート。この例では、インターフェイス 192.168.1.1 が使用されています。- なしアドレス:10.10.13.0/24、10.10.12.0/24、10.10.11.0/24、- サービスタイプ: ローカル、- Gateway IP アドレス:192.168.1.1	追加のルートは追加されませんでした
VLAN	MPLS-VLAN 10、インターネット-VLAN 20	なし (デフォルト 0)

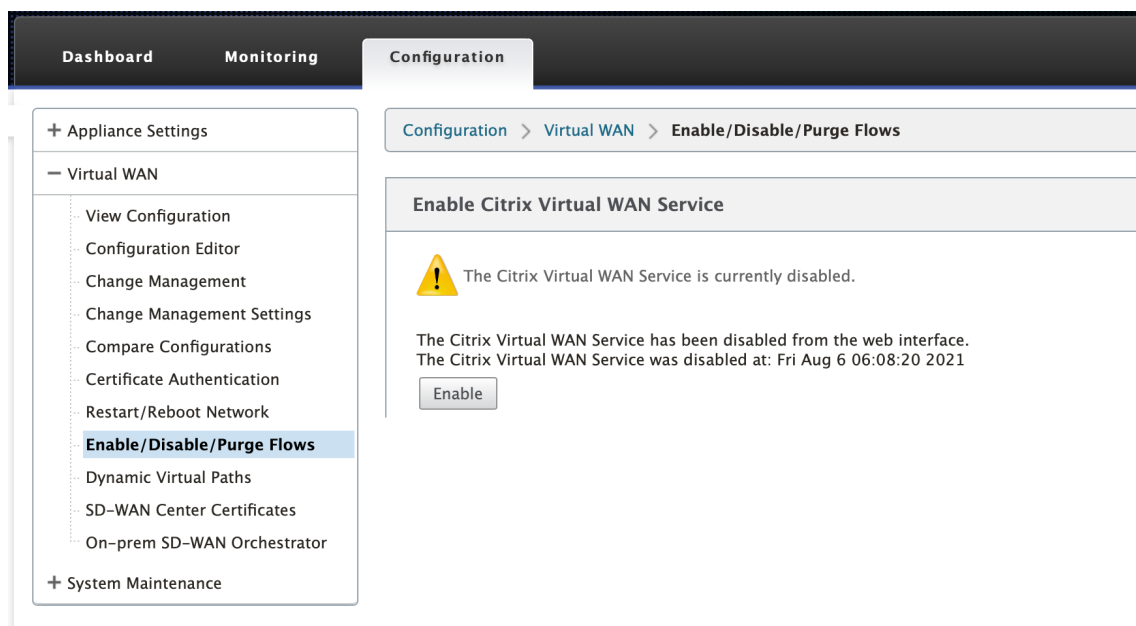
前提条件

1. SD-WAN アプライアンス Web 管理インターフェイスで、構成 > アプライアンスの設定 > 管理者インターフェイス > その他タブに移動し、スイッチコンソールをクリックします。

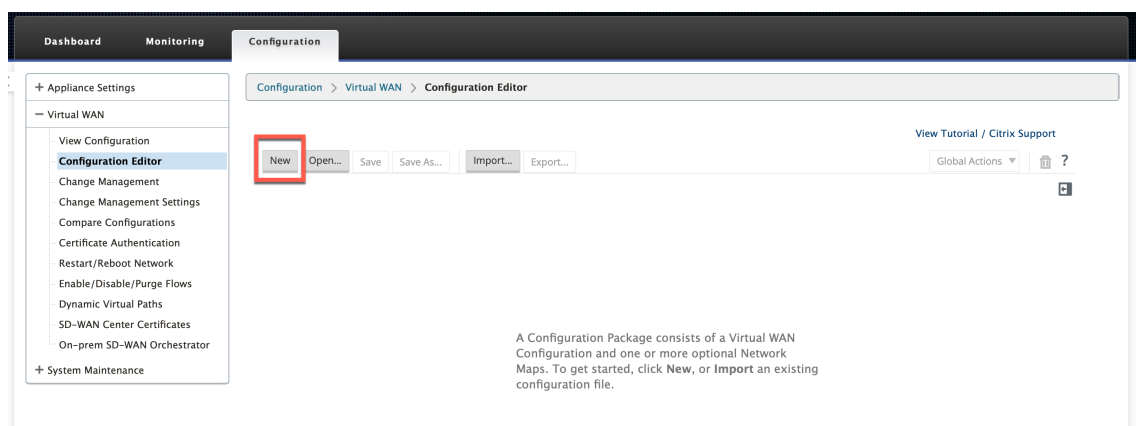
(注

) [クライアントコンソールに切り替え] が表示されている場合、アプライアンスはすでに MCN モードになっています。SD-WAN ネットワークには、アクティブな MCN が 1 つだけ必要です。

2. [** 構成] > [仮想 **WAN**] > [フローの有効化/無効化/消去] に移動し、[**Citrix** 仮想 **WAN** サービスの有効化] セクションで [有効] をクリックします。 **



3. 設定 > 仮想 WAN > 設定エディタに移動して、設定を開始します。[**New**] をクリックして、設定を開始します。[新規] をクリックすると、ファイル名に **Untitled_1** を持つ初期設定ファイルが作成されます。[オプションファイルの名前は]、後で [名前を付けて保存] ボタンを使用して変更できます。



データセンターサイト-仮想インラインモードの設定

データセンターサイトを作成する

1. 設定 > 仮想 WAN > 設定エディタ > サイトに移動し、+ サイトをクリックします。
2. サイトの名前と場所を入力します。[モデル (Model)] ドロップダウンリストからアプライアンスモデルを選択し、[モード (Mode)] ドロップダウンリストからプライマリ **MCN** を選択します。
3. [追加] をクリックします。

Add

Site Name:
SJC-DC

Secure Key:
f7944db45d32ca14

Model:
4000 ▼

Mode:
primary MCN ▼

Site Location:
AMER

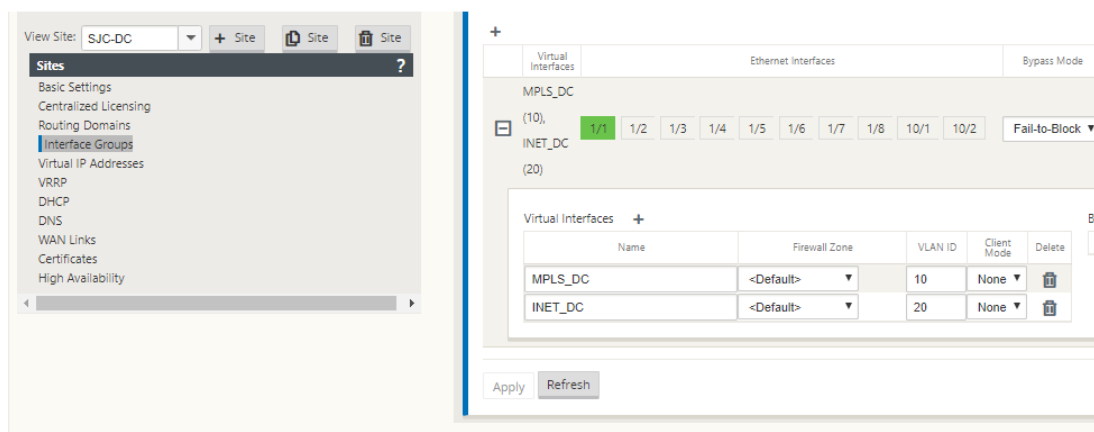
☒ Enable Site as Intermediate Node

Add Cancel

接続されたイーサネットインターフェイスに基づくインターフェイスグループの設定

仮想インラインモードの設定では、1つのイーサネットインターフェイス、つまりルーティングポリシーの影響を提供するアップストリームルータを接続するインターフェイスだけが使用されます（例：インターフェイス 1/5）。仮想インターフェイスごとに1つのイーサネット/物理インターフェイスだけが使用されるため、バイパスモードは Fail-to-Block (FTB) に設定されます。また、ブリッジペアはありません。

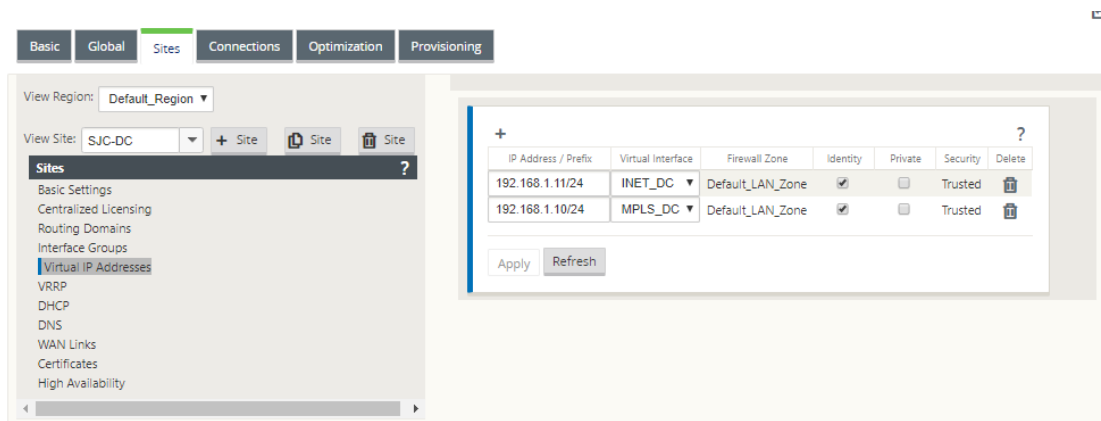
1. 構成エディタで、[サイト] > [[サイト名]] > [インターフェイスグループ] に移動します。[+] をクリックして、使用するインターフェイスを追加します。
2. アップストリームルータに接続するイーサネットインターフェイスを選択し、[仮想インターフェイス (Virtual Interfaces)] の横にある [+] をクリックします。MPLS リンクとインターネットリンクの両方の仮想インターフェイスを追加します。サンプルトポロジに従って、以下を追加します。
 - **VLAN 10** に設定された仮想インターフェイス **MPLS**
 - **VLAN 20** に設定された仮想インターフェイスインターネット
3. [バイパスモード] ドロップダウンリストから [**Fail-to-Block**] を選択します。[Apply] をクリックします。



仮想インターフェイスごとに仮想 **IP** アドレスを作成する

各 WAN リンクの適切なサブネット上に仮想 IP (VIP) アドレスを作成します。VIP は、仮想 WAN 環境内の 2 つの SD-WAN アプライアンス間の通信に使用されます。

1. 構成エディタで、[サイト] > [サイト名] > [仮想 **IP** アドレス] に移動します。[+] をクリックして VIP を作成します。
2. IP アドレス/プレフィックスを入力し、MPLS とインターネットに対応する仮想インターフェイスを選択します。
3. [**Apply**] をクリックします。



インターネット **WAN** リンクの作成

バースト速度ではなく物理レートに基づいてインターネット WAN リンクを作成します。

1. 構成エディタで、[サイト] > [サイト名] > [**WAN** リンク] に移動し、[+ リンク] をクリックします。名前を入力し、[アクセスタイプ] として [パブリックインターネット] を選択します。[追加] をクリックします。

2. 現物レートを入力します。[パブリック IP を自動検出する] チェックボックスは選択しないでください。MCN として構成されている SD-WAN アプライアンスの場合、[パブリック IP を自動検出] チェックボックスは選択できません。

WAN Link: SJC-DC-INET Section: Settings + Add Link Delete Link

Basic Settings

Link Name: SJC-DC-INET

Access Type: Public Internet WAN Link Template: <None>

LAN to WAN

Physical Rate (kbps): 20000

☒ Set Permitted From Physical

Permitted Rate (kbps): 20000

WAN to LAN

Physical Rate (kbps): 20000

☒ Set Permitted From Physical

Permitted Rate (kbps): 20000

Tracking IP Address:

☐ Autodetect Public IP

Public IP Address:

Advanced Settings

Eligibility

Metered/Standby Link

Provisioning

Apply Revert

3. [セクション (Section)] ドロップダウンリストから [アクセスインターフェイス (Access Interfaces)] を選択し、[+] ボタンをクリックして、インターネットリンクに固有のインターフェイスの詳細を追加します。
4. インターネット WAN 仮想 IP アドレスとゲートウェイアドレスを入力します。プロキシ ARP では、イーサネットインターフェイスが 2 つ未満の場合はチェックされません。
5. [Apply] をクリックします。

WAN Link: SJC-DC-INET Section: Access Interfaces + Add Link Delete Link

Name	Virtual Interface	IP Address	Gateway IP Address	Virtual Path Mode	Proxy ARP	Gateway MAC Address Binding	Delete
SJC-DC-INET-AI-1	INET_DC	192.168.1.11	192.168.1.1	Primary	<input type="checkbox"/>	<input checked="" type="checkbox"/>	

Apply Refresh

MPLS リンクの作成

1. [サイト] > [サイト名] > [WAN リンク] ページで、[セクション] ドロップダウンリストから [設定] を選択します。[+ リンク (+ Link)] ボタンをクリックして、MPLS 用の WAN リンクを追加します。
2. MPLS WAN リンク名を入力し、[アクセスタイプ] を [プライベートイントラネット] として選択します。[追加] をクリックします。
3. 現物レートおよびその他の詳細を入力します。[Apply] をクリックします。

Basic Settings

LAN to WAN

Physical Rate (kbps):
100000

☒ Set Permitted From Physical

Permitted Rate (kbps):
100000

WAN to LAN

Physical Rate (kbps):
100000

☒ Set Permitted From Physical

Permitted Rate (kbps):
100000

Access Type:

Private Intranet

☐ Autodetect Public IP

Public IP Address:

Tracking IP Address:

Name	Virtual Interface	IP Address	Gateway IP Address	Virtual Path Mode	Proxy ARP	Gateway MAC Address Binding	Delete
SJC-DC-MPLS-A...	MPLS_DC	192.168.1.10	192.168.1.9	Primary	<input type="checkbox"/>	<input checked="" type="checkbox"/>	

4. [セクション (Section)] ドロップダウンリストから [アクセスインターフェイス (Access Interfaces)] を選択し、[+] ボタンをクリックして、MPLS リンクに固有のインターフェイスの詳細を追加します。
5. MPLS 仮想 IP アドレスと Gateway アドレスを入力します。プロキシ ARP では、イーサネットインターフェイスが 2 つ未満の場合はチェックされません。
6. [Apply] をクリックします。

WAN Link: SJC-DC-MPLS Section: Access Interfaces (IPv4)

+ Link

Link

+

Name	Virtual Interface	IP Address	Gateway IP Address	Virtual Path Mode	Proxy ARP	Gateway MAC Address Binding	Delete
SJC-DC-MPLS-A...	MPLS_DC	192.168.1.10	192.168.1.1	Primary	<input type="checkbox"/>	<input checked="" type="checkbox"/>	

Apply

Revert

ルートを設定する

データセンター側で、任意の物理インターフェイスを経由して LAN サブネット（10.10.11.0/24、10.10.12.0/24、10.10.13.0/24 など）に到達する方法について、SD-WAN アプライアンスにルートを追加します。

VLAN 10 上の 0/1/0.1 –192.168.1.1

VLAN 20 上の 0/1/0.2 –192.168.2.1

この例では、インターフェイス 192.168.1.1 が使用されています。

設定エディタで、[接続] > [ルート] に移動し、[+] をクリックしてルートを追加します。

ネットワーク **IP** アドレス、コスト、および **Gateway** アドレスを入力します。[追加] をクリックします。

Edit?×

Network IP Address

10.10.11.0/24

Routing Domain

Default_RoutingD

Cost

5

Service Type

Local

Gateway IP Address

192.168.1.1

☒ Export Route

☐ Summary Route

☐ Eligibility Based On Path

Path:

<None>

☐ Eligibility Based On Gateway

Apply

Cancel

ブランチサイトのインライン展開設定

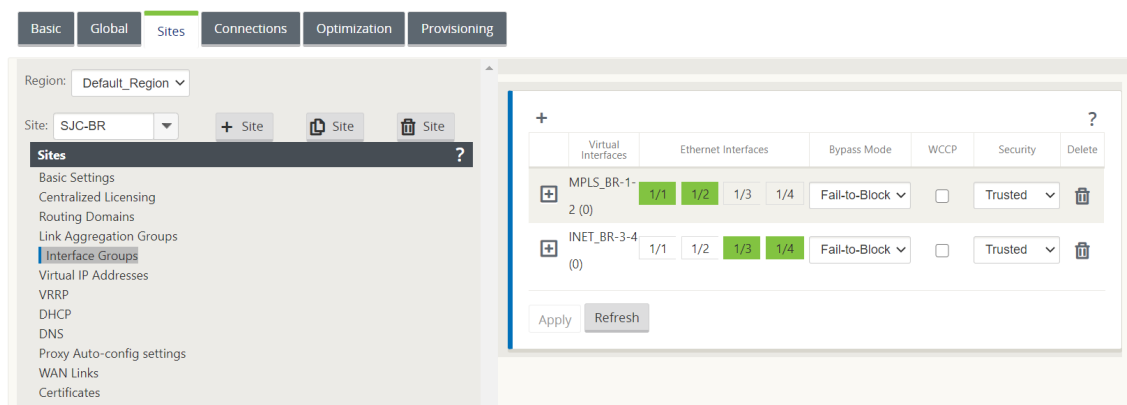
ブランチサイトの作成

1. [構成エディタ] > [サイト] に移動し、[+ サイト] をクリックします。
2. サイトの名前と場所を入力します。[Model] ドロップダウンリストからアプライアンスモデルを選択し、[**Mode**] ドロップダウンリストから [**Client**] を選択します。
3. [追加] をクリックします。

接続されたイーサネットインターフェイスに基づくインターフェイスグループの設定

1. 構成エディタで、[サイト] > [[クライアントサイト名]] > [インターフェイスグループ] に移動します。[+] をクリックして、使用するインターフェイスを追加します。インラインモード設定では、インターフェイスペア 1/3、1/4、インターフェイスペア 1/1 および 1/2 の 4 つのイーサネットインターフェイスが使用されます。
2. 仮想インターフェイスごとに 2 つのイーサネット/物理インターフェイスが使用されるため、バイパスモードを fail-to-Wire に設定します。ブリッジペアは 2 つあります。
3. [仮想インターフェイス] の横にある [+] をクリックし、インターネットおよび MPLS リンクを使用して、バースト速度ではなく物理レートに基づいて WAN リンクを設定します。
 - ブリッジペア 1/3 および 1/4 に設定された仮想インターフェイスインターネット
 - ブリッジペア 1/1 および 1/2 に設定された仮想インターフェイス **MPLS**。
4. [**Bridge Pairs**] の横にある [+] をクリックし、適切なインターフェイスを選択してブリッジペアを作成します。

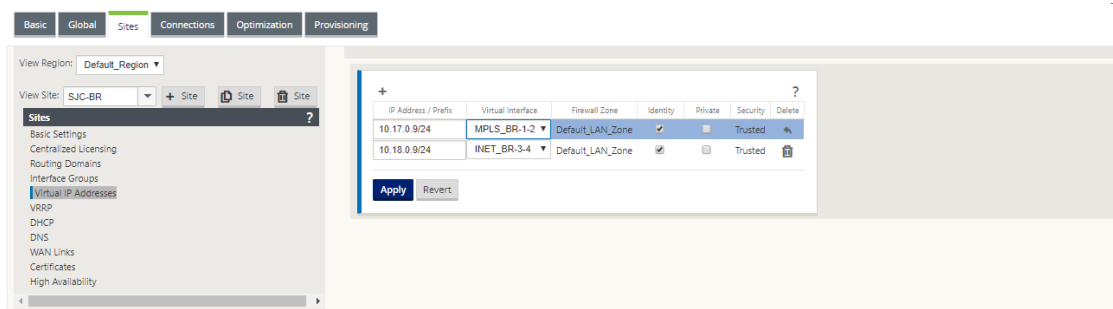
「[前提条件](#)」セクションの「ブランチトポロジ-インラインモードトポロジ図」を参照し、インターフェイスグループを入力します。



各仮想インターフェイスの仮想 IP (VIP) アドレスを作成

各 WAN リンクの適切なサブネット上に仮想 IP アドレスを作成します。VIP は、仮想 WAN 環境内の 2 つの SD-WAN アプライアンス間の通信に使用されます。

1. 構成エディタで、[サイト] > [サイト名] > [仮想 IP アドレス] に移動します。[+] をクリックして VIP を作成します。
2. IP アドレス/プレフィックスを入力し、MPLS とインターネットに対応する仮想インターフェイスを選択します。
3. [**Apply**] をクリックします。



インターネット **WAN** リンクの作成

インターネットリンクを使用してバースト速度ではなく、物理レートに基づいて WAN リンクを設定するには

1. [**WAN リンク**] に移動し、[+ リンク] ボタンをクリックして、インターネットリンクの WAN リンクを追加します。名前を入力し、[アクセスタイプ] として [パブリックインターネット] を選択します。[追加] をクリックします。

- インターネットリンクの詳細を入力し、[パブリック IP アドレスを自動検出する] チェックボックスをオンにします。
- [セクション (Section)] ドロップダウンリストから [アクセスインターフェイス (Access Interfaces)] を選択し、[+] をクリックして、インターネットリンクに固有のインターフェイスの詳細を追加します。
- インターネット WAN 仮想 IP アドレスとゲートウェイアドレスを入力します。プロキシ ARP では、イーサネットインターフェイスが 2 つ未満の場合はチェックされません。

WAN Link: SJC-BR-INET Section: Settings + Add Link Delete Link

Basic Settings

Note: Changing the access type of this WAN Link may cause automatically generated Paths to this link to be added or removed.

Link Name: SJC-BR-INET

Access Type: Public Internet WAN Link Template: <None>

LAN to WAN

Physical Rate (kbps): 2000

☒ Set Permitted From Physical ☐ Auto Learn

Permitted Rate (kbps): 2000

WAN to LAN

Physical Rate (kbps): 2000

☒ Set Permitted From Physical ☐ Auto Learn

Permitted Rate (kbps): 2000

Tracking IP Address:

☒ Autodetect Public IP

Public IP Address:

Basic Global Sites Connections Optimization Provisioning

View Region: Default_Region

View Site: SJC-BR + Site Site Site

Sites

- Basic Settings
- Centralized Licensing
- Routing Domains
- Interface Groups
- Virtual IP Addresses
- VRRP
- DHCP
- DNS
- WAN Links
- Certificates
- High Availability

IP Address / Prefix	Virtual Interface	Firewall Zone	Identity	Private	Security	Delete
10.17.0.9/24	MPLS_BR-1-2	Default_LAN_Zone	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Trusted	
10.18.0.9/24	INET_BR-3-4	Default_LAN_Zone	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Trusted	

Apply Revert

MPLS WAN リンクの作成

- [WAN リンク] に移動し、[セクション] ドロップダウンリストから [設定] を選択します。[+ リンク (+ Link)] ボタンをクリックして、MPLS リンクの WAN リンクを追加します。

2. MPLS WAN リンク名およびその他の詳細を入力します。[アクセスタイプ] を [プライベートイントラネット] として選択します。

The screenshot shows the 'Settings' section for a WAN Link named 'SJC-BR-MPLS'. The 'Access Type' is set to 'Private MPLS'. The 'WAN Link Template' is set to '<None>'. Below this, there are two columns for 'LAN to WAN' and 'WAN to LAN' settings. Each column has a 'Physical Rate (kbps)' field set to '10000' and a 'Permitted Rate (kbps)' field set to '10000'. Both 'Set Permitted From Physical' checkboxes are checked. At the bottom, there is a table with four rows: 'MPLS Queues', 'Advanced Settings', 'Metered/Standby Link', and 'Provisioning'. Each row has a '+' button and a '?' icon. The 'Apply' and 'Revert' buttons are at the bottom left.

Section	Action	Help
MPLS Queues	+ Add	?
Advanced Settings		?
Metered/Standby Link		?
Provisioning		?

3. [セクション (Section)] ドロップダウンリストから [アクセスインターフェイス (Access Interfaces)] を選択し、[+] ボタンをクリックして、MPLS リンクに固有のインターフェイスの詳細を追加します。
4. MPLS 仮想 IP アドレスと Gateway アドレスを入力します。プロキシ ARP では、イーサネットインターフェイスが 2 つ未満の場合はチェックされません。

ルートを設定する

ルートは、前の設定に基づいて自動作成されます。このリモートブランチオフィスに固有のサブネットがさらに存在する場合は、それらのバックエンドサブネットに到達するためにトラフィックを転送するゲートウェイを識別する特定のルートを追加する必要があります。

オートパスグループの作成

1. 構成エディタで、[グローバル] > [**Autopath Groups**] に移動します。[+] をクリックします。
2. 名前を入力し、[適用] をクリックします。
3. 要件に従って Autopath グループを設定し、[**Apply**] をクリックします。

4. [接続] > [**WAN リンク**] に移動します。[**WAN リンク (WAN Links)**] ドロップダウンリストからインターネット **WAN** リンクを選択し、[**セクション (Section)**] ドロップダウンリストから仮想パスを選択します。
5. [使用] チェックボックスをオンにし、各サイト（データセンターとブランチの両方）のイントラネット WAN リンクの [**Autopath Group**] チェックボックスから、新しく作成したオートパスグループを選択します。

2 つの Autopath Group をデフォルトとしてマークすることはできません。マークされている場合、監査エラーが発生します。

The screenshot shows a configuration table for a Virtual Path Service. The 'Autopath Group' column has a dropdown menu set to '<None>'. A red box highlights the dropdown menu. Above the table, there is a label 'UDP Port Switching' with a blue arrow pointing to the 'Alt Port' column. The table has columns: Virtual Path Service, Use, Tunnel Header Size (bytes), Active MTU Detect, UDP Port, UDP Hole Punching, Enable, Alt Port, Interval (min), and Autopath Group. The row for 'SJC_DC-SJC-BR' has the following values: Use is checked, Tunnel Header Size is 0, Active MTU Detect is unchecked, UDP Port is 4980, UDP Hole Punching is unchecked, Enable is unchecked, Alt Port is empty, Interval is 1440, and Autopath Group is '<None>'. Below the table are 'Apply' and 'Revert' buttons.

アクセスタイプが [プライベートイントラネット] の WAN リンクの仮想パスを手動で追加すると、[パス] の下に仮想パスが設定されます。

前の手順をすべて完了したら、[SD-WAN アプライアンスパッケージの準備に進みます](#)。

監査エラーの解決

データセンターサイトとブランチサイトの構成が完了すると、DC サイトと BR サイトの両方で監査エラーを解決するように警告されます。監査エラーを解決します (存在する場合)。

SD-WAN ネットワークの構築

May 10, 2021

SD-WAN オーバーレイルートテーブルを構築せずに SD-WAN オーバーレイネットワークを構築するには、次の手順を実行します。

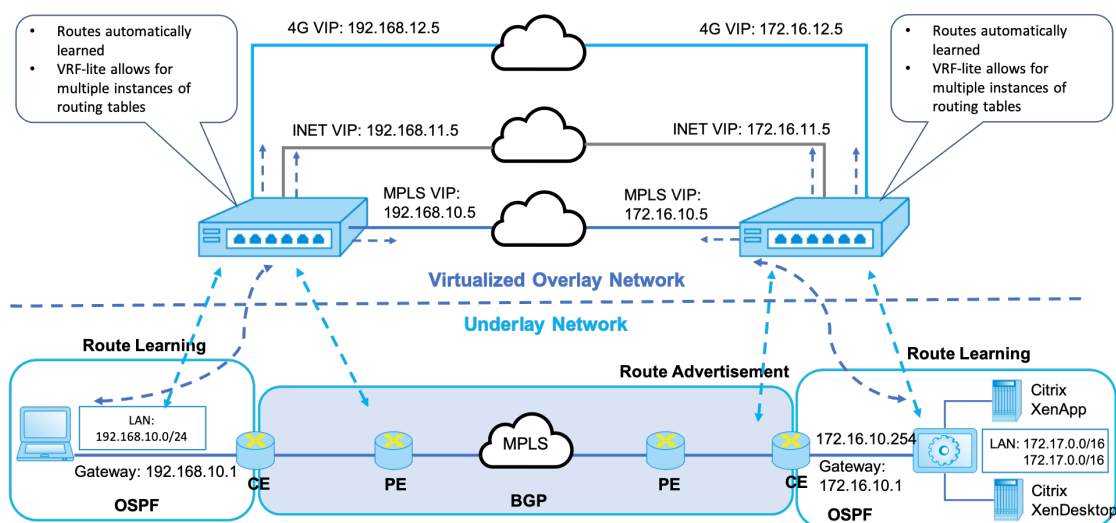
1. 2 つの SD-WAN アプライアンス間の各 WAN リンクにわたって WAN パストンネルを作成します。
2. 各 WAN リンクのエンドポイントを表すように仮想 IP を設定します。現在の L3 ネットワークを介して暗号化された WAN パスを確立できます。
3. 2、3、および 4 つの WAN パス (物理リンク) を 1 つの仮想パスに集約すると、最もインテリジェントでコスト効率が悪い既存のアンダーレイではなく、SD-WAN オーバーレイネットワークを利用してパケットを WAN を通過できるようになります。

SD-WAN ルーティングコンポーネントとネットワークポロジ

- Local: サブネットがこのサイトに存在する (SD-WAN 環境にアダプタイズされる)
- 仮想パス—仮想パスを通じて、選択したサイト・アプライアンスに送信されます。
- イントラネット—SD-WAN アプライアンスがないサイト

- インターネット-インターネットにバインドされたトラフィック
- パススルー: 手つかずのトラフィック、一方のブリッジインターフェイスで他方のブリッジインターフェイスへ
- デフォルトルート (0.0.0.0/0) 定義-SD-WAN オーバーレイルートテーブルによってキャプチャされないパススルートラフィックに使用されます。または MCN で使用され、インターネットトラフィックのバックホールのためにすべてのトラフィックを MCN ノードに転送するようにクライアントサイトに指示します。

SD-WAN overlay dynamic network routing



Premium (エンタープライズ) エディションでのみ WAN 最適化

May 10, 2021

SD-WAN Premium (エンタープライズ) エディション・アプライアンスには、WAN 仮想化に加えて、フル機能の WAN Optimization 機能が搭載されています。一部のお客様は、SD-WAN サービスに移行する前に WAN Optimization 機能を実装することを好む場合があります。この導入ユースケースでは、Premium Edition アプライアンスを利用して WAN 最適化サービスを利用するための手順について説明します。

Citrix SD-WAN 製品プラットフォームエディションには、次のアプライアンスが含まれます。

- SD-WAN: SD-WAN Standard Edition アプライアンス
- Premium (エンタープライズ): SD-WAN Premium エディションアプライアンス
- WANOP: SD-WAN WANOP Edition アプライアンス

Premium (Enterprise) Edition アプライアンスを既存の分散 WANOP ネットワークに統合するには、DC サイトで SD-WAN (物理または仮想) アプライアンスを MCN として構成します。SD-WAN アプライアンスは、ネットワークのすべての構成を管理します。ブランチサイトと DC サイトの MCN の間に仮想パスが確立されます。この仮想パスは、アプライアンス間の制御トラフィックの送信にのみ使用されます。ブランチアプライアンスでは、データトラフィックはイントラネットサービスとして処理されます。イントラネットトラフィックはカプセル化されず、既存の WAN リンクを経由して DC サイトに到達します。DC サイトの WANOP アプライアンスは、エンドツーエンドのトラフィック最適化を提供するために、トラフィックパス内に配置する必要があります。

ヘッドエンドに SD-WAN ハードウェアアプライアンスを持たないお客様のサイトでは、HA ペアの VPX アプライアンス (2 つの仮想 WAN VPX) をワンアームモードで MCN として使用できます。ワンアームモードの場合、トラフィックを SD-WAN アプライアンスにリダイレクトするには、サードパーティルータの PBR 規則が必要です。

このドキュメントでは、DC サイトアプライアンスが冗長性のために HA モードで展開されていることを前提としています。この展開では、HA モードは必須ではありません。

前提条件

- DC サイトに HA モードで展開された WANOP アプライアンスのペアと SD-WAN アプライアンスのペア。
- ブランチサイトの Premium Edition アプライアンス。

ネットワークトポロジ

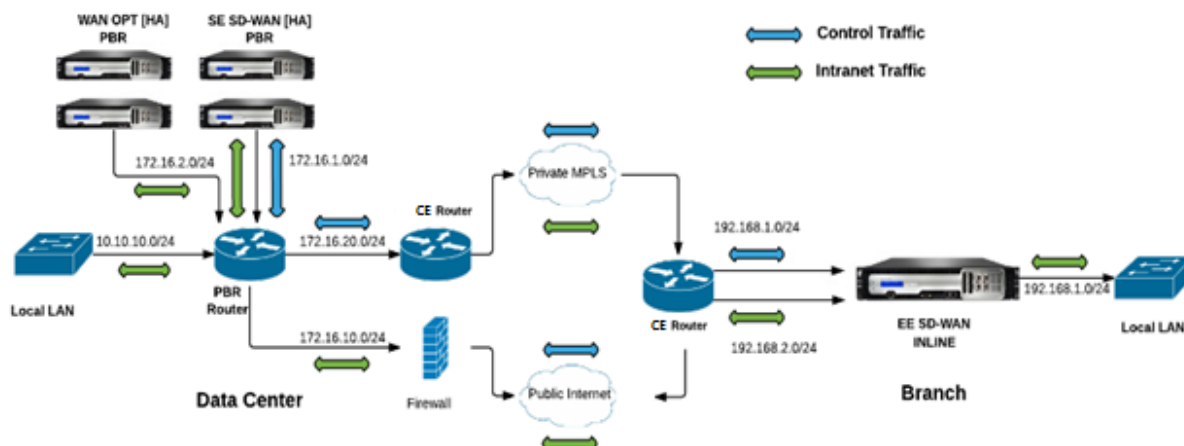
PBR 導入における SD-WAN スタンダードエディションおよび WANOP アプライアンス:

次の図では、DC サイトの SD-WAN SE アプライアンスと WAN OP アプライアンスの両方がワンアームモードで展開されています。SD-WAN アプライアンスは PBR 展開をサポートし、WANOP アプライアンスは PBR と WCCP の両方をサポートします。DC サイトの WAN から受信した制御トラフィック (仮想パストラフィック) は、PBR ルータによって SD-WAN アプライアンスにリダイレクトされます。データトラフィックは、PBR ルータによって WAN Optimization アプライアンスにリダイレクトされます。

WAN から DC LAN へのトラフィックフロー:

- CE (カスタマーエッジ) ルータ-> PBR ルータ-> SD-WAN-> PBR ルータ-> LAN
- CE (カスタマーエッジ) ルータ-> PBR ルータ-> WAN OPT-> PBR ルータ-> LAN

同じトラフィックフローが逆方向に続きます。



PBR モードの SD-WAN スタンダードエディション、インライン展開での WANOP:

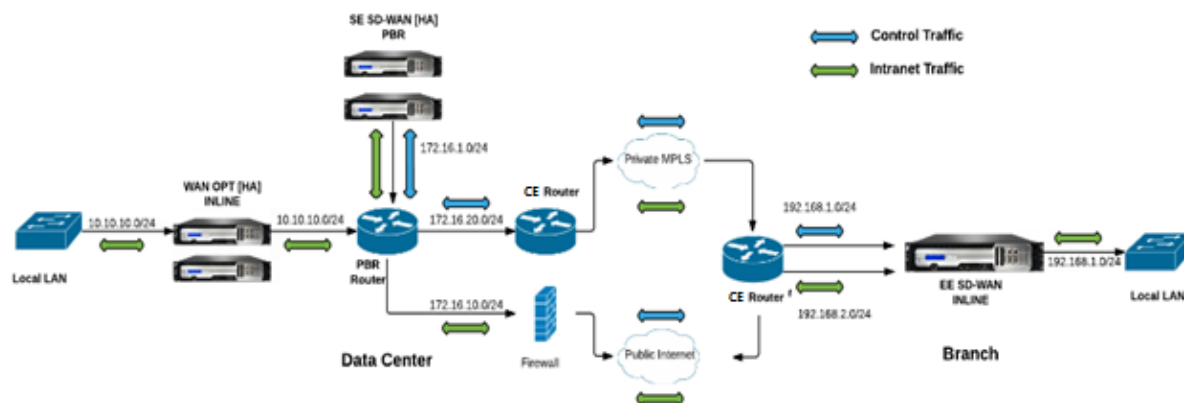
次の図では、DC サイトの SD-WAN アプライアンスはワンアームモードでデプロイされ、WANOP アプライアンスはインラインモードでデプロイされます。

DC サイトの WAN から受信した制御トラフィック（仮想パストラフィック）は、PBR ルータによって SD-WAN アプライアンスにリダイレクトされます。データトラフィックは、PBR ルータによって WAN Optimization アプライアンス（インライン）に転送されます。

WAN から DC LAN へのトラフィックフロー:

- CE（カスタマーエッジ）ルータ-> PBR ルータ-> SD-WAN-> PBR ルータ-> LAN
- CE（カスタマーエッジ）ルータ-> PBR ルータ-> WAN OPT-> LAN

同じトラフィックフローが逆方向に続きます。



構成の手順

1. DC [MCN] で SD-WAN アプライアンスを構成して、DC サイトとブランチサイト間の仮想パスを確立します。

構成, [MCN とクライアント間の仮想パスサービスを参照してください](#)。

2. DC サイトでイントラネットサービスを構成します。

- a) MCN (DC サイト) で、**[構成] > [仮想 WAN] > [構成エディタ] > [接続] > [サイト (DC)] > [イントラネットサービス]** の順に選択します。**[+]** 記号をクリックして、イントラネットサービスを追加します。
- b) **[イントラネットサービス]** の 1 つ以上の WAN リンクを選択し、**[適用]** をクリックします。
- c) 同じ **サイト (DC)** の下の **[ルート]** に移動し、**[+]** 記号をクリックしてコストが 5 未満のリモートネットワークを追加し、**[追加]** をクリックします。

たとえば、**[ネットワーク IP アドレス]** フィールドに **192.168.1.0/24** と入力し、**[イントラネット]** として **[サービスタイプ]** を選択します。

注

イントラネットルートが優先されるためには、各サイトのコストを 5 未満にする必要があります。

3. ブランチサイトでイントラネットサービスを構成します。

- a) ブランチサイトで、上記の **手順 2** のサブステップ a から c を繰り返します。

たとえば、**[ネットワーク IP アドレス]** フィールドに **172.16.1.0/24** と入力し、**[イントラネット]** として **[サービスタイプ]** を選択します。

4. 変更管理 を実行して、構成をブランチサイトにアップロードおよび配布します。

「[構成パッケージと変更管理のエクスポート](#)」を参照してください。

デフォルトでは、トラフィックは仮想パスを経由して、ブランチから DC に送信されます。

注

PBR ルータは、提供された展開手順に従って、トラフィックをリダイレクトするように設定する必要があります。

WAN Optimization の設定の詳細については、[有効化-設定-WAN 最適化](#)を参照してください。

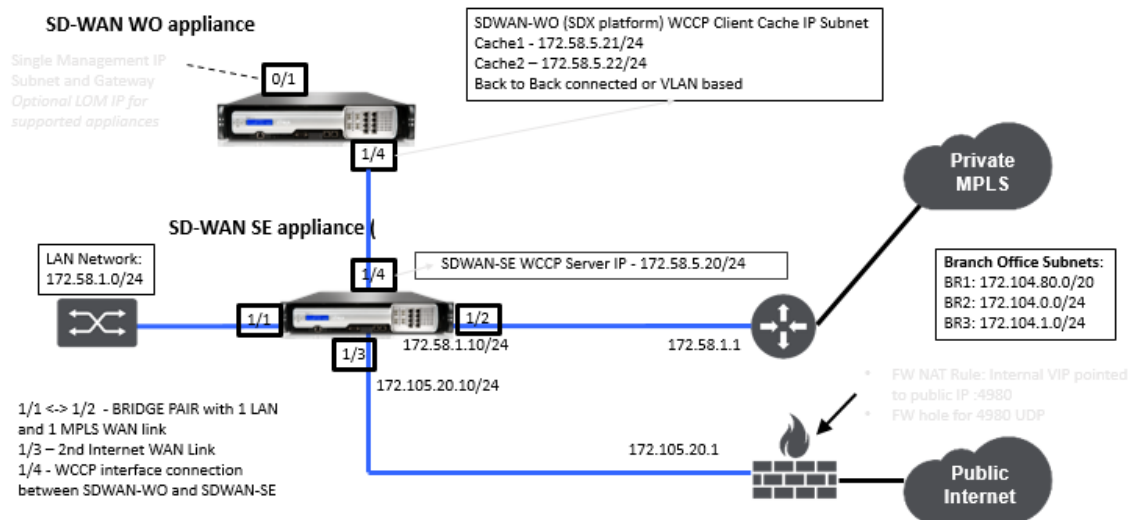
2 ボックスモード

May 10, 2021

2 ボックスモードは、SD-WAN SE アプライアンスが WCCP ルーターおよび SDWAN-WANOP として機能する WCCP ワンアームベースの展開です。(4000/5000) アプライアンスは WCCP クライアントとして機能し、WCCP コンバージェンスの確立を支援します。このようにすべての仮想 path/Intranet SD-WAN SE アプライアンスに到達するサービス指向 TCP パケットは、SD-WAN SE と WANOP の両方の利点を顧客のトラフィックに提供することにより、最適化の利点のために SDWAN-WANOP アプライアンスにリダイレクトされます。

2 ボックスモードは、次のアプライアンスモデルでのみサポートされます。

- SD-WAN SE アプライアンス-4000、4100、および 5100
- SD-WAN WANOP アプライアンス-4000、4100、5000、および 5100



注

Two Box モードが有効の場合、高可用性および WCCP 配置モードにアクセスできません。ただし、これらの展開モードは、ユーザーが管理するために使用できます。

重要

- Two Box Mode が有効の場合、レガシー WCCP 配置は無効になりますが、サービスグループのコンバージェンスは WCCP モニタリングページからしか確認できません。Two BoxMode の監視セクションの下に個別の GUI ページはありません。
- Standard Edition アプライアンスで実行されている WCCP プロセスが、短い時間間隔内に複数回、たとえば 1 分間に 3 回再起動すると、サービスグループは自動的にシャットダウンします。このようなシナリオでは、WANOP アプライアンスで WCCP コンバージェンスを取得するには、WANOP アプライアンスの Web GUI で WCCP 機能を再度有効にします。
- Standard Edition アプライアンスの構成に関連する WCCP 構成または WAN 最適化に変更があると、外部 WANOP アプライアンスがリポートします。例えば、enabling/disabling 構成エディターのインターフェイスグループの WCCP チェックボックスに続いて変更管理プロセスを実行すると、WANOP アプライアンスも再起動します。

注

また、2 つのボックスモードを実装する際には、次の点に注意してください。

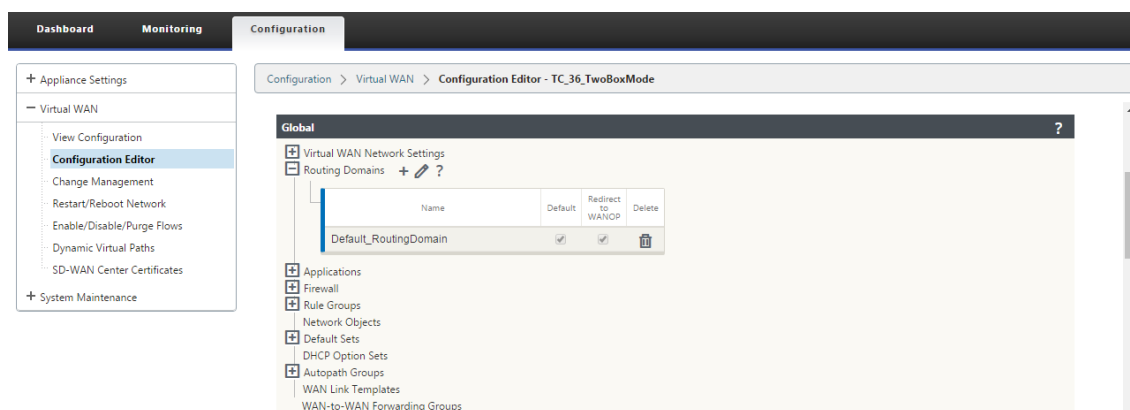
- 構成エディタから WANOP アプライアンスにリダイレクトするようにルーティングドメインを選択した場合は、WCCP が有効になっているインターフェイスグループに追加する必要があります。
- パートナーサイトでも、同じルーティングドメインのトラフィックを選択する必要があります。たとえば、**MCN > Branch01** では、WAN 最適化のメリットを観察できます。

- WCCP が有効になっているインターフェイスグループでルーティングドメインが選択されている場合、ブリッジドインターフェイスを含む別のインターフェイスグループには、同じルーティングドメインが設定されている必要があります。WCCP 対応のインターフェイスグループにルーティングドメインが設定されている場合にのみ、WAN 最適化の利点を備えたエンドツーエンドのトラフィックフローを送信するだけでは不十分です。

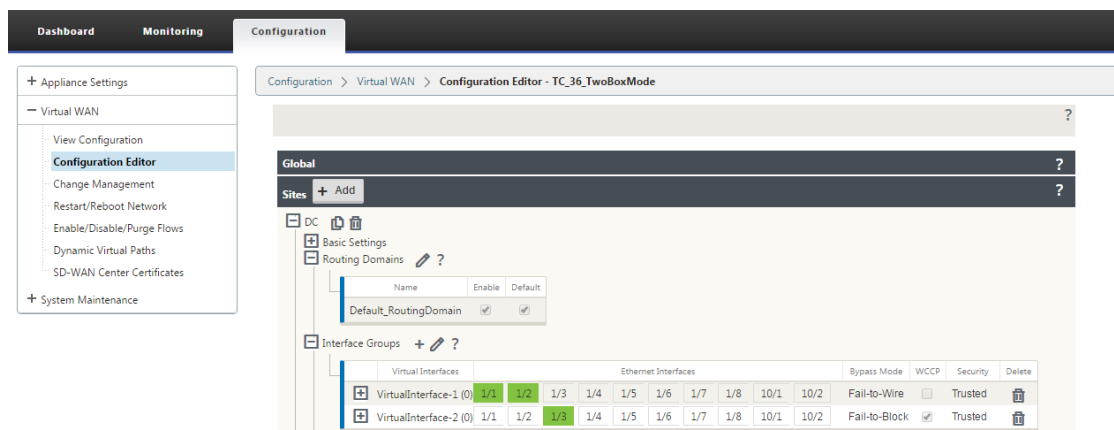
Citrix SD-WAN 標準版

DC サイトまたはブランチサイトの Standard Edition アプライアンスで 2 ボックスモードソリューションを構成するには、次の手順を実行します。

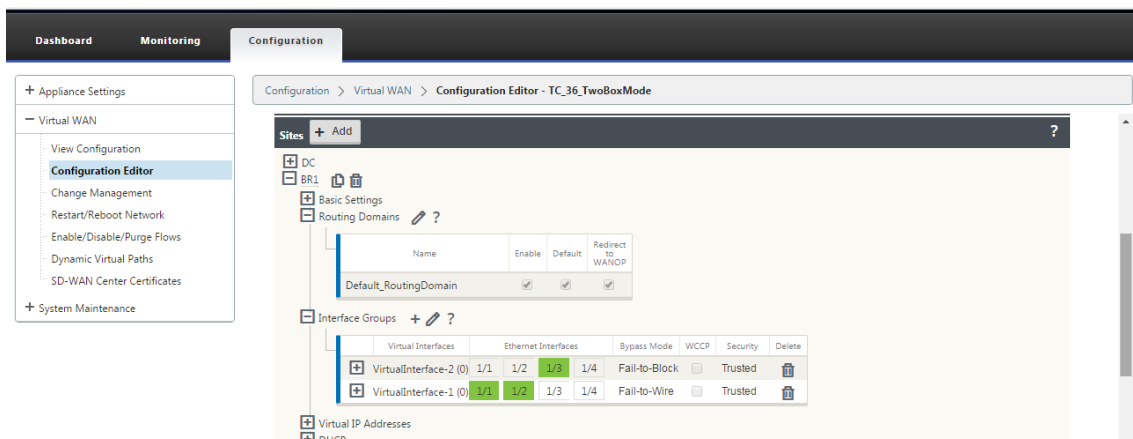
1. SD-WAN SE Web 管理インターフェイスで、[構成] > [仮想 WAN] > [構成エディタ] に移動します。既存の構成パッケージを開くか、パッケージを作成します。
2. 選択した構成パッケージで、[Advanced] タブに移動して構成の詳細を表示します。
3. [グローバル 設定] を開き、[ルーティングドメイン] を展開し、[WANOP にリダイレクト] チェックボックスが有効になっていることを確認します。



4. DC を展開して、アプライアンスが有効になっている 仮想 ネットワーク インターフェイスを示すインターフェイスグループ 設定で、仮想インターフェイスの **WCCP** を有効にします。



5. [サイト + 追加] を展開し、ブランチルーティングドメインとインターフェイスグループの設定を表示します。ブランチサイトの [**WANOP** へのリダイレクト] チェックボックスは、ルーティングドメインに対して有効になっています。



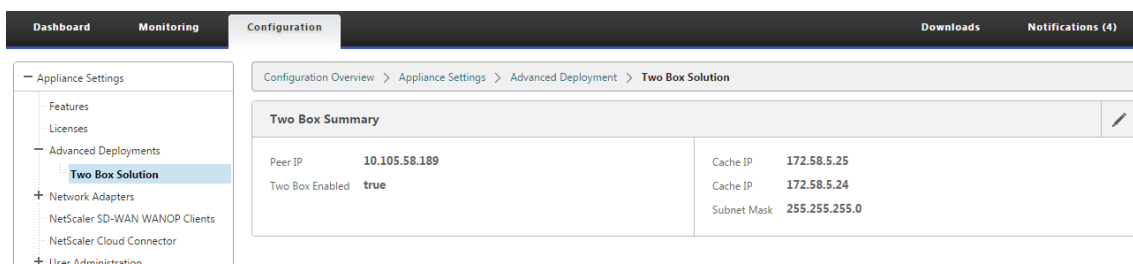
注

WCCP リスナーは、イーサネットインターフェイスが 1 つだけ設定されている仮想ネットワークインターフェイスに対してだけ有効にする必要があります。ブリッジペアで WCCP リスナーを有効にしないでください。SD-WAN SE アプライアンスと SD-WAN WANOP アプライアンス間の ONE-ARM インターフェイスで有効にすることを意図しています。

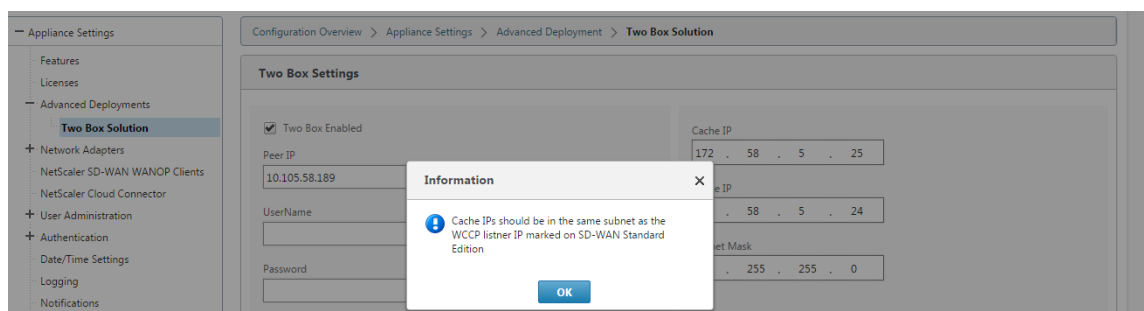
Citrix SD-WAN WANOP 構成

SD-WAN WANOP アプライアンス Web GUI で 2 ボックス配置モードを設定するには、次の手順を実行します。

1. SD-WAN WANOP ウェブ管理インターフェイスで、「構成」>「アプライアンスの設定」>「高度な展開」>「Two Box ソリューション」の順に選択します。



2. 2 ボックスモードの設定を編集するには、[編集] アイコンをクリックします。キャッシュ IP の情報ダイアログが表示されます。[OK] をクリックします。



3. 「2 ボックス有効」チェックボックスを有効 にします。
4. ピア **IP** を入力します。ピア IP は、SD-WAN StandardEdition アプライアンスの IP アドレスです。
5. ユーザー資格情報を入力し、[**Apply**] をクリックします。

Two Box Settings

☒ Two Box Enabled

Peer IP
10.105.58.189

UserName

Password

Cache IP
172 . 58 . 5 . 25

Cache IP
172 . 58 . 5 . 24

Subnet Mask
255 . 255 . 255 . 0

Apply **Cancel**

2 ボックスモードの構成と管理性

以下は、展開のために考慮すべき 2 つのボックスモード構成と管理性のポイントの一部です。

- SD-WAN WANOP 設定は、SD-WAN SE 構成エディタから統合ペインとして設定できます。
 - サービスクラス
 - アプリケーション分類子
 - 特徴
 - システムチューニング

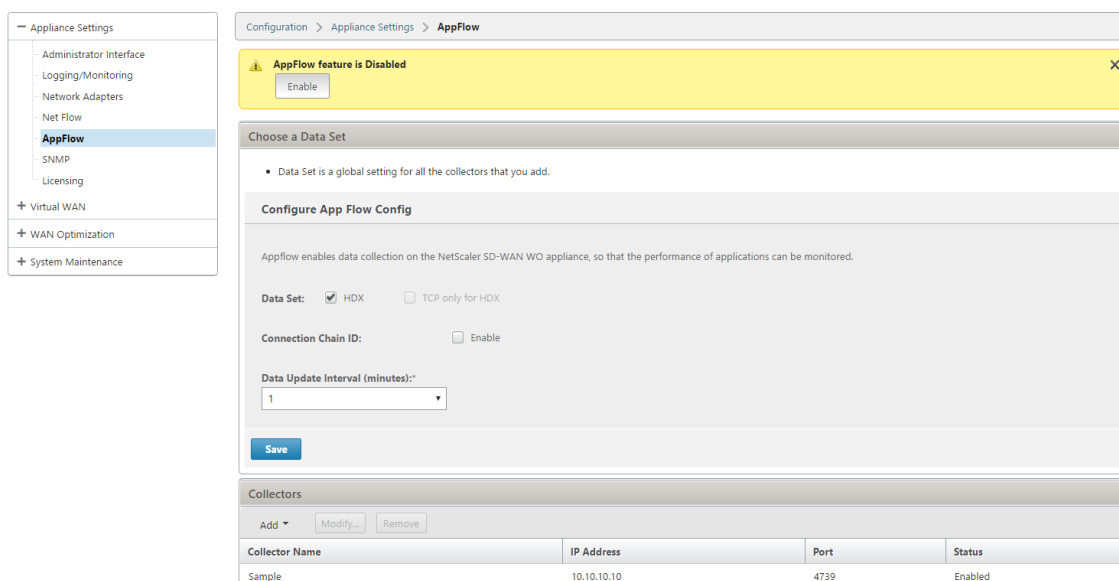
監視

SD-WAN SE アプライアンスの WebUI の [監視] ページを使用して、SD-WAN WANOP トラフィックを直接監視できます。これにより、データトラフィックの処理中に、SDWAN-SE アプライアンスと SDWAN-WO アプライアンスの両方を単一ペインで監視できます。SDWAN-SE UI の [WAN Optimization] ノードで、接続の詳細、セキュアパートナーの詳細などを表示できます。

Monitoring > WAN Optimization > Accelerated Connections										
Accelerated Connections										
Action	Initiator	Responder	Duration	Idle	Bytes Transferred	Compression Ratio/Type	Bandwidth Savings (%)	SSL Proxy	Service Class	State
	172.58.1.135 : 35664	172.58.2.238 : 5001	0m 5s	0m 0s	15.32 MB	N/A (None)	54.4	False	Iperf	Open

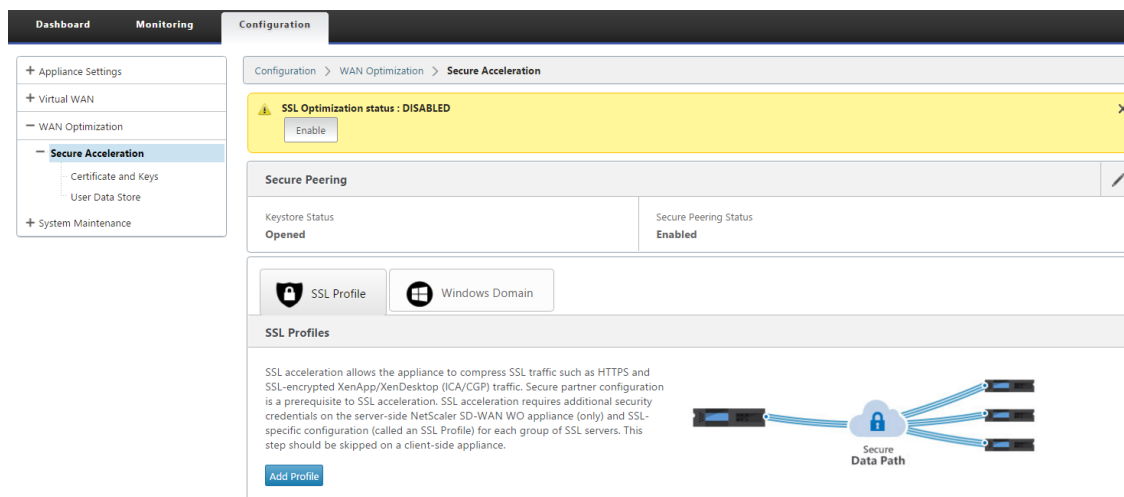
構成

APPFLOW ノードの下 SDWAN-SE 構成 ページから直接 **APPFLOW** を構成できます。これにより、SDWAN-SE は、APPFLOW の構成、およびサービスクラス、アプリケーション分類子などの他のデータ処理構成属性の単一ペインとして機能できます。SDWAN-SE で行われた構成は、SDWAN-WO 構成に反映され、シームレスな APPFLOW 機能のサポートを維持します。



Citrix Application Delivery Management (ADM) によってすでに検出されている SD-WAN WANOP を 2 ボックスモードで使用する場合は、このモードをオフにするまで、Citrix ADM を使用して分離して構成しないでください。これは、トラフィック処理用の WANOP の構成が、2 ボックスモードの SD-WAN SE アプライアンスによって管理されるためです。

高度な Optimization またはセキュアアクセラレーションは、SDWAN-WO アプライアンスで設定する場合と同様に、SDWAN-SE アプライアンス上で直接構成する必要があります。これは、ドメイン参加やセキュア Acceleration/SSL 高度な最適化または SSL プロキシ用のプロファイル作成などの構成の単一ペインの構成を維持するのに役立ちます。



- ライセンスは、SD-WAN SE および SD-WAN WANOP アプライアンスごとに個別に管理する必要があります。
- ソフトウェアアップグレードは、SD-WAN SE および SD-WAN WANOP アプライアンスごとに、それぞれのソフトウェアパッケージで個別に管理する必要があります。たとえば、SD-WAN SE の場合は tar.gz、

SD-WAN WANOP の場合は upg をアップグレードします。

- データパス統合は、WCCP 展開モードを介して SD-WAN SE と外部 WANOP アプライアンス間で構成する必要があります。
 - データパスレベルでは、WCCP と仮想 WAN の両方の機能が、WANOP と SE の間のデータパス統合を通じてワンアームモードで外部的に提供され、最適化のメリットが得られます。

統一された構成と監視

SD-WAN SE および SDWAN-WANOP アプライアンスでツーボックスモードを有効にすると、SD-WAN-EE アプライアンスでのツーボックス構成の表示と同様に、SD-WAN SE アプライアンスで設定を表示できます。

1. 構成 > 仮想 **WAN** > **WAN Optimization**
2. 「構成」 > 「アプライアンスの設定」の「Appflow」ノード
3. [構成] の [WAN Optimization] ノード。

この情報は、SD-WAN SE アプライアンスで 2 ボックスモードになっている SD-WAN WANOP アプライアンスからリダイレクトされます。

SSL アクセラレーションや AppFlow など、WANOP に関連する設定を、SD-WAN SE Web GUI から行うことができるようになった。

接続、圧縮、などのトラフィック関連の統計 CIFS/SMB, ICA Advanced、MAPI、およびパートナーは、SD-WAN プレミアム（エンタープライズ）エディションアプライアンスと同様の [監視]>**WAN** 最適化の SD-WAN SE WebGUI から監視できるようになりました。

DashboardMonitoringConfiguration

+ Appliance Settings

+ Virtual WAN

- WAN Optimization

+ Secure Acceleration

+ System Maintenance

Configuration > WAN Optimization

SSL Optimization status : DISABLED

Enable

Secure Peering

Keystore Status
Opened

Secure Peering Status
Enabled

SSL Profile

Windows Domain

DashboardMonitoringConfiguration

Statistics

Flows

Routing Protocols

Firewall

IKE/IPsec

Performance Reports

Qos Reports

Usage Reports

Availability Reports

Appliance Reports

DHCP Server/Relay

+ WAN Optimization

Monitoring > Statistics

Statistics

Show: Paths (Summary) ☐ Enable Auto Refresh 5 seconds Refresh ☒ Show latest data.

Path Statistics Summary

Filter: in Any column Apply

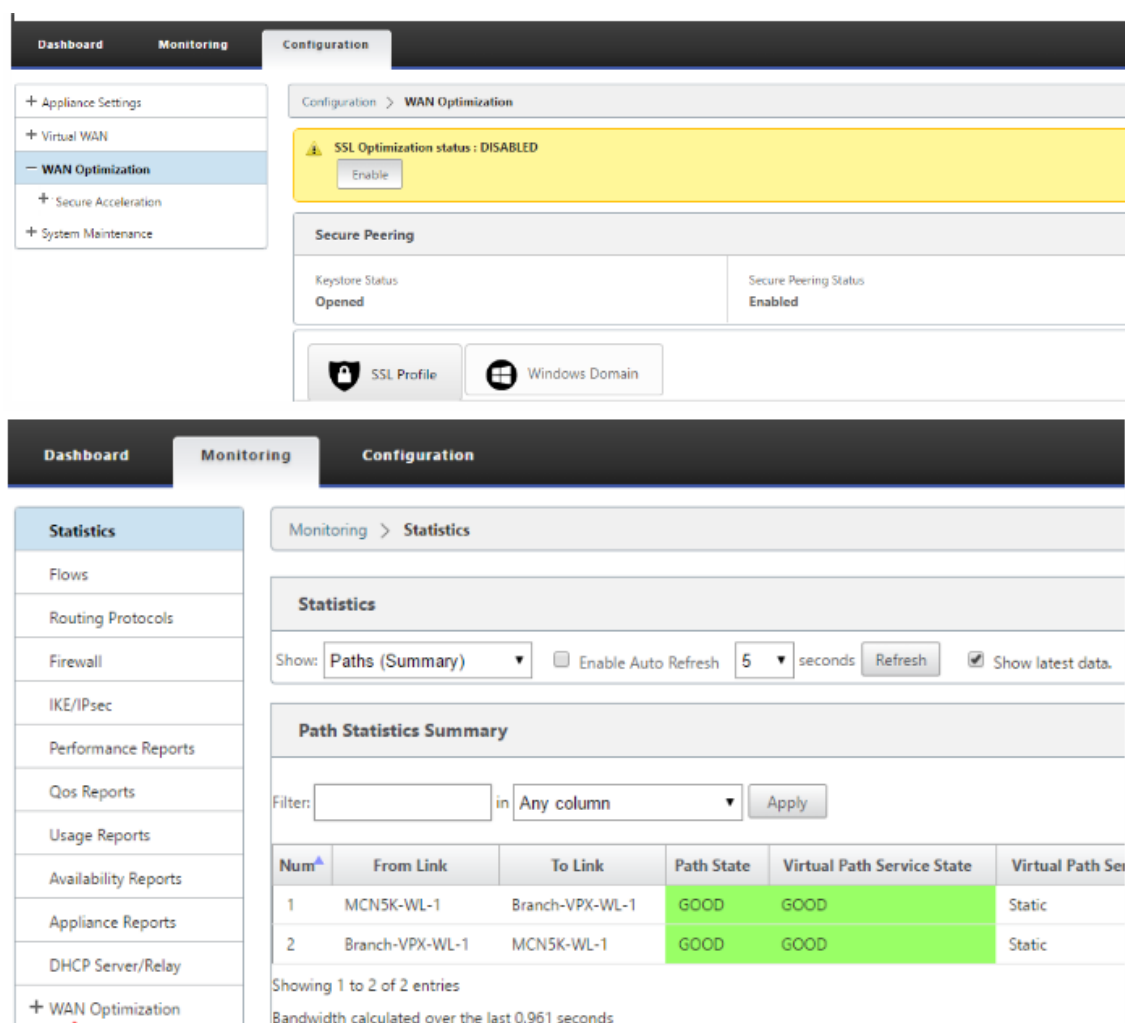
Num	From Link	To Link	Path State	Virtual Path Service State	Virtual Path Se
1	MCN5K-WL-1	Branch-VPX-WL-1	GOOD	GOOD	Static
2	Branch-VPX-WL-1	MCN5K-WL-1	GOOD	GOOD	Static

Showing 1 to 2 of 2 entries

Bandwidth calculated over the last 0.961 seconds

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

331



2 ボックスモードでの SD-WAN WANOP アプライアンスの管理 IP アドレスの変更

SDWAN-WANOP アプライアンスの管理 IP アドレスをツーボックスモードで変更するには:

1. SD- WAN SE アプライアンスで `clear_wo_sync` コマンドを実行します。これにより、GUI リダイレクション用に SD-WAN WANOP IP アドレス情報がクリアされます。
2. SD-WAN WANOP アプライアンスで 2 ボックスモード構成を無効または有効にします。SD-WAN WANOP アプライアンスの新しい IP アドレス (変更された IP) が SD-WAN SE に送信されます。新しく変更された IP アドレスが URL リダイレクトページに表示されます。

管理 IP アドレスは、ピア IP アドレスの構成に使用されます。

SD-WAN WANOP アプライアンスで 2 ボックスモードを無効にする

SD-WAN WANOP および SD-WAN SE アプライアンスを無効にするか 2 ボックスモードから切り離すには:

1. SD-WAN WANOP アプライアンスから TwoBox モードを無効にします。
2. SD-WAN SE Web GUI では、SD-WAN WANOP アプライアンスの 2 つのボックスモードページが表示されることが予想されます。これらのページを消去するには、`clear_wo_sync` コマンドを実行します。

高可用性

November 8, 2021

このトピックでは、SD-WAN アプライアンス (Standard Edition および Premium (Enterprise) Edition) でサポートされる高可用性 (高可用性) の展開と構成について説明します。

Citrix SD-WAN アプライアンスは、アクティブ/スタンバイの役割のアプライアンスのペアとして、高可用性構成で展開できます。高可用性配置には、次の 3 つのモードがあります。

- パラレルインライン高可用性
- フェール・ツー・ワイヤー高可用性
- ワンアーム高可用性

これらの高可用性展開モードは、仮想ルータ冗長プロトコル (VRRP) に似ており、独自の SD-WAN プロトコルを使用します。SD-WAN ネットワーク内のクライアントノード (クライアント) とマスターコントロールノード (MCN) の両方を高可用性構成で展開できます。プライマリアプライアンスとセカンダリアプライアンスは、同じプラットフォームモデルである必要があります。

高可用性構成では、サイトの 1 つの SD-WAN アプライアンスがアクティブアプライアンスとして指定されます。スタンバイアプライアンスはアクティブアプライアンスを監視します。構成は両方のアプライアンスにミラーリングされます。スタンバイ・アプライアンスがアクティブ・アプライアンスとの接続性を一定期間失った場合、スタンバイ・アプライアンスはアクティブ・アプライアンスの ID を引き受け、トラフィックの負荷を引き継ぎます。デプロイモードに応じて、この高速フェールオーバーは、ネットワークを通過するアプリケーショントラフィックへの影響を最小限に抑えます。

高可用性展開モード

ワンアームモード:

ワンアームモードでは、高可用性アプライアンスペアがデータパスの外にあります。アプリケーショントラフィックは、ポリシーベースルーティング (PBR) を使用してアプライアンスペアにリダイレクトされます。ワンアーム・モードは、ネットワーク内の単一の挿入ポイントが不可能な場合、または配線へのフェイル・トゥ・ワイヤーの課題に対処するために実装されます。スタンバイアプライアンスは、アクティブアプライアンスおよびルータと同じ VLAN またはサブネットに追加できます。

One-Arm モードでは、SD-WAN アプライアンスはデータネットワークサブネットに存在しないことをお勧めします。仮想パストラフィックは PBR を通過する必要はなく、ルートループを回避します。SD-WAN アプライアンスとルータは、イーサネットポートを介して、または同じ VLAN 内に直接接続する必要があります。

- フォールバックのための **IP SLA** モニタリング:

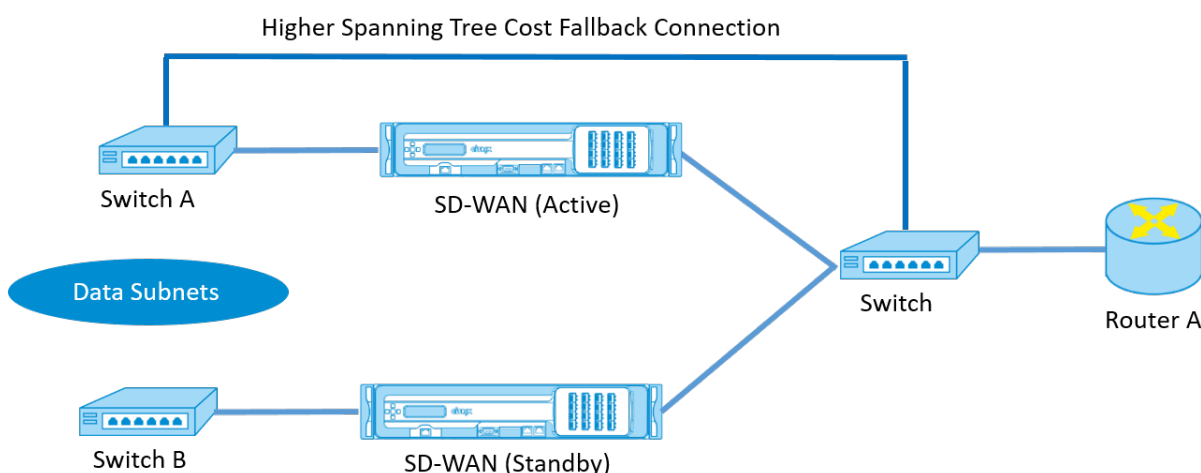
SD-WAN アプライアンスの 1 つがアクティブである限り、仮想パスがダウンしていても、アクティブトラフィックはフローします。SD-WAN アプライアンスは、トラフィックをイントラネットトラフィックとしてルータにリダイレクトします。ただし、アクティブ/スタンバイ SD-WAN アプライアンスの両方が非アクティブになると、ルータはトラフィックをアプライアンスにリダイレクトしようとします。次のアプライアンスに到達できない場合、ルータで IP SLA モニタリングを設定して PBR を無効にすることができます。これにより、ルータがフォールバックしてルート検索を実行し、パケットを適切に転送できます。

並列インライン高可用性モード:

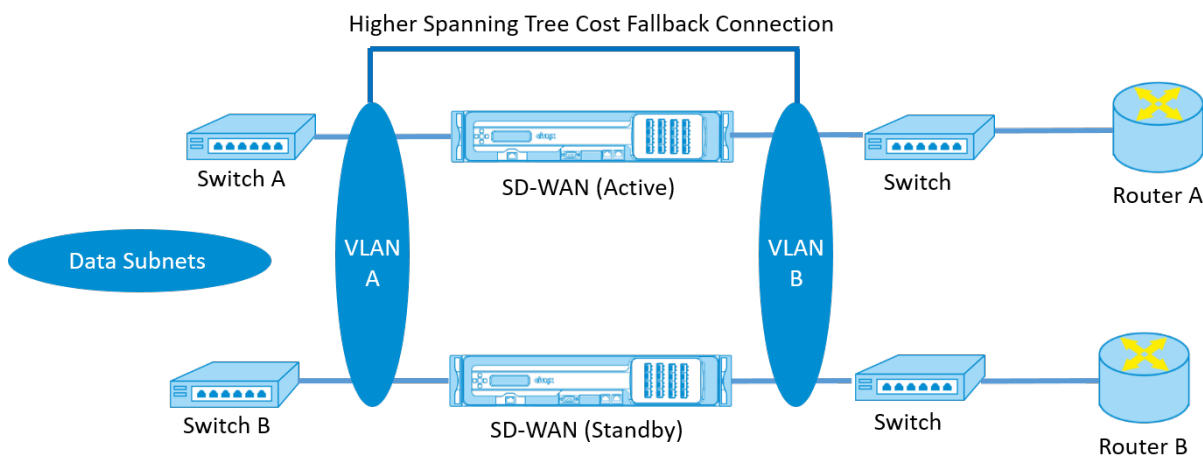
パラレルインライン高可用性モードでは、SD-WAN アプライアンスはデータパスにインラインで配置されます。アクティブアプライアンスを経由するパスは 1 つだけ使用されます。バイパスインターフェイスグループは、フェールオーバー中のブリッジンググループを回避するために fail-to-block に設定されることに注意してください。

高可用性ステートは、インラインインターフェイスグループを介して、またはアプライアンス間の直接接続を介して監視できます。External Tracking を使用して、アップストリームまたはダウンストリームのネットワークインフラストラクチャの到達可能性を監視できます。たとえば、必要に応じて、高可用性状態の変更を指示するスイッチポートの障害。

アクティブ SD-WAN アプライアンスとスタンバイ SD-WAN アプライアンスの両方が無効または障害が発生した場合、スイッチとルータ間でターシャリパスを直接使用できます。このパスは、通常の条件で使用されないように、SD-WAN パスよりもスパニングツリーコストが高い必要があります。パラレルインライン高可用性モードでのフェールオーバーは、設定されているフェールオーバー時間によって異なります。デフォルトのフェールオーバー時間は 1000 ミリ秒です。ただし、フェールオーバーのトラフィックへの影響は 3～5 秒です。ターシャリパスへのフォールバックは、スパニングツリーの再コンバージェンスの間、トラフィックに影響を与えます。他の WAN リンクへのパス外接続がある場合は、両方のアプライアンスを接続する必要があります。



複数のルータが VRRP を使用している可能性があるより複雑なシナリオでは、LAN 側のスイッチとルータがレイヤ 2 で到達可能であることを確認するために、ルーティング不能 VLAN が推奨されます。



フェール・ツー・ワイヤ・モード：

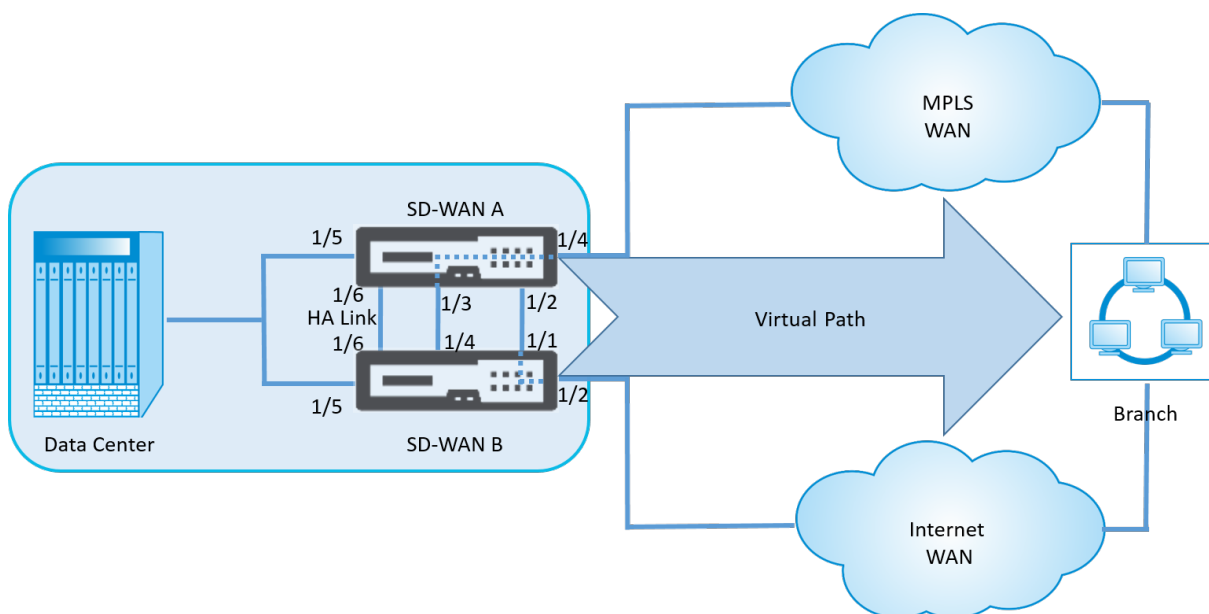
Fail-to-Wire モードでは、SD-WAN アプライアンスは同じデータパスでインラインになります。バイパスインターフェイスグループは、スタンバイアプライアンスがパススルーまたはバイパス状態である状態で、Fail-to-Wire モードである必要があります。別のポート上の 2 つのアプライアンス間の直接接続を構成し、高可用性インターフェイスグループに使用する必要があります。

注

- フェールツーワイヤモードでの高可用性スイッチオーバーには、Fail-to-Wire モードからの回復にポートが遅延するため、約 10 ～12 秒かかります。
- アプライアンス間の高可用性接続に障害が発生すると、両方のアプライアンスがアクティブ状態になり、サービスが中断されます。サービスの中断を軽減するには、単一障害点がないように、複数の高可用性接続を割り当てます。
- 高可用性 Fail-to-Wire モードでは、ステートコンバージェンスを支援するために、高可用性制御交換メカニズム用にハードウェアアプライアンスのペアで別個のポートを使用することが不可欠です。

SD-WAN アプライアンスがアクティブからスタンバイに切り替わる時に物理的な状態が変化するため、オートネゴシエーションがイーサネットポートでかかる時間に応じて、フェールオーバーによって接続が部分的に切断されることがあります。

次の図に、Fail-to-Wire 展開の例を示します。



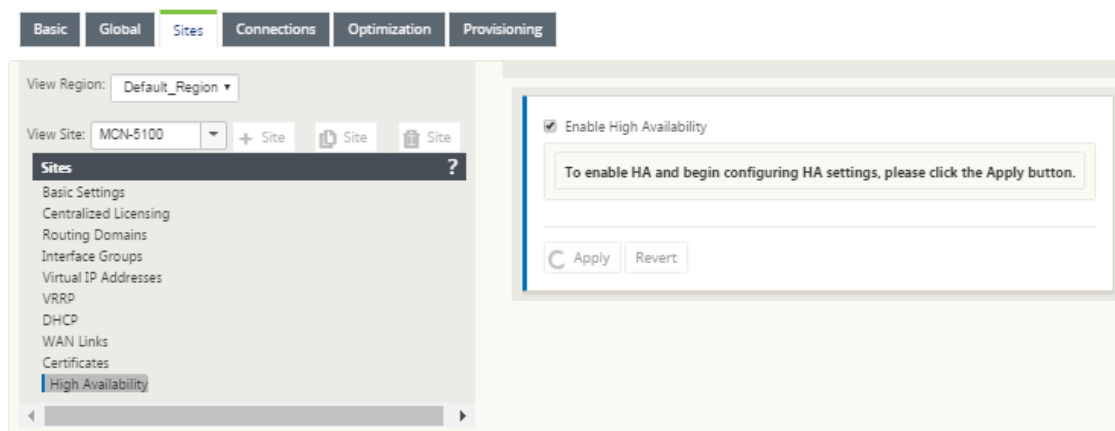
One-Arm 高可用性構成または Parallel Inline 高可用性構成は、フェールオーバー中の中断を最小限に抑えるために大量のトラフィックを転送するデータセンターまたはサイトにお勧めします。

フェールオーバー中に最小限のサービス損失が許容できる場合は、Fail-to-Wire 高可用性モードが適しています。Fail-to-Wire 高可用性モードは、アプライアンスの障害から保護し、パラレルインライン高可用性はすべての障害から保護します。すべてのシナリオにおいて、高可用性は、システム障害時に SD-WAN ネットワークの継続性を維持するために有用です。

高可用性の構成

高可用性を構成するには、次の手順を実行します。

1. 構成エディタで、[サイト] > [** サイト名 **] > [高可用性] に移動します。[高可用性の有効化] を選択し、[適用] をクリックします。



☒ Enable High Availability

HA Appliance Name:	Failover Time (ms):	Shared Base MAC:
MATRIZ-1	1000	AA:AA:AA:00:00:00

☐ Swap Primary/Secondary ☐ Primary Reclaim ☐ HA Fail-to-Wire Mode

HA IP Interfaces +

	Virtual Interface	Control IP Addresses		
		Primary	Secondary	Delete
	LAN (100)	10.0.15.241	10.0.15.240	
	INET (0)	10.213.16.35	10.213.16.34	

2. 次のパラメータに値を入力します。

- 高可用性アプライアンス名: 高可用性（セカンダリ）アプライアンスの名前。
- フェイルオーバー時間: プライマリアプライアンスとの接続後、スタンバイアプライアンスがアクティブになるまでの待機時間（ミリ秒単位）。
- 共有ベース **MAC**: 高可用性ペアアプライアンスの共有 MAC アドレス。フェールオーバーが発生すると、セカンダリアプライアンスの仮想 MAC アドレスは、障害が発生したプライマリアプライアンスと同じになります。
- プライマリ/セカンダリのスワップ: 選択すると、高可用性ペアの両方のアプライアンスが同時に起動すると、セカンダリアプライアンスがプライマリアプライアンスになり、優先されます。
- **Primary Reclaim**: 選択すると、フェイルオーバーイベント後の再起動時に、指定されたプライマリアプライアンスが制御を再利用します。
- 高可用性フェイル-ワイヤモード: **Fail-to-Wire** 高可用性展開モードを有効にする場合に選択します。

注

ハイパーバイザーおよびクラウドベースのプラットフォームの場合は、共有ベース **MAC** を無効にするオプションを選択して、共有仮想 MAC アドレスを無効にします。

Hypervisor ベースのプラットフォームでは、ハイパーバイザーで無差別モードが有効になっていることを確認して、高可用性の共有 MAC アドレスからのパケットソースを許可します。無差別モードが有効になっていない場合は、共有ベース **MAC** を無効にするオプションを有効にできます。

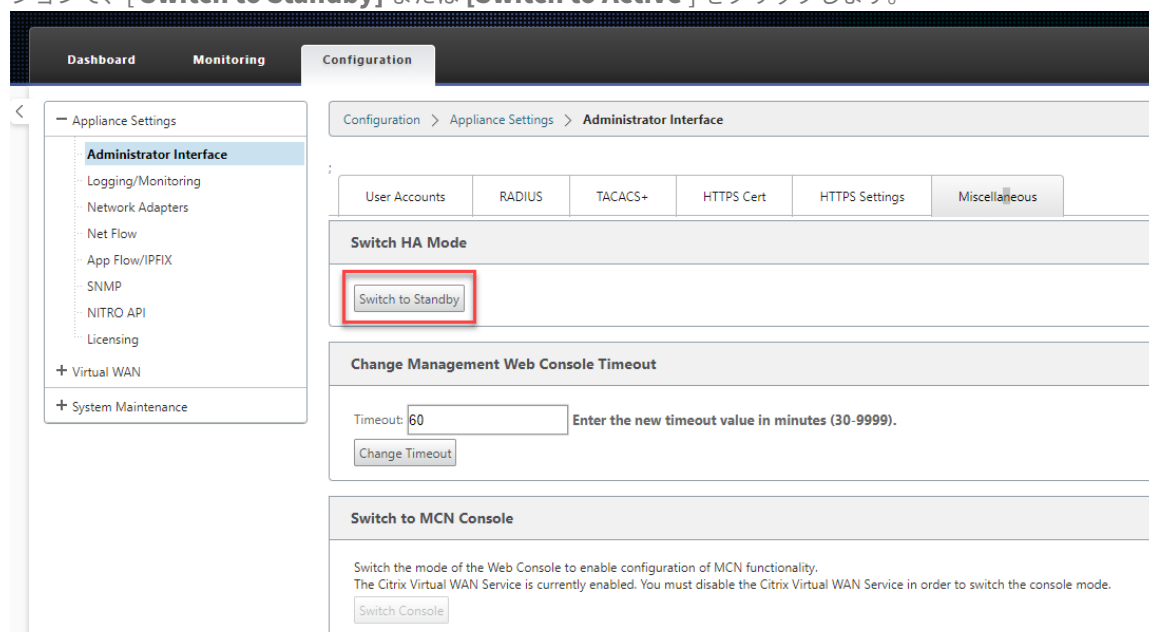
インターフェイスグループを設定するには、**[高可用性 IP Interfaces]** の横にある **[+]** をクリックします。次のパラメータに「値」を入力します。

- 仮想インターフェイス—高可用性ペア内のアプライアンス間の通信に使用される仮想インターフェイス。アクティブアプライアンスの到達可能性を監視します。ワンアーム高可用性モードの場合、必要なインターフェイスグループは 1 つだけです。
- プライマリ—プライミアプライアンスの一意の仮想 IP アドレス。セカンダリアプライアンスは、プライマリ仮想 IP アドレスを使用して、プライミアプライアンスと通信します。
- セカンダリ—セカンダリアプライアンスの一意の仮想 IP アドレス。プライミアプライアンスは、セカンダリ仮想 IP アドレスを使用してセカンダリアプライアンスと通信します。

新しい 高可用性 **IP** インターフェイス エントリの左側にある **[+]** をクリックします。[**External Tracking IP Address**] フィールドに、ARP 要求に応答する外部デバイスの IP アドレスを入力して、プライミアプライアンスの状態を特定し、**[Apply]** をクリックします。

注：

アプライアンスから HA スイッチオーバーを手動でトリガーすることもできます。構成 > アプライアンスの設定 > 管理者インターフェイス > その他に移動します。HA アプライアンスに応じて、[Switch HA Mode] セクションで、**[Switch to Standby]** または **[Switch to Active]** をクリックします。



監視

高可用性構成を監視するには、次の手順を実行します。

高可用性が実装されているアクティブおよびスタンバイアプライアンスの SD-WAN Web 管理インターフェイスにログインします。[ダッシュボード] タブに高可用性ステータスを表示します。

DashboardMonitoringConfiguration

System Status

Name:

BLR_DC-Appliance

Model:

4000

Appliance Mode:

MCN

Management IP Address:

10.105.58.172

Appliance Uptime:

3 days, 7 hours, 1 minutes, 43.0 seconds

Service Uptime:

3 days, 6 hours, 39 minutes, 51.0 seconds

Routing Domain Enabled:

Default_RoutingDomain

High Availability Status

Local Appliance:

Active

Peer Appliance:

Standby

Last Update Received:

0 seconds ago

DashboardMonitoringConfiguration

System Status

Name:

BLR_DC-BLR_DC_HA

Model:

4000

Appliance Mode:

MCN

Management IP Address:

10.105.58.142

Appliance Uptime:

1 weeks, 1 days, 12 hours, 41 minutes, 5.3 seconds

Service Uptime:

3 days, 6 hours, 50 minutes, 31.0 seconds

Routing Domain Enabled:

Default_RoutingDomain

High Availability Status

Local Appliance:

Standby

Peer Appliance:

Active

Last Update Received:

0 seconds ago

アクティブおよびスタンバイの高可用性アプライアンスのネットワークアダプタの詳細については、「構成」>「アプライアンスの設定」>「ネットワークアダプタ」>「イーサネット」タブに移動します。

DashboardMonitoringConfiguration

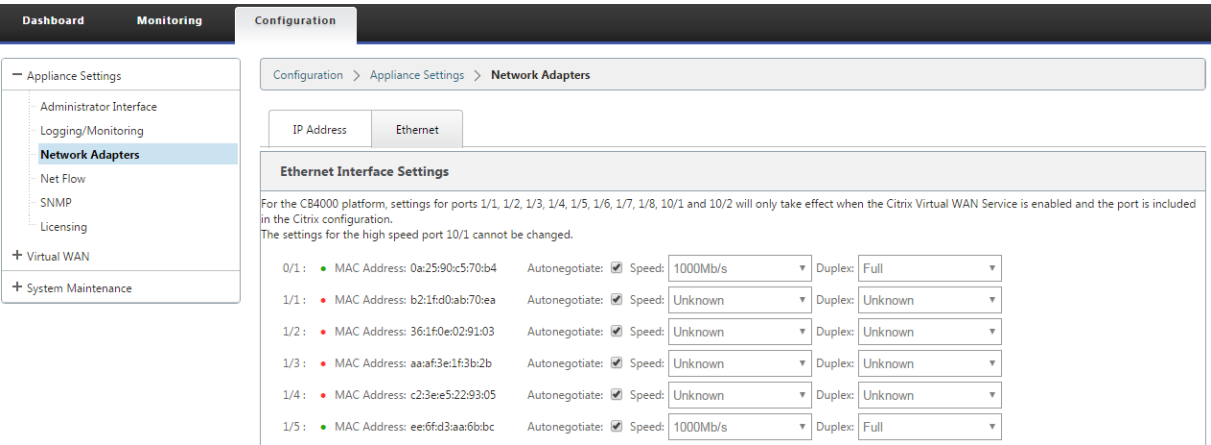
Configuration > Appliance Settings > Network Adapters

IP AddressEthernet

Ethernet Interface Settings

For the CB4000 platform, settings for ports 1/1, 1/2, 1/3, 1/4, 1/5, 1/6, 1/7, 1/8, 10/1 and 10/2 will only take effect when the Citrix Virtual WAN Service is in the Citrix configuration.
The settings for the high speed port 10/1 cannot be changed.

0/1 :	MAC Address: 0a:c4:7a:14:c9:d6	Autonegotiate: <input checked="" type="checkbox"/>	Speed: 1000Mb/s	Duplex: Full
1/1 :	MAC Address: 5a:4c:f8:f0:71:b2	Autonegotiate: <input checked="" type="checkbox"/>	Speed: Unknown	Duplex: Unknown
1/2 :	MAC Address: d6:1e:72:d5:d1:18	Autonegotiate: <input checked="" type="checkbox"/>	Speed: 1000Mb/s	Duplex: Full
1/3 :	MAC Address: 66:4f:9d:c5:48:d2	Autonegotiate: <input checked="" type="checkbox"/>	Speed: Unknown	Duplex: Unknown
1/4 :	MAC Address: 46:63:cb:5d:39:db	Autonegotiate: <input checked="" type="checkbox"/>	Speed: 1000Mb/s	Duplex: Full
1/5 :	MAC Address: 06:7b:ce:9a:c5:dd	Autonegotiate: <input checked="" type="checkbox"/>	Speed: 1000Mb/s	Duplex: Full



トラブルシューティング

SD-WAN アプライアンスを高可用性（HA）モードに設定するときに、次のトラブルシューティング手順を実行します。

- 1. スプリットブレインの問題の主な理由は、HA アプライアンス間の通信の問題が原因です。
 - SD-WAN アプライアンス間の接続に問題があるかどうかを確認します（両方の SD-WAN アプライアンスのポートがアップまたはダウンしているなど）。
 - 1 つの SD-WAN アプライアンスのみをアクティブにするには、いずれかの SD-WAN アプライアンスで SD-WAN サービスを無効にする必要があります。

- 2. **SDWAN_common.log** ファイルにログインした HA 関連ログを確認できます。

注：
すべての高可用性関連ログは、キーワード **racp** で記録されます。

- 3. **SDWAN_common.log** ファイル内のポート関連のイベント（HA が有効なポートがダウンまたはアップになったなど）を確認できます。
- 4. HA 状態の変更ごとに、1 つの SD-WAN イベントが記録されます。したがって、ログがロールオーバーされた場合、イベントログを確認してイベントの詳細を取得できます。

光ファイバ Y ケーブルを使用したエッジモードの高可用性の有効化

September 26, 2023

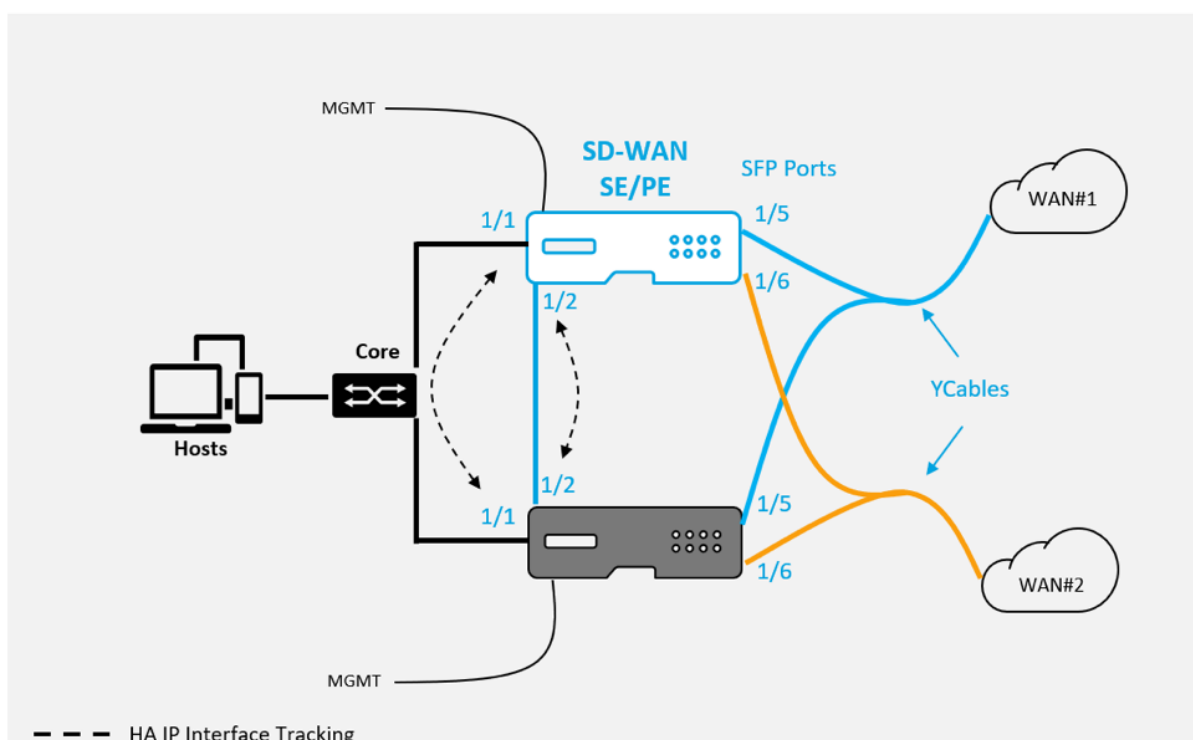
注：リリース 10.2 バージョン 2 では、この機能は 1100 SE/PE アプライアンスにだけ適用できます。

次の手順では、WAN リンクサービスプロバイダーからのハンドオフが光ファイバであるエッジモードで配置された 1100 SE/PE アプライアンスで High Availability (HA; 高可用性) を有効にする手順について説明します。

1100 アプライアンスで使用可能な SFP (小型フォーム・ファクタ・プラグ) ポートを光ファイバ Y ケーブルとともに使用すると、エッジ・モード導入で高可用性機能を実現できます。

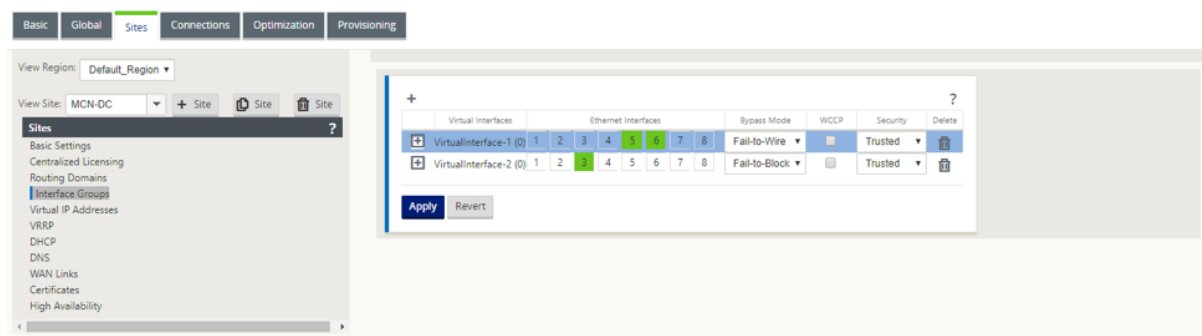
1100 SE/PE アプライアンスでは、スプリッターケーブルのスプリットエンドは、HA ペアで設定された 2 つの 1100 アプライアンスのファイバポートに接続します。

光ファイバ Y ケーブルには 3 つの端があります。一方の端はプロバイダのファイバハンドオフに接続し、もう一方の端は HA ペアに展開された 2 つの 1100 SE/PE アプライアンス上の WAN リンク用に設定された SFP ポートに接続します。スプリッターケーブルは、1 つの入力信号を複数の信号に分割するために使用されます。



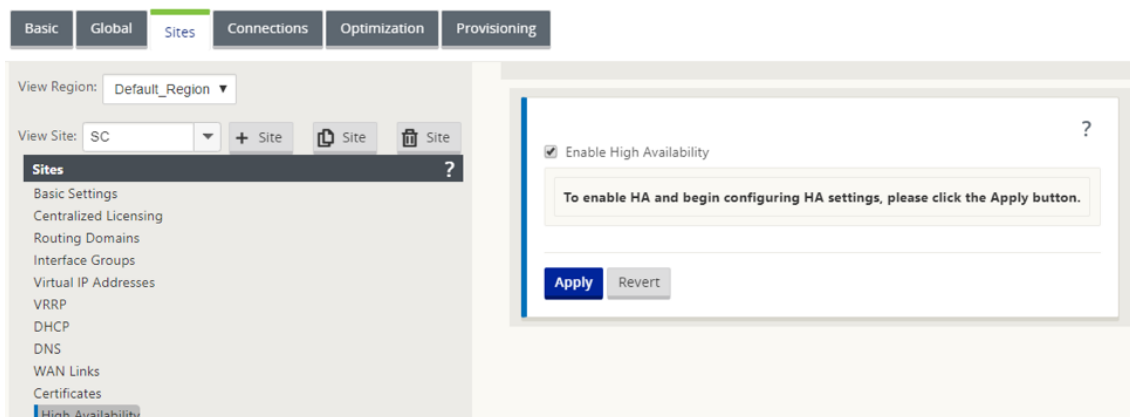
前提条件:

1. 1100 SE/PE アプライアンスでは、ポート 1/5 および 1/6 は SFP ポートです。Y ケーブルのスプリッタの端を、HA ペアの両方のアプライアンスのいずれかのポートに接続します。詳細については、[1100 SE](#)を参照してください。
2. SFP ポートを SD-WAN アプライアンス構成に追加します。SFP ポートの設定は、ネットワークインターフェイスポートの設定と同じです。詳しくは、「[インターフェイスグループの設定方法](#)」を参照してください。設定に 1/5 または 1/6 ポートを追加すると、Y ケーブルサポート機能を有効にできます。

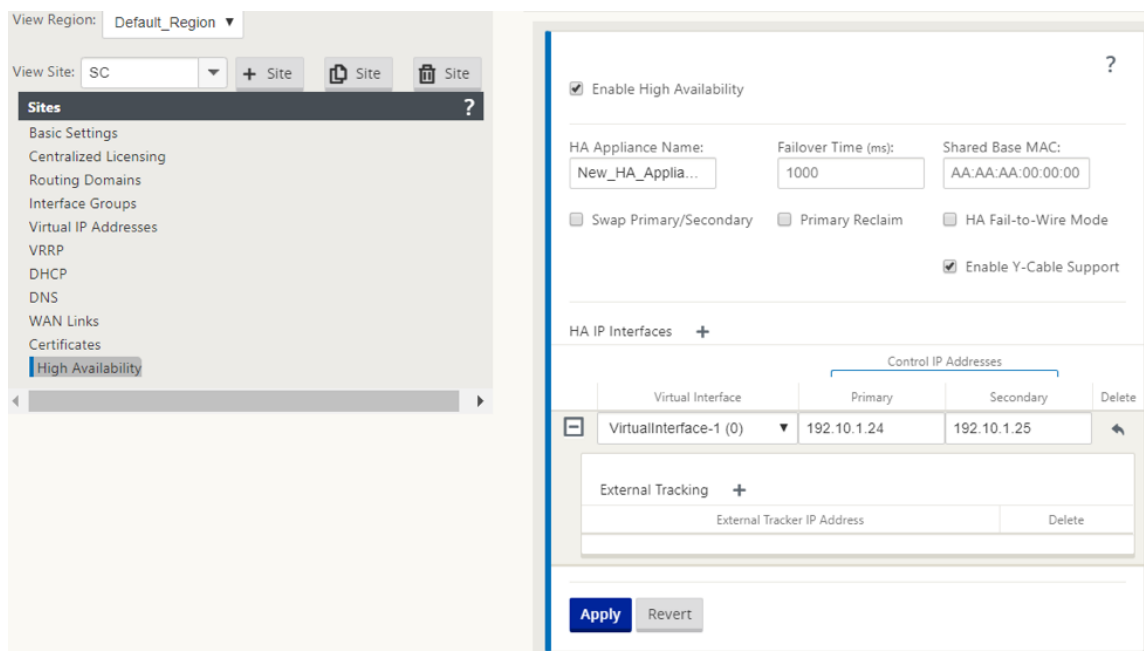


Y ケーブルを使用して高可用性を有効にするには、次の手順を実行します。

1. 1100 SE/PE アプライアンスの GUI で、[構成] > [仮想 WAN] > [構成エディタ] > [サイト] に移動します。[高可用性の有効化] をクリックします。



2. [Y ケーブルサポートを有効にする] をクリックします。
3. Y ケーブルに接続されたインターフェイス以外のインターフェイスを使用して HA IP インターフェイスを追加します (例: 1/1 LAN 方向インターフェイス、または 1/2 直接接続されたインターフェイス)。Y ケーブル機能が有効の場合、SFP ポートを HA IP インターフェイスに使用できません。



4. 設定を適用、ステージングおよびアクティブ化します。

制限事項:

- Y ケーブルを使用した HA フェールツーワイヤモードの設定はサポートされていません。
- Y ケーブルに接続された SFP は、HA IP インターフェイストラッキングとして使用できません。
- この展開をサポートするには、リリース 10.2.2 以降、11.0 以降が必要です。

ゼロタッチ

November 8, 2021

注

ゼロタッチ展開サービスは、一部の Citrix SD-WAN アプライアンスでのみサポートされます。

- SD-WAN 110 Standard Edition
- SD-WAN 210 Standard Edition
- SD-WAN 410 Standard Edition
- SD-WAN 2100 Standard Edition
- SD-WAN 1000 Standard Edition (再イメージ化が必要)
- SD-WAN 1000 Enterprise Edition (Premium Edition) (再イメージが必要です)
- SD-WAN 1100 Standard Edition
- SD-WAN 1100 Premium (Enterprise) Edition

- SD-WAN 2000 Standard Edition (再イメージ化が必要)
- SD-WAN 2000 Enterprise Edition (Premium Edition (再イメージが必要です))
- SD-WAN 2100 Enterprise Edition (Premium Edition)
- SD-WAN AWS VPX インスタンス

ゼロタッチ展開クラウドサービスは、Citrix が運用および管理するクラウドベースのサービスで、Citrix SD-WAN ネットワーク内の新しいアプライアンスを検出できます。主に支店またはクラウドサービスオフィスでの Citrix SD-WAN の展開プロセスの合理化に焦点を当てています。ゼロタッチデプロイメントクラウドサービスは、パブリックインターネットアクセスを介して、ネットワーク内のどこからでもパブリックにアクセスできます。ゼロタッチデプロイメントクラウドサービスは、セキュアソケットレイヤー (SSL) プロトコルを介してアクセスします。

ゼロタッチ展開クラウドサービスは、ゼロタッチ対応デバイス (SD-WAN 410-SE、2100-SE) を購入した Citrix のお客様の格納された識別情報をホストするバックエンドの Citrix サービスと安全に通信します。バックエンドサービスは、Zero Touch Deployment 要求を認証し、Citrix SD-WAN アプライアンスのカスタマーアカウントとシリアル番号の間の関連付けを適切に検証します。

ZTD ハイレベルアーキテクチャとワークフロー:

データ・センター・サイト:

Citrix SD-WAN 管理者-**SD-WAN** 環境の管理者権限を持つユーザーで、次の主な役割を担います。

- Citrix SD-WAN Center ネットワーク構成ツールを使用した構成の作成、またはマスターコントロールノード (MCN) SD-WAN アプライアンスからの構成のインポート
- 新しいサイトノードの展開のためにゼロタッチ展開サービスを開始する Citrix Cloud ログイン。

注

SD-WAN Center がプロキシサーバ経由でインターネットに接続されている場合は、SD-WAN Center でプロキシサーバの設定を構成する必要があります。詳細については、「[ゼロタッチ展開のプロキシサーバ設定](#)」を参照してください。

ネットワーク管理者—エンタープライズネットワーク管理 (DHCP、DNS、インターネット、ファイアウォールなど) を担当するユーザー

- 必要に応じて、**SD-WAN Center** から **FQDN *sdwanzt.citrixnetworkapi.net*** へのアウトバウンド通信用のファイアウォールを構成します。

リモート・サイト:

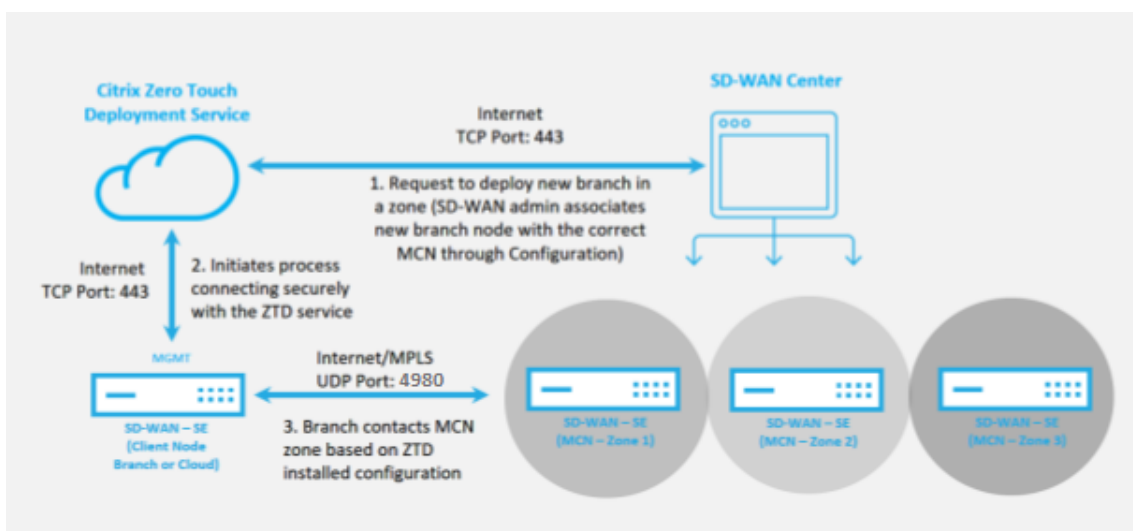
オンサイト・インストーラー—オンサイト・アクティビティの担当者、または雇用されたインストーラー。主に次の責任があります。

- Citrix SD-WAN アプライアンスを物理的に解凍します。
- ZTD 対応でないアプライアンスのイメージを再作成します。

- 必須: SD-WAN 1000-SE、2000-SE、1000-EE、2000-EE
- 不要: SD-WAN 410-SE、2100-SE
- アプライアンスの電源ケーブル。
- 管理インターフェイス (MGMT、0/1 など) でインターネットに接続するためにアプライアンスをケーブル接続します。
- データインターフェイス (Apa.WAN、Apb.WAN、apc.WAN、0/2、0/3、0/5 など) で WAN リンク接続用にアプライアンスをケーブル接続します。

注

インタフェースのレイアウトはモデルごとに異なるため、データおよび管理ポートの識別に関するドキュメントを参照してください。

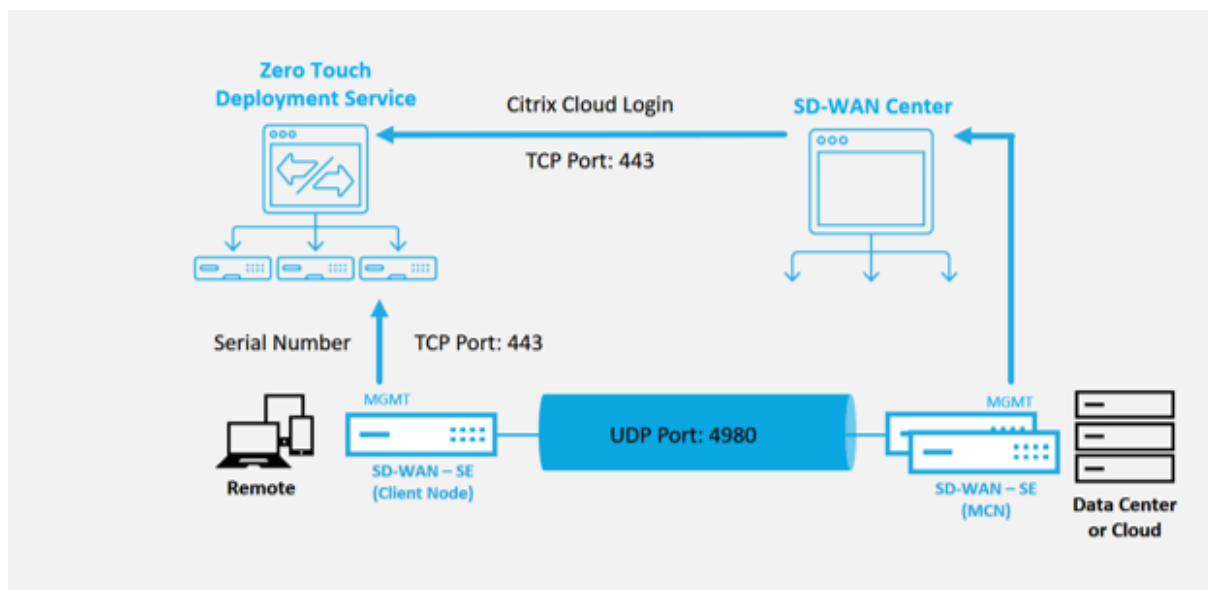


ゼロタッチ展開サービスを開始する前に、次の前提条件が必要です。

- マスターコントロールノード (MCN) に昇格したアクティブに実行されている SD-WAN。
- 仮想パス経由の MCN に接続して、SD-WAN Center をアクティブに実行しています。
- <https://onboarding.cloud.com> で作成された Citrix Cloud ログイン資格情報 (アカウント作成に関する以下の説明を参照)。
- 管理ネットワーク接続 (SD-WAN Center および SD-WAN アプライアンス) をポート 443 でインターネットに直接接続するか、プロキシサーバー経由で接続します。
- (オプション) MCN への有効な仮想パス接続を使用してクライアントモードでブランチオフィスで動作するアクティブに実行されている少なくとも 1 つの SD-WAN アプライアンス。

最後の前提条件は必須ではありませんが、新しく追加されたサイトで Zero Touch Deployment が完了したときに、アンダーレイネットワークで仮想パスを確立できるかどうかを SD-WAN 管理者が検証できます。これは主に、適切

なファイアウォールポリシーとルートポリシーが NAT トラフィックに適宜配置されているか、または UDP ポート 4980 がネットワークに正常に侵入して MCN に到達できることを確認します。



ゼロタッチ展開サービスの概要:

Zero Touch Deployment Service は、SD-WAN Center と連携して機能し、ブランチオフィスの SD-WAN アプライアンスを簡単に導入できます。SD-WAN Center は、SD-WAN 標準および Enterprise (Premium) Edition アプライアンスの中央管理ツールとして構成および使用されます。ゼロタッチ展開サービス（またはゼロタッチ展開クラウドサービス）を使用するには、管理者は最初に環境に最初の SD-WAN デバイスを展開してから、SD-WAN Center を管理の中心点として構成および展開する必要があります。リリース 9.1 以降の SD-WAN Center がポート 443 にパブリックインターネットに接続してインストールされると、SD-WAN Center は自動的にクラウドサービスを開始し、必要なコンポーネントをインストールします。これにより、ゼロタッチデプロイ機能のロックを解除し、GUI でゼロタッチデプロイオプションを使用できるようになります。SD-WAN Center の、ゼロタッチ展開は、SD-WAN Center ソフトウェアでは既定では使用できません。これは、管理者がゼロタッチ配置に関連するオンサイトアクティビティを開始する前に、アンダーレイネットワーク上に適切な予備コンポーネントが存在することを確認するために意図的に設計されています。

SD-WAN 環境が稼働し始めたら、Citrix Cloud アカウントのログインを作成することにより、ゼロタッチ展開サービスへの登録が完了します。SD-WAN Center がゼロタッチ展開サービスと通信できる場合、GUI は [設定] タブの下にゼロタッチ展開オプションを公開します。ゼロタッチサービスにログインすると、特定の SD-WAN 環境に関連付けられたカスタマー ID が認証され、SD-WAN Center が登録されます。さらに、ゼロタッチデプロイアプライアンスの展開をさらに認証するためのアカウントのロックが解除されます。

SD-WAN 管理者は、SD-WAN Center ネットワーク構成ツールを使用して、テンプレートまたはサイトのクローン作成機能を使用して SD-WAN 構成を構築し、新しいサイトを追加する必要があります。新しい設定は SD-WAN Center で使用され、新しく追加されたサイトのゼロタッチ展開の展開を開始します。SD-WAN 管理者がゼロタッチ展開プロセスを使用して展開するサイトを開始する場合、シリアル番号を事前に入力し、オンサイトインストーラへの電子メール通信を開始してオンサイトを開始することで、ゼロタッチ展開に使用するアプライアンスを事前認証す

るオプションがあります。アクティビティ。

オンサイトインストーラーは、サイトがゼロタッチ展開の準備ができているという電子メール通信を受信し、DHCP IP アドレスの割り当てと MGMT ポートでのインターネットアクセスのためにアプライアンスの電源を入れてケーブル接続するインストール手順を開始できます。また、LAN ポートおよび WAN ポートでのケーブル配線。それ以外はすべてゼロタッチ展開サービスによって開始され、アクティベーション URL を使用して進行状況が監視されます。インストールするリモートノードがクラウドインスタンスである場合、アクティベーション URL を開くと、ワークフローが開始され、指定されたクラウド環境にインスタンスが自動的にインストールされます。ローカルインストーラーによるアクションは必要ありません。

ゼロタッチデプロイメントクラウドサービスは、次のアクションを自動化します。

ブランチアプライアンスで新機能が利用できる場合は、ゼロタッチデプロイメントエージェントをダウンロードして更新します。

- シリアル番号を検証して、ブランチアプライアンスを認証します。
- SD-WAN 管理者がサイトを SD-WAN Center を使用してゼロタッチ展開を受け入れたことを認証します。
- SD-WAN Center から、ターゲットアプライアンスに固有の設定ファイルをプルします。
- 対象のアプライアンスに固有の構成ファイルをブランチアプライアンスにプッシュします。
- ブランチアプライアンスに構成ファイルをインストールします。
- 不足している SD-WAN ソフトウェアコンポーネントまたは必要な更新をブランチアプライアンスにプッシュします。
- 仮想パスの確立を確認するための一時的な 10 Mbps ライセンスファイルをブランチアプライアンスにプッシュします。
- ブランチアプライアンスで SD-WAN サービスを有効にします。

SD-WAN 管理者がアプライアンスに永久ライセンスファイルをインストールするには、さらに多くの手順が必要です。

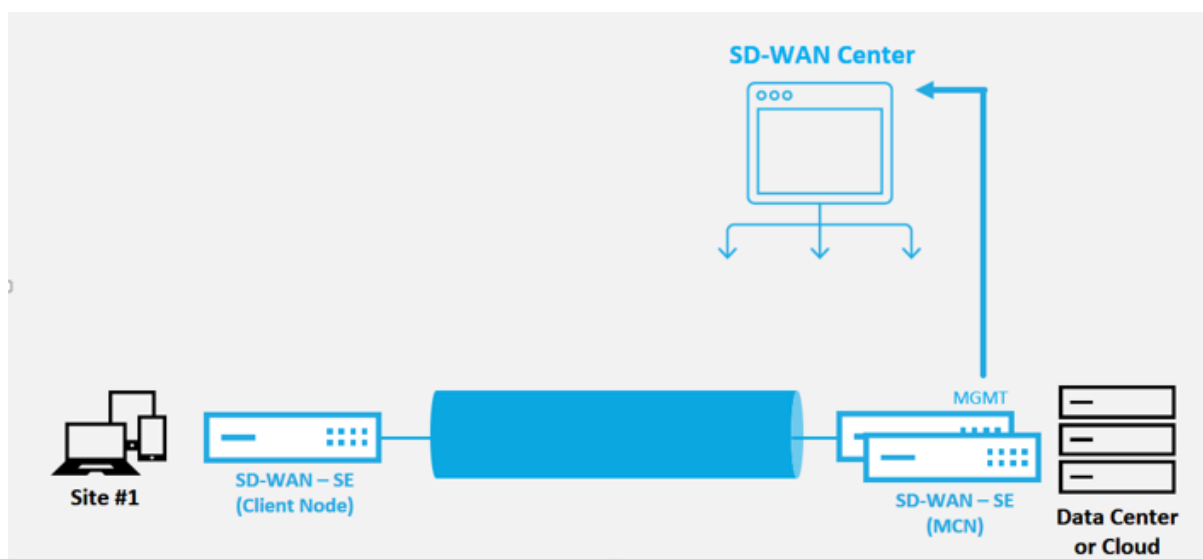
(
注

) MCN で使用されているアプライアンスソフトウェアのバージョンが同じであるブランチ設定を実行している間は、ゼロタッチ展開プロセスでアプライアンスソフトウェアファイルが再度ダウンロードされることはありません。この変更は、工場出荷時の新品のアプライアンス、工場出荷時のデフォルトにリセットされたアプライアンス、および管理上の構成のリセットに適用されます。設定がリセットされた場合は、[**Reboot after revert**] チェックボックスをオンにして、ゼロタッチ展開プロセスを開始します。

ゼロタッチ展開デバイス手順

以下の手順では、ゼロタッチ展開サービスを使用して新しいサイトを展開するために必要な手順を詳しく説明します。実行中の MCN と 1 つのクライアントノードがすでに SD-WAN Center との適切な通信で動作しており、アンダー

レイネットワーク全体の接続を確認する仮想パスを確立します。SD-WAN 管理者がゼロタッチの展開を開始するには、次の手順が必要です。



ゼロタッチ展開サービスを構成する方法

SD-WAN Center には、新しく接続されたアプライアンスから SD-WAN エンタープライズネットワークに参加するための要求を受け付ける機能があります。要求は、ゼロタッチ展開サービスを介して Web インターフェイスに転送されます。アプライアンスがサービスに接続すると、構成とソフトウェアのアップグレードパッケージがダウンロードされます。

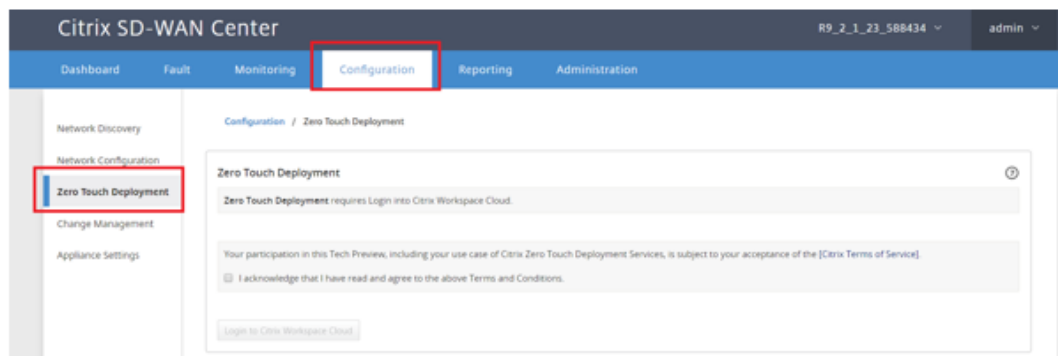
設定ワークフロー:

- [**SD-WAN Center**] > [新しいサイト構成の作成] にアクセスするか、既存の構成をインポートして保存します。
- Citrix Cloud にログインして、ゼロタッチ展開サービスを有効にします。SD-WAN Center Web 管理インターフェイスに「ゼロタッチ配置」メニューオプションが表示されるようになりました。
- SD-WAN Center で、設定 > ** ゼロタッチ展開 > 展開新しいサイトへのナビゲート **。
- アプライアンスを選択して [有効化] をクリックし、[デプロイ] をクリックします。
- インストーラがアクティベーションメールを受信し、シリアル番号を入力 > アクティベーション > アプライアンスが正常にデプロイされました。

ゼロタッチ展開サービスを構成するには:

1. ゼロタッチ展開機能を有効にした SD-WAN Center をインストールします。
 - a) DHCP が割り当てられた IP アドレスを持つ SD-WAN Center をインストールします。

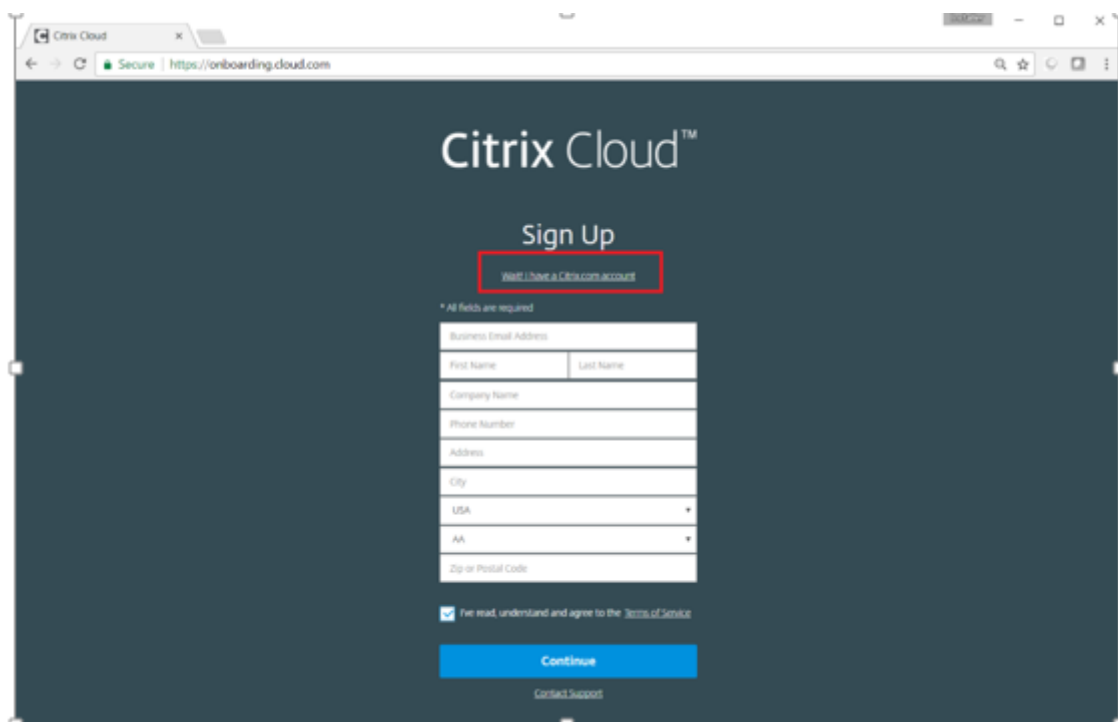
- b) SD-WAN Center に適切な管理 IP アドレスとネットワーク DNS アドレスが割り当てられ、管理ネットワークを介してパブリックインターネットに接続できることを確認します。
- c) SD-WAN Center を最新の SD-WAN ソフトウェアリリースバージョンにアップグレードします。
- d) 適切なインターネット接続により、SD-WAN Center はゼロタッチ展開クラウドサービスを開始し、ゼロタッチ展開に固有のファームウェアアップデートを自動的にダウンロードしてインストールします。この Call Home 手順が失敗すると、次のゼロタッチ展開オプションが GUI で使用できなくなります。



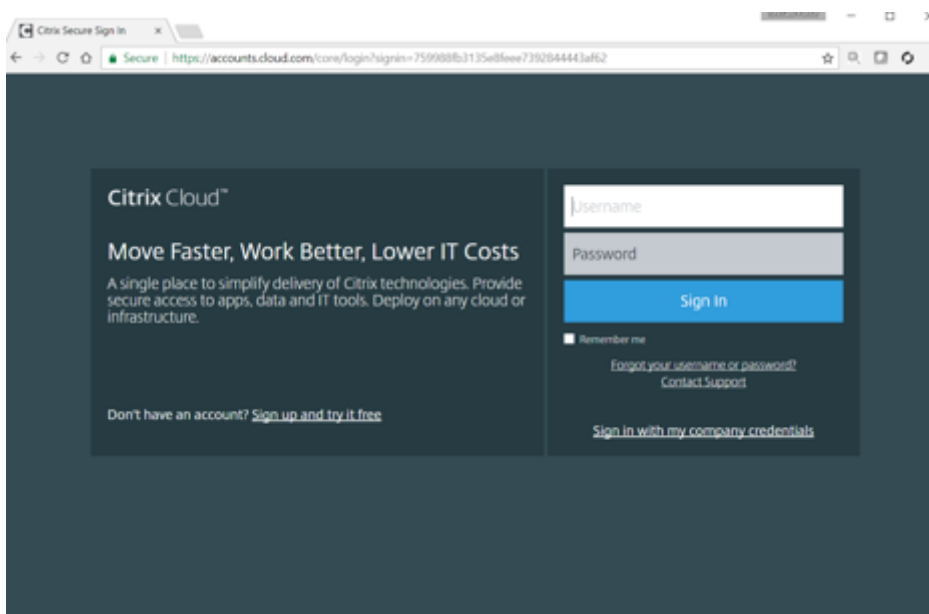
- e) 利用規約を読み、上記の利用規約を読み、同意したことを認めますを選択します。
- f) **Citrix Cloud** アカウントがすでに作成されている場合は、[**Citrix Workspace Cloud** にログイン] ボタンをクリックします。
- g) Citrix Cloud アカウントにログインし、ログインが成功したという次のメッセージが表示されたら、このウィンドウを閉じないでください。**SD-WAN CENTER GUI** が更新されるまでにさらに **20** 秒かかります。ウィンドウが完了したら、ウィンドウを単独で閉じる必要があります。



2. クラウドログインアカウントを作成するには、以下の手順に従います。ウェブブラウザを開いて <https://onboarding.cloud.com>
3. 「待って、**Citrix.com** アカウントを持っています」のリンクをクリックします。



4. 既存の Citrix アカウントでサインインします。



5. SD-WAN Center Zero Touch Deployment ページにログインすると、次の理由により、ゼロタッチ展開に使用できるサイトがないことがあります。

- アクティブな構成が [構成] ドロップダウンメニューから選択されていません
- 現在アクティブな構成のすべてのサイトが既に展開されています
- 構成は SD-WAN Center を使用して構築されたものではなく、MCN で利用可能な構成エディタを使用

して構築されたものでした。

- ゼロタッチ対応アプライアンス（410-SE、2100-SE、Cloud VPX など）を参照する構成でサイトが構築されていない

6. SD-WAN SD-WAN Center ネットワーク構成を使用して、**ZTD** 対応 **SD-WAN** アプライアンスを備えた新しいリモートサイトを追加するように設定を更新します **。

SD-WAN 設定が SD-WAN Center ネットワーク設定を使用して構築されていない場合は、MCN からアクティブな設定をインポートし、SD-WAN Center を使用して設定の変更を開始します。Zero Touch Deployment 機能を使用するには、SD-WAN 管理者は SD-WAN Center を使用して設定を構築する必要があります。ゼロタッチ展開の対象となる新しいサイトを追加するには、以下の手順を使用する必要があります。

- a) 新しいサイトの詳細（つまり、アプライアンスモデル、インターフェイスグループの使用、仮想 IP アドレス、帯域幅を備えた WAN リンク、およびそれぞれの Gateway）を最初に概説することにより、SD-WAN アプライアンス展開用の新しいサイトを設計します。

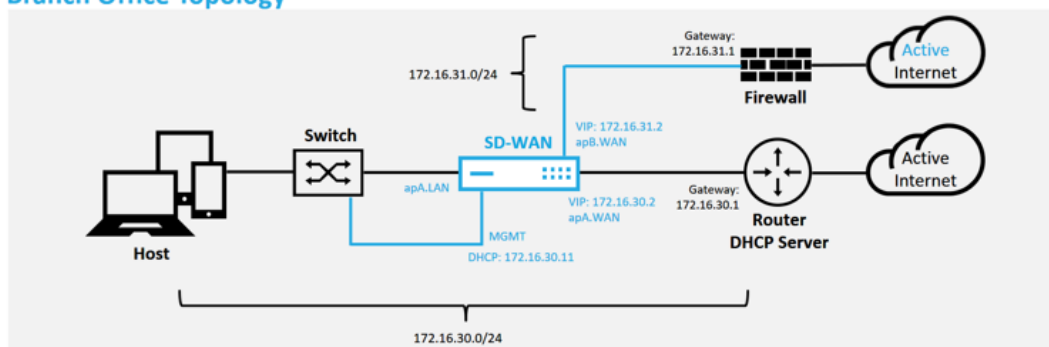
重要

モデルとして VPX が選択されているサイトノードも一覧表示されますが、現在、ゼロタッチデプロイメントサポートは AWS VPX インスタンスでのみ利用可能です。

注

- Citrix SD-WAN Center のサポート Web ブラウザを使用していることを確認します
- Citrix Workspace ログイン中に、Web ブラウザーがポップアップウィンドウをブロックしていないことを確認します。

Branch Office Topology



これは、ブランチオフィスサイトの展開の例です。SD-WAN アプライアンスは、172.16.30.0/24 ネットワーク経由で既存の MPLS WAN リンクのパスに物理的に展開され、既存のバックアップリンクを使用してアクティブ状態にし、その 2 番目の WAN リンクを別のサブネット 172.16.31.0/24.

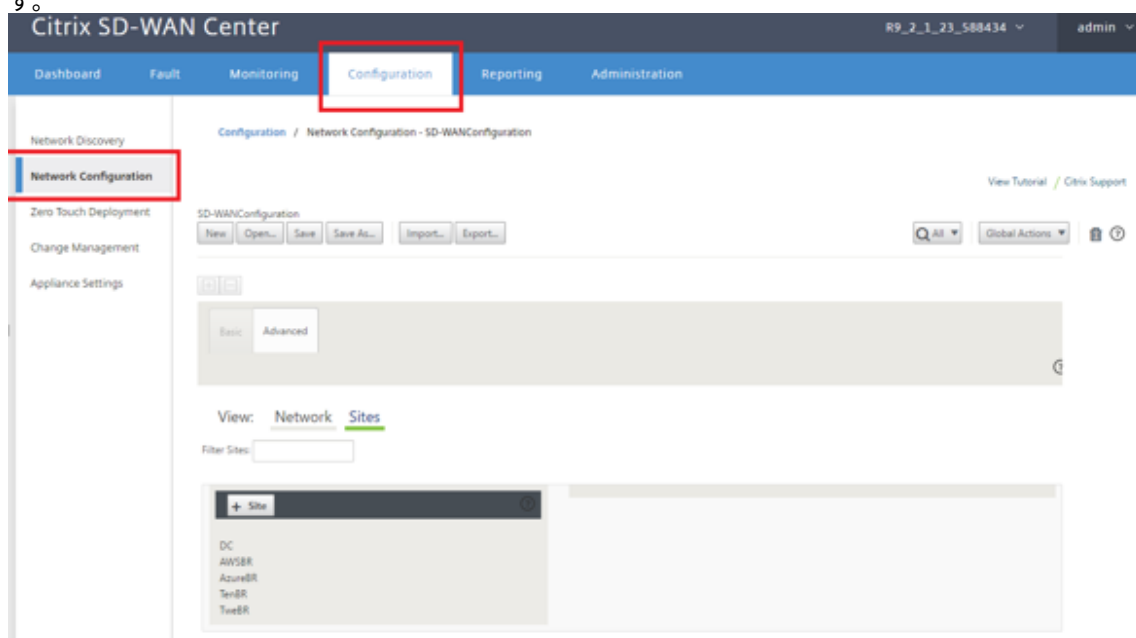
注

SD-WAN アプライアンスは、デフォルトの IP アドレス 192.168.100.1/16 を自動的に割り当てます。DHCP がデフォルトで有効になっている場合、ネットワーク内の DHCP サーバは、デフォ

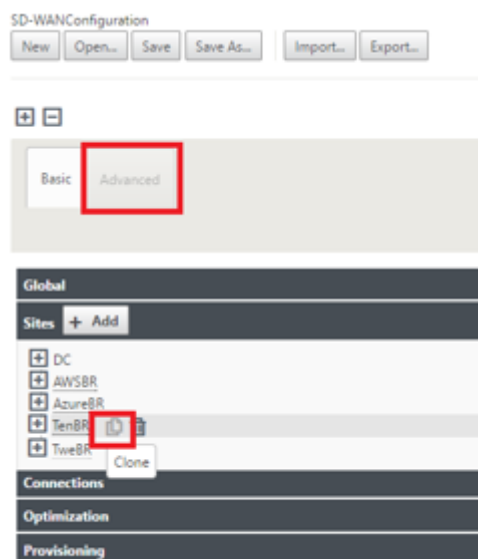
ルトと重複するサブネット内の 2 番目の IP アドレスをアプライアンスに提供することがあります。これにより、アプライアンスがゼロタッチデプロイメント Cloud Service に接続できない可能性があるアプライアンスでルーティングの問題が発生する可能性があります。DHCP サーバーを構成して、192.168.0.0/16 の範囲外の IP アドレスを割り当てます。

ネットワーク内の SD-WAN 製品の配置には、さまざまな展開モードを使用できます。上記の例では、SD-WAN が既存のネットワークインフラストラクチャの上にオーバーレイとして展開されています。新しいサイトの場合、SD-WAN 管理者は、SD-WAN をエッジモードまたは Gateway モードで展開することを選択できます。これにより、WAN エッジルータとファイアウォールが不要になり、エッジルーティングとファイアウォールのネットワークニーズを SD-WAN ソリューションに統合できます。

7. SD-WAN Center Web 管理インターフェイスを開き、[設定]>[** ネットワーク設定 **] ページに移動します。



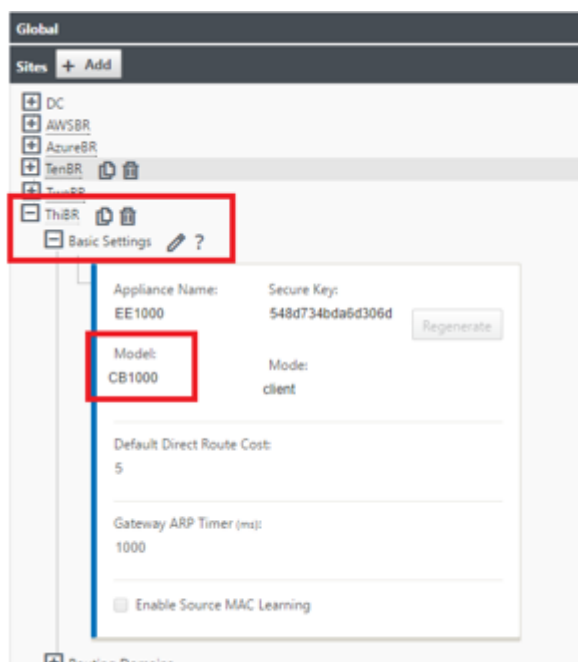
8. 作業設定が既に設定されていることを確認するか、MCN から設定をインポートします。
9. [詳細] タブに移動して、サイトを作成します。
10. [サイト] タイルを開いて、現在構成されているサイトを表示します。
11. 既存のサイトのクローン機能を使用して、新しいサイトの構成をすばやく構築しました。



12. この新しいブランチサイト

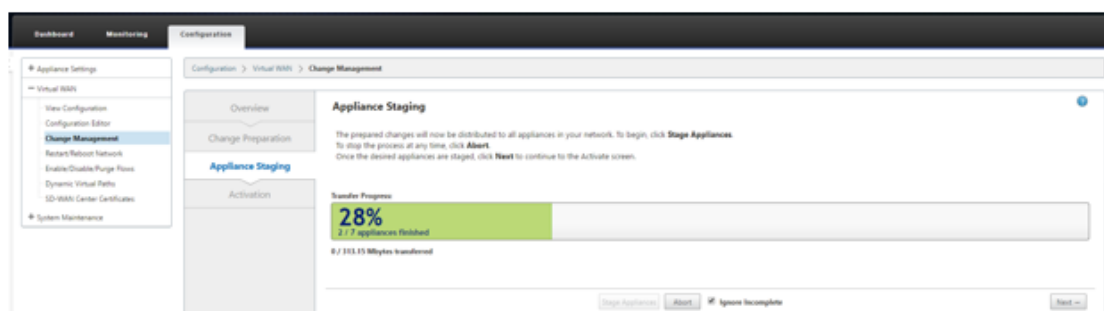
ての必須フィールドに入力します。

- 新しいサイトのクローンを作成した後、サイトの [基本設定] に移動し、ゼロタッチサービスをサポートする SD-WAN のモデルが正しく選択されていることを確認します。



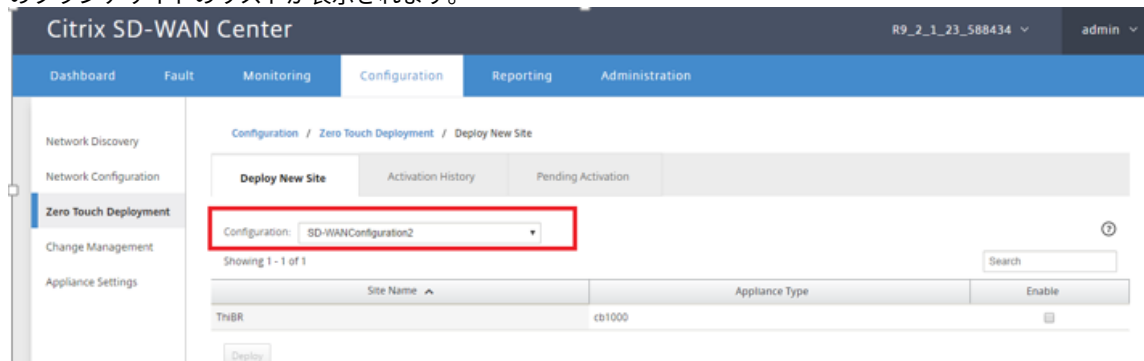
サイトの SD-WAN モデルは更新できますが、更新されたアプライアンスはクローン作成に使用されたインターフェイスレイアウトよりも新しいインターフェイスレイアウトを持つ場合があるため、インターフェイスグループの再定義が必要になる場合があることに注意してください。

14. 新しい構成を SD-WAN Center に保存し、変更管理受信トレイへのエクスポートオプションを使用して、変更管理を使用して構成をプッシュします。
15. 変更管理の手順に従って、新しい構成を適切にステージングします。これにより、既存の SD-WAN デバイスは、ゼロタッチで展開される新しいサイトを認識します。「Ignore Concomplete」オプションを使用して、まだ実行する必要がある新しいサイトに構成をプッシュすることをスキップする必要があります。ゼロタッチ導入ワークフロー。

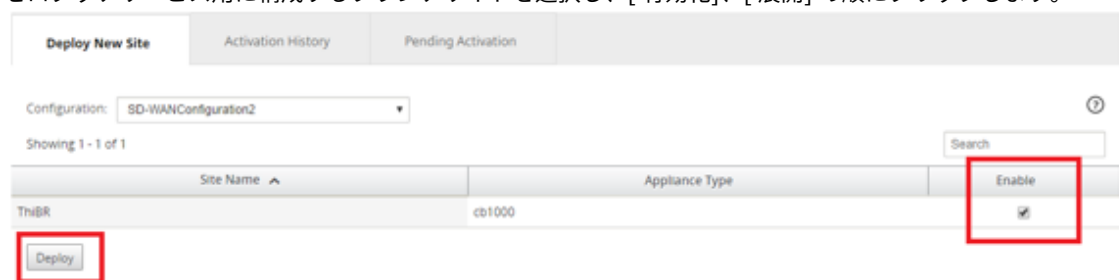


16. SD-WAN Center のゼロタッチ展開ページに戻り、新しいアクティブな構成が実行されている状態で、新しいサイトを展開できます。
17. [ゼロタッチ展開] ページの [新しいサイトの展開] タブで、実行中のネットワーク設定ファイルを選択します。
18. 実行構成ファイルを選択すると、ゼロタッチでサポートされている未展開の SD-WAN デバイスを持つすべて

のブランチサイトのリストが表示されます。



19. ゼロタッチサービス用に構成するブランチサイトを選択し、[有効化]、[展開]の順にクリックします。



20. Deploy New Site ポップアップウィンドウが表示されます。管理者は、必要に応じて、シリアル番号、ブランチサイトのストリートアドレス、インストーラの電子メールアドレス、その他のメモを提供できます。

Deploy New Site

Site Name:
ThiBR

Serial Number:
[Redacted]

Street Address:
123 Street Dr

Installer Email:
ztdinstaller@citrix.com

Additional Notes:
 1) Cable all WAN and LAN interfaces to match the topology and configuration built in earlier steps
 2) Cable the management interface (MGMT, 0/1) in the

Deploy Cancel

注

シリアル番号入力フィールドはオプションであり、入力されているかどうかに応じて、インストーラーが担当するオンサイトのアクティビティが変更されます。

- シリアル番号フィールドが入力されている場合—インストーラは、deploy site コマンドで生成されたアクティベーション URL にシリアル番号を入力する必要がありません
- シリアル番号フィールドが黒のままの場合—インストーラは、deploy site コマンドで生成されたアクティベーション URL に、アプライアンスの正しいシリアル番号を入力します。

21. [展開] ボタンをクリックすると、「サイト構成が展開されました。」というメッセージが表示されます。この操作により、以前にゼロタッチデプロイ Cloud Service に登録された SD-WAN Center がトリガーされ、この特定のサイトの構成がゼロタッチデプロイ Cloud Service に格納される一時的なものになります。
22. [保留中のアクティブ化] タブに移動して、ブランチサイト情報が正常に入力され、インストーラーアクティビティが保留中の状態になったことを確認します。

Deploy New Site Activation History Pending Activation					
Showing 1 - 1 of 1					
Site Name	Serial No	Installer Email	Address	Status	Action
ThiBR		ztinstall@.com	123 Street Dr	Connecting	
Delete Modify					

注

情報が正しくない場合は、[Pending Activation] 状態のゼロタッチ展開を [Delete] または [Modify] にオプションとして選択できます。保留中のアクティブ化ページからサイトが削除されると、そのサイトは [新しいサイトのデプロイ] タブページでデプロイできるようになります。アクティベーションの保留からブランチサイトを削除することを選択すると、インストーラーに送信されたアクティベーションリンクは無効になります。

SD-WAN 管理者が [シリアル番号] フィールドに入力しなかった場合、ステータスフィールドには「接続中」ではなく「インストーラを待機中」と表示されます。

23. 次の一連の作業は、オンサイトインストーラによって実行されます。
 - a) インストーラーは、SD-WAN 管理者がサイトの展開時に使用した電子メールアドレスのメールボックスを確認します。

NetScaler SD-WAN Cloud Service Activation Link @ThiBR



- b) インターネットブラウザウィンドウで、ゼロタッチ展開アクティベーション URL を開きます（例 <https://sdwanzt.citrixnetworkapi.net>）。
- c) SD-WAN 管理者がサイトの展開手順でシリアル番号を事前に入力しなかった場合は、インストーラが物理アプライアンスのシリアル番号を特定し、アクティベーション URL にシリアル番号を手動で入力し、[**Activate**] ボタンをクリックします。



- d) 管理者がシリアル番号情報を事前に入力している場合、アクティベーション URL は次のステップに進んでいます。



- e) 次のアクションを実行するには、設置者が現場にいる必要があります。

- 前の手順で構築したトポロジと構成に一致するように、すべての WAN および LAN インターフェイスをケーブルで接続します。
- 管理インターフェース (MGMT、0/1) DHCP IP アドレスと、DNS および FQDN から IP アドレスへの解決によりインターネットへの接続を提供するネットワークのセグメント内。
- SD-WAN アプライアンスの電源ケーブル。
- アプライアンスの電源スイッチをオンにします。

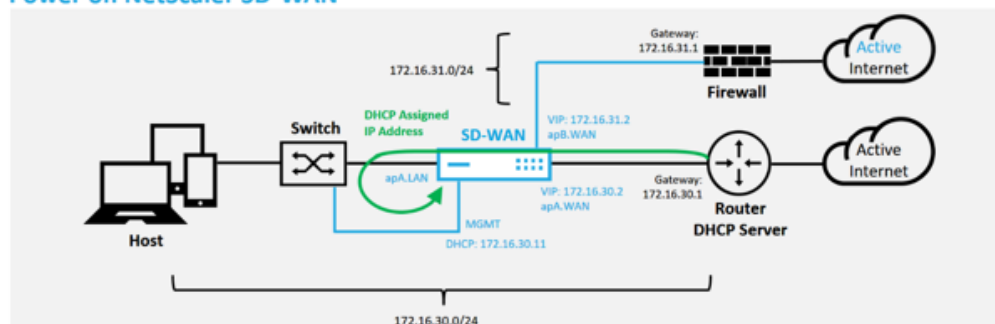
注

ほとんどのアプライアンスは、電源ケーブルを接続すると自動的に電源が入ります。アプライアンスによっては、アプライアンスの前面にある電源スイッチを使用して電源をオンにする必要がある場合や、アプライアンスの背面にある電源スイッチを使用する場合があります。一部の電源スイッチでは、ユニットの電源が入るまで電源ボタンを押し続ける必要があります。

24. 次の一連のステップは、ゼロタッチ展開サービスの助けを借りて自動化されますが、次の前提条件が利用可能である必要があります。

- ブランチアプライアンスの電源がオンになっている必要があります
 - 管理と DNS IP アドレスを割り当てるには、既存のネットワークで DHCP を使用できる必要があります
 - DHCP に割り当てられた IP アドレスには、FQDN を解決する機能を備えたインターネットへの接続が必要です。
 - IP 割り当ては、他の前提条件が満たされている限り、手動で構成できます。
- a) アプライアンスはネットワークの DHCP サーバーから IP アドレスを取得します。この例のトポロジでは、これは工場出荷時のデフォルト状態のアプライアンスのバイパスされたデータインターフェイスを介して行われます。

Power on NetScaler SD-WAN



- b) アプライアンスがアンダーレイネットワーク DHCP サーバーから Web 管理および DNS IP アドレスを取得すると、アプライアンスはゼロタッチ展開サービスを開始し、ゼロタッチ展開に関連するソフトウェアアップデートをダウンロードします。

c) ゼロタッチデプロイメントクラウドサービスへの接続に成功すると、デプロイメントプロセスは自動的に次の処理を実行します。

- SD-WAN Center によって以前に保存された構成ファイルをダウンロードします。
- ローカルアプライアンスへの構成の適用
- 10 MB の一時ライセンスファイルをダウンロードしてインストールする
- 必要に応じて、ソフトウェアの更新をダウンロードしてインストールします
- SD-WAN サービスをアクティブ化する



d) SD-WAN Center Web 管理インターフェイスでさらに確認することができます。Zero Touch Deployment メニューには、アクティベーション履歴タブに正常にアクティベーションされたアプライアンスが表示されます。

The screenshot shows the 'Configuration / Zero Touch Deployment / Activation History' page. It includes a table with the following data:

Site Name	Serial No	Installer Email	Address	Status Details	Activation Date	Status	Action
ThBR	3F6P8Z307	ztdinstaller@outlook.com	123 Street Dr	Appliance Activated	May 11 22:18:03 2017 UTC	Activated	

e) 仮想パスは、ゼロタッチデプロイメントクラウドサービスから渡された構成を MCN が信頼せず、MCN ダッシュボードに「構成バージョンの不一致」と報告するため、接続状態ですぐに表示されない場合があります。

System Status

Name: DC
 Model: VPX
 Appliance Mode: MCN
 Serial Number: 1079975b-b067-ae77-1718-d7bdf0375a2b
 Management IP Address: 172.16.10.51
 Appliance Uptime: 3 weeks, 5 days, 22 hours, 45 minutes, 35.2 seconds
 Service Uptime: 1 weeks, 2 days, 20 hours, 58 minutes, 57.0 seconds
 Routing Domain Enabled: Default_RoutingDomain

Local Versions

Software Version: 9.2.1.23.588434
 Built On: Apr 21 2017 at 05:23:29
 Hardware Version: VPX
 OS Partition Version: 4.6

Virtual Path Service Status

Virtual Path DC-AWSBR: Uptime: 1 hours, 12 minutes, 48.0 seconds.
 Virtual Path 'DC-AzureBR' is currently dead.
 Virtual Path 'DC-ThiBR' is currently dead (Configuration version mismatch)
 Virtual Path 'DC-WashDC' is currently dead.
 Virtual Path 'DC-FouBR' is currently dead.

- f) 構成は新しくインストールされたブランチオフィスアプライアンスに再配信され、ステータスは [MCN] > [構成] > [仮想 WAN] > [変更管理] ページで監視されます（このプロセスが完了するまで数分かかる場合があります）。

Change Process Overview

The Change Management process allows a user to upload changes to the network, whether it be a configuration, software, or both. This three-step workflow is a set of checks and processes that ensure that configuration changes and software updates are applied in a reliable, fail-safe way.

Step 1 Change Preparation
 Upload File to MCN

Step 2 Appliance Staging
 Transfer File to Clients

Step 3 Activation
 Activate Change

Clicking the **Activate Staged** button will skip to the Appliance Staging step, where you may switch to a previously-staged appliance package (if present).

Configuration Filenames: Active - In2-ZTD-TenTeeThiBRWSAzure-DO-NOT-ALTER.cfg Staged - SD-WANConfiguration.zip

Site-Appliance	Model	Status	Currently Active	Currently Staged	Traffic Interruption	Download Package			
DC-VPX	CB076		9.2.1.23.588434	2019 Jun 5/11/17	9.2.1.23.588434	1047 Jun 5/11/17	<1 min	198 ms	active / staged
AzureBR-Azure-001	CB005		9.2.1.23.588434	2019 Jun 5/11/17	9.2.1.23.588434	1047 Jun 5/11/17	<3 min	80 s	active / staged
FouBR-00410	CB410	Not Connected					Loc Chg Hlpr		active / none
ThiBR-00100	CB1000	Not Connected					Loc Chg Hlpr		active / staged
ThiBR-00100	CB1000	40%	9.2.1.23.588434	2148 Jun 5/11/17			Loc Chg Hlpr		active / staged
ThiBR-00400	CB400	Not Connected					Loc Chg Hlpr		active / staged

- g) SD-WAN 管理者は、リモートサイトの確立された仮想パスのヘッドエンド MCN Web 管理ページを監視できます。

Monitoring > Statistics

Statistics

Show: **Paths (Summary)** ☒ Enable Auto Refresh 5 seconds **Stop** ☒ Show latest data. Processing...

Path Statistics Summary

Filter: TH in Any column **Apply**

Num	From Link	To Link	Path State	Virtual Path Service State	Virtual Path
13	DC-A5	ThiBR-Wifi	GOOD	GOOD	Static
14	DC-B4	ThiBR-4G	GOOD	GOOD	Static
15	ThiBR-4G	DC-B4	GOOD	GOOD	Static
16	ThiBR-Wifi	DC-A5	GOOD	GOOD	Static

Showing 1 to 4 of 4 entries (filtered from 24 total entries)

Bandwidth calculated over the last 4.762 seconds

- h) SD-WAN Center は、[設定] > [ネットワーク探索] > [インベントリとステータス] ページから、オンサイトアプライアンスの DHCP 割り当てられた IP アドレスを識別するためにも使用できます。

Configuration / Network Discovery / Inventory And Status

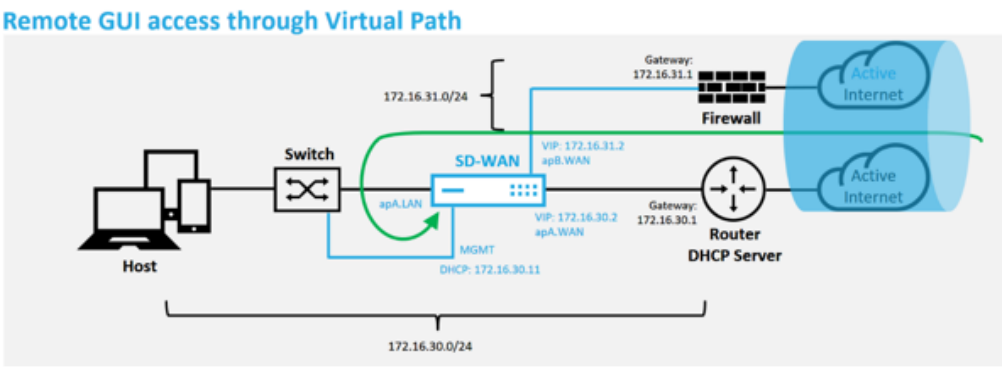
SSL Certificate Discovery Settings **Inventory And Status**

Showing 1 - 7 of 7

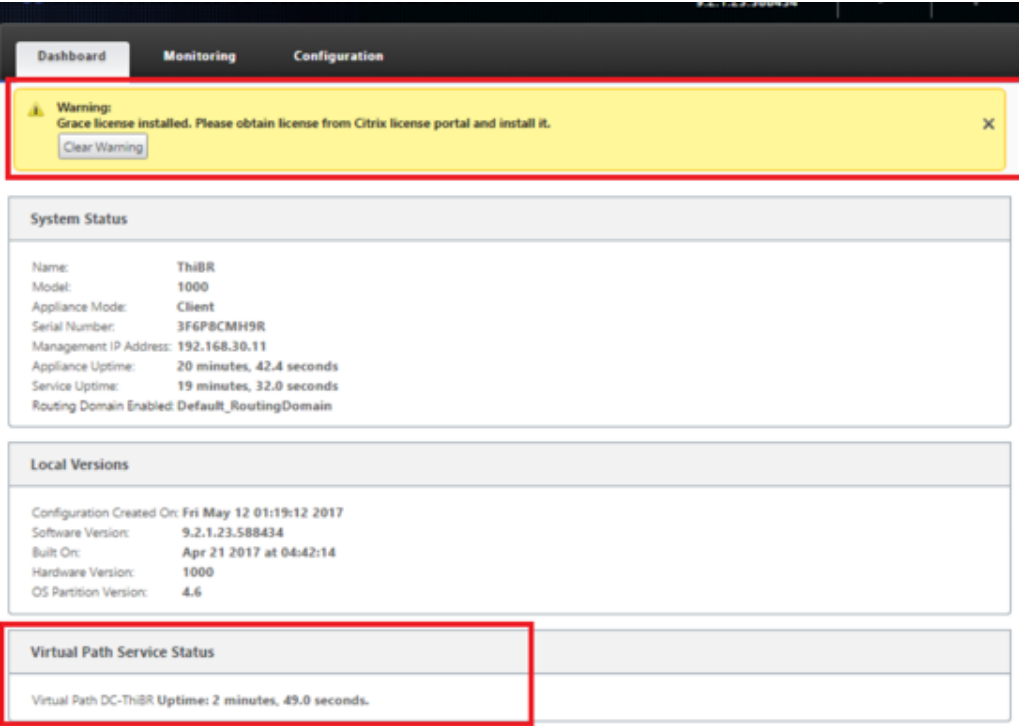
Poll	State	Name	MGT IP Address	Model	Serial Number	Software	Registry Timestamp	Last Successful Poll	Latest Record	Download
<input checked="" type="checkbox"/>	Stats in Sync	DC	172.16.10.51	cbvpx	1079975b-b067-ae77-171b-d7bd0375a2b	R9_2_1_33_588434	1494551952	05/11/17 19:02	05/11/17 19:01	
<input checked="" type="checkbox"/>	Unknown	AWSBR								
<input checked="" type="checkbox"/>	Not Reachable	AzureBR	192.168.202.4							
<input checked="" type="checkbox"/>	Unknown	FouBR								
<input checked="" type="checkbox"/>	Not Reachable	TenBR	192.168.10.11							
<input checked="" type="checkbox"/>	Not Reachable	ThiBR	192.168.30.11							
<input checked="" type="checkbox"/>	Unknown	TweBR								

Apply

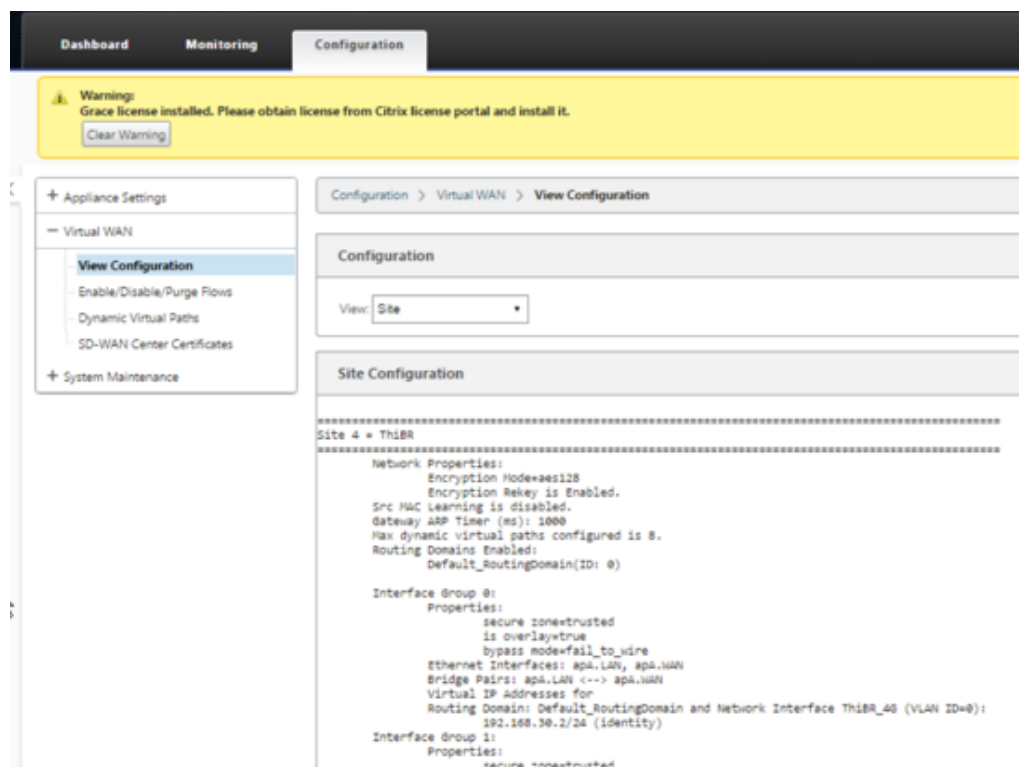
- i) この時点で、SD-WAN ネットワーク管理者は、SD-WAN オーバーレイネットワークを使用して、オンサイトアプライアンスへの Web 管理アクセスを取得できます。



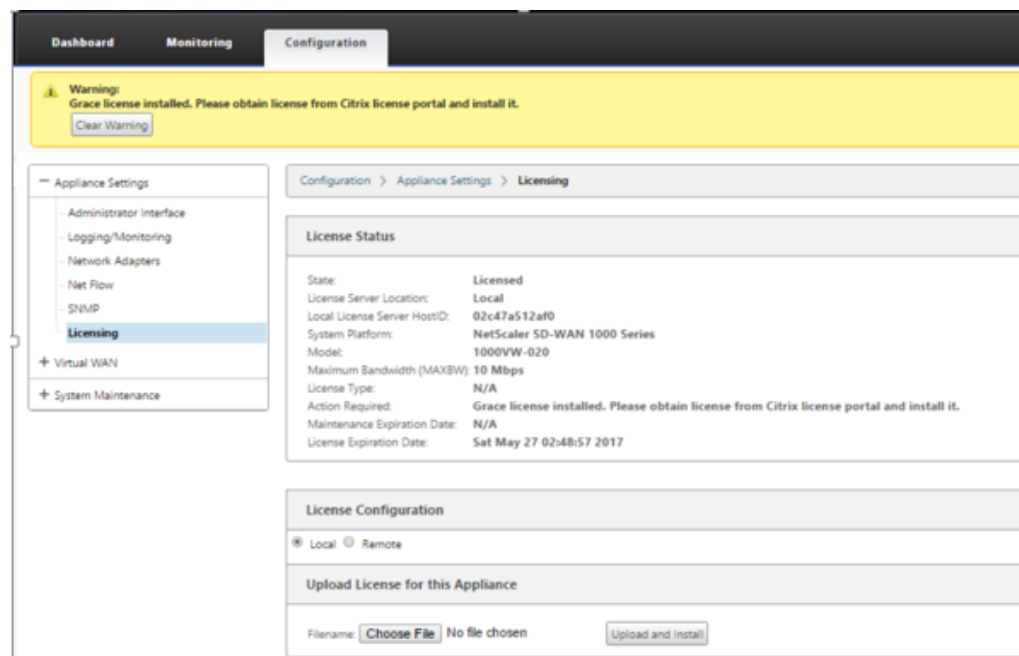
j) リモートサイトアプライアンスへの Web 管理アクセスは、アプライアンスに 10 Mbps の一時的な猶予ライセンスがインストールされていることを示しています。これにより、仮想パスサービスステータスをアクティブとして報告することができます。



k) アプライアンスの構成は、構成 > 仮想 **WAN** > 「構成の表示」ページを使用して検証できます。



- l) アプライアンスライセンスファイルは、構成 > アプライアンスの設定 > ライセンス ページを使用して永久ライセンスに更新できます。



永続ライセンスファイルをアップロードしてインストールすると、Grace License 警告バナーが消え、ライセンスインストールプロセス中にリモートサイトへの接続が失われることはありません (ping がゼロにドロップされます)。

オンプレミスのゼロタッチ

May 10, 2021

ゼロタッチサービスを使用して SD-WAN アプライアンスをデプロイする方法については、トピック「[ゼロタッチ展開サービスを構成する方法](#)」を参照してください。

AWS

May 10, 2021

以下のセクションでは、AWS 環境に ZTD をデプロイする方法について説明します。

AWS でのデプロイ:

SD-WAN リリース 9.3 では、ゼロタッチ展開機能がクラウドインスタンスに拡張されました。ゼロタッチデプロイメントプロセス 4 つのクラウドインスタンスをデプロイする手順は、ゼロタッチサービスのアプライアンスデプロイとは少し異なります。

1. SD-WAN Center ネットワーク構成を使用して、ZTD 対応の SD-WAN クラウドデバイスを持つ新しいリモートサイトを追加するように構成を更新します。

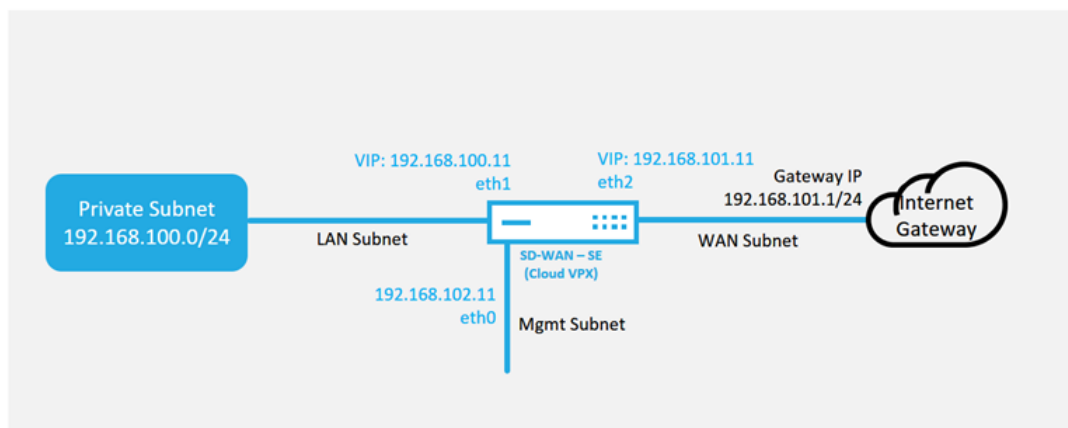
SD-WAN 設定が SD-WAN Center ネットワーク設定を使用して構築されていない場合は、MCN からアクティブな設定をインポートし、SD-WAN Center を使用して設定の変更を開始します。Zero Touch Deployment 機能を使用するには、SD-WAN 管理者は SD-WAN Center を使用して設定を構築する必要があります。ゼロタッチ展開を対象とする新しいクラウドノードを追加するには、次の手順を使用する必要があります。

- a) 最初に新しいサイトの詳細（つまり、VPX サイズ、インターフェイスグループの使用状況、仮想 IP アドレス、帯域幅を備えた WAN リンク、およびそれぞれの Gateway）を概説することにより、SD-WAN クラウド展開用の新しいサイトを設計します。

注

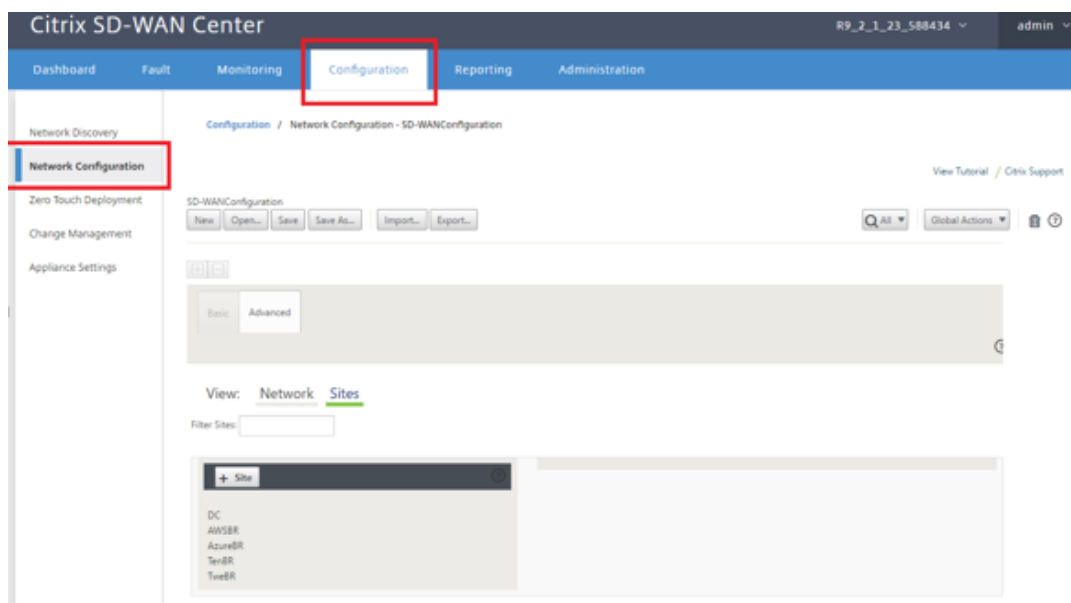
- クラウドにデプロイされた SD-WAN インスタンスは、Edge/Gateway モード。
- クラウドインスタンスのテンプレートは、管理、LAN、WAN（順序）の 3 つのインターフェイスに制限されています。
- SD-WAN VPX で使用可能なクラウドテンプレートは、現在、VPC で使用可能なサブネットの #.#..11 IP アドレスを取得するためにハードセットされています。

Cloud Topology with NetScaler SD-WAN



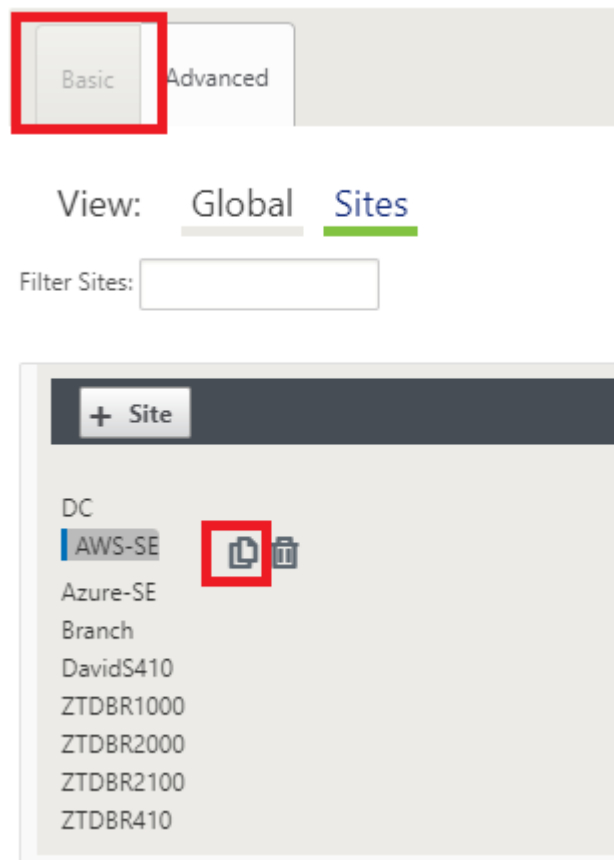
これは、SD-WAN クラウド展開サイトの展開例です。Citrix SD-WAN デバイスは、このクラウドネットワーク内の単一のインターネット WAN リンクサービスを提供するエッジデバイスとして展開されます。リモートサイトは、クラウド用のこの同じ Internet Gateway に接続する複数の異なるインターネット WAN リンクを活用して、任意の SD-WAN 展開サイトからクラウドインフラストラクチャへの耐障害性と集約帯域幅接続を提供します。これにより、コスト効率に優れ、信頼性の高いクラウド接続が可能になります。

- b) SD-WAN Center Web 管理インターフェイスを開き、[設定]>[** ネットワーク設定 **] ページに移動します。



- c) 動作中の構成がすでに配置されていることを確認するか、MCN から構成をインポートします。
- d) [基本] タブに移動して、新しいサイトを作成します。
- e) [サイト] タイルを開いて、現在構成されているサイトを表示します。
- f) 既存のサイトのクローン機能を利用して新しいクラウドサイトの構成をすばやく構築するか、新しいサ

イトを手動で構築します。



g) この新しいクラウドサイト用に設計したトポロジから、必要なフィールドをすべて入力します。

クラウド ZTD 展開で使用するテンプレートは、管理サブネット、LAN サブネット、および WAN サブネットの #..11 IP アドレスを使用するのが難しいことに注意してください。各インターフェイスで予想される.11 IP ホストアドレスと一致するように設定されていない場合、デバイスはクラウド環境ゲートウェイへの ARP と MCN の仮想パスへの IP 接続を適切に確立できません。

Clone Site

Please review the following fields and make the appropriate changes for the new Site.

Site Name: AWS-SE ! Appliance Name: AWS-SE-CBVPX Secure Key: 4a460b14f0228091

Routing Domains

Name	Enable	Default
Default_RoutingDomain	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Virtual Interfaces

Name	VLAN ID	DHCP
E1Vlan0	0	<input type="checkbox"/>
E2Vlan0	0	<input type="checkbox"/>

Virtual IP Addresses

Include	Virtual Interface	Virtual IP Address/Prefix
<input checked="" type="checkbox"/>	E1Vlan0	192.168.100.11/2 !
<input checked="" type="checkbox"/>	E2Vlan0	192.168.101.11/2 !

Local Routes

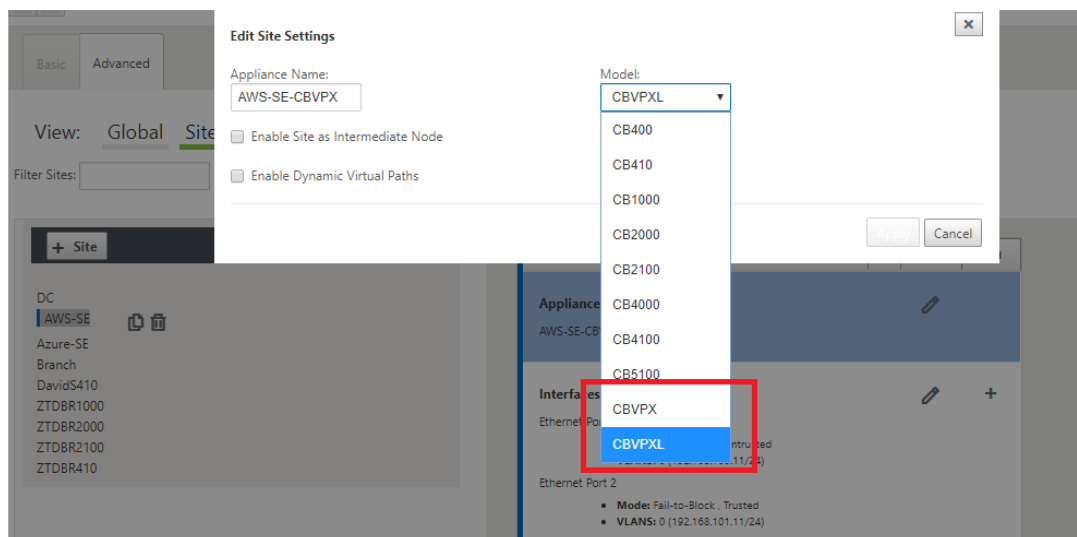
Include	Network Address	Routing Domain	Gateway
---------	-----------------	----------------	---------

WAN Links

Include Link	WAN Link	Access Type
<input checked="" type="checkbox"/>	AWS-INET !	Public Internet

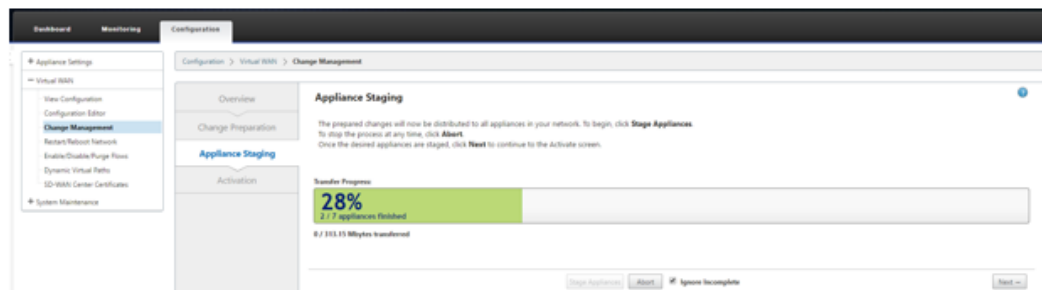
Include Interface	Access Interface	Virtual Interface	Virtual IP Address	Gateway
<input checked="" type="checkbox"/>	AWS-INET-AI-1	E2Vlan0	192.168.101.11 !	192.168.101.1 !

- h) 新しいサイトのクローンを作成したら、サイトの【基本設定】に移動し、ゼロタッチサービスをサポートする SD-WAN のモデルが正しく選択されていることを確認します。



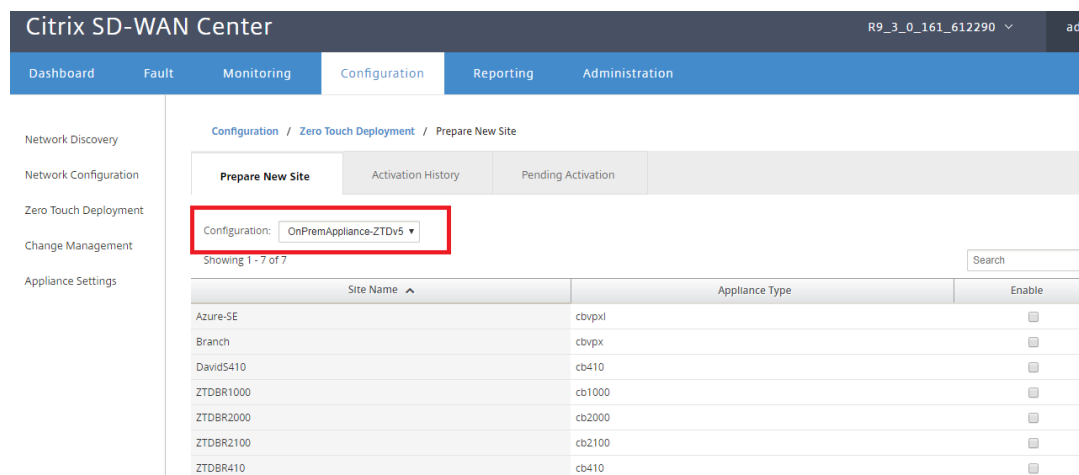
- i) 新しい構成を SD-WAN Center に保存し、変更管理受信トレイへのエクスポートオプションを使用して、変更管理 を使用して構成をプッシュします。
- j) 変更管理手順に従って新しい構成を適切にステージングします。これにより、既存の SD-WAN デバイ

スが、ゼロタッチで展開される新しいサイトを認識します。[Ignore In freted] オプションを使用して、新しいサイトに構成をプッシュしないようにする必要があります。は引き続き ZTD ワークフローを通過する必要があります。

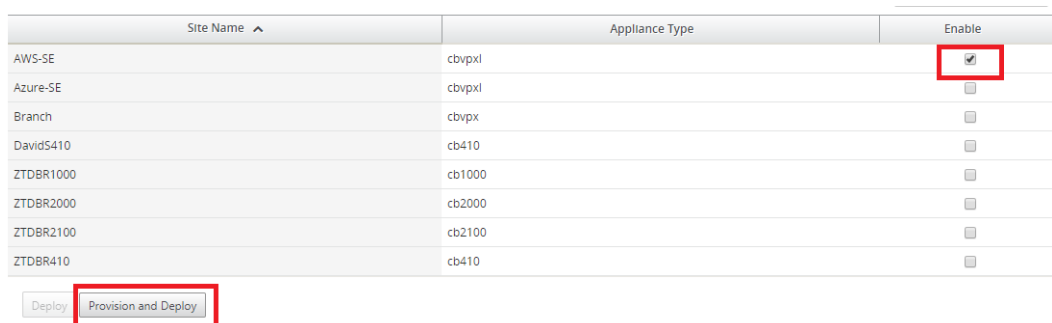


2. SD-WAN Center のゼロタッチ展開ページに戻り、新しいアクティブな構成を実行すると、新しいサイトを展開できるようになります。

- [ゼロタッチ展開] ページの [新しいサイトの展開] タブで、実行中のネットワーク構成ファイルを選択します。
- 実行構成ファイルを選択すると、ゼロタッチでサポートされている展開されていない Citrix SD-WAN デバイスを持つすべてのブランチサイトのリストが表示されます。



- Zero Touch サービスを使用してデプロイするターゲットクラウドサイトを選択し、[有効にする]、[プロビジョニングとデプロイ] の順にクリックします。

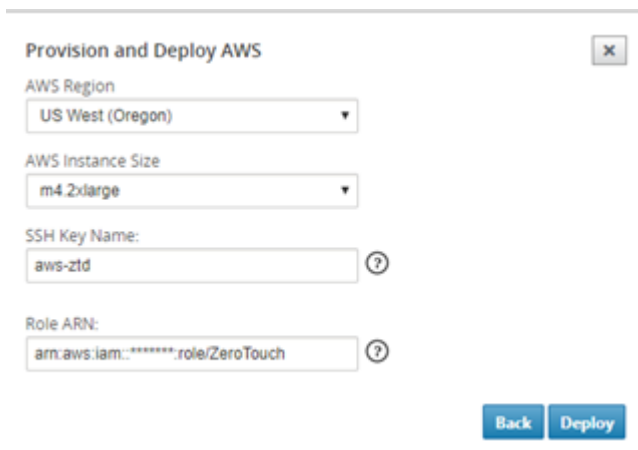


- d) ポップアップウィンドウが表示され、Citrix SD-WAN 管理者がゼロタッチの展開を開始できます。

アクティベーション URL を配信できる電子メールアドレスを入力し、目的のクラウドの プロビジョニングタイプを選択します。



- e) [次へ] をクリックし、適切なリージョン、インスタンスのサイズを選択し、SSH キー名とロール ARN フィールドに適切に設定します。



注

クラウドアカウントで SSH キーとロール ARN を設定する方法のガイダンスについては、ヘルプリンクを利用してください。また、選択したリージョンがアカウントで利用可能なリージョンと一致し、選択したインスタンスサイズが、SD-WAN 構成で選択したモデルとして VPX または VPXL と一致していることを確認します。

- f) 以前に ZTD クラウドサービスに登録されていた SD-WAN Center を起動して、ZTD クラウドサービスに保存されているサイトの設定を共有します。
- g) [**Pending Activation**] タブに移動して、サイト情報が正常に入力され、Provisioning 状態になったことを確認します。

Configuration / Zero Touch Deployment / Pending Activation

Prepare New Site	Activation History	Pending Activation
------------------	--------------------	--------------------

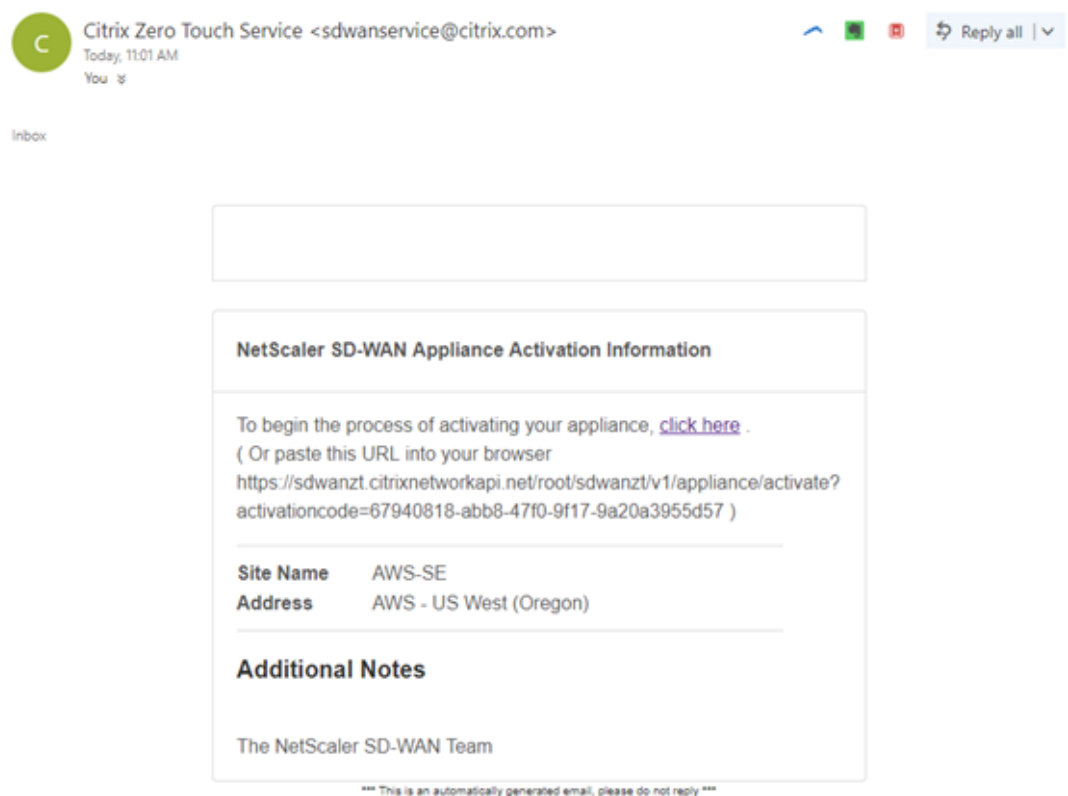
Showing 1 - 1 of 1

Site Name	Serial No	Installer Email	Address	Status	Action
AWS-SE	2E20EFCF-1A26-42DC-86D0-5624FD27C37F	ztdinstaller@outlook.com	AWS - US West (Oregon)	Provisioning	

3. クラウド管理者としてゼロタッチ導入プロセスを開始します。

- a) インストーラーは、サイトの展開時に SD-WAN 管理者が使用した電子メールアドレスのメールボックスを確認する必要があります。

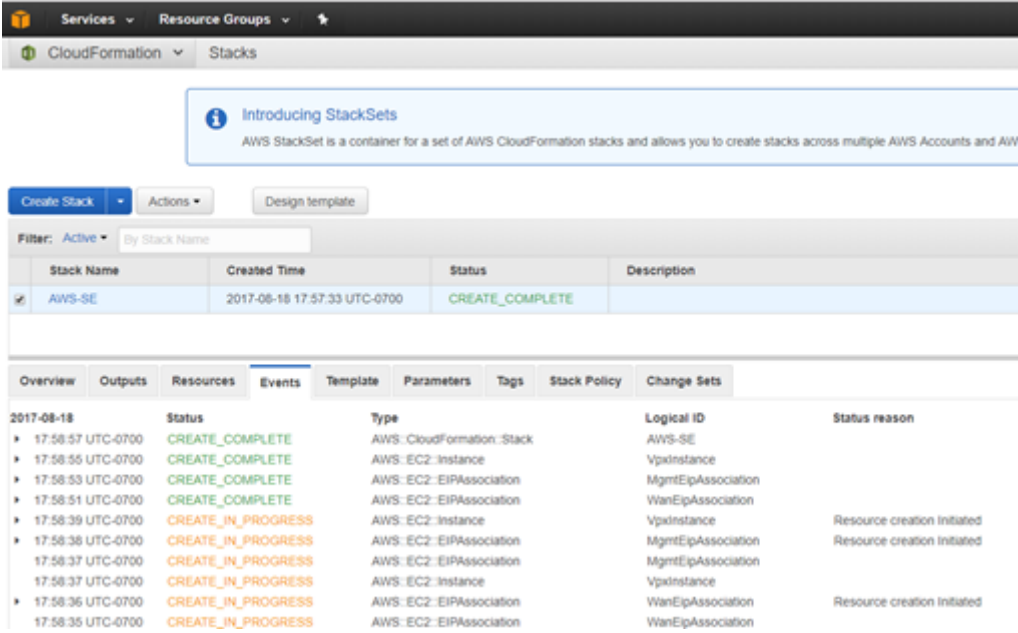
NetScaler SD-WAN Cloud Service Activation Link @AWS-SE



- b) 電子メールにあるアクティベーション URL をインターネットブラウザウィンドウで開きます（例; <https://sdwanzt.citrixnetworkapi.net>）。
- c) SSH キーとロール ARN が正しく入力されている場合、ゼロタッチ展開サービスはすぐに SD-WAN インスタンスのプロビジョニングを開始します。それ以外の場合は、接続エラーがすぐに表示されます。



d) AWS コンソールでの追加のトラブルシューティングでは、クラウド形成サービスを利用して、プロビジョニングプロセス中に発生するイベントをキャッチできます。

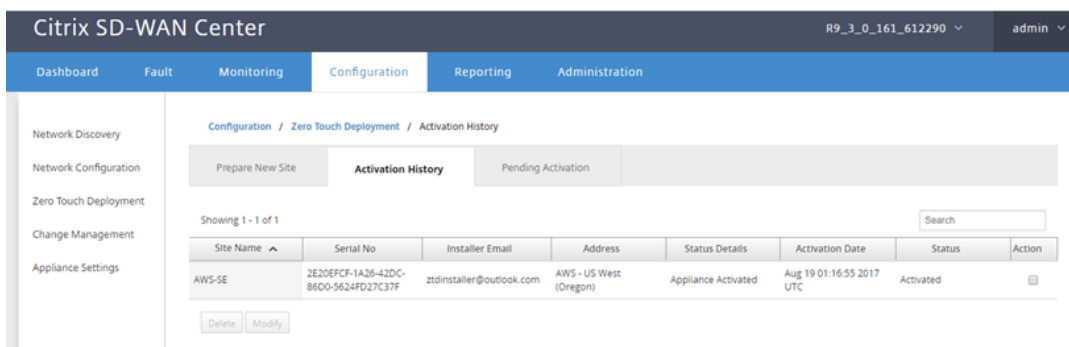


- e) プロビジョニングプロセスを許可する ~8-10 分とアクティベーション別 ~3-5 完全に完了するまで数分。
- f) SD-WAN クラウドインスタンスの ZTD クラウドサービスへの接続が成功すると、サービスは自動的に以下を実行します。

- SD-WAN Center によって以前に保存されたサイト固有の設定ファイルをダウンロードします。
- ローカルインスタンスへの構成の適用
- 10 MB の一時ライセンスファイルをダウンロードしてインストールする
- 必要に応じて、ソフトウェアの更新をダウンロードしてインストールします
- SD-WAN サービスをアクティブ化する



- g) SD-WAN Center Web 管理インターフェイスでさらに確認を行うことができます。ゼロタッチ展開メニューには、アクティベーション履歴タブに正常にアクティベートされたアプライアンスが表示されます。



- h) 仮想パスは接続状態ですぐに表示されないことがあります。これは、MCN が ZTD Cloud Service から受け継がれた設定を信頼していない可能性があり、MCN ダッシュボード で設定バージョンの不一致を報告するためです。

The screenshot displays the Citrix SD-WAN 11.4 monitoring interface. At the top, there are three tabs: **Dashboard**, **Monitoring**, and **Configuration**. The **Monitoring** tab is selected.

System Status

Name:	DC
Model:	VPX
Appliance Mode:	MCN
Serial Number:	b536a38c-5f48-b720-4f8d-b3f50b23f69f
Management IP Address:	172.16.10.30
Appliance Uptime:	1 weeks, 2 days, 3 hours, 50 minutes, 18.3 seconds
Service Uptime:	1 weeks, 2 days, 3 hours, 42 minutes, 19.0 seconds
Routing Domain Enabled:	Default_RoutingDomain

Local Versions

Software Version:	9.3.0.161.612290
Built On:	Aug 8 2017 at 14:45:01
Hardware Version:	VPX
OS Partition Version:	4.6

Virtual Path Service Status

Virtual Path DC-Branch:	Uptime: 1 days, 1 hours, 1 minutes, 12.0 seconds.
Virtual Path 'DC-DavidS410' is currently dead.	
Virtual Path DC-ZTDBR1000:	Uptime: 1 days, 1 hours, 1 minutes, 12.0 seconds.
Virtual Path 'DC-ZTDBR2000' is currently dead.	
Virtual Path 'DC-ZTDBR2100' is currently dead.	
Virtual Path 'DC-ZTDBR410' is currently dead.	
Virtual Path 'DC-AWS-SE' is currently dead (Configuration version mismatch)	
Virtual Path 'DC-Azure-SE' is currently dead.	

- i) 構成は、新しくインストールされたブランチオフィスアプライアンスに自動的に再配信されます。このステータスは、[**MCN**] > [構成] > [仮想 **WAN**] > [変更管理] ページで監視できます (接続によっては、このプロセスが完了するまで数分かかる場合があります)。

DashboardMonitoringConfiguration

+ Appliance Settings

- Virtual WAN

View Configuration

Configuration Editor

Change Management

Change Management Settings

Restart/Reboot Network

Enable/Disable/Purge Flows

Dynamic Virtual Paths

SD-WAN Center Certificates

+ System Maintenance

Configuration > Virtual WAN > Change Management

Overview

Change Preparation

Appliance Staging

Activation

Change Process Overview

The Change Management process allows a user to upload changes to the network, whether it t processes that ensure that configuration changes and software updates are applied in a reliable

Step 1

Change Preparation

Upload Files to MCN

MCN

Step 2

Appliance

Transfer Files

MCN

Clicking the **Activate Staged** button will skip to the Appliance Staging step, where you may switch to a pr

Configuration Filenames: Active - OnPremAppliance-ZTDv5.zip Stag

Search

Site-Appliance	Model	State	Currently Active		Current
			Software	Config	Software
DC-DC_SDWAN	CBVPX		9.3.0.161.612290	10:55 on 8/18/17	9.3.0.161.612290
AWS-SE-AWS-SE-CBVPX	CBVPXL	6%	9.3.0.161.612290		
Azure-SE-Azure-SE-CBVPX	CBVPXL	Not Connected			
Branch-Branch_SDWAN	CBVPX		9.3.0.161.612290	10:55 on 8/18/17	9.3.0.161.612290

j) SD-WAN 管理者は、新しく追加されたクラウドサイトの確立された仮想パスについて、ヘッドエンドの MCN Web 管理ページを監視できます。

DashboardMonitoringConfiguration

Statistics

Flows

Routing Protocols

Firewall

IKE/IPsec

Performance Reports

Qos Reports

Usage Reports

Availability Reports

Appliance Reports

DHCP Server/Relay

Monitoring > Statistics

Statistics

Show: Paths (Summary) Enable Auto Refresh 5 seconds Start Show latest data.

Path Statistics Summary

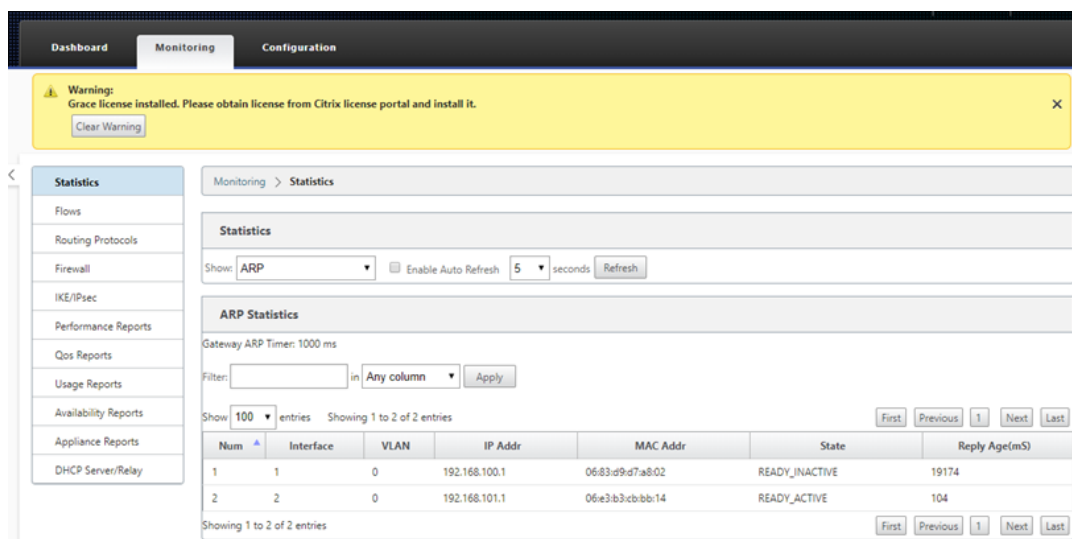
Filter: AWS Any column Apply

Num	From Link	To Link	Path State	Virtual Path Service State	Virtual Path Service Type	BOWT	Jitter (mS)	Loss %	kbps	Congestion
27	DC-INET	AWS-INET	GOOD	GOOD	Static	26	2	0.00	16.20	NO
28	AWS-INET	DC-INET	GOOD	GOOD	Static	26	2	0.00	15.13	NO

Showing 1 to 2 of 2 entries (filtered from 30 total entries)

Bandwidth calculated over the last 0.956 seconds

k) トラブルシューティングが必要な場合は、Provisioning 中にクラウド環境によって割り当てられたパブリック IP を使用して SD-WAN インスタンスのユーザーインターフェイスを開き、[**Monitoring**] > [**Statistics**] ページの [ARP] テーブルを使用して、予想されるゲートウェイへの接続に関する問題を特定します。は、診断でトレースルートとパケットキャプチャオプションを使用します。



Azure

May 10, 2021

クラウドインスタンスのゼロタッチ展開プロセスを展開する手順は、ゼロタッチサービスのアプライアンス展開とは少し異なります。

SD-WAN Center のネットワーク構成を使用して、ZTD 対応の SD-WAN クラウドデバイスを持つ新しいリモートサイトを追加するように構成を更新します。

SD-WAN 設定が SD-WAN Center ネットワーク設定を使用して構築されていない場合は、MCN からアクティブな設定をインポートし、SD-WAN Center を使用して設定の変更を開始します。Zero Touch Deployment 機能を使用するには、SD-WAN 管理者は SD-WAN Center を使用して設定を構築する必要があります。ゼロタッチ展開を対象とする新しいクラウドノードを追加するには、次の手順を使用する必要があります。

- 最初に新しいサイトの詳細（つまり、VPX サイズ、インターフェイスグループの使用状況、仮想 IP アドレス、帯域幅を備えた WAN リンク、およびそれぞれの Gateway）を概説することにより、SD-WAN クラウド展開用の新しいサイトを設計します。

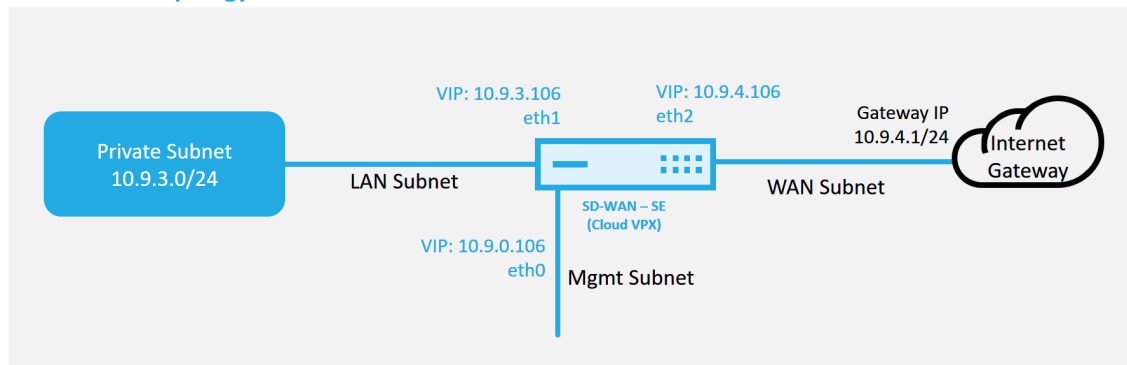
注

- クラウドにデプロイされた SD-WAN インスタンスは、Edge/Gateway モード。
- クラウドインスタンスのテンプレートは 3 つのインターフェースに制限されています。管理、LAN、WAN（この順序で）。
- SD-WAN VPX で使用できる Azure クラウドテンプレートは、現在、WAN に 10.9.4.106 IP、LAN に 10.9.3.106 IP、管理アドレスに 10.9.0.16 IP を取得するようにハードセットされています。ゼ

口タッチの対象となる Azure ノードの SD-WAN 構成は、このレイアウトと一致する必要があります。

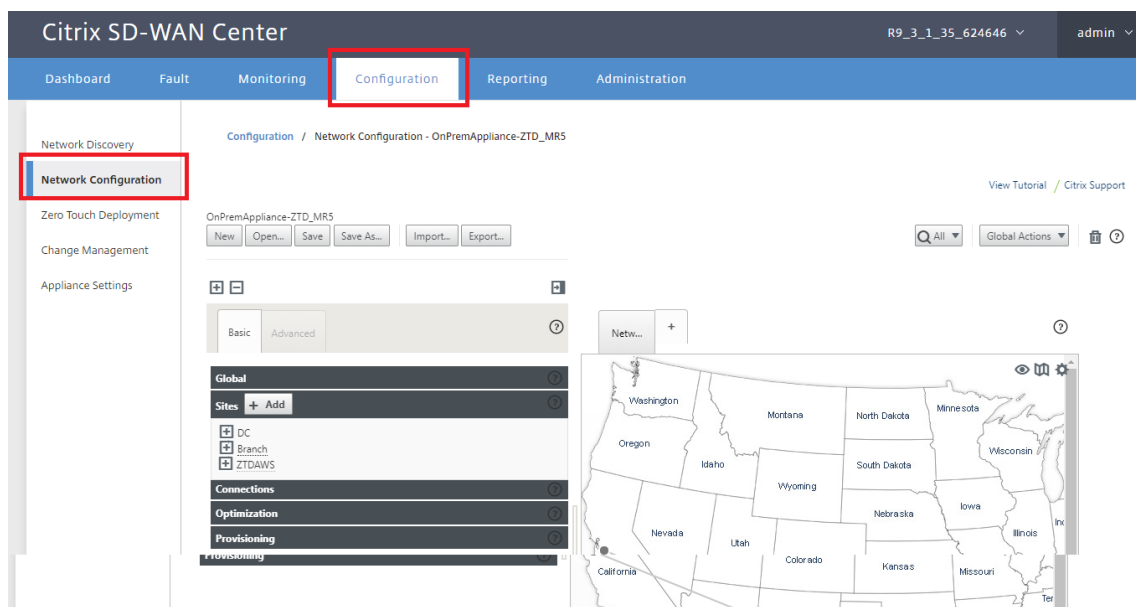
- 構成内の Azure サイト名は、特殊文字を含まないすべて小文字にする必要があります（ztdazure など）。

Azure Cloud Topology with NetScaler SD-WAN



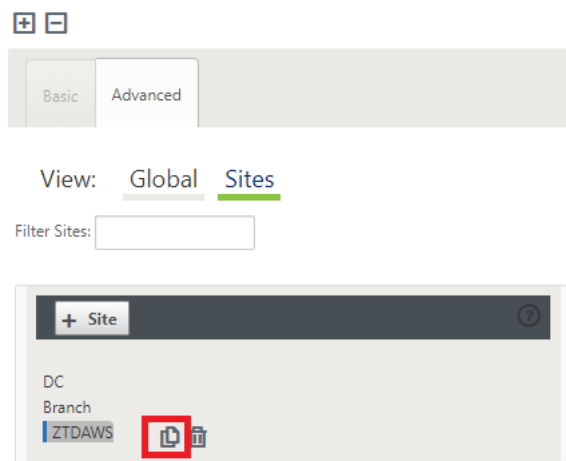
これは、SD-WAN クラウド展開サイトの展開例です。Citrix SD-WAN デバイスは、このクラウドネットワーク内の単一のインターネット WAN リンクサービスを提供するエッジデバイスとして展開されます。リモートサイトは、クラウド用のこの同じ Internet Gateway に接続する複数の異なるインターネット WAN リンクを活用して、任意の SD-WAN 展開サイトからクラウドインフラストラクチャへの耐障害性と集約帯域幅接続を提供します。これにより、費用対効果が高く、信頼性の高いクラウドへの接続が可能になります。

2. SD-WAN Center Web 管理インターフェイスを開き、[設定] > [** ネットワーク設定 **] ページに移動します。



3. 動作中の構成がすでに配置されていることを確認するか、MCN から構成をインポートします。
4. [基本] タブに移動して、新しいサイトを作成します。

5. [サイト] タイルを開いて、現在構成されているサイトを表示します。
6. 既存のサイトのクローン機能を利用して新しいクラウドサイトの構成をすばやく構築するか、新しいサイトを手動で構築します。



7. この新しいクラウドサイト用に以前に設計されたトポロジのすべての必須フィールドに入力します。

Azure クラウド ZTD デプロイメントに使用できるテンプレートは現在、WAN に 10.9.4.106 IP、LAN に 10.9.3.106 IP、管理アドレスに 10.9.0.16 IP を取得するようにハードセットされていることに注意してください。各インターフェースの予想される VIP アドレスと一致するように設定されていない場合、デバイスはクラウド環境ゲートウェイへの ARP と MCN の仮想パスへの IP 接続を適切に確立できません。

サイト名が Azure が期待するものに準拠していることが重要です。サイト名は、特殊文字を使用せず、すべての小文字、少なくとも 6 文字でなければなりません。次の正規表現 `^[a-z][a-z0-9-]{1,61}[a-z0-9]$` を確認する必要があります。

Clone Site

Please review the following fields and make the appropriate changes for the new Site.

Site Name: Appliance Name: Secure Key:

Routing Domains

Name	Enable	Default
Default_RoutingDomain	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Virtual Interfaces

Name	VLAN ID	DHCP
E1Vlan0	0	<input type="checkbox"/>
E2Vlan0	0	<input type="checkbox"/>

Virtual IP Addresses

Include	Virtual Interface	Virtual IP Address/Prefix
<input checked="" type="checkbox"/>	E1Vlan0	10.9.3.106/24
<input checked="" type="checkbox"/>	E2Vlan0	10.9.4.106/24

Local Routes

Include	Network Address	Routing Domain	Gateway
---------	-----------------	----------------	---------

WAN Links

Include Link	WAN Link	Access Type
<input checked="" type="checkbox"/>	Azure-INET	Public Internet

Access Interfaces

Include Interface	Access Interface	Virtual Interface	Virtual IP Address	Gateway
<input checked="" type="checkbox"/>	Azure-WL-1-AI-1	E2Vlan0	10.9.4.106	10.9.4.1

GRE Tunnels

Include	Name	Source IP	Destination IP	Tunnel IP / Prefix
---------	------	-----------	----------------	--------------------

Clone Cancel

8. 新しいサイトのクローンを作成したら、サイトの【基本設定】に移動し、ゼロタッチサービスをサポートする SD-WAN のモデルが正しく選択されていることを確認します。

Edit Site Settings

Appliance Name:

Model:

☐ Enable Site as Intermediate Node

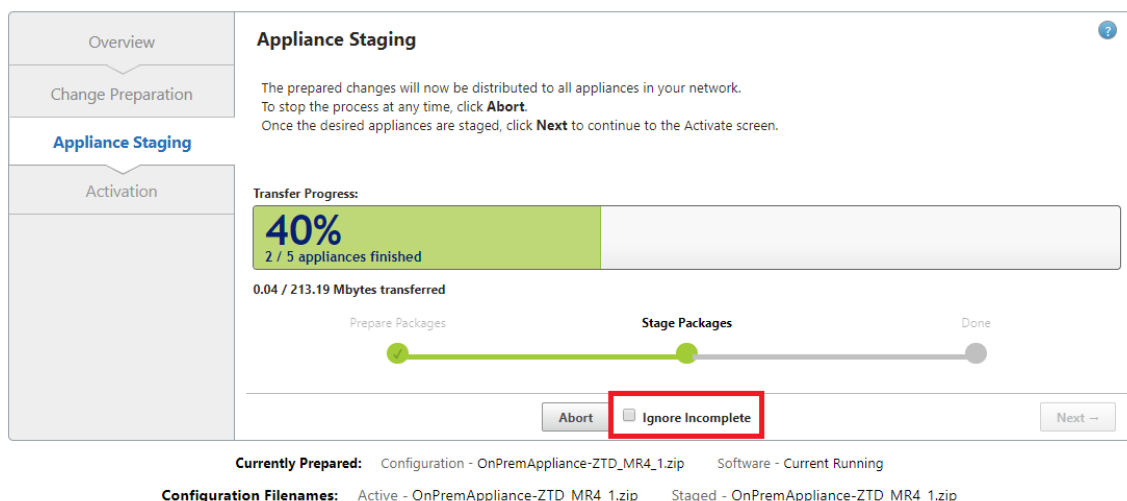
☐ Enable Dynamic Virtual Paths

Apply Cancel

Appliance: azure-CBVPXL

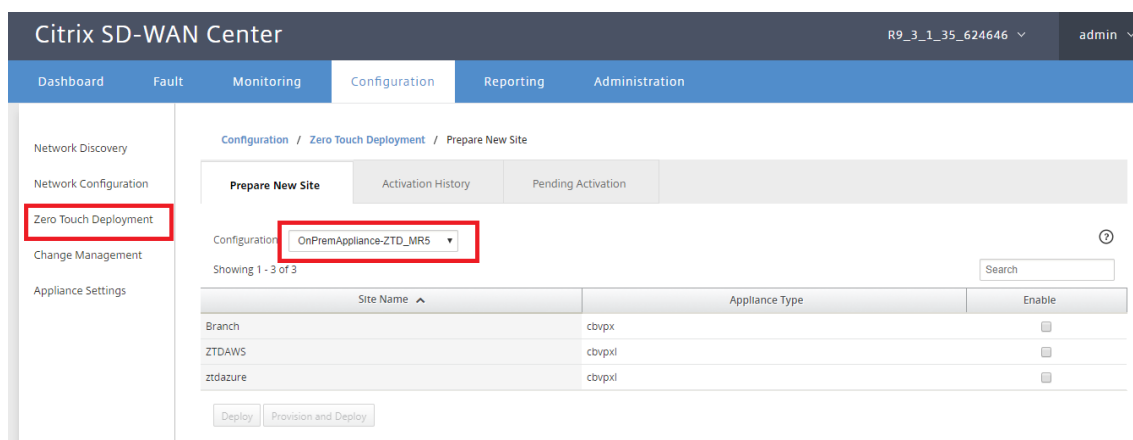
Interfaces: Ethernet Port

9. 新しい構成を SD-WAN Center に保存し、変更管理受信トレイへのエクスポートオプションを使用して、変更管理を使用して構成をプッシュします。
10. 変更管理手順に従って新しい構成を適切にステージングします。これにより、既存の SD-WAN デバイスが、ゼロタッチで展開される新しいサイトを認識します。[Ignore In freted] オプションを使用して、新しいサイトに構成をプッシュしないようにする必要があります。は引き続き ZTD ワークフローを通過する必要があります。



SD-WAN Center の [ゼロタッチデプロイ] ページに移動し、新しいアクティブな構成が実行されている状態で、新しいサイトを **SD-WAN Center** のプロビジョニングとデプロイ **Azure** で使用できるようになります (ステップ 1/2)

1. Zero Touch Deployment ページで、Citrix アカウントの認証情報を使用してログインします。[新しいサイトの展開] タブで、実行中のネットワーク構成ファイルを選択します。
2. 実行構成ファイルを選択すると、ZTD 対応の Citrix SD-WAN デバイスを持つすべてのブランチサイトのリストが表示されます。



3. Zero Touch サービスを使用してデプロイするターゲットクラウドサイトを選択し、[有効にする]、[プロビジョニングとデプロイ] の順にクリックします。

Configuration / Zero Touch Deployment / Prepare New Site

Prepare New Site Activation History Pending Activation

Configuration: OnPremAppliance-ZTD_MR5

Showing 1 - 3 of 3

Site Name ^	Appliance Type	Enable
Branch	cbvpx	<input type="checkbox"/>
ZTDAWS	cbvpxl	<input type="checkbox"/>
ztdazure	cbvpxl	<input checked="" type="checkbox"/>

Deploy Provision and Deploy

4. ポップアップウィンドウが表示され、Citrix SD-WAN 管理者がゼロタッチの展開を開始できます。サイト名が Azure の要件 (特殊文字のない小文字) に準拠していることを確認します。ライセンス認証 URL を配信できる電子メールアドレスを入力し、目的のクラウドの [プロビジョニングの種類] として [Azure] を選択し、[次へ] をクリックします。

Provision and Deploy

Site Name:
ztdazure

Installer Email:
ztdinstaller@outlook.com

Provision Type
AZURE

Next

5. [次へ] をクリックすると、Azure のプロビジョニングとデプロイ (ステップ 1/2) ウィンドウには、Azure アカウントから取得したの入力が必要になります。

Azure アカウントから情報を取得したら、各必須フィールドをコピーして貼り付けます。以下の手順では、Azure アカウントから必要なサブスクリプション ID、アプリケーション ID、秘密キー、およびテナント ID を取得し、[次へ] をクリックして続行する方法の概要を説明します。

Provision and Deploy Azure (step 1 of 2)

Subscription ID:
52dd5bd9-2671-4cd3-8029-0f7d68108d53

Application ID:
2382ebde-09b4-4ec8-9098-0bdd6e113a54

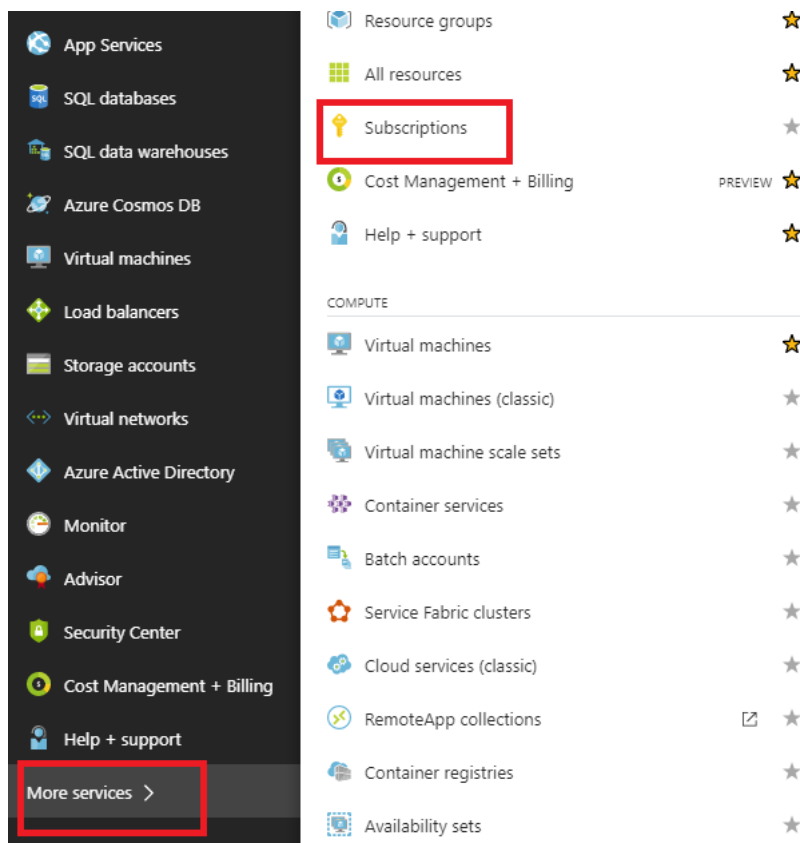
Secret Key:
om5RZX9bY2T+GzJbP0qoCgtm1fBEMS...

Tenant ID:
335836de-42ef-43a2-b145-348c2ee9ca5b

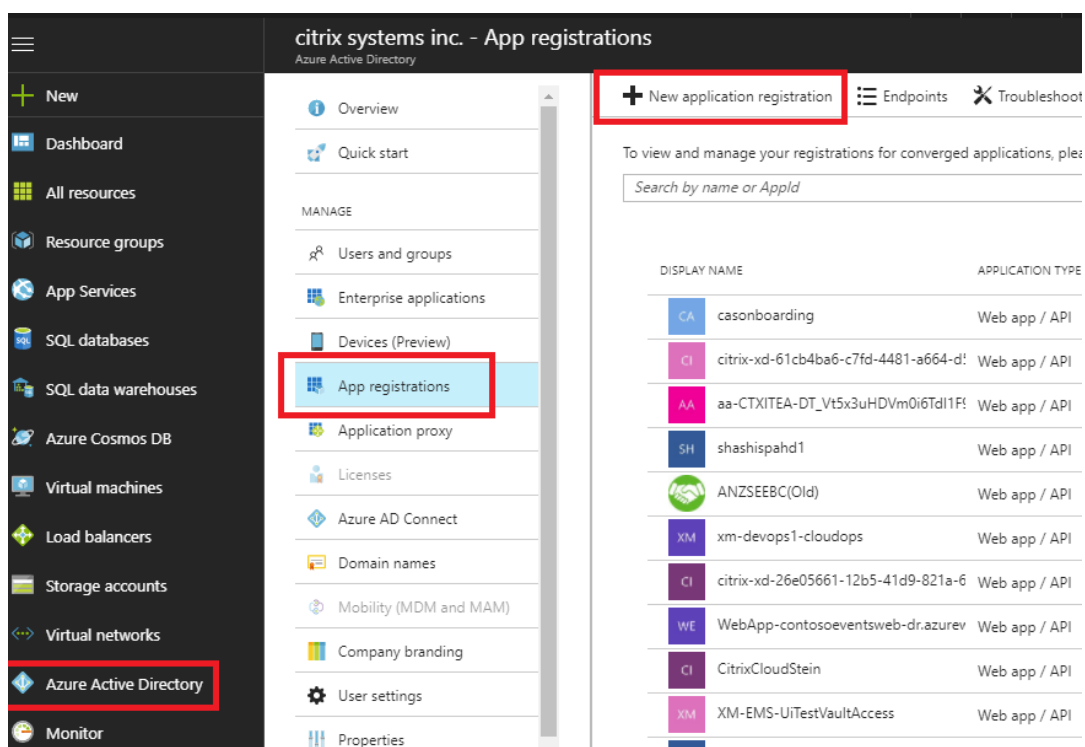
SSH Public Key:
ssh-rsa
AAAAAB3NzaC1yc2EAAAABJQAAAAQEAu9I2mFuhPLsVINVh+
s2piG3uv2lshYlBaE4nH3y3lazeEhhl6Ng4rAf+LPSoZcBJLHh3
nAEAJmcyJTfwmt61Yd4y339ciasEDmPEWEzqcyFGaQ0i/DFI

[Back](#) [Next](#)

- a) Azure アカウントで、[その他のサービス] に移動し、[サブスクリプション] を選択することで、必要なサブスクリプション ID を特定できます。



- b) 必要な * アプリケーション ID を特定するには、Azure Active Directory、アプリケーションの登録に移動し、[新しいアプリケーション登録] をクリックします。



- c) アプリ登録の作成メニューで、[名前] と [サインオン URL] (任意の URL でもかまいません。唯一の要件は、有効であることが必要です) を入力し、[作成] をクリックします。

Create

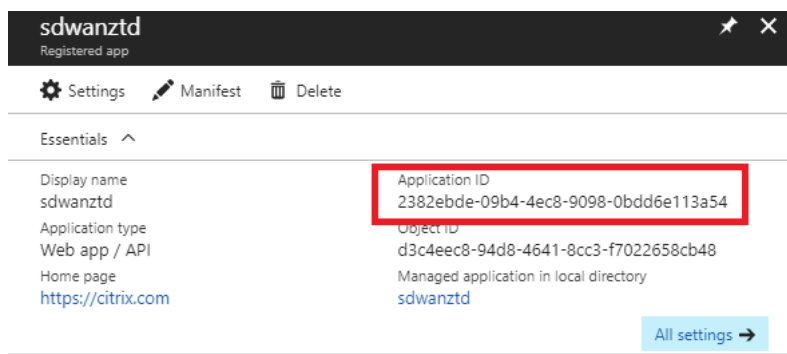
* Name ✓

Application type

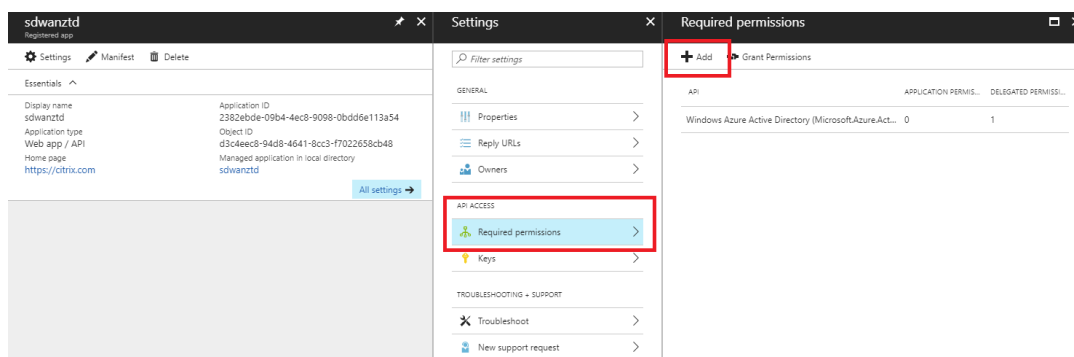
* Sign-on URL ✓

Create

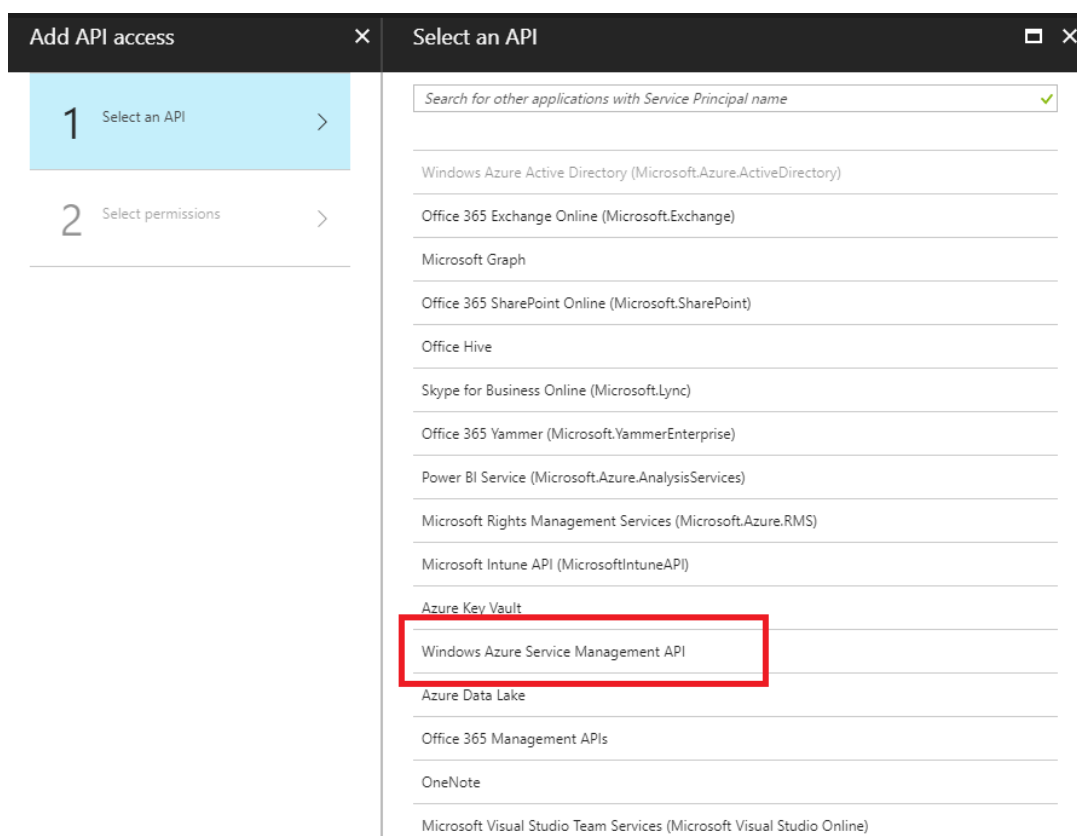
- d) 新しく作成された登録済みアプリを検索して開き、アプリケーション ID をメモします。



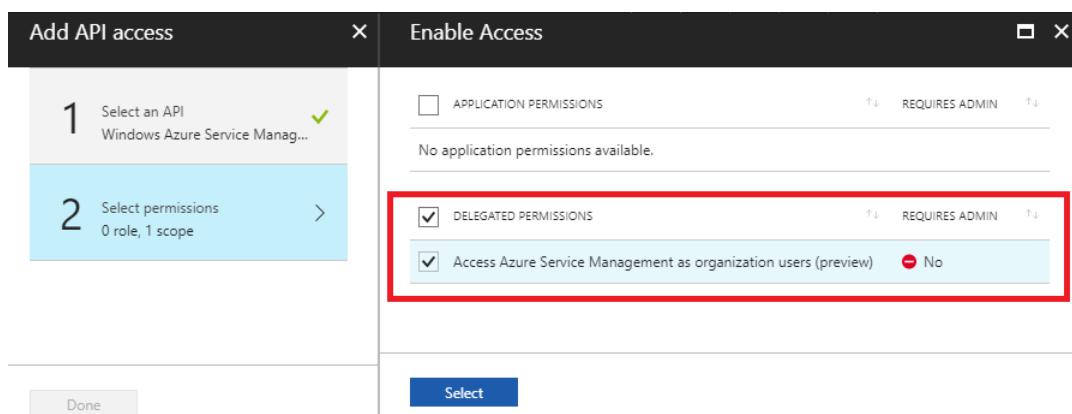
- e) 新しく作成した登録アプリを再度開き、必要なセキュリティキーを特定するには、[API アクセス] で [必要なアクセス許可] を選択し、サードパーティがプロビジョニングとインスタンスを許可します。次に、[追加] を選択します。



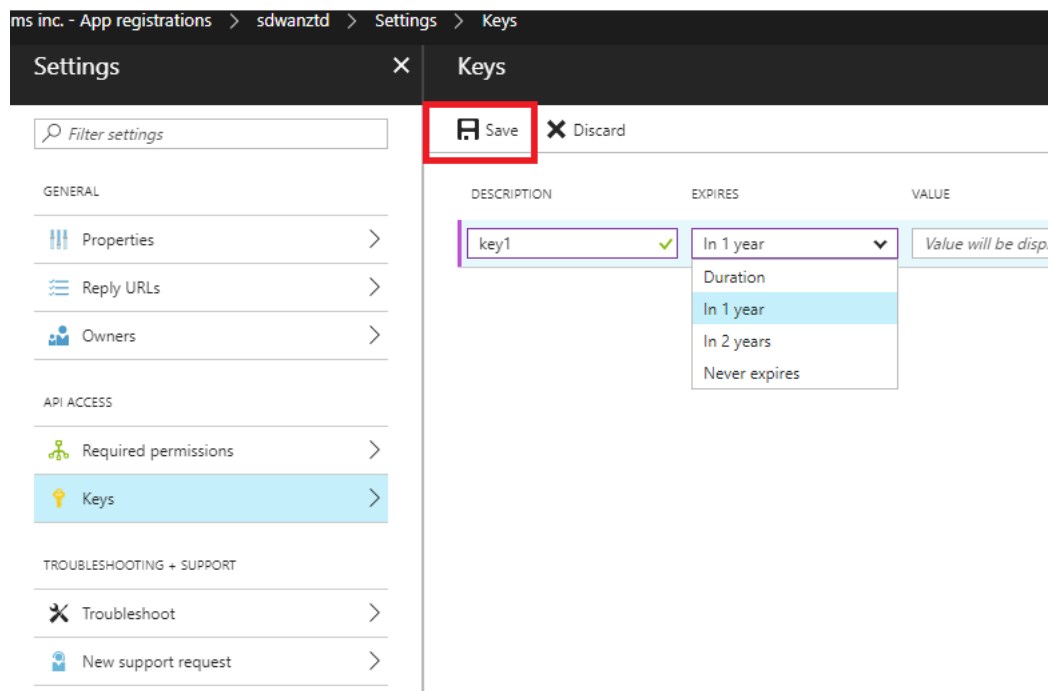
- f) 必要なアクセス許可を追加する場合は、[API を選択] を選択し、[Windows Azure サービス管理 API] を強調表示します。



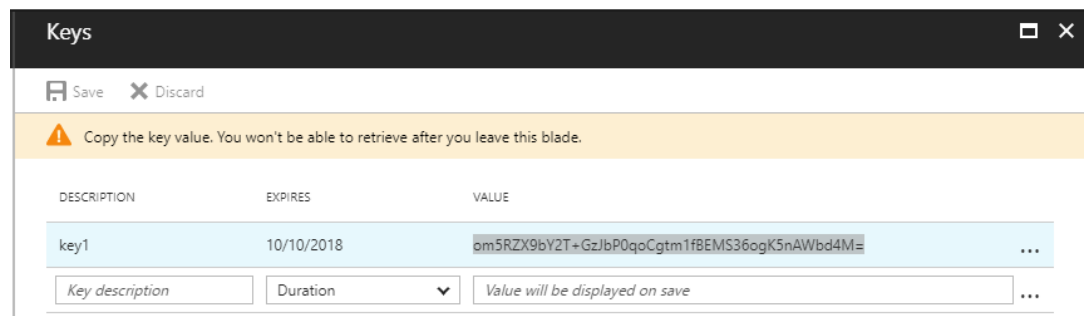
- g) 代理アクセス権限 を有効にしてインスタンスをプロビジョニングし、[**Select and Done**] をクリックします。



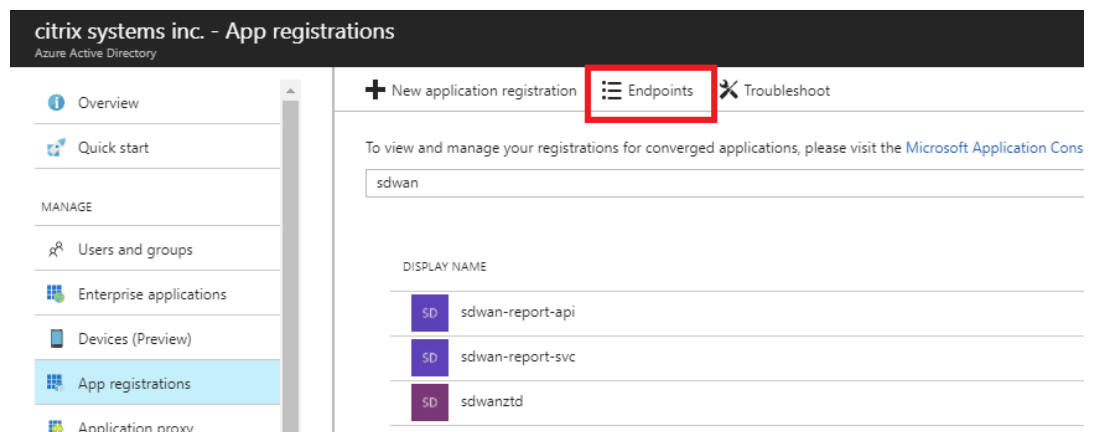
- h) この登録済みアプリの場合、[API アクセス] で [キー] を選択し、秘密キーの説明とキーが有効になるまでの所要時間を作成します。次に、[**Save**] をクリックすると、シークレットキー が生成されます (キーは Provisioning プロセスでのみ必要であり、インスタンスが利用可能になった後に削除できます)。



- i) 秘密鍵をコピーして保存します（後でこれを取得することはできません）。

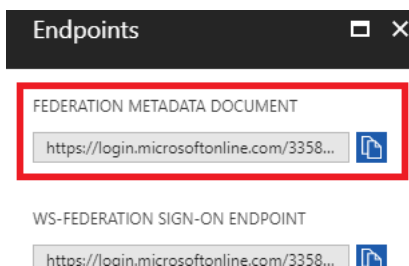


- j) 必要なテナント **ID** を特定するには、[アプリ登録] ペインに戻り、[エンドポイント] を選択します。

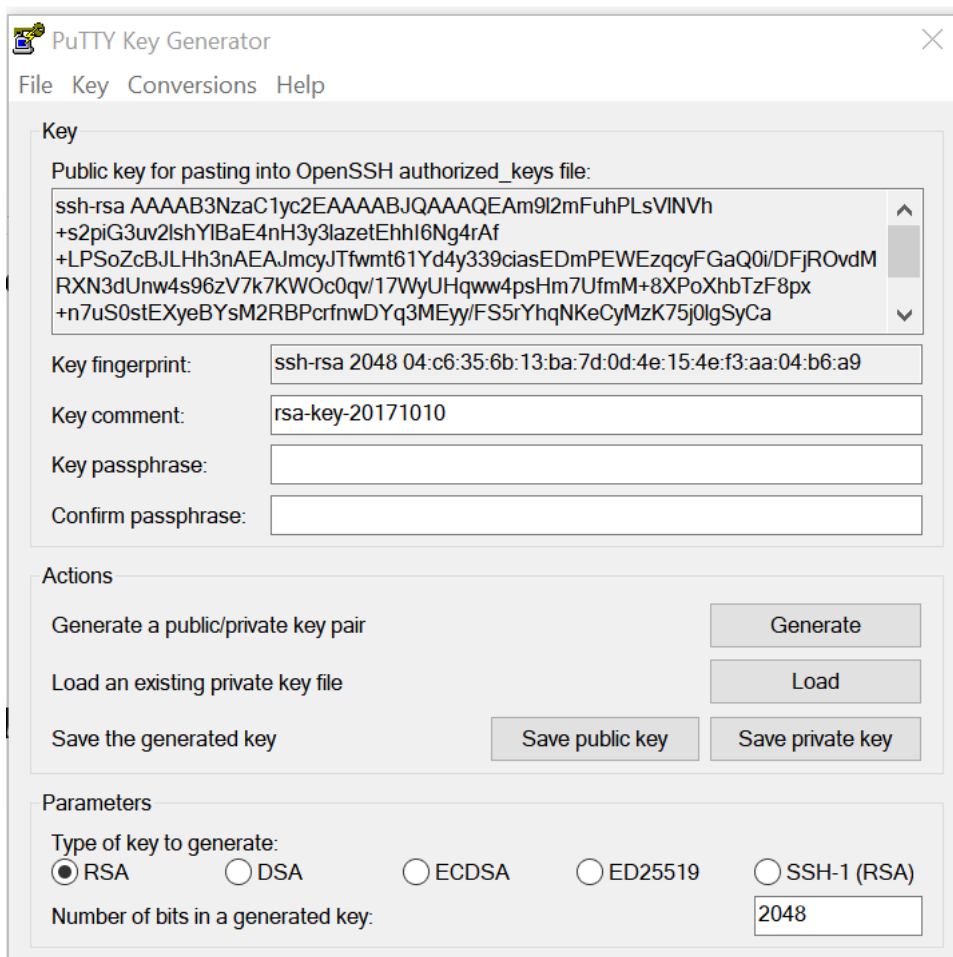


- k) テナント ID を識別するために、フェデレーションメタデータドキュメントをコピーします（テナント ID は URL 内の **online.com/** と **/federation** の間にある 36 文字の文字列であることに注意して

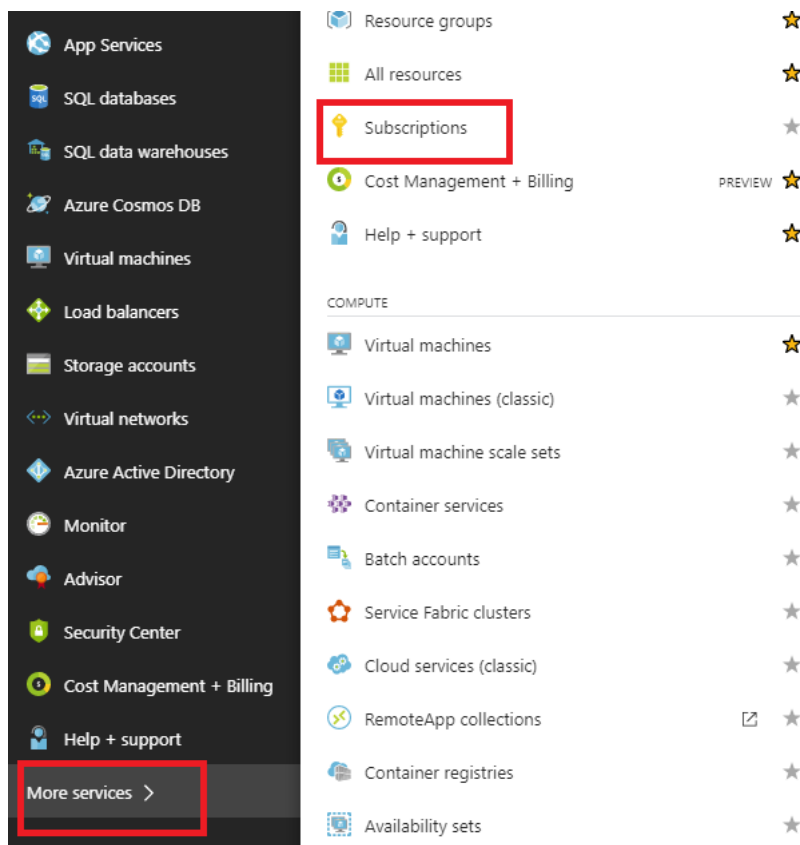
ください)。



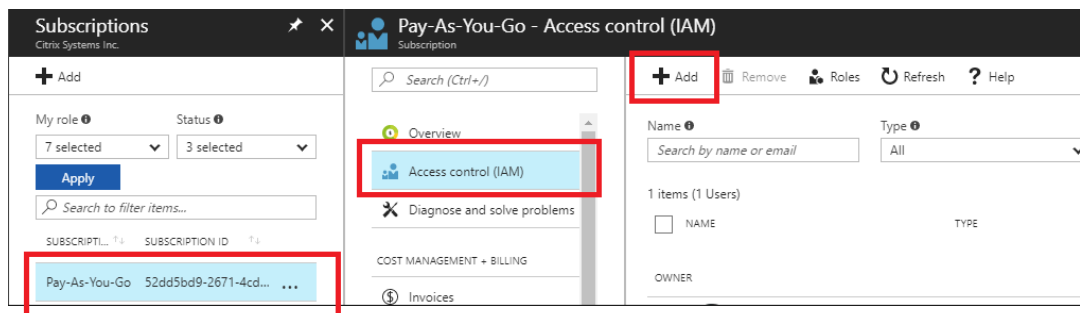
- l) 最後に必要な項目は **SSH** 公開鍵です。これは、パテキージェネレータまたは `ssh-keygen` を使用して作成することができ、認証に利用されるため、パスワードがログインする必要はありません。SSH 公開鍵はコピーできます（見出しの `ssh-rsa` と末尾の `rsa-key` 文字列を含む）。この公開鍵は、Citrix ゼロタッチ展開サービスへの SD-WAN Center 入力を通じて共有されます。



- m) アプリケーションにロールを割り当てるには、追加の手順が必要です。「その他のサービス」、「サブスクリプション」に戻ります。



- n) アクティブなサブスクリプションを選択し、アクセス制御 (**AIM**) を選択し、次に [追加] をクリックします。



- o) [アクセス許可の追加] ペインで、[所有者の ロール] を選択し、**Azure AD** ユーザー、グループ、またはアプリケーションへのアクセス権を割り当て、[選択] フィールド で登録済みアプリを検索して、Zero Touch Deployment Cloud Service が Azure でインスタンスを作成および構成できるようにします。サブスクリプション。アプリを特定したら、[保存] をクリックする前に、アプリを選択し、[選択済み] メンバーとして入力されていることを確認します。

Add permissions [X]

Role [Owner]

Assign access to [Azure AD user, group, or application]

Select [ztd] ✓

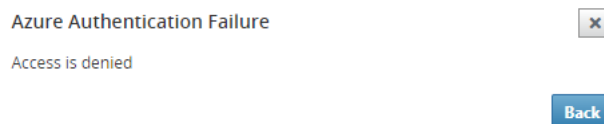
mbx_ztduser
mbx_ztduser@citrite.net

Selected members:

ztd [Remove]

[Save] [Discard]

- p) 必要な入力を収集し、SD-WAN Center に入力したら、[**Next**] をクリックします。入力が正しくない場合は、認証に失敗します。



SD-WAN Center の Azure のプロビジョニングとデプロイ (ステップ 2/2)

1. Azure 認証が成功したら、適切なフィールドに入力して目的の Azure リージョンと適切なインスタンスサイズを選択し、[デプロイ] をクリックします。

Provision and Deploy Azure (step 2 of 2)

Azure Region
West US ▼

Azure Instance Size
Standard_D4_v2 ▼

WAN subnet address prefix:
10.9.4.0/24

LAN subnet address prefix:
10.9.3.0/24

Management subnet prefix:
10.9.0.0/24

Back Deploy

2. SD-WAN Center の [アクティブ化を保留中] タブに移動すると、展開の現在のステータスを追跡できます。

Citrix SD-WAN Center R9_3_1_35_624646 admin

Dashboard Fault Monitoring Configuration Reporting Administration

Configuration / Zero Touch Deployment / Pending Activation

Prepare New Site Activation History **Pending Activation**

Showing 1 - 1 of 1

Site Name	Serial No	Installer Email	Address	Status	Action
ztdazure	B0F20EC1-9DEE-4902-B072-D593536C6C02	ztdinstaller@outlook.com	AZURE - West US 2	Provisioning	

Delete Modify

3. 手順 1 で入力したメールアドレスにアクティベーションコードが記載された電子メールが配信され、電子メールを入手して アクティベーション URL を開いてプロセスをトリガーし、アクティベーションステータスを確認します。

Focused Other Filter

NetScaler SD-WAN Team
NetScaler SD-WAN Cloud Service As 3:44 PM
NetScaler SD-WAN Appliance Activation Info...

NetScaler SD-WAN Cloud Service Activation Link @uswestazure

NT NetScaler SD-WAN Team <sdwanservice@citrix.com>
Today, 3:44 PM
You

NetScaler SD-WAN Appliance Activation Information

To check the activation status, [click here](#)
(Or copy and paste this link into your Browser's address bar
https://sdwanzt.citrixnetworkapi.net/root/sdwanzt/v1/appliance/activate?
activationcode=4f19b443-7e89-4b69-9872-07ebee8ac2).

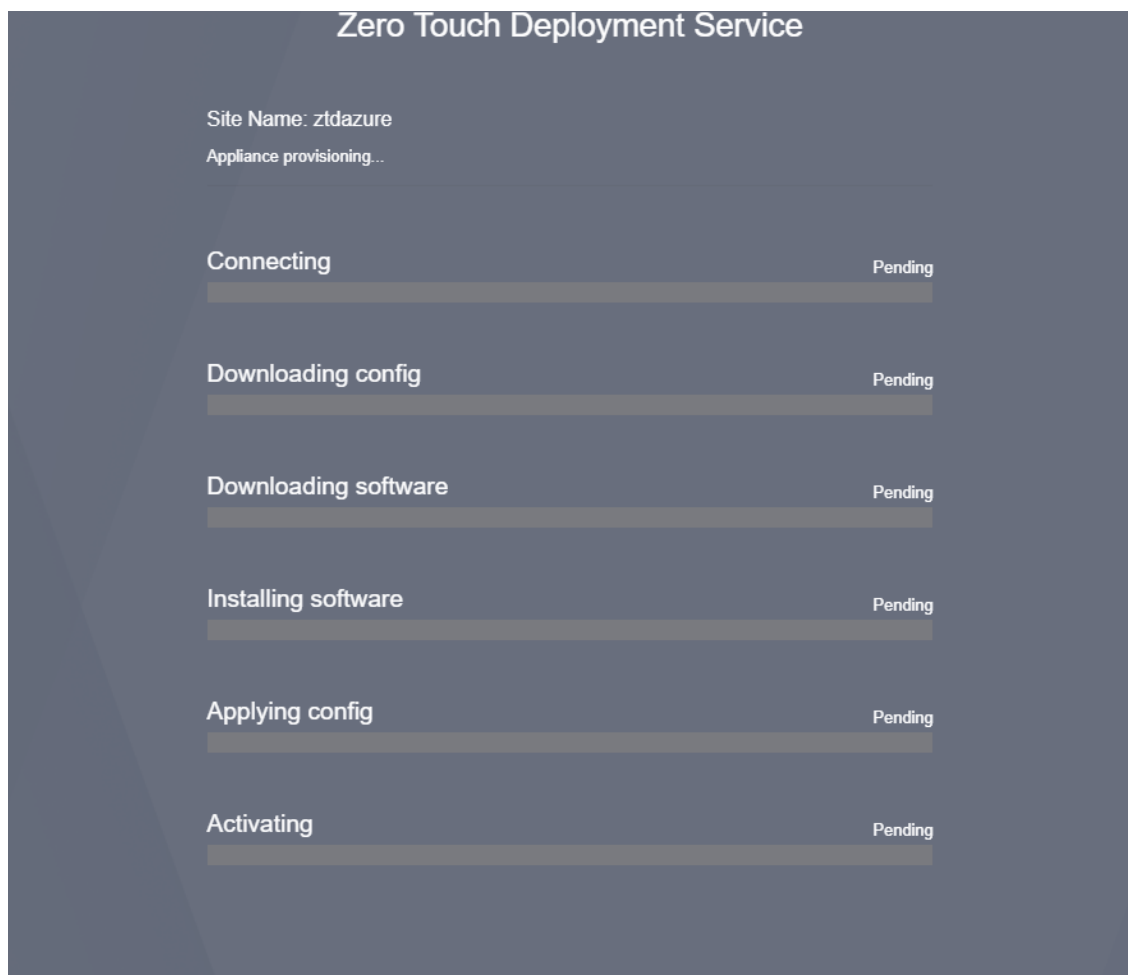
Site Name uswestazure
Address AZURE - West US

Additional Notes

The NetScaler SD-WAN Team

*** This is an automatically generated email, please do not reply ***

4. 手順 1 で入力したメールアドレスにアクティベーション URL が記載されたメールが届きます。電子メールを入手し、アクティベーション **URL** を開いてプロセスをトリガーし、アクティベーションステータスを確認します。



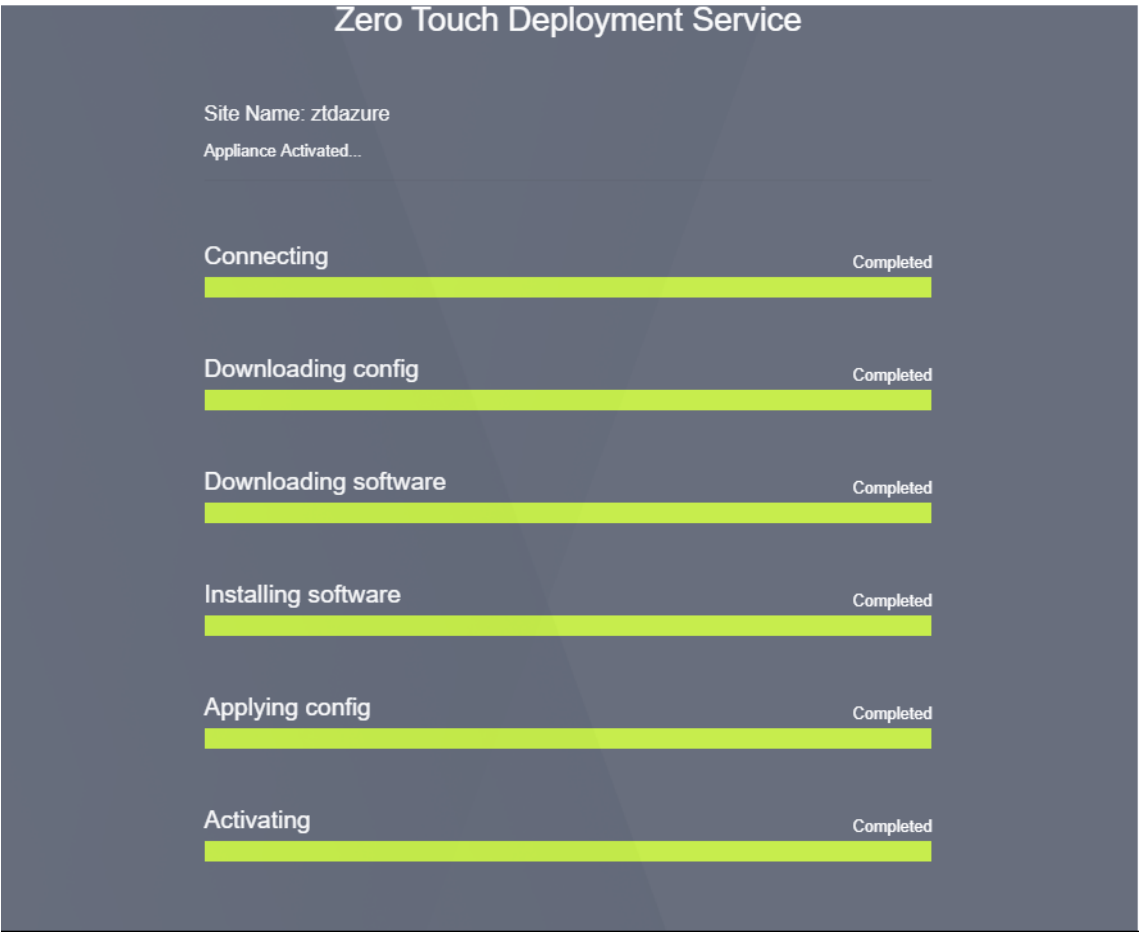
5. SD-WAN クラウドサービスによってインスタンスがプロビジョニングされるまで数分かかります。自動的に作成される リソースグループのアクティビティログ の下で、Azure Portal でアクティビティを監視できます。Provisioning に関する問題やエラーはすべてここに入力され、アクティブ化ステータスで SD-WAN センターにレプリケートされます。

OPERATION NAME	STATUS	TIME	TIME STAMP	SUBSCRIPTION	EVENT INITIATED BY
Purchase	Succeeded	Just now	Fri Oct 13 20...	Pay-As-You-Go	ztd
Write Deployments	Succeeded	5 min ago	Fri Oct 13 20...	Pay-As-You-Go	
Write NetworkSecurity	Succeeded	5 min ago	Fri Oct 13 20...	Pay-As-You-Go	
Write VirtualNetworks	Accepted	5 min ago	Fri Oct 13 20...	Pay-As-You-Go	
Write PublicIPaddress	Succeeded	5 min ago	Fri Oct 13 20...	Pay-As-You-Go	
Write NetworkInterface	Succeeded	4 min ago	Fri Oct 13 20...	Pay-As-You-Go	
Write StorageAccount	Succeeded	5 min ago	Fri Oct 13 20...	Pay-As-You-Go	
Write VirtualMachines	Succeeded	Just now	Fri Oct 13 20...	Pay-As-You-Go	
Validate	Started	6 min ago	Fri Oct 13 20...	Pay-As-You-Go	ztd
Update resource group	Started	6 min ago	Fri Oct 13 20...	Pay-As-You-Go	ztd

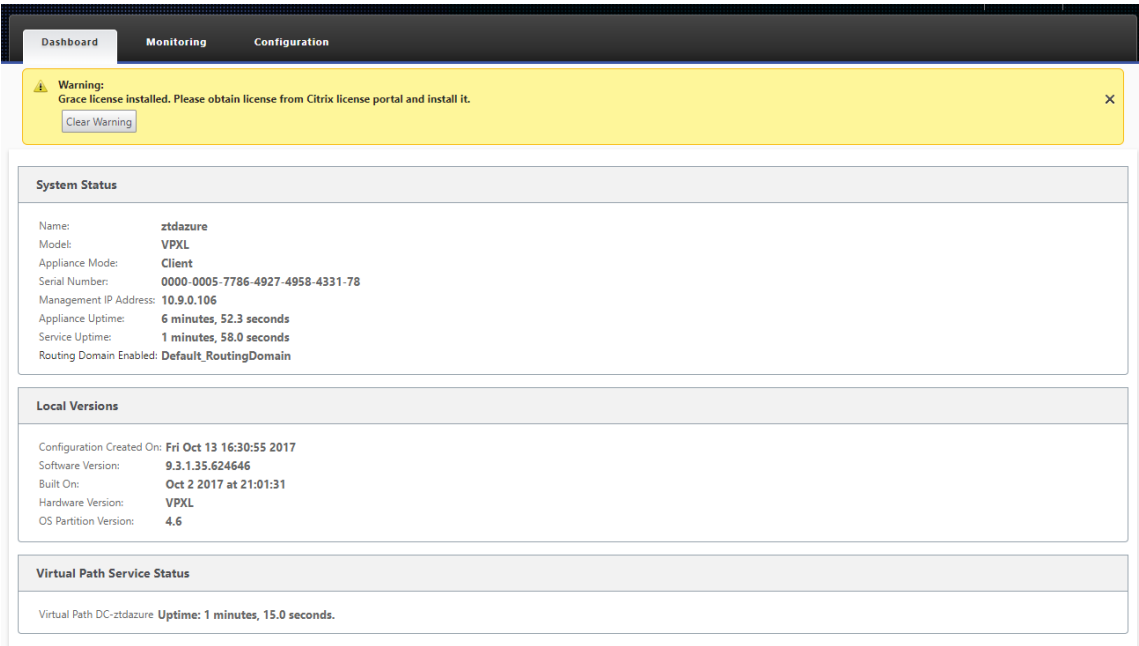
6. Azure Portal では、正常に起動されたインスタンスは [仮想マシン] の下で使用できます。割り当てられたパブリック IP を取得するには、インスタンスの [概要] に移動します。

Public IP address: 52.247.213.21

7. VM が実行状態になった後、サービスが到達し、構成、ソフトウェア、およびライセンスのダウンロードプロセスを開始するまでに 1 分かかります。



8. SD-WAN クラウドサービスの各手順が自動的に複雑になった後、Azure ポータルから取得したパブリック IP を使用して SD-WAN インスタンスの Web インターフェイスにログインします。



9. [Citrix SD-WAN 監視統計情報] ページでは、MCN から Azure の SD-WAN インスタンスへの正常な接続が識別されます。

Warning:
Grace license installed. Please obtain license from Citrix license portal and install it.
[Clear Warning](#)

Monitoring > Statistics

Statistics
Show: **Paths (Summary)** ☐ Enable Auto Refresh 5 seconds [Refresh](#) ☒ Show latest data.

Path Statistics Summary

Filter: in **Any column** [Apply](#) Show 100 entries

Num	From Link	To Link	Path State	Virtual Path Service State	Virtual Path Service Type	BOWT	Jitter (mS)	Loss %	kbps	Congestion
1	Azure-INET	DC-INET	GOOD	GOOD	Static	2	2	0.00	10.83	NO
2	DC-INET	Azure-INET	GOOD	GOOD	Static	2	2	0.00	17.60	NO

Showing 1 to 2 of 2 entries
Bandwidth calculated over the last 0.051 seconds

10. さらに、Provisioning の成功（または失敗）は、SD-WAN Center の [アクティベーション履歴] ページに記録されます。

Citrix SD-WAN Center R9_3_1_35_624646 admin

Dashboard Fault Monitoring **Configuration** Reporting Administration

Configuration / Zero Touch Deployment / Activation History

Prepare New Site **Activation History** Pending Activation

Showing 1 - 1 of 1 Search

Site Name	Serial No	Installer Email	Address	Status Details	Activation Date	Status	Action
ztdazure	C736A440-0A37-4676-AF5D-CCDB74220783	ztdinstaller@outlook.com	AZURE - West US	Appliance Activated	Oct 14 15:10:13 2017 UTC	Activated	[icon]

単一リージョンの展開

May 10, 2021

リージョンを使用すると、分散管理を使用してネットワーク階層を定義できます。リージョンは、そのリージョンのネットワーク制御ノード（MCN）によって実行される機能を引き継ぐリージョナル制御ノード（RCN）を定義する必要があります。MCN は、デフォルトリージョンの Controller です。

静的仮想パスと動的仮想パスは、リージョン間で許可されません。RCN は、リージョン間のトラフィックを管理します。

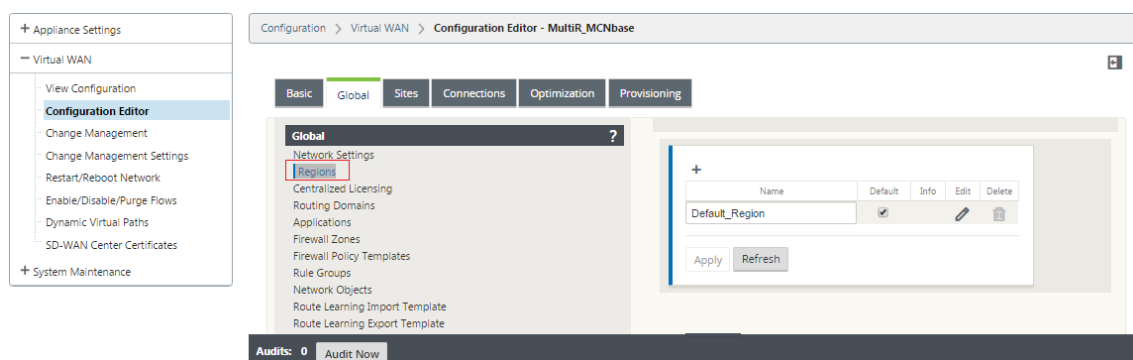
SD-WAN ネットワークでの単一リージョン展開では、550 未満のネットワークサイトをサポートできます。

SD-WAN アプライアンスの GUI の構成エディタでデフォルトの領域を構成できます。基本エディタは、MCN ノードとクライアント SD-WAN ノードを持つ小規模なネットワークだけを作成するのに便利です。MCN、RCN、クライアント、または高度な機能を使用してマルチリージョンネットワークを構成するには、構成エディタで他の構成オプションを使用します。

単一リージョン展開を構成するには、次の手順に従います。

1. 構成エディタの「グローバル」タブに移動します。[リージョン]を選択します。デフォルトのリージョン設定オプションが表示されます。

デフォルトのリージョンの名前と説明は、編集することで変更できます。



2. **Default_Region** を編集して、名前を変更し、サブネットを設定します。
3. [強制内部 **VIP** マッチング] または [外部 **VIP** マッチングを許可] のどちらを使用するかに基づいて、インターバル **VIP** マッチングを有効にします。
 - 強制内部 VIP: 有効にすると、リージョン内のすべての非プライベート仮想 IP アドレスが、設定されたサブネットと一致するように強制されます。
 - 許可された外部 VIP-有効にすると、他のリージョンからの非プライベート仮想 IP アドレスが、設定されたサブネットと一致することを許可されます。
4. サブネットを追加するには、[+] をクリックします。

Edit

Name:

Default_Region

Description:

☐ Force Internal VIP Matching☐ Allow External VIP Matching

Subnets +

Routing Domain	Network	Delete
Default_RoutingDomain ▾	*	

Apply

Cancel

5. ルーティングドメインを選択し、ネットワーク アドレスを入力します。[適用] をクリックします。ネットワークアドレスは、サブネットの IP アドレスとマスクです。

マルチリージョンの展開

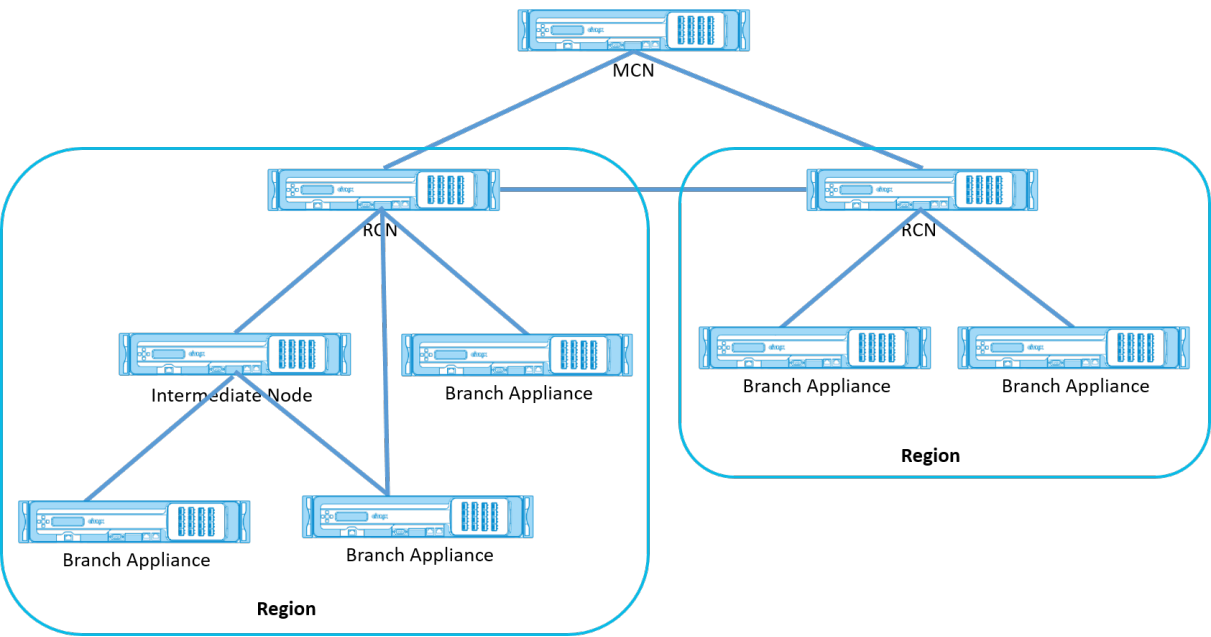
November 8, 2021

マスターコントロールノード (MCN) として構成された SD-WAN アプライアンスは、マルチリージョンの展開をサポートします。MCN は、複数の地域制御ノード (RCN) を管理します。各 RCN は、複数のクライアントサイトを管理します。MCN を使用して、一部のクライアントサイトを直接管理することもできます。

MCN をネットワークの制御ノードとし、RCN をリージョンの制御ノードとして使用すると、SD-WAN は最大 6000 のサイトを管理できます。

マルチリージョン展開では、ネットワークをリージョンにフラグメント化し、ブランチ (クライアント) > RCN > MCN などの階層型ネットワークを設定できます。

1 つのリージョンの MCN は、最大 1000 のサイトで構成できます。既存のサイトを既定のリージョンに保持し、RCN とそのサイトを持つ新しいリージョンを複数リージョン展開に追加できます。



次の表に、プライマリおよびセカンダリ MCN/RCN の設定でサポートされているプラットフォームの一覧を示します。

メモ

- Premium Edition (PE) アプライアンスは、以前は Enterprise Edition (EE) と呼ばれていました。
- Citrix SD-WAN 210 SE アプライアンスは、SD-WAN Orchestrator が管理するネットワークでのみ MCN として使用します。

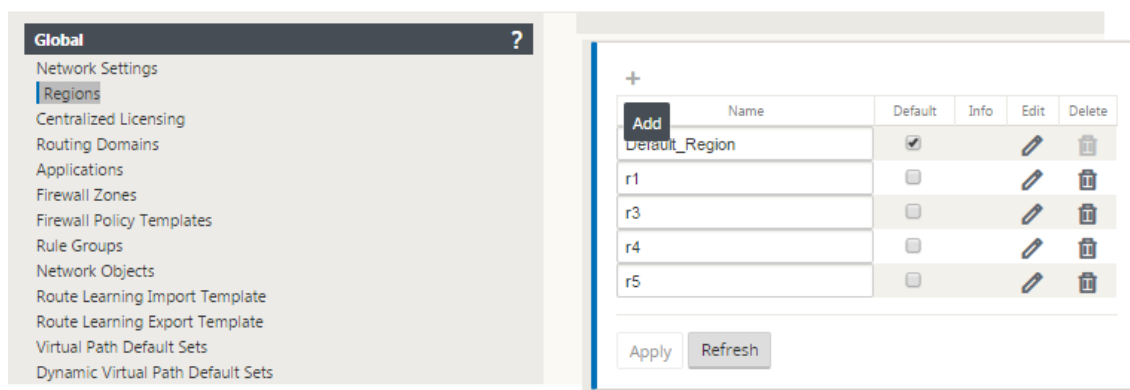
プラットフォーム・Edition	プライマリ/セカンダリ MCN	プライマリ/セカンダリ RCN
110-SE	いいえ	いいえ
210-SE	はい	はい
400-SE	はい	いいえ
410-SE	はい	いいえ
1000-SE, 1000-PE	はい	いいえ
1100-SE, 1100-PE	はい	はい
VPX-SE、VPXL-SE	はい	はい
2000-SE, 2100-SE, 2000-PE, 2100-PE, 4000-SE, 4100-SE, 5100-SE, 5100-PE, 6100-SE	はい	はい

SD-WAN ネットワークのマルチリージョン展開を設定するには、次の手順を実行します。

1. 構成エディタの「グローバル」タブに移動します。リージョン]を選択します。デフォルトのリージョン設定オプションが表示されます。

デフォルトのリージョンの名前と説明は、編集することで変更できます。

2. [+ 追加] をクリックして、新しいリージョンを追加します。



Add

Name:

Description:

☐ Force Internal VIP Matching

☐ Allow External VIP Matching

Subnets +

Add

Cancel

3. リージョンの「名称」および「摘要」を入力します。
4. [強制内部 **VIP** マッチング] または [外部 **VIP** マッチングを許可] のどちらを使用するかに基づいて、内部 **VIP** マッチングを有効にします。
 - 強制内部 **VIP**: 有効にすると、リージョン内のすべての非プライベート仮想 IP アドレスが、設定されたサブネットと一致するように強制されます。
 - 許可された外部 **VIP**-有効にすると、他のリージョンからの非プライベート仮想 IP アドレスが、設定されたサブネットと一致することを許可されます。
5. サブネットを追加するには、[+] をクリックします。ルーティングドメインを選択します。

Subnets +

Routing Domain	Network	Delete
<Default>		

<Default>
Default_RoutingDomain
WCCP_RoutingDomain

Add Cancel

6. ネットワーク アドレスを入力します。[追加] をクリックします。ネットワークアドレスは、サブネットの IP アドレスとマスクです。新しく作成されたリージョンが、既存のリージョンのリストに追加されます。

「デフォルト」 (**Default**) チェックボックスを選択すると、目的の領域をデフォルトとして使用できます。

+

Name	Default	Info	Edit	Dele
Default_Region	<input checked="" type="checkbox"/>			

Apply Refresh

If enabled, the Region will be used as the default Region for the network

注

MCN を GEO サイトまたはクライアントサイトにクローンすることができます。

SD-WAN Center では、マルチリージョンの展開がサポートされています。詳細については、[SD-WAN Center マルチリージョンの展開とレポート](#)を参照してください。

変更管理の概要ビュー

マルチリージョン展開で構成されたアプライアンスの変更管理プロセスを実行すると、SD-WAN アプライアンスの GUI に変更管理の概要テーブルが表示されます。

[リージョン] 列には、ネットワークで現在設定されているリージョンのリストが表示されます。特定のリージョンの変更管理サマリーは、サマリーテーブルで選択することで表示できます。

デフォルトのリージョンの概要:

Global Multi-Region Summary

Search

Region	Total Sites	Not Connected	Preparing/Staging	Staged	Failed
Default_Region	5	1	0	4	0
AMEA_r1	32	0	0	32	0
APAC_r1	2	0	0	2	0
AMER-1	Data not available				

Region - Default_Region Details

Show25entries

Search

CustomizeRefresh

Site-Appliance	Model	State	Currently Active		Currently Staged		Traffic Interruption		Download Package
			Software	Config	Software	Config	Expected	Actual	
MCN1-MCN1-CB4100	CB4100	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 min		active / staged
APAC_RCN-APAC_RCN-CB1000	CB1000	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec		active / staged
BR1-BR1-CBVPXL	CBVPXL	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec		active / staged
RCN01-2000-RCN01-2000	CB2000	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec		active / staged
AMER-1RCN-5100-AMER-1RCN-5100	CB5100	Not Needed	Not Connected				Loc Chg Mgt		none / staged

Previous1Next

リージョンの要約:

Global Multi-Region Summary

Search

Region	Total Sites	Not Connected	Preparing/Staging	Staged	Failed
Default_Region	5	1	0	4	0
AMEA_r1	32	0	0	32	0
APAC_r1	2	0	0	2	0
AMER-1	Data not available				

Region - AMEA_r1 Details

Show25entries

Search

CustomizeRefresh

Site-Appliance	Model	State	Currently Active		Currently Staged		Traffic Interruption		Download Package
			Software	Config	Software	Config	Expected	Actual	
AMEA_r1_vpx01-AMEA_r1_vpx01	CBVPX	Done	10.1.0.14.661523	15:54 on 2/28/18	10.1.0.14.661523	16:11 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx02-AMEA_r1_vpx02	CBVPX	Done	10.1.0.14.661523	15:54 on 2/28/18	10.1.0.14.661523	16:11 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx03-AMEA_r1_vpx03	CBVPX	Done	10.1.0.14.661523	15:54 on 2/28/18	10.1.0.14.661523	16:11 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx04-AMEA_r1_vpx04	CBVPX	Done	10.1.0.14.661523	15:54 on 2/28/18	10.1.0.14.661523	16:11 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx05-AMEA_r1_vpx05	CBVPX	Done	10.1.0.14.661523	15:54 on 2/28/18	10.1.0.14.661523	16:11 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx06-AMEA_r1_vpx06	CBVPX	Done	10.1.0.14.661523	15:54 on 2/28/18	10.1.0.14.661523	16:11 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx07-AMEA_r1_vpx07	CBVPX	Done	10.1.0.14.661523	15:54 on 2/28/18	10.1.0.14.661523	16:11 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx08-AMEA_r1_vpx08	CBVPX	Done	10.1.0.14.661523	15:54 on 2/28/18	10.1.0.14.661523	16:11 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx13-AMEA_r1_vpx13	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx14-AMEA_r1_vpx14	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx15-AMEA_r1_vpx15	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx16-AMEA_r1_vpx16	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx17-AMEA_r1_vpx17	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx18-AMEA_r1_vpx18	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx19-AMEA_r1_vpx19	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx20-AMEA_r1_vpx20	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx33-AMEA_r1_vpx20	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx34-AMEA_r1_vpx20	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx35-vpx35	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx36-vpx36	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx37-vpx37	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx38-vpx38	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx39-vpx39	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx40-vpx40	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx49-vpx49	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged

Previous12Next

注

場合によっては、[グローバルマルチリージョンの概要] テーブルに表示される [サイトの合計] の値が、残りの列の合計より小さくなることがあります。

たとえば、分岐ノードが接続されていない場合、分岐が 2 回カウントされます。1 回は「未接続」として、1 回は「準備/ステー징」>としてカウントされます。

Citrix Virtual Apps and Desktops のワークロードの構成ガイド

May 10, 2021

Citrix SD-WAN は、SaaS、クラウド、仮想アプリケーション向けに柔軟で自動化されたセキュアな接続性とパフォーマンスにより、デジタル変革を加速する次世代の WAN Edge ソリューションであり、常時稼働の Workspace 環境を実現します。

Citrix SD-WAN は、Citrix Virtual Apps and Desktops Service を使用している組織がクラウド内の Citrix Virtual Apps and Desktops のワークロードに接続するために推奨される最適な方法です。詳しくは、「[Citrix ブログ](#)」を参照してください。

このドキュメントでは、Azure 上の Citrix Virtual Apps and Desktops ワークロードとの接続用に Citrix SD-WAN を構成する方法について説明します。

長所

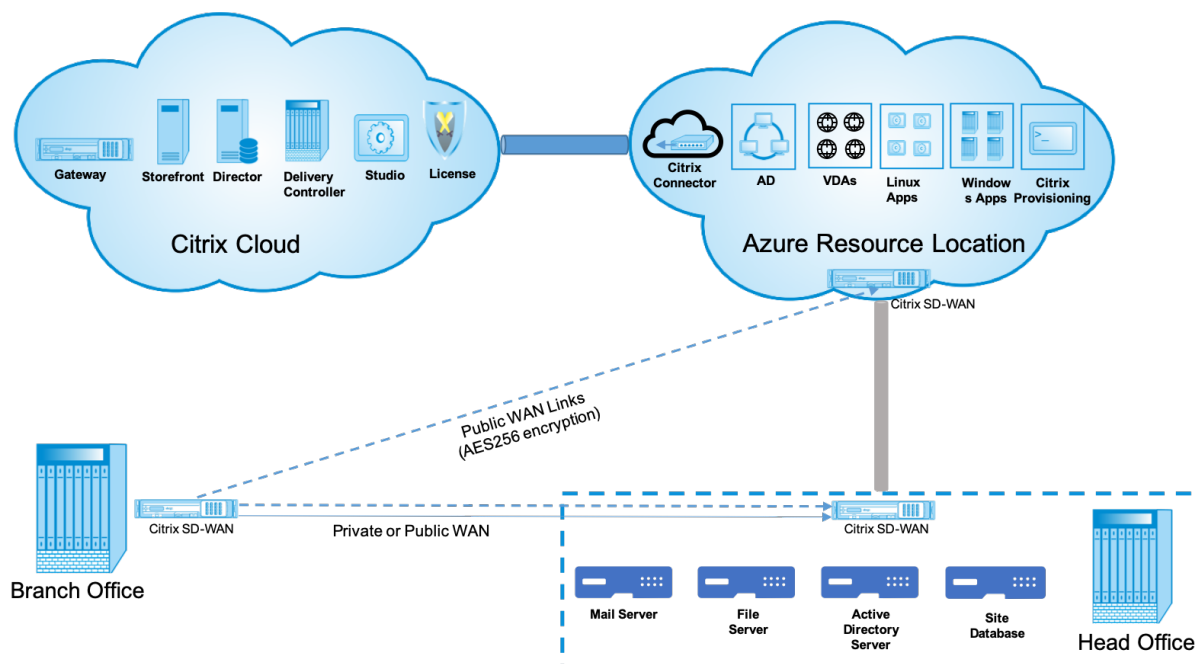
- ガイド付きワークフローにより、Citrix Virtual Apps and Desktops で SD-WAN を簡単にセットアップ
- 高度な SD-WAN テクノロジーにより、常時オンで高性能な接続を実現
- すべての接続 (VDA から DC、ユーザーから VDA、VDA からクラウド、ユーザーからクラウド) にわたるメリット
- データセンターへのトラフィックのバックホールに比べてレイテンシを低減
- QoS (サービス品質) を確保するためのトラフィック管理
 - HDX/ICA トラフィックストリーム間の QoS (シングルポートマルチストリーム HDX 自動 QoS)
 - HDX と他のトラフィック間の QoS
 - ユーザー間の HDX QoS 公平性
 - エンドツーエンド QoS
- リンク・ボンディングにより、より高速なパフォーマンスを実現する帯域幅を提供
- Azure でのシームレスなリンクフェールオーバーと SD-WAN 冗長性による高可用性
- 最適化された VoIP エクスペリエンス (ジッタを削減し、パケット損失を最小限に抑えるためのパケットレーズ、QoS、ローカルブレイクアウトによるレイテンシ低減)
- Azure ExpressRoute に比べて、コストを大幅に削減し、デプロイが迅速で容易であることが必要

前提条件

Citrix Virtual Apps and Desktops のワークロード機能を評価および展開するには、次の前提条件に従ってください。

- 既存の SD-WAN ネットワークがあるか、新しいネットワークを構築する必要があります。
- Citrix Virtual Apps and Desktops サービスへのサブスクリプションが必要です。
- マルチストリームの HDX AutoQoS や詳細な可視性などの SD-WAN 機能を使用するには、ネットワーク内のすべての SD-WAN サイトに対してネットワークロケーションサービス (NLS) を構成する必要があります。
- クライアントエンドポイントが存在する場所 (多くの場合、データセンター環境に共存する) に DNS サーバーと AD を展開する必要があります。または、Azure Active Directory (AAD) を利用することもできます。
- DNS サーバーは、内部 (プライベート) と外部 (パブリック) IP の両方を解決できる必要があります。
- ファイアウォール内の許可リストに FQDN (sdwan-location.citrixnetworkapi.net) が追加されていることを確認します。これは、SD-WAN 仮想パスを介してトラフィックを送信する際に重要な、ネットワークロケーションサービスの FQDN です。また、ワイルドカード FQDN のホワイトリスト登録に慣れている場合は、*.citrixnetworkapi.net を許可リストに追加することをお勧めします。これは、ゼロタッチプロビジョニングなどの他の Citrix Cloud サービスのサブドメインであるため、*.citrixnetworkapi.net を許可リストに追加します。
- SD-WAN オーケストレーターを使用して SD-WAN ネットワークを管理するには、sdwan.cloud.com に登録します。SD-WAN Orchestrator は、Citrix SD-WAN 用の Citrix Cloud ベースのマルチテナント管理プラットフォームです。

展開アーキテクチャ



デプロイメントには、次のエンティティが必要です。

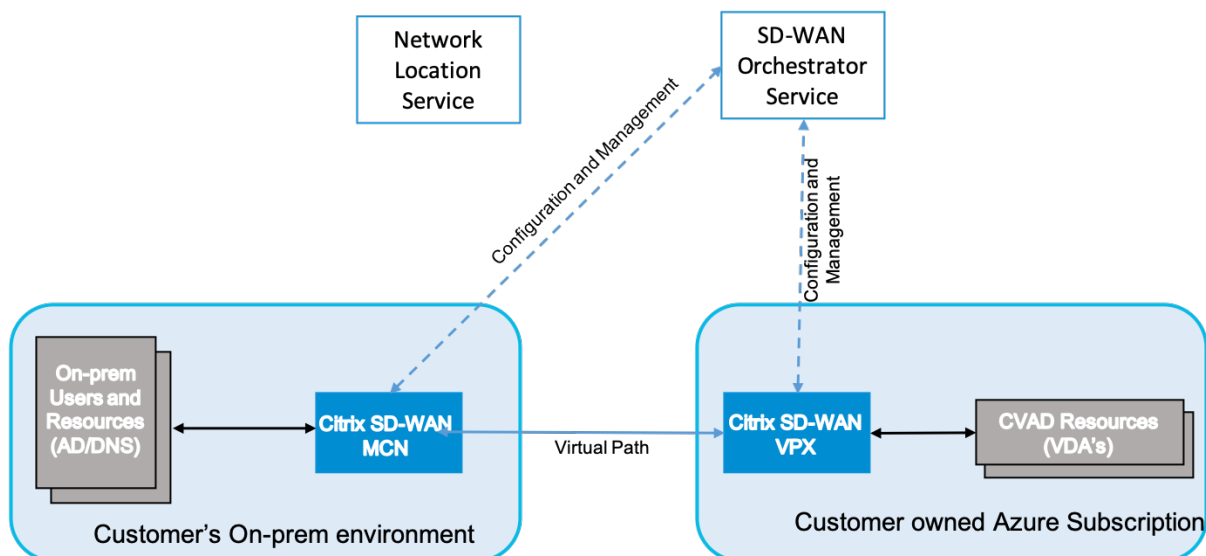
- SD-WAN アプライアンスをホストするオンプレミスの場所。ブランチモードまたは **MCN** (マスターコントロールノード) として展開できます。ブランチモードまたは MCN には、クライアントマシン、アクティブディレクトリ、および DNS が含まれます。ただし、Azure の DNS と AD を使用することもできます。ほとんどのシナリオでは、オンプレミスの場所はデータセンターとして機能し、MCN を収容します。

- **Citrix Virtual Apps and Desktops** クラウドサービス—Citrix Virtual Apps と Desktops は、IT 部門が仮想マシン、アプリケーション、およびセキュリティを制御できる仮想化ソリューションを提供し、どのデバイスにもどこからでもアクセスできます。エンドユーザーは、デバイスのオペレーティングシステムやインターフェイスとは無関係に、アプリケーションとデスクトップを使用できます。

Citrix Virtual Apps and Desktops サービスを使用すると、セキュアな仮想アプリとデスクトップを任意のデバイスに配信できます。また、製品のインストール、セットアップ、構成、アップグレード、監視のほとんどを Citrix に任せます。どのデバイスに対しても最高のユーザーエクスペリエンスを提供しながら、アプリケーション、ポリシー、ユーザーを完全に制御できます。

- **Citrix** コネクタ/クラウドコネクタ -Citrix Cloud Connector を介してリソースをサービスに接続します。このコネクタは、Citrix Cloud とリソースの場所間の通信チャネルとして機能します。Cloud Connector によって、VPN や IPsec トンネルなどの複雑なネットワークやインフラストラクチャを構成せずにクラウドを管理できます。リソースの場所には、アプリケーションとデスクトップを利用者に配信するためのマシンやその他のリソースが含まれています。
- **SD-WAN Orchestrator** —Citrix SD-WAN Orchestrator は、クラウドでホストされるマルチテナント管理サービスです。Citrix パートナーは、SD-WAN Orchestrator を使用して、単一の画面と適切なロールベースのアクセス制御で複数の顧客を管理できます。
- 仮想および物理 **SD-WAN** アプライアンス—これは、クラウド (VM) 内およびデータセンターおよびブランチ (物理アプライアンスまたは VM) 内のオンプレミスの複数のインスタンスとして実行され、これらの場所間およびパブリックインターネットとの接続を提供します。Citrix Virtual Apps and Desktops の SD-WAN インスタンスは、Azure Marketplace 経由でこれらのインスタンスをプロビジョニングすることにより、単一または仮想アプライアンスのセット (高可用性展開の場合) として作成されます。他の場所 (DC および支店) の SD-WAN アプライアンスは、お客様によって作成されます。これらのすべての SD-WAN アプライアンスは、SD-WAN Orchestrator を介して SD-WAN 管理者によって (構成およびソフトウェアのアップグレードの観点から) 管理されます。

展開と構成



一般的な展開では、Citrix SD-WAN アプライアンス（ハードウェアまたは VPX）を DC/大規模オフィスに MCN として展開します。通常、お客様の DC はオンプレミスのユーザーとリソース（AD や DNS サーバーなど）をホストします。一部のシナリオでは、Azure Active Directory サービス（AADS）と DNS を使用できます。これらのサービスは、Citrix SD-WAN および CMD 統合でサポートされています。

お客様が管理する Azure サブスクリプション内で、お客様は Citrix SD-WAN 仮想アプライアンスと VDA を展開する必要があります。SD-WAN アプライアンスは、SD-WAN Orchestrator を介して管理されます。SD-WAN アプライアンスが構成されると、既存の Citrix SD-WAN ネットワークに接続され、構成、可視性、管理などのタスクは SD-WAN Orchestrator を介して処理されます。

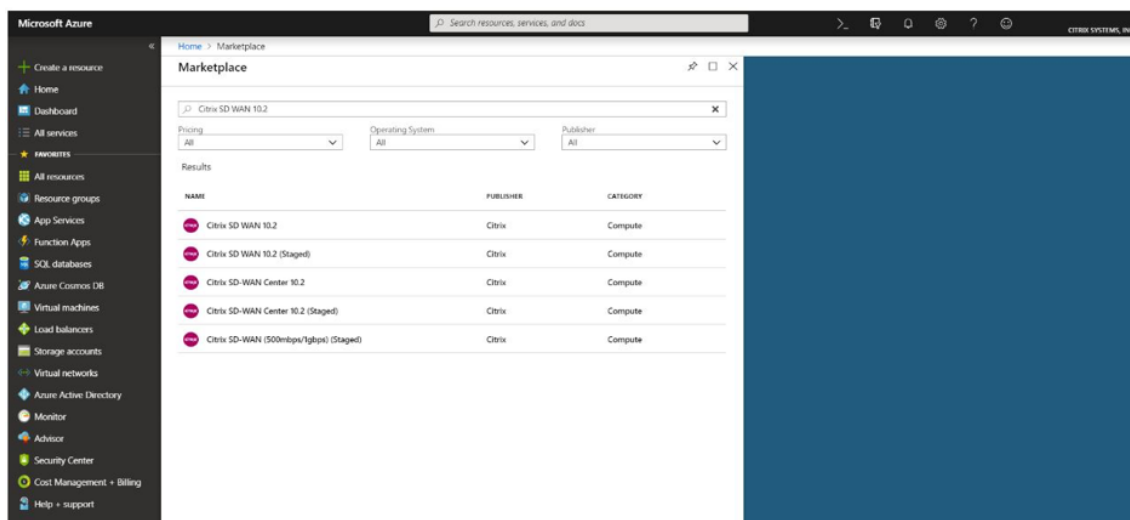
この統合の第 3 のコンポーネントは、内部ユーザーが Gateway をバイパスして VDA に直接接続できるようにするネットワークロケーションサービス（NLS）です。これにより、内部ネットワークトラフィックの待ち時間が短縮されます。NLS は、手動または Citrix SD-WAN Orchestrator を使用して構成できます。詳しくは、「[NLS](#)」を参照してください。

構成

Citrix SD-WAN VM は、（お客様の必要に応じて）指定されたリージョン内に展開され、MPLS、インターネット、または 4G/LTE を介して複数のブランチオフィスの場所に接続できます。仮想ネットワーク（VNET）インフラストラクチャ内で、SD-WAN Standard Edition (SE) VM は Gateway モードでデプロイされます。VNET には Azure Gateway へのルートがあります。SD-WAN インスタンスには、インターネット接続用の Azure Gateway へのルートがあります。このルートは手動で作成する必要があります。

1. Web ブラウザーで、[Azure ポータル](#)に移動します。Microsoft Azure アカウントにログインし、Citrix SD-WAN Standard Edition を検索します。

2. 検索結果で、Citrix SD-WAN Standard Edition ソリューションを選択します。説明を確認し、選択したソリューションが正しいことを確認した後、[作成] をクリックします。

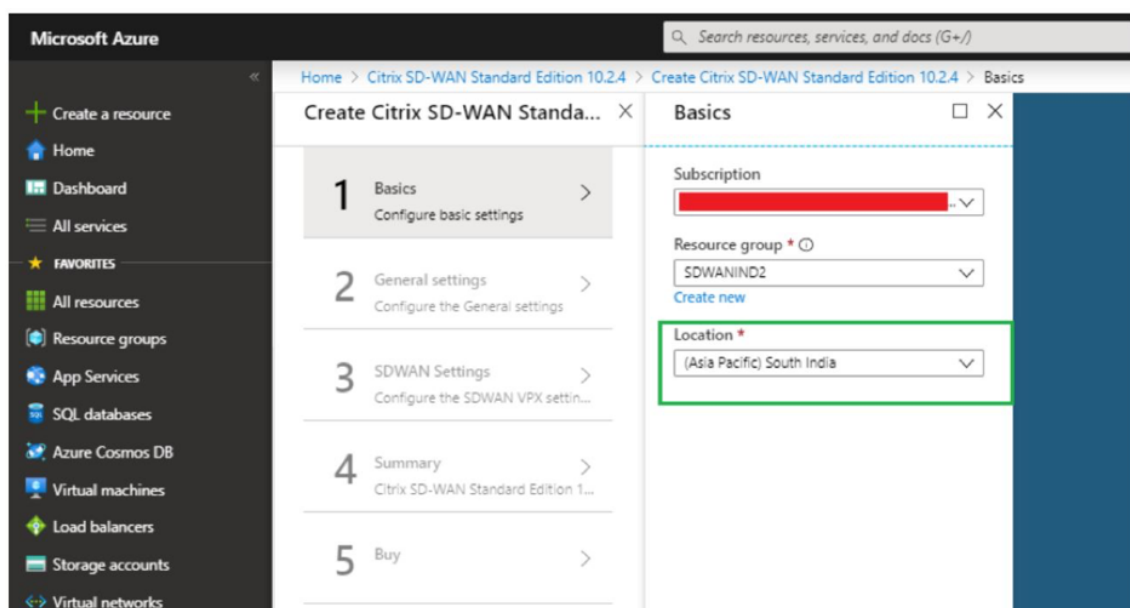


[Create] をクリックすると、仮想マシンを作成するために必要な詳細を尋ねるウィザードが表示されます。

3. [基本設定] ページで、SD-WAN SE ソリューションを展開するリソースグループを選択します。

リソースグループは、Azure ソリューションの関連リソースを保持するコンテナです。リソースグループには、ソリューションのすべてのリソースを含めることも、グループとして管理するリソースのみを含めることもできます。デプロイメントに基づいて、リソースをリソースグループに割り当てる方法を決定できます。

Citrix SD-WAN の場合は、選択するリソースグループを空にする必要があります。同様に、SD-WAN インスタンスをデプロイする Azure リージョンを選択します。リージョンは、Citrix Virtual Apps and Desktops リソースが展開されるリージョンと同じである必要があります。



4. [管理者設定] ページで、仮想マシンの名前を指定します。ユーザ名と強力なパスワードを選択します。パスワード

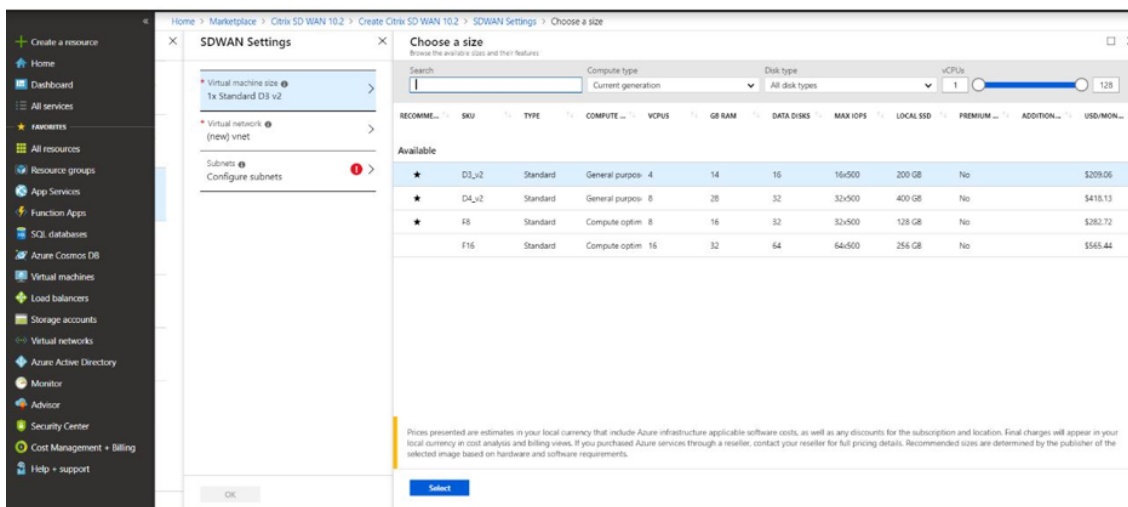
ードは大文字、特殊文字で構成され、9 文字以上である必要があります。[OK] をクリックします。

このパスワードは、インスタンスの管理インターフェイスにゲストユーザーとしてログインするために必要です。インスタンスへの管理者アクセスを取得するには、インスタンスの Provisioning 中に作成されたユーザー名およびパスワードとして admin を使用します。インスタンスの Provisioning 中に作成されたユーザー名を使用すると、読み取り専用アクセスが取得されます。また、ここで展開の種類を選択します。

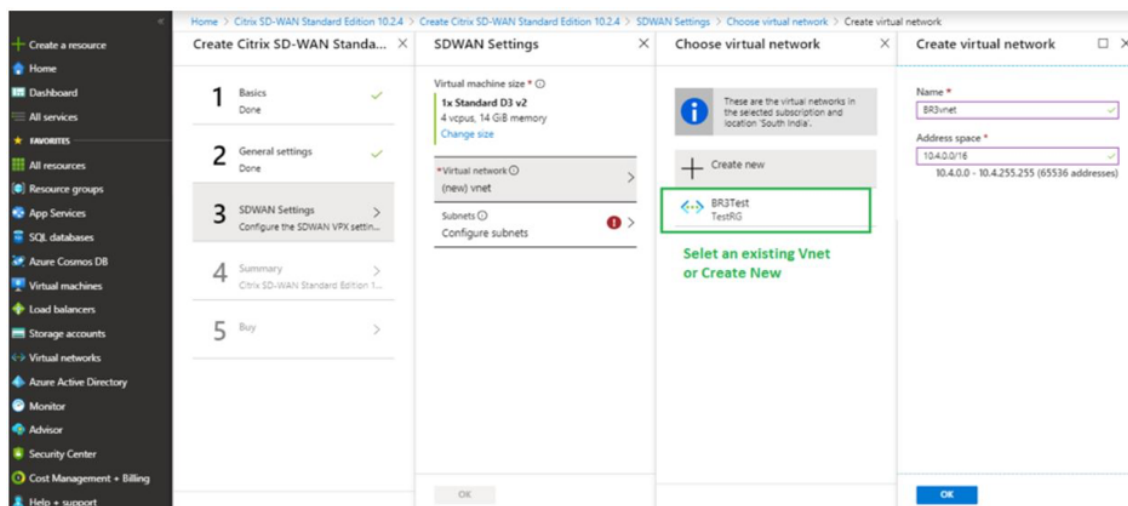
単一のインスタンスをデプロイする場合は、[HA Deployment mode] オプションから [disabled] を選択し、それ以外の場合は [enabled] を選択します。本番ネットワークの場合、インスタンスの障害からネットワークを保護するため、インスタンスを常に HA モードで展開することをお勧めします。

5. **SD-WAN** 設定 ページで、イメージを実行するインスタンスを選択します。要件に応じて、次のインスタンスタイプを選択します。

- インスタンスタイプ D3_V2。最大単一方向スループットが 200 Mbps で、最大 16 のブランチに直接接続できます。
- インスタンスタイプ D4_V2。最大単一方向スループットが 500 Mbps で、最大 16 のブランチに直接接続できます。
- インスタンスタイプ F8 標準。最大単一方向スループットが 1 Gbps で、最大 64 のブランチに直接接続できます。
- インスタンスタイプ F16 標準。最大単一方向スループットが 1 Gbps で、最大 128 のブランチに直接接続できます。



6. 新しい仮想ネットワーク (VNet) を作成するか、既存の VNet を使用します。このステップでは、SD-WAN VPX VM のインターフェイスに割り当てるサブネットを選択するため、これは展開にとって最も重要なステップです。



AUX サブネットは、HA モードでインスタンスをデプロイする場合のみ必要です。SD-WAN インスタンスが Citrix Virtual Apps and Desktops リソースと同じ VNet にデプロイされ、SD-WAN VPX アプライアンスの LAN インターフェイスと同じサブネット上にあることを確認します。

SDWAN Settings

Virtual machine size * ⓘ
1x Standard D3 v2
4 vcpus, 14 GiB memory
[Change size](#)

*Virtual network ⓘ
(new) BR3vnet

Subnets ⓘ
Configure subnets ⓘ

OK

Subnets

Manangement subnet name *
snet-mgmt ✓

Manangement subnet address prefix *
10.4.0.0/24 ✓

LAN subnet name *
snet-lan ✓

LAN subnet address prefix *
10.4.1.0/24 ✓

WAN subnet name *
snet-wan ✓

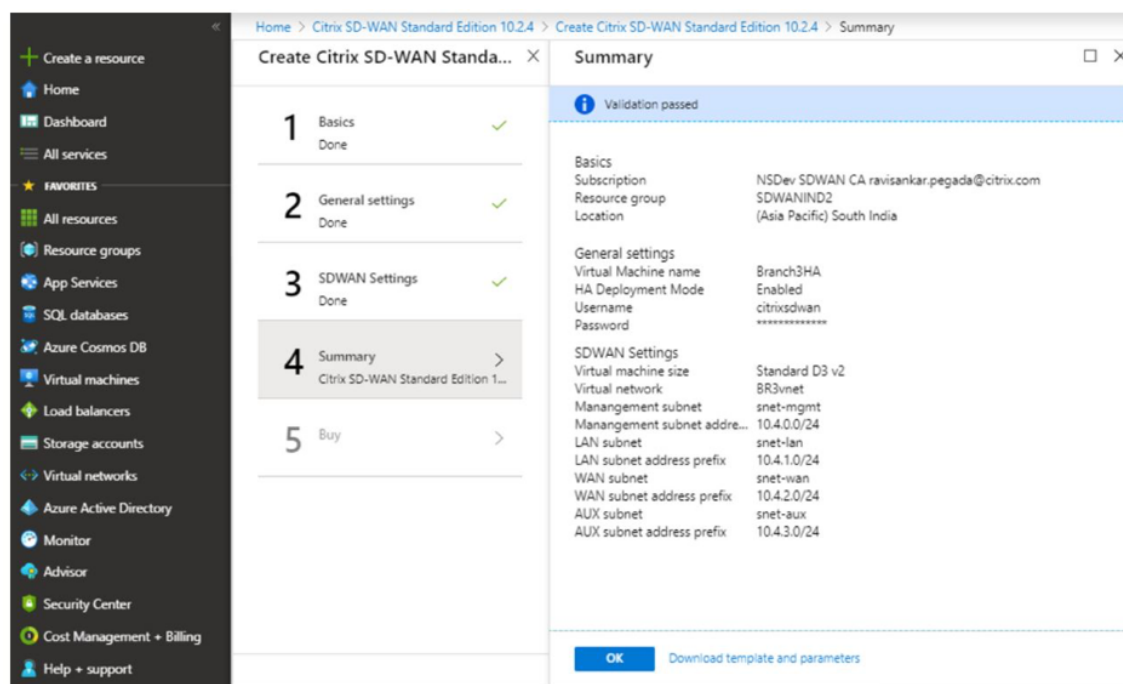
WAN subnet address prefix *
10.4.2.0/24 ✓

AUX subnet name *
snet-aux ✓

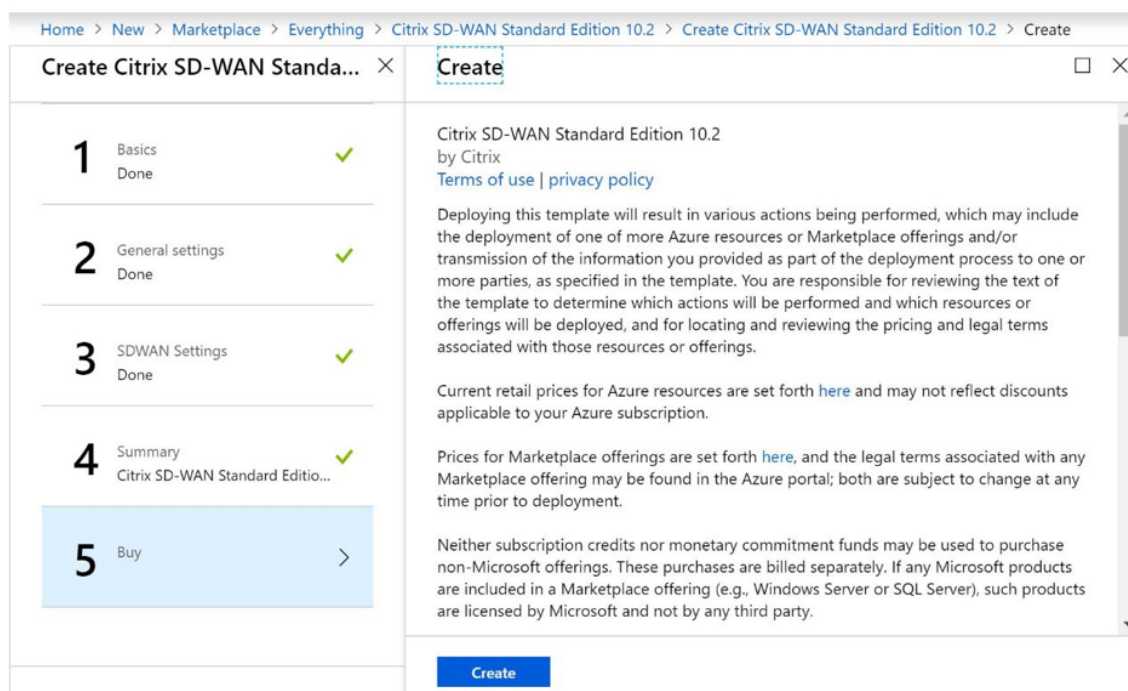
AUX subnet address prefix *
10.4.3.0/24 ✓

OK

7. [概要] ページで構成を確認し、[OK] をクリックします。



8. [**Buy**] ページで、[**Create**] をクリックして、インスタンスの Provisioning プロセスを開始します。インスタンスがプロビジョニングされるまでに約 10 分かかる場合があります。Azure 管理ポータルに、インスタンスの作成の成功/失敗を示す通知が表示されます。



インスタンスが正常に作成されたら、SD-WAN インスタンスの管理インターフェイスに割り当てられたパブリック IP を取得します。これは、インスタンスがプロビジョニングされているリソースグループの networking セクションの下にあります。取得したら、それを使用してインスタンスにログインできます。

注:

admin アクセスでは、ユーザー名は **admin** で、パスワードはインスタンスの作成時に設定したものです。

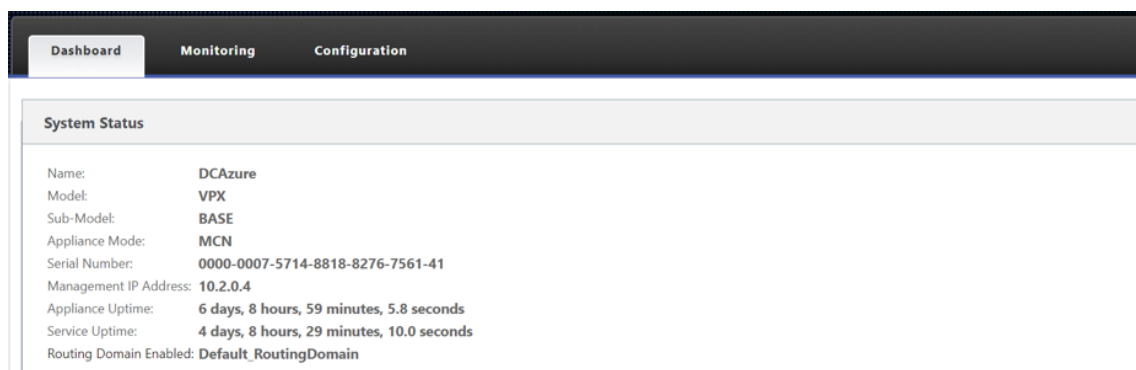
9. サイトがプロビジョニングされたら、SD-WAN Orchestrator にログインして構成します。前提条件で説明したように、サイトを構成するには SD-WAN Orchestrator のエンタイトルメントが必要です。まだ持っていない場合は、[Citrix SD-WAN Orchestrator オンボーディング](#)を参照してください。
10. SD-WAN ネットワークが既にある場合は、Azure でプロビジョニングしたサイトの構成の作成に進みます。それ以外の場合は、MCN を作成する必要があります。詳しくは、「[ネットワーク構成](#)」を参照してください。
11. SD-WAN Orchestrator にアクセスし、すでに MCN をセットアップしたら、SD-WAN Orchestrator にログインし、[**+ New**] サイト をクリックして SD-WAN VPX アプライアンス (Azure でプロビジョニングした) の設定を開始します。

12. 一意のサイト名を指定し、イメージを Provisioning するリージョンに基づいてアドレスを入力します。Azure でインスタンスをセットアップするには、[基本設定](#)を参照してください。

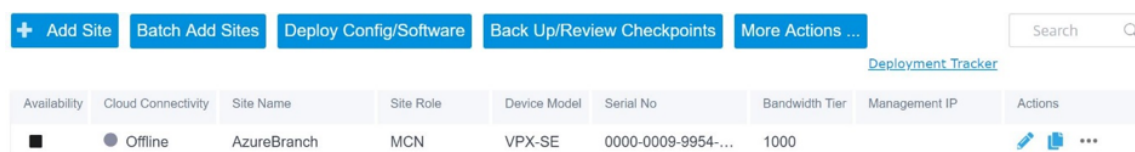
注:

Azure でインスタンスのシリアル番号を取得するには、パブリック管理 IP 経由でインスタンスにログインします。シリアル番号は、ダッシュボード画面に表示されます。HA でインスタンスを設定する場合は、両方のシリアル番号をキャプチャする必要があります。また、インスタンスの設定時に、インターフェイスが **Trusted** として選択されていることを確認します。

13. Azure 上の LAN および WAN インターフェイスに関連付けられた IP アドレスを取得します。**Azure** ポータル > リソースグループ > **SD-WAN** がプロビジョニングされているリソースグループ > **SD-WAN VM** > ネットワークに移動します。



14. 一度インスタンスの設定を完了します。[構成] > [ネットワーク構成のホーム] に移動して、[構成/ソフトウェアの展開] をクリックします。



15. 問題がなく、構成が正確である場合は、構成展開を実行した後、Azure のインスタンスと MCN の間の仮想パスを作成する必要があります。

Citrix Virtual Apps and Desktops の構成

展開と構成 セクションで強調されているように、AD/DNS は DC として機能するオンプレミスの場所に存在し、SD-WAN を備えた配置では、LAN ネットワーク上の SD-WAN の背後に表示されます。ここで設定する必要があるのは、AD/DNS の IP です。Azure Active Directory サービス/DNS を利用している場合は、DNS IP として **168.63.129.16** を構成します。

オンプレミスの AD/DNS を使用している場合。SD-WAN アプライアンスから DNS の IP に ping を実行できるかどうかを確認します。これを行うには、[トラブルシューティング] > [診断] に移動します。[**Ping**] チェックボックスをオンにして、SD-WAN アプライアンスの LAN インターフェイス/デフォルトインターフェイスから AD/DNS の IP への ping を開始します。

The screenshot displays the Citrix Cloud SD-WAN Orchestrator interface. The top navigation bar shows 'Citrix Cloud' and 'SD-WAN Orchestrator'. Below this, the breadcrumb path is 'Customer cloudDNATest / Site All Sites'. The left sidebar contains a menu with 'Dashboard', 'Reports', 'Configuration', 'Troubleshooting' (expanded), and 'Administration'. Under 'Troubleshooting', there are links for 'Audit Logs', 'Device Logs', and 'Diagnostics'. The main content area is titled 'Network Troubleshooting : Diagnostics'. It features a form with the following elements:

- Test type selection: ☒ Ping, ☐ Traceroute, ☐ Packet Capture, ☐ Bandwidth Test.
- Source Site: A dark blue button labeled 'Source Site'.
- Source Site dropdown: A dropdown menu showing 'cDNTestCMD'.
- PING: A dark blue button labeled 'PING'.
- Form fields:
 - IP Address: An empty text input field.
 - Interface: A dropdown menu showing 'Default'.
 - Gateway IP (Optional): A dropdown menu showing 'Default'.
 - Routing Domain: A dropdown menu showing 'Default_RoutingDomain'.
 - Packet Size (KB): A text input field containing '70'.

ping が成功した場合、それはあなたの AD/DNS が正常に到達できることを意味し、そうでなければ、それはあなたの AD/DNS への到達可能性を妨げているネットワークにルーティングの問題があることを意味します。可能であれば、同じ LAN セグメントで AD と SD-WAN アプライアンスをホストしてみてください。

それでも問題が解決しない場合は、ネットワーク管理者に連絡してください。この手順を正常に完了しないと、カタログの作成手順は成功せず、グローバル **DNS IP** が構成されていないというエラーメッセージが表示されます。

注:

DNS が内部 IP と外部 IP の両方を解決できることを確認します。

ネットワークロケーションサービス

Citrix Cloud のネットワークロケーションサービスを使用すると、加入者のワークスペースでできるようにするアプリやデスクトップへの内部トラフィックを最適化して、HDX セッションを高速化できます。内部ネットワークと外部ネットワークの両方のユーザーは、外部 Gateway を介して VDA に接続する必要があります。これは外部ユーザーにとっては妥当な処理ですが、内部ユーザーにとっては仮想リソースへの接続が遅くなります。**Network Location** サービスを使用すると、内部ユーザーは Gateway をバイパスして VDA に直接接続できるため、内部ネットワークトラフィックの待ち時間が短縮されます。

構成

ネットワークロケーションサービスをセットアップするには、次のいずれかの方法を使用します。

- **Citrix SD-WAN Orchestrator:** Citrix SD-WAN Orchestrator を使用した NLS の構成の詳細については、「[ネットワークロケーションサービス](#)」を参照してください。
- **Citrix** が提供するネットワークロケーションサービス **PowerShell** モジュール: PowerShell モジュールを使用して NLS を構成する方法の詳細については、[PowerShell モジュールと構成](#)を参照してください。

ネットワークの場所は、内部ユーザが接続しているネットワークのパブリック IP 範囲を共有します。加入者が Workspace から Virtual Apps and Desktops セッションを起動すると、Citrix Cloud は、加入者が接続元のネットワークのパブリック IP アドレスに基づいて、社内ネットワークの内部または外部にあるかどうかを検出します。

利用者が内部ネットワークから接続している場合、Citrix Cloud では接続が Citrix Gateway を経由せず VDA に直接ルーティングされます。利用者が外部から接続している場合、Citrix Cloud では利用者が予定どおり Citrix Gateway を経由してルーティングされ、内部ネットワークの VDA にリダイレクトされます。

注:

ネットワークロケーションサービスで構成する必要があるパブリック IP は、WAN リンクに割り当てられたパブリック IP である必要があります。

ドメイン・ネーム・システム

November 8, 2021

ドメインネームシステム (**DNS**) は、人間が読めるドメイン名を機械読める IP アドレスに変換し、その逆も同様です。Citrix SD-WAN には、次の DNS 機能があります。

- DNS プロキシ
- DNS 透過転送

次のタイプの DNS サービスを使用して、DNS プロキシまたは DNS 透過転送を設定できます。

- **静的 DNS** サービス: 静的 IPv4 DNS サーバーの IP アドレスを構成できます。内部、ISP、グーグル、またはその他のオープンソース DNS サービスを作成できます。スタティック DNS サービスは、グローバルレベルとサイトレベルで構成できます。
- **ダイナミック DNS** サービス: ダイナミック IPv4 DNS サーバーの IP アドレスを構成できます。動的 DNS サービスは、サイトレベルでのみ構成できます。サイトごとに許可される動的 DNS サービスは 1 つだけです。
- **StaticV6 DNS** サービス: 静的 IPv6 DNS サーバーの IP アドレスを構成できます。内部、ISP、グーグル、またはその他のオープンソース DNS サービスを作成できます。StaticV6 DNS サービスは、グローバルレベルおよびサイトレベルで構成できます。
- **DynamicV6 DNS** サービス: ダイナミック IPv6 DNS サーバーの IP アドレスを構成できます。DynamicV6 DNS サービスは、サイトレベルでのみ構成できます。サイトごとに許可される動的 DNS サービスは 1 つだけです。

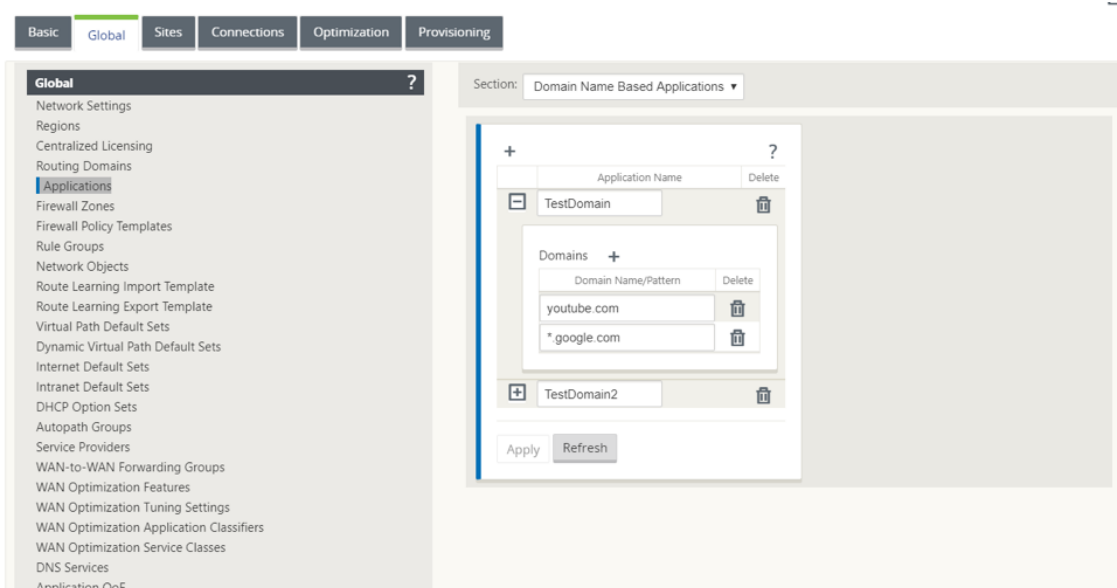
DNS プロキシ

アプリケーションのドメイン名に基づいて DNS 要求の操作に役立つ複数のフォワーダーを持つプロキシを構成できます。DNS 転送は、UDP 接続を介して受信される要求に対して機能します。

SD-WAN を DNS プロキシとして設定するには、次の手順を実行します。

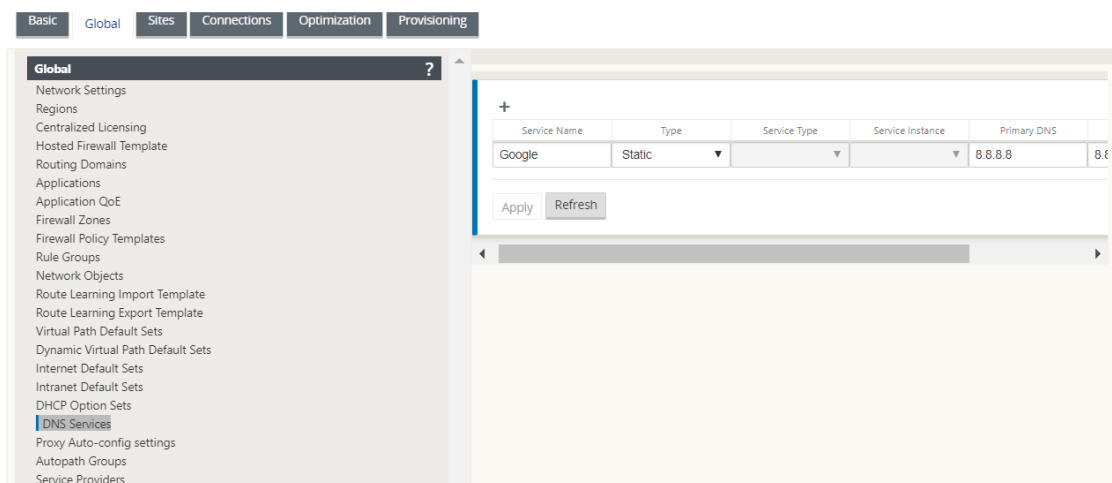
1. ドメイン名ベースのアプリケーションを定義します。設定エディタで、グローバル > アプリケーション > ドメイン名ベースのアプリケーションに移動します。

アプリケーション名と必要なドメイン名またはパターンを入力します。複数のドメイン名をアプリケーションとしてグループ化できます。完全なドメイン名を入力することも、先頭にワイルドカードを使用することもできます。たとえば `*.google.com`



2. 必要な DNS サービスを定義します。静的または動的 DNS サービスを定義できます。

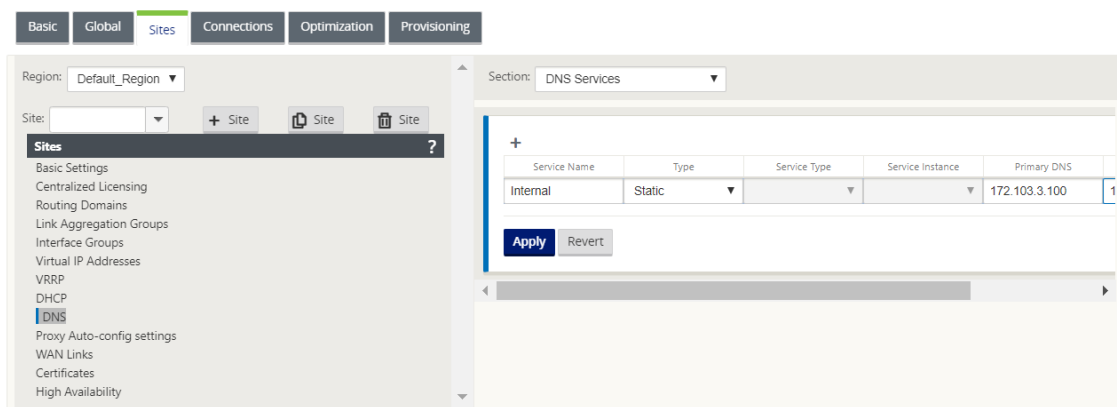
静的 DNS サービスを構成するには、[グローバル] > [**DNS サービス**] に移動し、[静的] (IPv4 アドレスの場合) または [**StaticV6**] (IPv6 アドレスの場合) を選択します。サービス名と、プライマリとセカンダリ DNS サーバの IP アドレスのペアを入力します。



注

Office 365 ブレークアウトポリシーを構成している場合は、Quad9 DNS サービスが自動作成されます。詳細については、「[Office 365 の最適化](#)」を参照してください。

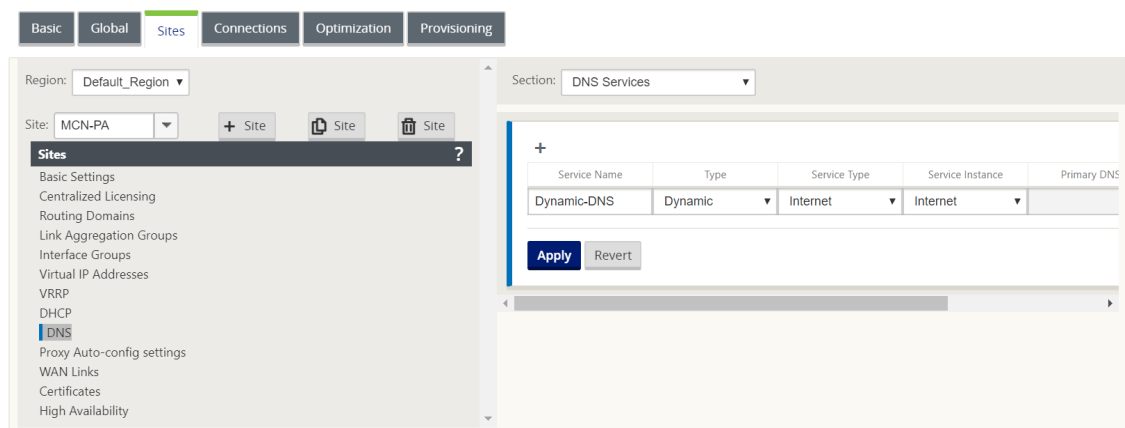
また、個々のサイトレベルで静的 DNS サービスを定義することもできます。サイトレベルの DNS サービス設定は、グローバル設定を上書きします。サイト固有の静的 DNS サービスを構成するには、[サイト] > [**DNS サービス**] に移動し、[静的] (IPv4 アドレスの場合) または [**StaticV6**] (IPv6 アドレスの場合) を選択します。



ダイナミック DNS サービスを構成するには、[サイト] > [**DNS サービス**] に移動し、[**** 動的として種類 ****] (IPv4 アドレスの場合) または **DynamicV6** (IPv6 アドレスの場合) を選択します。[サービス名] を入力し、[サービスタイプ] と [サービスインスタンス] で [インターネット] を選択します。

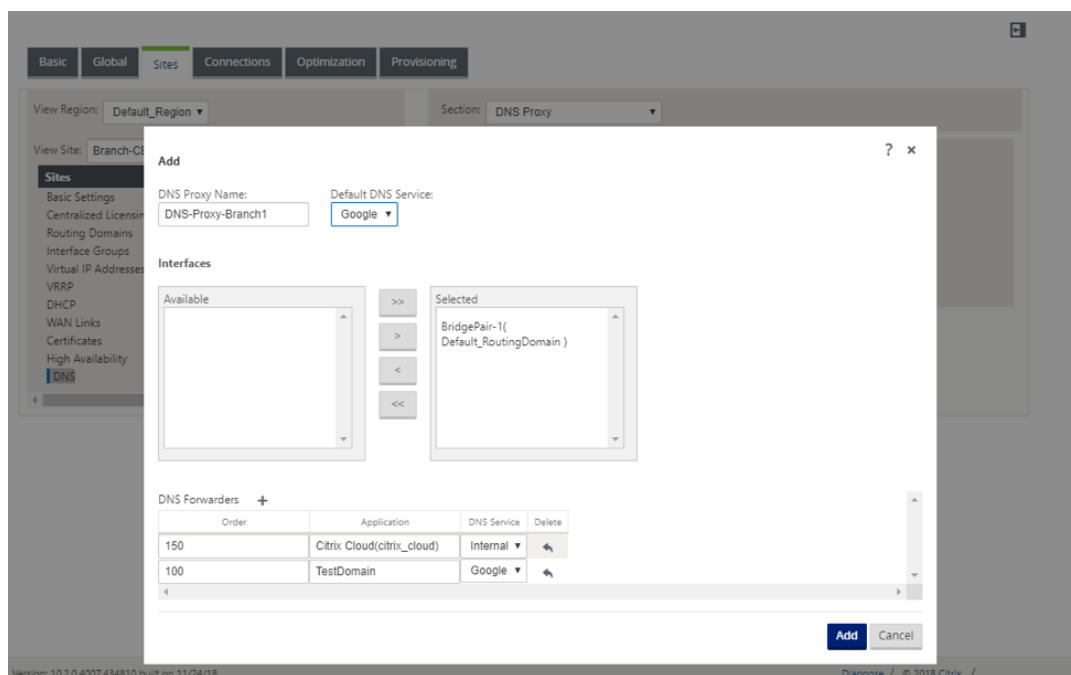
注

動的 DNS サービスは、サイトレベルでのみ構成できます。サイトごとに許可される動的 DNS サービスは 1 つだけです。



3. サイトの DNS プロキシを構成します。サイト] > [DNS] > [DNS プロキシ] に移動します。[+] をクリックします。次のパラメーターの値を入力します。

- **DNS** プロキシ名: DNS プロキシの名前。
- **IPv4** 既定の **DNS** サービス: DNS フォワードルックアップで一致しないアプリケーションがない場合、DNS 要求の転送先となる IPv4 既定の DNS サービス。
- **IPv6** 既定の **DNS** サービス: DNS フォワードルックアップで一致しないアプリケーションがない場合、DNS 要求の転送先の IPv6 既定の DNS サービス。
- インターフェイス: DNS 要求が傍受されるインターフェイス。信頼できるインターフェイスだけが許可されます。
- **DNS** フォワーダー: DNS フォワーダーのリスト。
 - 順序: フォワーダーの優先順位。
 - アプリケーション: 選択した DNS サービスに DNS 要求を転送する必要があるアプリケーション。
 - **IPv4 DNS** サービス: 指定されたアプリケーションの DNS 要求が転送される IPv4 DNS サービス。
 - **IPv6 DNS** サービス: 指定されたアプリケーションの DNS 要求が転送される IPv6 DNS サービス。



注

DNS プロキシは、次の SD-WAN アプライアンスでは設定できません。

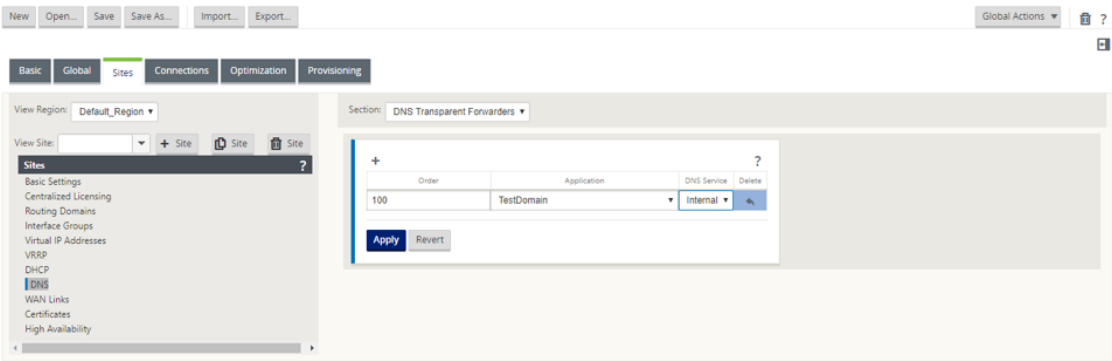
- Citrix SD-WAN 1000 SE/PE
- Citrix SD-WAN 2000 SE/PE
- Citrix SD-WAN 4000 SE

DNS トランスペアレントフォワーダ

Citrix SD-WAN は、透過的な DNS フォワーダとして構成できます。このモードでは、SD-WAN は IP アドレス宛てではない DNS 要求を代行受信し、指定した DNS サービスに転送できます。信頼できるインターフェイス上のローカルサービスからの DNS 要求だけが傍受されます。DNS 要求が DNS フォワーダリスト内のアプリケーションと一致する場合、その要求は設定された DNS サービスに転送されます。DNS 転送は、UDP 接続経由で着信する要求に対してのみサポートされます。

SD-WAN を DNS トランスペアレントフォワーダとして設定するには、次の手順を実行します。

1. [サイト] > [DNS] > [DNS トランスペアレントフォワーダー] に移動します。[+] をクリックします。
2. 次のパラメーターの値を入力します。
 - 順序: フォワーダの優先順位。
 - アプリケーション: 選択した DNS サービスに DNS 要求を転送する必要があるアプリケーション。
 - **IPv4 DNS** サービス: 指定されたアプリケーションの DNS 要求が転送される IPv4 DNS サービス。
 - **IPv6 DNS** サービス: 指定されたアプリケーションの DNS 要求が転送される IPv6 DNS サービス。



同様に、必要に応じて他の DNS トランスペアレントフォワーダを追加します。

3. **[Apply]** をクリックします。

監視

プロキシ統計情報およびトランスペアレントフォワーダ統計情報を表示するには、[モニタリング] > [DNS] に移動します。

アプリケーション名、DNS サービス名、DNS サービスの状態、および DNS サービスへのヒット数を表示できます。

プロキシ統計情報

Dashboard	Monitoring	Configuration
Statistics	Monitoring > DNS	
Flows		
Routing Protocols		
Firewall		
IKE/IPsec		
ICMP		
Performance Reports		
Qos Reports		
Usage Reports		
Availability Reports		
Appliance Reports		
DHCP Server/Relay		
VRRP		
PPPoE		
DNS		

DNS Statistics

Refresh

Proxy Statistics

Search:

Proxy Name	Application Name	DNS Service Name	DNS Service Active	Hits
DNS_Proxy1	office365_optimize	Quad9	YES	2
DNS_Proxy1	office365_allow	Quad9	YES	8
DNS_Proxy1	office365_default	Quad9	YES	6
DNS_Proxy1	Any	Google	YES	17

Showing 1 to 4 of 4 entries

Transparent Forwarder Statistics

Search:

Application Name	DNS Service Name	DNS Service Active	Hits
office365_allow	Quad9	YES	0
office365_default	Quad9	YES	0
office365_optimize	Quad9	YES	0

Showing 1 to 3 of 3 entries

トランスペアレントフォワーダの統計

Dashboard

Monitoring

Configuration

Statistics

Flows

Routing Protocols

Firewall

IKE/IPsec

ICMP

Performance Reports

Qos Reports

Usage Reports

Availability Reports

Appliance Reports

DHCP Server/Relay

VRRP

PPPoE

DNS

Monitoring > DNS

DNS Statistics

Refresh

Proxy Statistics

Search:

Proxy Name	Application Name	DNS Service Name	DNS Service Active	Hits
No Proxy Stats at this time.				
Showing 0 to 0 of 0 entries				

Transparent Forwarder Statistics

Search:

Application Name	DNS Service Name	DNS Service Active	Hits
SocialMedia	Google	YES	5
OnlineShopping	Google	YES	2
office365_optimize	Quad9	YES	1
office365_default	Quad9	YES	11
office365_allow	Quad9	YES	8

Showing 1 to 5 of 5 entries

DHCP サーバと DHCP リレー

November 17, 2022

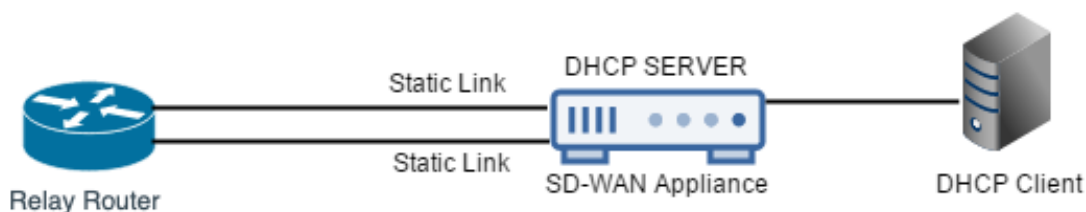
Citrix SD-WAN では、Standard Edition または Premium Edition のアプライアンスを DHCP サーバまたは DHCP リレーエージェントとして使用できます。DHCP サーバ機能を使用すると、SD-WAN アプライアンスの LAN/WAN インターフェイスと同じネットワーク上のデバイスが、SD-WAN アプライアンスから IP 設定を取得できます。DHCP リレー機能を使用すると、SD-WAN アプライアンスは DHCP クライアントとサーバ間で DHCP パケットを転送できます。

DHCP サーバおよび DHCP リレー機能を使用する利点は次のとおりです。

- クライアントサイトの機器の量を減らします。
- クライアントサイトのルーターを置き換える (エッジルーターサービスの容易な展開)。
- クライアントサイトネットワークを簡素化します。
- CLI コマンドを使用しないルータの設定
- 単純なクライアントサイトでの手動構成を減らします。

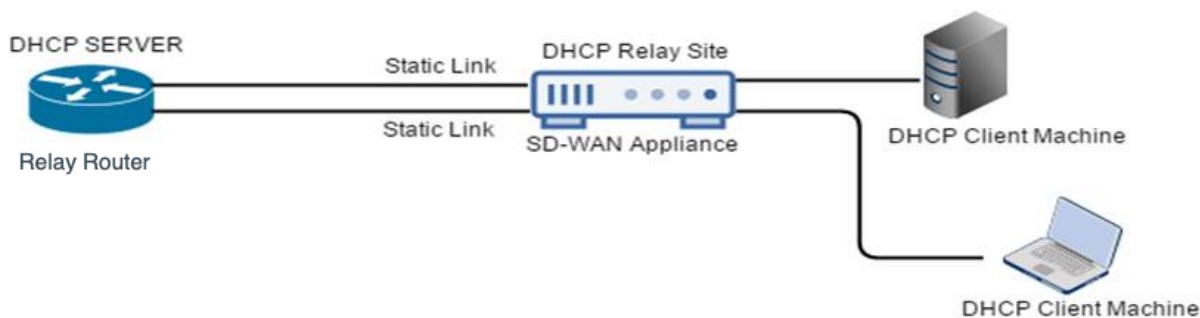
DHCP サーバ

Citrix SD-WAN アプライアンスは、DHCP サーバとして構成できます。ネットワーク内の指定されたアドレスブールの IP アドレスを DHCP クライアントに割り当てて管理することができます。DHCP サーバは、ドメインネームシステム (DNS) サーバの IP アドレスやデフォルトルータなど、さらに多くのパラメータを割り当てるように設定できます。DHCP サーバは、アドレス割り当て要求と更新を受け入れます。DHCP サーバは、ローカルに接続された LAN セグメントからのブロードキャストや、ネットワーク内の他の DHCP リレーエージェントによって転送された DHCP 要求からのブロードキャストも受け付けます。



DHCP リレー

DHCP リレーエージェントは、クライアントとサーバ間で DHCP パケットを転送するホストまたはルータです。ネットワーク管理者は、SD-WAN アプライアンスの DHCP リレーサービスを使用して、ローカルの DHCP クライアントとリモートの DHCP サーバー間で要求と応答をリレーできます。これにより、ローカルホストはリモート DHCP サーバーからダイナミック IP アドレスを取得できます。リレーエージェントは DHCP メッセージを受信し、新しい DHCP メッセージを生成して別のインターフェイスに送信します。



DHCP サーバと DHCP リレーの設定

November 8, 2021

設定エディタを使用した DHCP サーバと DHCP リレーの設定

構成エディタを使用して、ネットワーク上のアプライアンスの DHCP サーバおよび DHCP リレー設定を構成できます。構成は、変更管理プロセスを通じて SD-WAN ネットワーク内のアプライアンスにプッシュされます。

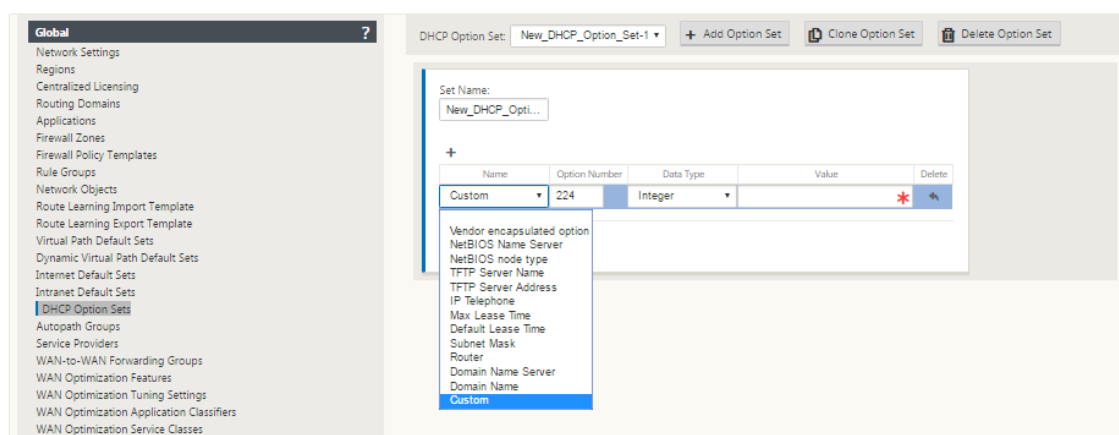
構成エディタを使用してサイトを DHCP サーバとして構成するには、次の手順を実行します。

1. [構成エディタ] > [サイト] > [[サイト名]] > [DHCP] > [サーバーサブネット] に移動します。[+] をクリックします。

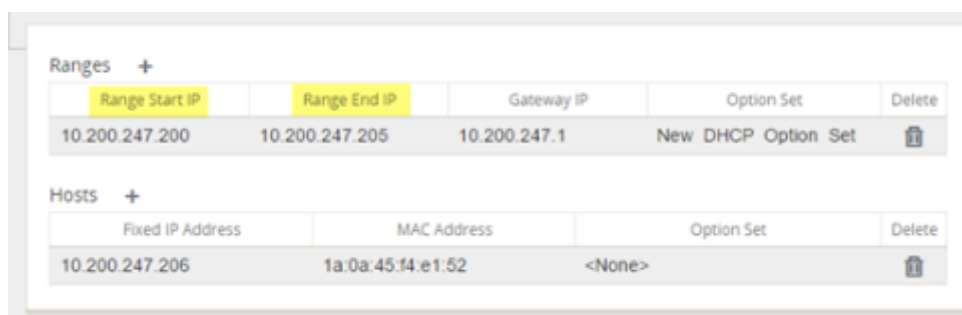
- 複数のドメインが存在する場合は、構成済みのルーティングドメインを選択します。
- DHCP 要求の受信に使用する仮想インターフェイスを選択します。DHCP サーバがアドレスを提供するために使用する IP サブネットは、自動的に設定されます。
- ドメイン名、プライマリ **DNS**、およびセカンダリ **DNS** を入力します。DHCP サーバはこの情報をクライアントに転送します。
- [**Enable**] をクリックして、サブネットを有効にします。
- クライアントに IP アドレスを割り当てるために使用されるダイナミック IP アドレスプールを構成します。範囲の開始 IP アドレスと終了 IP アドレスを指定し、オプションセットを選択します。

(注

) DHCP オプションセットは、個々の IP アドレス範囲に適用できる DHCP 設定のグループです。DHCP オプションセットを作成するには、[グローバル] > [**DHCP** オプションセット] に移動します。必要な DHCP オプションを選択し、その値を指定します。



- MAC アドレスに基づいて固定 IP アドレスを必要とする個々のホストを設定します。リサーバー IP アドレスとも呼ばれます。[固定 IP アドレス]、[**MAC** アドレス]、および [オプションセット] を選択します。

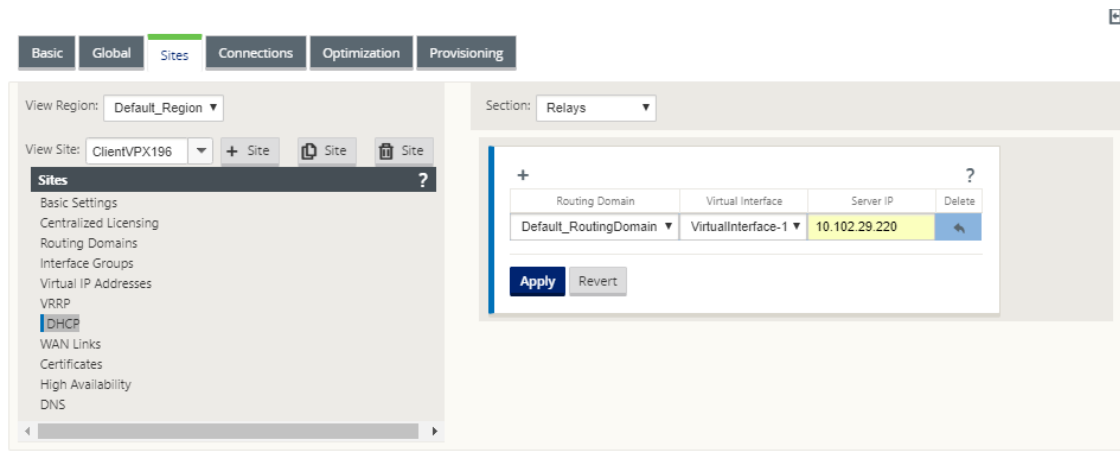


注

固定 IP アドレスの場合、**Gateway IP** は **DHCP** オプションセットで Router オプションを設定することによって設定されます。

構成エディタを使用して、サイトを DHCP リレーとして設定するには、次の手順を実行します。

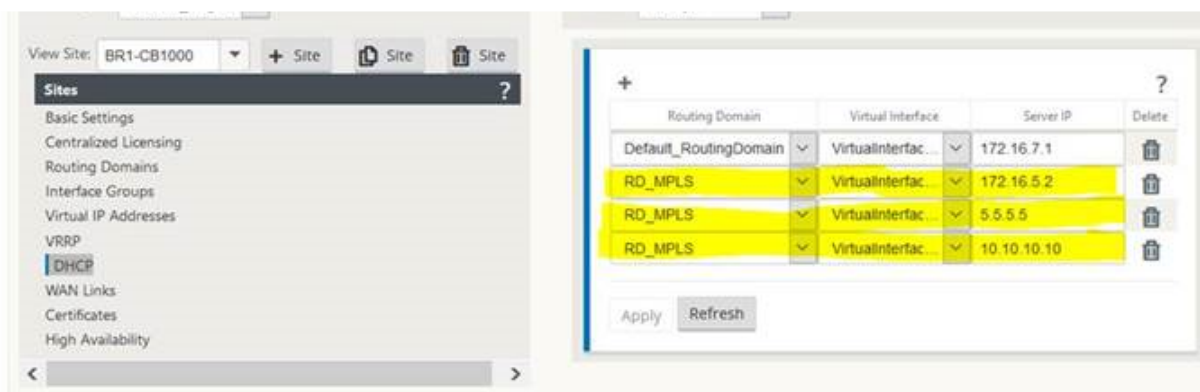
1. [構成エディタ] > [サイト] > [サイト名] > [**DHCP**] > [リレー] に移動します。[+] をクリックします。
2. 複数のドメインが存在する場合は、構成済みのルーティングドメインを選択します。
3. リモート DHCP サーバーと通信する仮想インターフェイスを選択します。
4. リレーがクライアントからの要求と応答を転送するために使用する DHCP サーバ IP を入力します。



共通の仮想ネットワークインターフェイスを使用して単一の DHCP リレーを構成し、複数の DHCP サーバーを指し示すことができます。

(注

) 仮想インターフェイスごとに 1 つのリレーエージェントがスポンされ、リレーエージェントごとに合計 16 の DHCP サーバを設定できます。サイトには最大 16 のリレーエージェントを設定できます。



DHCP サーバデータベースからクライアントのリストを表示するには、Web 管理インターフェイスで、[モニター] > [**DHCP** サーバ/リレー] に移動します。

Show DHCP Server Client Database						
Routing Domain	Client IP Address	Lease Start Time	Lease End Time	Client MAC Address	Client Hostname	State
Default_RoutingDomain	10.200.247.200	Mon Jul 11 15:23:23 2016	Mon Jul 11 15:29:23 2016	3a:1a:dc:67:ca:b4	TexasF_Angelina2_TN	active

Close

アプライアンスの設定を使用して、**SD-WAN** アプライアンスを **DHCP** サーバーまたは **DHCP** リレーとして構成する

個別の SD-WAN アプライアンスは、アプライアンスの設定ページから手動で DHCP サーバーまたは DHCP リレーとして構成できます。

SD-WAN アプライアンスで DHCP サーバーを有効にするには、次の手順を実行します。

1. [構成] > [アプライアンスの設定] > [ネットワークアダプタ] に移動します。[ネットワークアダプタ] ページで、[管理インターフェイス **DHCP** サーバー] ペインを探します。
2. [**DHCP** サーバを有効にする] をクリックしてサーバを起動し、リース時間 (分単位) と [ドメイン名] を入力し、[開始 **IP** アドレス] と [終了 **IP** アドレス **] を入力して **IP** アドレスの範囲 ** を定義します。

注:

サーバーの IP アドレスプールは、管理ネットワーク内にある必要があります。

Management Interface DHCP Server

If you plan to use the DHCP Server or DHCP Relay services on a Citrix Appliance configured for High Availability (HA), do not configure either service on both the Active and Standby appliance. Doing so will lead to duplicate IP addresses on the defined management network.

When HA switches from the Active to the Standby Citrix Appliance, the DHCP Server and DHCP Relay service settings are not applied on the Standby appliance and will stop working.

The Management Interface DHCP Server will use the current Management Interface IP settings (gateway, subnet mask, and DNS servers) for DHCP offers. The DHCP Server IP range, defined by Start and End IP Address, must be valid in the Management Interface subnet.

DHCP Server Status: stopped

Enable DHCP Server: ☒

Lease Time (minutes):

Domain Name:

Start IP Address:

End IP Address:

3. [設定の変更] をクリックして、DHCP サーバーの設定を終了します。

注

高可用性 (HA) 用に構成された SD-WAN アプライアンスで DHCP サーバを使用する場合は、アクティ

ブアプライアンスとスタンバイアプライアンスの両方でサービスを構成しないでください。これにより、定義された管理ネットワーク上で IP アドレスが重複します。

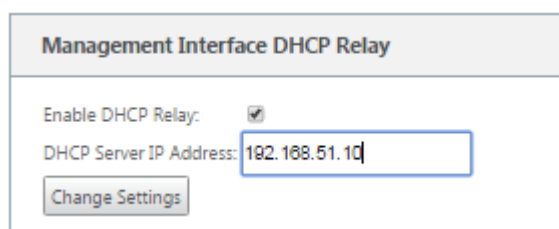
4. [クライアントの表示] をクリックして現在の DHCP クライアントを表示し、[クライアントのクリア] をクリックして DHCP クライアントのリースを解放します。

SD-WAN アプライアンスで DHCP リレーサービスを有効にするには:

1. [構成] > [アプライアンスの設定] > [ネットワークアダプタ] に移動します。[ネットワークアダプタ] ページで、[管理インターフェイス **DHCP** リレー] ペインを探します。
2. [**DHCP** リレーの有効化] チェックボックスをクリックして、サービスを有効にします。 **DHCP** サーバの **IP** アドレスを入力し、[設定の変更 (**Change Settings**)] をクリックして、アプライアンスを DHCP リレーエージェントとして使用します。

注

高可用性 (HA) 用に構成されたアプライアンスで DHCP リレーサービスを使用する場合は、アクティブアプライアンスとスタンバイアプライアンスの両方でサービスを構成しないでください。これにより、定義された管理ネットワーク上で IP アドレスが重複します。



DHCP クライアントによる WAN リンク IP アドレスの学習

June 8, 2022

Citrix SD-WAN アプライアンスは、DHCP クライアントによる WAN リンクの IP アドレス学習をサポートします。この機能により、SD-WAN アプライアンスの導入に必要な手動設定の量が削減され、静的 IP アドレスを購入する必要がなくなり、ISP のコストが削減されます。SD-WAN アプライアンスは、信頼できないインターフェイス上の WAN リンクのダイナミック IP アドレスを取得できます。これにより、この機能を実行するために中間 WAN ルーターが不要になります。

注

- DHCP クライアントは、クライアントノードとして構成された信頼できないブリッジドインターフェイスに対してのみ構成できます。
- DHCP クライアントとデータポートは、パブリック IP アドレスが設定されている場合のみ、MCN/RCN

で有効にできます。

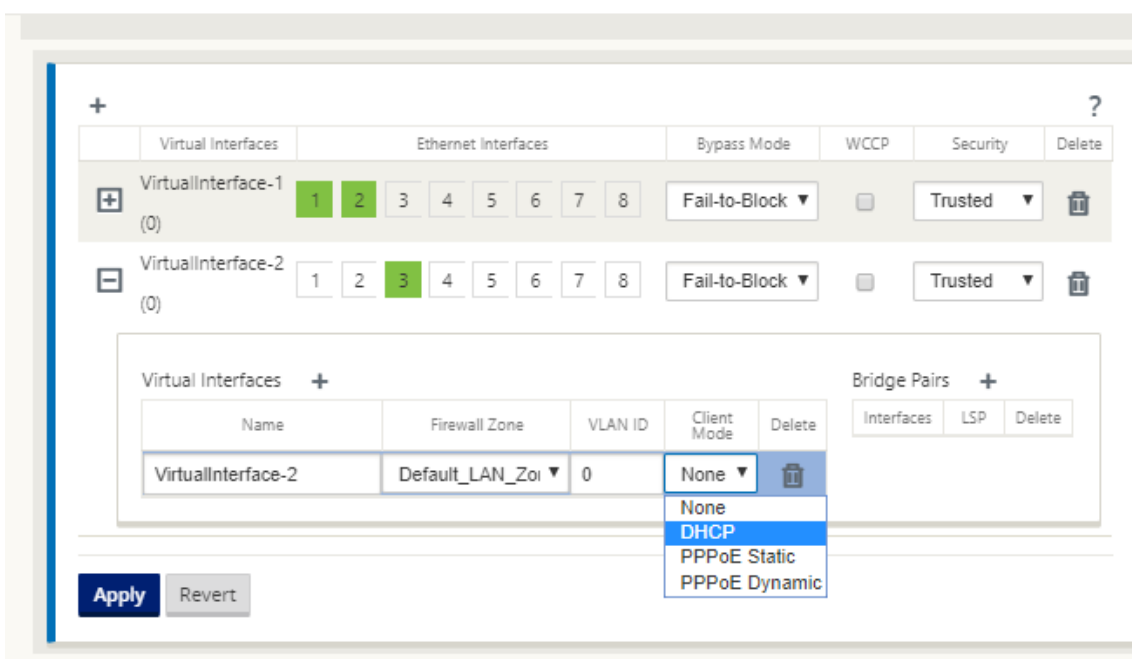
- ワンアームまたはポリシーベースルーティング (PBR) 展開は、DHCP クライアント構成のサイトではサポートされません。
- DHCP イベントはクライアント側からのみログに記録され、DHCP サーバーログは生成されません。

フェールツーブロックモードで信頼できない仮想インターフェイスに DHCP を設定するには、次の手順を実行します。

1. 構成エディタで、[サイト] > [サイト名] > [インターフェイスグループ] > [仮想インターフェイス] に移動します。

注

インターフェイスグループ内の物理インターフェイスは、単一のインターフェイス上の非ブリッジドペアである必要があります。



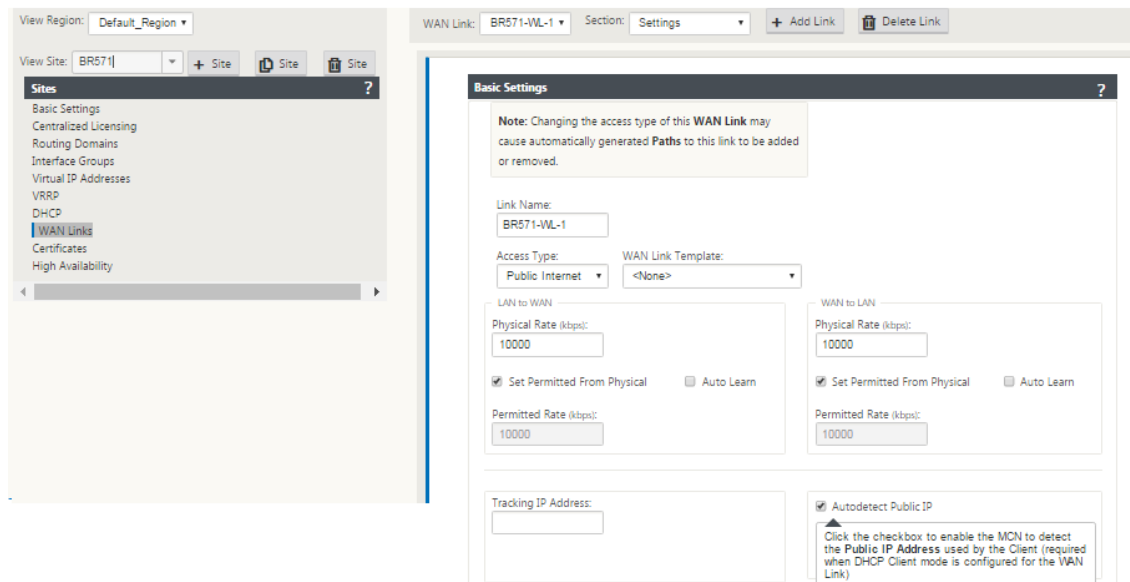
2. クライアントモードとして、次のオプションのいずれかを選択します。

- DHCP IPv4 のみ
- DHCP IPv6 のみ
- DHCP IPv4 IPv6

SLAAC と DHCP IPv6 または DHCP IPv4 IPv6 の両方が有効の場合、DHCPv6 はステートレスモードで機能します。

1. [**WAN** リンク] > [**WAN** リンク名] > [** 設定] ** > [基本設定] に移動します。

2. MCN でクライアントが使用する パブリック IP アドレスを検出できるようにするには、[パブリック IP の自動検出] チェックボックスをオンにします。これは、WAN リンクに DHCP クライアントモードが設定されている場合に必要です。

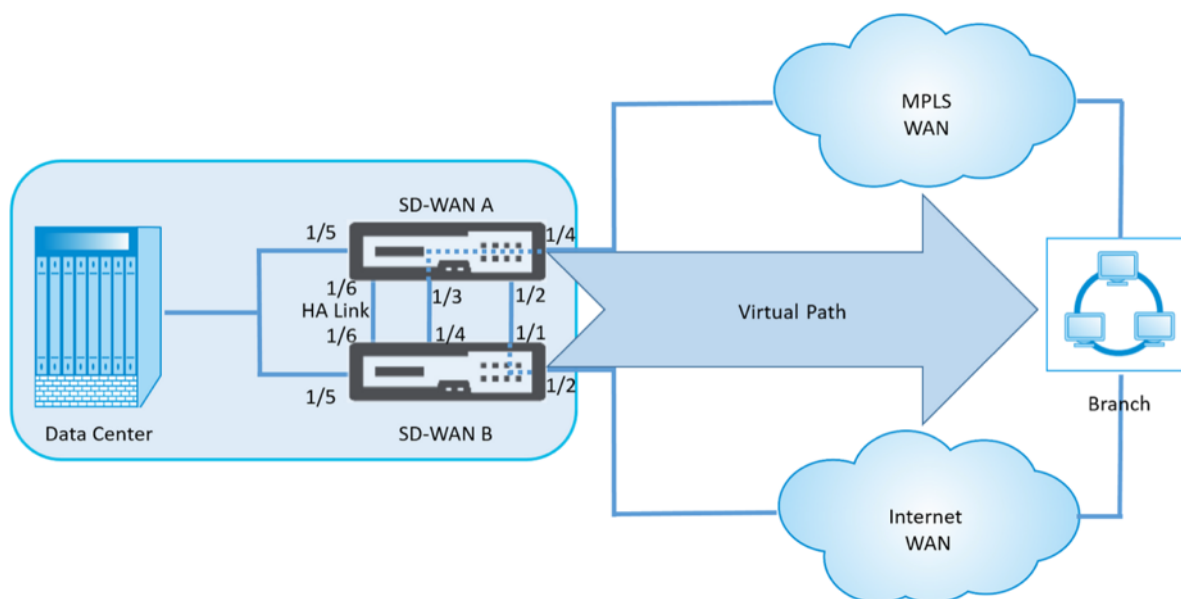


フェールツーワイヤポートでの **DHCP** サポート

以前は、DHCP クライアントは Fail-to-Block ポートでのみサポートされていました。11.2.0 リリースでは、シリアル High Availability (HA) 展開のブランチサイトのフェールツーワイヤポートで DHCP クライアント機能が拡張されました。この拡張機能:

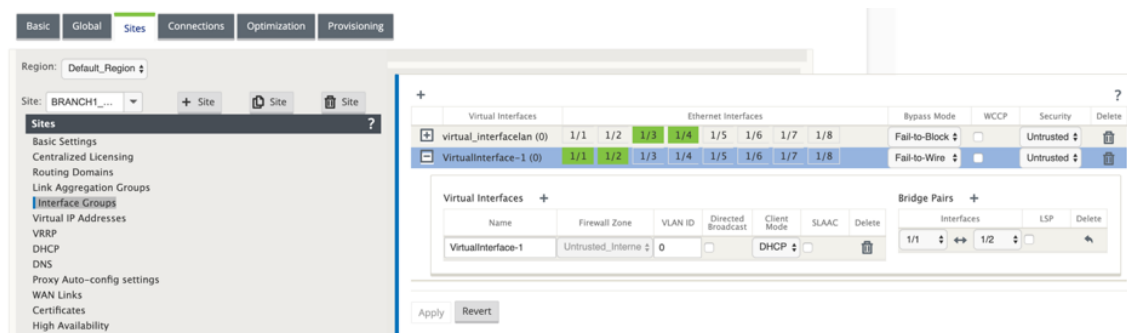
- Fail-to-Wire ブリッジペアおよびシリアル HA 配置を持つ信頼できないインターフェイスグループで DHCP クライアント設定を許可します。
- プライベートイントラネット **WAN** リンクの一部として DHCP インターフェイスを選択できるようにします。

DHCP クライアントがプライベートイントラネットリンクでサポートされるようになりました。



Fail-to-Wire モードで信頼できない仮想インターフェイスに DHCP を設定するには、次の手順を実行します。

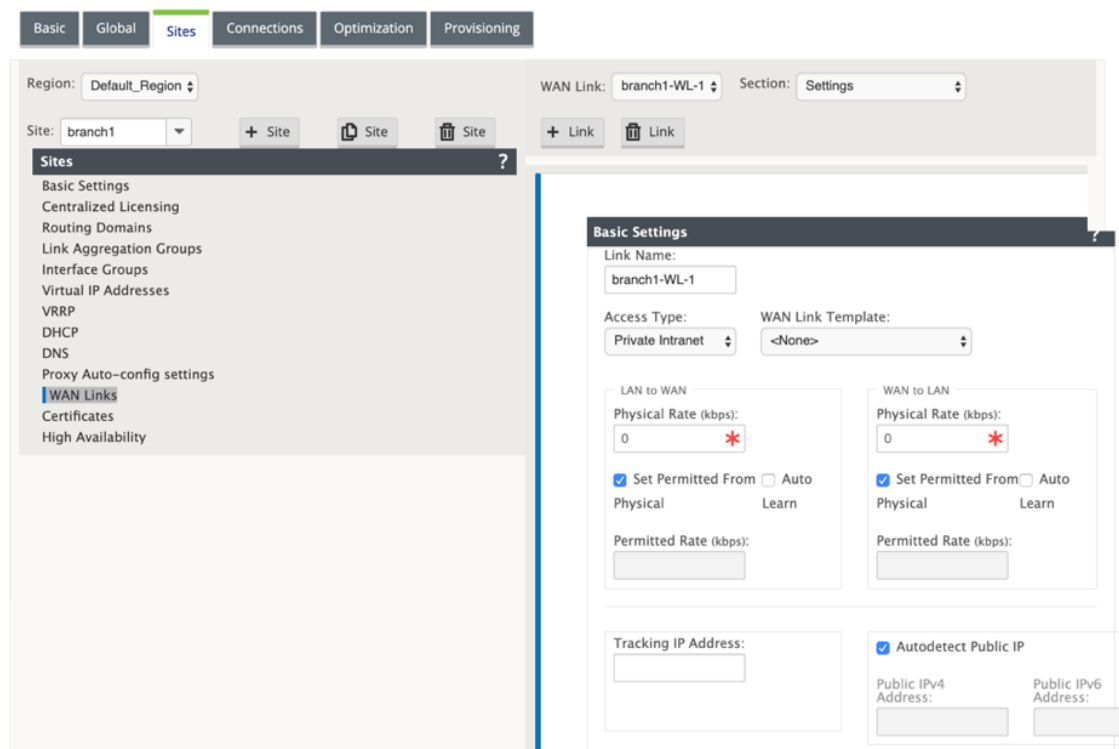
1. 構成エディタで、[サイト] > [サイト名] > [インターフェイスグループ] > [仮想インターフェイス] に移動します。



2. クライアントモードとして次のいずれかのオプションを選択し、ブリッジペアを追加します。

- DHCP IPv4 のみ
- DHCP IPv6 のみ
- DHCP IPv4 IPv6

3. [WAN リンク] に移動し、[+] をクリックし、ドロップダウンリストから [WAN リンク名] を選択し、[セクション] フィールドで [設定] > [基本設定] を選択します。
4. MCN でクライアントが使用する パブリック IP アドレスを検出できるようにするには、[パブリック IP の自動検出] チェックボックスをオンにします。これは、WAN リンクに DHCP クライアントモードが設定されている場合に必要です。



注:

インターフェイス間でパケットがブリッジされる可能性があるため、LAN インターフェイスは Fail-to-Wire ペアに接続しないでください。

DHCP クライアントの WAN リンクの監視

ランタイム仮想 IP アドレス、サブネットマスク、および Gateway の設定は、*SDWANVW_ip_learned.log* というログファイルに記録され、アーカイブされます。イベントは、ダイナミック仮想 IP が学習、リリース、または期限切れになったとき、および学習された Gateway または DHCP サーバとの通信の問題が発生した場合に生成されます。または、アーカイブされたログファイルで重複した IP アドレスが検出された場合。サイトで重複した IP が検出された場合、動的仮想 IP アドレスは解放され、サイトのすべての仮想インターフェイスが一意的仮想 IP アドレスを取得するまで更新されます。

DHCP クライアントの WAN リンクを監視するには

1. SD-WAN アプライアンスの [フローの有効化/無効化/消去] ページの [DHCP クライアント WAN リンク] テーブルに、学習された IP のステータスが表示されます。
2. IP の更新を要求できます。これにより、リース時間が更新されます。[**Release Rnew**] を選択すると、新しい IP アドレス、または同じ IP アドレスを新しいリースとともに発行することもできます。

DHCP Client WAN Links									
Ethernet Interface	Virtual Interface	WAN Link	IP Address / Prefix	Gateway IP Address	Lease Duration Seconds	Remaining Seconds	Expiration Date	Action	
X2	VLAN349	SFWL3-Inter	10.30.30.55/24	10.30.30.2	1800	1640	9:13 on 1/8/2016	Renew	Submit
X2	VLAN350	SFWL4-Inter	10.20.20.53/24	10.20.20.2	86400	71035	4:29 on 1/9/2016	Renew	Submit

DHCP ログ

Citrix SD-WAN では、IP アドレスの DHCP サーバーログを生成できます。エンドポイントに IP アドレスが割り当てられるたびに、ログが生成されます。ログには、IP アドレス割り当てのタイムスタンプ、リース期間、MAC アドレス、クライアント ID などの詳細が含まれます。クライアント ID **none** は、DHCP 要求に存在しないことを示しています。

DHCP ログを生成して表示するには、[構成] > [ログ/監視] に移動します。ドロップダウンリストから **SD-WAN_dhcp.log** オプションを選択し、[ログの表示] をクリックします。

```
Feb  4 11:58:30 BR1-Primary dhcpd: Internet Systems Consortium DHCP Server 4.3.2
Feb  4 11:58:30 BR1-Primary dhcpd: Copyright 2004-2015 Internet Systems Consortium.
Feb  4 11:58:30 BR1-Primary dhcpd: All rights reserved.
Feb  4 11:58:30 BR1-Primary dhcpd: For info, please visit https://www.isc.org/software/dhcp/
Feb  4 11:58:30 BR1-Primary dhcpd: wrote 0 deleted host decls to leases file.
Feb  4 11:58:30 BR1-Primary dhcpd: wrote 0 new dynamic host decls to leases file.
Feb  4 11:58:30 BR1-Primary dhcpd: wrote 1 leases to leases file.
Feb  4 11:58:30 BR1-Primary dhcpd: listening on LPF/vni-1/36:00:00:52:9f:cc/172.58.3.0/24
Feb  4 11:58:30 BR1-Primary dhcpd: sending on LPF/vni-1/36:00:00:52:9f:cc/172.58.3.0/24
Feb  4 11:58:30 BR1-Primary dhcpd: Server starting service.
Feb  4 11:58:30 BR1-Primary dhcpd: listening on LPF/vni-0/de:82:2f:9e:4c:3d/172.58.30.0/24
Feb  4 11:58:30 BR1-Primary dhcpd: sending on LPF/vni-0/de:82:2f:9e:4c:3d/172.58.30.0/24
Feb  4 11:58:30 BR1-Primary dhcpd: Server starting service.
Feb  4 11:58:31 BR1-Primary dhcpd: DHCPDISCOVER from 02:63:f0:de:19:3f via vni-0
Feb  4 11:58:31 BR1-Primary dhcpd: DHCPOFFER on 172.58.30.151 to 02:63:f0:de:19:3f via vni-0
Feb  4 11:58:31 BR1-Primary dhcpd: DHCPREQUEST for 172.58.30.151 from 02:63:f0:de:19:3f via vni-0
Feb  4 11:58:31 BR1-Primary dhcpd: DHCPACK on 172.58.30.151 to 02:63:f0:de:19:3f via vni-0
Feb  4 11:58:31 BR1-Primary dhcpd: Lease time start : 4 1970/01/01 00:00:00; Lease time end : 4 1970/01/01 00:00:00; for IP : MAC-Address : 02:63:f0:de:19:3f; Client-Id : <none>
```

注

これらのログは、Citrix SD-WAN が DHCP サーバーとして動作する場合にのみ生成されます。

ダイナミック PAC ファイルのカスタマイズ

May 10, 2021

ミッションクリティカルな SaaS アプリケーションと分散型ワークフォースの企業導入の増加に伴い、レイテンシーと輻輳を低減することが非常に重要になります。レイテンシーと輻輳は、データセンターを通過するトラフィックをバックホールする従来の方法に固有のものです。Citrix SD-WAN では、Office 365 などの SaaS アプリケーションを直接インターネットから抜け出すことができます。詳しくは、「Office 365 の最適化」を参照してください。

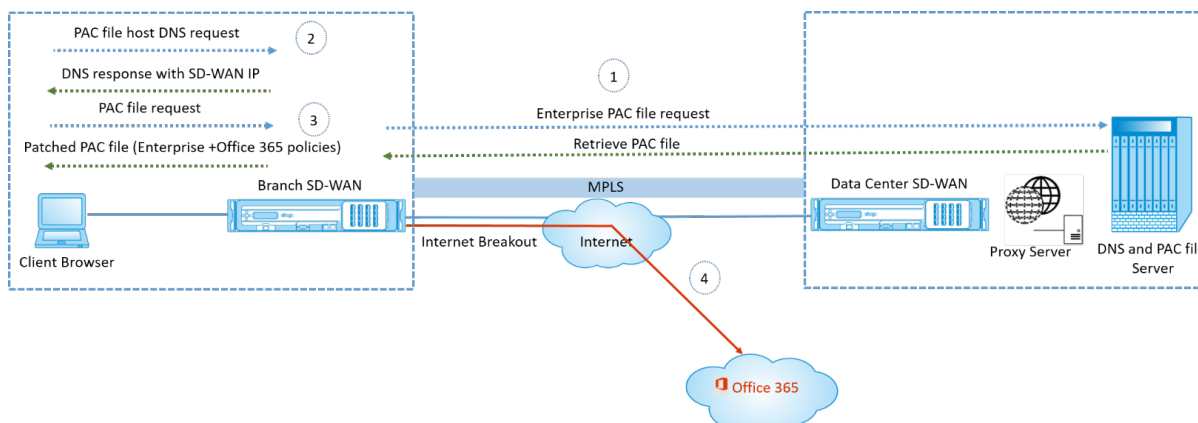
企業展開で明示的な Web プロキシが設定されている場合、すべてのトラフィックが Web プロキシに誘導されるため、分類や直接インターネットブレイクアウトが難しくなります。解決策は、エンタープライズ PAC (Proxy

Auto-Config) ファイルをカスタマイズすることによって、SaaS アプリケーショントラフィックがプロキシされないようにすることです。

Citrix SD-WAN 11.0 では、カスタム PAC ファイルを動的に生成して提供することにより、Office 365 アプリケーショントラフィックのプロキシバイパスとローカルインターネットブレイクアウトが可能になります。PAC ファイルは、Web ブラウザーの要求が送信先に直接送信されるか、Web プロキシサーバーに送信されるかを定義する JavaScript 関数です。

PAC ファイルのカスタマイズの仕組み

理想的には、内部 Web サーバー上のエンタープライズネットワークホスト PAC ファイル、これらのプロキシ設定はグループポリシーを介して配布されます。クライアントブラウザは、エンタープライズ Web サーバから PAC ファイルを要求します。Citrix SD-WAN アプライアンスは、Office 365 ブレイクアウトが有効なサイト用にカスタマイズされた PAC ファイルを提供します。



1. Citrix SD-WAN は、エンタープライズ Web サーバーからエンタープライズ PAC ファイルの最新のコピーを定期的に要求し、取得します。Citrix SD-WAN アプライアンスは、オフィス 365 の URL をエンタープライズ PAC ファイルにパッチします。エンタープライズ PAC ファイルには、Office 365 の URL にシームレスにパッチが適用されるブレースホルダ (SD-WAN 固有のタグ) が必要です。
2. クライアントブラウザは、エンタープライズ PAC ファイルホストの DNS 要求を生成します。Citrix SD-WAN は、プロキシ構成ファイル FQDN に対する要求を代行受信し、Citrix SD-WAN VIP に応答します。
3. クライアントブラウザが PAC ファイルを要求します。Citrix SD-WAN アプライアンスは、パッチが適用された PAC ファイルをローカルで提供します。PAC ファイルには、エンタープライズプロキシ構成と Office 365 の URL 除外ポリシーが含まれています。
4. Office 365 アプリケーションの要求を受信すると、Citrix SD-WAN アプライアンスは直接インターネットブレイクアウトを実行します。

前提条件

1. 企業は、PAC ファイルをホストする必要があります。
2. PAC ファイルには、プレースホルダ `SDWAN_TAG` または Office 365 の URL にパッチを適用するための `findproxyforurl` 関数が 1 つある必要があります。
3. PAC ファイルの URL は、IP ベースではなく、ドメインベースである必要があります。
4. PAC ファイルは、信頼されたアイデンティティ VIP を介してのみ提供されます。
5. Citrix SD-WAN アプライアンスは、管理インターフェイス経由でエンタープライズ PAC ファイルをダウンロードできる必要があります。

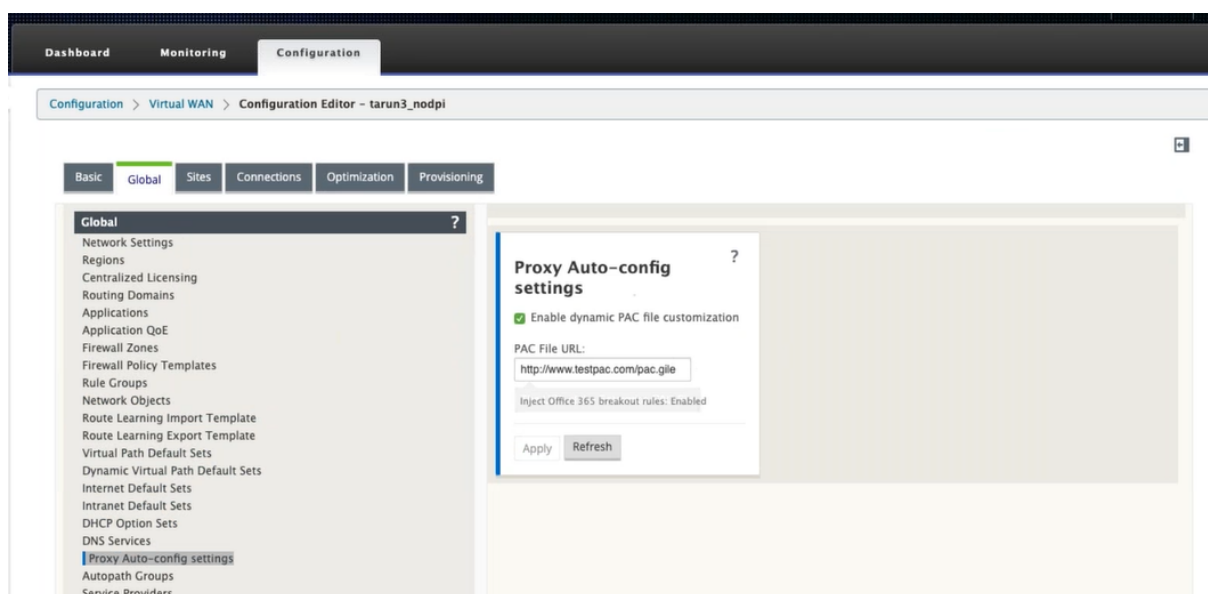
PAC ファイルのカスタマイズを設定する

PAC ファイルのカスタマイズは、グローバルに有効にすることも、サイトレベルで有効にすることもできます。

注:

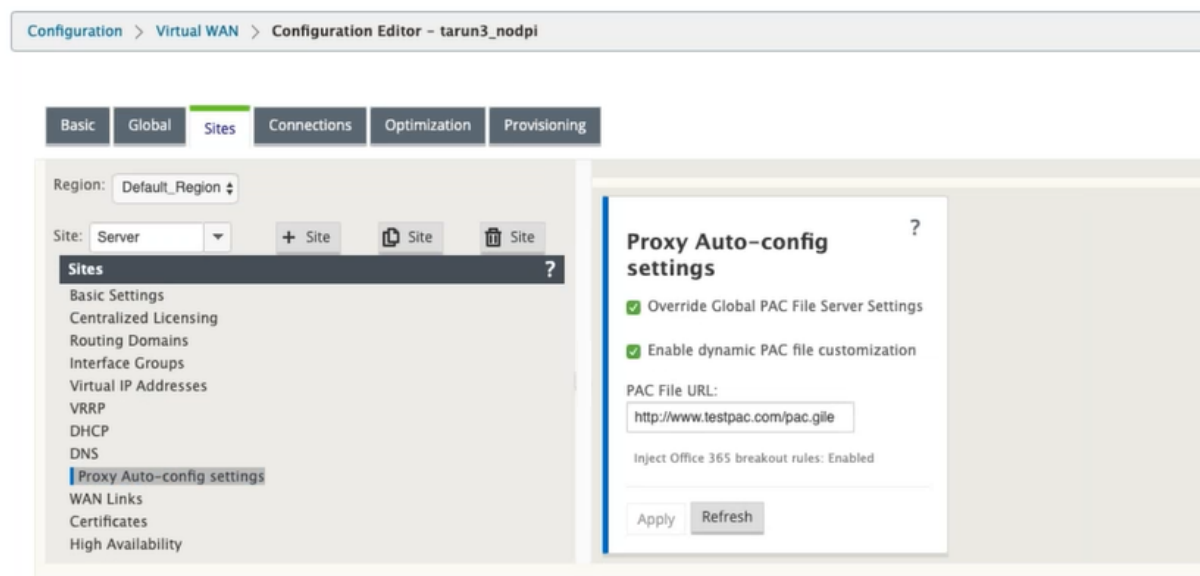
Office 365 ブレークアウトオプションは、PAC ファイルの動的カスタマイズを有効にする必要があります。
Office 365 ブレークアウトを有効にする方法については、「[Office 365 の最適化](#)」を参照してください。

ダイナミック PAC ファイルのカスタマイズをすべてのサイトでグローバルに設定するには、設定エディタで [グローバル] > [プロキシ自動設定設定] に移動します。



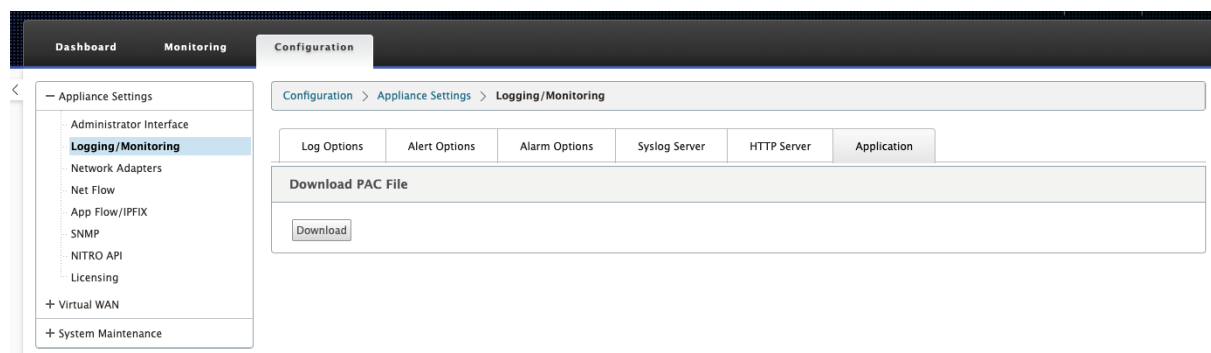
[ダイナミック **PAC** ファイルのカスタマイズを有効にする] を選択します。[**PAC** ファイル URL] フィールドに、エンタープライズ PAC ファイルサーバの URL を入力します。Office 365 ブレークアウトルールは、エンタープライズ PAC ファイルに動的に修正されます。

サイトの PAC ファイルの動的カスタマイズを構成するには、[サイト]>[サイト]>[プロキシ自動構成設定] に移動します。また、グローバル PAC ファイルサーバの設定を上書きし、別の PAC ファイルサーバの URL を指定することもできます。

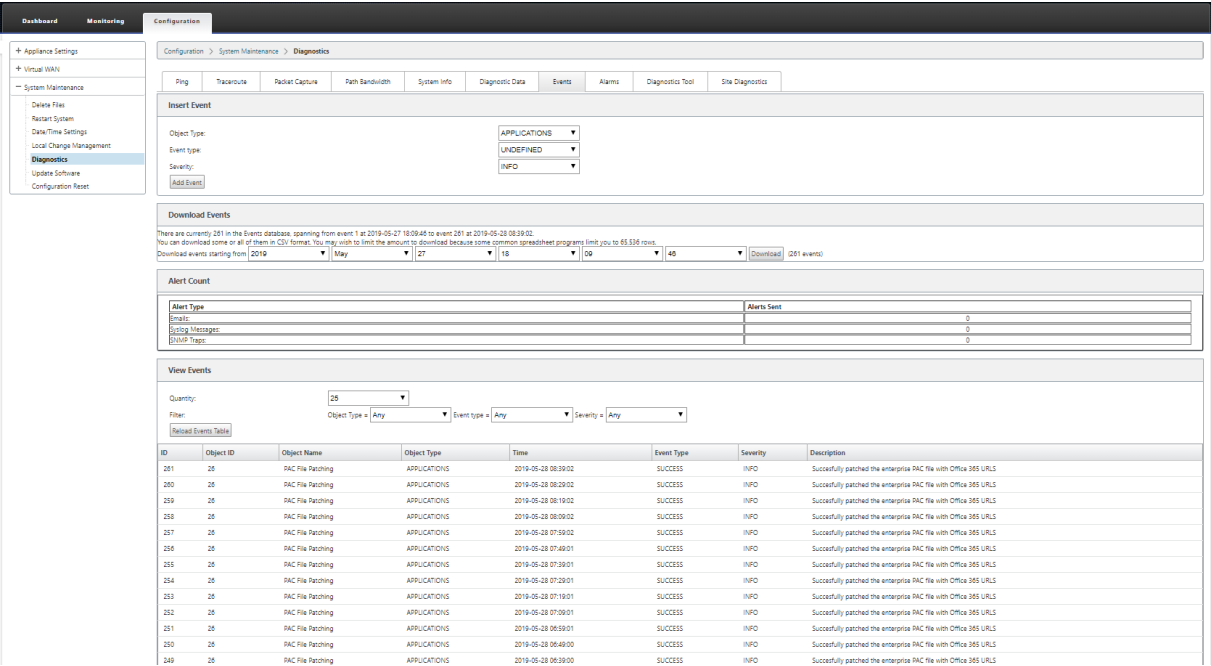


トラブルシューティング

カスタマイズした PAC ファイルは、Citrix SD-WAN アプライアンスからダウンロードしてトラブルシューティングを行うことができます。「構成」>「アプライアンスの設定」>「ログ/監視」>「アプリケーション」の順に選択し、「ダウンロード」をクリックします。



PAC ファイルのパッチ適用のステータスは、[イベント] セクションで表示し、[構成] > [システムメンテナンス] > [診断] の順に選択し、[イベント] タブをクリックします。



制限事項

- HTTPS PAC ファイルサーバー要求はサポートされていません。
- ルーティングドメインまたはセキュリティゾーンの PAC ファイルなど、ネットワーク内の複数の PAC ファイルはサポートされません。
- Citrix SD-WAN 上の PAC ファイルをゼロから生成することはできません。
- DHCP を介した WPAD はサポートされていません。

GRE トンネル

May 10, 2021

GRE トンネル機能を使用すると、LAN またはイントラネット上の GRE トンネルを終了するように Citrix SD-WAN アプライアンスを構成できます。サイトを GRE トンネル終端ノードとして設定しない場合は、この手順を省略して、[MCN サイトの WAN リンクの設定](#)に進んでください。

GRE トンネルを設定するには、次の手順を実行します。

新しい MCN サイトの [Sites] ビューで続行し、[**GRE Tun nels**] ラベルの左側にある [+] をクリックします。新しいサイトの **GRE** トンネル テーブルが開きます。詳細については、GRE のトピックを参照してください。

「[MCN サイトへの GRE トンネルの設定](#)」を参照してください。

「[ブランチサイトの GRE トンネルの設定](#)」を参照してください。

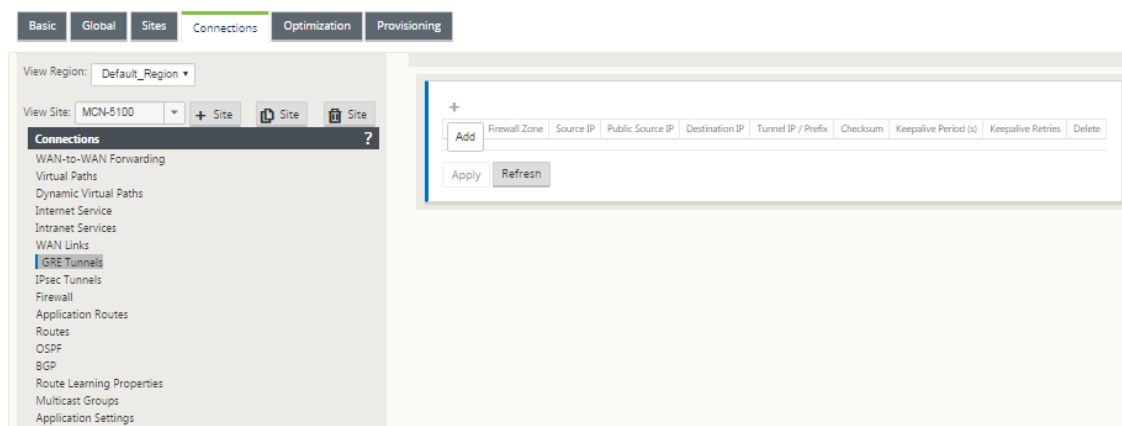
MCN サイトの GRE トンネルの設定（任意）

November 8, 2021

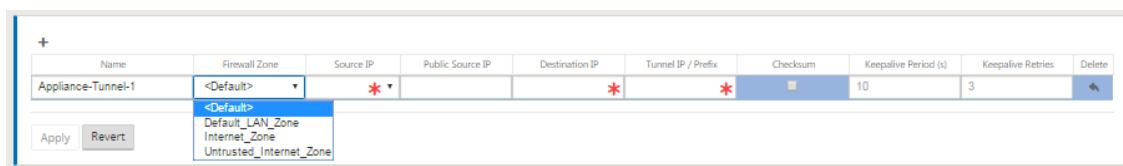
GRE トンネル機能を使用すると、LAN またはイントラネット上の GRE トンネルを終了するように Citrix SD-WAN アプライアンスを構成できます。このサイトを GRE トンネル終端ノードとして設定しない場合は、この手順をスキップして、[MCN サイトの WAN リンクの設定のセクションに進んでください](#)。

GRE トンネルを設定するには、次の手順を実行します。

1. 新しい MCN サイトの [接続] タブで続行し、[**GRE トンネル**] をクリックします。これにより、新しいサイトの **GRE** トンネル テーブルが開きます。



2. **GRE** トンネルの右側にある [+] をクリックします。これにより、新しい空の GRE トンネルエントリがテーブルに追加され、編集用が開きます。



3. GRE トンネルの設定を行います。

以下のコマンドを実行します。

- サービスタイプ-ドロップダウンリストからサービスタイプを [イントラネット] または [LAN] のいずれかを選択します。
- 名前:
 - サービスの種類が [イントラネット] の場合は、ドロップダウンメニューで構成されたイントラネットサービスのリストから選択します。

- サービスタイプが LAN の場合は、新しい GRE トンネルの名前を入力するか、デフォルトを受け入れます。
- デフォルトでは、名前付け形式が使用されます。**Appliance-Tunnel- <number>**-ここで、<number> は、このサイトに設定されている GRE トンネルの数を 1 増分したものです。
- イン트라ネットサービスタイプ-イン트라ネットサービスタイプの場合、ドロップダウンリストから [デフォルト] または [zScaler] を選択します。
- ファイアウォールゾーン -GRE トンネルのファイアウォールゾーンを選択します。
- **[Source IP]**: このフィールドのドロップダウンメニューからトンネルの送信元 IP アドレスを選択します。メニューオプションは、このサイトに対して構成されている仮想インターフェイスのリストです。GRE トンネルを設定する前に、少なくとも 1 つの仮想インターフェイスを設定してください。手順については、「[MCN サイトの仮想インターフェイスグループの構成](#)」および「[MCN サイトの仮想 IP アドレスの設定](#)」を参照してください。
- **Public Source IP**: GRE トンネル内のパケットの送信元アドレスとして使用する IP アドレスを入力します。送信元 IP アドレスは、GRE トンネルの始点です。
- **宛先 IP** -ホストの宛先として使用する IP アドレスを入力します。宛先 IP アドレスは、GRE トンネルのエンドポイントです。
- **[Tunnel IP/Prefix]**: GRE トンネルインターフェイスに使用する IP アドレスとプレフィックスを入力します。
- **[Checksum]**: ** トンネル GRE ヘッダーのチェックサムを有効にするには、[Checksum] ボックスを選択します。 **
- **[Keepalive Period]**: キープア ライブメッセージ間の待機時間 (秒単位) を入力します。0 に設定した場合、キープアライブパケットは送信されませんが、トンネルはアップしたままになります。デフォルトは 10 です。
- **[キープアライブの再試行 (Keepalive Retries)]**: 仮想 WAN アプライアンスがトンネルをダウンさせる前に試行する必要があるキープアライブの再試行回数を入力します。デフォルトは 3 です。

4. **[Apply]** をクリックします。これにより、設定が送信され、新しい GRE トンネルがテーブルに追加されます。

+									
Name	Firewall Zone	Source IP	Public Source IP	Destination IP	Tunnel IP / Prefix	Checksum	Keepalive Period (s)	Keepalive Retries	Delete
Appliance-Tunnel-1	Default_LAN_Zo	192.113.59.5	192.113.59.6	10.199.81.237	10.199.100.220	<input checked="" type="checkbox"/>	10	3	

Apply Revert

5. さらに多くの GRE トンネルを設定するには、**GRE** トンネルの右側にある **[+]** をクリックし、前の手順に従って進みます。

次のステップは、[MCN サイトの WAN リンクを設定すること](#)です。

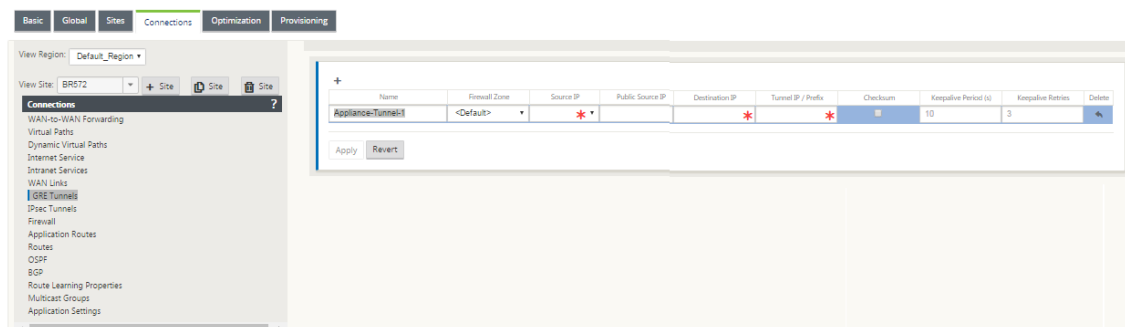
ブランチサイトの **GRE** トンネルの設定

November 8, 2021

GRE トンネル機能を使用すると、LAN またはイントラネット上の GRE トンネルを終了するように Citrix SD-WAN アプライアンスを構成できます。このブランチサイトを LAN GRE トンネル終端ノードとして設定しない場合は、この手順をスキップして、[ブランチサイトの WAN リンクの設定の項に進んでください](#)。

ブランチサイトの LAN GRE トンネルを設定するには、次の手順を実行します。

1. 新しいブランチサイトの接続ビューで続行し、[**GRE Tunnels**] をクリックします。新しいサイトの **GRE** トンネルビューが開きます。
2. [**GRE トンネル**] の右にある [+] をクリックします。これにより、新しい空の GRE トンネルエントリがテーブルに追加され、編集用に開きます。

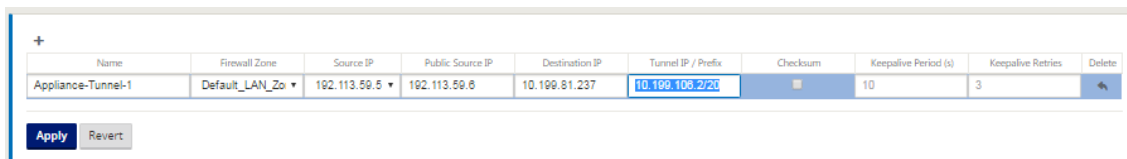


3. GRE トンネルの設定を行います。以下のコマンドを実行します。
 - サービスタイプ-ドロップダウンリストからサービスタイプを [イントラネット] または [LAN] のいずれかを選択します。
 - 名前:
 - サービスの種類が [イントラネット] の場合は、ドロップダウンメニューで構成されたイントラネットサービスのリストから選択します。
 - サービスタイプが LAN の場合は、新しい GRE トンネルの名前を入力するか、デフォルトを受け入れます。
 - デフォルトでは、名前付け形式が使用されます。 **Appliance-Tunnel- <number>**-ここで、<number> は、このサイトに設定されている GRE トンネルの数を 1 増分したものです。
 - イントラネットサービスタイプ-イントラネットサービスタイプの場合、ドロップダウンリストから [デフォルト] または [**zScaler**] を選択します。
 - ファイアウォールゾーン -GRE トンネルのファイアウォールゾーンを選択します。
 - [**Source IP**]: このフィールドのドロップダウンメニューからトンネルの送信元 IP アドレスを選択します。メニューオプションは、このサイト用に構成した仮想 IP アドレスのリストです。LAN GRE トン

ネルを設定する前に、少なくとも 1 つの仮想インターフェイスと 1 つの仮想 IP アドレスを設定してください。手順については、「[ブランチサイトの仮想インターフェイスグループの設定](#)」および「[ブランチサイトの仮想 IP アドレスの設定](#)」の項を参照してください。

- **Public Source IP** : GRE トンネル内のパケットの送信元アドレスとして使用する IP アドレスを入力します。送信元 IP アドレスは、GRE トンネルの始点です。
- 宛先 **IP** –ホストの宛先として使用する IP アドレスを入力します。宛先 IP アドレスは、GRE トンネルのエンドポイントです。
- **[Tunnel IP/Prefix]**: GRE トンネルインターフェイスに使用する IP アドレスとプレフィックスを入力します。
- **[Checksum]**: ** トンネル GRE ヘッダーのチェックサムを有効にするには、[Checksum] ボックスを選択します。 **
- **[Keepalive Per itods]**: キープアライブメッセージ間の待機時間（秒単位）を入力します。0 に設定した場合、キープアライブパケットは送信されませんが、トンネルはアップしたままになります。デフォルトは 10 です。
- **[キープアライブの再試行 (Keepalive Retries)]**: 仮想 WAN アプライアンスがトンネルをダウンさせる前に試行する必要があるキープアライブの再試行回数を入力します。デフォルトは 3 です。

4. **[Apply]** をクリックします。これにより、設定が送信され、新しい GRE トンネルエントリがテーブルに追加されます。



Name	Firewall Zone	Source IP	Public Source IP	Destination IP	Tunnel IP / Prefix	Checksum	Keepalive Period (s)	Keepalive Retries	Delete
Appliance-Tunnel-1	Default_LAN_Zo	192.113.59.5	192.113.59.6	10.199.81.237	10.199.106.2/20	<input checked="" type="checkbox"/>	10	3	

Apply Revert

5. さらに多くの GRE トンネルを設定するには、**[GRE Tunnels]** ラベルの右側にある **[+]** をクリックし、前の手順に従って進みます。

次のステップは、[ブランチサイトの WAN リンクを設定すること](#)です。

帯域内およびバックアップ管理

February 8, 2022

帯域内管理

Citrix SD-WAN では、帯域外管理と帯域内管理の 2 つの方法で SD-WAN アプライアンスを管理できます。アウトオブバンド管理では、管理トラフィックだけを伝送する管理用に予約されたポートを使用して管理 IP を作成できます。

インバンド管理では、SD-WAN データポートを管理に使用できます。追加の管理パスを設定することなく、データトラフィックと管理トラフィックの両方を伝送します。

インバンド管理では、仮想 IP アドレスが Web UI や SSH などの管理サービスに接続できます。IP サービスに使用できるように有効になっている複数の信頼できるインターフェイスで、インバンド管理を有効にできます。管理 IP とインバンド仮想 IP を使用して、Web UI と SSH にアクセスできます。

Citrix SD-WAN 11.4.2 リリース以降、SD-WAN アプライアンスでインバンド管理を構成し、インバンド管理ポートを介して Citrix SD-WAN Orchestrator サービスへの接続を確立する必要があります。そうしないと、管理ポートが接続されておらず、インバンド IP アドレスも構成されていないと、アプライアンスは Citrix SD-WAN Orchestrator サービスへの接続を失います。

注

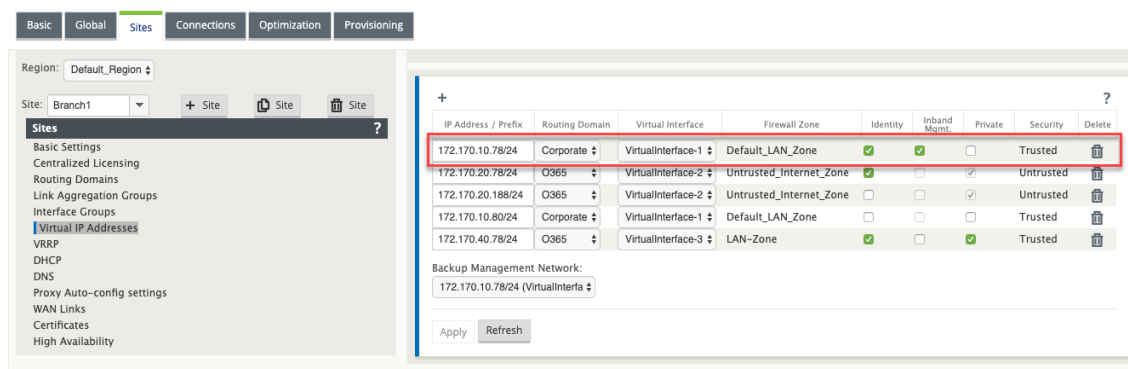
- Citrix SD-WAN Center は、帯域内管理による高可用性アプライアンスへの接続をサポートしていません。
- サービスタイプを【任意】に設定できるのは、MCN 設定エディタだけです。Citrix SD-WAN Orchestrator サービスでは、宛先 NAT ポリシーのサービスタイプを【任意】に設定できません。
- 管理接続だけがインバンド HA の場合、サービスを無効にしないでください。
サービスを無効にすると、アプライアンスからロックアウトできます。

仮想 IP で帯域内管理を有効にするには、次の手順を実行します。

1. 構成エディタで、[サイト] > [仮想 IP アドレス] に移動します。
2. インバンド管理を有効にする仮想 IP に対して [インバンド管理 (Inband Mgmt)] を選択します。

注:

インターフェイスのセキュリティタイプが [**Trusted**] で、[**Identity**] が有効になっていることを確認します。



3. [適用] をクリックします。

仮想 IP アドレスの構成手順の詳細については、「[仮想 IP を構成する方法](#)」を参照してください。

Citrix SD-WAN 11.3.1 リリース以降、帯域内管理は高可用性アプライアンスのペアをサポートします。プライマリアプライアンスとセカンダリアプライアンスの間の通信は、NAT を使用する仮想インターフェイスを介して行われます。

次のポートは、HA アプライアンスの管理サービスとの通信を可能にします。

- HTTPS
 - 443-アクティブな HA に接続する
 - 444-HA プライマリにリダイレクト
 - 445-HA セカンダリにリダイレクト
- SSH
 - 22-アクティブな HA に接続する
 - 23-HA プライマリにリダイレクト
 - 24-HA セカンダリにリダイレクト
- SNMP
 - 161-アクティブな HA に接続する
 - 162-HA プライマリにリダイレクト
 - 163-HA セカンダリにリダイレクト

宛先 NAT ポリシーを使用して、ポートを入力せずにインバンド HA への接続を可能にする IP アドレスを作成します。

たとえば、アプライアンスへのアクセスには、次のインバンド IP アドレスが使用されます。

- アクティブなアプライアンス-1.0.1.2
- プライマリアプライアンス-1.0.1.10
- セカンダリアプライアンス-1.0.1.11

帯域内管理仮想 IP アドレスと同じネットワークにある 2 つの新しい仮想 IP アドレスを作成します。この例では、1.0.1.2/24 がインバンド管理仮想 IP アドレスで、1.0.1.2/24 がバックアップネットワークとして選択されます。1.0.1.10 と 1.0.1.11 は、作成される新しい仮想 IP アドレスです。1.0.1.10 はプライマリアプライアンスへのアクセスに使用され、1.0.1.11 はセカンダリアプライアンスへのアクセスに使用されます。

Basic Global **Sites** Connections Optimization Provisioning

Region: Default_Region

Site: DC + Site Site Site

Sites ?

- Basic Settings
- Centralized Licensing
- Routing Domains
- Link Aggregation Groups
- Interface Groups
- Virtual IP Addresses**
- VRRP
- DHCP
- DNS
- Proxy Auto-config settings
- NDP Router Advertisement
- Prefix Delegation Group
- WAN Links
- Certificates
- High Availability

Section: IPv4

IP Address / Prefix	Virtual Interface	Firewall Zone	Identity	Inband Mgmt.	Private	Security	Delete
1.0.0.2/24	E1Vlan0	Default_LAN_Zone	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Trusted	
1.0.1.2/24	E2Vlan0	Default_LAN_Zone	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Trusted	
6.0.0.1/24	E3Vlan0	Default_LAN_Zone	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Trusted	
1.0.1.11/24	E2Vlan0	Default_LAN_Zone	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Trusted	
1.0.1.10/24	E2Vlan0	Default_LAN_Zone	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Trusted	

Backup Management Network: 1.0.1.2/24 (E2Vlan0) DNS Proxy Name:

Apply Refresh

宛先 NAT ポリシーを作成します。6 つの DNAT ポリシーは、サービスのベースポートを適切なインバンド HA ポートにリダイレクトします。設定を適用すると、内部 IP アドレスを使用してプライマリおよびセカンダリアプライアンスに直接アクセスできます。

Basic Global Sites **Connections** Optimization Provisioning

Region: Default_Region

Site: DC + Site Site Site

Connections ?

- WAN-to-WAN Forwarding
- Virtual Paths
- Dynamic Virtual Paths
- Internet Service
- Intranet Services
- WAN Links
- GRE Tunnels
- IPsec Tunnels
- Firewall**
- Application Routes
- Routes
- OSPF
- BGP
- Route Learning Properties
- Inter Routing Domain Services
- Multicast Groups
- Applications

Section: Destination NAT Policies

Priority	Direction	Service	Inside IP Address	Inside Port	Outside IP Address	Outside Port	Edit	Delete	Clone
100	Inbound	Any	1.0.1.10/32	443	1.0.1.2	444			
200	Inbound	Any	1.0.1.11/32	443	1.0.1.2	445			
300	Inbound	Any	1.0.1.10/32	22	1.0.1.2	23			
400	Inbound	Any	1.0.1.11/32	22	1.0.1.2	24			
500	Inbound	Any	1.0.1.10/32	161	1.0.1.2	162			
600	Inbound	Any	1.0.1.11/32	161	1.0.1.2	163			

Apply Refresh

帯域内管理のモニタリング

前の例では、172.170.10.78 仮想 IP でインバンド管理を有効にしました。この IP を使用して、Web UI と SSH にアクセスできます。

Web UI で、[モニタリング] > [ファイアウォール] に移動します。ポート 22 および 443 の仮想 IP を使用してアクセスする SSH および Web UI が [宛先 IP アドレス] 列に表示されます。

The screenshot displays the 'Firewall Statistics' page in the Citrix SD-WAN 11.4 web interface. The 'Connections' table is visible, showing various network connections. The 'Destination IP' field is highlighted with a red box, indicating the IP address '172.170.10.78'.

Routing Domain	Application	Family	IP Protocol	IP Address	Port	Service Type	Service Name	Zone	Destination IP Address	Port	Service Type	Service Name	Zone	State	Is NAT	Packets	Bytes	PPS	kbps	Received		
Corporate	Secure Shell(ssh)	Encrypted	TCP	172.170.10.135	54257	Local	VirtualInterface-1	Default_LAN_Zone	172.170.10.78	22	IPHost	-	Default_LAN_Zone	ESTABLISHED	No	78	6824	0.364	0.295	53	7429	0.247
Corporate	HyperText Transfer Protocol Secure(https)	Web	TCP	172.170.10.135	54298	Local	VirtualInterface-1	Default_LAN_Zone	172.170.10.78	443	IPHost	-	Default_LAN_Zone	ESTABLISHED	No	129	10130	5.692	3.319	234	338238	9.583
Corporate	HyperText Transfer Protocol Secure(https)	Web	TCP	172.170.10.135	54299	Local	VirtualInterface-1	Default_LAN_Zone	172.170.10.78	443	IPHost	-	Default_LAN_Zone	ESTABLISHED	No	565	28811	23.147	9.443	1087	1594099	44.533
Corporate	HyperText Transfer Protocol Secure(https)	Web	TCP	172.170.10.135	54300	Local	VirtualInterface-1	Default_LAN_Zone	172.170.10.78	443	IPHost	-	Default_LAN_Zone	ESTABLISHED	No	90	9201	3.691	3.019	157	212744	6.439
Corporate	HyperText Transfer Protocol Secure(https)	Web	TCP	172.170.10.135	54301	Local	VirtualInterface-1	Default_LAN_Zone	172.170.10.78	443	IPHost	-	Default_LAN_Zone	ESTABLISHED	No	111	7987	4.554	2.621	202	291743	8.287
Corporate	HyperText Transfer Protocol Secure(https)	Web	TCP	172.170.10.135	54302	Local	VirtualInterface-1	Default_LAN_Zone	172.170.10.78	443	IPHost	-	Default_LAN_Zone	CLOSED	No	6	776	0.419	0.434	4	309	0.280
Corporate	HyperText Transfer Protocol Secure(https)	Web	TCP	172.170.10.135	54303	Local	VirtualInterface-1	Default_LAN_Zone	172.170.10.78	443	IPHost	-	Default_LAN_Zone	CLOSED	No	6	776	0.422	0.437	4	309	0.282
Corporate	HyperText Transfer Protocol Secure(https)	Web	TCP	172.170.10.135	54289	Local	VirtualInterface-1	Default_LAN_Zone	172.170.10.78	443	IPHost	-	Default_LAN_Zone	CLOSED	No	355	20266	13.558	10.878	1666	13982449	25.435

注

インバンド管理は、次の SD-WAN アプライアンスではサポートされていません。

- Citrix SD-WAN 1000 SE/PE
- Citrix SD-WAN 2000 SE/PE
- Citrix SD-WAN 4000 SE

帯域内 Provisioning

SD-WAN アプライアンスを家庭や小規模の支店などのシンプルな環境に導入する必要性が大幅に高まっています。シンプルな展開のために個別の管理アクセスを構成すると、オーバーヘッドが増えます。帯域内管理機能とともにゼロタッチ導入により、指定されたデータポートを介したプロビジョニングと構成管理が可能になります。ゼロタッチ配置は、指定されたデータポートでサポートされ、ゼロタッチ配置用に別の管理ポートを使用する必要はありません。また、Citrix SD-WAN では、データポートがダウンした場合に、管理トラフィックを管理ポートにシームレスにフェイルオーバーできます。

帯域内 Provisioning をサポートする工場出荷状態のアプライアンスは、データまたは管理ポートをインターネットに接続するだけでプロビジョニングできます。インバンド Provisioning をサポートするアプライアンスには、LAN および WAN 用の特定のポートがあります。工場出荷時リセット状態のアプライアンスには、ゼロタッチデプロイメントサービスとの接続を確立できるデフォルト設定があります。LAN ポートは DHCP サーバーとして機能し、DHCP クライアントとして機能する WAN ポートにダイナミック IP を割り当てます。WAN リンクは、Quad 9 DNS サービスを監視して WAN 接続を決定します。

注

インバンド Provisioning は、SD-WAN 110 SE および SD-WAN VPX プラットフォームにのみ適用されます。

IP アドレスが取得され、ゼロタッチ展開サービスとの接続が確立されると、構成パッケージがダウンロードされ、アプライアンスにインストールされます。SD-WAN Center によるゼロタッチ展開の詳細については、[ゼロタッチ展開を参照してください](#)。SD-WAN Orchestrator によるゼロタッチ展開の詳細については、[ゼロタッチ展開を参照してください](#)。

注: データポートを介した SD-WAN アプライアンスのプロビジョニングの日数では、アプライアンスソフトウェアのバージョンは SD-WAN 11.1.0 以降である必要があります。

工場出荷時リセット状態のアプライアンスのデフォルト設定には、次の設定が含まれます。

- LAN ポート上の DHCP サーバ
- WAN ポート上の DHCP クライアント
- DNS の QUAD9 構成
- デフォルトの LAN IP は 192.168.0.1 です。
- 35 日間の猶予ライセンス

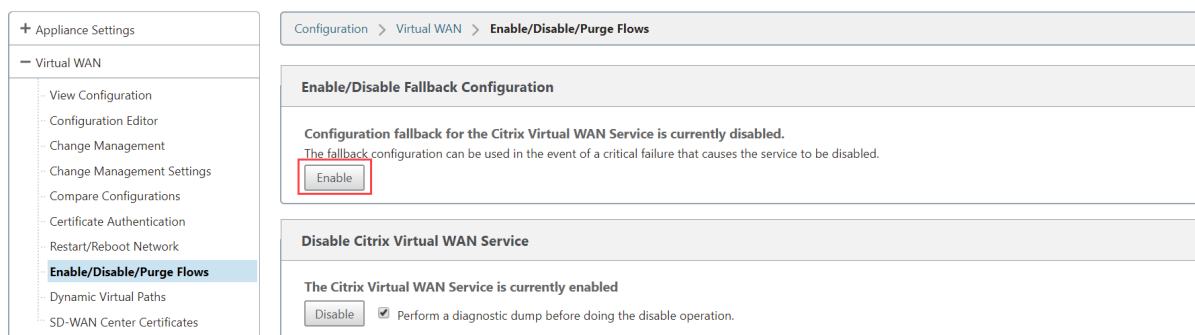
アプライアンスがプロビジョニングされると、デフォルトの設定は無効になり、ゼロタッチデプロイメントサービスから受信した設定によって上書きされます。アプライアンスのライセンスまたは猶予ライセンスの有効期限が切れると、デフォルト構成がアクティブになります。これにより、アプライアンスはゼロタッチデプロイメントサービスに接続したままになり、ゼロタッチデプロイメントで管理されたライセンスを受け取ることができます。

デフォルト/フォールバック構成

フォールバック構成により、リンク障害、構成の不一致、またはソフトウェアの不一致が発生しても、アプライアンスはゼロタッチ展開サービスに接続したままになります。フォールバック構成は、デフォルト構成プロファイルを持つアプライアンスではデフォルトで有効になっています。また、既存の LAN ネットワーク設定に従ってフォールバック構成を編集することもできます。

注: 最初のアプライアンスを Provisioning した後、フォールバック構成でゼロタッチデプロイメントサービス接続が有効になっていることを確認します。

フォールバック構成が無効になっている場合は、[構成] > [アプライアンス設定] > [デフォルト/フォールバック構成 **] > [有効] をクリックして、フォールバック構成を有効にできます **。



次の表に、異なるプラットフォームでのフォールバック構成用に事前に指定された WAN ポートおよび LAN ポートの詳細を示します。

プラットフォーム	WAN ポート	LAN ポート
110	1/2	1/1
110-LTE	1/2、LTE-1	1/1
210	1/4, 1/5	1/3
210-LTE	1/4, 1/5, LTE-1	1/3
VPX	2	1
410	1/4, 1/5, 1/6	1/3 (FTB)
1100	1/4, 1/5, 1/6	1/3 (FTB)

Citrix SD-WAN 11.3.1 リリースからは、WAN ポートの設定を構成できます。WAN ポートは、DHCP クライアントを使用して独立した WAN リンクとして構成し、Quad9 DNS サービスを監視して WAN 接続を特定できます。DHCP がない場合、WAN ポートに WAN IP/スタティック IP を設定して、初期プロビジョニングにインバンド管理を使用できます。

注:

スタティック IP を使用してイーサネットポートだけを設定できます。スタティック IP は、LTE-1 ポートおよび LTE-E1 ポートでは設定できません。LTE-1 ポートと LTE-E1 ポートを WAN として追加できますが、設定フィールドは編集できません。

WAN ポートを追加すると、そのポートは [**WAN 設定 (ポート:2)**] セクションの下に追加されます。[**DHCP モード**] チェックボックスは既定でオンになっています。[**DHCP Mode**] チェックボックスをオンにすると、[**IP アドレス**]、[**Gateway IP アドレス**]、および [**VLAN ID**] テキストフィールドはグレー表示されます。スタティック IP を設定する場合は、[**DHCP Mode**] チェックボックスをオフにします。

WAN Settings (Ports: 2)				
Port	DHCP Mode	IP Address	Gateway IP Address	VLAN ID
2	<input type="checkbox"/>	11.11.11.10/24	11.11.11.11	50
4	<input checked="" type="checkbox"/>			
5	<input checked="" type="checkbox"/>			
				Wan Tracking IP Address
				9.9.9.9
				9.9.9.9

デフォルトでは、[**WAN トラッキング IP アドレス**] フィールドには 9.9.9.9 が自動的に入力されます。必要に応じて住所を変更できます。

注:

[動的 **DNS** サーバー] チェックボックスをオンにする場合は、[**DHCP モード**] を選択した状態で、少なくとも 1 つの WAN ポートを追加または構成してください。

LAN ネットワークに従ってフォールバック構成をカスタマイズするには、次の手順を実行します。

1. [構成] > [アプライアンス設定] > [デフォルト/フォールバック構成] に移動します。
2. ネットワーク要件に従って、次の LAN 設定の値を編集します。これは、ゼロタッチ展開サービスとの接続を確立するために必要な最小構成です。

- **VLAN ID:** LAN ポートをグループ化する必要がある VLAN ID。
- **IP アドレス:** LAN ポートに割り当てられた仮想 IP アドレス。
- **DHCP 有効:** LAN ポートを DHCP サーバとして有効にします。DHCP サーバは、LAN ポート上のクライアントにダイナミック IP アドレスを割り当てます。
- **DHCP 開始および DHCP 終了:** DHCP が LAN ポート上のクライアントに IP を動的に割り当てるために使用する IP アドレスの範囲。
- **DNS サーバー:** プライマリ DNS サーバーの IP アドレス。
- **代替 DNS サーバー:** セカンダリ DNS サーバーの IP アドレス。
- **インターネットアクセス:** 他のフィルタリングを行わずに、すべての LAN クライアントへのインターネットアクセスを許可します。

Fallback Configuration

The fallback configuration provides basic network functionality when a critical failure occurs and the system can no longer function.

WAN Settings (Ports: 1)

WAN settings are currently not configurable. WAN ports are configured as independent WAN Links using DHCP client and monitor the Quad9 DNS service to determine WAN connectivity.

LAN Settings (Ports: 2)

VLAN ID:
IP Address:
DHCP Enabled: ☐
DHCP Start:
DHCP End:
DNS Server:
Alt DNS Server:
Internet Access: ☐ ?

Port Settings

Port Name	Mode		
1	<input checked="" type="radio"/> WAN	<input type="radio"/> LAN	<input type="radio"/> Disabled
2	<input type="radio"/> WAN	<input checked="" type="radio"/> LAN	<input type="radio"/> Disabled
3	<input type="radio"/> WAN	<input type="radio"/> LAN	<input checked="" type="radio"/> Disabled
4	<input type="radio"/> WAN	<input type="radio"/> LAN	<input checked="" type="radio"/> Disabled
5	<input type="radio"/> WAN	<input type="radio"/> LAN	<input checked="" type="radio"/> Disabled
6	<input type="radio"/> WAN	<input type="radio"/> LAN	<input checked="" type="radio"/> Disabled
7	<input type="radio"/> WAN	<input type="radio"/> LAN	<input checked="" type="radio"/> Disabled
8	<input type="radio"/> WAN	<input type="radio"/> LAN	<input checked="" type="radio"/> Disabled

Unassigned Port Bypass Mode:

Apply

3. 各ポートのモードを設定します。ポートは、LAN ポートまたは WAN ポートのどちらでもかまいません。また、無効にすることもできます。表示されるポートは、アプライアンスのモデルによって異なります。また、

ポートバイパスモードを **Fail-to-Block** または **Fail-to-Wire** に設定します。

フォールバック設定をデフォルト設定にリセットするには、[**Reset**] をクリックします。

注

フォールバック設定は、次の SD-WAN アプライアンスではサポートされていません。

- Citrix SD-WAN 1000 SE/PE
- Citrix SD-WAN 2000 SE/PE
- Citrix SD-WAN 4000 SE

構成可能な管理ポートまたはデータポート

インバンド管理により、データポートはデータトラフィックと管理トラフィックの両方を伝送できるため、専用の管理ポートは不要です。これにより、すでにポート密度が低いローエンドアプライアンスでは管理ポートが使用されな
いままになります。Citrix SD-WAN を使用すると、管理ポートをデータポートまたは管理ポートとして動作するよう
に構成できます。

注

管理ポートをデータポートに変換できるのは、次のプラットフォームだけです。

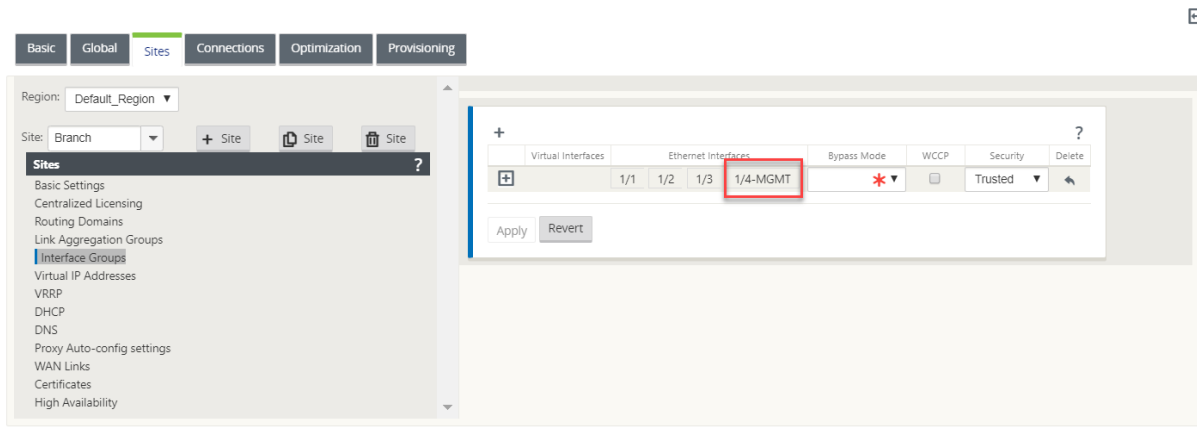
- Citrix SD-WAN 110 SE/LTE
- Citrix SD-WAN 210 SE/LTE

設定エディタで、設定内の管理ポートを使用します。構成がアクティブになると、管理ポートはデータポートに変換
されます。

注

管理ポートを設定できるのは、アプライアンスの他の信頼できるインターフェイスでインバンド管理が有効に
なっている場合だけです。

管理インターフェイスを設定するには、構成エディタで [サイト] に移動し、サイトを選択して [インターフェイスグ
ループ] をクリックします。MGMT インターフェイスは設定可能です。インターフェイスグループの設定の詳細につ
いては、「[インターフェイスグループの設定方法](#)」を参照してください。



管理機能を実行するように管理ポートを再設定するには、設定を削除します。管理ポートを使用せずに構成を作成し、アクティブにします。

バックアップ管理ネットワーク

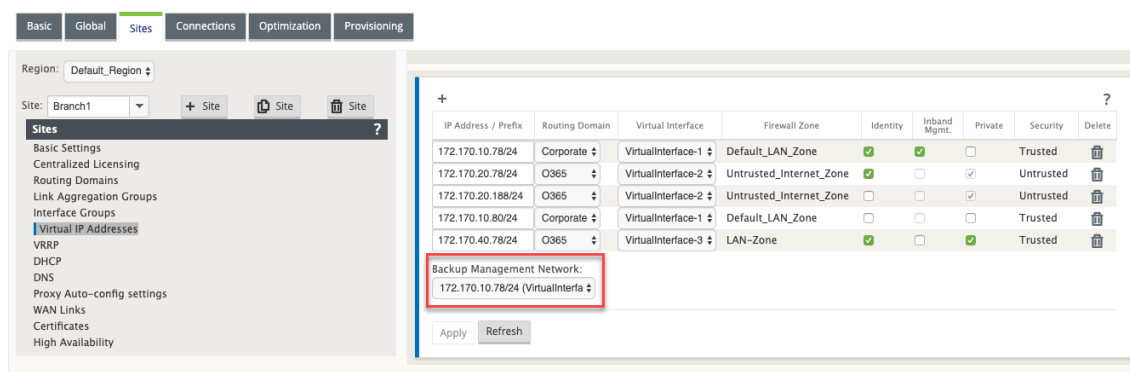
仮想 IP アドレスをバックアップ管理ネットワークとして設定できます。管理ポートにデフォルト Gateway が設定されていない場合、管理 IP アドレスとして使用されます。

注

サイトに 1 つのルーティングドメインで構成されたインターネットサービスがある場合、ID が有効な信頼できるインターフェイスが既定でバックアップ管理ネットワークとして選択されます。

仮想 IP をバックアップ管理ネットワークとして選択するには、以下の手順に従ってください。

1. 構成エディタで、[サイト] > [仮想 IP アドレス] に移動します。
2. バックアップ管理ネットワークとして仮想 IP アドレスを選択します。



3. インバンドおよびバックアップ管理プレーンを介したすべての DNS 要求の転送先の DNS プロキシを選択します。

注

DNS プロキシは、インバンド管理とバックアップ管理ネットワークの両方が仮想 IP に対して有効になっている場合にのみ選択できます。

4. [適用] をクリックします。

仮想 IP アドレスの構成手順の詳細については、「[仮想 IP アドレスの構成方法](#)」を参照してください。

バックアップ管理の監視

前の例では、バックアップ管理ネットワークとして 172.170.10.78 の仮想 IP を選択しています。管理 IP アドレスがデフォルト Gateway で設定されていない場合は、この IP を使用して Web UI と SSH にアクセスできます。

Web UI で、[モニタリング]>[ファイアウォール]に移動します。この仮想 IP アドレスは、SSH および Web UI アクセスの送信元 IP アドレスとして確認できます。

Monitoring > Firewall

Firewall Statistics

Statistics:

Connections

Maximum entries to display:

50

Filtering:

Routing Domain:

Any

Application:

Any

Family:

Any

IP Protocol:

Any

Source Zone:

Any

Destination Zone:

Any

Source Service Type:

Any

Source Service Instance:

Any

Source IP:

172.170.10.78

Source Port:

*

Destination Service Type:

Any

Destination Service Instance:

Any

Destination IP:

*

Destination Port:

*

Refresh

Clear Connections

Help

Show latest data

Show Drops

Connections

Routing Domain	Application	Family	IP Protocol	Source				Destination				State	Is NAT	Sent			Received					
				IP Address	Port	Service Type	Service Name	Zone	IP Address	Port	Service Type	Service Name	Zone	Packets	Bytes	PPS	Packets	Bytes	PPS			
Corporate	Transmission Control Protocol(Tcp)	Network Service	TCP	172.170.10.78	49818	IPHost	-	Default_LAN_Zone	18.210.2.11	443	Internet	Branch1-Internet	Untrusted_Internet_Zone	SYN_SENT	Yes	1	60	-	-	0	0	-
Corporate	Domain Name Service(dns)	Network Service	UDP	172.170.10.78	58939	IPHost	-	Default_LAN_Zone	10.105.147.14	53	Internet	Branch1-Internet	Untrusted_Internet_Zone	NEW	Yes	2	148	-	-	0	0	-
Corporate	Domain Name Service(dns)	Network Service	UDP	172.170.10.78	43012	IPHost	-	Default_LAN_Zone	10.105.147.14	53	Internet	Branch1-Internet	Untrusted_Internet_Zone	ESTABLISHED	Yes	2	168	0.070	0.047	2	297	0.070
Corporate	Domain Name Service(dns)	Network Service	UDP	172.170.10.78	36558	IPHost	-	Default_LAN_Zone	10.105.147.14	53	Internet	Branch1-Internet	Untrusted_Internet_Zone	ESTABLISHED	Yes	2	148	0.011	0.007	2	277	0.011
Corporate	HyperText Transfer Protocol Secure(https)	Web	TCP	172.170.10.78	60824	IPHost	-	Default_LAN_Zone	18.235.40.8	443	Internet	Branch1-Internet	Untrusted_Internet_Zone	ESTABLISHED	Yes	9	1271	0.176	0.199	7	4069	0.137
Corporate	Domain Name Service(dns)	Network Service	UDP	172.170.10.78	60585	IPHost	-	Default_LAN_Zone	10.105.147.14	53	Internet	Branch1-Internet	Untrusted_Internet_Zone	ESTABLISHED	Yes	1	80	0.003	0.002	1	128	0.002
Corporate	Domain Name Service(dns)	Network Service	UDP	172.170.10.78	58010	IPHost	-	Default_LAN_Zone	10.105.147.14	53	Internet	Branch1-Internet	Untrusted_Internet_Zone	ESTABLISHED	Yes	1	80	0.020	0.013	1	80	0.020
Corporate	Domain Name Service(dns)	Network Service	UDP	172.170.10.78	36684	IPHost	-	Default_LAN_Zone	10.105.147.14	53	Internet	Branch1-Internet	Untrusted_Internet_Zone	ESTABLISHED	Yes	1	80	0.006	0.004	1	161	0.006
Corporate	Domain Name Service(dns)	Network Service	UDP	172.170.10.78	33173	IPHost	-	Default_LAN_Zone	10.105.147.14	53	Internet	Branch1-Internet	Untrusted_Internet_Zone	ESTABLISHED	Yes	1	80	0.003	0.002	1	80	0.003
Corporate	Domain Name Service(dns)	Network Service	UDP	172.170.10.78	53914	IPHost	-	Default_LAN_Zone	10.105.147.14	53	Internet	Branch1-Internet	Untrusted_Internet_Zone	ESTABLISHED	Yes	1	80	0.006	0.004	1	128	0.006
Corporate	Domain Name Service(dns)	Network Service	UDP	172.170.10.78	53708	IPHost	-	Default_LAN_Zone	10.105.147.14	53	Internet	Branch1-Internet	Untrusted_Internet_Zone	ESTABLISHED	Yes	2	128	0.013	0.006	2	144	0.013
Corporate	Domain Name Service(dns)	Network Service	UDP	172.170.10.78	43704	IPHost	-	Default_LAN_Zone	10.105.147.14	53	Internet	Branch1-Internet	Untrusted_Internet_Zone	ESTABLISHED	Yes	1	80	0.003	0.002	1	128	0.003

インターネットアクセス

May 10, 2021

インターネットサービスは、エンドユーザーサイトとパブリックインターネット上のサイト間のトラフィックに使用されます。インターネットサービストラフィックはSD-WANによってカプセル化されず、仮想パスサービスを通して配信されるトラフィックと同じ機能を持ちません。ただし、SD-WANでこのトラフィックを分類し、考慮することが重要です。インターネットサービスとして識別されるトラフィックにより、管理者が設定した構成に従って、仮

想パスおよびイントラネットトラフィックを介して配信されるトラフィックに対するインターネットトラフィックのレート制限によって、SD-WAN のリンク帯域幅をアクティブに管理できるようになります。SD-WAN には、帯域幅の Provisioning 機能に加えて、複数のインターネット WAN リンクを使用してインターネットサービス経由で配信されるトラフィックの負荷分散機能が追加されています。また、プライマリまたはセカンダリ構成でインターネット WAN リンクを使用することもできます。

SD-WAN アプライアンスの Internet Service を使用したインターネットトラフィック制御は、次の展開モードで構成できます。

- 統合ファイアウォールを使用したブランチでの直接インターネットブレイクアウト
- Secure Web Gateway への支店転送での直接インターネットブレイクアウト
- インターネットからデータセンター MCN へのバックホール

Internet Traffic Control

Direct Internet Breakout at Branch with Integrated Firewall



Direct Internet Breakout at Branch with forwarding to Secure Web Gateway



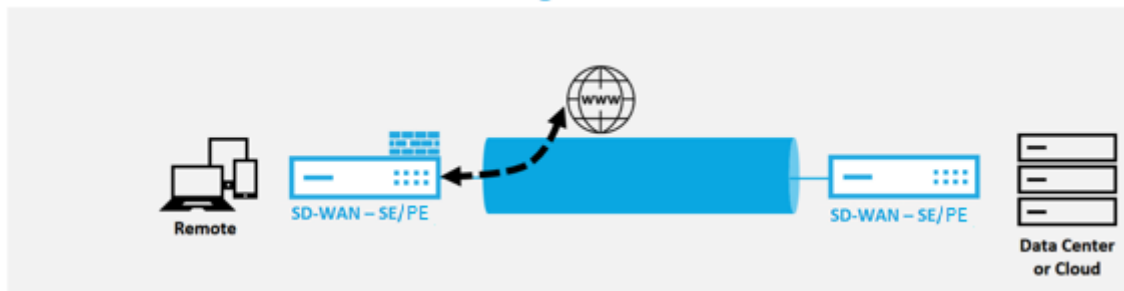
Backhaul Internet to Data Center MCN



統合ファイアウォールを使用したブランチでの直接インターネットブレイクアウト

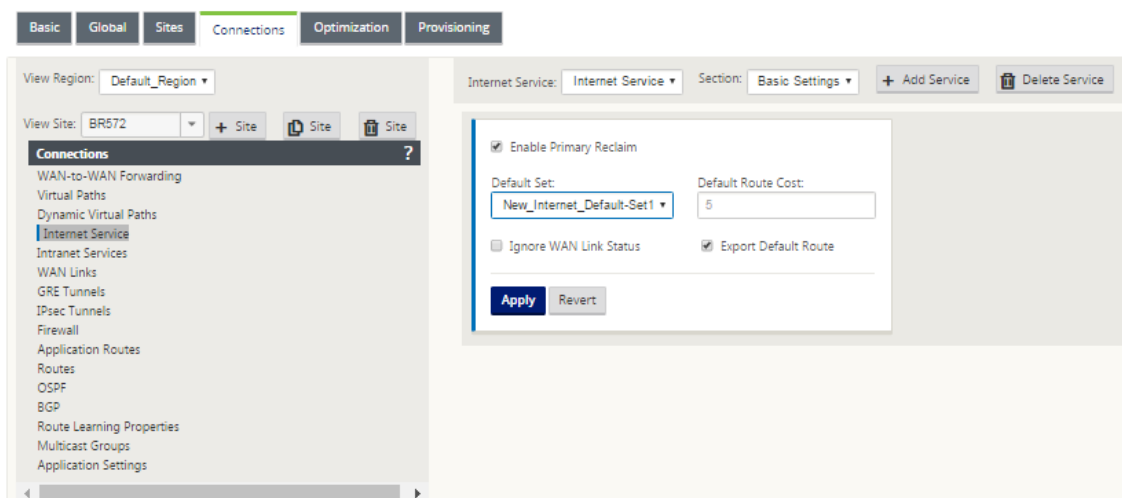
May 10, 2021

Direct Internet Breakout at Branch with Integrated Firewall

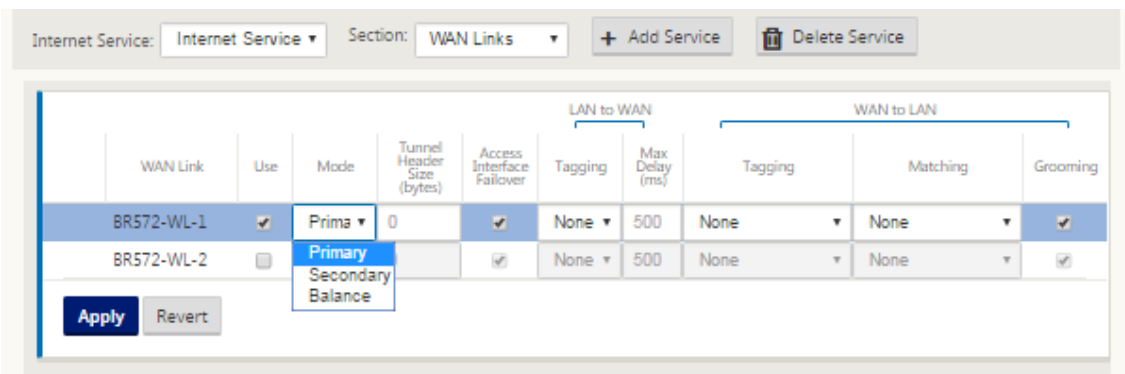


任意のサイト（クライアントノードまたは MCN）でインターネットサービスを有効にするには、次の手順を実行します。

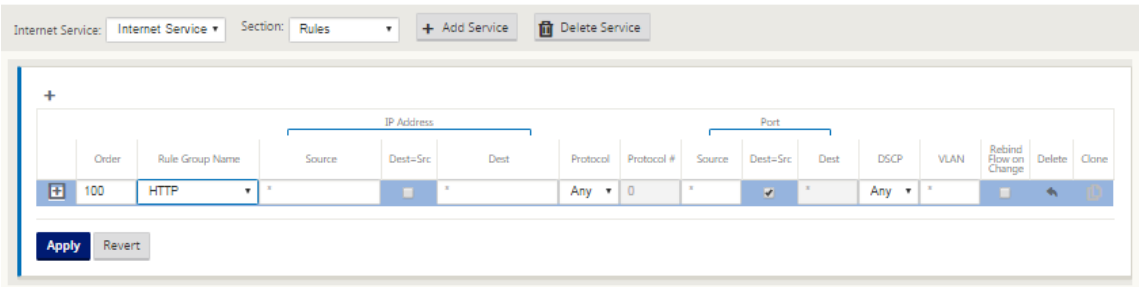
1. 構成エディタで、[接続] タイルに移動します。追加 (+) アイコンをクリックして、そのサイトのインターネットサービスを追加します。サイトごとに作成できるインターネットサービスは 1 つだけです。
2. [インターネットサービスの 基本設定] には、WAN リンクが使用できないときにインターネットサービスをどのように動作させるかに関するオプションがいくつかあります。インターネットデフォルトセットは、インターネットサービスを有効にした構成内の任意のノードに適用できる規則のセットを使用して、グローバルタイルで定義できます。これにより、各ノードを個別に構成することなく、インターネットサービスの管理を一元的に制御できます。



3. [インターネットサービス WAN リンク] ノードでは、[サイト] タイルに構築された WAN リンクを使用して、インターネットトラフィックに使用する WAN リンクを選択できます。他のオプションに加えて、[プライマリ]、[セカンダリ]、[バランス] の各モードも使用できます。これにより、管理者は利用可能な WAN リンクを同時に使用することも、アクティブ/パッシブ役割で使用することもできます。



4. サイトノード固有のルールが使用可能で、グローバルデフォルトセットで構成された一般設定を一意に上書きして、各サイトのカスタマイズ機能を有効にします。モードには、特定の WAN リンクを介した目的の配信や、フィルタリングされたトラフィックのパススルーまたは廃棄を可能にするオーバーライドサービスとしての配信が含まれます。

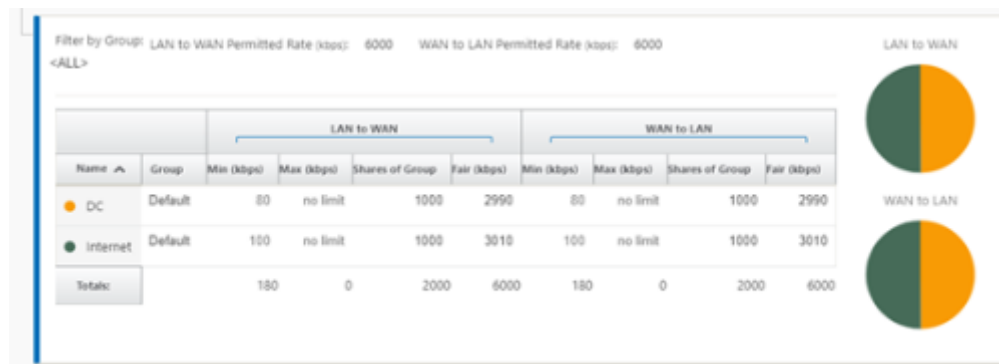


ノードに対してインターネットサービスが作成されると、その特定のノードのルートテーブルが自動的に更新され、サービスタイプに等しいインターネット、ルートコストが5のルート 0.0.0.0/0 ルートで更新されます。そうでない場合は、サービスタイプとしてパススルーを使用したコスト 16 のデフォルトルートが制定され、インターネットトラフィックは配線するアンダーレイネットワークに引き渡される。

Order	Network IP Address	Cost	Service Type	Service Name	Gateway IP Address	Info	Edit	Delete
1	172.16.100.2/24	5	Local			①		
2	172.16.200.2/24	5	Local			①		
3	172.16.30.2/24	5	Local			①		
4	192.168.10.2/24	5	Local			①		
5	0.0.0.0/0	5	Internet			①		
6	0.0.0.0/0	16	Passthrough			①		

サイトノードでインターネットサービスを有効にすると、[プロビジョニング] タイルが使用可能になります。これにより、WAN リンクを使用するさまざまなサービス間で、WAN リンクの帯域幅の双方向 (LAN から

WAN または WAN から LAN へ) 分散が可能になります。[Services] セクションでは、帯域幅割り当てをさらに微調整できます。さらに、フェアシェアを有効にして、フェア配布が制定される前に、すべてのサービスが最小の予約帯域幅を受け取ることができます。



インターネットサービスは、Citrix SD-WAN でサポートされているさまざまな展開モードで使用できます。

- インライン展開モード (SD-WAN オーバーレイ)

Citrix SD-WAN は、どのネットワークでもオーバーレイソリューションとして導入できます。オーバーレイソリューションとして、SD-WAN は通常、既存のエッジルーターやファイアウォールの背後に展開されます。SD-WAN がネットワークファイアウォールの背後に展開されている場合、インターフェイスを信頼できるものとして構成し、インターネットトラフィックをインターネット Gateway としてファイアウォールに配信できます。

- エッジモードまたはゲートウェイモード

Citrix SD-WAN をエッジデバイスとして展開し、既存のエッジルーターやファイアウォールデバイスを置き換えることができます。オンボードファイアウォール機能により、SD-WAN は直接インターネット接続からネットワークを保護できます。このモードでは、パブリックインターネットリンクに接続されているインターフェイスが信頼できないように設定され、暗号化が強制的に有効になり、ファイアウォールとダイナミック NAT 機能が有効になり、ネットワークを保護します。

Secure Web Gateway による直接インターネットアクセス

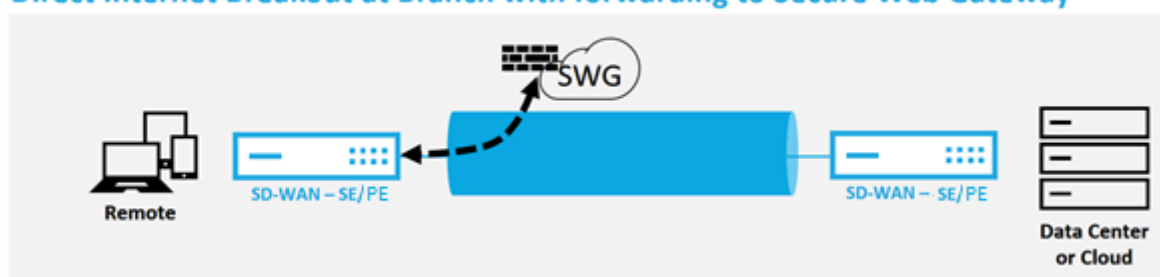
November 8, 2021

トラフィックを保護し、ポリシーを適用するために、企業は多くの場合、MPLS リンクを使用して、ブランチトラフィックを企業のデータセンターにバックホールします。データセンターは、セキュリティポリシーを適用し、セキュリティアプライアンスを介してトラフィックをフィルタリングしてマルウェアを検出し、トラフィックを ISP 経由でルーティングします。プライベート MPLS リンクを介したこのようなバックホールは高価です。また、レイテンシーが大きくなるため、ブランチサイトでのユーザーエクスペリエンスが低下します。また、ユーザーがセキュリティ制御をバイパスするリスクもあります。

バックホールに代わる方法として、支店にセキュリティアプライアンスを追加する方法があります。ただし、複数のアプライアンスをインストールして、サイト全体で一貫したポリシーを維持するにつれて、コストと複雑さが増大します。最も重要なのは、支店の数が多い場合、コスト管理は実用的ではありません。

もう 1 つの方法は、コスト、複雑さ、または遅延を追加せずにセキュリティを強化することです。これは、Citrix SD-WAN を使用してすべての支店のインターネットトラフィックを Secure Web Gateway Service にルーティングすることです。サードパーティの Secure Web Gateway Service を使用すると、接続されているすべてのネットワークで使用できる、きめ細かな一元的なセキュリティポリシー作成が可能になります。ポリシーは、ユーザーがデータセンターにいるかブランチサイトにいるかにかかわらず、一貫して適用されます。Secure Web Gateway ソリューションはクラウドベースであるため、高価なセキュリティアプライアンスをネットワークに追加する必要はありません。

Direct Internet Breakout at Branch with forwarding to Secure Web Gateway



Citrix SD-WAN は、次のサードパーティの Secure Web Gateway ソリューションをサポートしています。

- [Zscaler](#)
- [フォースポイント](#)
- [パロ・アルト](#)
- [Citrix Secure Internet Access](#)

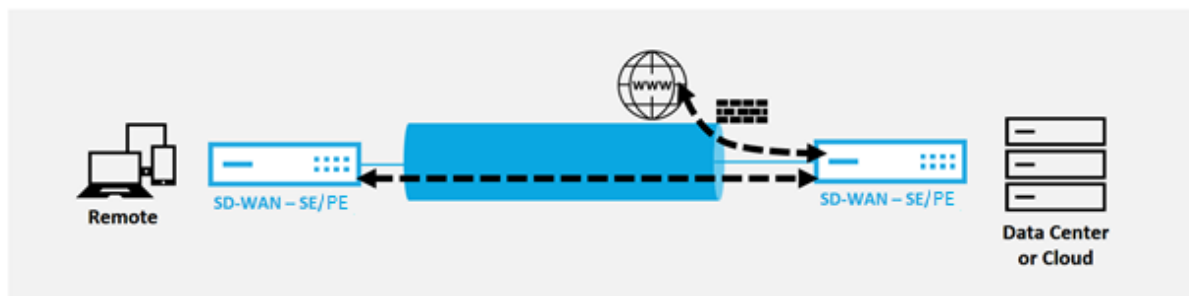
バックホールインターネット

May 10, 2021

Citrix SD-WAN ソリューションでは、インターネットトラフィックを MCN サイトまたは他のブランチサイトにバックホールできます。バックホールは、インターネット宛てのトラフィックが、インターネットにアクセスできる別の定義済みサイトを介して送り返されることを示します。セキュリティ上の問題やアンダーレイネットワークポロジが原因で、インターネットに直接アクセスできないネットワークに便利です。たとえば、内蔵の SD-WAN ファイアウォールがそのサイトのセキュリティ要件を満たしていない外部ファイアウォールがないリモートサイトが挙げられます。環境によっては、データセンターで強化された DMZ を経由するすべてのリモートサイトのインターネットトラフィックをバックホールすることが最善のアプローチである場合があります。ただし、この方法では、次の点に注意しなければならない制限があり、アンダーレイ WAN リンクのサイズが適切になります。

- インターネットトラフィックのバックホールは、インターネット接続にレイテンシーを増大させ、データセンターのブランチサイトの距離に応じて変化します。
- インターネットトラフィックのバックホールは、仮想パスの帯域幅を消費し、WAN リンクのサイジングに考慮されます。
- インターネットトラフィックのバックホールは、データセンターでインターネット WAN リンクを過剰にサブスクリブする可能性があります。

Backhaul Internet to Data Center MCN



すべての Citrix SD-WAN デバイスは、1 つのデバイスに最大 8 つの異なるインターネット WAN リンクを終了できます。集約された WAN リンクのライセンスされたスループット機能は、Citrix SD-WAN のデータシートに各アプリケーションごとに一覧表示されます。

Citrix SD-WAN ソリューションは、次の構成でインターネットトラフィックのバックホールをサポートします。

1. MCN サイトノード、またはインターネットサービスが必要なその他のサイトノードでインターネットサービスを有効にします。

注

他のすべてのサイトが WAN から WAN への転送グループにある場合は、インターネットサービスとエクスポートルートを実効にします。

2. インターネットトラフィックがバックホールされるブランチノードで、0.0.0.0/0 ルートを手動で追加して、すべてのデフォルトトラフィックを仮想パスサービスに送信します。ネクストホップは MCN (中間サイト) として表されます。

Add Route

Network IP Address: 0.0.0.0/0 Cost: 5 Service Type: Virtual Path Gateway IP Address:

Next Hop Site: DC

☐ Eligibility Based On Path

Path: <None>

Add Cancel

3. ブランチサイトのルートテーブルに、目的のバックホールルート以外のトラフィックを誘導する他の低コストのルートがないことを確認します。

Order	Network IP Address	Cost	Service Type	Service Name	Gateway IP Address	Info	Edit	Delete
1	172.16.100.2/24	5	Local			ⓘ		
2	172.16.30.2/24	5	Local			ⓘ		
3	192.168.10.2/24	5	Local			ⓘ		
4	0.0.0.0/0	5	Virtual Path	DC		ⓘ	✎	🗑
5	0.0.0.0/0	16	Passthrough			ⓘ		

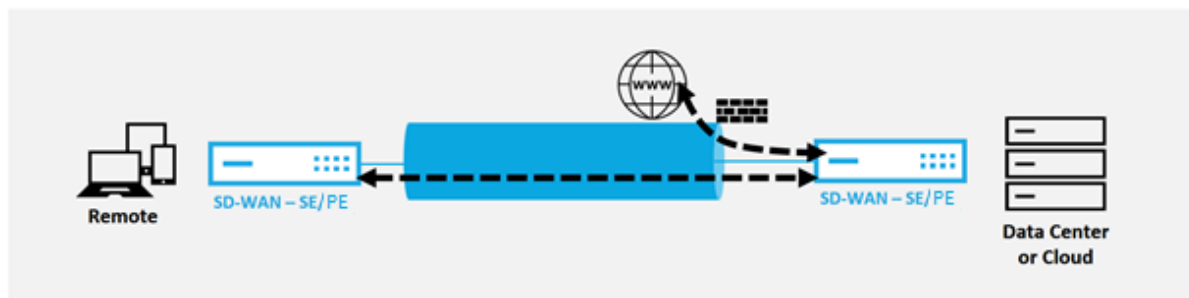
ヘアピンモード

May 10, 2021

ヘアピンの展開では、ローカルインターネットサービスが使用できない場合や、トラフィックが遅い場合に、バックホールまたはヘアピンを介したインターネットアクセスにリモートハブサイトを実装できます。特定のサイトからのバックホールを許可することで、クライアントサイト間に高帯域幅ルーティングを適用できます。

非 WAN から WAN 転送サイトへのヘアピン展開の目的は、より効率的な展開プロセスを提供し、技術的な実装を合理化することです。必要に応じて、リモートハブサイトを使用してインターネットアクセスでき、フローを仮想パス経由で SD-WAN ネットワークにルーティングできます。

Backhaul Internet to Data Center MCN



たとえば、複数の SD-WAN サイト A と B を持つ管理者が、サイト A のインターネットサービスが不十分な場合を考えます。サイト B には使用可能なインターネットサービスがあり、サイト A からサイト B へのトラフィックだけをバックホールします。戦略的に重み付けされたルートコストや、トラフィックを受信すべきでないサイトへの伝播を複雑にすることなく、これを実現できます。

また、ルートテーブルは、Hairpin デプロイメントのすべてのサイトで共有されるわけではありません。たとえば、サイト A とサイト B の間でサイト C を介してトラフィックがヘアピンされている場合、サイト C だけがサイト A と B のルートを確認します。WAN から WAN への転送とは異なり、サイト A とサイト B は互いのルートテーブルを共有しません。

サイト A とサイト B の間でサイト C を介してトラフィックがヘアピンされる場合は、両方のサイトのネクストホップが中間サイト C であることを示す静的ルートをサイト A とサイト B に追加する必要があります。

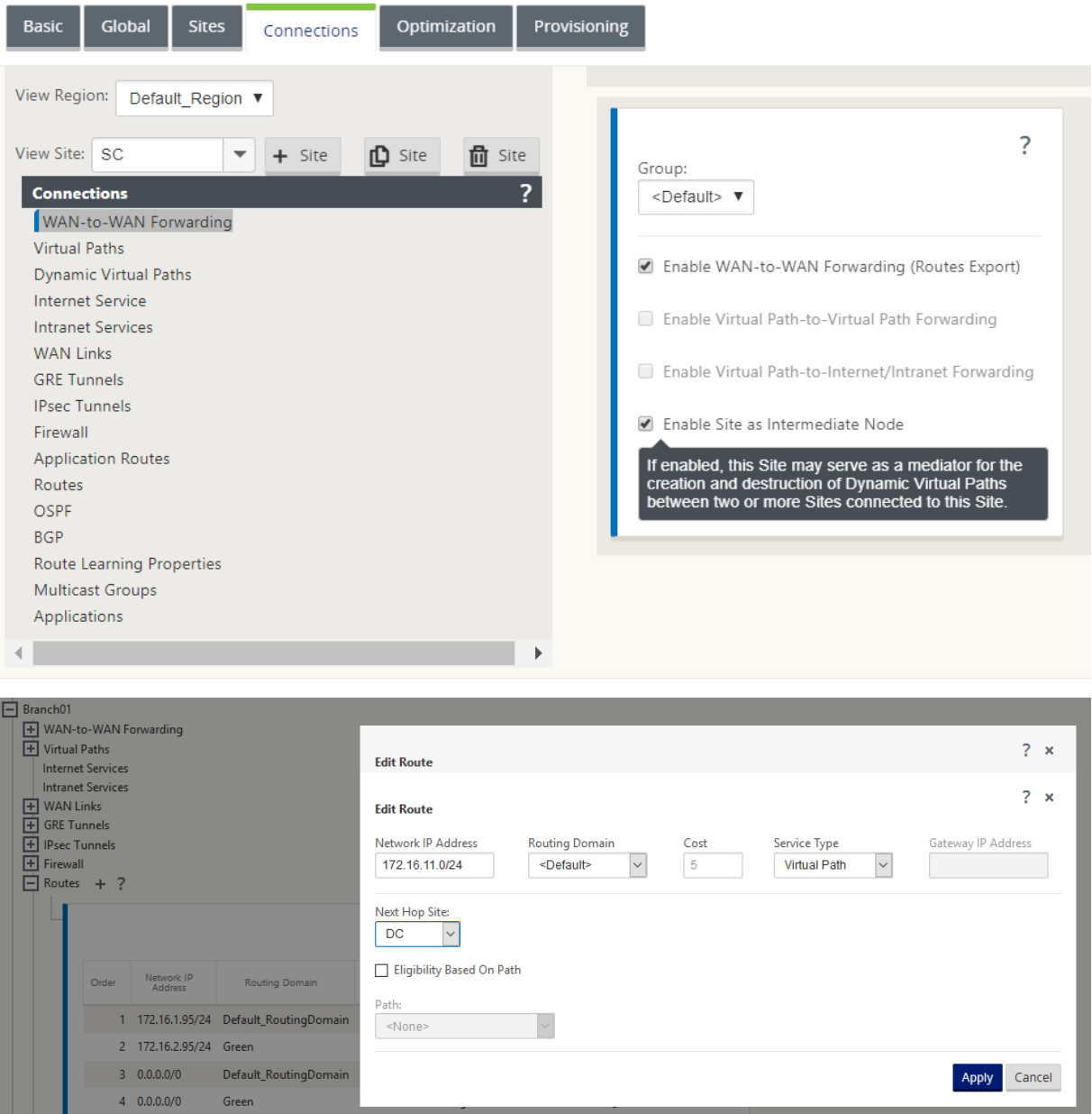
WAN から WAN への転送と Hairpin の配置には、次のような違いがあります。

1. 動的仮想パスは構成されていません。常に、中間サイトは 2 つのサイト間のトラフィックをすべて認識します。
2. WAN から WAN への転送グループには参加しません。

WAN から WAN への転送とヘアピンの配置は、相互に排他的です。任意の時点で設定できるのは、そのうちの 1 つだけです。

Citrix SD-WAN SE/PE および VPX (仮想) アプライアンスは、ヘアピンの展開をサポートします。0.0.0.0/0 ルートを設定して、追加のロケーションに影響を与えずに 2 つのロケーション間のトラフィックをヘアピンできるようになりました。イントラネットトラフィックにヘアピンを使用する場合、特定のイントラネットルートがクライアントサイトに追加され、仮想パスを通じてヘアピンサイトにイントラネットトラフィックを転送します。ヘアピン機能を実現するために WAN から WAN への転送を有効にする必要はなくなりました。

ヘアピンの展開は、構成エディターから Citrix SD-WAN Web 管理インターフェースを使用して構成できます。



ホストされたファイアウォール

May 10, 2021

現在、Citrix SD-WAN は、以下のホストされたファイアウォールをサポートしています。

- [Palo Alto Networks](#)
- [Check Point](#)

Palo Alto Networks SD-WAN 1100 プラットフォーム上のファイアウォール統合

May 10, 2021

Citrix SD-WAN は、Palo Alto Networks の次世代仮想マシンのホスティングをサポートしています (VM) SD-WAN 1100 プラットフォーム上のシリーズファイアウォール。サポートされている仮想マシンモデルは次のとおりです。

- VM 50
- VM 100

Palo Alto Networks 仮想マシンシリーズのファイアウォールは、SD-WAN 1100 プラットフォーム上で仮想マシンとして動作します。ファイアウォール仮想マシンは **Virtual Wire** モードで統合され、2 つのデータ仮想インターフェイスが接続されています。SD-WAN でポリシーを構成することで、必要なトラフィックをファイアウォール仮想マシンにリダイレクトできます。

長所

以下は、SD-WAN 1100 プラットフォームでの Palo Alto Networks 統合の主な目標または利点です。

- 支店デバイスの統合:SD-WAN と高度なセキュリティの両方を実行する単一のアプライアンス
- LAN-to-LAN、LAN-インターネット、およびインターネット-LAN のトラフィックを保護するオンプレム NGFW（次世代ファイアウォール）によるブランチオフィスのセキュリティ

構成の手順

Palo Alto Networks 仮想マシンを SD-WAN に統合するには、以下の構成が必要です。

- ファイアウォール仮想マシンのプロビジョニング
- セキュリティ仮想マシンへのトラフィックリダイレクトを有効にする

注:

トラフィックのリダイレクトを有効にする前に、ファイアウォール仮想マシンを最初にプロビジョニングする必要があります。

Palo Alto Networks 仮想マシンのプロビジョニング

ファイアウォール仮想マシンをプロビジョニングするには、次の 2 つの方法があります。

- SD-WAN センターによるプロビジョニング
- SD-WAN アプライアンス GUI によるプロビジョニング

SD-WAN センターを介したファイアウォール仮想マシンの Provisioning

前提条件

- セカンダリストレージを SD-WAN Center に追加して、ファイアウォール VM イメージファイルを保存します。詳しくは、「システム要件とインストール」を参照してください。
- ファイアウォール VM イメージファイル用にセカンダリパーティションからストレージを予約します。ストレージ制限を設定するには、[管理] > [ストレージのメンテナンス] に移動します。
 - リストから必要なストレージ量を選択します。
 - [適用] をクリックします。

Administration / Storage Maintenance

Region: Default_Region

Host	File System	Type	Size (MB)	Available (MB)	Active/Migrate Data
Local*	/dev/xvda2	ext3	7288	3471	
Local	/dev/xvdb	ext3	14910	12921	

Apply

Note: Software image storage reserved will be reduced while calculating the secondary partition Size(MB) and Available(MB)

Software Image Storage Reservation

Note: User can modify the storage reservation only if the SD-WAN Center has secondary partition mounted and it should operate in headend mode

Amount of storage to reserve from secondary partition storage(Active) is: 10GB

Apply

Thresholds

SD-WAN Center Database Storage and Auto Cleanup settings are misconfigured, SD-WAN Center will reach auto cleanup threshold before the configured 6 months.

Stop stats polling when storage usage exceeds 55% of active storage size

☐ Notify user when storage usage exceeds 10% of active storage size

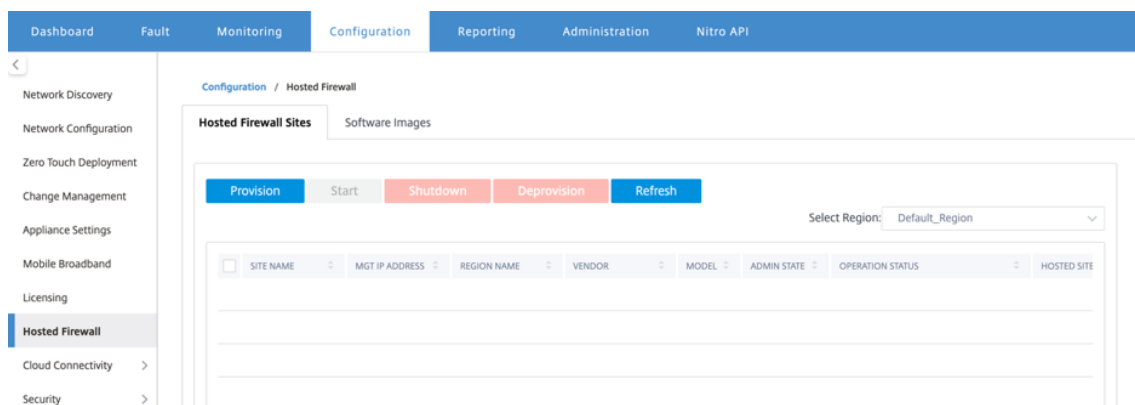
Apply

注:

ストレージは、条件が満たされた場合にアクティブであるセカンダリパーティションから予約されています。

SD-WAN Center プラットフォーム経由でファイアウォール仮想マシンを Provisioning するには、次の手順を実行します。

1. Citrix SD-WAN Center GUI で、[構成] > [ホストされたファイアウォール] を選択します。



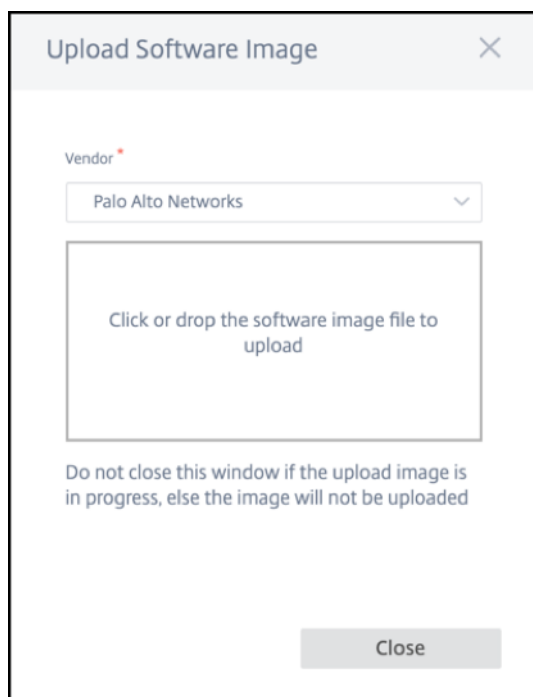
ドロップダウンリストから [Region] を選択すると、選択したリージョンのプロビジョニングされたサイトの詳細を表示できます。

2. ソフトウェアイメージをアップロードします。

注:

ソフトウェアイメージをアップロードするのに十分なディスク領域があることを確認してください。

[設定] > [ホストファイアウォール] > [ソフトウェアイメージ] に移動し、ドロップダウンリストから [Palo Alto Networks] としてベンダー名を選択します。アップロードするボックスに、ソフトウェアイメージファイルをクリックまたはドロップします。



進行中のアップロード処理を示すステータスバーが表示されます。イメージファイルが 100% アップロードされた则表示されるまで、[**Refresh**] をクリックしたり、その他のアクションを実行したりしないでください。

- 更新: [更新] オプションをクリックして、最新のイメージファイルの詳細を取得します。

- 削除: 既存のイメージファイルを削除するには、[削除] オプションをクリックします。

注

- デフォルト以外のリージョンのサイトでファイアウォール仮想マシンをプロビジョニングするには、各コレクタノードにイメージファイルをアップロードします。
- Palo Alto VM イメージを SDWAN センターから削除すると、SDWAN センターストレージからイメージが削除され、アプライアンスからは削除されません。

3. プロビジョニングについては、[ホストされたファイアウォールサイト] タブに戻り、[プロビジョニング] をクリックします。

Provision Virtual Machine

Vendor *

Palo Alto Networks

Vendor Virtual Machine Model *

VM50

Software Image *

PA-VM-KVM-9.0.1.qcow2

Please ensure to upload this image in the collector, for non-default region sites provisioning

Region *

Region1

Sites for Firewall Hosting *

DC () X

Please ensure to select both primary and secondary sites if the sites are in High availability mode

Management Server Primary IP Address/Domain Name

Enter Management Server Primary IP Address or domain name

Management Server Secondary IP Address/Domain Name

Enter Management Server Secondary IP Address or domain name

Virtual Machine Authentication Key

Enter the virtual authentication key to be used in the Management server

Authentication Code

Enter the authentication code to be used for licensing

Start Provision

Cancel

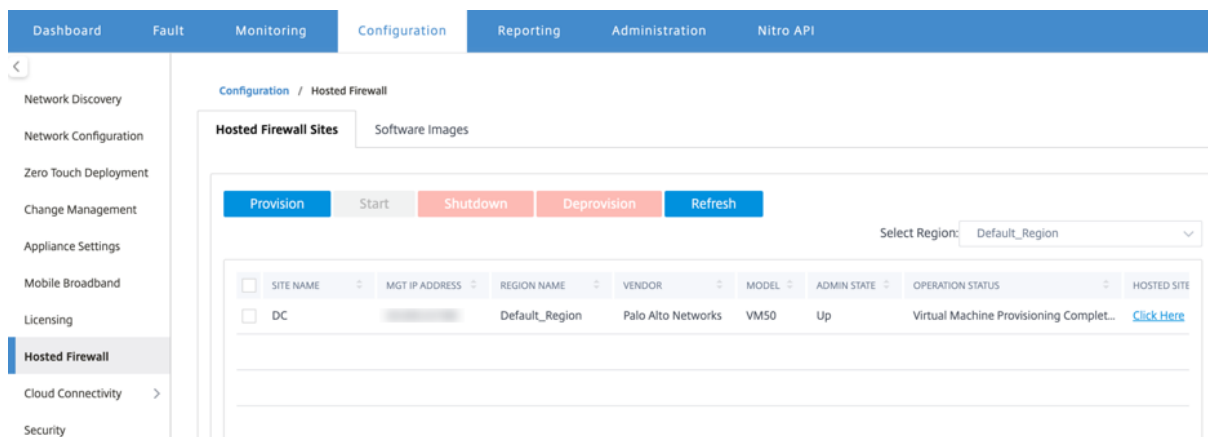
- ベンダー: ドロップダウンリストから [**Palo Alto Networks**] としてベンダー名を選択します。
- ベンダー仮想マシンモデル: リストから仮想マシンのモデル番号を選択します。
- ソフトウェアイメージ: プロビジョニングするイメージファイルを選択します。
- リージョン: リストからリージョンを選択します。
- [ファイアウォールホスティングのサイト]: ファイアウォールホスティングのリストのサイトを選択します。サイトが高可用性モードの場合は、プライマリサイトとセカンダリサイトの両方を選択する必要があります。

- 管理サーバーのプライマリ **IP** アドレス/ドメイン名: 管理プライマリ IP アドレスまたは完全修飾ドメイン名を入力します (オプション)。
- 管理サーバーのセカンダリ **IP** アドレス/ドメイン名: 管理サーバーのセカンダリ IP アドレスまたは完全修飾ドメイン名を入力します (オプション)。
- 仮想マシン認証キー: 管理サーバーで使用する仮想認証キーを入力します。
- 認証コード: ライセンスに使用する仮想認証コードを入力します。

4. 「プロビジョニングの開始」をクリックします。

5. 最新のステータスを取得するには、[**Refresh**] をクリックします。Palo Alto Networks 仮想マシンが完全に起動すると、SD-WAN Center UI に反映されます。

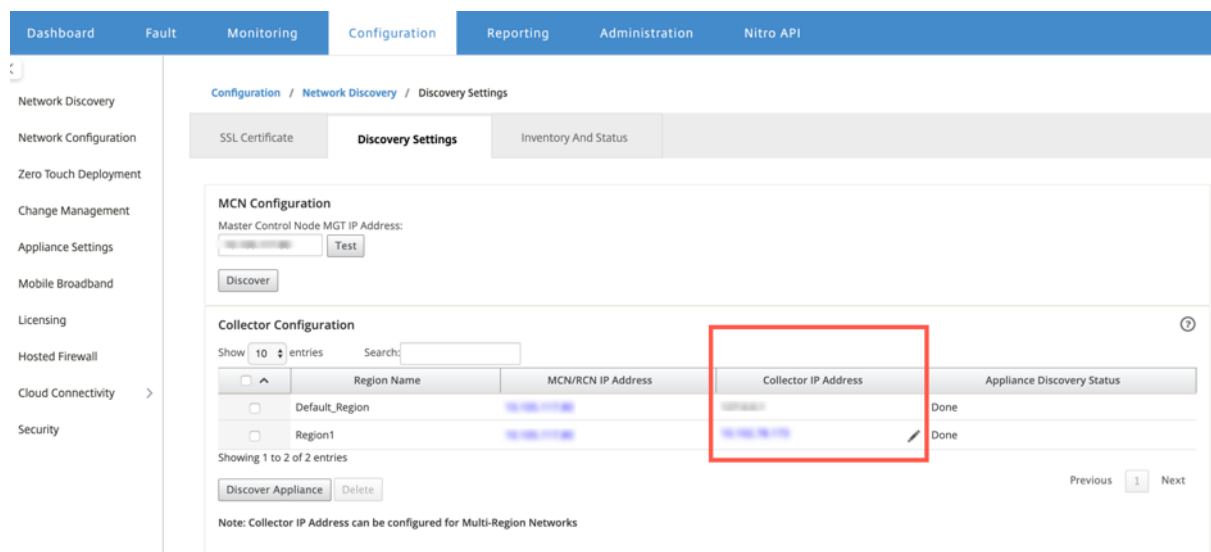
必要に応じて、仮想マシンを開始、シャットダウン、プロビジョニング解除 できます。



- サイト名: サイト名が表示されます。
- 管理 **IP**: サイトの管理 IP アドレスを表示します。
- リージョン名: リージョン名が表示されます。
- ベンダー: ベンダー名 (パロアルトネットワーク) を表示します。
- モデル: モデル番号 (VM50/VM100) が表示されます。
- 管理状態: ベンダー仮想マシンの状態 (アップ/ダウン)。
- 操作ステータス: 操作ステータスメッセージを表示します。
- ホストサイト: Palo Alto Networks 仮想マシンの GUI にアクセスするには、**【ここをクリック】** リンクを使用します。

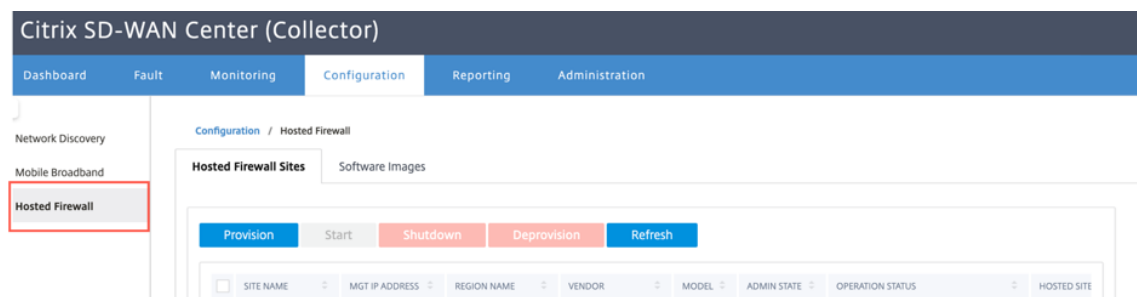
デフォルト以外のリージョンサイトをプロビジョニングするには、SD-WAN Center Collector にソフトウェアイメージをアップロードする必要があります。Palo Alto Networks は、SD-WAN Center ヘッドエンド GUI または SD-WAN Center コレクタから両方ともプロビジョニングできます。

SD-WAN Center コレクタの IP アドレスを取得するには、[**構成**] > [**ネットワーク探索**] > [**探索の設定**] タブを選択します。



SD-WAN コレクタから Palo Alto Networks をプロビジョニングするには:

1. SD-WAN Collector GUI から、[構成]に移動し、[ホストされたファイアウォール]を選択します。



2. ソフトウェアイメージタブに移動して、ソフトウェアイメージをアップロードします。
3. [ホストされたファイアウォールサイト] タブの [プロビジョニング] をクリックします。
4. 次の詳細を入力し、「プロビジョニングの開始」をクリックします。

Vendor *

Palo Alto Networks

Vendor Virtual Machine Model *

VM50

Software Image *

PA-VM-KVM-8.1.3.qcow2

Please ensure to upload this image in the collector, for non-default region sites provisioning

Sites for Firewall Hosting *

BRANCH-PA () X

Please ensure to select both primary and secondary sites if the sites are in High availability mode

Management Server Primary IP Address/Domain Name

Enter Management Server Primary IP Address or domain name

Management Server Secondary IP Address/Domain Name

Enter Management Server Secondary IP Address or domain name

Virtual Machine Authentication Key

Enter the virtual authentication key to be used in the Management server

Authentication Code

Enter the authentication code to be used for licensing

Start Provision Cancel

- ベンダー: ドロップダウンリストから [**Palo Alto Networks**] としてベンダー名を選択します。
- ベンダー仮想マシンモデル: リストから仮想マシンのモデル番号を選択します。
- ソフトウェアイメージ: プロビジョニングするイメージファイルを選択します。
- リージョン: リストからリージョンを選択します。
- [ファイアウォールホスティングのサイト]: ファイアウォールホスティングのリストのサイトを選択します。サイトが高可用性モードの場合は、プライマリサイトとセカンダリサイトの両方を選択する必要があります。
- 管理サーバーのプライマリ **IP** アドレス/ドメイン名: 管理プライマリ IP アドレスまたは完全修飾ドメイン名を入力します (オプション)。
- 管理サーバーのセカンダリ **IP** アドレス/ドメイン名: 管理サーバーのセカンダリ IP アドレスまたは完全修飾ドメイン名を入力します (オプション)。
- 仮想マシン認証キー: 管理サーバーで使用する仮想認証キーを入力します。

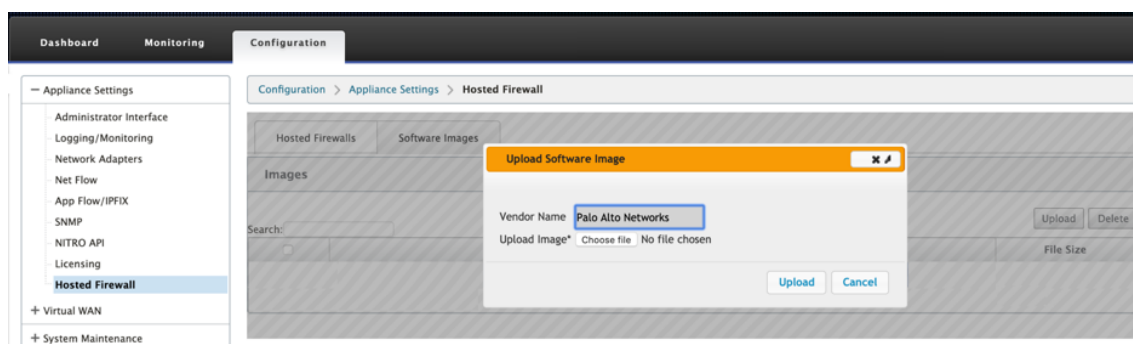
- 認証コード：ライセンスに使用する仮想認証コードを入力します。

5. 「プロビジョニングの開始」をクリックします。

SD-WAN アプライアンスの GUI によるファイアウォール仮想マシンの Provisioning

SD-WAN プラットフォームで、ホストされた仮想マシンをプロビジョニングして起動します。Provisioning の手順は、次のとおりです。

1. Citrix SD-WAN GUI で、[構成] > [アプライアンスの設定] の順に 展開し、[ホストされたファイアウォール] を選択します。
2. ソフトウェアイメージをアップロードします。
 - [ソフトウェアイメージ] タブを選択します。[**Palo Alto Networks**] としてベンダー名を選択します。
 - ソフトウェアイメージファイルを選択します。
 - [アップロード] をクリックします。

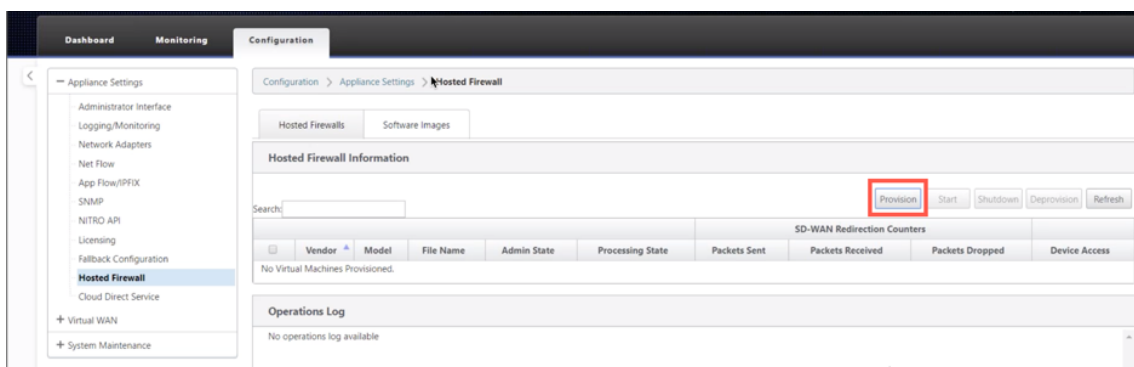


注：

アップロードできるソフトウェアイメージは最大 2 つです。Palo Alto Networks 仮想マシンイメージのアップロードには、帯域幅の可用性によっては、時間がかかる場合があります。

アップロードプロセスを追跡するステータスバーが表示されます。画像が正常にアップロードされると、ファイルの詳細が反映されます。Provisioning に使用されるイメージは削除できません。画像ファイルに 100% アップロードされた则表示されるまで、アクションを実行したり、他のページに戻ったりしないでください。

3. プロビジョニングの場合は、[ホストされたファイアウォール] タブを選択し、[プロビジョニング] ボタンをクリックします。

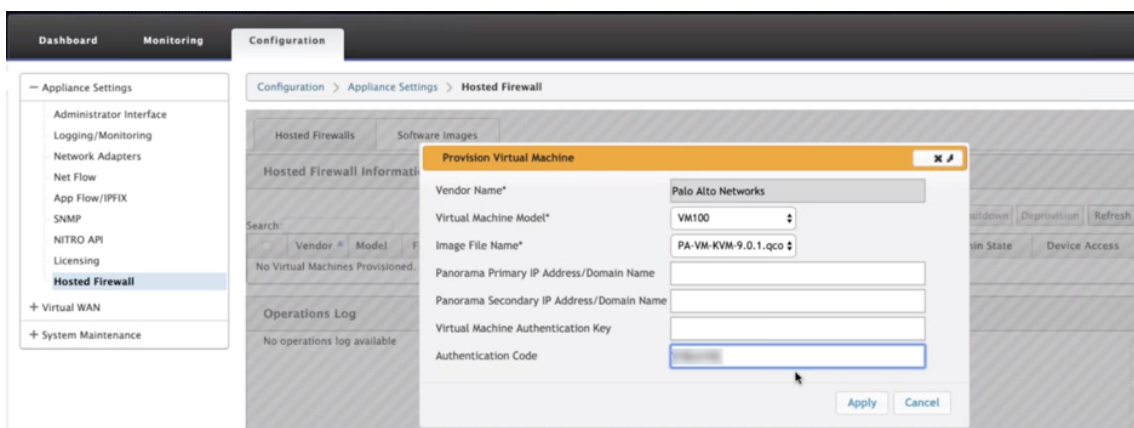


4. Provisioning について次の詳細を入力します。

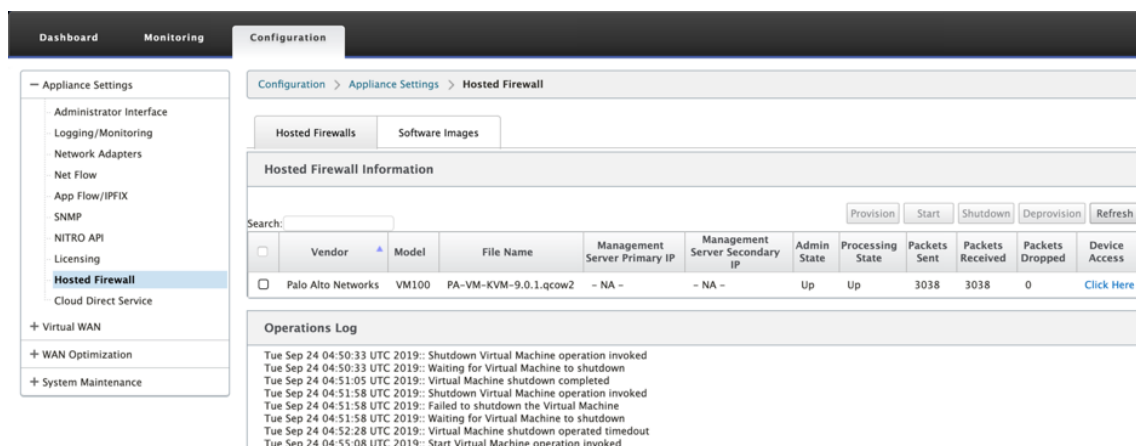
- ベンダー名: **Palo Alto** ネットワークとしてベンダーを選択します。
- 仮想マシンモデル: リストから仮想マシンのモデル番号を選択します。
- イメージファイル名: イメージファイルを選択します。
- パノラマプライマリ IP アドレス/ドメイン名: パノラマプライマリ IP アドレスまたは完全修飾ドメイン名を指定します (オプション)。
- パノラマセカンダリ IP アドレス/ドメイン名: パノラマセカンダリ IP アドレスまたは完全修飾ドメイン名を指定します (オプション)。
- 仮想マシン認証キー: 仮想マシン認証キーを指定します (オプション)。

Palo Alto Networks 仮想マシンをパノラマに自動登録するには、仮想マシン認証キーが必要です。

- 認証コード: 認証コード (仮想マシンライセンスコード) を入力します (オプション)。
- [適用] をクリックします。



- 最新のステータスを取得するには、[**Refresh**] をクリックします。Palo Alto Networks 仮想マシンが完全に起動すると、操作ログの詳細とともに SD-WAN UI に反映されます。



- 管理状態: 仮想マシンが起動中か停止中かを示します。
- 処理状態: 仮想マシンのデータベース処理状態。
- 送信パケット: SD-WAN からセキュリティ仮想マシンに送信されるパケット。
- 受信パケット: セキュリティ仮想マシンから SD-WAN によって受信されたパケット。
- Packet Dropped: SD-WAN によってドロップされたパケット (セキュリティ仮想マシンがダウンした場合など)。
- デバイスアクセス: セキュリティ仮想マシンへの GUI アクセスを取得するには、リンクをクリックします。

必要に応じて、仮想マシンを開始、シャットダウン、プロビジョニング解除できます。ここをクリック オプションを使用して、Palo Alto Networks 仮想マシンの GUI にアクセスするか、管理 IP と 4100 ポート (管理 IP: 4100) を使用します。

注

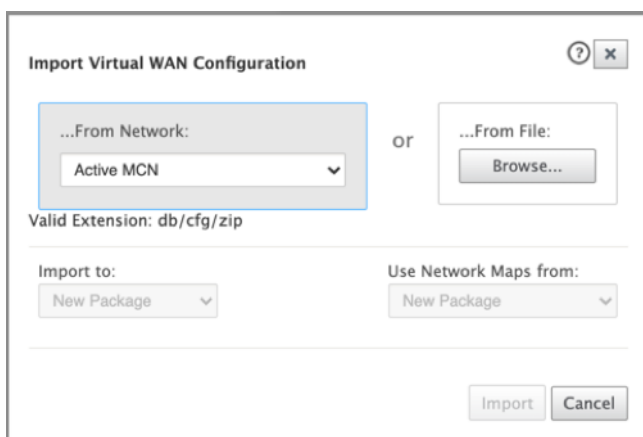
パロアルトネットワークスの GUI にアクセスするには、常にシークレットモードを使用してください。

トラフィックリダイレクト

トラフィックリダイレクトの設定は、MCN の構成エディターまたは SD-WAN Center の構成エディターを使用を行うことができます。

SD-WAN センターで構成エディター内を移動するには、次の手順を実行します。

1. Citrix SD-WAN Center UI を開き、[構成] > [ネットワーク構成のインポート] に移動します。アクティブ MCN から仮想 WAN 設定をインポートし、[**Import**] をクリックします。



The dialog box is titled "Import Virtual WAN Configuration" and includes a help icon and a close button in the top right corner. It features two main sections for configuration source selection, separated by an "OR" label. The left section, labeled "...From Network:", contains a dropdown menu currently showing "Active MCN". The right section, labeled "...From File:", contains a "Browse..." button. Below these sections, the text "Valid Extension: db/cfg/zip" is displayed. Further down, there are two more dropdown menus: "Import to:" (showing "New Package") and "Use Network Maps from:" (showing "New Package"). At the bottom right, there are "Import" and "Cancel" buttons.

残りの手順は、MCN を介したトラフィックリダイレクション設定と同様です。

MCN の構成エディタ内を移動するには、次の手順を実行します。

1. [グローバル] > [ネットワーク設定] で [接続の一致タイプ] を対称に設定します。

Global

- Network Settings
- Regions
- Centralized Licensing
- Hosted Firewall Template
- Routing Domains
- Applications
- Application QoS
- Firewall Zones
- Firewall Policy Templates
- Rule Groups
- Network Objects
- Route Learning Import Template
- Route Learning Export Template
- Virtual Path Default Sets
- Dynamic Virtual Path Default Sets
- Internet Default Sets
- Intranet Default Sets
- DHCP Option Sets
- DNS Services
- Proxy Auto-config settings
- Autopath Groups
- Service Providers
- WAN-to-WAN Forwarding Groups
- WAN Optimization Features
- WAN Optimization Tuning Settings
- WAN Optimization Application Classifiers
- WAN Optimization Service Classes

Global Security Settings

Note: Changing the **Network Encryption Mode** may cause **Site Secure Keys** to be truncated or regenerated if they do not meet the requirements of the new mode.

Network Encryption Mode: AES 128-Bit

☒ Enable Encryption Key Rotation

☐ Enable Extended Packet Encryption Header

☐ Enable Extended Packet Authentication Trailer

Extended Packet Authentication Trailer Type: 32-Bit Checksum

☐ Enable FIPS Mode

☐ Enable Appliance Authentication

Network Secure Key: 72d050ce5ca54c... **Regenerate**

Global Firewall Settings

Global Policy Template: New_Firewall_... Default Firewall Action: Allow ☒ Default Connection State Tracking

Connection Match Type: Symmetric

Denied Timeout (s): 30

TCP Initial Timeout (s): 120 TCP Idle Timeout (s): 7440

TCP Closing Timeout (s): 60 TCP Time Wait Timeout (s): 120 TCP Closed Timeout (s): 10

UDP Initial Timeout (s): 30 UDP Idle Timeout (s): 300

ICMP Initial Timeout (s): 30 ICMP Idle Timeout (s): 60

Generic Initial Timeout (s): 30 Generic Idle Timeout (s): 300

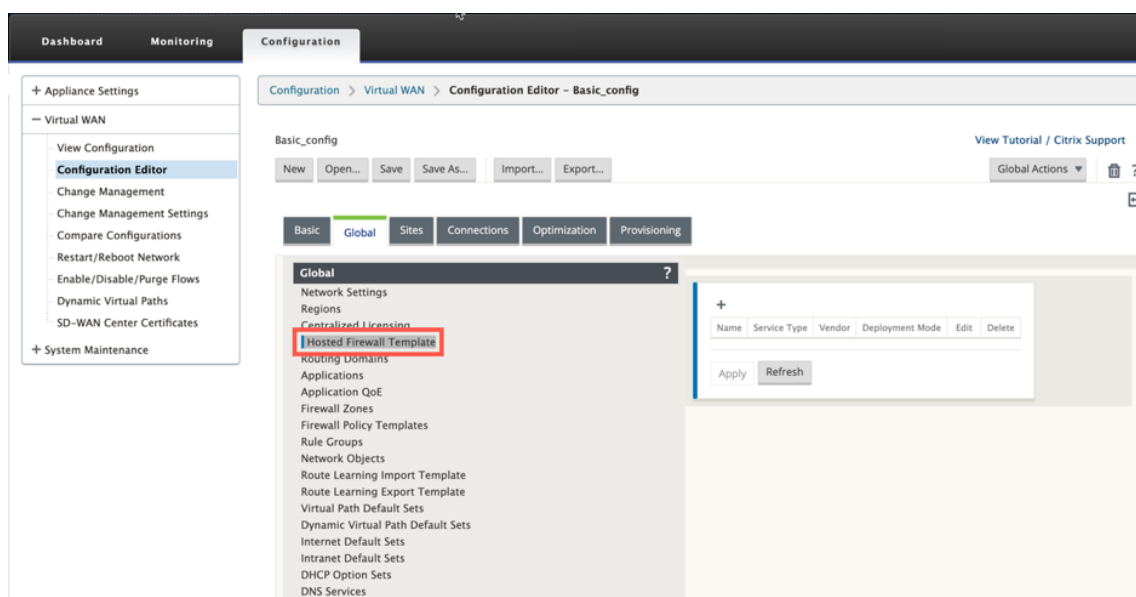
Global On-Demand Bandwidth Limit Setting

Default maximum total WAN-to-LAN bandwidth, as a percentage of bandwidth provided by non-standby WAN links in the Virtual Path (%): 120

Apply **Revert**

デフォルトでは、SD-WAN ファイアウォールポリシーは方向固有です。対称マッチタイプは、指定された一致基準を使用して接続に一致し、両方向にポリシーアクションを適用します。

2. **Citrix SD-WAN UI** を開き、[構成] > [仮想 WAN] を展開し、[構成エディタ] を選択し、[グローバル] セクションで [ホストされたファイアウォールテンプレート] を選択します。



3. [+] をクリックし、次のスクリーンショットで必要な情報を入力し、[**Hosted Firewall**] テンプレートを追加し、[**Add**] をクリックします。

Edit

Name:

PaloAlto-NGFW

Model:

VM50

Primary Management Server IP/FQDN:

Vendor

Palo Alto Networks

Deployment Mode:

Virtual Wire

Secondary Management Server IP/FQDN:

Service Redirection Interfaces +

Name	Input Interface	Output Interface	VLAN ID	Delete
INTERNET-OUT	Interface-1	Interface-2	0	
INTERNET-IN	Interface-2	Interface-1	0	

Apply

Cancel

ホストされたファイアウォールテンプレートを使用すると、SD-WAN アプライアンスでホストされているファイアウォール仮想マシンへのトラフィックリダイレクトを構成できます。テンプレートを構成するために必要な入力はこちらのとおりです。

- [名前]: ホストされているファイアウォールテンプレートの名前。
- ベンダー: ファイアウォールベンダーの名前。
- 配置モード: [配置モード] フィールドは自動的に入力され、グレー表示されます。**Palo Alto** ネットワークスのベンダーの場合、展開モードは **Virtual Wire** です。

- モデル: ホストされたファイアウォールの仮想マシンモデル。Palo Alto Networks ベンダーの場合、仮想マシンのモデル番号を VM 50/VM 100 として選択できます。
- プライマリ管理サーバ **IP/FQDN**: パノラマのプライマリ管理サーバ IP/FQDN。
- セカンダリ管理サーバ **IP/FQDN**: パノラマのセカンダリ管理サーバ IP/FQDN。
- サービスリダイレクトインターフェイス: SD-WAN とホストされたファイアウォール間のトラフィックリダイレクトに使用される論理インターフェイスです。

Interface-1、Interface-2 は、ホストされているファイアウォールの最初の 2 つのインターフェイスを指します。トラフィックリダイレクションに VLAN を使用する場合は、ホストされたファイアウォールで同じ VLAN を設定する必要があります。トラフィックリダイレクション用に設定された VLAN は、SD-WAN およびホステッドファイアウォールの内部にあります。

注

リダイレクション入力インターフェイスは、接続イニシエータの方向から選択する必要があります。リダイレクションインターフェイスは、応答トラフィック用に自動的に選択されます。たとえば、発信インターネットトラフィックが Interface-1 でホストされているファイアウォールにリダイレクトされると、応答トラフィックは Interface-2 でホストされているファイアウォールに自動的にリダイレクトされます。インターネットインバウンドトラフィックがない場合、上記の例では Interface-2 は必要ありません。

Palo Alto Networks ファイアウォールをホストするには、物理インターフェイスが 2 つだけ割り当てられます。複数のゾーンからのトラフィックをホストされたファイアウォールにリダイレクトする必要がある場合は、内部 VLAN を使用して複数のサブインターフェイスを作成し、ホストされたファイアウォールの異なるファイアウォールゾーンに関連付けることができます。

SD-WAN ファイアウォールポリシーまたはサイトレベルのポリシーを使用して、すべてのトラフィックを Palo Alto Networks 仮想マシンにリダイレクトできます。

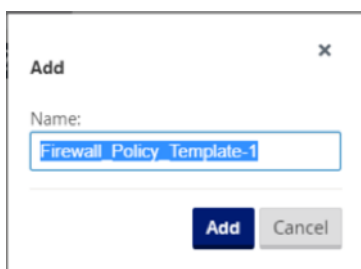
注

SD-WAN ファイアウォールポリシーが自動的に作成され、ホストされているファイアウォール管理サーバーとの間のトラフィックを許可します。これにより、ホストされたファイアウォール宛ての管理トラフィック（または）がリダイレクトされるのを回避できます。

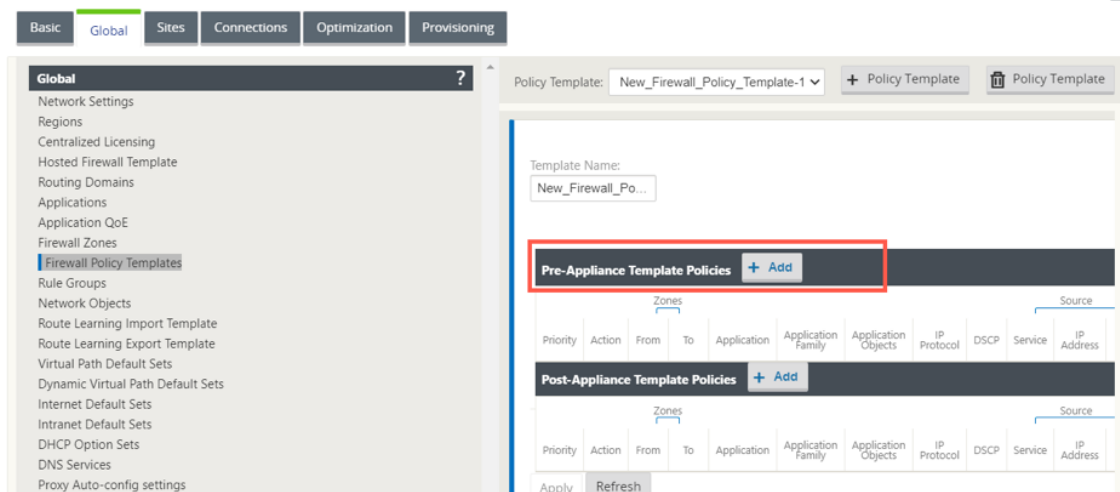
ファイアウォール仮想マシンへのトラフィックのリダイレクトは、SD-WAN ファイアウォールポリシーを使用して実行できます。SD-WAN ファイアウォールポリシーを作成するには、グローバルセクションのファイアウォールポリシーテンプレートまたはサイトレベルのどちらを使用するか 2 つの方法があります。

方法-1

1. Citrix SD-WAN GUI から、[構成] > [仮想 **WAN**] を展開し、[構成エディタ] に移動します。[グローバル] タブに移動し、[ファイアウォールポリシーテンプレート] を選択します。[+ ポリシーテンプレート] をクリックします。ポリシーテンプレートに名前を指定し、[Add] をクリックします。



2. [プレアプライアンステンプレートポリシー] の横にある [+ 追加] をクリックします。



3. ポリシータイプを [ホストされたファイアウォール] に変更します。アクションフィールドは、リダイレクトに自動入力されます。ドロップダウンリストから、** ホストされたファイアウォールテンプレートとサービスリダイレクトインターフェイスを選択します **。必要に応じて、他の一致基準を入力します。

Priority: Policy Type: **Hosted Firewall** ▼

Match Criteria

From Zones

Zone	Enable
Any	<input checked="" type="checkbox"/>
Default_LAN_Zone	<input type="checkbox"/>
Inter_Routing_Domain_Zone	<input type="checkbox"/>
Internet_Zone	<input type="checkbox"/>

To Zones

Zone	Enable
Any	<input checked="" type="checkbox"/>
Default_LAN_Zone	<input type="checkbox"/>
Inter_Routing_Domain_Zone	<input type="checkbox"/>
Internet_Zone	<input type="checkbox"/>

Traffic Match Type: **IP Protocol** ▼ IP Protocol: **Any** ▼ DSCP: **Any** ▼ ☐ Match Established

Application Objects: **Any** ▼

Source Service Type: **Any** ▼ Source Service Name: **Any** ▼ Source IP: Source Port:

Dest Service Type: **Any** ▼ Dest Service Name: **Any** ▼ Dest IP: Dest Port:

Actions

Action: **Redirect** ▼ ☒ Allow Fragments Connection State Tracking: **No Tracking** ▼

Hosted Firewall Template: **PaloAlto-NGFW** ▼ Service Redirection Interface: **INTERNET-OUT** ▼

4. [接続] > [ファイアウォール] に移動し、[名前] フィールドで (作成した) ファイアウォールポリシーを選択します。[適用] をクリックします。

Basic Global Sites **Connections** Optimization Provisioning

Region: **Default_Region** ▼

Site: **BR1100** ▼ + Site Site Site

Connections ?

- WAN-to-WAN Forwarding
- Virtual Paths
- Dynamic Virtual Paths
- Internet Service
- Intranet Services
- WAN Links
- GRE Tunnels
- IPsec Tunnels
- Firewall**
- Application Routes
- Routes
- OSPF
- BGP
- Route Learning Properties
- Inter Routing Domain Services
- Multicast Groups

Section: **Settings** ▼

Policy Templates + ?

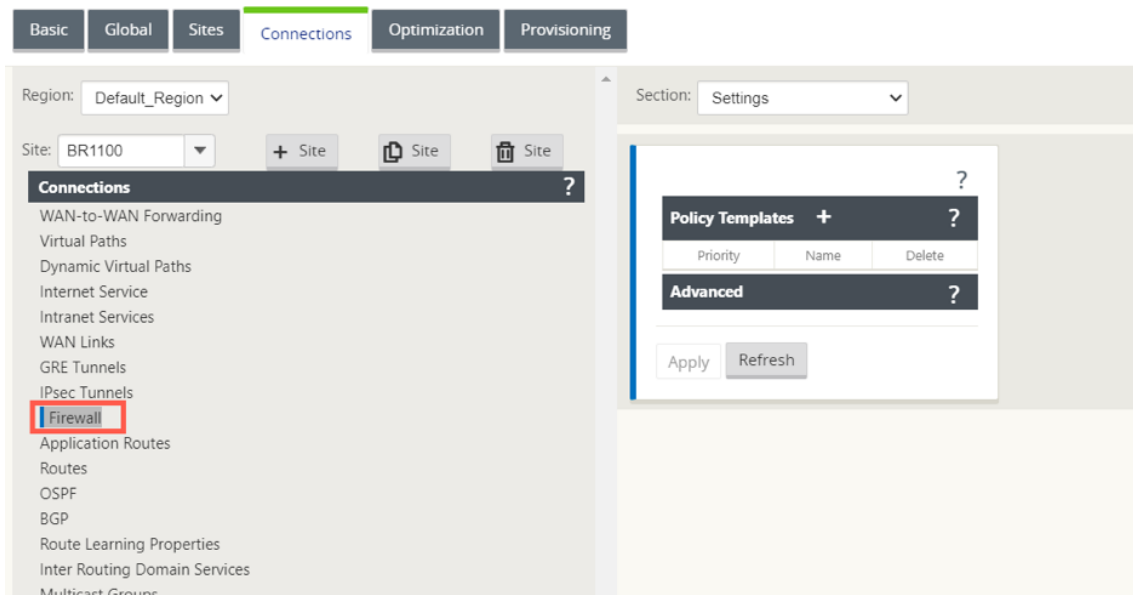
Priority	Name	Delete
100	New_Firewall_P... ▼	

Advanced ?

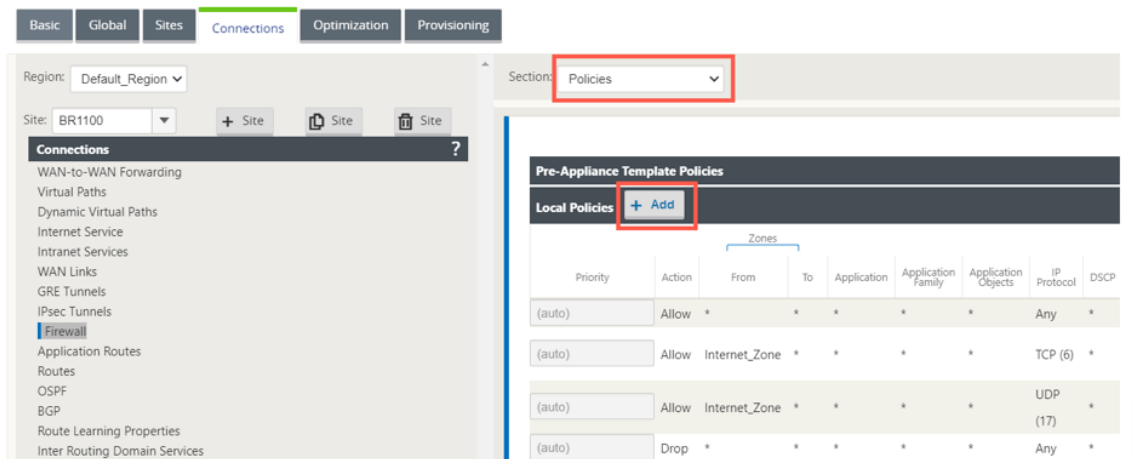
Apply **Revert**

方法-2

1. すべてのトラフィックをリダイレクトするには、[構成エディタ] > [仮想 WAN] で、[接続] タブに移動し、[ファイアウォール] を選択します。



2. [セクション] ドロップダウンリストから [ポリシー] を選択し、[+ 追加] をクリックして新しいファイアウォールポリシーを作成します。



3. ポリシータイプを [ホストされたファイアウォール] に変更します。アクションフィールドは、リダイレクトに自動入力されます。ドロップダウンリストから、** ホストされたファイアウォールテンプレートとサービスリダイレクトインターフェイスを選択します **。[追加] をクリックします。

Priority: 100

Policy Type: Hosted Firewall ▼

Match Criteria

From Zones

Zone	Enable
Any	<input checked="" type="checkbox"/>
Default_LAN_Zone	<input type="checkbox"/>
Inter_Routing_Domain_Zone	<input type="checkbox"/>
Internet_Zone	<input type="checkbox"/>

To Zones

Zone	Enable
Any	<input checked="" type="checkbox"/>
Default_LAN_Zone	<input type="checkbox"/>
Inter_Routing_Domain_Zone	<input type="checkbox"/>
Internet_Zone	<input type="checkbox"/>

Traffic Match Type: IP Protocol ▼

IP Protocol: Any ▼

DSCP: Any ▼

☐ Match Established

Application Objects: Any ▼

Source Service Type: Any ▼

Source Service Name: Any ▼

Source IP: *

Source Port: *

Dest Service Type: Any ▼

Dest Service Name: Any ▼

Dest IP: *

Dest Port: *

Actions

Action: Redirect ▼

☒ Allow Fragments

Connection State Tracking: No Tracking ▼

Hosted Firewall Template: PaloAlto-NGFW ▼

Service Redirection Interface: INTERNET-OUT ▼

すべてのネットワーク構成が起動して実行モードになっている間は、[監視]>[ファイアウォール]>[統計 リスト]の[フィルタポリシー]を選択して接続を監視できます。

Dashboard

Monitoring

Configuration

Statistics

Flows

Routing Protocols

Firewall

IKE/IPsec

ICMP

Performance Reports

Qos Reports

Usage Reports

Availability Reports

Appliance Reports

DHCP Server/Relay

VRRP

PPPoE

DNS

Monitoring > Firewall

Firewall Statistics

Statistics: Filter Policies

Maximum entries to display: 50

Filtering: Application: Any Family: Any IP Protocol: Any

Filter Policy Action: Any Source Service Type: Any Source Service Name: Any Source IP:

Destination Service Type: Any Destination Service Name: Any Destination IP:

Source Port: Destination Port: Source Zone: Any Destination Zone: Any DSCP: Any

Refresh Show latest data.

Help

Filter Policies

Default Policy=Allow(Not Tracked) Packets=42 Bytes=3528 Match In Progress Packets=0 Bytes=0

ID	Application	Family	IP Protocol	DSCP	Service Type	Service Name	IP Address	Port or ICMP Type	Zone	Service Type	Service Name	IP Address	Port or ICMP Code	Zone	Action	Conn Match Type	Track Connection	Allow Fragments
1	*	*	*	*	*	-	*	NA	*	Internet	-	*	NA	*	Redirect	Symmetric	No	Yes
2	*	*	*	*	Internet	-	*	NA	*	*	-	*	NA	*	Redirect	Symmetric	No	Yes
3	*	*	*	*	*	-	*	NA	*	Virtual Path	-	*	NA	*	Redirect	Symmetric	No	Yes
4	*	*	*	*	Virtual Path	-	*	NA	*	*	-	*	NA	*	Redirect	Symmetric	No	Yes
5	*	*	*	*	* IPHost	-	*	NA	*	*	-	*	NA	*	Allow	Symmetric	No	Yes
6	*	*	TCP	*	Internet	-	*	Internet_Zone	*	172.147.93.174/32	5001	*	Allow	Symmetric	No	Yes	Yes	
7	*	*	UDP	*	Internet	-	*	Internet_Zone	*	172.147.93.174/32	5001	*	Allow	Symmetric	No	Yes	Yes	
8	*	*	*	*	Internet	-	*	NA	*	*	-	*	NA	*	Drop	Symmetric	No	Yes

Filter Policies Displayed: 8 Filter Policies In Use: 8/1000

Palo Alto Networks UI を使用して、SD-WAN サービスチェーンテンプレートで行った設定と Palo Alto Networks 設定の間のマッピングを確認できます。

paloalto

Dashboard

ACC

Monitor

Policies

Objects

Network

Device

Commit

Config

Search

Interfaces

Virtual Wires

Virtual Routers

IPSec Tunnels

GRE Tunnels

DHCP

DNS Proxy

GlobalProtect

Portals

Gateways

MDM

Device Block List

Clientless Apps

Clientless App Groups

QoS

LLDP

Network Profiles

GlobalProtect IPSec Crypto

IKE Gateways

IPSec Crypto

IKE Crypto

Monitor

Interface Mgmt

Zone Protection

QoS Profile

LLDP Profile

BFD Profile

Ethernet

VLAN

Loopback

Tunnel

Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Tag	VLAN / Virtual Wire	Security Zone	Features	Comment
ethernet1/1	Virtual Wire		none	none	none	Untagged	VWIRE-INET	LAN		
ethernet1/1.10	Virtual Wire		none	none	none	10	VWIRE-INTRANET	LAN		
ethernet1/2	Virtual Wire		none	none	none	Untagged	VWIRE-INET	Internet		
ethernet1/2.10	Virtual Wire		none	none	none	10	VWIRE-INTRANET	Internet		
ethernet1/3			none	none	none	Untagged	none	none		
ethernet1/4			none	none	none	Untagged	none	none		
ethernet1/5			none	none	none	Untagged	none	none		
ethernet1/6			none	none	none	Untagged	none	none		
ethernet1/7			none	none	none	Untagged	none	none		
ethernet1/8			none	none	none	Untagged	none	none		
ethernet1/9			none	none	none	Untagged	none	none		
ethernet1/10			none	none	none	Untagged	none	none		
ethernet1/11			none	none	none	Untagged	none	none		
ethernet1/12			none	none	none	Untagged	none	none		
ethernet1/13			none	none	none	Untagged	none	none		
ethernet1/14			none	none	none	Untagged	none	none		
ethernet1/15			none	none	none	Untagged	none	none		
ethernet1/16			none	none	none	Untagged	none	none		

メモ

1100 アプライアンスでクラウドダイレクトまたは **SD-WAN WANOP (PE)** がすでにプロビジョニングされている場合は、Palo Alto ネットワークスの仮想マシンをプロビジョニングできません。

ユースケース—SD-WAN 1100 上のホスト型ファイアウォール

Citrix SD-WAN 1100 アプライアンスを使用して実装されたユースケースシナリオを次に示します。

ユースケース 1: すべてのトラフィックをホストファイアウォールにリダイレクトする

このユースケースは、すべてのトラフィックがホストされた次世代ファイアウォールによって処理される小規模なブランチユースケースに適用されます。リダイレクトされたトラフィックのスループットの量は 100 Mbps に制限されるため、帯域幅要件を考慮する必要があります。

これを実現するには、次のスクリーンショットに示すように、トラフィックに一致するファイアウォールルールを作成し、[** リダイレクトとしてアクション **]を使用します。

Priority: 100

Policy Type: Hosted Firewall

Match Criteria

From Zones

Zone	Enable
Any	<input checked="" type="checkbox"/>
Default_LAN_Zone	<input type="checkbox"/>
Inter_Routing_Domain_Zone	<input type="checkbox"/>
Internet_Zone	<input type="checkbox"/>

To Zones

Zone	Enable
Any	<input checked="" type="checkbox"/>
Default_LAN_Zone	<input type="checkbox"/>
Inter_Routing_Domain_Zone	<input type="checkbox"/>
Internet_Zone	<input type="checkbox"/>

Traffic Match Type: IP Protocol

IP Protocol: Any

DSCP: Any

Match Established: ☐

Application Objects: Any

Source Service Type: Any

Source Service Name: Any

Source IP: *

Source Port: *

Dest Service Type: Any

Dest Service Name: *

Dest IP: *

Dest Port: *

Actions

Action: Redirect

Allow Fragments: ☒

Connection State Tracking: No Tracking

Hosted Firewall Template: PA-Template

Service Redirection Interface: PA-Intf

ユースケース 2: インターネットトラフィックのみをホスト型ファイアウォールにリダイレクトする

このユースケースは、インターネットにバインドされたトラフィックが、サポートされているリダイレクトされたトラフィックのスループットの量を超えないすべてのブランチサイトに適用されます。この場合、データセンターへの

ブランチトラフィックは、データセンターにデプロイされたセキュリティアプライアンス/サービスによって処理されます。

これを実現するには、次のスクリーンショットに示すように、任意のトラフィックに一致するファイアウォールルールを作成し、** リダイレクトとしてアクションを使用します **。

Priority: 100

Policy Type: Hosted Firewall

Match Criteria

From Zones

Zone	Enable
Any	<input checked="" type="checkbox"/>
Default_LAN_Zone	<input type="checkbox"/>
Inter_Routing_Domain_Zone	<input type="checkbox"/>
Internet_Zone	<input type="checkbox"/>

To Zones

Zone	Enable
Any	<input checked="" type="checkbox"/>
Default_LAN_Zone	<input type="checkbox"/>
Inter_Routing_Domain_Zone	<input type="checkbox"/>
Internet_Zone	<input type="checkbox"/>

Traffic Match Type: IP Protocol

IP Protocol: Any

DSCP: Any

☐ Match Established

Application Objects: Any

Source Service Type: Any

Source Service Name: Any

Source IP: *

Source Port: *

Dest Service Type: Internet

Dest Service Name: Any

Dest IP: *

Dest Port: *

Actions

Action: Redirect

☒ Allow Fragments

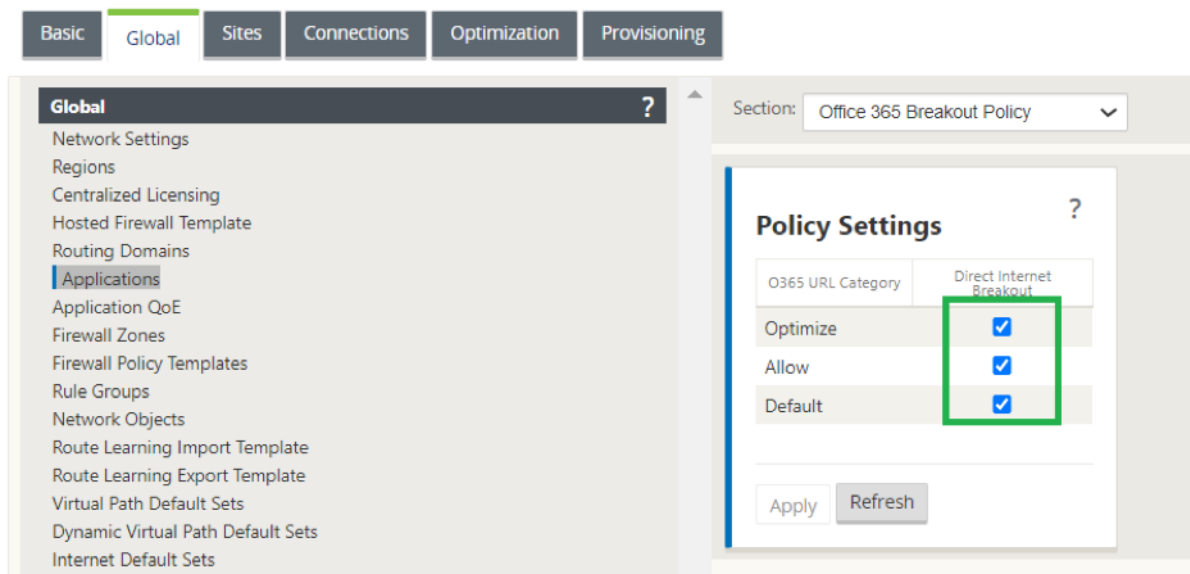
Connection State Tracking: No Tracking

Hosted Firewall Template: PA-Template

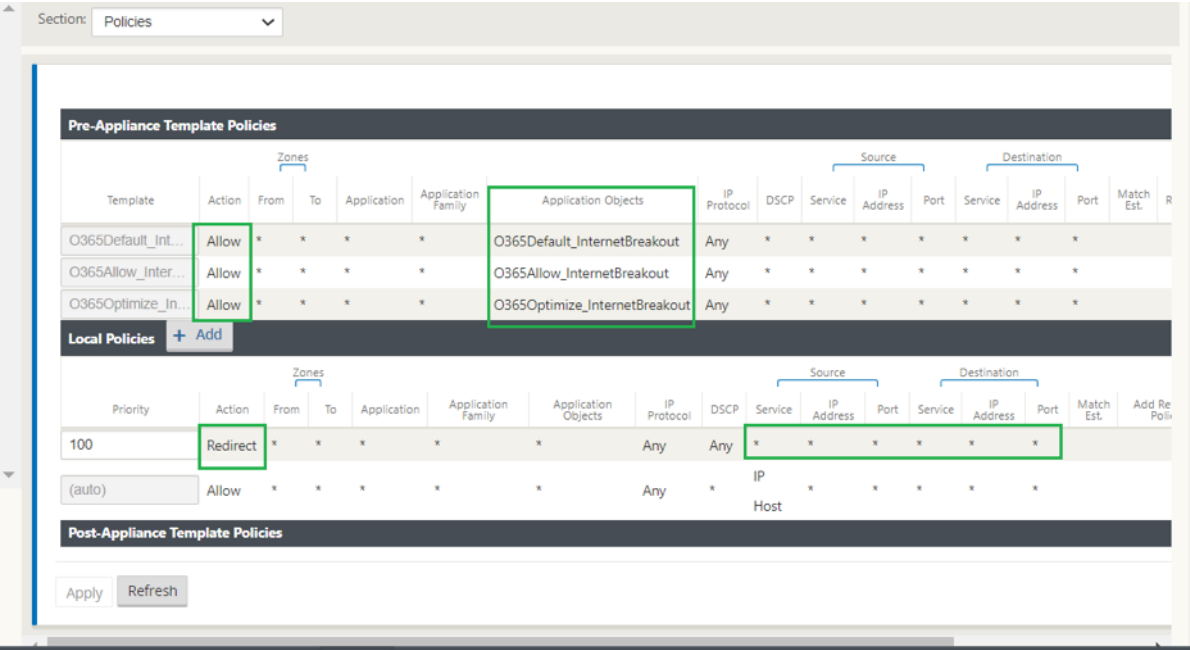
Service Redirection Interface: PA-Intf

ユースケース **3**: 信頼できるインターネット **SaaS** アプリケーション用のインターネットブレイクアウトを直接送信し、残りのすべてのトラフィックをホストされた **VM** にリダイレクトします

このユースケースでは、Office 365 などの信頼できる SaaS アプリケーションに対して直接インターネットブレイクアウトを実行するためのファイアウォール規則が追加されます。次のスクリーンショットに示すように、まず Office 365 ブレイクアウトポリシーを有効にします。



これにより、次のスクリーンショットに示すように、Office 365 トラフィックを許可する事前アプライアンステンプレートポリシーが自動的に追加されます。次に、以下に述べるように、残りのすべてのトラフィックをホストされたファイアウォールにリダイレクトするファイアウォールルールを追加します。



注：
ホストされたファイアウォール構成は、Citrix SD-WAN の構成とは無関係です。したがって、ホストされたファイアウォールは、企業のセキュリティ要件に従って構成できます。

SD-WAN 1100 プラットフォームでの **Check Point** ファイアウォールの統合

November 8, 2021

Citrix SD-WAN は、SD-WAN **1100** プラットフォームでの **Check Point Quantum Edge** のホスティングをサポートしています。

Check Point Quantum Edge は、SD-WAN 1100 プラットフォーム上の仮想マシンとして実行されます。ファイアウォール仮想マシンは、Bridge モードで統合され、2 つのデータ仮想インターフェイスが接続されています。SD-WAN でポリシーを構成することで、必要なトラフィックをファイアウォール仮想マシンにリダイレクトできます。

注

Citrix SD-WAN 11.3.1 以降では、新しいサイトでの仮想マシンのプロビジョニングでは、Check Point 仮想マシンのバージョン 80.20 以上がサポートされています。

長所

次に、SD-WAN 1100 プラットフォームでの Check Point 統合の主な目標または利点を示します。

- 支店デバイスの統合:SD-WAN と高度なセキュリティの両方を実行する単一のアプライアンス
- LAN-to-LAN、LAN-インターネット、およびインターネット-LAN のトラフィックを保護するオンプレム NGFW（次世代ファイアウォール）によるブランチオフィスのセキュリティ

構成の手順

Check Point ファイアウォール仮想マシンを SD-WAN に統合するには、次の構成が必要です。

- ファイアウォール仮想マシンのプロビジョニング
- セキュリティ仮想マシンへのトラフィックリダイレクトを有効にする

注:

トラフィックのリダイレクトを有効にする前に、ファイアウォール仮想マシンを最初にプロビジョニングする必要があります。

プロビジョニング **Check Point** ファイアウォール仮想マシン

ファイアウォール仮想マシンをプロビジョニングするには、次の 2 つの方法があります。

- SD-WAN センターによるプロビジョニング
- SD-WAN アプライアンス GUI によるプロビジョニング

SD-WAN センターを介したファイアウォール仮想マシンの Provisioning

前提条件

- セカンダリストレージを SD-WAN Center に追加して、ファイアウォール VM イメージファイルを保存します。詳細については、「システム要件とインストール」を参照してください。
- ファイアウォール VM イメージファイル用にセカンダリパーティションからストレージを予約します。ストレージ制限を設定するには、[管理] > [ストレージのメンテナンス] に移動します。
 - リストから必要なストレージ量を選択します。
 - [Apply] をクリックします。

Administration / Storage Maintenance

Region: Default Region

Host	File System	Type	Size (MB)	Available (MB)	Active/Migrate Data
Local*	/dev/xvda2	ext3	7288	3471	
Local	/dev/xvdb	ext3	14910	12921	

Apply

Note: Software image storage reserved will be reduced while calculating the secondary partition Size(MB) and Available(MB)

Software Image Storage Reservation

Note: User can modify the storage reservation only if the SD-WAN Center has secondary partition mounted and it should operate in headend mode

Amount of storage to reserve from secondary partition storage(Active) is: 10GB

Apply

Thresholds

SD-WAN Center Database Storage and Auto Cleanup settings are misconfigured, SD-WAN Center will reach auto cleanup threshold before the configured 6 months.

Stop stats polling when storage usage exceeds 55% of active storage size

☐ Notify user when storage usage exceeds 10% of active storage size

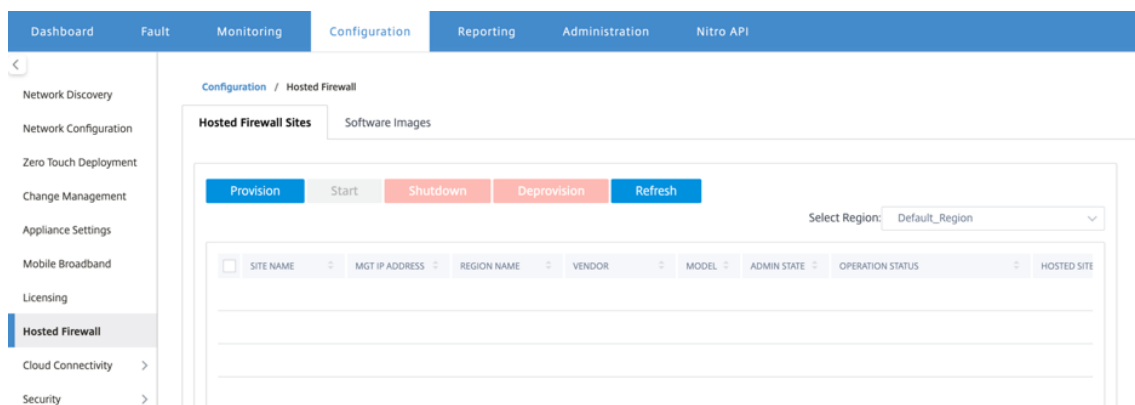
Apply

注:

ストレージは、条件が満たされた場合にアクティブであるセカンダリパーティションから予約されています。

SD-WAN Center プラットフォーム経由でファイアウォール仮想マシンを Provisioning するには、次の手順を実行します。

1. Citrix SD-WAN Center GUI で、[構成] > [ホストされたファイアウォール] を選択します。



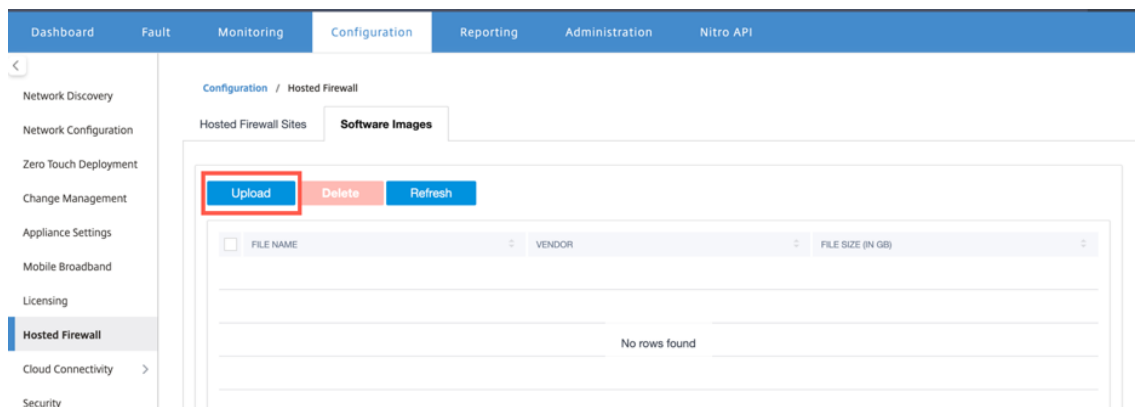
ドロップダウンリストから [Region] を選択すると、選択したリージョンのプロビジョニングされたサイトの詳細を表示できます。

2. ソフトウェアイメージをアップロードします。

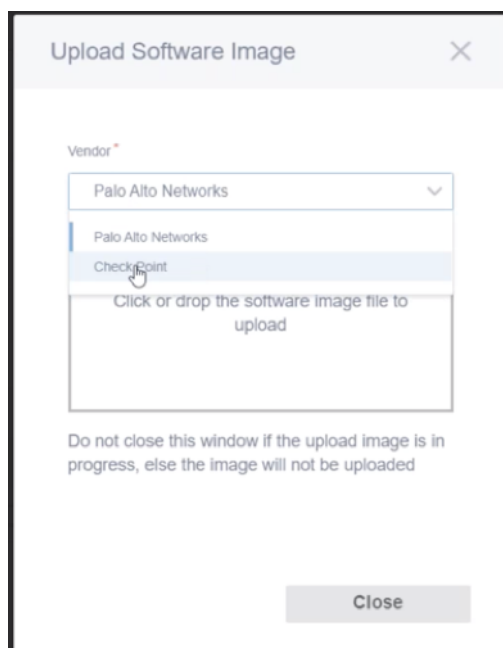
注:

ソフトウェアイメージをアップロードするのに十分なディスク領域があることを確認してください。

[設定] > [ホストされたファイアウォール] > [ソフトウェアイメージ] に移動し、[アップロード] をクリックします。



3. ドロップダウンリストから [**Check Point **] としてベンダー名を選択します。アップロードするボックスに、ソフトウェアイメージファイルをクリックまたはドロップします。



進行中のアップロード処理を示すステータスバーが表示されます。イメージファイルが 100% アップロードされた则表示されるまで、[**Refresh**] をクリックしたり、その他のアクションを実行したりしないでください。

- 更新: [更新] オプションをクリックして、最新のイメージファイルの詳細を取得します。
- 削除: 既存のイメージファイルを削除するには、[削除] オプションをクリックします。

注:

デフォルト以外のリージョンのサイト部分にファイアウォール仮想マシンをプロビジョニングするには、各コレクターノードにイメージファイルをアップロードします。

4. プロビジョニングの場合は、[ホストされたファイアウォールサイト] タブに戻り、[プロビジョニング] をクリックします。

Provision Virtual Machine

Vendor *
Check Point

Vendor Virtual Machine Model *
EDGE

Region *
Region where the sites available

Software Image *
Choose the Image to provision

Please ensure to upload this image in the collector for non-default region sites provisioning

Sites for Firewall Hosting *
Sites to host the firewall

Please ensure to select both primary and secondary sites if the sites are in High availability mode

Management Server Primary IP Address/Domain Name
Enter Management Server Primary IP Address or domain name

Virtual Machine SIC Key
Enter the SIC key

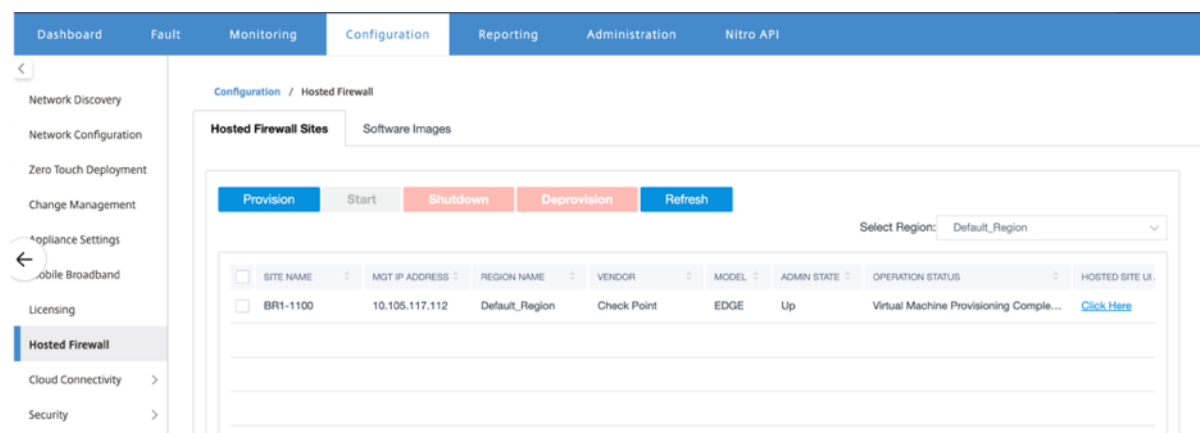
Start Provision Cancel

- 仕入先: ドロップダウンリストから [**Check Point **] として仕入先名を選択します。
- ベンダー仮想マシンモデル: 仮想マシンモデルフィールドは Edge として自動的に入力されます。
- リージョン: リストからリージョンを選択します。
- ソフトウェアイメージ: プロビジョニングするイメージファイルを選択します。
- [ファイアウォールホスティングのサイト]: ファイアウォールホスティングのリストのサイトを選択します。サイトが高可用性モードの場合は、プライマリサイトとセカンダリサイトの両方を選択する必要があります。
- 管理サーバーのプライマリ **IP** アドレス/ドメイン名: 管理プライマリ IP アドレスまたは完全修飾ドメイン名を入力します (オプション)。
- 仮想マシン **SIC** キー: 仮想マシンのセキュア内部通信 (SIC) キーを入力します。SIC は、**Check Point** コンポーネント間に信頼できる接続を作成します。

5. 「プロビジョニングの開始」をクリックします。

6. 最新のステータスを取得するには、[**Refresh**] をクリックします。Check Point 仮想マシンが完全に起動すると、SD-WAN Center UI に反映されます。

必要に応じて、仮想マシンを開始、シャットダウン、プロビジョニング解除 できます。

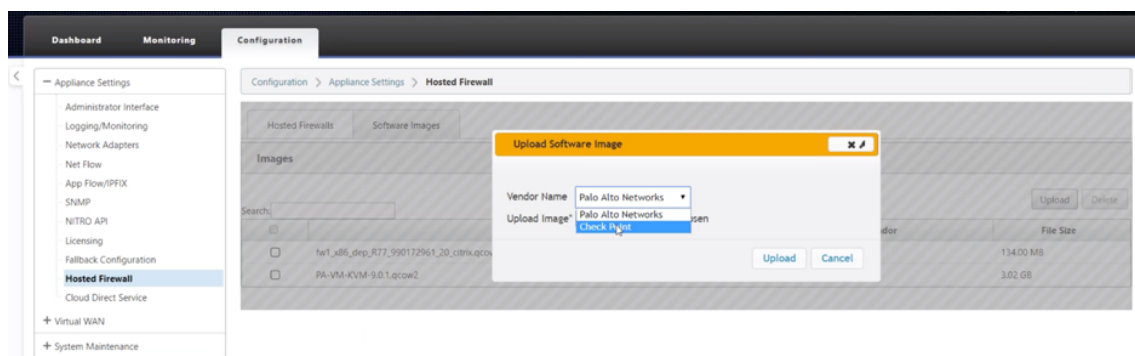


- サイト名: サイト名が表示されます。
- 管理 IP: サイトの管理 IP アドレスを表示します。
- リージョン名: リージョン名が表示されます。
- 仕入先: 仕入先名 (Check Point) が表示されます。
- [モデル]: モデル- エッジを表示します。
- 管理状態: ベンダー仮想マシンの状態 (アップ/ダウン)。
- 操作ステータス: 最後の工程ステータスメッセージを表示します。
- ホストサイト **UI** アクセス: Check Point 仮想マシンの GUI にアクセスするには、**【ここをクリック】** リンクを使用します。

SD-WAN アプライアンスの GUI によるファイアウォール仮想マシンの Provisioning

SD-WAN プラットフォームで、ホストされた仮想マシンをプロビジョニングして起動します。Provisioning の手順は、次のとおりです。

1. Citrix SD-WAN GUI から、[構成] >> [アプライアンスの設定] [ホストされたファイアウォール] を選択します。
2. ソフトウェアイメージをアップロードします。
 - [ソフトウェアイメージ] タブを選択します。 **Check Point** としてベンダー名を選択します。
 - ソフトウェアイメージファイルを選択します。
 - [アップロード] をクリックします。

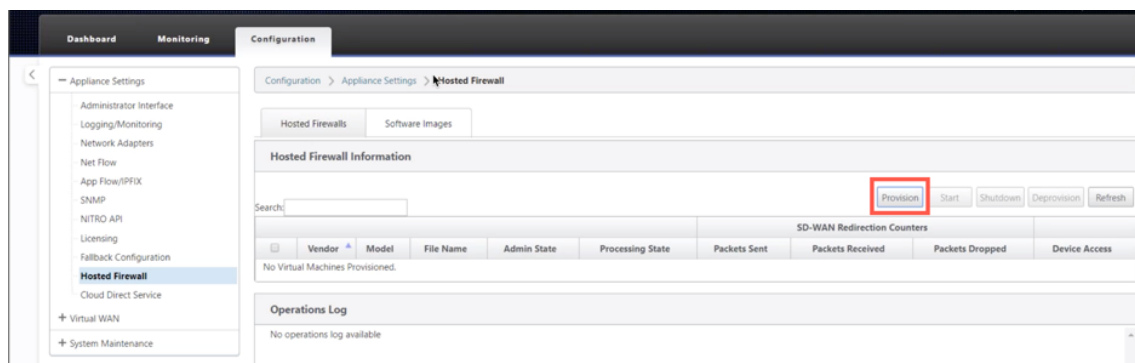


注:

アップロードできる画像は最大2つです。Check Point 仮想マシンイメージのアップロードには、帯域幅の可用性によっては、時間がかかる場合があります。

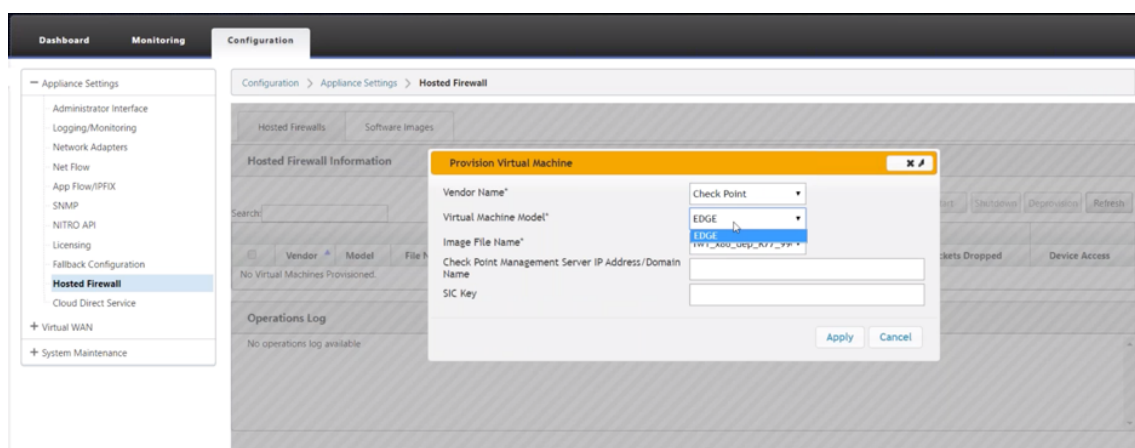
アップロードプロセスを追跡するステータスバーが表示されます。画像が正常にアップロードされると、ファイルの詳細が反映されます。Provisioning に使用されるイメージは削除できません。画像ファイルに 100% アップロードされた则表示されるまで、アクションを実行したり、他のページに戻ったりしないでください。

3. プロビジョニングの場合は、[ホストされたファイアウォール] タブを選択し、[プロビジョニング] ボタンをクリックします。

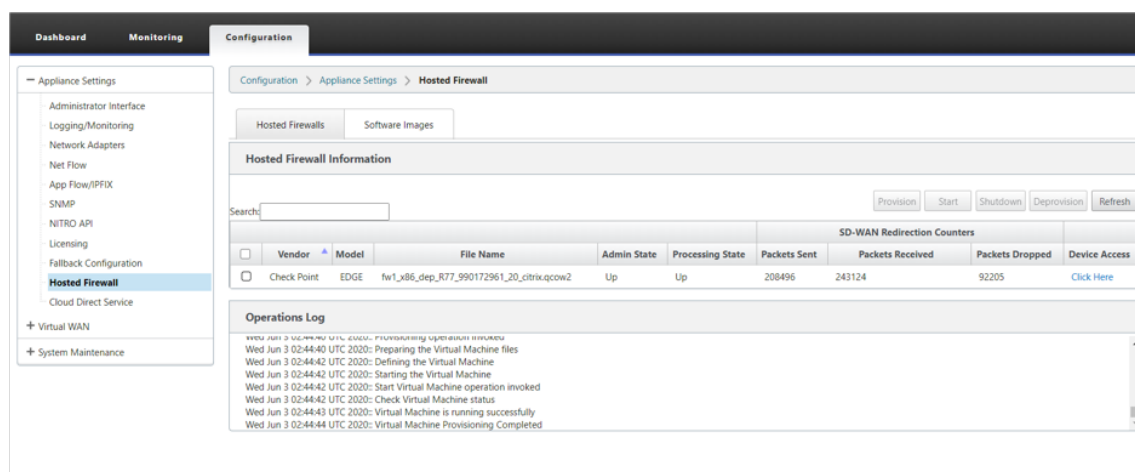


4. Provisioning について次の詳細を入力します。

- 仕入先名: **Check Point** として仕入先名を選択します。
- 仮想マシンモデル: 仮想マシンモデルは **Edge** として自動的に入力されます。
- [イメージファイル名]: イメージファイル名が自動入力されます。
- Check Point** 管理サーバーの **IP** アドレス/ドメイン: Check Point 管理サーバーの IP アドレス/ドメインを指定します。
- SIC** キー: SIC キーを指定します (オプション)。SIC は、**Check Point** コンポーネント間に信頼できる接続を作成します。[Apply] をクリックします。



5. 最新のステータスを取得するには、[**Refresh**] をクリックします。Check Point 仮想マシンが完全に起動すると、操作ログの詳細とともに SD-WAN UI に反映されます。



- 管理状態: 仮想マシンが起動中か停止中かを示します。
- 処理状態: 仮想マシンのデータベース処理状態。
- パケット送信: SD-WAN からセキュリティ仮想マシンに送信されたパケット。
- 受信パケット: SD-WAN がセキュリティ仮想マシンから受信したパケット。
- パケットドロップ: SD-WAN によってドロップされたパケット (セキュリティ仮想マシンがダウンしている場合など)。
- デバイスアクセス: セキュリティ仮想マシンへの GUI アクセスを取得するには、リンクをクリックします。

必要に応じて、仮想マシンを開始、シャットダウン、プロビジョニング解除できます。【[ここをクリック](#)】オプションを使用して、Check Point 仮想マシンの GUI にアクセスするか、管理 IP と 4100 ポート (管理 IP: 4100) を使用します。

注:

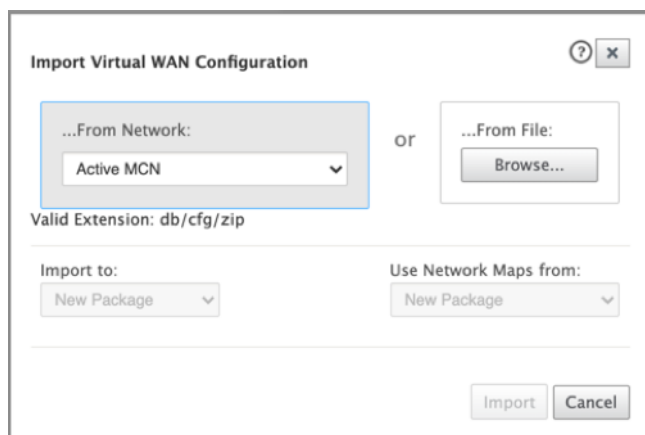
Check Point GUI にアクセスするには、常にシークレットモードを使用してください。

トラフィックをエッジにリダイレクト

トラフィックリダイレクトの設定は、MCN の構成エディターまたは SD-WAN Center の構成エディターを使用して行うことができます。

SD-WAN センターで構成エディター内を移動するには、次の手順を実行します。

1. Citrix SD-WAN Center UI を開き、[構成] > [ネットワーク構成のインポート] に移動します。アクティブ MCN から仮想 WAN 設定をインポートし、[**Import**] をクリックします。



残りの手順は、MCN を介したトラフィックリダイレクション設定と同様です。

MCN の構成エディタ内を移動するには、次の手順を実行します。

1. [グローバル] > [ネットワーク設定] で [接続の一致タイプ] を対称に設定します。

Global

- Network Settings
- Regions
- Centralized Licensing
- Hosted Firewall Template
- Routing Domains
- Applications
- Application QoE
- Firewall Zones
- Firewall Policy Templates
- Rule Groups
- Network Objects
- Route Learning Import Template
- Route Learning Export Template
- Virtual Path Default Sets
- Dynamic Virtual Path Default Sets
- Internet Default Sets
- Intranet Default Sets
- DHCP Option Sets
- DNS Services
- Proxy Auto-config settings
- Autopath Groups
- Service Providers
- WAN-to-WAN Forwarding Groups
- WAN Optimization Features
- WAN Optimization Tuning Settings
- WAN Optimization Application Classifiers
- WAN Optimization Service Classes

Global Security Settings

Note: Changing the **Network Encryption Mode** may cause **Site Secure Keys** to be truncated or regenerated if they do not meet the requirements of the new mode.

Network Encryption Mode: AES 128-Bit

☒ Enable Encryption Key Rotation

☐ Enable Extended Packet Encryption Header

☐ Enable Extended Packet Authentication Trailer

Extended Packet Authentication Trailer Type: 32-Bit Checksum

☐ Enable FIPS Mode

☐ Enable Appliance Authentication

Network Secure Key: 72d050ce5ca54c... **Regenerate**

Global Firewall Settings

Global Policy Template: New_Firewall_... Default Firewall Action: Allow ☒ Default Connection State Tracking

Connection Match Type: Symmetric

Denied Timeout (s): 30

TCP Initial Timeout (s): 120 TCP Idle Timeout (s): 7440

TCP Closing Timeout (s): 60 TCP Time Wait Timeout (s): 120 TCP Closed Timeout (s): 10

UDP Initial Timeout (s): 30 UDP Idle Timeout (s): 300

ICMP Initial Timeout (s): 30 ICMP Idle Timeout (s): 60

Generic Initial Timeout (s): 30 Generic Idle Timeout (s): 300

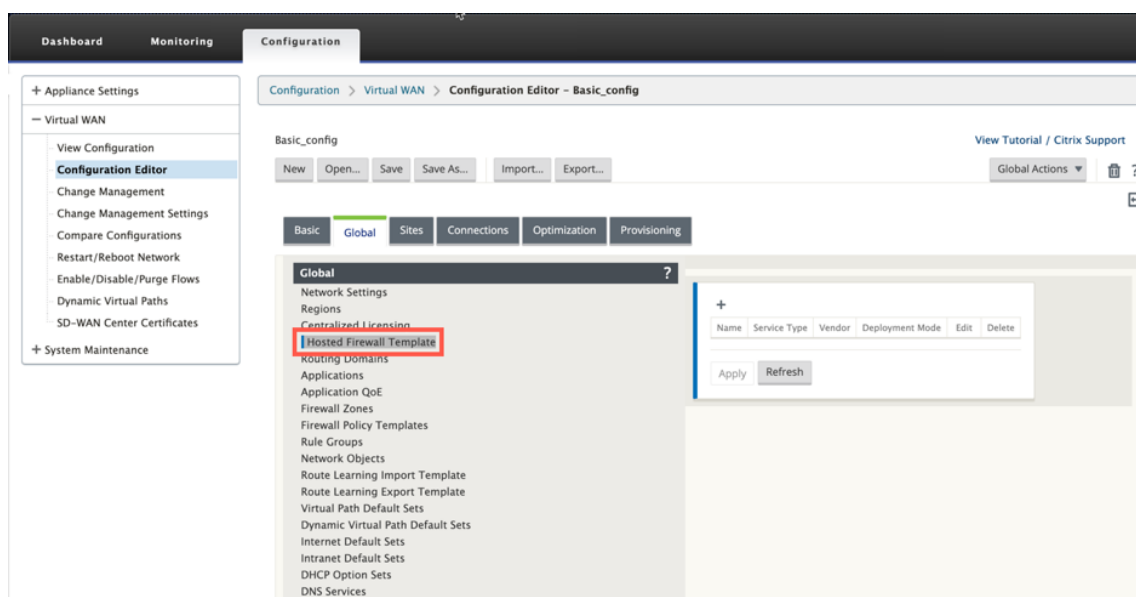
Global On-Demand Bandwidth Limit Setting

Default maximum total WAN-to-LAN bandwidth, as a percentage of bandwidth provided by non-standby WAN links in the Virtual Path (%): 120

Apply **Revert**

デフォルトでは、SD-WAN ファイアウォールポリシーは方向固有です。対称マッチタイプは、指定された一致基準を使用して接続を照合し、両方向に対してポリシーアクションを適用します。

2. Citrix SD-WAN UI を開き、[構成] [仮想 **WAN** の展開] [構成エディター] を選択し、[グローバル] セクションの [ホストされたファイアウォールテンプレート] を選択します。



3. [+] をクリックし、ホストされたファイアウォールテンプレートを追加するには、次のスクリーンショットで利用可能な必要な情報を入力します。[追加] をクリックします。

×

Edit

Name:

CheckPoint-NGFW

Model:

Edge

Primary Management Server IP/FQDN:

Vendor

Check Point

Deployment Mode:

Bridge

Secondary Management Server IP/FQDN:

Service Redirection Interfaces

+

Name	Input Interface	Output Interface	VLAN ID	Delete
INTERNET-OUT	Interface-1	Interface-2	0	
INTERNET-IN	Interface-2	Interface-1	0	

Apply

Cancel

ホストされたファイアウォールテンプレートを使用すると、SD-WAN プラットフォームでホストされているファイアウォール仮想マシンへのトラフィックリダイレクトを構成できます。テンプレートを構成するために必要な入力は次のとおりです。

- 名前: ホストされているファイアウォールテンプレートの名前。
- ベンダー: ファイアウォールのベンダーの名前—Check Point。
- 配置モード: [配置モード] フィールドは自動的に入力され、グレー表示されます。**Check Point** ベンダーの場合、展開モードは **Bridge** です。

- モデル: ホストされたファイアウォールの仮想マシンモデル。 **Check Point** としてベンダーを選択すると、モデルフィールドにエッジが自動的に入力されます。
- プライマリ管理サーバー **IP/FQDN**: プライマリ管理サーバー IP/FQDN。
- セカンダリ管理サーバー **IP/FQDN**: セカンダリ管理サーバー IP/FQDN。
- サービスリダイレクトインターフェイス: SD-WAN とホストされるファイアウォール間のトラフィックリダイレクトに使用される論理インターフェイスです。

(注

) リダイレクト入力インターフェイスは、接続イニシエータの方向から選択する必要があります。出力インターフェイスは、応答トラフィックに対して自動的に選択されます。たとえば、発信インターネットトラフィックが Interface-1 でホストされているファイアウォールにリダイレクトされると、応答トラフィックは Interface-2 でホストされているファイアウォールに自動的にリダイレクトされます。また、インターネットインバウンドトラフィックがない場合は、Interface-2 は必要ありません。

Check Point 仮想マシンに割り当てられるデータインターフェイスは 2 つだけです。

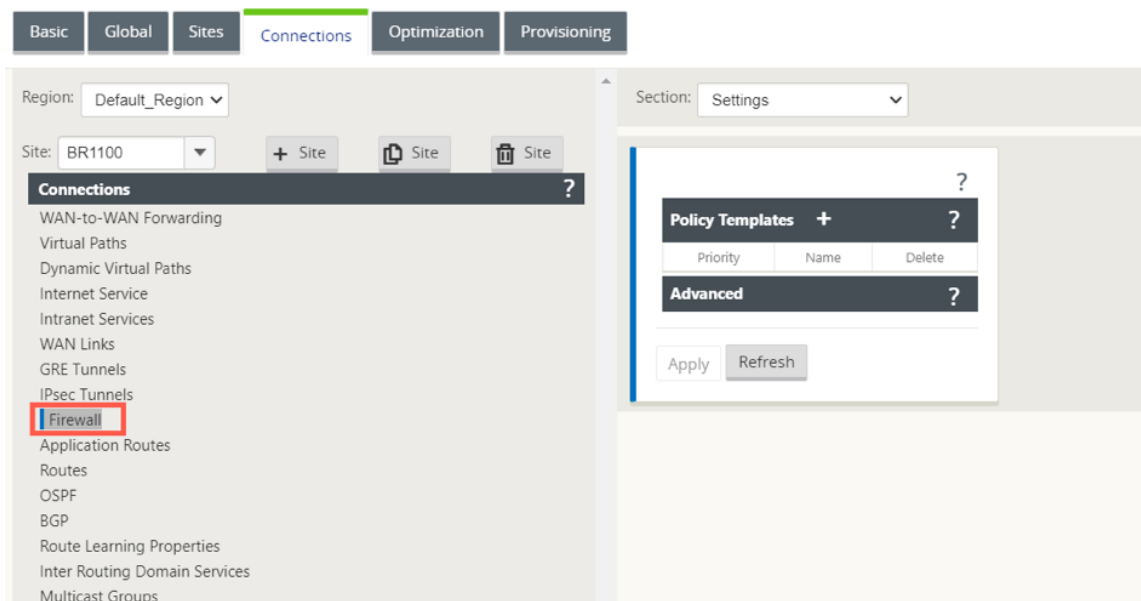
注:

SD-WAN ファイアウォールポリシーは、ホストされたファイアウォール管理サーバーとのトラフィックを許可するように自動的に作成されます。これにより、ホストされたファイアウォール宛ての管理トラフィック（または）がリダイレクトされるのを回避できます。

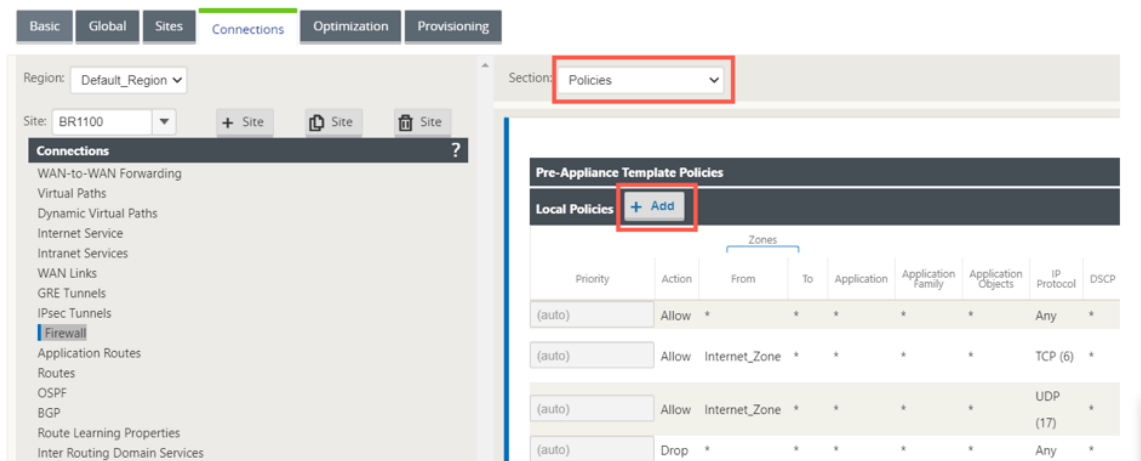
ファイアウォール仮想マシンへのトラフィックのリダイレクトは、SD-WAN ファイアウォールポリシーを使用して実行できます。SD-WAN ファイアウォールポリシーを作成するには、[**Global**] セクションのファイアウォールポリシーテンプレートを使用するか、サイトレベルで作成する方法の 2 つがあります。

方法-1

1. Citrix SD-WAN GUI から、[構成] > [仮想 **WAN**] を展開し、[構成エディタ] に移動します。接続の下 [ファイアウォール] を選択します。



2. [セクション] ドロップダウンリストから [ポリシー] を選択し、[+ 追加] をクリックしてファイアウォールポリシーを作成します。



3. ポリシータイプを [ホストされたファイアウォール] に変更します。アクションフィールドは、リダイレクトに自動入力されます。ドロップダウンリストから、** ホストされたファイアウォールテンプレートとサービスリダイレクトインターフェイスを選択します **。[追加] をクリックします。

Priority: 400

Policy Type: Hosted Firewall

Match Criteria

From Zones

Zone	Enable
Any	<input checked="" type="checkbox"/>
Default_LAN_Zone	<input type="checkbox"/>
Inter_Routing_Domain_Zone	<input type="checkbox"/>
Internet_Zone	<input type="checkbox"/>

To Zones

Zone	Enable
Any	<input checked="" type="checkbox"/>
Default_LAN_Zone	<input type="checkbox"/>
Inter_Routing_Domain_Zone	<input type="checkbox"/>
Internet_Zone	<input type="checkbox"/>

Traffic Match Type: IP Protocol

IP Protocol: Any

DSCP: Any

☐ Match Established

Application Objects: Any

Source Service Type: Any

Source Service Name: Any

Source IP: *

Source Port: *

Dest Service Type: Any

Dest Service Name: Any

Dest IP: *

Dest Port: *

Actions

Action: Redirect

☒ Allow Fragments

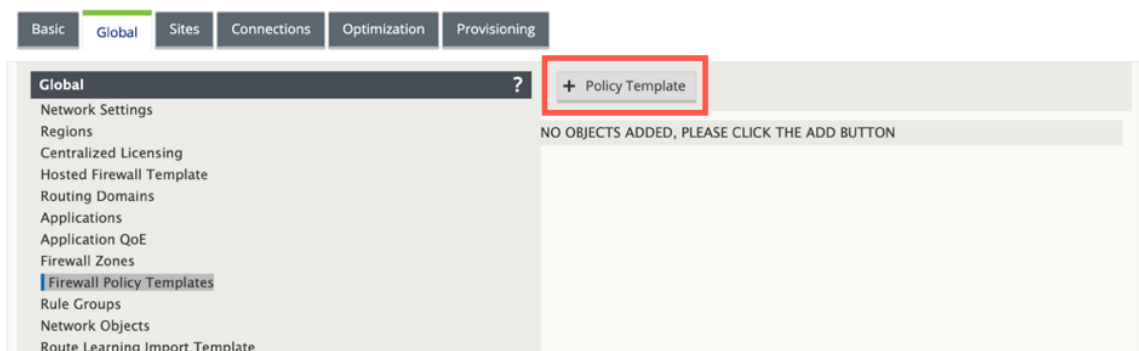
Connection State Tracking: No Tracking

Hosted Firewall Template: CheckPoint-NGFW

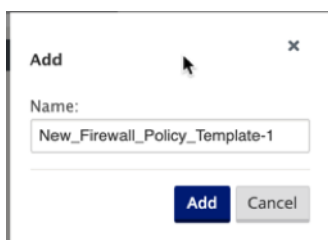
Service Redirection Interface: INTERNET-OUT

方法-2

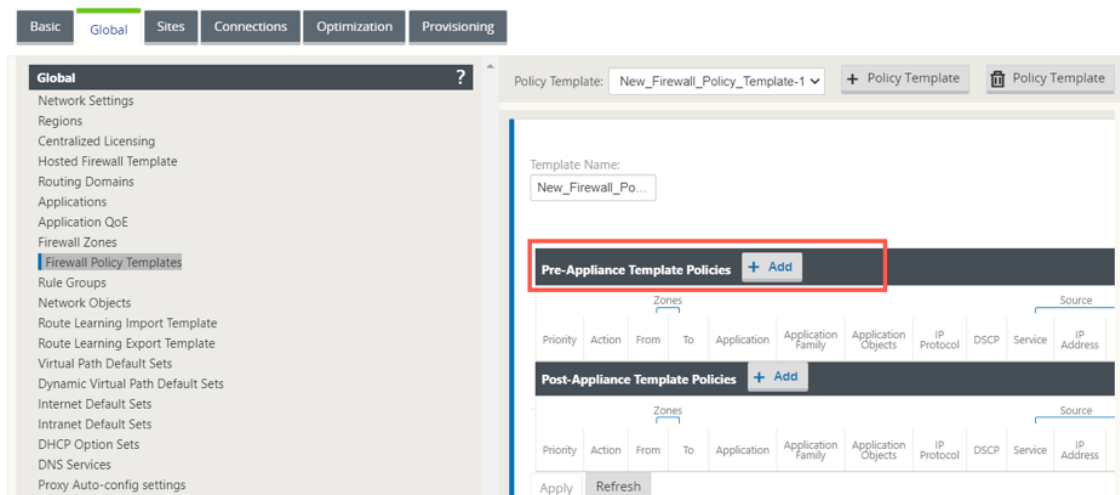
1. [グローバル] タブに移動し、[ファイアウォールポリシーテンプレート] を選択します。[+ ポリシーテンプレート] をクリックします。



2. ポリシーテンプレートに名前を指定し、[Add] をクリックします。



3. [プレアプライアンステンプレートポリシー] の横にある [+ 追加] をクリックします。



4. ポリシータイプを【ホストされたファイアウォール】に変更します。[アクション] フィールドは [リダイレクト] に自動的に入力されます。ドロップダウンリストから、** ホストされたファイアウォールテンプレートとサービスリダイレクトインターフェイスを選択します **。[追加] をクリックします。

Priority: Policy Type: **Hosted Firewall**

Match Criteria

From Zones

Zone	Enable
Any	<input checked="" type="checkbox"/>
Default_LAN_Zone	<input type="checkbox"/>
Inter_Routing_Domain_Zone	<input type="checkbox"/>
Internet_Zone	<input type="checkbox"/>

To Zones

Zone	Enable
Any	<input checked="" type="checkbox"/>
Default_LAN_Zone	<input type="checkbox"/>
Inter_Routing_Domain_Zone	<input type="checkbox"/>
Internet_Zone	<input type="checkbox"/>

Traffic Match Type: **IP Protocol** IP Protocol: **Any** DSCP: **Any** ☐ Match Established

Application Objects: **Any**

Source Service Type: **Any** Source Service Name: **Any** Source IP: Source Port:

Dest Service Type: **Any** Dest Service Name: **Any** Dest IP: Dest Port:

Actions

Action: **Redirect** ☒ Allow Fragments Connection State Tracking: **No Tracking**

Hosted Firewall Template: **CheckPoint-NGFW** Service Redirection Interface: **INTERNET-OUT**

5. [接続] > [ファイアウォール] に移動し、[名前] フィールドで (作成した) ファイアウォールポリシーを選択します。[**Apply**] をクリックします。

Basic Global Sites **Connections** Optimization Provisioning

Region: **Default_Region**

Site: **BR1100** + Site Site Site

Connections

- WAN-to-WAN Forwarding
- Virtual Paths
- Dynamic Virtual Paths
- Internet Service
- Intranet Services
- WAN Links
- GRE Tunnels
- IPsec Tunnels
- Firewall**
- Application Routes
- Routes
- OSPF
- BGP
- Route Learning Properties
- Inter Routing Domain Services
- Multicast Groups

Section: **Settings**

Policy Templates + ?

Priority	Name	Delete
100	New_Firewall_P...	

Advanced ?

Apply Revert

すべてのネットワーク構成が起動して実行モードになっている間は、[監視]>[ファイアウォール]>[統計リスト]の[フィルタポリシー]を選択して接続を監視できます。

Dashboard

Monitoring

Configuration

Statistics

Flows

Routing Protocols

Firewall

IKE/IPsec

ICMP

Performance Reports

Qos Reports

Usage Reports

Availability Reports

Appliance Reports

DHCP Server/Relay

VRRP

PPPoE

DNS

Monitoring > Firewall

Firewall Statistics

Statistics: Filter Policies

Maximum entries to display: 50

Filtering: Application: Any Family: Any IP Protocol: Any

Filter Policy Action: Any Source Service Type: Any Source Service Name: Any Source IP: *

Destination Service Type: Any Destination Service Name: Any Destination IP: *

Source Port: * Destination Port: * Source Zone: Any Destination Zone: Any DSCP: Any

Refresh

Show latest data.

Help

Filter Policies

Default Policy-Allow(Not Tracked) Packets=42 Bytes=3528

Match In Progress Packets=0 Bytes=0

ID	Application	Family	IP Protocol	DSCP	Source				Destination				Action	Conn Match Type	Track Connection	Allow Fragments		
					Service Type	Service Name	IP Address	Port or ICMP Type	Zone	Service Type	Service Name	IP Address					Port or ICMP Type	Zone
1	*	*	*	*	*	-	*	NA	*	Internet	-	*	NA	*	Redirect	Symmetric	No	Yes
2	*	*	*	*	Internet	-	*	NA	*	*	-	*	NA	*	Redirect	Symmetric	No	Yes
3	*	*	*	*	*	-	*	NA	*	Virtual Path	-	*	NA	*	Redirect	Symmetric	No	Yes
4	*	*	*	*	Virtual Path	-	*	NA	*	*	-	*	NA	*	Redirect	Symmetric	No	Yes
5	*	*	*	*	* IPHost	-	*	NA	*	*	-	*	NA	*	Allow	Symmetric	No	Yes
6	*	*	TCP	*	Internet	-	*	Internet_Zone	*	172.147.93.174/32	5001	*	Allow	Symmetric	No	Yes	Yes	
7	*	*	UDP	*	Internet	-	*	Internet_Zone	*	172.147.93.174/32	5001	*	Allow	Symmetric	No	Yes	Yes	
8	*	*	*	*	Internet	-	*	NA	*	*	-	*	NA	*	Drop	Symmetric	No	Yes

Filter Policies Displayed: 8

Filter Policies In Use: 8/1000

リンク集約グループ

November 8, 2021

リンク集約グループ（LAG）機能を使用すると、SD-WAN アプライアンス上の 2 つ以上のポートをグループ化して、1 つのポートとして連携させることができます。これにより、可用性の向上、リンクの冗長性、およびパフォーマンスの向上が保証されます。

以前は、LAG ではアクティブ-バックアップ・モードのみがサポートされていました。Citrix SD-WAN 11.3 リリース以降では、802.3AD リンクアグリゲーション制御プロトコル（LACP）プロトコルベースのネゴシエーションがサポートされています。LACP は標準プロトコルであり、LAG 用のより多くの機能を提供します。

アクティブバックアップモードでは、いつでも 1 つのポートだけがアクティブになり、他のポートはバックアップモードになります。アクティブサポートおよびバックアップサポートは、LAG 機能についてデータプレーン開発キット (DPDK) パッケージに依存しています。

LACP を使用すると、すべてのポートで同時にトラフィックを送信できます。利点として、リンク冗長メカニズムと

ともに帯域幅を増やすことができます。LACP 実装では、アクティブ-アクティブモードがサポートされています。アクティブ-バックアップモードでは、SD-WAN UI からフル LACP アクティブ-アクティブモードを選択することもできます。

LAG 機能は、次の DPDK でサポートされているプラットフォームでのみ使用できます。

- Citrix SD-WAN 110 SE
- Citrix SD-WAN 210 SE
- Citrix SD-WAN 410 SE
- Citrix SD-WAN 1100 SE/PE
- Citrix SD-WAN 4100、および 5100 SE
- Citrix SD-WAN 6100 SE
- Citrix SD-WAN 2100 SE

LACP LAG 機能は、次のプラットフォームでは使用できません。

- Citrix SD-WAN 1000 SE/PE
- Citrix SD-WAN 2000 SE/PE
- Citrix SD-WAN 4000 SE

注

LAG 機能は、VPX/VPXL プラットフォームではサポートされていません。

制限事項

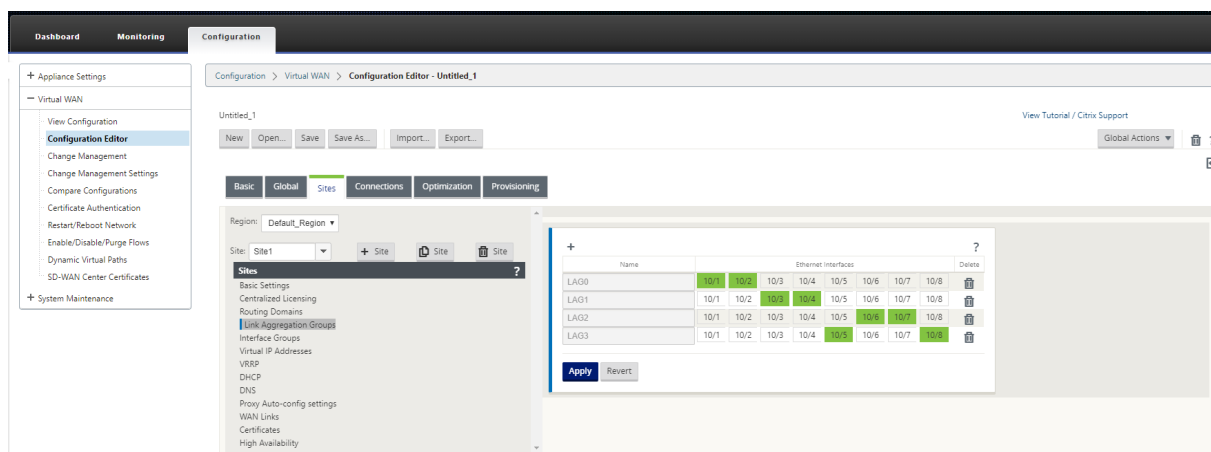
- Citrix SD-WAN アプライアンスの各 LAG にグループ化された最大 4 つのポートを持つ最大 4 つの LAG を作成できます。
- ポートプライオリティおよびシステムプライオリティオプションは、LACP 実装ではサポートされません。

11.3 リリース以降、LACP 実装の SD-WAN では、ポートは常にアクティブモードになります。つまり、SD-WAN は常にネゴシエーションを開始できます。

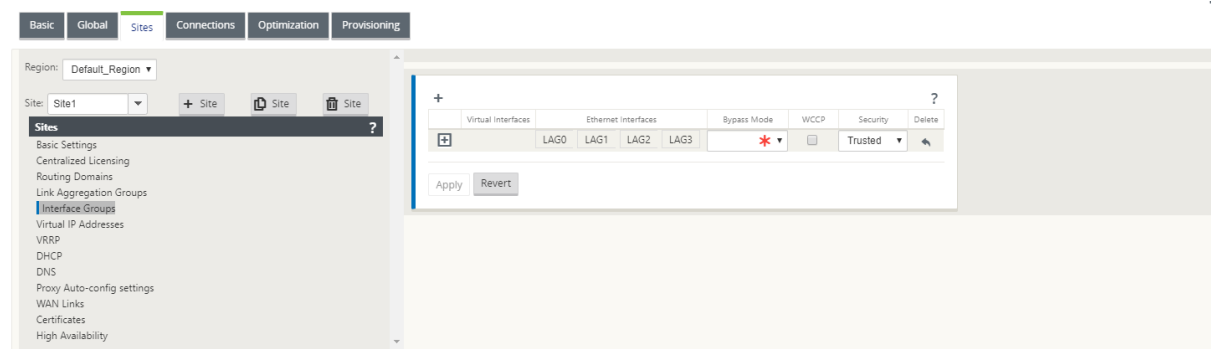
注

Citrix SD-WAN 210 および 410 アプライアンスの場合、最大 3 つのポートをグループ化した LAG を 1 つだけ作成できます。

リンク集約グループを構成するには、構成エディタで、[サイト] > [リンク集約グループ] に移動します。使用可能なすべての物理ポートとイーサネットインターフェイスを表示できます。[+] をクリックして LAG を作成します。



メンバーポートを選択し、[**Apply**] をクリックします。ポートが LAG に追加されると、メンバーポートではなく、インターフェイスグループ内の LAG だけが表示されます。



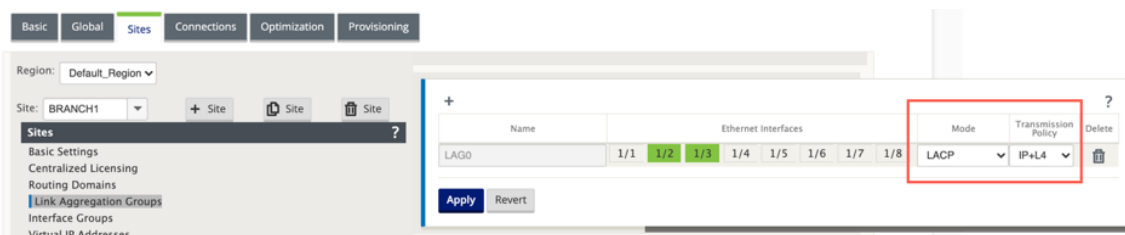
同様に、LAG を LACP モードで設定する場合は、次のようにします。

1. [**+**] をクリックして LAG を作成し、イーサネットインターフェイスポートを選択します。
2. ドロップダウンリストから **LACP** として構成モードを選択します。
3. ドロップダウンリストから [転送ポリシー] を選択します。

注:

モードがアクティブ-バックアップとして選択した場合、[転送ポリシー] フィールドは無効になります。

4. [**Apply**] をクリックします。



LAG グループには多数のポートが存在するため、転送ポリシーは、トラフィックの送信に使用できるポートを選択す

るのに役立ちます。転送ポリシーフィールドは、集約モードがアクティブ-アクティブの場合にのみ有効にできます。MAC+IP と IP+L4 の 2 つの転送ポリシーが定義されています。

- **MAC+IP:** 特定のパケットのリンク選択は、レイヤ 2 および 3 パラメータに基づいています。したがって、送信元および宛先の MAC アドレスと IP アドレスは、これらのパラメータを取り、ハッシュします。ハッシュによると、それはポートを選択します。
- **IP+L4:** IP+L4 ポリシーは、送信元と宛先 IP、およびレイヤ 4 ポートおよびプロトコルに基づいています。IP+L4 ポリシーは、どのパケットがどのポートを通過するかを通知します。
同じパラメータを持つパケットは、常にいずれかのリンクに送信されます。つまり、同じフローまたは単一のフロー（送信元と宛先 Mac および IP）は常に同じポートを通過し、他のポートに分散しません。利点として、順序がずれたパケットは宛先デバイスに到達できません

LAG を使用して仮想インターフェイスを作成できます。これらのインターフェイスは、LAN/WAN リンクおよび HA の設定にさらに使用されます。

注

LAG がインターフェイスグループのイーサネットインターフェイスとして使用される場合、[リンクステート伝播 \(LSP\)](#) 機能はサポートされません。

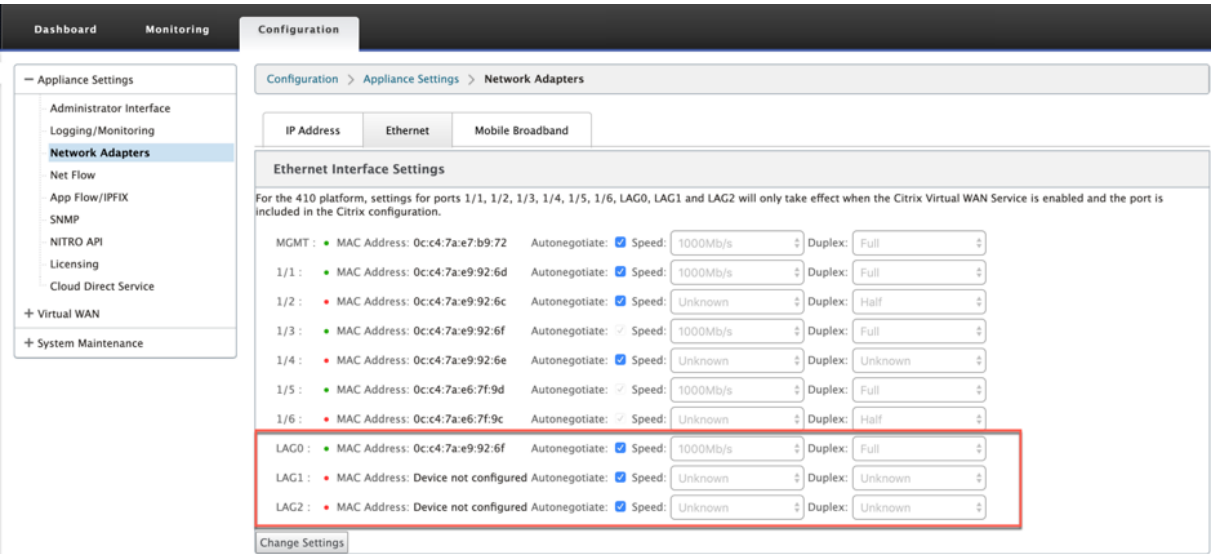
監視とトラブルシューティング

統計またはリンクの状態を表示するには、[監視] > [統計] に移動します。[**Show**] ドロップダウンリストから [**Ethernet**] を選択します。

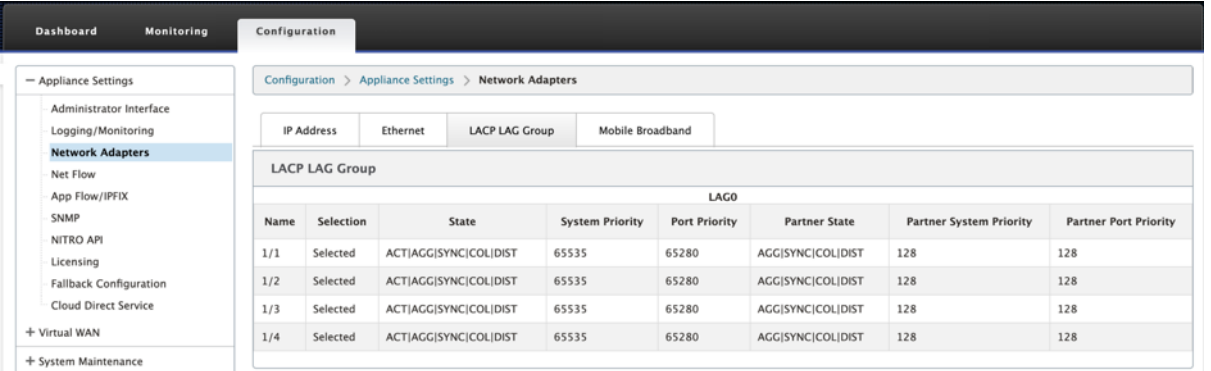
The screenshot shows the 'Monitoring > Statistics' page in the Citrix SD-WAN interface. The 'Statistics' section is active, and 'Ethernet' is selected in the 'Show' dropdown. The 'Ethernet Statistics' table displays the following data:

Port	Link State	Frames Sent	Bytes Sent	Frames Received	Bytes Received	Errors
LAG0	UP	228799	20119310	210823	16480420	0
1/4	UP	976632	86479280	951719	79790814	0
1/1	UP	0	0	10134	718152	0

アクティブおよびスタンバイの LAG ポートを表示するには、[構成] > [アプライアンスの設定] > [** ネットワーク アダプタ] ** > [イーサネット] の順に移動します。



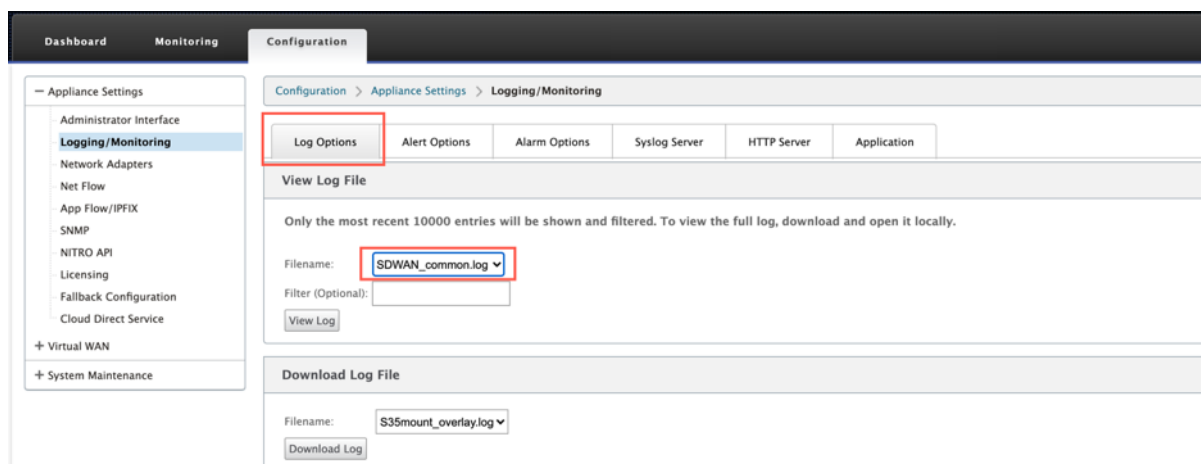
[**LACP LAG** グループ] タブを選択して、LACP LAG グループに関連するさまざまな詳細を表示します。



注

個々のメンバポートの設定は変更できません。LAG に対する構成の変更は、メンバポートに自動的にプッシュされます。

詳細なトラブルシューティングのために、ログファイルをダウンロードできます。[構成] > [ログ/監視] に移動し、[ログオプション] タブで [SDWAN_common.log] を選択します。



リンク状態の伝播

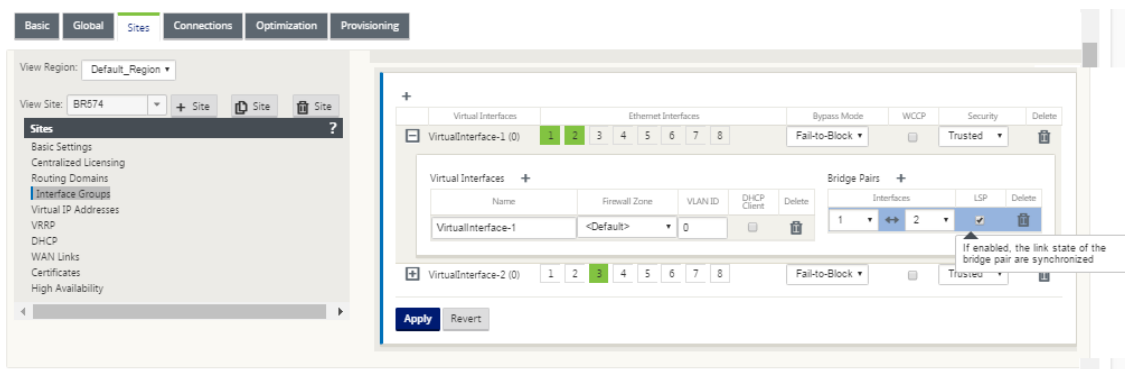
May 10, 2021

Link State Propagation (LSP; Link State Propagation) 機能を使用すると、ネットワーク管理者はバイパスペアのリンクステートを同期化しておき、リンクの反対側の接続デバイスが、リンクが非アクティブであるときに表示できるようになります。バイパスペアの1つのポートが非アクティブになると、結合されたリンクは管理上非アクティブになります。ネットワークアーキテクチャにパラレルフェールオーバーネットワークが含まれている場合、トラフィックは強制的にそのネットワークに移行します。中断されたリンクが復元されると、対応するリンクが自動的にアクティブになります。

リンク状態の伝播を構成する方法

リンク状態の伝播を構成するには、次の手順を実行します。

1. [構成エディタ] > [サイト] > [サイト [名]] > [インターフェイスグループ] に移動します。
2. [仮想インターフェイス] を展開し、[ブリッジペア] で [LSP] チェックボックスをクリックして、ブリッジペアのリンクステート伝播を有効にします。[適用] をクリックして設定を保存します。



リンク統計情報のモニタリング

リンク統計情報を監視するには、次の手順を実行します。

1. [**Monitor**] > [**Statistics**] ページで、[**Show**] ドロップダウンメニューから [**Ethernet**] を選択して、リンク状態伝播を有効にしたバイパスポートペアのステータスを表示します。LAN 側リンクがダウンし、後でバイパスペアの WAN 側リンクが管理上 Disabled になっていることに注意します。

Statistics

Show: **Ethernet** ☐ Enable Auto Refresh 5 seconds Refresh

Ethernet Statistics

Filter: in Any column Apply

Show 100 entries Showing 1 to 2 of 2 entries

Port	Link State	Frames Sent	Bytes Sent	Frames Received	Bytes Received	Errors
1	DOWN	132885	8755483	212584	15332801	0
2	DISABLED	17984552	1531084459	18189043	1584612144	3258

Showing 1 to 2 of 2 entries

2. 構成 > アプライアンスの設定 > ネットワークアダプタ > イーサネットタブに移動します。管理上ダウンしているポートは、[**Ethernet Interface Settings**] リストに赤色のアスタリスク (*) で示されます。

Ethernet Interface Settings

1:	MAC Address: 0c:c4:7a:12:bc:8d	Autonegotiate: <input checked="" type="checkbox"/>	Speed: Unknown	Duplex: Unknown
2:	* MAC Address: 0c:c4:7a:12:bc:8c	Autonegotiate: <input checked="" type="checkbox"/>	Speed: Unknown	Duplex: Unknown
3:	MAC Address: 0c:c4:7a:12:bc:8f	Autonegotiate: <input checked="" type="checkbox"/>	Speed: Unknown	Duplex: Unknown
4:	MAC Address: 0c:c4:7a:12:bc:8e	Autonegotiate: <input checked="" type="checkbox"/>	Speed: Unknown	Duplex: Unknown
5:	MAC Address: 0c:c4:7a:12:bc:91	Autonegotiate: <input checked="" type="checkbox"/>	Speed: Unknown	Duplex: Unknown
MGT:	MAC Address: 0c:c4:7a:12:bc:90	Autonegotiate: <input checked="" type="checkbox"/>	Speed: 100Mb/s	Duplex: Full
X1:	MAC Address: 00:25:90:ed:22:9f	Autonegotiate: <input checked="" type="checkbox"/>	Speed: Unknown	Duplex: Unknown
X2:	MAC Address: 00:25:90:ed:22:9e	Autonegotiate: <input checked="" type="checkbox"/>	Speed: Unknown	Duplex: Unknown
X3:	MAC Address: 00:25:90:ed:22:9d	Autonegotiate: <input checked="" type="checkbox"/>	Speed: Unknown	Duplex: Unknown
X4:	MAC Address: 00:25:90:ed:22:9c	Autonegotiate: <input checked="" type="checkbox"/>	Speed: Unknown	Duplex: Unknown

* interface disabled by Port State Reflection

Change Settings

メータリングおよびスタンバイ WAN リンク

May 10, 2021

Citrix SD-WAN では、従量制課金リンクの有効化がサポートされています。これは、使用可能な他のすべての WAN リンクが無効になっているときに、ユーザーのトラフィックが特定のインターネット WAN リンクでのみ転送されるように構成できます。

従量制課金リンクは、使用量に基づいて請求されるリンクの帯域幅を節約します。従量制課金リンクを使用すると、リンクを [Last Resort] リンクとして設定できます。これにより、他のすべての従量制課金リンクが停止または低下するまで、リンクの使用が許可されません。[最後のリゾート設定] は、通常、サイトへの WAN リンク (MPLS、ブロードバンドインターネット、4G/LTE) が 3 つあり、WAN リンクの 1 つが 4G/LTE であり、必要でない限り使用を許可するにはコストがかかりすぎる可能性があります。メータリングはデフォルトでは有効になっていないため、任意のアクセスタイプ (パブリックインターネット、プライベート MPLS、プライベートイントラネット) の WAN リンクで有効にできます。メータリングが有効な場合は、必要に応じて次の項目を設定できます。

- データキャップ
- 請求サイクル (週次/月次)
- 開始日
- スタンバイモード
- 優先度
- Active heartbeat interval: 少なくともハートビート間隔の間パス上にトラフィック (ユーザー/コントローラ) がない場合に、アプライアンスから仮想パスの反対側のピアにハートビートメッセージが送信される間隔

ローカルの従量制課金リンクでは、アプライアンスのダッシュボードの下部に **WAN** リンクメータリング テーブルが表示され、メータリング情報が示されます。

ローカルの従量制課金リンクでの帯域幅使用率は、設定されたデータキャップに対して追跡されます。使用量が構成済みデータ上限の 50%、75%、または 90% を超えると、アプライアンスはユーザーに警告するイベントを生成し、アプライアンスのダッシュボードの上部に警告バナーが表示されます。この使用状況アラートイベントは SD-WAN センターでも表示できます。従量制課金パスは、1 つまたは 2 つの従量制課金リンクで形成できます。2 つの従量制課金リンク間にパスが形成されている場合、従量制課金パスで使用されるアクティブハートビートインターバルは、リンクで設定された 2 つのアクティブハートビートインターバルのうち大きい方になります。

従量制課金パスは非スタンバイパスであり、常にユーザトラフィックに適格です。GOOD 状態にある非従量制課金パスが少なくとも 1 つある場合、従量制課金パスは制御トラフィックの削減量を伝送し、フォワーディングプレーンが重複パケットのパスを検索するときに回避されます。

スタンバイモード

WAN リンクのスタンバイモードは、デフォルトで無効になっています。スタンバイモードを有効にするには、次の 2 つのモードのどちらでスタンバイリンクが動作するかを指定する必要があります。

- オンデマンド: いずれかの条件が満たされたときにアクティブになるスタンバイリンク。

仮想パスで使用可能な帯域幅が、設定されたオンデマンド帯域幅制限よりも小さく、十分な使用量がある場合。十分な使用量は、現在の使用可能な帯域幅の 95% 以上 (ON_DEMAND_USAGE_THRESHOLD_PCT) として定義されるか、現在の使用可能な帯域幅と現在の使用量の差が 250 kbps 未満 (ON_DEMAND_THRESHOLD_GAP_KBPS) の場合、両方のパラメータは t2_variables を使用して変更できます。パスが無効になっているか、無効になっています。

- **Last-resort** : すべての非スタンバイリンクおよびオンデマンドスタンバイリンクがデッドまたは無効になったときにだけアクティブになるスタンバイリンク。
- スタンバイプライオリティは、スタンバイリンクが複数ある場合に、スタンバイリンクがアクティブになる順序を示します。
 - プライオリティ 1 のスタンバイリンクが先にアクティブになり、プライオリティ 3 のスタンバイリンクが最後にアクティブになります
 - 複数のスタンバイリンクに同じプライオリティを割り当てることができます

スタンバイリンクを設定する場合、スタンバイプライオリティと 2 つのハートビートインターバルを指定できます。

- アクティブハートビート間隔: スタンバイパスがアクティブなときに使用されるハートビート間隔 (デフォルト 50ms/1s/2s/3s/4s/5s/6s/7s/8s/9s/10s)
- スタンバイハートビート間隔: スタンバイパスが非アクティブのときに使用されるハートビート間隔 (デフォルトは 1s/2s/3s/4s/5s/6s/7s/8s/9s/10s/無効)

スタンバイパスは、1 つまたは 2 つのスタンバイリンクで形成されます。

- **On -Demand**: オンデマンドスタンバイパスは次の間で形成されます。
 - 非スタンバイリンクとオンデマンドスタンバイリンク
 - 2 つのオンデマンドスタンバイリンク
- **Last-Resort** : 最終リゾートスタンバイパスは次の間に形成されます。
 - 非スタンバイリンクおよび最終リゾートスタンバイリンク
 - オンデマンドスタンバイリンクおよびラストリゾートスタンバイリンク
 - 2 つの最終リゾートスタンバイリンク

スタンバイパスで使用されるハートビートインターバルは、次のように決定されます。

- 2 つのリンクのうち少なくとも 1 つでスタンバイハートビートが無効になっている場合、非アクティブな間はスタンバイパスでハートビートが無効になります。
- いずれかのリンクでスタンバイハートビートが無効になっていない場合、スタンバイパスがスタンバイのときに 2 つの値のうち大きい方が使用されます。
- 両方のリンクでアクティブハートビートインターバルが設定されている場合、スタンバイパスがアクティブなときに 2 つの値のうち大きい方が使用されます。

ハートビート (キープアライブ) メッセージ:

- 非スタンバイパスでは、ハートビートメッセージが送信されるのは、少なくともハートビートインターバルの間にトラフィック (制御またはユーザ) がいない場合だけです。ハートビート間隔は、パスの状態によって異なります。非スタンバイ、非従量制課金 パスの場合:

- パス状態が GOOD の場合、50 ミリ秒
- パス状態が BAD の場合、25 ミリ秒

スタンバイパスでは、使用されるハートビート間隔は、アクティビティ状態とパスの状態によって異なります。

- 非アクティブな間、ハートビートが無効になっていない場合、ハートビートメッセージは設定されたスタンバイハートビートインターバルで定期的送信されます。これは、他のトラフィックは許可されないためです。
- パス状態が GOOD の場合に、設定されたアクティブハートビートインターバルが使用されます。
- パスの状態が BAD の場合、設定されたアクティブハートビートインターバル 1/2 が使用されます。
- 非スタンバイパスと同様に、アクティブ中は、少なくとも設定されたアクティブハートビートインターバルの間にトラフィック（制御またはユーザ）がない場合に限り、ハートビートメッセージが送信されます。
- パス状態が GOOD の場合に、設定されたスタンバイハートビートインターバルが使用されます。
- パスの状態が BAD の場合、設定されたスタンバイハートビートインターバルの 1/2 が使用されます。

非アクティブの場合、スタンバイパスはユーザトラフィックに対して適格ではありません。非アクティブなスタンバイパスで送信される制御プロトコルメッセージは、ハートビートメッセージだけです。ハートビートメッセージは、接続障害検出および品質メトリックの収集用です。スタンバイパスがアクティブの場合、時間コストを追加したユーザトラフィックに適格です。これは、フォワーディングパスの選択中に非スタンバイパスが使用可能な場合、そのパスが優先されるようにするために行われます。

非アクティブのハートビートが無効になっているスタンバイパスのパス状態は、GOOD であると見なされ、[**Monitoring**] の [Path Statistics] テーブルに GOOD と表示されます。アクティブになると、仮想パスピアから聞くまで DEAD 状態で開始される非スタンバイパスとは異なり、GOOD 状態で開始されます。仮想パスピアとの接続が検出されない場合、パスは BAD になり、次に DEAD になります。仮想パスピアとの接続が再確立されると、パスが BAD になり、その後再び GOOD になります。

このようなスタンバイパスが DEAD になってから非アクティブになった場合、パスの状態は（仮定）GOOD に変更されません。その代わり、すぐに使用できないように、時間の間 DEAD 状態に保たれます。これは、正常な DEAD パスを想定した低いプライオリティのパスグループと、実際に GOOD パスを持つ高いプライオリティのパスグループの間でアクティビティが振動するのを防ぐためです。この保留期間 (NO_HB_PATH_ON_HOLD_PERIOD_MS) は 5 分に設定され、t2_ 変数を使用して変更できます。

仮想パスでパス MTU 検出が有効になっている場合、パスがスタンバイ状態の間、スタンバイパスの MTU は仮想パスの MTU の計算に使用されません。スタンバイパスがアクティブになると、仮想パスの MTU は、スタンバイパスの MTU を考慮して再計算されます。（仮想パスの MTU は、仮想パス内のすべてのアクティブパスの中で最小のパス MTU です）。

スタンバイパスがスタンバイとアクティブの間で移行すると、イベントとログメッセージが生成されます。

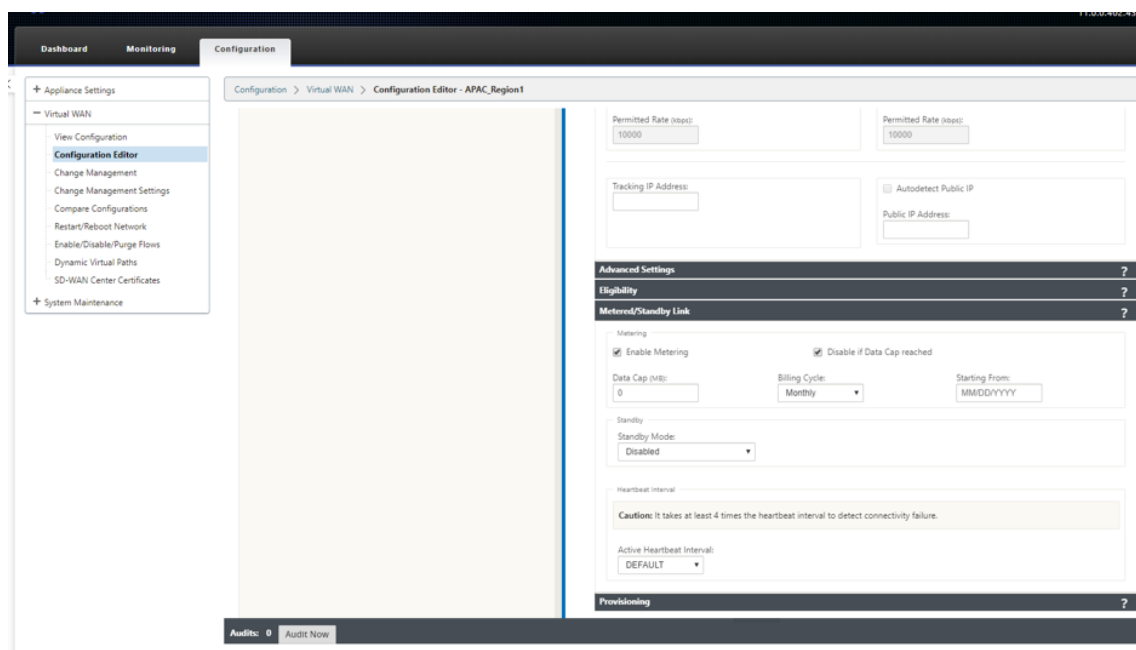
構成の前提条件：

- メーターリンクは、任意のアクセスタイプである場合があります。
- サイトのすべてのリンクは、メータリングを有効にして構成できます。

- スタンバイリンクは、[パブリックインターネット] または [プライベートイントラネット] のアクセスタイプです。プライベート MPLS アクセスタイプの WAN リンクは、スタンバイリンクとして設定できません。
- サイトごとに少なくとも 1 つの非スタンバイリンクを設定する必要があります。サイトごとに最大 3 つのスタンバイリンクがサポートされます。
- インターネット/イントラネットサービスは、オンデマンドスタンバイリンクで構成されていない可能性があります。オンデマンドスタンバイリンクは、仮想パスサービスのみをサポートします。
- インターネットサービスは、last-resort スタンバイリンクで設定されている場合がありますが、サポートされているのは負荷分散モードだけです。
- イントラネットサービスは、ラストリゾートスタンバイリンクで構成されている可能性があります。サポートされているのはセカンダリモードのみで、プライマリ再要求を有効にする必要があります。

従量制課金リンクを設定するには:

1. SD-WAN Web 管理インターフェイスで、[構成] > [仮想 WAN] > [構成エディタ] > [追加] を選択するか、ドロップダウンリストから [サイト] を選択し、[WAN リンク] を選択し、[**Meteed/Standby Link**] タブをクリックして展開します。



2. [メータリングを有効にする] チェックボックスをオンにします。[データ上限]、[請求サイクルの開始日]、[使用済み概算]、および [アクティブハートビート間隔] の値を指定できます。

Metering

☒ Enable Metering ☒ Disable if Data Cap reached

Data Cap (MB): Billing Cycle: Starting From:

Standby

Standby Mode:

Heartbeat Interval

Caution: It takes at least 4 times the heartbeat interval to detect connectivity failure.

Active Heartbeat Interval:

3. データ上限に達した場合のリンクを無効にする:

- [データ上限に達したらリンクを無効にする] チェックボックスがオンの場合、データ使用量がデータ上限に達すると、次の請求サイクルまで、従量制課金リンクとその関連パスがすべて無効になります。
- 既定では、[データ上限に達したらリンクを無効にする] チェックボックスはオフの状態になります。このチェックボックスは、データ上限に達した後、次の請求サイクルまで継続される従量制課金リンクの現在のモードまたは状態セットを保持します。

4. 従量制課金リンクが設定されている場合は、従量制課金リンクに既に使用されている概算データを MB 単位で入力できます。

従量制課金リンクの使用状況を追跡するには、現在の請求サイクルでリンクがすでに数日間使用されている場合は、従量制課金リンクにおおよその使用量を入力する必要があります。このおおよその使用量は、最初のサイクルのみを対象としています。開始日から現在の日付までの合計使用量が計算され、ダッシュボードに表示されます。

Metered/Standby Link

Metering

☒ Enable Metering ☒ Disable Link if Data Cap reached

Data Cap (MB): **Approximate Data Already Used (MB):** Billing Cycle: Starting From:

Standby

Standby Mode:

構成の更新を実行した後、ダッシュボードで使用状況の詳細を表示できます。

WAN Link Name: DC-WL-1
Total Usage: **999.35 MBs of 500 MBs**
Data Usage: 0.00 MBs
Control Usage: 999.35 MBs
Usage(in %): 199
Billing Cycle: MONTHLY
Starting From: 05/06/2020
Days Elapsed: 8 days of 31 days

スタンバイリンクを設定するには、次の手順を実行します。

1. デフォルトでは、WAN リンクのスタンバイモードは無効です。WAN リンクをスタンバイとして設定するには、ドロップダウンリストからいずれかのスタンバイモード（Last-Resort/On-Demand）を選択します。

Standby

Standby Mode: Last-Resort Priority: 1

Heartbeat Interval

Caution: It takes at least 4 times the heartbeat interval to detect connectivity failure.

Active Heartbeat Interval: 1 second Standby Heartbeat Interval: 1 second

Provisioning ?

Apply Revert

2. スタンバイモードを選択したら、スタンバイプライオリティ、アクティブハートビートインターバル、およびスタンバイハートビートインターバルを適宜選択します。[適用] をクリックして、設定を検証します。
3. オンデマンドスタンバイリンクが設定されている場合、グローバルなデフォルトのオンデマンド帯域幅制限（120%）が仮想パスに適用されます。これは、仮想パスで許可される WAN-to-LAN 帯域幅の最大値を指定します。これは、仮想パス内のすべての非スタンバイリンクによって提供される総帯域幅に対するパーセンテージで表されます。仮想パスで使用可能な帯域幅が制限を下回っている限り、十分な使用量があれば、アプライアンスは帯域幅を補完するためにオンデマンドパスをアクティブ化しようとします。
4. グローバルなデフォルトのオンデマンド帯域幅制限を表示または変更するには、[グローバル] > [仮想 WAN ネットワーク 設定] セクションを開きます。

Global Security Settings

Note: Changing the **Network Encryption Mode** may cause **Site Secure Keys** to be truncated or regenerated if they do not meet the requirements of the new mode.

Network Encryption Mode:
AES 128-Bit

☒ Enable Encryption Key Rotation

☐ Enable Extended Packet Encryption Header

☐ Enable Extended Packet Authentication Trailer

Extended Packet Authentication Trailer Type:
32-Bit Checksum

☐ Enable FIPS Mode

Network Secure Key:

*

Regenerate

Global Firewall Settings

Global Policy Template:
<None>

Default Firewall Action:
Allow

☐ Default Connection State Tracking

Denied Timeout (s):
30

TCP Initial Timeout (s):
120

TCP Idle Timeout (s):
7440

TCP Closing Timeout (s):
60

TCP Time Wait Timeout (s):
120

TCP Closed Timeout (s):
10

UDP Initial Timeout (s):
30

UDP Idle Timeout (s):
300

ICMP Initial Timeout (s):
30

ICMP Idle Timeout (s):
60

Generic Initial Timeout (s):
30

Generic Idle Timeout (s):
300

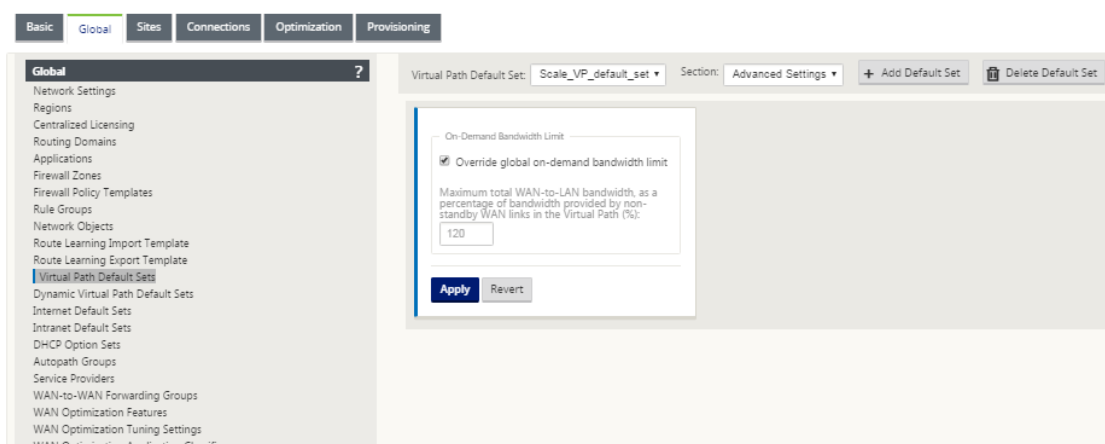
Global On-Demand Bandwidth Limit Setting

Default maximum total WAN-to-LAN bandwidth, as a percentage of bandwidth provided by non-standby WAN links in the Virtual Path (%):
120

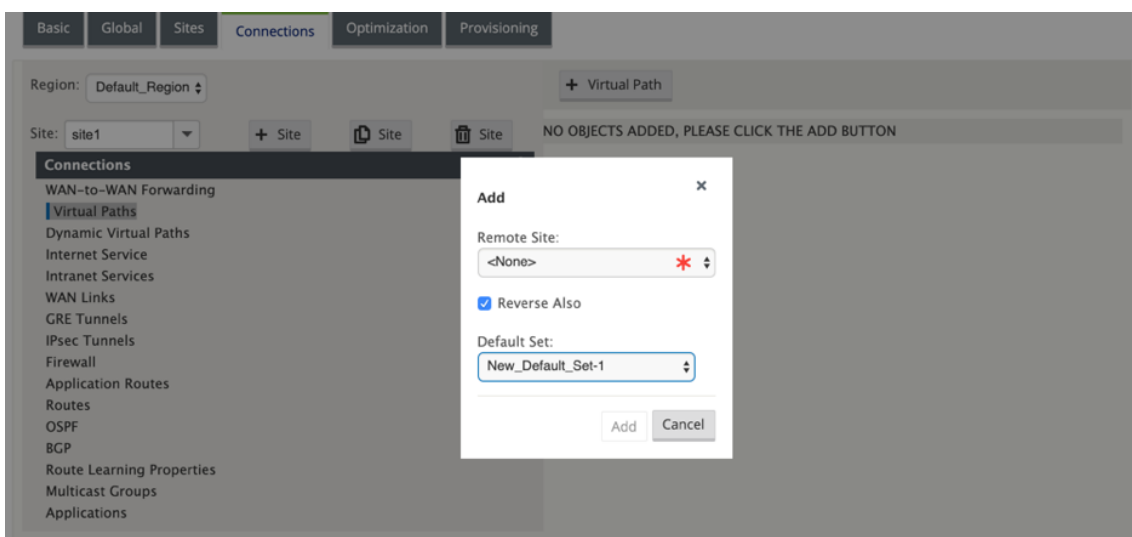
Apply

Refresh

5. 仮想パスに固有のオンデマンド帯域幅制限を適用し、グローバルなデフォルト設定を変更しない場合は、仮想パスのデフォルトセットを作成し、[詳細設定] でオンデマンド帯域幅制限を変更できます。

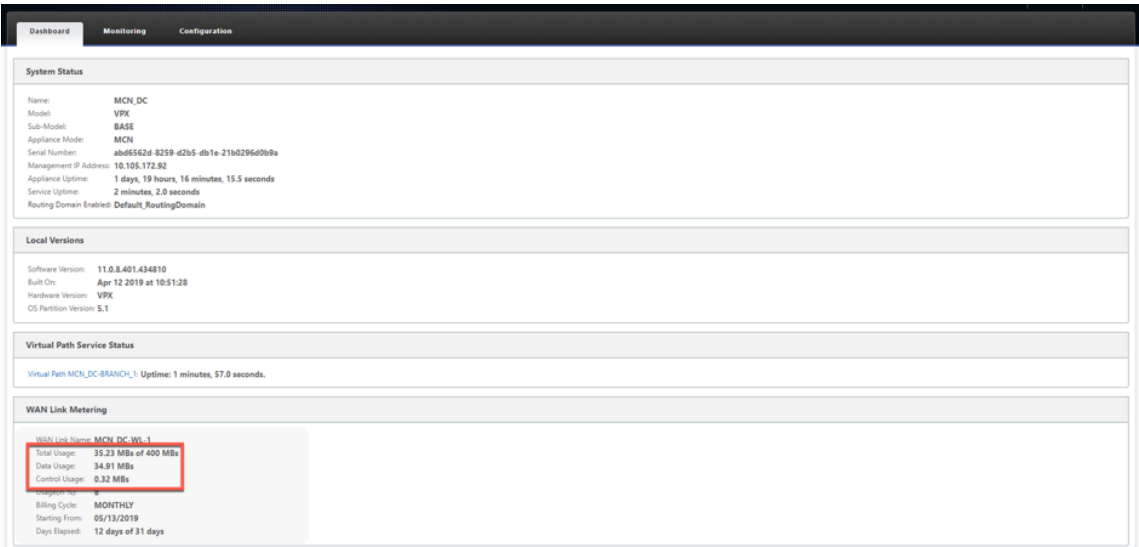


6. 特定の仮想パスに設定を適用するには、[接続] > [仮想パス] セクションに移動し、[+ 仮想パス] をクリックします。

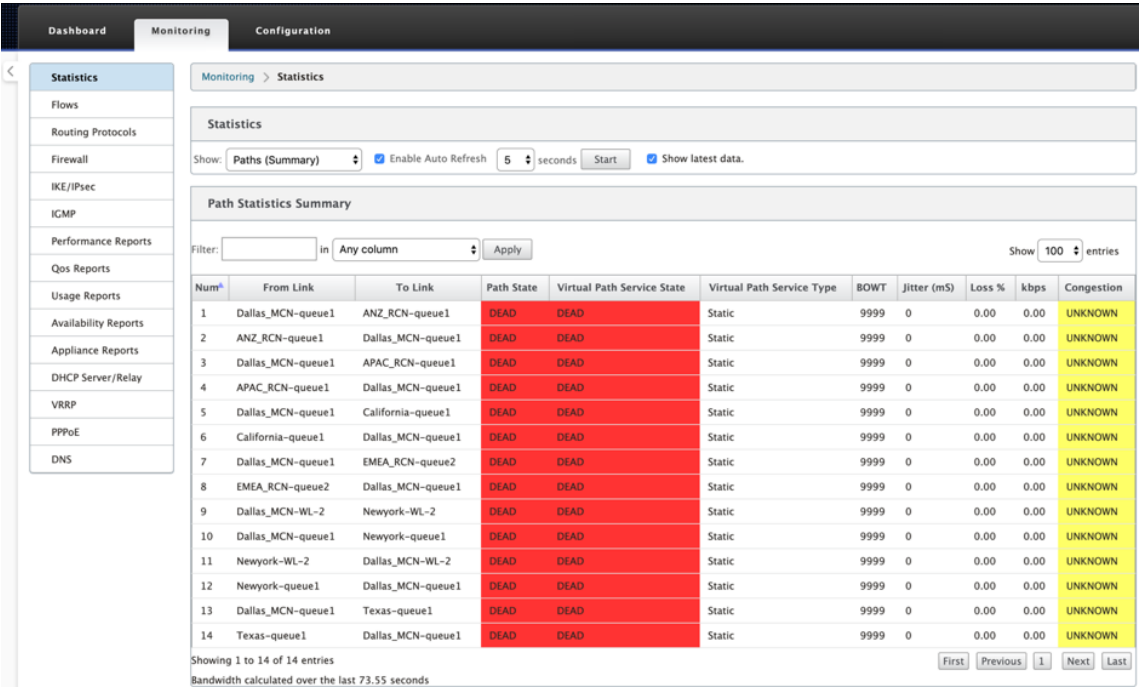


従量制課金およびスタンバイ WAN リンクの監視

- [ダッシュボード] ページには、次の **WAN** リンクメータリング 情報と使用値が表示されます。
 - **WAN** リンク名: WAN リンク名を表示します。
 - 合計使用量: 合計トラフィック使用量（データ使用量 + 制御使用量）が表示されます。
 - [データ使用状況]: ユーザートラフィック別の使用状況を表示します。
 - 制御の使用状況: 制御トラフィックごとの使用状況を表示します。
 - 使用量 (%): 使用済みデータ上限値をパーセンテージ（合計使用量/データ上限値）x 100 で表示します。
 - 請求サイクル: 請求頻度（週単位/月単位）
 - 開始日: 請求サイクルの開始日
 - 経過日数: 経過時間（日、時、分、秒単位）



- パス統計（[モニタリング] > [統計] > [パス]）が表示されると、スクリーンショットのように従量制課金リンクとスタンバイリンクがマークされます。



- ローカルまたはリモートのオンデマンドスタンバイリンクを持つ仮想パスがアプライアンスに存在する場合、WAN リンクの使用状況の統計情報を表示すると、ページの下部にオンデマンド帯域幅を示す追加のテーブルが表示されます（[モニタリング] > [統計] > [WAN リンクの使用状況]）。

Local WAN-to-LAN On Demand WAN Link Usages

Filter: in Any column

Show 100 entries Showing 0 to 0 of 0 entries

First Previous Next Last

WAN Link	WAN Link Mode	Standby Priority	Configured	Adaptive Bandwidth Detection	Virtual Path Name	Virtual Path On Demand Bandwidth Limit Kbps	Virtual Path Available Bandwidth Kbps	In Use
No data available in table								

Showing 0 to 0 of 0 entries

First Previous Next Last

Bandwidth calculated over the last 5.078 seconds

- 従量制課金リンクの使用量が、設定されたデータ上限の 50% を超えると、ダッシュボードの上部に警告バナーが表示されます。さらに、使用量が構成済みのデータ上限の 75% を超えると、ダッシュボードの下部に向けた数値計測情報が強調表示されます。

The data usage on the following Metered Wanlinks have reached the threshold:
• BR1-WL-1-New : 75%.

System Status

Name

BR1

Model

VPX

Sub-Model

BASE

Appliance Mode

Client

Serial Number

aa4580cb-7527-8dee-fbea-9824a89142e6

Management IP Address

10.105.184.72

Appliance Uptime

10 hours, 7 minutes, 34.6 seconds

Service Uptime

9 hours, 17 minutes, 53.0 seconds

Routing Domain Enabled

Default, RoutingDomain

Local Versions

Configuration Created On

Thu Apr 18 20:08:57 2019

Software Version

11.0.13.401.434810

Built On

Apr 18 2019 at 19:35:14

Hardware Version

VPX

OS Partition Version

5.1

Virtual Path Service Status

Virtual Path DC-BR1 Uptime

9 hours, 17 minutes, 43.0 seconds.

WAN Link Metering

WAN Link Name

BR1-WL-1-New

Total Usage

329.58 MBs of 400 MBs

Data Usage

258.09 MBs

Control Usage

71.48 MBs

Usage (%)

82

Billing Cycle

MONTHLY

Starting From

07/17/2019

Days Elapsed

3 days of 31 days

WAN リンク使用イベントは、設定済みデータ上限の 50%、75%、および 90% を超えると、アプライアンスでも生成されます。

17654	1	RL-TB-CL1-WL-2	WAN LINK	2017-05-24 10:22:58	USAGE_3	WARNING	Total usage 1.84 Gbytes used (91% of limit 2.00 Gbytes) in 1 of 31 days in this billing cycle since 00:00:00 05/24/2017
17653	1	RL-TB-CL1-WL-2	WAN LINK	2017-05-24 10:17:58	USAGE_2	WARNING	Total usage 1.52 Gbytes used (75% of limit 2.00 Gbytes) in 1 of 31 days in this billing cycle since 00:00:00 05/24/2017
17652	1	RL-TB-CL1-WL-2	WAN LINK	2017-05-24 10:09:58	USAGE_1	WARNING	Total usage 1.00 Gbytes used (50% of limit 2.00 Gbytes) in 1 of 31 days in this billing cycle since 00:00:00 05/24/2017

- スタンバイパスがスタンバイ状態とアクティブ状態の間で移行すると、アプライアンスによってイベントが生成されます。

24640	3	RL-TB-MCN-WL-2->RL-TB-CL2-WL-2	PATH	2017-05-26 10:18:32	STANDBY	NOTICE	Virtual Path RL-TB-MCN-RL-TB-CL2 Backup Path RL-TB-MCN-WL-2->RL-TB-CL2-WL-2 has become standby
24639	1	RL-TB-MCN-WL-1->RL-TB-CL2-WL-2	PATH	2017-05-26 10:18:32	STANDBY	NOTICE	Virtual Path RL-TB-MCN-RL-TB-CL2 Backup Path RL-TB-MCN-WL-1->RL-TB-CL2-WL-2 has become standby
24638	1	RL-TB-CL2-WL-1->RL-TB-MCN-WL-2	PATH	2017-05-26 10:18:27	GOOD	NOTICE	Virtual Path RL-TB-MCN-RL-TB-CL2 Path RL-TB-CL2-WL-1->RL-TB-MCN-WL-2 state has changed from BAD to GOOD because notified by peer.
24637	2	RL-TB-MCN-WL-2->RL-TB-CL2-WL-1	PATH	2017-05-26 10:18:27	GOOD	NOTICE	Virtual Path RL-TB-MCN-RL-TB-CL2 Path RL-TB-MCN-WL-2->RL-TB-CL2-WL-1 state has changed from BAD to GOOD .
24636	2	RL-TB-MCN-RL-TB-CL2	VIRTUAL PATH	2017-05-26 10:18:27	GOOD	NOTICE	The state of Virtual Path RL-TB-MCN-RL-TB-CL2 has changed from BAD to GOOD
24635	0	RL-TB-CL2-WL-1->RL-TB-MCN-WL-1	PATH	2017-05-26 10:18:27	GOOD	NOTICE	Virtual Path RL-TB-MCN-RL-TB-CL2 Path RL-TB-CL2-WL-1->RL-TB-MCN-WL-1 state has changed from BAD to GOOD because notified by peer.
24634	0	RL-TB-MCN-WL-1->RL-TB-CL2-WL-1	PATH	2017-05-26 10:18:27	GOOD	NOTICE	Virtual Path RL-TB-MCN-RL-TB-CL2 Path RL-TB-MCN-WL-1->RL-TB-CL2-WL-1 state has changed from BAD to GOOD .
24633	3	RL-TB-MCN-WL-2->RL-TB-CL2-WL-2	PATH	2017-05-26 10:18:27	ACTIVE	ERROR	Virtual Path RL-TB-MCN-RL-TB-CL2 Backup Path RL-TB-MCN-WL-2->RL-TB-CL2-WL-2 has become active
24632	1	RL-TB-MCN-WL-1->RL-TB-CL2-WL-2	PATH	2017-05-26 10:18:27	ACTIVE	ERROR	Virtual Path RL-TB-MCN-RL-TB-CL2 Backup Path RL-TB-MCN-WL-1->RL-TB-CL2-WL-2 has become active

2. 各パスに設定されたアクティブハートビート間隔とスタンバイハートビート間隔は、[構成] > [** 仮想 WAN] > [構成の ** 表示] > [パス] で確認できます。

DashboardMonitoringConfiguration

+ Appliance Settings

- Virtual WAN

View Configuration

Configuration Editor

Change Management

Change Management Settings

Compare Configurations

Restart/Reboot Network

Enable/Disable/Purge Flows

Dynamic Virtual Paths

SD-WAN Center Certificates

+ System Maintenance

Configuration > Virtual WAN > View Configuration

Configuration

View: Paths

Path Configuration

Paths on virtual path 3 'Dallas_MCN-ANZ_RCN':

Path ID	From Link	To Link	Primary Src IP Address	Primary Dst IP Address	Secondary Src IP Address	Secondary Dst IP Address	Src Port	Dst Port	Alt Src
0	Dallas_MCN-queue1	ANZ_RCN-queue1	192.168.1.10	192.168.90.10	-	-	4980	4980	
0	ANZ_RCN-queue1	Dallas_MCN-queue1	192.168.90.10	192.168.1.10	-	-	4980	4980	

From Link

To Link

Realtime Eligible

Interactive Eligible

Bulk Eligible

Path Group

Standby Heartbeat Interval(ms)

Active Heartbeat Interval(ms)

Dallas_MCN-queue1

ANZ_RCN-queue1

YES

YES

YES

0

n/a

n/a

ANZ_RCN-queue1

Dallas_MCN-queue1

YES

YES

YES

0

n/a

n/a

Paths on virtual path 8 'Dallas_MCN-APAC_RCN':

Path ID	From Link	To Link	Primary Src IP Address	Primary Dst IP Address	Secondary Src IP Address	Secondary Dst IP Address	Src Port	Dst Port	Alt Src
0	Dallas_MCN-queue1	APAC_RCN-queue1	192.168.1.10	192.168.80.10	-	-	4980	4980	
0	APAC_RCN-queue1	Dallas_MCN-queue1	192.168.80.10	192.168.1.10	-	-	4980	4980	

From Link

To Link

Realtime Eligible

Interactive Eligible

Bulk Eligible

Path Group

Standby Heartbeat Interval(ms)

Active Heartbeat Interval(ms)

Dallas_MCN-queue1

APAC_RCN-queue1

YES

YES

YES

0

n/a

n/a

APAC_RCN-queue1

Dallas_MCN-queue1

YES

YES

YES

0

n/a

n/a

Paths on virtual path 9 'Dallas_MCN-California':

Path ID	From Link	To Link	Primary Src IP Address	Primary Dst IP Address	Secondary Src IP Address	Secondary Dst IP Address	Src Port	Dst Port	Alt Src
0	Dallas_MCN-queue1	California-queue1	192.168.1.10	192.168.50.10	-	-	4980	4980	
0	California-queue1	Dallas_MCN-queue1	192.168.50.10	192.168.1.10	-	-	4980	4980	

From Link

To Link

Realtime Eligible

Interactive Eligible

Bulk Eligible

Path Group

Standby Heartbeat Interval(ms)

Active Heartbeat Interval(ms)

Dallas_MCN-queue1

California-queue1

YES

YES

YES

0

n/a

n/a

California-queue1

Dallas_MCN-queue1

YES

YES

YES

0

n/a

n/a

Paths on virtual path 12 'Dallas_MCN-EMEA_RCN':

Path ID	From Link	To Link	Primary Src IP Address	Primary Dst IP Address	Secondary Src IP Address	Secondary Dst IP Address	Src Port	Dst Port	Alt Src
0	Dallas_MCN-queue1	EMEA_RCN-queue2	192.168.1.10	17.1.1.10	-	-	4980	4980	
0	EMEA_RCN-queue2	Dallas_MCN-queue1	17.1.1.10	192.168.1.10	-	-	4980	4980	

From Link

To Link

Realtime Eligible

Interactive Eligible

Bulk Eligible

Path Group

Standby Heartbeat Interval(ms)

Active Heartbeat Interval(ms)

Dallas_MCN-queue1

EMEA_RCN-queue2

YES

YES

YES

0

n/a

n/a

EMEA_RCN-queue2

Dallas_MCN-queue1

YES

YES

YES

0

n/a

n/a

Paths on virtual path 13 'Dallas_MCN-Newyork':

Path ID	From Link	To Link	Primary Src IP Address	Primary Dst IP Address	Secondary Src IP Address	Secondary Dst IP Address	Src Port	Dst Port	Alt Src
1	Dallas_MCN-queue1	Newyork-queue1	192.168.1.10	192.168.70.10	-	-	4980	4980	
0	Dallas_MCN-WL-2	Newyork-WL-2	192.168.10.10	192.168.60.10	-	-	4980	4980	
0	Newyork-WL-2	Dallas_MCN-WL-2	192.168.60.10	192.168.10.10	-	-	4980	4980	
1	Newyork-queue1	Dallas_MCN-queue1	192.168.70.10	192.168.1.10	-	-	4980	4980	

From Link

To Link

Realtime Eligible

Interactive Eligible

Bulk Eligible

Path Group

Standby Heartbeat Interval(ms)

Active Heartbeat Interval(ms)

Dallas_MCN-queue1

Newyork-queue1

YES

YES

YES

0

n/a

n/a

Dallas_MCN-WL-2

Newyork-WL-2

YES

YES

YES

0

n/a

n/a

Newyork-WL-2

Dallas_MCN-WL-2

YES

YES

YES

0

n/a

n/a

Newyork-queue1

Dallas_MCN-queue1

YES

YES

YES

0

n/a

n/a

Paths on virtual path 14 'Dallas_MCN-Texas':

Path ID	From Link	To Link	Primary Src IP Address	Primary Dst IP Address	Secondary Src IP Address	Secondary Dst IP Address	Src Port	Dst Port	Alt Src
0	Dallas_MCN-queue1	Texas-queue1	192.168.1.10	192.168.40.10	-	-	4980	4980	
0	Texas-queue1	Dallas_MCN-queue1	192.168.40.10	192.168.1.10	-	-	4980	4980	

From Link

To Link

Realtime Eligible

Interactive Eligible

Bulk Eligible

Path Group

Standby Heartbeat Interval(ms)

Active Heartbeat Interval(ms)

Dallas_MCN-queue1

Texas-queue1

YES

YES

YES

0

n/a

n/a

Texas-queue1

Dallas_MCN-queue1

YES

YES

YES

0

n/a

n/a

Office 365 の最適化

November 8, 2021

Office 365 の最適化機能は、Office 365 を最適化するために、[Microsoft Office 365 のネットワーク接続原則に準拠しています](#)。Office 365 は、グローバルに配置された複数のサービスエンドポイント (フロントドア) を通じてサービスとして提供されます。Office 365 トラフィックに最適なユーザーエクスペリエンスを実現するには、Office 365 トラフィックをブランチ環境からインターネットに直接リダイレクトすることをお勧めします。中央プロキシへのバックホールなどのプラクティスは避けてください。Outlook、Word などの Office 365 トラフィックはレイテンシーの影響を受けやすく、バックホールトラフィックによってレイテンシーが増加し、ユーザーエクスペリエンスが低下します。Citrix SD-WAN を使用すると、インターネットへの Office 365 トラフィックを突破するポリシーを構成できます。

Office 365 トラフィックは、世界中の Microsoft Office 365 インフラストラクチャのエッジに存在する最も近い Office 365 サービスエンドポイントに送信されます。トラフィックがフロントドアに到達すると、それは Microsoft のネットワークを経由し、実際の宛先に到達します。顧客ネットワークから Office 365 エンドポイントへのラウンドトリップ時間が短縮されるため、レイテンシーが最小限に抑えられます。

Office 365 エンドポイント

Office 365 エンドポイントは、ネットワークアドレスとサブネットのセットです。Office 365 エンドポイントは、最適化、許可、および既定のカテゴリに分類されます。Citrix SD-WAN 11.4.0 では、[最適化] と [許可] カテゴリをより細かく分類し、ネットワークに依存する Office 365 トラフィックのパフォーマンスを向上させるために、選択的なブッキングを可能にします。ネットワークに依存するトラフィックを、クラウドの SD-WAN (クラウドダイレクトまたは Azure 上の SD-WAN VPX)、または自宅の SD-WAN デバイスから近くのある SD-WAN に、より信頼性の高いインターネット接続で転送することで、QoS と優れた接続復元性を実現します。トラフィックを最寄りのトラフィックにステアリングする場合と比べて、QoS と優れた接続復元性を実現します。Office 365 フロントドア、レイテンシーの増加を犠牲に。QoS を備えた予約済み SD-WAN ソリューションは、VoIP のドロップアウトと切断を減らし、ジッタを減らし、Microsoft Teams のメディア品質の平均オピニオンスコアを向上させます。

- 最適化 - これらのエンドポイントは、Office 365 のすべてのサービスと機能への接続を提供し、可用性、パフォーマンス、待ち時間に敏感です。Office 365 の帯域幅、接続、データ量の 75% 以上を占めています。すべての Optimize エンドポイントは、Microsoft データセンターでホストされます。これらのエンドポイントへのサービスリクエストは、ブランチからインターネットにブレイクアウトする必要があり、データセンターを通過してはなりません。

最適化カテゴリは、次のサブカテゴリに分類されます。

- 1 - [Teams Realtime](#)
- 2 - [Exchange Online](#)
- 3 - [SharePoint Optimize](#)

アップグレードに関する考慮事項については、「[アップグレードに関する重要な考慮事項](#)」を参照してください。

- 許可 - これらのエンドポイントは、特定の Office 365 サービスおよび機能への接続のみを提供し、ネットワークのパフォーマンスと待ち時間にはそれほど敏感ではありません。Office 365 の帯域幅と接続数の表現も低くなります。これらのエンドポイントは、Microsoft データセンターでホストされます。これらのエンドポイントへのサービスリクエストは、ブランチからインターネットにブレイクアウトしたり、データセンターを経由したりする可能性があります。

[許可] カテゴリは、次のサブカテゴリに分類されます。

- 1 - Teams TCP Fallback
- 2 - Exchange Mail
- 3 - SharePoint Allow
- 4 - Office365 Common

アップグレードに関する考慮事項については、「[アップグレードに関する重要な考慮事項](#)」を参照してください。

注:

Teams リアルタイムサブカテゴリは、UDP リアルタイムトランスポートプロトコルを使用して Microsoft Teams トラフィックを管理しますが、**Teams TCP** フォールバックサブカテゴリは TCP トランスポート層プロトコルを使用します。メディアトラフィックはレイテンシーに敏感であるため、このトラフィックは可能な限り最も直接的なパスを利用し、トランスポート層プロトコルとして TCP ではなく UDP を使用する方が望ましい場合があります（品質面では、インタラクティブリアルタイムメディアでは最も好ましいトランスポート）。UDP は Teams メディアトラフィックの優先プロトコルですが、ファイアウォールで特定のポートを許可する必要があります。ポートが許可されていない場合、Teams トラフィックは TCP をフォールバックとして使用します。Teams TCP フォールバックの最適化を有効にすると、このシナリオでは Teams アプリケーションの配信が向上します。詳細については、「[Microsoft Teams の呼び出しフロー](#)」を参照してください。

- デフォルト - これらのエンドポイントは、最適化を必要としない Office 365 サービスを提供し、通常のインターネットトラフィックとして扱うことができます。これらのエンドポイントの一部は、Microsoft データセンターでホストされていない可能性があります。このカテゴリのトラフィックは、遅延の変化の影響を受けません。したがって、このタイプのトラフィックを直接遮断しても、インターネットのブレイクアウトと比較してパフォーマンスが向上することはありません。さらに、このカテゴリのトラフィックは Office 365 トラフィックであるとは限りません。したがって、ネットワークで Office 365 ブレイクアウトを有効にする場合は、このオプションを無効にすることをお勧めします。

Office 365 の最適化の仕組み

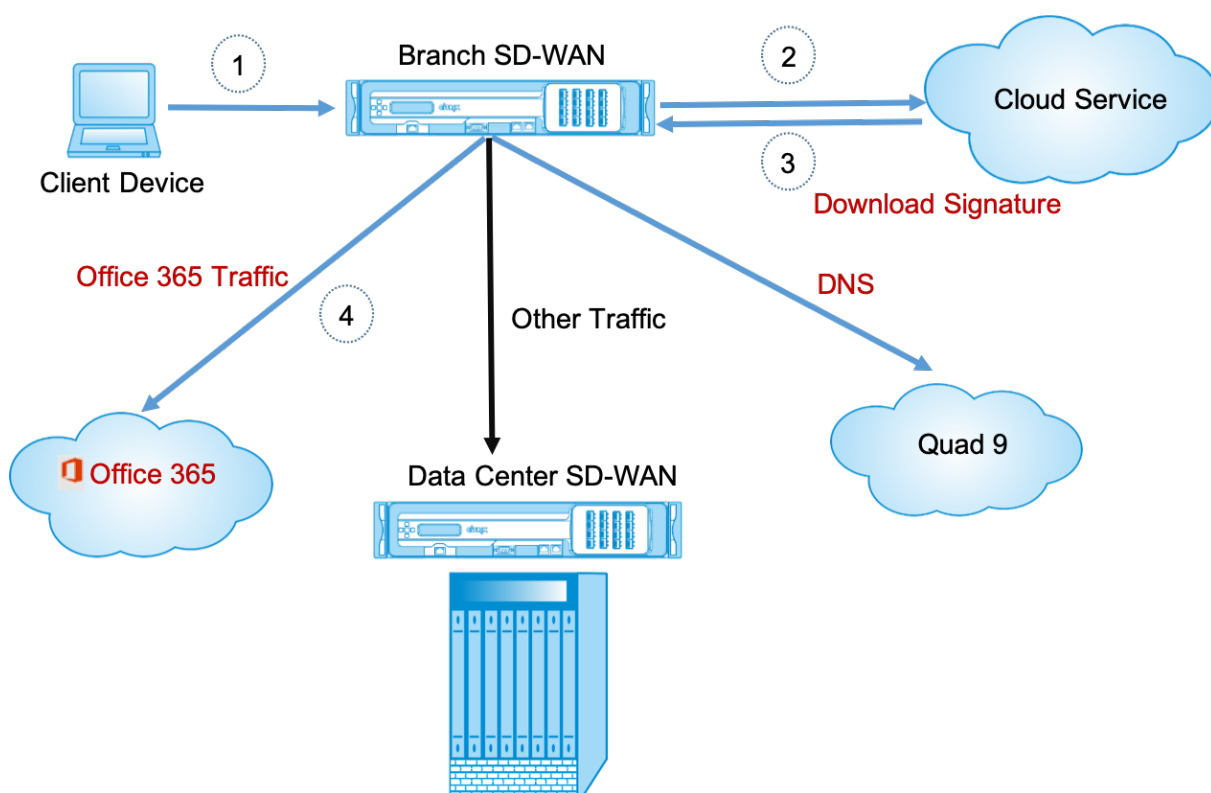
Microsoft エンドポイントの署名は最大で 1 日に 1 回更新されます。アプライアンス上のエージェントは、毎日 Citrix サービス (sdwan-app-routing.citrixnetworkapi.net) をポーリングして、最新のエンドポイント署名のセットを取得します。SD-WAN アプライアンスは、アプライアンスの電源がオンになると、毎日 1 回、Citrix サービス (sdwan-app-routing.citrixnetworkapi.net) をポーリングします。使用可能な新しいシグニチャがある場合、アプライアンスはそのシグニチャをダウンロードし、データベースに保存します。シグニチャは、基本的に、どのト

ラフィックステアリングポリシーを構成できるかに基づいて Office 365 トラフィックを検出するために使用される URL と IP のリストです。

注:

Office 365 の既定のカテゴリを除き、Office 365 ブレークアウト機能が有効かどうかに関係なく、Office 365 トラフィックの最初のパケット検出と分類が既定で実行されます。

Office 365 アプリケーションの要求が到着すると、アプリケーション分類子は、最初のパケット分類子データベース検索、識別、および Office 365 トラフィックをマークします。Office 365 トラフィックが分類されると、自動作成されたアプリケーションルートとファイアウォールポリシーが有効になり、インターネットに直接トラフィックが遮断されます。Office 365 の DNS 要求は、Quad9 などの特定の DNS サービスに転送されます。詳細については、「[ドメインネームシステム](#)」を参照してください。



署名は、クラウドサービス (sdwan-app-routing.citrixnetworkapi.net) からダウンロードされます。

Office 365 ブレークアウトを構成する

Office 365 ブレイクアウトポリシーでは、ブランチから直接抜け出すことができる Office 365 トラフィックのカテゴリを指定できます。Office 365 ブレークアウトを有効にして構成をコンパイルすると、DNS オブジェクト、アプリケーションオブジェクト、アプリケーションルート、およびファイアウォールポリシーテンプレートが自動的に作成され、インターネットサービスを使用してブランチサイトに適用されます。

前提条件

次の項目があることを確認します。

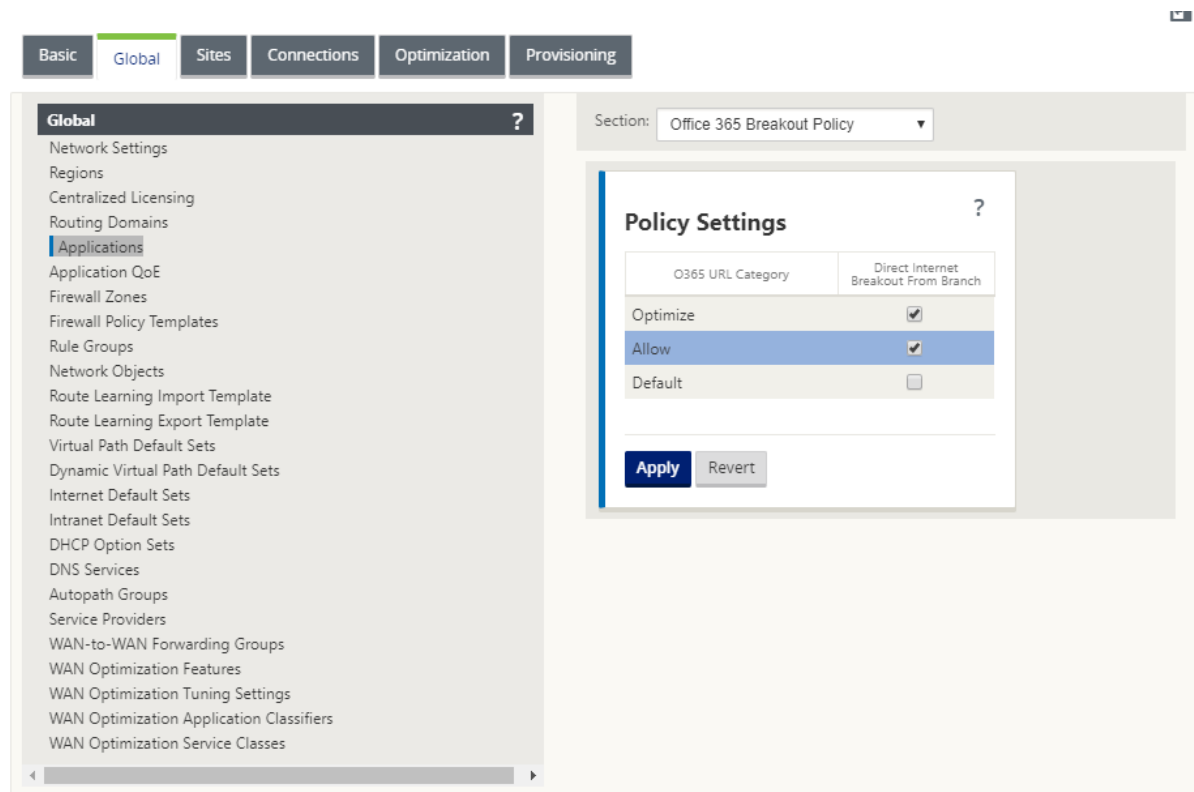
1. Office 365 のブレイクアウトを実行するには、アプライアンスでインターネットサービスを構成する必要があります。インターネットサービスの構成の詳細については、「[インターネットアクセス](#)」を参照してください。
2. 管理インターフェイスにインターネット接続があることを確認します。

Citrix SD-WAN Web インターフェイスを使用して、管理インターフェイスの設定を構成できます。

3. 管理 DNS が設定されていることを確認します。管理インターフェイス DNS を設定するには、構成 > アプライアンスの設定 > ネットワークアダプタに移動します。[**DNS 設定**] セクションで、プライマリ DNS サーバーとセカンダリ DNS サーバーの詳細を指定し、[設定の変更] をクリックします。

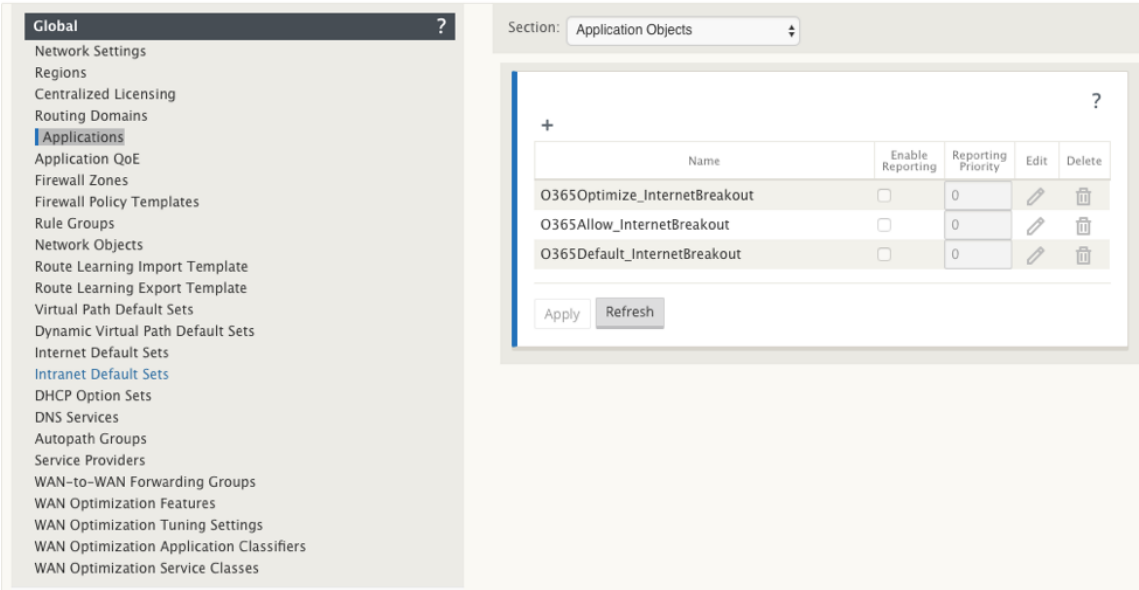
The screenshot displays the Citrix SD-WAN Web interface. The top navigation bar includes 'Dashboard', 'Monitoring', and 'Configuration'. The left sidebar lists various settings categories, with 'Network Adapters' selected. The main content area shows the 'Configuration > Appliance Settings > Network Adapters' path. Under the 'Management Interface IP' section, there are tabs for 'IP Address', 'Ethernet', and 'Mobile Broadband'. The 'IP Address' tab is active, showing fields for 'IP Address' (10.105.147.52), 'Subnet Mask' (255.255.255.0), and 'Gateway IP Address' (10.105.147.1). Below these fields are 'Change Settings' and 'Clear Settings' buttons. The 'DNS Settings' section is highlighted with a red box and contains fields for 'Primary DNS' and 'Secondary DNS', along with 'Change Settings' and 'Clear Settings' buttons.

[**Office 365** ブレイクアウトポリシー] 設定は、[グローバル設定] の下で使用できます。インターネットブレイクアウトに必要な Office 365 カテゴリを選択し、[適用] をクリックします。

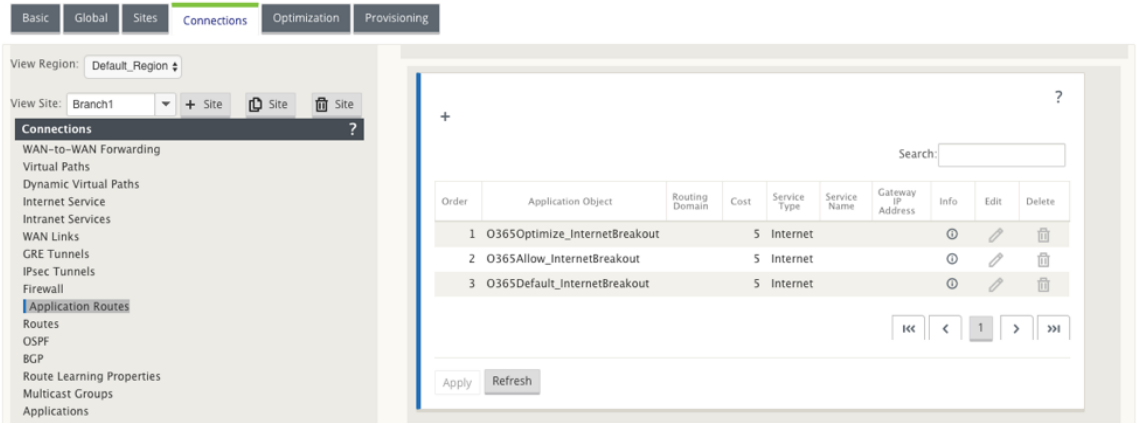


Office 365 を構成した後、ポリシー設定をブレイクアウトし、構成をコンパイルします。次の設定は自動入力されます。

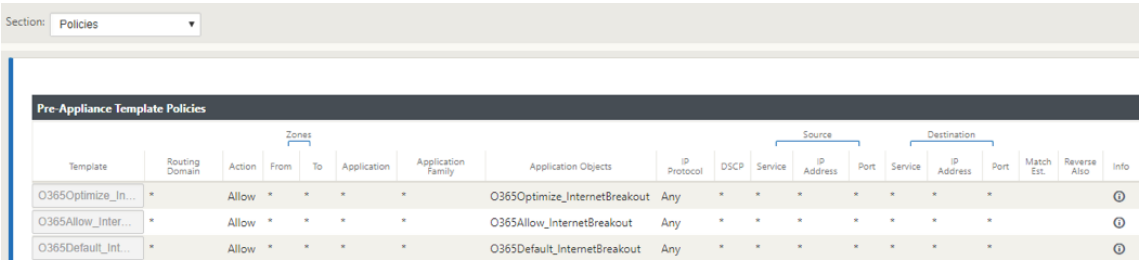
- **DNS** オブジェクト -DNS オブジェクトは、ユーザが設定されている DNS サービスに転送されるトラフィックのタイプを指定します。DNS 要求はすべての信頼されたインターフェイスで受信され、DNS フォワーダーは Office 365 の DNS 要求を Quad9 サービスに送信するために含まれます。このフォワーダ規則は、最も高い優先順位を取ります。詳細については、「ドメインネームサービス」セクションを参照してください。
- アプリケーションオブジェクト -ユーザーが選択した Office 365 カテゴリまたはサブカテゴリを持つアプリケーションオブジェクトが作成されます。****** あなたはデフォルトのカテゴリと最適化と許可のサブカテゴリを選択した場合 ******、次のスクリーンショットに示すように、対応するアプリケーションオブジェクトが作成されます。



- アプリケーションルート: アプリケーションルートは、インターネットサービスの種類の Office 365 アプリケーションオブジェクトごとに作成されます。アップグレードに関する考慮事項については、「[アップグレードに関する重要な考慮事項](#)」を参照してください。



- ファイアウォール事前アプライアンスポリシーテンプレート: 構成済みの Office 365 カテゴリごとに、グローバル事前アプライアンスポリシーテンプレートが作成されます。このテンプレートは、インターネットサービスを持つすべてのブランチサイトに適用されます。アプライアンスの前ポリシーは、ローカルおよびアプライアンスの後ポリシーテンプレートよりも優先されます。アップグレードに関する考慮事項については、「[アップグレードに関する重要な考慮事項](#)」を参照してください。

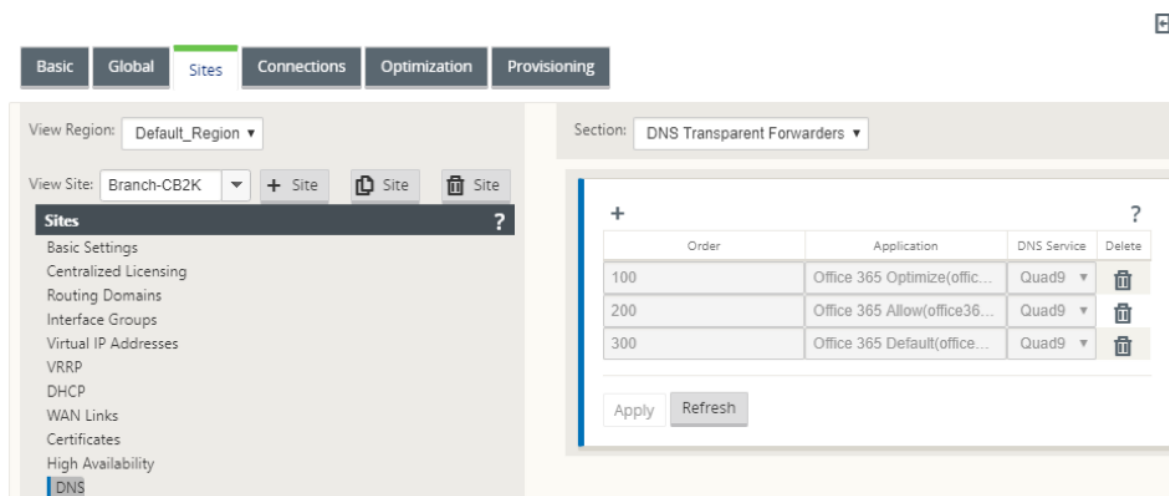


Office 365 の透過的なフォワーダー

Office 365 のブランチは、DNS 要求から始まります。Office 365 ドメインを経由する DNS 要求は、ローカルで操作する必要があります。Office 365 のインターネットブレイクアウトを有効にすると、内部 DNS ルートが決定され、透過フォワーダーリストが自動的に設定されます。Office 365 の DNS 要求は、既定でオープンソースの DNS サービス Quad 9 に転送されます。Quad 9 DNS サービスは、安全でスケーラブルで、マルチポップな存在感を持っています。必要に応じて DNS サービスを変更できます。

Office 365 アプリケーション用の透過的なフォワーダーは、インターネットサービスと Office 365 ブレイクアウトが有効になっているすべてのブランチで作成されます。

別の DNS プロキシを使用している場合、または SD-WAN が DNS プロキシとして構成されている場合、Office 365 アプリケーションのフォワーダーがフォワーダー一覧に自動的に入力されます。



アップグレードに関する重要な考慮事項

カテゴリを最適化して許可する

[Office 365 の最適化] および [許可] カテゴリでインターネットブレイクアウトポリシーを有効にした場合、Citrix SD-WAN 11.4.0 へのアップグレード時に、対応するサブカテゴリのインターネットブレイクアウトポリシーが自動的に有効になります。

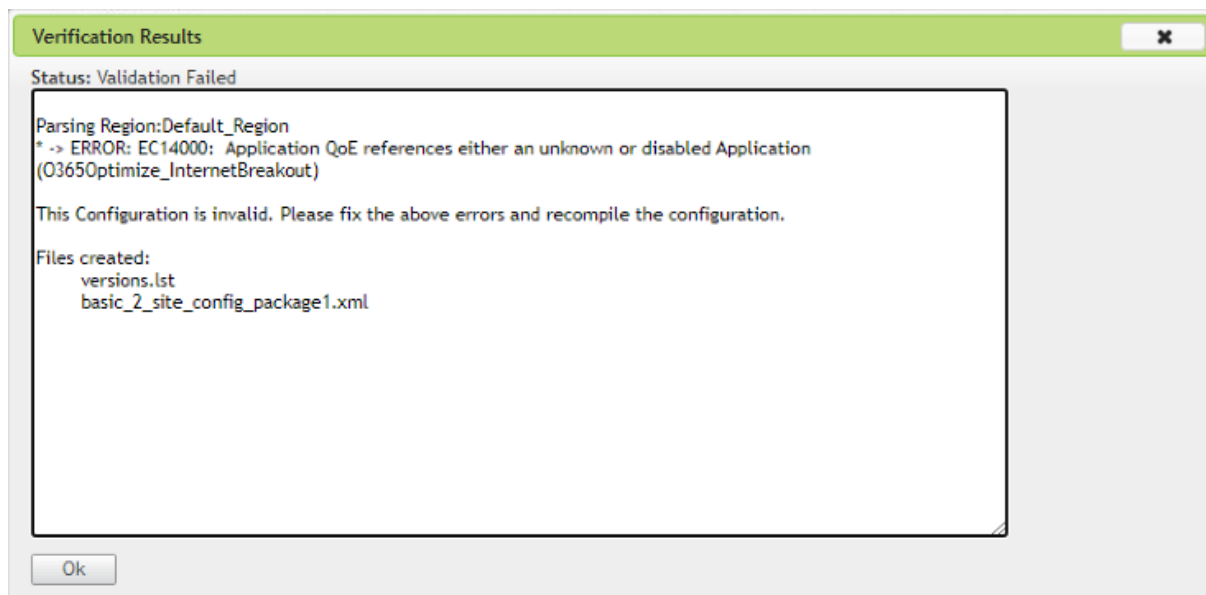
Citrix SD-WAN 11.4.0 より古いソフトウェアバージョンにダウングレードする場合、Citrix SD-WAN 11.4.0 バージョンで対応するサブカテゴリを有効にしたかどうかに関係なく、[Office 365 の最適化] または [許可] カテゴリでインターネットブレイクアウトを手動で有効にする必要があります。そうじゃない

Office 365 アプリケーションオブジェクト

****O365Optimize_internetBreakout** および **O365Allow_InternetBreakout** 自動生成されたアプリケーションオブジェクトを使用してルール/ルートを作成した場合は **、Citrix SD-WAN 11.4.0 にアップグレードする

前に、ルール/ルートを削除してください。アップグレード後、対応する新しいアプリケーションオブジェクトを使用してルール/ルートを作成できます。

ルール/ルートを削除せずに Citrix SD-WAN 11.4.0 のアップグレードを続行すると、エラーが表示され、アップグレードは失敗します。以下の例では、ユーザーがアプリケーション QoE プロファイルを構成し、ルール/ルートを削除せずに Citrix SD-WAN 11.4.0 にアップグレードしようとするときにエラーが表示されます。



注:

このアップグレードは、自動作成されたルール/ルートには必要ありません。これは、作成したルール/ルートにのみ適用されます。

DNS

Office365 の最適化および Office 365 許可アプリケーションを使用して DNS プロキシルールまたは DNS 透過フォワードルールを作成した場合は **、Citrix SD-WAN 11.4.0 にアップグレードする前にルールを削除してください。アップグレード後、対応する新しいアプリケーションを使用してルールを再度作成できます。

古い DNS プロキシまたは透過フォワードルールを削除せずに Citrix SD-WAN 11.4.0 のアップグレードを続行すると、エラーは表示されず、アップグレードも成功します。ただし、Citrix SD-WAN 11.4.0 では、DNS プロキシルールと透過転送ルールは有効になりません。

注:

このアクティビティは、自動作成された DNS ルールには適用されません。これは、作成した DNS ルールにのみ適用されます。

監視

Office 365 アプリケーションの統計情報は、次の SD-WAN 統計レポートで監視できます。

- ファイアウォールの統計情報

Connections																											
		Source							Destination							Sent				Received							
Routing Domain	Application	Family	IP Protocol	IP Address	Port	Service Type	Service Name	Zone	IP Address	Port	Service Type	Service Name	Zone	State	In NAT	Packets	Bytes	PPS	Mbps	Packets	Bytes	PPS	Mbps	Age (s)	Last Activity (s)	Related Objects	
Default_RoutingDomain	Windows (Lendownload)	9966	TCP	172.176.10.103	80962	Local	VirtualInterface-1	Default_LAN_Zone	104.127.231.20	443	Internet	Branch-1-Internet	Internet_Zone	ESTABLISHED	Yes	15	1868	0.071	0.071	13	1281	6.062	0.236	21	3980		ViewThisPage NAT ViewThisPage
Default_RoutingDomain	Office 365 Common(O365_common)	9966	TCP	172.176.10.103	80718	Local	VirtualInterface-1	Default_LAN_Zone	52.168.238.4	443	Internet	Branch-1-Internet	Internet_Zone	ESTABLISHED	Yes	54	3076	0.577	0.772	18	4780	6.764	1.401	13	2390		ViewThisPage NAT ViewThisPage
Default_RoutingDomain	Office 365 Common(O365_common)	9966	TCP	172.176.10.103	80932	Local	VirtualInterface-1	Default_LAN_Zone	13.107.6.171	443	Internet	Branch-1-Internet	Internet_Zone	ESTABLISHED	Yes	1055	803930	5.471	22.491	1880	68935	6.481	18.274	29	4362		ViewThisPage NAT ViewThisPage
Default_RoutingDomain	Office 365 Common(O365_common)	9966	TCP	172.176.10.103	80945	Local	VirtualInterface-1	Default_LAN_Zone	13.107.6.171	443	Internet	Branch-1-Internet	Internet_Zone	ESTABLISHED	Yes	60	23010	0.231	0.766	12	11614	0.287	0.449	29	3968		ViewThisPage NAT ViewThisPage
Default_RoutingDomain	Office 365 Common(O365_common)	9966	TCP	172.176.10.103	80962	Local	VirtualInterface-1	Default_LAN_Zone	13.107.6.138	443	Internet	Branch-1-Internet	Internet_Zone	ESTABLISHED	Yes	391	131932	0.903	2.443	412	24064	0.953	6.688	42	14217		ViewThisPage NAT ViewThisPage
Default_RoutingDomain	Office 365 Common(O365_common)	9966	TCP	172.176.10.103	80981	Local	VirtualInterface-1	Default_LAN_Zone	40.128.12.101	443	Internet	Branch-1-Internet	Internet_Zone	ESTABLISHED	Yes	22	4238	0.073	0.116	17	39802	0.591	0.881	294	3806		ViewThisPage NAT ViewThisPage
Default_RoutingDomain	Office 365 Common(O365_common)	9966	TCP	172.176.10.103	59279	Local	VirtualInterface-1	Default_LAN_Zone	52.108.238.4	443	Internet	Branch-1-Internet	Internet_Zone	ESTABLISHED	Yes	28	8499	0.317	0.769	23	10058	0.820	0.910	48	24049		ViewThisPage NAT ViewThisPage
Default_RoutingDomain	Office 365 Common(O365_common)	9966	TCP	172.176.10.103	59276	Local	VirtualInterface-1	Default_LAN_Zone	52.108.238.4	443	Internet	Branch-1-Internet	Internet_Zone	ESTABLISHED	Yes	65	7864	0.741	0.717	72	10058	0.628	0.716	48	24049		ViewThisPage NAT ViewThisPage
Default_RoutingDomain	Office 365 Common(O365_common)	9966	TCP	172.176.10.103	62018	Local	VirtualInterface-1	Default_LAN_Zone	52.108.36.1	443	Internet	Branch-1-Internet	Internet_Zone	ESTABLISHED	Yes	21	4379	0.032	1.539	15	10058	0.068	0.746	23	3968		ViewThisPage NAT ViewThisPage
Default_RoutingDomain	Office 365 Common(O365_common)	9966	TCP	172.176.10.103	59262	Local	VirtualInterface-1	Default_LAN_Zone	40.128.12.32	443	Internet	Branch-1-Internet	Internet_Zone	ESTABLISHED	Yes	38	19423	0.217	0.743	29	14058	0.173	1.187	16	886		ViewThisPage NAT ViewThisPage
Default_RoutingDomain	Microsoft(Microsoft)	9966	TCP	172.176.10.103	60287	Local	VirtualInterface-1	Default_LAN_Zone	13.107.6.160	443	Internet	Branch-1-Internet	Internet_Zone	ESTABLISHED	Yes	17	7321	0.124	0.166	42	24064	0.147	0.278	29	6827		ViewThisPage NAT ViewThisPage
Default_RoutingDomain	Microsoft(Microsoft)	9966	TCP	172.176.10.103	60247	Local	VirtualInterface-1	Default_LAN_Zone	52.230.219.4	443	Internet	Branch-1-Internet	Internet_Zone	ESTABLISHED	Yes	24	3618	0.088	0.115	19	9621	0.078	0.138	21	4075		ViewThisPage NAT ViewThisPage
Default_RoutingDomain	Microsoft(Microsoft)	9966	TCP	172.176.10.103	60261	Local	VirtualInterface-1	Default_LAN_Zone	23.55.18.151	443	Internet	Branch-1-Internet	Internet_Zone	ESTABLISHED	Yes	14	1766	0.063	0.064	13	9869	0.039	0.232	21	4935		ViewThisPage NAT ViewThisPage
Default_RoutingDomain	Microsoft Skype for Business (Formerly Microsoft Lync Online) (Office 365)(sync_online)	9966	TCP	172.176.10.103	59277	Local	VirtualInterface-1	Default_LAN_Zone	13.107.3.128	443	Internet	Branch-1-Internet	Internet_Zone	ESTABLISHED	Yes	21	2330	0.028	0.254	22	11047	0.229	1.441	74	1883		ViewThisPage NAT ViewThisPage
Default_RoutingDomain	Microsoft Skype for Business (Formerly Microsoft Lync Online) (Office 365)(sync_online)	9966	TCP	172.176.10.103	62015	Local	VirtualInterface-1	Default_LAN_Zone	52.114.74.44	443	Internet	Branch-1-Internet	Internet_Zone	ESTABLISHED	Yes	16	5435	0.337	0.635	11	9605	0.211	0.475	14	7092		ViewThisPage NAT ViewThisPage
Default_RoutingDomain	Microsoft SharePoint Online (Office 365)(sharepoint_online)	9966	TCP	172.176.10.103	60309	Local	VirtualInterface-1	Default_LAN_Zone	13.107.6.168	443	Internet	Branch-1-Internet	Internet_Zone	ESTABLISHED	Yes	56	8714	0.188	0.246	68	13272	0.240	0.422	28	31023		ViewThisPage NAT ViewThisPage
Default_RoutingDomain	Microsoft SharePoint Online (Office 365)(sharepoint_online)	9966	TCP	172.176.10.103	60298	Local	VirtualInterface-1	Default_LAN_Zone	13.107.138.9	443	Internet	Branch-1-Internet	Internet_Zone	ESTABLISHED	Yes	600	230710	2.118	6.755	700	38421	2.031	10.277	296	23487		ViewThisPage NAT ViewThisPage

- フロー

Flows Data														
LAN to WAN Flows														
Details	Routing Domain	Source IP Address	Dest IP Address	Source Port	Dest Port	IPP	Hit Count	Service Type	Service Name	Age (mS)	Packets	Bytes	PPS	Application
⊕	Optimize	172.147.100.146	52.98.65.178	57930	443	TCP	4	INTERNET	-	120979	3	156	0.000	outlook
⊕	Optimize	172.147.100.146	13.107.18.11	57931	443	TCP	15	INTERNET	-	26513	14	1683	0.018	outlook
⊕	Optimize	172.147.100.146	13.107.42.11	57891	443	TCP	20	INTERNET	-	8418	19	1903	0.036	outlook
⊕	Optimize	172.147.100.146	40.100.136.146	57926	443	TCP	14	INTERNET	-	730	13	2118	0.036	outlook
⊕	Optimize	172.147.100.146	40.97.229.82	57918	443	TCP	15	INTERNET	-	1229	14	2178	0.036	outlook
⊕	Optimize	172.147.100.146	52.98.65.178	57929	443	TCP	4	INTERNET	-	121224	3	156	0.000	outlook
⊕	Optimize	172.147.100.146	34.203.255.247	51236	443	TCP	5	INTERNET	-	599759	4	164	0.000	okta
⊕	Optimize	172.147.100.146	34.203.255.247	51237	443	TCP	4	INTERNET	-	592420	3	123	0.000	okta
⊕	Optimize	172.147.100.146	13.107.6.156	51298	443	TCP	29	INTERNET	-	42061	28	11416	0.018	office365_common
⊕	Optimize	172.147.100.146	20.190.140.51	57935	443	TCP	16	INTERNET	-	24735	15	4184	0.018	office365_common
⊕	Optimize	172.147.100.146	13.67.50.225	57897	443	TCP	3	INTERNET	-	2250	2	81	0.047	office365_common
⊕	Optimize	172.147.100.146	13.67.50.225	51228	443	TCP	4	INTERNET	-	603355	3	123	0.000	office365_common
⊕	Optimize	172.147.100.146	13.107.6.156	51255	443	TCP	249	INTERNET	-	377061	248	85307	0.000	office365_common
⊕	Optimize	172.147.100.146	52.109.124.84	57939	443	TCP	20	INTERNET	-	22933	19	4679	0.018	office365_common
⊕	Optimize	172.147.100.146	13.67.50.225	51346	443	TCP	3	INTERNET	-	5900	2	81	0.044	office365_common

- DNS 統計情報

Dashboard	Monitoring	Configuration
Statistics	Monitoring > DNS	
Flows		
Routing Protocols		
Firewall		
IKE/IPsec		
IGMP		
Performance Reports		
QoS Reports		
Usage Reports		
Availability Reports		
Appliance Reports		
DHCP Server/Relay		
VRRP		
PPPoE		
DNS		
DNS Statistics		
Refresh		
Proxy Statistics		
Search:		
Proxy Name	Application Name	DNS Service Name
DNS_Proxy1	office365_optimize	Quad9
DNS_Proxy1	office365_allow	Quad9
DNS_Proxy1	office365_default	Quad9
DNS_Proxy1	Any	Google
Showing 1 to 4 of 4 entries		
Transparent Forwarder Statistics		
Search:		
Application Name	DNS Service Name	DNS Service Active
office365_allow	Quad9	YES
office365_default	Quad9	YES
office365_optimize	Quad9	YES
Showing 1 to 3 of 3 entries		

- アプリケーションルート統計情報

Monitoring > Statistics

Statistics

Show: Application Routes ☒ Enable Auto Refresh 5 seconds ☐ Clear Counters on Refresh Processing...

Application Route Statistics

Maximum allowed routes: 64000

Application Routes for routing domain : Default_RoutingDomain

Filter: In Any column

Show 100 entries Showing 1 to 3 of 3 entries

Num	Application Object	Gateway IP Address	Service	Firewall Zone	Reachable	Site	Type	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
0	O365Optimize_InternetBreakout	*	Internet	Internet_Zone	YES	Branch1	Static	5	1792	YES	N/A	N/A
2	O365Allow_InternetBreakout	*	Internet	Internet_Zone	YES	Branch1	Static	5	1395	YES	N/A	N/A
1	O365Default_InternetBreakout	*	Internet	Internet_Zone	YES	Branch1	Static	5	0	YES	N/A	N/A

Showing 1 to 3 of 3 entries

SD-WAN Center アプリケーションレポートで Office 365 アプリケーションの統計情報を表示することもできます。

Routing Domain: Any

Applications HDX App QoS MOS Services Classes Sites Virtual Paths Paths WAN Links MPLS Queues Ethernet GRE IPsec Events

Report Type: Top Applications Select Site:

Show Bandwidth/Data in KbpsKB Filters: +

10 / page Showing 1 - 10 of 12

Application Name	Aggregate Data	Aggregate Outgoing Data	Aggregate Incoming Data	Average Bandwidth	Average Outgoing Bandwidth	Average Incoming Bandwidth
Office 365 Common	644.22	445.29	198.93	28.63	19.79	8.84
Microsoft Office 365	440.82	21.42	419.40	19.59	0.95	18.64
Microsoft Outlook (Office 365)	264.79	31.72	233.07	11.77	1.41	10.36
Microsoft Skype for Business (formerly Microsoft Lync Online) (Office 365)	215.94	178.94	37.00	9.60	7.95	1.64
Microsoft SharePoint Online (Office 365)	28.48	6.09	22.39	1.27	0.27	0.99
Google Generic	24.09	3.63	20.46	3.21	0.48	2.73
Microsoft	13.29	4.01	9.28	0.59	0.18	0.41
Domain Name Service	6.30	6.30	0.00	0.42	0.42	0.00

トラブルシューティング

SD-WAN アプライアンスの [イベント (Events)] セクションでサービスエラーを表示できます。

エラーを確認するには、[構成] > [システムメンテナンス] > [診断] の順に選択し、[イベント] タブをクリックします。

Dashboard Monitoring Configuration

Configuration > System Maintenance > Diagnostics

Ping Traceroute Packet Capture Path Bandwidth System Info Diagnostic Data **Events** Alarms Diagnostics Tool

Site Diagnostics

Insert Event

Object Type: USER EVENT

Event type: UNDEFINED

Severity: DEBUG

Citrix サービス (sdwan-app-routing.citrixnetworkapi.net) への接続に問題がある場合、エラーメッセージは [イベントの表示] テーブルに表示されます。

View Events

Quantity: 25

Filter: Object Type = APPLICATIONS Event type = FAILURE Severity = ERROR

Reload Events Table

ID	Object ID	Object Name	Object Type	Time	Event Type	Severity	Description
13839	26	Endpoints Update	APPLICATIONS	2019-02-12 09:02:15	FAILURE	ERROR	Failed to connect to the service API

Times are in UTC

接続エラーも **SDWAN_DPI.log** に記録されます。ログを表示するには、[構成] > [アプライアンスの設定] > [ログ/監視] > [ログオプション] に移動します。ドロップダウンリストから **SDWAN_dpi.log** を選択し、[ログの表示] をクリックします。

ログファイルをダウンロードすることもできます。ログファイルをダウンロードするには、[Download Log file] セクションの下でのドロップダウンリストから必要な ログファイルを選択し、[Download Log] をクリックします。

制限事項

- Office 365 ブレークアウトポリシーが構成されている場合、構成された IP アドレスのカテゴリ宛ての接続では、ディープパケットインスペクションは実行されません。
- 自動作成されたファイアウォールポリシーとアプリケーションルートは編集できません。
- 自動作成されたファイアウォールポリシーの優先順位が最も低く、編集できません。
- 自動作成されたアプリケーションルートのルートコストは 5 です。このルートは、低コストのルートで上書きできます。

Office 365 ビーコンサービス

Microsoft は、WAN リンクを介した Office 365 の到達可能性を測定する Office 365 ビーコンサービスを提供しています。ビーコンサービスは、基本的に URL です-sdwan.measure.office.com/apc/trans.png は、定期的にブ

ローブされます。プローブは、インターネット対応のすべての WAN リンクについて、各アプライアンス上で実行されます。プローブごとに HTTP 要求がビーコンサービスに送信され、HTTP 応答が予期されます。HTTP 応答は、Office 365 サービスの可用性と到達可能性を確認します。

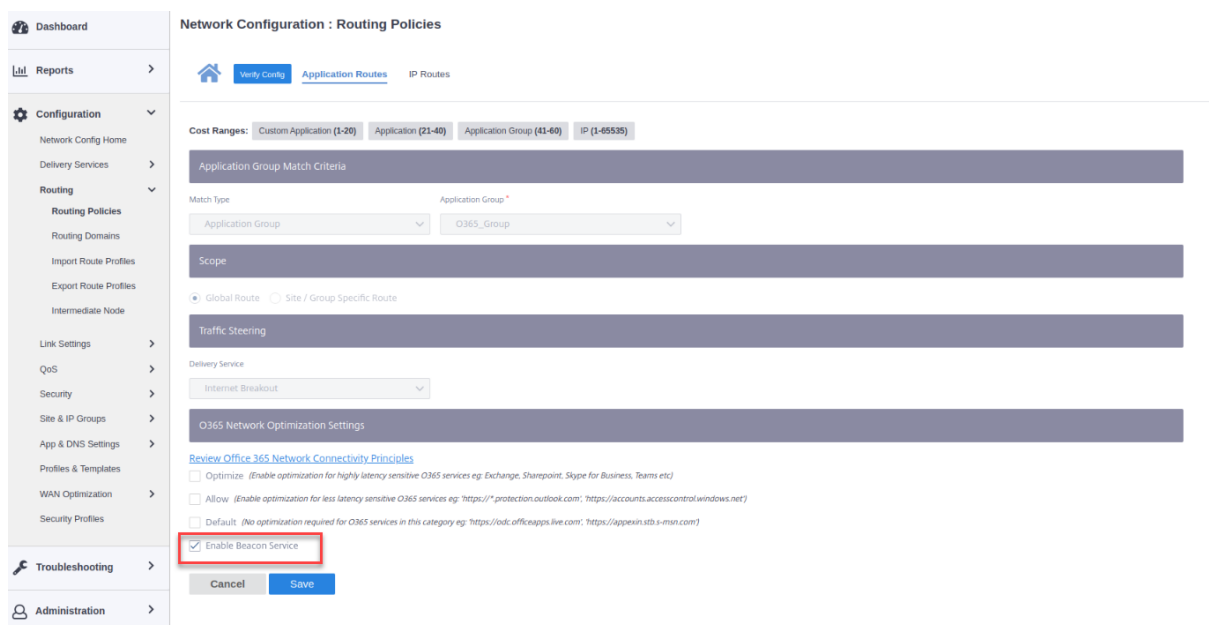
Citrix SD-WAN を使用すると、ビーコンプロービングを実行できるだけでなく、各 WAN リンクを介して Office 365 エンドポイントに到達するレイテンシーも決定できます。待機時間は、WAN リンクを介して Office 365 ビーコンサービスから要求を送信し、応答を取得するのにかかるラウンドトリップ時間です。これにより、ネットワーク管理者は、ビーコンサービスの待ち時間レポートを表示し、Office 365 の直接ブレイクアウトに最適なインターネットリンクを手動で選択できます。ビーコンのプローブは、Citrix SD-WAN Orchestrator を介してのみ有効になります。既定では、Citrix SD-WAN Orchestrator を使用して Office 365 ブレイクアウトが有効になっている場合、インターネットが有効なすべての WAN リンクでビーコンプローブが有効になります。

注

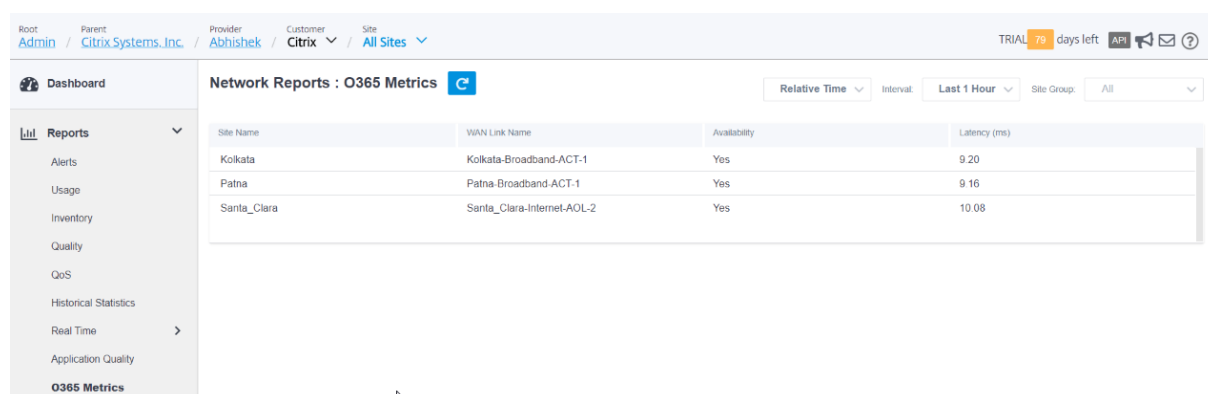
従量制課金リンクでは、Office 365 ビーコンプローブが有効になっていません。

Office 365 ビーコンプロービングを無効にし、SD-WAN Orchestrator で遅延レポートを表示するように選択できます。詳細については、「[Office 365 の最適化](#)」を参照してください。

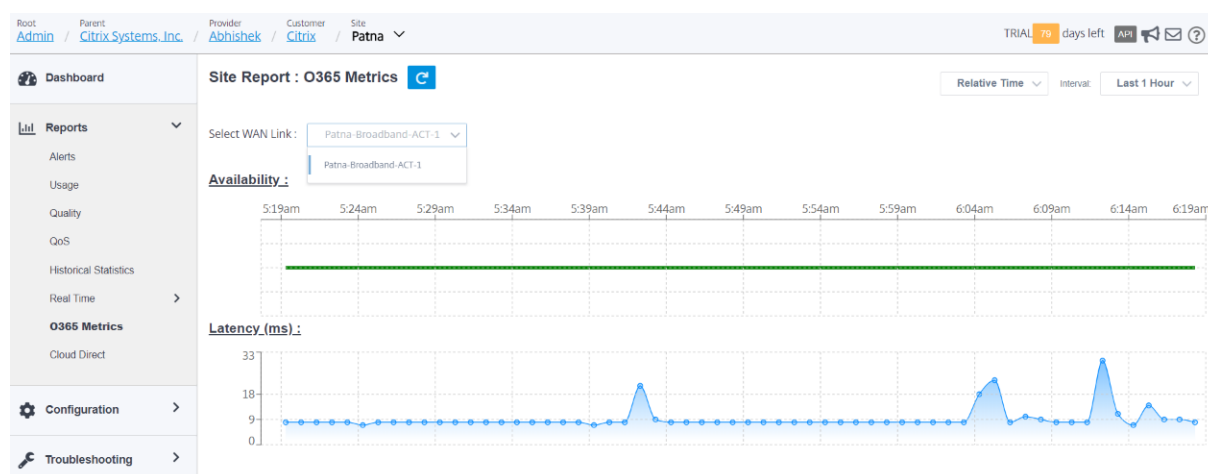
Office 365 ビーコンサービスを無効にするには、SD-WAN Orchestrator で、ネットワークレベルで [構成] > [ルーティング] > [** ルーティングポリシー **] > [O365 ネットワーク最適化の設定] に移動し、[ビーコンサービスを有効にする] をオフにします。



ビーコンのプローブ可用性と待ち時間のレポートを表示するには、Citrix SD-WAN Orchestrator で、ネットワークレベルで [レポート] > [O365 メトリック] に移動します。



ビーコンサービスの詳細なサイトレベルレポートを表示するには、SD-WAN Orchestrator でサイトレベルで [レポート] > [O365 メトリック] に移動します。



Citrix Cloud および Cloud サービスの最適化

August 30, 2022

Citrix Cloud および **Gateway** サービスの最適化機能の強化により、Citrix Cloud および Gateway Service 宛でのトラフィックを検出してルーティングできます。ポリシーを作成して、トラフィックをインターネットに直接遮断するか、または仮想パスを経由してバックホールルート経由で送信することができます。この機能がない場合、デフォルトルートが仮想パスの場合、ゲートウェイサービスはお客様のデータセンターにヘアピンバックし、インターネットに不要な遅延を追加します。さらに、Citrix Gateway サービスと Citrix Cloud トラフィックを可視化し、仮想パスよりも優先する QoS ポリシーを作成できます。

Citrix SD-WAN ソフトウェアバージョン 11.2.1 以降では、Citrix Cloud と Gateway サービスのブレイクアウト機能がデフォルトで有効になっています。

11.3.0 以下の Citrix SD-WAN ソフトウェアでは、Citrix Cloud および Gateway サービスのブレイクアウト機能が無効になっていない場合にのみ、Citrix Cloud および Gateway サービスのトラフィックの最初のパケット検出と

分類が実行されます。

Citrix SD-WAN ソフトウェアバージョン 11.3.0 以降では、Citrix Cloud および Gateway サービスのブレイクアウト機能が有効かどうかに関係なく、Citrix Cloud および Gateway サービスのトラフィックの最初のパケット検出と分類が実行されます。

注

- Citrix SD-WAN Orchestrator を使用してのみ、Citrix Cloud および Gateway サービスの最適化を構成できます。詳細については、「[Gateway サービスの最適化](#)」を参照してください。
- **Citrix SD-WAN Orchestrator** トラフィック最適化は、Citrix SD-WAN ソフトウェアバージョン 11.2.3 以降から導入されています。目標は、より詳細な分類を提供し、Citrix Cloud からの Citrix SD-WAN Orchestrator トラフィックおよびその他の依存サービスのトラフィックを個別に識別し、インターネットブレイクアウトオプションを提供することです。その結果、お客様は Citrix SD-WAN Orchestrator トラフィックのみを最適化することを選択できるようになりました。
- Citrix SD-WAN 11.4.3 以降、Citrix SD-WAN Orchestrator サービスのトラフィック署名は、アプライアンスソフトウェアビルドとともにパッケージ化され、Citrix SD-WAN Orchestrator サービスからの変更管理のステージングプロセス中にアプライアンスにロードされます。この手順は、初期セットアップまたはソフトウェアのアップグレード後に、アプライアンスが Citrix SD-WAN Orchestrator サービスから署名をダウンロードするのを妨げる可能性のある制限を克服するのに役立ちます。

Citrix Cloud および Cloud サービスのカテゴリ

分類および最適化の目的で使用されるトラフィックカテゴリ次に示します。

- **Citrix Cloud:** Citrix Cloud Web UI および API 宛てのトラフィックを検出してルーティングできるようにします。
 - Citrix SD-WAN Orchestrator と依存する重要なサービス:
 - * **Citrix SD-WAN Orchestrator:** Citrix SD-WAN アプライアンスと Citrix SD-WAN Orchestrator 間の接続を確立し、維持するために必要なハートビートやその他のトラフィックからインターネットに直接ブレイクアウトできます。
 - * **Citrix Cloud** ダウンロードサービス: Citrix SD-WAN アプライアンスにアプライアンスソフトウェア、構成、スクリプトなどを直接インターネットでダウンロードできるようにします。
- **Citrix Gateway** サービス: Citrix Gateway Service 宛てのトラフィック（制御およびデータ）を検出してルーティングできるようにします。
 - **Gateway** サービスクライアントデータ: クライアントと **Citrix Gateway Service** 間の ICA データ通線の直接インターネットブレイクアウトを有効にします。高帯域幅と低レイテンシが必要です。

- **Gateway** サービスサーバーデータ: 仮想デリバリーエージェント (VDA) と Citrix Gateway サービス間の ICA データトンネルの直接インターネットブレイクアウトを有効にします。これは、高帯域幅と低レイテンシーを必要とし、VDA リソースの場所 (VDA から Citrix Gateway サービスへの接続) でのみ関連します。
- **Gateway** サービス制御トラフィック: 制御トラフィックからインターネットへの直接ブレイクアウトを有効にします。QoS に関する具体的な考慮事項はありません。
- **Gateway** サービス **Web** プロキシトラフィック: Web プロキシトラフィックの直接インターネットブレイクアウトを有効にします。高い帯域幅が必要ですが、レイテンシーの要件は異なる場合があります。

監視

Gateway サービスの統計情報は、次の SD-WAN 統計レポートで監視できます。

- ファイアウォールの統計情報

Connections																						
			Source					Destination					Stats									
Application	Family	IP Protocol	IP Address	Port	Service Type	Service Name	Zone	IP Address	Port	Service Type	Service Name	Zone	Status	In NAT	Packets	Bytes	PPS	Kbps	Packets	Bytes	PPS	Kbps
Citrix Cloud Web UI and Affinity Cloud Web UI	Custom Application	TCP	10.23.1.5	1234	Local	WF-1-LAN-1	Default_LAN_Zone	12.177.206.73	443	Internet	Branch1_Site-Internet	Internet_Zone	ESTABLISHED	Yes	7	425	0.276	0.204	6	4581	0.231	1.218
Domain Name Service(s)	Network Service	UDP	10.23.1.5	15454	Local	WF-1-LAN-1	Default_LAN_Zone	9.9.9.9	53	Internet	Branch1_Site-Internet	Internet_Zone	ESTABLISHED	Yes	1	70	0.039	0.002	1	198	0.039	0.001
Domain Name Service(s)	Network Service	UDP	10.23.1.5	15916	Local	WF-1-LAN-1	Default_LAN_Zone	9.9.9.9	53	Internet	Branch1_Site-Internet	Internet_Zone	ESTABLISHED	Yes	1	70	0.039	0.002	1	198	0.039	0.001
Citrix Cloud Web UI and Affinity Cloud Web UI	Custom Application	TCP	10.23.1.5	1234	Local	WF-1-LAN-1	Default_LAN_Zone	12.177.206.73	443	Internet	Branch1_Site-Internet	Internet_Zone	ESTABLISHED	Yes	7	425	0.276	0.204	6	4581	0.231	1.218
Domain Name Service(s)	Network Service	UDP	10.23.1.5	12361	Local	WF-1-LAN-1	Default_LAN_Zone	9.9.9.9	53	Internet	Branch1_Site-Internet	Internet_Zone	ESTABLISHED	Yes	1	70	0.039	0.002	1	198	0.039	0.001
Citrix Gateway service Client Dataings client_data	Web	UDP	10.23.1.5	15546	Local	WF-1-LAN-1	Default_LAN_Zone	13.93.207.26	443	Internet	Branch1_Site-Internet	Internet_Zone	ESTABLISHED	Yes	15	2132	0.587	0.861	13	4514	0.509	1.413
Citrix Gateway service Client Dataings client_data	Web	TCP	10.23.1.5	1223	Local	WF-1-LAN-1	Default_LAN_Zone	13.93.207.26	443	Internet	Branch1_Site-Internet	Internet_Zone	ESTABLISHED	Yes	166	18005	8.875	7.701	247	137619	13.206	58.990
Citrix Cloud Web UI and Affinity Cloud Web UI	Custom Application	TCP	10.23.1.5	1235	Local	WF-1-LAN-1	Default_LAN_Zone	12.177.206.73	443	Internet	Branch1_Site-Internet	Internet_Zone	ESTABLISHED	Yes	45	21131	0.141	0.530	43	21189	0.135	0.516

Connections Displayed: 8
Connections in Use: 49/128000

Connections																						
			Source					Destination					Stats									
Application	Family	IP Protocol	IP Address	Port	Service Type	Service Name	Zone	IP Address	Port	Service Type	Service Name	Zone	Status	In NAT	Packets	Bytes	PPS	Kbps	Packets	Bytes	PPS	Kbps
Citrix Cloud Download Services (cloud_download_svc)	Web	TCP	172.16.30.30	40900	Local	WF-1-LAN-1	Default_LAN_Zone	14.238.77.219	80	Internet	BRANCH1_KVMNPH-Internet	Internet_Zone	ESTABLISHED	Yes	3	180	0.034	0.440	0	0	0.000	0.000
Citrix SD-WAN Download Services (sdwan_download_svc)	Web	TCP	172.16.30.30	34934	Local	WF-1-LAN-1	Default_LAN_Zone	14.238.77.219	443	Internet	BRANCH1_KVMNPH-Internet	Internet_Zone	CLOSED	Yes	11	1380	1.980	5.833	12	6668	3.076	9.251
Domain Name Service(s)	Network Service	UDP	172.16.30.30	41158	Local	WF-1-LAN-1	Default_LAN_Zone	9.9.9.9	53	Virtual Path	MCN_KVMNPH-BRANCH1_KVMNPH	Any	ESTABLISHED	No	2	112	0.030	0.202	2	116	0.010	0.081
Domain Name Service(s)	Network Service	UDP	172.16.30.30	41883	Local	WF-1-LAN-1	Default_LAN_Zone	9.9.9.9	53	Internet	BRANCH1_KVMNPH-Internet	Internet_Zone	ESTABLISHED	Yes	2	174	0.274	0.191	2	388	0.274	0.426
Domain Name Service(s)	Network Service	UDP	172.16.30.30	39368	Local	WF-1-LAN-1	Default_LAN_Zone	9.9.9.9	53	Internet	BRANCH1_KVMNPH-Internet	Internet_Zone	ESTABLISHED	Yes	2	164	0.157	0.152	2	368	0.157	0.290
Google Gcm/gcm/google	Web	TCP	172.16.30.30	14534	Local	WF-1-LAN-1	Default_LAN_Zone	172.217.31.206	80	Virtual Path	MCN_KVMNPH-BRANCH1_KVMNPH	Any	CLOSED	No	6	394	1.126	0.801	5	796	1.271	1.419

Connections Displayed: 6
Connections in Use: 6/128000

- フロー

Monitoring > Flows																						
Select Flows																						
Flow Type: <input checked="" type="checkbox"/> LAN to WAN <input checked="" type="checkbox"/> WAN to LAN <input type="checkbox"/> Internet Local Balancing Table <input type="checkbox"/> TCP Termination Table																						
Main Flows to Display (Per Flow Type): <input type="text" value="50"/> <input type="button" value="Go"/>																						
Filter (Optional): <input type="text" value="Internet"/> <input type="button" value="Apply"/>																						
<input type="button" value="Refresh"/>																						
Flows Data																						
Switch LAN to WAN and WAN to LAN Flows																						
172.16.70.5	40.112.143.211	LAN to WAN	40927	443	TCP	default	10	INTERNET	-	LOCAL	6421	9	940	1.302	1.170	0.000	0.000	214	N/A	N/A	N/A	N/A
172.16.70.4	9.9.9.9	LAN to WAN	54577	53	UDP	default	2	INTERNET	-	LOCAL	8646	1	74	0.116	0.008	0.000	0.000	214	N/A	N/A	N/A	N/A
172.16.70.5	52.168.75.17	LAN to WAN	63914	443	TCP	default	2	INTERNET	-	LOCAL	3198716	1	166	0.000	0.000	0.000	0.000	214	N/A	N/A	N/A	N/A
172.16.70.5	40.112.143.211	LAN to WAN	50231	443	TCP	default	9	INTERNET	-	LOCAL	1079	8	906	7.106	8.438	0.000	0.000	214	N/A	N/A	N/A	N/A
172.16.70.4	40.112.143.211	LAN to WAN	50231	443	TCP	default	9	INTERNET	-	LOCAL	6481	8	906	1.240	1.123	0.000	0.000	214	N/A	N/A	N/A	N/A
172.16.70.5	40.112.143.211	LAN to WAN	49930	443	TCP	default	9	INTERNET	-	LOCAL	3701	8	906	2.137	1.939	0.000	0.000	214	N/A	N/A	N/A	N/A
172.16.70.5	40.112.143.211	LAN to WAN	62117	443	TCP	default	940	INTERNET	-	LOCAL	360542	444	97918	0.112	0.010	0.000	0.000	214	N/A	N/A	N/A	N/A
172.16.70.4	40.112.143.211	LAN to WAN	64200	443	TCP	default	640	INTERNET	-	LOCAL	4062	846	40126	0.161	0.147	0.000	0.000	214	N/A	N/A	N/A	N/A
172.16.70.4	15.81.161.240	LAN to WAN	63304	443	TCP	default	3011	INTERNET	-	LOCAL	3199117	3014	1073108	0.762	1.172	0.000	0.000	214	N/A	N/A	N/A	N/A
9.9.9.9	172.16.70.5	WAN to LAN	11	50230	UDP	default	1	INTERNET	-	LOCAL	3711	1	212	0.267	0.002	0.000	0.000	214	N/A	N/A	N/A	N/A
40.112.143.211	172.16.70.4	WAN to LAN	443	50230	TCP	default	12	INTERNET	-	LOCAL	3712	12	5209	3.100	11.060	0.000	0.000	214	N/A	N/A	N/A	N/A
40.112.143.211	172.16.70.4	WAN to LAN	443	50230	TCP	default	12	INTERNET	-	LOCAL	8521	12	5209	3.086	4.913	0.000	0.000	214	N/A	N/A	N/A	N/A
40.112.143.211	172.16.70.5	WAN to LAN	443	49930	TCP	default	12	INTERNET	-	LOCAL	1108	12	5209	10.476	16.800	0.000	0.000	214	N/A	N/A	N/A	N/A
40.112.143.211	172.16.70.5	WAN to LAN	443	49930	TCP	default	12	INTERNET	-	LOCAL	9028	12	5209	1.476	4.524	0.000	0.000	214	N/A	N/A	N/A	N/A
40.112.143.211	172.16.70.5	WAN to LAN	443	64000	TCP	default	412	INTERNET	-	LOCAL	961	412	144015	0.209	0.122	0.000	0.000	214	N/A	N/A	N/A	N/A
40.112.143.211	172.16.70.4	WAN to LAN	443	62453	TCP	default	327	INTERNET	-	LOCAL	3604809	327	38200	0.000	0.000	0.000	0.000	214	N/A	N/A	N/A	N/A

Total LAN to WAN Flows displayed: 18 out of 70
Total WAN to LAN Flows displayed: 15 out of 69

Flows Data																				
Both LAN to WAN and WAN to LAN Flows																				
Toggle Columns																				
IP	DSCP	HS Count	Service Type	Service Name	LAN GW IP	Age (mS)	Packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	App Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type	Application
IP	default	3	INTERNET	-	LOCAL	8034	2	174	0.249	0.173	0.000	0.000	147	N/A	N/A	N/A	N/A	N/A	N/A	N/A
P	default	4	INTERNET	-	LOCAL	2875	3	180	0.507	0.244	0.000	0.000	147	N/A	N/A	N/A	N/A	N/A	N/A	citrix_cloud_download_svc
P	default	16	INTERNET	-	LOCAL	4059	15	1372	1.927	1.410	0.000	0.000	147	N/A	N/A	N/A	N/A	N/A	N/A	citrix_sdwan_orchestrator
IP	default	3	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	LOCAL	6447	2	112	0.310	0.139	0.141	0.000	57	N/A	13	INTERACTIVE	BRANCH1_KVMVPX-Internet-ACT-1->MCN_KVMVPX-Internet-ACT-1	N/A	Load Balanced, Reliable	N/A
P	default	7	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	LOCAL	5967	6	394	0.969	0.509	0.442	0.000	1	N/A	13	INTERACTIVE	BRANCH1_KVMVPX-Internet-ACT-1->MCN_KVMVPX-Internet-ACT-1	N/A	Load Balanced, Reliable	google_gen

DNS 統計情報

Monitoring > DNS

DNS Statistics				
Refresh				

Proxy Statistics				
Search:				
Proxy Name	Application Name	DNS Service Name	DNS Service Active	Hits
Default	office365_optimize	Quad9	YES	0
Default	citrix_cloud_web_ui_api	Quad9	YES	4
Default	ngs_client_data	Quad9	YES	14
Default	ngs_server_data	Quad9	YES	0
Default	ngs_control_traffic	Quad9	YES	2286
Default	ngs_web_proxy	Quad9	YES	0
Default	Any	azureDNS	YES	51490
Showing 1 to 7 of 7 entries				

Transparent Forwarder Statistics

Search:

Application Name	DNS Service Name	DNS Service Active	Hits
citrix_cloud_web_ui_api	Quad9	YES	0
ngs_client_data	Quad9	YES	0
ngs_control_traffic	Quad9	YES	0
ngs_server_data	Quad9	YES	0
ngs_web_proxy	Quad9	YES	0
office365_optimize	Quad9	YES	0

Showing 1 to 6 of 6 entries

Transparent Forwarder Statistics

Search:

Application Name	DNS Service Name	DNS Service Active	Hits
citrix_cloud_download_svc	Quad9	YES	1
citrix_sdwan_orchestrator	Quad9	YES	1

Showing 1 to 2 of 2 entries

アプリケーションルート統計情報

Monitoring > Statistics

Statistics

Show: Application Routes ☐ Enable Auto Refresh 5 seconds Refresh ☒ Clear Counters on Refresh

Application Route Statistics

Maximum allowed routes: 64000

Application Routes for routing domain : Default_RoutingDomain

Filter: in Any column Apply

Show 100 entries Showing 1 to 6 of 6 entries

Num	Application Object	Gateway IP Address	Service	Firewall Zone	Reachable	Site	Type	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
0	O365Optimize_InternetBreakout	*	Internet	Untrusted_Internet_Zon	YES	azure07	Static	50	7	YES	N/A	N/A
1	NGS_WebProxy_Breakout	*	Internet	Untrusted_Internet_Zon	YES	azure07	Static	50	0	YES	N/A	N/A
2	NGS_ServerData_Breakout	*	Internet	Untrusted_Internet_Zon	YES	azure07	Static	50	44	YES	N/A	N/A
3	NGS_ControlTraffic_Breakout	*	Internet	Untrusted_Internet_Zon	YES	azure07	Static	50	72	YES	N/A	N/A
4	NGS_ClientData_Breakout	*	Internet	Untrusted_Internet_Zon	YES	azure07	Static	50	0	YES	N/A	N/A
5	CitrixCloud_Breakout	*	Internet	Untrusted_Internet_Zon	YES	azure07	Static	50	0	YES	N/A	N/A

Showing 1 to 6 of 6 entries

Application Route Statistics

Maximum allowed routes: 64000

Application Routes for routing domain : Default_RoutingDomain

Filter: in Any column Apply

Show 100 entries Showing 1 to 2 of 2 entries

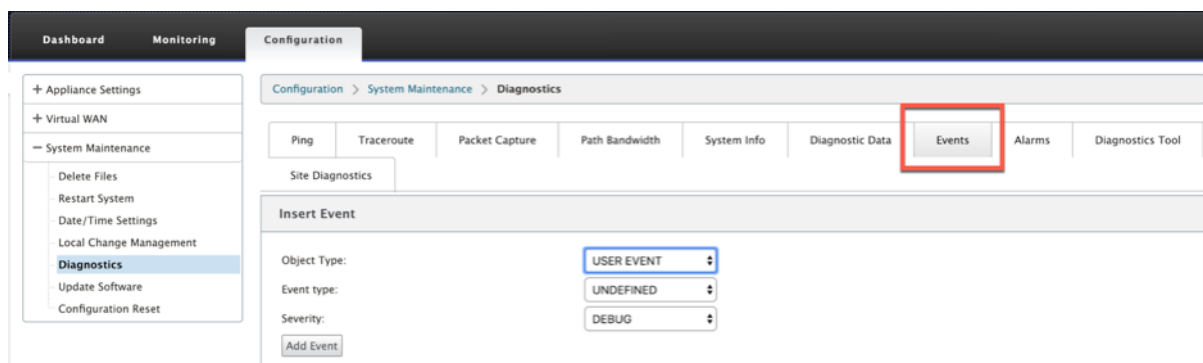
Num	Application Object	Gateway IP Address	Service	Firewall Zone	Reachable	Site	Type	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
0	CitrixSdwanOrchestrator_Breakout	*	Internet	Internet_Zone	YES	BRANCH1_KVMVPK	Static	50	35	YES	N/A	N/A
1	CitrixCloudDownloadSvc_Breakout	*	Internet	Internet_Zone	YES	BRANCH1_KVMVPK	Static	50	8	YES	N/A	N/A

Showing 1 to 2 of 2 entries

トラブルシューティング

SD-WAN アプライアンスの [イベント (Events)] セクションでサービスエラーを表示できます。

エラーを確認するには、[構成] > [システムメンテナンス] > [診断] の順に選択し、[イベント] タブをクリックします。



Citrix サービス (sdwan-app-routing.citrixnetworkapi.net) への接続に問題がある場合、エラーメッセージは [イベントの表示] テーブルに表示されます。

View Events

Quantity: 25

Filter: Object Type = APPLICATIONS Event type = FAILURE Severity = ERROR

Reload Events Table

ID	Object ID	Object Name	Object Type	Time	Event Type	Severity	Description
13839	26	Endpoints Update	APPLICATIONS	2019-02-12 09:02:15	FAILURE	ERROR	Failed to connect to the service API

Times are in UTC

接続エラーも **SDWAN_DPI.log** に記録されます。ログを表示するには、[構成] > [アプライアンスの設定] > [ログ/監視] > [ログオプション] に移動します。ドロップダウンリストから **SDWAN_dpi.log** を選択し、[ログの表示] をクリックします。

ログファイルをダウンロードすることもできます。ログファイルをダウンロードするには、[Download Log file] セクションの下にドロップダウンリストから必要な ログファイルを選択し、[Download Log] をクリックします。

Citrix SD-WAN アプライアンスのオンプレミス構成用の Citrix SD-WAN オーケストレータ

November 17, 2022

オンプレミス向け Citrix SD-WAN Orchestrator は、Citrix SD-WAN Orchestrator サービスのオンプレミスソフトウェアバージョンです。オンプレミス向け Citrix SD-WAN Orchestrator は、Citrix パートナーが適切な役割ベースのアクセス制御を使用して、複数の顧客を一元管理するための単一ペイン管理プラットフォームを提供します。

Citrix SD-WAN アプライアンスとオンプレミス向けの Citrix SD-WAN Orchestrator 間の接続を確立するには、オーケストレータの接続を有効にし、オンプレミスアイデンティティ用に Citrix SD-WAN Orchestrator を指定します。

注

- SD-WAN アプライアンスでのオンプレミス **SD-WAN** オーケストレータ構成機能が **SD-WAN** アプライアンスで構成されている場合、**Cloud Orchestrator** ゼロタッチ展開は機能しません。
- Citrix SD-WAN Orchestrator リリース 11.3.0 で構成された SD-WAN アプライアンス上のオンプレミス構成用 Citrix SD-WAN Orchestrator がリリース 10.2.7 にダウングレードされた場合、SD-WAN アプライアンスのオンプレミス向け Citrix SD-WAN オーケストレータは失われます。リリース 11.3.0 からリリース 10.2.7 へのダウングレードはサポートされていません。回避策は、ダウングレード後にオンプレミスアイデンティティ用に Citrix SD-WAN Orchestrator を再構成することです。
- SD-WAN アプライアンスを 11.3.0 から 11.1.1/11.2.0/10.2.7 ソフトウェアバージョンにダウングレードした後、Citrix SD-WAN アプライアンスの UI でアイデンティティ設定を再度適用する必要があります。オンプレミス構成または SD-WAN アプライアンス接続用の Citrix SD-WAN Orchestrator に関連する問題がある場合は、オンプレミス接続用の Citrix SD-WAN Orchestrator を無効にしてから、Citrix SD-WAN Orchestrator をオンプレミス接続用に再度有効にします。

Citrix SD-WAN Orchestrator をオンプレミス接続で有効にするには:

1. SD-WAN アプライアンス UI で、設定 > 仮想 **WAN** > オンプレミス **SD-WAN Orchestrator** に移動します。
2. [オンプレミ **SD-WAN Orchestrator** 接続を有効にする] チェックボックスをオンにします。

3. オンプレミス IP アドレスまたはドメイン用の Citrix SD-WAN Orchestrator、または両方（IP アドレスとドメイン）を構成用に入力します。

ドメインのみを構成する場合は、ローカル DNS サーバーに DNS レコードを追加し、SD-WAN アプライアンスに DNS サーバーの IP アドレスを構成する必要があります。構成するには、[構成] > [ネットワークアダプタ] > [IP アドレス] に移動します。

たとえば、オンプレミisdメイン用の Citrix SD-WAN Orchestrator が **citrix.com** として構成されている場合は、次の FQDN の DNS サーバーおよびオンプレミス IP アドレス用の Citrix SD-WAN オーケストレータの DNS レコードを作成する必要があります。

- download.citrix.com

- sdwanzt.citrix.com
- sdwan-home.citrix.com

高度な構成では、次のようになります。

たとえば、オーケストレータのオンプレミスドメインが **citrix.com** として構成されている場合、ダウンロード管理サービスドメインは **download.citrix.com** として構成され、統計管理サービスドメインは **statistics.ics.citrix.com** として構成されます。次に、以下の FQDN と対応する IP アドレスの DNS レコードを DNS サーバに作成する必要があります。

- download.citrix.com
- sdwanzt.citrix.com
- statistics.citrix.com

The screenshot shows the Citrix SD-WAN Configuration interface. The left sidebar contains a menu with options like 'Appliance Settings', 'Virtual WAN', and 'System Maintenance'. The main content area is titled 'Configuration > Virtual WAN > On-prem SD-WAN Orchestrator'. It contains two sections: 'On-prem SD-WAN Orchestrator Identity' and 'Authentication Type'. The 'Identity' section has checkboxes for 'Enable On-prem SD-WAN Orchestrator Connectivity' and 'Advanced Configuration'. Below these are input fields for IP addresses and domains for the Orchestrator, Download Management Service, and Statistics Management Service. The 'Authentication Type' section has a dropdown menu set to 'No Authentication' and an 'Apply' button.

Orchestrator オンプレミスでは、ダウンロード、独立したサーバーインスタンスでの統計などの実行サービスをサポートし、大規模なネットワークのスケラビリティを向上させることができます。詳細構成を選択し、ダウンロード管理サービスと統計管理サービスを構成できます。

[詳細設定] チェックボックスをオンにして、次の詳細を入力します。

- **ダウンロード管理サービス IP/ドメイン:** SD-WAN ソフトウェアおよび構成のダウンロードの側面を独立したサーバーインスタンスにオフロードするのに役立つ IP アドレス/ドメインを提供し、大規模ネットワークのスケラビリティを向上させます。
- **統計管理サービス IP/ドメイン:** SD-WAN 統計情報の収集と管理をデバイスから独立したサーバーインスタンスへオフロードできる IP アドレス/ドメインを提供し、大規模ネットワークのスケラビリティを向上させます。

4. [認証タイプ] を選択します。SD-WAN アプライアンスと Citrix SD-WAN Orchestrator 間でオンプレミス接続用にサポートされている認証の種類は次のとおりです。

- 認証なし—オンプレミスの SD-WAN オーケストレータと SD-WAN アプライアンス間の認証は行われません。**SD-WAN** アプライアンスまたはオンプレミス **SD-WANOrchestrator** 証明書を使用する必要はありません。ただし、MPLS などのセキュアなネットワークがある場合は、このオプションを使用できます。
- 一方向認証—一方向認証の種類を選択するには、Orchestrator オンプレミスの証明書をアップロードする必要があります。Orchestrator オンプレミスから Orchestrator オンプレミス証明書をダウンロードし、[アップロード] をクリックします SD-WAN アプライアンスは、アップロードされた証明書を使用して Orchestrator をオンプレミスで信頼します。
- 双方向認証—Orchestrator オンプレミス証明書とアプライアンス証明書は相互に交換する必要があります。双方向認証の場合は、Orchestrator 上のオンプレミスで SD-WAN アプライアンス証明書を再生成、ダウンロード、アップロードする必要があります。SD-WAN アプライアンスとオンプレミスの Orchestrator は、交換された証明書を使用して相互に信頼します。

注:

一方向認証または双方向認証のみを使用することをお勧めします。[認証なし] の場合は、DNS が DNS 攻撃から保護されていることを確認します。

Orchestrator オンプレミスの認証タイプが無効になっている場合、アプライアンスは、認証なし、一方向認証、または双方向認証モードのいずれかを使用して ** Orchestrator をオンプレミスに接続できます。

Orchestrator オンプレミス認証タイプが有効になっている場合、アプライアンスは双方向認証を介してオンプレミスの Orchestrator にのみ接続できます。

オンプレミスの Orchestrator の認証タイプを有効状態から無効にすると、一方向認証モードの既存のアプライアンスは切断状態になります。接続するには、アプライアンス認証の種類を [双方向認証] に変更し、SD-WAN アプライアンス証明書をオンプレミスの Orchestrator にアップロードする必要があります。

注

- 生成される証明書は X509 自己署名証明書です。
- 証明書の有効期限が切れたり、侵害されたりした場合は、証明書を再生成する必要があります。
- 証明書の有効期間は 10 年です。
- フィンガープリント、開始日、終了日などの証明書の詳細を表示できます。
- お客様は、オンプレミスの Orchestrator と SD-WAN アプライアンスの間で証明書を再生成し、交換する必要があります。これにより、オンプレミスの Orchestrator とのアプライアンス接続が失われるのを防ぐことができます。

Authentication Type

No Authentication : No Authentication between On-prem SD-WAN Orchestrator and SD-WAN Appliance. Customer can use this option if they have already secure network. For eg: MPLS

One-way Authentication : SD-WAN Appliance will authenticate On-prem SD-WAN Orchestrator. On-prem SD-WAN Orchestrator certificate should be uploaded on SD-WAN Appliance.

Two-way Authentication : On-prem SD-WAN Orchestrator and SD-WAN Appliance authenticates each other. SD-WAN Appliance and On-prem SD-WAN Orchestrator certificates should be exchanged each other.

Authentication Type Two-way Authentication

Apply

On-prem SD-WAN Orchestrator Certificate

Certificate Filename: Choose file No file chosen Upload

Certificate Details

Certificate Fingerprint: 75:38:C2:32:AC:07:6E:26:6C:D9:C6:08:73:A2:73:8D:81:91:5A:4C
Start Date: Jul 22 11:26:32 2020 GMT
End Date: Jul 20 11:26:32 2030 GMT

SD-WAN Appliance Certificate

Certificate Details

Certificate Fingerprint: FC:36:3C:E5:EF:C2:F8:ED:48:20:0C:28:6C:5D:8A:82:55:CE:04:DD
Start Date: Jul 21 06:07:08 2020 GMT
End Date: Jul 19 06:07:08 2030 GMT

Regenerate Download

5. [設定の適用] をクリックします。

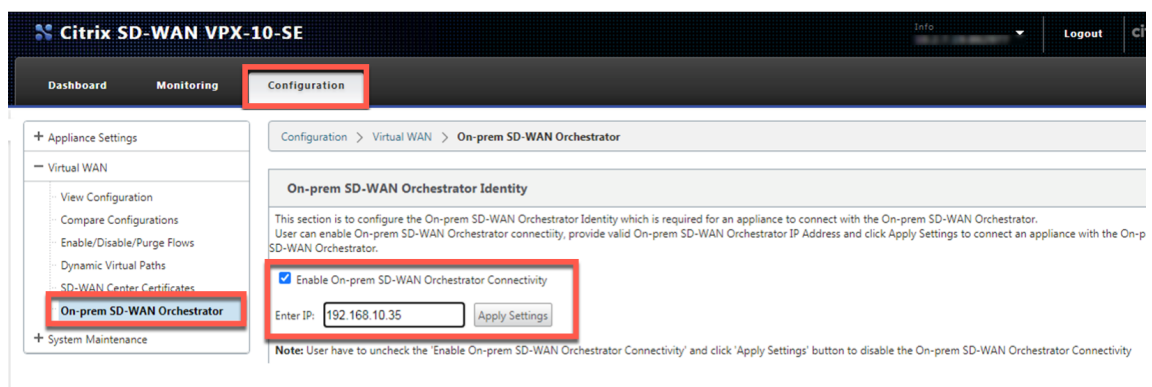
Citrix SD-WAN Orchestrator のオンプレミス接続を無効にするには、[**Citrix SD-WAN Orchestrator** のオンプレミス接続を有効にする] オプションをオフにして、[設定の適用] をクリックします。Orchestrator オンプレミスの管理対象ネットワークを Cloud Orchestrator または MCN 管理対象ネットワークに変換するには、オンプレミス接続用の Citrix SD-WAN Orchestrator を無効にし、構成のリセットを実行する必要があります。設定をリセットするには、[構成] > [システムメンテナンス] > [構成のリセット] に移動します。

オンプレミス向け **Citrix SD-WAN** オーケストレータを使用して、ソフトウェアバージョン **10.2.7**、**11.1.1**、または **11.2.0** で実行されている **Citrix SD-WAN** アプライアンスを展開する

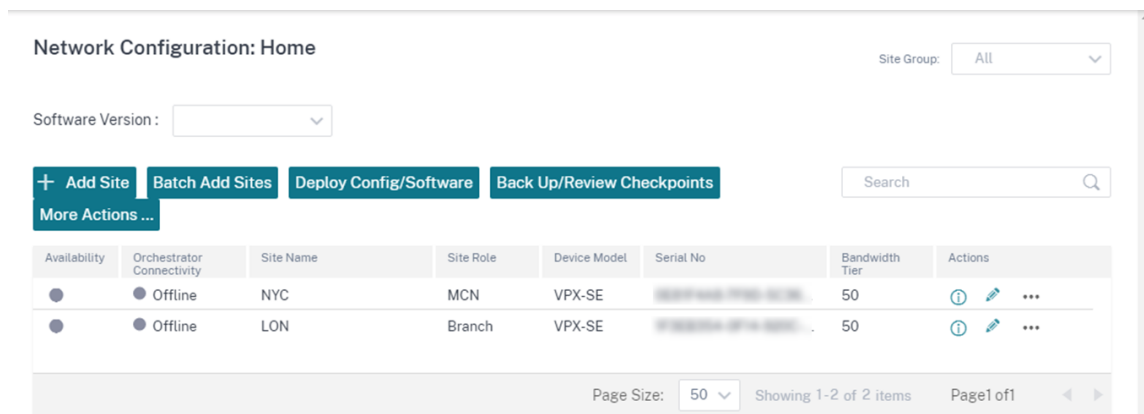
注：

ソフトウェアバージョン 10.2.7、11.1.1、または 11.2.0 で Citrix SD-WAN アプライアンスを展開するには、オンプレミスバージョン 11.1 以降用の Citrix SD-WAN Orchestrator が必要です。

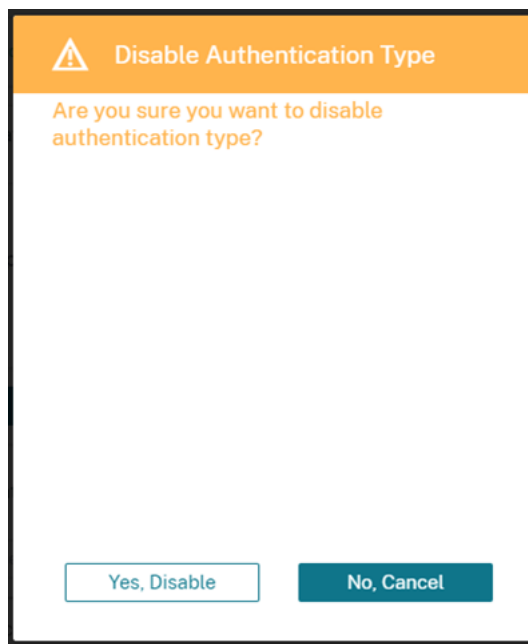
- ソフトウェアバージョン 10.2.7、11.1.1、または 11.2.0 の Citrix SD-WAN アプライアンスごとに、アプライアンスの Web インターフェイスにログインし、次の手順を実行します。
 - [構成] > [仮想 WAN] > [オンプレミス **SD-WAN Orchestrator**] に移動し、[オンプレミス **SD-WAN Orchestrator** 接続を有効にする] チェックボックスを選択します。
 - オンプレミス用の Citrix SD-WAN Orchestrator の IP アドレスを入力します。
 - [設定の適用] をクリックします。



2. オンプレミスの UI 用の Citrix SD-WAN Orchestrator にログインします。サイトを作成し、構成を構築します。それぞれのサイト構成内の各 Citrix SD-WAN アプライアンスのシリアル番号を入力します。構成を保存します。



3. [管理] > [証明書認証] に移動し、[認証タイプ] トグルを [オフ] にします。[はい、無効にする] をクリックして、[無効な認証の種類] ポップアップを承認します。



Network Administration: Certificate Authentication

Disabled authentication type successfully.

X

Authentication Type

On-prem Orchestrator Certificate

Certificate Details:

Certificate Fingerprint:

[REDACTED]

Start Date:July 13 05:57:34 2021 GMT

End Date:July 11 05:57:34 2031 GMT

Regenerate

Download

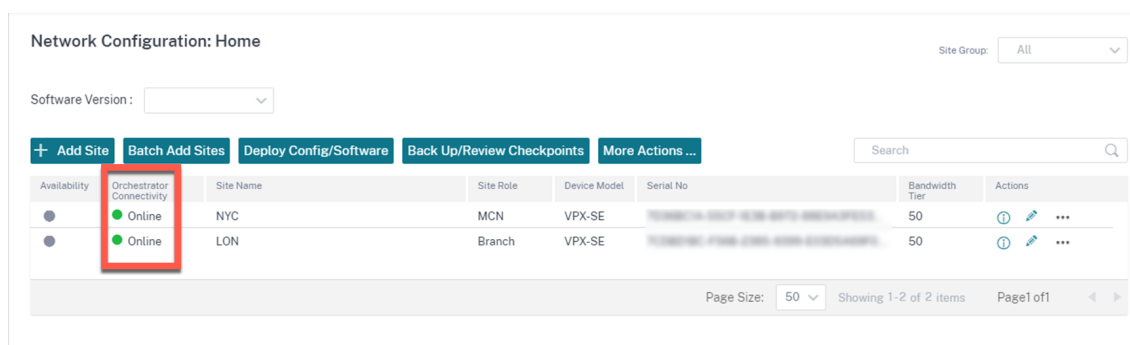
Appliance Certificate

Select an appliance ▾

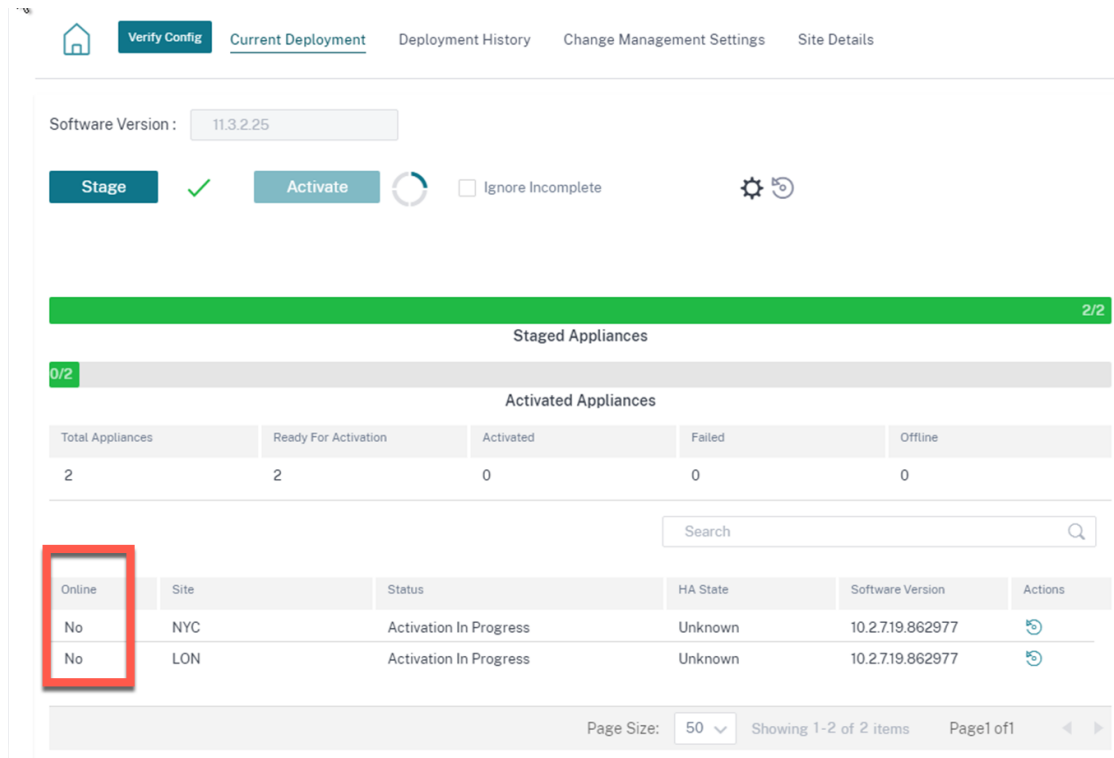
Click here to select the file or drag and drop the selected file.
Allowed file type is .pem

Upload

4. [構成]>[ネットワーク構成のホームページ] ページで、SD-WAN アプライアンスは[クラウド接続] 列に[オンライン]と表示されます。これは、オンプレミス用の Citrix SD-WAN Orchestrator および適切な IP アドレスを使用したオンプレミス接続用の Citrix SD-WAN Orchestrator or に対して有効になっている SD-WAN アプライアンスで証明書認証が無効になっているためです。デバイスがオンラインとして報告されるまで、数分かかります。



5. 公開されているソフトウェアのバージョン (11.3.0 以上) を選択し、[構成/ソフトウェアの展開] をクリックします。公開されているソフトウェアバージョンの選択の詳細については、「ソフトウェア」を参照してください。 ** サイトをステージングしてアクティブ化します **。アクティベーション後、アプライアンスの [オンライン] 列に [いいえ] と表示されます。



6. [管理] > [ZTD 設定] > [非クラウド ZTD] に移動します。[+ サイト] をクリックし、サイトを追加します。各アプライアンスの管理 IP およびログインクレデンシャルを入力します。[+] をクリックして、サイトをさらに追加します。[追加] をクリックします。

Network Administration: ZTD Settings

[Non-Cloud ZTD](#) [Cloud Brokered ZTD \(Preview\)](#)



- Non-Cloud ZTD Settings helps to configure On-prem SD-WAN Orchestrator Information on SD-WAN Appliances running 11.3.0 and above releases.
- Multiple sites can also be added by importing a .csv file with all the site details.
[Click here](#) to download a sample .csv file.

Add Sites

Site Name	Management IP	Username	Freshly Provisioned	Password	New Password	
NYC	192.168.10.200	admin	<input type="checkbox"/>	*****		—
LON	192.168.10.201	admin	<input type="checkbox"/>	*****	New password	+

Add

Cancel

7. [**Refresh**] をクリックして、構成のステータスを監視します。サイトが正常に構成されると、[構成ステータス] 列に [サイトは正常に構成されました] と表示されます。

Non-Cloud ZTD Settings			
+ Site	Import	Delete All	Refresh
Site Name	Management IP	Configuration Status	Actions
NYC	192.168.10.200	Site is configured successfully	
LON	192.168.10.201	Site is configured successfully	

Page Size: 50

Showing 1-2 of 2 items

Page 1 of 1

8. 設定 > ネットワーク設定のホームページに移動します。正常に構成されたサイトは、[オーケストレータの接続] 列に [オンライン] と表示されます。

Network Configuration: Home

Site Group: All

Software Version: 11.3.2.25

+ Add Site

Batch Add Sites

Deploy Config/Software

Back Up/Review Checkpoints

More Actions ...

Search

Availability	Orchestrator Connectivity	Site Name	Site Role	Device Model	Serial No	Bandwidth Tier	Actions
<div><div></div></div>	<div><div>Online</div></div>	NYC	MCN	VPX-SE	7D36BC1A-55CF-1E3B-B972-88E9A3FE53...	50	<div><div></div><div></div><div></div></div>
<div><div></div></div>	<div><div>Online</div></div>	LON	Branch	VPX-SE	7CDBD1BC-F56B-2385-9399-E03D5A69F0...	50	<div><div></div><div></div><div></div></div>

Page Size: 50

Showing 1-2 of 2 items

Page1 of1

Page Size: 50

Showing 1-2 of 2 items

Page 1 of 1

9. 同じプロセスに従って、サイトを追加します。上記の手順を実行しても、既存のサイト展開には影響しません。

PPPoE セッション

May 10, 2021

PPPoE (Point-to-Point Protocol over Ethernet) は、イーサネット LAN 上の複数のコンピュータユーザーを、一般的な顧客構内のアプライアンス (Citrix SD-WAN など) を介してリモートサイトに接続します。PPPoE を使用すると、ユーザーは共通のデジタル加入者線 (DSL)、ケーブルモデム、またはインターネットへのワイヤレス接続を共有できます。PPPoE は、ダイヤルアップ接続で一般的に使用される Point-to-Point Protocol (PPP; ポイントツーポイントプロトコル) と、LAN 内の複数のユーザをサポートするイーサネットプロトコルを組み合わせています。PPP プロトコル情報は、イーサネットフレーム内にカプセル化されます。

Citrix SD-WAN アプライアンスは、PPPoE を使用して、ダイヤルアップ接続とは異なり、継続的な DSL およびケーブルモデム接続をサポートするインターネットサービスプロバイダ (ISP) を提供します。PPPoE は、「検出」と呼ばれる初期交換を通じて互いのネットワークアドレスを学習するために、各ユーザーリモートサイトセッションを提供します。個々のユーザーとリモートサイト (ISP プロバイダーなど) の間にセッションが確立されると、セッションを監視できます。企業は、イーサネットと PPPoE を使用して、DSL 回線を介して共有インターネットアクセスを使用します。

Citrix SD-WAN は、PPPoE クライアントとして機能します。PPPoE サーバで認証し、ダイナミック IP アドレスを取得するか、固定 IP アドレスを使用して PPPoE 接続を確立します。

PPPoE セッションを正常に確立するには、次のことが必要です。

- 仮想ネットワークインターフェイス (VNI) を設定します。
- PPPoE セッションを作成するための一意の資格情報。
- WAN リンクを設定します。各 VNI に設定できる WAN リンクは 1 つだけです。
- 仮想 IP アドレスを設定します。各セッションは、指定された設定に基づいて、一意の IP アドレス (動的、または静的) を取得します。
- アプライアンスをブリッジモードで展開し、静的 IP アドレスで PPPoE を使用し、インターフェイスを「信頼済み」に設定します。
- スタティック IP は、サーバ提案の IP を強制的に設定することを推奨します。設定されたスタティック IP と異なる場合は、エラーが発生する可能性があります。
- アプライアンスをエッジデバイスとして展開し、ダイナミック IP で PPPoE を使用し、インターフェイスを「信頼できない」として構成します。
- サポートされている認証プロトコルは、PAP、CHAP、EAP-MD5、EAP-SRP です。
- 複数のセッションの最大数は、設定されている VNI の数によって異なります。
- インターフェイスグループごとに複数の PPPoE セッションをサポートするために、複数の VNI を作成します。

注:

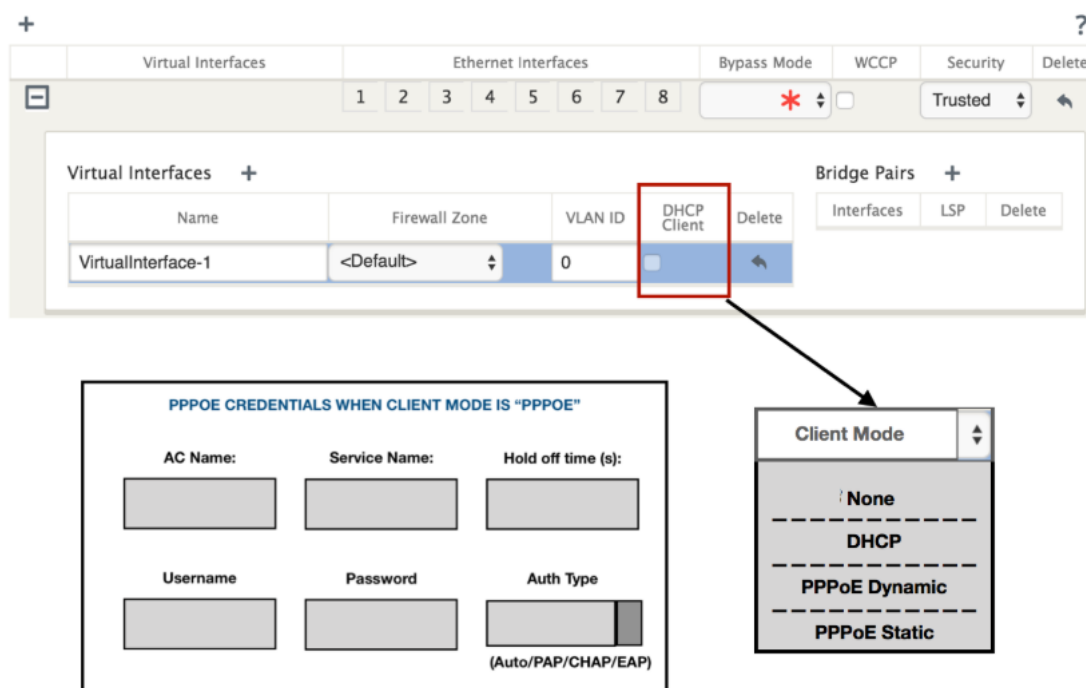
同じ 802.1Q VLAN タグを使用して複数の VNI を作成できます。

PPPoE 設定の制限事項

- 802.1q VLAN タギングはサポートされません。
- EAP-TLS 認証はサポートされていません。
- アドレス/制御圧縮
- 収縮圧縮。
- プロトコルフィールド圧縮ネゴシエーション
- 圧縮制御プロトコル。
- BSD 圧縮圧縮。
- IPv6 および IPX プロトコル。
- PPP マルチリンク。
- Van Jacobson スタイルの TCP/IP ヘッダー圧縮。
- Van Jacobson スタイルの TCP/IP ヘッダー圧縮の接続 ID 圧縮オプション。
- PPPoE は LTE インターフェイスではサポートされていません

Citrix SD-WAN 11.3.1 リリースでは、TCP の最大セグメントサイズ (MSS) を調整するために、追加 8 バイトの PPPoE ヘッダーが考慮されています。余分な 8 バイトの PPPoE ヘッダーは、MTU に基づいて同期パケットの MSS を調整します。

PPPoE の設定を容易にするため、**DHCP** クライアントオプションは、[サイト 設定] の SD-WAN Web 管理インターフェイスの [クライアントモード] という新しいオプションに置き換えられます。



次の表に、MCN アプライアンスおよびブランチ SD-WAN アプライアンスで利用できるクライアントモード PPPoE 構成オプションを示します。

MCN

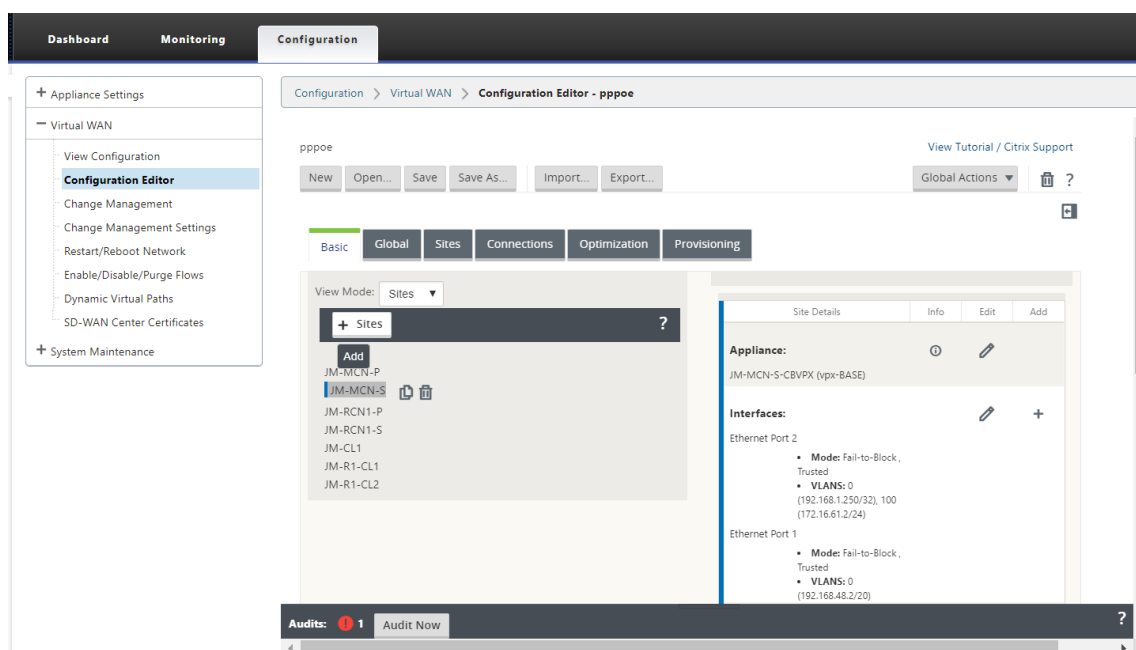
- なし
- PPPoE スタティック

ブランチ

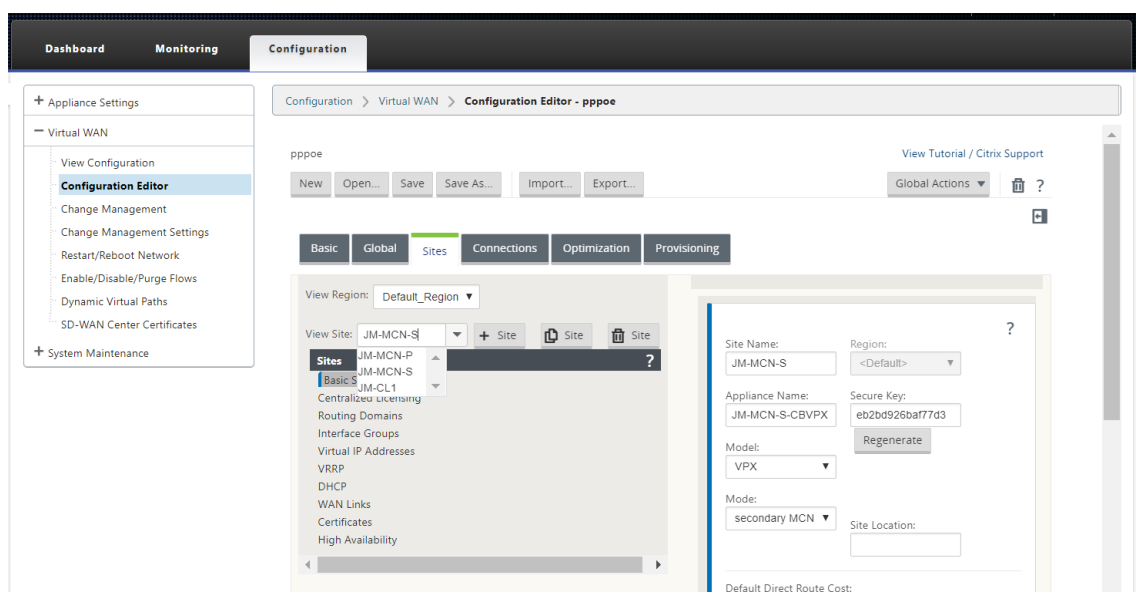
- なし
- PPPoE スタティック
- PPPoE ダイナミック
- DHCP

MCN アプライアンスの構成

1. SD-WAN MCN アプライアンス GUI で、[構成]>[仮想 **WAN**]>[構成エディタ]に移動します。[基本] タブの下にサイトを追加します。詳細については、[MCN の設定](#)のブランチノード構成を参照してください。



2. 新しいサイトが作成されたら、[サイト] タブを開きます。[サイトの表示] ドロップダウンリストから、新しく作成したサイトを選択します。

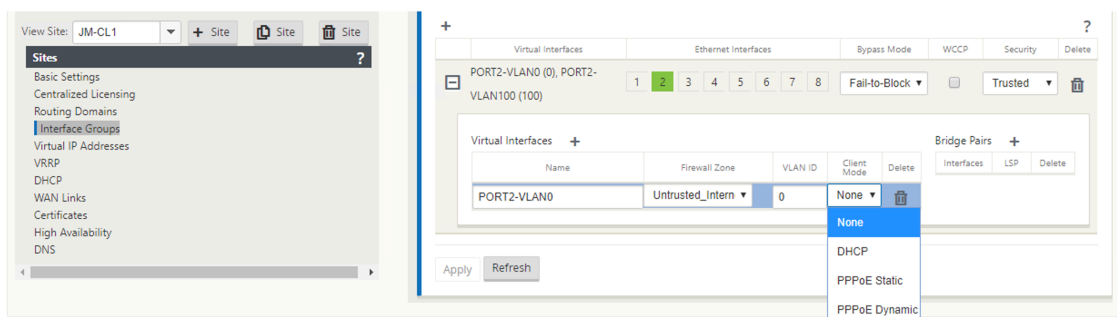


3. MCN サイトの [インターフェイスグループ] を選択します。以下を実行します：

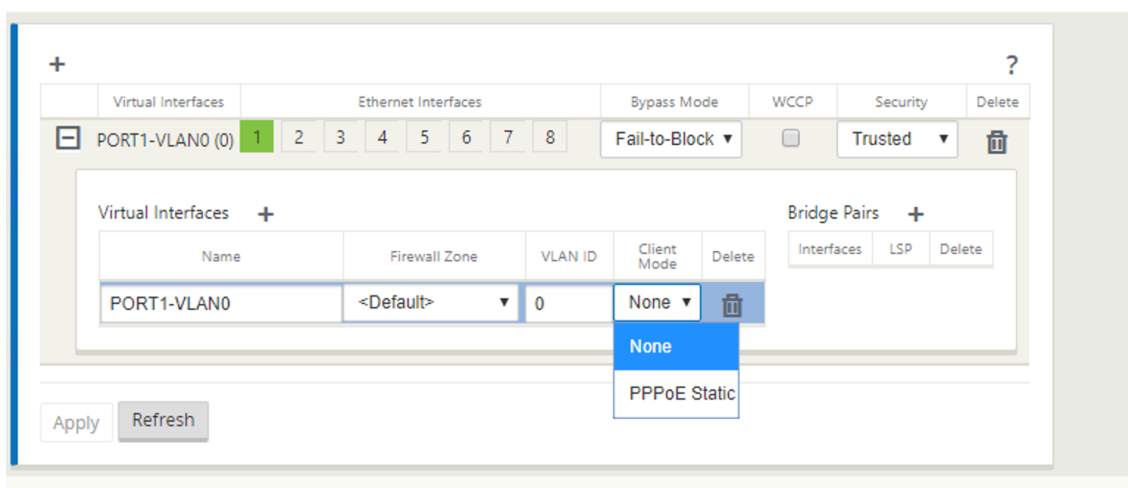
- 仮想インターフェイスの追加
- イーサネットインターフェイスを設定します。
- バイパスモードを設定します。
- 必要に応じて、**WCCP** を選択します。
- [セキュリティ]-[信頼済み/信頼されていない] を選択します。

仮想インターフェイスの場合：

- 名前、ファイアウォールゾーン、VLAN ID、およびクライアントモードを設定します。
- 複数のインターフェイスが設定された VNI では、PPPoE 接続に使用できるインターフェイスは 1 つだけです。
- 複数のインターフェイスが設定された VNI で PPPoE 接続が異なるインターフェイスに変更された場合、モニターページを使用して既存のセッションを停止し、新しいセッションを開始すると、新しいインターフェイスで新しいセッションを確立できます。



4. MCN アプライアンスの [クライアントモード] オプションのネットワーク構成要件に基づいて、[PPPoE 静的] または [なし] を選択します。さらに次のオプションが表示されます。



次の PPPoE パラメータを設定し、[**Apply**] をクリックします。

- [コンセントレータ (AC) 名] フィールドにアクセスします。
- サービス名。
- ホールドオフ再接続時間（デフォルトはただちに再接続されます。' 0' ）
- 認証タイプ-(AUTO/PAP/CHAP/EAP)。
 - Auth オプションが Auto に設定されている場合、SD-WAN アプライアンスは、サーバーから受信したサポートされている認証プロトコル要求を受け入れます。
 - Auth オプションが PAP/CHAP/EAP に設定されている場合、特定の認証プロトコルだけが適用されます。PAP が設定内にあり、サーバが CHAP を使用して認証要求を送信した場合、接続要求は拒否されます。サーバが PAP とネゴシエートしない場合、認証エラーが発生します。
- CHAP には、CHAP、Microsoft CHAP、および Microsoft CHAPv2 が含まれます。
- EAP は EAP-MD5 をサポートします。
- ユーザ名とパスワード。

次の図は、ブランチ SD-WAN アプライアンスの PPPoE クライアントモードオプションを示しています。[PPPoE ダイナミック] が選択されている場合、VNI は「信頼できない」である必要があります。

WAN リンクの設定

1. SD-WAN GUI で、[サイト] > [WAN リンク] に移動します。PPPoE スタティック VNI またはダイナミック VNI ごとに、WAN リンクの作成は 1 つだけ許可されます。WAN リンクの設定は、クライアントモードの VNI の選択によって異なります。
2. VNI に PPPoE ダイナミッククライアントモードが設定されている場合は、次の手順を実行します。
 - IP アドレスフィールドとゲートウェイ IP アドレスフィールドは非アクティブになります。

- 仮想パスモードが「プライマリ」に設定されています。
- プロキシ ARP は設定できません。

デフォルトでは、[ゲートウェイ MAC アドレスバインディング] が選択されています。

Name	Virtual Interface	IP Address	Gateway IP Address	Virtual Path Mode	Proxy ARP	Gateway MAC Address Binding	Delete
RL-MCN-S-WL-1...	PORT2-VLAN0			Primary	<input type="checkbox"/>	<input checked="" type="checkbox"/>	

3. VNI に PPPoE スタティッククライアントモードが設定されている場合は、IP アドレスを設定します。

Name	Virtual Interface	IP Address	Gateway IP Address	Virtual Path Mode	Proxy ARP	Gateway MAC Address Binding	Delete
RL-MCN-S-WL-1...	PORT2-VLAN0	192.168.1.250		Primary	<input type="checkbox"/>	<input checked="" type="checkbox"/>	

注:

サーバが設定された静的 IP アドレスを尊重せず、別の IP アドレスを提供すると、エラーが発生します。PPPoE セッションは、サーバーが設定された IP アドレスを受け入れるまで、定期的に接続の再確立を試みます。

PPPoE セッションの監視

PPPoE セッションを監視するには、SD-WAN GUI の [モニタリング] > [PPPoE] ページに移動します。

PPPoE ページには、PPPoE スタティッククライアントモードまたはダイナミッククライアントモードが設定された VNI のステータス情報が表示されます。トラブルシューティングの目的で、手動でセッションを開始または停止できます。

- VNI が起動して準備ができている場合は、**IP** カラムと **Gateway IP** カラムにセッションの現在の値が表示されます。これは、最近受信した値であることを示します。
- VNI が停止しているか、障害状態の場合、値は最後に受信された値です。

- [Gateway IP] 列の上にマウスを置くと、セッションと IP の受信元の PPPoE アクセスコンセントレータの MAC アドレスが表示されます。
- 「状態」の値の上にマウスを置くとメッセージが表示され、「失敗」状態の方が便利です。

Dashboard

Monitoring

Configuration

Statistics

Flows

Routing Protocols

Firewall

IKE/IPsec

IGMP

Performance Reports

Qos Reports

Usage Reports

Availability Reports

Appliance Reports

DHCP Server/Relay

VRRP

PPPoE

Monitoring > PPPoE

PPPoE Monitoring

Virtual Interface	IP Address	Gateway IP	Session ID	State	Action
PORT2-VLAN0	192.168.1.22	192.168.1.254	18	Ready	Stop
abcd	0.0.0.0	0.0.0.0	0	Failed	Start
newVif	0.0.0.0	0.0.0.0	0	Stopped	Start

[State] 列には、緑、赤、黄、および値の 3 つのカラーコードを使用して PPPoE セッションのステータスが表示されます。次の表では、状態と説明について説明します。ステートの上にマウスポインタを置くと、説明が表示されます。

PPPoE セッションタイプ	色	説明
構成済み	黄	VNI には PPPoE が設定されています。これは初期状態です。
ダイヤル中	黄	VNI が設定されると、PPPoE ディスカバリーを開始して PPPoE セッション状態がダイヤル状態に移行します。パケット情報がキャプチャされます。
セッション	黄	VNI は、ディスカバリー状態からセッション状態に移行されます。動的な場合は IP の受信を待機するか、静的な場合は、アドバタイズされた IP のサーバからの確認応答を待機します。
準備完了	緑	IP パケットが受信され、VNI および関連する WAN リンクが使用可能になります。
失敗	赤	PPP/PPPoE セッションが終了しました。失敗の原因は、無効な構成または致命的なエラーが原因である可能性があります。セッションは 30 秒後に再接続を試みます。

PPPoE セッションタイプ	色	説明
停止しました	黄色	PPP/PPPoE セッションは手動で停止されます。
終了中	黄色	理由により終了する中間状態。この状態は、一定時間（通常のエラーの場合は 5 秒、致命的なエラーの場合は 30 秒）後に自動的に開始されます。
無効	黄色	SD-WAN サービスは無効です。

PPPoE セッション障害のトラブルシューティング

[Monitoring] ページで、PPPoE セッションの確立に問題がある場合、次の手順を実行します。

- [失敗] ステータスの上にマウスを置くと、最近の失敗の理由が表示されます。
- 新しいセッションを確立したり、アクティブな PPPoE セッションのトラブルシューティングを行うには、[監視] → [PPPoE] ページを使用してセッションを再起動します。
- PPPoE セッションを手動で停止した場合、手動で開始して構成の変更がアクティブになるか、サービスが再起動されるまで、PPPoE セッションを開始できません。

PPPoE セッションは、次の理由により失敗することがあります。

- 設定内のユーザ名/パスワードが正しくないために SD-WAN がピアに対して自身を認証できない場合
- PPP ネゴシエーションが失敗します。ネゴシエーションは、少なくとも 1 つのネットワークプロトコルが実行されているポイントに到達しません。
- システムメモリまたはシステムリソースの問題。
- 構成が無効または不正です（AC 名またはサービス名が間違っています）。
- オペレーティングシステムエラーのため、シリアルポートを開けませんでした。
- エコーパケットに対する応答が受信されない（リンクが不良であるか、サーバが応答していない）。
- 1 分以内に、が連続的に失敗したダイヤルセッションがいくつか発生しました。

10 回連続して失敗した後、失敗の理由が観察されます。

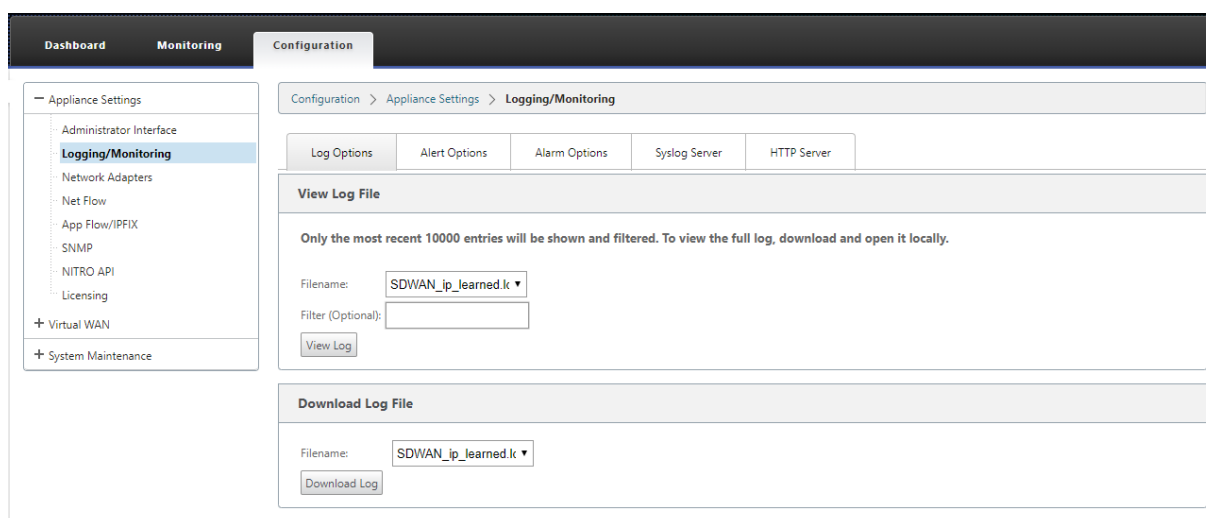
- 障害が正常であれば、すぐに再起動します。
- 失敗がエラーの場合、再起動は 10 秒間戻ります。
- 失敗が致命的である場合、再起動は 30 秒間戻ってから再起動します。

LCP Echo 要求パケットは、SD-WAN から 60 秒ごとに生成され、5 つのエコー応答を受信できなかった場合はリンク障害と見なされ、セッションが再確立されます。

PPPoE ログファイル

SDWAN_IP_learned.log ファイルには、PPPoE に関連するログが含まれています。

SD-WAN GUI から *SDWAN_IP_learned.log* ファイルを表示またはダウンロードするには、アプライアンスの設定 > ログ/監視 > ログオプションに移動します。*SDWAN_IP_learned.log* ファイルを表示またはダウンロードします。



サービス品質

November 17, 2022

オフィスの場所とデータセンターまたはクラウド間のネットワークでは、高品質のビデオやリアルタイムの音声など、多数のアプリケーションやデータを転送する必要があります。帯域幅に敏感なアプリケーションは、ネットワークの機能とリソースを拡張します。Citrix SD-WAN は、保証された、安全で、測定可能な、予測可能なネットワークサービスを提供します。これは、ネットワーク上の遅延、ジッタ、帯域幅、およびパケット損失を管理することによって実現されます。

Citrix SD-WAN ソリューションには、高度なアプリケーション QoS（サービス品質）エンジンが含まれており、アプリケーショントラフィックにアクセスし、重要なアプリケーションに優先順位を付けます。また、WAN ネットワーク品質の要件を理解し、品質特性に基づいてネットワークパスをリアルタイムで選択します。

次の項のトピックでは、QoS クラス、IP ルール、アプリケーション QoS ルール、およびアプリケーション QoS を定義するために必要なその他のコンポーネントについて説明します。

クラス

November 8, 2021

Citrix SD-WAN 構成では、仮想パスを通過するすべてのトラフィックに適用されるアプリケーションおよび IP/ポートベースの QoS ポリシーのデフォルトセットが提供されます。これらの設定は、展開のニーズに合わせてカスタマイズできます。

クラスは、トラフィックの優先順位付けに役立ちます。アプリケーションおよび IP/ポートベースの QoS ポリシーは、トラフィックを分類し、設定で指定された適切なクラスに配置します。

アプリケーションの QoS と IP アドレス/ポートベースの QoS の詳細については、[アプリケーション名別のルール](#)、[IP アドレスとポート番号によるルールをそれぞれ参照してください](#)。

SD-WAN は 17 のクラス (ID: 0 ~16) を提供します。以下は、すべての 17 クラスのデフォルト設定です。

Virtual Path Default Set: New_Default_Set-1 Section: Classes + Add Default Set Delete Default Set

ID	Name	Type	Initial				Sustained		Reset
			Period	Rate	%/Kbps	Share %	Rate	Share %	
0	HDX_priority_tag_0	Realtime	0	30	%	0	30	0	
1	HDX_priority_tag_1	Interactive	0	0	%	20	0	20	
2	HDX_priority_tag_2	Interactive	0	0	%	6	0	6	
3	HDX_priority_tag_3	Interactive	0	0	%	2	0	2	
4	class_4	Bulk		0	%	0	0	0	
5	class_5	Bulk		0	%	0	0	0	
6	class_6	Bulk		0	%	0	0	0	
7	class_7	Bulk		0	%	0	0	0	
8	class_8	Bulk		0	%	0	0	0	
9	class_9	Bulk		0	%	0	0	0	
10	realtime_class	Realtime	0	30	%	0	30	0	
11	interactive_high_class	Interactive	0	0	%	20	0	20	
12	interactive_medium_class	Interactive	0	0	%	13	0	13	
13	interactive_low_class	Interactive	0	0	%	6	0	6	
14	interactive_very_low_class	Interactive	0	0	%	3	0	3	
15	bulk_background_class	Bulk		0	%	0	0	100	
16	bulk_unused_class	Bulk		0	%	0	0	0	

Apply Revert

以下は、クラスの異なるタイプです。

- **リアルタイム:** 低遅延、低帯域幅、時間依存型のトラフィックに使用されます。リアルタイムアプリケーションは時間に依存しますが、実際には高帯域幅 (Voice over IP など) を必要としません。リアルタイムアプリケーションは、レイテンシーとジッタの影響を受けますが、ある程度の損失を許容できます。
- **Interactive:** 低～中レイテンシーおよび低～中帯域幅要件の対話型トラフィックに使用されます。通常、対

話はクライアントとサーバーの間で行われます。通信は、高帯域幅を必要としない場合がありますが、損失や遅延に敏感です。

- **バルク:** 高帯域幅トラフィックおよび高遅延に耐えるアプリケーションに使用されます。ファイル転送を処理し、高帯域幅を必要とするアプリケーションは、バルククラスに分類されます。これらのアプリケーションは、人間の干渉をほとんど伴わず、ほとんどシステム自体によって処理されます。

クラス間の帯域幅共有

帯域幅は、クラス間で次のように共有されます。

- **リアルタイム:** リアルタイムクラスにヒットするトラフィックは低遅延であることが保証され、競合するトラフィックが存在する場合、帯域幅はクラスシェアまで制限されます。
- **インタラクティブ:** 対話型クラスに当たるトラフィックは、リアルタイムトラフィックを提供した後、残りの帯域幅を取得し、利用可能な帯域幅は、対話型クラス間で公平に共有されます。
- **バルク:** バルクがベストエフォートです。リアルタイムトラフィックおよびインタラクティブトラフィックを提供した後に残された帯域幅は、公平な共有ベースでバルククラスに与えられます。リアルタイムトラフィックおよびインタラクティブトラフィックが使用可能な帯域幅をすべて利用すると、バルクトラフィックが枯渇する可能性があります。

注:

競合がない場合、すべてのクラスが使用可能な帯域幅を使用できます。

次に、クラス設定に基づく帯域幅分散の例を示します。

仮想パス上に 10 Mbps の集約帯域幅があるとします。クラス設定が

- リアルタイム:30%
- インタラクティブハイ:40%
- インタラクティブ媒体:20%
- インタラクティブロー:10%
- バルク:100%。

帯域幅分布の結果は

- リアルタイムトラフィックは、必要に応じて 10Mbps (3 Mbps) の 30% を取得します。10% 未満で済む場合は、残りの帯域幅が他のクラスで使用可能になります。
- 対話型クラスは、残りの帯域幅をフェアシェアベース (4 Mbps: 2 Mbps: 1 Mbps) で共有します。
- リアルタイムのインタラクティブトラフィックが共有を完全に使用していないときに残ったものは、Bulk クラスに与えられます。

クラスをカスタマイズするには、次の手順に従います。

1. 仮想パスのデフォルトセットが使用されている場合は、[グローバル] > [仮想パスのデフォルトセット] でクラスを変更できます。

注:

仮想パスレベル (接続-> 仮想パス-> クラス) でクラスを変更することもできます

2. 「デフォルトセットを追加」をクリックし、デフォルトセットの名前を入力して、「追加」をクリックします。[セクション] フィールドで、[クラス] を選択します。
3. [Name] フィールドで、デフォルト名をそのまま使用するか、任意の名前を入力します。
4. [タイプ] フィールドで、クラスタイプ ([リアルタイム]、[インタラクティブ]、[バルク]) を選択します。
5. リアルタイムクラスの場合、次の属性を指定できます。
 - 初期期間: 持続レートに切り替える前に初期レートを適用する期間 (ミリ秒単位)。
 - 初期レート: 初期期間中にパケットがキューから出る最大レートまたはパーセンテージ。
 - 持続レート: 最初の期間後にパケットがキューから出る最大レートまたはパーセンテージ。
6. 対話型クラスの場合、次の属性を指定できます。
 - [InitialPeriod]: 持続パーセンテージに切り替える前に、使用可能な帯域幅の初期パーセンテージを適用する期間 (ミリ秒単位)。通常、20 ミリ秒
 - 初期共有%: 初期期間中にリアルタイムにサービスを提供した後に残っている仮想パス帯域幅の最大シェアです。
 - 持続共有%: 初期期間の後にリアルタイムトラフィックを処理した後に残っている仮想パス帯域幅の最大シェアです。
7. バルククラスの場合は、リアルタイムおよび対話型トラフィックを処理した後にバルククラスに使用される残りの仮想パス帯域幅を決定する持続共有% だけを指定できます。
8. [Apply] をクリックします。

注:

構成を保存し、変更管理の受信トレイにエクスポートし、変更管理プロセスを開始します。

IP アドレスとポート番号による規則

May 10, 2021

IP アドレスとポート番号によるルール機能を使用すると、ネットワークのルールを作成し、ルールに基づいてサービス品質 (QoS) を決定するのに役立ちます。ネットワーク用のカスタムルールを作成できます。たとえば、次のルー

ルを作成できます。—送信元 IP アドレスが 172.186.30.74、宛先 IP アドレスが 172.186.10.89 の場合は、送信モードを「永続パス、**LAN** を **WAN** クラスに 10 (realtime_class)」に設定します。

構成エディタを使用して、トラフィックフローのルールを作成し、そのルールをアプリケーションとクラスに関連付けることができます。フローのトラフィックをフィルタリングするための基準を指定し、一般的な動作、LAN から WAN への動作、WAN から LAN への動作、およびパケットインスペクション規則を適用できます。

ルールは、サイトレベルまたはグローバルレベルでローカルに作成できます。複数のサイトで同じルールが必要な場合は、[グローバル] > [仮想パスのデフォルトセット] > [ルール] で、ルールのテンプレートをグローバルに作成できます。このテンプレートは、ルールの適用が必要なサイトに添付できます。サイトがグローバルに作成されたルールテンプレートに関連付けられている場合でも、サイト固有のルールを作成できます。このような場合、サイト固有のルールが優先され、グローバルに作成されたルールテンプレートが上書きされます。

IP アドレスとポート番号によるルールの作成

1. SD-WAN 設定エディタで、[グローバル] > [仮想パスデフォルトセット] に移動します。

注:

サイトレベルでルールを作成するには、[サイト] > [接続] > [仮想パス] > [ルール] に移動します。

2. 「デフォルトセットを追加」をクリックし、デフォルトセットの名前を入力して、「追加」をクリックします。「セクション」フィールドで「ルール」を選択し、「+」をクリックします。
3. [順序] フィールドに、他の規則に関連して規則が適用されるタイミングを定義する順序値を入力します。
4. [ルールグループ名] フィールドで、ルールグループを選択します。同じルールグループを持つルールの統計情報はグループ化され、まとめて表示できます。

ルールグループを表示するには、[モニタリング] > [統計] に移動し、[表示] フィールドで [ルールグループ] を選択します。

カスタムアプリケーションを追加することもできます。詳しくは、「[ルールグループを追加して MOS を有効にする](#)」を参照してください。

5. [Routing Domain] フィールドで、設定済みのルーティングドメインの 1 つを選択します。
6. ルール一致基準を定義して、次のようにリストされたパラメータに基づいてサービスをフィルタリングできます。フィルタリングの後、ルール設定は、これらの基準に一致するサービスに適用されます。

- 送信元 IP アドレス: トラフィックと照合する送信元 IP アドレスおよびサブネットマスク。
- 宛先 IP アドレス: トラフィックと照合する宛先 IP アドレスおよびサブネットマスク。

注

[**Dest=Src**] チェックボックスが選択されている場合、送信元 IP アドレスは宛先 IP アドレスにも使用されます。

- プロトコル: トラフィックと照合するプロトコル。
- [Source Port]: トラフィックと照合する送信元ポート番号またはポート範囲。
- 宛先ポート: トラフィックと照合する宛先ポート番号またはポート範囲。

注

[**Dest=Src**] チェックボックスが選択されている場合、送信元ポートは宛先ポートにも使用されます。

- **DSCP**: トラフィックと照合する IP ヘッダー内の **DSCP** タグ。
- **VLAN**: トラフィックと照合する **VLAN ID** 。

7. 新しいルールの横にある追加 (+) アイコンをクリックします。
8. [プロトコルを使用してプロパティを初期化] をクリックして、ルールのデフォルトとプロトコルの推奨設定を適用して、ルールのプロパティを初期化します。これにより、デフォルトのルール設定が入力されます。次の手順に示すように、設定を手動でカスタマイズすることもできます。
9. [**WAN 全般**] タイルをクリックして、次のプロパティを構成します。
 - 送信モード: 次のいずれかの送信モードを選択します。
 - ロードバランスパス: フローのトラフィックは、サービスの複数のパス間で分散されます。トラフィックは、そのパスが使用されるまで、最適パスを介して送信されます。残りのパケットは、次の最適パスを介して送信されます。
 - 永続パス: フローのトラフィックは、パスが使用できなくなるまで、同じパス上に残ります。
 - 重複パス: フローのトラフィックが複数のパス間で重複するため、信頼性が向上します。
 - オーバーライドサービス: フローのトラフィックは、別のサービスにオーバーライドされます。[オーバーライドサービス] フィールドで、サービスがオーバーライドするサービスタイプを選択します。たとえば、仮想パスサービスは、イントラネット、インターネット、またはパススルーサービスに上書きできます。
 - 失われたパケットの再送信: このルールに一致するトラフィックを、信頼できるサービス経路でリモートアプライアンスに送信し、失われたパケットを再送信します。
 - **TCP** 終端を有効にする: このフローのトラフィックの TCP 終端を有効にします。パケットの確認応答のラウンドトリップ時間が短縮されるため、スループットが向上します。
 - 優先 **WAN** リンク: フローが最初に使用する WAN リンク。
 - 永続インピーダンス: トラフィックが同じパス内に留まる最小時間 (ミリ秒単位)。パスが設定値よりも長い待機時間になります。

- **IP、TCP、および UDP** を有効にする: IP、TCP、および UDP パケットのヘッダーを圧縮します。

注:

IPv6 パケットはヘッダー圧縮をサポートしていません。

- **GRE** を有効にする: **GRE** パケットのヘッダーを圧縮します。
- パケット集約を有効にする: 小さなパケットを大きなパケットに集約します。
- パフォーマンスの追跡: このルールのパフォーマンス属性をセッションデータベースに記録します (損失、ジッタ、遅延、帯域幅など)。

10. [**LAN to WAN**] タイルをクリックして、このルールの LAN から WAN への動作を構成します。

- クラス: このルールに関連付けるクラスを選択します。

注

ルールを適用する前にクラスをカスタマイズすることもできます。詳細については、「[クラスをカスタマイズする方法](#)」を参照してください。

- **Large Packet Size**: このサイズ以下のパケットには、[**Class**] フィールドの右側にあるフィールドで指定された [**Drop **Limit**] および [**Drop Depth****] の値が割り当てられます。

このサイズより大きいパケットには、画面の [Large Packets] セクションのデフォルトの [**Drop Limit**] フィールドおよび [**Drop Depth**] フィールドで指定された値が割り当てられます。

- [**Drop Limit**]: クラススケジューラで待機しているパケットがドロップされるまでの時間。バルククラスには適用されません。
- ドロップ深度: パケットがドロップされるキュー深度のしきい値。
- **RED** を有効にする: Random Early Detection (RED; ランダム早期検出) は、輻輳が発生したときにパケットを廃棄することにより、クラスリソースの公平な共有を保証します。
- [**Resassign Size**]: パケット長を超えると、[Reassign Class] フィールドで指定したクラスにパケットが再割り当てされます。
- [**ReassignClass**]: パケット長が [Reassign Size] フィールドで指定したパケット長を超えた場合に使用されるクラス。
- **Disable Limit**: 重複パケットが帯域幅を消費するのを防ぐために重複を無効にできる時間。
- **Disable Depth**: クラススケジューラのキューの深さ。この時点で、重複パケットは生成されません。
- **TCP** スタンドアロン **ACK** クラス: 大きなファイル転送中に TCP スタンドアロン確認がマッピングされる優先度の高いクラス。

LAN to WAN

General

Class: 3 (citrix_class_3) Drop Limit (ms): 60

Large Packet Size (bytes): 0 ☒ Enable RED

Large Packets

Drop Limit (ms): 50 Drop Depth (bytes): 128000

Duplicate Packets

Disable Limit (ms): 0 Disable Depth (bytes): 128000

Reassign

Reassign Class: 1 (citrix_class_1) Drop Limit (ms): 50

Reassign Size (bytes): 2000 Large Packet Size (bytes): 0 ☒ Enable RED

Large Packets

Drop Limit (ms): 1 Drop Depth (bytes): 0

Duplicate Packets

Disable Limit (ms): 0 Disable Depth (bytes): 128000

TCP Standalone ACK

TCP Standalone ACK Class: Disabled <Default> Drop Limit (ms): 50

Large Packet Size (bytes): 0 ☒ Enable RED

Large Packets

Drop Limit (ms): 0 Drop Depth (bytes): 0

11. [**WAN to LAN**] タイルをクリックして、このルール WAN から LAN への動作を構成します。

- パケットの再シーケンシングを有効にする：宛先で正しい順序でパケットを順序付けします。
- [**Hold Time**]: パケットが再シーケンス処理のために保持され、その後パケットが LAN に送信される時間間隔。
- 遅延再シーケンス処理パケットの破棄：再シーケンス処理に必要なパケットが LAN に送信された後に到着した順不同パケットを廃棄します。
- **DSCP** タグ：LAN に送信する前に、このルールに一致するパケットに適用される DSCP タグ。

WAN to LAN

Packet Resequencing

☒ Enable Packet Resequencing Hold Time (ms):

☒ Discard Late Resequencing Packets

DSCP Tag: af12

12. [ディープパケットインスペクション] タイルをクリックし、[パッシブ **FTP** 検出を有効にする] を選択して、FTP データ転送に使用されるポートをルールが検出し、検出されたポートにルール設定を自動的に適用できるようにします。

13. [適用] をクリックします。

注

設定を保存し、変更管理の受信トレイにエクスポートして、変更管理プロセスを開始します。

規則の確認

構成エディタで、[監視]>[フロー]に移動します。「フロー」ページの上部にある**「フローの選択」セクションにある「フロータイプ**」フィールドを選択します。[Flow Type] フィールドの横には、表示するフロー情報を選択するためのチェックボックスが並んでいます。フロー情報が設定された規則に従っているかどうかを確認します。

例：
「送信元 IP アドレスが 172.186.30.74、宛先 IP アドレスが 172.186.10.89 の場合、送信モードを永続パスに設定する」というルールには、次のフローデータが表示されます。

Select Flows

Flow Type: ☒ LAN to WAN ☒ WAN to LAN ☐ Internet Load Balancing Table ☐ TCP Termination Table

Max Rows to Display (Per Flow Type): 50

Filter (Optional): Help

Refresh

Flows Data

Both LAN to WAN and WAN to LAN Flows

Details	Source IP Address	Dest IP Address	Direction	Source Port	Dest Port	IP	IP DSCP	HT Count	Service	Service Name	LAN GW IP	Age (ms)	Packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	App Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type	Application
<input checked="" type="checkbox"/>	172.186.30.74	172.186.10.89	LAN to WAN	55502	5003	TCP	default	88311	Virtual Path	DC-Client-1	LOCAL	0	88251	126639068	7558.028	86763.328	3446.461	0.000	1	N/A	9	BULK	DC-WL-1->Client-1-WL-1	N/A	Persistent	iperf
<input checked="" type="checkbox"/>	172.186.10.89	172.186.30.74	WAN to LAN	5003	55502	TCP	default	45207	Virtual Path	DC-Client-1	LOCAL	1	45207	2385488	3871.687	1634.405	1765.480	0.000	69	N/A	N/A	N/A	N/A	N/A	Persistent	iperf

Total LAN to WAN flows displayed: 1 out of 1
Total WAN to LAN flows displayed: 1 out of 1

構成エディタで、[監視]>[統計]に移動し、構成済みのルールを確認します。

Statistics

Flows

Routing Protocols

Firewall

IKE/IPsec

IGMP

Performance Reports

Qos Reports

Usage Reports

Availability Reports

Appliance Reports

DHCP Server/Relay

VRRP

PPPoE

DNS

Monitoring > Statistics

Statistics

Show: Rules ☒ Enable Auto Refresh 5 seconds Stop

Rule Statistics

Filter: in Any column Apply

Show 100 entries Showing 1 to 100 of 275 entries

Num#	Site	Service	IP Address		IP Proto	Port		VLAN ID	IP DSCP	LAN to WAN		WAN to LAN						
			Src	Dst		Src	Dst			Bytes	Packets	Bytes	Packets	Jitter (ms)	Packets Lost	Avg Latency (ms)	Min Latency (ms)	Max Latency (ms)
0	DC	DC-Client-1	*	*	TCP	5003	*	*	*	0	0	0	0					
1	DC	DC-Client-1	*	*	TCP	*	5003	*	*	426121168	285604	0	0					
2	DC	DC-Client-1	*	*	TCP	5060-5061	*	*	ef	0	0	0	0					
3	DC	DC-Client-1	*	*	TCP	*	5060-5061	*	ef	0	0	0	0					
4	DC	DC-Client-1	*	*	UDP	5060-5061	*	*	ef	0	0	0	0					
5	DC	DC-Client-1	*	*	UDP	*	5060-5061	*	ef	0	0	0	0					

アプリケーション名による規則

May 10, 2021

アプリケーション分類機能を使用すると、Citrix SD-WAN アプライアンスは着信トラフィックを解析し、特定のアプリケーションまたはアプリケーションファミリに属するものとして分類できます。この分類により、アプリケーションルールを作成して適用することにより、個々のアプリケーションファミリまたはアプリケーションファミリの QoS を強化できます。

アプリケーション、アプリケーションファミリ、またはアプリケーションオブジェクトマッチタイプに基づいてトラフィックフローをフィルタリングし、アプリケーションルールを適用できます。アプリケーションルールは、インターネットプロトコル (IP) ルールに似ています。IP 規則の詳細については、規則「[IP アドレスとポート番号による](#)」を参照してください。

すべてのアプリケーションルールに対して、転送モードを指定できます。使用可能な送信モードを次に示します。

- **ロードバランスポス**: フローのアプリケーショントラフィックは、複数のパス間で分散されます。トラフィックは、そのパスが使用されるまで、最適パスを介して送信されます。残りのパケットは、次の最適パスを介して送信されます。
- **永続パス**: アプリケーショントラフィックは、パスが使用できなくなるまで同じパス上に残ります。
- **重複パス**: アプリケーショントラフィックは複数のパス間で重複するため、信頼性が向上します。

アプリケーションルールはクラスに関連付けられています。クラスの詳細については、[クラスのカスタマイズ](#)を参照してください。

デフォルトでは、以下の 5 つの事前定義されたアプリケーションルールが Citrix ICA アプリケーションで使用できます。

規則	クラス	モード	送信されたパケットの再送信	パケットの集約の有効にする	パケットの再送信の有効化	リシークの保持時間 (ミリ秒)	レイテンシーの破棄	ドロップ制限 (ミリ秒)	ドロップ深度 (バイト)	RED を有効にする	無効の限界 (ミリ秒)	深度の無効化 (バイト)
HDX_Priority_0 (HDX_priority_tag_0)	負荷分散	パス	True	False	True	250	True	350	30000	True	0	128000
HDX_Priority_1 (HDX_priority_tag_1)	負荷分散	パス	True	False	True	250	True	350	30000	True	0	128000

			失われたパケット	パケット集約	再シーク	リシーク	レイトリ	ドロップ	ドロップ	RED	無効	深度の無効化
規則	クラス	モード	送信の再送信	有効にする	有効化	間 (ミリ秒)	ケットの破棄	制限 (ミリ秒)	深度 (バイト)	を有効にする	限界 (ミリ秒)	(バイト)
HDX_Priority_2	11	分散パス	True	False	True	250	True	350	30000	True	0	128000
(HDX_priority_tag_2)												
HDX_Priority_3	11	分散パス	True	False	True	250	True	350	30000	True	0	128000
(HDX_priority_tag_3)												
HDX	11	分散パス	True	False	True	250	True	350	30000	True	0	128000
(inter-active_high_class)												

アプリケーションルールの適用方法

SD-WAN ネットワークでは、着信パケットが SD-WAN アプライアンスに到達すると、最初の少数のパケットが DPI 分類を受けません。この時点で、クラス、TCP 終端などの IP 規則属性がパケットに適用されます。DPI 分類後、Class、transmit モードなどのアプリケーションルールの属性は、IP ルールの属性を上書きします。

IP ルールは、アプリケーションルールと比較して、属性のより多くの数を持っています。アプリケーションルールはいくつかの IP ルール属性だけを上書きし、残りの IP ルール属性はパケットで処理されたままになります。

たとえば、SMTP プロトコルを使用する Google Mail などのウェブメールアプリケーションのアプリケーションルールを指定したとします。SMTP プロトコルの IP ルールセットは、最初に DPI 分類の前に適用されます。パケットを解析し、Google Mail アプリケーションに属するものとして分類した後、Google Mail アプリケーション用に指定されたアプリケーションルールが適用されます。

アプリケーションルールの作成

アプリケーション・ルールを作成する手順は、次のとおりです。

1. SD-WAN 設定エディタで、[グローバル] > [仮想パステフォルトセット] に移動します。

2. 「デフォルトセットを追加」をクリックし、デフォルトセットの名前を入力して、「追加」をクリックします。[セクション] フィールドで [アプリケーション QoS] を選択し、[+] をクリックします。

注

[接続] > [仮想パス] > [アプリケーション QoS] または [** グローバル] > [動的仮想パスの ** デフォルトセット] > [アプリケーション QoS] の順に選択して、アプリケーションルールを作成することもできます。

3. [順序] フィールドに、他の規則に関連して規則が適用されるタイミングを定義する順序値を入力します。

4. [**Match Type**] フィールドで、次のいずれかのマッチタイプを選択します。

- [アプリケーション] —この一致タイプを選択した場合は、このフィルタの一致基準として使用するアプリケーションを指定します。
- 「アプリケーションファミリ」 —この一致タイプを選択した場合は、このフィルタの一致基準として使用するアプリケーションファミリを選択します。
- 「アプリケーション・オブジェクト」 —この一致タイプを選択した場合は、このフィルタの一致基準として使用するアプリケーション・オブジェクトを選択します。

アプリケーション、アプリケーションファミリ、およびアプリケーションオブジェクトの詳細については、「

[アプリケーション分類](#)」を参照してください。

5. [ルールグループ名] フィールドで、ルールグループを選択します。同じルールグループを持つルールの統計情報はグループ化され、まとめて表示できます。

ルールグループを表示するには、[監視] > [統計] に移動し、[表示] フィールドで [ルールグループ] を選択します。

カスタムルールグループを追加することもできます。詳しくは、「[カスタムアプリケーションの追加と MOS の有効化](#)」を参照してください。

6. アプリケーショントラフィックをフィルタリングするために、次のアプリケーションルールの一致基準を指定します。フィルタリングの後、ルール設定は、これらの基準に一致するサービスに適用されます。

- 送信元 **IP** アドレス: トラフィックと照合する送信元 IP アドレスおよびサブネットマスク。
- 宛先 **IP** アドレス: トラフィックと照合する宛先 IP アドレスおよびサブネットマスク。
- **[Source Port]**: トラフィックと照合する送信元ポート番号またはポート範囲。
- 宛先ポート: トラフィックと照合する宛先ポート番号またはポート範囲。

注

送信元と宛先のインターネットプロトコルアドレスが同じ場合は、[**Src = Dest**] を選択します。

7. 次の一般的な WAN 設定を構成します。

- [**Transmit Mode**] フィールドで、次のいずれかの送信モードを選択します。
 - ロードバランスパス: フローのアプリケーショントラフィックは、複数のパス間で分散されます。トラフィックは、そのパスが完全に使用されるまで、最適パスを介して送信されます。残りのパケットは、次の最適パスを介して送信されます。
 - 永続パス: アプリケーショントラフィックは、パスが使用できなくなるまで同じパス上に残ります。
[**Persistent Impedance**] フィールドで、パス上の待機時間が設定された値よりも長くなるまで、トラフィックが同じパスに留まる最小時間をミリ秒単位で指定します。
 - 重複パス: アプリケーショントラフィックは複数のパス間で重複するため、信頼性が向上します。
- [失われたパケットを再送信] をオンにすると、このルールに一致するトラフィックが信頼できるサービス経路でリモートアプライアンスに送信され、失われたパケットが再送信されます。

8. LAN から WAN への設定を構成します。

- クラス: このルールを関連付けるクラスを選択します。
ルールを適用する前にクラスをカスタマイズすることもできます。詳細については、「[クラスのカスタマイズ](#)」を参照してください。
- [**Drop Limit**]: クラススケジューラで待機しているパケットがドロップされるまでの時間。バルククラスには適用されません。

- ドロップ深度: パケットがドロップされるまでのキューの深さのしきい値。
- **RED** を有効にする: Random Early Detection (RED; ランダム早期検出) は、輻輳が発生したときにパケットを廃棄することにより、クラスリソースの公平な共有を保証します。
- **Disable Limit**: 重複パケットが帯域幅を消費するのを防ぐために、重複を無効にする時間。
- **Disable Depth**: クラススケジューラのキューの深さ。この時点で、重複パケットは生成されません。

9. この規則に対して、次の WAN から LAN への動作を設定します。

- パケットの再シーケンシングを有効にする: 宛先で正しい順序でパケットをシーケンスします。
- **[Resquence Hold Time]**: パケットがリシーケンシングのために保持され、その後パケットが LAN に送信される時間間隔。
- 遅延再シーケンス処理パケットの破棄: 再シーケンス処理に必要なパケットが LAN に送信された後に到着した順不同パケットを廃棄します。

10. [適用] をクリックします。

アプリケーションルールがトラフィックフローに適用されるかどうかを確認するには、[**Monitoring] > [Flows] に移動します。 **

アプリのルール ID を書き留め、クラスタイプと送信モードがルール構成に従っているかどうかを確認します。

Flows Data																			
Both LAN to WAN and WAN to LAN flows																			
Source IP Address	Dest IP Address	Direction	Source Port	Dest Port	IPF	IP DSCP	Hit Count	Service Type	Service Name	LAN GW IP	Age (mS)	Packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	App Rule ID
172.16.30.74	172.16.10.89	LAN to WAN	35118	5001	UDP	default	4961	Virtual Path	DC-Client-1	LOCAL	0	4959	7428582	292.687	3507.565	126.441	0.000	48	0
																			11
																			INTERACTIVE
																			DC-WL-1->Client-1-WL-1
																			N/A
																			Duplicate

[Monitoring] > [**Statistics] > [Application QoS] の順に選択すると、各サイトでアップロード、ダウンロード、ドロップされたパケット数やバイト数などの **アプリケーション QoS** を監視 ** できます。

Num パラメーターは、アプリルール ID を示します。フローから取得したアプリルール ID を確認します。

Dashboard Monitoring Configuration																			
Monitoring > Statistics																			
Statistics																			
Show: Application QoS Enable Auto Refresh: 5 seconds Refresh																			
Application QoS Statistics																			
Filter: Any column Apply																			
Show: 100 entries Showing 1 to 12 of 12 entries																			
Num	Site	Service	IP Address	Port	Sec	Dest	Sec	Dest	Application Object	Application	Family	Bytes	Packets	LAN to WAN	WAN to LAN	Dropped	Bytes	Packets	Last Hit (DdHMM ago)
0	DC	DC-Client-1	*	*	*	*	*	*	iperf	*	*	26325792	32262	0	0	287616	192	00:00	
1	DC	DC-Client-1	*	*	*	*	*	*	ica_priority_0	*	*	0	0	0	0	0	0	0	
2	DC	DC-Client-1	*	*	*	*	*	*	ica_priority_1	*	*	0	0	0	0	0	0	0	
3	DC	DC-Client-1	*	*	*	*	*	*	ica_priority_2	*	*	0	0	0	0	0	0	0	
4	DC	DC-Client-1	*	*	*	*	*	*	ica_priority_3	*	*	0	0	0	0	0	0	0	
5	DC	DC-Client-1	*	*	*	*	*	*	ica	*	*	0	0	0	0	0	0	0	
6	Client-1	DC-Client-1	*	*	*	*	*	*	iperf	*	*	0	0	4710	5	1464	1	00:38	

カスタムアプリケーションの作成

アプリケーション・オブジェクトを使用して、次の一致タイプに基づいてカスタム・アプリケーションを定義できます。

- IP プロトコル
- アプリケーション名
- アプリケーションファミリ

DPI 分類器は、着信パケットを分析し、指定された一致基準に基づいてアプリケーションとして分類します。これらの分類済みカスタムアプリケーションは、QoS、ファイアウォール、およびアプリケーションルーティングで使用できます。

ヒント

1 つ以上のマッチタイプを指定できます。

SD-WAN Center では、分類されたカスタムアプリケーションのレポートを表示できます。詳しくは、「[アプリケーションレポート](#)」を参照してください。

カスタム・アプリケーションを作成するには、次の手順に従います。

1. 構成エディタで、「グローバル」>「アプリケーション」>「カスタムアプリケーション **」の順に選択し、「**+」をクリックします。

Match Type	Application Family	Application	Protocol	Network IP Address 1	Port 1
IP Protocol			TCP (6)	*	*

2. 次のパラメーターを設定します。

- **[名前]:** カスタムアプリケーションの名前
- **レポートを有効にする:** SD-WAN Center でカスタムアプリケーションレポートを表示できるようにします。詳しくは、「[アプリケーションレポート](#)」を参照してください。
- **優先度:** カスタムアプリケーションの優先度。着信パケットが 2 つ以上のカスタムアプリケーション定義と一致すると、最もプライオリティの高いカスタムアプリケーション定義が適用されます。

3. [アプリケーション一致条件] セクションの [+] をクリックします。

4. 次のいずれかのマッチタイプを選択します。

- **IP プロトコル:** プロトコル、ネットワーク IP アドレス、ポート番号、および DSCP タグを指定します。

- アプリケーション: アプリケーション名、ネットワーク IP アドレス、ポート番号、および DSCP タグを指定します。
 - アプリケーションファミリー: アプリケーションファミリーを選択し、ネットワーク IP アドレス、ポート番号、および DSCP タグを指定します。
5. アプリケーションの一致基準を追加するには、[+] をクリックします。
 6. [適用] をクリックします。

ルールグループを追加して **MOS** を有効にする

May 10, 2021

ネットワーク内の特定のアプリケーションは、そのアプリケーションに適用される規則のグループによって定義できます。SD-WAN 構成エディタには、ルールグループのデフォルトリストが表示されます。また、カスタム規則グループを作成し、個別の IP 規則またはアプリケーション QoS 規則をアプリケーションにタグ付けすることもできます。

規則の詳細については、[IP アドレスとポート番号による規則](#)および[アプリケーション名による規則](#)を参照してください。

同じルールグループを持つルールの統計情報は、グループ化され、まとめて表示できます。

ルールグループに基づいて統計情報を表示するには、[モニタリング]>[統計]に移動し、[表示]フィールドで[ルールグループ]を選択します。

平均オピニオンスコア (MOS) は、アプリケーションがエンドユーザーに提供するエクスペリエンスの品質の数値指標です。主に VoIP アプリケーションに使用されます。SD-WAN では、トラフィックを VoIP コールであるかのように判断することで、非 VoIP アプリケーションの品質を評価するためにも使用されます。

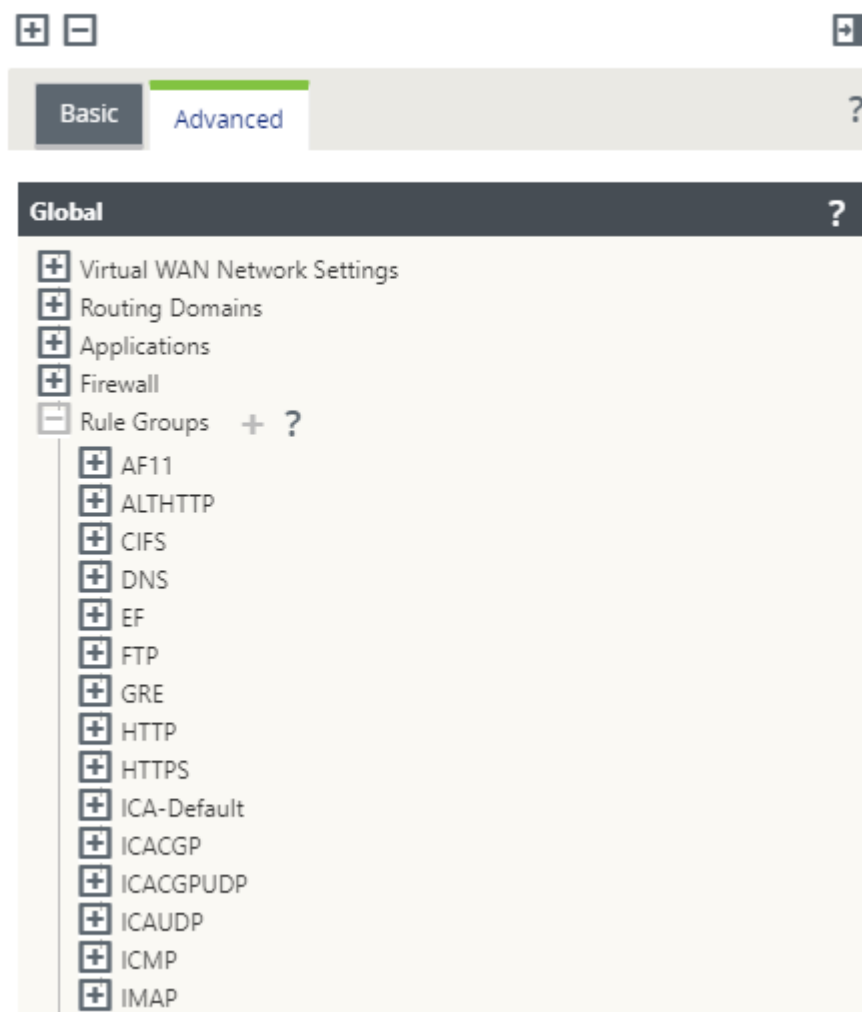
平均 MOS スコアは、サンプリング間隔が 1 分で計算されます。他のサードパーティ製ツールによって計算される MoS スコアは、使用するサンプリング間隔によって異なる場合があります。

SD-WAN Center には、仮想パスを通過する既存のトラフィックの MOS が表示されます。SD-WAN Center で MOS を表示する方法については、[アプリケーション向け MOS](#)を参照してください。

カスタム・ルール・グループを追加するには、次の手順に従います。

1. 構成エディタで、[グローバル]>[規則グループ]に移動します。。ルールグループのデフォルトリストが表示されます。
2. 追加 (+) アイコンをクリックします。
3. アプリケーション名を入力します。

4. 編集アイコンをクリックし、[**MOS** を有効にする] を選択します。



5. [適用] をクリックします。

注

- [Enable MOS] を選択して、デフォルトアプリケーションの **MOS** 推定を有効にすることもできます。
- アプリケーションの MOS を推定し、SD-WAN Center に表示するには、[ルール] の [パフォーマンスの追跡] オプションを有効にします。詳細については、[アプリケーション向け MOS](#) を参照してください。

アプリケーション分類

November 17, 2022

Citrix SD-WAN アプライアンスは、ディープ・パケット・インスペクション (DPI) を実行して、次の手法を使用してアプリケーションを識別および分類します。

- DPI ライブラリの分類
- Citrix 独自の独立コンピューティングアーキテクチャ (ICA) 分類
- アプリケーションベンダー API (たとえば、Office 365 用の Microsoft REST API)
- ドメイン名ベースのアプリケーション分類

DPI ライブラリの分類

ディープパケットインスペクション (DPI) ライブラリは、数千もの商用アプリケーションを認識します。これにより、アプリケーションのリアルタイムの検出とクラス分けが可能になります。SD-WAN アプライアンスは DPI テクノロジーを使用して、着信パケットを分析し、トラフィックを特定のアプリケーションまたはアプリケーションファミリーに属するものとして分類します。各接続のアプリケーション分類には、数個のパケットが必要です。

DPI ライブラリ分類を有効にするには、構成エディタで、[グローバル] > [アプリケーション] > [DPI 設定] に移動し、[ディープパケットインスペクションを有効にする] チェックボックスをオンにします。

ICA の分類

Citrix SD-WAN アプライアンスでは、Virtual Apps and Desktops の Citrix HDX トラフィックを識別および分類することもできます。Citrix SD-WAN は、ICA プロトコルの次のバリエーションを認識します。

- ICA
- ICA-CGP
- シングルストリーム ICA (SSI)
- マルチストリーム ICA (MSI)
- TCP 経由の ICA
- ICA オーバー UDP/EDT
- 非標準ポート経由の ICA (マルチポート ICA を含む)
- HDX アダプティブ トランスポート
- WebSocket 経由の ICA (HTML5 レシーバで使用)

注

SSL/TLS または DTLS 経由で配信される ICA トラフィックの分類は、SD-WAN Standard Edition ではサポートされませんが、SD-WAN Premium Edition と SD-WAN WANOP Edition ではサポートされます。

ネットワークトラフィックの分類は、初期接続またはフロー確立時に行われます。したがって、既存の接続は ICA に分類されません。接続テーブルを手動でクリアすると、接続の分類も失われます。

Framehawk トラフィックとオーディオオーバー UDP/RTP は、HDX アプリケーションには分類されません。「UDP」または「不明なプロトコル」のいずれかとして報告されます。

リリース 10 バージョン 1 以降、SD-WAN アプライアンスは、シングルポート構成であっても、マルチストリーム ICA の各 ICA データストリームを区別することができます。各 ICA ストリームは、優先順位付けのための独自のデフォルト QoS クラスを持つ個別のアプリケーションとして分類されます。

- マルチストリーム ICA 機能を正しく動作させるには、SD-WAN Standard Edition 10.1 以降、または SD-WAN Premium Edition が必要です。
- SD-WAN Center で HDX ユーザーベースのレポートを表示するには、SD-WAN Standard Edition または Premium Edition 11.0 以降が必要です。

HDX 情報仮想チャネルの最小ソフトウェア要件:

- Citrix Virtual Apps and Desktops (以前の XenApp および XenDesktop) の最新リリース。前提条件となる機能が XenApp および XenDesktop 7.17 で導入され、7.15 長期サービスリリースには含まれていないためです。
- マルチストリーム ICA および HDX インサイト情報仮想チャネル CTXNSAP をサポートする Citrix Workspace アプリ (またはその前身である Citrix Receiver) のバージョン。[Citrix Workspace アプリの機能マトリックス](#)で、**NSAP VC** およびマルチポート/マルチストリーム **ICA** を使用した **HDX Insight** を探します。現在サポートされているリリースバージョンについては、[HDX Insights](#)を参照してください。
- 11.2 以降のリリースでは、マルチストリーム ICA が使用中の HDX リアルタイムトラフィックでパケットの複製がデフォルトで有効になりました。

分類されると、ICA アプリケーションをアプリケーションルールで使用したり、他の分類済みアプリケーションと同様のアプリケーション統計を表示したりできます。

ICA アプリケーションには、以下の優先順位タグに対して 5 つのデフォルトのアプリケーションルールがあります。

- 独立コンピューティングアーキテクチャ (Citrix) (ICA)
- ICA リアルタイム (ica_priority_0)
- ICA インタラクティブ (ica_priority_1)
- ICA バルクトランスファー (ica_priority_2)
- ICA の背景 (ica_priority_3)

詳細については、「[アプリケーション名別のルール](#)」を参照してください。

マルチストリーム ICA をサポートしていないソフトウェアを 1 つのポート上で組み合わせて実行している場合、QoS を実行するには、ICA ストリームごとに 1 つずつ、複数のポートを設定する必要があります。

XA/XD サーバーポリシーで構成された非標準ポートで HDX を分類するには、これらのポートを ICA ポート構成に追加する必要があります。また、これらのポートのトラフィックを有効な IP ルールに一致させるには、ICA IP ルールを更新する必要があります。

ICA IP とポートの一覧では、XA/XD ポリシーで使用する非標準ポートを指定して、HDX 分類を処理できます。IP アドレスは、ポートを特定の宛先にさらに制限するために使用されます。任意の IP アドレスを宛先とするポートには

“*” を使用します。SSL ポートを組み合わせた IP アドレスは、トラフィックが最終的に ICA に分類されていない場合でも、トラフィックが ICA である可能性が高いことを示すためにも使用されます。この表示は、Citrix Application Delivery Management でマルチホップレポートをサポートするために L4 AppFlow レコードを送信するために使用されます。

ICA ベースの分類を有効にするには、構成エディタで [グローバル] > [アプリケーション] > [DPI 設定] に移動し、[**Citrix ICA** アプリケーションのディープパケットインスペクションを有効にする] チェックボックスをオンにします。

アプリケーションベンダー **API** ベースの分類

Citrix SD-WAN では、次のアプリケーションベンダー API ベースの分類がサポートされています。

- Office 365。詳細については、「[Office 365 の最適化](#)」を参照してください。
- Citrix Cloud および Citrix Gateway サービス。詳細については、「[Gateway サービスの最適化](#)」を参照してください。

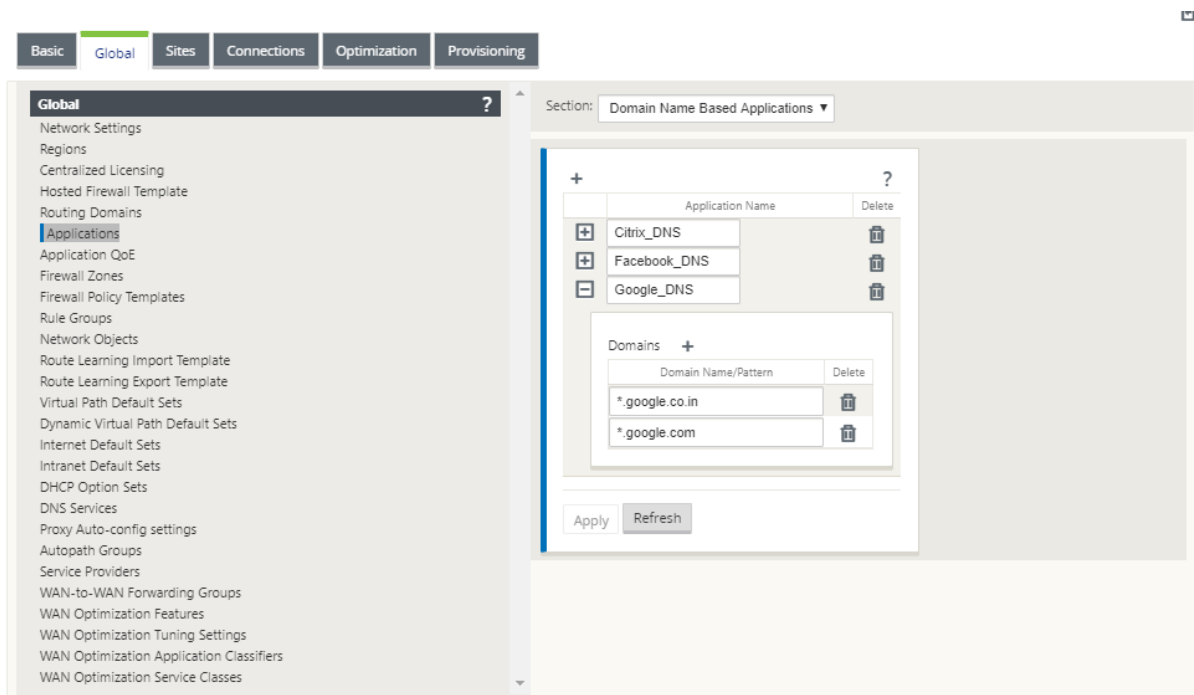
ドメイン名ベースのアプリケーション分類

DPI 分類エンジンが拡張され、ドメイン名とパターンに基づいてアプリケーションを分類できるようになりました。DNS フォワーダが DNS 要求を代行受信して解析すると、DPI エンジンは IP 分類子を使用して最初のパケット分類を実行します。さらに DPI ライブラリと ICA 分類が行われ、ドメイン名ベースのアプリケーション ID が追加されます。

ドメイン名ベースのアプリケーション機能を使用すると、複数のドメイン名をグループ化し、単一のアプリケーションとして扱うことができます。ファイアウォール、アプリケーションステアリング、QoS、およびその他のルールを簡単に適用できます。最大 64 のドメイン名ベースのアプリケーションを構成できます。

ドメイン名ベースのアプリケーションを定義するには、設定エディタで、[グローバル] > [アプリケーション] > [ドメイン名ベースのアプリケーション] に移動します。アプリケーション名を入力し、必要なドメイン名またはパターンを追加します。完全なドメイン名を入力することも、先頭にワイルドカードを使用することもできます。次のドメイン名の形式を使用できます。

- example.com
- *.example.com



分類されたドメイン名ベースのアプリケーションは、次の設定に使用されます。

- [DNS プロキシ](#)
- [DNS トランスペアレントフォワーダ](#)
- [アプリケーションオブジェクト](#)
- [アプリケーションルート](#)
- [ファイアウォールポリシー](#)
- [アプリケーション QoS ルール](#)
- [アプリケーション QoE](#)

注

11.4.2 リリース以降、ドメイン名ベースのアプリケーションは、Citrix SD-WAN Orchestrator サービスで構成可能なポートとプロトコルをサポートします。詳しくは、「[ドメインとアプリケーション](#)」を参照してください。

制限事項

- ドメイン名ベースのアプリケーションに対応する DNS 要求/応答がない場合、DPI エンジンではドメイン名ベースのアプリケーションを分類しないため、ドメイン名ベースのアプリケーションに対応するアプリケーションルールを適用しません。
- ポート範囲にポート 80 および/またはポート 443 が含まれ、ドメイン名ベースのアプリケーションに対応する特定の IP アドレス一致タイプが含まれるようにアプリケーションオブジェクトが作成された場合、DPI エンジンではドメイン名ベースのアプリケーションを分類しません。

- 明示的な Web プロキシが設定されている場合は、DNS 応答が必ず同じ IP アドレスを返すとは限らないように、すべてのドメイン名パターンを PAC ファイルに追加する必要があります。
- ドメイン名ベースのアプリケーション分類は、設定のアップグレード時にリセットされます。再分類は、DPI ライブラリ分類、ICA 分類、ベンダーアプリケーション API ベースの分類など、11.0.2 以前のリリース分類手法に基づいて行われます。
- ドメイン名ベースのアプリケーション分類によって学習されたアプリケーションシグニチャ（宛先 IP アドレス）は、設定の更新時にリセットされます。
- 標準 DNS クエリとその応答のみが処理されます。
- AAAA レコードまたは IPv6 レコードはサポートされていません。
- 複数のパケットに分割された DNS 応答レコードは処理されません。単一のパケット内の DNS 応答のみが処理されます。
- TCP 経由の DNS はサポートされていません。
- ドメイン名のパターンとしてサポートされるのは、トップレベルドメインのみです。

暗号化されたトラフィックの分類

Citrix SD-WAN アプライアンスは、アプリケーションレポートの一部として暗号化されたトラフィックを次の 2 つの方法で検出してレポートします。

- HTTPS トラフィックの場合、DPI エンジンが SSL 証明書を検査して、サービスの名前（たとえば Facebook、Twitter）を含む共通名を読み取ります。アプリケーションアーキテクチャによっては、複数のサービスタイプ（たとえば、電子メール、ニュースなど）に 1 つの証明書だけが使用されることがあります。サービスによって使用する証明書が異なる場合、DPI エンジンがサービスを区別できます。
- 独自の暗号化プロトコルを使用するアプリケーションの場合、DPI エンジンがフロー内のバイナリパターンを探します。たとえば、Skype の場合、DPI エンジンが証明書内のバイナリパターンを探してアプリケーションを決定します。

アプリケーション分類設定を構成するには、次の手順に従います。

1. 構成エディタで、[グローバル] > [アプリケーション] > [設定] をクリックします。

Settings ?

☒ Enable Deep Packet Inspection

☒ Enable Deep Packet Inspection for Citrix ICA Applications

Citrix ICA Deep Packet Inspection Settings

☒ Enable HDX User Reporting

☒ Enable Multi-Stream ICA

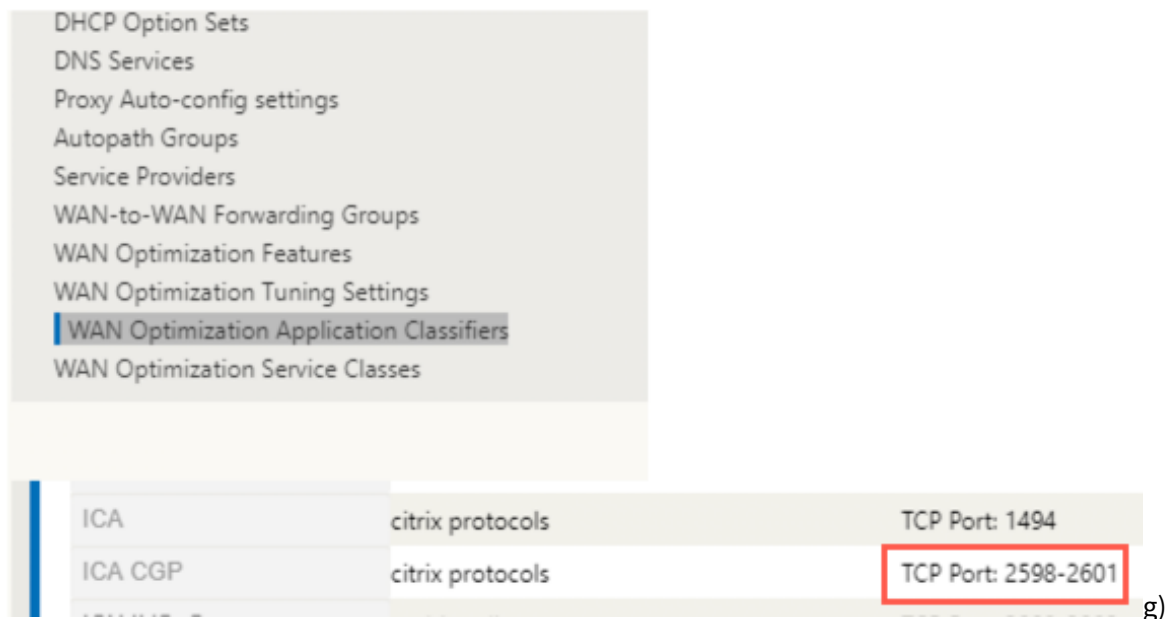
DPI ICA IP and Port List

DPI ICA IP-1:	DPI ICA Port-1:
<input type="text"/>	<input type="text" value="2599"/>
DPI ICA IP-2:	DPI ICA Port-2:
<input type="text"/>	<input type="text" value="2600"/>
DPI ICA IP-3:	DPI ICA Port-3:
<input type="text"/>	<input type="text" value="2601"/>
DPI ICA IP-4:	DPI ICA Port-4:
<input type="text"/>	<input type="text"/>
DPI ICA IP-5:	DPI ICA Port-5 :
<input type="text"/>	<input type="text"/>

注

マルチポート展開用に追加の ICA ポートを追加する場合は、WAN 最適化アプリケーション分類子でこれらのポートを追加する必要があります。そうしないと、3 つの追加ポートのトラフィックは WANOP に転送されません。ICA が最適化するように構成されている場合、デフォルトの 2598 ポートのみが転

送されます。



2. [ディープパケットインスペクションを有効にする]を選択します。これにより、アプライアンスでアプリケーションの分類が可能になります。SD-WAN Center では、アプリケーションの統計情報を表示、監視できます。詳細については、「[アプリケーションレポート](#)」を参照してください。

注

デフォルトでは、ディープパケットインスペクションを有効にすると、分類されたデータの統計情報が収集されます。

3. [Citrix ICA アプリケーションのディープパケットインスペクションを有効にする]を選択します。これにより、Citrix ICA アプリケーションの分類が可能になり、ユーザー、セッション、およびフローカウン트의統計情報が収集されます。このオプションを有効にしないと、HDX トラフィックのフレーバーの一部が分類され、QoE が計算されますが、SD-WAN Center の統計情報は利用できません。SD-WAN Center では、ICA アプリケーションの統計情報を表示、監視できます。このオプションは、デフォルトで有効になっています。詳しくは、[HDX レポートを参照してください](#)。
4. [HDX ユーザーレポートを有効にする]を選択して、新しく追加されたユーザーベースのレポート（[HDX サマリー]、[HDX ユーザーセッション]、[HDX アプリ]）を生成します。これらのレポートは、SD-WAN Center で使用できます。これは、HDX サイト統計レポートには適用されません。このオプションは、DPI オプションを有効にするのと同様に、グローバルレベルおよびサイトレベルで使用できます。HDX User Reporting をサイトレベルで有効にするには、構成エディタで、[接続] > [アプリケーション] の順にクリックします。

5. **DPI ICA** ポートで、HDX 分類を処理する XA/XD ポリシーで使用される非標準ポートを指定します。標準ポート番号 2598 または 1494 は、内部的にすでに含まれているため、このリストには含めないでください。

6. [**DPI ICA IP**] で、ポートを特定の宛先にさらに制限するために使用する IP アドレスを指定します。

注

任意の IP アドレスを宛先とするポートには “*” を使用します。

7. [適用] をクリックします。

アプリケーション分類設定は、各サイトで個別に構成できます。[接続] をクリックし、サイトを選択して、[アプリケーションの設定] をクリックします。また、グローバルアプリケーション設定を使用することもできます。

アプリケーションの検索

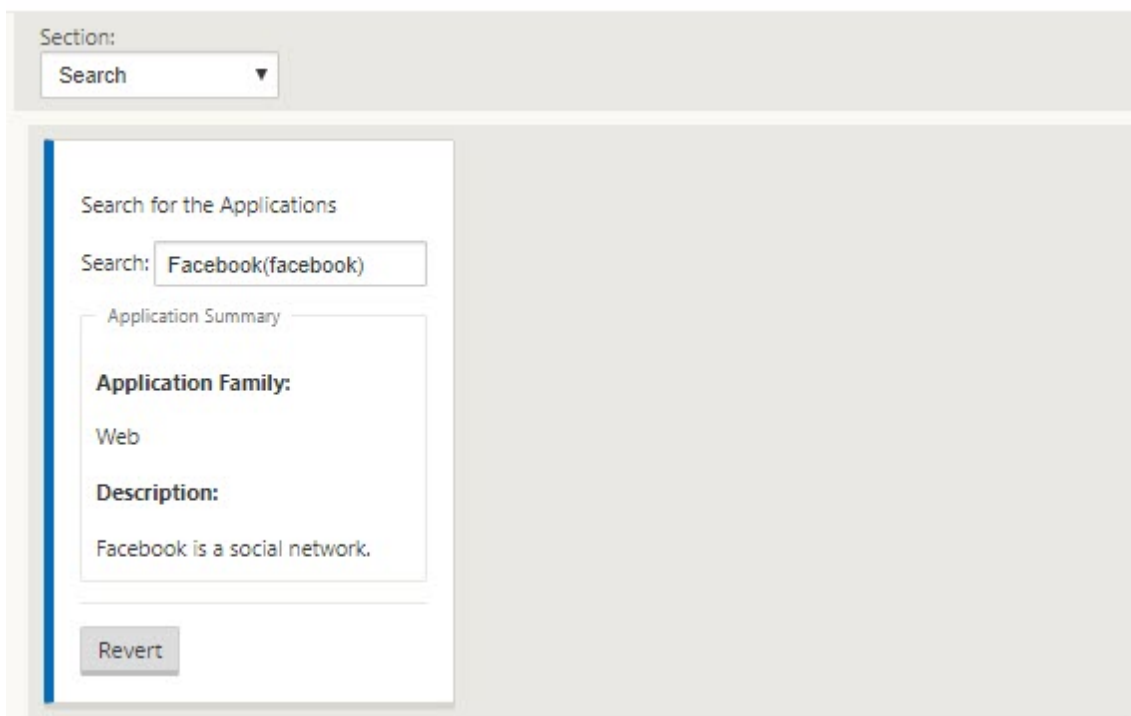
アプリケーションを検索して、アプリケーション・ファミリー名を特定できます。アプリケーションの簡単な説明も提供されます。

アプリケーションを検索する手順は、次のとおりです。

1. 構成エディターで、[グローバル] > [アプリケーション] > [検索] をクリックします。

2. [Search] フィールドにアプリケーションの名前を入力し、[Enter] をクリックします。

アプリケーションとアプリケーション・ファミリ名の簡単な説明が表示されます。



Section: Search

Search for the Applications

Search: Facebook(facebook)

Application Summary

Application Family:

Web

Description:

Facebook is a social network.

Revert

次の機能では、このアプリケーションをマッチタイプとして使用します。

- [ファイアウォールポリシー](#)
- [アプリケーション QoS ルール](#)
- [アプリケーション QoE](#)

注

SD-WAN アプライアンスがディープパケットインスペクションを使用して識別できるアプリケーションについては、[アプリケーションシングニチャライブラリ](#)を参照してください。

アプリケーションオブジェクト

アプリケーションオブジェクトを使用すると、異なるタイプの一致基準を 1 つのオブジェクトにグループ化できます。このオブジェクトは、ファイアウォールポリシーおよびアプリケーションステアリングで使用できます。IP プロトコル、アプリケーション、およびアプリケーションファミリは、使用可能な一致タイプです。

次の機能では、アプリケーションオブジェクトがマッチタイプとして使用されます。

- [アプリケーションルート](#)
- [ファイアウォールポリシー](#)

- [アプリケーション QoS ルール](#)
- [アプリケーション QoE](#)

アプリケーション・オブジェクトを作成する手順は、次のとおりです。

1. 構成エディタで、[グローバル]>[アプリケーション]>[アプリケーションオブジェクト]をクリックします。
2. [追加]をクリックし、[名前]フィールドにオブジェクトの名前を入力します。

Match Type	Application Family	Application	Protocol	Network IP Address 1	Port 1
Application		Salesforce(salesforce)	Any	192.168.3.4/3	*
Application		Onjira.com (JIRA)(jira)	Any	192.168.4.4/3	*

3. **Citrix SD-WAN Center** でのカスタムアプリケーションレポートの表示を有効にするには、[レポートを有効にする]を選択します。詳細については、「[アプリケーションレポート](#)」を参照してください。
4. [**Priority**] フィールドに、アプリケーションオブジェクトの優先度を入力します。着信パケットが2つ以上のアプリケーションオブジェクト定義と一致すると、プライオリティが最も高いアプリケーションオブジェクトが適用されます。
5. [アプリケーション一致基準] セクションの [+] をクリックします。
6. 次のいずれかのマッチタイプを選択します。
 - **IP プロトコル:** プロトコル、ネットワーク IP アドレス、ポート番号、および DSCP タグを指定します。
 - **アプリケーション:** アプリケーション名、ネットワーク IP アドレス、ポート番号、および DSCP タグを指定します。
 - **アプリケーションファミリー:** アプリケーションファミリーを選択し、ネットワーク IP アドレス、ポート番号、および DSCP タグを指定します。
7. [+] をクリックして、アプリケーションの一致基準をさらに追加します。
8. [追加] をクリックします。

ファイアウォールでのアプリケーション分類の使用

トラフィックをアプリケーション、アプリケーションファミリー、またはドメイン名として分類すると、アプリケーション、アプリケーションファミリー、およびアプリケーションオブジェクトを一致タイプとして使用して、トラフィックをフィルタリングし、ファイアウォールポリシーとルールを適用できます。これは、すべてのプレポリシー、ポスト

トポリシー、およびローカルポリシーに適用されます。ファイアウォールの詳細については、「[ステートフルファイアウォールと NAT のサポート](#)」を参照してください。

Edit Firewall Policy ? x

Priority: 100

From Zones

Zone	Enable
Any	<input checked="" type="checkbox"/>
Default_LAN_Zone	<input type="checkbox"/>
Internet_Zone	<input type="checkbox"/>
Untrusted_Internet_Zone	<input type="checkbox"/>

To Zones

Zone	Enable
Any	<input checked="" type="checkbox"/>
Default_LAN_Zone	<input type="checkbox"/>
Internet_Zone	<input type="checkbox"/>
Untrusted_Internet_Zone	<input type="checkbox"/>

Action: **Allow** Log Interval (s): 0 ☐ Log Start ☐ Log End Connection State Tracking: Use Site Setting

Match Type: **IP Protocol** (selected)
 Application Objects: Any Application: Application Family: Application Objects

DSCP: Any ☒ Allow Fragments ☐ Reverse Also ☐ Match Established

Source Service Type: Any Source Service Name: Any Source IP: * Source Port: *

Dest Service Type: Any Dest Service Name: Any Dest IP: * Dest Port: *

Apply **Cancel**

アプリケーション分類の表示

アプリケーションの分類を有効にすると、次のレポートでアプリケーション名とアプリケーション・ファミリの詳細を表示できます。

- ファイアウォール接続の統計情報
- フロー情報
- アプリケーション統計

ファイアウォール接続の統計情報

構成エディタで、**【監視】 > 【ファイアウォール】**に移動します。**【接続】**セクションの**【アプリケーション】**列と**【ファミリ】**列には、アプリケーションとその関連ファミリが一覧表示されます。

DashboardMonitoringConfiguration

Monitoring > Firewall

Firewall Statistics

Statistics:ConnectionsMaximum entries to display:50Filtering:Application:AnyFamily:AnyIP Protocol:AnySource Zone:AnyDestination Zone:AnySource Service Type:AnySource Service Instance:AnyDestination Service Type:AnyDestination Service Instance:AnySource IP:AnySource Port:AnyDestination IP:AnyDestination Port:AnyRefreshClear ConnectionsHelp

Connections

Application		Family	IP Protocol	IP Address	Port	Service Type	Service Name	Zone	IP Address	Port	Service Type	Service Name	Zone	State	Is NAT	Packets	Bytes	PPS	kbps
GoToMeeting Online Meeting(gotomeeting)	Audio/Video	TCP	172.16.30.30	54612	Local	Site1_VI_1	Default_LAN_Zone	216.115.208.241	80	Virtual Path	MCN_KVMVPK-BRANCH1_KVMVPK	Internet_Zone	CLOSED	No	4	259	0.716	0.371	
Domain Name Service(dns)	Network Service	UDP	172.16.30.30	47397	Local	Site1_VI_1	Default_LAN_Zone	8.8.8.8	53	Virtual Path	MCN_KVMVPK-BRANCH1_KVMVPK	Internet_Zone	ESTABLISHED	No	1	60	0.262	0.126	
Network Time Protocol(ntp)	Network Service	UDP	172.16.30.30	48743	Local	Site1_VI_1	Default_LAN_Zone	91.189.94.4	123	Virtual Path	MCN_KVMVPK-BRANCH1_KVMVPK	Internet_Zone	NEW	No	1	76	0.264	0.160	
Domain Name Service(dns)	Network Service	UDP	172.16.30.30	41348	Local	Site1_VI_1	Default_LAN_Zone	8.8.8.8	53	Virtual Path	MCN_KVMVPK-BRANCH1_KVMVPK	Internet_Zone	ESTABLISHED	No	2	118	0.476	0.225	
Domain Name Service(dns)	Network Service	UDP	172.16.30.30	44961	Local	Site1_VI_1	Default_LAN_Zone	8.8.8.8	53	Virtual Path	MCN_KVMVPK-BRANCH1_KVMVPK	Internet_Zone	ESTABLISHED	No	2	114	0.513	0.234	
Domain Name Service(dns)	Network Service	UDP	172.16.30.30	44119	Local	Site1_VI_1	Default_LAN_Zone	8.8.8.8	53	Virtual Path	MCN_KVMVPK-BRANCH1_KVMVPK	Internet_Zone	ESTABLISHED	No	1	60	0.263	0.126	
Google Generic(google_gen)	Web	TCP	172.16.30.30	45706	Local	Site1_VI_1	Default_LAN_Zone	172.217.26.206	80	Virtual Path	MCN_KVMVPK-BRANCH1_KVMVPK	Internet_Zone	CLOSED	No	6	394	1.017	0.534	
BING	Custom Application	TCP	172.16.30.30	45464	Local	Site1_VI_1	Default_LAN_Zone	204.79.197.200	80	Virtual Path	MCN_KVMVPK-BRANCH1_KVMVPK	Internet_Zone	CLOSED	No	31	1348	6.428	2.236	
Domain Name Service(dns)	Network Service	UDP	172.16.30.30	59856	Local	Site1_VI_1	Default_LAN_Zone	8.8.8.8	53	Virtual Path	MCN_KVMVPK-BRANCH1_KVMVPK	Internet_Zone	ESTABLISHED	No	2	116	0.410	0.190	
Domain Name Service(dns)	Network Service	UDP	172.16.30.30	49607	Local	Site1_VI_1	Default_LAN_Zone	8.8.8.8	53	Virtual Path	MCN_KVMVPK-BRANCH1_KVMVPK	Internet_Zone	ESTABLISHED	No	2	122	0.354	0.173	
Mozilla.com - Mozilla.org(mozilla)	Web	TCP	172.16.30.30	46324	Local	Site1_VI_1	Default_LAN_Zone	63.245.208.195	80	Virtual Path	MCN_KVMVPK-BRANCH1_KVMVPK	Internet_Zone	CLOSED	No	6	395	1.551	0.817	
Domain Name Service(dns)	Network Service	UDP	172.16.30.30	52889	Local	Site1_VI_1	Default_LAN_Zone	8.8.8.8	53	Virtual Path	MCN_KVMVPK-BRANCH1_KVMVPK	Internet_Zone	ESTABLISHED	No	2	112	0.332	0.149	
Microsoft(microsoft)	Web	TCP	172.16.30.30	51194	Local	Site1_VI_1	Default_LAN_Zone	104.215.148.63	80	Virtual Path	MCN_KVMVPK-BRANCH1_KVMVPK	Internet_Zone	CLOSED	No	6	397	1.433	0.758	

Connections Displayed: 13Connections in Use: 13/128000

アプリケーションの分類を使用可能にしない場合、「アプリケーション」列と「ファミリー」列にはデータが表示されません。

DashboardMonitoringConfiguration

Monitoring > Firewall

Firewall Statistics

Statistics:ConnectionsMaximum entries to display:50Filtering:Application:AnyFamily:AnyIP Protocol:AnySource Zone:AnyDestination Zone:AnySource Service Type:AnySource Service Instance:AnyDestination Service Type:AnyDestination Service Instance:AnySource IP:AnySource Port:AnyDestination IP:AnyDestination Port:AnyRefreshClear ConnectionsHelp

Connections

Application		Family	IP Protocol	IP Address	Port	Service Type	Service Name	Zone	IP Address	Port	Service Type	Service Name	Zone	State	Is NAT	Packets	Bytes	PPS	kbps	Received	Packets	Bytes	PPS	kbps	At (s)
*	*	TCP	172.16.30.30	54632	Local	Site1_VI_1	Default_LAN_Zone	216.115.208.241	80	Virtual Path	MCN_KVMVPK-BRANCH1_KVMVPK	Internet_Zone	CLOSED	No	4	259	0.909	0.471		3	217	0.682	0.395		
*	*	UDP	172.16.30.30	41664	Local	Site1_VI_1	Default_LAN_Zone	8.8.8.8	53	Virtual Path	MCN_KVMVPK-BRANCH1_KVMVPK	Internet_Zone	ESTABLISHED	No	2	112	0.383	0.171		2	156	0.383	0.239		
*	*	UDP	172.16.30.30	36817	Local	Site1_VI_1	Default_LAN_Zone	8.8.8.8	53	Virtual Path	MCN_KVMVPK-BRANCH1_KVMVPK	Internet_Zone	ESTABLISHED	No	2	122	0.408	0.199		2	196	0.408	0.320		
*	*	TCP	172.16.30.30	45726	Local	Site1_VI_1	Default_LAN_Zone	172.217.26.206	80	Virtual Path	MCN_KVMVPK-BRANCH1_KVMVPK	Internet_Zone	CLOSED	No	6	394	1.207	0.634		4	744	0.804	1.197		
*	*	TCP	172.16.30.30	45484	Local	Site1_VI_1	Default_LAN_Zone	204.79.197.200	80	Virtual Path	MCN_KVMVPK-BRANCH1_KVMVPK	Internet_Zone	CLOSED	No	26	1136	6.780	2.370		53	63972	13.820	133.449		
*	*	UDP	172.16.30.30	53904	Local	Site1_VI_1	Default_LAN_Zone	8.8.8.8	53	Virtual Path	MCN_KVMVPK-BRANCH1_KVMVPK	Internet_Zone	ESTABLISHED	No	2	118	0.589	0.278		2	272	0.589	0.641		
*	*	UDP	172.16.30.30	49809	Local	Site1_VI_1	Default_LAN_Zone	8.8.8.8	53	Virtual Path	MCN_KVMVPK-BRANCH1_KVMVPK	Internet_Zone	ESTABLISHED	No	2	116	0.513	0.238		2	354	0.513	0.727		
*	*	TCP	172.16.30.30	51214	Local	Site1_VI_1	Default_LAN_Zone	104.215.148.63	80	Virtual Path	MCN_KVMVPK-BRANCH1_KVMVPK	Internet_Zone	CLOSED	No	6	397	1.796	0.951		4	361	1.197	0.864		
*	*	TCP	172.16.30.30	46344	Local	Site1_VI_1	Default_LAN_Zone	63.245.208.195	80	Virtual Path	MCN_KVMVPK-BRANCH1_KVMVPK	Internet_Zone	CLOSED	No	6	395	1.904	1.003		4	387	1.269	0.982		
*	*	UDP	172.16.30.30	52627	Local	Site1_VI_1	Default_LAN_Zone	8.8.8.8	53	Virtual Path	MCN_KVMVPK-BRANCH1_KVMVPK	Internet_Zone	ESTABLISHED	No	2	114	0.622	0.283		2	210	0.622	0.522		

Connections Displayed: 10Connections in Use: 10/128000

フロー情報

設定エディタで、[モニタリング] > [フロー] に移動します。「フロー・データ」セクションの「アプリケーション」列にアプリケーションの詳細がリストされます。

Monitoring > Flows

Select Flows

Flow Type: ☒ LAN to WAN ☒ WAN to LAN ☐ Internet Load Balancing Table ☐ TCP Termination Table

Max Flows to Display (Per Flow Type): 50

Filter (Optional): Help

Refresh

Flows Data

Both LAN to WAN and WAN to LAN Flows

IP DSCP	Hit Count	Service Type	Service Name	LAN GW IP	Age (mS)	Packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	App Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type	Application
P default	3	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	LOCAL	6979	2	112	0.287	0.128	0.131	0.000	51	N/A	13	INTERACTIVE	Site1_Test-WL1->HQ1_Test-WL1	N/A	Load Balanced, Reliable	N/A
P default	3	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	LOCAL	4967	2	118	0.403	0.190	0.184	0.000	51	N/A	13	INTERACTIVE	Site1_Test-WL1->HQ1_Test-WL1	N/A	Load Balanced, Reliable	N/A
P default	28	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	LOCAL	4963	27	1176	4.950	1.725	2.257	0.000	28	N/A	14	INTERACTIVE	Site1_Test-WL1->HQ1_Test-WL1	N/A	Load Balanced, Reliable	bing
P default	3	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	LOCAL	4811	2	114	0.416	0.190	0.190	0.000	51	N/A	13	INTERACTIVE	Site1_Test-WL1->HQ1_Test-WL1	N/A	Load Balanced, Reliable	N/A
P default	5	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	LOCAL	5715	4	259	0.644	0.334	0.294	0.000	28	N/A	14	INTERACTIVE	Site1_Test-WL1->HQ1_Test-WL1	N/A	Load Balanced, Reliable	gotomeeting
P default	3	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	LOCAL	6717	2	122	0.298	0.145	0.136	0.000	51	N/A	13	INTERACTIVE	Site1_Test-WL1->HQ1_Test-WL1	N/A	Load Balanced, Reliable	N/A
P default	7	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	LOCAL	6692	6	394	0.876	0.460	0.399	0.000	28	N/A	14	INTERACTIVE	Site1_Test-WL1->HQ1_Test-WL1	N/A	Load Balanced, Reliable	google_gen
P default	7	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	LOCAL	4016	6	395	1.254	0.660	0.572	0.000	28	N/A	14	INTERACTIVE	Site1_Test-WL1->HQ1_Test-WL1	N/A	Load Balanced, Reliable	mozilla
P default	3	INTERNET	-	LOCAL	5711	2	116	0.350	0.162	0.000	0.000	135	N/A	N/A	N/A	N/A	N/A	N/A	N/A
P default	7	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	LOCAL	4775	6	397	1.222	0.647	0.557	0.000	28	N/A	14	INTERACTIVE	Site1_Test-WL1->HQ1_Test-WL1	N/A	Load Balanced, Reliable	microsoft
P default	2	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	LOCAL	6883	2	156	0.288	0.180	0.131	0.000	117	N/A	N/A	N/A	N/A	N/A	Load Balanced, Reliable	N/A
P default	2	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	LOCAL	4936	2	272	0.403	0.439	0.184	0.000	117	N/A	N/A	N/A	N/A	N/A	Load Balanced, Reliable	N/A
P default	53	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	LOCAL	4969	53	64273	9.730	94.396	4.437	0.000	94	N/A	N/A	N/A	N/A	N/A	Load Balanced, Reliable	bing
P cs4	2	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	LOCAL	4804	2	210	0.416	0.350	0.190	0.000	117	N/A	N/A	N/A	N/A	N/A	Load Balanced, Reliable	N/A

Total LAN to WAN flows displayed: 10 out of 10

Total WAN to LAN flows displayed: 10 out of 10

アプリケーション統計

構成エディタで、**[監視] > [統計]** に移動します。**[アプリケーション統計]** セクションの **[アプリケーション]** 列に、アプリケーションの詳細が表示されます。

DashboardMonitoringConfiguration

Monitoring > Statistics

Statistics

Show Applications ☐ Enable Auto Refresh 5 seconds Refresh ☒ Show latest data.

Applications Statistics

Filter: in Any column Apply

Show 100 entries Showing 1 to 35 of 35 entries

Application	Family	Bytes Received	Bytes Sent	Total Bytes
Adobe	Web	122923	45896	168819
Akamai Technologies CDN	Web	40935	87002	127937
Amazon Ad System	Web	25405	8439	33844
Amazon Generic Services	Web	44130	13405	57535
Amazon Web Services/Cloudfront CDN	Web	17147	3804	20951
Bing.com (formerly MSN Search)	Web	914343	74913	989256
BoldChat Live Chat	Web	224358	97936	322294
Clicktale	Web	323870	69287	393157

トラブルシューティング

アプリケーションの分類を有効にした後、**[Monitoring]** セクションの下にレポートを表示し、アプリケーションの詳細が表示されることを確認できます。詳細については、[アプリケーション分類の表示を参照してください](#)。

予期しない動作が発生した場合は、問題が発生している間に STS 診断バンドルを収集し、Citrix サポートチームと共有します。

STS バンドルは、**[構成] > [システムメンテナンス] > [診断] > [診断情報]** を使用して作成およびダウンロードできます。

QoS 公平性 (RED)

May 10, 2021

QoS 公平性機能は、QoS クラスと Random Early Detection (RED; ランダム早期検出) を使用して、複数の仮想パスフローの公平性を向上させます。仮想パスは、16 種類のクラスのいずれかに割り当てることができます。クラスは、次の 3 つの基本タイプのいずれかになります。

- リアルタイムクラスは、特定の帯域幅制限までプロンプトサービスを要求するトラフィックフローを提供します。総スループットよりも低レイテンシが推奨されます。
- インタラクティブクラスの優先順位は、リアルタイムよりも低くなりますが、バルクトラフィックよりも絶対的な優先順位を持ちます。
- バルククラスは、リアルタイムおよび対話型クラスから残っているものを取得します。これは、バルクトラフィックにとってレイテンシーはあまり重要ではないためです。

ユーザは、クラスごとに異なる帯域幅要件を指定します。これにより、仮想パススケジューラは、同じタイプの複数のクラスから競合する帯域幅要求を調停できます。スケジューラは、クラス間の公平性を達成するために、階層公平サービス曲線 (HFSC) アルゴリズムを使用します。

HFSC は、先入れ先出し (FIFO) の順序でクラスを提供します。パケットをスケジューリングする前に、Citrix SD-WAN はパケットクラスの保留中のトラフィック量を調べます。過剰なトラフィックが保留中の場合、パケットはキューに入れられずにドロップされます (テールドロップ)。

TCP がキューイングを引き起こすのはなぜですか？

TCP では、ネットワークがデータを送信できる速度を制御できません。帯域幅を制御するために、TCP は帯域幅ウィンドウの概念を実装しています。これは、ネットワークで許可される未確認トラフィックの量です。最初は小さなウィンドウから始まり、確認応答が受信されるたびに、そのウィンドウのサイズが 2 倍になります。これをスロースタートまたは指数関数的な成長フェーズと呼びます。

TCP は、ドロップされたパケットを検出することによってネットワークの輻輳を識別します。TCP スタックが 250 ms の遅延をもたらすパケットのバーストを送信する場合、TCP はパケットが廃棄されない場合に輻輳を検出しないため、ウィンドウのサイズは増加し続けます。待機時間が 600 ~ 800 ミリ秒に達するまで、この処理が続けられる場合があります。

TCP がスロースタートモードでない場合、パケット損失が検出されると帯域幅が半分になり、受信確認応答ごとに 1 パケットずつ許可帯域幅が増加します。したがって、TCP は、帯域幅を上向きに圧力をかけることとバッキングオフを交互に行います。残念ながら、パケット損失が検出されるまでに待機時間が 800 ミリ秒に達すると、帯域幅の削減によって伝送遅延が発生します。

QoS の公平性への影響

TCP 伝送遅延が発生すると、仮想パスクラス内で何らかの公平性保証を提供することは困難です。仮想パススケジューラは、大量のトラフィックが保持されないように、テールドロップ動作を適用する必要があります。TCP 接続の性質は、少数のトラフィックが仮想パスを満たすため、新しい TCP 接続で帯域幅の公平なシェアを得ることが困難になるようなものです。帯域幅を公平に共有するには、新しいパケットを送信するために帯域幅が使用可能であることを確認する必要があります。

ランダム早期検出

Random Early Detection (RED; ランダム早期検出) は、トラフィックキューがいっぱいになり、テールドロップこれにより、TCP 接続が達成できるスループットに影響を与えずに、仮想パススケジューラによる不必要なキューイングを防止できます。

RED の使い方

1. TCP セッションを開始して、仮想パスを作成します。RED を有効にすると、そのクラスの待機時間が定常状態で約 50 ミリ秒に留まることを確認します。
2. 2 番目の TCP セッションを開始し、両方の TCP セッションで仮想パスの帯域幅が均等に共有されていることを確認します。クラスの待機時間が定常状態のままであることを確認します。
3. 構成エディタを使用して RED を有効または無効にできること、およびパラメータに正しい値が表示されることを確認します。
4. SD-WAN GUI の [設定の表示] ページに、ルールに対して RED が有効になっているかどうかが表示されていることを確認します。

RED を有効にする方法

1. 構成エディタ > 接続 > 仮想パス > 仮想パスの [選択] > ルール > ルールの選択 (**VOIP**) などに移動します。
2. [**LAN** から **WAN** へ] ペインを展開します。[**LAN to WAN**] セクションで、[**RED** を有効にする] チェックボックスをオンにして、TCP ベースのルールに対して有効にします。

Virtual Path to Site: NSSDWANVPX_MCN-NSSDWAN1kBranch Section: Rules + Add Virtual Path Delete Virtual Path

Order	Rule Group Name	IP Address			Protocol	Protocol #	Port			DSC
		Source	Dest=Src	Dest			Source	Dest=Src	Dest	
100	IPERF	10.102.29.3/5	<input checked="" type="checkbox"/>	*	Any	0	*	<input checked="" type="checkbox"/>	*	Any

Initialize Properties Using Protocol

WAN General

LAN to WAN

General

Class: <Default>

Drop Limit (ms): 50 Drop Depth: 128000

Large Packet Size (bytes): 0

☒ Enable RED

Large Packets

Drop Limit (ms): 0 Drop Depth (bytes): 0

Duplicate Packets

Disable Limit (ms): 0 Disable Depth (bytes): 128000

MPLS キュー

May 10, 2021

この機能を使用すると、マルチプロトコルレイヤスイッチング (MPLS) WAN リンクを追加するときに SD-WAN 設定を簡単に作成できます。以前は、各 MPLS キューに 1 つの WAN リンクを作成する必要がありました。各 WAN リンクには、WAN リンクを作成するための一意の仮想 IP アドレス (VIP) と、プロバイダのキューイングスキームに対応する一意の Differentiated Services Code Point (DSCP) タグが必要です。各 MPLS キューに WAN リンクを定義した後、特定のキューにマッピングするイントラネットサービスが定義されます。

現在、新しい MPLS 固有の WAN リンク定義 (アクセスタイプ) が使用可能です。新しいプライベート MPLS アクセスタイプを選択すると、WAN リンクに関連付けられた MPLS キューを定義できます。これにより、MPLS WAN リンクに対するプロバイダのキューイング実装に対応する複数の DSCP タグを持つ 1 つの VIP を使用できます。これにより、イントラネットサービスが 1 つの MPLS WAN リンク上の複数の MPLS キューにマッピングされます。

MPLS プロバイダーが DSCP マーキングに基づいてトラフィックを識別できるようにして、プロバイダーがサービスクラスを適用できるようにします。

注

既存の MPLS 構成があり、プライベート MPLS アクセスタイプを実装する場合は、Citrix サポートにお問い合わせください。

プライベート **MPLS WAN** リンクの設定

1. WAN リンクアクセスタイプをプライベート MPLS として定義します。
2. サービスプロバイダー MPLS キューに対応する MPLS キューを定義します。
3. 仮想パスサービスの WAN リンクを有効にします（プライベート MPLS WAN リンクではデフォルトで有効）。
4. WAN リンクの仮想パスから、Autopath グループを割り当てます。

注

自動パスグループが WAN リンクレベルから割り当てられている場合、SD-WAN は、一致する DSCP タグに基づいて MCN キューとクライアント MPLS キューの間にパスを自動的に作成します。自動パスグループが MPLS キューレベルから割り当てられている場合、SD-WAN は DSCP タグが一致しているかどうかにかかわらず、パスを自動的に作成します。

5. MCN とクライアントで同じ Autopath Group が構成されていることを確認します。
6. WAN リンクのパスが自動的に構築されていることを確認します。
7. 必要に応じて、イントラネットサービスを特定のキューに割り当てます。

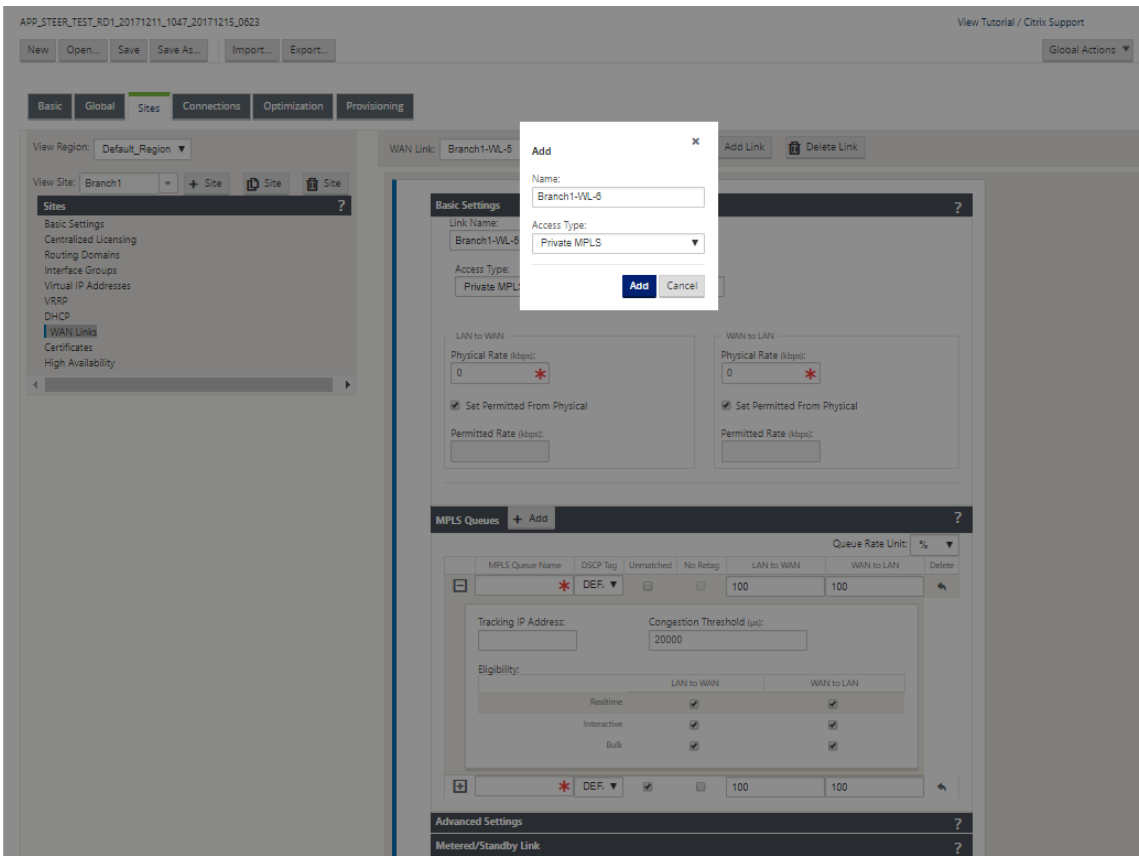
注

SD-WAN 設定では、プロバイダーベースのキューに対して 1 対 1 のマッピングがない場合があります。これは、特定の展開シナリオに基づいています。異なるプライベートアクセスタイプ間で自動パスグループを作成することはできません。たとえば、プライベートインターネットアクセスタイプとプライベート MPLS アクセスタイプの間に自動パスグループを作成することはできません。

プライベート **MPLS WAN** リンクの追加方法

プライベート MPLS 用の新しい WAN リンクアクセスタイプを設定するには、次の手順を実行します。

1. 構成エディタで、[サイト]>[サイト [名]]>[**WAN リンク**] に移動します。[リンクを追加] をクリックします。WAN リンク名を入力し、アクセスタイプとして [プライベート **MPLS**] を選択します。



2. [基本設定]の下に、新しい[**MPLS** キュー] タブが追加されました。[+ Add] をクリックして、特定の MPLS キューを追加します。これらは、サービスプロバイダによって定義されたキューに対応している必要があります。

フィールド	説明
MPLS キュー名	MPLS キュー名
DSCP タグ	キューに対するサービスプロバイダの DSCP タグ設定。
一致しません	有効にすると、構成ファイル内の定義されたタグと一致しない着信フレームは、このキューおよびこのキューに定義された帯域幅にマッピングされます。
LAN から WAN への許可レート (kbps)	SD-WAN デバイスがアップロードに使用できる帯域幅の量。これは、WAN リンクの定義された物理アップロードレートを超えることはできません。
WAN から WAN への許可レート (kbps)	SD-WAN デバイスがダウンロードに使用できる帯域幅の量。これは、WAN リンクの定義された物理ダウンロードレートを超えることはできません。

[+] をクリックして [MPLS キュー定義] を展開すると、その他のオプションが表示されます。これらのオプシ

ョンには、次のものがあります。

フィールド	説明
IP アドレスの追跡	WAN リンクトラッキングアドレス
輻輳しきい値	MPLS キューによってパケット送信が抑制され、輻輳が回避されるまでに定義された輻輳時間（マイクロ秒）。輻輳が設定しきい値を超えると、SD-WAN は送信レートをバックオフします。
参加資格	特定のトラフィッククラスを処理する MPLS キューの適格性。特定のトラフィッククラスに対して適格性が無効になっている場合、ネットワーク条件によって要求されない限り、そのトラフィッククラスが MPLS キューを通過することはほとんどありません。

既存のサービスプロバイダー WAN リンクキュー定義に対応する MPLS キューを設定します。

注

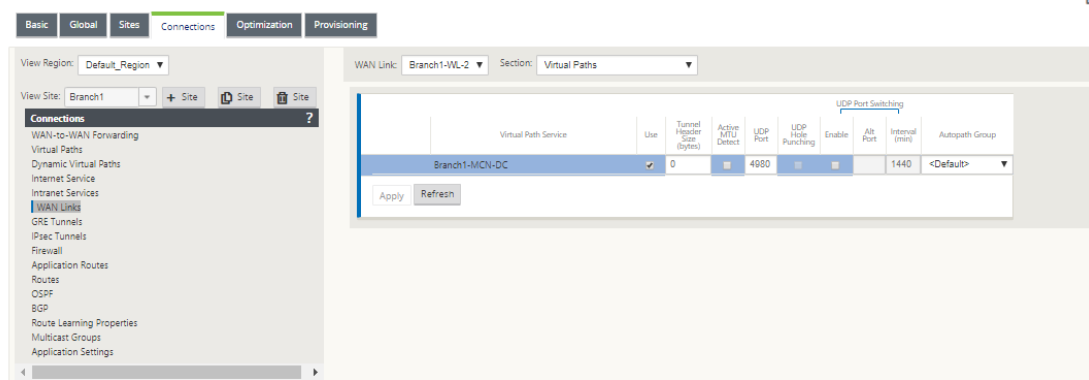
SD-WAN 9.1 より前に設定された既存の MPLS WAN リンクは影響を受けません。

プライベート **MPLS** の **WAN** リンクプロパティの定義

MPLS キューを持つプライベート MPLS WAN リンクを定義したら、特定の仮想パス定義の下で WAN リンクに自動パスグループを割り当てる必要があります。

autopath グループを割り当てるには、次の手順に従います。

1. **[接続]** > **[名]** > **[WAN リンク]** > **[MPLS WAN リンク名]** > **[仮想パス]** > **[仮想パス名]** > **[ローカルサイト]** > **[WAN リンク]** に移動し **[Edit]** をクリックします。
2. **「Autopath Group」** ドロップダウンメニューをクリックし、使用可能なグループから選択します。デフォルトでは、MPLS キューは MPLS WAN リンクに割り当てられた自動パスグループを継承します。選択した Autopath Group を継承するように個々の MPLS キューを設定するか、各 MPLS キューの **[Autopath Group]** ドロップダウンメニューから代替を選択するかを選択できます。



注

ローカルサイトのキューとリモートサイトのキュー間で DSCP タグに基づく 1 対 1 のマッピングがない場合は、MPLS キューを特定の Autopath Group にマッピングする必要があります。MPLS WAN リンクから自動パスグループを継承すると、一致する DSCP タグを持つキュー間のパスが自動的に生成されます。

仮想パス WAN リンクへの自動パスグループの割り当て

定義された Autopath Group は、MCN アプライアンスとクライアントアプライアンスで同じです。これにより、システムは自動的にパスを構築できます。MCN サイトでは、仮想パスに関連付けられた WAN リンクを展開することもできます。

WAN リンクの許可レートと輻輳の表示

SD-WAN Web インターフェイスでは、WAN リンクおよび WAN リンク使用率の許可レート、および WAN リンク、パス、または仮想パスが輻輳状態であるかどうかを表示できるようになりました。以前のリリースでは、この情報は SD-WAN ログファイルおよび CLI 経由でのみ入手できました。トラブルシューティングに役立つように、Web インターフェイスでこれらのオプションが使用できるようになりました。

許可された料金を表示

許可レートは、特定の WAN リンク、仮想パスサービス、イントラネットサービス、またはインターネットサービスが、特定の時点で使用できる帯域幅の量です。WAN リンクの許可レートはスタティックで、SD-WAN 設定で明示的に定義されます。仮想パスサービス、イントラネットサービス、またはインターネットサービスの許可率は、輻輳、ユーザーの要求、公正な共有に応じて時間の経過とともに変動しますが、常にサービスの最小予約帯域幅以上になります。

WAN リンクの監視

[モニタ] > [統計] の順に選択し、[表示] ドロップダウンリストから [**WAN リンク**] を選択します。

Monitoring > Statistics

Statistics

Show: WAN Link ☒ Enable Auto Refresh 5 seconds ☒ Show latest data: Processing...

WAN Link Statistics

Filter: in Any column

Show: 100 entries Showing 1 to 6 of 6 entries 1

WAN Link	Access Interface	IP Address	Proxy Address	Proxy ARP State	MAC	Last ARP Reply Age (ms)
Client-1-WL-1	N/A	172.186.10.75	N/A	N/A	N/A	N/A
Client-1-WL-2	N/A	172.186.20.75	N/A	N/A	N/A	N/A
Client-2-WL-1	N/A	172.186.70.50	N/A	N/A	N/A	N/A
Client-2-WL-2	N/A	172.186.80.50	N/A	N/A	N/A	N/A
DC-WL-1	DC-WL-1-AI-1	172.186.30.85	N/A	DISABLED	N/A	N/A
DC-WL-2	DC-WL-2-AI-1	172.186.40.85	N/A	DISABLED	N/A	N/A

Showing 1 to 6 of 6 entries 1

Virtual Path Service Data Rates

Filter: in Any column

Show: 100 entries Showing 1 to 4 of 4 entries 1

Name	Direction	Virtual Path Service Packets	Virtual Path Service kB	Delta Virtual Path Service Packets	Delta Virtual Path Service kB	Virtual Path Service kbps	IP,TCP,UDP Header Compression Bytes Saved
DC-WL-1	Recv	2618687	195069.42	289	26.16	37.81	0

[モニター] > [統計] の順に選択し、[表示] ドロップダウンリストから [**WAN リンクの使用状況**] を選択します。

Statistics

Show

WAN Link Usage

Enable Auto Refresh

5

seconds

Stop

Show latest data

Processing...

WAN Link Usage Statistics

Local WAN Links

Filter

in

Any column

Apply

Show

100

entries

Showing 1 to 6 of 6 entries

First

Previous

1

Next

Last

WAN Link	Direction	Packets	Delta Packets	Delta KB	Kbps	Permitted Kbps	Congestion
DC-WG-1	Send	2551622	238	17.69	28.24	100000	N/A
DC-WG-1	Recv	2630429	240	21.87	35.38	80000	NO
q1	Send	2358231	312	20.84	33.77	50000	N/A
q1	Recv	2366461	308	18.26	29.74	49000	NO
q2	Send	118164	306	16.32	26.77	50000	N/A
q2	Recv	128766	321	19.88	32.21	49000	NO

Showing 1 to 6 of 6 entries

First

Previous

1

Next

Last

Usage and Permitted Rates

Filter

in

Any column

Apply

Show

100

entries

Showing 1 to 14 of 14 entries

First

Previous

1

Next

Last

WAN Link	Service	Direction	Packets	Packets KB	Delta Packets	Delta KB	Kbps	Permitted Kbps	Congestion
DC-WG-1	DC-Client-1	Recv	1473996	134889.42	118	10.8	16.99	14481.65	NO
DC-WG-1	DC-Client-2	Recv	958409	71407.76	138	12.12	19.07	14490	NO
DC-WG-1	DC-Client-1	Send	1623618	108311624	134	10.34	16.27	14990	N/A
DC-WG-1	DC-Client-2	Send	930096	64771056	132	9.47	14.9	14990	N/A
DC-WG-1	Internet-Intranet	Send	0	0	0	0	0	50020	N/A
DC-WG-1	Internet-Intranet	Recv	208	55.25	0	0	0	49020	N/A
q1	DC-Client-1	Recv	1337987	96716.01	208	17.12	17.31	14510	NO
q1	DC-Client-2	Recv	821873	52380.57	106	7.4	11.64	14990	NO
q1	DC-Client-1	Send	1314280	97359168	210	10.51	21.26	23010	N/A
q1	DC-Client-2	Send	847803	57291606	109	7.33	11.88	14990	N/A
q2	DC-Client-1	Recv	91058	6260.83	237	15.83	24.94	14510	NO
q2	DC-Client-2	Recv	40378	2232.83	104	5.56	8.75	14990	NO
q2	DC-Client-1	Send	81296	4710784	208	17.12	17.31	23010	N/A
q2	DC-Client-2	Send	40353	2271700	105	5.81	8.83	14990	N/A

Showing 1 to 14 of 14 entries

First

Previous

1

Next

Last

Remote WAN Links

Filter

in

Any column

Apply

Show

100

entries

Showing 1 to 6 of 6 entries

First

Previous

1

Next

Last

WAN Link	Service	Direction	Congestion
Client-1-WG-1	DC-Client-1	Recv	NO
Client-2-WG-1	DC-Client-2	Recv	NO
q3	DC-Client-1	Recv	NO
q4	DC-Client-1	Recv	NO
q5	DC-Client-2	Recv	NO
q6	DC-Client-2	Recv	NO

Showing 1 to 6 of 6 entries

First

Previous

1

Next

Last

MPLS キューの監視

[モニタ] > [統計] に移動し、[表示] ドロップダウンリストから [MPLS キュー] を選択します。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

588

Show: MPLS Queues
☒ Enable Auto Refresh
5 seconds
Stop
☒ Show latest data.

MPLS Queue Statistics

Filter:
in Any column
Apply

Show 100 entries
Showing 1 to 4 of 4 entries
Processing...

First Previous 1 Next Last

Private MPLS	MPLS Queue	Access Interface	IP Address	Proxy Address	Proxy ARP State	MAC	Last ARP Reply Age (ms)
EE-Branch1-WL-2	SAMPLE-Queue1	EE-Branch1-WL-2-AI-1	172.184.19.19	N/A	DISABLED	N/A	N/A
EE-Branch1-WL-2	SAMPLE-Queue2	EE-Branch1-WL-2-AI-1	172.184.19.19	N/A	DISABLED	N/A	N/A
VPX-DC-WL-2	DC-Queue1	N/A	172.184.3.19	172.184.3.19	N/A	N/A	N/A
VPX-DC-WL-2	DC-Queue2	N/A	172.184.3.19	172.184.3.19	N/A	N/A	N/A

Showing 1 to 4 of 4 entries

First Previous 1 Next Last

Virtual Path Service Data Rates

Filter:
in Any column
Apply

Show 100 entries
Showing 1 to 4 of 4 entries

First Previous 1 Next Last

Name	Direction	Virtual Path Service Packets	Virtual Path Service kB	Delta Virtual Path Service Packets	Delta Virtual Path Service kB	Virtual Path Service kbps	Mismatched DSCP Packets	Mismatched DSCP kB	IP/TCP/UDP Header Compression Bytes Saved
SAMPLE-Queue1	Recv	14279	1177.77	251	20.72	33.15	5932	407.36	0
SAMPLE-Queue1	Send	13400	919.09	217	14.47	23.15	N/A	N/A	0
SAMPLE-Queue2	Recv	12806	705.61	216	11.84	18.95	5803	250.8	0
SAMPLE-Queue2	Send	13953	915.39	241	16.73	26.77	N/A	N/A	0

Showing 1 to 4 of 4 entries

First Previous 1 Next Last

MPLS キューのトラブルシューティング

MPLS キューのステータスを確認するには、[モニタ] > [統計] に移動し、[表示] ドロップダウンリストから [パス (要約)] を選択します。次の例では、MPLS キュー「q1」から「q3」へのパスが DEAD 状態であり、赤色で示されています。MPLS キュー「q1」から「q5」へのパスは GOOD 状態であり、緑色で表示されます。

Statistics

Show: Paths (Summary)
☒ Enable Auto Refresh
5 seconds
Stop
☒ Show latest data.
Processing...

Path Statistics Summary

Filter:
in Any column
Apply

Show 100 entries

Num	From Link	To Link	Path State	Virtual Path Service State	Virtual Path Service Type	BOWT	Jitter (mS)	Loss %	kbps	Congestion
1	DC-WL-1	Client-1-WL-1	GOOD	GOOD	Static	5	2	0.00	15.30	NO
2	q1	q3	DEAD	GOOD	Static	9999	0	0.00	12.53	UNKNOWN
3	q1	q4	DEAD	GOOD	Static	9999	0	0.00	8.92	UNKNOWN
4	q2	q3	DEAD	GOOD	Static	9999	0	0.00	8.92	UNKNOWN
5	q2	q4	DEAD	GOOD	Static	9999	0	0.00	8.92	UNKNOWN
6	Client-1-WL-1	DC-WL-1	GOOD	GOOD	Static	4	2	0.00	19.96	NO
7	q3	q1	DEAD	GOOD	Static	9999	0	0.00	0.00	UNKNOWN
8	q3	q2	DEAD	GOOD	Static	9999	0	0.00	0.00	UNKNOWN
9	q4	q1	DEAD	GOOD	Static	9999	0	0.00	0.00	UNKNOWN
10	q4	q2	DEAD	GOOD	Static	9999	0	0.00	0.00	UNKNOWN
11	DC-WL-1	Client-2-WL-1	GOOD	GOOD	Static	2	2	0.00	15.12	NO
12	q1	q5	GOOD	GOOD	Static	2	2	0.00	11.53	NO
13	q2	q6	GOOD	GOOD	Static	2	2	0.00	8.51	NO
14	Client-2-WL-1	DC-WL-1	GOOD	GOOD	Static	2	2	0.00	20.09	NO
15	q5	q1	GOOD	GOOD	Static	2	2	0.00	11.69	NO
16	q6	q2	GOOD	GOOD	Static	2	2	0.00	8.82	NO

パスの詳細については、[表示] ドロップダウンリストから [パス (詳細)] を選択します。状態の理由、継続時間、送信元ポート、宛先ポート、MTU などのパスに関する情報は、

次の例では、MPLS キュー「q1」から「q3」へのパスが DEAD 状態であり、その理由は PEER です。MPLS キュー「q3」から「q1」へのパスは停止しており、その理由は SILENCE です。次の表に、利用可能な理由のリストとその説明を示します。

理由	説明
GATEWAY	アプライアンスがゲートウェイに到達または検出できないため、パスは DEAD です
SILENCE	アプライアンスがピアサイトからパケットを受信していないため、パスは BAD または DEAD です
LOSS	パケット損失のためにパスが不正です
PEER	ピアサイトがパスが不正であると報告している

Show:

Paths (Detailed)

☒ Enable Auto Refresh 5 seconds

Stop

☒ Show latest data.

Processing...

Path Statistics Advanced

Filter: in

Any column

Apply

Show

100

 entries Showing 1 to 16 of 16 entries

First

Previous

1

Next

Last

Num	From Link	To Link	Congestion	Path State	Reason	Duration (S)	Virtual Path Service State	Src Port	Dst Port	MTU	BOWT	Jitter (mS)	Packets Received	OOO	Loss %	kbps	Virtual Path Service Type
1	DC-WL-1	Client-1-WL-1	NO	GOOD	N/A	386	GOOD	4980	4980	1488	5	2	116	0	0.00	13.79	Static
2	q1	q3	UNKNOWN	DEAD	PEER	44	GOOD	4980	4980	1488	9999	0	108	0	0.00	12.75	Static
3	q1	q4	UNKNOWN	DEAD	PEER	44	GOOD	4980	4980	1488	9999	0	106	0	0.00	8.40	Static
4	q2	q3	UNKNOWN	DEAD	PEER	44	GOOD	4980	4980	1488	9999	0	106	0	0.00	8.40	Static
5	q2	q4	UNKNOWN	DEAD	PEER	44	GOOD	4980	4980	1488	9999	0	106	0	0.00	8.40	Static
6	Client-1-WL-1	DC-WL-1	NO	GOOD	N/A	21325	GOOD	4980	4980	N/A	4	2	126	0	0.00	17.45	Static
7	q3	q1	UNKNOWN	DEAD	SILENCE	44	GOOD	4980	4980	N/A	9999	0	0	0	0.00	0.00	Static
8	q3	q2	UNKNOWN	DEAD	SILENCE	44	GOOD	4980	4980	N/A	9999	0	0	0	0.00	0.00	Static
9	q4	q1	UNKNOWN	DEAD	SILENCE	44	GOOD	4980	4980	N/A	9999	0	0	0	0.00	0.00	Static
10	q4	q2	UNKNOWN	DEAD	SILENCE	44	GOOD	4980	4980	N/A	9999	0	0	0	0.00	0.00	Static
11	DC-WL-1	Client-2-WL-1	NO	GOOD	N/A	235	GOOD	4980	4980	1488	2	2	130	0	0.00	14.41	Static
12	q1	q5	NO	GOOD	N/A	235	GOOD	4980	4980	1488	2	2	111	0	0.00	11.69	Static
13	q2	q6	NO	GOOD	N/A	234	GOOD	4980	4980	1488	2	2	107	0	0.00	8.72	Static
14	Client-2-WL-1	DC-WL-1	NO	GOOD	N/A	235	GOOD	4980	4980	N/A	2	2	142	0	0.00	19.40	Static
15	q5	q1	NO	GOOD	N/A	235	GOOD	4980	4980	N/A	2	2	110	0	0.00	11.27	Static
16	q6	q2	NO	GOOD	N/A	235	GOOD	4980	4980	N/A	2	2	107	0	0.00	8.50	Static

MPLS キューに関連付けられたアクセスインターフェイスおよび IP アドレスを確認するには、[Show] ドロップダウンリストから [Access Interfaces] を選択します。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

590

Show: **Access Interfaces** ☒ Enable Auto Refresh 5 seconds ☒ Show latest data. Processing...

Access Interface Statistics

Filter: in **Any column**

Show 100 entries Showing 1 to 3 of 3 entries

First Previous 1 Next Last

WAN Link	Access Interface	IP Address	Proxy Address	Proxy ARP State	MAC	Last ARP Reply Age (ms)
DC-WL-1	DC-WL-1-AI-1	172.186.30.85	N/A	N/A	N/A	N/A
q1	DC-WL-2-AI-1	172.186.40.85	N/A	N/A	N/A	N/A
q2	DC-WL-2-AI-1	172.186.40.85	N/A	N/A	N/A	N/A

Showing 1 to 3 of 3 entries

First Previous 1 Next Last

Virtual Path Service Data Rates

Filter: in **Any column**

Show 100 entries Showing 1 to 12 of 12 entries

First Previous 1 Next Last

WAN Link	Access Interface	Service Name	Direction	Virtual Path Service Packets	Virtual Path Service kB	Delta Virtual Path Service Packets	Delta Virtual Path Service kB	Virtual Path Service kbps	IP/TCP/UDP Header Compression Bytes Saved
DC-WL-1	DC-WL-1-AI-1	DC-Client-2	Recv	953815	71018.84	147	13.04	21.11	0
DC-WL-1	DC-WL-1-AI-1	DC-Client-1	Recv	1670099	124524.23	112	10.56	17.1	0
DC-WL-1	DC-WL-1-AI-1	DC-Client-2	Send	925756	62940.27	137	10.22	16.55	0
DC-WL-1	DC-WL-1-AI-1	DC-Client-1	Send	1619424	105451.88	141	11.16	18.07	0
q1	DC-WL-2-AI-1	DC-Client-1	Recv	1530107	96340.46	202	10.82	17.52	0
q1	DC-WL-2-AI-1	DC-Client-2	Recv	828314	52130.2	103	7.21	11.68	0
q1	DC-WL-2-AI-1	DC-Client-1	Send	1507265	94613.25	205	13.25	21.46	0
q1	DC-WL-2-AI-1	DC-Client-2	Send	843865	55794.07	104	7.3	11.81	0

詳細なトラブルシューティングのために、ログファイルをダウンロードできます。[構成] > [ログ/監視] に移動し、[ログオプション] タブで [SDWAN_paths.log] または [SDWAN_common.log] を選択します。

Dashboard

Monitoring

Configuration

Appliance Settings

Administrator Interface

Logging/Monitoring

Network Adapters

Net Flow

App Flow/PPFIX

SNMP

NITRO API

Licensing

Fallback Configuration

+ Virtual WAN

+ System Maintenance

Configuration > Appliance Settings > Logging/Monitoring

Log Options

Alert Options

Alarm Options

Syslog Server

HTTP Server

Application

View Log File

Only the most recent 10000 entries will be shown and filtered. To view the full log, download and open it locally.

Filename: SDWAN_paths.log

Filter (Optional):

View Log

Download Log File

Filename: S35mount_overlay.log

Download Log

レポート

May 10, 2021

アプリケーション QoE

複数のネットフローコレクタ

アプリケーション QoE

June 8, 2022

アプリケーション **QoE** とは、SD-WAN ネットワークにおけるアプリケーションの経験の品質を測定する指標です。2 つの SD-WAN アプライアンス間の仮想パスを通過するアプリケーションの品質を測定します。アプリケーション **QoE** スコアは 0 ～10 の値です。該当するスコア範囲によって、アプリケーションの品質が決まります。

品質	範囲
高	8-10
標準	4-8
低	0-4

アプリケーション **QoE** スコアは、アプリケーションの品質を測定し、問題のある傾向を特定するために使用できます。

QoE プロファイルを使用して、リアルタイムおよび対話型アプライアンスの品質しきい値を定義し、これらのプロファイルをアプリケーションまたはアプリケーションオブジェクトにマッピングできます。

注:

アプリケーション QoE を監視するには、ディープパケットインスペクションを有効にすることが不可欠です。詳しくは、「[アプリケーション分類](#)」を参照してください。

リアルタイムアプリケーション QoE

リアルタイムアプリケーションのアプリケーション QoE 計算では、MOS スコアから派生した Citrix の革新的な手法が使用されます。

デフォルトのしきい値は次のとおりです。

- レイテンシしきい値: 160
- ジッタしきい値: 30 ミリ秒
- パケット損失しきい値: 2%

遅延、損失、およびジッタに関するしきい値を満たすリアルタイムアプリケーションのフローは、品質が良いと見なされます。

リアルタイムアプリケーションの QoE は、しきい値を満たすフローの割合をフローサンプルの合計数で割った値から決定されます。

リアルタイムの QoE = (しきい値を満たすフローサンプル数/フローサンプルの合計数) * 100

これは、0 から 10 の範囲の QoE スコアとして表されます。

カスタムしきい値を使用して QoE プロファイルを作成し、アプリケーションまたはアプリケーションオブジェクトに適用できます。

注:

ネットワーク条件がリアルタイムトラフィックに設定されたしきい値を超えている場合、QoE 値はゼロになります。

対話型アプリケーション QoE

対話型アプリケーションのアプリケーション QoE では、パケット損失とバーストレートのしきい値に基づいて Citrix の革新的な技術を使用しています。

対話型アプリケーションは、パケット損失とスループットに影響されます。したがって、フロー内のパケット損失率、および入出力トラフィックのバーストレートを測定します。

設定可能なしきい値は、次のとおりです。

- パケット損失率。
- 入力バーストレートと比較して、予想される出力バーストレートのパーセンテージ。

デフォルトのしきい値は次のとおりです。

- パケット損失しきい値:1%
- バーストレート:60%

次の条件が満たされている場合、フローの品質は良好です。

- フローの損失の割合は、設定されたしきい値より小さくなります。
- 出力バーストレートは、少なくとも入力バーストレートに設定されたパーセンテージです。

アプリケーション QoE の設定

アプリケーションまたはアプリケーションオブジェクトをデフォルトまたはカスタム QoE プロファイルにマッピングします。

リアルタイムおよび対話型トラフィック用のカスタム QoE プロファイルを作成できます。

カスタム QoE プロファイルを作成するには、次の手順を実行します。

1. 構成エディタで、[グローバル] > [アプリケーション QoE] > [QoE プロファイル] に移動し、[+] をクリックします。
2. 次のパラメータの値を入力します。

- **Profile Name:** リアルタイムトラフィックおよびインタラクティブトラフィックのしきい値を設定するプロファイルを識別する名前。
- **Real-Time:** リアルタイム QoS ポリシーにヒットするトラフィックフローのしきい値を設定します。遅延、損失、およびジッタに関するしきい値を満たすリアルタイムアプリケーションのフローは、品質が良いと見なされます。
 - 片道レイテンシ: レイテンシのしきい値 (ミリ秒単位)。デフォルトの QoE プロファイル値は 160 ミリ秒です。
 - ジッタ: ジッタしきい値 (ミリ秒単位)。デフォルトの QoE プロファイル値は 30 ミリ秒です。
 - パケット損失: パケット損失の割合。デフォルトの QoE プロファイル値は 2% です。
- **Interactive:** 対話型 QoS ポリシーにヒットするトラフィックフローのしきい値を設定します。バースト率とパケット損失のしきい値を下回っていることを満たすインタラクティブアプリケーションのフローは、品質が良いと見なされます。
 - 予想バーストレート: 予想バーストレートのパーセンテージ。出力バーストレートは、入力バーストレートの設定済みパーセンテージ以上でなければなりません。デフォルトの QoE プロファイル値は 60% です。
 - フローあたりのパケット損失率: パケット損失の割合。デフォルトの QoE プロファイル値は 1% です。

Section: QoE Profiles

Profile Name	Realtime			Interactive		Delete
	One Way Latency (ms)	Jitter (ms)	Packet Loss (%)	Expected Burst Rate (%)	Packet loss per flow (%)	
TestProfile2	190	30	3.0	60.0	1.0	
DefaultQoEProfile	160	30	2.0	60.0	1.0	
TestProfile1	170	30	2.0	60.0	2.0	

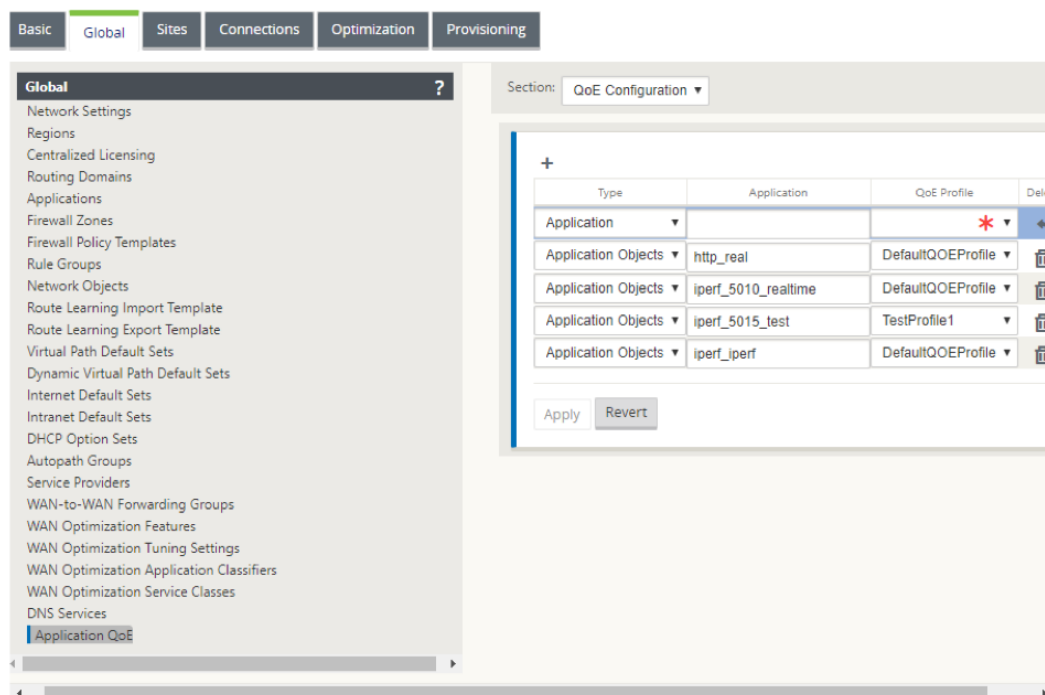
Apply Revert

3. [適用] をクリックします。

QoE プロファイルを使用してアプリケーションまたはアプリケーション・オブジェクトをマップするには、次の手順に従います。

1. 構成エディタで、[グローバル] > [アプリケーション QoE] > [QoE 設定] に移動し、[+] をクリックします。
2. 次のパラメータの値を選択します。
 - 型: DPI アプリケーションまたはアプリケーションオブジェクト。
 - **Application:** 選択したタイプに基づいて、アプリケーションまたはアプリケーション・オブジェクトを検索して選択します。

- **QoE プロファイル**: アプリケーションまたはアプリケーション・オブジェクトにマッピングする QoE プロファイルを選択します。



3. [適用] をクリックします。

QoE プロファイルを使用して、最大 10 個のアプリケーションまたはアプリケーションオブジェクトをマッピングできます。SD-WAN Center でアプリケーション QoE レポートを表示できます。詳細については、[アプリケーション QOE レポート](#) レポートを参照してください。

HDX QoE

May 10, 2021

レイテンシー、ジッタ、パケットドロップなどのネットワークパラメーターは、HDX ユーザーのユーザーエクスペリエンスに影響します。経験の品質（QoE）は、ユーザーが ICA の経験の質を理解し、確認するのに役立つように導入されています。QoE は計算されたインデックスで、ICA トラフィックのパフォーマンスを示します。ユーザーは、QoE を向上させるために、ルールとポリシーを調整できます。

QoE は 0 ～100 の数値で、値が大きいほどユーザーエクスペリエンスが向上します。QoE は、すべての ICA/HDX アプリケーションでデフォルトで有効になっています。

QoE の計算に使用されるパラメータは、クライアントとサーバー側にある 2 つの SD-WAN アプライアンス間で測定され、クライアントまたはサーバーアプライアンス自体の間で測定されません。遅延、ジッタ、およびパケットドロップはフローレベルで測定され、リンクレベルの統計情報とは異なる場合があります。エンドホスト（クライアント

またはサーバ) アプリケーションは、WAN でパケット損失があることを認識しません。再送信が成功すると、フローレベルのパケット損失レートはリンクレベルの損失よりも低くなります。ただし、その結果、レイテンシーとジッタが少し増加する可能性があります。

HDX トラフィックのデフォルト設定では、SD-WAN でパケットを再送信できるため、ネットワーク内のパケット損失により失われた QoE インデックス値が向上します。

Citrix SD-WAN Orchestrator の HDX ダッシュボードでは、HDX アプリケーションの全体的な品質をグラフィカルに表示できます。HDX アプリケーションは、次の 3 つの品質カテゴリに分類されます。

品質	QoE 範囲
高	80-100
標準	50-80
低	0-50

HDX ダッシュボードには、QoE が最も少ない下位 5 つのサイトのリストも表示されます。

異なる時間間隔での QoE のグラフィック表示により、各サイトで HDX アプリケーションのパフォーマンスを監視できます。

詳しくは、「[HDX ダッシュボードとレポート](#)」を参照してください。

注

- WAN リンク遅延、ジッタ、およびパケットドロップが常にアプリケーションの遅延、ジッタ、およびパケットドロップと一致することを想定しないでください。WAN リンク損失は実際の WAN パケット損失と相関しますが、アプリケーションの損失は再送信後に発生し、WAN リンク損失よりも低くなります。
- GUI に表示される WAN リンクの待ち時間は、BOWT (ベストワンウェイタイム) です。これは、リンクの健全性を測定する手段として、リンクの最適メトリックです。アプリケーション QoE は、そのアプリケーションのすべてのパケットの合計および平均遅延を追跡し、計算します。これは、多くの場合、リンク BOWT と一致しません。
- MSI セッションが開始されると、ICA ハンドシェイク中に、セッションが一時的に 1 つの MSI ではなく 4 つの SSI としてカウントされることがあります。ハンドシェイクが完了すると、1 MSI に収束します。SQL テーブルが更新される前に変換が行われると、その分の ICA_Summary に表示されます。
- セッションの再接続では、初期プロトコル情報が交換されないため、SD-WAN は MSI を識別できないため、各接続は SSI 情報としてカウントされます。
- UDP 接続の場合、接続が閉じられた後、ICA_Summary で接続が閉じられ、更新されるまでに最大 5 分かかる場合があります。TCP 接続の場合、接続が閉じられた後、ICA_Summary で閉じていると表示されるまでに最大 2 分かかる場合があります。
- TCP セッションと UDP セッションの QoE は、TCP と UDP の間で本質的に異なるため、同じパス上で同じではない場合があります。

- 1 人のユーザーが 2 つの仮想デスクトップを起動すると、ユーザー数が 2 つと打ち消されます。

複数のネットフローコレクタ

February 8, 2022

ネットフローコレクタは、SD-WAN インターフェイスに出入りすると、IP ネットワークトラフィックを収集します。Net Flow によって提供されるデータを分析することで、トラフィックの送信元と宛先、サービスクラス、およびトラフィックの輻輳の原因を特定できます。Citrix SD-WAN デバイスは、構成済みの Net フローコレクターに基本的な Net フローバージョン 5 の統計データを送信するように構成できます。Citrix SD-WAN は、信頼できるトランスポートプロトコルによって隠されるトラフィックフローに対する Net Flow サポートを提供します。ソリューションの WAN エッジ上のデバイスは、SD-WAN カプセル化された UDP パケットだけが表示されるので、Net Flow レコードを収集できなくなります。NetFlow は、Citrix SD-WAN Standard および Premium (Enterprise) Edition アプライアンスでサポートされています。

Net Flow ホストを設定するには、次の手順を実行します。

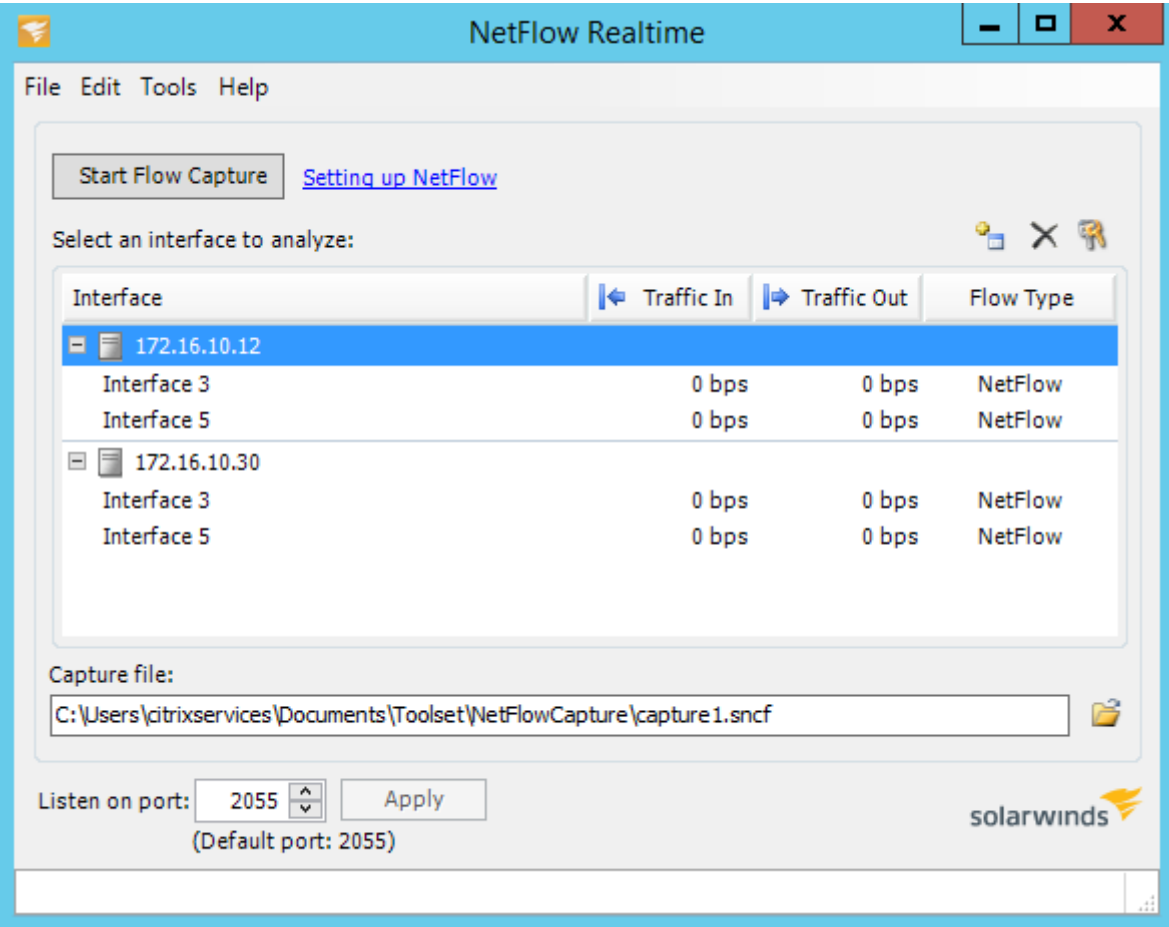
[構成] > [アプライアンス設定] > [ネットフロー] ** [**Netflow** ホスト設定] ページに移動します。[**NetFlow** を有効にする (Enable NetFlow)] チェックボックスをクリックし、最大 3 つのネットフローホストの **IP** アドレスとポート番号を入力し **、[設定の適用 (**Apply Settings**)] をクリックして変更を保存します。

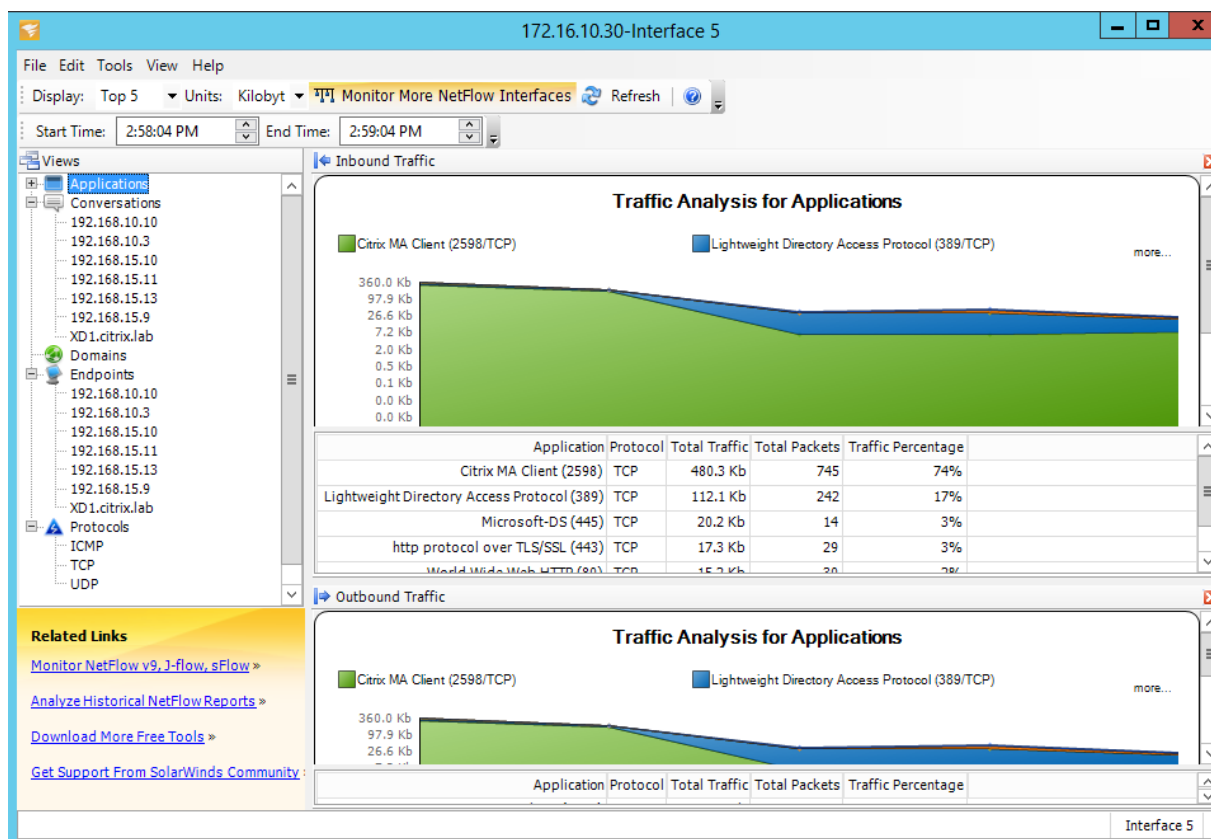
The screenshot displays the Citrix SD-WAN configuration web interface. The top navigation bar includes 'Dashboard', 'Monitoring', and 'Configuration'. The left sidebar shows 'Appliance Settings' with a tree view including 'Administrator Interface', 'Logging/Monitoring', 'Network Adapters', 'Net Flow' (highlighted), 'App Flow', 'SNMP', 'NITRO API', 'Licensing', 'Virtual WAN', and 'System Maintenance'. The main content area shows the 'Configuration > Appliance Settings > Net Flow' breadcrumb. The 'NetFlow Host Settings' section has a checked 'Enable NetFlow' checkbox. Below it, there are three rows for 'NetFlow Host 1', 'NetFlow Host 2 (Optional - can be left blank.)', and 'NetFlow Host 3 (Optional - can be left blank.)'. Each row contains input fields for 'IP Address' and 'Port'. The first row has '192.168.15.10' in the IP field and '2055' in the port field. An 'Apply Settings' button is at the bottom.

NetFlow エクスポート

Net Flow データは SD-WAN デバイス管理ポートからエクスポートされます。SNMP が設定されていない場合、Net Flow コレクタツールでは、SD-WAN デバイスが設定された管理 IP アドレスとしてリストされます。インターフェ

イスは、着信用 1 つ、発信用 2 つ（仮想パストラフィック）としてリストされます。詳細については、「[SNMP](#)」を参照してください。





NetFlow の制限事項

- SD-WAN Standard Edition および Premium Edition アプライアンスで Netflow を有効にすると、仮想パステータは指定された Netflow コレクタにストリーミングされます。この制限の 1 つは、SD-WAN で使用されている物理 WAN リンクを区別できないことです。ソリューションでは、集約された仮想パス情報（仮想パスは複数の個別の WAN パスで構成されている場合があります）がレポートされるため、個別の WAN パスの Netflow レコードをフィルタリングする方法はありません。
- TCP 制御ビットは N/A として報告されます。これは、SD-WAN が、TCPControlBits (IANA) の要素 ID 6 を持つ RFC 7011 に基づく Netflow エクスポートのインターネット標準に従っていないことを示します。TCP フラグがないと、フローデータのラウンドトリップ時間 (RTT)、遅延、ジッタ、およびその他のパフォーマンスメトリックを計算できません。セキュリティ側から、TCP フラグがないと、ネットフローコレクタは、FIN、ACK/RST、または SYN スキャンが発生しているかどうかを判別できません。

ルート統計情報

May 10, 2021

SD-WAN アプライアンスのルート統計情報を表示するには、SD-WAN GUI で [モニタリング] > [統計] > [ルート] に移動します。

Monitoring > Statistics

Statistics

Show: Routes Enable Auto Refresh 5 seconds Refresh Clear Counters on Refresh Purge dynamic routes

Route Statistics

Maximum allowed routes: 64000

Routes for routing domain : Default_RoutingDomain

Filter: in Any column Apply

Show: 100 entries Showing 1 to 10 of 10 entries

Details	Num	Network Addr	Gateway IP Address	Service	Firewall Zone	Reachable	Site IP Address	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
0	172.186.30.0/24	*	Local	Default_LAN_Zone	YES	*	DC	Static	-	-	5	55365	YES	N/A	N/A	
1	172.186.40.0/24	*	Local	Default_LAN_Zone	YES	*	DC	Static	-	-	5	0	YES	N/A	N/A	
2	172.186.50.0/24	*	New_Intranet_Service	Default_LAN_Zone	YES	*	DC	Static	-	-	5	11	YES	N/A	N/A	
3	172.186.10.0/24	*	DC-Client-1	Default_LAN_Zone	YES	*	Client-1	Dynamic	Virtual WAN	YES	10	27912	YES	N/A	N/A	
Site Path:		Client-1														
Optimal Route:		NO														
Summarized / Summary Route:		NO/NO														
4	172.186.20.0/24	*	DC-Client-1	Default_LAN_Zone	YES	*	Client-1	Dynamic	Virtual WAN	YES	10	0	YES	N/A	N/A	
5	172.186.10.0/24	*	New_Intranet_Service	Default_LAN_Zone	YES	*	DC	Static	-	-	15	0	YES	N/A	N/A	
6	172.186.20.0/24	*	New_Intranet_Service	Default_LAN_Zone	YES	*	DC	Static	-	-	15	0	YES	N/A	N/A	
7	0.0.0.0/0	*	Internet	Internet_Zone	YES	*	DC	Static	-	-	5	20	YES	N/A	N/A	
8	0.0.0.0/0	*	Passthrough	Any	YES	*	*	Static	-	-	65535	238	YES	N/A	N/A	
9	0.0.0.0/0	*	Discard	Any	YES	*	*	Static	-	-	65535	0	YES	N/A	N/A	

Showing 1 to 10 of 10 entries

次のパラメータを表示できます。

- ネットワークアドレス: ルートのネットワークアドレスとサブネットマスク。
- 詳細: [+] をクリックすると、次の情報が表示されます。
 - サイトパス: サイトパスは、受信したプレフィックスの真実のメトリックのソースです。これは、WAN から WAN への転送が複数のデバイスおよびメッシュ展開で有効になっている状況で使用されます。このようなプレフィックスが複数受信され、管理者はサイトパスを表示することでプレフィックスの属性を判断できます。
 - たとえば、Geo MCN とともに Branch1、Branch2、および MCN の単純なトポロジを考えます。Branch1 にはプレフィックス 172.16.1.0/24 があり、Branch2 に到達する必要があります。Geo MCN および MCN では、WAN から WAN への転送が有効になっています。
 - 接頭辞 172.16.1.0/24 は、Branch1-MCN-Branch2、Branch1-Geo-Branch2、Branch1-MCN-Geo-Branch2 を経由して Branch2 に到達できる。これらの個別のプレフィックスごとに、ルーティングテーブルがサイトパスメトリックで更新されます。サイトパスメトリックは、ルートプレフィックスの起点と、Branch2 に到達するためのコストを示します。
 - **Optimal Route:** Optimal Route は、ルートが他のすべてのルートと比較してそのサブネットに到達するのに最適なルートであるかどうかを示します。この最適ルートは、他のサイトにエクスポートされます。
 - **Summarized/Summary Route:** サマリールートは、スーパーネットに含まれる複数のプレフィックスを要約するために、管理者が明示的に設定したルートです。集約ルートは、集約ルートに含まれるプレフィックスです。

たとえば、サマリールート 172.16.0.0/16 があるとします。これはサマリールートだけであり、サマリールートではありません。サマリールートには、サマリー 'YES' とサマリー 'NO' があります。172.16.1.0/24、172.16.2.0/24、172.16.3.0/24 のような他のサブネットが少ない場合、これらの 3 つのルートはサマリールートまたはスーパーネットに該当するため、サマリールートと呼ばれます。集約されたルートには、集約された「YES」と集約された「NO」があります。

- **Gateway IP** アドレス: このルートに到達するために使用されるゲートウェイ/ルートの IP アドレス。
- サービス: Citrix SD-WAN サービスのタイプ。
- ファイアウォールゾーン: ルートによって使用されるファイアウォールゾーン。
- 到達可能: ルートが到達可能かどうか。
- サイト **IP** アドレス: サイトの IP アドレス。
- サイト: サイトの名前。
- タイプ: ルートのタイプは、ルート学習のソースによって異なります。LAN 側のルートと、設定時に手動で入力したルートは、スタティックルートです。SD-WAN またはダイナミックルーティングピアから学習されたルートは、ダイナミックルートです。
- プロトコル: プレフィックスのプロトコル。
 - ローカル: アプライアンスのローカル仮想 IP。
 - 仮想 **WAN**: ピア SD-WAN アプライアンスから学習されたプレフィックス。
 - **OSPF**: OSPF ダイナミックルーティングピアから学習されたプレフィックス。
 - **BGP**: **BGP** ダイナミックルーティングピアから学習されたプレフィックス。
- **Neighbor Direct**: サブネットが、ルートがアプライアンスに到達したブランチに接続されているかどうかを示します。
- コスト: 宛先ネットワークへの最適なパスを決定するために使用されるコスト。
- ヒット数: そのサブネットにパケットを転送するためにルートがヒットした回数。
- 適格: ルートが適格であることを示します。トラフィック処理中にヒットしたプレフィックスへのパケットの転送またはルーティングに使用されます。
- 適格タイプ: 次の 2 つの適格タイプを使用できます。
 - **Gateway** の適格: ゲートウェイが到達可能かどうかを判断します。
 - パスの適格性: パスが DEAD か否かを決定します。
- 適格値: ルートがシステムに作成されているときに、Gateway または構成内のパスに対して選択された値。たとえば、パス MCN-WL-1->BR1-WL-2 に基づいてルートを適格に呼び出すことができます。したがって、ルートセクションのこのルートの適格性値は MCN-WL-1->BR1-WL-2 の値です。

ルーティング

May 10, 2021

動的ルーティング

Citrix SD-WAN では、ダイナミックルーティング機能の下に、既知のルーティングプロトコルのサポートが導入されます。この機能により、LAN サブネットの検出が容易になり、仮想パスルートが BGP および OSPF プロトコルを使用してネットワーク内でよりシームレスに動作するようにアドバタイズされます。これにより、スタティックルート設定や正常なルータフェールオーバーを必要とせずに、SD-WAN を既存の環境にシームレスに展開できます。

ルートフィルタリング

ルート学習が有効なネットワークの場合、Citrix SD-WAN により、ルーティングネイバーにアドバタイズされる SD-WAN ルートと、ルーティングネイバーから受信されるルートをより詳細に制御できます。

- エクスポートフィルタは、特定の一致基準に基づいて OSPF および BGP プロトコルを使用してアドバタイズメント用のルートを含めるか除外するために使用されます。
- インポートフィルタは、特定の一致基準に基づいて OSPF および BGP ネイバーを使用して受信したルートを受け入れるか、受け付けないかに使用します。

ルートフィルタリングは、SD-WAN ネットワーク（データセンター/ブランチ）の LAN ルートおよび仮想パスルートに実装され、BGP と OSPF を使用して SD-WAN 以外のネットワークにアドバタイズされます。

ルート集約

ルート集約により、ルータが維持する必要のあるルート数が減少します。サマリールートは、複数のルートを表すために使用される 1 つのルートです。1 つのルートアドバタイズメントを送信することで帯域幅を節約し、ルータ間のリンク数を削減します。1 つのルートアドレスだけが維持されるため、メモリを節約できます。CPU リソースは、再帰的なルックアップを避けることによって、より効率的に使用されます。

VRRP

Virtual Router Redundancy Protocol (VRRP) 仮想ルータ冗長プロトコル) は、デバイスの冗長性を提供し、スタティックデフォルトルーティング環境に固有の単一障害点を排除する、広く使用されているプロトコルです VRRP を使用すると、1 つのグループを形成するように 2 つ以上のルータを設定できます。このグループは、1 つの仮想 IP アドレスと 1 つの仮想 MAC アドレスを持つ単一のデフォルト Gateway として表示されます。

Citrix SD-WAN（リリースバージョン 10.0 以降）は、VRRP バージョン 2 およびバージョン 3 をサポートし、サードパーティのルーターとの相互動作をサポートします。SD-WAN アプライアンスはマスタールーターとして機能し、サイト間で仮想パスサービスを使用するようにトラフィックを誘導します。仮想インターフェイス IP を VRRP IP として設定し、手動でプライオリティをピアルータよりも高い値に設定することで、SD-WAN アプライアンスを VRRP マスターとして設定できます。アドバタイズメント間隔と preempt オプションを設定できます。

CLI を使用したルーティング機能へのアクセス

ダイナミックルーティングおよびプロトコルステータスに関連する追加情報を表示できます。次のコマンドと構文を入力して、ルーティングデーモンにアクセスし、コマンドのリストを表示します。

```
'  
dynamic_routing?  
'
```

SD-WAN オーバーレイルーティング

May 10, 2021

Citrix SD-WAN は、リモートサイト、データセンター、クラウドネットワーク間の耐障害性と堅牢な接続を提供します。SD-WAN ソリューションでは、ネットワーク内の SD-WAN アプライアンス間にトンネルを確立することで、既存のアンダーレイネットワークにオーバーレイするルートテーブルを適用することで、サイト間の接続が可能になります。SD-WAN ルートテーブルは、既存のルーティングインフラストラクチャと完全に置き換えたり、共存したりできます。

Citrix SD-WAN アプライアンスは、可用性、損失、遅延、ジッタ、輻輳特性の観点から単方向で利用可能なパスを測定し、パケットごとに最適なパスを選択します。つまり、サイト A からサイト B まで選択したパスは、必ずしもサイト B からサイト A まで選択したパスである必要はありません。特定の時間における最適なパスは、各方向で個別に選択されます。Citrix SD-WAN では、パケットベースのパス選択により、ネットワークの変更に迅速に対応できます。SD-WAN アプライアンスは、2 つまたは 3 つのパケットが欠落した後でパスの停止を検出できるため、アプリケーショントラフィックを次善の WAN パスにシームレスにフェールオーバーできます。SD-WAN アプライアンスは、すべての WAN リンクステータスを約 50 ミリ秒で再計算します。次の記事では、Citrix SD-WAN ネットワーク内の詳細なルーティング構成について説明します。

Citrix SD-WAN ルートテーブル

SD-WAN 設定では、特定のサイトのスタティックルートエントリと、サポートされているルーティングプロトコル (OSPF、eBGP、iBGP など) を介してアンダーレイネットワークから学習されたルートエントリが許可されます。ルートは、ネクストホップだけでなく、サービスタイプによって定義されます。これにより、ルートの転送方法が決まります。使用中の主なサービスタイプは次のとおりです。

- ローカルサービス：SD-WAN アプライアンスにローカルなルートまたはサブネットを示します。これには、仮想インターフェイスサブネット（ローカルルートを自動的に作成）、およびルートテーブルに定義されたローカルルート（ローカルネクストホップを使用）が含まれます。ルートは、このローカルサイトへの仮想パスを持つ他の SD-WAN アプライアンスにアドバタイズされます。このルートは、パートナーとして信頼されている場合に構成されます。

注

デフォルトルートとサマリールートをローカルルートとして追加する場合は、注意が必要です。これらのルートは、他のサイトで仮想パスルートになることがあります。常にルートテーブルをチェックして、正しいルーティングが有効であることを確認します。

- **[Virtual Path]**：リモートの SD-WAN サイトから学習した、仮想パスを通して到達可能なローカルルートを示します。これらのルートは通常自動ですが、仮想パスルートはサイトで手動で追加できます。このルートのトラフィックはすべて、この宛先ルート（サブネット）に対して定義された仮想パスに転送されます。
- イン트라ネット：プライベート WAN リンク（MPLS、P2P、VPN など）を介して到達可能なルートを示します。たとえば、MPLS ネットワーク上にあり、SD-WAN アプライアンスを持たないリモートブランチなどです。これらのルートは、特定の WAN ルータに転送する必要があることを前提としています。イントラネットサービスは既定では有効になっていません。このルート（サブネット）に一致するトラフィックは、SD-WAN ソリューションを持たないサイトに配信するために、このアプライアンスのイントラネットとして分類されます。

注

イントラネットルートを追加する場合、ネクストホップはなく、イントラネットサービスへの転送があります。サービスは、指定された WAN リンクに関連付けられています。

- インターネット-イントラネットに似ていますが、プライベート WAN リンクではなくパブリックインターネット WAN リンクに流れるトラフィックを定義するために使用されます。1 つのユニークな違いは、インターネットサービスを複数の WAN リンクに関連付けて、負荷分散（フローごと）に設定するか、アクティブ/バックアップに設定できることです。インターネットサービスが有効の場合（デフォルトではオフになっています）、デフォルトのインターネットルートが作成されます。このルート（サブネット）に一致するトラフィックは、パブリックインターネットリソースに配信するために、このアプライアンスのインターネットとして分類されます。

注

インターネットサービスルートは、仮想パスを介してインターネットアクセスをバックホールしているかどうかに応じて、他の SD-WAN アプライアンスにアドバタイズしたり、エクスポートできないようにしたりできます。

- パススルーアプライアンスがインラインモードの場合、このサービスは最後の手段または上書きサービスとして機能します。宛先 IP アドレスが他のルートと一致しない場合、SD-WAN アプライアンスはそのアドレスを WAN リンクネクストホップに転送するだけです。デフォルトルート：0.0.0.0/0 コスト 16 パススルー

ートが自動的に作成されます。SD-WAN アプライアンスがパス外またはエッジ/ゲートウェイモードで展開されている場合、パススルーは機能しません。このルート（サブネット）に一致するトラフィックはすべて、このアプライアンスのパススルーとして分類されます。パススルートラフィックは可能な限り制限されることを推奨します。

注

パススルーは、POC の実行時に多数のルーティングを設定する必要がない場合に役立ちます。ただし、SD-WAN はパススルーに送信されるトラフィックの WAN リンク利用率を考慮しないため、本番環境では注意が必要です。また、問題をトラブルシューティングする場合や、仮想パスを介して特定の IP フローを配信できないようにする場合にも役立ちます。

- **Discard**：これはサービスではなく、一致した場合にパケットをドロップする最後の手段ルートです。通常、SD-WAN アプライアンスがパスの外に展開されている場合、この動作は期待されません。すべてのキャッチルートとして、イントラネットサービスまたはローカルルートが必要です。それ以外の場合、パススルーサービスが存在しないため、トラフィックは破棄されます（パススルーデフォルトルートが存在する場合でも）。

SD-WAN 構成エディタでは、使用可能なサイトごとにルートテーブルをカスタマイズできます。

The screenshot shows the Citrix SD-WAN configuration interface. The 'Connections' tab is selected, and the 'Routes' section is expanded in the left sidebar. The main area displays a table of routes for the 'MCN1' site.

Order	Network IP Address	Cost	Service Type	Service Name	Gateway IP Address	Info	Edit	Delete
1	172.120.21.100/32	5	Passthrough					
2	172.120.21.64/32	4	Internet					
3	172.120.21.65/32	4	Passthrough					
4	172.120.24.64/32	4	Internet					
5	10.101.0.0/22	5	Virtual Path	BR1				
6	224.225.1.1/32	5	Multicast					
7	224.225.1.2/32	5	Multicast					
8	224.225.1.3/32	5	Multicast					
9	172.120.24.7/24	5	Local					
10	182.120.24.7/24	5	Local					
11	0.0.0.0/0	5	Internet					
12	0.0.0.0/0	65535	Passthrough					

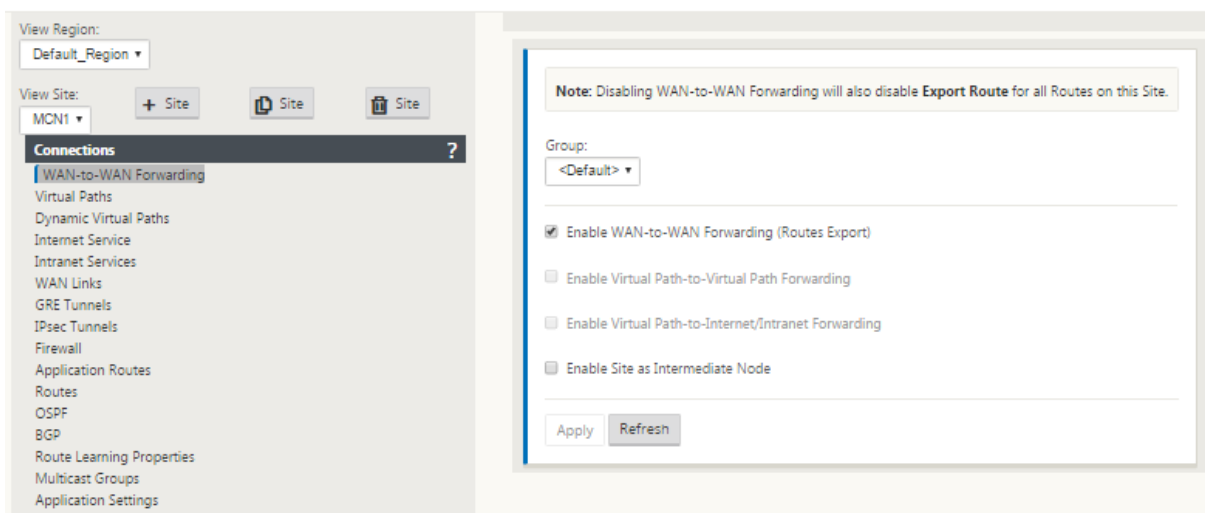
ルートテーブルエントリは、さまざまな入力から設定されます。

- 設定された仮想 IP アドレス（VIP）は、サービスタイプローカルルートとして自動入力されます。構成エディタは、異なるサイトノードへの同じ VIP 割り当てを防止します。
- ローカルサイトで有効になっているインターネットサービスは、直接インターネットブレイクアウトのためにデフォルトルート（0.0.0.0/0）をローカルに自動入力します。

- 管理者は、サイトごとにスタティックルートを定義しました。スタティックルートは、サービスタイプローカルルートとしても定義されます。
- デフォルト (0.0.0.0/0) では、コスト 16 がパススルーとして定義されたすべてのルートがキャッチされます。

管理者は、上記のルートの 1 つを設定できますが、ルートコストに加えて、サービスタイプに応じてサービスタイプ、ネクストホップ、または Gateway を含めることもできます。デフォルトのルートコストは、各ルートタイプに自動的に追加されます (デフォルトのルートコストについては、次の表を参照してください)。また、信頼されたルートだけが他の SD-WAN アプライアンスにアドバタイズされます。信頼できないルートは、ローカルアプライアンスでのみ使用されます。

クライアントノードルートは、デフォルトでは MCN ノードにのみアドバタイズされ、他のクライアントノードはアドバタイズされません。クライアントノードルートを別のクライアントノードに表示するには、MCN ノードで WAN から WAN への転送を有効にする必要があります。



グローバル設定で WAN-to-WAN 転送 (ルートエクスポートテンプレート) が有効になっている場合、MCN サイトは SD-WAN オーバーレイに参加しているすべてのクライアントにアドバタイズされたルートを共有します。この機能をオンにすると、MCN を通過する通信で、異なるクライアントノードサイトにあるホスト間の IP 接続が可能になります。ローカルクライアントノードのルートテーブルは、[**Monitoring**] > [****Statistics**] ページで、[**Show**] ドロップダウンリストで [ルート] を選択して監視できます **。

Statistics

Flows

Routing Protocols

Firewall

IKE/IPsec

IGMP

Performance Reports

Qos Reports

Usage Reports

Availability Reports

Appliance Reports

DHCP Server/Relay

VRRP Protocol

Monitoring > Statistics

Statistics

Show: Routes Enable Auto Refresh 5 seconds Refresh Clear Counters on Refresh Purge dynamic routes

Route Statistics

Maximum allowed routes: 64000

Routes for routing domain : Default_RoutingDomain

Filter: in Any column Apply

Show 100 entries Showing 1 to 54 of 54 entries

Num#	Network Addr	Gateway IP Address	Service	Firewall Zone	Reachable	Site IP Address	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
0	172.120.21.64/32	*	Internet	Internet_Zone	YES	*	MCN1	Static	-	-	4	0	YES	N/A	N/A
1	172.120.24.64/32	*	Internet	Internet_Zone	YES	*	MCN1	Static	-	-	4	0	YES	N/A	N/A
2	172.120.21.65/32	*	Passthrough	Any	YES	*	*	Static	-	-	4	0	YES	N/A	N/A
3	224.225.1.1/32	*	Multicast	Any	YES	*	MCN1	Static	-	-	5	0	YES	N/A	N/A
4	224.225.1.2/32	*	Multicast	Any	YES	*	MCN1	Static	-	-	5	0	YES	N/A	N/A
5	224.225.1.3/32	*	Multicast	Any	YES	*	MCN1	Static	-	-	5	0	YES	N/A	N/A
6	172.120.21.100/32	*	Passthrough	Any	YES	*	*	Static	-	-	5	0	YES	N/A	N/A
7	172.120.24.64/32	*	MCN1-BR1	Default_LAN_Zone	YES	*	BR1	Dynamic	Virtual WAN	YES	9	0	YES	N/A	N/A
8	172.120.24.0/24	*	Local	Default_LAN_Zone	YES	*	MCN1	Static	-	-	5	3458	YES	N/A	N/A
9	182.120.24.0/24	*	Local	Default_LAN_Zone	YES	*	MCN1	Static	-	-	5	0	YES	N/A	N/A
10	172.120.10.0/24	*	MCN1-APAC_RCIN	Default_LAN_Zone	YES	*	APAC_RCIN	Dynamic	Virtual WAN	YES	10	0	YES	N/A	N/A
11	172.120.21.0/24	*	MCN1-BR1	Default_LAN_Zone	YES	*	BR1	Dynamic	Virtual WAN	YES	10	0	YES	N/A	N/A
12	182.120.10.0/24	*	MCN1-APAC_RCIN	Default_LAN_Zone	YES	*	APAC_RCIN	Dynamic	Virtual WAN	YES	10	0	YES	N/A	N/A
13	192.168.255.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	RCN01-2000	Dynamic	Virtual WAN	YES	10	0	YES	N/A	N/A
14	192.172.0.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpn01	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
15	192.172.1.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpn02	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
16	192.172.2.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpn03	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
17	192.172.3.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpn04	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
18	192.172.4.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpn05	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
19	192.172.5.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpn06	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
20	192.172.6.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpn07	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
21	192.172.7.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpn08	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
22	192.172.12.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpn13	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
23	192.172.13.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpn14	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
24	192.172.14.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpn15	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
25	192.172.15.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpn16	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
26	192.172.16.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpn17	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
27	192.172.17.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpn18	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
28	192.172.18.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpn19	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
29	192.172.19.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpn20	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
30	192.120.10.0/24	*	MCN1-APAC_RCIN	Default_LAN_Zone	YES	*	APAC_RCIN	Dynamic	Virtual WAN	YES	11	0	YES	N/A	N/A
31	172.108.0.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpn01	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
32	172.108.1.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpn02	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
33	172.108.2.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpn03	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
34	172.108.3.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpn04	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
35	172.108.4.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpn05	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
36	172.108.5.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpn06	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
37	172.108.6.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpn07	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
38	172.108.7.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpn08	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
39	172.108.12.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpn13	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
40	172.108.13.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpn14	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
41	172.108.14.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpn15	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
42	172.108.15.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpn16	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
43	172.108.16.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpn17	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
44	172.108.17.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpn18	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
45	172.108.18.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpn19	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
46	172.108.19.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpn20	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
47	10.101.0.0/22	*	MCN1-BR1	Any	YES	*	BR1	Static	-	-	5	0	YES	N/A	N/A
48	10.101.0.0/22	*	MCN1-BR1	Default_LAN_Zone	YES	*	BR1	Dynamic	Virtual WAN	YES	10	88	YES	N/A	N/A
49	172.105.96.0/20	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	RCN01-2000	Dynamic	Virtual WAN	YES	10	0	YES	N/A	N/A
50	0.0.0.0/0	*	Internet	Internet_Zone	YES	*	MCN1	Static	-	-	5	401109	YES	N/A	N/A
51	0.0.0.0/0	*	MCN1-BR1	Default_LAN_Zone	YES	*	BR1	Dynamic	Virtual WAN	YES	10	88	YES	N/A	N/A
52	0.0.0.0/0	*	Passthrough	Any	YES	*	*	Static	-	-	65535	40031844	YES	N/A	N/A
53	0.0.0.0/0	*	Discard	Any	YES	*	*	Static	-	-	65535	0	YES	N/A	N/A

Showing 1 to 54 of 54 entries

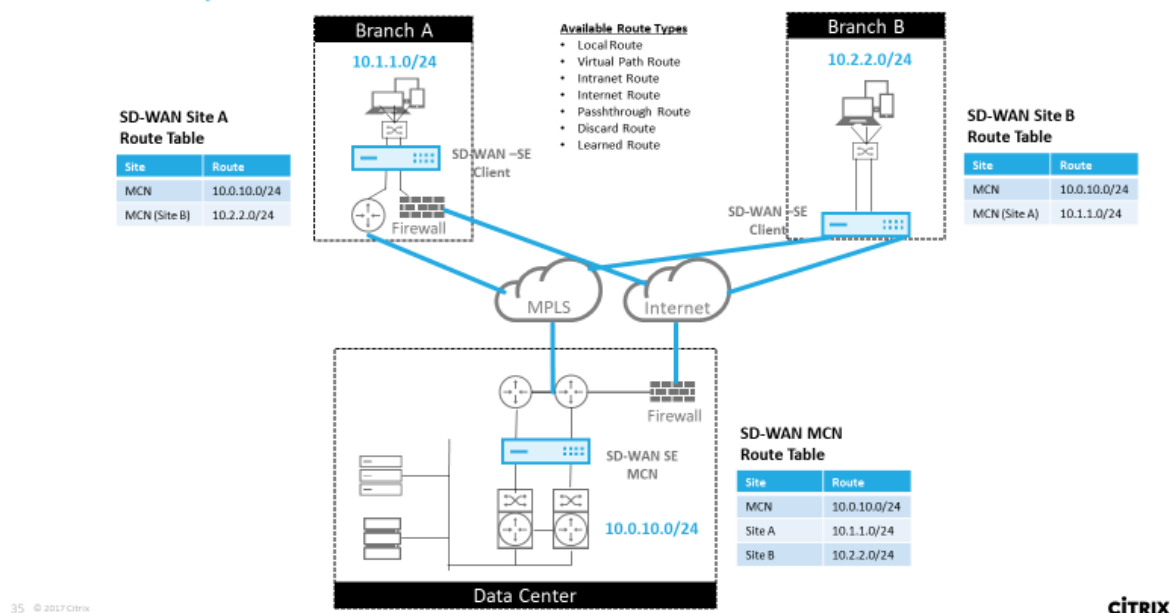
First Previous 1 Next Last

リモートブランチオフィスのサブネットの各ルートは、MCN 経由で接続する仮想パスを介してサービスとしてアドバタイズされます。[サイト] 列には、宛先がローカルサブネットとして存在するクライアントノードが表示されます。

次の例では、**WAN** ツー **WAN** 転送（ルートエクスポート）が有効の場合、支店 A は MCN を経由する支店 B サブネ

ット (10.2.2.0/24) のルートテーブルエントリをネクストホップとして持っています。

SD-WAN Overlay Route Tables



定義されたルートで **Citrix SD-WAN** トラフィックが一致する方法

Citrix SD-WAN で定義されたルートの照合プロセスは、宛先サブネットの最長のプレフィックス一致に基づきます (ルーターの操作に似ています)。ルートの具体性が高いほど、マッチングされるルートの変化が高くなります。ソートは次の順序で行われます。

1. 最長プレフィックス一致
2. コスト
3. サービス

したがって、/32 ルートは、常に /31 ルートの前にあります。2つの /32 ルートの場合、コスト 4 ルートは常にコスト 5 ルートの前にあります。2つの /32 コスト 5 ルートの場合、ルートは順序付けされた IP ホストに基づいて選択されます。サービスの順序は次のとおりです。ローカル、仮想パス、イントラネット、インターネット、パススルー、破棄。

例として、次の 2 つのルートを次のように考える。

- 192.168.1.0/24 コスト 5
- 192.168.1.64/26 コスト 10

192.168.1.65 ホスト宛てのパケットは、コストが高い場合でも、後者のルートを使用します。これに基づいて、パススルーサービスへのデフォルトルートなど、すべてのルートをキャッチする他のトラフィックと、Virtual Path オーバーレイを介して配信されるルートのみを設定を行うことが一般的です。

ルートは、同じプレフィックスを持つサイトノードルートテーブルで構成できます。タイブレークは、ルートコスト、サービスタイプ（仮想パス、イントラネット、インターネットなど）、およびネクストホップ IP に移動します。

Citrix SD-WAN ルーティングパケットフロー

- LAN から WAN（仮想パス）のトラフィックルート照合：
 1. 着信トラフィックは LAN インターフェイスによって受信され、処理されます。
 2. 受信したフレームは、最長プレフィクス一致のルートテーブルと比較されます。
 3. 一致が見つかった場合、フレームはルールエンジンによって処理され、フローデータベースにフローが作成されます。
- WAN から LAN（仮想パス）のトラフィックルート照合：
 1. 仮想パストラフィックはトンネルから SD-WAN によって受信され、処理されます。
 2. アプライアンスは、ソース IP アドレスを比較して、ソースがローカルであるかどうかを確認します。
 - 「はい」の場合：WAN は適格で、IP 宛先をルーティングテーブル/仮想パスに一致させます。
 - 「いいえ」の場合、WAN から WAN への転送が有効になります。
 3. (WAN から WAN への転送は無効) ローカルルートに基づいて LAN に転送します。
 4. (WAN から WAN への転送が有効) ルートテーブルに基づいて仮想パスに転送します。
- 非仮想パストラフィック：
 1. 着信トラフィックは LAN インターフェイスで受信され、処理されます。
 2. 受信したフレームは、最長プレフィクス一致のルートテーブルと比較されます。
 3. 一致が見つかった場合、フレームはルールエンジンによって処理され、フローデータベースにフローが作成されます。

Citrix SD-WAN ルーティングプロトコルのサポート

Citrix SD-WAN リリース 9.1 では、OSPF および BGP ルーティングプロトコルを構成に導入しました。SD-WAN にルーティングプロトコルを導入すると、ルーティングプロトコルがアクティブに使用されている、より複雑なアンダーレイネットワークに SD-WAN を簡単に統合できます。同じルーティングプロトコルを SD-WAN で有効にすると、SD-WAN オーバーレイを利用するように示すサブネットの設定が容易になりました。さらに、ルーティングプロトコルにより、SD-WAN サイトと非 SD-WAN サイト間の通信が可能になり、共通のルーティングプロトコルを使用して既存のカスタマーエッジルータに直接通信できます。アンダーレイネットワークで動作するルーティングプロトコルに参加する Citrix SD-WAN は、SD-WAN の展開モード（インラインモード、仮想インラインモード、エッジ/ゲートウェイモード）に関係なく実行できます。また、SD-WAN は「学習専用」モードで展開できます。この場

合、SD-WAN はルートを受信できますが、ルートをアンダーレイにアドバタイズすることはできません。これは、ルーティングインフラストラクチャが複雑または不確実であるネットワークに SD-WAN ソリューションを導入する場合に便利です。

重要

気をつけなければ、不要なルートを漏らすのは簡単です。

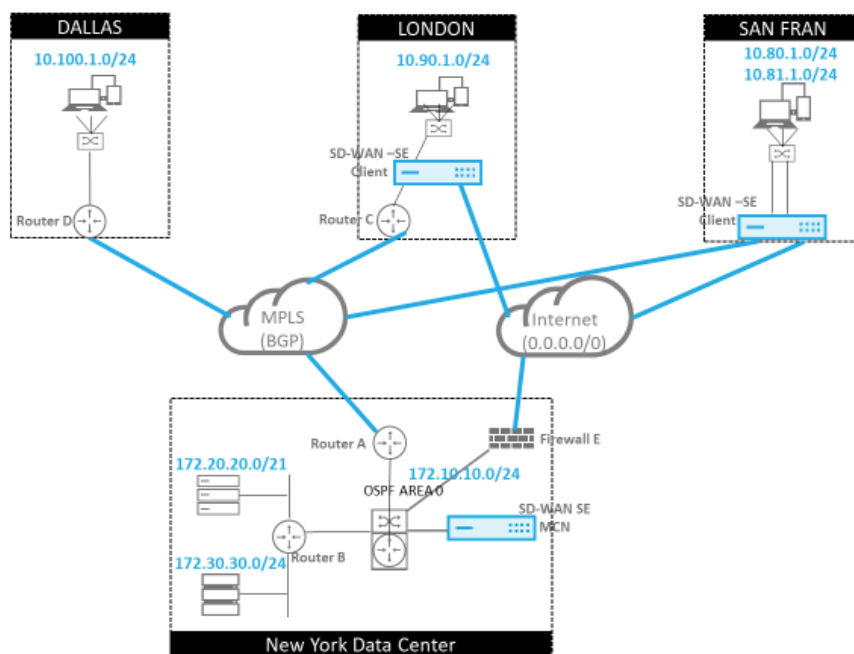
SD-WAN 仮想パスルートテーブルは、BGP（サイト間と考える）と同様に、外部ゲートウェイプロトコル（EGP）として機能します。たとえば、SD-WAN が SD-WAN アプライアンスから OSPF へのルートをアドバタイズする場合、通常はサイトおよびプロトコルの外部と見なされます。

注

インフラストラクチャ全体にわたって（WAN 経由で）IGP が存在する環境は、SD-WAN アドバタイズされたルートの使用方法が複雑になるため、注意してください。EIGRP は市場で広く使用されており、SD-WAN はそのプロトコルと相互運用できません。

SD-WAN 配置にルーティングプロトコルを導入する際の課題の 1 つは、SD-WAN サービスが有効になり、ネットワーク内で動作するまでルートテーブルを使用できないことです。そのため、最初に SD-WAN アプライアンスからのルートのアドバタイズを有効にすることは推奨されません。SD-WAN でルーティングプロトコルを段階的に導入するには、インポートフィルタとエクスポートフィルタを使用します。

私たちは、次の例を見直すことによって詳しく見てみましょう：



37 © 2017 Citrix

CITRIX

この例では、ルーティングプロトコルの使用例を調べます。前述のネットワークには、ニューヨーク、ダラス、ロンドン、サンフランシスコの 4 つの拠点があります。SD-WAN アプライアンスをこれらの 3 つの場所に導入し、SD-WAN を使用してハイブリッド WAN ネットワークを作成します。このネットワークでは、MPLS とインターネット WAN

リンクを使用して仮想化 WAN を提供します。ダラスには SD-WAN デバイスがないため、アンダーレイと SD-WAN オーバーレイネットワーク間の完全な接続を確保するために、そのサイトへの既存のルートプロトコルとの統合方法を検討する必要があります。

ネットワーク例では、MPLS ネットワーク上の 4 つのロケーションすべて間で eBGP が使用されます。各ロケーションには、独自の自律システム番号 (ASN) があります。

New York データセンターでは、コアデータセンターサブネットをリモートサイトにアドバタイズし、New York Firewall (E; ニューヨークファイアウォール) からのデフォルトルートをアナウンスするために OSPF が実行されています。この例では、ロンドン支店とサンフランシスコ支店にインターネットへのパスがあるにもかかわらず、すべてのインターネットトラフィックがデータセンターにバックホールされます。

また、サンフランシスコのサイトには、ルータがないことにも注意する必要があります。SD-WAN はエッジ/Gateway モードで展開され、そのアプライアンスはサンフランシスコサブネットのデフォルトゲートウェイであり、MPLS への eBGP にも参加します。

- New York データセンターでは、SD-WAN が仮想インラインモードで展開されていることに注意してください。この目的は、既存の OSPF ルーティングプロトコルに参加して、トラフィックを優先 Gateway としてアプライアンスに転送することです。
- London サイトは、従来のインラインモードで展開されます。アップストリーム WAN ルータ (C) は、引き続き London サブネットのデフォルト Gateway になります。
- サンフランシスコサイトはこのネットワークに新しく導入されたサイトであり、SD-WAN は Edge/Gateway モードで展開され、新しい San Francisco サブネットのデフォルトゲートウェイとして機能する予定です。

SD-WAN を実装する前に、既存のアンダーレイルートテーブルの一部を確認してください。

ニューヨークコアルータ B:

```
vyos@VYOS-ROUTER-B-CORE:~$ show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - ISIS, B - BGP, > - selected route, * - FIB route

O>* 0.0.0.0/0 [110/10] via 172.10.10.3, eth1, 00:08:56
O>* 10.90.1.0/24 [110/20] via 172.10.10.1, eth1, 00:21:02
O>* 10.100.1.0/24 [110/20] via 172.10.10.1, eth1, 00:21:02
C>* 127.0.0.0/8 is directly connected, lo
O 172.10.10.0/24 [110/10] is directly connected, eth1, 1d20h00m
C>* 172.10.10.0/24 is directly connected, eth1
C>* 172.20.20.0/24 is directly connected, eth2
C>* 172.30.30.0/24 is directly connected, eth3
C>* 192.168.65.0/24 is directly connected, eth0
```

ローカル New York サブネット (172.x.x.x) は、直接接続されたルータ B で使用でき、ルートテーブルから、デフォルトルートが 172.10.10.3 (ファイアウォール E) であることが特定されます。また、ダラス (10.90.1.0/24) とロンドン (10.100.1.0/24) のサブネットが 172.10.10.1 (MPLS ルータ A) を介して利用可能であることがわかります。ルートコストは、eBGP から学習されたことを示します。

注

この例では、サンフランシスコはルートとしてリストされていません。これは、SD-WAN のサイトをエッジ/ゲートウェイモードで展開していないためです。

```
vyos@VYATTA-ROUTER-A:~$ show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - ISIS, B - BGP, > - selected route, * - FIB route

O>* 0.0.0.0/0 [110/10] via 172.10.10.3, eth1, 00:09:52
B>* 10.90.1.0/24 [20/1] via 192.168.10.2, eth2, 1d23h09m
B>* 10.100.1.0/24 [20/1] via 192.168.10.3, eth2, 1d23h10m
C>* 127.0.0.0/8 is directly connected, lo
O 172.10.10.0/24 [110/10] is directly connected, eth1, 1d20h01m
C>* 172.10.10.0/24 is directly connected, eth1
O>* 172.20.20.0/24 [110/20] via 172.10.10.2, eth1, 00:21:58
O>* 172.30.30.0/24 [110/20] via 172.10.10.2, eth1, 00:21:58
C>* 192.168.10.0/24 is directly connected, eth2
O 192.168.65.0/24 [110/20] via 172.10.10.2, 1d19h57m
C>* 192.168.65.0/24 is directly connected, eth0
```

New York WAN ルータ (A) では、OSPF によって学習されたルートと、eBGP を介して MPLS 経由で学習されたルートがリストされます。工順コストに注意してください。BGP は、OSPF 110/10 と比較して、デフォルトで 20/1 の低い管理ドメインとコストです。

ダラス・ルータ **D**:

ダラス WAN ルータ (D) では、すべてのルートが MPLS 経由で学習されます。

```
vyos@VYATTA-ROUTER-D:~$ show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - ISIS, B - BGP, > - selected route, * - FIB route

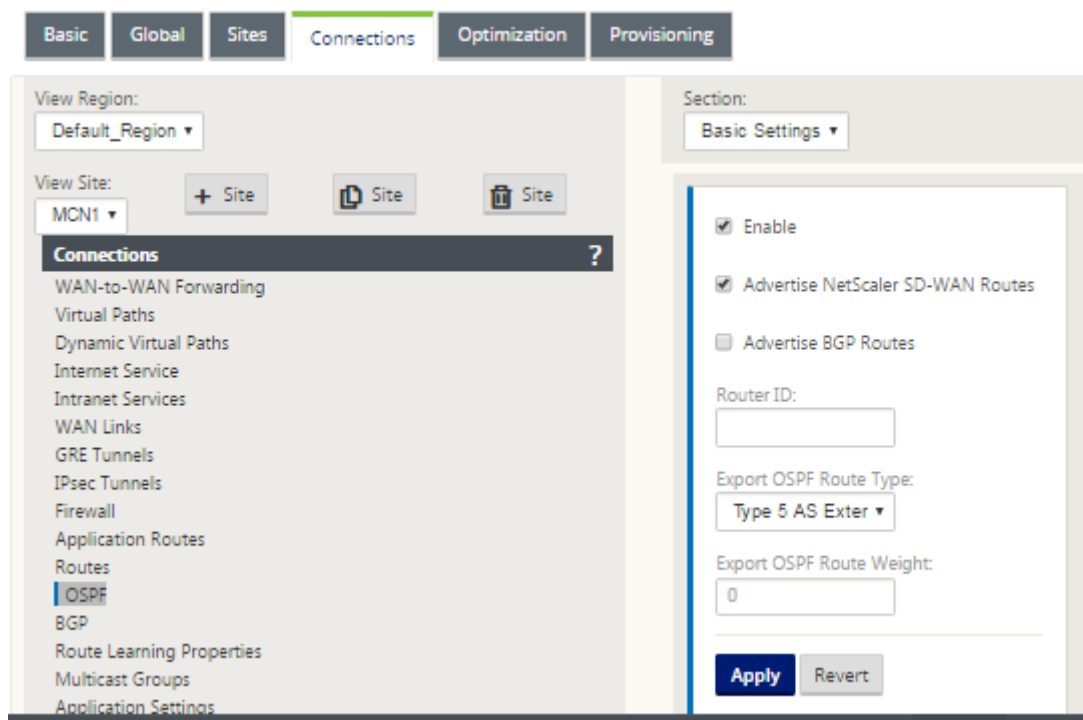
B>* 0.0.0.0/0 [20/10] via 192.168.10.1, eth2, 00:10:17
B>* 10.90.1.0/24 [20/1] via 192.168.10.2, eth2, 1d23h10m
C>* 10.100.1.0/24 is directly connected, eth1
C>* 127.0.0.0/8 is directly connected, lo
B>* 172.10.10.0/24 [20/1] via 192.168.10.1, eth2, 1d23h10m
B>* 172.20.20.0/24 [20/20] via 192.168.10.1, eth2, 00:22:17
B>* 172.30.30.0/24 [20/20] via 192.168.10.1, eth2, 00:22:17
C>* 192.168.10.0/24 is directly connected, eth2
C>* 192.168.65.0/24 is directly connected, eth0
```

注

この例では、192.168.65.0/24 サブネットを無視できます。これは管理ネットワークであり、この例には関連していません。すべてのルータは管理サブネットに接続されますが、どのルーティングプロトコルでもアドバタイズされません。

Citrix SD-WAN では、我々は、接続 > サイトの表示 > OSPF > 基本設定 の下で、ニューヨークのサイトにある

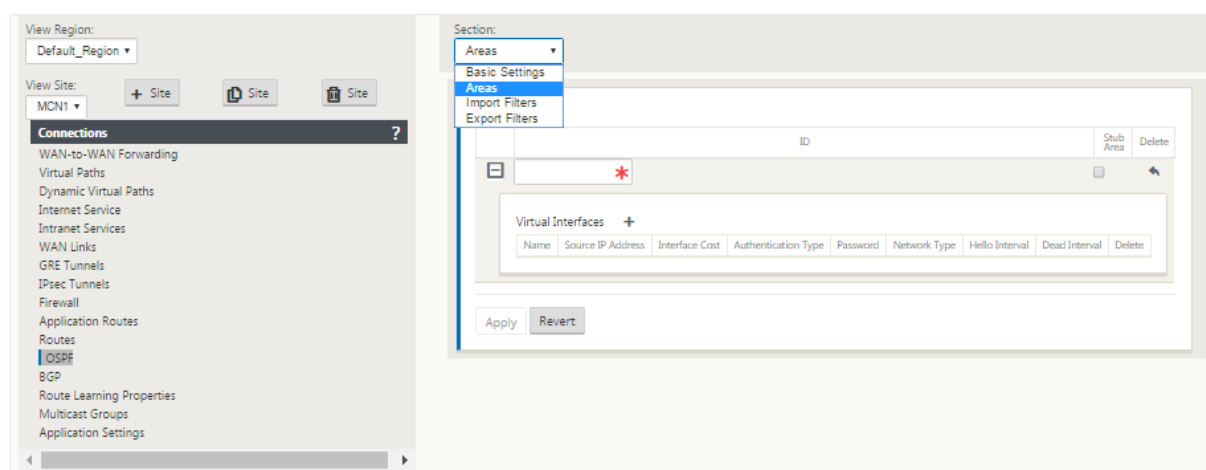
SD-WAN 上で **OSPF** を有効にすることにより、SD-WAN オーバーレイを追加することができます:



注

エクスポート **OSPF** ルートタイプは、デフォルトでタイプ 5 外部です。これは、SD-WAN ルーティングテーブルが OSPF プロトコルの外部と見なされるため、OSPF は内部（エリア内）で学習されたルートを優先するため、SD-WAN によってアドバタイズされるルートが優先されない可能性があるためです。

OSPF が WAN 全体（つまり MPLS ネットワーク）で使用されている場合、これをタイプ 1 のエリア内に変更できます。OSPF エリアは、次に示すように設定できます。



仮想インターフェイス（172.10.10.0）から派生したローカルネットワークで追加されたエリア 0 は、その他の設定はすべてデフォルトのままです。

新しい San Francisco サイトでは、eBGP は MPLS ネットワークに直接接続され、サイトのカスタマーエッジルートとして動作するため、有効にする必要があります。BGP は、[接続] > [サイトの表示] > [**BGP**] > [基本設定] で有効にできます。

自律システム番号 13 に注意してください。

Section: Basic Properties

☒ Enable

☒ Advertise NetScaler SD-WAN Routes

☐ Advertise OSPF Routes

Router ID:
192.168.10.4

Local Autonomous System:
13

Apply Revert

Section: Neighbors

Virtual Interface	Source IP	Neighbor IP	Neighbor AS	Hold Time(s)	Local Preference	BGP Metric	Multi Hop	Password	Delete
V1	192.168.10.4	192.168.10.1	65011	3600	100		<input checked="" type="checkbox"/>		

Policies +

Order	Network Address	BGP Community(AA:NN)	AS Path	BGP Policy	Direction	Delete
(auto)	<Manual>	<Manual>	*	<Accept>		

V1	192.168.10.4	192.168.10.2	65012	3600	100	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
----	--------------	--------------	-------	------	-----	-------------------------------------	-------------------------------------	--	--

Apply Refresh

eBGP は、他のロケーションとピアリングします。各 ASN は異なります。

仮想パスルーティングテーブルと、使用中のダイナミックルートプロトコルの間でルートがどのように渡されるかを理解することが重要です。ルーティンググループを作成したり、ルートをアドバタイズしたりするのは簡単です。フィルタメカニズムは、ルーティングテーブルに出入りする内容を制御する機能を提供します。各場所を順番に検討します。

- サンフランシスコロケーションには、2 つのローカルサブネット **10.80.1.0/24** と **10.81.1.0/24** があります。ダラスなどのサイトがアンダーレイネットワーク経由でサンフランシスコのサイトに到達し、ロンドンやニューヨークなどのサイトが Virtual Path オーバーレイネットワーク経由でサンフランシスコに到達できるように、eBGP を通じてこれらのサイトを宣伝したいと考えています。また、SD-WAN 仮想パスオーバーレイがダウンし、環境が MPLS だけの使用にフォールバックする必要がある場合に備えて、すべてのサイトへの

eBGP 到達可能性について学習します。また、SD-WAN が eBGP から SD-WAN ルータに学習する内容を再評価する必要もありません。このためには、フィルタを次のように構成する必要があります。

- eBGP からすべてのルートをインポートします。SD-WAN アプライアンスにルートを再読み込み/エクスポートしないでください。

Order	Source Router	Destination	Prefix	Next Hop	Protocol	Route Tag	Cost	AS Path Length	Include	Enabled	Delete	Clone
100	*	<Manual>	eq *	*	Any	*	eq *	eq *	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
<div><input type="checkbox"/> Export Route to Citrix Appliances Citrix SD-WAN Cost: 6 Service Type: Local Service Name: <None> <input type="checkbox"/> Eligibility Based On Gateway Path: <None></div>												
200	*	<Manual>	eq *	*	Any	*	eq *	eq *	<input checked="" type="checkbox"/>	<input type="checkbox"/>		
200	*	<Manual>	eq *	*	Any	*	eq *	eq *	<input type="checkbox"/>	<input checked="" type="checkbox"/>		

Apply Revert

- ローカルルートを eBGP にエクスポートする

エクスポートのデフォルトのルールは、すべてをエクスポートすることです。ルール 200 は、ルートを再検証しないようにフォールトルールを上書きするために使用されます。任意のプレフィクス SD-WAN に一致するすべてのルートが、仮想パスを通して学習しました。

Order	Network Address	Prefix	NetScaler SD-WAN Cost	Service Type	Site/Service Name	Gateway IP Address	Include	Enabled	Delete	Clone
100	<Manual> *	eq 24	eq *	Local	<Any>	*	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
200	<Manual> 0.0.0.0	eq *	eq *	Any	<Any>	*	<input type="checkbox"/>	<input checked="" type="checkbox"/>		
(auto)	<Manual> *	eq *	eq *	Any	<Any>	*	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		

Citrix SD-WAN アプライアンスを展開した後、ダラスサイトにある BGP ルータのルートテーブルをリフレッシュできます。10.80.1.0/24 および 10.81.1.0/24 サブネットが、サンフランシスコ SD-WAN からの eBGP を介して正しく認識されていることがわかります。

ダラスルータ **D**:

```
vyos@VYATTA-ROUTER-D:~$ show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
      I - ISIS, B - BGP, > - selected route, * - FIB route

B>* 0.0.0.0/0 [20/10] via 192.168.10.1, eth2, 00:00:01
B>* 10.80.1.0/24 [20/0] via 192.168.10.4, eth2, 3d19h07m
B>* 10.81.1.0/24 [20/0] via 192.168.10.4, eth2, 3d19h07m
B>* 10.90.1.0/24 [20/1] via 192.168.10.2, eth2, 4d23h38m
C>* 10.100.1.0/24 is directly connected, eth1
C>* 127.0.0.0/8 is directly connected, lo
B>* 172.10.10.0/24 [20/1] via 192.168.10.1, eth2, 4d23h38m
B>* 172.20.20.0/24 [20/20] via 192.168.10.1, eth2, 00:00:01
B>* 172.30.30.0/24 [20/20] via 192.168.10.1, eth2, 00:00:01
B 192.168.10.0/24 [20/0] via 192.168.10.4 inactive, 3d19h07m
C>* 192.168.10.0/24 is directly connected, eth2
C>* 192.168.65.0/24 is directly connected, eth0
```

さらに、Citrix SD-WAN ルートテーブルは、[モニタリング] > [統計] > [ルートの表示] ページで確認できます。

サンフランシスコの **Citrix SD-WAN**:

Routes for routing domain : Default_RoutingDomain

Filter: in Any column Apply

Show 100 entries Showing 1 to 16 of 16 entries

Num	Network Addr	Gateway IP Address	Service	Reachable	Site IP Address	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
0	10.81.1.0/24	10.80.1.20	Local	YES	*	SFO	Static	-	-	5	0	YES	N/A	N/A
1	10.80.1.0/24	*	Local	YES	*	SFO	Static	-	-	5	0	YES	N/A	N/A
2	192.168.10.0/24	*	Local	YES	*	SFO	Static	-	-	5	122	YES	N/A	N/A
3	172.10.10.0/24	*	NYC-SFO	YES	*	NYC	Static	-	-	5	0	YES	N/A	N/A
4	172.30.30.0/24	192.168.10.1	Local	YES	*	SFO	Dynamic	BGP	-	6	0	YES	N/A	N/A
5	172.20.20.0/24	192.168.10.1	Local	YES	*	SFO	Dynamic	BGP	-	6	0	YES	N/A	N/A
6	172.10.10.0/24	192.168.10.1	Local	YES	*	SFO	Dynamic	BGP	-	6	0	YES	N/A	N/A
7	10.100.1.0/24	192.168.10.3	Local	YES	*	SFO	Dynamic	BGP	-	6	0	YES	N/A	N/A
8	10.90.1.0/24	192.168.10.2	Local	YES	*	SFO	Dynamic	BGP	-	6	0	YES	N/A	N/A
9	172.20.20.0/24	*	NYC-SFO	YES	*	NYC	Dynamic	Virtual WAN	YES	6	0	YES	N/A	N/A
10	10.100.1.0/24	*	NYC-SFO	YES	*	NYC	Dynamic	Virtual WAN	YES	6	0	YES	N/A	N/A
11	172.30.30.0/24	*	NYC-SFO	YES	*	NYC	Dynamic	Virtual WAN	YES	6	0	YES	N/A	N/A
12	0.0.0.0/0	192.168.10.1	Local	YES	*	SFO	Dynamic	BGP	-	6	0	YES	N/A	N/A
13	0.0.0.0/0	*	NYC-SFO	YES	*	NYC	Dynamic	Virtual WAN	YES	6	0	YES	N/A	N/A
14	0.0.0.0/0	*	Passthrough	YES	*	*	Static	-	-	16	0	YES	N/A	N/A
15	0.0.0.0/0	*	Discard	YES	*	*	Static	-	-	16	0	YES	N/A	N/A

Showing 1 to 16 of 16 entries

Citrix SD-WAN は、仮想パスオーバーレイを介して利用可能なルートを含め、学習されたすべてのルートを表示します。

私たちは、ニューヨークのデータセンターにある 172.10.10.0/24 を考えてみましょう。このルートは、次の 2 つの方法で学習されています。

- 仮想パスルート（番号 3）として、サービス = コストが 5 の NYC-SFO で、static と入力します。これは、ニューヨークの SD-WAN アプライアンスによってアドバタイズされるローカルサブネットです。アプライアンスに直接接続されているか、または設定に入力された手動スタティックルートであるという点ではスタティックです。サイト間の仮想パスが稼働状態/稼働状態にあるため、到達可能です。

- BGP（番号 6）を介してアドバタイズされたルートとして、コストは 6 です。これは現在、フォールバックルートと見なされます。

プレフィクスが等しく、コストが異なるため、SD-WAN は仮想パスルートを使用できない限り、仮想パスルートを使用します。この場合、フォールバックルートは BGP を介して学習されます。

さて、ルート 172.20.20.0/24 を考えてみましょう。

- これは仮想パスルート（番号 9）として学習されますが、ダイナミックタイプでコストは 6 です。これは、リモート SD-WAN アプライアンスがルーティングプロトコル（この場合は OSPF）を介してこのルートを学習したことを意味します。デフォルトでは、ルートコストは高くなります。
- SD-WAN は、同じコストで BGP を介してこのルートを学習します。したがって、この場合、このルートは仮想パスルートよりも優先されます。

正しいルーティングを確保するには、BGP ルートコストを増やして、仮想パスルートがあり、それが優先ルートであるかどうかを確認する必要があります。これは、インポートフィルタのルートウェイトをデフォルトの 6 よりも大きく調整することで実行できます。

The screenshot shows the 'Import Filter' configuration window. The 'NetScaler SD-WAN Cost' is set to 10. The 'Service Type' is set to 'Local'. The 'Eligibility Based On Gateway' checkbox is checked. The 'Path' is set to '<None>'. The 'Apply' button is highlighted.

調整を行った後、San Francisco アプライアンスの SD-WAN ルートテーブルを更新して、調整されたルートコストを確認できます。フィルタオプションを使用して、表示されているリストにフォーカスします。

Routes for routing domain : Default_RoutingDomain

Filter: 172.20.20.0/24 in Any column Apply

Show 100 entries Showing 1 to 2 of 2 entries (filtered from 16 total entries)

Num	Network Addr	Gateway IP Address	Service	Reachable	Site IP Address	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
5	172.20.20.0/24	*	NYC-SFO	YES	*	NYC	Dynamic	Virtual WAN	YES	6	0	YES	N/A	N/A
8	172.20.20.0/24	192.168.10.1	Local	YES	*	SFO	Dynamic	BGP	-	10	0	YES	N/A	N/A

Showing 1 to 2 of 2 entries (filtered from 16 total entries)

最後に、サンフランシスコ SD-WAN で学習されたデフォルトルートを見てみましょう。私たちは、すべてのインターネットトラフィックをニューヨークにバックホールしたいと考えています。仮想パスを使用して送信するか、またはフォールバックとして MPLS ネットワークを介して送信することがわかります。

Routes for routing domain : Default_RoutingDomain

Filter: 0.0.0.0/0 in Any column Apply

Show 100 entries Showing 1 to 4 of 4 entries (filtered from 16 total entries)

Num	Network Addr	Gateway IP Address	Service	Reachable	Site IP Address	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
12	0.0.0.0/0	*	NYC-SFO	YES	*	NYC	Dynamic	Virtual WAN	YES	6	0	YES	N/A	N/A
13	0.0.0.0/0	192.168.10.1	Local	YES	*	SFO	Dynamic	BGP	-	10	0	YES	N/A	N/A
14	0.0.0.0/0	*	Passthrough	YES	*	*	Static	-	-	16	0	YES	N/A	N/A
15	0.0.0.0/0	*	Discard	YES	*	*	Static	-	-	16	0	YES	N/A	N/A

Showing 1 to 4 of 4 entries (filtered from 16 total entries)

また、コスト 16 のパススルーおよび廃棄ルートも表示されます。これらは、削除できない自動ルートです。デバイスがインラインの場合、パススルールートは最後の手段として使用されるため、パケットをより特定のルートと照合できない場合、SD-WAN はそのパケットをインターフェイスグループのネクストホップに渡します。SD-WAN がパス外またはエッジ/ゲートウェイモードの場合、パススルーサービスは存在しません。この場合、SD-WAN はデフォルトの廃棄ルートを使用してパケットをドロップします。Hit Count は、各ルートにヒットしているパケットの数を示します。このパケットは、トラブルシューティングの際に役立ちます。

ここでは、ニューヨークのサイトに焦点を当て、仮想パスがアクティブなときに、リモートサイト（ロンドンとサンフランシスコ）宛てのトラフィックを SD-WAN アプライアンスに転送します。

New York のサイトには、複数のサブネットがあります。

- 172.10.10.0/24（直接接続）
- 172.20.20.0/24（コアルータ B から OSPF 経由でアドバタイズされる）
- 172.30.30.0/24（コアルータ B から OSPF 経由でアドバタイズされる）

また、MPLS を介してダラス（10.100.1.0/24）へのトラフィックフローを提供する必要があります。

最後に、すべてのインターネット接続トラフィックが 172.10.10.3 を経由して、ネクストホップとしてファイアウォール E にルーティングされるようにします。SD-WAN は、OSPF を介してこのデフォルトルートを学習し、仮想パスを介してアドバタイズします。ニューヨークのサイトのフィルタは次のとおりです。

Order	Source Router	Destination	Prefix	Next Hop	Protocol	Cost	Include	Enabled	Delete	Clone
100	*	<Manual> 192.168.65.0/24	eq *	*	Any	eq *	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<div><input type="checkbox"/> Export Route to Citrix Appliances</div> <div><input type="checkbox"/> Eligibility Based On Gateway</div> <div>NetScaler SD-WAN Cost: 6</div> <div>Service Type: Local</div> <div>Service Name:</div> <div><input type="checkbox"/> Eligibility Based On Path</div> <div>Path: <None></div>										
200	*	<Manual> 192.168.10.0/24	eq *	*	Any	eq *	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
300	*	<Manual> *	eq *	*	Any	eq *	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(auto)	*	<Manual> *	eq *	*	Any	eq *	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

New York SD-WAN サイトは、管理ネットワークのすべてのルートをインポートします。これは無視してもかまいません。フィルタ 200 に集中できます。

200 * <Manual> 192.168.10.0/24 eq * * Any eq * [check] [check] [trash] [clone]

☐ Export Route to Citrix Appliances ☐ Eligibility Based On Gateway

NetScaler SD-WAN Cost: 6 Service Type: Local Service Name:

☐ Eligibility Based On Path

Path: <None>

フィルタ 200 は、到達可能性のために 192.168.10.0/24 (MPLS コア) をインポートするために使用されますが、仮想パスにはエクスポートされません。[含める] チェックボックスをオンにし、[Citrix アプライアンスへのルートをエクスポート] チェックボックスがオフになっていることを確認します。その後、他のすべてのルートが含まれます。

エクスポートフィルタでは、192.168.10.0/24 のルートを除外できます。これは、サンフランシスコサイト内で直接接続されたサブネットとして、このルートをソースでフィルタリングできないため、この終端では抑制されるためです。

	Order	Network Address	Prefix	NetScaler SD-WAN Cost	Service Type	Site/Service Name	Gateway IP Address	Include	Enabled	Delete	Clone
[+]	100	<Manual> 192.168.10.0/24	eq *	eq *	Any	<Any>	*	<input type="checkbox"/>	<input checked="" type="checkbox"/>	[trash]	[clone]
	(auto)	<Manual> *	eq *	eq *	Any	<Any>	*	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		

次に、New York サイトのコアルートから更新されたルートテーブルを確認してみましょう。

ニューヨークルータ B:

```
vyos@VYOS-ROUTER-B-CORE:~$ show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
      I - ISIS, B - BGP, > - selected route, * - FIB route

O>* 0.0.0.0/0 [110/10] via 172.10.10.3, eth1, 4d22h22m
O>* 10.80.1.0/24 [110/15] via 172.10.10.10, eth1, 3d19h49m
O>* 10.81.1.0/24 [110/15] via 172.10.10.10, eth1, 3d19h49m
O>* 10.90.1.0/24 [110/15] via 172.10.10.10, eth1, 3d19h50m
O>* 10.100.1.0/24 [110/20] via 172.10.10.1, eth1, 4d22h22m
C>* 127.0.0.0/8 is directly connected, lo
O 172.10.10.0/24 [110/10] is directly connected, eth1, 4d22h22m
C>* 172.10.10.0/24 is directly connected, eth1
C>* 172.20.20.0/24 is directly connected, eth2
C>* 172.30.30.0/24 is directly connected, eth3
C>* 192.168.65.0/24 is directly connected, eth0
```

サンフランシスコ (10.80.1.0 および 10.81.1.0) およびロンドン (10.90.1.0) のサブネットが、New York SD-WAN アプライアンス (172.10.10.10) を介してアドバタイズされていることがわかります。ルート 10.100.1.0/24 は、まだアンダーレイ MPLS ルータ A を介してアドバタイズされています。ここでは、New York サイトの SD-WAN ルートテーブルを確認します。

ニューヨークのサイト **SD-WAN** ルートテーブル:

Routes for routing domain : Default_RoutingDomain

Filter: in Any column

Show 100 entries Showing 1 to 11 of 11 entries

Num	Network Addr	Gateway IP Address	Service	Reachable	Site IP Address	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
0	172.10.10.0/24	*	Local	YES	*	NYC	Static	-	-	5	0	YES	N/A	N/A
1	10.90.1.0/24	*	NYC-LON	YES	*	LON	Static	-	-	5	0	YES	N/A	N/A
2	10.81.1.0/24	10.80.1.20	NYC-SFO	YES	*	SFO	Static	-	-	5	0	YES	N/A	N/A
3	10.80.1.0/24	*	NYC-SFO	YES	*	SFO	Static	-	-	5	0	YES	N/A	N/A
4	192.168.10.0/24	*	NYC-SFO	YES	*	SFO	Static	-	-	5	0	YES	N/A	N/A
5	172.30.30.0/24	172.10.10.2	Local	YES	*	NYC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
6	172.20.20.0/24	172.10.10.2	Local	YES	*	NYC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
7	10.100.1.0/24	172.10.10.1	Local	YES	*	NYC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
8	0.0.0.0/0	172.10.10.3	Local	YES	*	NYC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
9	0.0.0.0/0	*	Passthrough	YES	*	*	Static	-	-	16	0	YES	N/A	N/A
10	0.0.0.0/0	*	Discard	YES	*	*	Static	-	-	16	0	YES	N/A	N/A

OSPF を介して学習されたローカルサブネット、MPLS ルータ A から学習されたダラスサイトへのルート、およびサンフランシスコサイトとロンドンサイトのリモートサブネットの両方の正しいルートを確認できます。MPLS ルータ A を見てみましょう。このルータは OSPF および BGP に参加しています。

```
vyos@VYATTA-ROUTER-A:~$ show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
I - ISIS, B - BGP, > - selected route, * - FIB route

O>* 0.0.0.0/0 [110/10] via 172.10.10.3, eth1, 00:04:12
O 10.80.1.0/24 [110/15] via 172.10.10.10, 00:04:13
B>* 10.80.1.0/24 [20/0] via 192.168.10.4, eth2, 00:05:09
O 10.81.1.0/24 [110/15] via 172.10.10.10, 00:04:13
B>* 10.81.1.0/24 [20/0] via 192.168.10.4, eth2, 00:05:09
O 10.90.1.0/24 [110/15] via 172.10.10.10, 00:04:13
B>* 10.90.1.0/24 [20/1] via 192.168.10.2, eth2, 00:05:11
S>* 10.90.1.10/32 [5/0] via 192.168.10.2, eth2
B>* 10.100.1.0/24 [20/1] via 192.168.10.3, eth2, 00:04:28
C>* 127.0.0.0/8 is directly connected, lo
O 172.10.10.0/24 [110/10] is directly connected, eth1, 00:05:24
C>* 172.10.10.0/24 is directly connected, eth1
O>* 172.20.20.0/24 [110/20] via 172.10.10.2, eth1, 00:04:12
O>* 172.30.30.0/24 [110/20] via 172.10.10.2, eth1, 00:04:12
B 192.168.10.0/24 [20/0] via 192.168.10.4 inactive, 00:05:09
C>* 192.168.10.0/24 is directly connected, eth2
O 192.168.65.0/24 [110/20] via 172.10.10.2, 00:04:12
C>* 192.168.65.0/24 is directly connected, eth0
```

ルートテーブルから、このルータ A は BGP および OSPF を介してリモートサブネットを学習しています。BGP ルートのアドミニストレーティブディスタンスとコスト (20/5) が OSPF (110/10) よりも低いため、優先されます。この例では、コアルートが 1 つしかないネットワークでは、これは問題にならない可能性があります。ただし、ここに着信するトラフィックは、SD-WAN アプライアンス (172.10.10.10) に送信されるのではなく、MPLS ネットワーク経由で配信されます。ルーティングの対称性を完全に維持する場合は、eBGP 経由で学習したルートではなく、172.10.10.10 からのルートからのルート優先が得られるように、AD/メトリックコストを調整するルートマップが必要です。

また、「バックドア」ルートを設定して、ルータが BGP ルート経由で OSPF ルートを優先するようにすることもできます。SD-WAN 仮想 IP アドレスがロンドンサイトの SD-WAN アプライアンスへのスタティックルートに注目してください。

```
S>* 10.90.1.10/32 [5/0] via 192.168.10.2, eth2
```

これは、MPLS パスがダウンした場合に、仮想パスが New York サイトの SD-WAN アプライアンスに再ルーティングされるようにするために必要です。10.90.1.0/24 のルートが 172.10.10.10（ニューヨーク SD-WAN）経由でアドバタイズされるためです。また、仮想パスがそれ自体に戻らないように、SD-WAN アプライアンスで UDP 4,980 パケットをドロップするオーバーライドサービスルールを作成することをお勧めします。

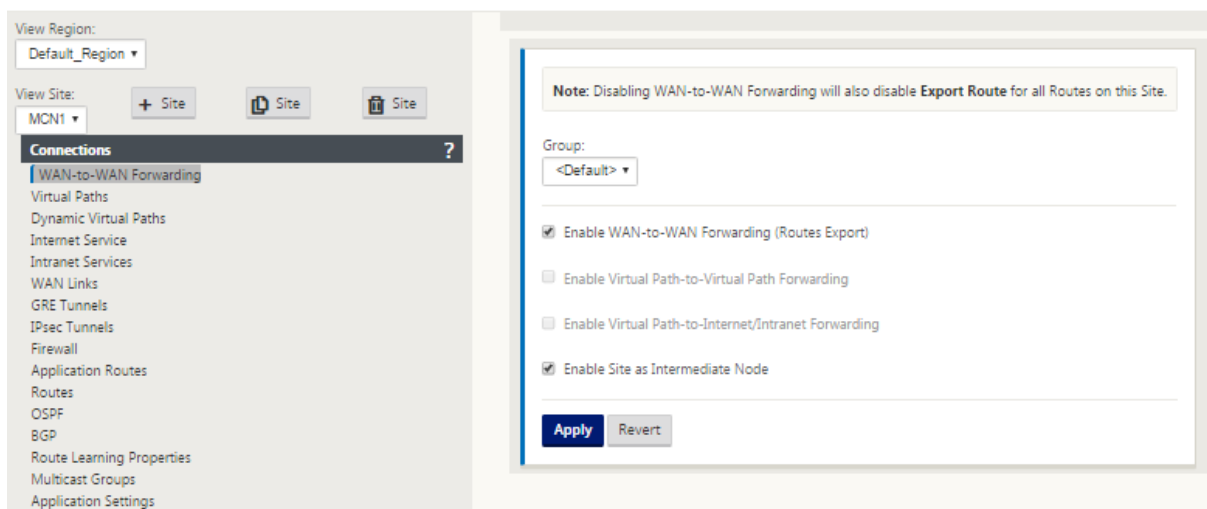
動的仮想パス

動的仮想パスは、2 つのクライアントノード間で許可され、2 つのサイト間で直接通信するためのオンデマンド仮想パスを構築できます。動的仮想パスの利点は、MCN または 2 つの仮想パスを通過することなく、トラフィックが 1 つのクライアントノードから 2 番目のクライアントノードに直接フローできることです。これにより、トラフィックフローにレイテンシーが増える可能性があります。動的仮想パスは、ユーザー定義のトラフィックしきい値に基づいて動的に構築および削除されます。これらのしきい値は、パケット/秒 (pps) または帯域幅 (kbps) のいずれかとして定義されます。この機能により、ダイナミックフルメッシュ SD-WAN オーバーレイトポロジが可能になります。

動的仮想パスのしきい値が満たされると、クライアントノードは、サイト間で利用可能なすべての WAN パスを使用して相互の仮想パスを動的に作成し、次のようにそのパスをフル活用します。

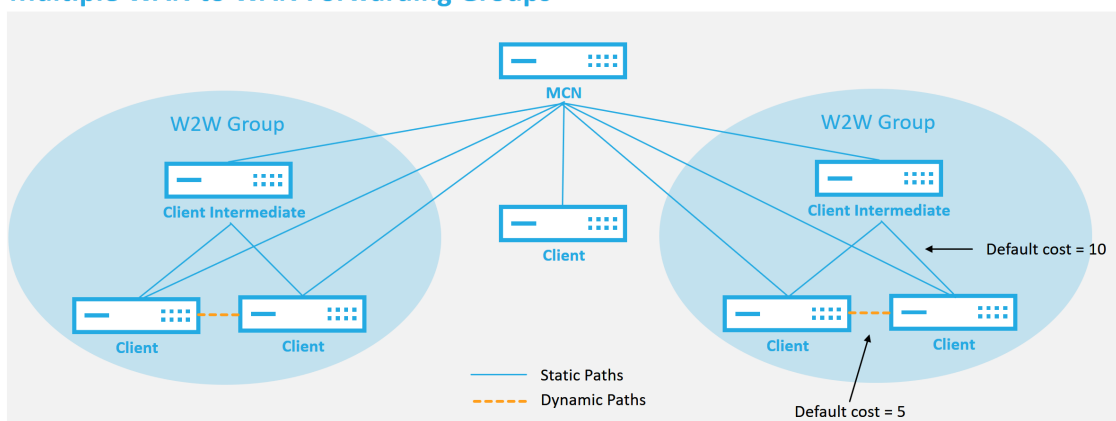
- バルクデータが存在する場合は送信し、損失がないことを確認し、
- 対話型データを送信し、損失がないことを確認してから
- バルクデータおよびインタラクティブデータが安定していると見なされた後にリアルタイムデータを送信する（損失なし、許容レベルなし）
- 一括データまたは対話型データがない場合、動的仮想パスが一定期間安定した後、リアルタイムデータを送信する
- ユーザーデータがユーザー定義の期間に設定されたしきい値を下回ると、動的仮想パスは破棄されます。

動的仮想パスには、中間サイトの概念があります。中間サイトは、MCN サイト、または静的仮想パスが構成され、2 つ以上の他のクライアントノードに接続されているネットワーク内の他のサイトです。もう 1 つの設計上の考慮事項の要件は、WAN-to-WAN 転送を有効にして、すべてのサイトからのすべてのルートを動的仮想パスが必要なクライアントノードにアドバタイズできるようにすることです。クライアントノード通信を監視し、動的パスを確立して切断する必要がある時期を指示するには、この中間サイトに対して WAN ツー WAN 転送に加えて、【サイトを中間ノードとして有効にする】を有効にする必要があります。



SD-WAN 構成では複数の WAN-to-WAN フォワーディンググループを使用できるため、特定のクライアントノード間のパス確立に対するフルコントロールが可能になります。

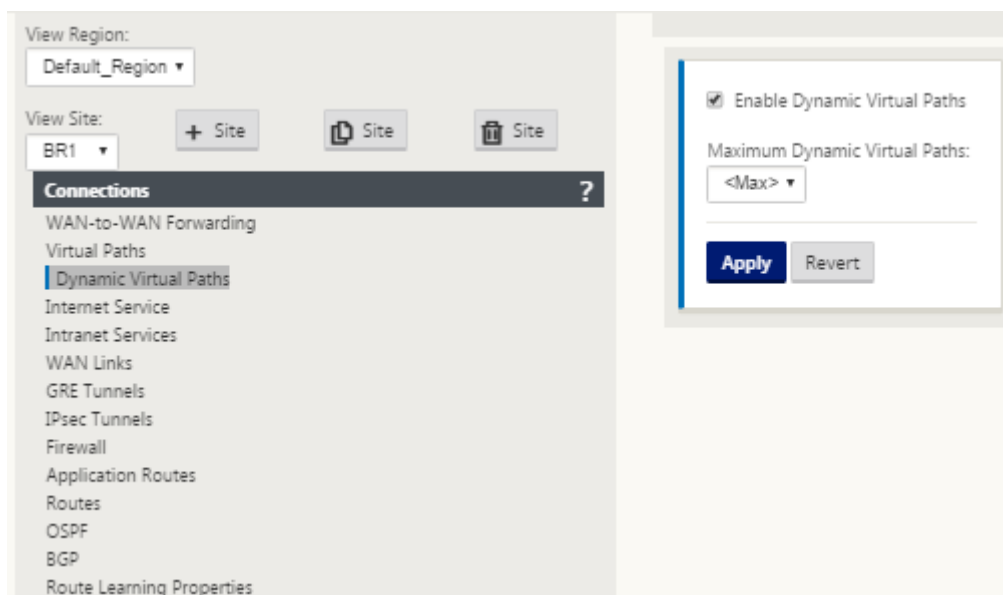
Multiple WAN to WAN Forwarding Groups



WAN to WAN Forwarding Group:

- A network can have multiple WAN to WAN Forwarding Groups
- Direct dynamic path will have a lower cost than through the intermediate node

クライアントノードを中間サイトとして動作させるには、その **WAN-to-WAN** フォワーディンググループに関連付けられているクライアントとの間で、静的な仮想パスを構成する必要があります。さらに、クライアントノードでは、クライアントノードごとに [動的仮想パスの有効化] オプションをオンにする必要があります。



各 SD-WAN デバイスには、それぞれ固有のルートテーブルがあり、各ルートに次の詳細が定義されています。

- Num: 一致プロセスに基づくこのアプライアンスのルートの順序（最下位の Num が最初に処理される）
- ネットワーク・アドレス: サブネットまたはホスト・アドレス
- 必要に応じてゲートウェイ
- サービス: このルートに適用されるサービス
- ファイアウォールゾーン—ルートのファイアウォールゾーン分類
- 到達可能: このサイトの仮想パスの状態がアクティブ
- サイトルートが存在することが予想されるサイトの名前
- Type: ルートタイプの識別（スタティックまたはダイナミック）
- ネイバーダイレクト
- コスト-特定のルートのコスト
- [Hit Count]: パケットごとにルートが使用された回数。これは、ルートが正しくヒットしていることを確認するために使用されます。
- 対象外
- 適格性タイプ
- 適格性値

次に、SD-WAN サイトルートテーブルの例を示します。

Routes for routing domain : Default_RoutingDomain

Filter: in Any column Apply

Show 100 entries Showing 1 to 13 of 13 entries

First Previous 1 Next Last

Num	Network Addr	Gateway IP Address	Service	Firewall Zone	Reachable	Site IP Address	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
0	172.16.10.0/24	192.168.15.1	DC-AWS	Default_LAN_Zone	YES	*	DC	Static	-	-	4	0	YES	N/A	N/A
1	192.168.100.0/24	*	Local	Default_LAN_Zone	YES	*	AWS	Static	-	-	5	0	YES	N/A	N/A
2	192.168.15.0/24	*	DC-AWS	Default_LAN_Zone	YES	*	DC	Static	-	-	5	0	YES	N/A	N/A
3	172.16.250.0/24	*	DC-AWS	Default_LAN_Zone	YES	*	DC	Static	-	-	5	0	YES	N/A	N/A
4	172.16.150.0/24	*	DC-AWS	Default_LAN_Zone	YES	*	DC	Static	-	-	5	0	YES	N/A	N/A
5	192.168.200.0/24	*	DC-AWS	Default_LAN_Zone	NO	*	Azure	Static	-	-	15	0	YES	N/A	N/A
6	192.168.10.0/24	*	DC-AWS	Default_LAN_Zone	YES	*	Branch	Static	-	-	15	0	YES	N/A	N/A
7	172.16.200.0/24	*	DC-AWS	Default_LAN_Zone	YES	*	Branch	Static	-	-	15	0	YES	N/A	N/A
8	172.16.100.0/24	*	DC-AWS	Default_LAN_Zone	YES	*	Branch	Static	-	-	15	0	YES	N/A	N/A
9	172.16.30.0/24	*	DC-AWS	Default_LAN_Zone	YES	*	Branch	Static	-	-	15	0	YES	N/A	N/A
10	0.0.0.0/0	*	Internet	Untrusted_Internet_Zon	YES	*	*	Static	-	-	5	1	YES	N/A	N/A
11	0.0.0.0/0	*	Passthrough	Any	YES	*	*	Static	-	-	16	0	YES	N/A	N/A
12	0.0.0.0/0	*	Discard	Any	YES	*	*	Static	-	-	16	0	YES	N/A	N/A

Showing 1 to 13 of 13 entries

First Previous 1 Next Last

前述の SD-WAN ルートテーブルから、従来のルータでは通常使用できない要素が増えています。最も注目すべきは「到達可能」列です。この列は、WAN パスの状態に応じて、ルートをアクティブまたは非アクティブ（yes/no）にします。ここにリストされているルートは、サービスのさまざまな状態（例として仮想パスがダウンしている）に基づいて抑制されます。ルートを強制的に不適格にする可能性があるその他のイベントには、パスダウン状態、ネクストホップ到達不能、または WAN リンクダウンがあります。

前の表から、14 の定義されたルートを見ることができます。ルートまたはルートのグループの説明は、次のように記述されます。

- Route 0: MCN では、これは DC サイトに存在するホストサブネットルートです。172.16.10.0/24 は DC LAN にあり、192.168.15.1 は LAN 上の Gateway で、そのサブネットに到達するネクストホップです。
- Route 1: ルートテーブルを表示するこの SD-WAN デバイスへのローカルルートです。
- Route 2—4: DC サイト SD-WAN 用に設定された仮想インターフェイスの一部であるサブネットです。これらのサブネットは、定義された信頼された仮想インターフェイスから派生します。
- Route 5: これは、MCN によって共有される別のクライアントノードへの共有ルートで、そのサイトと MCN 間の仮想パスがダウンしているため、到達可能性ステータスが No です。
- Route 6—9: これらのルートは、別のクライアントサイトに存在します。このルートでは、仮想パス上のリモートサイト宛での WAN 入力トラフィックを照合するために、仮想パスルートが作成されます。
- Route 10 —インターネットサービスが定義されている場合、システムは、このローカルサイトの直接インターネットブレイクアウトのキャッチオールルートを追加します。
- Route 11: パススルーは、既存のルートに一致しない場合にパケットが通過できるようにシステムによって常に追加されるデフォルトのルートです。パススルーはクリーンアップされません。通常、ローカルブロードキャストと ARP トラフィックはこのサービスにマッピングされます。
- Route 12: Discard は、未定義のものをドロップするためにシステムによって常に追加されるデフォルトのルートです。

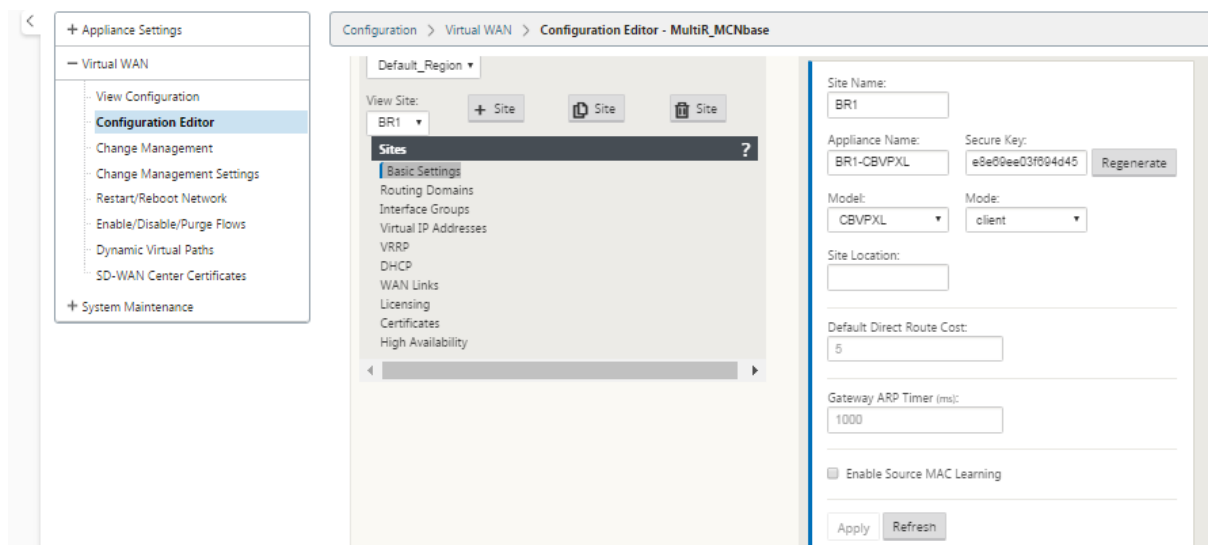
デフォルトのルートコスト値:

- WAN から WAN への転送—10
- デフォルトの直接ルートコスト—5
- 自動生成されたルート—5
- 仮想パス—5
- ローカル—5
- イントラネット—5
- インターネット—5
- パススルー—5
- オプション：ルートはサービスレベルとして定義される 0.0.0.0/0 です。

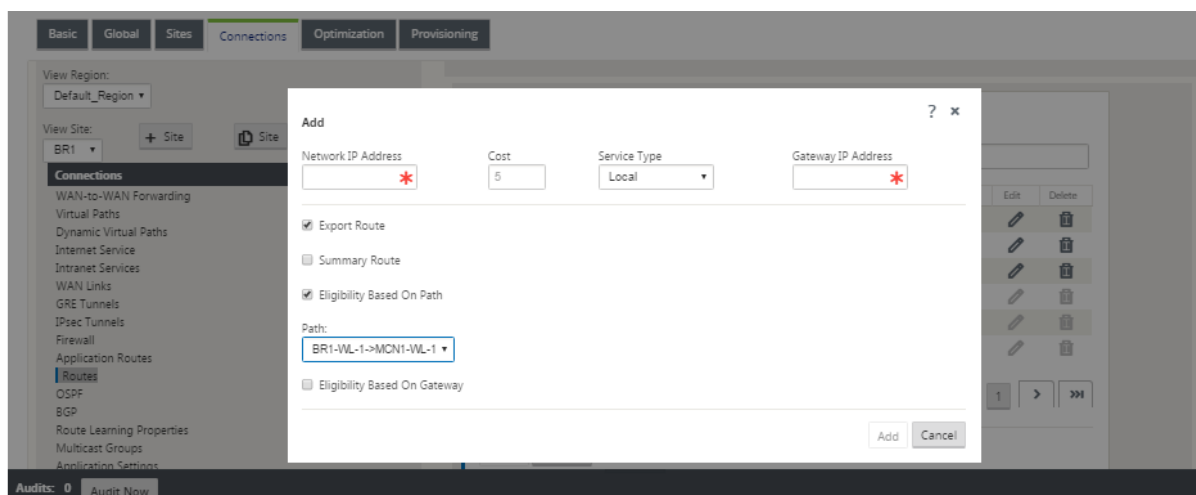
これらのルートを定義したら、定義されたルートを使用してトラフィックがどのように流れるかを理解することが重要です。これらのトラフィックフローは、次のフローに分割されます。

- LAN から WAN（仮想パス）：SD-WAN オーバーレイトンネルに入るトラフィック
- WAN から LAN（仮想パス）：SD-WAN オーバーレイトンネルに存在するトラフィック
- 非仮想パストラフィック：アンダーレイネットワークにルーティングされるトラフィック

デフォルトのルートコストは、サイトごとに変更できます。構成は、[サイトの表示] > [基本設定] で確認できます。



スタティックルートは、[接続] > [サイト] > [ルート] ノードで サイトごとに定義できます。



ルートは、仮想パスまたはゲートウェイ IP 可用性に結び付けることができます。インターネットルートは、目的の動作に応じて仮想パスオーバーレイにエクスポートすることも、エクスポートしないこともできます。また、SD-WAN にアダプタイズされるプレフィックス（つまり、最終手段のコストの高いルート）を取得していない場合でも、ステティック仮想パスルートを作成して、トラフィックを仮想パスに強制することもできます。SD-WAN は、仮想 IP アドレス (VIP) をプライベートにすることで、ローカルサブネットのアダプタイズを抑制することもできます。

IP Address / Prefix	Virtual Interface	Firewall Zone	Identity	Private	Security	Delete
172.10.10.10/24	E1Vlan0	Default_LAN_Zone	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Trusted	
172.10.10.11/24	E1Vlan0	Default_LAN_Zone	<input type="checkbox"/>	<input type="checkbox"/>	Trusted	

Apply **Revert**

注

設定では、各ルートドメインに少なくとも 1 つの非プライベート VIP が必要です。

イントラネットとインターネットルート

イントラネットサービスタイプおよびインターネットサービスタイプでは、これらのタイプのサービスをサポートするために SD-WAN リンクを定義しておく必要があります。これは、これらのサービスのいずれかに定義されたルートのための前提条件です。WAN リンクがイントラネットサービスをサポートするように定義されていない場合、WAN リンクはローカルルートと見なされます。イントラネット、インターネット、パススルールートは、構成されているサイト/アプライアンスにのみ関連します。

イントラネット、インターネット、またはパススルールートを定義する場合、設計上の考慮事項は次のとおりです。

- WAN リンクにサービスが定義されている必要があります (イントラネット/インターネットー必須)
- イントラネット/インターネットには、WAN リンク用に Gateway が定義されている必要があります。

- ローカル SD-WAN デバイスに関連します
- イン트라ネット・ルートは仮想パスを介して学習できますが、それは高コストで学習できます
- インターネットサービスでは、自動的にデフォルトルートが作成され (0.0.0.0/0)、最大コストですべてのルートをキャッチします
- パススルーが動作すると仮定しないでください。テスト/検証する必要があります。また、仮想パスをダウン/無効にしてテストして目的の動作を確認します
- ルートテーブルは、ルート学習機能が有効でない限り、スタティックです

複数のルーティングパラメータでサポートされる最大制限は次のとおりです。

- 最大ルーティングドメイン:255
- WAN リンクあたりの最大アクセスインターフェイス:64
- サイトあたりの BGP ネイバーの最大数: 255
- サイトあたりの最大 OSPF エリア:255
- OSPF エリアあたりの仮想インターフェイスの最大数:255
- サイトあたりのルートラーニングインポートフィルタの最大数:512
- サイトあたりのルートラーニングエクスポートフィルタの最大数:512
- BGP ルーティングポリシーの最大数:255
- BGP コミュニティストリングオブジェクトの最大数: 255

ルーティングドメイン

May 10, 2021

Citrix SD-WAN では、ルーティングドメインを使用することにより、ネットワークのセグメント化によりセキュリティと管理が容易になります。たとえば、ゲストネットワークトラフィックを従業員のトラフィックから分離したり、大規模な企業ネットワークをセグメント化するために個別のルーティングドメインを作成したり、トラフィックをセグメント化して複数のカスタマーネットワークをサポートしたりできます。各ルーティングドメインには独自のルーティングテーブルがあり、IP サブネットのオーバーラップをサポートできます。

Citrix SD-WAN アプライアンスは、ルーティングドメイン用の OSPF および BGP ルーティングプロトコルを実装し、ネットワークトラフィックを制御およびセグメント化します。

仮想パスは、アクセスポイントの定義に関係なく、すべてのルーティングドメインを使用して通信できます。これは、SD-WAN カプセル化にパケットのルーティングドメイン情報が含まれているためです。したがって、両方のエンドネットワークは、パケットがどこに属しているかを認識します。ルーティングドメインごとに WAN リンクまたはアクセスインターフェイスを作成する必要はありません。

ルーティングドメイン機能を設定するときに考慮すべきポイントのリストを次に示します。

- デフォルトでは、ルーティングドメインは MCN で有効になっています。
- ルーティングドメインは、ブランチサイトで有効になります。
- 有効な各ルーティングドメインには、仮想インターフェイスと仮想 IP が関連付けられている必要があります。
- ルーティングの選択は、次のすべての設定の一部です。
 - インターフェイスグループ
 - 仮想 IP
 - GRE
 - WAN リンク-> アクセスインターフェイス
 - IPSec トンネル
 - ルート
 - 規則
- ルーティングドメインは、複数のドメインが作成された場合に限り、Web インターフェイス設定で公開されます。
- パブリックインターネットリンクの場合、作成できるプライマリアクセスインターフェイスとセカンダリアクセスインターフェイスは 1 つだけです。
- プライベートイントラネット/MPLS リンクの場合、ルーティングドメインごとに 1 つのプライマリおよびセカンダリアksesインターフェイスを作成できます。

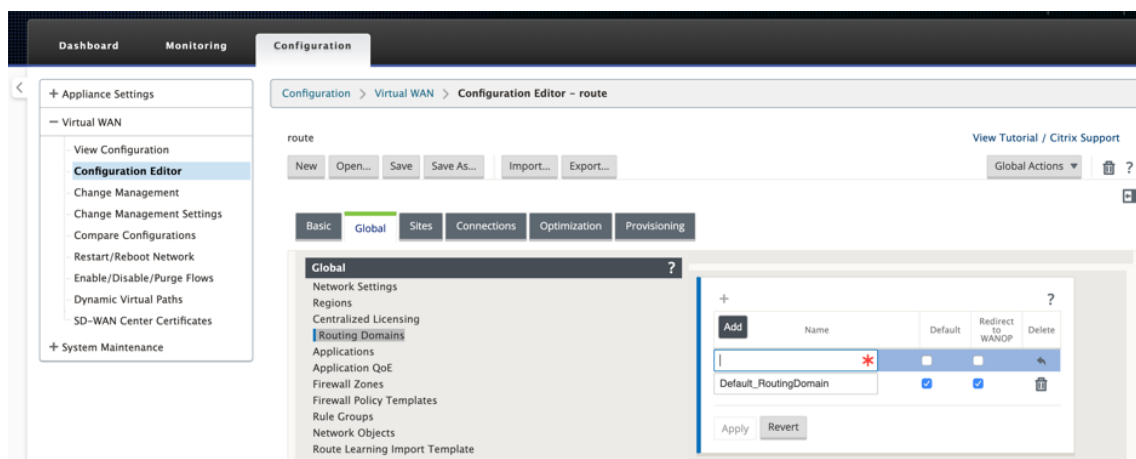
ルーティングドメインの構成

May 10, 2021

Citrix SD-WAN アプライアンスは、ルーティングプロトコルを構成して、企業ネットワーク、支店ネットワーク、データセンターネットワークを管理するための単一の管理ポイントを提供します。最大 254 個のルーティングドメインを設定できます。

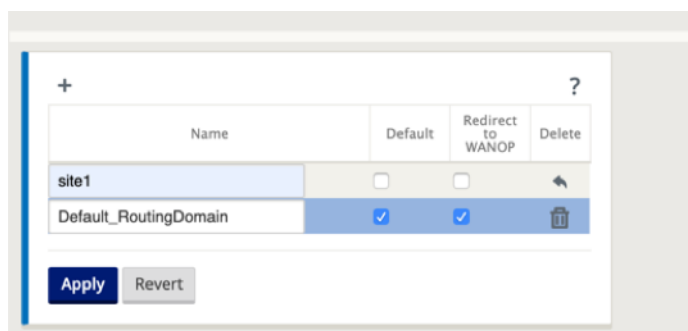
ルーティングドメインを構成するには、次の手順を実行します。

1. SD-WAN Web インターフェイスで、[構成] > [仮想 **WAN**] > [構成エディタ] に移動します。構成エディターで、「グローバル」 > 「ルーティングドメイン」に移動し、「追加」 **(+)** をクリックして、新しいルーティングドメインの名前を入力します。

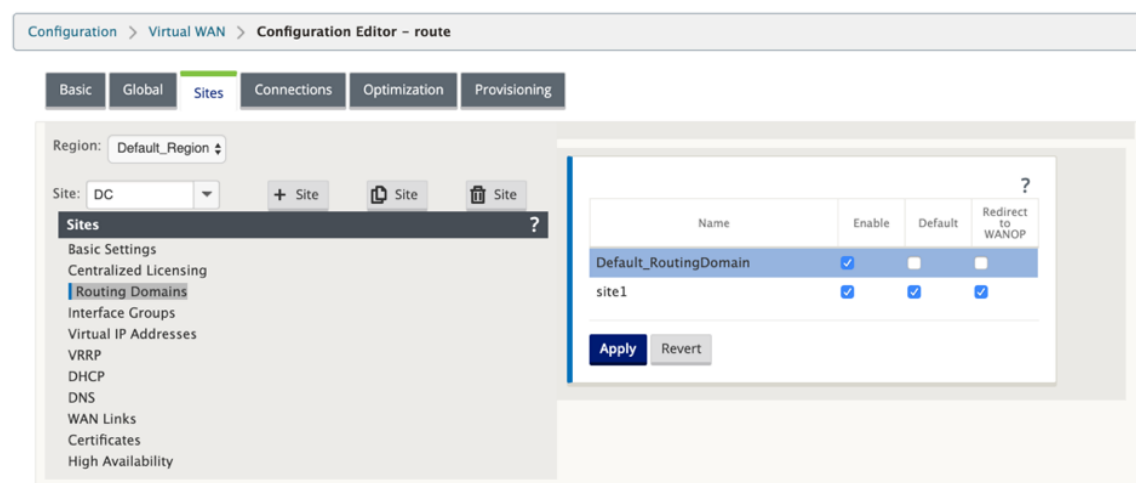


2. このルーティングドメインをデフォルトに設定する場合は、[デフォルト] チェックボックスをオンにします。
[適用] をクリックして変更を保存します。単一のルーティングドメインを実装する場合は、明示的な設定は必要ありません。

すべての新しい設定には、デフォルトのルーティングドメインが自動的に設定されます。



3. 「サイト」→「[クライアントサイト名]」>「ルーティングドメイン」に移動します。[Enable] チェックボックスをクリックして、サイトに対して構成済みのルーティングドメインを有効にします。
4. [デフォルト] チェックボックスをクリックして、そのルーティングドメインをサイトのデフォルトにします。
[適用] をクリックして変更を保存します。



注

「ルーティングドメインに対して 有効にする」をオフにすると、サイトで使用できなくなります。

11.0.2 リリースでは、ルーティング可能な仮想 **IP (VIP)** を持たないルーティングドメインは、次の機能で許可されます。

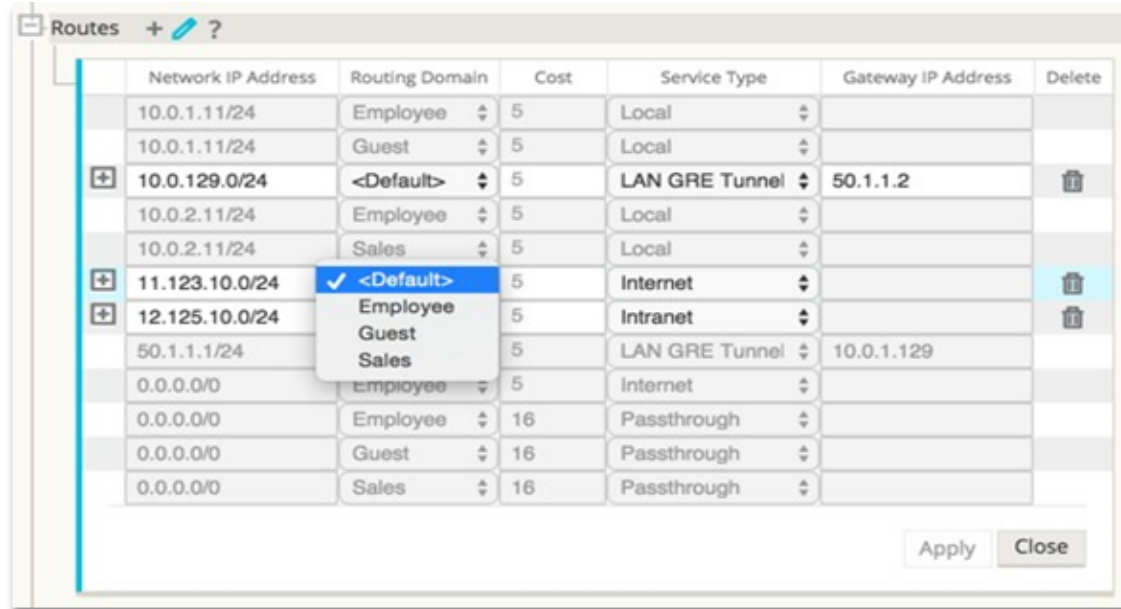
- デバイスに、信頼できないインターフェイスまたはインターフェイスがないルーティングドメインを持たせるようにします。
- 中間サイトに物理的な存在がないルーティングドメインを介して、ブランチが相互に通信できるようにします。

ルートの設定

May 10, 2021

ルートを構成するには、次の手順に従います。

1. 構成エディタで、**[接続] > [[サイト名]] > [ルート]** に移動します。
2. ドロップダウンメニューから ルーティングドメイン を選択します。新しいルートは、デフォルトのルーティングドメインに自動的に関連付けられます。詳細な手順については、[ルートの設定](#)を参照してください。



Configuration > Virtual WAN > View Configuration

Configuration

View: Routes Current configuration file (perf-open-pipe-cb410-cb5100-b67-v1.cfg) View File

Route Configuration

Routes for routing domain 'Default_RoutingDomain' :

Num	Network Addr	Gateway IP Address or Next_Hop	Service	Site	Cost	Type	Neighbor Direct	Route Eligibil Type
0	172.109.4.11/32	*	IPHost	DC2-201	5	Static	-	-
1	172.109.32.11/32	*	IPHost	DC2-201	5	Static	-	-
2	192.109.0.0/24	*	DC1-212-DC2-201	DC1-212	5	Static	-	-
3	172.109.4.0/23	*	Local	DC2-201	5	Static	-	-
4	172.109.32.0/22	*	Local	DC2-201	5	Static	-	-
5	172.109.0.0/20	*	DC1-212-DC2-201	DC1-212	5	Static	-	-
6	0.0.0.0/0	*	Passthrough	*	16	Static	-	-
7	0.0.0.0/0	*	Discard	*	16	Static	-	-

ルートを設定したら、[構成]>[仮想 WAN]>[表示]>[ルート]に移動して、設定済みのルーティングドメインのルートテーブルを検証します。

CLI を使用してルーティングにアクセスする

May 10, 2021

Citrix SD-WAN リリースバージョン 10.0 では、動的ルーティングとプロトコルの状態に関連する追加情報を表示できます。次のコマンドと構文を入力して、ルーティングデーモンにアクセスし、コマンドの一覧を表示します。

```
1 dynamic_routing?
2 <!--NeedCopy-->
```

動的ルーティング

November 8, 2021

Citrix SD-WAN では、次の 2 つの動的ルーティングプロトコルがサポートされています。

- Open Shortest Path First (OSPF)
- Border Gateway Protocol (BGP)

Citrix SD-WAN 11.3.1 のリリースより前のリリースでは、動的ルーティング機能は単一のルーター ID に対してのみ使用できました。一意のルータ ID は、プロトコル全体（OSPF および BGP 用）にグローバルに設定することも、ルータ ID を指定しないこともできます。ルータ ID を指定しない場合、ダイナミックルーティングに参加する Virtual Network Instances (VNI; 仮想ネットワークインスタンス) の最小 IP がデフォルトのルータ ID として自動的に選択されます。

Citrix SD-WAN 11.3.1 リリース以降では、プロトコル全体のルーター ID を構成できるだけでなく、ルーティングドメインごとにルーター ID を構成することもできます。この機能強化により、異なるルータ ID の安定したコンパージョンスを使用して、複数のインスタンス間で安定したダイナミックルーティングを有効にできます。

特定のルーティングドメインにルータ ID を設定する場合、特定のルータ ID がプロトコルレベルのルーティングドメインを上書きします。

(注

) ダイナミックルータ ID は、次の SD-WAN アプライアンスでは設定できません。

- Citrix SD-WAN 1000 SE/PE
- Citrix SD-WAN 2000 SE/PE
- Citrix SD-WAN 4000 SE

OSPF

OSPF は、Internet Engineering Task Force (IETF) の Interior Gateway Protocol (IGP) グループによってインターネットプロトコル (IP) ネットワーク向けに開発されたルーティングプロトコルである。OSI の Intermediate System to Intermediate System (IS-IS) ルーティングプロトコルの初期バージョンが含まれています。

OSPF プロトコルはオープンです。つまり、その仕様はパブリックドメイン (RFC 1247) にあります。OSPF は、ダイクストラと呼ばれる最短パスファースト (SPF) アルゴリズムに基づいています。これは、リンクステートルーティングプロトコルで、同じ階層領域内の他のすべてのルータに Link-State Advertising (LSA; リンクステートアドバタイズメント) を送信するようコールします。接続されているインターフェイス、使用されるメトリック、およびその他の変数に関する情報は、OSPF LSA に含まれます。OSPF ルータは、各ノードへの最短パスを計算するために SPF アルゴリズムによって使用されるリンクステート情報を蓄積します。

Citrix SD-WAN アプライアンス (Standard Edition と Premium (Enterprise) Edition) を構成して、OSPF を使用してルートを学習し、ルートをアドバタイズできるようになりました。

注

- Citrix SD-WAN アプライアンスは、デフォルトの DR 優先順位が「0」に設定されているため、各マルチアクセスネットワーク上で代表ルータ (DR) および BDR (バックアップ代表ルータ) として参加しません。
- Citrix SD-WAN アプライアンスは、エリア境界ルータ (ABR) としての要約をサポートしていません。

OSPF の設定

OSPF を設定するには、次の手順を実行します。

1. 設定エディタで、[接続] > [リージョン] > [サイト] > [OSPF] > [基本設定] に移動します。
2. [有効化] をクリックし、次のパラメータの値を選択または入力して、[適用] をクリックします。

- **Citrix SD-WAN** ルートのアドバタイズ: OSPF 経由で Citrix SD-WAN ルートをアドバタイズできるようにします。OSPF 再配布用のタグを指定することもできます。
- **BGP** ルートのアドバタイズ: BGP ピアから学習したルートを OSPF 経由でアドバタイズできるようにします。OSPF 再配布用のタグを指定することもできます。
- ルータ **ID**: 一意のルータ識別子。ルータは OSPF アドバタイズメントに使用されます。ルータ ID が指定されていない場合は、SD-WAN ネットワークでホストされている最も低い仮想 IP として自動的に選択されます。
- **OSPF** ルートタイプのエクスポート: Citrix SD-WAN ルートを OSPF ピアにエリア内ルートまたは外部ルートとしてアドバタイズします。
- **OSPF** ルートウェイトのエクスポート: Citrix SD-WAN ルートを OSPF にエクスポートする場合は、このウェイトを各ルートの Citrix SD-WAN コストに追加します。
- プロトコルプリファレンス: プレフィックスが複数のルーティングプロトコルを介して学習される場合、プロトコルプリファレンス値によってルーティングプロトコルの選択が決まります。詳細については、「[プロトコルプリファレンス](#)」を参照してください。

The screenshot displays the Citrix SD-WAN configuration interface. The top navigation bar includes tabs for Basic, Global, Sites, Connections, Optimization, and Provisioning. The 'Connections' tab is active, and the left sidebar shows a list of connection types, with 'OSPF' selected. The main configuration area is titled 'Section: Basic Settings'. It contains several settings: 'Enable' is checked; 'Advertise Citrix SD-WAN Routes' is checked with a 'Tag Value' of 10; 'Advertise BGP Routes' is checked with a 'Tag Value' of 20; 'Router ID' is set to 5.5.5.5; 'Export OSPF Route Type' is set to 'Type 5 AS Extern'; 'Export OSPF Route Weight' is set to 4; and 'Protocol Preference' is set to 150. At the bottom, there are 'Apply' and 'Revert' buttons.

3. [**OSPF**]-> [エリア] を展開し、[編集] をクリックします。

Section: Areas

+ ID Stub Area Delete

1

Virtual Interfaces +

Name	Source IP Address	Interface Cost	Authentication Type	Password	Network Type	Hello Interval	Dead Interval	Delete
VirtualInterface	172.111.64.5	10	None		Auto	10	40	

Apply Revert

- ルートを学習し、アドバタイズする エリア **ID** を入力します。
- 特定の仮想 IP アドレスの ID がチェックされていない場合、関連付けられた仮想インターフェイスは IP サービスでできません。
- [**Name**] メニューから、使用可能な仮想インターフェイスのいずれかを選択します。仮想インターフェイスは、送信元 **IP** アドレスを決定します。
- インタフェース・コストを入力します（デフォルトは 10 です）。
- メニューから [認証タイプ] を選択します。
- 手順 8 で「パスワード」または「**MD5**」を選択した場合は、「パスワード関連テキスト」フィールドに入力します。
- [**Hello Interval**] フィールドに、直接接続されたネイバーに Hello プロトコルパケットを送信するまでの待機時間を入力します（デフォルトは 10 秒）。
- [**Dead Interval**] フィールドに、ルータをデッドとしてマークするまでの待機間隔を入力します。デフォルトのデッドインターバルは 40 秒です。
- [適用] をクリックして変更を保存します。

スタブエリア

スタブエリアは外部ルートからシールドされ、同じ OSPF ドメインの他のエリアに属するネットワークに関する情報を受信します。

[スタブエリア] チェックボックスをオンにします。

Section: Areas

ID	Stub Area	Delete
1	<input type="checkbox"/>	

Virtual Interfaces +

Name	Source IP Address	Interface Cost	Authentication Type	Password	Network Type	Hello Interval	Dead Interval	CREATE
VirtualInterface-1	172.111.64.5	10	None		Auto	10	40	

Apply Revert

If enabled, the Area will avoid flooding external routes

OSPF 再配布タグ

OSPF タグを使用すると、OSPF と他のプロトコル間の相互再配布中にルーティングループが発生しないようにできます。OSPF ドメインで、同じサブネットへの SD-WAN および BGP で学習されたルートがある場合、OSPF ループ防止メカニズムはそのルートをループとして識別し、ルートを無視します。SD-WAN ルートと BGP 学習ルートに異なるタグを指定すると、これらのルートを OSPF ルーティングテーブルにインストールできます。

SD-WAN および BGP を通じて学習されたルートの OSPF 再配布タグは、[OSPF の基本設定] セクションで設定できます。

Section: Basic Settings ▾

☒ Enable

☒ Advertise Citrix SD-WAN Routes Tag Value: 10

☒ Advertise BGP Routes Tag Value: 20

Router ID:
5.5.5.5

Export OSPF Route Type:
Type 5 AS Exterr ▾

Export OSPF Route Weight:
4

Protocol Preference:
150

Apply Revert

BGP

BGP は、自律システム間ルーティングプロトコルです。自律ネットワークまたはネットワークのグループは、共通の管理下および共通のルーティングポリシーで管理されます。BGP は、インターネットのルーティング情報を交換するために使用され、ISP 間で使用されるプロトコルです。カスタマーネットワークは、RIP や OSPF などの内部 Gateway プロトコルを展開して、ネットワーク内のルーティング情報を交換します。カスタマーは ISP に接続し、ISP は BGP を使用してカスタマーと ISP のルートを交換します。自律システム (AS) 間で BGP を使用する場合、プロトコルは External BGP (EBGP) と呼ばれます。サービスプロバイダーが BGP を使用して AS 内でルートを交換している場合、このプロトコルは Interior BGP (IBGP) と呼ばれます。

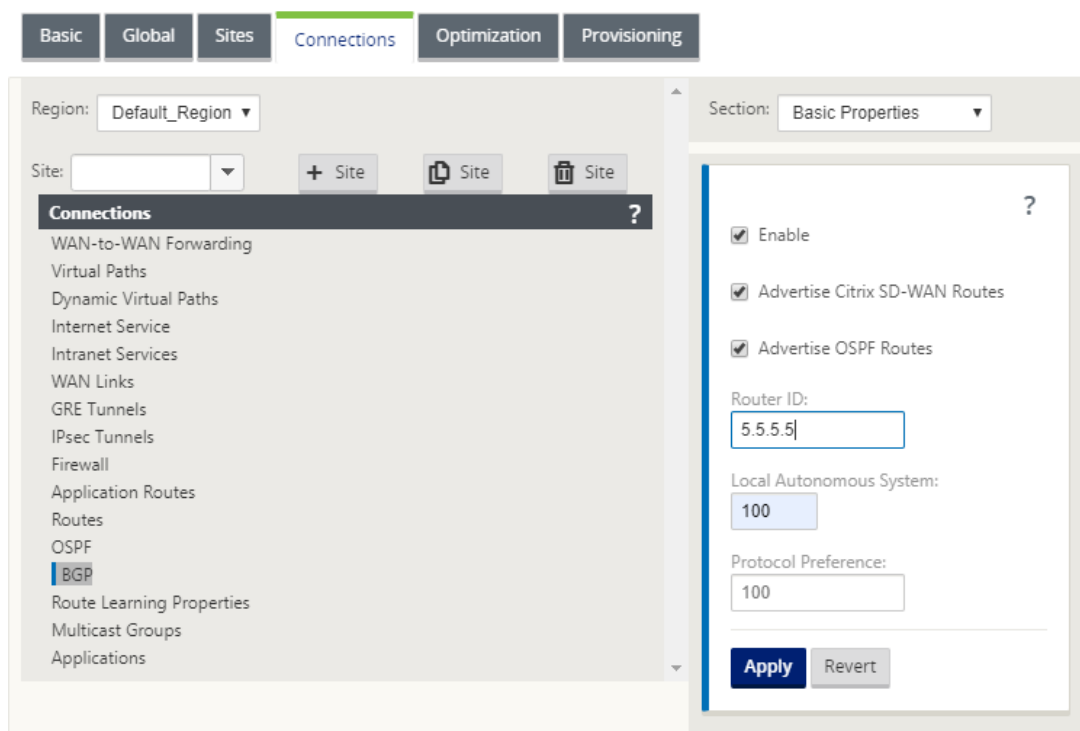
BGP は、インターネット上に展開される堅牢でスケーラブルなルーティングプロトコルです。スケーラビリティを実

現するために、BGP は属性と呼ばれる多数のルートパラメータを使用して、ルーティングポリシーを定義し、安定したルーティング環境を維持します。BGP ネイバーは、ネイバー間の TCP 接続が最初に確立されたときに、完全なルーティング情報を交換します。ルーティングテーブルへの変更が検出されると、BGP ルータは、変更されたルートだけをネイバーに送信します。BGP ルータは定期的なルーティングアップデートを送信せず、宛先ネットワークへの最適パスのみをアドバタイズします。Citrix SD-WAN アプライアンスは、ルートを学習し、BGP を使用してルートをアドバタイズするように構成できます。

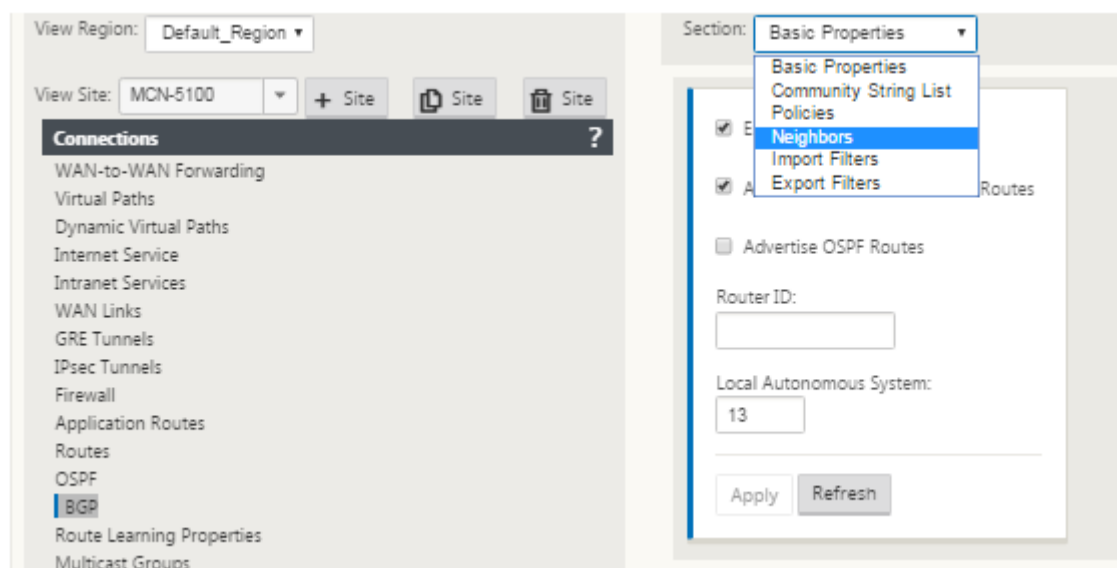
BGP の設定

BGP を設定するには、次の手順を実行します。

1. 構成エディタで、[接続] > [リージョン] > [サイト] > [BGP] > [基本設定] に移動します。
2. [有効化] をクリックし、次のパラメータの値を選択または入力して、[適用] をクリックします。
 - **Citrix SD-WAN** ルートのアドバタイズ: Citrix SD-WAN ルートを BGP 経由でアドバタイズできるようにします。
 - **OSPF** ルートのアドバタイズ: OSPF ピアから学習したルートを BGP 経由でアドバタイズできるようにします。
 - ルータ **ID**: 一意のルータ識別子。ルータは OSPF アドバイズメントに使用されます。ルータ ID が指定されていない場合は、SD-WAN ネットワークでホストされている最も低い仮想 IP として自動的に選択されます。
 - ローカル自律システム: ルートの学習およびアドバタイズ先のローカル自律システム番号。自律システム番号は、ネイバールータ上の自律システム番号と一致する必要があります。
 - プロトコルプリファレンス: プレフィクスが複数のルーティングプロトコルを介して学習される場合、プロトコルプリファレンス値によってルーティングプロトコルの選択が決まります。詳細については、「[プロトコルプリファレンス](#)」を参照してください。



3. [基本設定] > [ネイバー] を展開し、[追加] (+) アイコンをクリックします。



Section: Neighbors

	Virtual Interface	Source IP	Neighbor IP	Neighbor AS	Hold Time(s)	Local Preference	IGP Metric	Multi Hop	Password	Delete
	VirtualInterface-	172.111.64.5		13	180	100	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		

Policies +

Order	Network Address	BGP Community(AA:NN)	AS Path	BGP Policy	Direction	Delete
-------	-----------------	----------------------	---------	------------	-----------	--------

Apply Revert

複数のルーティングドメインを持つサイトの場合、ルーティングドメインを選択します。ルーティングドメインは、使用可能な仮想インターフェイスを決定します。

4. メニューから仮想インターフェイスを選択します。仮想インターフェイスは、送信元 IP アドレスを決定します。
5. [ネイバー IP] フィールドに **IBGP** ネイバルータの **IP** アドレスを入力し、[ネイバー AS] フィールドにローカル自律システム番号を入力します。
6. [**Hold Time (s)**] フィールドに、ネイバーのダウンを宣言する前に待機するホールドタイムを秒単位で入力します（デフォルトは 180）。
7. [**Local Preference (s)**] フィールドに、複数の BGP ルートからの選択に使用される Local Preference 値を秒単位で入力します（デフォルトは 100）。
8. [**IGP Metric**] チェックボックスをクリックして、内部距離の比較を有効にして最適ルートを計算します。
9. [マルチホップ (Multi-Hop)] チェックボックスをオンにして、ルートのマルチホップを有効にします。
10. [**P** assword] フィールドに、BGP セッションの MD5 認証用のパスワードを入力します（認証は不要です）。

注

iBGP のルートリフレクタおよびコンフェデレーションの設定は、SD-WAN ネットワークではサポートされていません。

外部 **BGP** (eBGP)

Citrix SD-WAN アプライアンスは、LAN 側のスイッチ、WAN 側のルーターに接続します。SD-WAN テクノロジーが企業のネットワーク展開に不可欠になり始めるにつれ、SD-WAN アプライアンスがルーターを置き換えます。SD-WAN は eBGP ダイナミックルーティングプロトコルを実装して、専用のルーティングデバイスとして機能します。

SD-WAN アプライアンスは、eBGP を使用して WAN 側へのピアルータとのネイバーシップを確立し、ピアとの間でルートを学習し、アドバタイズできます。eBGP 学習ルートのインポートとエクスポートは、ピアデバイス上で選

択できます。また、SD-WAN スタティック、仮想パスラーニングされたルートを eBGP ピアにアドバタイズするように設定することもできます。

詳細については、次のユースケースを参照してください。

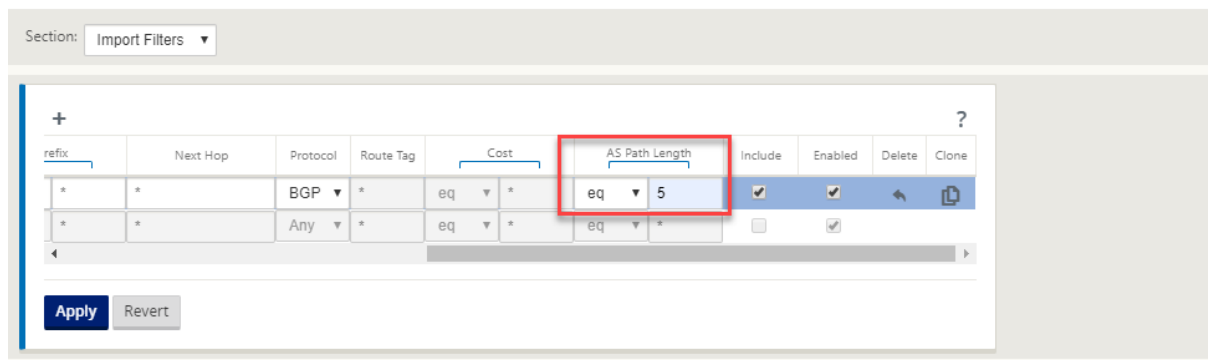
- [SD-WAN サイト eBGP を介した非 SD-WAN サイトとの通信](#)
- [仮想パスと eBGP を使用した SD-WAN サイト間の通信](#)
- [ワンアームトポロジでの OSPF の実装](#)
- [MPLS ネットワークでの OSPF タイプ 5 からタイプ 1 への配置](#)
- [SD-WAN および非 SD-WAN（サードパーティ）アプライアンス OSPF 展開](#)
- [高可用性セットアップで SD-WAN ネットワークを使用した OSPF の実装](#)

AS パスの長さ

BGP プロトコルは、**AS** パス長属性を使用して最適ルートを決定します。AS パスの長さは、ルート内で通過する自律システムの数を示します。Citrix SD-WAN は、**BGP AS** パス長 属性を使用してルートをフィルタリングおよびインポートします。

非 SD-WAN アプライアンスは、AS パスの長さに基づいてルートをインポートすることにより、トラフィックをプライマリ DC またはセカンダリ DC SD-WAN アプライアンスにルーティングできます。また、ルータ上のプライマリ DC アプライアンスの AS パス長を増やすだけで、ルータからセカンダリ DC へのトラフィックを動的に誘導することもできます。ルートコストを変更し、設定の更新を実行する必要がなくなります。

インポートフィルタで AS パスの長さを設定するには、プロトコルとして BGP を選択し、述語を選択して、**AS** パスの長さを入力します。詳細については、「[ルートフィルタリング](#)」を参照してください。



ルート統計情報のモニタリング

[モニタ] > [統計] に移動します。[表示] ドロップダウンメニューから [ルート] を選択します。

Citrix SD-WAN ネットワークでは、ルートが動的か静的にかかわらず、適用可能なルートのすべての機能がサポートされています。

Monitoring > Statistics

Statistics

Show: Routes

Enable Auto Refresh

 5 seconds

Refresh

Clear Counters on Refresh

Purge dynamic routes

Route Statistics

Maximum allowed routes: 16000

Routes for routing domain : Default_RoutingDomain

Filter: in Any column

Apply

Show 100 entries Showing 1 to 28 of 28 entries

First

Previous

1

Next

Last

Num	Network Addr	Gateway IP Address	Service	Reachable	Site IP Address	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
0	115.1.1.0/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
1	115.168.0.16/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
2	115.168.0.12/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
3	115.168.0.8/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
4	115.168.0.4/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
5	115.168.0.0/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
6	115.14.14.0/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
7	115.13.13.0/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
8	115.12.12.0/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
9	115.10.10.0/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
10	115.9.9.16/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
11	115.8.8.12/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
12	115.7.7.8/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
13	115.6.6.4/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
14	115.5.5.0/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
15	115.4.4.0/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
16	115.3.3.0/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
17	115.2.2.0/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
18	182.120.1.0/24	*	Local	YES	*	pod2_DC	Static	-	-	5	0	YES	N/A	N/A
19	172.120.1.0/24	*	Local	YES	*	pod2_DC	Static	-	-	5	0	YES	N/A	N/A
20	182.120.2.0/24	*	pod2_DC-pod3_Br	YES	*	pod3_Br	Static	-	-	5	0	YES	N/A	N/A
21	172.120.2.0/24	*	pod2_DC-pod3_Br	YES	*	pod3_Br	Static	-	-	5	0	YES	N/A	N/A
22	182.120.0.0/24	*	pod2_DC-pod1_Br	YES	*	pod1_Br	Static	-	-	5	0	YES	N/A	N/A
23	172.120.0.0/24	*	pod2_DC-pod1_Br	YES	*	pod1_Br	Static	-	-	5	0	YES	N/A	N/A
24	192.120.1.0/24	172.120.1.2	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	75612	YES	N/A	N/A
25	192.120.0.0/24	*	pod2_DC-pod1_Br	YES	*	pod1_Br	Dynamic	Virtual WAN	YES	6	75612	YES	N/A	N/A
26	0.0.0.0/0	*	Passthrough	YES	*	*	Static	-	-	16	0	YES	N/A	N/A
27	0.0.0.0/0	*	Discard	YES	*	*	Static	-	-	16	0	YES	N/A	N/A

Showing 1 to 28 of 28 entries

First

Previous

1

Next

Last

OSPF

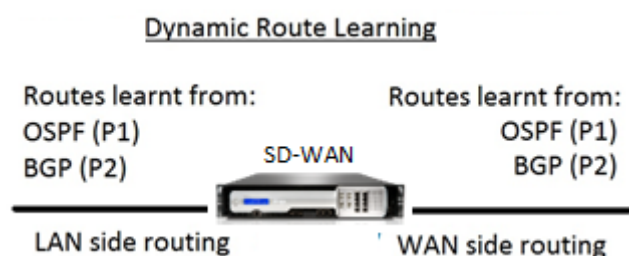
May 10, 2021

LAN 側: ダイナミックルートラーニング

ゲートウェイモードで展開された Citrix SD-WAN アプライアンスの LAN ポートで実行されている OSPF:

Citrix SD-WAN アプライアンスは、必要なルーティングプロトコル（OSPF および BGP）ごとに、ローカルカスタマーネットワーク（ブランチとデータセンターの両方）内でレイヤー 3 ルーティングアダプタイズメントのルート検出を実行します。学習されたルートは動的にキャプチャされ、表示されます。

これにより、SD-WAN 管理者は、SD-WAN ネットワークの一部である各アプライアンスの LAN 側のネットワーク環境を静的に定義する必要がなくなります。



WAN 側: ダイナミックルート共有

タイプ 5 AS-外部 LSA の学習を制限することにより、STUB エリアとして定義されたエリアを持つ Citrix SD-WAN アプライアンス。

Citrix SD-WAN アプライアンスは、ローカルで学習された動的ルートを MCN でアドバタイズできます。MCN は、これらのルートをネットワーク内の他の SD-WAN アプライアンスに中継できます。この情報を動的に交換することで、変化するネットワーク全体でサイト間の接続を維持できます。

OSPF 展開モード

以前のリリースでは、SD-WAN からの OSPF インスタンス学習ルートは、タイプ 5 LSA のみの外部ルートとして扱われていました。これらのルートは、タイプ 5 外部 LSA のネイバールータにアドバタイズされました。その結果、SD-WAN ルートは、OSPF パス選択アルゴリズムに従って、あまり優先されないルートになりました。

最新リリースでは、SD-WAN はルートをエリア内ルート（LSA タイプ 1）としてアドバタイズし、OSPF パス選択アルゴリズムを使用してルートコストに従って優先権を取得できるようになりました。ルートコストを設定し、ネイバールータにアドバタイズできます。これにより、SD-WAN アプライアンスを以下に説明するワンアームモードで展開できます。

ワンアームトポロジでの OSPF の実装

ワンアーム設定では、OSPF 配置でルータに複雑な PBR または WCCP 設定が必要です。デフォルトのエクスポートルートタイプをタイプ 5 からタイプ 1 に変更することで、この展開を簡素化できます。SD-WAN ルートがコストの

少ないエリア内ルートとしてアドバタイズされ、SD-WAN アプライアンスがアクティブになると、ネイバールータは SD-WAN ルートを選択し、SD-WAN ネットワーク経由のトラフィックの転送を自動的に開始します。PBR または WCCP の追加設定は不要です。

前提条件:

- DC サイトおよびブランチサイトの SD-WAN アプライアンスは、最新のリリースバージョンを実行している必要があります。
- エンドツーエンドの IP 接続を構成し、正常に動作する必要があります。
- OSPF はすべてのサイトで有効になっています。

OSPF タイプ 1 を設定するには、次の手順を実行します。

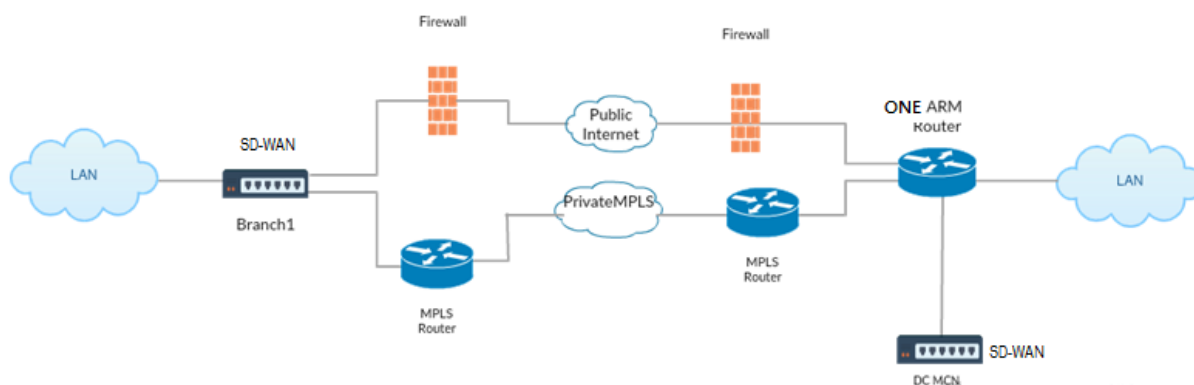
1. DC サイトとブランチサイトの両方で仮想インターフェイスと **WAN** リンクを構成して、それらの間に仮想パスを作成できるようにします。
2. [接続]>[MCN]>[ルート学習]>[OSPF]>[基本設定] で、[OSPF ルートタイプを ** タイプ 1 イントラエリアとしてエクスポート **] を選択します。
3. 構成を保存し、ステージングし、構成をアクティブにします。

[
OSPF ルートタイプのエクスポート] で、次のルートタイプが表示されている必要があります。

- タイプ 5 AS 外部
- タイプ 1 イントラエリア

タイプ **5 AS** 外部ルートを設定できる必要があります。

変更された設定をアクティブ化した後、[設定]>[仮想 WAN]>[設定の表示]>[ダイナミックルーティング] で、ルートタイプの変更を確認する必要があります。

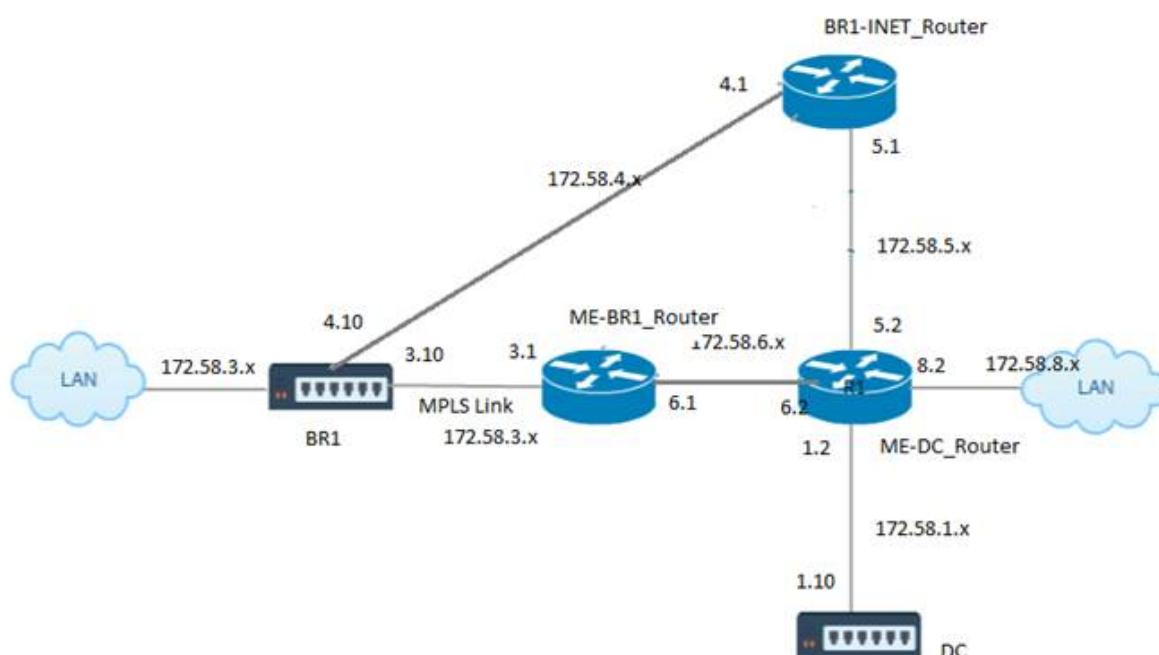


上の図に示すように、DC MCN はワンアームトポロジで展開されます。DC サイトがアップしている場合、ワンアームルータは、ローカル LAN から他のサイト（宛先 IP アドレスが同じサブネット内にある支店のローカル LAN など）にすべてのトラフィックを転送します。次に、SD-WAN アプライアンスはすべてのパケットをラップし、すべてのパケットの宛先 IP でルータに送信します。アドレスを、ブランチ仮想 IP アドレスに入力します。ルータは、これらのパケットを WAN に転送します。

DC サイトがダウンしている場合、ルータは、ローカル LAN から他のサイト（ブランチサイトのローカル LAN、宛先 IP はサブネット内）へのすべてのトラフィックを SD-WAN アプライアンスではなく、直接 WAN に転送します。

MPLS ネットワークにおける OSPF タイプ 5 からタイプ 1 への配置

SD-WAN アプライアンスを使用して設定された MPLS ネットワークでのループ形成を回避するために、次の展開モードが用意されています。次の図は、標準的な MPLS ネットワーク実装を示しています。



上の図では、次のようになります。

- OSPF は、エリア 0 の ME-BR1_router と ME-DC_router の間で設定されます。
- OSPF は、エリア 0 の ME-DC_router と DC の間で設定されます。

推奨構成:

- エリア 0 上の DC VW および ME-DC_Router
- エリア 0 上の ME-BR1_Router および ME-DC_Router
- エリア 0 上の BR1 VW および ME-BR1_Router

Me-DC_Router では、次の操作を行います。

1. 172.58.3.10/32 (MPLS リンク用の BR1 の仮想 IP) から 172.58.6.1 までのスタティックルートを追加
2. 172.58.4.10/32 (INET 用 BR1 の仮想 IP) から 172.58.5.1 までのスタティックルートを追加

スタティックルートを追加すると、ME-DC_router と DC SD-WAN アプライアンスの間のループ形成を防ぐことができます。スタティックルートを追加しない場合、MCN は ME-DC Router にトラフィックを転送し、ルータから MCN に戻して、ループを継続的に作成します。

PBR ルートではなく、宛先ホスト IP ベースのルートであるスタティックルートは、選択したパスおよびその後実行されるカプセル化に基づいて DC 側から選択される正しいリンクに向かって通過します。したがって、これらのスタティックルートが設定されている場合、BR1 SD-WAN アプライアンスの任意の宛先仮想 IP を持つカプセル化されたパケットは、DC MCN によって選択された最適パスに従ってこれらのリンクを使用します。

IPHOST ルートがインストールされている場合（スタティック仮想 IP が設定されていない場合）、ループ形成を回避するために ACL を追加します。

- BR1 SD-WAN アプライアンスによってアドバタイズされる IPHOST ルートが MCN ルータ *ME-DC_Router* によってインストールされ、上記のようにスタティックルートとして追加されていない場合、ME-BR1_Router と ME-DC_Router 間の OSPF 参加インターフェイス（172.58.6.x）がダウンすると、ループが形成される可能性があります。これは、このインターフェイスがダウンしていると、IPHOST ルートが ME-DC_router のルーティングテーブルからフラッシュされるためです。
- この場合、MCN は BR1 VIP 宛てのカプセル化されたパケットを ME-DC Router に転送し、ルータから MCN に戻してループを継続的に行います。

ME-BR1_Router では、次のようにします。

ME-BR1_Router <-> ME-DC_router と ME-DC_Router <-> DC (SD-WAN) の間で同じ **AREA-ID** が使用されている場合、**DC** によって同じネットワークに対してアドバタイズされたコストよりも高いコストで **172.58.3.x** ネットワークを **ME-DC_Router** にアドバタイズします。

- OSPF 10^8/BW のコストメトリック計算に基づいて、ルートプレフィックスのコストはインターフェイスタイプに基づいています。SD-WAN アプライアンスは、デフォルトの SD-WAN コストが 5 で、仮想パスと仮想 WAN 固有のスタティックルートを外部ルータまたはピアルータにアドバタイズします。
- ME-BR1_router が 172.58.3.0/24 を内部 OSPF タイプ 1 ルートとして DC (SD-WAN) とともにアドバタイズし、内部 OSPF タイプ 1 ルートと同じプレフィックスをアドバタイズする場合、コスト計算に従って、デフォルトで ME-BR1_router のルートが設定されます。これは、コストが SD-WAN のデフォルトのコストは 5 です。これを回避し、SD-WAN アプライアンスを最初に優先ルートとして選択するには、ME-BR1_Router で上位になるようにインターフェイスコスト (172.58.3.1) を操作して、DC SD-WAN ルートが ME-DC_router のルーティングテーブルで設定されるようにする必要があります。

これにより、DC SD-WAN アプライアンスに障害が発生しても、ME-BR1_router を次の優先 Gateway として使用する代替ルートによって、中断のないトラフィックフローが保証されます。

ME-DC_router は、172.58.8.0/24 ネットワークを DC SD-WAN と ME-BR1_router の両方にアドバタイズするための送信元として使用します。

このルートを使用すると、DC SD-WAN は、カプセル解除後に LAN サブネットを認識しているアップストリームルータにパケットを送信できます。DC SD-WAN がダウンした場合、レガシールーティングインフラストラクチャは、

ME-BR1_router が 172.58.8.x ネットワークに到達するネクストホップとして ME-DC_router を使用するのに役立ちます。

OSPF エクスポートされたルートを [基本 **OSPF** 設定] で Type1 として設定するには、次の手順を実行します。

1. DC サイトとブランチサイトの両方で仮想インターフェイスと **WAN** リンクを構成して、それらの間に仮想パスを作成します。
2. [接続]>[MCN]>[ルート学習]>[OSPF]>[基本設定] で、[**OSPF** ルートタイプのエクスポート] で [タイプ **1** イントラエリア] を選択します。
3. 設定、ステージを保存し、同じことをアクティブにします。[**OSPF** ルートタイプのエクスポート] で、次の **2** つのルートタイプが表示されている必要があります。
 - タイプ 5 AS 外部
 - タイプ 1 イントラエリア

変更した設定をアクティブ化すると、[設定]>[仮想 **WAN**]>[設定の表示]>[動的ルーティング] でルートタイプの変更を確認できます。

ルートは、SD-WAN アプライアンスによってタイプ 5 外部 AS としてアドバタイズされる必要があります。SD-WAN を介して学習されたルートは、ネイバルルータでタイプ 5 AS 外部ルートとして表示する必要があります。

[基本的な **OSPF** 設定] で OSPF エクスポートされたルートウェイトを設定するには、次の手順を実行します。

1. DC サイトとブランチサイトの両方で仮想インターフェイスと WAN リンクを構成して、それらの間に仮想パスを作成します。
2. [接続]>[MCN]>[ルート学習]>[**OSPF**]>[基本設定] で、[**OSPF** ルートウェイトのエクスポート] を設定します。
3. 設定、ステージを保存し、同じことをアクティブにします。
4. ここで、[OSPF ルートウェイトのエクスポート] を **1** ～**65529** までの任意の数値に設定します。
5. 変更した設定をアクティブ化すると、[設定]>[仮想 **WAN**]>[設定の表示]>[ダイナミックルーティング] でルートの重みを確認できます。エクスポートされるデフォルトのルートウェイトは 0 でなければなりません。ルートの実際のコストは SD-WAN のコストだけである必要があります。

[エクスポートフィルタ設定] で OSPF でエクスポートされたルートを Type1 として設定するには、次の手順を実行します。

1. DC とブランチの両方で仮想インターフェイスと **WAN** リンクを設定し、それらの間に仮想パスを作成できるように 1. [接続]>[**MCN**]>[ルート学習]>[**OSPF**]>[エクスポートフィルタ] でエクスポートフィルタを設定します。
2. フィルタを展開します。[**OSPF** ルートタイプのエクスポート] を [タイプ **1** イントラエリア 内ルート] に設定します。
3. 設定、ステージを保存し、同じことをアクティブにします。[**OSPF** ルートタイプのエクスポート] で、次の **2** つのルートタイプが表示されている必要があります。

- タイプ 5 AS 外部
- タイプ 1 イントラエリア

変更された設定をアクティブ化した後、ユーザは【構成】>【** 仮想 WAN】>【設定の表示】** で、ルートタイプの変更を確認できる必要があります。ルートタイプは、タイプ 5 AS External として表示する必要があります。

【エクスポートフィルタ】設定で OSPF でエクスポートされたルートウェイトを設定するには、次の手順を実行します。

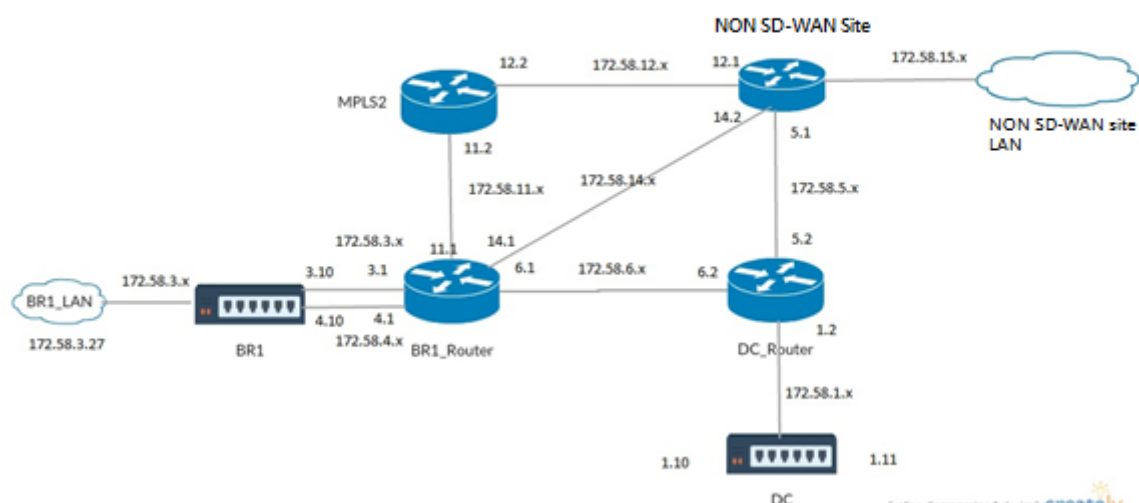
1. DC と Branch の両方で仮想インターフェイスと WAN リンクを設定して、それらの間に仮想パスを作成できるようにします。
2. 【接続】>【MCN】>【ルート学習】>【OSPF】>【エクスポートフィルタ】で、エクスポートフィルタを設定します。
3. フィルタを展開します。【OSPF ルートウェイトのエクスポート】を **1 ~ 65529** までの任意の数値に設定します。
4. 設定、ステージを保存し、同じことをアクティブにします。

変更された設定をアクティブ化した後、ユーザは【構成】>【** 仮想 WAN】>【設定の表示】** で、ルートタイプの変更を確認できる必要があります。

【エクスポートフィルタ】で設定されたルートウェイトは、【基本 OSPF 設定】で設定された重みよりも優先する必要があります。

SD-WAN およびサードパーティ（SD-WAN 以外）アプライアンスの展開

下の図に示すように、サードパーティのアプライアンスサイトは、サイト B に直接トラフィックを送信することで、サイト B の LAN にアクセスすることができます。トラフィックを直接送信できない場合、フォールバックルートはサイト A に送信され、DC からブランチサイト間の仮想パスを使用してブランチに到達します。失敗した場合は、MPLS2 を使用してブランチサイトにアクセスしてください。



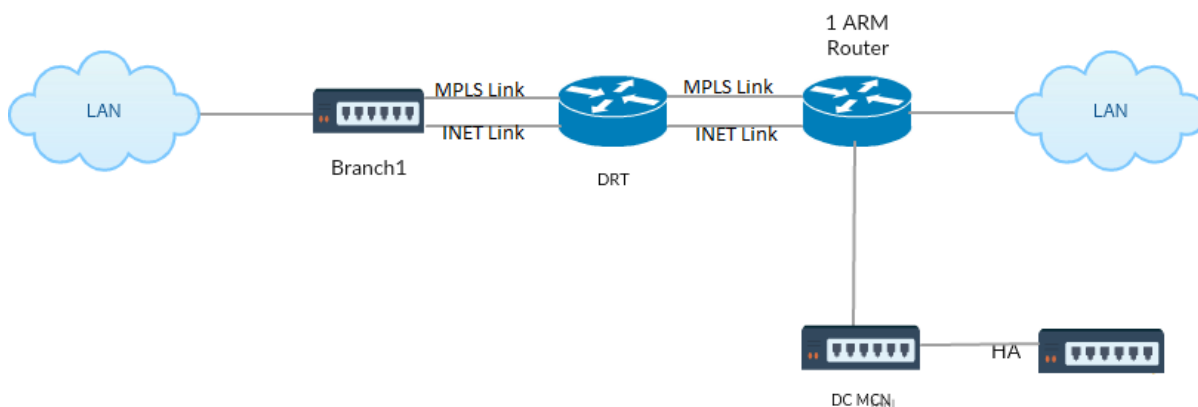
構成手順:

1. サイト間に仮想パスが作成されるように、**DC** とブランチの両方で仮想インターフェイスと **WAN** リンクを設定します。
2. SD-WAN アプライアンスで、エクスポートルートタイプをタイプ **1** に設定し、コストを **195** として割り当てます。
3. 設定を保存、ステージングし、アクティブ化します。
4. DC サイトとブランチサイトのエンドホスト間でトラフィックを送信します。
5. R1 と R2 の間のリンクをシャットダウンします。
6. DC サイトとブランチサイトのエンドホスト間でトラフィックを送信します。
7. R1 と R2 の間のリンクを解除します。
8. DC サイトとブランチサイトのエンドホスト間でトラフィックを送信します。
9. 仮想パスがダウンするように、DC サイトで仮想 WAN サービスを無効にします。
10. DC サイトとブランチサイトのエンドホスト間でトラフィックを送信します。

設定の確認:

1. 最初は、ステップ 4 で、すべてのトラフィックが SD-WAN アプライアンスを通過します。
2. ステップ 6 では、R1 と R2 の間のリンクが切断されると、トラフィックは R3 を介して SD-WAN にルーティングされます。
3. ステップ 8 では、トラフィックは、LAN ルータ R1 のネクストホップとして R2 を持つ SD-WAN アプライアンスを通過します。
4. ステップ 10 では、DC アプライアンスと BR1 アプライアンス間で仮想 WAN パスがダウンし、SD-WAN ネットワークが設定される前と同じようにトラフィックが正常に流れる必要があります。

トラフィックフローは、SD-WAN GUI の [モニタリング] > [フロー] で確認できます。

高可用性セットアップでの **SD-WAN** ネットワークでの **OSPF** の実装

スタンバイアプライアンスへのフェールオーバー中に高可用性サイトを持つ OSPF Type-5 から Type-1 への高可用性セットアップで展開されます。

HA 展開で OSPF を設定するには、次の手順を実行します。

1. DC とブランチの両方で仮想インターフェイスと **WAN** リンクを設定して、それらの間に仮想パスを作成します。
2. 高可用性をセットアップします。
3. ルートタイプをタイプ **1** に設定し、ルートウェイト を **50** に設定してエクスポートします。
4. 設定、ステージを保存し、同じことをアクティブにします。
5. トラフィックフローを開始します。
6. [**Monitor**] > [**Statistics**] > [**Routes**] で、コストが最も少ない OSPF ルートのヒットカウントが増加することを確認します。
7. アクティブ MCN をダウンさせ、動作を確認します。
8. 元のアクティブ MCN をバックアップします。
9. [ダッシュボード] > [高可用性ステータス] が HA ローカルアプライアンス、およびピアアプライアンスがアクティブおよびスタンバイの場合は正しく表示されます。
10. [設定] > [設定 の 表示] > [ダイナミックルーティング] では、OSPF が有効になり、**export_ospf_route_type** が **Type1**、**export_ospf_route_weight** が **50** と表示されます。
11. フェールオーバー後でも、高可用性ステータスは、ローカルおよびピアアプライアンスの正しい OSPF 設定を表示します。
12. 表示 モニター > 統計 > ルート。最小のコストで OSPF ルートのヒットカウントが増加します。
13. フェールバック後、高可用性ステータスは、ローカルおよびピアアプライアンスの正しい OSPF 設定を示します。
14. [**Monitor**] > [**Statistics**] > [Routes] の順にクリックして、低コストの OSPF ルートのヒットカウントが増加することを確認します。

トラブルシューティング

OSPF パラメータは、[モニタリング] > [ルーティングプロトコル] の下に表示されます。

Dashboard

Monitoring

Configuration

Statistics

Flows

Routing Protocols

Firewall

IKE/IPsec

IGMP

Performance Reports

Qos Reports

Usage Reports

Availability Reports

Appliance Reports

DHCP Server/Relay

VRRP

Monitoring > Routing Protocols

Dynamic Routing Protocol

View: OSPF Interface Routing Domain: Default_RoutingDomain Refresh

OSPF Interface

ospf_rdomain_0:
Interface vni-0 (172.58.1.0/24)
Type: broadcast
Area: 0.0.0.0 (0)
State: DROther
Priority: 0
Cost: 10
Hello timer: 10
Wait timer: 40
Dead timer: 40
Retransmit timer: 5
Designated router (ID): 105.105.105.105
Designated router (IP): 172.58.1.28
Backup designated router (ID): 0.0.0.0
Backup designated router (IP): 0.0.0.0

Dashboard

Monitoring

Configuration

Statistics

Flows

Routing Protocols

Firewall

IKE/IPsec

IGMP

Performance Reports

Qos Reports

Monitoring > Routing Protocols

Dynamic Routing Protocol

View: OSPF Neighbors Routing Domain: Default_RoutingDomain Refresh

OSPF Neighbors

ospf_rdomain_0:

Router ID	Pri	State	DTime	Interface	Router IP
105.105.105.105	1	Full/DR	00:39	vni-0	172.58.1.28

また、ダイナミックルーティングログを確認して、OSPF コンバージェンスに問題がないかどうかを確認することもできます。

Diagnose

Debug Logging: ☒ On ☐ Off

Filename: ▼

BGP

May 10, 2021

SD-WAN BGP ルーティング機能を使用すると、次のことが可能になります。

- ネイバーまたは他のピアルータ（iBGP または eBGP）の AS 番号を設定します。
- いずれかの方向（インポートまたはエクスポート）で、ネイバー単位でネットワークセットに選択的に適用する BGP ポリシーを作成します。SD-WAN アプライアンスは、サイトごとに 8 つのポリシーをサポートし、1 つのポリシーには最大 8 つのネットワークオブジェクト（または 8 つのネットワーク）が関連付けられています。
- ユーザは、ポリシーごとに、複数のコミュニティストリング、AS-PATH-PREPEND、MED 属性を設定できます。ユーザーは、ポリシーごとに最大 10 の属性を設定できます。

注：

パスの選択と操作には、ローカルプリファレンスと IGP メトリックだけが許可されます。

ポリシーの設定

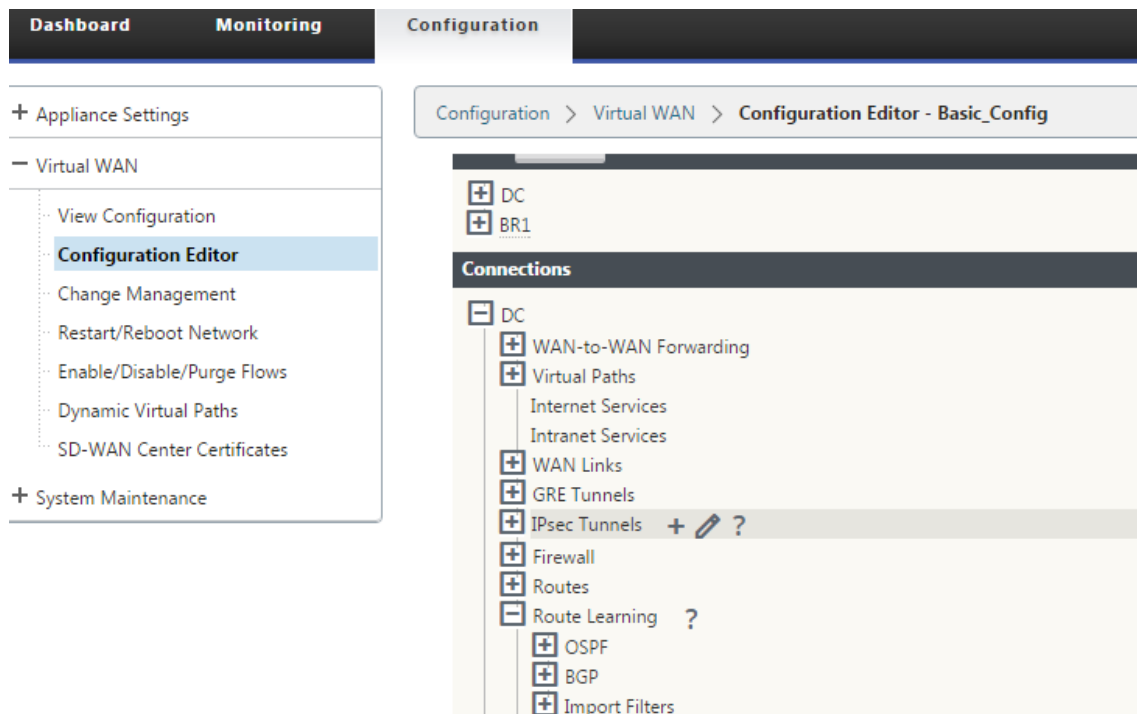
SD-WAN Web 管理インターフェイスでは、構成エディタに **[R **oute Learning] > [BGP]** の下に BGP ポリシーという新しいセクションが追加されました。** このセクションでは、ポリシーを構成する BGP 属性を追加できます。コミュニティストリングの追加、AS パスの先頭追加、および MED の設定がサポートされています。

各コミュニティストリングを手動で設定するか、ドロップダウンメニューから **[アドバタイズなし]** または **[エクスポートコミュニティストリングなし]** を選択できます。手動設定の場合、AS 番号とコミュニティを入力できます。 **[Insert/Remove]** を選択して、ルートにタグを付けたり、ルートからコミュニティを削除したりできます。

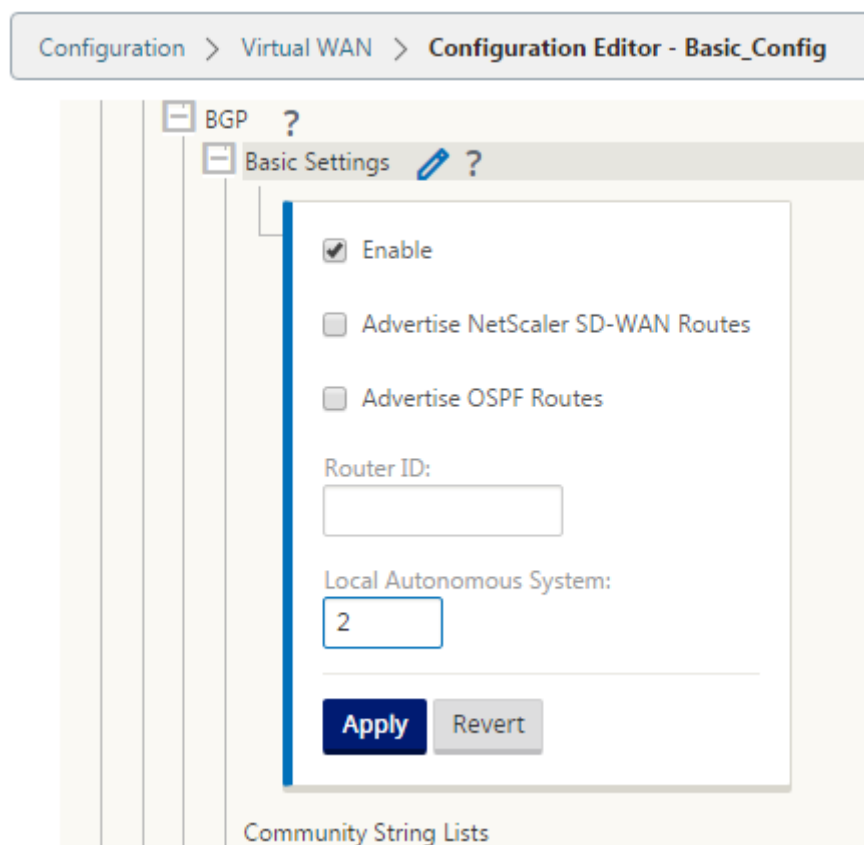
ローカルネットワークの外部をアドバタイズする前に AS パスにローカル AS を付加する回数を設定できます。ルートを照合するために MED を設定できます。

BGP ポリシーを設定するには、次の手順を実行します。

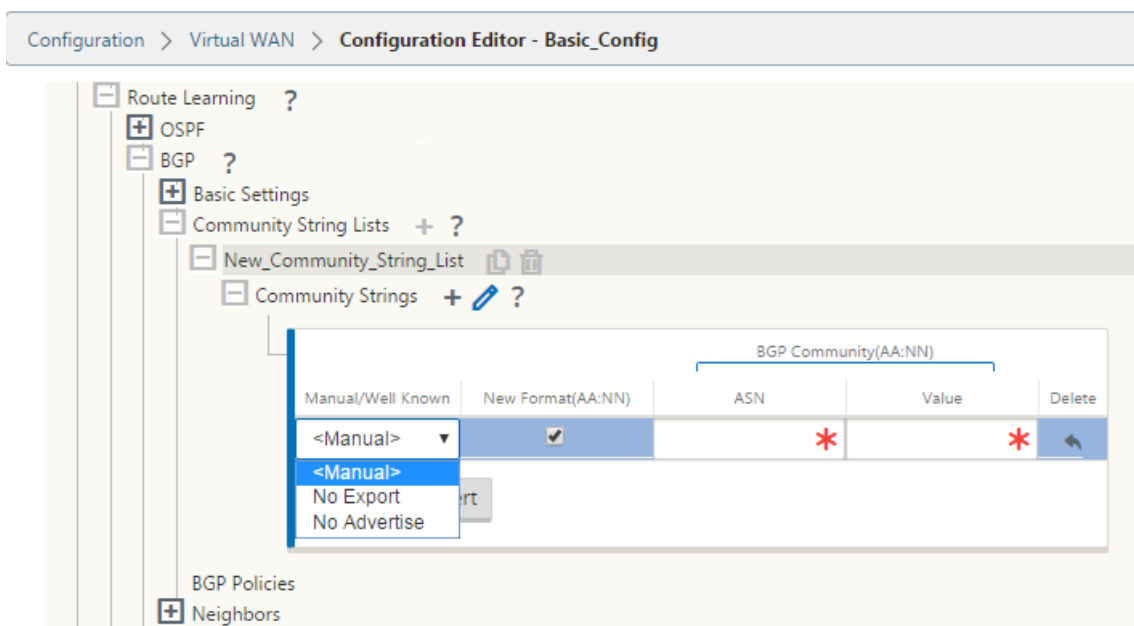
1. NetScaler SD-WAN Web 管理インターフェイスで、[構成] > [仮想 WAN] > [構成エディタ] の順に選択します。既存の構成パッケージを開きます。[サイト] > [**DC** または 支店 の設定] に移動します。



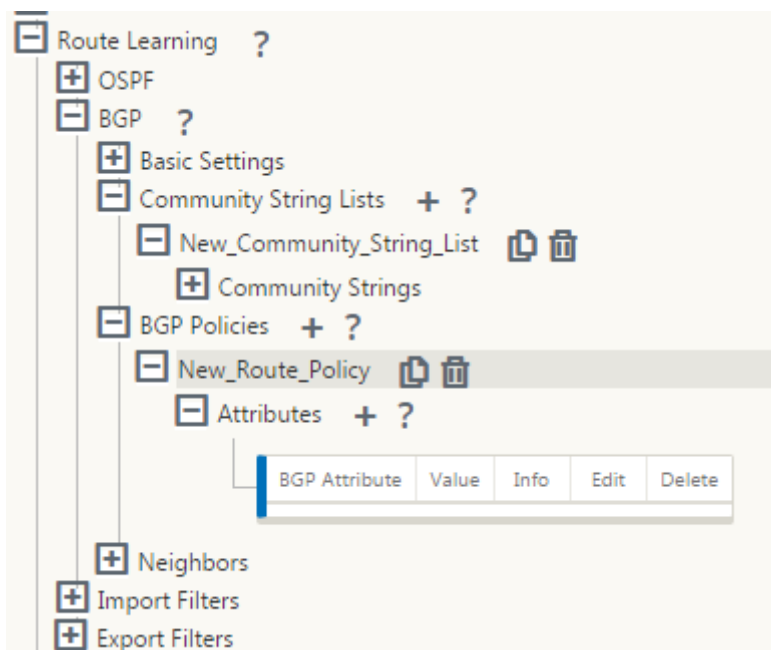
2. [**BGP**] を展開し、[基本設定] の [有効] をクリックします。ルータ **ID** と ローカル自律システム 値を入力し、[**Apply**] をクリックします。



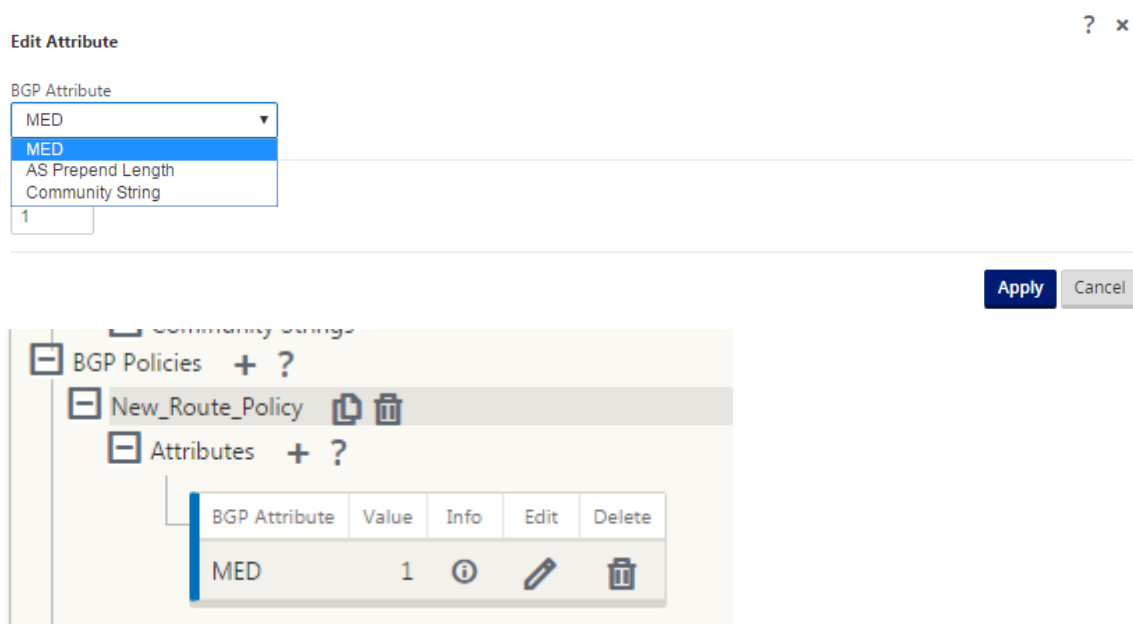
3. [コミュニティストリングリスト] の横にある [+] 記号をクリックします。各コミュニティストリングを手動で設定するか、ドロップダウンメニューから [アドバタイズなし] または [エクスポートコミュニティストリングなし] を選択します。手動設定の場合、AS 番号とコミュニティを入力できます。コミュニティストリングを含むルートに [**Insert/Remove** tagging] を選択するか、ピアから受信したルートからコミュニティストリングを削除できます。



4. BGP ポリシーを展開して、**BGP** ポリシーを設定します。BGP アトリビュートを 新しいルートポリシーに追加します。



5. BGP アトリビュートを編集するには、[Attributes] の横の [+] 記号をクリックします。「属性の編集」ウィンドウが表示されます。ドロップダウンメニューから目的の BGP 属性を選択します。選択に従って、[**MED**]、[**AS** プリペンド長]、または [コミュニティストリング] に値を入力します。[適用] をクリックします。



注

どのポリシーでも、1つの属性の出現は1つだけであり、同じ属性を複数回出現することはできません。2台のMEDまたは2台のASパスの先頭にすることはできません。先頭にMED/AS-PATHを追加/コミュニティストリング、またはその組み合わせを指定できます。

ネイバーの設定

eBGPを設定するには、既存のBGPネイバーセクションにカラムを追加して、ネイバーAS番号を設定します。SD-WAN 9.2 構成エディタを使用して以前の設定をインポートすると、このフィールドにはローカルAS番号があらかじめ入力されています。

また、ネイバー設定には、オプションの詳細セクション（展開可能な行）があり、各ネイバーのポリシーを追加できます。

アドバンストネイバーの設定

このオプションを使用すると、ネットワークオブジェクトを追加し、そのネットワークオブジェクトに設定されたBGPポリシーを追加できます。これは、特定のルートを照合するルートマップとACLを作成し、そのネイバーのBGP属性を設定するのと似ています。このポリシーが着信ルートまたは発信ルートに適用されているかどうかを示す方向を指定できます。

デフォルトのポリシー <accept> はすべてのルートに適用されます。承認ポリシーと拒否ポリシーはデフォルトで、変更できません。

ネットワークアドレス（宛先アドレス）、ASパス、コミュニティストリングに基づいてルートを照合し、ポリシーを割り当てて適用するポリシーの方向を選択できます。

ネイバーを設定するには、次の手順を実行します。

1. 次に示すように、[**Add**] をクリックしてネイバーを設定します。

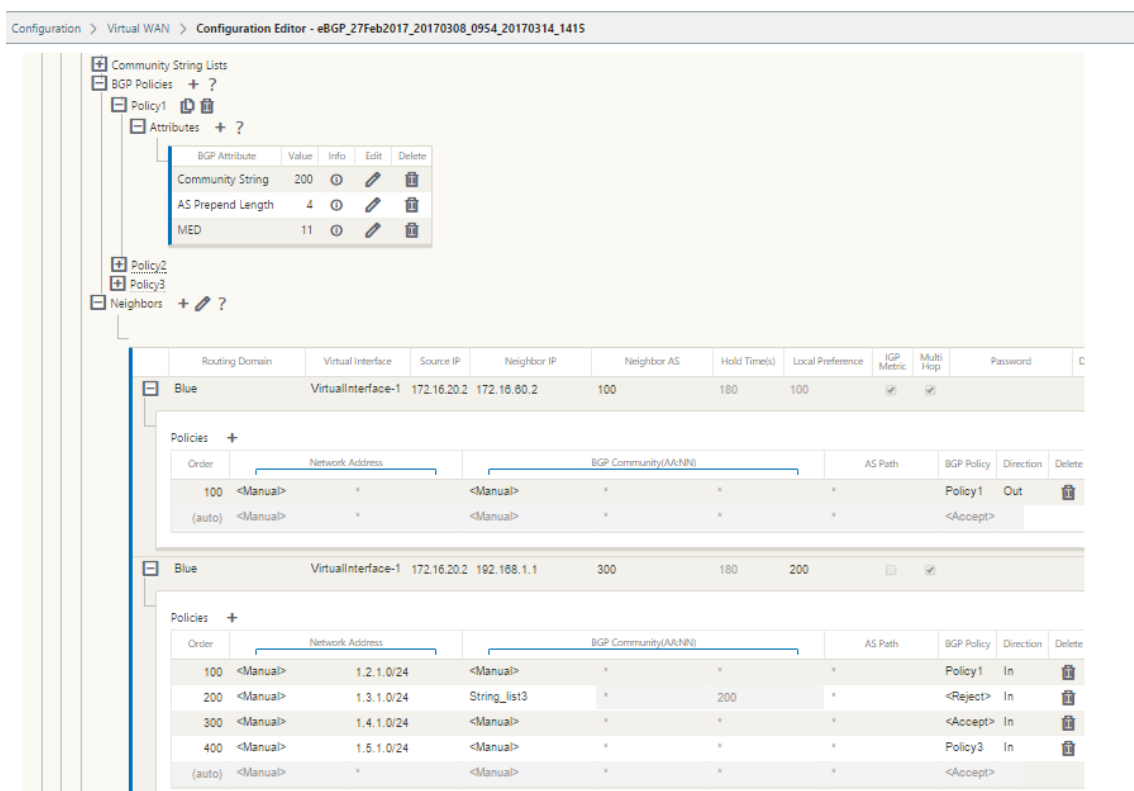
The screenshot shows the 'Neighbors' configuration page. At the top, there is a header with a minus icon, the word 'Neighbors', and a plus icon followed by a question mark. Below this is a table with columns: Interface, Source IP, Neighbor IP, Neighbor AS, Hold Time(s), Local Preference, IGP Metric, Multi Hop, Password, and Delete. An 'Add' button is located to the left of the 'Interface' column.

2. + 記号をクリックします。仮想インターフェイスを選択します。ネイバー **IP** アドレスを入力します。

The screenshot shows the 'Neighbors' configuration page with one neighbor added. The table has columns: Virtual Interface, Source IP, Neighbor IP, Neighbor AS, Hold Time(s), Local Preference, IGP Metric, Multi Hop, Password, and Delete. The first row shows 'VirtualInterface-1' for Virtual Interface, '172.58.1.20' for Source IP, a red asterisk for Neighbor IP, '2' for Neighbor AS, '180' for Hold Time(s), '100' for Local Preference, and checked boxes for IGP Metric and Multi Hop. Below the table is a 'Policies' section with an 'Add' button and a table with columns: Order, Network Address, BGP Community(AA:NN), AS Path, BGP Policy, Direction, and Delete. The 'Apply' and 'Revert' buttons are at the bottom.

3. ポリシーを追加します。必要に応じて、[ネットワークアドレス]、[**BGP コミュニティ**]、および [**AS** パスの詳細] を選択します。[適用] をクリックします。

The screenshot shows the 'Neighbors' configuration page with a policy added. The table has columns: Virtual Interface, Source IP, Neighbor IP, Neighbor AS, Hold Time(s), and Local Preference. The first row shows 'VirtualInterface-1' for Virtual Interface, '172.58.1.20' for Source IP, a red asterisk for Neighbor IP, '2' for Neighbor AS, '180' for Hold Time(s), and '100' for Local Preference. Below the table is a 'Policies' section with an 'Add' button and a table with columns: Order, Network Address, BGP Community(AA:NN), and AS Path. The first row shows '100' for Order, '<Manual>' for Network Address, '<Manual>' for BGP Community(AA:NN), and '*' for AS Path. A dropdown menu is open for the BGP Community(AA:NN) column, showing '<Manual>' and 'New_Community_String_List'. The 'Apply' and 'Revert' buttons are at the bottom.



4. [モニタリング] > [ルーティングプロトコル] > [ダイナミックルーティングプロトコル] の順に選択し、DC またはブランチサイトアプライアンスに設定された BGP ポリシーとネイバーを監視します。

デバッグロギングを有効にし、ルーティング用のログファイルを表示するには、[**Monitor**] > [**Routing Protocol**] ページを使用します。ルーティングデーモンのログは、別々のログファイルに分割されます。標準ルーティング情報は `dynamic_routing.log` に格納され、動的ルーティングの問題は `dynamic_routing_diagnostics.log` に格納されます。この情報は、ルーティングプロトコルの監視から参照できます。

BGP ソフト再設定

BGP ピアのルーティングポリシーには、インバウンドまたはアウトバウンドルーティングテーブルの更新に影響する可能性のあるルートマップ、配布リスト、プレフィクスリスト、フィルタリストなどの設定が含まれます。ルーティングポリシーに変更があった場合、新しいポリシーを有効にするには、BGP セッションをクリアまたはリセットする必要があります。

ハードリセットを使用して BGP セッションをクリアすると、キャッシュが無効になり、キャッシュ内の情報が利用できなくなると、ネットワークの動作に悪影響が生じます。

BGP ソフトリセット拡張機能は、格納されているルーティングテーブルの更新情報に依存しない着信 BGP ルーティングテーブルアップデートのダイナミックソフトリセットを自動的にサポートします。

トラブルシューティング

BGP パラメータを表示するには、[モニタリング] > [ルーティングプロトコル] に移動し、[**View**] フィールドから [**BGP State**] を選択します。

Dashboard

Monitoring

Configuration

Statistics

Flows

Routing Protocols

Firewall

IKE/IPsec

IGMP

Performance Reports

Qos Reports

Usage Reports

Availability Reports

Appliance Reports

DHCP Server/Relay

VRRP

PPPoE

DNS

Monitoring > Routing Protocols

Dynamic Routing Protocol

View: BGP State Routing Domain: Default_RoutingDomain BGP Session: <ALL>

Reset Session

Refresh

BGP State

name	proto	table	state	since	info
bgp1_rdomain_0	BGP	T0	up	2020-08-27 10:46:44	Established
Preference: 100					
Input filter: neighbour_0_in					
Output filter: neighbour_0_out					
Routes: 8 imported, 4 exported, 1 preferred					
Route change stats:					
Import updates:	received	rejected	filtered	ignored	accepted
Import withdraws:	16	0	0	8	8
Export updates:	0	0	---	0	0
Export withdraws:	43	19	18	---	6
Export withdraws:	2	---	---	---	2
BGP state: Established					
Neighbor address: 172.58.1.28					
Neighbor AS: 10					
Citrix SD-WAN Interface: vni-0					
Neighbor ID: 105.105.105.105					
Neighbor caps: refresh AS4					
Session: internal multihop AS4					
Source address: 172.58.1.10					
Hold timer: 130/180					
Keepalive timer: 46/60					

ダイナミックルーティングログを確認して、BGP コンバージェンスに問題がないかどうかを確認できます。

Diagnose

Debug Logging: ☒ On ☐ Off

Filename:

dynamic_routing_diagnostics.log

View Log

iBGP

May 10, 2021

iBGP が LAN 側に、eBGP が WAN 側に Citrix SD-WAN アプライアンス:

Citrix SD-WAN アプライアンスは、LAN 側に iBGP、WAN 側に eBGP を使用して展開すると、NEXT HOP SELF を使用して IGP ドメインに学習されたすべての eBGP ルートをアドバタイズします。

リニアネットワークポロジ内の複数の iBGP LAN ルーターは、ダイレクトピアリング機能を持ち、Citrix SD-WAN でメッシュ化されています。

制限事項:

- AS パスプリペンド、Med、およびコミュニティ属性はサポートされていません。
- 再配布中の OSPF と BGP 間のルートフィルタリングはサポートされていません。OSPF から学習されたルートはすべて BGP ピアにアドバタイズされるか（または）、その逆も同様です。
- ルート集約はサポートされていません。
- 最大 16 の BGP ピア（iBGP および eBGP を含む）だけを設定できます。

eBGP

May 10, 2021

eBGP 経由で非 SD-WAN サイトと通信する SD-WAN サイト

SD-WAN アプライアンスのないサイトが、単一の WAN パスで SD-WAN アプライアンス（サイト A）を使用する別のサイトと通信している場合（インターネットのみが使用可能）、SD-WAN アプライアンスのあるサイト（サイト A）がインターネット接続を失った場合、SD-WAN を使用しないサイトは、別の SD-WAN を介してサイト A と通信できます。アプライアンスサイト（サイト B）で設定します。サイト B は、SD-WAN アプライアンスのないサイトからサイト A にトラフィックをファネルします。

仮想パスと eBGP を使用した SD-WAN サイト間の通信

Virtual WAN アプライアンスが稼働している間に、2 つのサイト間で仮想パスがダウンしている場合に、リモートサイトのローカルサブネットと通信するためのアンダーレイルートラーニングを提供します。

アプリケーションルート

May 10, 2021

一般的なエンタープライズネットワークでは、ブランチオフィスはオンプレミスデータセンター、クラウドデータセンター、または SaaS アプリケーション上のアプリケーションにアクセスします。アプリケーションルーティング機能により、ネットワークを介してアプリケーションを簡単かつコスト効率よく操作できます。たとえば、ブランチサイトのユーザーが SaaS アプリケーションにアクセスしようとする、ブランチオフィスが最初にデータセンターを経由することなく、インターネット上の SaaS アプリケーションに直接アクセスできるように、トラフィックをルーティングできます。

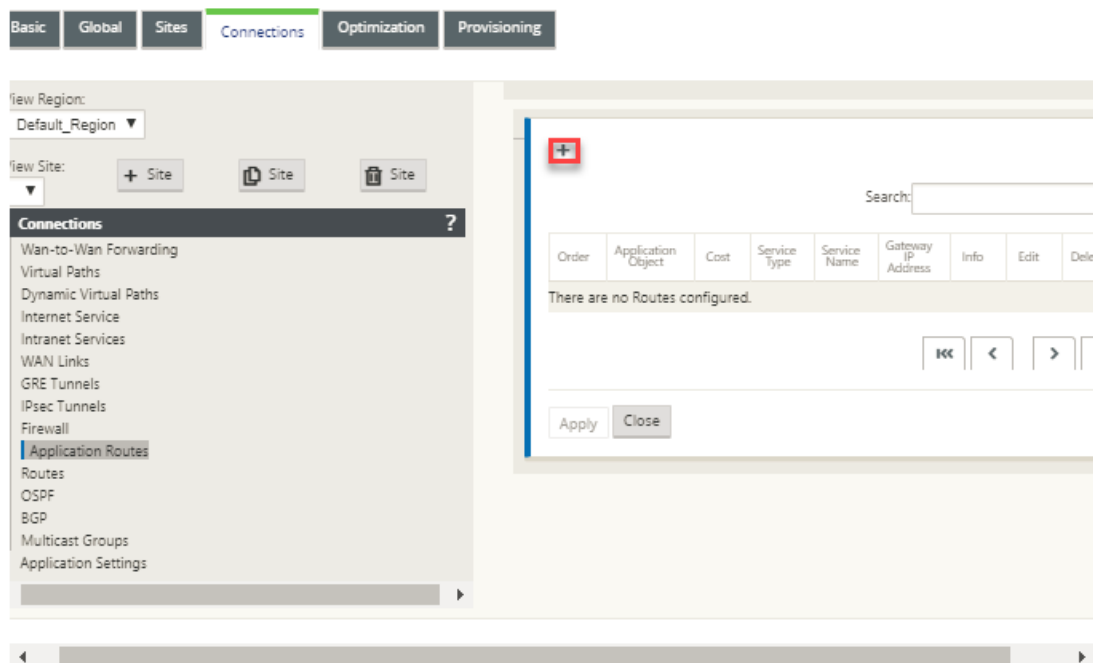
Citrix SD-WAN では、次のサービスのアプリケーションルートを定義できます。

- **仮想パス:** このサービスは、仮想パスを通過するトラフィックを管理します。仮想パスは、2 つの WAN リンク間の論理リンクです。これは、2 つの SD-WAN ノード間で高いサービス・レベル通信を提供するために結合された WAN パスの集合で構成されます。SD-WAN アプライアンスは、パス単位でネットワークを測定し、変化するアプリケーション需要や WAN 条件に適応します。仮想パスは、スタティック（常に存在）またはダイナミック（2 つの SD-WAN アプライアンス間のトラフィックが設定されたしきい値に達した場合のみ存在）のいずれかになります。
- **インターネット:** このサービスは、エンタープライズサイトとパブリックインターネット上のサイト間のトラフィックを管理します。インターネットトラフィックはカプセル化されません。輻輳が発生すると、SD-WAN は、仮想パス、およびイントラネットトラフィックに対するレート制限によって、帯域幅を積極的に管理します。
- **イントラネット:** このサービスは、仮想パス経由の送信用に定義されていないエンタープライズイントラネットトラフィックを管理します。イントラネットトラフィックはカプセル化されません。SD-WAN は、輻輳時にこのトラフィックを他のサービスタイプと比較してレート制限することにより、帯域幅を管理します。特定の条件下では、イントラネットフォールバックが仮想パス上に構成されている場合、通常は仮想パスを通過するトラフィックは、代わりにイントラネットトラフィックとして扱うことができます。
- **ローカル:** このサービスは、他のサービスと一致しないサイトへのローカルトラフィックを管理します。SD-WAN は、ローカルルートを送信元および宛先とするトラフィックを無視します。
- **GRE トンネル:** このサービスは、GRE トンネル宛の IP トラフィックを管理し、サイトで設定された LAN GRE トンネルに一致します。GRE トンネル機能を使用すると、LAN 上の GRE トンネルを終了するように SD-WAN アプライアンスを設定できます。サービスタイプ GRE Tunnel のルートの場合、Gateway はローカル GRE トンネルのトンネルサブネットの 1 つに存在する必要があります。
- **LAN IPsec トンネル:** このサービスは、LAN IPsec トンネル宛の IP トラフィックを管理し、サイトで構成された LAN IPsec トンネルを照合します。LAN IPsec トンネル機能を使用すると、LAN または WAN 側で IPsec トンネルを終了するように SD-WAN アプライアンスを構成できます。

アプリケーションのサービスステアリングを実行するには、最初のパケット自体でアプリケーションを識別することが重要です。最初は、トラフィックが分類され、アプリケーションが認識されると、パケットは IP ルートを通過します。対応するアプリケーションルートが使用されます。最初のパケット分類は、アプリケーションオブジェクトに関連付けられた IP サブネットとポートを学習することによって達成されます。これらは、DPI 分類器の履歴分類結果とユーザ設定の IP ポート一致タイプを使用して取得されます。

アプリケーション・ルーティングを構成するには、次の手順に従います。

1. 構成エディタで、[接続] > [アプリケーションルート] に移動し、[+] をクリックします。



2. [追加] ページで、次のパラメータを設定します。

- **アプリケーション・オブジェクト**: 操作するアプリケーション・オブジェクト。ここで作成したアプリケーションオブジェクトが一覧表示されます。詳細については、[アプリケーション分類](#)トピックの「アプリケーションオブジェクト」セクションを参照してください。

- **ルーティングドメイン**: アプリケーションルートで使用するルーティングドメイン。設定済みのルーティングドメインの1つを選択します。
- **コスト**: このルートのルート優先度を決定する重み。低コストのルートは、高コストのルートよりも優先されます。指定できる範囲は1～65534です。デフォルト値は5です。
- **サービスタイプ**: 次のサービスのいずれかを選択します。これにより、アプリケーションがサービスに

マッピングされます。

- 仮想パス: アプリケーショントラフィックを仮想パストラフィックとして識別し、仮想パスルールに基づいて仮想パスを照合します。[**Next Hop Site**] フィールドに、仮想パスパケットの送信先となるネクストホップリモートサイトを入力します。

注

仮想パスアプリケーションルートに到達するフローは、ダイナミック仮想パスを通過しません。

- インターネット: アプリケーショントラフィックをインターネットトラフィックとして識別し、インターネットサービスと照合します。
- [イントラネット]: アプリケーショントラフィックをイントラネットトラフィックとして識別し、イントラネットルールに基づいてイントラネットサービスと照合します。[イントラネットサービス] フィールドで、ルートに使用するイントラネットサービスを選択します。
- [ローカル]: アプリケーショントラフィックをサイトに対してローカルとして識別し、サービスと一致しません。ローカルルートをソースおよび宛先とするトラフィックは無視されます。

注

ローカルサービスタイプの場合、DPI 分類が完了すると、設定された IP ルートがルーティング決定を行います。

- **GRE** トンネル: アプリケーショントラフィックが GRE トンネルの宛先であると識別され、サイトで設定された LAN GRE トンネルと一致します。[**Gateway IP Address**] フィールドに、LAN GRE トンネルのサブネット内にある必要のあるゲートウェイの IP アドレスを入力します。ゲートウェイに到達できないときにルートがトラフィックを受信しないようにするには、[ゲートウェイに基づく適格性] を選択します。
- **LAN IPsec** トンネル: アプリケーショントラフィックが LAN IPsec トンネル宛てであると識別され、サイトで構成された LAN IPsec トンネルと一致します。[**IPSec Tunnel**] フィールドで、設定済みの IPSec トンネルの 1 つを選択します。トンネルに到達できないときにルートがトラフィックを受信しないようにするには、[トンネルに基づく適格性] を選択します。

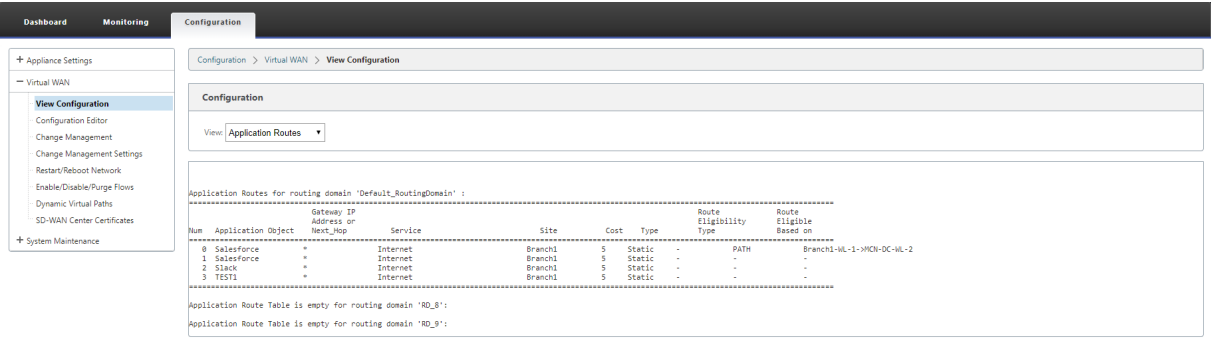
注

カスタムアプリケーションのサービスを選択したら、そのサービスを変更しないでください。

- [パスに基づく適格性]: 指定したパスがダウンしたときにルートがトラフィックを受信しないようにする場合に選択します。[**Path**] フィールドで、ルートの適格性の決定に使用するパスを指定します。

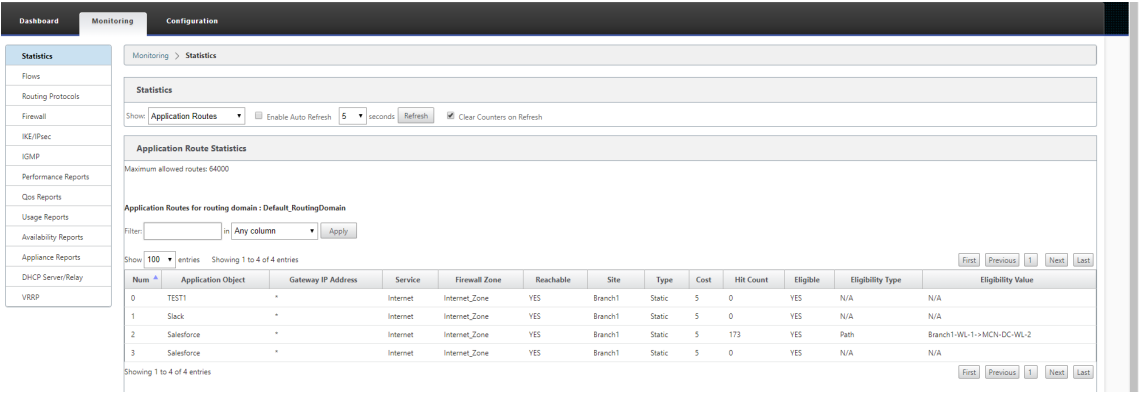
3. [適用] をクリックします。

SD-WAN アプライアンスに構成されているアプリケーションルートを表示する。SD-WAN GUI で、[設定] > [仮想 WAN] > [設定の表示] に移動します。[表示] ドロップダウンメニューから [アプリケーションルート] を選択します。



アプリケーション・ルートの統計データを表示する手順は、次のとおりです。

1. SD-WAN GUI で、[モニタリング] > [統計] に移動します。
2. [表示] ドロップダウンリストから、[アプリケーションルート] を選択します。



次の統計を表示できます。

- アプリケーション・オブジェクト: アプリケーション・オブジェクトの名前。
- **Gateway IP** アドレス: GRE トンネルサービスタイプのアプリケーションオブジェクトで使用するゲートウェイ IP アドレス。
- サービス: アプリケーション・オブジェクトにマップされたサービス・タイプ。
- ファイアウォールゾーン: このルートが属するファイアウォールゾーン。
- 到達可能: アプリケーションルートのステータス。
- サイト: サイトの名前。
- **[Type]**: ルートが静的か動的かを示します。
- コスト: ルートの優先度。
- **Hit Count**: トラフィックを処理するためにアプリケーションルートが使用される回数。
- 適格: アプリケーションルートがトラフィックを送信できるかどうかを示します。
- 適格タイプ: この工順に適用される工順適格条件のタイプ。適格性タイプは、パス、ゲートウェイ、またはトンネルです。
- 適格値: 工順適格条件に対して指定された値。

注

現在のリリースでは、アプリケーションファミリに属するアプリケーションオブジェクト（アプリケーションオブジェクトで定義されているマッチタイプ）は操作できません。

トラブルシューティング

アプリケーションルートを作成したら、[**Monitoring**] セクションを使用して、目的のサービスにアプリケーションが正しくルーティングされていることを確認できます。

アプリケーションが目的のサービスに正しくルーティングされているかどうかを確認するには、次のページに移動します。

- モニタリング > 統計 > アプリケーションルート
- モニタリング > フロー
- モニタリング > ファイアウォール

予期しないルーティング動作が発生した場合は、問題が発生している間に STS 診断バンドルを収集し、Citrix サポートチームと共有します。

STS バンドルは、[構成] > [システムメンテナンス] > [診断] > [診断情報] を使用して作成およびダウンロードできます。

ルートフィルタリング

May 10, 2021

ルート学習が有効なネットワークの場合、Citrix SD-WAN により、ルーティングネイバーにアドバタイズされる SD-WAN ルートと、ルーティングネイバーから受信されるルートをより詳細に制御できます。

- エクスポートフィルタは、特定の一致基準に基づいて OSPF および BGP プロトコルを使用してアドバタイズメント用のルートを含めるか除外するために使用されます。エクスポートフィルタルールは、ダイナミックルーティングプロトコルで SD-WAN ルートをアドバタイズするときに満たす必要があるルールです。デフォルトでは、すべてのルートがピアにアドバタイズされます。
- インポートフィルタは、特定の一致基準に基づいて OSPF および BGP ネイバーを使用して受信したルートを受け入れるか、受け付けないかに使用します。インポートフィルタルールは、ダイナミックルートを SD-WAN ルートデータベースにインポートする前に満たす必要があるルールです。デフォルトでは、ルートはインポートされません。

ルートフィルタリングは、SD-WAN ネットワーク（データセンター/ブランチ）の LAN ルートおよび仮想パスルートに実装され、BGP と OSPF を使用して SD-WAN 以外のネットワークにアドバタイズされます。




最大 512 のエクスポートフィルタと 512 のインポートフィルタを設定できます。これは、ルーティングドメインごとの制限ではなく、全体的な制限です。

エクスポートフィルタの構成

構成エディタで、[接続]>[リージョン]>[サイト]>[OSPF]または[BGP]>[フィルタのエクスポート]に移動します。

Section: Export Filters

+

	Order	Network Address	Prefix	Citrix SD-WAN Cost	Service Type	Site/Service Name	Gateway IP Address	Include	Enabled	Delete	Clone			
	100	<Manual>	10.102.29.220/16	eq	12	eq	10	Virtual Path	Client-1	*	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
<div>Export OSPF Route Type: Type 5 AS External</div> <div>Export OSPF Route Weight: 4</div>														
	100	<Manual>	*	eq	*	eq	*	Any	<Any>	*	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		

Apply Revert

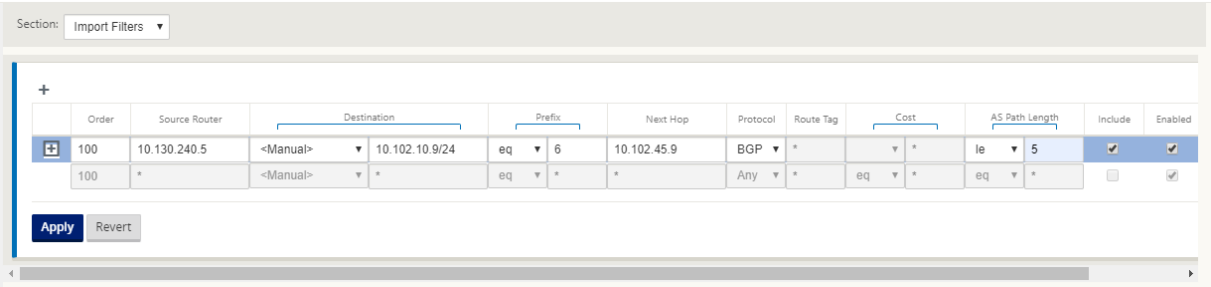
作成する各エクスポートフィルタを作成するには、次の基準を使用します。

フィールド条件	説明	値
Order	フィルタが優先される順序。ルートが一致する最初のフィルタは、そのルートに適用されます	100, 200, 300, 400, 500, 600
ネットワークアドレス	ルートのネットワークを記述する設定済みの Network Object の IP アドレス とサブネットマスクを入力します。	<ul style="list-style-type: none"> IP アドレス
前	プレフィクスでルートを照合するには、メニューから一致述語を選択し、隣接するフィールドに Route プレフィクスを入力します。	<ul style="list-style-type: none"> eq: 等しい,- lt: より小さい,- le: より小さい,- gt: より大きい,- ge: より大きい
Citrix SD-WAN コスト	エクスポートされたルートの選択を絞り込むために使用される方法（述語）と SD-WAN ルートコスト	数値
サービスの種類	Citrix SD-WAN サービスのリストから、一致するルートに割り当てられるサービスタイプを選択します。	任意、ローカル、仮想パス、インターネット、イントラネット、LAN GRE トンネル、LAN IPsec トンネル

フィールド条件	説明	値
サイト/サービス名	イントラネット、LAN GRE トンネル、および LAN IPsec トンネルの場合は、使用する構成済みのサービスタイプの名前を指定します。	テキスト文字列
Gateway IP アドレス	サービスタイプとして LAN GRE トンネルを選択した場合は、トンネルの Gateway IP を入力します。	IP アドレス
含める	[このフィルタに一致するルートを含める] チェックボックスをオンにします。それ以外の場合、一致するルートは無視されます	なし
有効です	[このフィルタを有効にする] チェックボックスをオンにします。それ以外の場合、フィルタは無視されます	なし
削除	このフィルタを削除するには、削除アイコンを選択します。	なし
複製	既存のフィルターのコピーを作成するには、クローンアイコンをクリックします。	なし

インポートフィルタの構成

構成エディタで、[接続] > [リージョン] > [サイト] > [OSPF] または [BGP] > [フィルタのインポート] に移動します。



作成する各エクスポートフィルタを作成するには、次の基準を使用します。

フィールド条件	説明	値
Order	フィルタが優先される順序。ルートが一致する最初のフィルタは、そのルートに適用されます	100, 200, 300, 400, 500, 600
送信元ルータ	送信元ルータの IP アドレス。iBGP だけに適用されます。	• IP アドレス
接続先	ルートの宛先の IP アドレスとサブネットマスク	• IP アドレス
前	プレフィクスでルートを照合するには、メニューから一致述語を選択し、隣接するフィールドに Route プレフィクスを入力します。	• eq: 等しい,- lt: より小さい,- le: より小さい,- gt: より大きい,- ge: より大きい
次ホップ	ネクストホップの IP アドレス	• IP アドレス
プロトコル	ルートの学習に使用するルーティングプロトコル	OSPF または BGP
ルートタグ	フィルタが一致する OSPF ルートタグ。OSPF ルートタグにより、OSPF と他のプロトコル間の相互再配布中のルーティングループを防止	数値
コスト	インポート用の OSPF ルートの照合に使用されるルートコスト	数値
AS パスの長さ	インポート用の BGP ルートの照合に使用される AS パスの長さ	数値
含める	[このフィルタに一致するルートを含める] チェックボックスをオンにします。それ以外の場合、一致するルートは無視されます	なし
有効です	[このフィルタを有効にする] チェックボックスをオンにします。それ以外の場合、フィルタは無視されます	なし
削除	このフィルタを削除するには、[削除] アイコンをクリックします。	なし
複製	既存のフィルターのコピーを作成するには、クローンアイコンをクリックします。	なし

ルートポリシーフィルタテンプレートの設定

さまざまなフィルタルールを使用して複数のインポートフィルタテンプレートまたはエクスポートフィルタテンプレートを作成し、各サイトでテンプレートを関連付けることができます。

ユーザーが作成したサイトレベルのインポート/エクスポートフィルタルールがより優先されます。テンプレートルールは、接続の **R**oute **L**earning セクションでサイトに関連付けられると、ユーザが作成したルールに従います。

The image displays two screenshots of the Citrix SD-WAN management interface, specifically the 'Connections' tab. Both screenshots show the 'View Region' set to 'Default_Region' and the 'View Site' dropdown set to an empty state. The 'Connections' list on the left includes: WAN-to-WAN Forwarding, Virtual Paths, Dynamic Virtual Paths, Internet Service, Intranet Services, WAN Links, GRE Tunnels, IPsec Tunnels, Firewall, Application Routes, Routes, OSPF, BGP, Route Learning Properties (highlighted), Multicast Groups, and Application Settings.

The top screenshot shows the 'Import Template' section on the right. It contains a dropdown menu for 'Import Filter Template' and two buttons: 'Apply' and 'Refresh'.

The bottom screenshot shows the 'Export Template' section on the right. It contains a dropdown menu for 'Export Filter Template' and two buttons: 'Apply' and 'Refresh'.

ルート集約

May 10, 2021

企業ネットワークのサイズが大きくなるにつれて、ルータはルーティングテーブル内の多数のルートを維持する必要があります。ルータでは、大規模なルーティングテーブルを検索し、個々のルートを維持するために、CPU、メモリ、および帯域幅のリソースを増やす必要があります。サマリールートには、ローカルサービスタイプと廃棄サービスタイプを設定できます。このサマリールートは、ネクストホップデバイスにアドバタイズされます。

ローカルサブネットのサマリールートを設定するには、次の手順を実行します。

1. 設定エディタで、[接続] > [ルート] に移動し、[+] をクリックしてルートを追加します。
2. [ルートの追加] ページで、次のパラメータを設定し、[追加] をクリックします。
 - ネットワーク **IP** アドレス: 計算されたサマリールート IP アドレス。
 - コスト: このルートのルート優先度を決定する重み。低コストのルートは、高コストのルートよりも優先されます。指定できる範囲は 1 ~15 です。デフォルト値は 5 です。
 - ルーティングドメイン: 企業ネットワーク、ブランチオフィスネットワーク、データセンターネットワークを管理するための単一の管理ポイントを提供するルーティングプロトコル。
 - [サービスタイプ]: [ローカルサービスタイプ] を選択します。

注

サマリールートには、ローカル サービスタイプと 廃棄 サービスタイプだけを選択できます。

- ゲートウェイ **IP** アドレス: このルートのゲートウェイ IP アドレス。
- [ルートをエクスポート]: ルートを他の接続されたサイトにエクスポートします。
- **Summary Route**: 他のすべての一致するサブネットではなく、接続されている他のデバイスに、ルートを 1 つのサマリールートとしてアドバタイズします。

?

x

Add

Network IP Address

172.16.0.0/22

Routing Domain

Default_Routing[▼

Cost

5

Service Type

Local ▼

Gateway IP Address

☒ Export Route

☒ Summary Route

☐ Eligibility Based On Path

Path:

<None> ▼

☐ Eligibility Based On Gateway

Add

Cancel

トラブルシューティング

MCN で設定された集約ルートは、仮想パスを経由してブランチに送信されます。ブランチのルートテーブルに仮想パスの詳細が表示されない場合は、ブランチダッシュボードを確認します。ダッシュボードには、MCN とブランチ間の仮想パスのステータスが表示されます。

Dashboard **Monitoring** **Configuration**

System Status

Name:	BR1_VPX
Model:	VPX
Sub-Model:	BASE
Appliance Mode:	Client
Serial Number:	5f4519dd-e39a-d3f6-24a6-6ba0e6578d2c
Management IP Address:	10.105.172.7
Appliance Uptime:	6 days, 56 minutes, 1.4 seconds
Service Uptime:	6 days, 50 minutes, 39.0 seconds
Routing Domain Enabled:	Default_RoutingDomain

Local Versions

Configuration Created On:	Wed Sep 2 11:15:54 2020
Software Version:	11.2.1.53.864510
Built On:	Aug 25 2020 at 19:02:21
Hardware Version:	VPX
OS Partition Version:	5.1

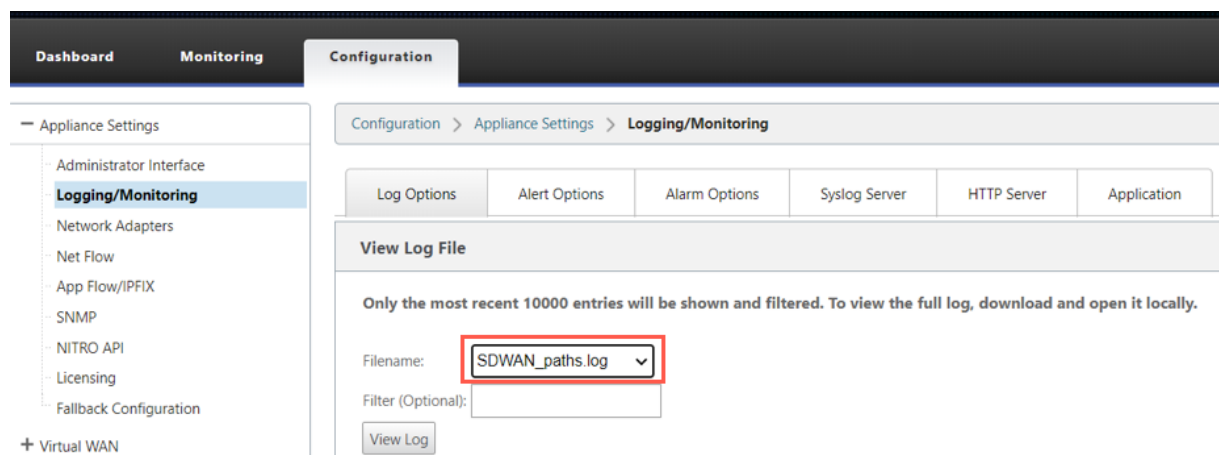
Virtual Path Service Status

Virtual Path MCN_VPX-BR1_VPX	Uptime: 6 days, 50 minutes, 19.0 seconds.
------------------------------	---

仮想パスがダウンしている場合は、[構成]>[ログ/監視]で、その理由を確認します。

[ファイル名] ドロップダウンリストから、次のいずれかのファイルを選択して、検証します。

- SDWAN_paths.log
- SDWAN_common.log



プロトコルプリファレンス

May 10, 2021

プロトコルの優先設定は、Citrix SD-WAN 固有の機能です。これは、ルータのアドミニストレーティブディスタンスに似ています。

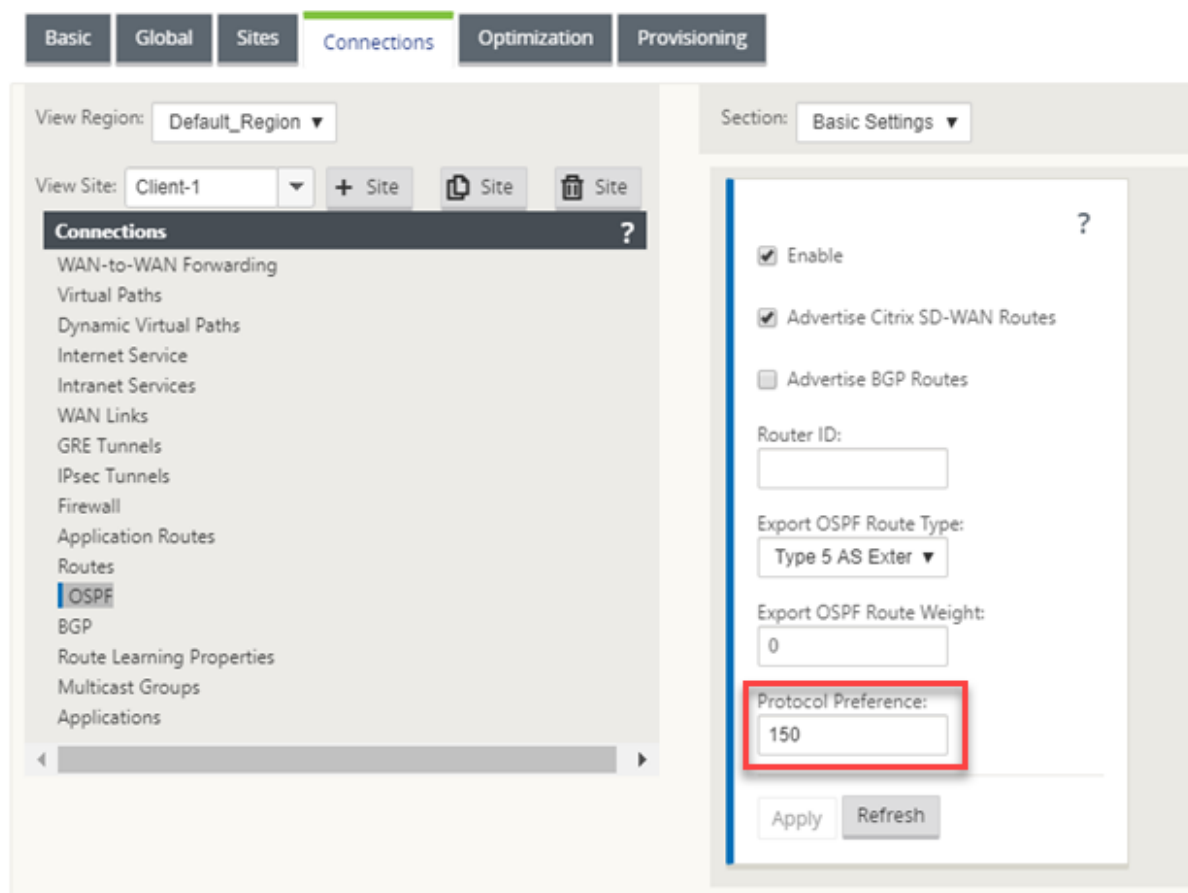
Citrix SD-WAN が仮想パス、OSPF プロトコル、または BGP プロトコルを介してルートプレフィックスを同時に学習する場合、次のデフォルトの優先順位に従います。

- OSPF-150
- BGP-100
- SD-WAN-250

優先順位が最も高いプロトコルが最も優先されます。プロトコルプリファレンス値が最も高いプロトコルを使用するルート

また、BGP または OSPF プロトコルを設定しながら、プロトコルプリファレンス値を設定することで、OSPF プロトコル上で BGP プロトコルを使用することもできます。100 ～200 の範囲でプリファレンスを指定できます。

プロトコルの優先順位情報は Citrix SD-WAN アプライアンスのローカルであり、ピアネットワーク要素にはアドバタイズされません。



マルチキャストルーティング

May 10, 2021

マルチキャストルーティングにより、1 対多のトラフィックを効率的に配信できます。マルチキャスト送信元は、マルチキャストトラフィックを 1 つのストリームでマルチキャストグループに送信します。マルチキャストグループには、マルチキャスト通信に IGMP プロトコルを使用するホストや隣接ルータなどのレシーバが含まれます。Voice over IP、ビデオオンデマンド、IP テレビ、およびビデオ会議は、マルチキャストルーティングを使用する一般的なテクノロジーの一部です。Citrix SD-WAN アプライアンスでマルチキャストルーティングを有効にすると、アプライアンスはマルチキャストルーターとして機能します。

送信元固有のマルチキャスト

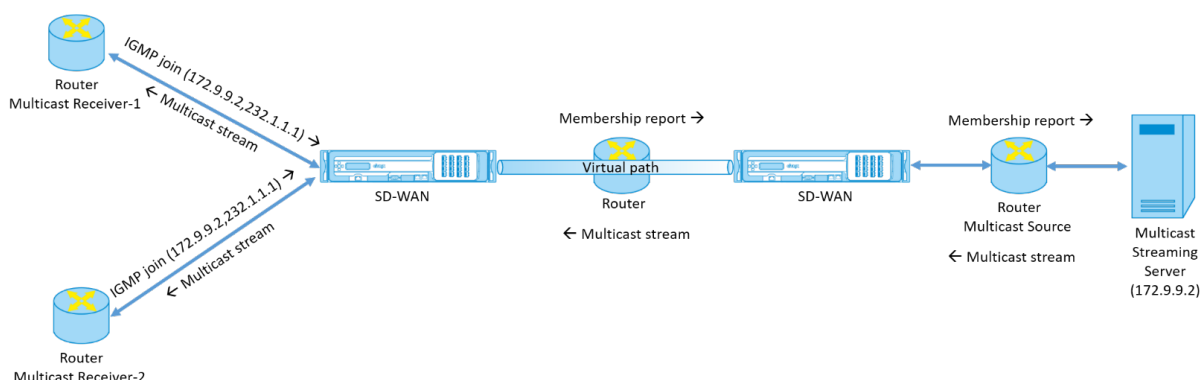
通常、マルチキャストプロトコルを使用すると、マルチキャストレシーバは任意の送信元からマルチキャストトラフィックを受信できます。Source Specific Multicast (SSM; ソース固有マルチキャスト) では、レシーバがマルチキャストトラフィックを受信する送信元を指定できます。これにより、レシーバは、マルチキャストストリームを送信

するすべてのソースに対してオープンリスナーではなく、特定のマルチキャストソースをリスンすることを保証します。SSM は、考えられるすべての送信元からのトラフィックの消費に使用されるリソースのコストを削減します。また、受信者が既知の送信者からのトラフィックを確実に受信することによって、セキュリティ層を提供します。

次のトポロジは、ブランチサイトの 2 つのマルチキャストレシーバと、データセンターの 1 つのマルチキャストサーバ (172.9.9.2) を示しています。マルチキャストサーバは特定のグループ (232.1.1.1) でトラフィックをストリーミングし、レシーバはグループに参加します。マルチキャストグループでストリーミングされるトラフィックは、グループに加入したすべてのレシーバに中継されます。

注

SSM が機能するためには、マルチキャストグループ IP が 232.0.0.0/8 の範囲内にある必要があります。



1. マルチキャストレシーバは、IP IGMP Join 要求を送信します。これは、レシーバがマルチキャストグループに加入し、送信元からマルチキャストストリームを受信することを示します。IGMP Join には、マルチキャスト送信元とグループ (S, G) の 2 つの属性が含まれます。IGMP バージョン 3 は、マルチキャスト送信元および受信側の SSM に使用され、一部の include 特定の送信元アドレスをリレーします。SSM を使用すると、レシーバは特定のマルチキャストサーバからストリームを明示的に受信できます。その送信元アドレスは、JOIN 要求の一部としてレシーバによって明示的に提供されます。この例では、IGMP v3 Join 要求が、ソース 172.9.9.2 を含む明示的なインクルード送信元リストを使用してトリガーされ、グループ 232.1.1.1 経由でマルチキャストストリームを送信するアドレスになります。
2. 支店の Citrix SD-WAN は、これらの受信機からのすべての IGMP 要求をリスンし、それをメンバーシップレポートに変換し、仮想パス経由でデータセンターの SD-WAN アプライアンスに送信します。
3. データセンターの Citrix SD-WAN アプライアンスは、仮想パスを介してメンバーシップレポートを受信し、マルチキャストソースに転送し、制御チャネルを確立します。
4. マルチキャスト送信元は、仮想パスを介してマルチキャストストリームをマルチキャストレシーバに送信します。

コントロールチャネルトラフィックとマルチキャストストリームは、ブランチとデータセンター間の確立された仮想パスを通過します。Citrix SD-WAN オーバーレイパスにより、マルチキャストトラフィックが WAN の劣化やリンクの停止を防ぐことができます。

マルチキャストの構成

マルチキャストを設定するには、送信元と宛先の両方で SD-WAN アプライアンスで次の操作を実行します。

1. マルチキャストグループの作成: マルチキャストグループの名前と IP アドレスを指定します。マルチキャストグループ IP は、送信元固有のマルチキャストに対して 232.0.0.0/8 の範囲内に必要があります。
2. IGMP プロキシを有効にする—Citrix SD-WAN アプライアンスを IGMP プロキシとして構成し、マルチキャストルーティング用の IGMP 制御チャンネル情報を伝送できます。IGMP V3 は、単一送信元マルチキャストに必要です。
3. アップストリームおよびダウンストリームサービスの定義: アップストリームインターフェイスにより、IGMP PROXY は、トラフィックをストリームする実際のマルチキャストソースに近い SD-WAN アプライアンスに接続できます。ダウンストリームインターフェイスを使用すると、IGMP Proxy は、トラフィックをストリームする実際のマルチキャストソースから遠く離れたホストに接続できます。
アップストリームとダウンストリームのサービスは、ソースのアプライアンスとデスティネーションのアプライアンスで異なります。

Citrix SD-WAN アプライアンスでマルチキャストを構成するには、[接続] > [マルチキャストグループ] に移動します。マルチキャストグループの名前と IP アドレスを指定して、マルチキャストグループを作成します。[**IGMP** プロキシを有効にする] をクリックします。

The screenshot shows the 'Multicast Groups' configuration page. At the top, there's a dropdown for 'Multicast Groups' set to 'Grp2' and a 'Section' dropdown set to 'Basic Settings'. Below these are two buttons: '+ Group' and 'Group' with a trash icon. A modal dialog is open in the center with the following fields: 'Group Name:' with 'Grp2' entered, 'Multicast Group IP:' with '232.1.1.1' entered, and a checked checkbox for 'Enable IGMP Proxy'. At the bottom of the dialog are 'Apply' and 'Revert' buttons.

ブランチアプライアンスおよびデータセンターアプライアンスのアップストリームパスとダウンストリームパスを設定します。

アプライアンスがマルチキャストレシーバ（ブランチ）に近い場合、アプライアンスは仮想パスインターフェイスでマルチキャストトラフィックを受信し、ローカルインターフェイス上のトラフィックを受信者に送信します。

Multicast Groups: Grp2 ▼ Section: Service ▼

+ Group - Group

Service Type	Service Instance	Direction	Upstream	Delete
Virtual Path ▼	BANGALOR... ▼	Receive ▼	<input checked="" type="checkbox"/>	
Local ▼	DAKC_Airtel... ▼	Send ▼	<input type="checkbox"/>	

Apply Refresh

アプライアンスがマルチキャストソース（データセンター）に近い場合、アプライアンスはローカルインターフェイスでマルチキャストトラフィックを受信し、仮想パスインターフェイス上でトラフィックを送信します。

Multicast Groups: DC1_Grp ▼ Section: Service ▼

+ Group - Group

Service Type	Service Instance	Direction	Upstream	Delete
Virtual Path ▼	GUWAHATI-BR ▼	Send ▼	<input type="checkbox"/>	
Local ▼	DAKC_TATA... ▼	Receive ▼	<input checked="" type="checkbox"/>	

Apply Refresh

監視

IGMP 統計情報

マルチキャストレシーバが加入グループ要求を開始すると、アプライアンスの [**Monitoring**] > [**IGMP**] でレシーバの詳細を確認できます。この情報は、発信元と宛先の両方のアプライアンスで確認できます。

次の図は、IGMP バージョン 3 の加入が開始され、特定の送信元アドレスを含めるためにフィルタタイプの INCLUDE が使用されていることを示しています。IGMP メンバーの統計情報も確認できます。

Dashboard

Monitoring

Configuration

Statistics

Flows

Routing Protocols

Firewall

IKE/IPsec

IGMP

Performance Reports

Qos Reports

Usage Reports

Availability Reports

Appliance Reports

DHCP Server/Relay

VRRP

PPPoE

DNS

Monitoring > IGMP

Filter/Purge

Refresh

Purge IGMP Group

Purge IGMP Stats

IGMP PROXY Groups

Max Groups to Display: 50 Service Type to Display: Refresh

Type	Name	Group	Filter	Version	Packets Sent	Bytes Sent
HOST	VIF-1-Bridge-1	232.1.1.1	INCLUDE	IGMPv3	4285	6418930

Total Groups Displayed: 1 out of 1

IGMP Stats

Max IGMP Stats to Display: 50 Stats Type to Display: MEMBER Refresh

Type	Description	Value
MEMBER	Add Member	1
MEMBER	Remove Member	0
MEMBER	Current Member	1

Total IGMP Stats Displayed: 3 out of 70

仮想パスルートコストの構成

May 10, 2021

Citrix SD-WAN では、データセンター管理に関連する次のルーティング機能強化がサポートされています。

たとえば、北米とヨーロッパの 2 つのデータセンターを持つ SD-WAN ネットワークを考えます。北米のすべてのサイトで北米のデータセンターを経由するトラフィックをルーティングし、ヨーロッパのすべてのサイトで欧州のデータセンターを使用したいとします。これまでの、SD-WAN 9.3 以前のリリースバージョンでは、データセンター管理のこの機能はサポートされていませんでした。これは、仮想パスルートコストの導入によって実装されます。

- 仮想パスルートコスト：ルートがリモートサイトから学習されたときにルートコストに追加される個々の仮想パスに対して、仮想パスルートコストを設定できます。

この機能により、WAN から WAN への転送コストが無効化または削除されます。

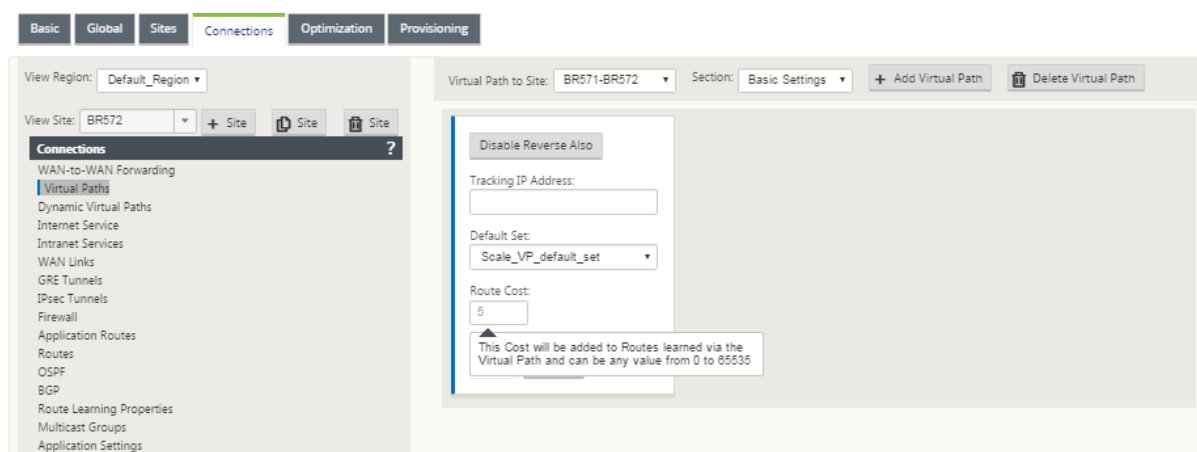
- OSPF ルートコスト: インポートフィルタで [OSPF ルートコストのコピー] を有効にすると、**OSPF** ルートコスト (タイプ 1 メトリック) をインポートできるようになりました。OSPF ルートコストは、SD-WAN コストではなく、ルート選択で考慮されます。15 ではなく 65534 までのコストがサポートされますが、ルートがリモートサイトから学習された場合に追加される適切な仮想パスルートコストに対応することをお勧めします。
- BGP-MED への VP コスト: SD-WAN ルートを BGP ピアにエクスポート (再配布) するときに、SD-WAN ルートの仮想パスルートコストを BGP MED 値にコピーできるようになりました。これは、BGP ポリシーを作成し、各ネイバーの「OUT」方向に適用することで、個々のネイバーに対して設定できます。
- どのサイトも、他のサイトへの複数の仮想パスを持つことができます。場合によっては、より多くの仮想パスを経由してサービスに接続できるブランチがある場合、ブランチサイトから 2 つの仮想パスが存在することがあります。一方の仮想パスは DC1 を経由し、もう一方の仮想パスは DC2 を経由します。DC1 は MCN であり、DC2 は Geo-MCN であり、静的仮想パスを持つ別のサイトとして構成できます。
- 各 VP の既定のコストを 1 として追加します。仮想パスルートコストは、サイトの各仮想パスにコストを関連付けるのに役立ちます。これは、デフォルトのサイトコストではなく、特定の仮想パス上のルート交換/更新を操作するのに役立ちます。これにより、トラフィックを送信するためにどのデータセンターを優先するかを操作できます。
- 各 VP の小さい範囲 (1 ~10 など) でコストを設定できます。
- ダイナミックルーティングで学習したルートを含め、ルーティングプリファレンスを示すために、ネイバーサイトと共有するすべてのルートに仮想パスコストを追加する必要があります。
- 静的仮想パスは、動的仮想パスよりも低コストである必要はありません。

注

VP ルートコストは、リリースバージョン 10.0 より前のリリースバージョンに存在した WAN から WAN への転送コストを非推奨にします。WAN から WAN への転送コストに基づくルーティング決定は、VP ルートコストを使用して再影響を受ける必要があります。リリースバージョン 10.0 に移行すると、WAN から WAN への転送コストは重要ではないためです。

仮想パスルートコストの設定方法

仮想パスルートは、SD-WAN GUI で、[接続] > [リージョンの表示] > [サイトの表示] > [仮想パス] > [基本設定] の下で構成できます。すべてのルートは、基本的な Citrix SD-WAN コスト + VP のルートコストとともにインストールされ、複数の仮想パスのルートコストに影響を与えます。



ユースケース:

たとえば、サブネット 172.16.2.0/24 と 172.16.3.0/24 があります。両方のサブネットを使用して SD-WAN にトラフィックを送信するデータセンターの DC1 と DC2 が 2 つあるとします。デフォルトの仮想パスルートコストでは、ルーティングに影響を与えることはできません。これは、最初にインストールされたルートによって、最初に DC2 または DC1 のいずれかになることができるからです。

仮想パスを使用すると、DC2 仮想パスのほうが仮想パスルートコスト（10 など）が大きくなり、DC1 のデフォルト VP ルートコストは 5 になります。この操作は、DC1 を最初に、DC2 を次に、両方のルートをインストールするのに役立ちます。

4 つのルートがあり、2 つのルートは 172.16.2.0/24 までです。1 つは低コストで DC1 経由で、1 つは高コストで DC2 経由で、172.16.3.0/24 の場合はさらに 2 つです。

監視とトラブルシューティング

ルーティングテーブルには、仮想パス経由でブランチサイトに接続されている 2 つのサイトによってアドバタイズされた同じサブネットが、仮想パスのルートコストを追加したコストよりも優先してインストールされる方法が表示されます。

ルートコストおよびルーティングテーブルで使用されているルートを確認するには、[モニタリング] > [統計] > [表示] フィールドの下に移動し、[ルート] を選択します。ルートコストとヒット数は、同じページで確認できます。

次の図は、同じルートの 2 つの異なるコストを持つルートテーブルを示しています。このコストは 172.16.6.0/24 で、サービス **DC-Branch01** と GEOMCN-Branch01** のコストは 10 と 11 です。

Monitoring > Statistics

Statistics

Show: Routes ☐ Enable Auto Refresh 5 seconds Refresh ☒ Clear Counters on Refresh

Routing Domain: <ALL> Purge dynamic routes

Route Statistics

Maximum allowed routes: 64000

Routes for routing domain : Default_RoutingDomain

Filter: in Any column Apply

Show 100 entries Showing 1 to 18 of 18 entries

First Previous 1

Details	Num	Network Addr	Gateway IP Address	Service	Firewall Zone	Reachable	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type
✦	0	172.16.60.0/24	*	Local	Default_LAN_Zone	YES	Branch01	Static	-	-	5	0	YES	N/A
✦	1	172.16.61.0/24	*	Local	Default_LAN_Zone	YES	Branch01	Static	-	-	5	0	YES	N/A
✦	2	172.16.41.0/24	*	DC-Branch01	Default_LAN_Zone	YES	DC	Dynamic	Virtual WAN	YES	10	0	YES	N/A
✦	3	172.16.40.0/24	*	DC-Branch01	Default_LAN_Zone	YES	DC	Dynamic	Virtual WAN	YES	10	0	YES	N/A
✦	4	172.16.6.0/24	*	DC-Branch01	Default_LAN_Zone	YES	DC	Dynamic	Virtual WAN	YES	10	0	YES	N/A
✦	5	172.16.4.0/24	*	DC-Branch01	Default_LAN_Zone	YES	DC	Dynamic	Virtual WAN	YES	10	0	YES	N/A
✦	6	172.16.3.0/24	*	DC-Branch01	Default_LAN_Zone	YES	DC	Dynamic	Virtual WAN	YES	10	0	YES	N/A
✦	7	172.16.2.0/24	*	DC-Branch01	Default_LAN_Zone	YES	DC	Dynamic	Virtual WAN	YES	10	0	YES	N/A
✦	8	172.16.51.0/24	*	GeoMCN-Branch01	Default_LAN_Zone	YES	GeoMCN	Dynamic	Virtual WAN	YES	11	0	YES	N/A
✦	9	172.16.50.0/24	*	GeoMCN-Branch01	Default_LAN_Zone	YES	GeoMCN	Dynamic	Virtual WAN	YES	11	0	YES	N/A
✦	10	172.16.6.0/24	*	GeoMCN-Branch01	Default_LAN_Zone	YES	GeoMCN	Dynamic	Virtual WAN	YES	11	0	YES	N/A
✦	11	172.16.4.0/24	*	GeoMCN-Branch01	Default_LAN_Zone	YES	GeoMCN	Dynamic	Virtual WAN	YES	11	0	YES	N/A

仮想ルータ冗長プロトコルの設定

May 10, 2021

Virtual Router Redundancy Protocol (VRRP) 仮想ルータ冗長プロトコル) は、デバイスの冗長性を提供し、スタティックデフォルトルーティング環境に固有の単一障害点を排除する、広く使用されているプロトコルです VRRP を使用すると、1 つのグループを形成するように 2 つ以上のルータを設定できます。このグループは、1 つの仮想 IP アドレスと 1 つの仮想 MAC アドレスを持つ単一のデフォルト Gateway として表示されます。

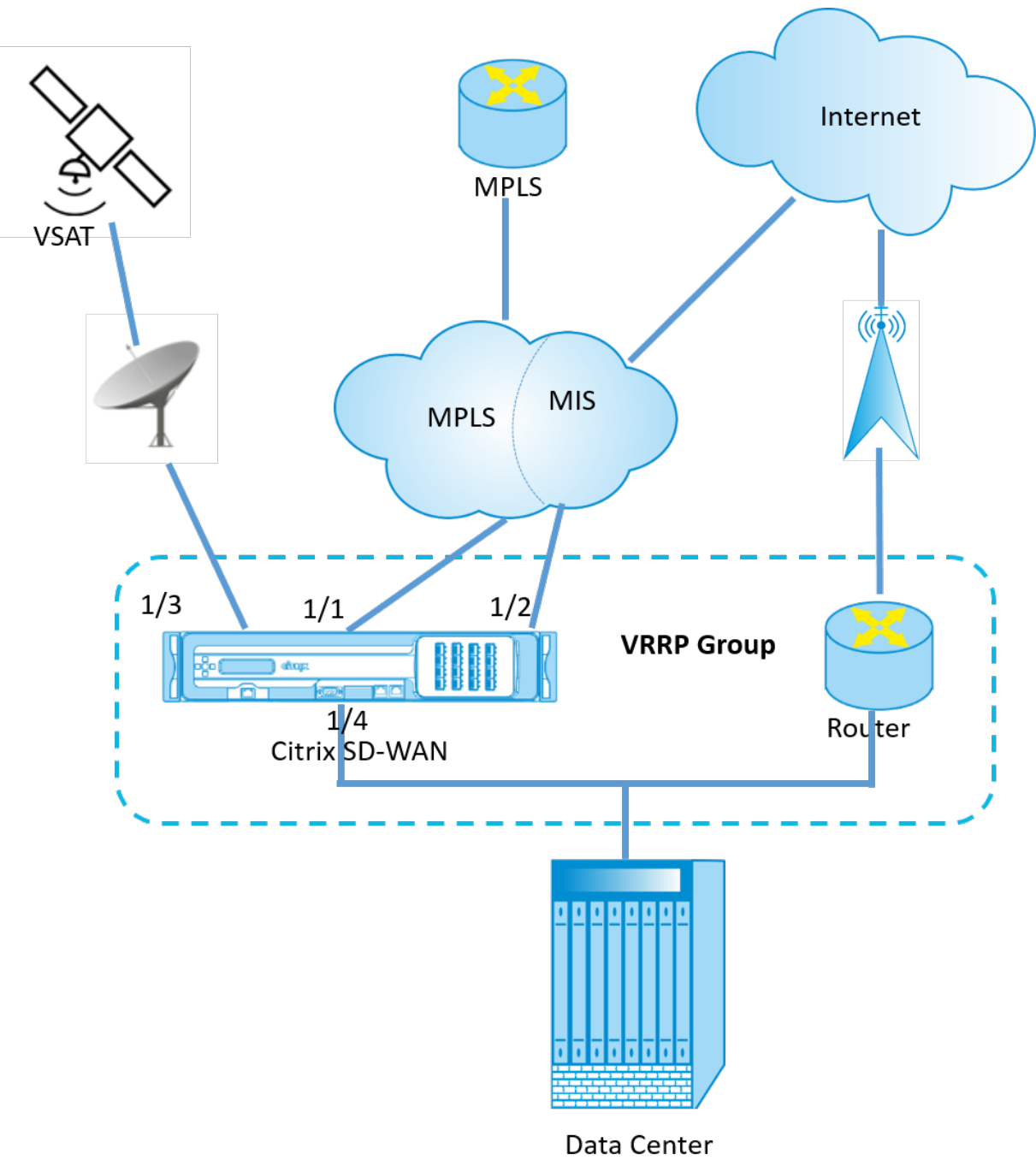
プライマリ/マスタールータに障害が発生すると、バックアップルータが自動的に引き継ぎます。VRRP 設定では、マスタールータは、アドバタイズメントと呼ばれる VRRP パケットをバックアップルータに送信します。マスタールータがアドバタイズメントの送信を停止すると、バックアップルータはインターバルタイマーを設定します。この保留期間内にアドバタイズメントが受信されない場合、バックアップルータはフェールオーバールーチンを開始します。

VRRP は、プライオリティが最も高いルータがマスターになる選択プロセスを指定します。ルータ間でプライオリティが同じ場合、IP アドレスの最も大きいルータがマスターになります。他のルータはバックアップ状態です。マスターに障害が発生した場合、新しいルータがグループに加入した場合、または既存のルータがグループを離れると、再び選出プロセスが開始されます。

VRRP は、すべてのエンドホストでダイナミックルーティングまたはルータディスカバリプロトコルを設定せずに、高可用性デフォルトパスを保証します。

Citrix SD-WAN リリースバージョン 10.1 では、VRRP バージョン 2 およびバージョン 3 がサポートされ、サードパーティ製のルーターとの相互動作が可能です。SD-WAN アプライアンスはマスタールーターとして機能し、サイト間で仮想パスサービスを使用するようにトラフィックを誘導します。仮想インターフェイス IP を VRRP IP として設定し、手動でプライオリティをピアルーターよりも高い値に設定することで、SD-WAN アプライアンスを VRRP マスターとして設定できます。アドバタイズメント間隔と preempt オプションを設定できます。

以下のネットワーク図は、Citrix SD-WAN アプライアンスと VRRP グループとして構成されたルーターを示しています。SD-WAN アプライアンスはマスターとして設定されています。SD-WAN アプライアンスに障害が発生した場合、バックアップルーターはミリ秒以内に停止し、ダウンタイムが発生しないようにします。



VRRP インスタンスを設定するには、次の手順を実行します。

1. 構成エディタで、[サイト]>[サイト名]>[VRRP] に移動し、[+] をクリックします。

+	VRRP Group ID	Version	Priority	Advertisement Interval	Authentication type	Authentication text	Reclaim	Use Check
+	245	V3	255	1000	*	None	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Apply Revert								

1. VRRP インスタンスを設定します。次のフィールドに値を入力します。

- **VRRP グループ ID:** VRRP グループ ID。グループ ID は、1 ～255 の値の範囲である必要があります。バックアップルータでも同じグループ ID を設定する必要があります。

注

現時点では、最大 4 つのグループしか構成できません。

- バージョン: VRRP プロトコルのバージョン。VRRP プロトコル V2 と V3 のいずれかを選択できます。
- 優先度: VRRP グループの Citrix SD-WAN アプライアンスの優先度。プライオリティの範囲は 1 ～254 です。SD-WAN アプライアンスをマスターにするには、この値を maximum (254) に設定します。

注

ルータが VRRP IP アドレスの所有者である場合、プライオリティはデフォルトで 255 に設定されます。

- **Advertisement Interval:** SD-WAN アプライアンスがマスターであるときに VRRP アドバタイズメントが送信される頻度 (ミリ秒単位)。デフォルトのアドバタイズメント間隔は 1 秒です。
- 認証タイプ: [プレーンテキスト] を選択して、認証文字列を入力できます。認証文字列は、VRRP アドバタイズメントで暗号化なしでプレーンテキストとして送信されます。認証を設定しない場合は、[None] を選択します。
- 認証テキスト: VRRP アドバタイズメントで送信される認証文字列。このオプションは、認証の種類がプレーンテキストの場合に有効になります。

注

認証は VRRPv2 でのみサポートされます。

- 再利用: VRRP グループで SD-WAN アプライアンスのプライオリティが最も高い場合に、プリエンブションを有効にします。これは VRRP 選定プロセスで使用されます。
- **V2 チェックサムを使用:** VRRPv3 のサードパーティネットワークデバイスとの互換性を有効にします。デフォルトでは、VRRPv3 は v3 チェックサム計算方式を使用します。一部のサードパーティデバイスでは、VRRPv2 チェックサム計算しかサポートされない場合があります。そのような場合は、このオプションを有効にします。

VRRP IP アドレスを設定します。次のフィールドに値を入力し、[適用] をクリックします。

- 仮想インターフェイス: VRRP に使用される仮想インターフェイス。設定済みの仮想インターフェイスの 1 つを選択します。
- 仮想 IP アドレス: 仮想インターフェイスに割り当てられた仮想 IP アドレス。仮想インターフェイスに設定済みの仮想 IP アドレスのいずれかを選択します。
- **VRRP ルータ IP:** VRRP グループの仮想ルータ IP アドレス。デフォルトでは、SD-WAN アプライアンスの仮想 IP アドレスが仮想ルータ IP アドレスとして割り当てられます。

VRRP Group ID	Version	Priority	Advertisement Interval	Authentication type	Authentication text	Reclaim	Use V2 Checksum
245	V3	255	1000	None		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Virtual Router IPs

Virtual Interface	Virtual IP Address	VRRP Router IP	Delete
VirtualInterface-1	172.16.2.100/24	172.16.2.100	

Apply

Revert

VRRP 統計情報

VRRP 統計情報は、[モニタリング]>[**VRRP** プロトコル] の下に表示されます。

DashboardMonitoringConfiguration

Monitoring > VRRP Protocol

StatisticsFlowsRouting ProtocolsFirewallIKE/IPsecPerformance ReportsQos ReportsUsage ReportsAvailability ReportsAppliance ReportsDHCP Server/Relay**VRRP Protocol**

VRRP Instances									
VRRP ID	Version	Interface(s)	State	Priority	Virtual Router IP	Advertisement Interval	Enable	Disable	
20	2	LAN-7	Master	250	172.58.7.100	2000	<div>Enable</div>	<div>Disable</div>	
245	3	LAN	Master	200	172.58.5.20	1000	<div>Enable</div>	<div>Disable</div>	

次の統計データを表示できます。

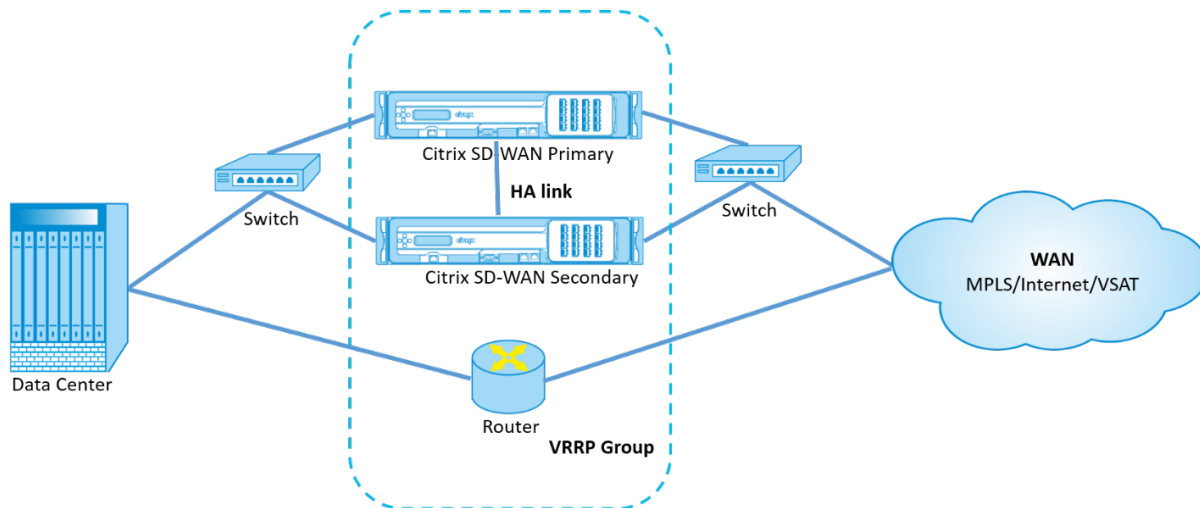
- **VRRP ID**: VRRP グループ ID
- バージョン: VRRP プロトコルのバージョン。
- インターフェイス: VRRP に使用される仮想インターフェイス。
- 状態: SD-WAN アプライアンスの VRRP 状態。アプライアンスがマスターかバックアップかを示します。
- プライオリティ: VRRP グループの SD-WAN アプライアンスのプライオリティ
- 仮想ルータ **IP**: VRRP グループの仮想ルータ IP アドレス。
- アドバタイズメント間隔: VRRP アドバタイズメントの頻度。
- **[Enable]**: SD-WAN アプライアンスで VRRP インスタンスを有効にする場合は、これを選択します。
- **[無効]**: SD-WAN アプライアンスの VRRP インスタンスを無効にする場合は、これを選択します。

制限事項

- VRRP は、ゲートウェイモード配置でのみサポートされます。
- 最大 4 つの VRRP ID (VRID) を設定できます。
- VRID には、最大 16 個の仮想ネットワークインターフェイスを使用できます。

高可用性および VRRP

SD-WAN ネットワーク上の高可用性機能と VRRP 機能の両方を利用することで、ネットワークのダウンタイムとトラフィックの中断を大幅に削減できます。アクティブ/スタンバイの役割で Citrix SD-WAN アプライアンスのペアをスタンバイルーターとともに展開し、VRRP グループを形成します。このグループは、1 つの仮想 IP アドレスと 1 つの仮想 MAC アドレスを持つ単一のデフォルト Gateway として表示されます。



上記の展開では、次の 2 つのケースがあります。

1 番目のケース：SD-WAN での高可用性フェールオーバータイマーは、**VRRP** フェールオーバータイマーと同じです。

予想される動作は、VRRP スイッチオーバーの前に高可用性スイッチオーバーが発生することです。つまり、トラフィックは新しい Active SD-WAN アプライアンスを引き続き通過します。この場合、SD-WAN は VRRP マスターロールを継続します。

2 番目のケース：VRRP フェールオーバータイマーよりも大きい **SD-WAN** での高可用性フェールオーバータイマーです。

想定される動作は、ルーターへの VRRP スイッチオーバーが発生することです。つまり、ルーターが VRRP マスターになり、トラフィックが SD-WAN アプライアンスをバイパスして、ルーターを一時的に流れる可能性があります。

ただし、高可用性スイッチオーバーが発生すると、SD-WAN が再び VRRP マスターになります。つまり、トラフィックは新しいアクティブ SD-WAN アプライアンスを通過します。

高可用性デプロイモードの詳細については、[高可用性](#)を参照してください。

ネットワークオブジェクトの構成

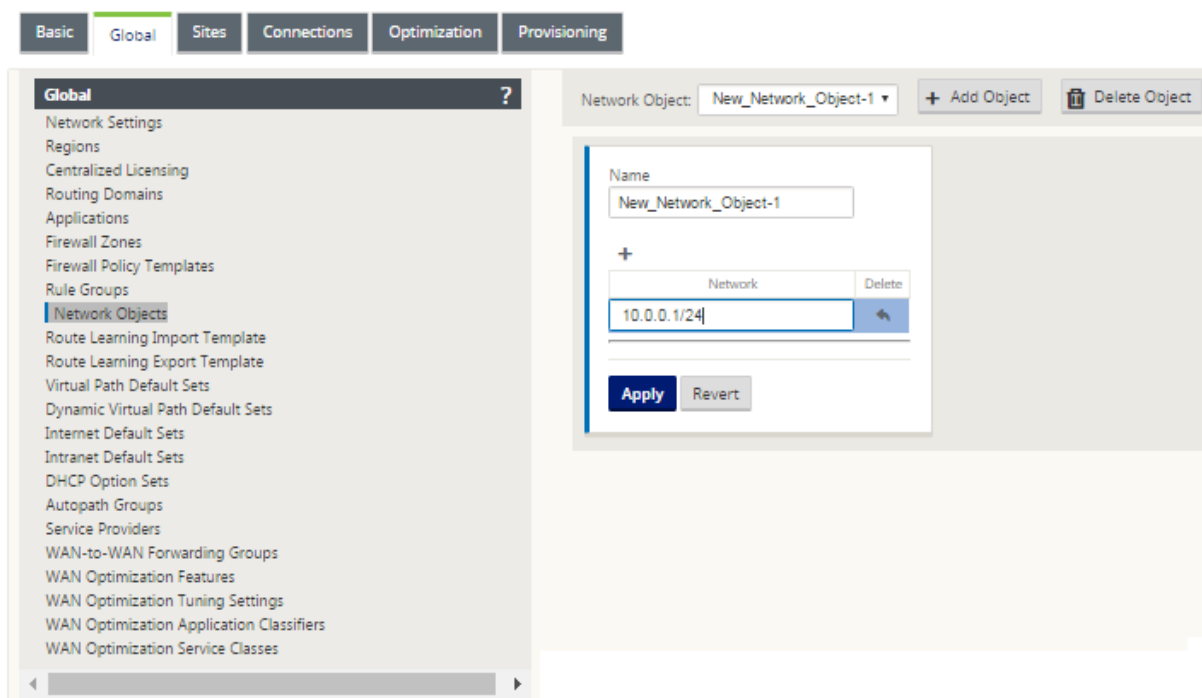
May 10, 2021

Citrix SD-WAN では、構成エディタの [グローバル] パネルにネットワークオブジェクトを追加するオプションが導入されています。ルートフィルタを定義するときに、サブネットごとにフィルタを作成するのではなく、複数のサブネットをまとめてグループ化し、1つのネットワークオブジェクトを参照できます。

ネットワーク・オブジェクトを構成するには、次の手順に従います。

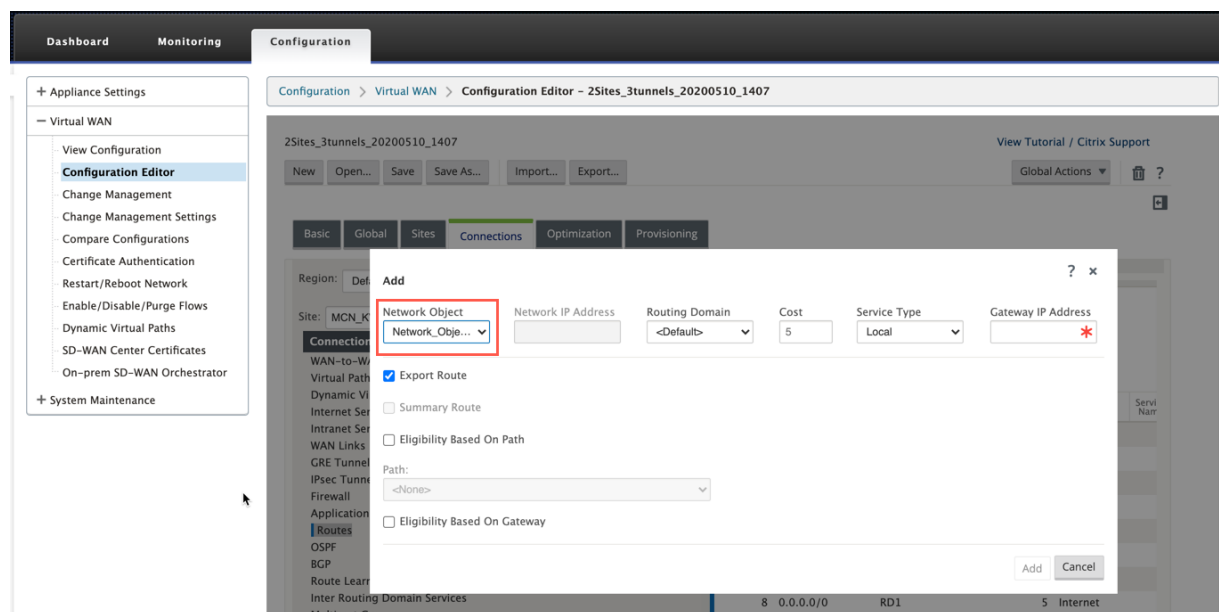
1. 設定エディタで、グローバル→ネットワークオブジェクトに移動し、追加 (+) をクリックします。
2. [ネットワーク] の下の [追加] (+) をクリックします。
3. 新しいネットワークオブジェクトの **IP** アドレスとサブネットを入力します。
4. [適用] をクリックして設定を保存します。

ネットワークオブジェクトの名前を編集するには、ネットワークオブジェクトの名前をクリックし、新しい名前を入力します。

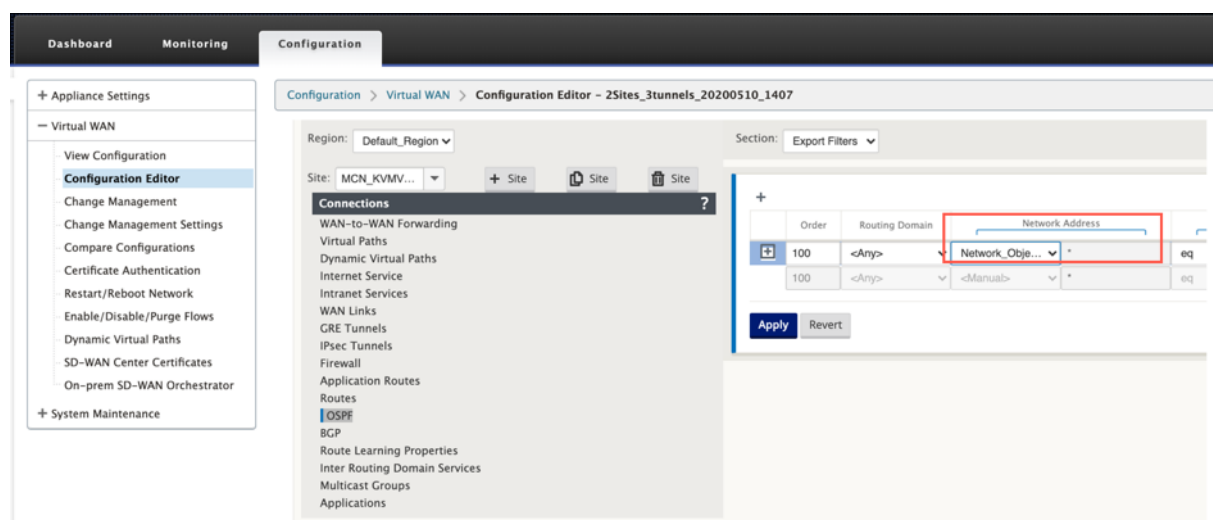


次の機能は、ネットワークオブジェクトを利用しています。

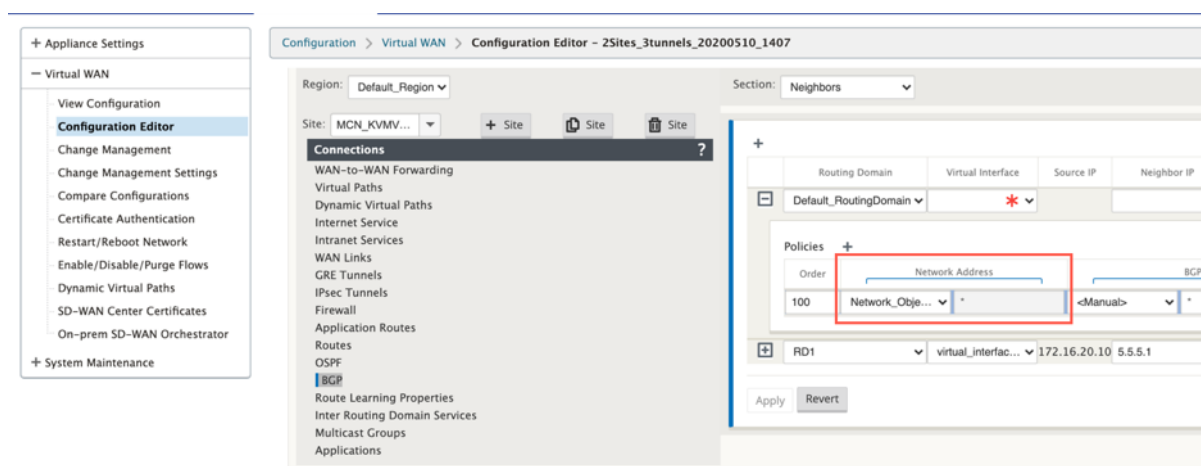
- ルート（設定エディタ > 接続 > ルート > + をクリック > ネットワークオブジェクト）



- BGP および OSPF インポートおよびエクスポートフィルタ（コンフィギュレーションエディタ > 接続 > **BGP/OSPF** > エクスポート/インポートフィルタ > + をクリック > ネットワークアドレス）



- BGP ネイバーポリシー（コンフィギュレーションエディタ > 接続 > **BGP** > ネイバー > ポリシー > + をクリック > ネットワークアドレス）



LAN セグメンテーションのルーティングサポート

May 10, 2021

SD-WAN Standard および Premium (Enterprise) Edition アプライアンスは、いずれかのアプライアンスが展開されている個別のサイト間で LAN セグメンテーションを実装します。アプライアンスは、使用可能な LAN 側 VLAN の記録を認識して維持し、別の SD-WAN 標準または Premium (Enterprise) Edition アプライアンスと遠隔地で接続できる他の LAN セグメント (VLAN) に関するルールを構成します。

上記の機能は、SD-WAN Standard または Premium (Enterprise) Edition アプライアンスで維持される Virtual Routing and Forwarding (VRF; 仮想ルーティングおよび転送) テーブルを使用して実装されます。このテーブルは、ローカル LAN セグメントにアクセス可能なリモート IP アドレス範囲を追跡します。この VLAN 間トラフィックは、2 つのアプライアンス間で確立された同じ仮想パスを経由して WAN を通過します (新しいパスを作成する必要はありません)。

この機能のユースケースの例として、WAN 管理者は VLAN を介してローカルブランチネットワーク環境をセグメント化でき、それらのセグメント (VLAN) の一部をインターネットにアクセスできる DC 側の LAN セグメントに提供する一方で、そのようなアクセスを取得できない場合もあります。VLAN と VLAN の関連付けの設定は、SD-WAN 管理 Web インターフェイスの MCN の構成エディタを使用して行います。

ルーティング間ドメインサービス

May 10, 2021

Citrix SD-WAN を使用すると、ルーティングドメインを使用してネットワークをセグメント化できるため、高いセキュリティと容易な管理が可能になります。ルーティングドメインを使用すると、トラフィックはオーバーレイネット

ワーク内で互いに隔離されます。各ルーティングドメインは、独自のルーティングテーブルを保持します。ルーティングドメインの詳細については、[ルーティングドメイン](#)を参照してください。

ただし、ルーティングドメイン間でトラフィックをルーティングする必要がある場合もあります。たとえば、プリンタ、スキャナ、メールサーバーなどの共有サービスが、個別のルーティングドメインとしてプロビジョニングされる場合などです。ルーティング間ドメインは、異なるルーティングドメインのユーザーが共有サービスにアクセスできるようにするために必要です。

Citrix SD-WAN は静的ルーティング間ドメインサービスを提供し、サイト内または異なるサイト間のルーティングドメイン間のルート漏洩を可能にします。これにより、エッジルータがルートリークを処理する必要がなくなります。ルーティング間ドメインサービスは、さらにルート、ファイアウォールポリシー、および NAT ルールを設定するために使用できます。

新しいファイアウォールゾーン **Inter_Routing_Domain_Zone** がデフォルトで作成され、ルーティングとフィルタリングのためのルーティング間ドメインサービスのファイアウォールゾーンとして機能します。

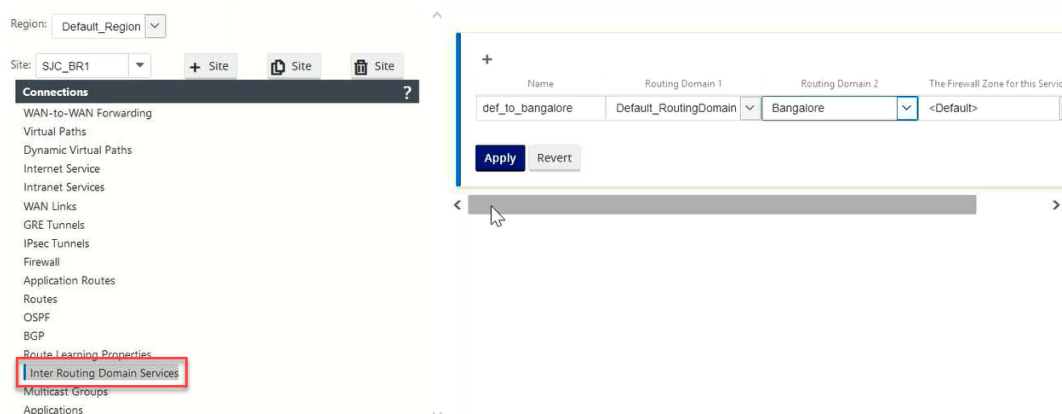
注

Citrix SD-WAN PE アプライアンスは、ルーティング間ドメインパケットに対して WAN 最適化機能を実行しません。

2 つのルーティングドメイン間でルーティング間ドメインサービスを構成します。

MCN と 2 つ以上のブランチを持つ SD-WAN ネットワークで、少なくとも 2 つのルーティングドメインをグローバルに設定したとします。デフォルトでは、すべてのルーティングドメインが MCN で有効になっています。他のサイトで必要なルーティングドメインを選択的に有効にします。ルーティングドメインの設定については、[ルーティングドメインの構成](#)を参照してください。

1. SD-WAN 構成エディタで、[接続] > [サイトの選択] > [ルーティング間ドメインサービス] に移動します。
2. [+] をクリックし、次のパラメータの値を入力します。
 - 名前: ルーティング間ドメインサービスの名前。
 - ルーティングドメイン **1**: ペアの最初のルーティングドメイン。
 - ルーティングドメイン **2**: ペアの 2 番目のルーティングドメイン。
 - ファイアウォールゾーン: サービスのファイアウォールゾーン。
 - デフォルト: Inter_Routing_Domain_Zone ファイアウォールゾーンが割り当てられます。
 - [なし]: ゾーンが選択されず、パケットの元のゾーンが保持されます。
 - ネットワーク内で構成されているすべてのゾーンが選択されることがあります。

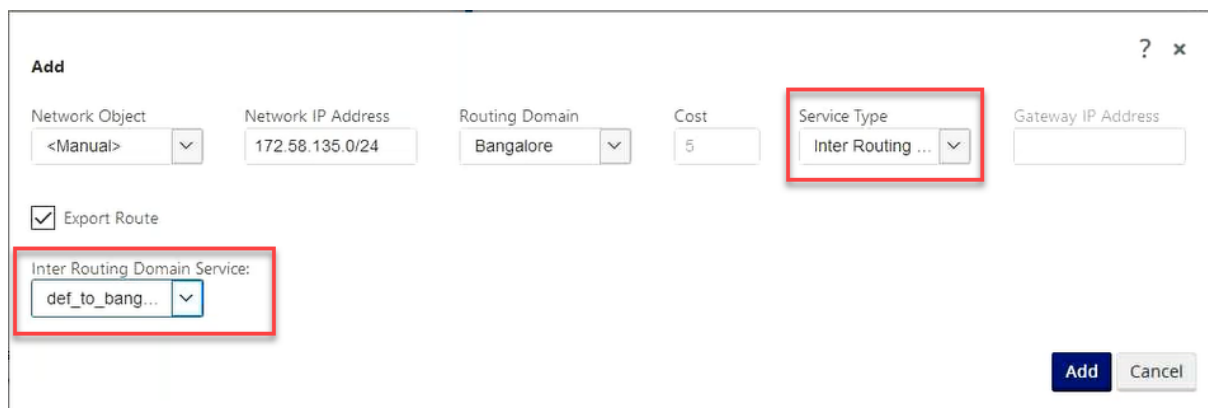


1. [適用] をクリックして、ルーティング間ドメインサービスを作成します。作成したサービスを使用して、ルート、ファイアウォールポリシー、および NAT ポリシーを作成できます。

注:

サイト上で有効になっていないルーティングドメインを使用して、ルーティング間ドメインサービスを構成することはできません。

インタールーティングドメインサービスを使用してルートを作成するには、サービスタイプを [** インタールーティングドメインサービス **] としてルートを作成し、ルーティングドメインサービスを選択します。ルートの設定の詳細については、[ルートの設定方法](#)を参照してください。



また、他の Routing Domain ペアからルートを追加して、2 つのルーティングドメイン間の接続を確立します。

ファイアウォールポリシーを構成して、ルーティングドメイン間のトラフィックフローを制御することもできます。ファイアウォールポリシーで、送信元および宛先サービスに対して [Inter-Routing ドメインサービス] を選択し、必要なファイアウォールアクションを選択します。ファイアウォールポリシーの設定については、[ポリシー](#)を参照してください。

Default_LAN_Zone ☐ ☐ Default_LAN_Zone ☐ ☐
 Internet_Zone ☐ ☐ Internet_Zone ☐ ☐
 Untrusted_Internet_Zone ☐ ☐ Untrusted_Internet_Zone ☐ ☐

Routing Domain
Any

Traffic Match Type: IP Protocol Any DSCP: Any ☐ Match Established

Application: Application Family: Any Application Objects: Any

Source Service Type: Inter Routing Domain Source Service Name: def_to_bangalore
 Dest Service Type: Inter Routing Domain Dest Service Name: def_to_bangalore

Source IP: * Source Port: *
 Dest IP: * Dest Port: *

Actions
 Action: Allow ☒ Allow Fragments Connection State Tracking: Use Site Setting
 Drop ☐ Log Start ☐ Log End ☐ Add Reverse Policy
 Reject
 Count and Continue

また、イントラネットサービスの種類を選択して、スタティック NAT ポリシーとダイナミック NAT ポリシーを構成することもできます。NAT ポリシーの設定の詳細については、[ネットワークアドレス変換](#)を参照してください。

Add ? x

Priority: 100 Routing Domain: *

Direction: Outbound Type: Port Restricted Service Type: Inter Routing ... Service Name: def_to_bang...

Inside Zone: Any Inside IP Address: * Outside IP Address: *

☐ Allow Related ☐ IPsec Passthrough ☐ GRE/PPTP Passthrough ☐ Port Parity ☐ Bind Responder Route

Port Forwarding Rules +

Routing Domain	Protocol	Outside Port	Inside IP Address	Inside Port	Fragments	Log Interval (s)	Log Start	Log End	Connection State Tracking	Delete
----------------	----------	--------------	-------------------	-------------	-----------	------------------	-----------	---------	---------------------------	--------

Add Cancel

監視

[監視] > [ファイアウォールの統計] > [接続] で、ルーティング間ドメインサービスを使用する ** 接続のモニタリン

グ統計情報 ** を表示できます。

Firewall Statistics

Statistics: **Connections**

Maximum entries to display: **50**

Filtering:

Routing Domain: **Any** Application: **Any** Family: **Any**

IP Protocol: **Any** Source Zone: **Any** Destination Zone: **Any**

Source Service Type: **Any** Source Service Instances: **Any** Source IP: ***** Source Port: *****

Destination Service Type: **Any** Destination Service Instances: **Any** Destination IP: ***** Destination Port: *****

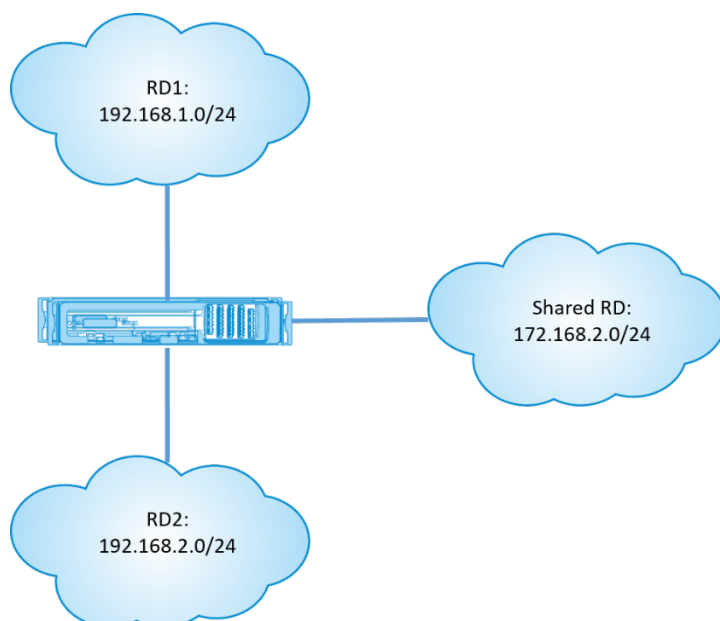
Connections

Routing Domain	Application	Family	IP Protocol	IP Address	Port	Service Type	Service Name	Zone	IP Address	Port	Service Type	Service Name	Zone	State	Is Rule	Packets	Bytes	PPS	k
Default_RoutingDomain	Internet Control Message Protocol(ICMP)	Network Service	ICMP	172.16.25.10	19973	Local	VIF-2-LAN-1	Default_LAN_Zone	172.16.1.10	19973	Inter-Routing-Domain	Default_to_MPLS	Inter_Routing_Domain_Zone	ESTABLISHED	Yes	10124	850416	0.999	
RD_MPLS	Internet Control Message Protocol(ICMP)	Network Service	ICMP	172.16.15.100	19973	Inter-Routing-Domain	Default_to_MPLS	Inter_Routing_Domain_Zone	172.16.1.10	19973	Virtual Path	DC_MON-BR3	Default_LAN_Zone	ESTABLISHED	No	10124	850416	0.999	

Connections Displayed: 2
Connections in Use: 2/128000

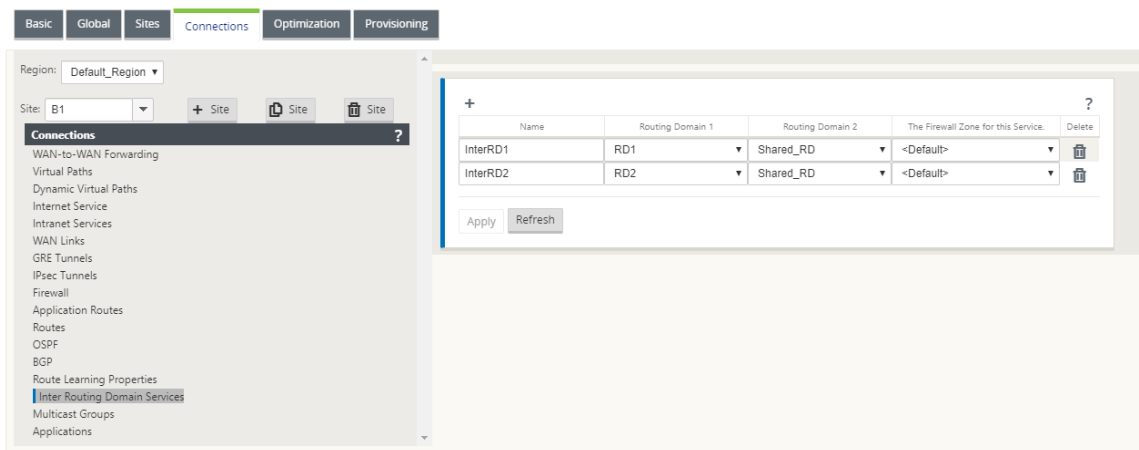
ユースケース: ルーティングドメイン間でのリソースの共有

異なるルーティングドメインのユーザーがプリンタやネットワークストレージなどの共通資産にアクセスする必要があるシナリオを考えてみましょう。図に示すように、ブランチ RD1、RD2、および共有 RD には 3 つのルーティングドメインがあります。



RD1 および RD2 のユーザーが共有 RD のリソースにアクセスできるようにするには、次の手順を実行します。

1. RD1 と共有 RD の間にルーティング間ドメインサービスを作成します。たとえば、**Inter RD1** です。
2. RD2 と共有 RD 間のルーティング間ドメインサービス (たとえば、**Inter-RD2**) を作成します。



3. RD1 および RD2 から共有 RD への静的ルートを構成します。RD1 で、ルート 172.168.2.0/24 を InterRD1 に追加します。

Add ? x

Network Object	Network IP Address	Routing Domain	Cost	Service Type	Gateway IP Address
<Manual>	172.168.2.0/24	RD1	5	Inter Routing Doi	

☒ Export Route

Inter Routing Domain Service:
InterRD1

Add **Cancel**

4. RD2 で、ルート 172.168.2.0/24 を InterRD2 に追加します。

Add ? x

Network Object	Network IP Address	Routing Domain	Cost	Service Type	Gateway IP Address
<Manual>	172.168.2.0/24	RD2	5	Inter Routing Doi	

☒ Export Route

Inter Routing Domain Service:
InterRD2

Add **Cancel**

5. 共有 RD の VIP を使用して InterRD1 にダイナミック NAT ルールを追加します。[応答側ルートのバインド] を有効にして、逆方向ルートが同じサービスタイプを使用するようにします。

Add ? x

Priority: Routing Domain:

Direction: Type: Service Type: Service Name:

Inside Zone: Inside IP Address: Outside IP Address:

☐ Allow Related ☐ IPsec Passthrough ☐ GRE/PPTP Passthrough ☐ Port Parity ☒ Bind Responder Route

Port Forwarding Rules +

Routing Domain	Protocol	Outside Port	Inside IP Address	Inside Port	Fragments	Log Interval (s)	Log Start	Log End	Connection State Tracking	Delete
----------------	----------	--------------	-------------------	-------------	-----------	------------------	-----------	---------	---------------------------	--------

Add **Cancel**

6. 共有 RD の VIP を使用して InterRD2 にダイナミック NAT ルールを追加します (たとえば、10.0.0.11)。パインドレスポンスルートを有効にして、リバースルートが同じサービスタイプを使用するようにします。

Add ? x

Priority: Routing Domain:

Direction: Type: Service Type: Service Name:

Inside Zone: Inside IP Address: Outside IP Address:

☐ Allow Related ☐ IPsec Passthrough ☐ GRE/PPTP Passthrough ☐ Port Parity ☒ Bind Responder Route

Port Forwarding Rules +

Routing Domain	Protocol	Outside Port	Inside IP Address	Inside Port	Fragments	Log Interval (s)	Log Start	Log End	Connection State Tracking	Delete
----------------	----------	--------------	-------------------	-------------	-----------	------------------	-----------	---------	---------------------------	--------

Add **Cancel**

7. フィルターを使用して、共有 RD 内のどのリソースが RD1/RD2 のユーザーからアクセスできるかを制限します。

ECMP 負荷分散

February 8, 2022

ECMP (等コストマルチパス) グループを使用すると、同じコスト、宛先、サービスで複数のパスをグループ化できます。接続またはセッション・データは、ECMP グループのタイプに応じて、ECMP グループ内のすべてのパスでロード・バランシングされます。たとえば、同じルートコストを持つブランチとデータセンターの間に 2 つの WAN リンクを持つネットワークがあるとして。従来、WAN リンクの 1 つはアクティブで、もう 1 つはフォールバックリンクとして機能している状態のままでした。ECMP グループを使用すると、これらの WAN リンクをグループ化して、

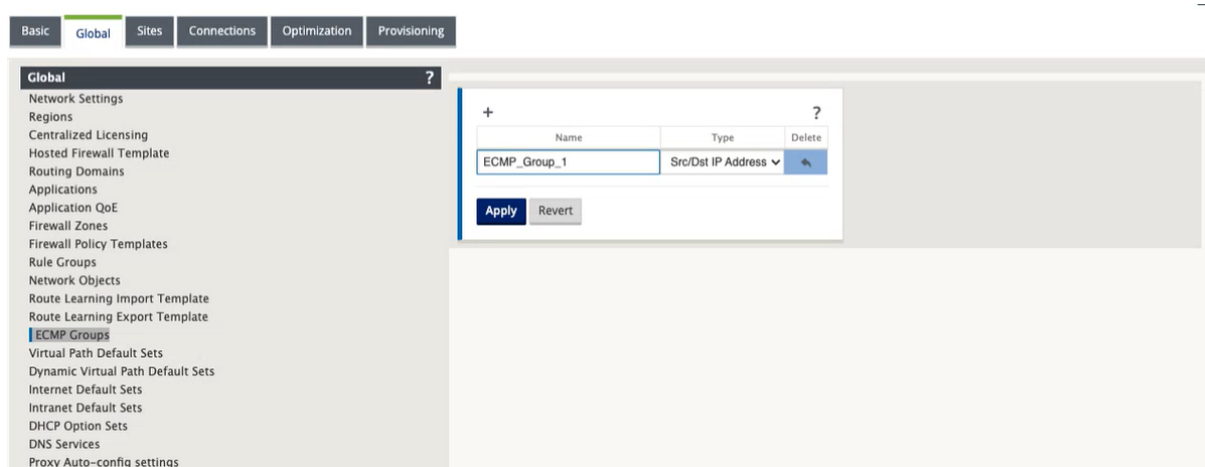
両方の WAN リンクを通じてトラフィックの負荷分散を行うことができます。ECMP 負荷分散により、次のことが保証されます

- 複数の等価コストパスへのトラフィックの分散
- 利用可能な帯域幅の最適な使用。
- リンクに障害が発生した場合に、他の ECMP メンバーパスへのトラフィックの動的転送 ECMP は、IPsec/GRE トンネルでスタティックルートをサポートします。

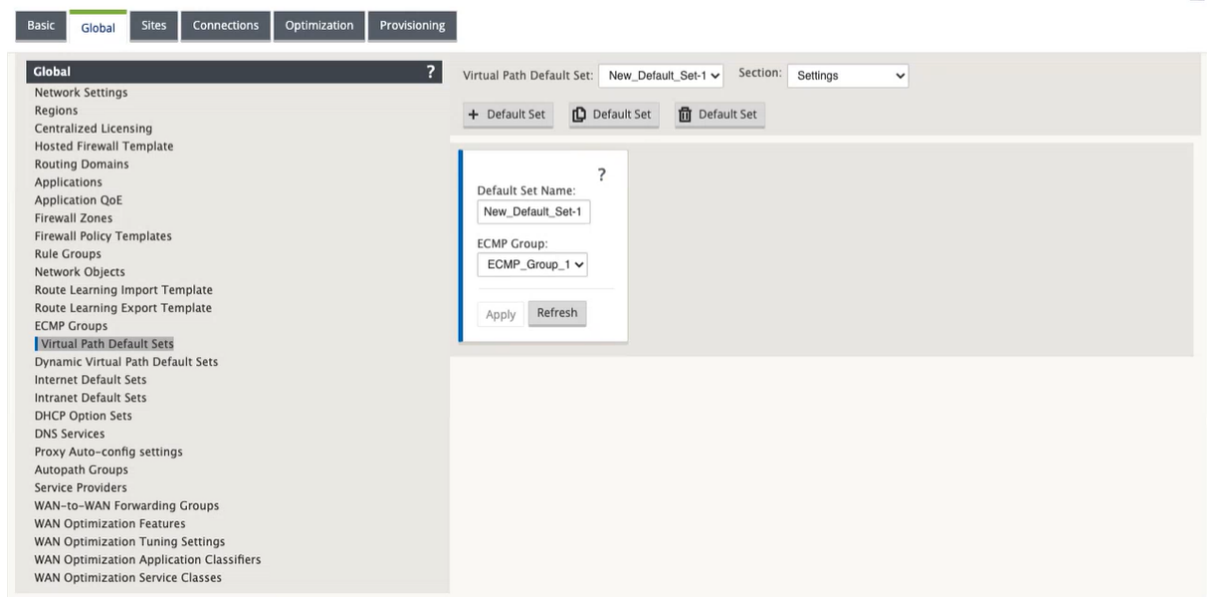
ECMP ロード・バランシングは、仮想パスおよびイントラネット・サービスでサポートされています。ECMP グループは、グローバルレベルで定義されます。ネットワークには、最大 254 の ECMP グループを定義できます。ECMP グループ内の ECMP 適格ルートの最大数は、アプライアンスとライセンスタイプによって異なります。Citrix SD-WAN では、次の 2 種類の ECMP グループがサポートされています。

- 送信元/宛先 IP アドレス: 複数のクライアントが同じ宛先に接続しようとするネットワークでは、同じコストの WAN リンク間で接続の負荷分散が行われます。
- セッション: 単一のクライアントが宛先に接続され、複数のセッションが生成されるネットワーク。セッションデータは、等コストの WAN リンク間で負荷分散されます。

ECMP グループを構成するには、構成エディタで [グローバル] > [**ECMP グループ**] に移動します。ECMP グループの名前を入力し、必要に応じて [**Src/Dst IP アドレス**] または [セッション] としてタイプを選択します。

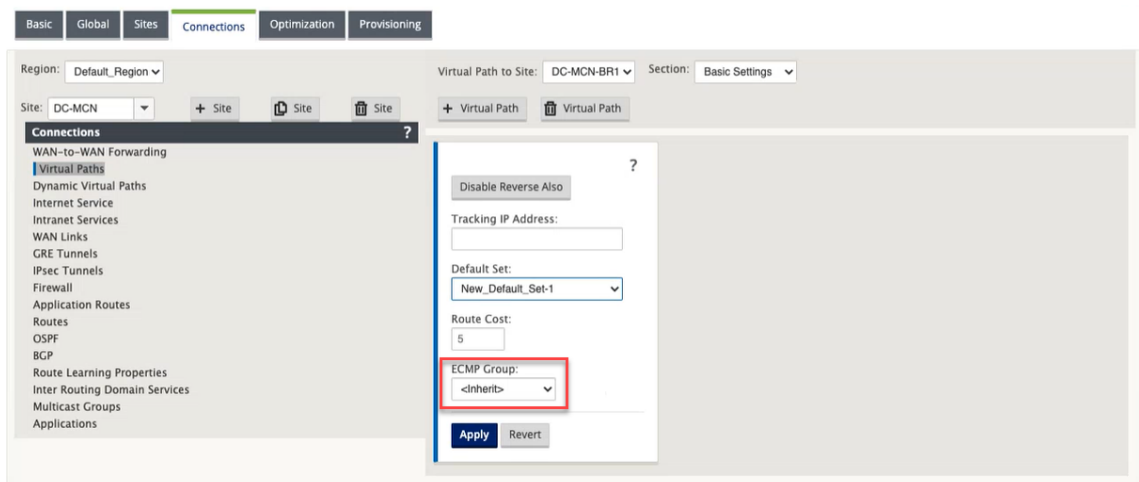


ECMP グループは、仮想パスおよびイントラネットのデフォルトセットに関連付けることができます。

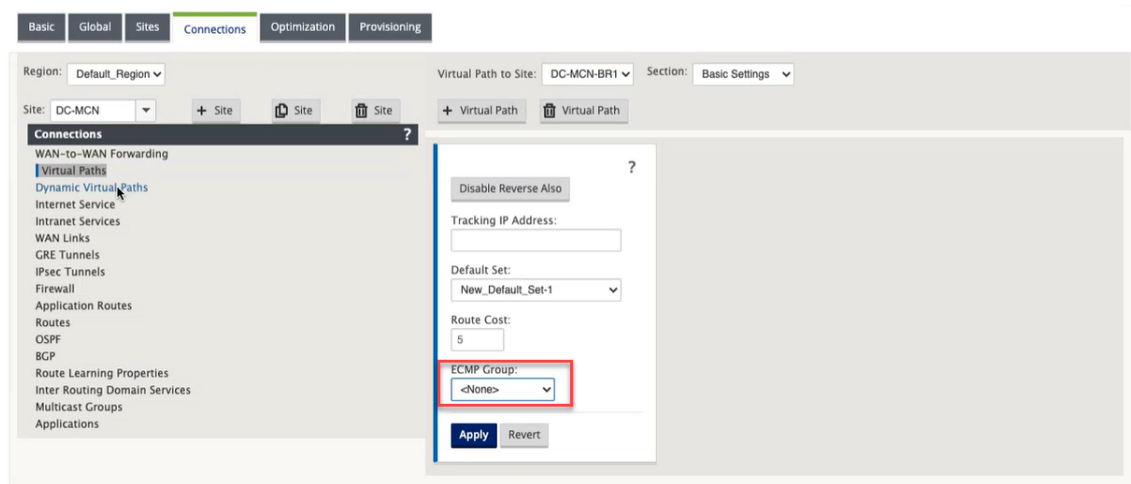


ECMP グループを仮想パスおよびイントラネットサービスに関連付けるには、次の 3 つの方法があります。

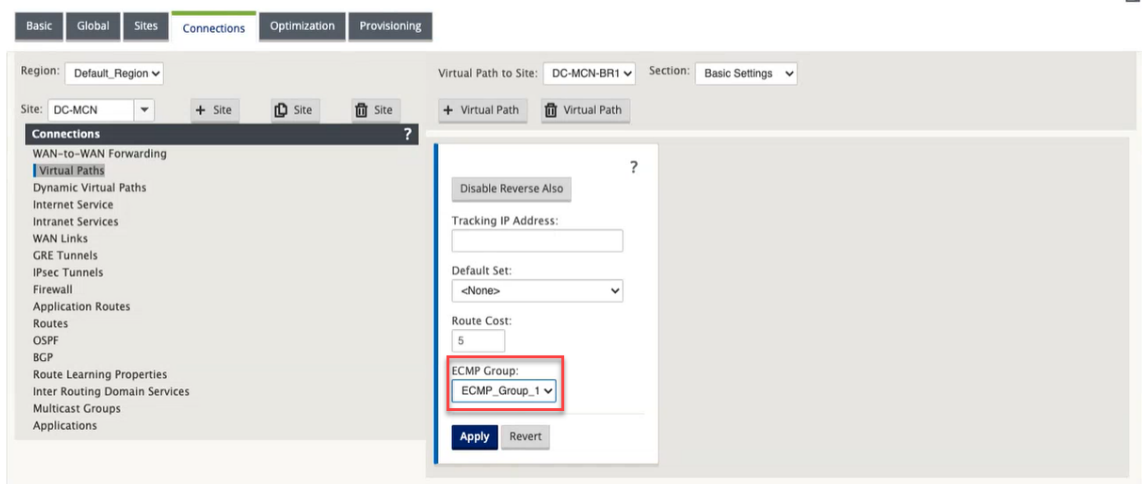
- 継承: サービスは、デフォルトセットに関連付けられた ECMP グループを継承します。デフォルトセットに関連付けられた ECMP グループがない場合、サービスはどの ECMP グループにも関連付けられません。



- なし: デフォルトセットが ECMP グループに関連付けられている場合でも、サービスはどの ECMP グループにも関連付けられません。



- **ECMP グループ:** グローバルレベルで定義された ECMP グループの 1 つを選択して、ECMP グループをサービスに関連付けます。選択した ECMP グループは、デフォルトセットに関連付けられた ECMP グループよりも優先されます。



ECMP 負荷分散を監視するには、SD-WAN UI で、[監視] > [統計] > [ルート] に移動し、ECMP グループ名を使用して検索結果をフィルタリングします。

Statistics

Show: Routes ☒ Enable Auto Refresh 5 seconds ☒ Clear Counters on Refresh

Routing Domain: <ALL>

Route Statistics

Maximum allowed routes: 64000

Routes for routing domain: Default_RoutingDomain

Filter: Tonowhere in ECMP Group Network Address Type: ALL

Show 100 entries Showing 1 to 4 of 4 entries (filtered from 35 total entries)

Details	Num	Network Addr	Gateway IP Address	Service	Firewall Zone	Reachable	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	ECMP Group	Eligible	Eligibility Type	Eligibility Value
	6	6.6.6.0/24	*	New_Intranet_Service-3	Intranet_Zone	YES	BR1	Static	-	-	5	0	Tonowhere	YES	N/A	N/A
	7	5.5.5.0/24	*	New_Intranet_Service-3	Intranet_Zone	YES	BR1	Static	-	-	5	630	Tonowhere	YES	Path	BR1_Inet1->DC_Inet1
	8	5.5.5.0/24	*	New_Intranet_Service-4	Intranet_Zone	YES	BR1	Static	-	-	5	315	Tonowhere	YES	N/A	N/A
	9	4.4.4.0/24	*	New_Intranet_Service-4	Intranet_Zone	YES	BR1	Static	-	-	5	0	Tonowhere	YES	N/A	N/A

Showing 1 to 4 of 4 entries (filtered from 35 total entries)

サンプルデータでは、共通の ECMP グループを持つサービス内のすべてのルートが ECMP グループに属していることがわかります。たとえば、**6.6.0/24** と **5.5.5.0/24** は **ECMP** グループに属します。ただし、トラフィックの負荷は、宛先 IP 5.5.5.0/24 を共有し、同じ ECMP グループに関連付けられているサービス **New_Intranet_Service-3** と **New_Intranet_Service-4** の間で分散されます。

(注

) SIA および Zscaler サービスでは、ECMP (アクティブ/アクティブ) を使用して 2 つの IPsec トンネルパス間で負荷分散できます。

ECMP 負荷分散機能は、次の SD-WAN アプライアンスではサポートされていません。

- Citrix SD-WAN 1000 SE/PE
- Citrix SD-WAN 2000 SE/PE
- Citrix SD-WAN 4000 SE

セキュアなピアリング

May 10, 2021

Premium (Enterprise) Edition アプライアンスはデータセンターにインストールでき、自動または手動によるセキュアピアリングの開始、SSL プロファイルの作成、サービスクラスに関連付け、Windows ドメインコントローラへのアプライアンスの参加が可能のため、ユーザー/管理者がスタンドアロン WANOP の拡張された豊富な機能を使用できます。アプライアンス。

次に、自動セキュアピアリングと手動セキュアピアリングでサポートされている展開モードを示します。

自動セキュアピアリングの展開:

「[DC サイトのスタンドアロン WANOP/SDWAN SE/WANOP から PE アプライアンスへの自動セキュアピアリングを実行するには](#)」を参照してください。

この展開を開始する手順:

- WANOP DC アプライアンスはリスニングオンモード (2312/非標準ポート) で、ブランチ PE は CONNECT-TO モードです。
- WANOP DC は PE アプライアンスへの自動セキュアピアリングを開始します。このピアリングは、プライベート CA 証明書と CERT キーペアをインストールし、WANOPs LISTEN-ON IP を使用して PE アプライアンスに CONNECT-TO を設定します。

「[DC サイトおよびブランチサイト PE アプライアンスで PE アプライアンスから開始される自動セキュアピアリングを実行するには](#)」を参照してください。

この展開を開始する手順:

- PE DC アプライアンスは、リスニングオンモード (ポート 443) です。ブランチ PE は CONNECT-to モードです。
- PE DC アプライアンスは、PE ブランチアプライアンスへの自動セキュアピアリングを開始します。このアプライアンスは、プライベート CA 証明書と CERT キーペアをインストールし、DC PE の LISTEN-ON IP を使用して PE ブランチアプライアンスに CONNECT-TO を設定します。
- PE の LISTEN-ON IP は、「WANOP にリダイレクト」が有効になっているルーティングドメインに関連付けられたインターフェイス IP にあります。

自動セキュアピアリングは、[WANOP/SDWAN SE アプライアンスで DC サイトおよびブランチの PE アプライアンスから開始されます](#)。

この展開を開始する手順:

- PE DC アプライアンスは、リスニングオンモード (ポート 443) です。ブランチ WANOP/SD-WAN SE は、接続モードです。
- PE DC アプライアンスは、ブランチ WANOP または SD-WAN SE アプライアンスへの自動セキュアピアリングを開始します。このアプライアンスは、プライベート CA 証明書と CERT キーペアをインストールし、DC PE の LISTEN-ON IP を使用して PE アプライアンスに CONNECT-TO を設定します。

セキュアピアリングの手動展開:

「[DC サイトの PE アプライアンスからブランチ PE アプライアンスへの手動セキュアピアリングを開始](#)」を参照してください。

この展開を開始する手順:

- PE DC アプライアンスは、リスニングオンモード (ポート 443) です。ブランチ PE は CONNECT-to モードです。
- PE の LISTEN-ON IP は、「WANOP にリダイレクト」が有効になっているルーティングドメインに関連付けられたインターフェイス IP にあります。

- 認証局の認証元から取得した CA と Cert Key のペア証明書を手動でアップロードします。

DC サイトの PE アプライアンスからブランチ WANOP/SDWAN-SE アプライアンスへの手動セキュアピアリングが開始されます。

この展開を開始する手順:

- PE DC アプライアンスは、リスニングオンモード（ポート 443）です。ブランチ WANOP/SD-WAN SE は、接続モードです。
- PE の LISTEN-ON IP は、「WANOP にリダイレクト」が有効になっているルーティングドメインに関連付けられたインターフェイス IP 内にある
- 認証局の認証元から取得した CA と Cert Key のペア証明書を手動でアップロードします。

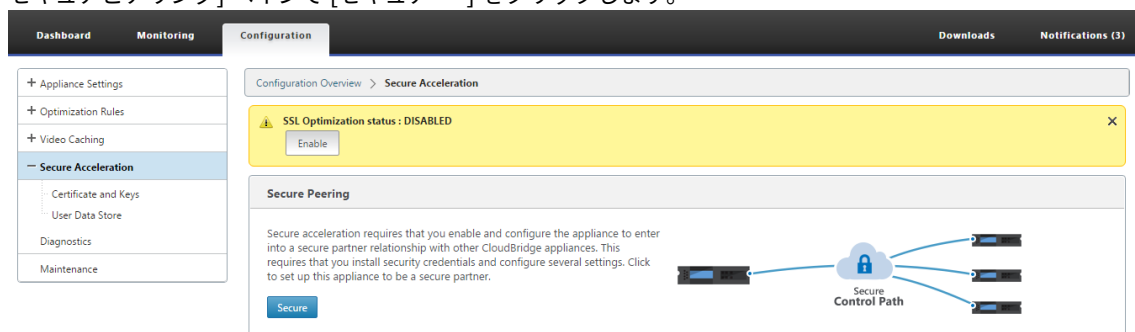
DC サイトのスタンドアロン SD-WAN SE および WANOP アプライアンスから PE アプライアンスへの自動セキュアピアリング

May 10, 2021

DC 側のスタンドアロンの SD-WAN SE および WANOP アプライアンスから PE アプライアンスで自動セキュアピアリングを実行するには、次の手順を実行します。

- WANOP DC アプライアンスは、リスニングオンモード（2312/非標準ポート）です。
- ブランチ PE アプライアンスは CONNECT-to モードです。
- WANOP DC は PE アプライアンスへの自動セキュアピアリングを開始します。このピアリングは、プライベート CA 証明書と CERT キーペアをインストールし、WANOPs LISTEN-ON IP を使用して PE アプライアンスに CONNECT-TO を設定します。

1. データセンターのスタンドアロン WANOP アプライアンスで、[セキュアアクセラレーション] ページの [**セキュアピアリング] ペインで [セキュア **] をクリックします。



2. キースタアのパスワードを入力するか、キースタアを無効にして、キースタア設定を構成します。

Dashboard Monitoring Configuration

← Back

Secure Peering

Keystore Settings

Security keys and settings are secured by the key store password. Each time the appliance restarts, the key store is closed automatically, and must be opened manually for secure acceleration to resume.

Keystore Password*

Confirm Keystore Password*

☐ Disable Keystore Password

Save Cancel

3. [プライベート CA] を選択して自動セキュアピアリングを実行して、セキュアピアリングを有効にします。

Dashboard Monitoring Configuration Downloads Notifications

← Back

Secure Peering

Keystore Settings

Keystore Status
Opened

Secure Peering Certificate and Keys

Secure communications with the CloudBridge partner appliance requires that you generate OpenSSL credentials, including CA Certificate and a Certificate/Key pair, and select a verification method. You can optionally change the OpenSSL cipher specification. If PrivateCA is selected, certificates and keys are generated automatically.

☒ Enable Secure Peering

Certificate Configuration

☒ Private CA ☐ CA Certificate

Save Cancel

4. アプライアンスレベルの CA 証明書とプライベート証明書とキーがローカル WANOP で生成され、AUTO セキュアピアリングを実行する REMOTE PEER を追加するためのテーブルが表示されます。
5. 「+」アイコンをクリックすると、ユーザー名とパスワードの付いた IP アドレスを追加するためのポップアップウィンドウが表示されます。資格情報を指定したリモート IP による認証が成功すると、要求がリモートマシンに送信されます。リモートマシンでは、CA Certificate と Private 証明書とキーをローカル（リモートマシン上）にインストールします。

Dashboard Monitoring Configuration Downloads Notifications (3)

← Back

Secure Peering

Keystore Settings

Keystore Status
Opened

Secure Peering Certificate and Keys

Secure Peering	Certificate/Key Pair Name	CA Certificate Store Name	Cipher Specification
Enabled	private_10_105_184_74	PrivateRootCA	!ADH:!AECDH:!MD5:HIGHER:STRENGTH

Connected Peers

+

注

- IP アドレス—リモート PREMIUM (ENTERPRISE) EDITION アプライアンス管理 IP の IP アドレス
- ユーザー名—リモート PREMIUM (ENTERPRISE) EDITION アプライアンスのユーザー名
- パスワード—リモートプレミアム（エンタープライズ）エディションアプライアンスのパスワード



認証に成功すると、セキュアピアリングが TRUE になり、リモートプレミアム（エンタープライズ）エディションアプライアンスの仮想 IP アドレスの 1 つとしてパートナーの IP アドレスが表示されます。

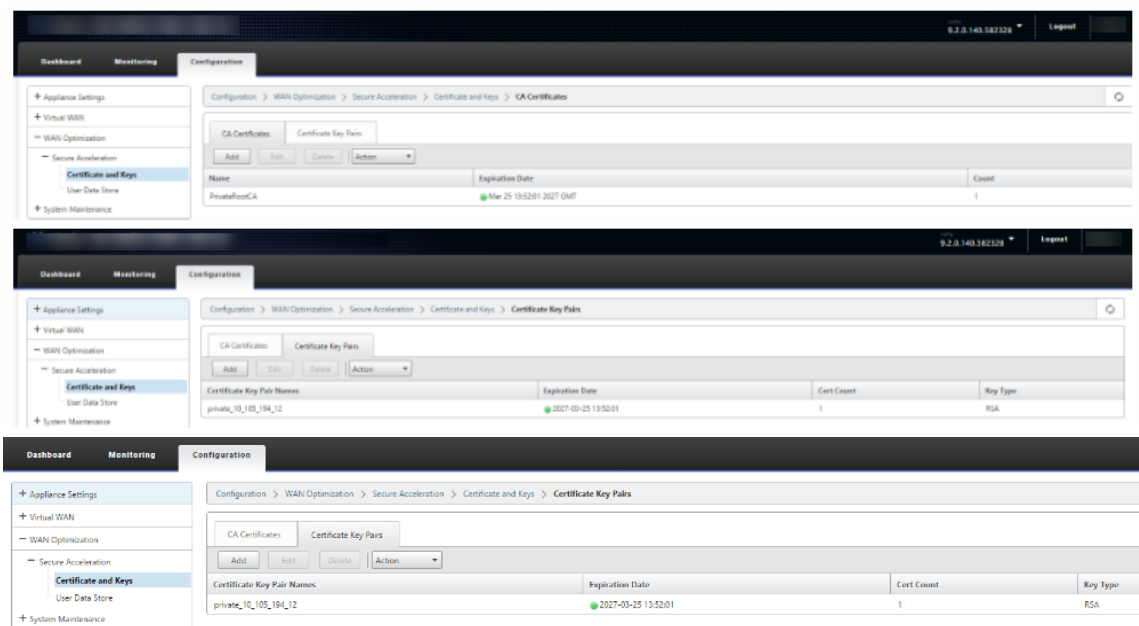
Peer Name	IP Address	Secure	Connection Status	Time Connected ↑	Time Since Last Contacted
CloudBridge1	172.184.1.19	True	Connected Available	7m 44s	0m 5s

↑ VIP of Remote EE App

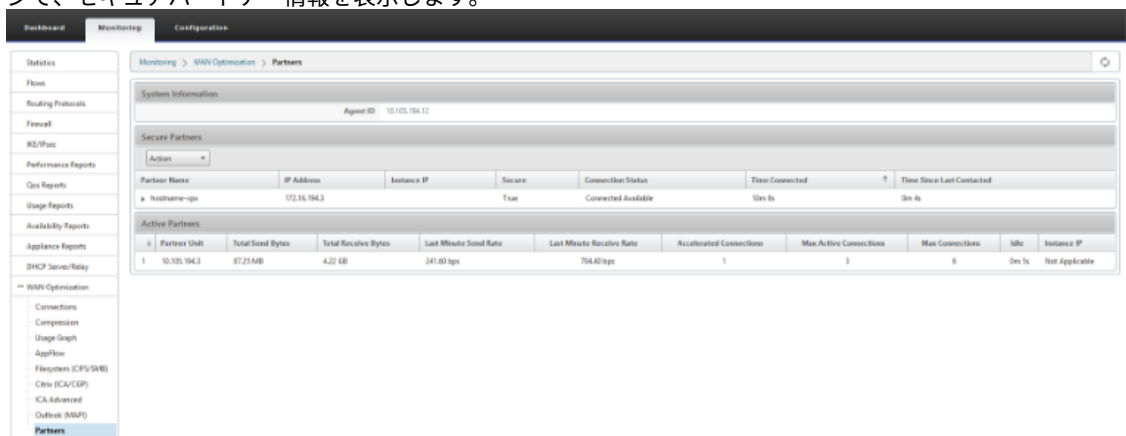
監視

[監視] ページの **[WANOptimization]** > [パートナー] の下にある、プレミアム（エンタープライズ）エディションアプライアンスのセキュアパートナー 情報を表示します。

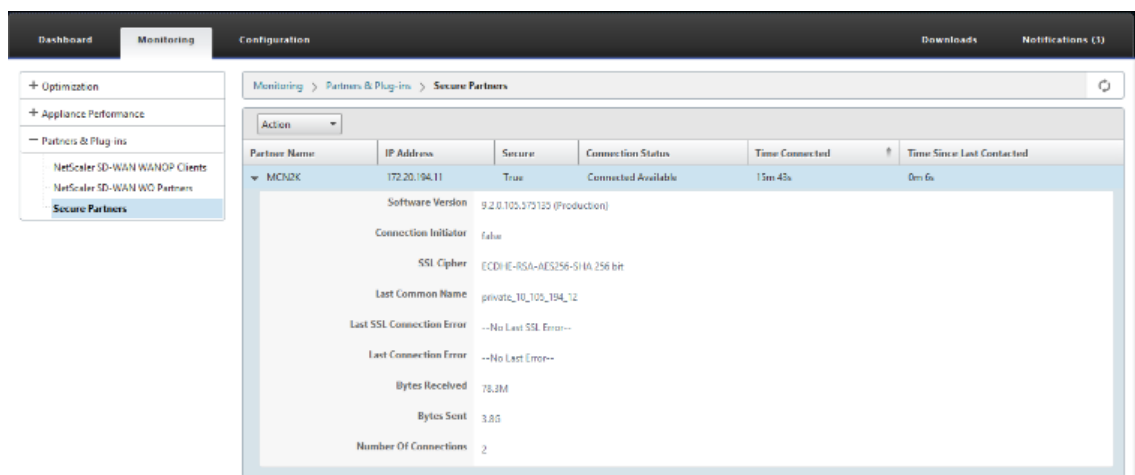
1. データストアの暗号化は、Premium (Enterprise) Edition アプライアンスの [最適化] ノードにある MCN から機能を有効化することで、Premium (Enterprise) Edition アプライアンス上で実行できます。
2. Premium (Enterprise) Edition アプライアンスの場合、セキュアピアリングは常に有効になります。
3. プライベート **CA** とプライベート証明書キーの ペアが正常に生成されたかどうかを確認するには、次の情報を確認します。



4. Premium (エンタープライズ) エディションアプライアンスの [監視] > [WAN 最適化] > [パートナー] ページで、セキュアパートナー情報を表示します。

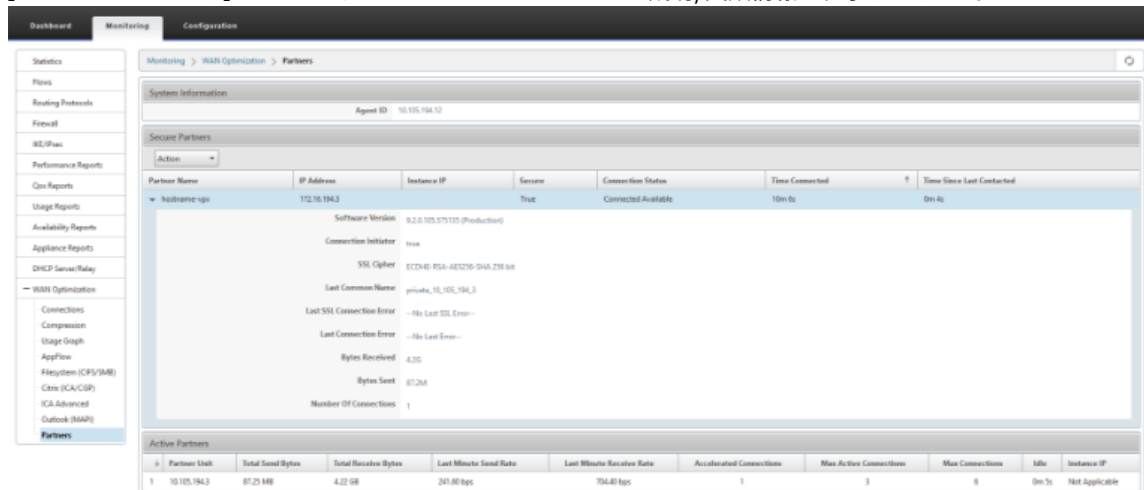


5. パートナーアプライアンスの [** 監視] > [パートナーとプラグイン] > [セキュア・パートナー] ページで、Premium (Enterprise) エディションアプライアンスのセキュア・パートナー情報を表示します**。

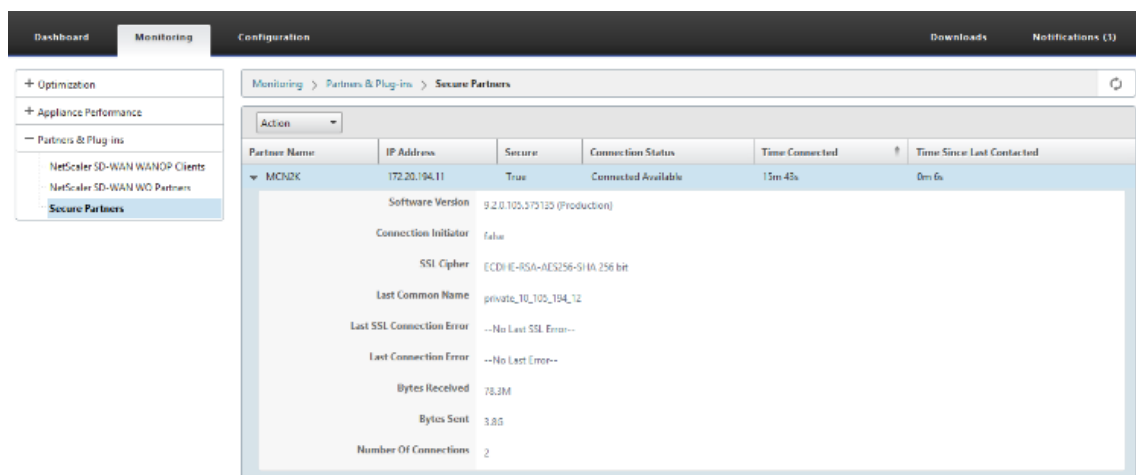


トラブルシューティング

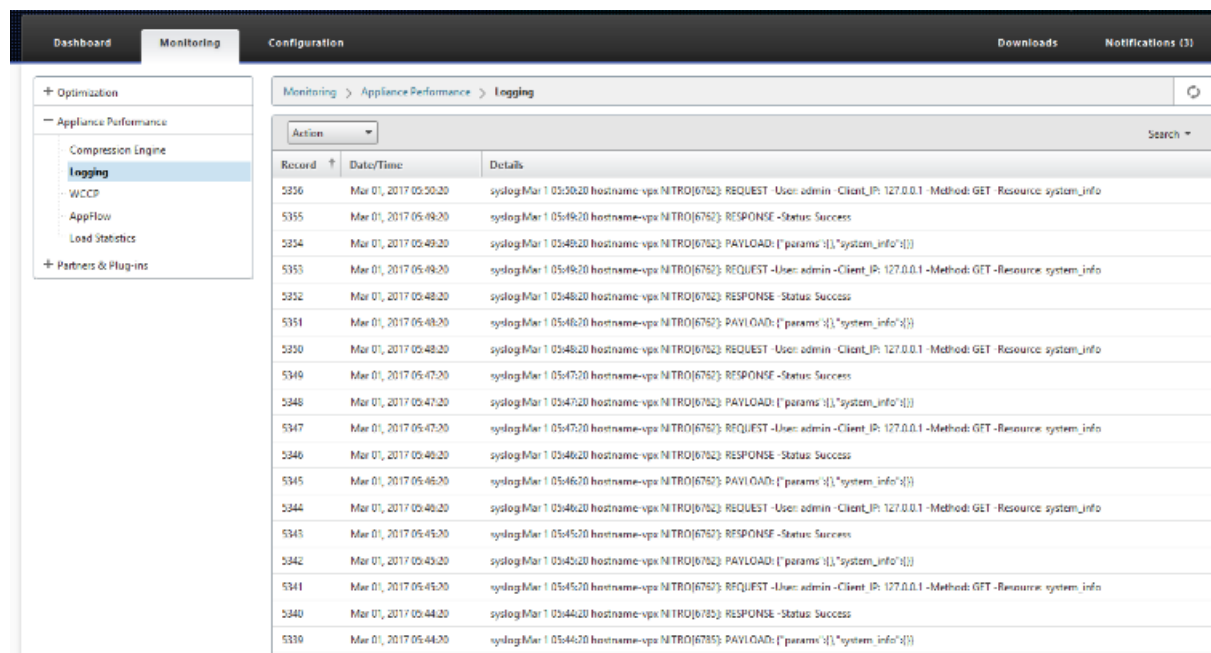
1. Premium (エンタープライズ) エディションアプライアンスの [監視] > [WAN 最適化] > [パートナー] > [セキュアパートナー] ページで、** セキュア・パートナーの成功/失敗情報を表示します **。



2. パートナーアプライアンスで、Premium (エンタープライズ) エディションアプライアンスの [監視] > [パートナーとプラグイン] > [セキュアパートナー] ページで、セキュアパートナー情報を表示します。



3. パートナーアプライアンスで、Premium（エンタープライズ）エディションアプライアンスの [監視] > [アプライアンスのパフォーマンス] > [ログ] ページの [セキュア・パートナー情報] を表示します。



DC サイトおよびブランチサイトの **PE** アプライアンスから、自動セキュアピアリングが開始されます

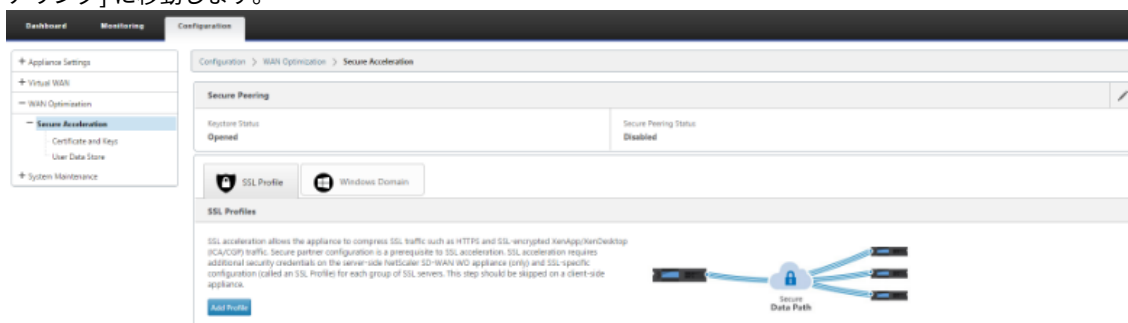
May 10, 2021

構成

DC の新しい Premium (Enterprise) Edition アプライアンスで自動セキュアピアリングを構成するには、次の手順を実行します。

- PE DC アプライアンスは、リスニングオンモード（ポート 443）です。ブランチ PE アプライアンスは CONNECT-to モードです。
- PE DC アプライアンスは、PE ブランチアプライアンスへの自動セキュアピアリングを開始します。このアプライアンスは、プライベート CA 証明書と CERT キーペアをインストールし、DC EE の LISTEN-ON IP を使用して PE ブランチアプライアンスに CONNECT-TO を設定します。
- PE アプライアンスの LISTEN-ON IP は、「WANOP にリダイレクト」が有効になっているルーティングドメインに関連付けられたインターフェイス IP にあります。

1. SD-WAN Web GUI で、[構成] > [**WAN Optimization**] > [セキュアアクセラレーション] > [セキュアピアリング] に移動します。



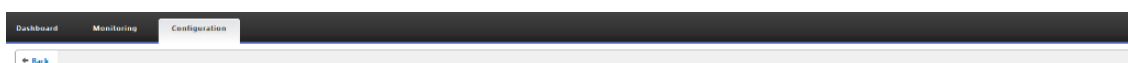
2. キーストアのパスワードを入力するか、キーストアを無効にして、キーストアを構成します。

Secure Peering

Keystore Settings

Security keys and settings are secured by the key store password. Each time the appliance restarts, the key store is closed automatically, and must be opened manually for secure acceleration to resume.

☐ Enable Keystore Password



Secure Peering

Keystore Settings

Security keys and settings are secured by the key store password. Each time the appliance restarts, the key store is closed automatically, and must be opened manually for secure acceleration to resume.

Keystore Status*

Open

☐ Change Keystore Password

☐ Disable Keystore Password

☐ Reset Keystore

Secure Peering

Keystore Settings

Security keys and settings are secured by the key store password. Each time the appliance restarts, the key store is closed automatically, and must be opened manually for secure acceleration to resume.

☒ Enable Keystore Password

Keystore Password*

Confirm Keystore Password*

3. 自動セキュアピアリングを実行するには、[プライベート **CA**] を選択して、セキュアピアリングを有効にします。

Secure Peering Certificate and Keys

Secure communications with the NetScaler SD-WAN VWO partner appliance requires that you generate OpenSSL credentials, including CA Certificate and a Certificate/Key pair, and select a verification method. You can optionally change the OpenSSL cipher specification. If PrivateCA is selected, certificates and keys are generated automatically.

☒ Enable Secure Peering

Certificate Configuration

☒ Private CA ☐ CA Certificate

Secure Peering Certificate and Keys

Secure Peering	Certificate/Key Pair Name	CA Certificate Store Name	Cipher Specification
Enabled	private_10_105_194_12	PrivateRootCA	IADH:IAECDH:IMD5-HIGH:@STRENGTH

Secure Peering	Certificate/Key Pair Name	CA Certificate Store Name	Cipher Specification
Enabled	private_10_105_194_12	PrivateRootCA	IADH:IAECDH:IMD5-HIGH:@STRENGTH

4. 「+」アイコンをクリックし、ユーザー名とパスワードで IP を追加します。指定されたりモート IP とクレデンシャルを使用した認証が成功すると、要求がリモートマシンに送信され、CA 証明書とプライベート証明書とキーがリモートマシンにローカルにインストールされます。

注

IP アドレス—リモート EE アプライアンス管理 IP の IP アドレス

ユーザー名—リモート EE アプライアンスのユーザー名

パスワード—リモート EE アプライアンスのパスワード

Connect Peer

IP Address: 10 . 105 . 194 . 3

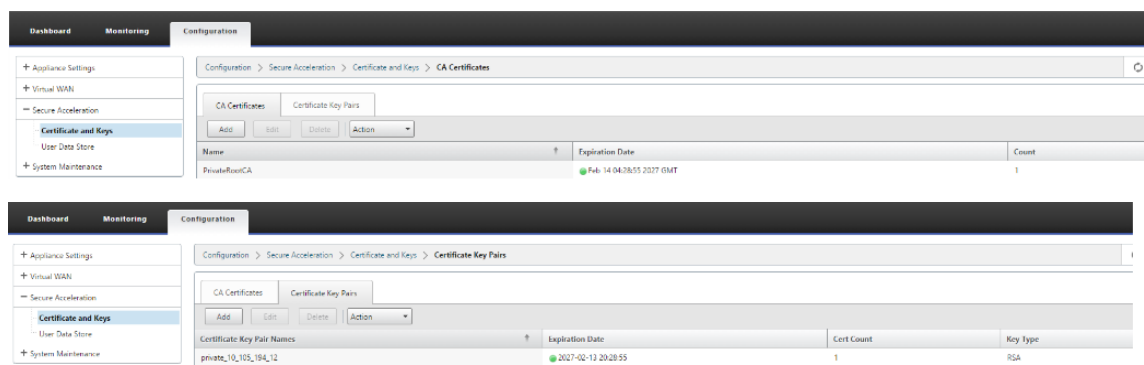
Username: admin

Password: ••••••••

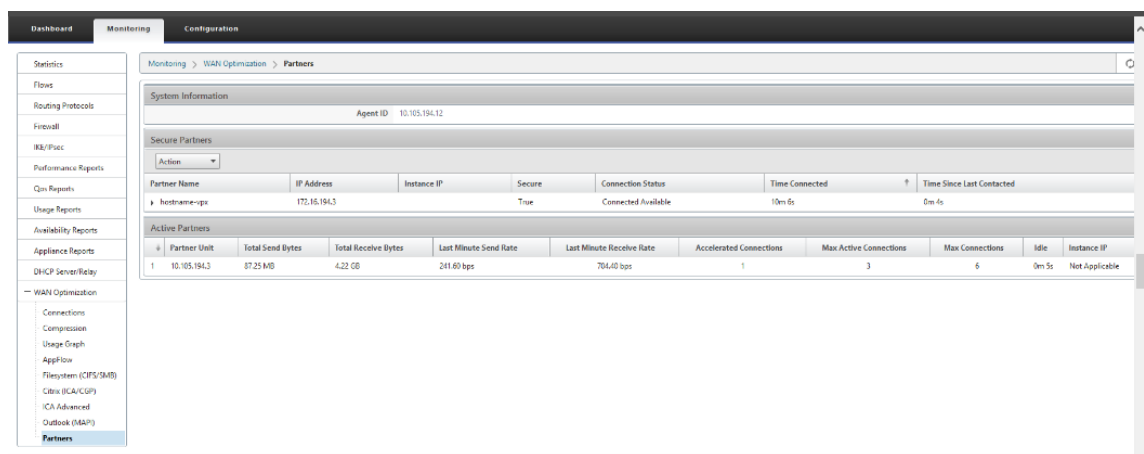
Connect **Close**

監視

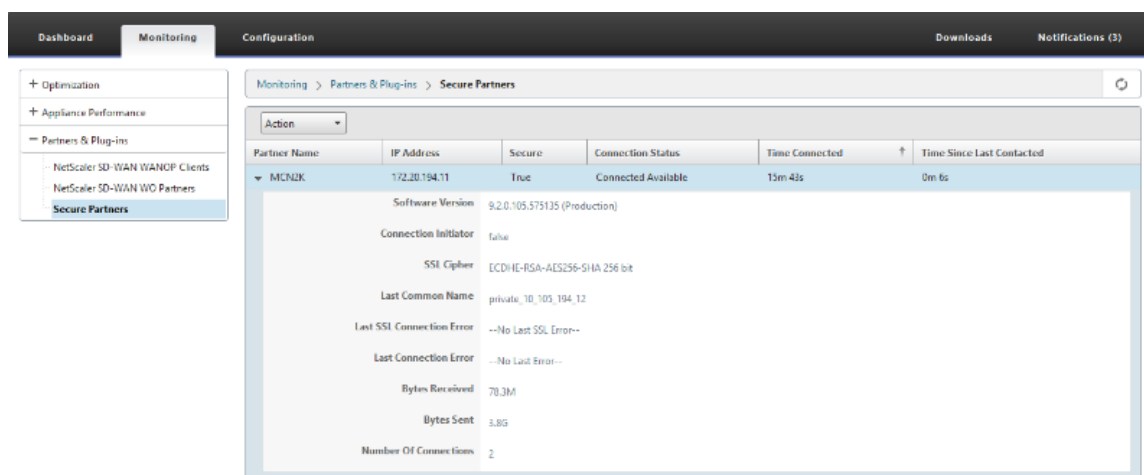
1. プライベート CA とプライベート証明書キーのペアが正常に生成されたかどうかを確認するには、以下に表示される情報を確認します。



2. Premium (エンタープライズ) エディションアプライアンスの [監視] > [WAN 最適化] > [パートナー] ページで、セキュアパートナー情報を表示します。



3. パートナーアプライアンスで、Premium (Enterprise) Edition アプライアンスの [監視] > [パートナーとプラグイン] > [セキュアパートナー] ページの [セキュアパートナー 情報] を表示します。



トラブルシューティング

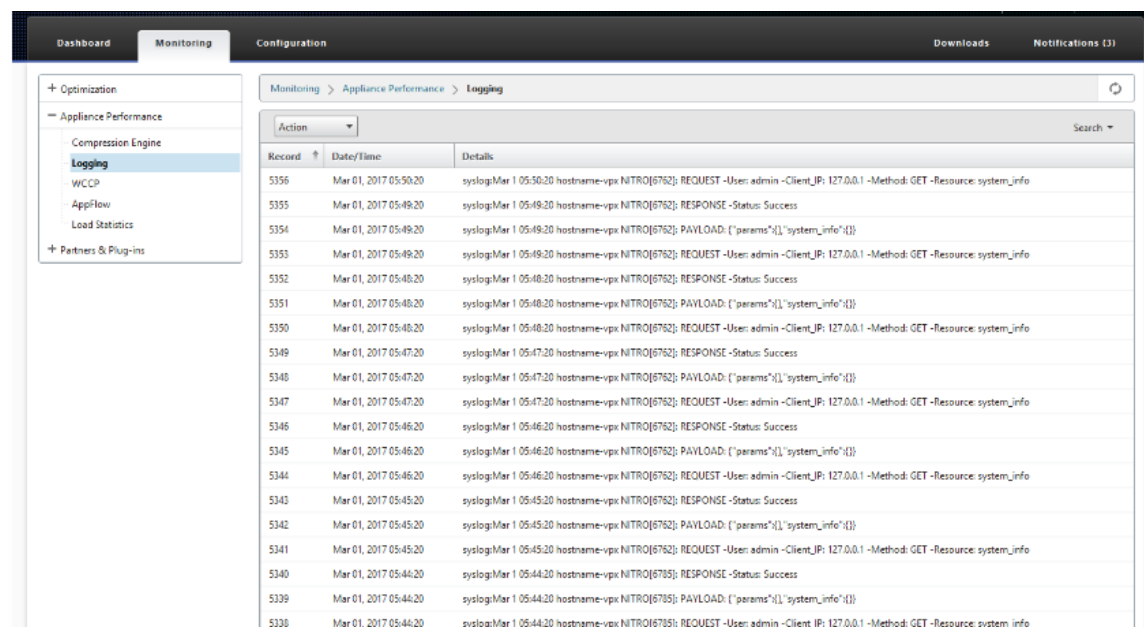
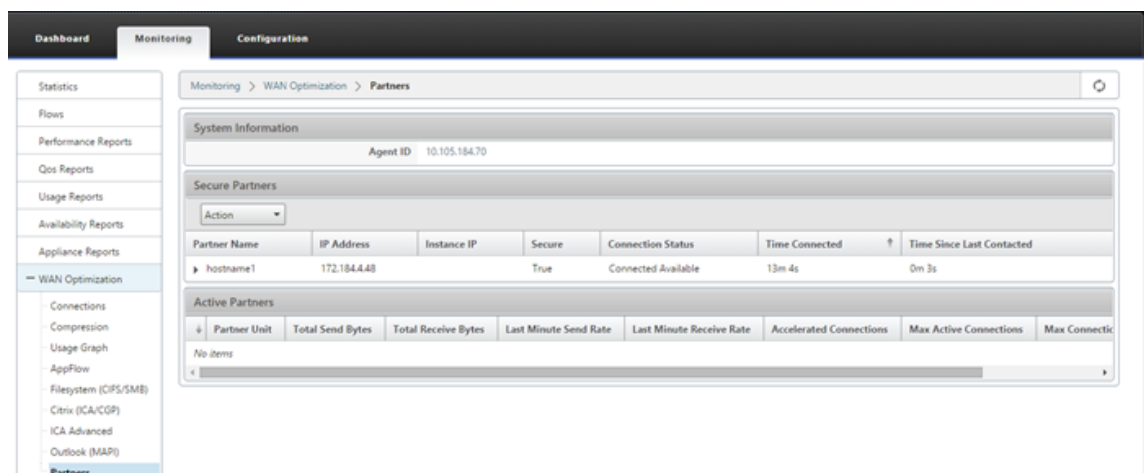
1. Premium (エンタープライズ) エディションアプライアンスの [監視] > [WAN 最適化] > [パートナー] > [セキュアパートナー] ページで、セキュア・パートナーの成功/失敗情報を表示します。

The screenshot shows the 'Secure Partners' page in the Citrix SD-WAN 11.4 interface. The left sidebar contains a navigation menu with options like Statistics, Flows, Routing Protocols, Firewall, IPS/IPSec, Performance Reports, QoS Reports, Usage Reports, Availability Reports, Appliance Reports, DHCP Server/Relay, WAN Optimization, Connections, Compression, Usage Graph, AppFlow, Filesystem (CIFS/SMB), Citrix (ICA/GOIP), ICA Advanced, and Outlook (MAP). The main content area is titled 'Monitoring > WAN Optimization > Partners'. It displays system information for Agent ID 10.105.194.12. Below this, there's a table for 'Secure Partners' with columns: Partner Name, IP Address, Instance IP, Secure, Connection Status, Time Connected, and Time Since Last Contacted. The table shows one partner named 'hostname-vpn' with IP 172.16.194.3, which is secure and connected. Below the table, there's a detailed view for the selected partner, showing software version (9.2.0.105.575135), connection initiator (true), SSL cipher (ECDHE-RSA-AES256-GCM-SHA 256 bit), last common name (private_10_105_194_3), last SSL connection error (No Last SSL Error), last connection error (No Last Error), bytes received (4.2G), bytes sent (67.2M), and number of connections (1). At the bottom, there's an 'Active Partners' table with columns: Partner Unit, Total Send Bytes, Total Receive Bytes, Last Minute Send Rate, Last Minute Receive Rate, Allocated Connections, Max Active Connections, Max Connections, Idle, and Instance IP. It shows one active partner with unit 10.105.194.3, sending 87.25 MB and receiving 4.22 GB, with rates of 247.80 bps and 704.40 bps, 1 allocated connection, 3 max active connections, 6 max connections, 0 idle, and instance IP Not Applicable.

2. パートナーアプライアンスで、Premium (Enterprise) Edition アプライアンスの [監視] > [パートナーとプラグイン] > [セキュアパートナー] ページの [セキュアパートナー 情報] を表示します。

The screenshot shows the 'Secure Partners' page in the Citrix SD-WAN 11.4 interface. The left sidebar contains a navigation menu with options like Optimization, Appliance Performance, Partners & Plug-ins, NetScaler SD-WAN WANOP Clients, NetScaler SD-WAN WO Partners, and Secure Partners. The main content area is titled 'Monitoring > Partners & Plug-ins > Secure Partners'. It displays a table for 'Secure Partners' with columns: Partner Name, IP Address, Secure, Connection Status, Time Connected, and Time Since Last Contacted. The table shows one partner named 'MCN2K' with IP 172.20.194.11, which is secure and connected. Below the table, there's a detailed view for the selected partner, showing software version (9.2.0.105.575135), connection initiator (false), SSL cipher (ECDHE-RSA-AES256-GCM-SHA 256 bit), last common name (private_10_105_194_12), last SSL connection error (No Last SSL Error), last connection error (No Last Error), bytes received (70.3M), bytes sent (3.8G), and number of connections (2).

3. パートナーアプライアンスで、Premium (Enterprise) Edition アプライアンスの [監視] > [アプライアンスのパフォーマンス] > [ログ] ページの [セキュリティで保護されたパートナー情報] を表示します。



スタンドアロンの **SD-WAN SE** および **WANOP** アプライアンスを使用して、**DC** サイトおよびブランチの **PE** アプライアンスから自動セキュアピアリングを開始

May 10, 2021

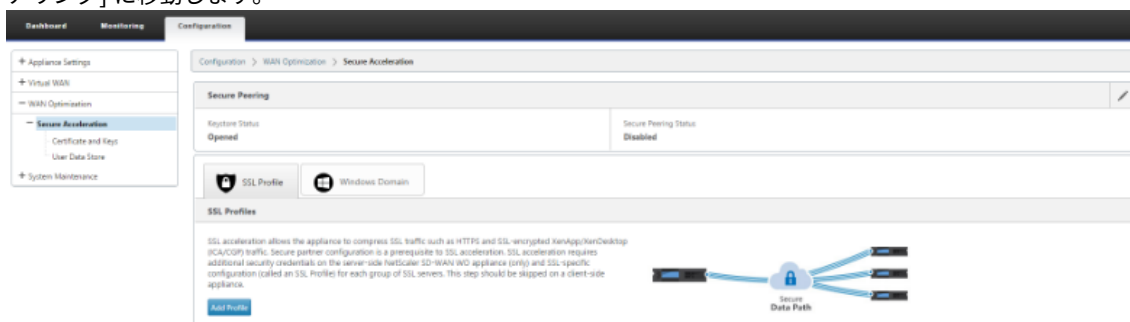
構成

スタンドアロン SD-WAN および WANOP アプライアンスを使用して、DC サイトおよびブランチで自動セキュアピアリング機能を備えた新しい Premium (Enterprise) Edition アプライアンスを構成するには、次の手順を実行し

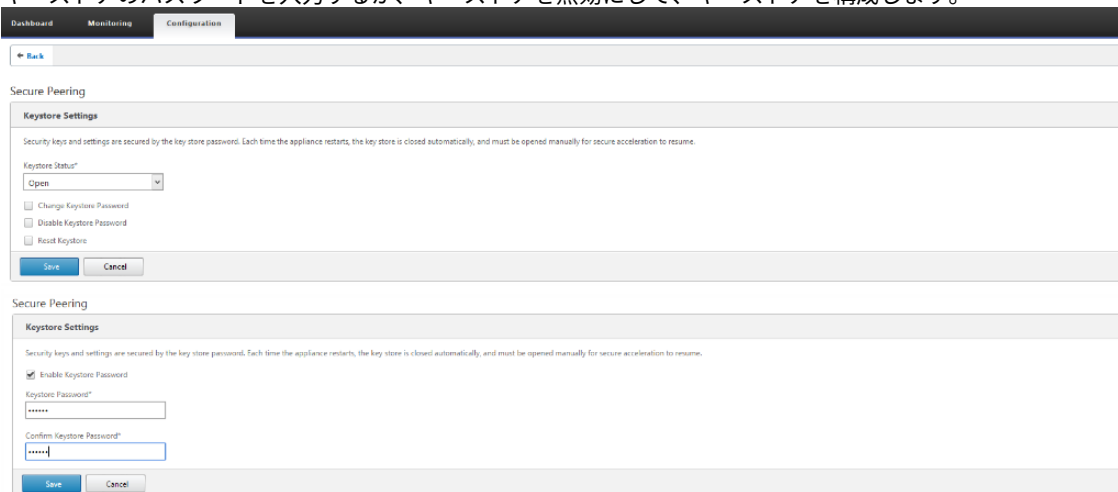
ます。

- PE DC アプライアンスは、リスニングオンモード（ポート 443）です。
- ブランチスタンドアロンの SD-WAN SE および WANOP は CONNECT-to モードです。
- PE DC アプライアンスは、ブランチスタンドアロンの SD-WAN SE および WANOP アプライアンスへの自動セキュアピアリングを開始します。このアプライアンスは、プライベート CA 証明書と CERT キーペアをインストールし、DC EE の LISTEN-ON IP を使用して PE アプライアンスに CONNECT-TO を設定します。

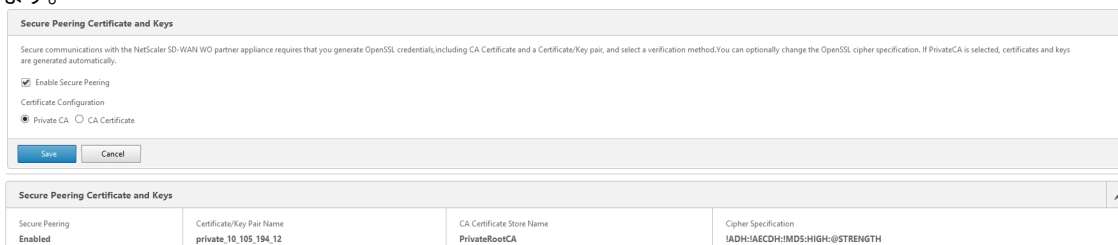
1. SD-WAN Web GUI で、[構成] > [**WAN Optimization**] > [セキュアアクセラレーション] > [セキュアピアリング] に移動します。



2. キーストアのパスワードを入力するか、キーストアを無効にして、キーストアを構成します。



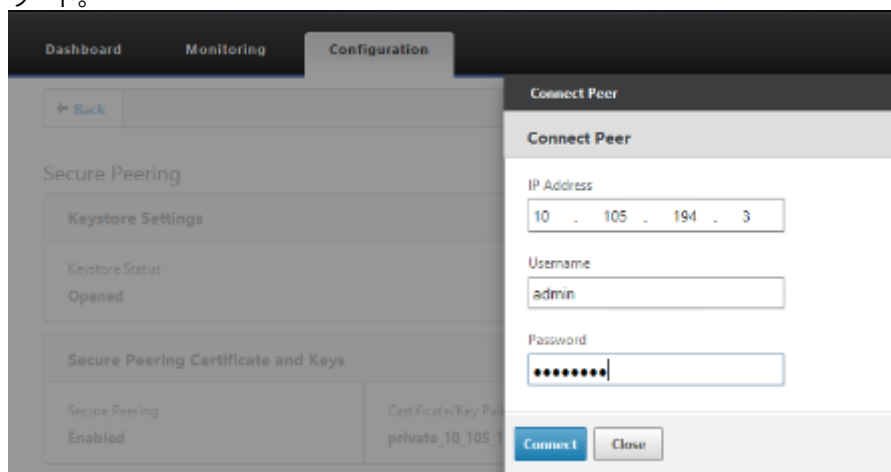
3. 自動セキュアピアリングを実行するには、[プライベート CA] を選択して、セキュアピアリングを有効にします。



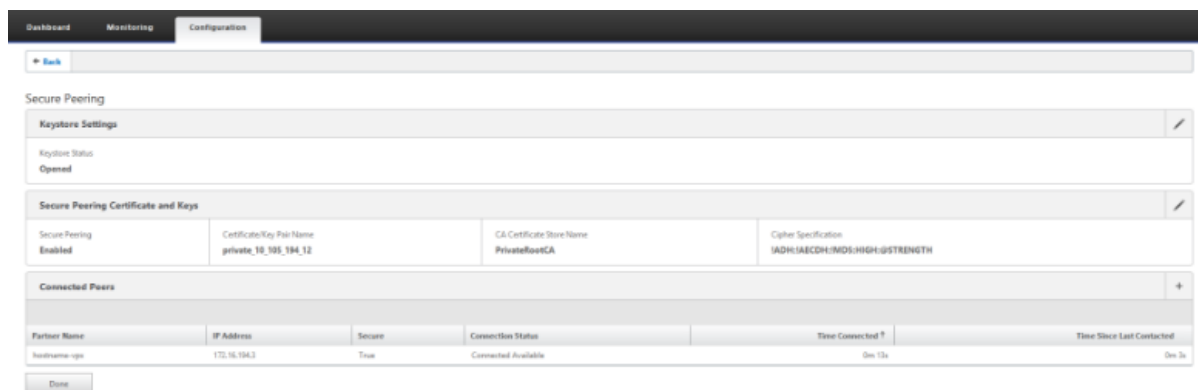
4. 「+」アイコンをクリックし、ユーザー名とパスワードで IP を追加します。指定されたりモート IP とクレデン

シャルを使用した認証が成功すると、要求がリモートマシンに送信され、CA 証明書とプライベート証明書とキーがリモートマシンにローカルにインストールされます。

- IP アドレス—リモート WANOP スタンドアロンまたは Standard Edition のアプライアンス管理 IP の IP アドレス。
- ユーザー名—リモート WANOP スタンドアロンまたは Standard Edition アプライアンスのユーザー名。
- パスワード—リモート WANOP スタンドアロンまたはスタンダードエディションアプライアンスのパスワード。

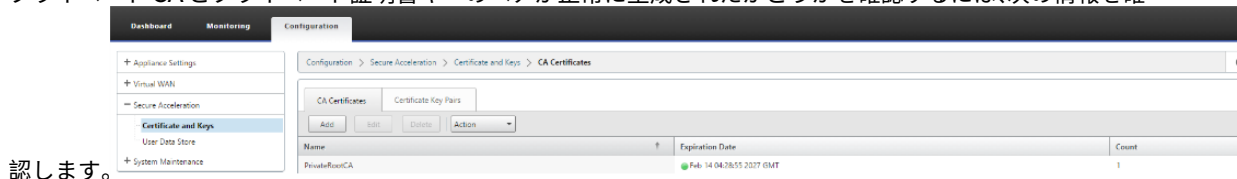


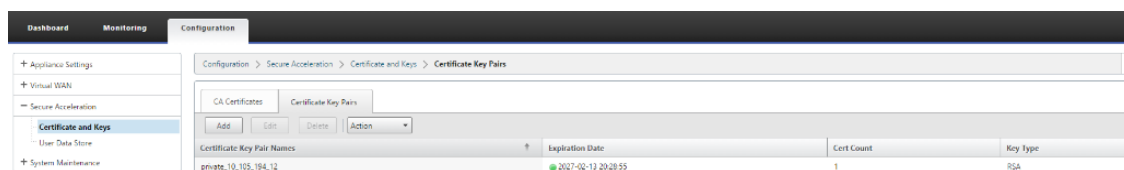
認証が成功すると、セキュアピアリングを TRUE として、パートナー IP をリモート WANOP スタンドアロンアプライアンスの仮想 IP の 1 つとして表示できます。



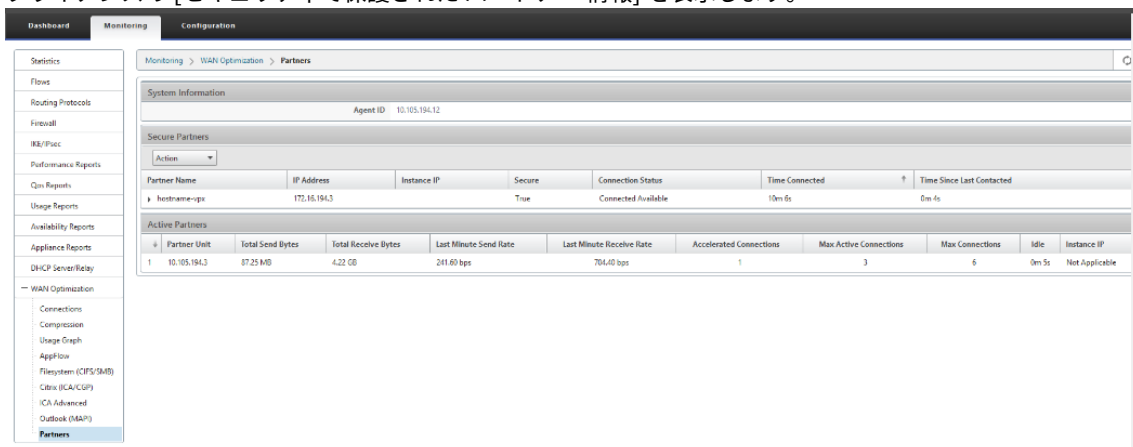
監視

1. プライベート CA とプライベート証明書キーのペアが正常に生成されたかどうかを確認するには、次の情報を確認します。

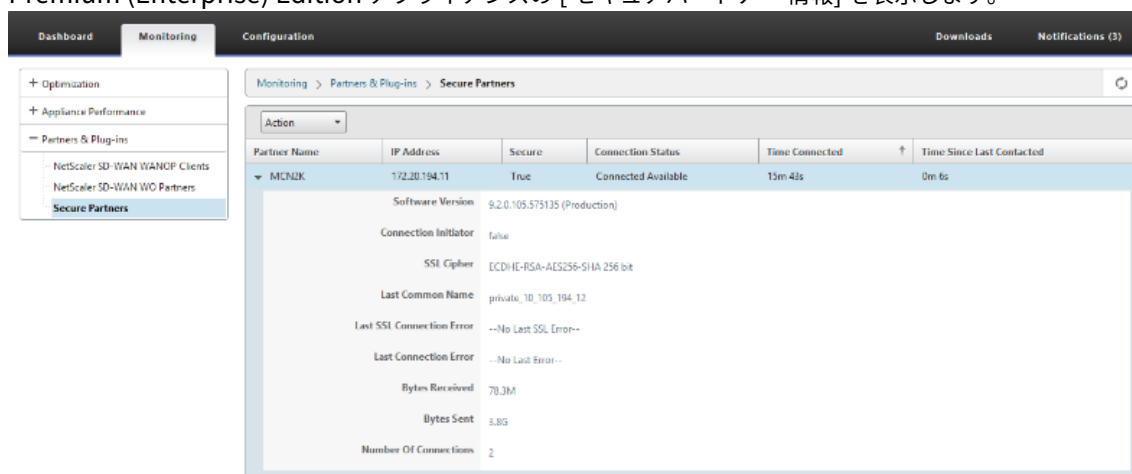




2. [監視] > [WAN Optimization] > [パートナー] ページで、プレミアム (エンタープライズ) エディションアプライアンスの [セキュリティで保護された パートナー 情報] を表示します。



3. パートナーアプライアンスで、[監視] > [パートナーと プラグイン] > [セキュアパートナー] ページで Premium (Enterprise) Edition アプライアンスの [セキュアパートナー 情報] を表示します。



トラブルシューティング

1. [監視] > [WAN Optimization] > [パートナー] > [セキュアパートナー] ページの Premium (Enterprise) Edition アプライアンスで、セキュア パートナーの 成功/失敗情報を表示します。

Monitoring > WAN Optimization > Partners

System Information
Agent ID: 10.105.194.12

Secure Partners

Partner Name	IP Address	Instance IP	Secure	Connection Status	Time Connected	Time Since Last Contacted
hostname-vpn	172.16.194.3		True	Connected Available	10m 4s	0m 4s

Software Version: 9.2.0.105.575135 (Production)
 Connection Initiator: true
 SSL Cipher: ECDHE-RSA-AES256-GCM-SHA-384
 Last Common Name: private_10_105_194_3
 Last SSL Connection Error: --No Last SSL Error--
 Last Connection Error: --No Last Error--
 Bytes Received: 4,20
 Bytes Sent: 67,284
 Number Of Connections: 1

Partner Unit	Total Send Bytes	Total Receive Bytes	Last Minute Send Rate	Last Minute Receive Rate	Accelerated Connections	Max Active Connections	Max Connections	Idle	Instance IP	
1	10.105.194.3	87.25 MB	4.22 GB	247.80 bps	704.40 bps	1	3	6	0m 5s	Not Applicable

2. パートナーアプライアンスで、Premium (Enterprise) Edition アプライアンスの [監視] > [パートナーとプラグイン] > [セキュアパートナー] ページの [セキュアパートナー情報] を表示します。

Monitoring > Partners & Plug-ins > Secure Partners

Partner Name	IP Address	Secure	Connection Status	Time Connected	Time Since Last Contacted
MCN2K	172.20.194.11	True	Connected Available	13m 44s	0m 6s

Software Version: 9.2.0.105.575135 (Production)
 Connection Initiator: false
 SSL Cipher: ECDHE-RSA-AES256-GCM-SHA-384
 Last Common Name: private_10_105_194_12
 Last SSL Connection Error: --No Last SSL Error--
 Last Connection Error: --No Last Error--
 Bytes Received: 70.3M
 Bytes Sent: 3.8G
 Number Of Connections: 2

3. パートナーアプライアンスで、Premium (Enterprise) Edition アプライアンスの [監視] > [アプライアンスのパフォーマンス] > [ログ] ページの [セキュアパートナー情報] を表示します。

Dashboard

Monitoring

Configuration

Downloads

Notifications (3)

+ Optimization

- Appliance Performance

Compression Engine

Logging

WCCP

AppFlow

Load Statistics

+ Partners & Plug-ins

Monitoring > Appliance Performance > Logging

Action

Search

Record	Date/Time	Details
5356	Mar 01, 2017 05:50:20	syslog:Mar 1 05:50:20 hostname-vpx NITRO[6762]: REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info
5355	Mar 01, 2017 05:49:20	syslog:Mar 1 05:49:20 hostname-vpx NITRO[6762]: RESPONSE -Status: Success
5354	Mar 01, 2017 05:49:20	syslog:Mar 1 05:49:20 hostname-vpx NITRO[6762]: PAYLOAD: {"params":{"system_info":{"
5353	Mar 01, 2017 05:49:20	syslog:Mar 1 05:49:20 hostname-vpx NITRO[6762]: REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info
5352	Mar 01, 2017 05:48:20	syslog:Mar 1 05:48:20 hostname-vpx NITRO[6762]: RESPONSE -Status: Success
5351	Mar 01, 2017 05:48:20	syslog:Mar 1 05:48:20 hostname-vpx NITRO[6762]: PAYLOAD: {"params":{"system_info":{"
5350	Mar 01, 2017 05:48:20	syslog:Mar 1 05:48:20 hostname-vpx NITRO[6762]: REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info
5349	Mar 01, 2017 05:47:20	syslog:Mar 1 05:47:20 hostname-vpx NITRO[6762]: RESPONSE -Status: Success
5348	Mar 01, 2017 05:47:20	syslog:Mar 1 05:47:20 hostname-vpx NITRO[6762]: PAYLOAD: {"params":{"system_info":{"
5347	Mar 01, 2017 05:47:20	syslog:Mar 1 05:47:20 hostname-vpx NITRO[6762]: REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info
5346	Mar 01, 2017 05:46:20	syslog:Mar 1 05:46:20 hostname-vpx NITRO[6762]: RESPONSE -Status: Success
5345	Mar 01, 2017 05:46:20	syslog:Mar 1 05:46:20 hostname-vpx NITRO[6762]: PAYLOAD: {"params":{"system_info":{"
5344	Mar 01, 2017 05:46:20	syslog:Mar 1 05:46:20 hostname-vpx NITRO[6762]: REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info
5343	Mar 01, 2017 05:45:20	syslog:Mar 1 05:45:20 hostname-vpx NITRO[6762]: RESPONSE -Status: Success
5342	Mar 01, 2017 05:45:20	syslog:Mar 1 05:45:20 hostname-vpx NITRO[6762]: PAYLOAD: {"params":{"system_info":{"
5341	Mar 01, 2017 05:45:20	syslog:Mar 1 05:45:20 hostname-vpx NITRO[6762]: REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info
5340	Mar 01, 2017 05:44:20	syslog:Mar 1 05:44:20 hostname-vpx NITRO[6762]: RESPONSE -Status: Success
5339	Mar 01, 2017 05:44:20	syslog:Mar 1 05:44:20 hostname-vpx NITRO[6762]: PAYLOAD: {"params":{"system_info":{"
5338	Mar 01, 2017 05:44:20	syslog:Mar 1 05:44:20 hostname-vpx NITRO[6762]: REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info

DC サイトおよびブランチ PE アプライアンスの PE アプライアンスから、手動によるセキュアピアリングを開始

May 10, 2021

この展開では、DC サイト PE アプライアンスがリスニングオンモードで構成され、ブランチサイト PE アプライアンスが接続先モードで構成されます。

- PE DC アプライアンスは、リスニングオンモード（ポート 443）です。
- ブランチ PE アプライアンスは CONNECT-to モードです。
- PE の LISTEN-ON IP は、「WANOP にリダイレクト」が有効になっているルーティングドメインに関連付けられたインターフェイス IP にあります。
- 認証局の認証元から取得した CA と Cert Key のペア証明書を手動でアップロードします。

構成

DC サイトの PE アプライアンスおよびブランチサイトの PE アプライアンスから開始される自動セキュアピアリングを設定するには、次の手順を実行します。

1. 本物の 証明書 から取得した **CA** 証明書と **CA** キー証明書をアップロードし、以下に示すように SD-WAN に提供します。

Configuration > Secure Acceleration > Certificate and Keys > CA Certificates

CA Certificates Certificate Key Pairs

Add Edit Delete Action

Name	Expiration Date	Count
CA	Feb 25 01:39:42 2032 GMT	1

Configuration > Secure Acceleration > Certificate and Keys > Certificate Key Pairs

CA Certificates Certificate Key Pairs

Add Edit Delete Action

Certificate Key Pair Names	Expiration Date	Cert Count	Key Type
CAKeyPair	2033-07-18 20:01:18	1	RSA

2. DC サイトの新しい PE アプライアンスで、SD-WAN Web GUI で、[設定]>[セキュアアクセラレーション]>[セキュアピアリング]の順に選択します。

Dashboard Monitoring Configuration

Configuration > WAN Optimization > Secure Acceleration

Secure Peering

Keystore Status: Opened Secure Peering Status: Disabled

SSL Profile Windows Domain

SSL Profiles

SSL acceleration allows the appliance to compress SSL traffic such as HTTPS and SSL-encrypted RDP/SSH/VPN traffic (ICA/COP) traffic. Secure peer configuration is a prerequisite to SSL acceleration. SSL acceleration requires additional security credentials on the server-side hardware SD-WAN WFO appliance (only) and SSL-specific configuration (called an SSL Profile) for each group of SSL servers. This step should be skipped on a client-side appliance.

Add Profile

3. キーストアのパスワードを入力するか、キーストアを無効にして、キーストアを構成します。

Secure Peering

Keystore Settings

Security keys and settings are secured by the key store password. Each time the appliance restarts, the key store is closed automatically, and must be opened manually for secure acceleration to resume.

☐ Enable Keystore Password

Save Cancel

Dashboard Monitoring Configuration

Secure Peering

Keystore Settings

Security keys and settings are secured by the key store password. Each time the appliance restarts, the key store is closed automatically, and must be opened manually for secure acceleration to resume.

Keystore Status: Open

☐ Change Keystore Password
☐ Disable Keystore Password
☐ Reset Keystore

Save Cancel

Secure Peering

Keystore Settings

Security keys and settings are secured by the key store password. Each time the appliance restarts, the key store is closed automatically, and must be opened manually for secure acceleration to resume.

☒ Enable Keystore Password

Keystore Password: *****

Confirm Keystore Password: *****

Save Cancel

4. [CA Certificate] オプションボタンを選択し、アップロードされた CA と CA キーのペア証明書を以下に示

すように適切に提供することで、セキュアピアリングを有効にします。

Secure Peering Certificate and Keys

Secure communications with the NetScaler SD-WAN WO partner appliance requires that you generate OpenSSL credentials, including CA Certificate and a Certificate/Key pair, and select a verification method. You can optionally change the OpenSSL cipher specification. If PrivateCA is selected, certificates and keys are generated automatically.

☒ Enable Secure Peering

Certificate Configuration

☐ Private CA ☒ CA Certificate

Certificate/Key Pair Name
CAKeyPair

CA Certificate Store Name
CA

Certificate Verification*
Signature/Expiration

SSL Cipher Specification
!ADH:!AECDH:!MD5:HIGH:@STRENGTH

☐ Edit Cipher Specification

5. 以下に示すように、ポート 443 とともにリモートマシンの仮想 IP を提供します。

Listen On and Connect To

Auto Discovery is typically enabled, when enabled, any authenticated peers can connect via the Listen On addresses. If disabled, secure communications are allowed only with peers on the Connect To list.

☒ Enable Auto-Discovery

Listen On

169.254.1.20 : 443 X

169.254.1.20 : 2312 X +

☒ Publish NAT addresses to peers

NAT Addresses

172.16.120.131 : 443 X +

Connect To

172.16.220.140 : 443 X +

監視

1. プライベート **CA** と秘密証明書キーのペアが正常に生成されたかどうかを検証するには、次の情報を確認します。

Dashboard Monitoring Configuration

Monitoring > WAN Optimization > Partners

System Information

Agent ID 10.105.194.12

Secure Partners

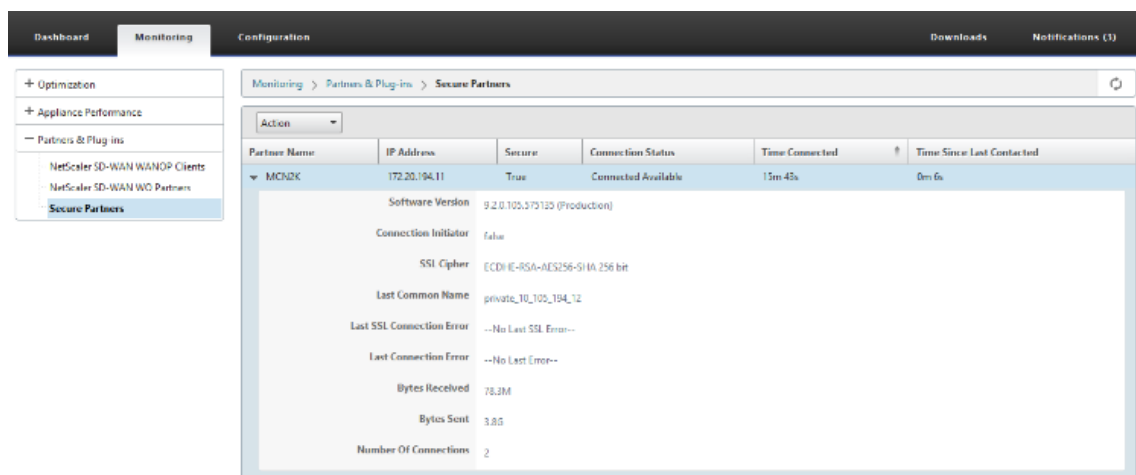
Action

Partner Name	IP Address	Instance IP	Secure	Connection Status	Time Connected	Time Since Last Contacted
heshame-gps	172.16.194.3		True	Connected Available	10m 5s	0m 4s

Active Partners

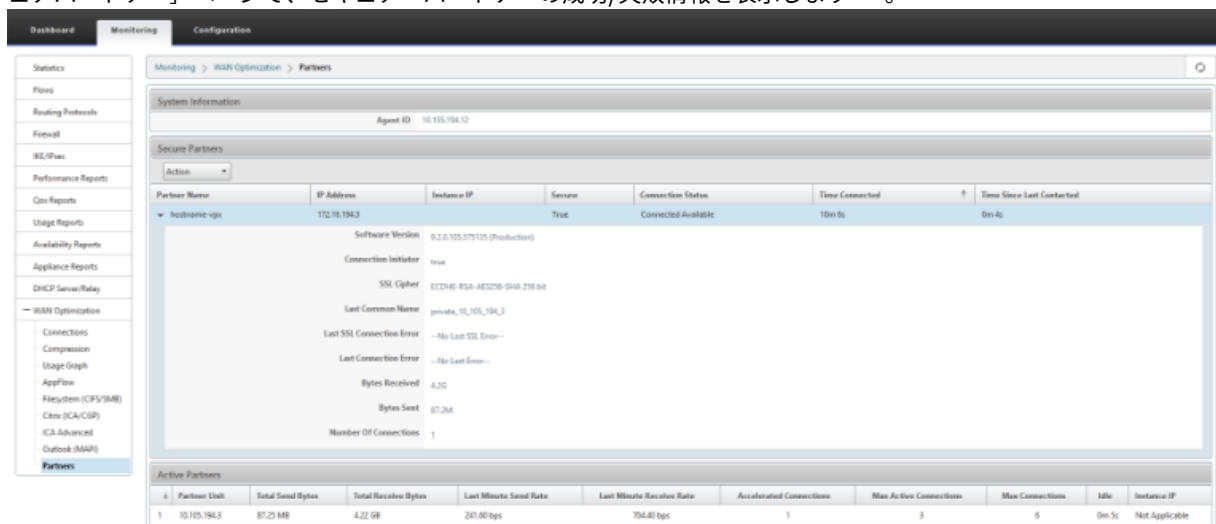
#	Partner Unit	Total Send Bytes	Total Receive Bytes	Last Minute Send Rate	Last Minute Receive Rate	Accelerated Connections	Max Active Connections	Max Connections	Idle	Instance IP
1	10.105.194.3	87.25 MB	4.22 GB	241.60 bps	704.00 bps	1	3	6	0m 5s	Not Applicable

2. パートナーアプライアンスで、Premium（エンタープライズ）エディションアプライアンスの [監視] > [パートナー] > [セキュアパートナー] ページの [**** セキュアパートナー情報**] を表示します ******。



トラブルシューティング

Premium (エンタープライズ) エディションアプライアンスの [監視] > **[WAN 最適化]** > [パートナー] > [セキュアパートナー] ページで、セキュア・パートナーの成功/失敗情報を表示します **。



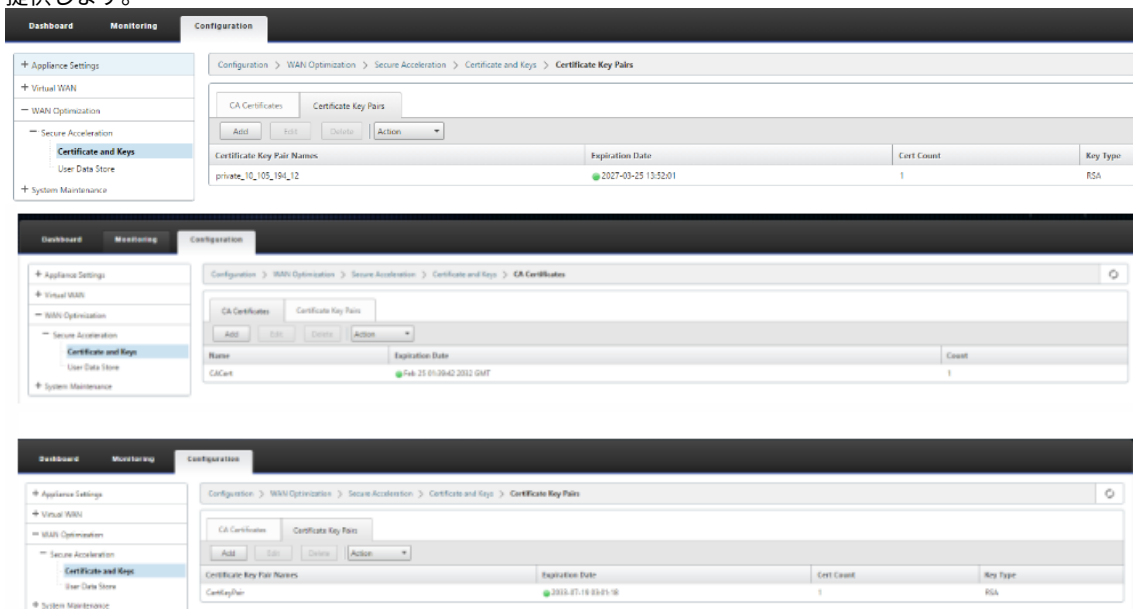
DC サイトの PE アプライアンスから、ブランチスタンドアロン SD-WAN SE および WANOP アプライアンスへの手動セキュアピアリング

May 10, 2021

- PE DC アプライアンスは、リスニングオンモード（ポート 443）です。
- ブランチ PE アプライアンスは CONNECT-to モードです。

- PE の LISTEN-ON IP は、「WANOP にリダイレクト」が有効になっているルーティングドメインに関連付けられたインターフェイス IP にあります。
- 認証局の本格的なソースから取得した CA 証明書と Cert Key ペアの証明書を手動でアップロードします。

1. 本物の 証明書 から取得した **CA** 証明書と **CA** キー証明書をアップロードし、以下に示すように SD-WAN に提供します。



2. DC サイトの新しい PE (Premium Edition) アプライアンスで、SD-WAN Web GUI で、[構成] > [セキュアアクセラレーション] > [セキュアピアリング] の順に選択します。



3. キーストアのパスワードを入力してキーストアを有効にするか、キーストアを無効にします。

Secure Peering

Keystore Settings

Security keys and settings are secured by the key store password. Each time the appliance restarts, the key store is closed automatically, and must be opened manually for secure acceleration to resume.

☐ Enable Keystore Password

DashboardMonitoringConfiguration

Back

Secure Peering

Keystore Settings

Security keys and settings are secured by the key store password. Each time the appliance restarts, the key store is closed automatically, and must be opened manually for secure acceleration to resume.

Keystore Status*
Open

☐ Change Keystore Password
☐ Disable Keystore Password
☐ Reset Keystore

SaveCancel

Secure Peering

Keystore Settings

Security keys and settings are secured by the key store password. Each time the appliance restarts, the key store is closed automatically, and must be opened manually for secure acceleration to resume.

☒ Enable Keystore Password

Keystore Password*

Confirm Keystore Password*

SaveCancel

4. [**CA Certificate**] オプションボタンを選択し、アップロードされた CA と CA キーのペア証明書を以下に示すように適切に提供することで、セキュアピアリングを有効にします。

Secure Peering Certificate and Keys

Secure communications with the NetScaler SD-WAN WO partner appliance requires that you generate OpenSSL credentials, including CA Certificate and a Certificate/Key pair, and select a verification method. You can optionally change the OpenSSL cipher specification. If PrivateCA is selected, certificates and keys are generated automatically.

☒ Enable Secure Peering

Certificate Configuration

☐ Private CA ☒ CA Certificate

Certificate/Key Pair Name
CAKeyPair

CA Certificate Store Name
CA

Certificate Verification*
Signature/Expiration

SSL Cipher Specification
[ADH:!AECDH:!MD5:HIGH:@STRENGTH]

☐ Edit Cipher Specification

SaveCancel

5. 以下に示すように、ポート 443 とともにリモートマシンの仮想 IP を提供します。

Listen On and Connect To

Connect To
172.16.194.3 443 × +

SaveCancel

Done

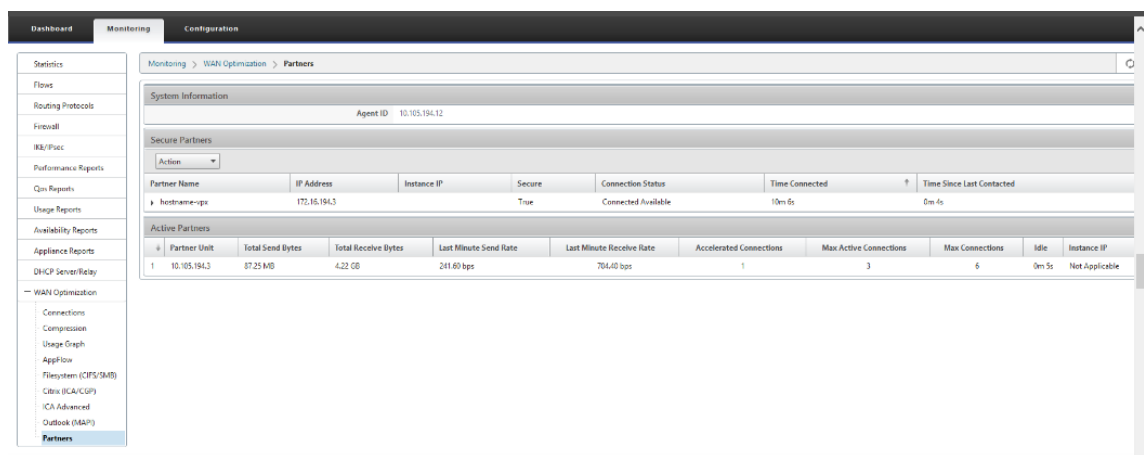
Listen On and Connect To

NAT IP published Yes	Auto Discovery Enabled	Listening On 172.20.194.11:443	Connected to 172.16.194.3:443
-------------------------	---------------------------	-----------------------------------	----------------------------------

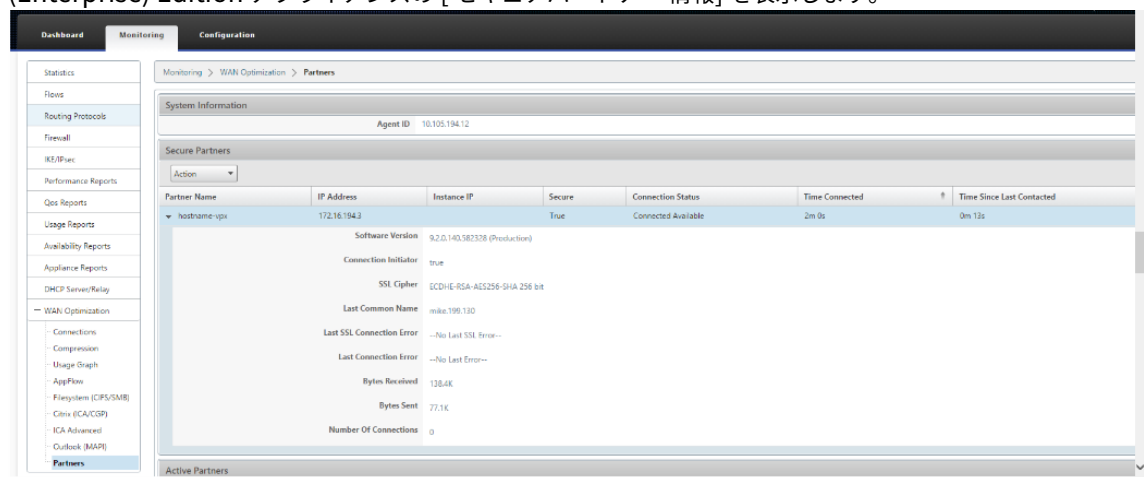
Done

監視

1. [監視] > [**WAN Optimization**] > [パートナー] ページで、プレミアム (エンタープライズ) エディションアプライアンスの [セキュリティで保護された パートナー 情報] を表示します。



2. パートナーアプライアンスで、[** 監視] > [パートナー] > [セキュアパートナー] ページで Premium (Enterprise) Edition アプライアンスの [セキュアパートナー 情報] を表示します。 **



トラブルシューティング

1. [監視] > [WAN Optimization] > [パートナー] > [セキュアパートナー] ページの Premium (Enterprise) Edition アプライアンスで、 ** セキュアパートナーの ** 成功 / 失敗情報 を表示します。

Dashboard

Monitoring

Configuration

Statistics

Flows

Routing Protocols

Firewall

RK/PPsec

Performance Reports

QoS Reports

Usage Reports

Availability Reports

Appliance Reports

DHCP Server/Relay

WAN Optimization

Connections

Compression

Usage Graph

AppFlow

Filesystem (CIFS/SMB)

Chive (CA/CDP)

ICA Advanced

Outlook (MAPI)

Partners

Monitoring > WAN Optimization > Partners

System Information

Agent ID 10.105.194.2

Secure Partners

Action

Partner Name	IP Address	Instance IP	Secure	Connection Status	Time Connected	Time Since Last Contacted
▼ hostname-vpn	172.16.194.3		True	Connected Available	10m 4s	0m 4s
<div>Software Version 9.2.0.101.575135 (Production)</div> <div>Connection Initiator true</div> <div>SSL Cipher ECDHE-RSA-AES128GCM-SHA256</div> <div>Last Common Name private_10.105.194.3</div> <div>Last SSL Connection Error --No Last SSL Error--</div> <div>Last Connection Error --No Last Error--</div> <div>Bytes Received 4,205</div> <div>Bytes Sent 67,284</div> <div>Number Of Connections 1</div>						

Active Partners

#	Partner Unit	Total Send Bytes	Total Receive Bytes	Last Minute Send Rate	Last Minute Receive Rate	Accelerated Connections	Max Active Connections	Max Connections	Idle	Instance IP
1	10.105.194.3	87.25 MB	4.22 GB	247.90 bps	704.40 bps	1	2	6	0m 5s	Not Applicable

2. パートナーアプライアンスで、Premium (Enterprise) Edition アプライアンスの [監視] > [アプライアンスのパフォーマンス] > [ログ] ページの [セキュアパートナー情報] を表示します。

Dashboard

Monitoring

Configuration

Downloads

Notifications (3)

+ Optimization

- Appliance Performance

Compression Engine

Logging

WCCP

AppFlow

Load Statistics

+ Partners & Plug-ins

Monitoring > Appliance Performance > Logging

Action

Record

Date/Time

Details

5356	Mar 01, 2017 05:50:20	syslog:Mar 1 05:50:20 hostname-vpx NITRO[6762]: REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info
5355	Mar 01, 2017 05:49:20	syslog:Mar 1 05:49:20 hostname-vpx NITRO[6762]: RESPONSE -Status: Success
5354	Mar 01, 2017 05:49:20	syslog:Mar 1 05:49:20 hostname-vpx NITRO[6762]: PAYLOAD: {'params':{'system_info':{}}
5353	Mar 01, 2017 05:49:20	syslog:Mar 1 05:49:20 hostname-vpx NITRO[6762]: REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info
5352	Mar 01, 2017 05:48:20	syslog:Mar 1 05:48:20 hostname-vpx NITRO[6762]: RESPONSE -Status: Success
5351	Mar 01, 2017 05:48:20	syslog:Mar 1 05:48:20 hostname-vpx NITRO[6762]: PAYLOAD: {'params':{'system_info':{}}
5350	Mar 01, 2017 05:48:20	syslog:Mar 1 05:48:20 hostname-vpx NITRO[6762]: REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info
5349	Mar 01, 2017 05:47:20	syslog:Mar 1 05:47:20 hostname-vpx NITRO[6762]: RESPONSE -Status: Success
5348	Mar 01, 2017 05:47:20	syslog:Mar 1 05:47:20 hostname-vpx NITRO[6762]: PAYLOAD: {'params':{'system_info':{}}
5347	Mar 01, 2017 05:47:20	syslog:Mar 1 05:47:20 hostname-vpx NITRO[6762]: REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info
5346	Mar 01, 2017 05:46:20	syslog:Mar 1 05:46:20 hostname-vpx NITRO[6762]: RESPONSE -Status: Success
5345	Mar 01, 2017 05:46:20	syslog:Mar 1 05:46:20 hostname-vpx NITRO[6762]: PAYLOAD: {'params':{'system_info':{}}
5344	Mar 01, 2017 05:46:20	syslog:Mar 1 05:46:20 hostname-vpx NITRO[6762]: REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info
5343	Mar 01, 2017 05:45:20	syslog:Mar 1 05:45:20 hostname-vpx NITRO[6762]: RESPONSE -Status: Success
5342	Mar 01, 2017 05:45:20	syslog:Mar 1 05:45:20 hostname-vpx NITRO[6762]: PAYLOAD: {'params':{'system_info':{}}
5341	Mar 01, 2017 05:45:20	syslog:Mar 1 05:45:20 hostname-vpx NITRO[6762]: REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info
5340	Mar 01, 2017 05:44:20	syslog:Mar 1 05:44:20 hostname-vpx NITRO[6762]: RESPONSE -Status: Success
5339	Mar 01, 2017 05:44:20	syslog:Mar 1 05:44:20 hostname-vpx NITRO[6762]: PAYLOAD: {'params':{'system_info':{}}
5338	Mar 01, 2017 05:44:20	syslog:Mar 1 05:44:20 hostname-vpx NITRO[6762]: REQUEST -User: admin -Client_IP: 127.0.0.1 -Method: GET -Resource: system_info

ドメイン参加と代理ユーザーの作成

May 10, 2021

DC から windows ドメインに新しいプレミアム（エンタープライズ）エディション（**PE**）アプライアンスを設定するには:

1. SD-WAN Web GUI で [Windows ドメイン] に移動し、[構成] > [セキュアアクセラレーション] に移動し、[

Windows ドメインに参加] をクリックします。

The screenshot shows the 'Configuration > Secure Acceleration' page. On the left, a sidebar contains 'Appliance Settings', 'Virtual WAN', 'Secure Acceleration' (selected), 'Certificate and Keys', 'User Data Store', and 'System Maintenance'. The main content area shows 'SSL Optimization status : ACTIVE' with a 'Disable' button. Below this is the 'Secure Peering' section with 'Keystore Status' as 'Opened' and 'Secure Peering Status' as 'Enabled'. The 'Windows Domain' tab is selected, showing a 'Join Windows Domain' button and a diagram of a Branch Office connected to a Datacenter via WAN. Below the diagram, text explains that joining the domain allows the appliance to be a trusted member of the domain's security infrastructure.

The 'Windows Domain' configuration form is shown below the main content area. It includes fields for 'Domain Name*', 'User Name*', and 'Password*', each with a 'Check Domain Join' link. There is a 'Leave Domain' checkbox and a 'DNS Servers*' dropdown menu with '10.105.194.17' selected. At the bottom are 'OK' and 'Cancel' buttons.

2. **Windows** ドメイン名を指定し、ドメイン参加 の事前チェックを実行します。

The screenshot shows the 'Configuration > Secure Acceleration' page with the 'Windows Domain' tab selected. A 'Domain Check : Summary' dialog box is open, displaying the results of a pre-join check. The dialog box has a title bar 'Domain Check : Summary' and a list of four tests, all marked with green checkmarks: 'DNS Reachability Test', 'Forward lookup Test', 'Domain Reachability Test', and 'Host Name Validation Test'. Below the list is a 'More' link and a 'Close' button.

3. 事前チェックの概要が正常に表示されたら、ドメインコントローラの資格情報を入力します。

SSL Profile

Windows Domain

Windows Domain

Join the server-side NetScaler SD-WAN appliance to a domain that the Windows file server and Exchange server are a part of. Joining the domain makes the appliance a trusted member of the Windows security system.

Domain Name*
2keepod.com
[Check Domain Join](#)

User Name*
administrator

Password*

[?](#)

☐ Leave Domain

DNS Servers*
10.105.194.17
[?](#)

OK

Cancel

Secure Peering

Keystore Status
Opened

SSL Profile

Windows Domain

Windows Domain

Join the server-side NetScaler SD-WAN appliance to a domain that the Windows file server and Exchange server are a part of. Joining the domain makes the appliance a trusted member of the Windows security system.

Domain Name*
2keepod.com
[Check Domain Join](#)

User Name*
administrator

Password*

[?](#)

☐ Leave Domain

DNS Servers*
10.105.194.17
[?](#)

OK

Cancel

Domain Join Operation

Joining Domain

Completed

4. ドメイン参加に成功すると、次の出力が得られます。

SSL Profile

Windows Domain

Windows Domain

Member of domain 2Keepod.com	DNS Server 10.105.194.17	Hostname hostname-vpx
------------------------------	-----------------------------	--------------------------

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

724

ユーザーを委任する

1. 以下に示すように、サービスを委任するデリゲートユーザーを追加します。

Delegate Users

Add X Edit Delete Services

Add a delegate user account of the Windows domain controller. The NetScaler SD-WAN appliance uses this account on behalf of the users, to authenticate them with the domain controller.

Domain Name* [Check Delegate User](#) ?

User Name*

Password*

Add Cancel

User Name	Domain Name	Status
No items		

2. 正しいドメイン名を指定し、代理ユーザーの事前チェックを実行します。

Delegate Users

Add X Edit

Add a delegate user account of the Windows domain controller. The NetScaler SD-WAN appliance uses this account on behalf of the users, to authenticate them with the domain controller.

Domain Name* [Check Delegate User](#)

User Name*

Password*

Add Cancel

⚙️ Delegate User Domain Check

⚙️ Trying to validate Delegate User Domain ...

Delegate User Check : Summary

Delegate User Check : Summary

✔ DNS Reachability Test

✔ Forward lookup Test

✔ Domain Reachability Test

⚠ Host Name Validation Test

✔ Kerberos config file check

⚠ Reverse lookup zone

✔ Time Skew Check

✔ Kerberos Port Check

✔ NTP Port Check

✔ Server record for kerberos

✔ Server record for ldap

▶ More

Close

3. 代理ユーザーの事前チェックが成功したら、代理ユーザーの有効な資格情報を入力します。

Delegate Users

Add X

Edit

Delete

Services

Add a delegate user account of the Windows domain controller. The NetScaler SD-WAN appliance uses this account on behalf of the users, to authenticate them with the domain controller.

Domain Name*

2keepod.com

Check Delegate User

User Name*

userdel

Password*

.....?

Add

Cancel

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

726

4. 代理ユーザが SD-WAN に正常に追加されると、成功メッセージが表示されます。

Delegate Users		
Add ▾ Edit Delete Services		
User Name	Domain Name	Status
userdel	2KEEPOD.COM	Success

5. 委任ユーザーによって委任されているすべてのサービスを確認するには、そのユーザーをポイントし、サービスを選択します。

Delegate User Details	
Delegate User Details ×	
Services	
cifs/WIN-KJ8BEBRNRUD.2KEEPOD.COM/2KEEPOD.COM	
exchangeMDB/WIN-KJ8BEBRNRUD.2KEEPOD.COM	
Close	

セキュリティ

May 10, 2021

このセクションのトピックでは、Citrix SD-WAN 展開に関する一般的なセキュリティガイダンスを提供します。

Citrix SD-WAN 展開のガイドライン

展開ライフサイクルを通じてセキュリティを維持するには、次のセキュリティを考慮することをお勧めします。

- 物理的セキュリティ
- アプライアンスのセキュリティ
- ネットワークセキュリティ
- 管理と管理

次のリンクで説明するトピックでは、を使用して SD-WAN ネットワークのセキュリティを設定する方法について詳しく説明します。

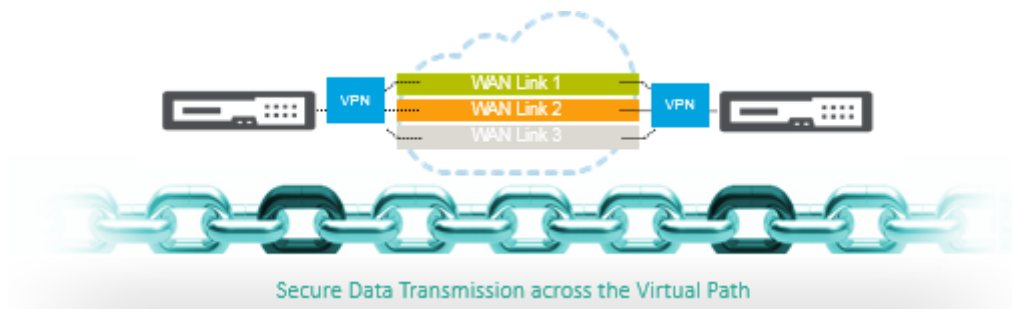
- [IPSec トンネル](#)
- [ファイアウォール](#)

IPsec トンネル終了

May 10, 2021

Citrix SD-WAN は IPsec 仮想パスをサポートしているため、サードパーティ製のデバイスが、Citrix SD-WAN アプライアンスの LAN または WAN 側で IPsec VPN トンネルを終了できます。140-2 レベル 1 FIPS 認定の IPsec 暗号化バイナリを使用して、SD-WAN アプライアンスで終端するサイト間の IPsec トンネルを保護できます。

また、Citrix SD-WAN は、差別化された仮想パストンネリングメカニズムを使用した耐障害性 IPsec トンネリングもサポートします。



Citrix SD-WAN と AWS トランジットゲートウェイとの統合

May 10, 2021

アマゾンウェブサービス (**AWS**) トランジット **Gateway** サービスを使用すると、Amazon 仮想プライベートクラウド (VPC) とオンプレミスのネットワークを 1 つのゲートウェイに接続できます。AWS で実行されるワークロードの数が増えるにつれて、複数のアカウントと Amazon VPC にまたがってネットワークを拡張し、その増加に対応できます。

ピアリングを使用して Amazon VPC のペアを接続できるようになりました。ただし、多くの Amazon VPC 間でポイントツーポイント接続を管理するには、接続ポリシーを一元管理する機能がないと、運用上のコストがかかり、煩雑になる可能性があります。オンプレミスの接続では、AWS VPN を個々の Amazon VPC にアタッチする必要があります。このソリューションは構築に時間がかかり、VPC の数が数百個に増えると、管理が難しい場合があります。

AWS Transit Gateway では、中央ゲートウェイからネットワーク経路で各 Amazon VPC、オンプレミスのデータセンター、またはリモートオフィスへの 1 つの接続を作成および管理するだけでかまいません。Transit Gateway は、スポークのように動作するすべての接続ネットワーク間でトラフィックがどのようにルーティングされるかを制御するハブとして機能します。このハブアンドスポークモデルでは、管理が大幅に簡素化され、運用コストが削減されます。これは、各ネットワークはトランジットゲートウェイにのみ接続し、他のすべてのネットワークには接続しないためです。新しい VPC はトランジットゲートウェイに接続され、トランジットゲートウェイに接続されている他のすべてのネットワークで自動的に利用できるようになります。この接続性の容易さにより、成長に合わせてネットワークの拡張が容易になります。

企業が増加するアプリケーション、サービス、インフラストラクチャをクラウドに移行するにつれ、SD-WAN を迅速に導入して、ブロードバンド接続のメリットを享受し、ブランチサイトのユーザーをクラウドリソースに直接接続します。インターネット転送サービスを使用してグローバルなプライベートネットワークを構築および管理し、地理的

に分散した場所とユーザーを近位ベースのクラウドリソースで接続するという複雑さには、多くの課題があります。**AWS** トランジットゲートウェイネットワークマネージャーは、このパラダイムを変更します。現在、AWS を使用する Citrix SD-WAN のお客様は、Citrix SD-WAN ブランチアプライアンスの AWS Transit Gateway を統合することにより、Citrix SD-WAN を AWS トランジットゲートウェイとともに使用できるようになりました。これにより、トランジットゲートウェイに接続されたすべての VPC に手を差し伸べる機能を持つユーザーに最高品質のエクスペリエンスを提供できます。

次に、Citrix SD-WAN と AWS トランジットゲートウェイを統合する手順を示します。

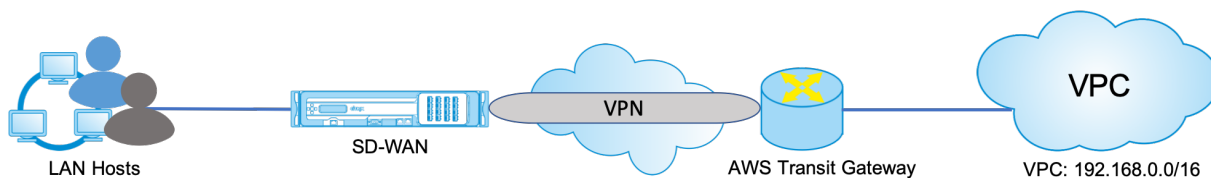
1. AWS トランジットゲートウェイを作成します。
2. VPN を中継ゲートウェイ（既存の VPN または新しい VPN のいずれか）に接続します。
3. オンプレミスまたは任意のクラウド（AWS、Azure、または GCP）にある SD-WAN サイトで VPN が設定されたトランジットゲートウェイに VPN を接続します。
4. Citrix SD-WAN から AWS Transit Gateway と IPsec トンネルを介したボーダーゲートウェイプロトコル（BGP）ピアリングを確立し、トランジットゲートウェイに接続されたネットワーク（VPC）を学習します。

使用例

ユースケースは、ブランチ環境から AWS 内（任意の VPC 内）にデプロイされたリソースに手を差し伸べます。AWS Transit Gateway を使用すると、トラフィックは BGP ルートを処理せずに、Transit Gateway に接続されたすべての VPC に到達できます。これを実現するには、次の方法を実行します。

- ブランチの Citrix SD-WAN アプライアンスから AWS トランジットゲートウェイへの IPsec を確立します。この展開方法では、トラフィックが IPsec を通過するため、SD-WAN の利点をすべて得ることはありません。
- AWS 内に Citrix SD-WAN アプライアンスをデプロイし、仮想パスを介してオンプレミスの Citrix SD-WAN アプライアンスに接続します。

どちらの方法を選択しても、トラフィックは、AWS インフラストラクチャ内のルーティングを手動で管理することなく、Transit Gateway に接続されている VPC に到達します。



AWS トランジットゲートウェイの設定

AWS トランジットゲートウェイを作成するには、VPC ダッシュボードに移動し、[トランジットゲートウェイ] セクションに移動します。

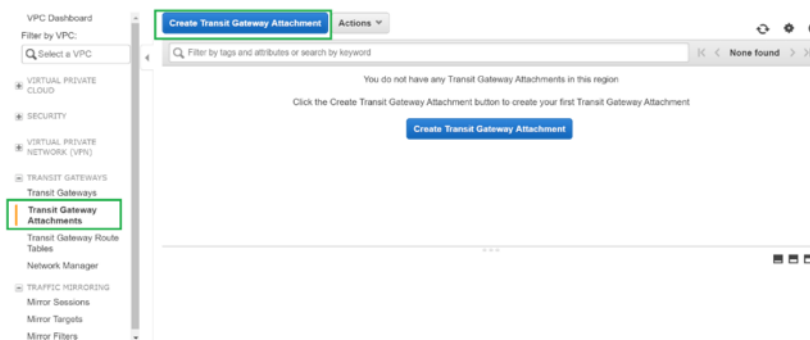
1. 次のスクリーンショットで強調表示されているとおりにトランジットゲートウェイ名、説明、Amazon ASN 番号を指定し、[**Create Transit Gateway**] をクリックします。

トランジットゲートウェイの作成が完了すると、ステータスが [**Available**] として表示されます。

Name	Transit Gateway ID	Owner ID	State
Citrix-TGW	tgw-087192c78b2ba0c8	55697391706	available

Transit Gateway: tgw-087192c78b2ba0c8	
Transit Gateway ID	tgw-087192c78b2ba0c8
State	available
DNS support	enable
Auto accept shared attachments	enable
Association route table ID	tgw-rs-02c2307c1b642e45
Propagation route table ID	tgw-rs-02c2307c1b642e45
Owner account ID	55697391706
Amazon ASN	65500
VPN ECMP support	enable
Default association route table	enable
Default propagation route table	enable

2. トランジットゲートウェイの添付ファイルを作成するには、「トランジットゲートウェイ」>「トランジットゲートウェイの添付ファイル」に移動し、「トランジットゲートウェイの添付ファイルの作成」をクリックします。



3. ドロップダウンリストから作成したトランジットゲートウェイを選択し、**VPC** としてアタッチメントタイプを選択します。添付ファイル名タグを指定し、作成したトランジットゲートウェイにアタッチする VPC ID を選択します。選択した VPC のサブネットの 1 つが自動選択されます。[アタッチメントを作成] をクリックして、VPC をトランジットゲートウェイにアタッチします。

Transit Gateway ID: tgn-attch-0c1c3a6294cc2d95

Attachment type: VPN

VPC Attachment

Attachment name: VPC102188

VPC ID: vpc-05b0c147aaf000405

Subnet ID	Subnet
subnet-043020b9b1703405	subnet-043020b9b1703405

4. VPC をトランジット Gateway にアタッチすると、リソースタイプ **VPC** がトランジットゲートウェイに関連付けられていることがわかります。

Name	Transit Gateway attachment ID	Transit Gateway ID	Resource type	Resource ID	State	Associated route table ID	Association state
VPC102188	tgn-attch-0c1c3a6294cc2d95	tgn-attch-0c1c3a6294cc2d95	VPC	vpc-05b0c147aaf000405	available	tgn-rb-0d02307c10a42e4d5	associated

5. VPN を使用して SD-WAN をトランジットゲートウェイに接続するには、ドロップダウンリストから トランジットゲートウェイ ID を選択し、[**Attachment type**] を **VPN** として選択します。正しいトランジットゲートウェイ ID を選択していることを確認します。

SD-WAN リンクのパブリック IP アドレスと BGP ASN 番号を指定して、新しい VPN カスタマーゲートウェイを接続します。[添付ファイルの作成] をクリックして、VPN をトランジットゲートウェイにアタッチします。

Transit Gateway ID: tgn-attch-0c1c3a6294cc2d95

Attachment type: VPN

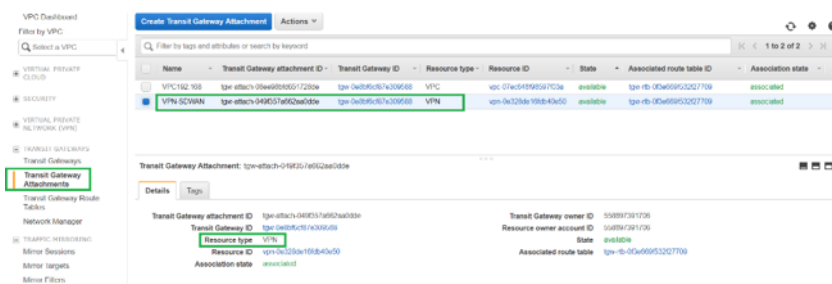
VPN Attachment

Customer Gateway: New

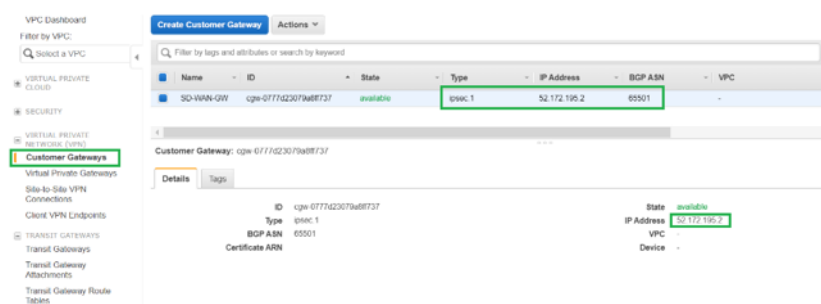
BGP ASN: 64511

Routing options: Enable BGP: On

6. 次のスクリーンショットに示すように、VPN は、トランジットゲートウェイに接続したら、あなたは詳細を表示することができます。

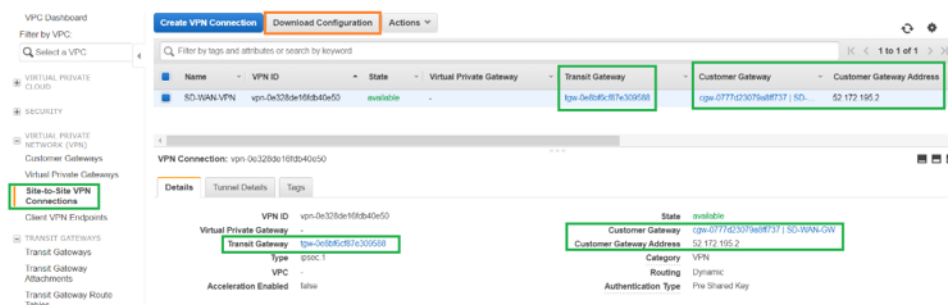


7. [カスタマーゲートウェイ]で、SD-WAN カスタマーゲートウェイとサイト間VPN 接続は、トランジットゲートウェイへのVPN 添付ファイルの一部として作成されます。SD-WAN カスタマーゲートウェイが、SD-WAN のWAN リンクパブリック IP アドレスを表すこのカスタマーゲートウェイの IP アドレスとともに作成されていることがわかります。

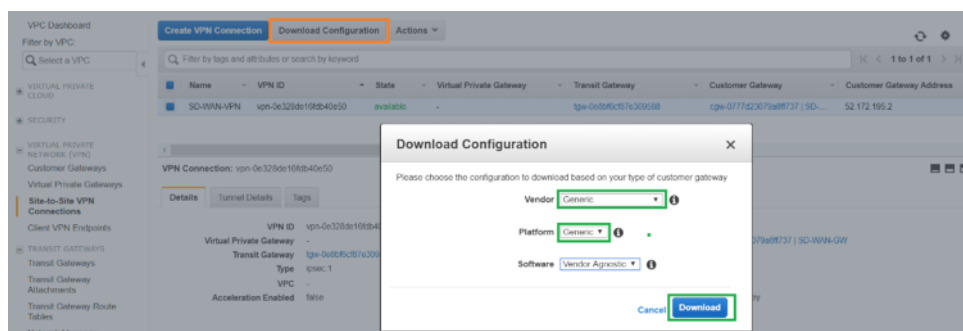


8. サイト間VPN 接続に移動し、**SD-WAN** カスタマーゲートウェイ **VPN** 設定をダウンロードします。この構成ファイルには、BGP ピア情報とともに 2 つの IPsec トンネル詳細があります。冗長性のために、SD-WAN からトランジットゲートウェイへの 2 つのトンネルが作成されます。

SD-WAN リンクのパブリック IP アドレスがカスタマーゲートウェイアドレスとして設定されていることがわかります。



9. [設定のダウンロード]をクリックし、VPN 構成ファイルをダウンロードします。[** ベンダー]、[プラットフォーム]、[ベンダーに依存しないソフトウェア]を選択します。**



ダウンロードした構成ファイルには、次の情報が含まれています。

- IKE 設定
- AWS トランジットゲートウェイの IPsec 設定
- トンネルインターフェイス構成
- BGP 構成

この情報は、高可用性（HA）用の 2 つの IPsec トンネルで使用できます。SD-WAN で設定する場合は、両方のトンネルエンドポイントを設定してください。参考のために次のスクリーンショットを参照してください。

#3: Tunnel Interface Configuration

Your Customer Gateway must be configured with a tunnel interface that is associated with the IPsec tunnel. All traffic transmitted to the tunnel interface is encrypted and transmitted to the Virtual Private Gateway.

The Customer Gateway and Virtual Private Gateway each have two addresses that relate to this IPsec tunnel. Each contains an outside address, upon which encrypted traffic is exchanged. Each also contain an inside address associated with the tunnel interface.

The Customer Gateway outside IP address was provided when the Customer Gateway was created. Changing the IP address requires the creation of a new Customer Gateway.

The Customer Gateway inside IP address should be configured on your tunnel interface.

Outside IP Addresses:

- Customer Gateway	: 52.172.195.2
- Virtual Private Gateway	: 3.133.37.22

Inside IP Addresses

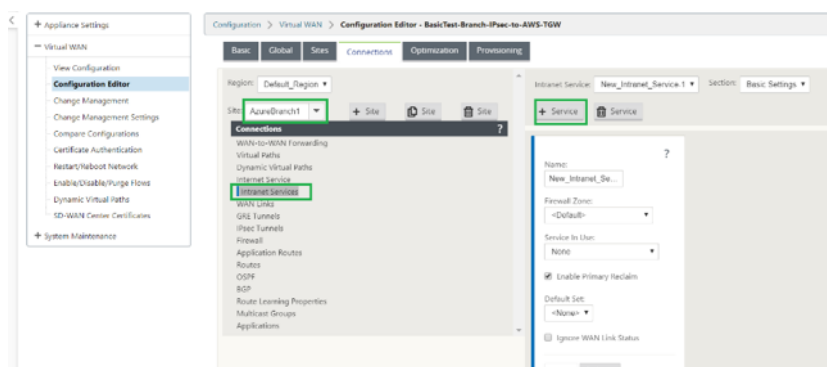
- Customer Gateway	: 169.254.216.178/30
- Virtual Private Gateway	: 169.254.216.177/30

Configure your tunnel to fragment at the optimal size:

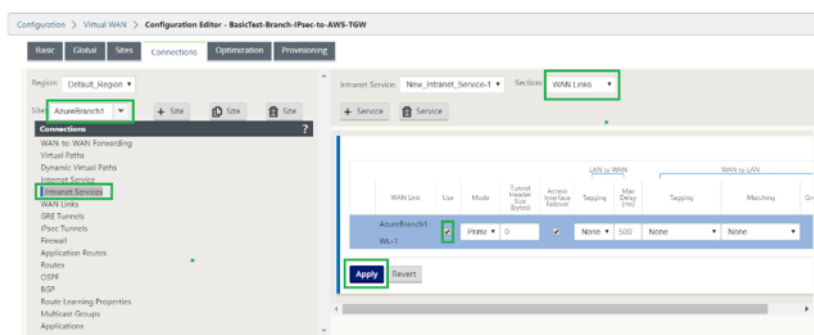
- Tunnel interface MTU	: 1436 bytes
------------------------	--------------

SD-WAN でイントラネットサービスを構成する

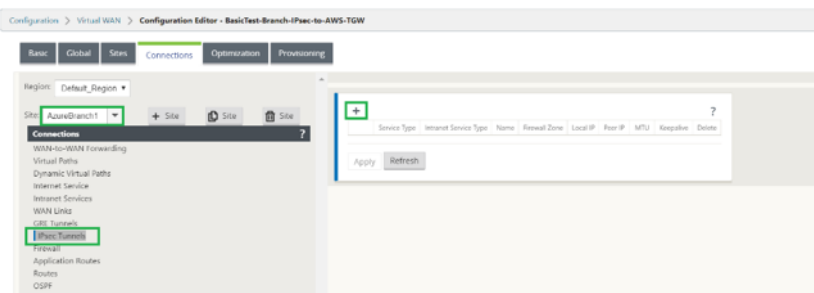
1. SD-WAN の IPsec トンネル構成で使用するイントラネットサービスを構成するには、[構成エディタ]> [接続] の順に選択し、ドロップダウンリストからサイトを選択し、[イントラネットサービス] を選択します。[+ サービス] をクリックして、新しいイントラネットサービスを追加します。



2. イン트라ネットサービスの追加後、このサービスに使用される WAN リンクを選択します (これを使用して、トランジットゲートウェイへのトンネルを確立します)。

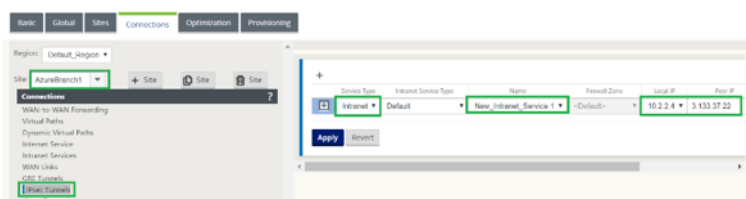


3. AWS Transit Gateway への IPsec トンネルを設定するには、[設定エディタ] > [接続] に移動し、ドロップダウンリストから [サイト] を選択し、[IPsec Tunnels] をクリックします。IPSec トンネルを追加するには、[+] オプションをクリックします。



4. [サービスタイプ] を [イン트라ネット] として選択し、追加した [イン트라ネットサービス名] を選択します。[ローカル IP アドレス] を [WAN リンク IP アドレス] として、[ピア アドレス] を [トランジットゲートウェイ仮想プライベートゲートウェイ IP アドレス] として選択します。

設定のアクティブ化後すぐに SD-WAN によってトンネルが開始されるようにするには、[**Keepalive**] チェックボックスをオンにします。



5. AWS からダウンロードした VPN 設定ファイルに基づいて IKE パラメータを設定します。

Service Type	Intranet Service Type	Name	Firewall Zone	Local IP	Peer IP
Intranet	Default	New_Intranet_Service-1	<Default>	10.2.2.4	3.133.37.22

IKE Settings

Version: IKEv1 Mode: Main

Identity: Auto Authentication: Pre-Shared Key Pre-Shared Key: [Redacted]

☒ Validate Peer Identity Peer Identity: Auto

DH Group: Group 2 (MODP1024) Hash Algorithm: SHA1 Encryption Mode: AES 128-Bit

Lifetime (s): 3600 Lifetime (s) Max: 86400 DPD Timeout (s): 300

6. AWS からダウンロードした VPN 設定ファイルに基づいて IPSec パラメータを設定します。また、トンネルを介して送信する ネットワークに基づいて、**IPsec** 保護された ネットワークを構成します。IPsec トンネル経由のトラフィックを許可するように構成されていることがわかります。

IPsec Settings

Tunnel Type: ESP+Auth PFS Group: Group 2 (MODP1024)

Encryption Mode: AES 128-Bit Hash Algorithm: SHA1

Lifetime (s): 28800 Lifetime (s) Max: 86400

Lifetime (KB): 0 Lifetime (KB) Max: 0

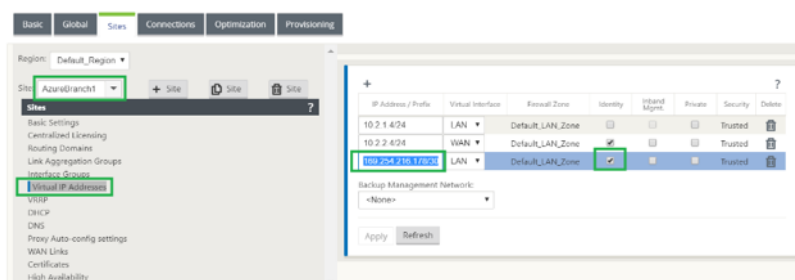
Network Mismatch Behavior: Drop

IPsec Protected Networks + Add

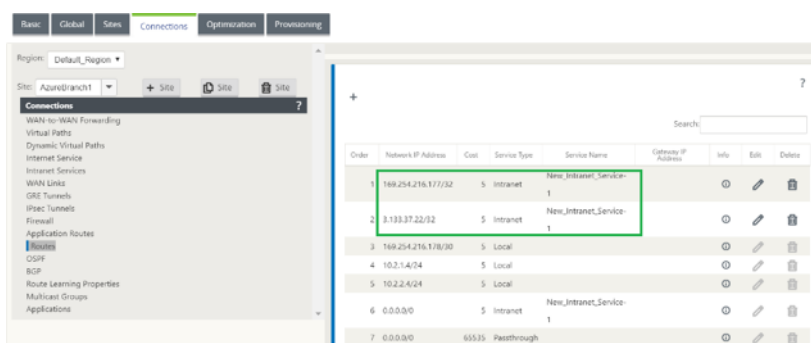
Source IP/Prefix	Destination IP/Prefix
0.0.0.0/0	0.0.0.0/0

Apply Revert

7. カスタマーゲートウェイの内部 **IP** アドレスを SD-WAN 上の仮想 IP アドレスの 1 つとして設定します。ダウンロードされた VPN 設定ファイルから、Tunnel-1 に関連する IP アドレス内のカスタマー Gateway を見つけます。このカスタマー Gateway の IP アドレスを SD-WAN 上の仮想 IP アドレスのいずれかとして設定し、[ID] チェックボックスをオンにします。

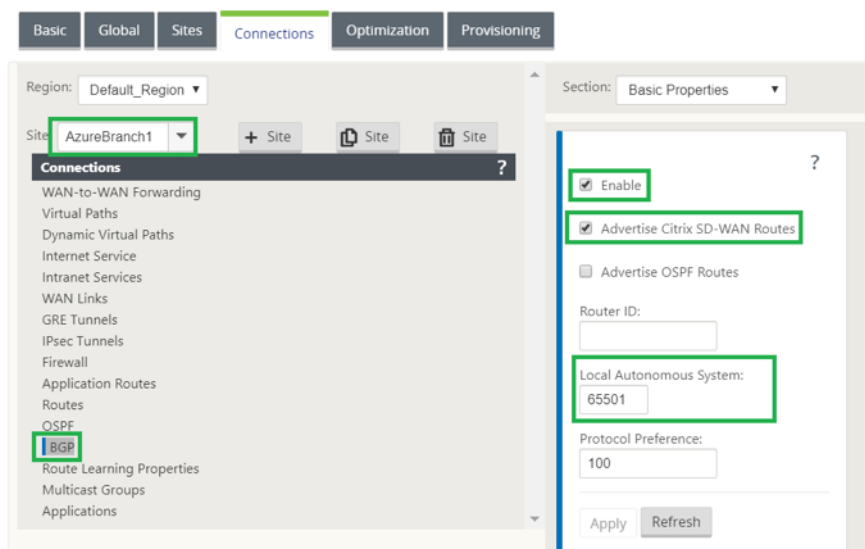


8. SD-WAN に ルート を追加して、トランジット ゲートウェイの仮想プライベート ゲートウェイに到達します。ダウンロードされた VPN 設定ファイルから、Tunnel-1 に関連する仮想プライベートゲートウェイの内側および外部 IP アドレスを検索します。サービスタイプをイントラネットとして仮想プライベートゲートウェイの内部と外部の IP アドレスにルートを追加し、上記の手順で作成したイントラネットサービスを選択します。



9. SD-WAN で **BGP** を設定します。適切な ASN 番号で BGP を有効にします。ダウンロードした VPN 構成ファイルから、Tunnel-1 に関連する BGP 構成オプションを探します。これらの詳細を使用して、SD-WAN に BGP ネイバーを追加します。

SD-WAN で BGP を有効にするには、[接続] に移動して、ドロップダウンリストからサイトを選択し、[**BGP**] を選択します。BGP を有効にするには、[Enable] チェックボックスをオンにします。[**Citrix SD-WAN ルートのアド バタイズ**] チェックボックスをクリックして、SD-WAN ルートをトランジットゲートウェイにアドバタイズします。BGP 設定オプションから カスタマーゲートウェイ **ASN** を使用し、ローカル自律システムとして設定します。

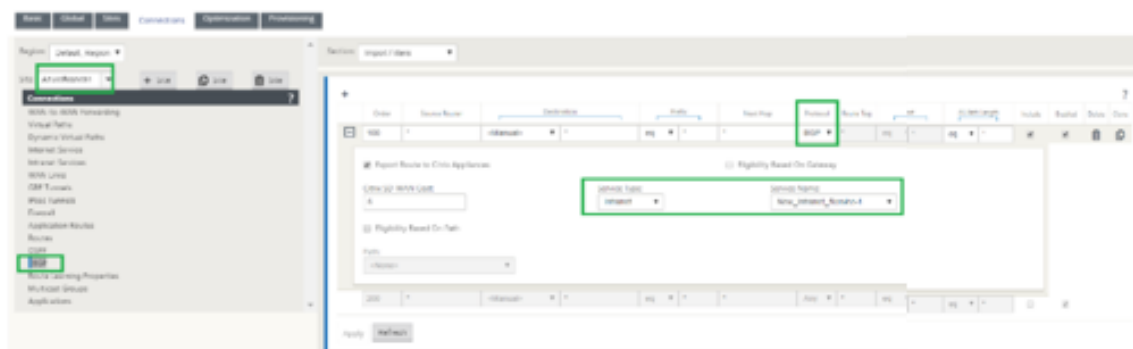


10. SD-WAN に BGP ネイバー を追加するには、[接続] に移動して、ドロップダウンリストからサイトを選択し、[**BGP**] を選択します。[ネイバー] セクションをクリックし、[+] オプションをクリックします。

ネイバーを追加するときに、**BGP** 設定オプションからネイバー **IP** アドレス と 仮想プライベートゲートウェイ **ASN** を使用します。送信元 **IP** は、AWS からダウンロードした設定ファイルの カスタマーゲートウェイ 内部 IP アドレス（SD-WAN で仮想 IP アドレスとして設定）と一致する必要があります。SD-WAN で マルチホップ が有効になっている BGP ネイバーを追加します。



11. インポートフィルタを追加して BGP ルートを SD-WAN にインポートするには、[接続] に移動し、ドロップダウンリストからサイトを選択し、[**BGP**] を選択して [**Import Filters**] セクションをクリックします。[+] オプションをクリックして、[インポート] フィルタを追加します。[**Protocol**] を [**BGP**] として選択し、[any] に一致させ、すべての BGP ルートをインポートします。[サービスタイプ] を [イン트라ネット] として選択し、作成したイン트라ネットサービスを選択します。これは、サービスタイプの BGP ルートをイン트라ネットとしてインポートするためです。



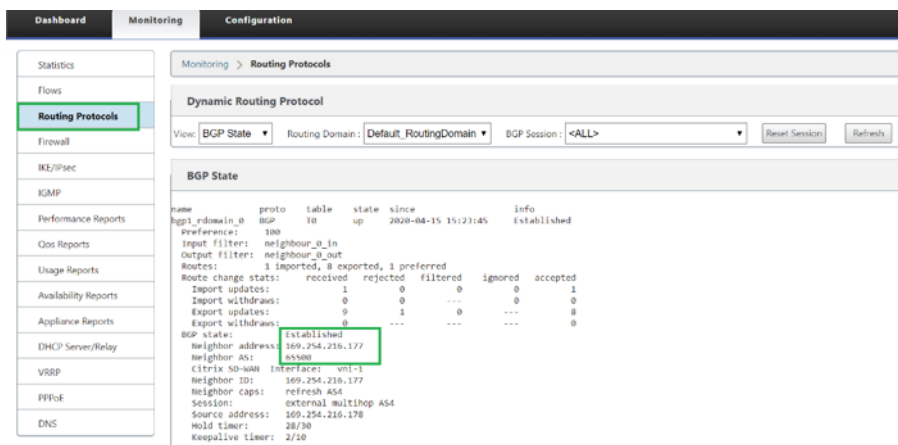
SD-WAN でのモニタリングとトラブルシューティング

1. SD-WAN で IPsec トンネル確立ステータスを確認するには、[モニタリング] > [統計情報] > [IPsec トンネル] に移動します。次のスクリーンショットでは、IPsec トンネルが SD-WAN から AWS Transit Gateway に向けて確立され、状態が **GOOD** であることがわかります。

また、この IPsec トンネルを介して送受信されるトラフィックの量を監視することもできます。

![SD-WANでの監視とトラブルシューティング] (/en-us/citrix-sd-wan/current-release/media/monitoring-and-troubleshooting-on-sdwan.png)

2. SD-WAN の **BGP** ピアリングステータスを確認するには、[モニタリング] > [ルーティングプロトコル] に移動し、[BGP ステート] を選択します。BGP 状態が [確立済み] として報告され、ネイバー **IP** アドレスとネイバー **ASN** が AWS BGP ネイバーの詳細と一致していることがわかります。これにより、IPsec トンネルを介して SD-WAN から AWS トランジットゲートウェイへの BGP ピアリングが確立されたことを確認できます。



VPC (192.168.0.0) が AWS トランジットゲートウェイにアタッチされています。SD-WAN は、この VPC ネットワーク (192.168.0.0) を AWS Transit Gateway から BGP 経由で学習しました。このルートは、上記の手順で作成したインポートフィルタに従って、サービスタイプがイントラネットで SD-WAN にインストールされました。

3. SD-WAN への BGP ルートのインストールを確認するには、[Monitoring] > [Statistics] > [Routes] の順に選択し、サービスタイプがイントラネットの BGP ルートとしてインストールされたネットワーク

192.168.0.0/16 を確認します。つまり、AWS Transit Gateway にアタッチされたネットワークを学習し、確立された IPsec トンネルを介してこれらのネットワークと通信できます。

Statistics

Rows

Routing Protocols

Firewall

IGMP/Spec

IGMP

Performance Reports

QoS Reports

Usage Reports

Availability Reports

Appliance Reports

DHCP Server/Relay

VRRP

IPSec

DNS

Monitoring > Statistics

Statistics

Show Routes ▾ ☐ Enable Auto Refresh 5 seconds Refresh ☒ Clear Counters on Refresh

Route Statistics

Maximum allowed routes: 40000

Routes for routing domain : Default_RoutingDomain

Filter: in Any column ▾

Show 100 ▾ entries Showing 1 to 11 of 11 entries

Details	Num	Network Addr	Gateway IP Address	Service	Firewall Zone	Reachable	Site IP Address	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible
0	1	169.254.216.177/32	*	New_Intranet_Service-1	Default_LAN_Zone	YES	*	AzureBranch1	Static	-	-	5	7	YES
1	3	3.133.37.22/32	*	New_Intranet_Service-1	Default_LAN_Zone	YES	*	AzureBranch1	Static	-	-	5	11	YES
2	2	169.254.216.176/30	*	Local	Default_LAN_Zone	YES	*	AzureBranch1	Static	-	-	5	0	YES
3	3	10.2.1.0/24	*	Local	Default_LAN_Zone	YES	*	AzureBranch1	Static	-	-	5	0	YES
4	4	10.2.2.0/24	*	Local	Default_LAN_Zone	YES	*	AzureBranch1	Static	-	-	5	0	YES
5	5	10.1.2.0/24	*	DCMCH-AzureBranch1	Default_LAN_Zone	YES	*	DCMCH	Dynamic	Virtual WAN	YES	10	0	YES
6	6	10.1.1.0/24	*	DCMCH-AzureBranch1	Default_LAN_Zone	YES	*	DCMCH	Dynamic	Virtual WAN	YES	10	0	YES
7	7	192.168.0.0/16	*	New_Intranet_Service-1	Default_LAN_Zone	YES	*	AzureBranch1	Dynamic	BGP	-	6	0	YES
8	8	0.0.0.0/0	*	New_Intranet_Service-1	Default_LAN_Zone	YES	*	AzureBranch1	Static	-	-	5	0	YES

AWS でのモニタリングおよびトラブルシューティング

1. AWS で IPsec トンネルの確立ステータスを確認するには、仮想プライベートネットワーク (VPN) > サイト間 VPN 接続に移動します。次のスクリーンショットでは、カスタマーゲートウェイアドレスは、あなたがトンネルを確立している使用して SD-WAN リンクのパブリック IP アドレスを表していることを確認することができます。

トンネルのステータスは **UP** と表示されます。また、AWS が SD-WAN から **8** つの **BGP** ルートを学習していることも観察できます。つまり、SD-WAN は AWS Transit Gateway を使用してトンネルを確立でき、BGP 経由でルートを交換することもできます。

VPC Dashboard

Filter by VPC: Select a VPC

Virtual Private Cloud

SECURITY

Virtual Private Networks (VPNs)

Customer Gateways

Virtual Private Gateways

Client VPN Endpoints

TRANSIT GATEWAYS

Traffic Mirroring

Monitor Sessions

Monitor Targets

Monitor Filters

Create VPN Connection Download Configuration Actions

Filter by tags and attributes or search by keyword

Name	VPN ID	Status	Virtual Private Gateway	Transit Gateway	Customer Gateway	Customer Gateway Address
SD-WAN VPN	vgn-0e320ba108b40a50	available	-	tgw-0e6b0c167a309688	cgw-077d3c79a8f737 / SD...	52.172.165.2

VPN Connection: vgn-0e320ba108b40a50

Details Tunnel Details Tags

Tunnel State

Tunnel Number	Outside IP Address	Inside IP CIDR	Status	Status Last Changed	Details	Certificate ARN
Tunnel 1	3.133.37.22	169.254.216.176/30	UP	April 15, 2020 at 8:54:05 PM UTC+9:30	8 BGP-ROUTERS	-
Tunnel 2	13.58.06.154	169.254.133.249/30	DOWN	April 15, 2020 at 12:03:46 PM UTC+	IPSEC IS DOWN	-

2. SD-WAN にダウンロードした構成ファイルに基づいて、2 番目のトンネルに関連する IPsec および BGP の詳細を設定します。

SD-WAN では、次のように、両方のトンネルに関連するステータスを監視できます。

Monitoring > Statistics

Statistics

Show: IPsec Tunnel (Enable Auto Refresh: 5 seconds) Refresh Show latest data.

IPsec Tunnel Statistics

Filter: Any column Apply

Show: 100 entries Showing 1 to 2 of 2 entries

Name	State	Service Type	Packets Received	Kbps Received	Packets Sent	Kbps Sent	Packets Dropped	Bytes Dropped	MTU
New Intranet Service-1	GOOD	Intranet	1	0.27	1	0.24	0	0	1434
New Intranet Service-2	GOOD	Intranet	1	0.27	1	0.24	0	0	1434

Showing 1 to 2 of 2 entries

3. 両方のトンネルに関連するステータスは、AWS で次のように監視できます。

VPN Connections

Name	VPN ID	State	Virtual Private Gateway	Transit Gateway	Customer Gateway	Customer Gateway Address
SD WAN VPN	vpm-0a32bde19db41e50	available	-	tgw-0a8b9f857e309588	cgw-0777423079a88737 SD...	52.172.165.2

VPN Connection: vpm-0a32bde19db41e50

Tunnel State

Tunnel Number	Outside IP Address	Inside IP CIDR	Status	Status Last Changed	Details	Certificate ARN
Tunnel 1	3.133.37.27	100.254.210.170/30	UP	April 16, 2020 at 11:58:30 AM UTC+5	11 RGP ROUTES	
Tunnel 2	13.58.96.104	100.254.133.240/30	UP	April 16, 2020 at 11:57:30 AM UTC+5	11 RGP ROUTES	

仮想パスおよびダイナミックパスの IPsec トンネルを構成する方法

May 10, 2021

Citrix SD-WAN ブランチサイト間の仮想パスおよび動的仮想パスの IPsec トンネルを構成するには:

1. [グローバル] > [仮想パスのデフォルトセット] または [動的仮想パスのデフォルトセット] に移動します。

Global

Virtual Path Default Set: Scale_VP_default_set Section: Default Set Name + Add Default Set - Delete Default Set

Default Set Name: Scale_VP_defau...

The name for this Virtual Path Default Set

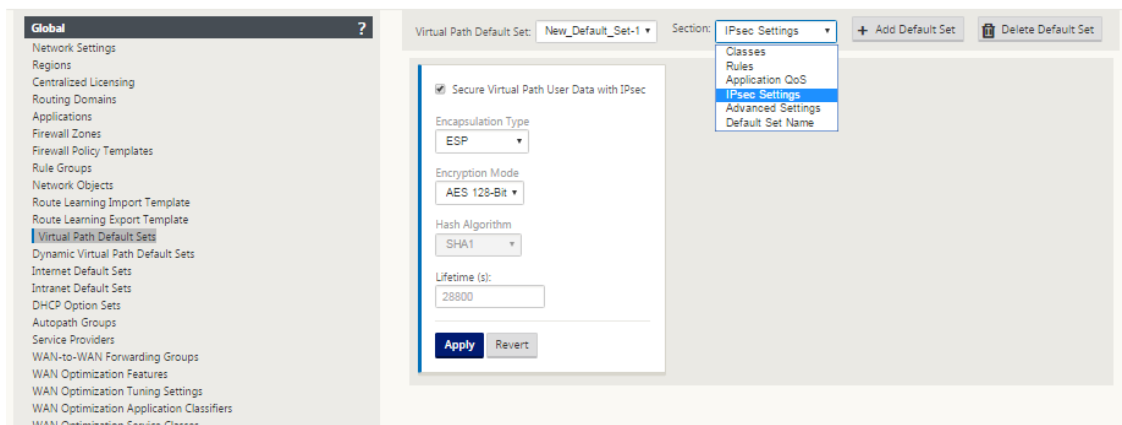
Apply Refresh

2. 新しいデフォルトセット（仮想または動的仮想パス）を作成し、IPsec を使用してセキュア仮想パスユーザーデータを有効にします。

3. IPsec 暗号化に使用できるオプションの 1 つを選択します。

- カプセル化タイプ:ESP、AH、または ESP+AH
- 暗号化モード:AES-CBC、AES 128、または 256 ビット
- ハッシュアルゴリズム: SHA1 または SHA-256

4. 作成した仮想パスのデフォルトセットを MCN ノードに適用します。これにより、MCN への仮想パスを持つすべてのクライアント・ノードに、同じデフォルト・セットが自動的に適用されます。

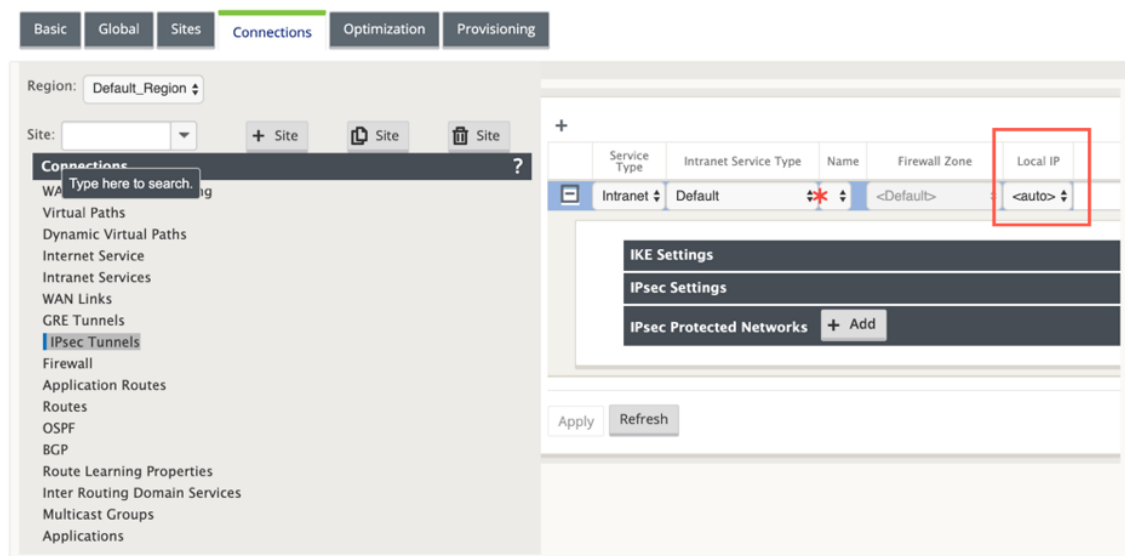


SD-WAN とサードパーティデバイス間の IPsec トンネルを構成する方法

November 8, 2021

イントラネットまたは LAN サービスの IPsec トンネルを構成するには、次の手順を実行します。

1. 構成エディタで、[接続] > [サイトの表示] > [**[サイト名]**] > [IPsec トンネル] に移動します。サービスタイプ (LAN またはイントラネット) を選択します。
2. サービスタイプの [名前] を入力します。イントラネットサービスの種類では、構成されたイントラネットサーバーによって、使用できるローカル IP アドレスが決まります。



アプライアンス上で WAN リンクが直接終端され、動的 IP が WAN リンクに割り当てられるときに、Citrix SD-WAN が IPsec トンネルを確立できるようになりました。

11.1.0 リリースでは、イントラネット IPsec トンネルは、ローカルトンネル IP アドレスが不明、または認識できない場合に構成する必要があります。これにより、DHCP を介してアドレスが割り当てられているインターフェイスに IPsec トンネルを作成できます。

IPsec トンネルのインターフェイスを設定するときに、ローカルトンネル IP を指定する必要があります。このインターフェイスは、トンネルタイプがイントラネットの場合、空の IP を選択できるように変更されています。

また、トンネルの種類が [イントラネット] の場合、未設定のアドレスのラベルは [自動] に変更されます。

ローカル IP が **Auto** に設定されている場合、その WAN リンク上のアクセスインターフェイスに組み込まれた IP アドレスを取得できます。この WAN リンクアクセスインターフェイスは、スタティックに設定された IP または DHCP から IP を取得する可能性があります。IPsec トンネルは、デフォルトでプライマリ WAN リンクアクセスインターフェイスを使用して確立されます。

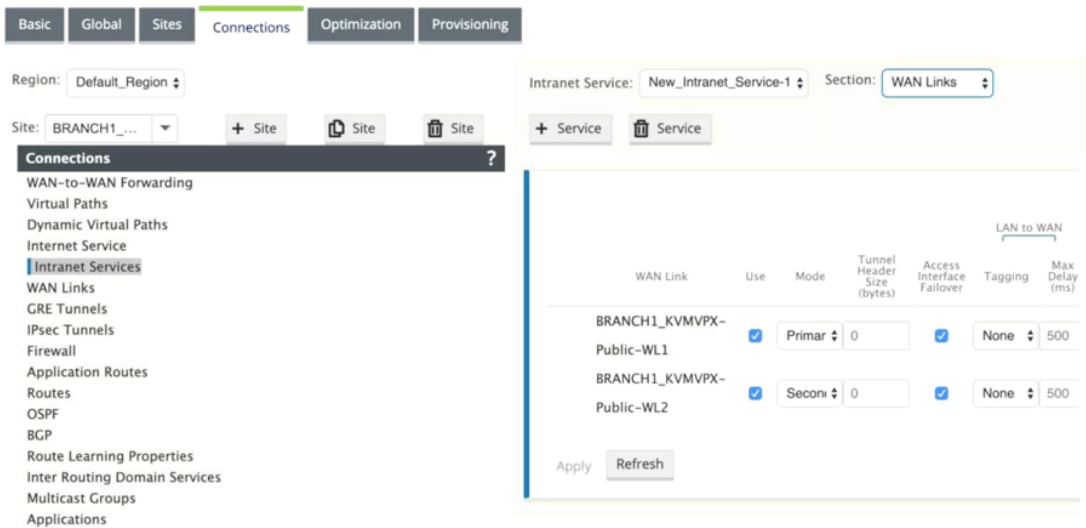
以前は、単一の WAN リンク上で IPsec トンネルを確立できます。これにより、リンク障害の発生時や、リンクのパケット損失が誤って高くなると、信頼性の高い接続が可能になるように、ブランチ環境がサービス損失にさらされます。

11.1.0 リリース以降では、2 つの WAN リンクを使用して IPsec トンネルを確立し、サービス中断期間からブランチ環境を保護できます。プライマリリンクがダウンすると、セカンダリリンクはミリ秒以内にアクティブ/アップになります。

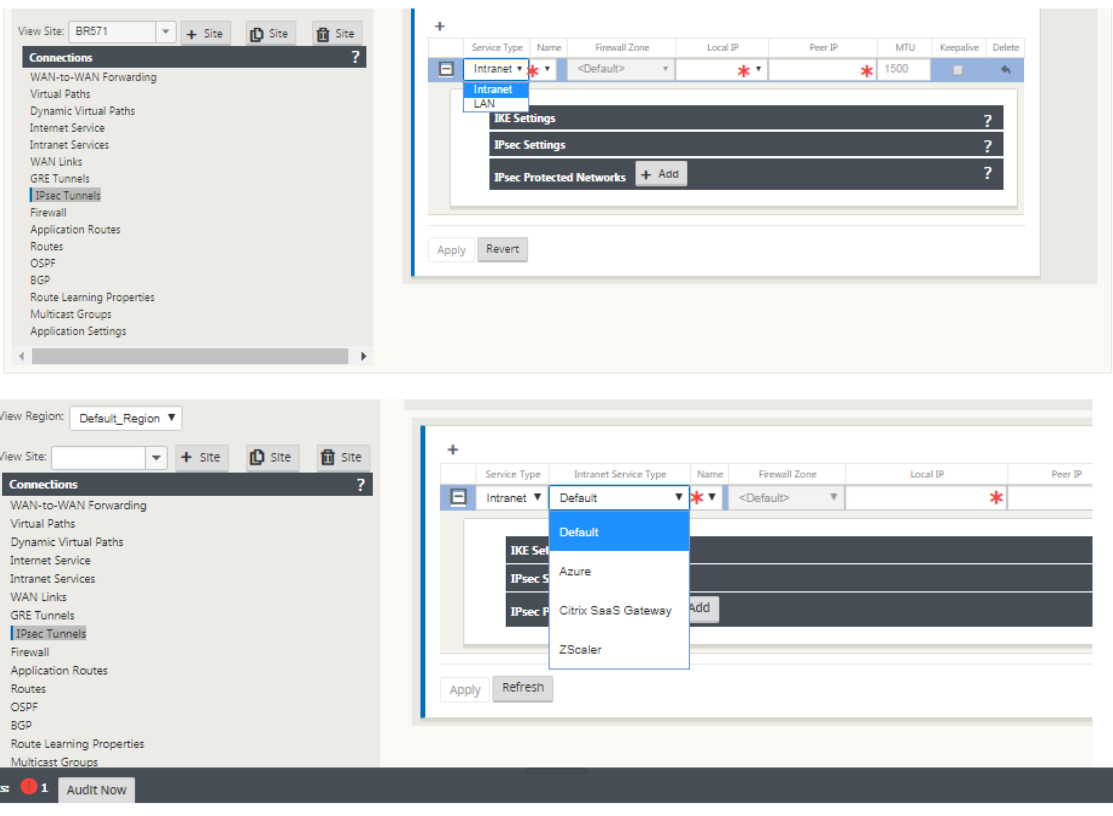
注

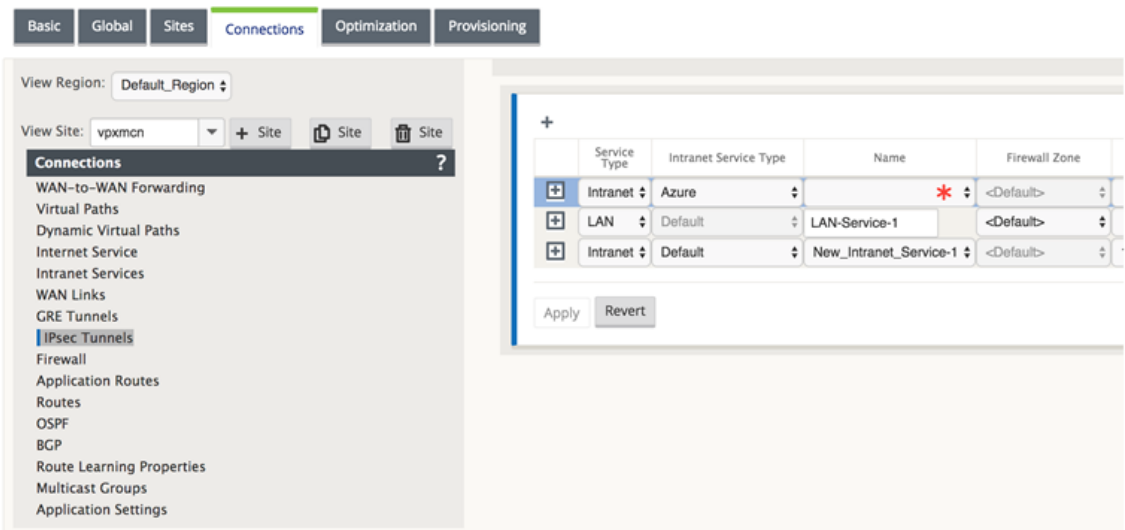
[<Auto>] オプションを選択すると、プライマリ WAN リンクアクセスインターフェイスを使用して

IPSec トンネルが確立されます。プライマリ WAN リンクがダウンすると、セカンダリ WAN リンクアクセスインターフェイスを使用して IPSec トンネルが確立されます。



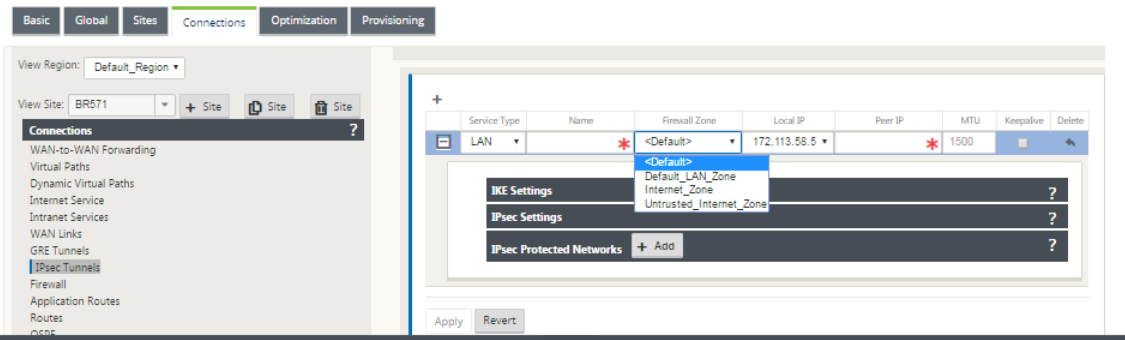
3. 使用可能なローカル IP アドレスを選択し、IPsec トンネルのピア IP アドレスを入力します。





注

[サービスタイプ] が [イントラネット] の場合、IP アドレスは選択したイントラネットサービスによって事前に決定されます。



4. 次の表に示す条件を適用して、IPSec 設定を構成します。終了したら、[適用] をクリックして設定を保存します。

フィールド	説明	値
サービスの種類	ドロップダウンメニューからサービスタイプを選択します。	イントラネット、LAN
名前	サービスの種類が [イントラネット] の場合は、ドロップダウンメニューで構成されたイントラネットサービスのリストから選択します。サービスタイプが LAN の場合は、一意の名前を入力します。	テキスト文字列

フィールド	説明	値
ローカル IP	このサイトで構成されている使用可能な仮想 IP アドレスのドロップダウンメニューから、IPsec トンネルのローカル IP アドレスを選択します。	IP アドレス
ピア IP	IPsec トンネルのピア IP アドレスを入力します。	IP アドレス
MTU	IKE フラグメントと IPsec フラグメントをフラグメント化するための MTU を入力します。	デフォルト:1500
IKE 設定	バージョン: ドロップダウンメニューから IKE バージョンを選択します。	IKEv1 IKEv2
Mode	ドロップダウンメニューからモードを選択します	FIPS 準拠: メイン、非 FIPS 準拠: アグレッシブ
ID	ドロップダウンメニューから ID を選択します	自動 IP アドレス手動 IP アドレスユーザ FQDN
認証	ドロップダウンメニューから認証タイプを選択します	事前共有キー: 事前共有キーを使用している場合は、このフィールドにコピーして貼り付けます。眼球 () アイコンをクリックして、事前共有キーを表示します。証明書:ID 証明書を使用している場合は、ドロップダウンメニューから選択します。
ピア ID の検証	IKE のピアを検証するには、このチェックボックスをオンにします。ピアの ID タイプがサポートされていない場合は、この機能を有効にしないでください。	なし
DH グループ	ドロップダウンメニューから、IKE キー生成に使用する Diffie-Hellman グループを選択します。	非 FIPS 準拠: グループ 1、FIPS 準拠: グループ 2 グループ 5 グループ 14 グループ 15 グループ 16 グループ 19 グループ 20 グループ 21
ハッシュアルゴリズム	ドロップダウンメニューからアルゴリズムを選択して、IKE メッセージを認証します。	非 FIPS 準拠:MD5 FIPS 準拠:SHA1 SHA-256
暗号化モード	ドロップダウンメニューから IKE メッセージの暗号化モードを選択します。	AES 128 ビット AES 192 ビット AES 256 ビット

フィールド	説明	値
ライフタイム	IKE セキュリティアソシエーションが存在するための優先期間を秒単位で入力します。	3600 秒（デフォルト）
最大寿命	IKE セキュリティアソシエーションの存在を許可する最大優先時間を秒単位で入力します。	86400 秒（デフォルト）
DPD タイムアウト	VPN 接続のデッドピア検出タイムアウトを秒単位で入力します。	300 秒（デフォルト）
IKEv2	ピア認証: ドロップダウンメニューから [ピア認証] を選択します。	ミラー化された事前共有キー証明書
IKE2-事前共有キー	ピア事前共有キー: 認証のために、IKEv2 ピア事前共有キーをこのフィールドに貼り付けます。眼球 () アイコンをクリックして、事前共有キーを表示します	テキスト文字列
整合性アルゴリズム	ドロップダウンメニューから、HMAC 検証に使用するハッシュアルゴリズムとしてアルゴリズムを選択します	非 FIPS 準拠:MD5 FIPS 準拠:SHA1 SHA-256

注:

終端側の IPsec ルータの設定にハッシュベースメッセージ認証コード (HMAC) が含まれている場合は、**SHA1** としてハッシュアルゴリズムを使用して IPsec モードを **EXP+Auth** に変更します。

IKE Settings?

Version:
IKEv1

Mode:
Aggressive

Identity:
Auto

Authentication:
Pre-Shared Key

Pre-Shared Key:

☒ Validate Peer Identity

Peer Identity:
Auto

DH Group:
Group 1 (MODP768)

Hash Algorithm:
MD5

Encryption Mode:
AES 128-Bit

Lifetime (s):
3600

Lifetime (s) Max:
86400

DPD Timeout (s):
300

IPsec Settings?

IPsec Protected Networks + Add?

IKE Settings?

Version:
IKEv2

Identity:
Auto

Authentication:
Pre-Shared Key

Pre-Shared Key:

Peer Authentication:
Mirrored

☒ Validate Peer Identity

Peer Identity:
Auto

DH Group:
Group 1 (MODP768)

Hash Algorithm:
MD5

Integrity Algorithm:
MD5

Encryption Mode:
AES 128-Bit

Lifetime (s):
3600

Lifetime (s) Max:
86400

DPD Timeout (s):
300

IPsec Settings?

IPsec Protected Networks + Add?

IPsec および IPsec で保護されたネットワーク設定

フィールド	説明	値
トンネルタイプ	ドロップダウンメニューからトンネルタイプを選択します。	ESP ESP+Auth ESP+NULL AH
PFS グループ	ドロップダウンメニューから [Diffie-Hellman] グループを選択して、完全な前方秘密鍵生成に使用します。	なしグループ 1 グループ 2 グループ 5 グループ 14 グループ 15 グループ 16 グループ 19 グループ 20 グループ 21

フィールド	説明	値
暗号化モード	ドロップダウンメニューから IPsec メッセージの 暗号化モード を選択します。	ESP または ESP+ 認証を選択した場合は、次のいずれかを選択します。 AES 128 ビット、AES 192 ビット、AES 256 ビット、AES 128 ビット GCM 64 ビット、AES 192 ビット GCM 64 ビット、AES 256 ビット GCM 64 ビット、AES 128 ビット GCM 96 ビット、AES 192 ビット GCM 96 ビット、AES 256 ビット GCM 96 ビット、AES 128 ビット GCM 128 ビット、AES 192 ビット GCM 128 ビット、AES 256 ビット GCM 128 ビットか AES 128/192/256 ビットは CBC をサポートしています。
ライフタイム	IPsec セキュリティアソシエーションの存在を許可する時間を秒単位で入力します。	28800 秒（デフォルト）
最大有効期間	IPSec セキュリティアソシエーションの存在を許可する最大時間を秒単位で入力します。	86400 秒（デフォルト）
ライフタイム (KB)	IPsec セキュリティアソシエーションが存在するデータ量をキロバイト単位で入力します。	キロバイト
最大寿命 (KB)	IPSec セキュリティアソシエーションの存在を許可するデータの最大量をキロバイト単位で入力します。	キロバイト
ネットワークの不一致動作	パケットが IPsec トンネルの保護されたネットワークと一致しない場合のアクションをドロップダウンメニューから選択します。	ドロップ、暗号化されていない送信、非 IPsec ルートの使用
IPsec 保護ネットワーク	送信元 IP /プレフィックス:[追加] (+[追加]) ボタンをクリックした後、IPsec トンネルが保護するネットワークトラフィックの [送信元 IP] と [プレフィックス] を入力します。	IP アドレス

フィールド	説明	値
IPSec 保護ネットワーク	宛先 IP /プレフィックス:IPsec トンネルが保護するネットワークトラフィックの宛先 IP とプレフィックスを入力します。	IP アドレス

IPsec Settings

Tunnel Type:

ESP

PFS Group:

<None>

Encryption Mode:

AES 128-Bit

Lifetime (s):

28800

Lifetime (s) Max:

86400

Lifetime (KB):

0

Lifetime (KB) Max:

0

Network Mismatch Behavior:

Drop

IPsec Protected Networks

+ Add

Apply

Revert

注

Citrix SD-WAN は、IPSec を介した Oracle クラウド・インフラストラクチャ（OCI）への接続をサポートしています。

IPsec トンネルの監視

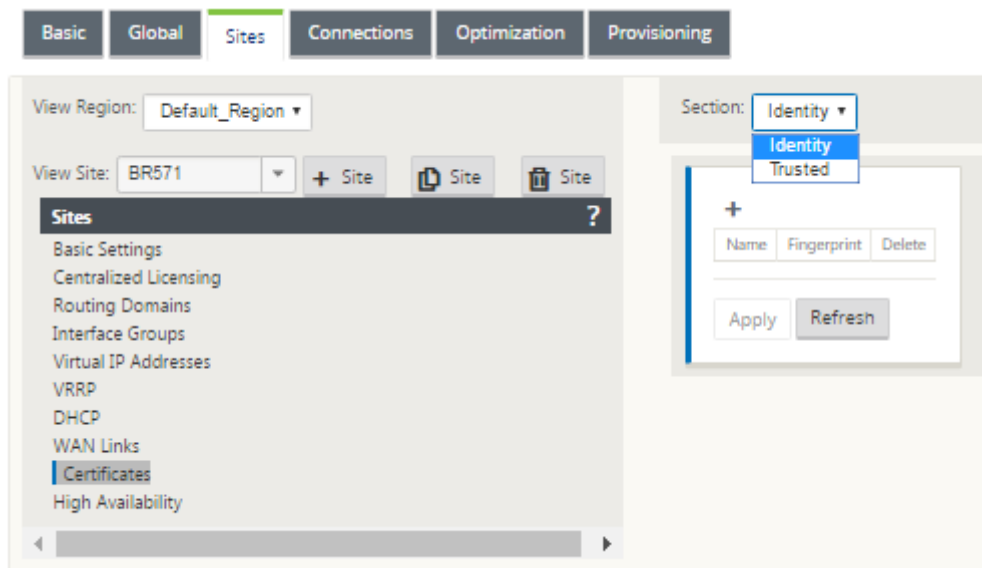
SD-WAN アプライアンスの GUI で「監視」>「IKE/IPSec」に移動し、IPSec トンネル設定を表示および監視します。

IKE 証明書を追加する方法

May 10, 2021

IKE ネゴシエーション用の証明書を実装するには、次の手順を実行します

1. [サイト] > [証明書] に移動し、必要な証明書を追加します。

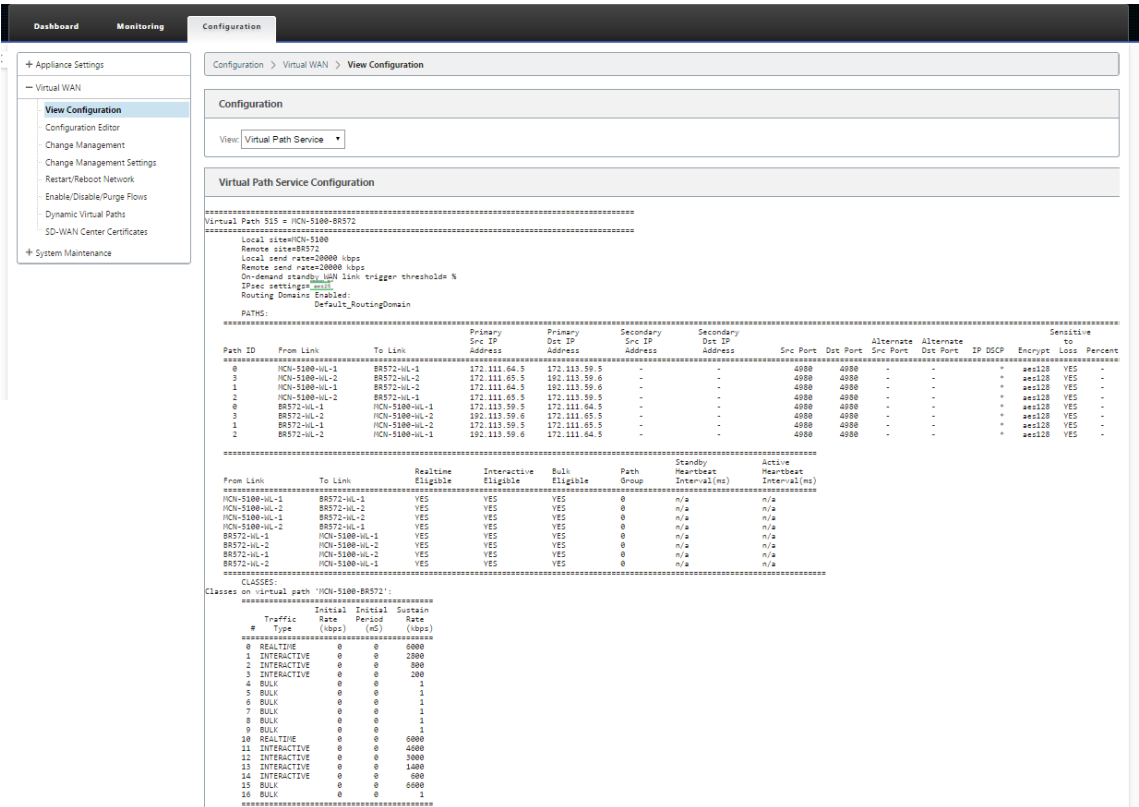


IPsec トンネルの設定を表示する方法

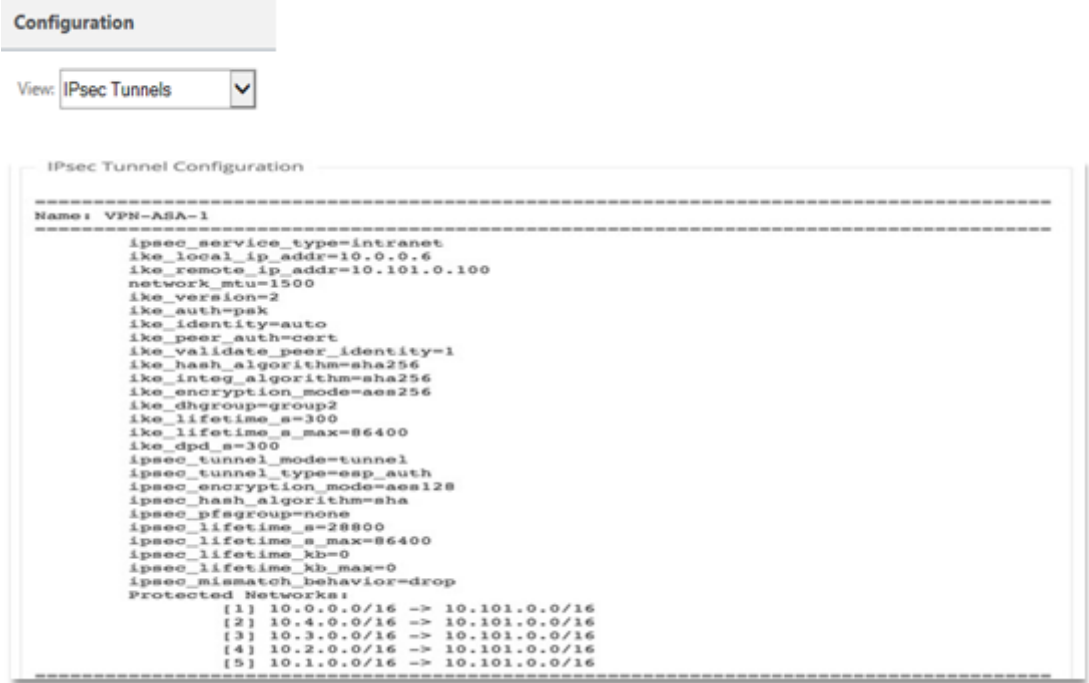
May 10, 2021

ipsec トンネルの設定を表示するには、次の手順を実行します。

1. [構成] > [仮想 WAN] > [構成の表示] に移動します。
2. ドロップダウンメニューから [仮想パスサービス] を選択します。IPsec 設定は、構成エディタで IPsec が有効になっている場合にのみ表示されます。



3. ドロップダウンメニューから [IPsec トンネル] を選択して、IPsec トンネル設定を表示します。



4. 各仮想パスは、次に示すように、独自の IPsec トンネルのステータスを表示します。

Dashboard **Monitoring** **Configuration**

System Status

Name: MCN-5100
 Model: 5100
 Appliance Mode: MCN
 Serial Number: 4H30GCNPD0
 Management IP Address: 10.199.107.201
 Appliance Uptime: 1 weeks, 3 days, 2 hours, 7 minutes, 28.6 seconds
 Service Uptime: 6 hours, 21 minutes, 54.0 seconds
 Routing Domain Enabled: Default_RoutingDomain

Local Versions

Software Version: 10.0.0.193.659091
 Built On: Feb 17 2018 at 17:32:45
 Hardware Version: 5100
 OS Partition Version: 4.6

Virtual Path Service Status

Virtual Path MCN-5100-BR572: Uptime: 5 hours, 59 minutes, 34.0 seconds. IPsec state: GOOD.
 Virtual Path MCN-5100-BR573: Uptime: 5 hours, 45 minutes, 0.0 seconds. IPsec state: GOOD.
 Virtual Path MCN-5100-BR574: Uptime: 4 hours, 56 minutes, 48.0 seconds.
 Virtual Path 'MCN-5100-BR575' is currently dead.
 Virtual Path MCN-5100-RCN1-5100: Uptime: 2 hours, 7 minutes, 3.0 seconds.
 Virtual Path 'MCN-5100-RCN3-2100' is currently dead (Configuration version mismatch)
 Virtual Path 'MCN-5100-RCN3Geo-2100' is currently dead.
 Virtual Path 'MCN-5100-RCN4-ESxIL' is currently dead.

IPsec の監視とログ

May 10, 2021

IPsec トンネルの統計情報を監視するには:

1. [監視] > [統計] に移動します。[Show] ドロップダウンメニューから [IPSec Tunnel] を選択します。

Statistics

Show: IPSec Tunnel Enable Auto Refresh 5 seconds Show latest data.

IPsec Tunnel Statistics

Filter: In Any column Apply

Show 100 entries Showing 1 to 8 of 8 entries

Name	State	Service Type	Packets Received	Kbps Received	Packets Sent	Kbps Sent	Packets Dropped	Bytes Dropped	MTU
AS-TB-NCN-AS-TB-CL-1	GOOD	Conduit	0	0	0	0	0	0	1359
AS-TB-NCN-AS-TB-CL-2	GOOD	Conduit	0	0	0	0	0	0	1359
AS-TB-NCN-AS-TB-CL-3	GOOD	Conduit	0	0	0	0	0	0	1359
AS-TB-NCN-AS-TB-CL-4	GOOD	Conduit	0	0	0	0	0	0	1359
VPN-ASA-1	GOOD	Intranet	0	0	0	0	0	0	1427
VPN-ASA-2	GOOD	LAN	0	0	0	0	0	0	1377
VPN-PaloAlto	GOOD	Intranet	0	0	0	0	0	0	1439
VPN-SonicWall	GOOD	Intranet	0	0	0	0	0	0	1456

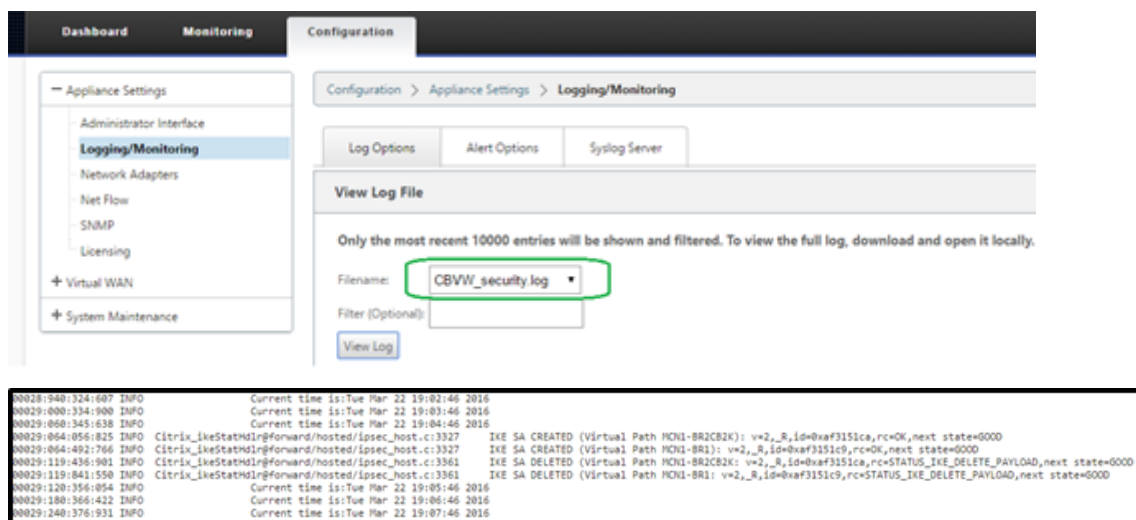
Showing 1 to 8 of 8 entries

2. [モニター] > [IKE/IPSec] に移動します。設定された IPsec トンネル、SD-WAN ネットワーク内に設定された 2 つのエンドポイントまたはモード VPN エンドポイント間の IKE および IPsec サービスアソシエーションを確認します。

ipsec ログを監視する方法

1. 「構成」 > 「アプライアンスの設定」 > 「ログ/監視」に移動します。ドロップダウンメニューから [ファイル名] を選択し、[ログの表示] をクリックします。IPsec トンネルの次のログ詳細を表示できます。

- IPsec トンネルの作成と削除
- IPsec トンネルステータスの変更



IPsec トンネルアラートを表示する方法

1. 「構成」 > 「アプライアンスの設定」 > 「ログ/監視」 > 「アラート・オプション」に移動します。
 2. IPsec トンネルの状態レポート用の電子メールおよび Syslog アラートを作成します。
- IPSEC_TUNNEL をイベントタイプの 1 つとしてサポートし、電子メールおよび Syslog 重大度フィルタを設定できます。

← Appliance Settings

Administrator Interface

Logging/Monitoring

Network Adapters

Net Flow

App Flow

SNMP

NETRO API

Licensing

+ Virtual WAN

+ System Maintenance

Configuration > Appliance Settings > Logging/Monitoring

Log OptionsAlert OptionsAlarm OptionsSyslog Server

Email Alerts

☐ Enable Email Alerts

Send Test Email

Destination Email Address(es):

SMTP Server Hostname or IP Address:

SMTP Server Port:

25

Source Email Address:

You may enter multiple destination email addresses separated with semicolons (;)

☐ Enable SMTP Authentication

SMTP User Name:

SMTP Password:

Verify SMTP Password:

General Event Configuration

Event Type	Alert if State Persists	Email	Email Severity Filter	Syslog	Syslog Severity Filter	SNMP	SNMP Severity Filter
SERVICE	<div>0</div>	<input type="checkbox"/>	<div>Warning</div>	<input type="checkbox"/>	<div>Warning</div>	<input type="checkbox"/>	<div>Warning</div>
VIRTUAL PATH	<div>0</div>	<input type="checkbox"/>	<div>Warning</div>	<input type="checkbox"/>	<div>Warning</div>	<input type="checkbox"/>	<div>Warning</div>
WAN LINK	<div>0</div>	<input type="checkbox"/>	<div>Warning</div>	<input type="checkbox"/>	<div>Warning</div>	<input type="checkbox"/>	<div>Warning</div>
PATH	<div>0</div>	<input type="checkbox"/>	<div>Warning</div>	<input type="checkbox"/>	<div>Warning</div>	<input type="checkbox"/>	<div>Warning</div>
DYNAMIC VIRTUAL PATH	<div>0</div>	<input type="checkbox"/>	<div>Warning</div>	<input type="checkbox"/>	<div>Warning</div>	<input type="checkbox"/>	<div>Warning</div>
WAN_LINK_CONGESTION	<div>0</div>	<input type="checkbox"/>	<div>Warning</div>	<input type="checkbox"/>	<div>Warning</div>	<input type="checkbox"/>	<div>Warning</div>
USAGE_CONGESTION	<div>0</div>	<input type="checkbox"/>	<div>Warning</div>	<input type="checkbox"/>	<div>Warning</div>	<input type="checkbox"/>	<div>Warning</div>
HARD_DISK		<input type="checkbox"/>	<div>Warning</div>	<input type="checkbox"/>	<div>Warning</div>	<input type="checkbox"/>	<div>Warning</div>
APPLIANCE		<input type="checkbox"/>	<div>Warning</div>	<input type="checkbox"/>	<div>Warning</div>	<input type="checkbox"/>	<div>Warning</div>
USER EVENT		<input type="checkbox"/>	<div>Warning</div>	<input type="checkbox"/>	<div>Warning</div>	<input type="checkbox"/>	<div>Warning</div>
CONFIG_UPDATE		<input type="checkbox"/>	<div>Warning</div>	<input type="checkbox"/>	<div>Warning</div>	<input type="checkbox"/>	<div>Warning</div>
SOFTWARE_UPDATE		<input type="checkbox"/>	<div>Warning</div>	<input type="checkbox"/>	<div>Warning</div>	<input type="checkbox"/>	<div>Warning</div>
PROXY_ARP		<input type="checkbox"/>	<div>Warning</div>	<input type="checkbox"/>	<div>Warning</div>	<input type="checkbox"/>	<div>Warning</div>
ETHERNET		<input type="checkbox"/>	<div>Warning</div>	<input type="checkbox"/>	<div>Warning</div>	<input type="checkbox"/>	<div>Warning</div>
WATCHDOG		<input type="checkbox"/>	<div>Warning</div>	<input type="checkbox"/>	<div>Warning</div>	<input type="checkbox"/>	<div>Warning</div>
APPLIANCE_SETTINGS_UPDATE		<input type="checkbox"/>	<div>Warning</div>	<input type="checkbox"/>	<div>Warning</div>	<input type="checkbox"/>	<div>Warning</div>
DISCOVERED_MTU		<input type="checkbox"/>	<div>Warning</div>	<input type="checkbox"/>	<div>Warning</div>	<input type="checkbox"/>	<div>Warning</div>
GRE_TUNNEL		<input type="checkbox"/>	<div>Warning</div>	<input type="checkbox"/>	<div>Warning</div>	<input type="checkbox"/>	<div>Warning</div>
IPSEC_TUNNEL		<input type="checkbox"/>	<div>Warning</div>	<input type="checkbox"/>	<div>Warning</div>	<input type="checkbox"/>	<div>Warning</div>
VIRTUAL_INTERFACE		<input type="checkbox"/>	<div>Warning</div>	<input type="checkbox"/>	<div>Warning</div>	<input type="checkbox"/>	<div>Warning</div>
LICENSE_EVENT		<input type="checkbox"/>	<div>Warning</div>	<input type="checkbox"/>	<div>Warning</div>	<input type="checkbox"/>	<div>Warning</div>

Apply Settings

IPsec トンネルイベントの監視方法

1. [構成]>[システムメンテナンス]>[診断]>[イベント]に移動します。

2. IPSEC_TUNNEL オブジェクトタイプに基づいてイベントを追加します。すべての IPsec 関連イベントのフィルタを作成します。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

754

DashboardMonitoringConfiguration

+ Appliance Settings

+ Virtual WAN

System Maintenance

- Delete Files
- Restart System
- Date/Time Settings
- Local Change Management
- Diagnostics**
- Update Software
- Configuration Reset
- Factory Reset

Configuration > System Maintenance > Diagnostics

PingTraceroutePacket CapturePath BandwidthSystem InfoDiagnostic DataEventsAlarmsDiagnostics Tool

Insert Event

Object Type:USER EVENT

Event type:UNDEFINED

Severity:DEBUG

Add Event

Download Events

There are currently 487678 in the Events database, spanning from event 183612 at 2018-01-18 18:24:55 to event 671289 at 2018-02-17 18:14:15. You can download some or all of them in CSV format. You may wish to limit the amount to download because some common spreadsheet programs limit you to 65,536 rows.

Download events starting from:2018January18182456Download487678 events

Alert Count

Alert Type	Alerts Sent
Emails:	0
syslog Messages:	0
SNMP Traps:	0

View Events

Quantity:25

Filter: Object Type = AnyEvent type = AnySeverity = Any

Reload Events Table

ID	Object ID	Object Name	Object Type	Time	Event Type	Severity	Description
671289	0	MCN-5100-WL-1->BR572-WL-1	PATH	2018-02-17 18:14:15	GOOD	NOTICE	Virtual Path MCN-5100-BR572 Path MCN-5100-WL-1->BR572-WL-1 state has changed from BAD to GOOD because notified by peer.
671288	1	MCN-5100-WL-1->BR572-WL-2	PATH	2018-02-17 18:14:15	GOOD	NOTICE	Virtual Path MCN-5100-BR572 Path MCN-5100-WL-1->BR572-WL-2 state has changed from BAD to GOOD because notified by peer.
671287	0	MCN-5100-WL-1->BR574-WL-1	PATH	2018-02-17 18:14:15	GOOD	NOTICE	Virtual Path MCN-5100-BR574 Path MCN-5100-WL-1->BR574-WL-1 state has changed from BAD to GOOD because notified by peer.
671286	2	MCN-5100-WL-2->BR572-WL-1	PATH	2018-02-17 18:14:14	GOOD	NOTICE	Virtual Path MCN-5100-BR572 Path MCN-5100-WL-2->BR572-WL-1 state has changed from BAD to GOOD because notified by peer.
671285	1	MCN-5100-WL-1->BR572-WL-2	PATH	2018-02-17 18:14:04	BAD	NOTICE	Virtual Path MCN-5100-BR572 Path MCN-5100-WL-1->BR572-WL-2 state has changed from GOOD to BAD because notified by peer.
671284	0	MCN-5100-WL-1->BR572-WL-1	PATH	2018-02-17 18:14:04	BAD	NOTICE	Virtual Path MCN-5100-BR572 Path MCN-5100-WL-1->BR572-WL-1 state has changed from GOOD to BAD because notified by peer.
671283	0	MCN-5100-WL-1->BR574-WL-1	PATH	2018-02-17 18:14:04	BAD	NOTICE	Virtual Path MCN-5100-BR574 Path MCN-5100-WL-1->BR574-WL-1 state has changed from GOOD to BAD because notified by peer.
671282	2	MCN-5100-WL-2->BR572-WL-1	PATH	2018-02-17 18:14:04	BAD	NOTICE	Virtual Path MCN-5100-BR572 Path MCN-5100-WL-2->BR572-WL-1 state has changed from GOOD to BAD because notified by peer.
671281	3	MCN-5100-WL-2->BR573-WL-2	PATH	2018-02-17 18:13:17	GOOD	NOTICE	Virtual Path MCN-5100-BR573 Path MCN-5100-WL-2->BR573-WL-2 state has changed from BAD to GOOD because notified by peer.
671280	1	MCN-5100-WL-1->BR572-WL-2	PATH	2018-02-17 18:13:17	GOOD	NOTICE	Virtual Path MCN-5100-BR572 Path MCN-5100-WL-1->BR572-WL-2 state has changed from BAD to GOOD because notified by peer.
671279	1	MCN-5100-WL-1->BR574-WL-2	PATH	2018-02-17 18:13:17	GOOD	NOTICE	Virtual Path MCN-5100-BR574 Path MCN-5100-WL-1->BR574-WL-2 state has changed from BAD to GOOD because notified by peer.
671278	2	MCN-5100-WL-2->BR574-WL-1	PATH	2018-02-17 18:13:17	GOOD	NOTICE	Virtual Path MCN-5100-BR574 Path MCN-5100-WL-2->BR574-WL-1 state has changed from BAD to GOOD because notified by peer.
671277	2	MCN-5100-WL-2->BR574-WL-1	PATH	2018-02-17 18:13:06	BAD	NOTICE	Virtual Path MCN-5100-BR574 Path MCN-5100-WL-2->BR574-WL-1 state has changed from GOOD to BAD because notified by peer.
671276	1	MCN-5100-WL-1->BR572-WL-2	PATH	2018-02-17 18:13:06	BAD	NOTICE	Virtual Path MCN-5100-BR572 Path MCN-5100-WL-1->BR572-WL-2 state has changed from GOOD to BAD because notified by peer.
671275	3	MCN-5100-WL-2->BR573-WL-2	PATH	2018-02-17 18:13:06	BAD	NOTICE	Virtual Path MCN-5100-BR573 Path MCN-5100-WL-2->BR573-WL-2 state has changed from GOOD to BAD because notified by peer.
671274	1	MCN-5100-WL-1->BR574-WL-2	PATH	2018-02-17 18:13:06	BAD	NOTICE	Virtual Path MCN-5100-BR574 Path MCN-5100-WL-1->BR574-WL-2 state has changed from GOOD to BAD because notified by peer.
671273	3	MCN-5100-WL-2->BR574-WL-2	PATH	2018-02-17 18:06:09	GOOD	NOTICE	Virtual Path MCN-5100-BR574 Path MCN-5100-WL-2->BR574-WL-2 state has changed from BAD to GOOD because notified by peer.
671272	0	MCN-5100-WL-1->BR574-WL-1	PATH	2018-02-17 18:06:09	GOOD	NOTICE	Virtual Path MCN-5100-BR574 Path MCN-5100-WL-1->BR574-WL-1 state has changed from BAD to GOOD because notified by peer.
671271	1	MCN-5100-WL-1->BR572-WL-2	PATH	2018-02-17 18:06:08	GOOD	NOTICE	Virtual Path MCN-5100-BR572 Path MCN-5100-WL-1->BR572-WL-2 state has changed from BAD to GOOD because notified by peer.
671270	1	MCN-5100-WL-1->BR572-WL-2	PATH	2018-02-17 18:05:58	BAD	NOTICE	Virtual Path MCN-5100-BR572 Path MCN-5100-WL-1->BR572-WL-2 state has changed from GOOD to BAD because notified by peer.
671269	0	MCN-5100-WL-1->BR574-WL-1	PATH	2018-02-17 18:05:58	BAD	NOTICE	Virtual Path MCN-5100-BR574 Path MCN-5100-WL-1->BR574-WL-1 state has changed from GOOD to BAD because notified by peer.
671268	3	MCN-5100-WL-2->BR574-WL-2	PATH	2018-02-17 18:05:57	BAD	NOTICE	Virtual Path MCN-5100-BR574 Path MCN-5100-WL-2->BR574-WL-2 state has changed from GOOD to BAD because notified by peer.
671267	1	MCN-5100-WL-1->BR573-WL-2	PATH	2018-02-17 18:05:59	GOOD	NOTICE	Virtual Path MCN-5100-BR573 Path MCN-5100-WL-1->BR573-WL-2 state has changed from BAD to GOOD because notified by peer.
671266	3	MCN-5100-WL-2->BR572-WL-2	PATH	2018-02-17 18:05:09	GOOD	NOTICE	Virtual Path MCN-5100-BR572 Path MCN-5100-WL-2->BR572-WL-2 state has changed from BAD to GOOD because notified by peer.
671265	1	MCN-5100-WL-1->BR573-WL-2	PATH	2018-02-17 18:04:58	BAD	NOTICE	Virtual Path MCN-5100-BR573 Path MCN-5100-WL-1->BR573-WL-2 state has changed from GOOD to BAD because notified by peer.

IPsec 非仮想パスルートの適格性

May 10, 2021

以前のリリースでは、トンネルが使用できなくなった場合でも、IPsec トンネルルートはルートテーブルに残っていました。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

755

Monitoring > Statistics

Statistics

Show: Routes Enable Auto Refresh 5 seconds Refresh Clear Counters on Refresh Purge dynamic routes

Route Statistics

Maximum allowed routes: 16000

Routes for routing domain : Default_RoutingDomain

Filter: in Any column Apply

Show 100 entries Showing 1 to 13 of 13 entries

Num	Network Addr	Gateway IP Address	Service	Firewall Zone	Reachable	Site IP Address	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
0	172.186.120.0/24	172.186.40.1	Local	Default_LAN_Zone	YES	*	DC	Static	-	-	5	11369	YES	N/A	N/A
1	172.186.50.0/24	*	Local	Default_LAN_Zone	YES	*	DC	Static	-	-	5	0	YES	N/A	N/A
2	172.186.40.0/24	*	Local	Default_LAN_Zone	YES	*	DC	Static	-	-	5	11389	YES	N/A	N/A
3	172.186.75.0/24	*	DC-BRANCH2	Default_LAN_Zone	YES	*	BRANCH2	Static	-	-	5	0	YES	N/A	N/A
4	172.186.30.0/24	*	DC-BRANCH1	Default_LAN_Zone	YES	*	BRANCH1	Static	-	-	5	0	YES	N/A	N/A
5	172.186.20.0/24	*	DC-BRANCH1	Default_LAN_Zone	YES	*	BRANCH1	Static	-	-	5	0	YES	N/A	N/A
6	172.186.160.0/24	172.186.40.1	Local	Default_LAN_Zone	YES	*	DC	Dynamic	BGP	-	6	0	YES	N/A	N/A
7	155.155.155.0/24	172.186.40.1	Local	Default_LAN_Zone	YES	*	DC	Dynamic	BGP	-	6	0	YES	N/A	N/A
8	172.186.30.0/24	*	New_Intranet_Service-1	Default_LAN_Zone	YES	*	DC	Static	-	-	15	0	YES	N/A	N/A
9	172.186.20.0/24	*	New_Intranet_Service-1	Default_LAN_Zone	YES	*	DC	Static	-	-	15	0	YES	N/A	N/A
10	16.16.0.0/16	172.186.40.1	Local	Default_LAN_Zone	YES	*	DC	Dynamic	BGP	-	6	0	YES	N/A	N/A
11	0.0.0.0/0	*	Passthrough	Any	YES	*	*	Static	-	-	16	0	YES	N/A	N/A
12	0.0.0.0/0	*	Discard	Any	YES	*	*	Static	-	-	16	0	YES	N/A	N/A

[接続] [サイト名] > [IPsec トンネル] の [キープアライブ] オプションを使用すると、この動作が強化され、IPsec トンネル が使用できなくなったときに IPsec 非仮想パスルートが不適格と見なされるようになりました。キープアライブオプションが有効の場合、SA は自動的に作成されます。トラフィックはトンネル経由で送信されません。

Basic Global Sites Connections Optimization Provisioning

View Region: Default_Region

View Site: BR573 + Site Site

Connections ?

WAN-to-WAN Forwarding

Virtual Paths

Dynamic Virtual Paths

Internet Service

Intranet Services

WAN Links

GRE Tunnels

IPsec Tunnels

Firewall

Application Routes

Routes

OSPF

BGP

Route Learning Properties

Multicast Groups

Application Settings

Audits: 0 Audit Now

+ Service Type Name Firewall Zone Local IP Peer IP MTU Keepalive Delete

Intranet * <Default> * *

1500

Apply Revert

IKE Settings ?

IPsec Settings ?

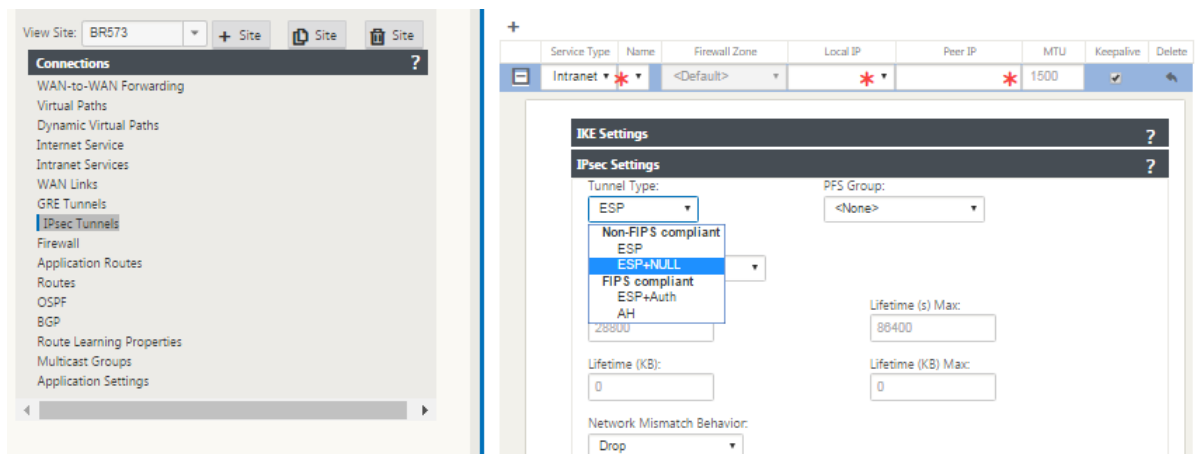
IPsec Protected Networks + Add ?

IPsec ヌル暗号化

May 10, 2021

以前のリリースでは、トンネルタイプ ESP+NULL が導入されました。IPsec ESP プロトコルを使用する場合、トラフィックは通常、暗号化および認証されます。ただし、Null 暗号化を使用すると、暗号化を使用しないように選択できます。ESP + NULL トンネルタイプでは、パケットは認証されますが、暗号化されません。

IPsec トンネルは、設定エディタの [IP sec 設定] セクションの ESP+NULL トンネルタイプで設定できます。



FIPS 準拠

May 10, 2021

Citrix SD-WAN では、FIPS モードでは、ユーザーは IPsec トンネルおよび仮想パスの IPsec 設定に FIPS 準拠の設定を構成する必要があります。

- FIPS 準拠の IKE モードを表示します。
- FIPS 準拠の IKE DH グループを表示します。このグループから、アプライアンスを FIPS 準拠モード（2,5,14～21）に設定するために必要なパラメータを選択できます。
- 仮想パスの IPsec 設定で FIPS 準拠の IPsec トンネルの種類を表示します
- IKE ハッシュおよび（IKEv2）整合性モード、IPsec 認証モード。
- FIPS ベースのライフタイム設定に対する監査エラーの実行

Citrix SD-WAN GUI を使用して FIPS コンプライアンスを有効にするには、次の手順に従います。

1. [構成] > [仮想 WAN] > [構成エディタ] > [グローバル] の順に選択し、[FIPS モードを有効にする] を選択します。

FIPS モードを有効にすると、設定中にチェックが実行され、IPsec 関連のすべての設定パラメータが FIPS 標準に準拠しているかどうかを確認されます。IPsec を構成するには、監査エラーと警告が表示されます。

仮想パス IPsec 設定を構成するには、次の手順を実行します。

- FIPS 準拠が必要なすべての仮想パスに対して、仮想パス IPsec トンネルを有効にします。仮想パスの IPsec 設定は、デフォルトセットによって制御されます。

- IPsec モードを AH または ESP+ 認証に変更してメッセージ認証を構成し、FIPS 承認ハッシュ機能を使用します。SHA1 は FIPS によって受け入れられますが、SHA256 を強く推奨します。
- IPsec ライフタイムは、8 時間 (28,800 秒) 以下に設定する必要があります。

仮想 WAN は、事前共有キーを持つ IKE バージョン 2 を使用して、次の設定を使用して、仮想パスを経由する IPsec トンネルをネゴシエートします。

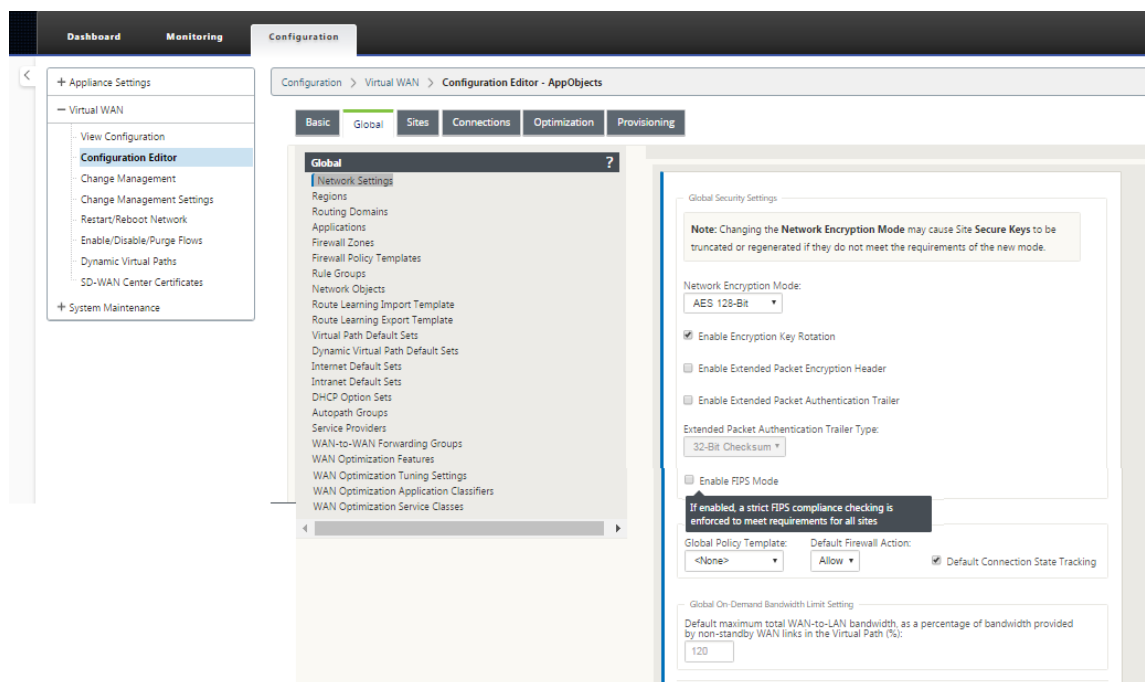
- DH グループ 19: キーネゴシエーションのための ECP256 (256 ビット楕円曲線)
- 256 ビット AES-CBC 暗号化
- メッセージ認証のための SHA256 ハッシュ
- メッセージの整合性のための SHA256 ハッシュ
- DH Group 2: MODP-1024 Perfect Forward Secrecy

サードパーティの IPsec トンネルを構成するには、次の設定を使用します。

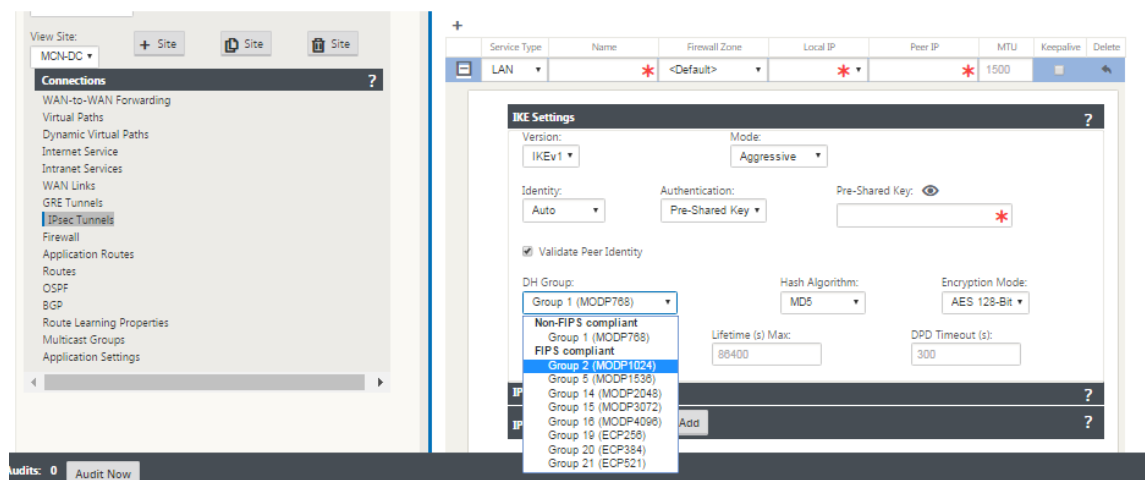
1. FIPS 承認済みの DH グループを構成します。グループ 2 と 5 は FIPS では許可されますが、グループ 14 以上を強く推奨します。
2. FIPS 承認ハッシュ関数を設定します。SHA1 は FIPS によって受け入れられますが、SHA256 を強くお勧めします。
3. IKEv2 を使用する場合は、FIPS 承認の整合性機能を設定します。SHA1 は FIPS によって受け入れられますが、SHA256 を強くお勧めします。
4. IKE ライフタイムおよび最大ライフタイムを 24 時間 (86,400 秒) 以下に設定します。
5. IPsec モードを AH または ESP+ 認証に変更して IPsec メッセージ認証を構成し、FIPS 承認ハッシュ機能を使用します。SHA1 は FIPS によって受け入れられますが、SHA256 を強く推奨します。
6. IPsec ライフタイムおよび最大ライフタイムを 8 時間 (28,800 秒) 以下に設定します。

IPsec トンネルを設定するには、次の手順を実行します。

1. MCN アプライアンスで、[構成] > [仮想 **WAN**] > [構成エディタ] の順に選択します。既存の構成パッケージを開きます。「接続」 > 「**IPsec** トンネル」の順に選択します。



2. 「接続」>「IPsec トンネル」の順に選択します。[LAN] または [イントラネットトンネル] を選択すると、画面で IKE 設定の FIPS 準拠のグループと非準拠のグループが区別されるため、FIPS 準拠を簡単に構成できます。



画面には、次の図に示すように、ハッシュアルゴリズムが FIPS に準拠しているかどうか也表示されます。

Service Type	Name	Firewall Zone	Local IP	Peer IP	MTU	Keepalive	Delete
LAN	*	<Default>	*	*	1500		

IKE Settings

Version: IKEv1 Mode: Aggressive

Identity: Auto Authentication: Pre-Shared Key Pre-Shared Key: *

☒ Validate Peer Identity

DH Group: Group 1 (MODP768) Hash Algorithm: MD5 Encryption Mode: AES 128-Bit

Lifetime (s): 3600 Lifetime (s) Max: 86400 DPD Timeout (s): 300

Non-FIPS compliant
MD5
FIPS compliant
SHA1
SHA-256

IPsec Settings

IPsec Protected Networks + Add

IPSec 設定の FIPS 準拠オプション

Service Type	Name	Firewall Zone	Local IP	Peer IP	MTU	Keepalive	Delete
LAN	*	<Default>	*	*	1500		

IKE Settings

IPsec Settings

Tunnel Type: ESP PFS Group: <None>

Non-FIPS compliant
ESP
ESP+NULL
FIPS compliant
ESP+Auth
AH

Lifetime (s) Max: 86400

Lifetime (KB): 0 Lifetime (KB) Max: 0

Network Mismatch Behavior: Drop

IPsec Protected Networks + Add

IPSec 構成が有効になっているときに FIPS 標準に準拠していない場合、監査エラーが発生する可能性があります。以下は、GUI に表示される監査エラーの種類です。

- の場合、FIPS モードが有効になり、非 FIPS 準拠オプションが選択されます。
- の場合、FIPS モードが有効になり、誤ったライフタイム値が入力されます。

- の場合、FIPS モードが有効になり、仮想パスのデフォルトセットの IPSec 設定も有効になり、不正なトンネルモードが選択されます (ESP 対 ESP_auth/AH)。
- FIPS モードを有効にすると、仮想パスのデフォルトセットの IPSec 設定も有効になり、誤ったライフタイム値が入力されます。

Citrix SD-WAN Secure Web Gateway

May 10, 2021

トラフィックを保護し、ポリシーを適用するために、企業は多くの場合、MPLS リンクを使用して、ブランチトラフィックを企業のデータセンターにバックホールします。データセンターは、セキュリティポリシーを適用し、セキュリティアプライアンスを介してトラフィックをフィルタリングしてマルウェアを検出し、トラフィックを ISP 経由でルーティングします。プライベート MPLS リンクを介したこのようなバックホールは高価です。また、レイテンシーが大きくなるため、ブランチサイトでのユーザーエクスペリエンスが低下します。また、ユーザーがセキュリティ制御をバイパスするリスクもあります。

バックホールに代わる方法として、支店にセキュリティアプライアンスを追加する方法があります。ただし、複数のアプライアンスをインストールして、サイト全体で一貫したポリシーを維持するにつれて、コストと複雑さが増大します。また、多くの支社がある場合、コスト管理は実用的ではありません。

Zscaler:

コスト、複雑さ、待ち時間を追加せずにセキュリティを強化する理想的なソリューションは、すべてのブランチインターネットトラフィックを Citrix SD-WAN アプライアンスから ZScaler Cloud セキュリティプラットフォームにルーティングすることです。その後、中央の Zscaler コンソールを使用して、ユーザーに詳細なセキュリティポリシーを作成できます。ポリシーは、ユーザーがデータセンターにいるかブランチサイトにいるかにかかわらず、一貫して適用されます。Zscaler セキュリティソリューションはクラウドベースであるため、ネットワークにセキュリティアプライアンスを追加する必要はありません。

FIPS コンプライアンス:

アメリカ国立標準技術研究所 (NIST) は、自主基準が存在しない地域で連邦情報処理基準 (FIPS) を開発しています。FIPS は、次の問題を解決します。

- 異なるシステム間の互換性。
- データとソフトウェアの移植性。
- コスト効率に優れたコンピュータセキュリティと機密情報のプライバシー

FIPS は、セキュリティシステムで使用される暗号化モジュールのセキュリティ要件を指定します。これらのセキュリティ標準を Citrix SD-WAN アプライアンスの処理に適用するには、FIPS モードを構成します。

フォースポイント:

Citrix SD-WAN を使用すると、ファイアウォールリダイレクト（宛先 NAT による透過プロキシ）機能を使用して、エンタープライズエッジにある SD-WAN アプライアンスから、Forcepoint クラウドホスト型セキュリティモジュールにインターネット（HTTP および HTTPS）トラフィックをリダイレクトできます。HTTP トラフィックをポート 80 からポート 8081 に、HTTPS トラフィックをポート 443 から最も近い Forcepoint クラウドプロキシサーバーのポート 8443 にリダイレクトできます。

GRE トンネルと IPsec トンネルを使用した Zscaler 統合

November 8, 2021

Zscaler Cloud Security Platform は、世界中の 100 以上のデータセンターで一連のセキュリティチェックの投稿として機能します。インターネットトラフィックを Zscaler にリダイレクトするだけで、店舗、支店、遠隔地をすぐに保護できます。Zscaler はユーザーとインターネットを接続し、暗号化または圧縮されている場合でも、トラフィックのすべてのバイトを検査します。

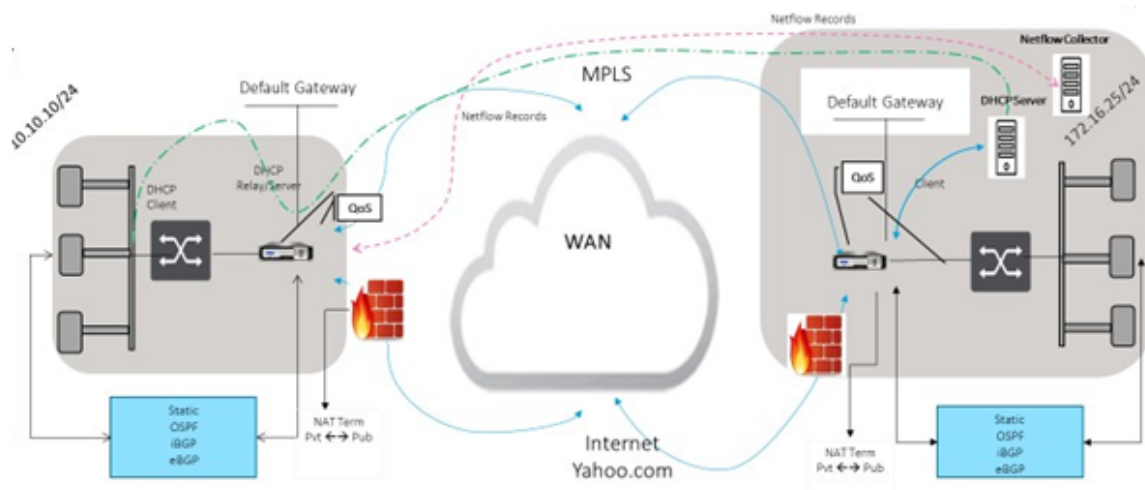
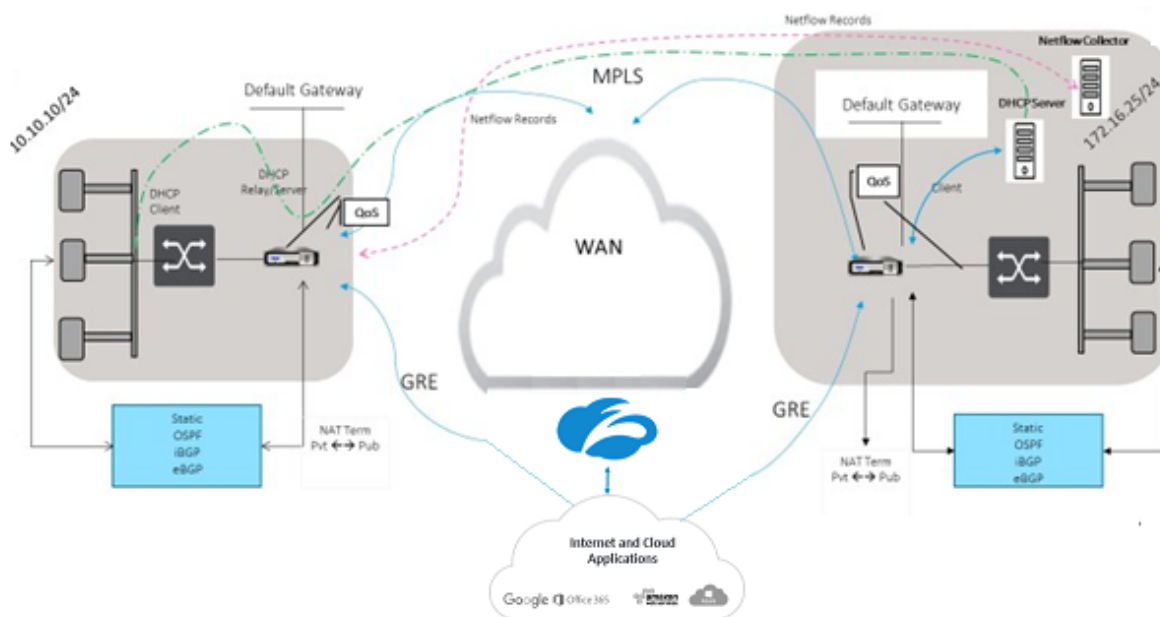
Citrix SD-WAN アプライアンスは、お客様のサイトの GRE トンネルを介して Zscaler クラウドネットワークに接続できます。SD-WAN アプライアンスを使用した Zscaler の展開では、次の機能がサポートされています。

- すべての GRE トラフィックを Zscaler に転送することで、直接インターネットブレイクアウトが可能になります。
- 顧客サイトごとに Zscaler を使用した直接インターネットアクセス（DIA）。
 - 一部のサイトでは、DIA にオンプレミスのセキュリティ機器を提供し、Zscaler を使用しない場合があります。
 - 一部のサイトでは、インターネットアクセス用に別の顧客サイトへのトラフィックのバックホールを選択する場合があります。
- 仮想ルーティングと転送の展開。
- インターネットサービスの一部としての 1 つの WAN リンク。

Zscaler はクラウドサービスです。サービスとして設定し、基になる WAN リンクを定義する必要があります。

- データセンターでインターネットサービスを設定し、GRE 経由でブランチします。
- 信頼できるパブリックインターネットリンクを、データセンターおよびブランチサイトで構成します。

トポロジ

CURRENT DEPLOYMENT MODEL WITH ON-PREMISE FIREWALL**ZSCALER SECURITY AS SERVICE DEPLOYMENT MODEL**

GRE トンネルまたは IPsec トンネルトラフィック転送を使用するには、次の手順を実行します。

1. Zscaler ヘルプポータルにログインします <https://help.zscaler.com/submit-ticket>。
2. チケットを発行し、GRE トンネルまたは IPsec トンネルの送信元 IP アドレスとして使用する静的パブリック IP アドレスを指定します。

Zscaler は、送信元 IP アドレスを使用してカスタマーの IP アドレスを識別します。送信元 IP はスタティックパブ

リック IP である必要があります。ZScaler は、トラフィックを送信する 2 つの ZEN IP アドレス（プライマリとセカンダリ）で応答します。GRE キープアライブメッセージを使用して、トンネルの健全性を判断できます。

Zscaler は、送信元 IP アドレス値を使用してカスタマーの IP アドレスを識別します。この値は、静的なパブリック IP アドレスである必要があります。Zscaler は、トラフィックのリダイレクト先となる 2 つの ZEN IP アドレス [DR1] で応答します。GRE キープアライブメッセージを使用して、トンネルの健全性を判断できます。

サンプル IP アドレス

プライマリ

内部ルータの IP アドレス:172.17.6.241/30

内部 ZEN IP アドレス:172.17.6.242/30

セカンダリ

内部ルーター IP アドレス:172.17.6.245/30

内部 ZEN IP アドレス:172.17.6.246/30

インターネットサービスの設定

インターネットサービスを構成するには、次の操作を行います。

1. [接続]-[インターネットサービス] に移動します。インターネットサービスを構成します。
2. [+ サービス] を選択し、必要に応じて設定 (基本設定、WAN リンク、およびルール) を有効にします。
3. [適用] を選択します。

サイトのインターネットサービスを有効にする方法の詳細については、「[統合ファイアウォールを使用したブランチでの直接インターネットブレイクアウト](#)」を参照してください。

インターネットサービスでは、次の設定を構成できます。

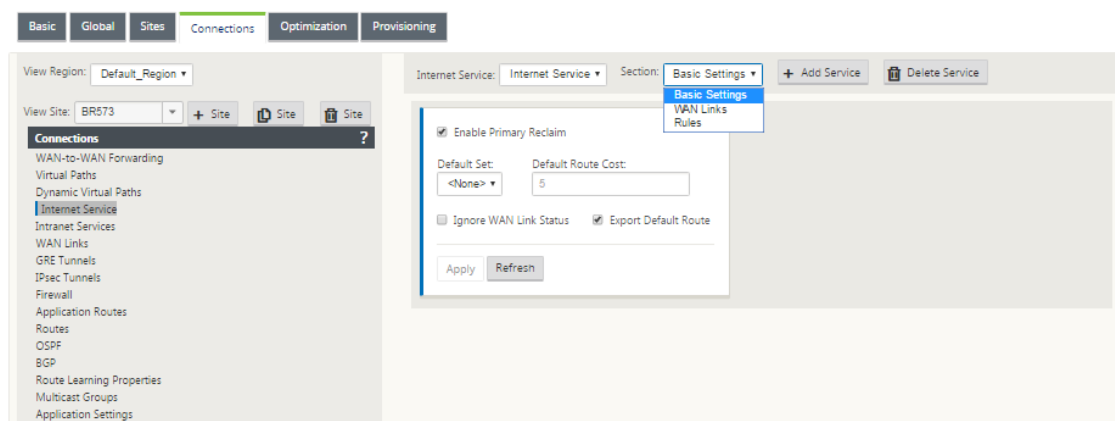
- [基本設定](#)
- [WAN リンク](#)
- [規則](#)

基本設定

ファイアウォールゾーンの設定は、インターネットサービスには構成できません。インターネットサービスが信頼されている場合は、**Internet_Zone** に割り当てられます。インターネットサービスが信頼されていない場合は、**Untrusted_Internet_Zone** に割り当てられます。

構成可能な基本設定は次のとおりです。

- プライマリ再利用を有効にする: 有効にすると、WAN リンク上のこのサービスに関連付けられている（使用 = プライマリ）使用状況は、その WAN リンク上のアクティブサービスとして強制的にステータスを再利用します。
- デフォルトセット: サイトのインターネットサービスのルールを設定するインターネットのデフォルトセットの名前。
- デフォルトルートコスト: デフォルト（0.0.0.0/0）インターネットルートに関連付けられたルートコスト。
- **WAN** リンクステータスを無視: 有効にすると、このサービス宛てのパケットは、このサービスのすべての WAN リンクが利用できない場合でも、このサービスを選択します。
- デフォルトルートのエクスポート: 有効にすると、WAN-to-WAN 転送が有効になっている場合、インターネットサービスのデフォルトルート 0.0.0.0/0 が他のサイトにエクスポートされます。



WAN リンク

設定可能な WAN リンクの設定は次のとおりです。

- 使用: サービスにこの WAN リンクの使用を許可します。[使用] (Use) が無効になっていると、他のすべてのオプションは使用できなくなります。
- **Mode**: トラフィックの冗長性または負荷分散のためのサービスモード（プライマリ、セカンダリ、またはバランス）。
- **トンネルヘッダーサイズ (バイト)**: トンネルヘッダーのサイズ（バイト単位）（該当する場合）。
- **アクセスインターフェイスフェールオーバー**: 有効にした場合、VLAN が一致しないインターネットまたはイントラネットパケットは引き続きサービスを使用できます。

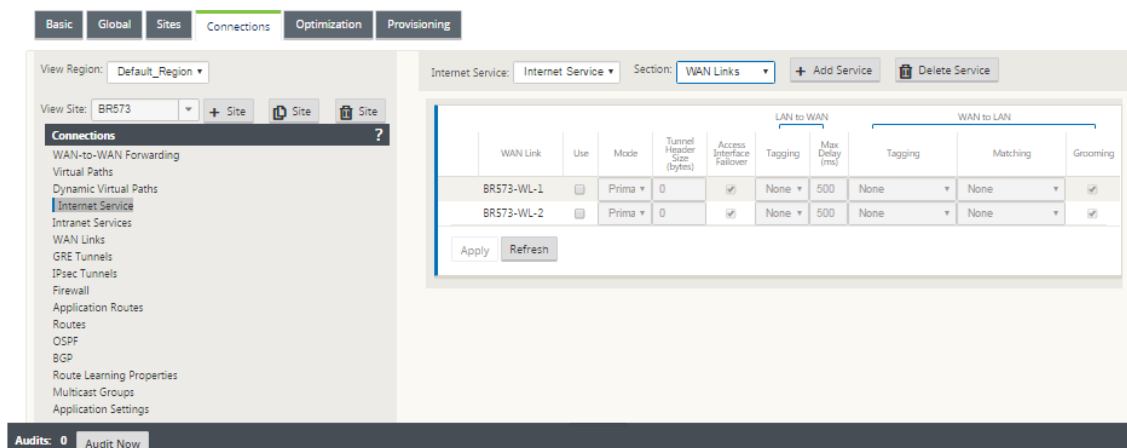
LAN から WAN

- タグ付け: サービス上の LAN から WAN へのパケットに適用する DSCP タグ。

- **Max Delay (ms):** WAN リンクの帯域幅を超えたときにパケットをバッファリングする最大時間（ミリ秒単位）。

WAN から LAN へ

- タグ付け: サービス上の WAN から LAN へのパケットに適用する DSCP タグ。
- 一致: このタグに一致するインターネット WAN から LAN へのパケットがサービスに割り当てられます。
- グルーミング: 有効にすると、WAN から LAN へのトラフィックがサービスのプロビジョニングされた帯域幅を超えないように、パケットはランダムにドロップされます。



規則

インターネットトラフィックは、定義されたルールに基づいて識別されます。ルール定義は、特定のトラフィックフローを照合するために使用されます。一致したら、トラフィックフローに適用するアクションを定義する必要があります。

使用可能なルールのリストは次のとおりです。

- 順序: ルールが適用され、自動的に再配布される順序。
- ルールグループ名: ルール統計の表示時にグループ単位で集計できるようにするルールに付けられる名前。同じルールグループ名を持つルールのすべての統計情報をまとめて表示できます。
- 送信元: ルールと一致する送信元 IP アドレスとサブネットマスク。
- **Dest-Src:** 有効にすると、送信元 IP アドレスが宛先 IP アドレスとしても使用されます。
- **Dest:** ルールと一致する宛先 IP アドレスとサブネットマスク。
- プロトコル: フィルタと一致するプロトコル名。
- **Protocol #:** フィルタと一致するプロトコル番号。
- **DSCP:** ルールと一致する IP ヘッダー内の DSCP タグ。

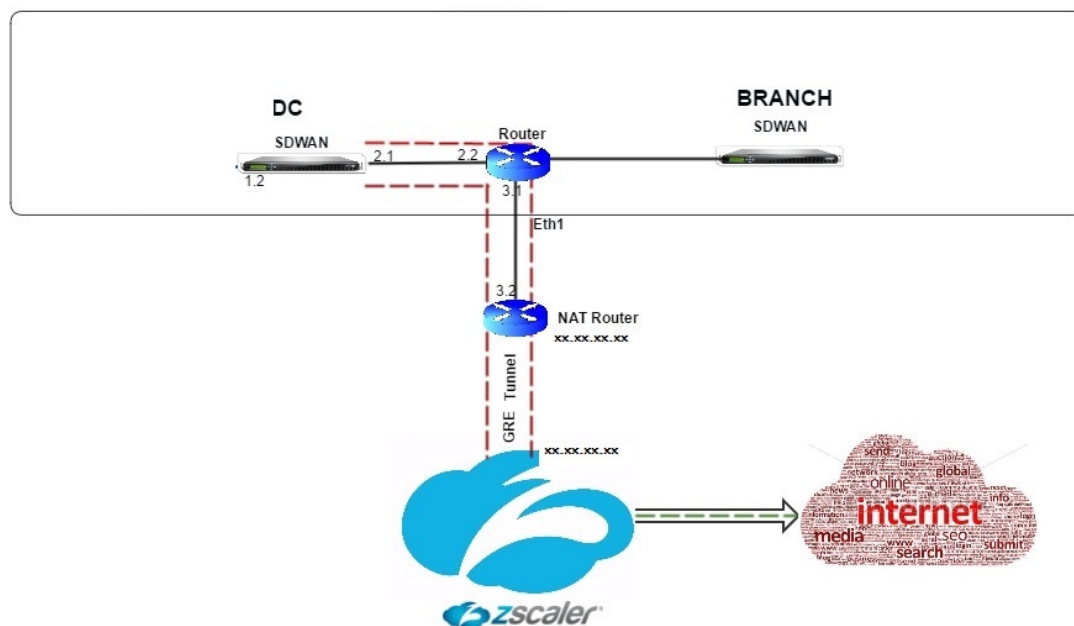
使用可能なアクションのリストを以下に示します。

- **WAN リンク:** インターネット負荷分散が有効な場合に、ルールに一致するフローによって使用される WAN リンク。
- **Override Service:** ルールに一致するフローの宛先サービス。
 - **Discard:** トラフィックをドロップします。
 - **パススルー:** フローをパススルーにマッピングし、トラフィックが変更されずにアプライアンスを通過できるようにします。

The screenshot shows the 'Rules' configuration page in Citrix SD-WAN. At the top, there are tabs for 'Internet Service' and 'Rules', along with '+ Add Service' and 'Delete Service' buttons. Below this is a table with columns for 'Order', 'Rule Group Name', 'Source', 'Dest-Src', 'Dest', 'Protocol', 'Protocol #', 'Source', 'Dest-Src', 'Dest', 'DSCP', 'VLAN', 'Rebind Flow on Change', 'Delete', and 'Clone'. The first rule is selected, showing 'Order: 100', 'Rule Group Name: <None>', 'Source: *', 'Dest-Src: *', 'Dest: *', 'Protocol: Any', 'Protocol #: 0', 'Source: *', 'Dest-Src: *', 'Dest: *', 'DSCP: Any', and 'VLAN: *'. Below the table is a configuration panel for the selected rule. It includes a 'Mode' dropdown set to 'WAN Link', a 'WAN Link' dropdown set to '<N/A>', an 'Override Service' dropdown set to '<N/A>', and an 'Enable Passive FTP Detection' checkbox which is unchecked. At the bottom of the panel are 'Apply' and 'Revert' buttons.

GRE トンネルの設定

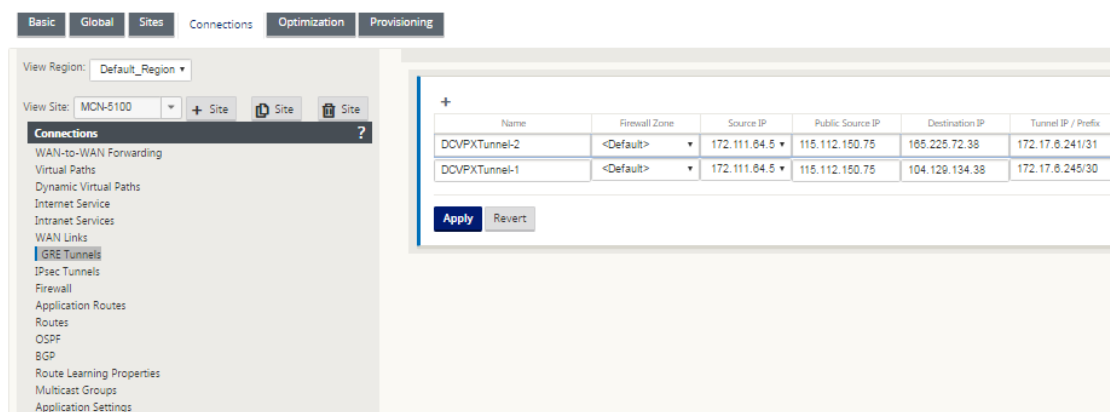
1. 送信元 IP アドレスは、トンネルの送信元 IP アドレスです。トンネル送信元 IP アドレスが NATted の場合、別の中間デバイスで NATted されている場合でも、パブリック送信元 IP アドレスはパブリックトンネル送信元 IP アドレスになります。
2. 宛先 IP アドレスは、ZScaler が提供する ZEN IP アドレスです。
3. 元のペイロードがカプセル化されている場合、送信元 IP アドレスと宛先 IP アドレスはルータ GRE ヘッダーです。
4. トンネル IP アドレスおよびプレフィックスは、GRE トンネル自体の IP アドレッシングです。これは、GRE トンネル経由でトラフィックをルーティングする場合に便利です。トラフィックには、この IP アドレスがゲートウェイアドレスとして必要です。



GRE トンネルを設定するには、次の手順を実行します。

1. 構成エディタで、[接続] > [サイト] > [**GRE トンネル**] に移動し、インターネットプレフィックスサービスを Zscaler GRE トンネルに転送するルートを設定します。

送信元 IP アドレスは、信頼できるリンクの仮想ネットワークインターフェイスからのみ選択できます。[GRE トンネルの設定方法を参照してください](#)。



GRE トンネルのルートの設定

インターネットプレフィックスサービスを Zscaler GRE トンネルに転送するルートを設定します。

- ZEN IP アドレス（トンネルの宛先 IP、上の図の 104.129.194.38）は、サービスタイプインターネットに設定する必要があります。これは、Zscaler 宛てのトラフィックがインターネットサービスから計上されるようにするために必要です。

- Zscaler 宛てのすべてのトラフィックは、デフォルトルート 0/0 と一致し、GRE トンネルを介して送信される必要があります。[DR1] GRE トンネルに使用される 0/0 ルートが、パススルーまたは他のサービスタイプよりも低コストであることを確認します。
- 同様に、Zscaler へのバックアップ GRE トンネルのコストは、プライマリ GRE トンネルのコストよりも高い必要があります。
- ZEN IP アドレスの非再帰ルートが存在することを確認します。

GRE トンネルのルートを設定するには、次の手順を実行します。

1. [接続] > [サイト] > [ルート] に移動し、ルートの作成手順については、[ルートの設定で説明されている手順に従います](#)。

Order	Network IP Address	Cost	Service Type	Service Name	Gateway IP Address	Info	Edit	Delete
1	104.129.194.38/32	5	Internet			ⓘ	✎	✖
2	165.225.72.38/32	5	Internet			ⓘ	✎	✖
3	172.17.6.241/30	5	GRE Tunnel		165.225.72.38	ⓘ		
4	172.17.6.245/30	5	GRE Tunnel		104.129.194.38	ⓘ		
5	172.16.1.2/24	5	Local			ⓘ		
6	172.16.4.0/24	5	Local		172.16.1.1	ⓘ	✎	✖
7	0.0.0.0/0	3	GRE Tunnel		172.17.6.242	ⓘ	✎	✖
8	0.0.0.0/0	4	GRE Tunnel		172.17.6.246	ⓘ	✎	✖
9	0.0.0.0/0	5	Internet			ⓘ		
10	0.0.0.0/0	16	Passthrough			ⓘ		

注

Zscaler IP アドレスに特定のルートがない場合は、ZEN IP アドレスと一致するようにルートプレフィックス 0.0.0.0/0 を設定し、GRE トンネルのカプセル化ループを介してルーティングします。この設定では、アクティブバックアップモードでトンネルを使用します。上の図に示す値を使用すると、トラフィックは Gateway IP アドレス 172.17.6.242 のトンネルに自動的に切り替わります。必要に応じて、バックホール仮想パスルートを設定します。それ以外の場合は、バックアップトンネルのキープアライブ間隔をゼロに設定します。これにより、Zscaler へのトンネルが両方とも失敗しても、サイトへの安全なインターネットアクセスを可能にします。

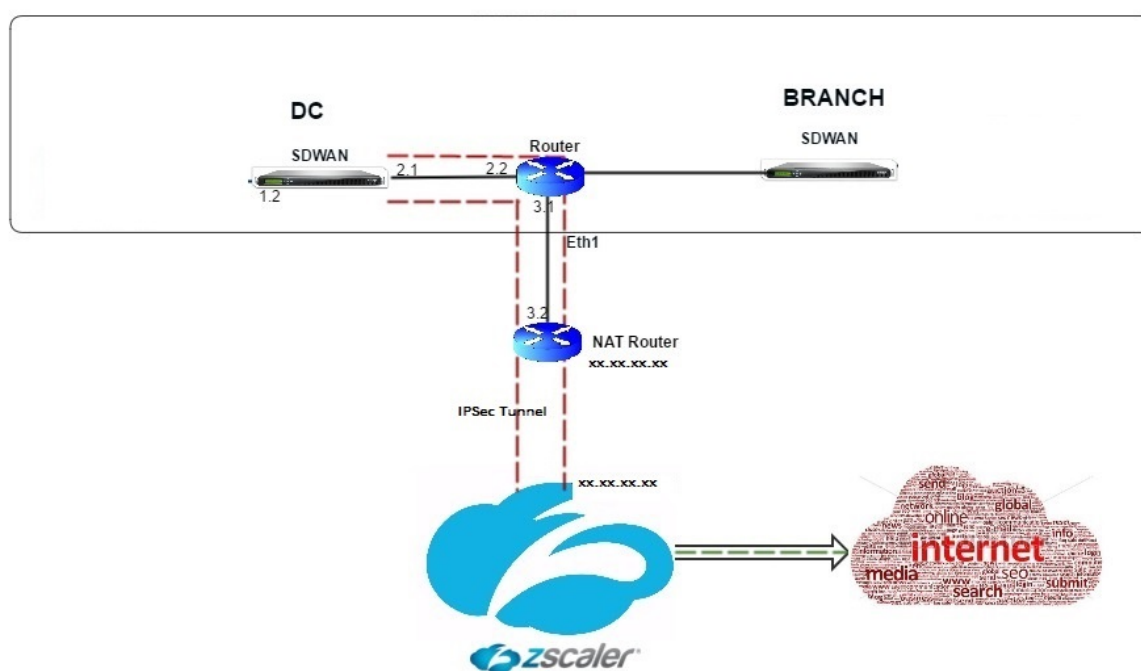
GRE キープアライブメッセージがサポートされています。**GRE** 送信元アドレスの **NAT** アドレスを提供するパブリックソース **IP** という新しいフィールドが、Citrix SD-WAN GUI インターフェイスに追加されます (SD-WAN アプライアンスのトンネルソースが中間デバイスによって NAT 接続されている場合)。Citrix SD-WAN GUI には、パブリックソース IP というフィールドが含まれています。このフィー

ルドには、Citrix SD-WAN アプライアンスのトンネルソースが中間デバイスによって NAT 変換されたときに、GRE ソースアドレスの NAT アドレスを提供します。

制限事項

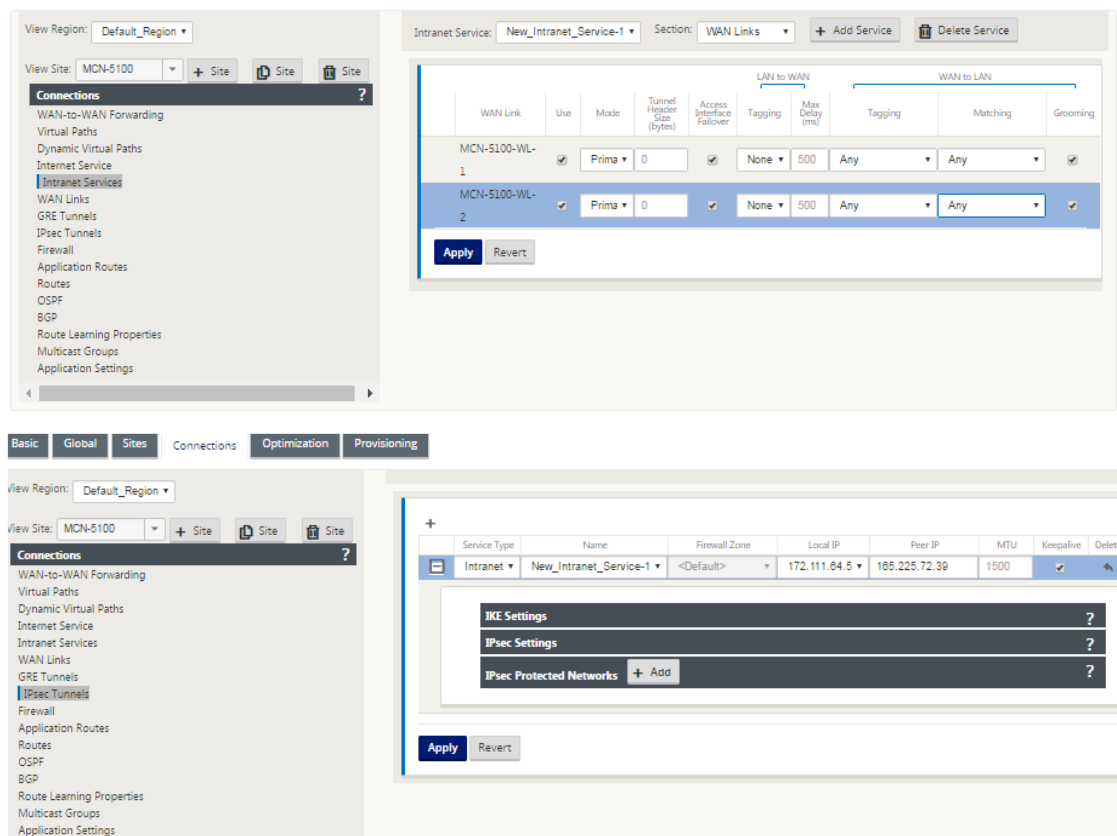
- 複数の VRF 配置はサポートされていません。
- プライマリバックアップ GRE トンネルは、高可用性設計モードでのみサポートされます。

IPSec トンネルを構成する

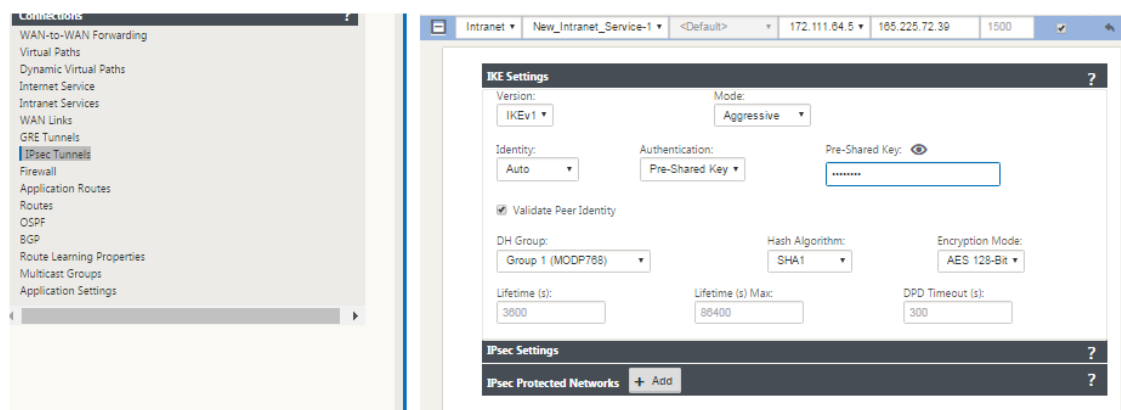


Citrix SD-WAN アプライアンス GUI でイントラネットまたは LAN サービス用の IPSec トンネルを構成するには、以下の手順に従ってください。

1. 設定エディタで、[接続] > [SiteName] > [IPSec トンネル] に移動し、サービスタイプ（LAN またはイントラネット）を選択します。
2. サービス・タイプの「名前」を入力します。イントラネットサービスの種類では、構成されたイントラネットサーバーによって、使用できるローカル IP アドレスが決まります。
3. 使用可能なローカル IP アドレスを選択し、リモートピアへの仮想パスのピア IP アドレスを入力します。



4. IKE 設定で [****IKEv1****] を選択します。Zscaler は IKEv1 のみをサポートしています。



5. [IPsec 設定] で、[トンネルの種類] に [**ESP-NULL**] を選択し、IPsec トンネルを介してトラフィックを Zscaler にリダイレクトします。IPsec トンネルはトラフィックを暗号化しません。

The screenshot displays the configuration page for an IPsec tunnel. It is divided into two main sections: 'IKE Settings' and 'IPsec Settings'. The 'IKE Settings' section includes fields for Tunnel Type (ESP+NULL), PFS Group (<None>), Hash Algorithm (SHA1), Lifetime (s) (28800), Lifetime (s) Max (86400), Lifetime (KB) (0), Lifetime (KB) Max (0), and Network Mismatch Behavior (Drop). The 'IPsec Settings' section has a header with a '+' icon and the text 'Add', and a question mark icon.

IKE Settings	
Tunnel Type:	ESP+NULL
PFS Group:	<None>
Hash Algorithm:	SHA1
Lifetime (s):	28800
Lifetime (s) Max:	86400
Lifetime (KB):	0
Lifetime (KB) Max:	0
Network Mismatch Behavior:	Drop

IPsec Settings	
+ Add	

6. インターネットトラフィックはリダイレクトされるため、宛先 IP/プレフィックスには任意の IP アドレスを使用できます。

The screenshot displays the configuration page for an IPsec tunnel. It is divided into two main sections: 'IKE Settings' and 'IPsec Settings'. The 'IKE Settings' section includes fields for Version (IKEv1), Mode (Aggressive), Identity (Auto), Authentication (Pre-Shared Key), Pre-Shared Key (masked), Validate Peer Identity (checked), DH Group (Group 1 (MODP768)), Hash Algorithm (SHA1), Encryption Mode (AES 128-Bit), Lifetime (s) (3600), Lifetime (s) Max (86400), and DPD Timeout (s) (300). The 'IPsec Settings' section has a header with a '+' icon and the text 'Add', and a question mark icon. Below this is a table for 'IPsec Protected Networks' with columns for Source IP/Prefix, Destination IP/Prefix, and Delete. The table contains one entry with Source IP/Prefix 172.16.4.0/24 and Destination IP/Prefix 0.0.0.0/0. At the bottom are 'Apply' and 'Revert' buttons.

IKE Settings	
Version:	IKEv1
Mode:	Aggressive
Identity:	Auto
Authentication:	Pre-Shared Key
Pre-Shared Key:	*****
<input checked="" type="checkbox"/> Validate Peer Identity	
DH Group:	Group 1 (MODP768)
Hash Algorithm:	SHA1
Encryption Mode:	AES 128-Bit
Lifetime (s):	3600
Lifetime (s) Max:	86400
DPD Timeout (s):	300

IPsec Settings	
+ Add	

Source IP/Prefix	Destination IP/Prefix	Delete
172.16.4.0/24	0.0.0.0/0	

Apply Revert

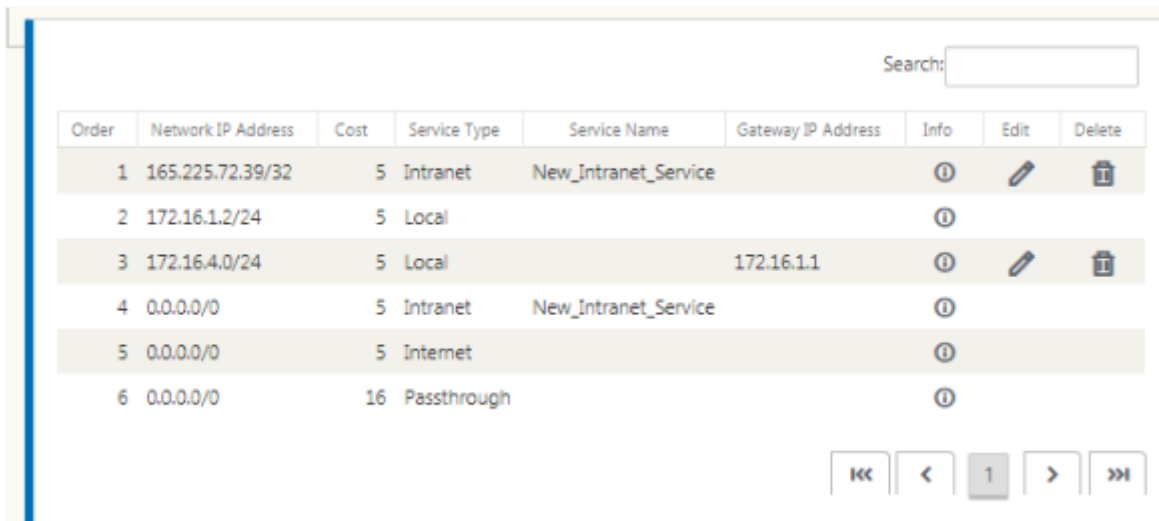
Citrix SD-WAN Web インターフェイスを使用した IPsec トンネルの構成の詳細については、「[IPsec トンネル](#)」ト

ピックを参照してください。

IPsec トンネルのルートの設定

IPsec ルートを設定するには、次の手順を実行します。

1. [接続] > [DC] > [ルート] に移動し、ルートの作成手順については、[ルートの設定で説明されている手順に従います](#)。



Order	Network IP Address	Cost	Service Type	Service Name	Gateway IP Address	Info	Edit	Delete
1	165.225.72.39/32	5	Intranet	New_Intranet_Service		ⓘ	✎	🗑️
2	172.16.1.2/24	5	Local			ⓘ		
3	172.16.4.0/24	5	Local		172.16.1.1	ⓘ	✎	🗑️
4	0.0.0.0/0	5	Intranet	New_Intranet_Service		ⓘ		
5	0.0.0.0/0	5	Internet			ⓘ		
6	0.0.0.0/0	16	Passthrough			ⓘ		

GRE および IPsec トンネルの統計情報をモニタするには、次の手順を実行します。

SD-WAN Web インターフェイスでは、モニタリング > **IPsec トンネル**。

統計情報 > **GRE** トンネルにナビゲートして下さい

詳細については、[を参照してください](#)。 [IPsec トンネルのモニタリング](#)および[GRE トンネルのトピック](#)。

Citrix SD-WAN での Forcepoint を使用したファイアウォールトラフィックリダイレクトのサポート

May 10, 2021

Forcepoint は次の機能をサポートしますが、SD-WAN はファイアウォールリダイレクト機能のみをサポートします。

- PKI を使用した IPsec
- PSK を使用した IPsec

- PAC ファイル設定を使用したプロキシチェーン
- 標準ヘッダーによるプロキシ連鎖
- 独自のヘッダーによるプロキシチェーンにより、クライアントの IP 範囲 (パートナーシップ/開発) を構成する必要がなくなります
- ファイアウォールリダイレクト (宛先 NAT による透過プロキシ)

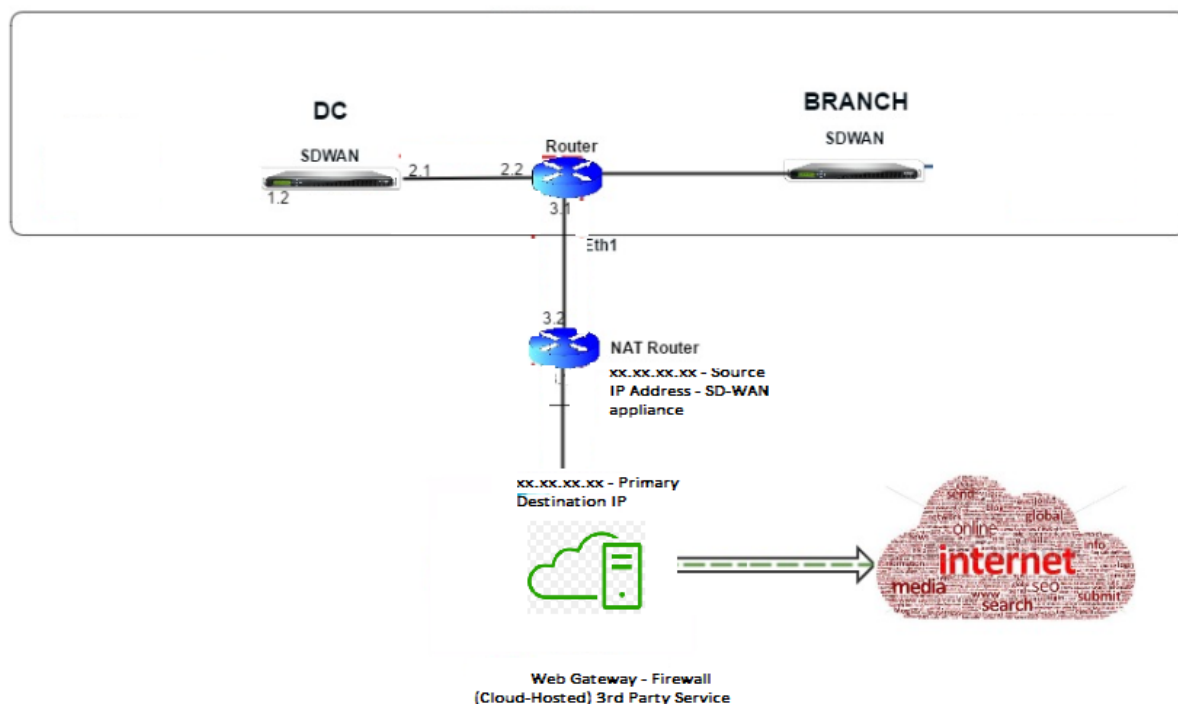
Destination NAT ポリシーを使用すると、企業は ForcePoint を使用してクラウドでホストされたセキュリティサービスを通じてインターネットトラフィックをルーティングできます。

SD-WAN アプライアンスで Destination NAT を構成し、安全なクラウドベースのファイアウォールサービスを通じてインターネットトラフィックをリダイレクトする方法を理解するには、次のユースケースを参照してください。

前提条件:

1. [Forcepoint ポータルサイト](#)にログインします。インターネットトラフィックを Forcepoint にリダイレクトする必要があるエンタープライズパブリック IP アドレスを指定して、ポリシーを作成します。インターネットトラフィックのリダイレクト先となるプライマリ IP アドレスとセカンダリ IP アドレスを取得します。
2. SD-WAN GUI で、DC サイトの SD-WAN アプライアンスで、WAN リンクに関連付けられたインターネットサービスを設定します。
3. 宛先 NAT は、インターネットトラフィックの宛先 IP アドレスを使用して実行されます。この宛先アドレスは、Forcepoint パブリック IP アドレスに変更されます。
4. 送信元 IP アドレスとプライマリ IP アドレスを指定して、宛先 NAT ポリシーを設定します。送信元 IP は、ポート 80 (http) および 443 (https) 内の SD-WAN アプライアンスのインターネット IP アドレスです。このアドレスは、外部ポート 8081 (http) および 8443 (https) で、クラウドベースのファイアウォール Gateway のプライマリ宛先 IP アドレスにリダイレクト/変換されます。
5. DNAT ポリシーを設定した後、DC で設定されたルートで、SD-WAN ネットワーク IP アドレスに対してインターネットサービスタイプが選択されていることを確認します。

Citrix SD-WAN での NAT サポートの詳細については、以下のトピック「[NAT の設定](#)」を参照してください



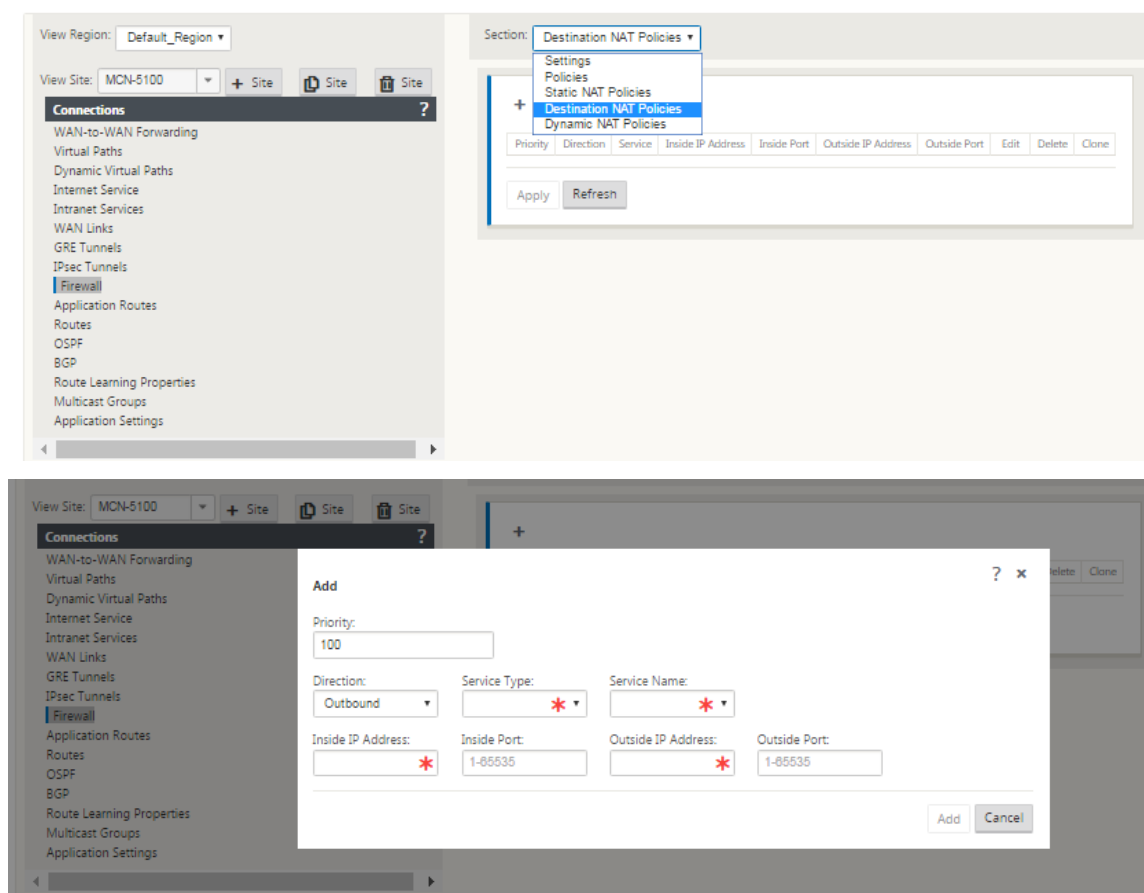
宛先 NAT (DNAT) の設定

Citrix SD-WAN GUI を使用して、宛先 NAT (DNAT) を構成します。設定で、特定の宛先 IP アドレスおよびポートに一致するトラフィックをリダイレクトする、1 つ以上の DNAT ポリシーを追加します。

宛先 NAT を設定するには、次の手順を実行します。

SD-WAN SE/VPX GUI で、[構成] → [仮想 WAN] → [構成エディタ] に移動します。[開く] をクリックして、既存のパッケージを開きます。保存済みの構成パッケージを選択します。また、ネットワーク構成の構築中に DNAT ルールを作成することもできます。

1. DC (MCN) で、インターネットサービスを構成します。[接続] → [ファイアウォール] に移動します。
2. [+ 追加] をクリックして、DNAT ポリシーを追加します。
3. [宛先 NAT ポリシーの追加] ダイアログボックスで、次の情報を入力します。
 - 優先度
 - 方向
 - サービスの種類
 - サービス名
 - 内部 IP アドレス
 - インサイドポート
 - 外部 IP アドレス
 - 外部ポート



4. スタティック NAT と同様に、ファイアウォールトラフィックリダイレクト用の宛先 NAT ルールをプロビジョニングします。
5. 一致基準と、NAT する宛先 IP/ポートを入力します。
6. 統計情報を使用して、DNAT 規則の接続照合を実行します。
7. 構成の更新中に DNAT ルールを削除または更新します。

宛先 **NAT** ポリシー（ファイアウォール）のモニタリング

Citrix SD-WAN GUI を使用して、現在の DNAT ポリシー構成を監視することもできます。

現在の宛先 NAT ポリシー設定をモニタするには、次の手順を実行します。

1. Citrix SD-WAN GUI で、[監視] > [ファイアウォール] > [**NAT** ポリシー] に移動します。
2. 監視する統計情報を含むタブを選択します。

The top screenshot displays the 'Firewall Statistics' page. The 'Statistics' dropdown is set to 'NAT Policies'. The 'Maximum entries to display' is set to 50. The 'NAT' section shows filters for IP Protocol (Any), NAT Type (Any), and Dynamic NAT Type (Any). The 'Service Type' is set to Any, and the 'Service Name' is set to Any. The 'Inside IP' is set to *, and the 'Inside Port' is set to *. The 'Outside IP' is set to *, and the 'Outside Port' is set to *. The 'Refresh' button is visible. Below the statistics, the 'NAT Policies' table is shown with one policy: '1 Dynamic PR - - Outbound * Internet - * * 172.16.2.101/32 0-65535 No No No 253825 26477410 452674 614179776 3 [Connections]'. The bottom screenshot displays the 'Connections' page. The 'Statistics' dropdown is set to 'Connections'. The 'Maximum entries to display' is set to 10. The 'Filtering' section shows filters for IP Protocol (Any), Source Zone (Any), Destination Zone (Any), Source Service Type (Any), Source Service Instance (Any), Source IP (Any), Source Port (Any), Destination Service Type (Any), Destination Service Instance (Any), Destination IP (Any), and Destination Port (Any). The 'Refresh' button is visible. Below the statistics, the 'Connections' table is shown with two entries: 'Domain Name Service(dns) Network Service UDP 172.16.6.10 9680 Virtual Path DC-MCN-BR1-CS2000 Default_LAN_Zone 10.140.50.5 53 Internet DC-MCN-Internet Internet_Zone ESTABLISHED' and 'Domain Name Service(dns) Network Service UDP 172.16.16.1 56451 Virtual Path DC-MCN-BR1-CS2000 Default_LAN_Zone 10.140.50.5 53 Internet DC-MCN-Internet Internet_Zone ESTABLISHED'.

IPsec トンネルを使用した Palo Alto 統合

May 10, 2021

Palo Alto Networks は、リモートネットワークを保護するためのクラウドベースのセキュリティインフラストラクチャを提供します。組織が SD-WAN ファブリックを保護する地域的なクラウドベースのファイアウォールをセットアップできるようにすることで、セキュリティを提供します。

リモートネットワーク用の Prisma Access サービスを使用すると、リモートネットワークロケーションをオンボーディングし、ユーザーにセキュリティを提供できます。すべてのリモートロケーションでのデバイスの設定と管理の複雑さを取り除きます。このサービスは、新しいリモートネットワークロケーションを簡単に追加し、運用上の課題を最小限に抑える効率的な方法を提供します。また、Panorama からポリシーを一元的に管理し、一貫した合理化されたりモートセキュリティを実現できます。ネットワークロケーション。

リモートネットワークの場所を Prisma Access サービスに接続するには、Palo Alto Networks 次世代ファイアウォールを使用するか、

SD-WAN を含むサードパーティの IPsec 準拠デバイスを使用して、サービスへの IPsec トンネルを確立できます。

- リモートネットワーク用の Prisma アクセスサービスの計画
- リモートネットワーク用の Prisma Access サービスの構成
- 設定インポートを備えたオンボードリモートネットワーク

Citrix SD-WAN ソリューションは、ブランチからのインターネットトラフィックを分割する機能をすでに提供しています。これは、各ブランチでの高価なセキュリティスタックの導入を回避しながら、より信頼性が高く、待機時間の短いユーザーエクスペリエンスを提供するために重要です。Citrix SD-WAN と Palo Alto Networks は、分散企業に、ブランチ内のユーザーをクラウド内のアプリケーションに接続するためのより信頼性が高く安全な方法を提供します。

Citrix SD-WAN アプライアンスは、最小限の構成で SD-WAN アプライアンスの場所から IPsec トンネルを介して Palo Alto クラウドサービス (Prisma Access Service) ネットワークに接続できます。あなたは、Citrix SD-WAN Center でパロアルトネットワークを構成することができます。

リモートネットワーク用の Prisma Access Service の構成を開始する前に、サービスを正常に有効にしてリモートネットワークの場所のユーザーにポリシーを適用できるように、次の構成の準備ができていることを確認してください。

1. サービス接続—ユーザーの認証や重要なネットワーク資産へのアクセスを可能にするために、リモートネットワークのロケーションが企業本社のインフラストラクチャにアクセスする必要がある場合、本社とリモートネットワークのロケーションが接続されています。

リモートネットワークの場所が自律的で、他の場所にあるインフラストラクチャにアクセスする必要がない場合は、サービス接続を設定する必要はありません（モバイルユーザーがアクセスを必要とする場合を除く）。

1. テンプレート—プリズマアクセスサービスは、リモートネットワーク用のプリズマアクセスサービスのテンプレートスタック (Remote_Network_Template_Stack) と最上位テンプレート (Remote_Network_Template) を自動的に作成します。リモートネットワーク用の Prisma アクセスサービスを構成するには、最上位のテンプレートを最初から構成するか、既存の Palo Alto Networks ファイアウォールを既にオンプレミスで実行している場合は既存の構成を利用します。

テンプレートには、リモートネットワークの場所とリモートネットワーク用の Prisma Access サービス、セキュリティポリシーで参照できるゾーン、およびログ転送プロファイル間のプロトコルネゴシエーションのための IPsec トンネルとインターネットキーエクスチェンジ (IKE) 構成を確立するための設定が必要です。リモートネットワークの Prisma Access サービスからログサービスにログを転送できること。

2. 親デバイスグループ—リモートネットワークの Prisma Access サービスでは、セキュリティポリシー、セキュリティプロファイル、およびその他のポリシーオブジェクト（アプリケーショングループとオブジェクト、アドレスグループなど）を含む親デバイスグループと、リモートネットワーク用の Prisma Access サービスは、IPsec トンネルを介してリモートネットワーク用の Prisma Access サービスにルーティングされるトラフィックのポリシーを一貫して適用できます。Panorama でポリシールールとオブジェクトを定義するか、既存のデバイスグループを使用して、リモートネットワークロケーションのユーザを保護する必要があります。

注:

ゾーンを参照する既存のデバイスグループを使用する場合は、ゾーンを定義する対応するテンプレートを Remote_Network_Template_Stack に追加してください。

これにより、リモートネットワーク用の Prisma Access サービスを構成するときにゾーンマッピングを完了できます。

3. **IP サブネット**—Prisma Access サービスがトラフィックをリモートネットワークにルーティングするには、Prisma Access サービスを使用してセキュリティ保護するサブネットワークのルーティング情報を指定する必要があります。リモートネットワークの場所で各サブネットワークへの静的ルートを定義するか、サービス接続場所と Prisma Access サービスの間に BGP を構成するか、両方の方法を組み合わせて使用できます。

スタティックルートを設定し、BGP を有効にすると、スタティックルートが優先されます。リモートネットワークの場所にいくつかのサブネットワークしかない場合は静的ルートを使用すると便利な場合がありますが、サブネットが重複している多くのリモートネットワークがある大規模な展開では、BGP を使用するとより簡単にスケーリングできます。

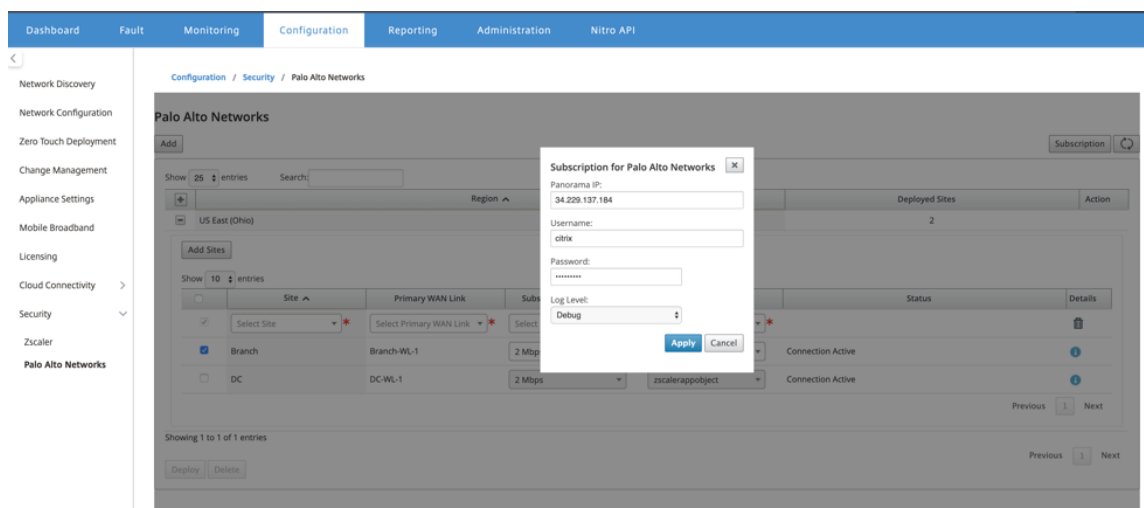
SD-WAN Center の Palo Alto Networks

以下の前提条件が満たされていることを確認してください。

- PRISMA ACCESS サービスからパノラマ IP アドレスを取得します。
- PRISMA ACCESS サービスでユーザー名とパスワードを取得します。
- SD-WAN アプライアンス GUI で IPsec トンネルを構成します。
- サイトが Citrix-IKE-Crypto-Default/Citrix-IPSec-Crypto-Default 以外の ike/ipsec プロファイルで構成された異なるサイトのあるリージョンにオンボーディングされていないことを確認してください。
- SD-WAN Center によって設定が更新されるときに、Prisma Access の設定を手動で変更しないようにしてください。

Citrix SD-WAN Center の GUI で、Palo Alto のサブスクリプション情報を入力します。

- パノラマ IP アドレスを設定します。この IP アドレスは Palo Alto (PRISMA ACCESS サービス) から取得できます。
- PRISMA ACCESS サービスで使用するユーザー名とパスワードを設定します。



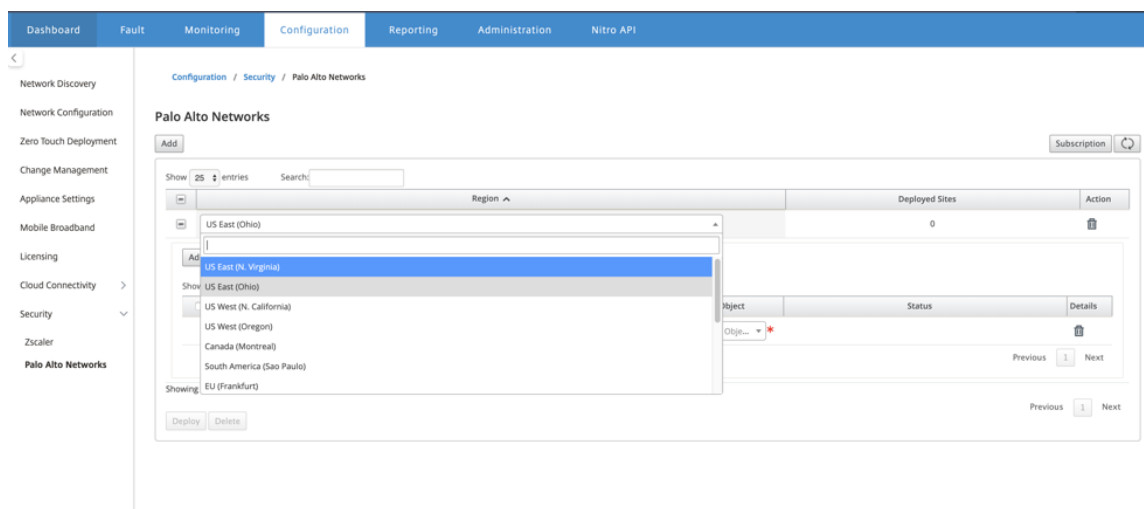
サイトを追加して展開する

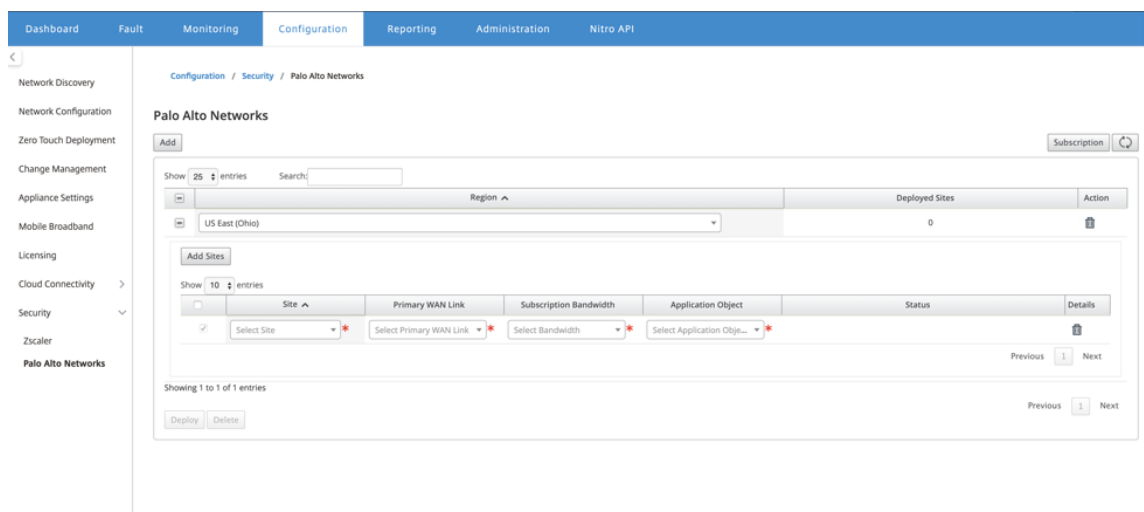
1. サイトをデプロイするには、PRISMA ACCESS ネットワークリージョンと Prisma Access リージョン用に構成する SD-WAN サイトを選択し、サイト WAN リンク、帯域幅、およびトラフィック選択用のアプリケーションオブジェクトを選択します。

注:

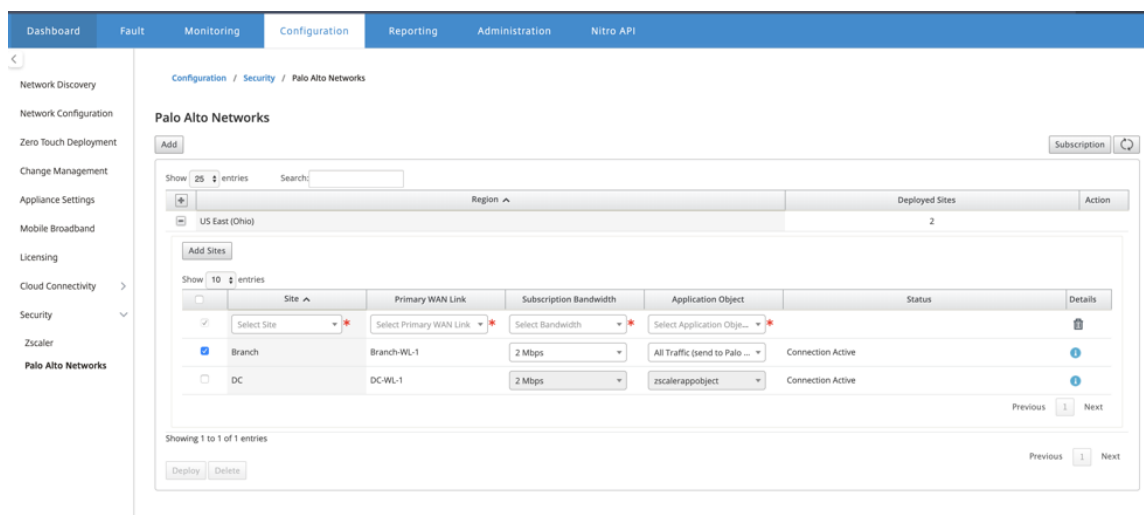
選択した帯域幅が使用可能な帯域幅の範囲を超えると、トラフィックフローが影響を受けます。

[アプリケーションオブジェクト] の選択の下にある [すべてのトラフィック] オプションを選択すると、インターネットにバインドされたすべてのトラフィックを PRISMA Access サービスにリダイレクトできます。

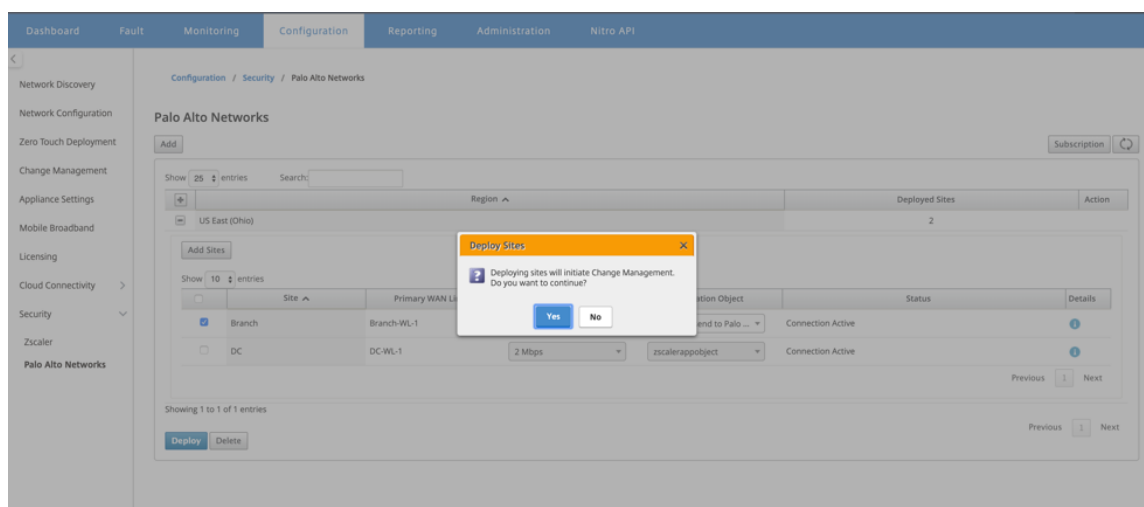




2. 必要に応じて、引き続き SD-WAN ブランチサイトを追加できます。



3. [展開] をクリックします。変更管理プロセスが開始されます。[Yes] をクリックして続行します。



展開後、トンネルの確立に使用される IPsec トンネル構成は次のとおりです。

Palo Alto Site Details

Application Object

Application Object Name: appobject

Match Criteria

Match Type	Application	Application Family	Protocol
application	Office 365 Default(office365_default)	-	-

IPsec Tunnels

panw_service_066318_1

Local IP: 192.168.100.3	Peer IP: 13.52.159.66
MTU: -	Firewall Zone: -
IKE Version: ikev2	DH Group: group2
IKE Hash Algorithm: sha256	IKE Integrity: sha256
IKE Encryption: aes256	IKE Identity: auto
Identity Data: -	IPsec Tunnel Type: esp
PF5 Group: none	IPsec Mismatch Behaviour: drop

ランディングページには、さまざまな SD-WAN リージョンで構成およびグループ化されたすべてのサイトのリストが表示されます。

Dashboard Fault Monitoring **Configuration** Reporting Administration Nitro API

Configuration / Security / Palo Alto Networks

Palo Alto Networks

Add

Subscription

Show 25 entries Search:

Region	Deployed Sites	Action
US East (Ohio)	2	

Add Sites

Show 10 entries

Site	Primary WAN Link	Subscription Bandwidth	Application Object	Status	Details
Branch	Branch-WL-1	2 Mbps	All Traffic (send to Palo ...)	Connection Active	
DC	DC-WL-1	2 Mbps	zscalerappobject	Connection Active	

Showing 1 to 1 of 1 entries

Deploy Delete

Previous 1 Next

エンドツーエンドのトラフィック接続を確認します。

- ブランチの LAN サブネットから、インターネットリソースにアクセスします。
- トラフィックが Citrix SD-WAN IPsec トンネルを通過して Palo Alto Prisma Access に到達することを確認します。
- Palo Alto セキュリティポリシーが [監視] タブのトラフィックに適用されていることを確認します。
- ブランチ内のホストへのインターネットからの応答が通過することを確認します。

ステートフルファイアウォールと **NAT** のサポート

May 10, 2021

この機能は、SD-WAN アプリケーションに組み込まれたファイアウォールを提供します。ファイアウォールは、サービスとゾーン間のポリシーを許可し、スタティック NAT、ダイナミック NAT (PAT)、およびポートフォワーディングによるダイナミック NAT をサポートします。ファイアウォール機能には、次のようなものがあります。

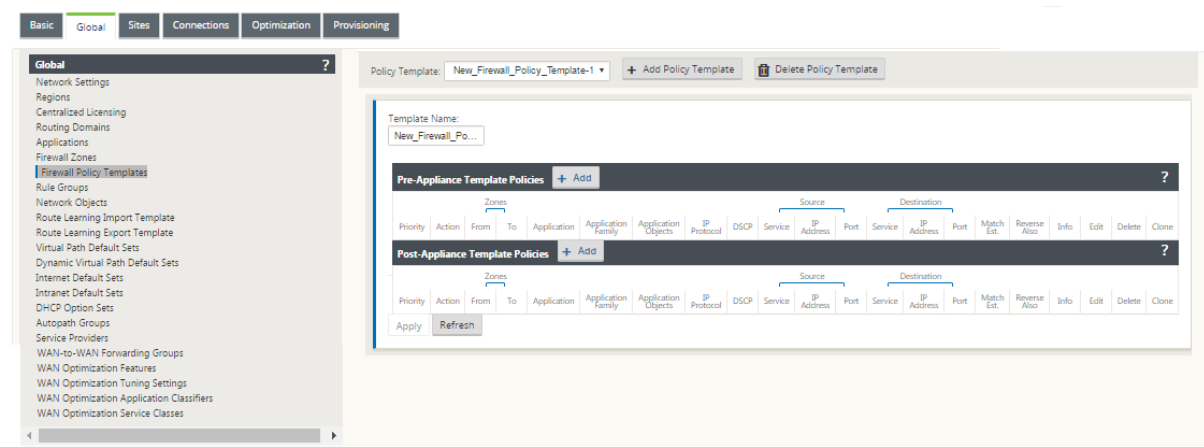
- SD-WAN ネットワーク内のユーザートラフィックのセキュリティを提供 (エンタープライズおよびサービスプロバイダー)
- (可能性) 外部機器の削減 (企業・サービスプロバイダー)
- 複数の顧客に対して同じ IP アドレス空間を使用する:NAT 機能 (サービスプロバイダー)
- グローバルな視点から複数のファイアウォールを適用する (サービスプロバイダ)
- ゾーン間のトラフィックフローのフィルタリング
- ゾーン内のサービス間のトラフィックのフィルタリング
- 異なるゾーンに存在するサービス間のトラフィックのフィルタリング
- サイトのサービス間のトラフィックのフィルタリング
- フローを許可、拒否、または拒否するフィルタポリシーの定義
- 選択したフローのフロー状態の追跡
- グローバルポリシーテンプレートの適用
- 信頼できないポート上のインターネットへのトラフィックに対するポートアドレス変換のサポート、およびポートフォワーディングのインバウンドとアウトバウンドのサポート
- スタティックネットワークアドレス変換 (スタティック NAT) の提供
- ダイナミックネットワークアドレス変換 (ダイナミック NAT) の提供
- ポートアドレス変換 (PAT)
- ポートフォワーディング

構成プロセスを簡素化するために、ファイアウォールポリシーはグローバル構成レベルで作成されます。このグローバル構成は、SD-WAN ネットワーク内のすべてのサイトに適用できる、アプライアンス前およびアプライアンス後のサイトのポリシーテンプレートで構成されます。

注

セキュリティ上の理由により、Fail-to-Wire インラインモードでファイアウォールを使用することは推奨されません。

グローバルポリシーテンプレート



事前ポリシーテンプレート

Priority:

From Zones

Zone	Enable
Any	<input checked="" type="checkbox"/>
Default_LAN_Zone	<input type="checkbox"/>
Internet_Zone	<input type="checkbox"/>
Untrusted_Internet_Zone	<input type="checkbox"/>

To Zones

Zone	Enable
Any	<input checked="" type="checkbox"/>
Default_LAN_Zone	<input type="checkbox"/>
Internet_Zone	<input type="checkbox"/>
Untrusted_Internet_Zone	<input type="checkbox"/>

Action: Log Interval (s): ☐ Log Start ☐ Log End Connection State Tracking:

Match Type: Application Objects: Application: Application Family:

IP Protocol: DSCP: ☒ Allow Fragments ☐ Reverse Also ☐ Match Established

Source Service Type: Source Service Name: Source IP: Source Port:

Dest Service Type: Dest Service Name: Dest IP: Dest Port:

ポストポリシーテンプレート

?

×

Add

Priority:

100

From Zones

Zone	Enable
Any	<input checked="" type="checkbox"/>
Default_LAN_Zone	<input type="checkbox"/>
Internet_Zone	<input type="checkbox"/>
Untrusted_Internet_Zone	<input type="checkbox"/>

To Zones

Zone	Enable
Any	<input checked="" type="checkbox"/>
Default_LAN_Zone	<input type="checkbox"/>
Internet_Zone	<input type="checkbox"/>
Untrusted_Internet_Zone	<input type="checkbox"/>

Action:

Allow

Log Interval (s):

0

☐ Log Start

☐ Log End

Connection State Tracking:

Use Site Setting

Match Type:

IP Protocol

Application Objects:

Any

Application:

Application Family:

IP Protocol:

Any

DSCP:

Any

☒ Allow Fragments

☐ Reverse Also

☐ Match Established

Source Service Type:

Any

Source Service Name:

Any

Source IP:

*

Source Port:

*

Dest Service Type:

Any

Dest Service Name:

Any

Dest IP:

*

Dest Port:

*

Add

Cancel

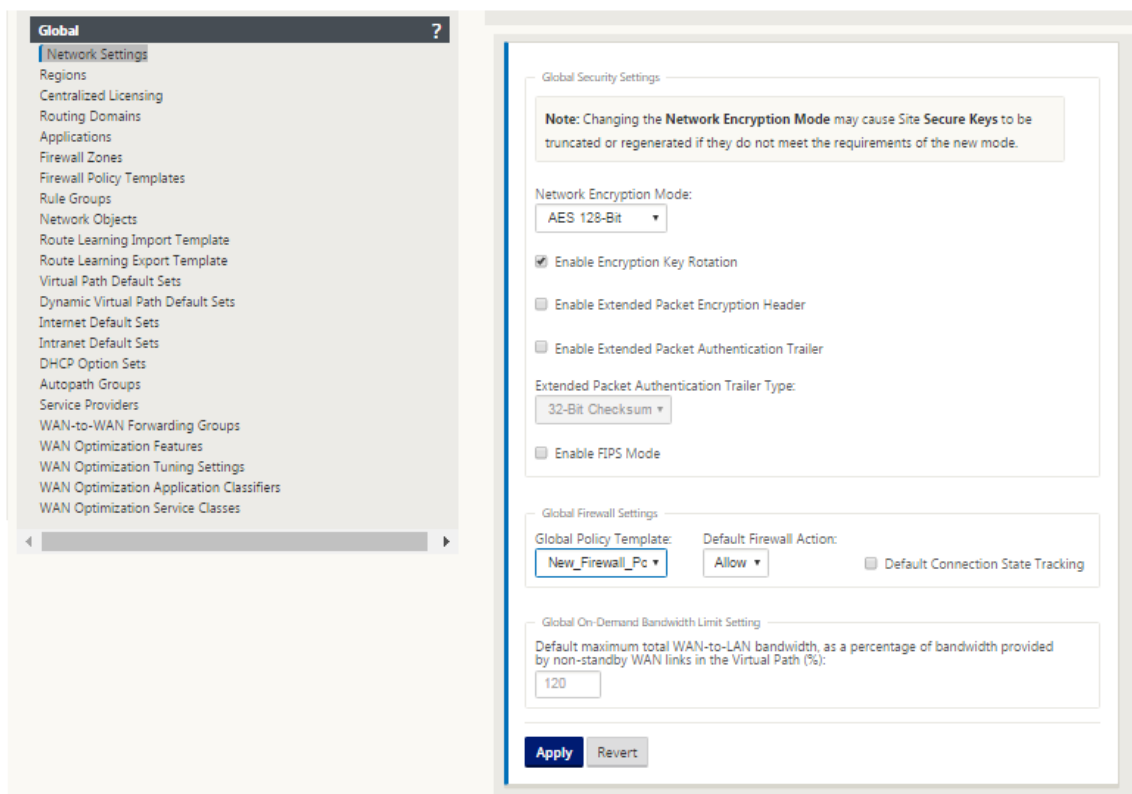
グローバルファイアウォールの設定

May 10, 2021

ファイアウォールポリシーテンプレートを作成したら、このポリシーを使用して NetScaler SD-WAN ネットワークのファイアウォール設定を構成できます。グローバルファイアウォール設定を使用すると、グローバルファイアウォールパラメータを構成できます。これらの設定は仮想 WAN ネットワーク上のすべてのサイトに適用されます。

グローバルファイアウォール設定を構成するには、次の手順を実行します。

1. 構成エディタで、[グローバル] > [ネットワーク設定] に移動し、編集アイコンをクリックします。



2. [グローバルファイアウォール設定] セクションで、次のオプションの値を選択します。

- グローバルポリシーテンプレート -SD-WAN ネットワーク内のすべてのアプライアンスに適用するファイアウォールポリシーテンプレートの選択、デフォルトのファイアウォールアクション-フィルタポリシーに一致しないパケットを許可するには、[Allow] を選択します。フィルタポリシーに一致しないパケットをドロップするには、[Drop, **Default Connection State Tracking**] を選択します。これにより、フィルタポリシーまたは NAT 規則に一致しない TCP、UDP、および ICMP フローに対して、方向接続状態追跡が有効になります。これにより、ファイアウォールポリシーが定義されていない場合でも、非対称フローがブロックされます。

3. [適用] をクリックします。

注

これらの設定をサイトレベルで構成することもできます。この設定は、グローバル設定よりも優先されます。

ファイアウォールの詳細設定

May 10, 2021

ファイアウォールの詳細設定は、サイトごとに個別に構成できます。これにより、グローバル設定が上書きされません。

ファイアウォールの詳細設定を構成するには

1. 構成エディタで、[接続] > [サイトの表示] > [ファイアウォール] > [設定] に移動します。

2. [ポリシーテンプレート] セクションで、[追加] をクリックします。次のパラメータの値を入力します。

- 優先度 -ポリシーがサイトに適用される順序。
- 名前: サイトで使用するポリシーテンプレートの名前。

3. [詳細設定] をクリックします。次のパラメーターの値を入力します。

- デフォルトのファイアウォール操作 -次のいずれかのオプションを選択します。
 - グローバル設定の使用 -NetScaler SD-WAN 設定で構成されたグローバル設定を使用します。
 - **Allow**-どのフィルタポリシーにも一致しないパケットも許可されます。
 - **Drop**: どのフィルタポリシーにも一致しないパケットはドロップされます。
- 「デフォルトの接続状態の追跡」 -次のいずれかのオプションを選択します。
 - グローバル設定の使用 -NetScaler SD-WAN 設定で構成されたグローバル設定を使用します。
 - **No Tracking**: 双方向接続状態追跡は、どのフィルタポリシーにも一致しないパケットでは実行されません。

- **Track** -双方向接続状態追跡は、どのフィルタポリシーまたは NAT 規則にも一致しない TCP、UDP、および ICMP パケットに対して実行されます。これにより、ファイアウォールポリシーが定義されていない場合でも、非対称フローがブロックされます。

- **Source Route Validation:** 有効にすると、送信元 IP アドレスによって決定される、パケットのルートとは異なるインターフェイスで受信したときにパケットがドロップされます。パケットが現在一致しているルートだけが考慮されます。
- **ソースごとの最大新規接続数:** ソース IP アドレスごとに許可される未確立接続の最大数。0 は無制限を意味します。この設定を使用して、ファイアウォールに対するサービス拒否攻撃を防止します。
- **ソースあたりの最大接続数:** ソース IP アドレスごとに許可される接続の最大数。0 は無制限を意味します。この設定を使用して、ファイアウォールに対するサービス拒否攻撃を防止します。

4. さまざまなタイムアウト設定を構成し、[**Apply**] をクリックします。

ゾーン

May 10, 2021

ネットワーク内のゾーンを構成し、トラフィックがゾーンに出入りする方法を制御するポリシーを定義できます。デフォルトでは、次のゾーンが作成されます。

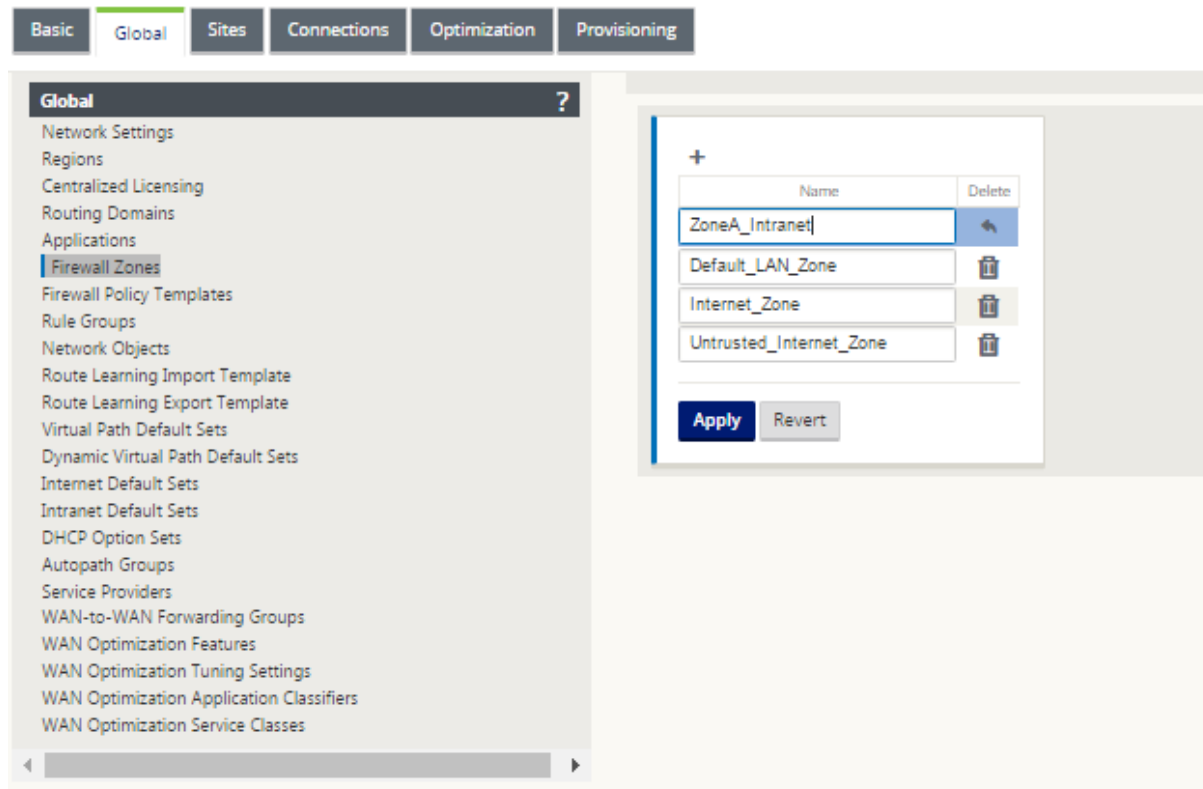
- **Zone**
 - 信頼されたインターフェイスを使用するインターネットサービスとの間で送受信されるトラフィックに適用されます。
- **Untrusted_Internet_Zone**
 - 信頼できないインターフェイスを使用するインターネットサービスとの間で送受信されるトラフィックに適用されます。
- **Default_LAN_Zone**
 - ゾーンが設定されていない設定可能なゾーンを持つオブジェクトへのトラフィックまたはオブジェクトからのトラフィックに適用されます。

独自のゾーンを作成し、次のタイプのオブジェクトに割り当てることができます。

- 仮想ネットワークインターフェイス (VNI)
- イントラネットサービス
- GRE トンネル

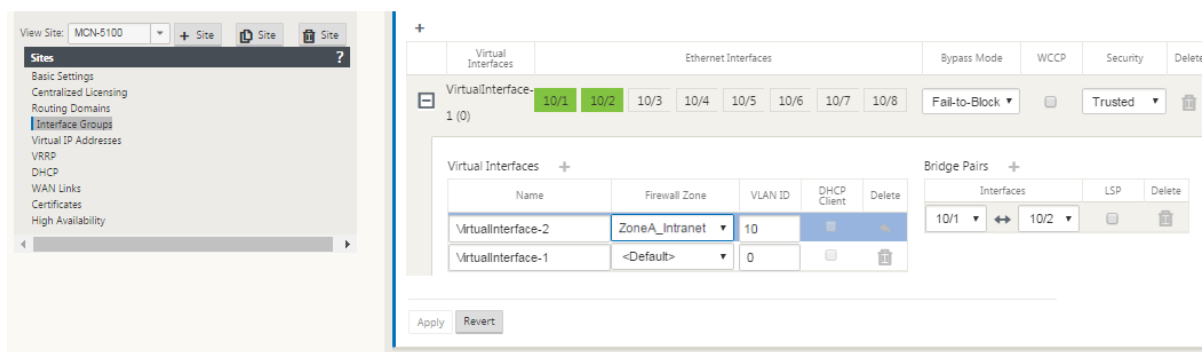
- LAN IPsec トンネル

次の図に、事前構成された 3 つのゾーンを示します。さらに、必要に応じて独自のゾーンを作成することもできます。この例では、ゾーン「zonea_ イントラネット」はユーザーが作成したゾーンです。SD-WAN アプライアンスのバイパスセグメント（ポート 1 および 2）の仮想インターフェイスに割り当てられます。



パケットの送信元ゾーンは、パケットが受信されるサービスまたは仮想ネットワークインターフェイスによって決まります。ただし、仮想パストラフィックは例外です。トラフィックが仮想パスに入ると、パケットはトラフィックを発信したゾーンでマークされ、その送信元ゾーンは仮想パスを介して伝送されます。これにより、仮想パスの受信側は、元のソースゾーンが仮想パスに入る前にポリシーを決定できます。

たとえば、ネットワーク管理者は、サイト A の VLAN 30 からのトラフィックだけがサイト B で VLAN 10 に入るようにポリシーを定義することができます。管理者は、各 VLAN にゾーンを割り当てて、これらのゾーン間のトラフィックを許可し、他のゾーンからのトラフィックをブロックするポリシーを作成できます。次のスクリーンショットは、ユーザーが「zonea_ イントラネット」ゾーンを VLAN 10 に割り当てる方法を示しています。この例では、「ZoneA_ イントラネット」ゾーンは、仮想インターフェイス「VirtualInterface2」に割り当てるためにユーザーによって事前に定義されています。



パケットの宛先ゾーンは、宛先ルートの一致に基づいて決定されます。SD-WAN アプライアンスがルートテーブルで宛先サブネットを検索すると、パケットはルートと一致します。ルートにはゾーンが割り当てられています。

- ソースゾーン

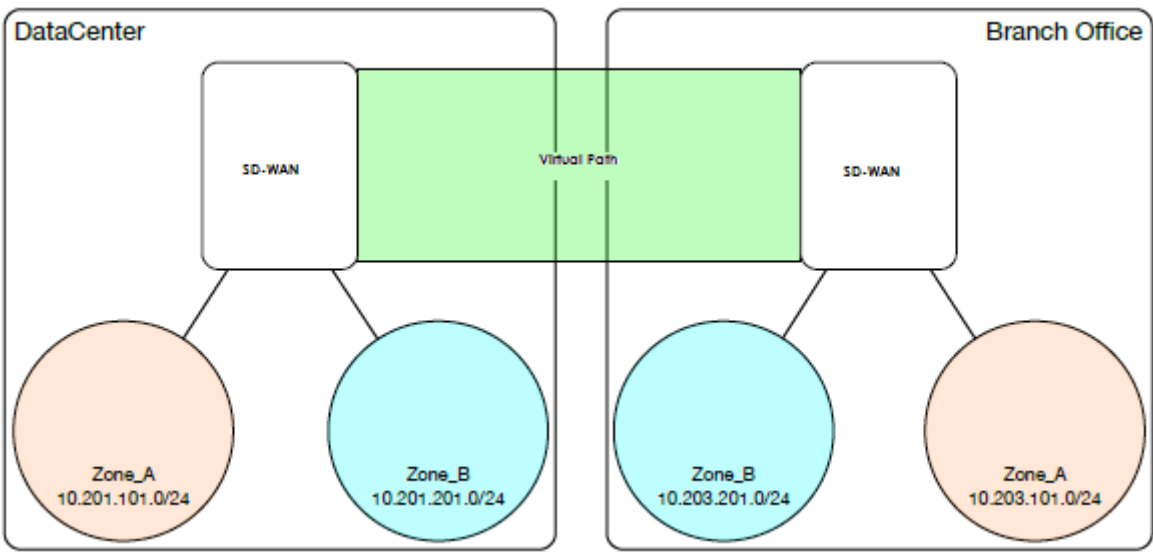
- 非仮想パス：で受信した仮想ネットワークインターフェイスパケットを介して決定されます。
- 仮想パス：パケットフローヘッダーのソースゾーンフィールドを介して決定されます。
- 仮想ネットワークインターフェイス-送信元サイトでパケットを受信しました。

- 宛先ゾーン

- パケットの宛先ルート検索により決定。

SD-WAN 内のリモートサイトと共有されるルートは、ダイナミックルーティングプロトコル（BGP、OSPF）を通じて学習されたルートなど、宛先ゾーンに関する情報を保持します。このメカニズムを使用すると、ゾーンは SD-WAN ネットワークでグローバルな重要性を獲得し、ネットワーク内でエンドツーエンドのフィルタリングを可能にします。ゾーンを使用すると、ネットワーク管理者は、顧客、事業部門、または部門に基づいてネットワークトラフィックを効率的にセグメント化できます。

SD-WAN ファイアウォールの機能を使用すると、次の図に示すように、1 つのゾーン内のサービス間のトラフィックをフィルタリングしたり、異なるゾーン内のサービス間で適用できるポリシーを作成したりできます。以下の例では、Zone_A と Zone_B があり、それぞれに LAN 仮想ネットワークインターフェイスがあります。



下のスクリーンショットは、割り当てられた仮想ネットワークインターフェイス（VNI）からの仮想 IP（VIP）のゾーンの継承を示しています。

IP Address / Prefix	Virtual Interface	Firewall Zone	Identity	Private	Security	Delete
172.16.187.11/24	VirtualInterface-1	Default_LAN_Zone	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Trusted	
172.16.187.12/24	VirtualInterface-1	Default_LAN_Zone	<input type="checkbox"/>	<input type="checkbox"/>	Trusted	

ポリシー

May 10, 2021

ポリシーを使用すると、特定のトラフィックフローの許可、拒否、またはカウントおよび継続を行うことができます。SD-WAN ネットワークが拡大するにつれて、これらのポリシーを各サイトに個別に適用することは困難になります。この問題を解決するには、ファイアウォールポリシーテンプレートを使用してファイアウォールフィルターのグループを作成できます。ファイアウォールポリシーテンプレートは、ネットワーク内のすべてのサイトに適用することも、特定のサイトにのみ適用することもできます。これらのポリシーは、アプライアンス前のテンプレート・ポリシーまたはアプライアンス後のテンプレート・ポリシーとして順序付けられます。ネットワーク全体のアプライアンス前およびアプライアンス後のテンプレート・ポリシーは、どちらもグローバル・レベルで構成されます。ローカルポリシーは、[接続] の下のサイトレベルで構成され、その特定のサイトにのみ適用されます。

Pre-Appliance Template Policies

Template	Routing Domain	Action	Zones		Application	Application Family	Application Objects	Source			Destination			IP Address	Port
			From	To				IP Protocol	DSCP	Service	IP Address	Port	Service		

Local Policies

+ Add

Priority	Routing Domain	Action	Zones		Application	Application Family	Application Objects	Source			Destination			IP Address	Port
			From	To				IP Protocol	DSCP	Service	IP Address	Port	Service		

Post-Appliance Template Policies

Template	Routing Domain	Action	Zones		Application	Application Family	Application Objects	Source			Destination			IP Address	Port
			From	To				IP Protocol	DSCP	Service	IP Address	Port	Service		

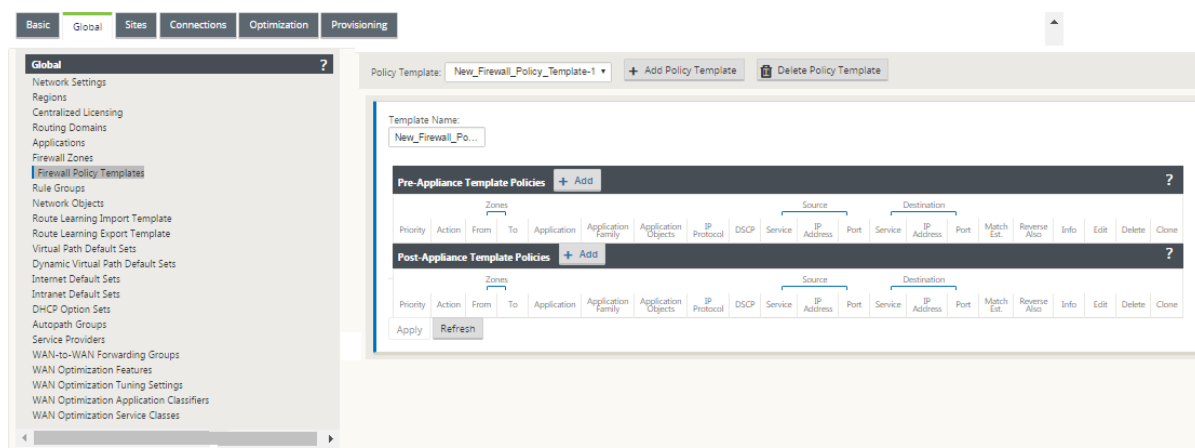
アプライアンスの前テンプレートポリシーは、ローカルサイトポリシーの前に適用されます。次に、ローカルサイトポリシーが適用されます。次に、アプライアンスポストテンプレートポリシーが適用されます。目標は、サイト固有のポリシーを適用する柔軟性を維持しながら、グローバルポリシーを適用できるようにすることで、構成プロセスを簡素化することです。

フィルタポリシー評価順序

- 1. Pre-templates –すべてのテンプレート「PRE」セクションからコンパイルされたポリシー。
- 2. Pre-Global –グローバル「PRE」セクションからコンパイルされたポリシー。
- 3. Local: アプライアンスレベルのポリシー。
- 4. [ローカル自動生成]: 自動的にローカルに生成されたポリシー。
- 5. ポストテンプレート–すべてのテンプレート「POST」セクションからコンパイルされたポリシー。
- 6. ポストグローバル–グローバル「POST」セクションからコンパイルされたポリシー。

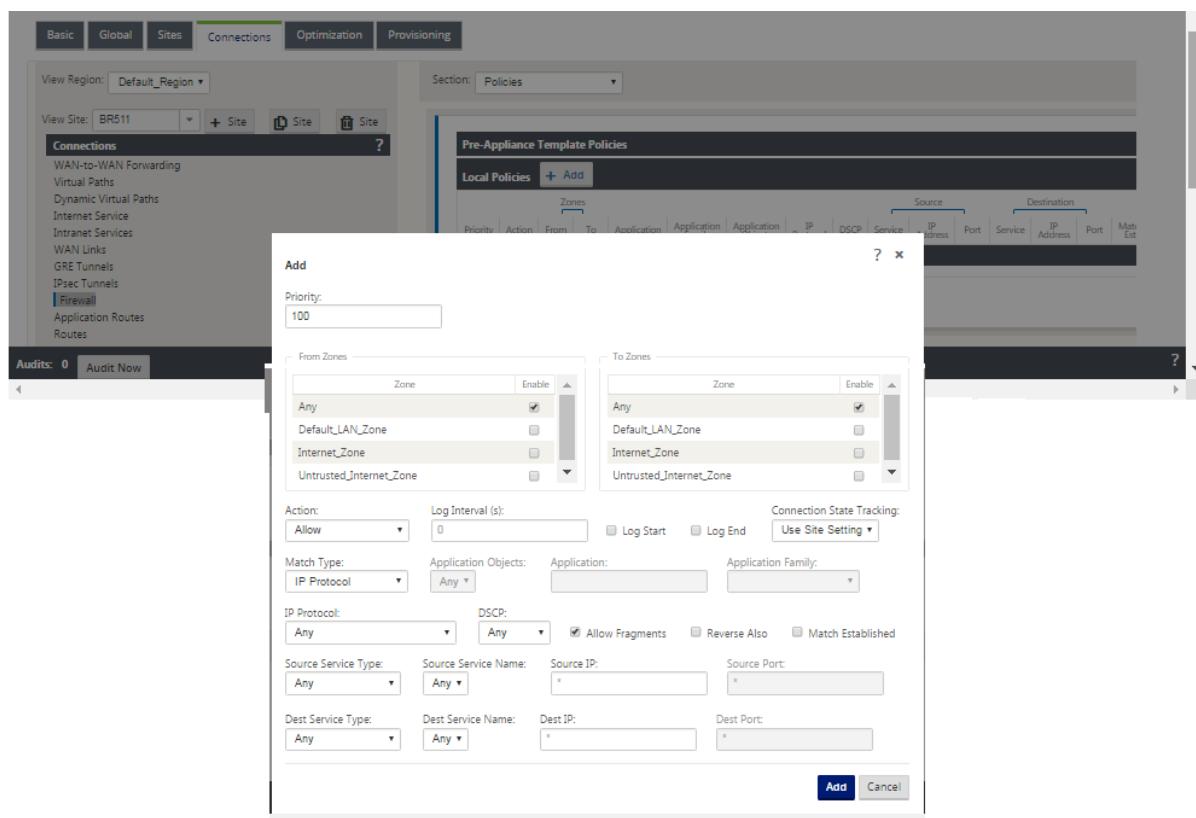
ポリシー定義-グローバルおよびローカル (サイト)

アプライアンス前およびアプライアンス後のテンプレート・ポリシーは、グローバル・レベルで構成できます。ローカルポリシーは、アプライアンスのサイトレベルで適用されます。



上のスクリーンショットは、SD-WAN ネットワークにグローバルに適用されるポリシーテンプレートを示しています。ネットワーク内のすべてのサイトにテンプレートを適用するには、[グローバル]>[ネットワーク設定]>[グローバルポリシーテンプレート]に移動し、特定のポリシーを選択します。サイトレベルでは、ポリシーテンプレートを追加したり、サイト固有のポリシーを作成できます。

ポリシーの特定の設定可能な属性は、以下のスクリーンショットに表示されます。これらの属性は、すべてのポリシーで同じです。



ポリシー属性

- **Priority** : 定義されたすべてのポリシー内でポリシーが適用される順序。優先順位の低いポリシーは、優先順位の高いポリシーの前に適用されます。
- **Zone** : フローには送信元ゾーンと宛先ゾーンがあります。
 - **[From Zone]**: ポリシーの送信元ゾーン。
 - **[宛先 Zone]**: ポリシーの宛先ゾーン。
- **[Action]**: 一致したフローに対して実行するアクション。
 - **Allow**: ファイアウォールを通過するフローを許可します。
 - **[Drop]**: パケットをドロップすることにより、ファイアウォールを通過するフローを拒否します。
 - **Reject**: ファイアウォールを通過するフローを拒否し、プロトコル固有の応答を送信します。TCP はリセットを送信し、ICMP はエラーメッセージを送信します。
 - **Count and Continue** : このフローのパケット数とバイト数をカウントしてから、ポリシーリストを続けます。
- **Log Interval** : ポリシーに一致するパケットの数をファイアウォールログファイルまたは syslog サーバに記録する間隔 (設定されている場合)。
 - **[Log Start]**: 選択すると、新しいフローのログエントリが作成されます。
 - **Log End** : フローが削除されたときに、フローのデータをログに記録します。

注

デフォルトの Log Interval の値である 0 は、ロギングがないことを意味します。

- **[Track]**: ファイアウォールがフローの状態を追跡し、この情報を **[Monitoring]** > **[Firewall]** > **[Connections]** テーブルに表示できるようにします。フローがトラッキングされていない場合、状態は NOT_TRACKED と表示されます。以下のプロトコルに基づく状態追跡については、表を参照してください。[ファイアウォール] > [設定] > [詳細設定] > [既定の追跡] でサイトレベルで定義された設定を使用します。
 - **No Track** : フロー状態が有効になっていません。
 - **[Track]** : (このポリシーに一致した) フローの現在の状態を表示します。
- 「一致タイプ」 (Match Type)-次のいずれかの一致タイプを選択します。
 - **[IP プロトコル]**: この一致タイプを選択した場合、フィルタが照合する IP プロトコルを選択します。オプションには、任意、TCP、UDP ICMP などがあります。
 - **[アプリケーション]** : この一致タイプを選択した場合は、このフィルタの一致基準として使用するアプリケーションを指定します。

- 「アプリケーションファミリー」 - この一致タイプを選択した場合は、このフィルタの一致基準として使用するアプリケーションファミリーを選択します。
- 「アプリケーション・オブジェクト」 - この一致タイプを選択した場合は、このフィルタの一致基準として使用するアプリケーション・ファミリーを選択します。

アプリケーション、アプリケーションファミリー、およびアプリケーションオブジェクトの詳細については、「[アプリケーション分類](#)」を参照してください。

- **DSCP** : ユーザが DSCP タグ設定を照合できるようにします。
- フラグメントを許可: このフィルタポリシーに一致する IP フラグメントを許可します。

注

ファイアウォールは、断片化されたフレームを再構成しません。

- **Reverse AtoH**: ソースとデスティネーションの設定を逆にしたこのフィルタポリシーのコピーを自動的に追加します。
- **Match 確立済み**: 発信パケットが許可された接続の着信パケットを照合します。
- ソースサービスタイプ-SD-WAN サービスを参照して、ローカル（アプライアンス）、仮想パス、イントラネット、IPHost、またはインターネットがサービスタイプの例です。
- **IPHost** オプション -ファイアウォールの新しいサービスタイプで、SD-WAN アプリケーションによって生成されるパケットに使用されます。たとえば、SD-WAN の Web UI から ping を実行すると、SD-WAN 仮想 IP アドレスからパケットが送信されます。この IP アドレスのポリシーを作成する場合、ユーザーは IPHost オプションを選択する必要があります。
- ソース・サービス名: サービス・タイプに関連付けられたサービスの名前。たとえば、「ソース・サービス・タイプ」で仮想パスが選択されている場合、これは特定の仮想パスの名前になります。これは必ずしも必要ではなく、選択したサービスタイプによって異なります。
- 送信元 **IP** アドレス-フィルタが照合に使用する一般的な IP アドレスとサブネットマスク。
- **Source Port** : 特定のアプリケーションが使用するソース・ポート。
- デスティネーション・サービス・タイプ -SD-WAN サービスに関するサービス-ローカル（アプライアンス）、仮想パス、イントラネット、IPHost、またはインターネットがサービスタイプの例です。
- 宛先サービス名: サービス・タイプに関連付けられたサービスの名前。これは必ずしも必要ではなく、選択したサービスタイプによって異なります。
- 宛先 **IP** アドレス -フィルタが照合に使用する一般的な IP アドレスとサブネットマスク。
- 宛先ポート-特定のアプリケーションが使用する宛先ポート (TCP プロトコル用の HTTP 宛先ポート 80)。

track オプションは、フローの詳細を提供します。状態テーブルで追跡される状態情報を以下に示します。

トラッキングオプションのステートテーブル

一貫性のある状態は、ごくわずかです。

- **INIT-** 接続が作成されましたが、最初のパケットは無効です。
- **O_DENIED-** 接続を作成したパケットは、フィルタポリシーによって拒否されます。
- **R_DENIED-** 応答側からのパケットは、フィルタポリシーによって拒否されます。
- **NOT_TRACKED-** 接続はステートフルに追跡されませんが、それ以外の場合は許可されます。
- **CLOSED-** 接続がタイムアウトしたか、プロトコルによって閉じられました。
- **DELETED-** 接続は削除中です。DELETED 状態はほとんど見られません。

その他の状態はすべてプロトコル固有であり、ステートフルトラッキングを有効にする必要があります。

TCP は、次の状態を報告できます。

- **SYN_SENT** -最初の TCP SYN メッセージが表示されます。
- **SYN_SENT2** -双方向で認識される SYN メッセージ。SYN+ACK なし（別名同時オープン）。
- **SYN_ACK_RCVD** -SYN+ACK を受信しました。
- **ESTABLISHED** - 2 番目の ACK を受信し、接続は完全に確立されています。
- **FIN_WAIT** - 最初に見られた FIN メッセージ。
- **CLOSE_WAIT** -両方向に表示される FIN メッセージ。
- **TIME_WAIT** -両方向で最後に確認された ACK。接続は再度開くのを待って閉じられました。

その他すべての IP プロトコル（特に ICMP および UDP）には、次の状態があります。

- **NEW** -一方向で表示されるパケット。
- 確立 済み-両方向で認識されるパケット。

ネットワークアドレス変換 (NAT)

May 10, 2021

ネットワークアドレス変換 (NAT) は、IP アドレスの保存を実行して、登録された IPv4 アドレスの限られた数を維持します。これにより、未登録の IP アドレスを使用するプライベート IP ネットワークがインターネットに接続できるようになります。Citrix SD-WAN の NAT 機能は、プライベート SD-WAN ネットワークをパブリックインターネットに接続します。内部ネットワーク内のプライベートアドレスを、合法的なパブリックアドレスに変換します。また、NAT は、ネットワーク全体のアドレスを 1 つだけインターネットにアドバタイズし、内部ネットワーク全体を隠すことで、セキュリティを強化します。Citrix SD-WAN では、次の種類の NAT がサポートされます。

- スタティック 1 対 1 NAT
- ダイナミック NAT (PAT-ポートアドレス変換)
- ポートフォワーディングルールを使用したダイナミック NAT

注

NAT 機能は、サイトレベルでのみ設定できます。NAT のグローバル構成 (テンプレート) はありません。すべての NAT ポリシーは、ソース NAT (「SNAT」) 変換から定義されます。対応する宛先 NAT (「DNAT」) 規則は、ユーザーに対して自動的に作成されます。

静的 NAT

June 8, 2022

スタティック NAT は、SD-WAN ネットワーク内のプライベート IP アドレスまたはサブネットを、SD-WAN ネットワーク外のパブリック IP アドレスまたはサブネットに 1 対 1 のマッピングです。スタティック NAT を設定するには、内部 IP アドレスと変換先の外部 IP アドレスを手動で入力します。スタティック NAT は、ローカル、仮想パス、インターネット、イントラネット、およびルーティング間ドメインサービスに対して構成できます。

インバウンドおよびアウトバウンド NAT

接続の方向は、内側から外側、または外側から内側にできます。NAT ルールが作成されると、方向一致タイプに応じて両方の方向に適用されます。

- **Inbound:** サービスで受信したパケットについて、送信元アドレスが変換されます。宛先アドレスは、サービス上で送信されるパケットに対して変換されます。たとえば、インターネットサービスから LAN サービスへ受信したパケット (インターネットから LAN へ) の場合、送信元 IP アドレスが変換されます。送信されたパケット (LAN からインターネットへ) では、宛先 IP アドレスが変換されます。
- **Outbound:** サービスで受信したパケットについて、宛先アドレスが変換されます。送信元アドレスは、サービス上で送信されるパケットに対して変換されます。たとえば、LAN サービスからインターネットサービスへ送信されたパケット (LAN からインターネット) の場合、送信元 IP アドレスが変換されます。受信パケット (インターネットから LAN へ) の場合、宛先 IP アドレスが変換されます。

ゾーン派生

インバウンドまたはアウトバウンドトラフィックの送信元および宛先ファイアウォールゾーンは、同じであってはいません。送信元と宛先の両方のファイアウォールゾーンが同じ場合、トラフィックに対して NAT は実行されません。

発信 NAT の場合、外部ゾーンはサービスから自動的に派生します。デフォルトでは、SD-WAN 上のすべてのサービスがゾーンに関連付けられます。たとえば、信頼できるインターネットリンク上のインターネットサービスは、信頼できるインターネットゾーンに関連付けられています。同様に、着信 NAT の場合、内部ゾーンはサービスから取得されます。

仮想パスサービスの場合、NAT ゾーンの導出が自動的に行われられないため、内部ゾーンと外部ゾーンを手動で入力する必要があります。NAT は、これらのゾーンに属するトラフィックに対してのみ実行されます。仮想パスのサブネット内に複数のゾーンが存在する可能性があるため、仮想パスのゾーンは派生できません。

スタティック NAT ポリシーの設定

スタティック NAT ポリシーを設定するには、設定エディタで、[接続] > [ファイアウォール] > [スタティック NAT ポリシー] に移動します。

Static NAT Policy configuration window showing the following settings:

- Priority: 100
- Direction: Outbound
- Service Type: Internet
- Service Name: Internet
- Inside Zone: Default_LAN_Zo
- Inside IP Address: 172.57.79.179/32
- Outside IP Address: 172.57.52.174/32
- Bind Responder Route: ☐
- Proxy ARP: ☐

- **Priority:** 定義されたすべてのポリシー内でポリシーが適用される順序。優先順位の低いポリシーは、優先順位の高いポリシーの前に適用されます。
- **方向:** 仮想インターフェイスまたはサービスから見たトラフィックが流れている方向。インバウンドトラフィックまたはアウトバウンドトラフィックのいずれかになります。
- **サービスタイプ:** NAT ポリシーが適用される SD-WAN サービスタイプ。スタティック NAT の場合、サポートされるサービスの種類は、ローカル、仮想パス、インターネット、イントラネット、およびインタールーティングドメインサービスです。
- **サービス名:** サービスタイプに対応する構成済みのサービス名を選択します。
- **Inside Zone:** 変換を許可するために、パケットの送信元となる必要がある内部ファイアウォールゾーンのマッチタイプ。
- **Outside Zone:** 変換を許可するために、パケットの送信元となる必要がある外部ファイアウォールゾーンのマッチタイプ。
- **内部 IP アドレス:** 一致基準が満たされた場合に変換する必要がある内部 IP アドレスおよびプレフィクス。
- **外部 IP アドレス:** 一致基準が満たされた場合に内部 IP アドレスが変換される外部 IP アドレスおよびプレフィクス。
- **レスポンスルートのバインド:** 非対称ルーティングを回避するために、応答トラフィックが受信されたのと同じサービスを介して送信されるようにします。

- プロキシ **ARP**: アプライアンスが外部 IP アドレスに対するローカル ARP 要求に応答することを保証します。

IPv6 インターネットサービスのスタティック NAT ポリシー

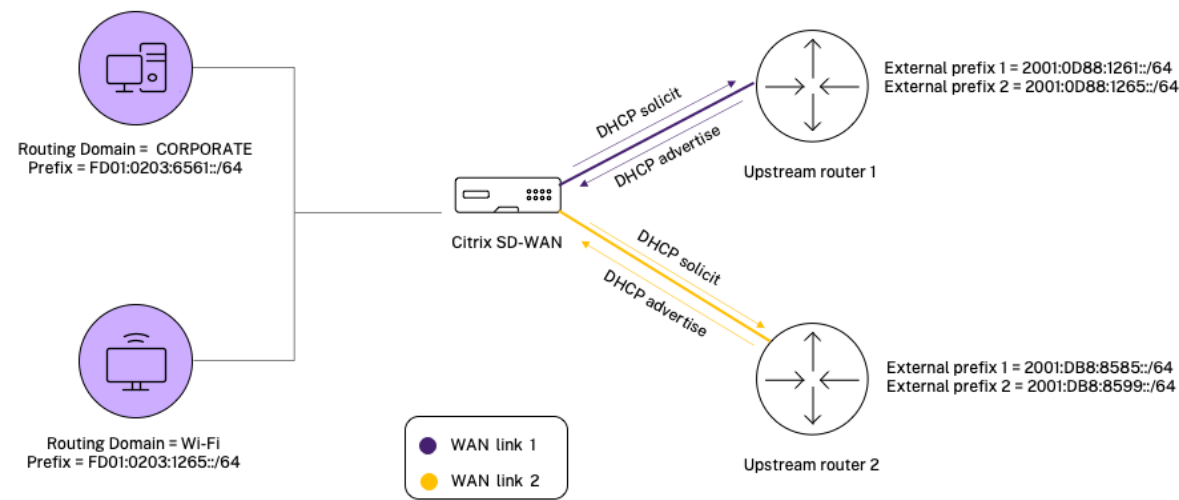
Citrix SD-WAN は、リリース 11.4.0 以降の IPv6 インターネットサービスの静的 NAT ポリシーをサポートします。IPv6 インターネットサービスのスタティック NAT ポリシーは、内部ネットワークプレフィックスと外部ネットワークプレフィックスのマッピングを指定します。必要なスタティック NAT ポリシーの数は、内部ネットワークの数と外部ネットワーク（WAN リンク）の数によって異なります。**M** 個の内部ネットワークと **N** 個の **WAN** リンクがある場合、必要なスタティック NAT ポリシーの数は **M x N** です。

Citrix SD-WAN リリース 11.4.0 以降では、静的 NAT ポリシーの作成中に、外部 IP アドレスを手動で入力するか、**PD** 経由で自動学習を有効にすることができます。**PD** による自動学習が有効になっている場合、Citrix SD-WAN アプライアンスは、DHCPv6 プレフィックス委任を介して上流の委任ルーターから委任されたプレフィックスを受信します。Citrix SD-WAN リリース 11.4.0 より前は、外部 IP アドレスはサービスから自動的に取得され、外部 IP アドレスを手動で入力するオプションはありませんでした。アプライアンスを 11.4.0 以降のリリースにアップグレードし、IPv6 インターネットサービス用にスタティック NAT ポリシーが設定されている場合は、ポリシーを手動で更新する必要があります。

設定例

次のトポロジでは、Citrix SD-WAN アプライアンスは 2 つの内部ネットワークと 2 つの WAN リンクで構成されます。

- 内部ネットワーク 1 は、ネットワークプレフィックス FD の企業ルーティングドメインに存在します 01:0203:6561::/64
- 内部ネットワーク 2 は、ネットワークプレフィックス FD を持つ Wi-Fi ルーティングドメインに存在します 01:0203:1265::/64
- SD-WAN アプライアンスは、WAN リンク 1 を介して DHCPv6 プレフィックス委任、2 つの委任プレフィックス 2001:0 D 88:1261::/64 および 2001:0 D 88:1265::/64 を介してアップストリーム委任ルータから受信します。これら 2 つの委任プレフィックスは、内部ネットワークからのトラフィックが WAN リンク 1 を通過するときに、外部ネットワークプレフィックスとして使用されます。
- WAN リンク 2 を介して、SD-WAN アプライアンスは DHCPv6 プレフィックス委任を介してアップストリーム委任ルータから、2 つの委任プレフィックス 2001: DB 8:8585::/64 および 2001: DB 8:8599::/64 を受信します。これら 2 つの委任プレフィックスは、内部ネットワークからのトラフィックが WAN リンク 2 を通過するときに、外部ネットワークプレフィックスとして使用されます。



このシナリオでは、M=2 内部ネットワークと N=2 WAN リンクがあります。したがって、IPv6 インターネットサービスの適切な展開に必要なスタティック NAT ポリシーの数は $2 \times 2 = 4$ です。次の 4 つのスタティック NAT ポリシーは、次のアドレス変換を指定します。

- 内部ネットワーク 1 から WAN リンク 1 経由
- 内部ネットワーク 1 から WAN リンク 2
- 内部ネットワーク 2 から WAN リンク 1 経由
- 内部ネットワーク 2 から WAN リンク 2 経由

これらのスタティック NAT ポリシーを設定するには、設定エディタで、[接続] > [ファイアウォール] > [スタティック NAT ポリシー] に移動します。

Section: Static NAT Policies

+

Priority	Routing Domain	Direction	Service	Inside Zone	Inside IP Address	Outside Zone	Outside IP Address	Edit	Delete	Clone
100	CORPORATE	Outbound	Internet	*	FD01:0203:6561::/64	Untrusted_Internet_Zone				
200	CORPORATE	Outbound	Internet	*	FD01:0203:6561::/64	Untrusted_Internet_Zone				
300	WIFI	Outbound	Internet	*	FD01:0203:1265::/64	Untrusted_Internet_Zone				
400	WIFI	Outbound	Internet	*	FD01:0203:1265::/64	Untrusted_Internet_Zone				

Apply Refresh

NAT ポリシーを作成する際は、[サービスタイプ] を [** インターネット]、[IP アドレスタイプ **] を [IPv6] として選択してください。WAN リンクを選択し、[内部 IP Address] フィールドに、内部ネットワークプレフィックスを入力します (/64 プレフィックスだけが許可されます)。[外部 IP アドレス (Outside IP Address)] フィールドには、

外部ネットワークプレフィックスを手動で入力するか、[PD 経由で自動学ぶ (**AutoLearn via PD**)] チェックボックスをオンにします。

次に、外部 IP アドレスがスタティック NAT ポリシーに手動で入力される例を示します。

Priority: <input type="text" value="100"/>	Routing Domain <input type="text" value="CORPORATE"/>		
Direction: <input type="text" value="Outbound"/>	Service Type: <input type="text" value="Internet"/>	Service Name: <input type="text" value="Internet"/>	WAN Link: <input type="text" value="O365t1-WL-1"/>
Inside Zone: <input type="text" value="<Any>"/>	IP Address Type: <input type="text" value="IPv6"/>	Inside IP Address: <input "="" type="text" value="FD01:0203:6561:..."/>	
Outside IP Address: <input type="text" value="2001:0D88:1265::/6"/>	<input type="checkbox"/> AutoLearn via PD		
<input checked="" type="checkbox"/> Bind Responder Route <input type="checkbox"/> Proxy ARP/NDP <input checked="" type="checkbox"/> Allow Related			
			<input type="button" value="Apply"/> <input type="button" value="Cancel"/>

[PD 経由の自動学習 (**AutoLearn via PD**)] チェックボックスをオンにする場合は、アップストリームルータが DHCPv6 プレフィックス委任をサポートしていることを確認します。Citrix SD-WAN はアップストリーム委任ルーターからプレフィックスを要求し、委任ルーターは Citrix SD-WAN にプレフィックスで応答します。Citrix SD-WAN は、この委任プレフィックスを使用して、内部 IP アドレスを外部 IP アドレスに変換します。

次に、**PD** 経由の自動学習が有効になっている例を示します。これにより、DHCPv6 プレフィックス委任によって外部ネットワークプレフィックスが取得されます。

Priority: <input type="text" value="200"/>	Routing Domain <input type="text" value="CORPORATE"/>		
Direction: <input type="text" value="Outbound"/>	Service Type: <input type="text" value="Internet"/>	Service Name: <input type="text" value="Internet"/>	WAN Link: <input type="text" value="O365t1-WL-2"/>
Inside Zone: <input type="text" value="<Any>"/>	IP Address Type: <input type="text" value="IPv6"/>	Inside IP Address: <input "="" type="text" value="FD01:0203:6561:..."/>	
Outside IP Address: <input type="text" value=""/>	<input checked="" type="checkbox"/> AutoLearn via PD		
<input checked="" type="checkbox"/> Bind Responder Route <input type="checkbox"/> Proxy ARP/NDP <input checked="" type="checkbox"/> Allow Related			
			<input type="button" value="Apply"/> <input type="button" value="Cancel"/>

監視

NAT を監視するには、[監視] > [ファイアウォール統計] > [接続] に移動します。接続では、NAT が完了しているかどうかを確認できます。

DashboardMonitoringConfiguration

Monitoring > Firewall

Firewall Statistics

Statistics:ConnectionsMaximum entries to display:50Filtering:Application:AnyFamily:AnyIP Protocol:AnySource Zone:AnyDestination Zone:AnySource Service Type:AnySource Service Instance:AnyDestination Service Type:AnyDestination Service Instance:AnySource IP:Source Port:Destination IP:Destination Port:RefreshClear ConnectionsHelpShow latest dataShow Additional Stats

Connections

Application	Family	IP Protocol	IP Address	Port	Source Service Type	Service Name	Zone	IP Address	Port	Service Type	Service Name	Zone	State	Is NAT	Packets	Bytes	PPS	Mbps	Packets	Bytes	PPS	Mbps	Age (s)
Internet Control Message Protocol(ICMP)	Network Service	ICMP	172.57.79.179	3261	Local	Guest_Ita_id	Default_LAN_Zone	172.57.70.176	3261	Internet	MCN-PA-Internet	Internet_Zone	ESTABLISHED	Yes	6	504	1,004	0.675	6	504	1,004	0.675	6

Connections Displayed: 1Connections In Use: 1/128000

任意の NAT ルールに PD 経由の自動学習が設定されているかどうかを確認するには、[構成] > [仮想 WAN] > [設定の表示] に移動し、[表示] ドロップダウンリストから [ファイアウォール] を選択します。[PD による自動学習] および [PD プレフィックス ID] 列に詳細が表示されます。

Interval (s)	Source Firewall Zone	Source Service Type	Source Service Instance	Source IP Address	Source Port	Source ICMP Type	Source ICMP Code	Destination Firewall Zone	Destination Service Type	Destination Service Instance	Destination IP
0	*	*	*	*	*	*	*	*	*	*	*
*	*	*	*	*	*	*	*	*	*	*	*
*	*	ANY	*	*	*	*	*	*	*	*	*
*	Untrusted_Internet_Zone	INTERNET	*	*	*	*	*	*	*	*	*
*	Untrusted_Internet_Zone	INTERNET	*	*	*	*	*	*	*	*	*
*	*	INTERNET	*	*	*	*	*	*	*	*	*
*	*	*	*	*	*	*	*	*	*	*	*
*	*	*	*	*	*	*	*	*	*	*	*

II WAN Link	Inside Firewall Zone	Inside IP Address	Inside Port	Auto-learn via PD	PD Prefix ID	Outside Firewall Zone	Outside IP Address	Outside Port
034513-0E-1	DC_LAN-Zone_Default	2006::/64	0	Yes	1	Untrusted_Internet_Zone	*	0
*	*	*	0	No	0	Untrusted_Internet_Zone	0.0.0.0/32	0
*	*	*	0	No	0	Untrusted_Internet_Zone	::/128	0
*	*	*	0	No	0	Untrusted_Internet_Zone	/32	0
*	*	*	0	No	0	Untrusted_Internet_Zone	/128	0
*	*	*	53	*	*	9.9.9.9	9.9.9.9	53
*	*	*	53	*	*	149.112.112.112	149.112.112.112	53

内部 IP アドレスと外部 IP アドレスのマッピングをさらに確認するには、[関連オブジェクト] の [ルート後 NAT] をクリックするか、[モニタリング] > [ファイアウォール統計] > [NAT ポリシー] に移動します。

次のスクリーンショットは、IPv4 スタティック NAT ポリシーにおける内部アドレスと外部アドレスのマッピングを示しています。

DashboardMonitoringConfiguration

Monitoring > Firewall

Firewall Statistics

Statistics:NAT PoliciesMaximum entries to display:50NAT:IP Protocol:AnyNAT Type:AnyDynamic NAT Type:AnyService Type:AnyService Name:AnyInside IP:Inside Port:Outside IP:Outside Port:RefreshShow latest dataHelp

NAT Policies

ID	Rule Type	Rule Parent	Direction	IP Protocol	Service Type	Service Name	Inside IP Address	Port	Outside IP Address	Port	Allow Related	Allow IPSec Passthrough	Allow GRE Passthrough	Packets Sent	Bytes Sent	Packets Received	Bytes Received	Connections	Related Objects
1	Static	-	Outbound	*	Internet	-	172.57.79.179/32	*	172.57.52.174/32	*	No	No	No	1971	165564	1635	137340	1	[Connections]

NAT Policies Displayed: 1NAT Policies In Use: 1/1000Port Restricted Dynamic NAT Policies In Use: 0/100Destination NAT Policies In Use: 0/100

次のスクリーンショットは、IPv6 スタティック NAT ポリシーにおける内部アドレスと外部アドレスのマッピングを示しています。

Monitoring > Firewall

Firewall Statistics

Statistics: NAT Policies

Maximum entries to display: 50

NAT: IP Protocol: Any NAT Type: Any Dynamic NAT Type: Any

Service Type: Any Service Name: Any

Inside IP: * Inside Port: * Outside IP: * Outside Port: *

Refresh

Show latest data.

Help

NAT Policies

ID	Rule Type	Rule Parent	Direction	IP Protocol	Service Type	Service Name	Inside		Outside		Allow Related	Allow IPSec Passthrough	Allow GRE Passthrough	Packets Sent	Bytes Sent	Packets Received
							IP Address	Port	IP Address	Port						
1	Static	-	Outbound	*	Internet	-	2006::/64	*	2004::/64	*	Yes	No	No	26	2144	
2	Dynamic PR	-	Outbound	*	Internet	-	*	*	172.170.11.85/32	*	No	No	No	390832	71419346	405
3	Dynamic Sym	-	Outbound	*	Internet	-	*	*	2004::85/128	*	No	No	No	51	4112	

NAT Policies Displayed: 3
NAT Policies In Use: 3/1000
Port Restricted Dynamic NAT Policies In Use: 2/100
Destination NAT Policies In Use: 0/100

ログ

NAT に関連するログは、ファイアウォールログで表示できます。NAT のログを表示するには、NAT ポリシーに一致するファイアウォールポリシーを作成し、ファイアウォールフィルタでロギングが有効になっていることを確認します。NAT ログには次の情報が表示されます。

- 日付と時刻
- ルーティングドメイン
- IP プロトコル
- 送信元ポート
- 送信元 IP アドレス
- 翻訳された IP アドレス
- 翻訳されたポート
- 宛先 IP アドレス
- Destination port

Edit ? x

Priority: Policy Type: **Built-in Firewall**

Match Criteria

From Zones

Zone	Enable
Any	<input checked="" type="checkbox"/>
Default_LAN_Zone	<input type="checkbox"/>
gre_zone	<input type="checkbox"/>
Inter Routing Domain Zone	<input type="checkbox"/>

To Zones

Zone	Enable
Any	<input checked="" type="checkbox"/>
Default_LAN_Zone	<input type="checkbox"/>
gre_zone	<input type="checkbox"/>
Inter Routing Domain Zone	<input type="checkbox"/>

Routing Domain: **Any**

Traffic Match Type: **IP Protocol** IP Protocol: **Any** DSCP: **Any** ☐ Match Established

Application: Application Family: Application Objects: **Any**

Source Service Type: **Any** Source Service Name: **Any** Source IP: Source Port:

Dest Service Type: **Any** Dest Service Name: **Any** Dest IP: Dest Port:

Actions

Action: **Allow** ☒ Allow Fragments Connection State Tracking: **Use Site Setting**

Logging & Other Options

Log Interval (s): ☒ Log Start ☒ Log End ☐ Add Reverse Policy

Apply **Cancel**

NAT ログを生成するには、[ログ/監視] > [ログオプション] に移動し、[**SDWAN_firewall.log**] を選択して [ログの表示] をクリックします。

Dashboard Monitoring **Configuration**

Configuration > Appliance Settings > **Logging/Monitoring**

Log Options Alert Options Alarm Options Syslog Server HTTP Server Application

View Log File

Only the most recent 10000 entries will be shown and filtered. To view the full log, download and open it locally.

Filename: **SDWAN_firewall.log** Filter (Optional):

View Log

Download Log File

Filename: **S35mount_overlay.log** **Download Log**

NAT 接続の詳細がログファイルに表示されます。

```

2020-05-11T10:14:19.861597+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.79.179-->172.57.70.176 (ID:10743)
2020-05-11T10:15:19.166668+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.70.176-->172.57.79.179 (ID:10743)
2020-05-11T10:15:19.986378+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.79.179-->172.57.70.176 (ID:10743)
2020-05-11T10:15:44.749959+0000 INFO conn_clear_all@forward/ NAT Connection DELETED for (Routing Domain Default_RoutingDomain) ICMP 172.57.70.176-->172.57.79.179 (ID:10743)
2020-05-11T10:15:44.750109+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 21 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.70.176-->172.57.79.179 (ID:10743)
2020-05-11T10:16:16.981504+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 21 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.79.179-->172.57.70.176 (ID:10743)
2020-05-11T10:16:20.108292+0000 INFO t2_firewall_monitor.pl NAT Connection CREATED for (Routing Domain Default_RoutingDomain) ICMP 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:16:21.299055+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 1 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:16:22.112286+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 1 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:17:21.768837+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:17:22.255262+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:18:22.235843+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 56 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:18:22.371729+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:19:21.353441+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:19:22.483705+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:20:22.374898+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:20:22.598370+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:21:20.464917+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:21:22.716765+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:22:20.474915+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 50 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:22:22.846123+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 54 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:23:09.456757+0000 INFO t2_firewall_monitor.pl NAT Connection DELETED for (Routing Domain Default_RoutingDomain) ICMP 172.57.79.179-->172.57.70.176 (ID:3261)

2022-02-14T11:43:53.184990+0000 WARN find_and_update_connection@forward/firewall/connection.c:4828 CONN 0x7ffffdbf5f168 Aborted, NAT
2022-02-14T11:43:53.185044+0000 INFO t2_firewall_monitor.pl NAT Connection CREATED for (Routing Domain Default_RoutingDomain) IPv6_
2022-02-14T11:43:53.565134+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 1 packets for (Routing Domain Default_RoutingDomain)
2022-02-14T11:43:59.572977+0000 INFO t2_firewall_monitor.pl Connection DELETED for (Routing Domain Default_RoutingDomain) IPv6_ICMP
2022-02-14T11:45:12.399564+0000 INFO t2_firewall_monitor.pl NAT Connection DELETED for (Routing Domain Default_RoutingDomain) UDP 1
2022-02-14T11:45:48.516174+0000 INFO t2_firewall_monitor.pl NAT Connection CREATED for (Routing Domain Default_RoutingDomain) IPv6_
2022-02-14T11:45:48.717951+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 488 packets for (Routing Domain Default_RoutingDomain)
2022-02-14T11:46:18.786955+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 1 packets for (Routing Domain Default_RoutingDomain)
2022-02-14T11:46:21.768939+0000 INFO t2_firewall_monitor.pl NAT Connection CREATED for (Routing Domain Default_RoutingDomain) TCP 2
2022-02-14T11:46:21.761368+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 3 packets for (Routing Domain Default_RoutingDomain)
2022-02-14T11:46:27.766610+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 1 packets for (Routing Domain Default_RoutingDomain)
2022-02-14T11:46:32.774464+0000 INFO t2_firewall_monitor.pl NAT Connection CREATED for (Routing Domain Default_RoutingDomain) TCP 2
2022-02-14T11:46:32.775063+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 1 packets for (Routing Domain Default_RoutingDomain)

```

ダイナミック NAT

June 8, 2022

ダイナミック NAT は、SD-WAN ネットワーク内のプライベート IP アドレスまたはサブネットを、SD-WAN ネットワーク外のパブリック IP アドレスまたはサブネットに多対 1 のマッピングです。LAN セグメント内の信頼できる (内部) IP アドレス経由の異なるゾーンおよびサブネットからのトラフィックは、単一のパブリック (外部) IP アドレス経由で送信されます。

ダイナミック NAT タイプ

ダイナミック NAT は、IP アドレス変換とともにポートアドレス変換 (PAT) を行います。ポート番号は、どのトラフィックがどの IP アドレスに属しているかを識別するために使用されます。すべての内部プライベート IP アドレスに 1 つのパブリック IP アドレスが使用されますが、各プライベート IP アドレスには異なるポート番号が割り当てられます。PAT は、1 つのパブリック IP アドレスを使用して複数のホストがインターネットに接続できるようにする費用対効果の高い方法です。

- **ポート制限:** ポート制限 NAT は、内部 IP アドレスとポートのペアに関連するすべての変換に同じ外部ポートを使用します。このモードは、通常、インターネット P2P アプリケーションを許可するために使用されます。
- **対称:** 対称 NAT は、内部 IP アドレス、内部ポート、外部 IP アドレス、および外部ポートタプルに関連するすべての変換に同じ外部ポートを使用します。通常、このモードは、セキュリティを強化したり、NAT セッションの最大数を拡張するために使用されます。

インバウンドおよびアウトバウンド NAT

接続の方向は、内側から外側、または外側から内側にできます。NAT ルールが作成されると、方向一致タイプに応じて両方の方向に適用されます。

- **Outbound:** サービスで受信したパケットについて、宛先アドレスが変換されます。送信元アドレスは、サービス上で送信されるパケットに対して変換されます。発信ダイナミック NAT は、ローカル、インターネット、イントラネット、およびルーティング間ドメインサービスでサポートされます。インターネットサービスやイントラネットサービスなどの WAN サービスの場合、構成された WAN リンク IP アドレスが外部 IP アドレスとして動的に選択されます。ローカルおよびインタールーティングドメインサービスの場合は、外部 IP アドレスを指定します。Outside ゾーンは、選択したサービスから取得されます。アウトバウンドダイナミック NAT の一般的な使用例は、LAN 内の複数のユーザーが、単一のパブリック IP アドレスを使用してインターネットに安全にアクセスできるようにすることです。
- **Inbound:** サービスで受信したパケットについて、送信元アドレスが変換されます。宛先アドレスは、サービス上で送信されるパケットに対して変換されます。インバウンドダイナミック NAT は、インターネットやイントラネットなどの WAN サービスではサポートされません。同じことを示す明示的な監査エラーがあります。インバウンドダイナミック NAT は、ローカルおよびインタールーティングドメインサービスでのみサポートされます。変換先の外部ゾーンと外部 IP アドレスを指定します。インバウンドダイナミック NAT の一般的な使用例は、外部ユーザーがプライベートネットワークでホストされている電子メールまたはウェブサーバーにアクセスできるようにすることです。

ダイナミック NAT ポリシーの設定

ダイナミック NAT ポリシーを設定するには、構成エディタで、[接続] > [ファイアウォール] > [ダイナミック NAT ポリシー] に移動します。

?

x

Add

Priority:

100

Direction:

Outbound

Type:

Port Restricted

Service Type:

Internet

Service Name:

Internet

Inside Zone:

Any

Inside IP Address:

*

☒ Allow Related

☐ IPsec Passthrough

☐ GRE/PPTP Passthrough

☒ Port Parity

☐ Bind Responder Route

Port Forwarding Rules

+

Protocol	Outside Port	Inside IP Address	Inside Port	Fragments	Log Interval (s)	Log Start	Log End	Connection State Tracking	Delete
----------	--------------	-------------------	-------------	-----------	------------------	-----------	---------	---------------------------	--------

Add

Cancel

- **Priority:** 定義されたすべてのポリシー内でポリシーが適用される順序。優先順位の低いポリシーは、優先順位の高いポリシーの前に適用されます。

- 方向: 仮想インターフェイスまたはサービスから見たトラフィックが流れている方向。インバウンドトラフィックまたはアウトバウンドトラフィックのいずれかになります。
- タイプ: 実行するダイナミック NAT のタイプ、ポート制限、または対称。
- サービスタイプ: ダイナミック NAT ポリシーが適用される SD-WAN サービスタイプ。インバウンドダイナミック NAT は、ローカルおよびインタールーティングドメインサービスでサポートされます。発信ダイナミック NAT は、ローカル、インターネット、イントラネット、およびルーティングドメインサービスでサポートされます。
- サービス名: サービスタイプに対応する設定済みのサービス名を選択します。
- **Inside Zone:** 変換を許可するために、パケットの送信元となる必要がある内部ファイアウォールゾーンのマッチタイプ。
- **[Outside Zone]:** インバウンドトラフィックの場合、変換を許可するためにパケットの送信元となる必要がある外部ファイアウォールゾーンのマッチタイプを指定します。
- 内部 **IP** アドレス: 一致基準が満たされた場合に変換する必要がある内部 IP アドレスおよびプレフィクス。内部 IP アドレスを示すには、「*」を入力します。
- 外部 **IP** アドレス: 一致基準が満たされた場合に内部 IP アドレスが変換される外部 IP アドレスおよびプレフィクス。インターネットサービスおよびイントラネットサービスを使用する発信トラフィックでは、構成された WAN リンク IP アドレスが外部 IP アドレスとして動的に選択されます。
- **[関連を許可]:** ルールに一致するフローに関連するトラフィックを許可します。たとえば、ポリシーに一致する特定のフローに関連する ICMP リダイレクション（フローに関連する何らかのタイプのエラーがある場合）。
- **IPsec** パススルー: IPsec (AH/ESP) セッションの変換を許可します。
- **GRE/PPTP** パススルー: GRE/PPTP セッションの変換を許可します。
- ポートパリティ: 有効の場合、NAT 接続の外部ポートはパリティを維持します（内部ポートが偶数であっても、外部ポートが奇数の場合は奇数）。
- **Bind Responder Route:** 非対称ルーティングを回避するために、応答トラフィックが受信されるのと同じサービスで送信されるようにします。

ポートフォワーディング

ポートフォワーディングを使用したダイナミック NAT では、特定のトラフィックを定義済みの IP アドレスにポート転送できます。これは、通常、Web サーバなどの内部ホストで使用されます。ダイナミック NAT を設定したら、ポートフォワーディングポリシーを定義できます。IP アドレス変換用のダイナミック NAT を設定し、外部ポートを内部ポートにマッピングするポートフォワーディングポリシーを定義します。ダイナミック NAT ポートフォワーディングは、通常、リモートホストがプライベートネットワーク上のホストまたはサーバーに接続できるようにするために使用されます。より詳細なユースケースについては、「[Citrix SD-WAN ダイナミック NAT](#)」の説明を参照してください。

Add ? x

Priority:
200

Direction: Inbound Type: Symmetric Service Type: Local Service Name: VirtualInterface...

Inside IP Address: * Outside Zone: Internet_Zone Outside IP Address: 172.147.12.83

☐ Allow Related ☐ IPsec Passthrough ☐ GRE/PPTP Passthrough ☐ Port Parity ☐ Bind Responder Route

Port Forwarding Rules +

Routing Domain	Protocol	Outside Port	Inside IP Address	Inside Port	Fragments	Log Interval (s)	Log Start	Log End	Connection State Tracking	Delete
Default_RoutingDomain	Both	443	15.15.15.1	443	<input checked="" type="checkbox"/>	0	<input type="checkbox"/>	<input type="checkbox"/>	Use Site Setting	

Add Cancel

- プロトコル: TCP、UDP、またはその両方。
- 外部ポート: 内部ポートにポート転送される外部ポート。
- 内部 **IP** アドレス: 一致するパケットを転送する内部アドレス。
- 内部ポート: 外部ポートが転送される内部ポート。
- [フラグメント]: フラグメント化されたパケットの転送を許可します。
- ログ間隔: ポリシーに一致するパケット数を syslog サーバにロギングする間隔 (秒)。デフォルトのログ間隔値 0 は、ログなしを意味します。
- ログ開始: 選択すると、新しいフローの新しいログエントリが作成されます。
- ログ終了: フローが削除されたときにフローのデータをログに記録します。
- 追跡: 規則に一致する TCP、UDP、および ICMP パケットに対して、双方向接続状態トラッキングが実行されます。この機能は、非対称ルーティングまたはチェックサムの失敗、プロトコル固有の検証のために、非合法に見えるフローをブロックします。状態の詳細は、[監視] > [ファイアウォール] > [接続] の下に表示されます。
-

すべてのポートフォワーディングルールには、親 NAT ルールがあります。外部 IP アドレスは、親 NAT ルールから取得されます。

自動作成されたダイナミック **NAT** ポリシー

インターネットサービスのダイナミック NAT ポリシーは、次の場合に自動的に作成されます。

- 信頼できないインターフェイス (WAN リンク) でのインターネットサービスの設定

- 単一の WAN リンク上のすべてのルーティングドメインに対するインターネットアクセスを有効にします。詳細については、「[ファイアウォールのセグメンテーションを構成する](#)」を参照してください。
- SD-WAN での DNS フォワーダーまたは DNS プロキシの設定詳細については、「[ドメインネームシステム](#)」を参照してください。

監視

ダイナミック NAT を監視するには、[監視]>[ファイアウォール統計]>[接続]に移動します。接続では、NAT が完了しているかどうかを確認できます。

The screenshot displays the 'Connections' tab under 'Firewall Statistics'. The table lists several connections for 'Domain Name Service(dns)' from internal IP 172.57.48.50 to external IP 10.140.50.5. All connections are in 'ESTABLISHED' state and are marked as 'Is NAT: Yes'.

内部 IP アドレスと外部 IP アドレスのマッピングをさらに確認するには、[関連オブジェクト]の[ルーティング前 NAT]または[ポストルート NAT]をクリックするか、[モニタリング]>[ファイアウォール統計]>[NAT ポリシー]に移動します。

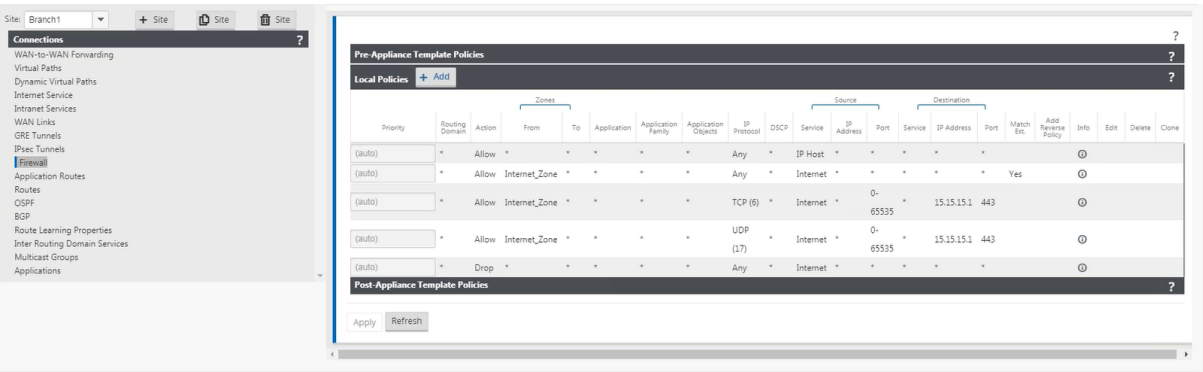
次のスクリーンショットは、タイプシメトリックダイナミック NAT 規則とそれに対応するポート転送規則の統計を示しています。

The screenshot displays the 'NAT Policies' tab. It shows two policies:

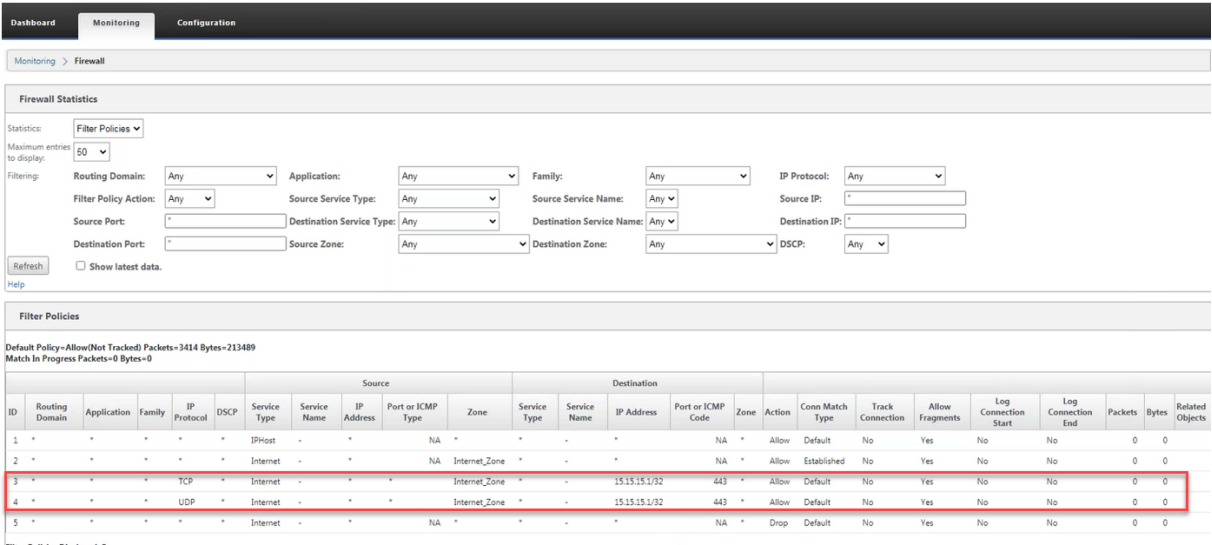
ID	Rule Type	Rule Parent	Direction	IP Protocol	Service Type	Service Name	Inside IP Address	Port	Outside IP Address	Port	Allow Related	Allow IPSec Passthrough	Allow GRE Passthrough	Packets Sent	Bytes Sent	Packets Received	Bytes Received	Connections	Related Objects
1	Dynamic Sym	-	Outbound	*	Internet	-	*	*	172.147.12.83/32	*	No	No	No	0	0	0	0	0	
2	Port Forward	1	Outbound	*	Internet	-	172.147.90.12/32	5001-5010	172.147.12.83/32	5001-5010	No	No	No	82	47232	8928	13374144	0	

Below the table, it states: NAT Policies Displayed: 2, NAT Policies In Use: 2/1000, Port Restricted Dynamic NAT Policies In Use: 0/100, Destination NAT Policies In Use: 0/100.

ポート転送規則が作成されると、対応するファイアウォール規則も作成されます。



[監視]>[ファイアウォール統計]>[フィルタポリシー]に移動すると、フィルタポリシーの統計を表示できます。



ログ

NATに関連するログは、ファイアウォールログで表示できます。NATのログを表示するには、NATポリシーに一致するファイアウォールポリシーを作成し、ファイアウォールフィルタでロギングが有効になっていることを確認します。NATログには次の情報が含まれます。

- 日付と時刻
- ルーティングドメイン
- IPプロトコル
- 送信元ポート
- 送信元IPアドレス
- 翻訳されたIPアドレス
- 翻訳されたポート
- 宛先IPアドレス
- Destination port

Edit ? x

Priority: Policy Type: **Built-in Firewall** ▼

Match Criteria

From Zones

Zone	Enable
Any	<input checked="" type="checkbox"/>
Default_LAN_Zone	<input type="checkbox"/>
gre_zone	<input type="checkbox"/>
Inter Routing Domain Zone	<input type="checkbox"/>

To Zones

Zone	Enable
Any	<input checked="" type="checkbox"/>
Default_LAN_Zone	<input type="checkbox"/>
gre_zone	<input type="checkbox"/>
Inter Routing Domain Zone	<input type="checkbox"/>

Routing Domain: **Any** ▼

Traffic Match Type: **IP Protocol** ▼ IP Protocol: **Any** ▼ DSCP: **Any** ▼ ☐ Match Established

Application: Application Family: Application Objects: **Any** ▼

Source Service Type: **Any** ▼ Source Service Name: **Any** ▼ Source IP: Source Port:

Dest Service Type: **Any** ▼ Dest Service Name: **Any** ▼ Dest IP: Dest Port:

Actions

Action: **Allow** ▼ ☒ Allow Fragments Connection State Tracking: **Use Site Setting** ▼

Logging & Other Options

Log Interval (s): ☒ Log Start ☒ Log End ☐ Add Reverse Policy

Apply Cancel

NAT ログを生成するには、[ログ/監視] > [ログオプション] に移動し、[**SDWAN_firewall.log**] を選択して [ログの表示] をクリックします。

Dashboard Monitoring **Configuration**

Configuration > Appliance Settings > **Logging/Monitoring**

Log Options Alert Options Alarm Options Syslog Server HTTP Server Application

View Log File

Only the most recent 10000 entries will be shown and filtered. To view the full log, download and open it locally.

Filename: **SDWAN_firewall.log** ▼ Filter (Optional):

View Log

Download Log File

Filename: **S35mount_overlay.log** ▼ **Download Log**

NAT 接続の詳細がログファイルに表示されます。

```

2020-05-11T10:14:19.861597+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.79.179-->172.57.79.176 (ID:10743)
2020-05-11T10:15:19.166666+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.176-->172.57.79.179 (ID:10743)
2020-05-11T10:15:19.986378+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.79.179-->172.57.79.176 (ID:10743)
2020-05-11T10:15:44.749959+0000 INFO conn_clear_all@forward/firewall/connection-48704 Removed 1 Connections
2020-05-11T10:15:44.750109+0000 INFO t2_firewall_monitor.pl NAT Connection DELETED for (Routing Domain Default_RoutingDomain) ICMP 172.57.79.179-->172.57.79.176 (ID:10743)
2020-05-11T10:16:16.981504+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 21 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.176-->172.57.79.179 (ID:10743)
2020-05-11T10:16:20.108292+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 21 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.79.179-->172.57.79.176 (ID:10743)
2020-05-11T10:16:21.299055+0000 INFO t2_firewall_monitor.pl NAT Connection CREATED for (Routing Domain Default_RoutingDomain) ICMP 172.57.79.179-->172.57.79.176 (ID:3261)
2020-05-11T10:16:22.112286+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 1 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.79.176 (ID:3261)
2020-05-11T10:16:22.112650+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 1 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.79.176-->172.57.79.179 (ID:3261)
2020-05-11T10:17:21.768837+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.79.176 (ID:3261)
2020-05-11T10:17:22.255262+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.79.176-->172.57.79.179 (ID:3261)
2020-05-11T10:18:22.235843+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 56 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.79.179-->172.57.79.179 (ID:3261)
2020-05-11T10:18:22.371729+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.79.176 (ID:3261)
2020-05-11T10:19:21.353441+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.79.176-->172.57.79.179 (ID:3261)
2020-05-11T10:19:22.483705+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.79.176 (ID:3261)
2020-05-11T10:20:22.374898+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.79.176-->172.57.79.179 (ID:3261)
2020-05-11T10:20:22.598370+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.79.176 (ID:3261)
2020-05-11T10:21:20.464917+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.79.179-->172.57.79.179 (ID:3261)
2020-05-11T10:21:22.716765+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.79.176 (ID:3261)
2020-05-11T10:22:20.474915+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 50 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.79.176 (ID:3261)
2020-05-11T10:22:22.846123+0000 INFO t2_firewall_monitor.pl Filter (1) ALLOWED 54 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.79.179-->172.57.79.179 (ID:3261)
2020-05-11T10:23:09.456757+0000 INFO t2_firewall_monitor.pl NAT Connection DELETED for (Routing Domain Default_RoutingDomain) ICMP 172.57.79.179-->172.57.79.176 (ID:3261)

```

仮想 WAN サービスの構成

May 10, 2021

Citrix SD-WAN 構成では、Citrix SD-WAN ネットワークのトポロジーについて説明し、定義します。SD-WAN ネットワークを展開する前に、仮想 WAN 構成を定義する必要があります。これを行うには、MCN アプライアンスの Citrix SD-WAN 管理 Web インターフェイスで構成エディターを使用します。

セキュリティと暗号化

SD-WAN の暗号化の有効化（仮想パス用）はオプションです。この機能の設定手順については、[仮想 WAN セキュリティおよび暗号化の有効化と設定（オプション）](#)を参照してください。

暗号化が有効な場合、SD-WAN は高度暗号化標準（AES）を使用して、仮想パスを通るトラフィックをセキュリティで保護します。AES 128 ビット暗号と 256 ビットの暗号の両方（キーサイズ）は SD-WAN アプライアンスでサポートされており、設定可能なオプションです。管理制御ノード（MCN）の管理 Web インターフェイスの構成エディタを使用して、これらの暗号化オプションおよびその他の暗号化オプションを選択、有効化、および構成できます。設定を変更し、SD-WAN ネットワーク全体に変更を配布するには、MCN に対する管理アクセス権が必要です。MCN がセキュリティで保護されると、暗号化設定とその配布もセキュリティで保護されます。

サイト間の認証は、仮想 WAN 構成で機能します。

ネットワーク構成には、各サイトの秘密キーがあります。各仮想パスについて、ネットワーク構成は、仮想パスの各端にあるサイトの秘密キーを組み合わせ、キーを生成します。仮想パスの最初のセットアップ後に発生する最初のキー交換は、その結合されたキーを使用してパケットを暗号化および復号化する能力に依存します。

仮想 WAN サービスの有効化

これが初期インストールおよび構成の場合、最後の手順として、ネットワーク内の各 SD-WAN アプライアンスで Virtual WAN サービスを手動で有効にする必要があります。サービスを有効にすると、仮想 WAN デモンが有効になり、起動します。

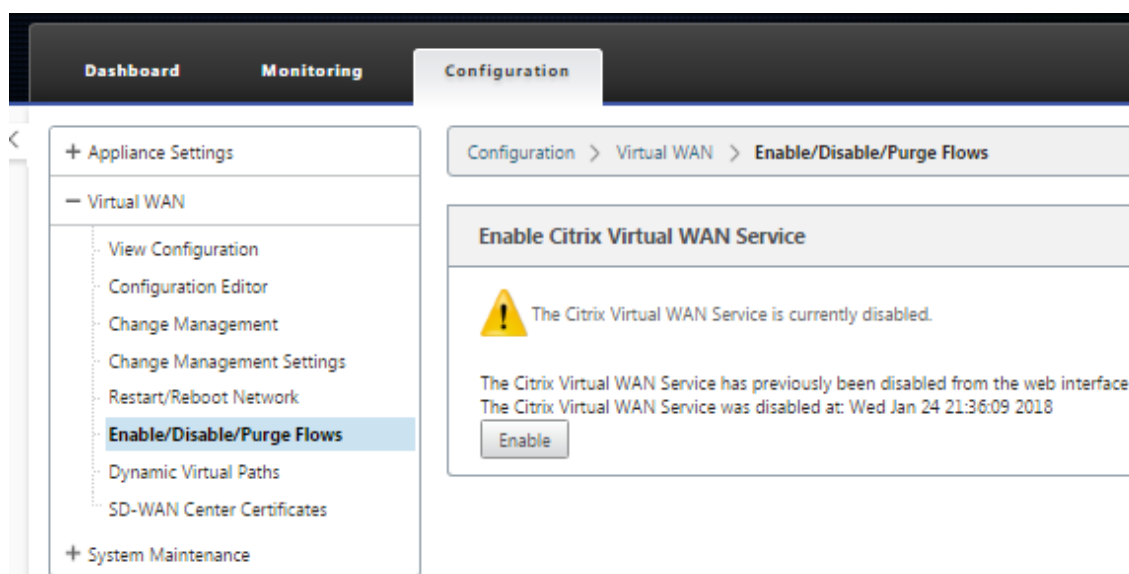
注

既存の展開を再構成する場合、MCN は更新された Appliance Packages をクライアントサイトに配布するときに、サービスを自動的に有効にします。この場合、この最後のステップはスキップできます。

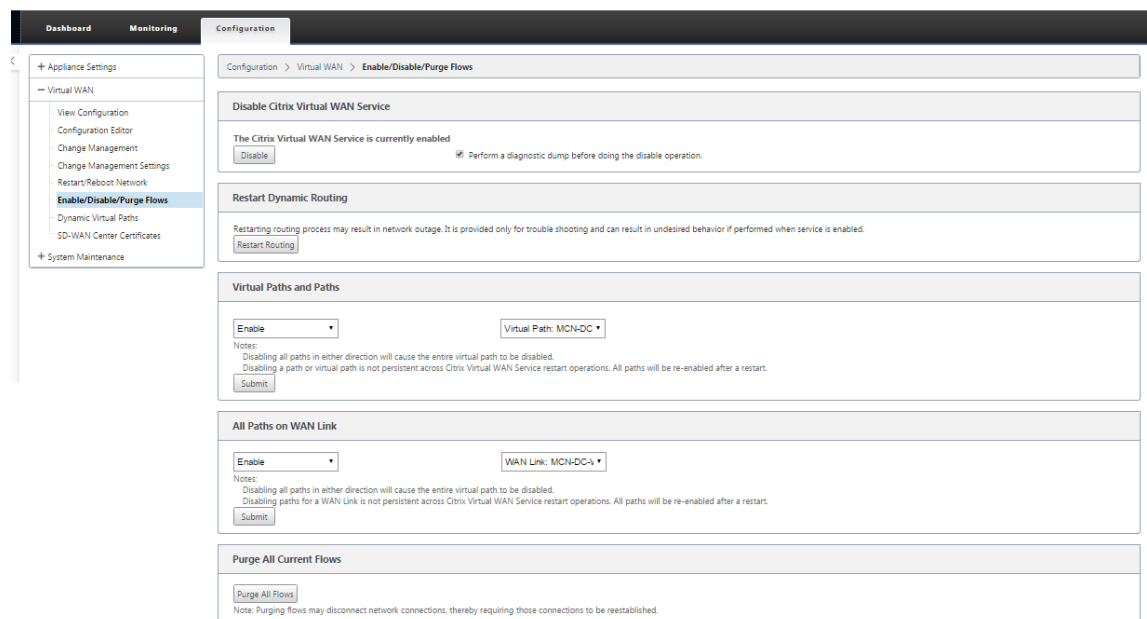
アプライアンスで仮想 WAN サービスを手動で有効にするには、次の手順を実行します。

1. アクティブ化するアプライアンスの管理 Web Interface にログインします。
2. [構成] タブを選択します。
3. ナビゲーションペインで、Virtual WAN ブランチを開き、[フローの有効化/無効化/パージ] を選択します。

仮想 WAN サービスを無効にすると、次に示すように [仮想 WAN サービスの有効化] ページが表示されます。サービスがすでに有効になっている場合は、「フローの有効化/無効化/パージ・フロー」ページが表示されます。



4. [有効] をクリックします。これにより、サービスが有効になり、「フローの有効化」、「無効化」、「パージ」ページが表示されます。



Virtual WAN サービスを有効にすると、その旨を示すステータスメッセージがページの上部セクションに表示されます。

注

このページでは、ネットワーク内の特定のパスと仮想パスを有効/無効にするオプション、およびすべてのフローを消去するオプションも表示されます。

これで、MCN およびブランチサイトクライアントアプライアンスでの SD-WAN のインストールとアクティベーションが完了します。[Monitoring] ページを使用して、アクティブ化を確認し、既存または潜在的な構成問題を診断できます。

ファイアウォールセグメンテーションの構成

May 10, 2021

Virtual Route Forwarding (VRF; バーチャルルートフォワーディング) ファイアウォールセグメンテーションでは、複数のルーティングドメインが共通のインターフェイスを介してインターネットにアクセスでき、各ドメインのトラフィックは他のドメインのトラフィックから分離されます。たとえば、従業員とゲストは、互いのトラフィックにアクセスすることなく、同じインターフェイスを介してインターネットにアクセスできます。

- ローカルゲストユーザインターネットアクセス
- 定義されたアプリケーションに対する従業員とユーザーのインターネットアクセス
- 従業員ユーザーは、MCN に他のすべてのトラフィックをヘアピンし続けることができます
- 特定のルーティングドメインに特定のルートを追加することをユーザーに許可します。

- 有効にすると、この機能はすべてのルーティングドメインに適用されます。

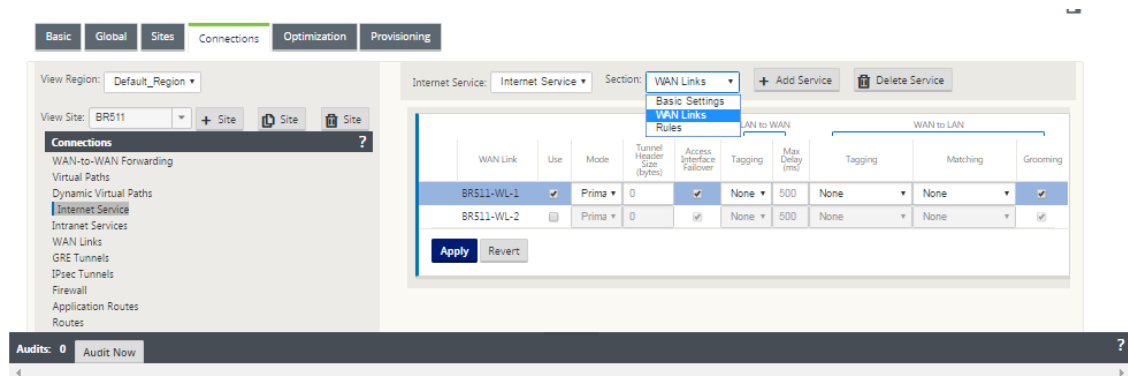
また、複数のアクセスインターフェイスを作成して、個別のパブリック向け IP アドレスを収容することもできます。どちらのオプションでも、各ユーザグループに必要なセキュリティが提供されます。

注

詳細については、「[VRF の設定](#)」を参照してください。

すべてのルーティングドメインに対してインターネットサービスを構成するには、次の手順を実行します。

1. サイトのインターネットサービスを作成します。[接続] > [リージョンの表示] > [サイトの表示] [サイト名] > [インターネットサービス] > [セクション] > [WAN リンク] に移動し、[WAN リンク] で [使用] チェックボックスをオンにします。



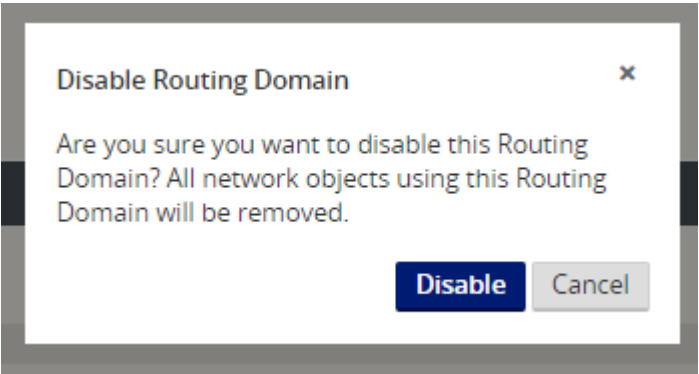
注

[接続] > [リージョンの表示] > [** サイトの表示 **] > [サイト名] > [ルート] の下に、ルーティングドメインごとに 1 つずつ 0.0.0.0/0 ルートが追加されていることがわかります。

Search: <input type="text"/>									
Order	Network IP Address	Routing Domain	Cost	Service Type	Service Name	Gateway IP Address	Info	Edit	Delete
1	10.200.247.41/24	Default	5	Local			ⓘ		
2	10.200.247.42/24	Default	5	Local			ⓘ		
3	10.200.247.6/24	Default	5	Local			ⓘ		
4	11.123.10.0/24		5	Intranet	Intranet-0		ⓘ	✎	🗑
5	11.20.20.11/24	Guest	5	Local			ⓘ		
6	12.125.10.0/24		5	Internet			ⓘ	✎	🗑
7	0.0.0.0/0	Default	5	Internet			ⓘ		
8	0.0.0.0/0	Guest	5	Internet			ⓘ		
9	0.0.0.0/0	Default	16	Passthrough			ⓘ		
10	0.0.0.0/0	Guest	16	Passthrough			ⓘ		

MCN ですべてのルーティングドメインを有効にする必要はなくなりました。

2. MCN でルーティングドメインを無効にすると、ドメインがブランチサイトで使用されている場合は、次のメッセージが表示されます。



3. 各ルーティングドメインがインターネットサービスを使用していることを確認するには、[**Monitor]>[Flows]の下の Web 管理インターフェイスの [Flows] テーブルにある [Routing Domain] 列を確認します。

★★

Flows Table

Both WAN Ingress and WAN Egress Flows

Routing Domain	Source IP Address	Dest IP Address	Direction	Source Port	Dest Port	IPP	DSCP	Hit Count	Service Type	Service Name	LAN GW IP	Age (ms)	Packets	Bytes	PPS	Customer kbps	Conduit Overhead kbps	IPsec Overhead kbps	Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type
Guest	11.20.20.20	12.125.10.20	WAN Ingress	8	3335	ICMP	default	62	INTERNET	-	LOCAL	74	62	5208	1.013	0.681	0.000	0.000	202	N/A	N/A	N/A	N/A	N/A
Default	10.200.247.200	12.125.10.20	WAN Ingress	8	16185	ICMP	default	66	INTERNET	-	LOCAL	311	66	5544	1.009	0.678	0.000	0.000	202	N/A	N/A	N/A	N/A	N/A
Guest	12.125.10.20	11.20.20.20	WAN Egress	0	18456	ICMP	default	62	INTERNET	-	LOCAL	94	62	5208	1.013	0.681	0.000	0.000	202	N/A	N/A	N/A	N/A	N/A
Default	12.125.10.20	10.200.247.200	WAN Egress	0	3968	ICMP	default	66	INTERNET	-	LOCAL	328	66	5544	1.008	0.678	0.000	0.000	202	N/A	N/A	N/A	N/A	N/A

Total INGRESS flows displayed: 2 out of 2
Total EGRESS flows displayed: 2 out of 2

4. [モニター]>[統計]>[ルート] で、各ルーティングドメインのルーティングテーブルを確認することもできます。

Routes for routing domain: Guest

Filter: [] in Any column [v] Apply

Show 100 entries Showing 1 to 5 of 5 entries

Num	Network Addr	Gateway IP Address	Service	Firewall Zone	Reachable	Site IP Address	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
0	11.20.20.0/24	*	Local	Default_LAN_Zone	YES	*	Angelina-CFB	Static	-	-	5	318	YES	N/A	N/A
1	11.10.10.0/24	*	DC-Angelina-CFB	Default_LAN_Zone	YES	*	DC	Static	-	-	5	0	YES	N/A	N/A
2	0.0.0.0/0	*	Internet	Untrusted_Internet_Zon	YES	*	*	Static	-	-	5	159	YES	N/A	N/A
3	0.0.0.0/0	*	Passthrough	Any	YES	*	*	Static	-	-	16	0	YES	N/A	N/A
4	0.0.0.0/0	*	Discard	Any	YES	*	*	Static	-	-	16	0	YES	N/A	N/A

Showing 1 to 5 of 5 entries

使用例

以前の Citrix SD-WAN リリースでは、仮想ルーティングと転送には以下の問題がありましたが、これらの問題は解決されています。

- ブランチサイトに複数のルーティングドメインがある場合、データセンター (MCN) のすべてのドメインを含める必要はありません。さまざまな顧客のトラフィックを安全な方法で分離する能力が必要
- 1つのサイトでインターネットにアクセスするには、複数のルーティングドメインに対して、アクセス可能なファイアウォール付きパブリック IP アドレスを 1 つ持つ必要があります (VRF lite を超えて拡張)。
- お客様は、異なるサービスをサポートするルーティングドメインごとにインターネットルートが必要です。

- ブランチサイトでの複数のルーティングドメイン
- 異なるルーティングドメインのインターネットアクセス。

ブランチサイトでの複数のルーティングドメイン

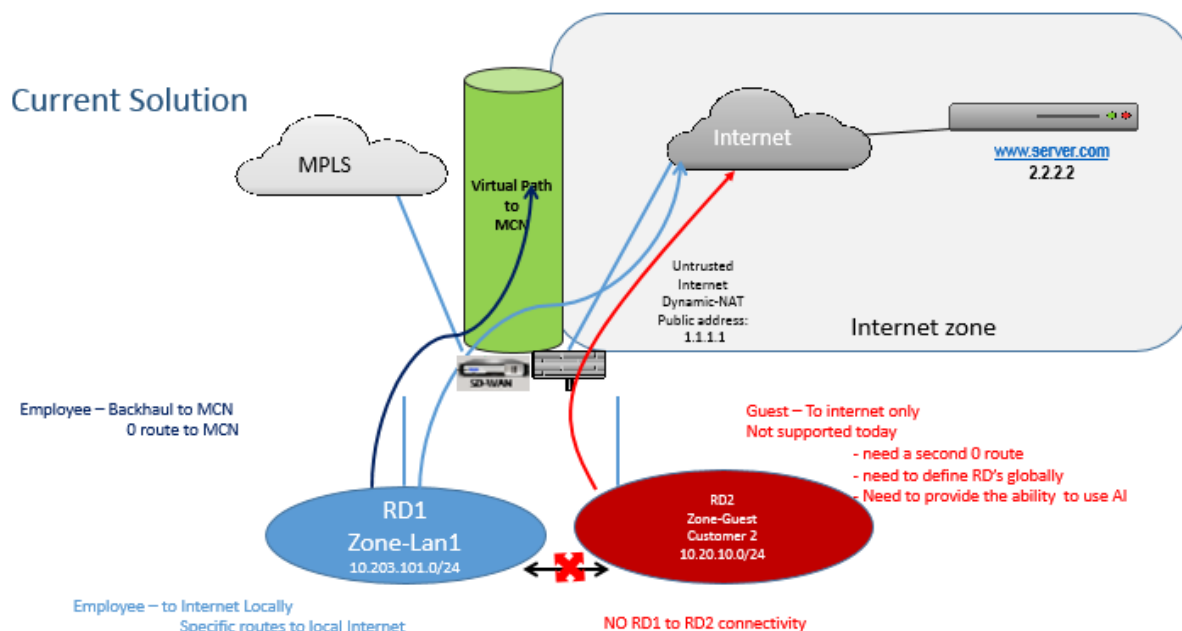
仮想転送およびルーティングファイアウォールのセグメント化機能強化により、次のことが行えます。

- 従業員やゲストなど、少なくとも 2 つのユーザーグループの安全な接続をサポートするインフラストラクチャをブランチサイトで提供します。このインフラストラクチャは、最大 16 のルーティングドメインをサポートできます。
- 各ルーティングドメインのトラフィックを、他のルーティングドメインのトラフィックから分離します。
- 各ルーティングドメインにインターネットアクセスを提供し、
 - 共通のアクセスインターフェイスが必要であり、許容される
 - 個別のパブリック向け IP アドレスを持つ各グループのアクセスインターフェイス
- 従業員のトラフィックは、ローカルインターネット（特定のアプリケーション）に直接ルーティングできます
- 従業員のトラフィックは、広範なフィルタリング（0 ルート）のために MCN にルーティングまたはバックホールできます
- ルーティングドメインのトラフィックは、ローカルインターネット（0 ルート）に直接ルーティングできます。
- 必要に応じて、ルーティングドメインごとに特定のルートをサポート
- ルーティングドメインは VLAN ベースです
- RD を MCN に配置する必要の要件を削除
- ルーティングドメインをブランチサイトでのみ構成できるようになりました
- アクセスインターフェイスに複数の RD を割り当てることができます（一度有効にすると）
- 各 RD には 0.0.0.0 のルートが割り当てられます
- RD に特定のルートを追加できるようにします
- 同じアクセスインターフェイスを使用して、異なる RD からのトラフィックがインターネットに出ることを許可します。
- RD ごとに異なるアクセスインターフェイスを構成できます。
- 一意のサブネットでなければならない（RD は VLAN に割り当てられる）
- 各 RD では、同じ FW デフォルトゾーンを使用できます。
- トラフィックは、ルーティングドメインを介して分離されます
- アウトバウンドフローには、フローヘッダーのコンポーネントとして RD があります。SD-WAN がリターンフローを正しいルーティングドメインにマッピングできるようにします。

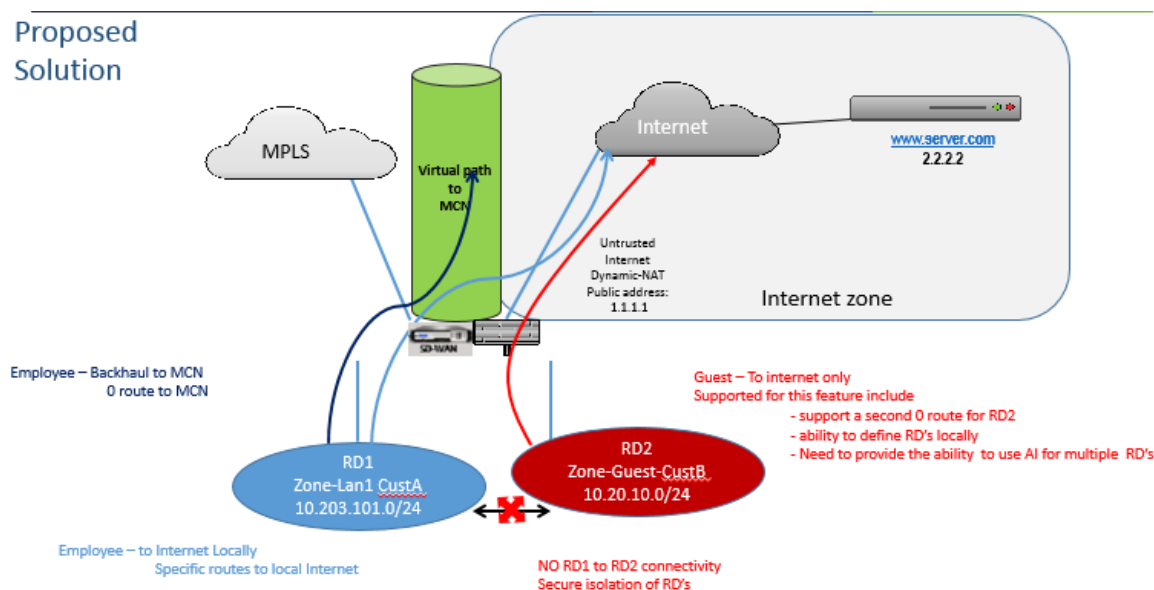
複数のルーティングドメインを設定するための前提条件

- インターネットアクセスが構成され、WAN リンクに割り当てられます。
- NAT 用に設定されたファイアウォールと正しいポリシーが適用されます。
- 2 番目のルーティングドメインがグローバルに追加されました。
- 各ルーティングドメインがサイトに追加されました。
- [サイト] > [サイト名] > [WAN リンク [名前名前]] > [WL2] > [アクセスインターフェイス] で、チェックボックスが使用可能であり、インターネットサービスが正しく定義されていることを確認します。このチェックボックスを選択できない場合、インターネットサービスは定義されていないか、サイトの WAN リンクに割り当てられていません。

展開シナリオ



Proposed Solution



制限事項

- すべてのルーティングドメインでインターネットアクセスを有効にするには、インターネットサービスをWANリンクに追加する必要があります。(このオプションを有効にするまで、このオプションを有効にするチェックボックスはグレー表示されます)。

すべてのルーティングドメインでインターネットアクセスを有効にしたら、Dynamic-NAT ルールを自動的に追加します。

- サイトあたり最大 16 のルーティングドメイン。
- アクセスインターフェイス (AI): サブネットごとに単一の AI。
- 複数の AI では、AI ごとに個別の VLAN が必要です。
- サイトに 2 つのルーティングドメインがあり、1 つの WAN リンクがある場合、両方のドメインは同じパブリック IP アドレスを使用します。
- すべてのルーティングドメインのインターネットアクセスが有効になっている場合、すべてのサイトがインターネットにルーティングできます。(1 つのルーティングドメインでインターネットアクセスを必要としない場合は、ファイアウォールを使用してトラフィックをブロックできます)。
- 複数のルーティングドメインで同じサブネットはサポートされません。
- 監査機能はありません
- WAN リンクは、インターネットアクセス用に共有されます。
- ルーティングドメインごとの QoS はありません。先着順です。

証明書認証

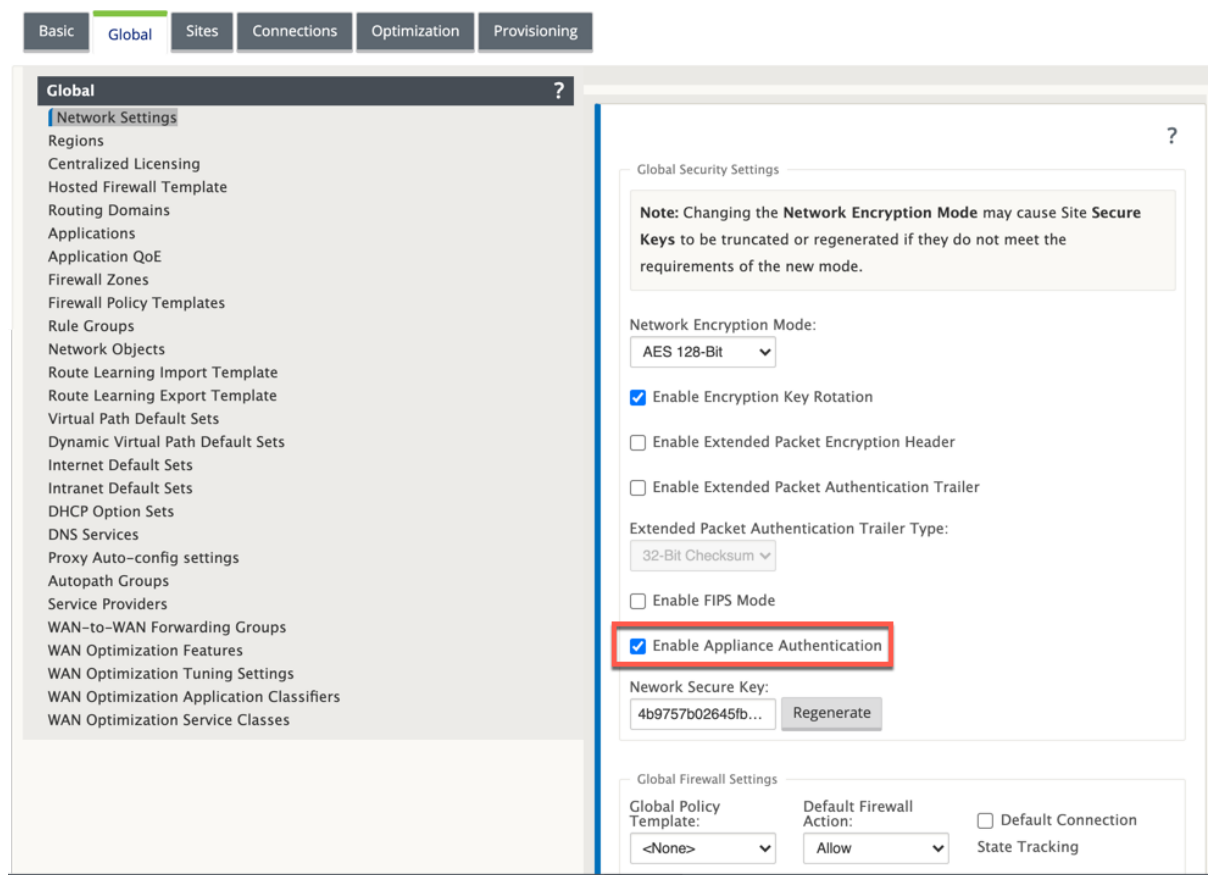
May 10, 2021

Citrix SD-WAN は、ネットワーク暗号化や仮想パスの IPsec トンネルなどのセキュリティ技術を使用して、SD-WAN ネットワーク上のアプライアンス間で安全なパスを確立します。Citrix SD-WAN 11.0.2 では、既存のセキュリティ対策に加えて、証明書ベースの認証が導入されています。

証明書認証。組織は、プライベート認証局（CA）によって発行された証明書を使用してアプライアンスを認証できます。アプライアンスは、仮想パスを確立する前に認証されます。たとえば、ブランチアプライアンスがデータセンターに接続しようとしたときに、ブランチからの証明書がデータセンターで想定される証明書と一致しない場合、仮想パスは確立されません。

CA によって発行された証明書は、公開鍵をアプライアンスの名前にバインドします。公開キーは、証明書で識別されるアプライアンスが所有する対応する秘密キーで動作します。

アプライアンス認証を有効にするには、構成エディターで [グローバル] > [ネットワーク設定] に移動し、[アプライアンス認証を有効にする] を選択します。



構成をステージングして適用すると、[構成] > [仮想 WAN] の下に新しい 証明書認証オプションが表示されます。

[証明書認証] ページから、仮想パス認証に使用されるすべての 証明書 を管理できます。

The screenshot displays the Citrix SD-WAN 11.4 Configuration interface. The left sidebar contains a menu with options like 'Appliance Settings', 'Virtual WAN', and 'System Maintenance'. The 'Virtual WAN' section is expanded, and 'Certificate Authentication' is highlighted with a red box. The main content area shows the 'Configuration > Virtual WAN > Certificate Authentication' path. Under the 'Installed Certificate' section, there are two tables: 'Issued to' and 'Issuer'. The 'Issued to' table lists details for the certificate recipient, and the 'Issuer' table lists details for the certificate issuer. Below these is the 'Certificate Details' section, which includes the Certificate Fingerprint, Start Date, End Date, and Serial Number.

Issued to:	
Country:	US
State/Province:	California
Locality:	San Jose
Organization:	Citrix Systems, Inc.
Organizational Unit:	Development
Common Name:	DC_MCN

Issuer:	
Country:	US
State/Province:	California
Locality:	San Jose
Organization:	Citrix Systems, Inc.
Organizational Unit:	Development
Common Name:	CitrixSigning
Email:	support@citrix.com

Certificate Details:	
Certificate Fingerprint:	880648D10F9E812680C3D8DD17A4FC860F84C9AC
Start Date:	Nov 23 05:32:37 2020 GMT
End Date:	Feb 25 05:32:37 2028 GMT
Serial Number:	1F8B496FCF2579C9

注

アプライアンス・ソフトウェアを SD-WAN バージョン 11.0 からバージョン 11.1 以降にアップグレードする場合は、「アプライアンス認証の有効化」オプションのチェックを外し、ソフトウェアのアップグレードを実行します。アップグレード・プロセスが完了したら、「アプライアンス認証を有効にする」オプションを選択します。

インストール済みの証明書

「インストールされた証明書」セクションには、アプライアンスにインストールされている証明書の概要が表示されます。アプライアンスは、この証明書を使用してネットワーク内で自身を識別します。

[発行先] セクションには、証明書の発行元に関する詳細が表示されます。証明書はアプライアンス 名にバインドされているため、証明書の共通 名はアプライアンスの名前と一致します。[発行者] セクションには、証明書に署名した認証局の詳細が表示されます。証明書の詳細には、証明書のフィンガープリント、シリアル番号、および証明書の有効期間が含まれます。

Installed Certificate	
Issued to:	Issuer:
Country: US	Country: US
State/Province: California	State/Province: California
Locality: San Jose	Locality: San Jose
Organization: Citrix Systems, Inc.	Organization: Citrix Systems, Inc.
Organizational Unit: Development	Organizational Unit: Development
Common Name: DC	Common Name: CitrixSigning
	Email: support@citrix.com
Certificate Details:	
Certificate Fingerprint: [REDACTED]	
Start Date: Aug 13 13:45:47 2019 GMT	
End Date: Aug 10 13:45:47 2029 GMT	
Serial Number: [REDACTED]	

ID バンドルをアップロード

Identity バンドルには、秘密鍵と秘密鍵に関連付けられた証明書が含まれます。CA によって発行されたアプライアンス証明書をアプライアンスにアップロードできます。証明書バンドルは PKCS 12 ファイルで、拡張子は.p12 です。パスワードで保護することを選択できます。パスワードフィールドを空白のままにすると、パスワード保護なしとして扱われます。

Upload Identity Bundle (PKCS12)	
File:	C:\ID\SD-WAN\11.0.2\S Browse...
Password:	●●●●●●●●
Upload Identity Bundle	

認証局バンドルのアップロード

証明書署名機関に対応する PKCS 12 バンドルをアップロードします。認証局バンドルには、シグネチャの完全なチェーン、ルート、およびすべての中間署名機関が含まれます。

Upload Certificate Authority Bundle (PKCS12)	
File:	C:\ID\SD-WAN\11.0.2\S Browse...
Upload CA Bundle	

Upload Network Certificates (PEM)	
File:	C:\ID\SD-WAN\11.0.2\S Browse...
Upload Network Bundle	

証明書署名リクエストの作成

アプライアンスは、署名されていない証明書を生成し、証明書署名要求（CSR）を作成できます。CA は、アプライアンスから CSR をダウンロードし、署名して、PEM または DER 形式でアプライアンスにアップロードし直すことができます。これは、アプライアンスのアイデンティティ証明書として使用されます。アプライアンスの CSR を作成するには、アプライアンスの共通名、組織の詳細、およびアドレスを指定します。

Create Certificate Signing Request (CSR)			
Common Name:	<input type="text" value="DC"/>	Business name / Organization:	<input type="text" value="Citrix"/>
Department Name / Organizational Unit:	<input type="text" value="Networks"/>	Town / City:	<input type="text" value="New York"/>
Province, Region, County or State:	<input type="text" value="USA"/>	Country:	<input type="text" value="US"/>
Email address:	<input type="text" value="johndoe@citrix"/>		
<input type="button" value="Create CSR"/>			

証明書失効リストマネージャ

証明書失効リスト（CRL）は、ネットワークで有効でなくなった証明書のシリアル番号の公開リストです。CRL ファイルは定期的にダウンロードされ、すべてのアプライアンスにローカルに保存されます。証明書が認証されると、応答側は CRL を調べて、インシエータ証明書がすでに失効しているかどうかを確認します。Citrix SD-WAN は現在、PEM および DER 形式のバージョン 1 の CRL をサポートしています。

CRL を有効にするには、[CRL 有効] オプションを選択します。CRL ファイルが維持される場所を指定します。HTTP、HTTPS、および FTP の場所がサポートされています。CRL ファイルを確認およびダウンロードする間隔を指定します。範囲は 1 ～1440 分です。

Certificate Revocation List Management (CRL)	
CRL Enabled:	<input checked="" type="checkbox"/>
CRL URI:	<input type="text" value="https://[redacted]/signingc"/>
CRL Update Interval (Minutes):	<input type="text" value="10"/>
<input type="button" value="Update Settings"/>	

注

virtua1 パスの再認証期間は 10 ～15 分です。CRL 更新間隔が短い期間に設定されている場合、更新された CRL リストには現在アクティブなシリアル番号が含まれる場合があります。アクティブ失効した証明書をネットワーク内で短時間利用できるようにする。

AppFlow と IPFIX

September 26, 2023

AppFlow および IPFIX は、ネットワークインフラストラクチャ内のアプリケーションおよびトランザクションデータを識別および収集するために使用されるフローエクスポート標準です。このデータにより、アプリケーショントラフィックの使用率とパフォーマンスの可視性が向上します。

フローレコードと呼ばれる収集されたデータは、1 つ以上の IPv4 または IPv6 コレクタに送信されます。コレクターはフローレコードを集約し、リアルタイムレポートまたは履歴レポートを生成します。

AppFlow

AppFlow は、HDX/ICA 接続のみのフローレベルデータをエクスポートします。HDX データセットテンプレートの TCP のみを有効にすることも、HDX データセットテンプレートを有効にすることもできます。HDX データセット用の TCP のみ [マルチホップデータ](#) を提供します。HDX データセットが [HDX インサイトデータ](#) を提供します。

注

HDX テンプレートは、Citrix SD-WAN PE エディションおよび 2 ボックスアプライアンスでのみ使用できます。これは、データセンターアプライアンス上で有効にする必要があります。

Splunk や Citrix ADM などの AppFlow コレクターには、これらのテンプレートを解釈して表示するためのダッシュボードがあります。

IPFIX

IPFIX は、すべての接続のフローレベルデータをエクスポートするために使用されるコレクタエクスポートプロトコルです。どの接続でも、パケット数、バイト数、サービスの種類、フロー方向、ルーティングドメイン、アプリケーション名などの情報を表示できます。IPFIX フローは、管理インターフェイスを介して送信されます。ほとんどのコレクタは IPFIX フローレコードを受信できますが、IPFIX テンプレートを解釈するためにカスタムダッシュボードを構築する必要がある場合があります。

IPFIX テンプレートは、データストリームが解釈される順序を定義します。コレクタは、テンプレートレコードを受信し、その後にデータレコードを受信します。Citrix SD-WAN では、テンプレート 611 および 613 を使用して IPv4 IPFIX フローデータをエクスポートし、615 および 616 を使用して IPv6 IPFIX フローデータをオプションテンプレート 612 とともにエクスポートします。

アプリケーションフロー情報 (IPFIX) は、IPv4 フローの場合はテンプレート 611、IPv6 フローの場合は 615、アプリケーション情報を含む 612 オプションテンプレートに従ってデータセットをエクスポートします。

基本プロパティ (IPFIX) は、IPv4 フローの場合はテンプレート 613、IPv6 フローの場合は 616 に従ってデータセットをエクスポートします。

次の表に、各 IPFIX テンプレートに関連付けられたフローデータの詳細なリストを示します。

アプリケーションフロー情報 (IPFIX)-V10 テンプレート

テンプレート ID-611

情報要素 (IE)	IE の名前と ID	タイプと長さ	説明
Observation point ID	observationPointId, 138	Unsigned32, 4	
Export process ID	exportingProcessId, 144	Unsigned32, 4	
Flow ID	flowId, 148	Unsigned64, 8	
Ipv4 SRC IP	sourceIPv4Address, 8	Ipv4address, 4	
Ipv4 DST IP	destinationIPv4Address, 12	Ipv4address, 4	
Ipvversion	ipVersion, 60	Unsigned8, 1	4 に設定します。
IP プロトコル番号	protocolIdentifier, 4	Unsigned8, 1	
パディング	-	Unsigned16, 2	
SRC ポート	sourceTransportPort, 7	Unsigned16, 2	
DST ポート	destinationTransportPort, 11	Unsigned16, 2	
Pkt カウント	packetDeltaCount, 2	Unsigned64, 8	
バイト数	octetDeltaCount, 1	Unsigned64, 8	
Time for first pkt in microseconds	flowStartMicroseconds, 154	dateTimeMicroseconds, 8	
Time for lastpkt in microseconds	flowEndMicroseconds, 155	dateTimeMicroseconds, 8	
IP ToS	ipClassOfService, 5	Unsigned8, 1	
Flow Flags	tcpControlBits, 6	Unsigned8, 2	現在 0 に設定されています。
フロー方向	flowDirection, 61	Unsigned8, 1	0x00: 入力フロー 0x01: 出力フロー WAN および LAN-LAN フローが SDWAN の可能性があります

情報要素 (IE)	IE の名前と ID	タイプと長さ	説明
入力インタフェース	ingressInterface, 10	Unsigned32, 4	Citrix SD-WAN は、複数のメンバーパスを介してデータフローを負荷分散するため、単一のデータフローに複数の入力/出力インターフェイスの組み合わせを設定できます。
出力インタフェース	egressInterface, 14	Unsigned32, 4	
入力 VLAN ID	vlanId, 58	Unsigned16, 2	Citrix SD-WAN は、複数のメンバーパスを介してデータフローを負荷分散するため、単一のデータフローに複数の入力/出力インターフェイスの組み合わせを設定できます。
出力 VLAN ID	postVlanId, 59	Unsigned16, 2	
VRF ID	ingressVRFID, 234	Unsigned32, 4	Set to 0x1E037F.
フローキーインジケータ	flowKeyIndicator, 173	Unsigned64, 8	
アプリケーション ID	applicationId, 95	octetArray, variable	アプリケーション ID は、DPI エンジンによって分類されるアプリケーションの ID と同じです。アプリケーション ID は一定のままです。カスタムドメイン名ベースのアプリケーションのアプリケーション ID は、構成が更新されるたびに更新されます。

テンプレート ID: 615 (IPv6 フロー) | 情報エレメント (IE)|IE 名と ID| タイプと len| コメント |

|---|

|Observation point ID|observationPointId, 138|Unsigned32, 4|

|Export process ID|exportingProcessId, 144|Unsigned32, 4|

|Flow ID|flowId, 148|Unsigned64, 8|

|Ipv6 SRC IP|sourceIPv6Address, 27|IPv6address, 16|

|Ipv6 DST IP|destinationIPv6Address, 28|IPv6address, 16|

|IPVersion|IPVersion、60|Unsigned8、
 1|6| |IP プロトコル番号 | プロトコル識別子、4| 署名解除 8、1| |
パディング	N/A	Unsigned16、2		
SRC ポート	ソーストランスポートポート、7	Unsigned16、2		
DST ポート	宛先トランスポートポート、11		Unsigned16、2	
PKT カウント	PacketDeltaCount、2	Unsigned64、8		
バイトカウント	OctetDeltaCount、1	Unsigned64、8		
マイクロ秒の最初の PKT の時間	flowStart マイクロ秒、154	DateTimeMicroSeconds、8		
lstPKT の時間 (マイクロ秒)	flowendMicroSeconds、155	DateTimeMeconds icroSeconds、8		
IPtos	ipclassofService、5	Unsigned8、1		
フローフラグ	TCPControlbits、6	Unsigned8、		
2	現在 0.		フロー方向	フロー方向、61
LAN フローは SDWAN				
入力顔	ingressInterface、10	Unsigned32、4	Citrix SD-WAN は、複数のメンバーパスを介してデータフローの負	
荷を分散するため、単一のデータフローに複数の入力/出力インターフェイスの組み合わせを持つことができます。				
出力インターフェイス	EgressInterface、14	Unsigned32、4	Citrix SD-WAN は、複数のメンバーパスを介してデ	
ータフローの負荷を分散するため、単一のデータフローに複数の入力/出力インターフェイスの組み合わせを持つこ				
とができます。				
入力 VLAN ID	vlanID、58	Unsigned16、2		
出力 VLAN ID	PostvlanID、59	Unsigned16、2		
VRF ID	ingressVrFID、234	Unsigned32、4		
フローキーインジケータ	フローキーインジケータ、173	Unsigned64、8	0x1e00 に設定 37F.	
アプリケーション ID	ApplicationID、95	OctetArray、変数	アプリケーション ID は、DPI エンジンによって分	
 類されたアプリケーションの ID と同じです。アプリケーション ID は一定のままです。カスタムドメイン名ベースの
 アプリケーションのアプリケーション ID は、設定の更新ごとに変更されます。|

テンプレート **612** (オプションテンプレート)

情報要素 (IE)	IE の名前と ID	種類	コメント
アプリケーション ID	applicationId, 95	octetArray	アプリケーション ID は、DPI エンジンによって分類されるアプリケーションの ID と同じです。アプリケーション ID は一定のままです。カスタムドメイン名ベースのアプリケーションのアプリケーション ID は、構成が更新されるたびに変更されます。
アプリケーション名	applicationName, 96	string	Citrix SDWAN 固有のプロプライエタリ・アプリケーションの名前を指定します。
アプリケーションの説明	applicationDescription, 94	string	アプリケーションの説明を指定します。

基本プロパティ (IPFIX) –V9 準拠テンプレート-テンプレート 613 (IPv4 フロー)

情報要素 (IE)	IE の名前と ID	タイプと長さ	コメント
Ipv4 SRC IP	sourceIPv4Address, 8	Ipv4address, 4	
Ipv4 DST IP	destinationIPv4Address, 12	Ipv4address, 4	
Ipvversion	ipVersion, 60	Unsigned8, 1	
IP プロトコル番号	protocolIdentifier, 4	Unsigned8, 1	
IP ToS	ipClassOfService, 5	Unsigned8, 1	
フロー方向	flowDirection, 61	Unsigned8, 1	0x00: 入力フロー 0x01: 出力フロー WAN および LAN-LAN フローが SDWAN の可能性があります
SRC ポート	sourceTransportPort, 7	Unsigned16, 2	
DST ポート	destinationTransportPort, 11	Unsigned16, 2	
Pkt カウント	packetDeltaCount, 2	Unsigned64, 8	

情報要素 (IE)	IE の名前と ID	タイプと長さ	コメント
バイト数	octetDeltaCount, 1	Unsigned64, 8	
入力インターフェース	ingressInterface, 10	Unsigned32, 4	Citrix SD-WAN は、複数のメンバーパスを介してデータフローを負荷分散するため、単一のデータフローに複数の入力/出力インターフェースの組み合わせを設定できます。
出力インターフェース	egressInterface, 14	Unsigned32, 4	
入力 VLAN ID	vlanId, 58	Unsigned16, 2	Citrix SD-WAN は、複数のメンバーパスを介してデータフローを負荷分散するため、単一のデータフローに複数の入力/出力インターフェースの組み合わせを設定できます。
出力 VLAN ID	postVlanId, 59	Unsigned16, 2	

テンプレート ID: **616** (IPv6 フロー) | 情報エレメント (IE)|IE 名と ID| タイプと len| コメント |
 |---|
 |ipv6 SRC IP|sourceIPv6Address, 27|IPv6address, 16|
 |ipv6 DST IP|destinationIPv6Address, 28|IPv6address, 16|
 |IPVersion|IPVersion, 60|Unsigned8,
 1|6| |IP
 プロトコル番号 | プロトコル番号 | プロトコル番号,4|unsigned8, 1| |IP 転位 |ipclassofService,
 5| 署名解除 8, 1| | フロー方向 | フロー方向, 61|Unsigned8, 1|0x00: 入力フロー 0x01: 出力フロー WAN お
 よび LAN-LAN フローは SDWAN|
 |SRC ポート |SourceTransportPort, 7|Unsigned16, 2| |
 |DST ポート |DestinationTransportPort,
 11|Unsigned16, 2| |PKT カウント |PacketDeltaCount,
 2|Unsigned64, 8| | バイトカウント |OctetDeltaCount, 1|Unsigned64, 8|
 入力インターフェース |ingressInterface, 10|Unsigned32,4|Citrix SD-WAN は、複数のメンバーパスを介してデ
 ータフローの負荷分散を行うため、単一のデータフローに複数の入力/出力インターフェースの組み合わせを持つこと
 ができます。 |
 | 出力インターフェース |EgressInterface, 14|Unsigned32, 4|Citrix SD-WAN は、複数のメンバーパスを介してデ
 ータフローの負荷を分散するため、単一のデータフローに複数の入力/出力インターフェースの組み合わせを持つこと

ができます。|

| 入力 VLAN ID|vlanID、58|Unsigned16、2||

| 出力 VLAN ID|PostvlanID、59|Unsigned16、2|

制限事項

- AppFlow は、IPv6 コレクタおよびフローレコードをサポートしていません。
- Net Flow のエクスポート間隔が 15 秒から 60 秒に増加します。
- AppFlow/IPfix フローは UDP 経由で送信され、接続が失われた場合、すべてのデータが再送信されるわけではありません。エクスポート間隔が X 分に設定されている場合、アプライアンスは X 分のデータのみを保存します。接続損失の X 分後に再送信されます。
- Citrix SD-WAN では、リリース 10 バージョン 2 では、**AppFlow** の設定はすべてのアプライアンスにローカルに設定されていますが、以前のリリースではグローバル設定でした。SD-WAN ソフトウェアリリースが以前のリリースのいずれかにダウングレードされ、いずれかのアプライアンスで AppFlow が設定されている場合は、すべてのアライアンスにグローバルに適用されます。

AppFlow/IPFIX の設定

AppFlow/IPFIX を個別の SD-WAN アプライアンスで構成することも、SD-WAN Center で構成して、アプライアンスグループに構成をプッシュすることもできます。

SD-WAN アプライアンスで AppFlow /IPFIX を構成するには:

1. Citrix SD-WAN SE/PE Web インターフェイスで、[構成] > [AppFlow/IPFIX] に移動します。
2. [有効] をクリックします。

3. [**Data Update Interval**] フィールドで、フローレポートを AppFlow/IPFIX コレクタにエクスポートする時間間隔を分単位で指定します。最大間隔は 10 分です。
4. **AppFlow** データセットテンプレートを選択すると、次のいずれかのデータセットテンプレートを選択できます。
 - **HDX 専用 (AppFlow)**: ICA 接続のマルチホップデータを収集して AppFlow コレクターに送信するための AppFlow データセットテンプレート。
 - **HDX (AppFlow)**: ICA 接続の HDX インサイトデータを収集して AppFlow コレクターに送信するための AppFlow データセットテンプレート。

注

HDX テンプレートは、Citrix SD-WAN PE および Two Box アプライアンスでのみ使用できます。

5. 最大 4 つの AppFlow または IPFIX コレクタを設定できます。各コレクタに対して、次のパラメータを指定します。
 - **IP アドレス**: 外部 AppFlow /IPFIX コレクタ・システムの IP アドレス。

- ポート：外部 AppFlow /IPFIX コレクタ・システムがリッスンするポート番号。デフォルト値は 4739 です。ポート番号は、使用するコレクタに応じて変更できます。
- アプリケーションフロー情報 (**IPFIX**)：IPFIX テンプレート 611、615、および 612 に従ってフローレコードを IPFIX コレクタに送信します。
- 基本プロパティ (**IPFIX**)：IPFIX テンプレート 613 および 616 に従って、フローレコードを IPFIX コレクタに送信します。
- **Citrix ADM**：Citrix ADM を AppFlow コレクターとして使用するには、これを選択します。

注

- Citrix ADM は現在、IPFIX 収集をサポートしていません。
- Citrix ADM は、AppFlow および IPFIX 用の IPv6 アドレスをサポートしていません。

- **Citrix ADM ユーザー**：Citrix ADM コレクターのユーザー名
- **パスワード**：Citrix ADM コレクタのパスワード。

ユーザー名とパスワードは、Citrix ADM にシームレスにログインしてフローデータを保存するために使用されます。

6. [設定の適用] をクリックします。

SD-WAN Center を使用して **AppFlow /IPFIX** コレクタを構成するには：

1. Citrix SD-WAN Center 管理 UI で、[構成] > [アプライアンスの設定] に移動します。
2. 「**AppFlow/IPFIX**」セクションに移動し、「ファイルに含める」を選択します。
3. [**IPFIX /AppFlow** 収集を有効にする] を選択します。

4. [データ更新間隔] フィールドで、AppFlow レポートが AppFlow/IPFIX コレクターにエクスポートされる時間間隔を分単位で指定します。

5. **AppFlow** データセット テンプレートを選択すると、次のいずれかのデータセットテンプレートを選択できます。

- **HDX** のみの **TCP**: ICA 接続のマルチホップデータを収集して AppFlow コレクターに送信する AppFlow データセットテンプレート。
- **HDX**: ICA 接続の HDX インサイトデータを収集して AppFlow ow コレクターに送信するための AppFlow データセットテンプレート。

注

HDX テンプレートは、Citrix SD-WAN PE および Two Box アプライアンスでのみ使用できます。

6. 最大 4 つの AppFlow または IPFIX コレクタを設定できます。各コレクタに対して、次のパラメータを指定します。

- **IPFIX/AppFlow** コレクタ: 外部 AppFlow/IPFIX コレクタシステムの IP アドレス。
- ポート: 外部 AppFlow /IPFIX コレクタ・システムがリッスンするポート番号。デフォルト値は 4739 です。ポート番号は、使用するコレクタに応じて変更できます。
- アプリケーションフロー情報: IPFIX テンプレート 611、615、および 612 に従って IPFIX コレクタにフローレコードを送信します。
- 基本プロパティ (**IPFIX**): IPFIX テンプレート 613 および 616 に従って、フローレコードを IPFIX コレクタに送信します。
- **Citrix ADM**: Citrix ADM を AppFlow コレクターとして使用するには、これを選択します。

注

Citrix ADM は現在、IPFIX 収集をサポートしていません。

- **Citrix ADM** ユーザー: Citrix ADM コレクターのユーザー名。
- パスワード: Citrix ADM コレクタのパスワード。

ユーザー名とパスワードは、Citrix ADM にシームレスにログインしてフローデータを保存するために使用されます。

7. 設定を保存し、管理アプライアンスにエクスポートします。

注

SD-WAN Center のバージョンが 10.2 より低く、SD-WAN アプライアンスのバージョンが 10.2 以降の場合は、次の条件を満たすことができます。

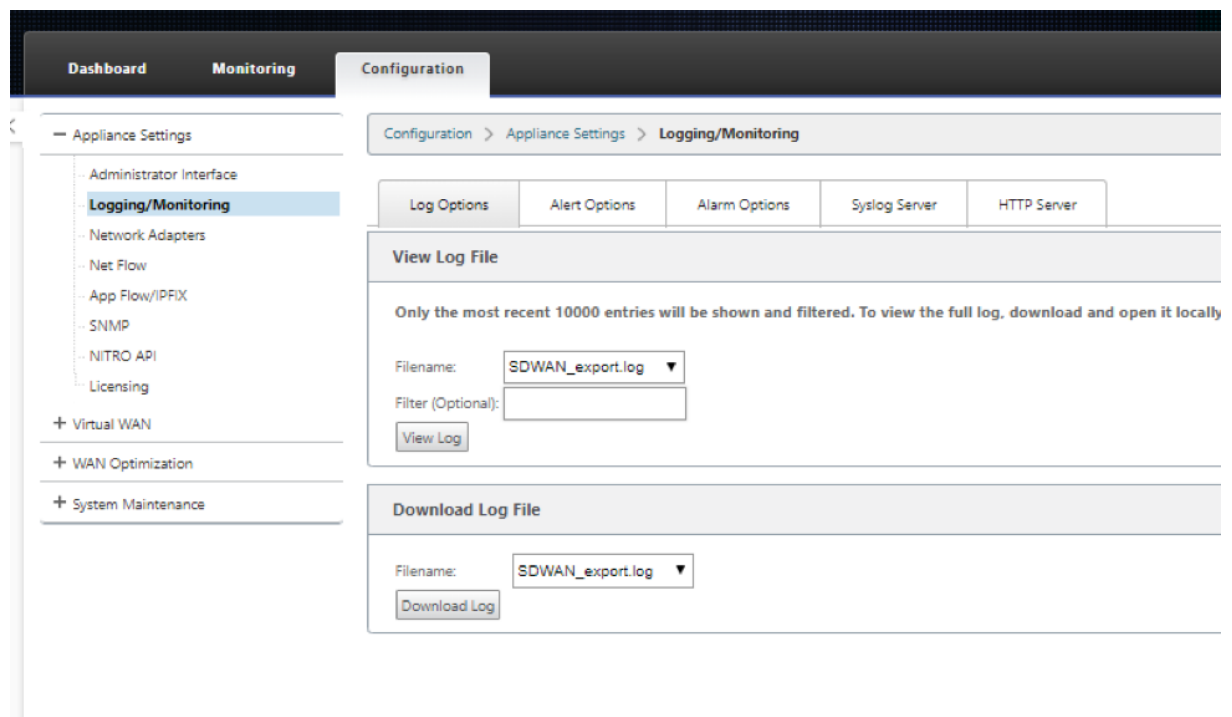
- アプライアンスでローカルコレクタが有効になっている場合、SD-WAN Center からプッシュされた AppFlow および IPFIX 設定は既存の設定に影響しません。
- アプライアンスでローカルコレクタが有効になっていない場合、SD-WAN Center からプッシュされた

AppFlow/IPFIX 設定がアプライアンスに適用されます。

- SD-WAN Center 構成でグローバルな AppFlow/IPFIX 構成が有効になっている場合、アプライアンスですべてのローカルコレクタが有効になります。

ログファイル

AppFlow/IPFIX エクスポートプロトコルに関連する問題のトラブルシューティングについては、SD-WAN_export.log ファイルを表示およびダウンロードできます。[構成] > [ログ記録/監視] に移動し、**SDWAN_Export.log** ファイルを選択します。



SNMP

November 17, 2022

Citrix SD-WAN は、SNMPV1/V2 機能をサポートし、SNMPv3 機能ごとに 1 つのユーザーアカウントのみをサポートします。この制限により、次の利点があります。

- ネットワークデバイスの SNMPv3 コンプライアンスの確保
- SNMPv3 機能の検証
- SNMPv3 の容易な設定

SNMPv3 のポーリングおよびトラップを構成するには、[構成] > [アプライアンスの設定] > [**SNMP**] ページの [SNMPv3] セクションに移動し、必要に応じてフィールドに入力します。

注：

IPv6 アドレスを構成するには、SNMP サーバーも IPv6 アドレスで構成されていることを確認してください。

DashboardMonitoringConfiguration

<

Appliance Settings

Administrator Interface

Logging/Monitoring

Network Adapters

Net Flow

App Flow

SNMP

NITRO API

Licensing

+ Virtual WAN

+ System Maintenance

Configuration > Appliance Settings > SNMP

ManagersDownload MIB File

SNMP

UDP Port:161

System Description:Citrix Virtual WAN Appliance

System Contact:support@citrix.com

System Location:Citrix

SNMP v1/v2

☐ Enable v1/v2 Agent

Community String:public

☐ Enable v1/v2 Traps

Send v1/v2 Test Trap

Destination IP Address(es):

Port:162

SNMP v3

☐ Enable v3 Agent

User Name:

Password:

Verify Password:

Authentication:MD5

Encryption:None

☐ Enable v3 Traps

Send v3 Test Trap

Destination IP Address(es):

Port:162

User Name:

Password:

Verify Password:

Authentication:MD5

Encryption:None

Apply Settings

標準 **MIB** サポート

SD-WAN アプライアンスでは、次の標準 MIB がサポートされています。

MIB	RFC (定義リンク)
DISMAN-EVENT-MIB	https://www.ietf.org/rfc/rfc2981.txt
IF-MIB	https://www.ietf.org/rfc/rfc2863.txt
IP-FORWARD-MIB	https://www.ietf.org/rfc/rfc4292.txt
IP-MIB (部分)	https://www.ietf.org/rfc/rfc4293.txt
Q-BRIDGE-MIB (部分)	http://www.ieee802.org/1/files/public/MIBs/IEEE8021-Q-BRIDGE-MIB-201112120000Z.mib
RFC1213-MIB	https://www.ietf.org/rfc/rfc1213.txt
SNMPv2-MIB	https://www.ietf.org/rfc/rfc3418.txt
TCP-MIB	https://www.ietf.org/rfc/rfc4022.txt
P-BRIDGE-MIB.txt	http://www.icir.org/fenner/mibs/extracted/P-BRIDGE-MIB-rfc2674.txt
RMON2-MIB.txt	https://www.ietf.org/rfc/rfc3273.txt
TOKEN-RING-RMON-MIB.txt	http://www.icir.org/fenner/mibs/extracted/TOKEN-RING-RMON-MIB-rmonmib-01.txt

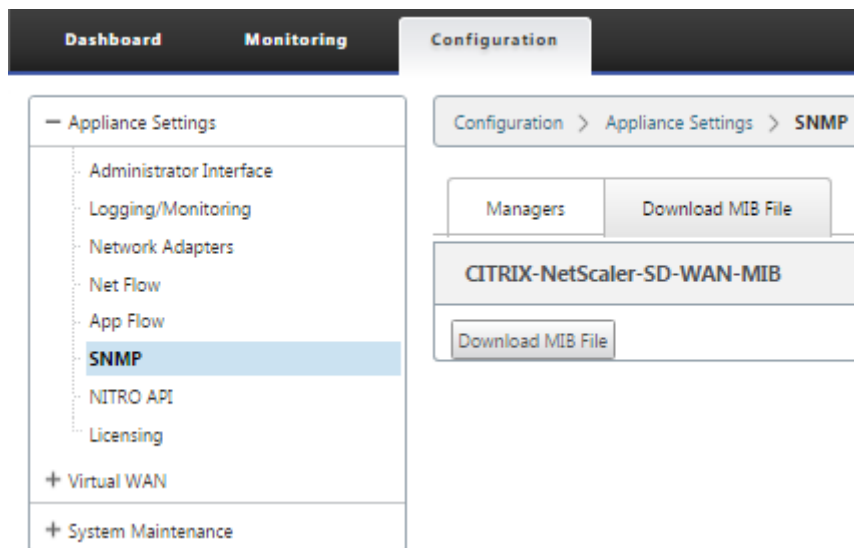
Citrix SD-WAN アプライアンスの監視を開始する前に、次の SNMP ファイルをダウンロードする必要があります。

- CITRIX-COMMON-MIB.txt
- APPACCELERATION-SMI.txt
- APPACCELERATION-PRODUCTS-MIB.txt
- APPACCELERATION-TC.txt
- APPACCELERATION-STATUS-MIB.txt
- APPCACHE-MIB.txt
- SDX-MIB-smiv2.mib

MIB ファイルは、SNMPv3 マネージャおよび SNMPv3 トラップリスナーによって使用されます。このファイルには、SD-WAN アプライアンスのエンタープライズ MIB が含まれており、SD-WAN 固有のイベントが提供されます。MIB ファイルをダウンロードするには、SD-WAN Web 管理インターフェイスで次の手順を実行します。

1. 設定 > アプライアンスの設定 > **SNMP** > **MIB** ファイルのダウンロードページに移動します **。
2. 必要な **MIB** ファイルを選択します。
3. [表示] をクリックします。

MIB ファイルが MIB ブラウザで開きます。



注

- これらの MIB のサポートは、Linux システム上の **net-snmp snmpd** デーモンプロセスによってデフォルトで提供されます。MIB は、ネットワーク管理アプリケーションをサポートするための基礎となります。
- イーサネットポートのパケットカウンタとバイトカウンタは、****ifTable** 内の IF-MIB** にあります。システム情報は、システムオブジェクトにあります。
- イーサネットポートは **ifTable** に含まれているため、SNMP サブシステムが動作していることを確認するには、このウォーキングで十分である必要があります。
- **Q-BRIDGE-MIB** と **IP-MIB** のサポートにより、ネットワークマッピングアプリケーションのサポートが提供されます。

管理インタフェース

May 10, 2021

Citrix SD-WAN アプライアンスは、次の管理オプションを使用して管理および保守できます。

- ユーザーアカウント

- RADIUS サーバー
- TACACS+ サーバ
- HTTPS 証明書
- HTTPS 設定
- その他

ユーザーアカウント

[構成] > [アプライアンスの設定] > [管理者インターフェイス] ページ > [ユーザーアカウント] タブで、新しいユーザーアカウントを追加し、既存のユーザーアカウントを管理できます。

新しく追加されたユーザーアカウントは、SD-WAN アプライアンスによるローカルまたはリモート認証のいずれかを選択できます。リモートで認証されるユーザーアカウントは、RADIUS または TACACS+ 認証サーバを使用して認証されます。

ユーザーロール

次のユーザーロールがサポートされています。

- ビューアー: ビューアーアカウントは、ダッシュボード、レポート、監視の各ページにアクセスできる読み取り専用アカウントです。
- 管理者: 管理者アカウントには、管理者権限があり、すべてのセクションに対する読み取り/書き込みアクセス権があります。

特権管理者 (admin) には以下の特権があります。

- 構成を変更管理インボックスにエクスポートして、ネットワークへの構成とソフトウェアの更新を実行できます。
- ネットワーク管理者とセキュリティ管理者の読み取り/書き込みアクセスを切り替えることもできます。
- ネットワークおよびセキュリティ関連の設定を維持します。
- セキュリティ管理者: セキュリティ管理者は、構成エディタのファイアウォールとセキュリティ関連の設定に対してのみ読み取り/書き込みアクセス権を持ち、残りのセクションには読み取り専用アクセス権があります。セキュリティ管理者は、スーパー管理者 (admin) 以外の他のユーザーに対して、ファイアウォールへの書き込みアクセスを有効または無効にすることもできます。
- ネットワーク管理者: ネットワーク管理者は、すべてのセクションに対する読み取り/書き込み権限を持ち、構成エディタのファイアウォールおよびセキュリティ関連の設定を除き、ブランチを完全にプロビジョニングできます。ホストされているファイアウォールノードは、ネットワーク管理者が利用できません。この場合、ネットワーク管理者は新しい構成をインポートする必要があります。

ネットワーク管理者とセキュリティ管理者の両方が、設定を変更し、ネットワーク上に展開することもできます。

注

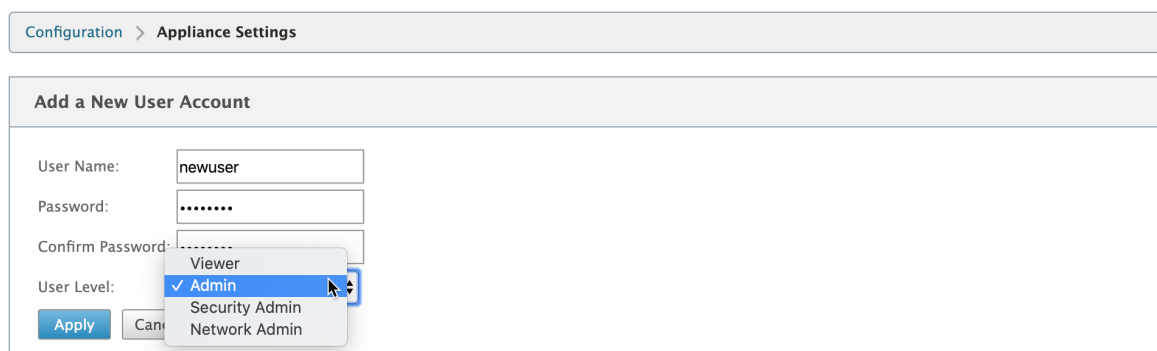
ネットワーク管理者およびセキュリティ管理者は、ユーザーアカウントを追加または削除できません。編集できるのは自分のアカウントのパスワードのみです。

The screenshot displays the Citrix SD-WAN VPX-50-SE Administrator Interface. The top navigation bar includes 'Dashboard', 'Monitoring', and 'Configuration'. The 'Configuration' tab is active, and the left sidebar shows 'Appliance Settings' with 'Administrator Interface' selected. The main content area is titled 'Configuration > Appliance Settings > Administrator Interface'. It contains several sections: 'User Accounts' (with sub-tabs for RADIUS, TACACS+, HTTPS Cert, HTTPS Settings, and Miscellaneous), 'Change Local User Password' (with fields for User Name, Current Password, New Password, and Confirm New Password), 'Delete Workspace For User' (with a User Name field and a 'Delete Selected User's Workspace' button), 'Manage Users' (with an 'Add User...' button and a 'Delete Selected User' button), and 'Firewall Access' (with a 'Disable Firewall Access' button). The 'User Name' field in all sections is set to 'admin'.

ユーザーの追加

ユーザーを追加するには、[ユーザーの管理] セクションの [ユーザーの追加] をクリックします。** ユーザ名とパスワードを入力します。[User **Level] ドロップダウンリストからユーザーロールを選択し、[Apply] をクリックします。

必要に応じて、ユーザーアカウントを削除することもできます。ユーザーを削除すると、そのユーザーに属するローカルファイルも削除されます。削除するには、[ユーザーの管理] セクションで、[ユーザー名] ドロップダウンリストからユーザーを選択し、[選択したユーザーの削除] をクリックします。



ユーザーのパスワードを変更する

管理者ロールは、SD-WAN アプライアンスによってローカルで認証されるユーザーアカウントのパスワードを変更できます。

パスワードを変更するには、[ローカルユーザーパスワードの変更] セクションで、[ユーザー名] ドロップダウンリストからユーザーを選択します。現在のパスワードと新しいパスワードを入力します。[パスワードの変更] をクリックします。

ユーザーのワークスペースの削除

ユーザーの [構成エディター] ワークスペースを削除できます。ワークスペースを削除しても、ユーザーアカウントは削除されません。選択したユーザーの保存済み設定とネットワークマップがすべて削除されます。

ユーザーのワークスペースを削除するには、「ユーザーのワークスペースの削除」セクションで、「ユーザー名」ドロップダウンリストからユーザーを選択します。[選択したユーザーのワークスペースを削除] をクリックします。

ファイアウォールへのアクセスを無効にする

ユーザーアカウントへのファイアウォールアクセスを無効にすることができます。無効にするには、[ユーザー名] ドロップダウンリストからユーザーを選択し、[ファイアウォールアクセスを無効にする] をクリックします。

RADIUS サーバー

1 台または 3 台の RADIUS サーバでユーザーアクセスを認証するように SD-WAN アプライアンスを設定できます。デフォルトのポートは 1812 です。

RADIUS サーバを構成するには、次の手順を実行します。

1. [構成] > [アプライアンス設定] > [管理者インターフェース] > [RADIUS] に移動します。

2. [**RADIUS** を有効にする] チェックボックスをオンにします。
3. サーバの **IP** アドレスと認証ポートを入力します **。最大 3 つのサーバ IP アドレスを構成できます。

注:

IPv6 アドレスを構成するには、RADIUS サーバにも IPv6 アドレスが設定されていることを確認してください。

4. サーバキーを入力し、確定します。
5. タイムアウト値を秒単位で入力します。
6. [保存] をクリックします。

RADIUS サーバ接続をテストすることもできます。** ユーザ名とパスワードを入力します。[Verify] ** をクリックします。

Configuration > Appliance Settings > Administrator Interface

User Accounts	RADIUS	TACACS+	HTTPS Cert	HTTPS Settings	Miscellaneous
---------------	---------------	---------	------------	----------------	---------------

RADIUS

Enable RADIUS ☒

Server 1 IP Address: Authentication Port:

Server 2 IP Address (Optional): Authentication Port:

Server 3 IP Address (Optional): Authentication Port:

Server Key:

Confirm Server Key:

Timeout (seconds): (Optional)

Test RADIUS Server Connection

User Name:

Password:

TACACS+ サーバ

TACACS+ サーバを認証用に設定できます。RADIUS 認証と同様に、TACACS+ は秘密キー、IP アドレス、およびポート番号を使用します。デフォルトのポート番号は 49 です。

TACACS+ サーバを設定するには、次の手順を実行します。

1. [構成] > [アプライアンス設定] > [管理者インターフェース] > [**TACACS+**] に移動します。
2. [**TACACS+** を有効にする] チェックボックスをオンにします。
3. サーバの **IP** アドレスと認証ポートを入力します **。最大 3 つのサーバ IP アドレスを構成できます。

注:

IPv6 アドレスを設定するには、TACACS+ サーバにも IPv6 アドレスが設定されていることを確認します。

4. [認証タイプ] として [**PAP**] または [**ASCII**] を選択します。

- PAP: パスワード認証プロトコル (PAP) を使用して、強力な共有秘密を TACACS+ サーバに割り当てることにより、ユーザ認証を強化します。
- [ASCII]: ASCII 文字セットを使用して、強力な共有秘密を TACACS+ サーバに割り当てることにより、ユーザ認証を強化します。

5. サーバキーを入力し、確定します。

6. タイムアウト値を秒単位で入力します。

7. [保存] をクリックします。

TACACS+ サーバ接続をテストすることもできます。 ** ユーザ名とパスワードを入力します。[Verify] ** をクリックします。

Configuration > Appliance Settings > Administrator Interface

User Accounts	RADIUS	TACACS+	HTTPS Cert	HTTPS Settings	Miscellaneous
TACACS+					
Enable TACACS+ <input checked="" type="checkbox"/>					
Server 1 IP Address:		f1f75:20389:58489:27:8916:3a0ff:fe85:a15e		Authentication Port: 49	
Server 2 IP Address (Optional):				Authentication Port:	
Server 3 IP Address (Optional):				Authentication Port:	
Authentication Type: <input checked="" type="radio"/> PAP <input type="radio"/> ASCII					
Server Key:					
Confirm Server Key:					
Timeout (seconds):		(Optional)			
<input type="button" value="Apply"/>					
Test TACACS+ Server Connection					
User Name:					
Password:					
<input type="button" value="Verify"/>					

NDP ルータアドバタイズメントおよびプレフィクス委任グループ

May 10, 2021

NDP ルータアドバタイズメント

IPv6 ネットワークでは、SD-WAN アプライアンスは Router Advertisement (RA; ルータアドバタイズメント) メッセージを定期的にマルチキャストして、その可用性を通知し、SD-WAN ネットワーク内の隣接アプライアンスに情報を伝達します。ルータアドバタイズメントには、IPv6 プレフィクス情報が含まれます。SD-WAN アプライアンスで実行されている Neighbor Discovery Protocol (NDP; 近隣探索プロトコル) は、これらのルータアドバタイズメントを使用して、同じリンク上のネイバーデバイスを判別しますまた、相互のリンクレイヤアドレスを決定し、ネイバーを検索し、アクティブなネイバーへのパスに関する到達可能性情報を保持します。

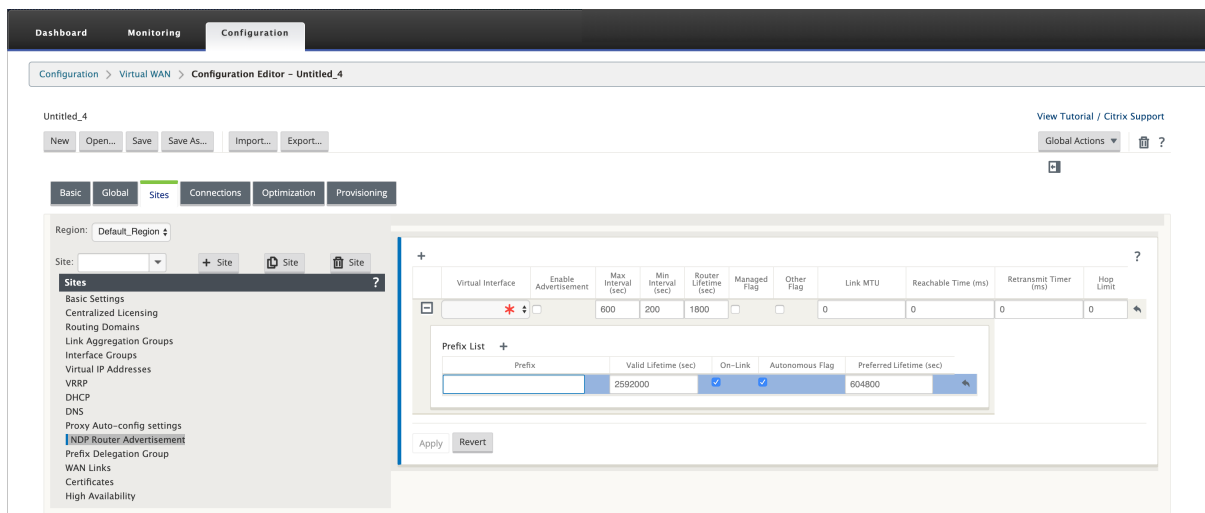
NDP ルータアドバタイズメントを設定するには、

1. 構成エディタで、[サイト] > [NDP ルーターアドバタイズメント] に移動します。
2. [+] をクリックし、[Virtual Interface] ドロップダウンリストで設定した仮想インターフェイスの 1 つを選択します。
3. [**Enable Advertisement**] チェックボックスをオンにして、選択した仮想インターフェイスの定期的なルータアドバタイズメントの送信とルータ要請への応答を有効にします。
4. 最大、最小、およびルータのライフタイム間隔を指定します。
 - [最大間隔]: 定期的な迷惑マルチキャストルータアドバタイズメントを送信するまでの最大許容時間 (秒単位)。
 - **Min Interval**: 定期的な未承諾マルチキャストルータアドバタイズメントを送信する間隔の最小時間 (秒単位)。
 - **Router Lifetime**: ルータがホストによって有効と見なされる時間 (秒)。0 は、ルータをデフォルトルータとして使用できないことを示します。
5. DHCPv6 プロトコルで IP アドレスを使用できる場合は、[管理フラグ] チェックボックスをオンにします。
6. DHCPv6 プロトコルを介して構成情報 (IP アドレス以外) を使用できる場合は、[Other Flag] チェックボックスをオンにします。
7. 選択したインターフェイスに対して、次の値を指定します。
 - リンク **MTU**: インターフェイスの推奨最大伝送ユニット (MTU)。
 - 到達可能時間: **NDP** プロトコルが到達可能な状態のままである時間 (ミリ秒単位)。
 - 再送信タイマー: IP アドレスを解決するか、ネイバーをプローブするときのネイバー送信要求メッセージの再送信間隔 (ミリ秒単位)。
 - **Hop Limit**: ルータアドバタイズメントに含めるホップの最大数。
8. プレフィクスに関連付けられた詳細を入力します。
 - プレフィクス: クラスレスドメイン間ルーティング (CIDR) 表記でのプレフィクスとプレフィクスの長さ。
 - 有効有効期間: プレフィックスが有効になるまでの時間 (秒)。-1 は無限を表し、プレフィックスが永遠に残ることを意味します。

- オンリンク: 選択すると、プレフィックスはネットワークに対してローカルと見なされます。
- 自律フラグ: 有効にすると、IP アドレスを生成するために、ホストのステートレスアドレス自動構成 (SLAAC) によってプレフィックスが使用されます。
- プレフィックス有効期間: プレフィックスが優先と見なされるまでの時間 (秒単位)。

9. [適用] をクリックします。

10. NDP ルータアダプタイズメント用の仮想インターフェイスをさらに構成するには、[+] をクリックします。



プレフィックス委任グループ

注:

Citrix SD-WAN 11.3 リリースでは、プレフィックス委任はサポートされていません。

Citrix SD-WAN アプライアンスは、DHCPv6 クライアントとして構成し、構成された WAN ポートを使用して ISP にプレフィックスを要求できます。Citrix SD-WAN アプライアンスがプレフィックスを受信すると、そのプレフィックスを使用して、LAN クライアントに対応するための IP アドレスのプールが作成されます。その後、Citrix SD-WAN アプライアンスは DHCP サーバーとして動作し、LAN ポート上のプレフィックスを LAN 側のクライアントにアドバタイズします。

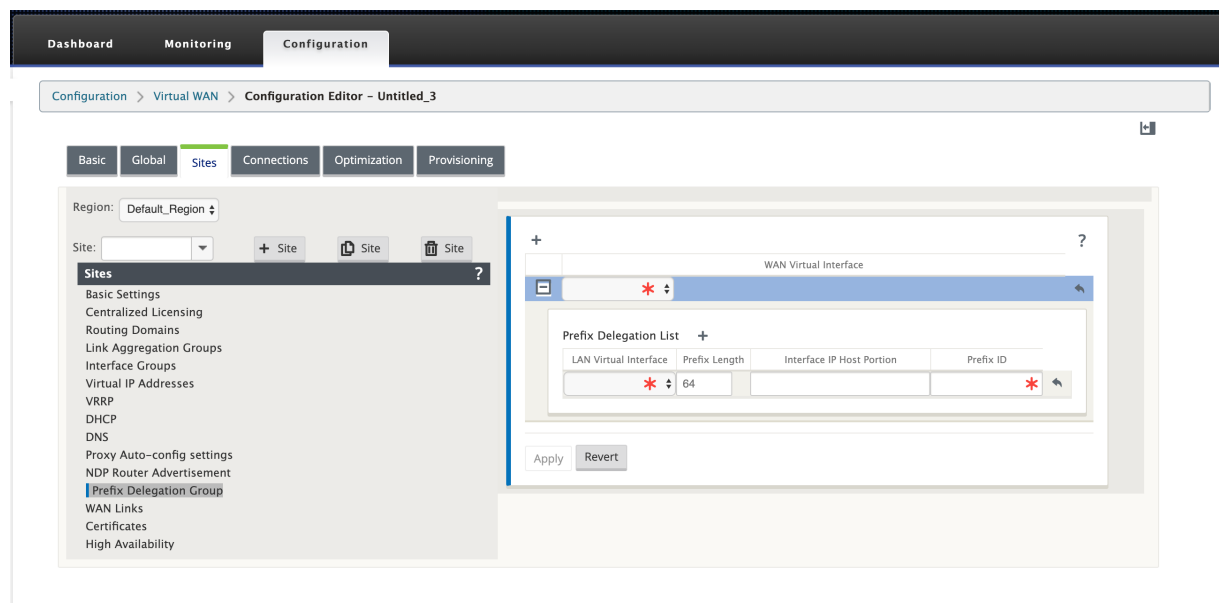
プレフィックス委任を設定するには、

1. 構成エディタで、[サイト] > [プレフィックス委任グループ] に移動します。
2. [+] をクリックし、ISP からプレフィックスが要求される設定済みの WAN 仮想インターフェイスを選択します。
3. 次の詳細を入力します。
 - **LAN** 仮想インターフェイス: プレフィックスが要求される設定済みの LAN 仮想インターフェイスのいずれかを選択します。
 - プレフィックス長: プレフィックスの一部であるグローバルユニキャスト IPv6 アドレスのビット数。

- インターフェイス **IP** ホスト部分: インターフェイスの IP アドレスに使用されるホスト部分。
- プレフィックス **ID**: LAN インターフェイスのプレフィックス委任要求を識別する一意の識別子。

4. [適用] をクリックします。

5. プレフィックス委任グループの一部としてさらに多くの WAN 仮想インターフェイスを設定するには、[+] をクリックします。



WAN の最適化

May 10, 2021

Citrix SD-WAN WANOP アプライアンスは、WAN リンクを最適化し、最大限の応答性とスループットを確保します。Citrix SD-WAN WANOP アプライアンスは、リンクの両端で 1 つずつペアで動作し、リンク上のトラフィックを高速化します。以下は、Citrix の SD-WAN の機能の一部です WANOP-

- 圧縮
- TCP プロトコルアクセラレーション
- トラフィック管理
- アプリケーションアクセラレーション
- Citrix の XenApp/XenDesktop (HDX) アクセラレーション
- 統合
- 監視と管理

Citrix SD-WAN WANOP 10.2 のインストール、展開、および機能の構成については、[Citrix SD-WAN WANOP](#) ドキュメントを参照してください。Citrix SD-WAN WANOP 10.2 の機能と手順は、Citrix SD-WAN WANOP リリースに記載されている手順と似ています。

Citrix SD-WAN Premium エディションで WAN 最適化機能を有効にして構成できます。詳細については、Citrix SD-WAN [「Premium Edition」](#) を参照してください。

WANOP Client Plug-in ソフトウェアを使用して、リモート Windows のラップトップまたはワークステーションでネットワークアクセラレーションを実現できます。詳しくは、[「WANOP クライアントプラグイン」](#) を参照してください。

Citrix SD-WAN Premium Edition

May 10, 2021

このセクションでは、仮想 WAN に対して SD-WAN Premium (エンタープライズ) エディションの WAN Optimization 機能を有効にして構成する手順を説明します。これを行うには、MCN の Web 管理インターフェイスで、構成エディターの [最適化] セクションフォームを使用します。

注

仮想 WAN の WAN Optimization 機能へのアクセス、有効化、構成、およびアクティブ化を行うには、SD-WAN Premium (Enterprise) Edition ライセンスをインストールしておく必要があります。SD-WAN Standard Edition では、これらの機能はサポートされていません。

最適化 セクションセットとパラメータを設定するには、最上位レベルの 2 つのステップがあります。これらは、依存性の順にリストされています。

1. WAN Optimization を有効にして、デフォルト 設定をカスタマイズするか、デフォルトをそのまま使用します。

デフォルト 構成は、WAN **Optimization** の対象となるすべてのサイトの基本最適化構成として使用されます。デフォルト の設定は事前に設定されており、カスタマイズできます。

注:

手順については、[最適化の有効化とデフォルト設定の構成](#)を参照してください。

2. (オプション) 個々のブランチサイトごとに WAN Optimization 設定をカスタマイズするか、それぞれの **Defaults** セットと設定をそのまま使用します。

デフォルトでは、デフォルト 構成は、WAN Optimization の対象となる各ブランチサイトに最初に適用されます。WAN Optimization は、1000-EE (Premium Edition) および 2000-EE (Premium Edition) のハードウェアアプライアンスでのみサポートされます。サポートされているブランチサイトごとに、既定のセ

ットと設定の組み合わせ、またはこれらのサブセットを受け入れるか変更するかを選択できます。手順については、「[ブランチサイトの最適化の構成](#)」を参照してください。

これらの手順を完了するには、構成エディタの「最適化」セクションで構成フォームを使用します。「最適化」セクションは、次のように構成されています。

- **Defaults—Defaults** ブランチには、次の子ブランチが含まれます。子ブランチには、それぞれのセットと設定を構成するための 1 つ以上のフォームが含まれます。
 - 既定の機能
 - デフォルトのチューニング設定
 - デフォルトアプリケーション分類子 (セット)
 - デフォルトのサービスクラス (セット)
- **** <Client Site Name>—**Optimization** セクション構成ツリーには、**WAN Optimization** をサポートする各クライアントノード (ブランチサイト) のブランチが含まれています。クライアントノードがサポートされていないアプライアンスモデルの場合、サイトは **Optimization** セクション構成ツリーに含まれません。ツリー内の各ブランチには、次の子ブランチが含まれています。これらの子ブランチには、それぞれのセットと設定を構成するための 1 つ以上のフォームが含まれます。
 - 既定の機能
 - デフォルトのチューニング設定
 - デフォルトのアプリケーション分類子 (セット)
 - デフォルトのサービスクラス (セット)

次のセクションでは、仮想 WAN で WAN Optimization を有効にし、デフォルトのセットと設定を構成する方法について説明します。

最適化を有効化し、デフォルトの機能設定を構成する

May 10, 2021

仮想 WAN で WAN Optimization を有効にするには、次の手順を実行します。

1. [最適化] セクションの [**** 機能**] 設定で WAN Optimization を有効にします。 **

このセクションには、プロセスのこの部分の手順が記載されています。

2. [サービスクラス] テーブルで、該当するサービスクラスごとに [**** アクセラレーション**] ポリシー設定を構成します。 **

この手順は、残りの最適化構成を完了した後、でさらに実行されます。手順については、「[最適化のデフォルトサービスクラスの設定](#)」の項を参照してください。この時点で、構成で WAN Optimization が有効になっていますが、仮想 WAN ではまだ有効になっていません。仮想 WAN で WAN Optimization を有効にしてアクティブ化するには、このガイドの以降の章で説明するように、仮想 WAN 構成を完了し、展開内の適格なサイトで仮想 WAN アプライアンスパッケージを生成し、ステージングし、アクティブ化する必要があります。

WAN Optimization を有効にして、[既定] セクションの [機能] 設定を構成するには、次の手順を実行します。

- a) 必要に応じて、管理 Web インターフェイスにログインし直して、構成エディタを開きます。

構成エディタを開くには、次の操作を行います。

- i. ページ上部の [構成] タブを選択して、[構成] ナビゲーション・ツリー（左ペイン）を開きます。
- ii. ナビゲーションツリーで、**Virtual WAN** ブランチの左側にある [+] をクリックして、そのブランチを開きます。
- iii. [仮想 **WAN**] ブランチで、[構成エディタ] を選択します。

- b) 変更する構成パッケージを開きます。

[開く] をクリックして [構成パッケージを開く] ダイアログボックスを表示し、[保存されたパッケージ] ドロップダウンメニューからパッケージを選択します。

これにより、選択したパッケージが構成エディタにロードされ、編集用を開きます。

WAN Optimization 機能を含む有効な現在のライセンスをお持ちの場合は、構成エディタの [最適化] セクションを使用できます。

注

[最適化] セクションが表示されない場合は、仮想 WAN に SD-WAN プレミアム (エンタープライズ) エディションのライセンスをインストールしていることを確認してください。SD-WAN Standard Edition は、WAN Optimization 機能をサポートしていません。

詳細と手順については、次のセクションを参照してください。

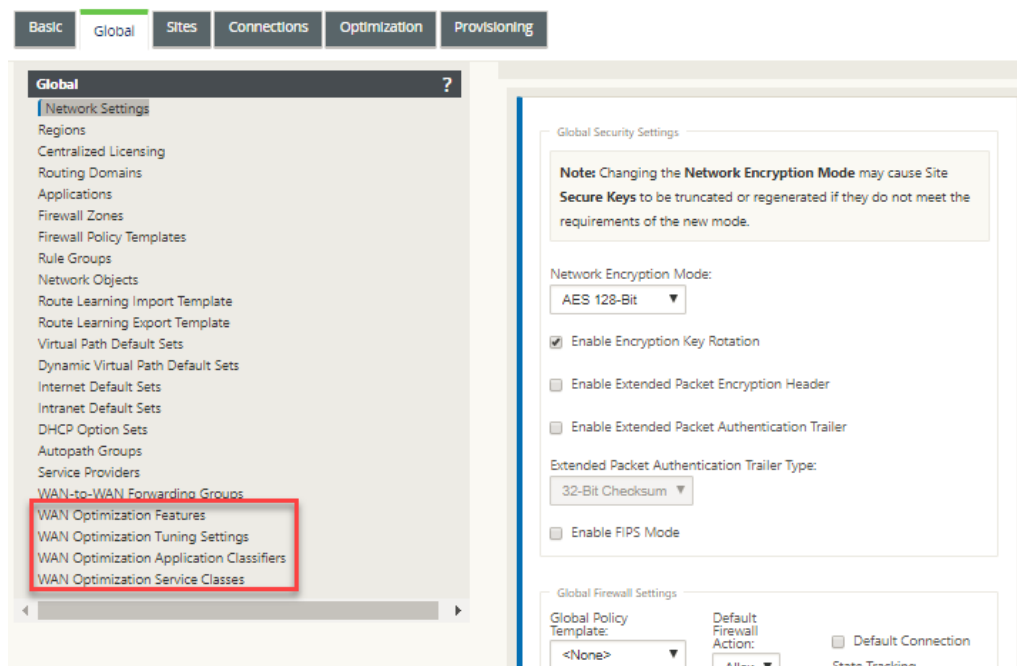
- [SD-WAN エディション](#)
- [ライセンス](#)

- c) [グローバル] タブをクリックします。

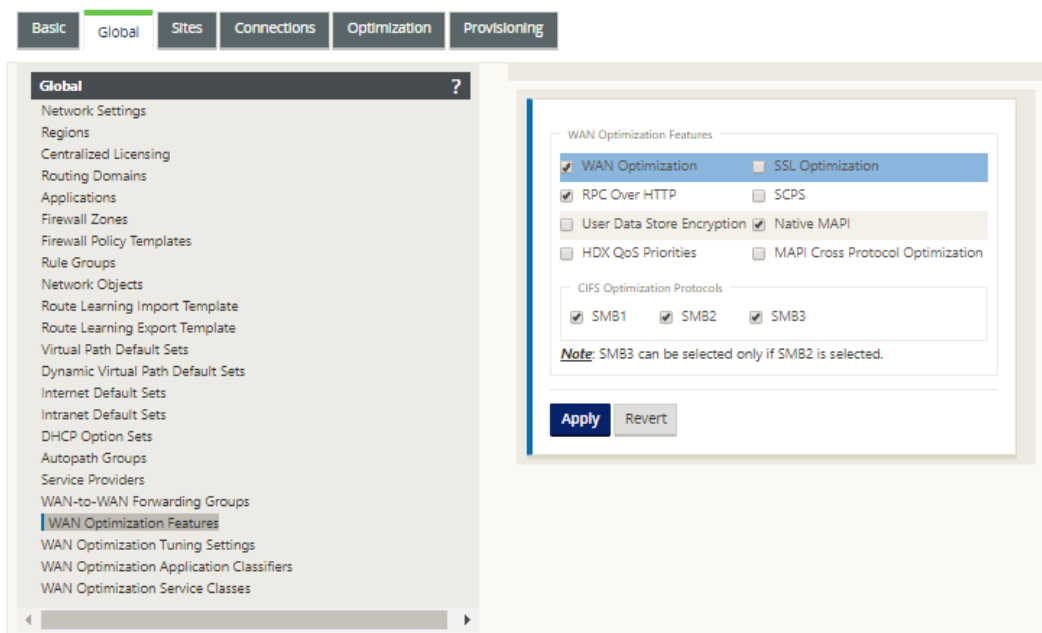
[**Global**] タブから、WAN 最適化の次のデフォルト設定を構成できます。

- WAN Optimization 機能
- WAN Optimization チューニング設定
- WAN Optimization アプリケーション分類子

- WAN Optimization サービスクラス



d) [**WAN Optimization 機能**] をクリックします。



e) [**WAN Optimization**] チェックボックスをオンにします。

[**WAN Optimization**] チェックボックスは、[**WAN Optimization 機能**] セクションの左上隅にあります。これにより、フォームを編集できるようになり、[適用] ボタンと [元に戻す] ボタンが表示されます。

注

この機能は有効にするためにのみ選択されます。WAN Optimization は、機能の構成を完了した後、[適用] をクリックするまで、[最適化] セクションまたは構成パッケージで有効になりません。さらに、最適化構成プロセスでさらに指示されているように、「サービスクラス」テーブルで、適用可能な各サービスクラスの「アクセラレーション」設定も構成する必要があります。（手順については、[最適化のデフォルトサービスクラスの設定](#) セクションに記載されています）最後に、仮想 WAN 構成全体を完了してから、仮想 WAN で WAN Optimization が有効化されず、有効化されません。仮想 WAN の適格なサイトで仮想 WAN アプライアンス・パッケージを生成し、ステージングし、配布し、アクティブ化します。

f) [機能] 設定を構成します。

チェックボックスをクリックして、オプションを選択または選択解除します。フォームで事前に選択されたデフォルト設定を受け入れるか、設定をカスタマイズできます。

注

デフォルトでは、[グローバル] タブで構成した設定は、ツリーに含まれる各ブランチサイトに自動的に適用されます。ただし、「[ブランチサイトの最適化の構成](#)」の項で説明されているように、特定のブランチの最適化設定をカスタマイズできます。

機能設定フォームには、次の 2 つのセクションがあります。

- **WAN Optimization** 機能
- **CIFS Optimization** プロトコル

WAN Optimization 機能の設定は次のとおりです。

- 「**WAN Optimization**」—この構成で WAN Optimization を有効にするには、チェックボックスをオンにします。これにより、圧縮、重複除外、TCP プロトコル最適化も可能になります。

注

他の [最適化] セクションのオプションを使用するには、[WAN 最適化] オプションを選択する必要があります。

- 「**SCPS**」—サテライトリンクの TCP プロトコルの最適化を有効にするには、チェックボックスをオンにします。
- **HDX QoS** 優先度—HDX サブチャネルの優先順位付けに基づいて ICA トラフィックの最適化を有効にするには、チェックボックスをオンにします。
- **[MAPI クロスプロトコル最適化]**—Microsoft Outlook (MAPI) トラフィックのクロスプロトコル最適化を有効にするには、このチェックボックスをオンにします。
- 「**SSL Optimization**」—SSL 暗号化を使用したトラフィックストリームの最適化を有効にするには、チェックボックスをオンにします。

- **[RPC over HTTP]** — RPC over HTTP を使用する Microsoft Exchange トラフィックの最適化を有効にするには、このチェックボックスをオンにします。
- 「ユーザーデータストアの暗号化」 — WAN Optimization の圧縮履歴の暗号化によるデータのセキュリティ強化を有効にするには、チェックボックスをオンにします。
- **[ネイティブ MAPI]** — Microsoft Exchange トラフィックの最適化を有効にするには、このチェックボックスをオンにします。

CIFS Optimization プロトコルの オプションは次のとおりです。

- **[SMB1]** — Windows ファイル共有の最適化 (SMB1) を有効にするには、このチェックボックスをオンにします。
- **[SMB2]** — Windows ファイル共有の最適化 (SMB2) を有効にするには、このチェックボックスをオンにします。
- **[SMB3]** — [Windows ファイル共有 (SMB3) の最適化] を有効にするには、このチェックボックスをオンにします。**SMB3** を選択する前に、まず **SMB2** オプションを選択する必要があります。

g) [適用] をクリックして、選択した 既定の機能 を有効にして構成パッケージに追加します。

次のステップは、最適化 のデフォルトの チューニング設定を構成することです。

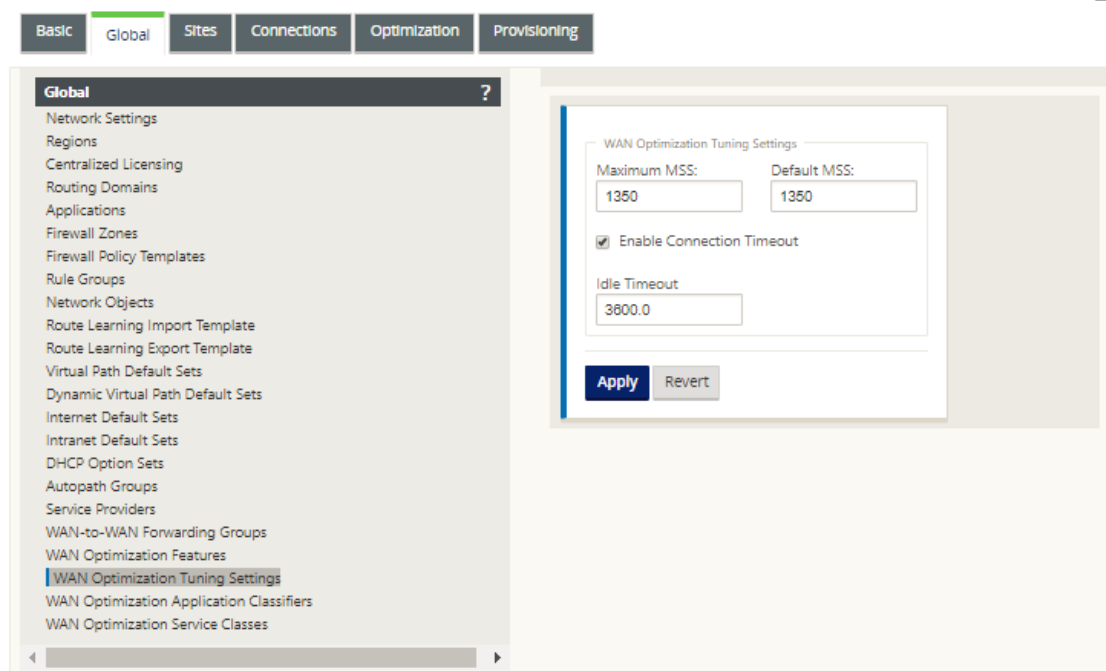
最適化のデフォルトチューニング設定の構成

May 10, 2021

[**Global**] タブで、WAN 最適化のデフォルトのチューニング設定を構成できます。

WAN Optimization のデフォルトの チューニング設定を構成するには、次の手順を実行します。

1. [グローバル] タブで、[**WAN Optimization** チューニング設定] をクリックします。



2. チューニング設定を選択して構成します。

「チューニング設定」オプションは次のとおりです。

- 「最大 **MSS**」—TCP セグメントの最大セグメントサイズ（MSS）の最大サイズ（バイト単位）を入力します。
- 「デフォルト **MSS**」—TCP セグメントの MSS のデフォルトサイズ（オクテット単位）を入力します。
- 「接続タイムアウトの有効化」—アイドルしきい値を超えたときに接続の自動終了を有効にする場合に選択します。
- 「**Idle Timeout**」—アイドル接続が終了するまでのアイドル時間の長さを指定するしきい値（秒単位）を入力します。このフィールドを構成するには、まず [接続タイムアウトの有効化] を選択する必要があります。

3. [適用] をクリックします。

これにより、変更された チューニング設定が グローバル設定に適用されます。

次の手順では、WAN Optimization アプリケーション分類子のデフォルトセットを設定します。

最適化の既定のアプリケーション分類子の構成

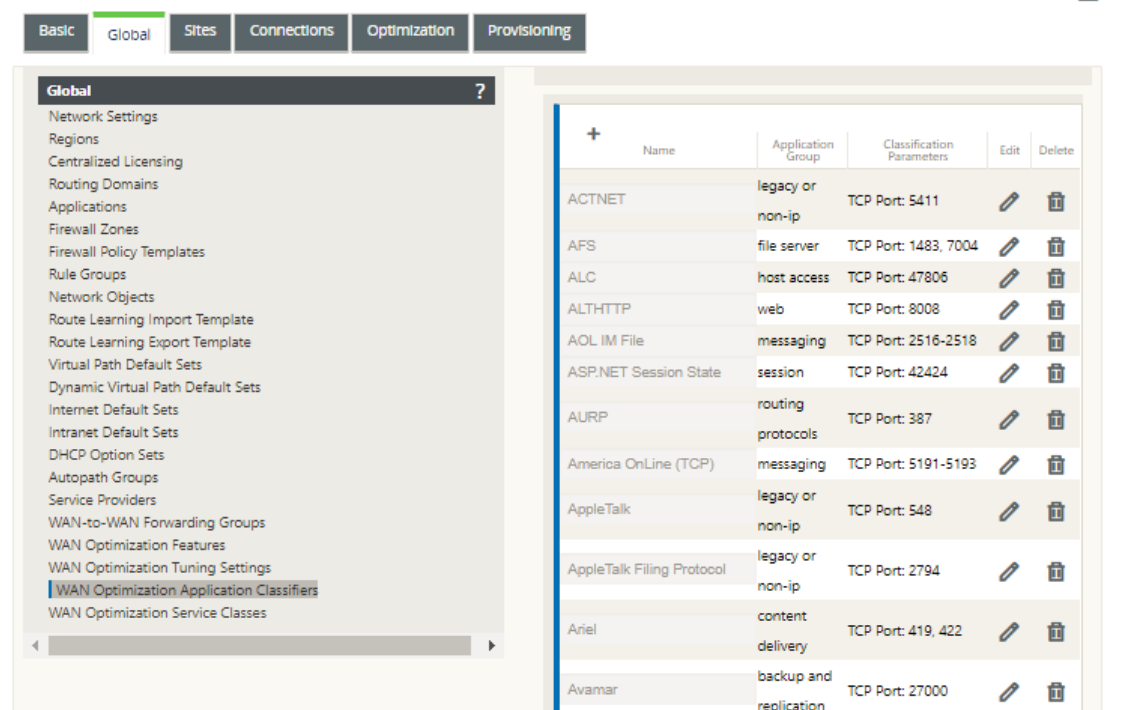
May 10, 2021

[**Global**] タブで、WAN 最適化のデフォルトのアプリケーション分類子設定を構成できます。

WAN Optimization アプリケーション分類子のデフォルトセットを設定するには、次の手順を実行します。

1. [グローバル] タブで、[**WAN Optimization** アプリケーション分類子] をクリックします。

「アプリケーション分類子」(Application Classifiers) テーブルが開き、アプリケーション分類子のデフォルトのセットが表示されます。



このテーブルは、設定フォームでもあります。このフォームを使用して、アプリケーション分類子を設定（編集）、削除、および追加して、カスタマイズされた既定のセットを作成できます。変更されたデフォルトのアプリケーション分類子セットおよび構成する個々のアプリケーション分類子設定は、最適化 セクションツリーに含まれるブランチサイトにデフォルトとして自動的に適用されます。

注

また、特定のブランチサイトごとに、アプリケーション分類子の セットと設定をカスタマイズすることもできます。手順については、[ブランチサイトの最適化の構成](#)を参照してください。

2. 既存のアプリケーション分類子を設定するには、その分類子エントリの [Edit] 列にある [**Edit**]（鉛筆アイコン）をクリックします。

選択したアプリケーション分類子を設定するためのポップアップ設定の 編集 フォームが開きます。

3. [**Port**] フィールドに、アプリケーション分類子のポート番号を入力するか、デフォルトをそのまま使用します。

4. [構成済み] の一覧でアプリケーショングループを追加または削除するか、デフォルトを受け入れます。

- 一覧にアプリケーショングループを追加するには、左側の [アプリケーショングループ 一覧] でアプリケーショングループを選択し、右矢印 (>) をクリックして、右側の [構成済み] リストにグループを追加します。すべての アプリケーショングループ を一覧に一度に追加するには、[すべて追加] 二重右矢印 (») をクリックします。
- リストからアプリケーショングループを削除するには、右側の [構成済み] リストでアプリケーショングループを選択し、[削除] 左矢印 (<) をクリックします。一覧からすべての アプリケーショングループ を一度に削除するには、[すべて削除] 二重左矢印 («) をクリックします。

5. [適用] をクリックします。

これにより、変更内容がアプリケーション分類子に適用され、【設定の編集】フォームが解除されます。

6. (オプション) デフォルトのアプリケーション分類子セットをカスタマイズします。

次のように、アプリケーション分類子を追加または削除して、デフォルトのセットをカスタマイズできます。

- アプリケーション分類子をセットから削除する手順は、次のとおりです。

アプリケーション分類子の エントリの「削除」列にあるゴミ箱アイコンをクリックして、テーブルからそのエントリを削除します。

- アプリケーション分類子をセットに追加する手順は、次のとおりです。

- a) [アプリケーション分類子] ブランチラベルの右側にある [+] をクリックします。

[設定の追加] フォームが表示されます。

- b) [Name] フィールドと [Port] フィールドにアプリケーション分類子の名前とポート番号を入力します。

- c) [構成済み] の一覧でアプリケーショングループを追加または削除します。

一覧にアプリケーショングループを追加するには、左側の [アプリケーショングループ一覧] でアプリケーショングループを選択し、右矢印 (➤) をクリックして、右側の [構成済み] リストにグループを追加します。すべてのアプリケーショングループを一覧に一度に追加するには、[すべて追加] 二重右矢印 (➤➤) をクリックします。

リストからアプリケーショングループを削除するには、右側の [構成済み] リストでアプリケーショングループを選択し、[削除] 左矢印 (⬅) をクリックします。一覧からすべてのアプリケーショングループを一度に削除するには、[すべて削除] 二重左矢印 (⬅⬅) をクリックします。

- d) [適用] をクリックします。

これにより、新しいアプリケーション分類子がセットに追加され、[**Add configuration**] フォームが中止されます。

次のステップでは、WAN Optimization サービスクラスのデフォルトセットを構成します。

最適化のデフォルトサービスクラスを構成する

May 10, 2021

[**Global**] タブで、WAN 最適化のデフォルトサービスクラス設定を構成できます。

WAN Optimization サービスクラスのデフォルトセットを構成するには、次の手順を実行します。

1. [グローバル] タブで、[**WAN Optimization** サービスクラス] をクリックします。

「サービスクラス」(**Service Class** es) テーブルが開き、デフォルトのサービスクラスセットが表示されます。

The screenshot shows the Citrix SD-WAN 11.4 management console. The 'Global' tab is selected, and the 'WAN Optimization Service Classes' section is highlighted in the left-hand navigation menu. The main area displays a table of service classes.

Order	Name	Status	Acceleration	Edit	Delete
100	ICA	ENABLED	none		
200	Web (Private)	ENABLED	none		
300	Web (Private-Secure)	ENABLED	none		
400	Web (Internet)	ENABLED	none		
500	Web (Internet-Secure)	ENABLED	none		
600	CIFS	ENABLED	none		
700	NFS	ENABLED	none		
800	Microsoft Exchange (MAPI)	ENABLED	none		
900	Mail (Other)	ENABLED	none		
1000	VOIP and Multimedia	ENABLED	none		
1100	FTP Data	ENABLED	none		
1200	FTP Control	ENABLED	none		
1300	Instant Messaging	ENABLED	none		
1400	Session Applications	ENABLED	none		
1500	Directory and Security	ENABLED	none		
1600	Database Applications	ENABLED	none		

このテーブルは、設定フォームでもあります。このフォームを使用して、サービスクラスを設定（編集）、削除、および追加して、カスタマイズされた既定のセットを作成できます。変更されたデフォルトのサービスクラス・セットおよび構成した個々のサービスクラスの設定は、最適化 セクション・ツリーに含まれるブランチ・サイトにデフォルトとして自動的に適用されます。

注

また、特定のブランチサイトごとに サービスクラス セットと設定をカスタマイズすることもできます。ブランチサイトの 最適化 設定をカスタマイズする手順については、「[ブランチサイトの最適化の構成](#)」の項を参照してください。

2. 既存のサービスクラスを設定するには、[Service Class] テーブルでそのクラスエントリの [**Edit**] 列にある [Edit]（鉛筆アイコン）をクリックします。

選択したサービスクラスを設定するためのポップアップ設定 を編集 フォームが開きます。

Edit

Name: Order: ☒ Enabled

Acceleration Policy:

☒ Enable AppFlow Reporting ☐ Exclude from SSL Tunnel

Filter Rules +

Application	Source IP Address	Destination IP Address	Direction	Edit	Delete
ICA, ICA CGP			BIDIRECTIONAL		

3. サービスクラスの基本設定を構成します。

基本的な設定は次のとおりです。

- 「有効」—新しいサービスクラスを有効にする場合に選択します。このクラスはデフォルトで有効になっています。
- 「アクセラレーションポリシー」—「アクセラレーションポリシー」ドロップダウンメニューからポリシーを選択します。使用できるオプションは、次のとおりです：
 - **disk**—圧縮に使用するトラフィック履歴を保存する場所としてアプライアンスディスクを指定する場合は、このポリシーを選択します。これにより、このサービスクラスのディスクベース圧縮 (DBC) ポリシーが有効になります。一般的に、アプライアンスは、トラフィックに適した ** ディスク ** または メモリ をストレージの場所として自動的に選択するため、通常はディスクのポリシーが最適です。
 - **none**：このサービスクラスに対してアクセラレーションポリシーを有効にしない場合は、このオプションを選択します。通常、**none** というポリシーは、圧縮不可能な暗号化トラフィックとリアルタイムビデオにのみ使用されます。
 - **flow control Only**：圧縮を無効にしますが、フロー制御アクセラレーションを有効にするには、このポリシーを選択します。常に暗号化されるサービス、および FTP 制御チャネルの場合はこれを選択します。
 - **memory**：圧縮に使用されるトラフィック履歴を保存する場所としてメモリを指定するには、このポリシーを選択します。
- 「AppFlow レポートを有効にする」—このサービスクラスに対して AppFlow レポートを有効にする場合は、これを選択します。AppFlow は、ネットワークインフラストラクチャによって処理されるアプリケーショントランザクションデータのロックを解除するための業界標準です。WAN Optimization AppFlow インターフェイスは、任意の AppFlow コレクタと連携してレポートを生成します。コレク

タは、AppFlow オープン標準 (<http://www.appflow.org>) を使用して、アプライアンスから詳細情報を受け取ります。

AppFlow の詳細については、Citrix ドキュメントポータル<http://docs.citrix.com/>にある Citrix CloudBridge 7.4 製品ドキュメントを参照してください。

注

WAN Optimization AppFlow レポートを表示するには、[モニタリング] タブを選択し、ナビゲーションツリー (左ペイン) で [**WAN Optimization**] ブランチを開き、[**AppFlow**] を選択します。「[仮想 WAN の監視](#)」も参照してください。

- 「**SSL** トンネルから除外」 — サービスクラスに関連付けられたトラフィックを SSL トンネリングから除外する場合に選択します。

4. サービスクラスの フィルタ規則 を設定します。

既存のルールを編集するには、次の操作を行います。

- [フィルタルール] テーブル (フォームの下部) で、編集するルールの [編集] 列にある [編集] (鉛筆のアイコン) をクリックします。

これにより、選択したフィルタ規則のフィルタ規則設定が表示されます。

The screenshot shows the 'Edit' dialog box for a filter rule. The 'Filter Rules' section is highlighted with a red box. It contains the following elements:

- Name:** ICA
- Enabled:** ☒
- Acceleration Policy:** disk
- Enable AppFlow Reporting:** ☒
- Exclude from SSL Tunnel:** ☐
- Filter Rules:**
 - Direction:** BIDIRECTIONAL
 - Applications:**
 - Available:** ACTNET, AFS, ALC, ALTHHTTP, AOL IM File
 - Configured:** ICA, ICA CGP
 - Source IP Address:** [Empty field]
 - Destination IP Address:** [Empty field]

- [方向] ドロップダウンメニューからフィルタの方向を選択します。

次のいずれかのオプションを選択します:

- 双方向
- 単方向

c) [構成済み]の一覧でアプリケーションを追加または削除します。

リストにアプリケーションを追加するには、左側の [アプリケーション] リストでアプリケーションを選択し、右矢印 (➤) をクリックして、右側の [構成済み] リストにグループを追加します。すべてのアプリケーションを一覧に一度に追加するには、[すべて追加] 二重右矢印 (➤➤) をクリックします。

リストからアプリケーションを削除するには、右側の [構成済み] リストでアプリケーションを選択し、[削除] 左矢印 (◀) をクリックします。一覧からすべてのアプリケーションを一度に削除するには、[すべて削除] 二重左矢印 (◀◀) をクリックします。

d) 下にスクロールして、フォームの切り捨てられた部分を表示します。

[**Filter Rules**] の設定セクションは多少長いため、スクロールバーを使用してフォームの切り捨てられた部分を表示する必要があります。

e) [送信元 IP アドレス] フィールドに 送信元 **IP** アドレスを入力します。

f) 入力した送信元 IP アドレスの右側にある [+] をクリックします。

これにより、指定した IP アドレスが 送信元 **IP** アドレス テーブルに追加されます。



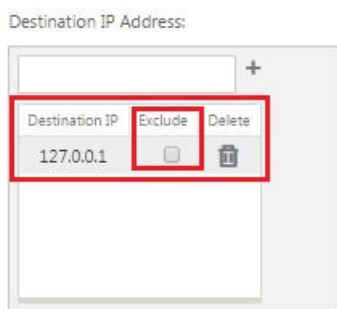
g) このフィルタ規則の送信元 IP アドレスを含めるか除外するかを指定します。

[除外] チェックボックスをオンにして、指定した送信元 IP アドレスをこのフィルタ規則から除外します。アドレスを含めるには、チェックボックスの選択を解除します。

h) [宛先 IP アドレス] フィールドに 宛先 **IP** アドレスを入力します。

i) 先ほど入力した [宛先 IP アドレス] の右側にある [+] をクリックします。

これにより、指定した IP アドレスが 送信元 **IP** アドレス テーブルに追加されます。



j) このフィルタ規則の宛先 IP アドレスを含めるか除外するかを指定します。

[除外] チェックボックスをオンにして、指定した宛先 IP アドレスをこのフィルタ規則から除外します。アドレスを含めるには、チェックボックスの選択を解除します。

k) [適用] をクリックします。

これにより、変更内容がルールに適用され、[フィルタルール 設定] セクションが非表示になります。

5. (オプション) デフォルトの サービスクラス セットをカスタマイズします。

次のように、サービスクラスを追加または削除して、デフォルトセットをカスタマイズできます。

- セットからサービスクラスを削除する手順は、次のとおりです。

テーブル内のサービスクラス・エントリの「削除」(**Delete**) 列にあるゴミ箱アイコンをクリックして、そのエントリを削除します。

- サービスクラスをセットに追加するには、次の手順に従います。

a) [サービスクラス] ブランチのラベルの右側にある [+] をクリックします。

[設定の 追加] フォームが表示されます。

b) 「名前」フィールドに新しいサービスクラスの名前を入力します。

c) 新しいサービスクラスを設定します。

新しいサービスクラスを設定する手順は、既存のサービスクラスを変更する場合と同じです。手順については、このセクションの前の手順を参照してください。

“3. サービスクラスの基本設定を行います。

“4. サービスクラスのフィルタ規則を設定します。

d) [**Add**] をクリックして、新しいサービスクラスをデフォルトセットに追加し、[**Add configuration**] フォームを閉じます。

6. (オプション、推奨) 構成パッケージ を保存します。

これで、グローバル WAN Optimization 構成が完了し、ブランチサイトの 最適化 セットと設定の構成を開始できます。

ブランチサイトの最適化を構成する

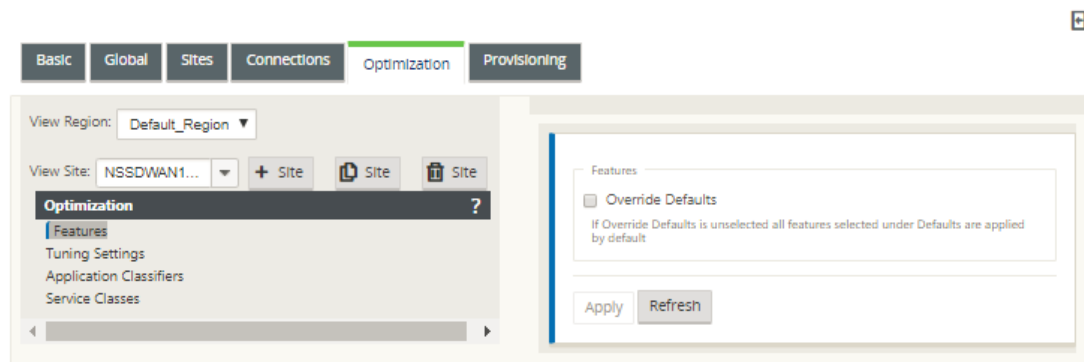
May 10, 2021

デフォルトのグローバル構成が完了したら、各ブランチサイトのセットと設定をカスタマイズできます。

構成したグローバル設定は、[最適化] セクションに含まれる各ブランチサイトに自動的に適用されます。デフォルトを受け入れるか、特定のブランチの設定をカスタマイズするかを選択できます。ブランチサイトの 最適化 セットと設定の構成手順は、グローバルデフォルトの設定と同じですが、いくつかの小さな違いがあります。

ブランチサイトの 最適化 構成をカスタマイズするには、次の手順を実行します。

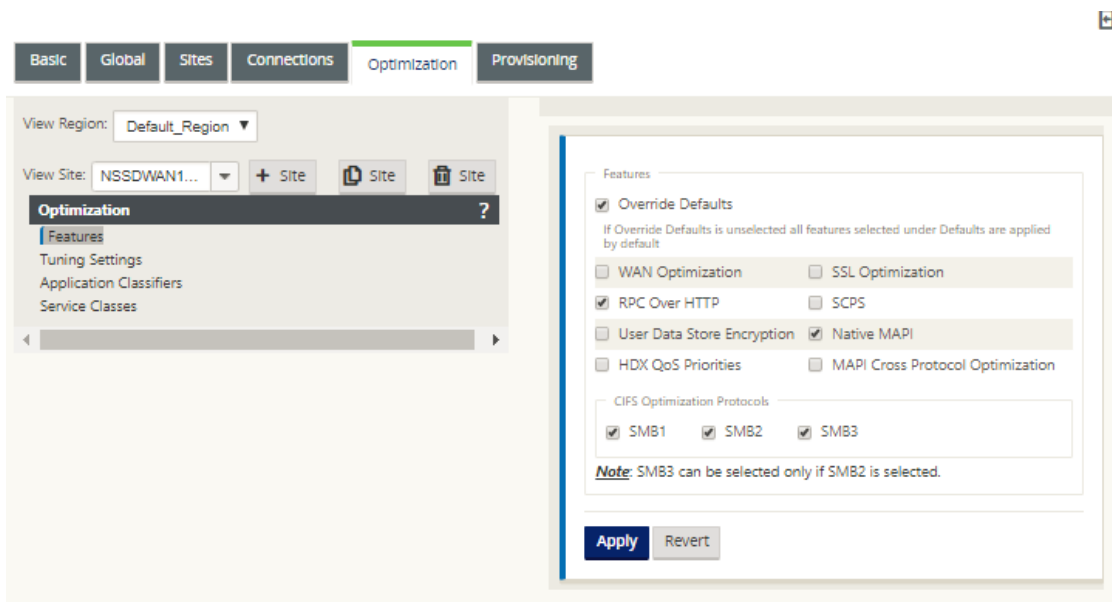
1. [最適化] タブの [サイトの表示] フィールドで、サイトを選択します。



2. 「デフォルトを上書き」チェックボックスを選択します。

これにより、その構成カテゴリの最上位の設定フォームが表示され、編集用に開きます。

下の画像は、トップレベル設定設定フォームの例を示しています。この例では、機能 セットです。



3. 設定の変更を入力します。

この時点から、各ブランチサイトの **Optimization** カテゴリの構成プロセスは、対応するグローバルセクションカテゴリと同じになります。特定のカテゴリのセットまたは設定を構成する方法については、以下の該当するセクションを参照してください。

- [最適化の有効化と既定の機能設定の構成](#)
- 「[最適化のデフォルト・チューニング設定の構成](#)」を参照してください。
- 「[最適化のデフォルトアプリケーション分類子の設定](#)」を参照してください。
- 「[最適化のデフォルトサービスクラスの設定](#)」を参照してください。

4. (オプション、推奨) 構成パッケージ を保存します。

これで、仮想 WAN の 最適化 セクションセットと設定の構成が完了しました。

SSL プロファイルの設定

May 10, 2021

セキュリティと使いやすさのために、すべての SSL 関連の設定は、アプライアンスの新しい設定エディタから利用できます。SD-WAN Premium (Enterprise) エディションおよび 2 ボックスデプロイでは、サービスクラスは構成エディタから構成されるため、SSL プロファイルをアタッチすることはできません。サービスクラスへの SSL プロファイルマッピングの式に対応するために、SSL プロファイルのワークフローが変更され、プロファイルノードにサービスクラスをアタッチできるようになります。

制限の 1 つは、SSL プロファイルがサービスクラス内のすべてのルールにアタッチされることです。SSL プロファイルを特定のルールに選択的にアタッチする必要がある場合、サービスクラス設定は詳細ルールに分割され、さらに選択できるようになります。

注

SSL プロファイルに関連付けることができるのは、フィルタールールの方向が単方向に設定されているサービスクラスのみです。

The screenshot shows the 'Configuration' tab in the Citrix SD-WAN Web GUI. The 'SSL Profile' section is active, displaying fields for 'Profile Name*' (Test), 'Profile Enabled' (checked), 'Parse Subject Alternative Names' (unchecked), and 'Virtual Host Name'. Below these is the 'Service Classes' section, which is highlighted with a red box. It contains two lists: 'Available (19)' and 'Configured (3)'. The 'Available' list includes RPCoverHTTP, ICA, Web (Private), and Web (Private-Secure). The 'Configured' list includes Iperf, Secure Applications, and Web (Internet-Secure). Arrows indicate the ability to move items between the two lists. At the bottom, the 'Proxy Type' is set to 'Split'.

データセンターで新しい Premium (Enterprise) Edition アプライアンスで SSL プロファイルを作成するには:

1. SD-WAN Web GUI で、[設定] > [セキュアアクセラレーション] ページに移動します。[プロファイルの追加] をクリックします。**SSL** プロファイルを作成します。

Dashboard Monitoring Configuration

Configuration > WAN Optimization > Secure Acceleration

Secure Peering

Keystore Status: Opened | Secure Peering Status: Disabled

SSL Profile | Windows Domain

SSL Profiles

SSL acceleration allows the appliance to compress SSL traffic such as HTTPS and SSL-encrypted XenApp/XenDesktop (ICA/COP) traffic. Secure partner configuration is a prerequisite to SSL acceleration. SSL acceleration requires additional security credentials on the server-side NetScaler SD-WAN WO appliance (only) and SSL-specific configuration (called an SSL Profile) for each group of SSL servers. This step should be skipped on a client-side appliance.

[Add Profile](#)

[Back](#)

Create SSL Profile

☒ Manually add Profile ☐ Import Profile

Profile Name*

☒ Profile Enabled

☐ Parse Subject Alternative Names

Virtual Host Name

Service Classes

Available (21) [Select All](#)

ICA	+
Web (Private)	+
Web (Private-Secure)	+
Web (Internet)	+

Configured (0) [Remove All](#)

No items

Proxy Type

☐ Split ☒ Transparent

SSL Server's Private Key*

private_10_105_199_6 [+](#)

2. [**SSL** プロファイルの作成] ページで、プロファイル名を指定し、このプロファイルに関連付ける [サービスクラス] を選択します。[プロキシタイプ] を選択し、関連データを入力して [作成] をクリックします。

Create SSL Profile

Manually add Profile

Import Profile

Profile Name*

SampleProfile

Profile Enabled

Parse Subject Alternative Names

Virtual Host Name

Service Classes

Available (20)Select All

Web (Private)+

ICA+

Web (Private-Secure)+

Web (Internet-Secure)+

Configured (1)Remove All

Web (Internet)-

Proxy Type

Split

Transparent

SSL Server's Private Key*

private_10_105_199_6

Create

Close

3. SSL プロファイルが正常に作成され、サービスクラスが関連付けられた後、以下に示すように、SSL プロファイル情報を表示します。

<div><div>SSL Profile</div><div>Windows Domain</div></div>		<div><div>Add</div><div>Edit</div><div>Delete</div><div>Action</div></div>	
Profile Name	Proxy Type	Profile In Use	Profile Enabled
SampleProfile	transparent	✓	✓

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

866

Citrix WAN 最適化クライアントプラグイン

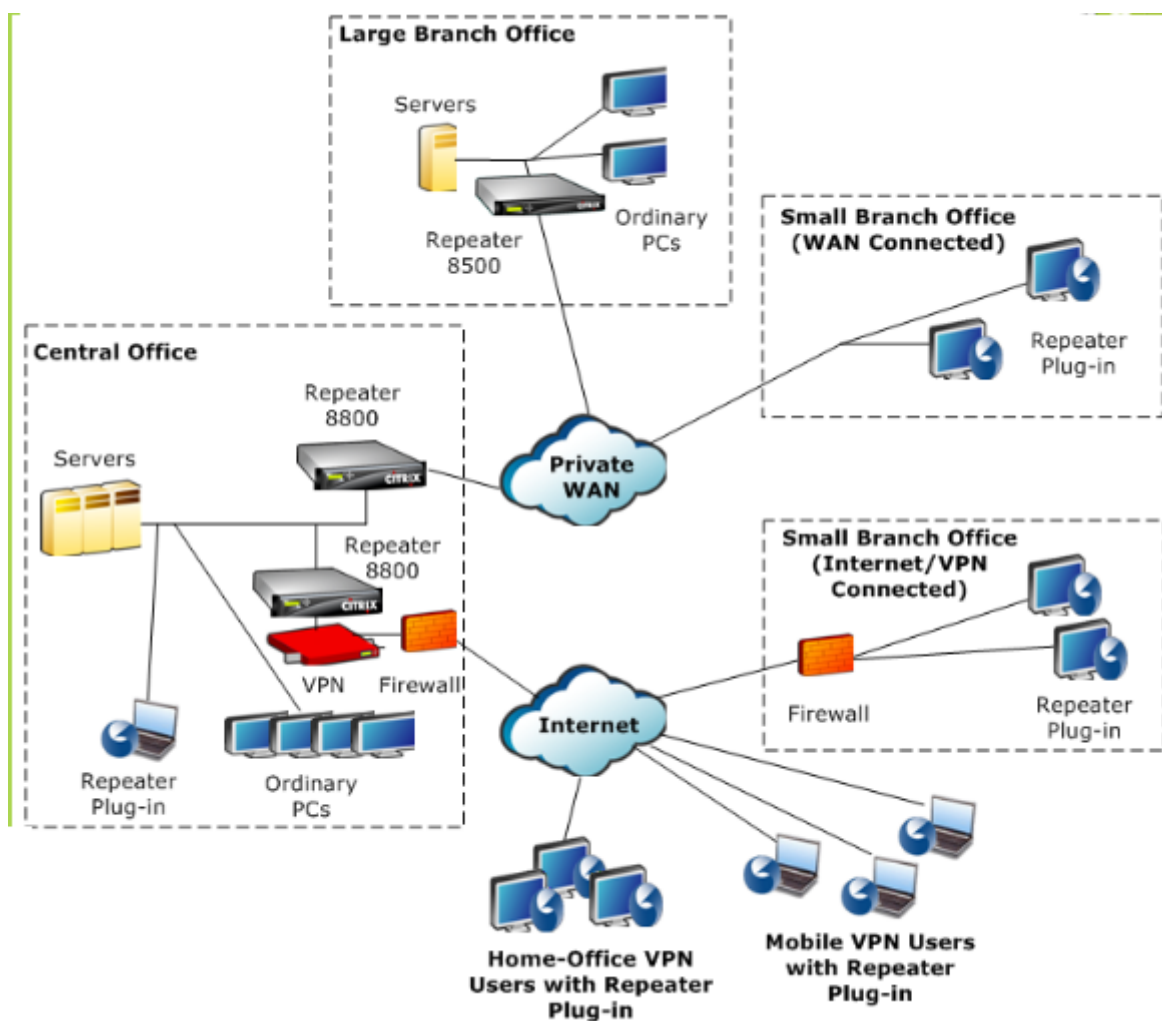
May 10, 2021

Citrix WANOP クライアントプラグインは、Windows ノートパソコンやワークステーションで動作するソフトウェアベースのネットワークアクセラレータで、WANOP クライアントプラグインアプライアンスを使用するオフィスだけでなく、どこでもアクセラレーションを提供します。リンクのもう一方の端にある Citrix WANOP クライアントプラグインアプライアンスに接続します。

WANOP クライアントプラグインの動作原理は、通常、WANOP クライアントプラグインアプライアンスの原理と同じです。プラグインのドキュメントに含まれていないトピックについては、より大きなドキュメントセットを参照してください。

プラグインは、標準の Microsoft インストールファイル (MSI) として配布されます。プラグインの展開では、リンクの反対側に WANOP Client Plug-in アプライアンスのプラグイン固有の設定が必要です。WANOP Client Plug-in アプライアンスの DNS または IP アドレス、およびその他のいくつかのパラメータを使用して MSI ファイルをカスタマイズする場合、ユーザーは Windows コンピューターにプラグインをインストールするときに構成情報を入力する必要はありません。

図 1: WANOP クライアントプラグインを示す典型的な WANOP クライアントプラグインネットワーク



注

プラグインは Citrix Receiver 1.2 以降でサポートされており、Citrix Receiver で配布および管理できます。

ハードウェアとソフトウェアの要件

May 10, 2021

アクセラレーションリンクのクライアント側では、

WANOP Client Plug-in は Windows デスクトップおよびノートブックシステムではサポートされますが、ネットブックやシンクライアントではサポートされません。WANOP クライアントプラグインを実行するコンピューターには、以下の最低限のハードウェア仕様をお勧めします。

- Pentium4 クラス CPU

- 2GB の RAM
- 2GB の空きディスク容量

WANOP クライアントプラグインは Windows10 プラットフォームでサポートされており、次のシステム要件が必要です。

- 4GB RAM
- 10GB の空きディスク容量

WANOP クライアントプラグインは、次のオペレーティングシステムでサポートされています。

- Windows XP Home
- Windows XP Professional
- Windows Vista (Home Basic、Home Premium、Business、Enterprise、Ultimate のすべての 32 ビットバージョン)
- Windows 7 (Home Basic、Home Premium、Professional、Enterprise、および Ultimate のすべての 32 ビットおよび 64 ビットバージョン)
- Windows 8 (32 ビットおよび 64 ビットバージョンの Premium (Enterprise) Edition)
- Windows 10 (32 ビットおよび 64 ビットバージョンの Premium (Enterprise) Edition)

サーバー側では、次のアプライアンスが現在、WANOP クライアントプラグインのデプロイメントをサポートしています。

- Repeater 8500 Series
- Repeater 8800 Series
- WANOP クライアントプラグイン VPX
- WANOP クライアントプラグイン 2000
- WANOP クライアントプラグイン 3000
- WANOP クライアントプラグイン 4000
- WANOP クライアントプラグイン 5000

WANOP プラグインの仕組み

May 10, 2021

WANOP クライアントプラグイン製品は既存のものを使用します WAN/VPN インフラ。プラグインがインストールされているコンピューターは、プラグインのインストール前と同じように、LAN、WAN、およびインターネットに引

き続きアクセスします。ルーティングテーブル、ネットワーク設定、クライアントアプリケーション、またはサーバーアプリケーションを変更する必要はありません。

Citrix Access Gateway VPN には、少量の WANOP クライアントプラグイン固有の構成が必要です。

プラグインとアプライアンスによる接続の処理方法には、トランスペアレントモードとリダイレクタモード ** の 2 つのバリエーションがあります。リダイレクタは、新しい展開では推奨されないレガシーモードです。

- プラグインからアプライアンスへのアクセラレーションの透過モード は、アプライアンスからアプライアンスへのアクセラレーションと非常によく似ています。WANOP クライアントプラグインアプライアンスは、プラグインとサーバー間を移動するときにパケットがたどるパス内にある必要があります。アプライアンス間のアクセラレーションと同様に、透過モードは透過プロキシとして動作し、接続の一方の端からもう一方の端までの送信元と宛先の IP アドレスとポート番号を保持します。
- リダイレクタモード（推奨されません）は、明示的なプロキシを使用します。プラグインは、発信パケットをアプライアンスのリダイレクタ IP アドレスに再アドレス指定します。次に、アプライアンスはパケットをサーバーに再アドレス指定し、リターンアドレスをプラグインではなく自身を指すように変更します。このモードでは、アプライアンスは WAN インターフェースとサーバー間のパスと物理的にインラインである必要はありません（これは理想的な展開ですが）。

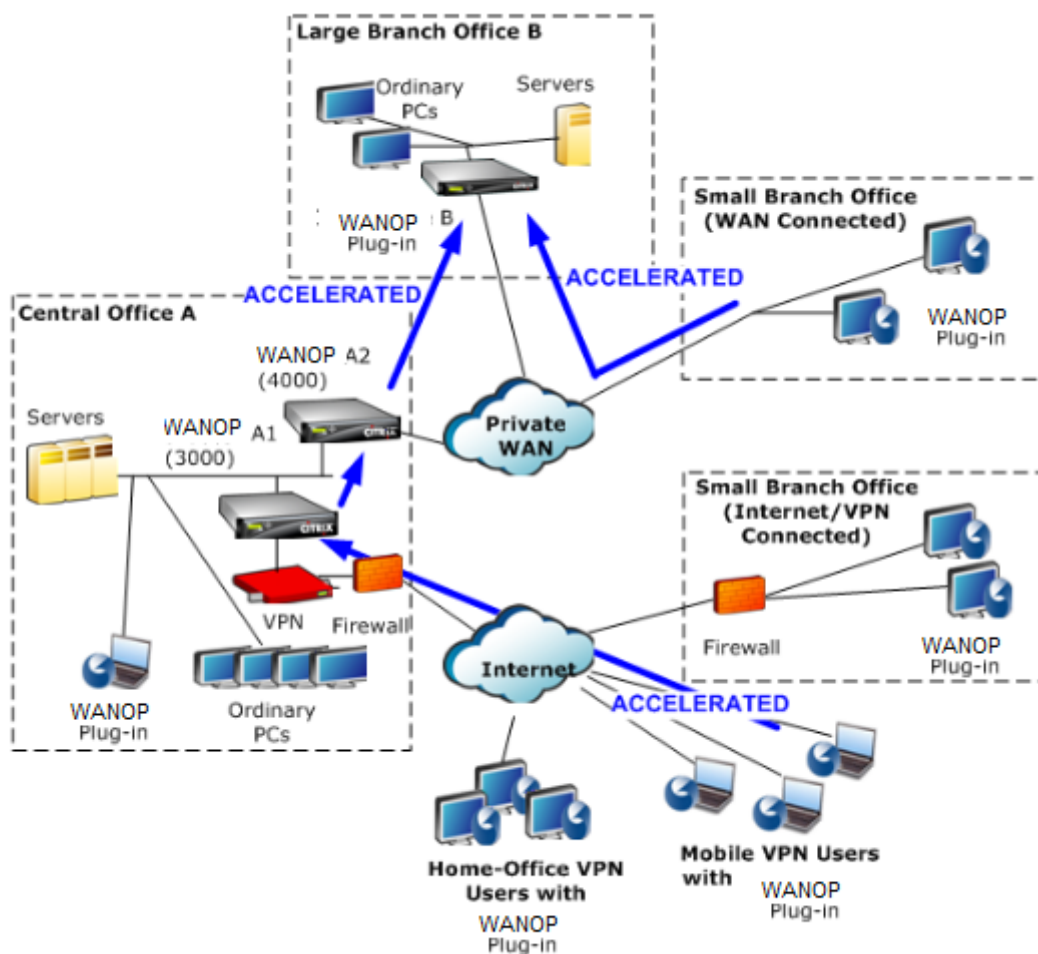
ベストプラクティス：可能な場合は透過モードを使用し、必要な場合はリダイレクタモードを使用します。

透過モード

透過モードでは、高速化された接続のパケットは、アプライアンス間の高速化の場合と同様に、ターゲットアプライアンスを通過する必要があります。

プラグインは、アクセラレーションに使用できるアプライアンスのリストで構成されます。各アプライアンスへの接続を試み、シグナリング接続を開きます。シグナリング接続が成功すると、プラグインはアプライアンスからアクセラレーションルールをダウンロードし、アプライアンスがアクセラレーションできる接続の宛先アドレスを送信します。

図 1: 透過モード、3 つの加速パスを強調表示



注

- トラフィックフロー：トランスパレントモードは、WANOP クライアントプラグインとプラグイン対応アプライアンスの間の接続を高速化します。
- ライセンス-アプライアンスには、必要な数のプラグインをサポートするためのライセンスが必要です。この図では、Repeater A1 はサイト A のプラグインアクセラレーションを提供するため、Repeater A2 にプラグインアクセラレーションのライセンスを付与する必要はありません。
- デイジーチェーン-接続がターゲットアプライアンスに向かう途中で複数のアプライアンスを通過する場合、中央のアプライアンスで「デイジーチェーン」を有効にする必要があります。そうしないと、アクセラレーションがブロックされます。この図では、大規模ブランチオフィス B を宛先とするホームオフィスおよびモバイル VPN ユーザからのトラフィックが、Repeater B によって加速されます。これを機能させるには、Repeater A1 および A2 でデイジーチェーンが有効になっている必要があります。

プラグインが新しい接続を開くたびに、加速ルールを参照します。宛先アドレスがいずれかのルールに一致する場合、プラグインは、接続の最初のパケット（SYN パケット）にアクセラレーションオプションを付加することにより、接続をアクセラレーションしようとします。プラグインに認識されているアプライアンスが SYN-ACK 応答パケットに

アクセラレーションオプションを接続すると、そのアプライアンスとのアクセラレーション接続が確立されます。

アプリケーションとサーバーは、高速接続が確立されたことを認識していません。プラグインソフトウェアとアプライアンスだけが、加速が行われていることを認識しています。

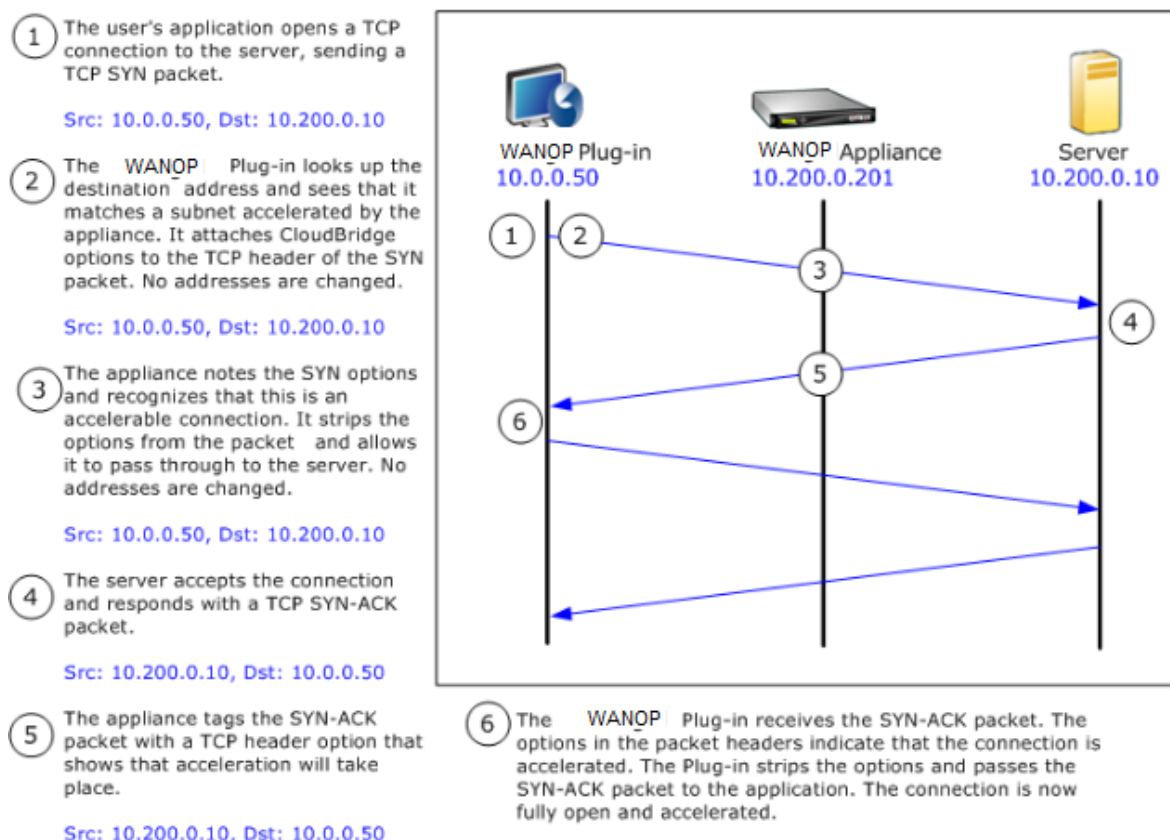
透過モードは、アプライアンス間のアクセラレーションに似ていますが、同じではありません。違いは次のとおりです。

- クライアントが開始する接続のみ-透過モードは、プラグインを備えたシステムによって開始される接続のみを受け入れます。プラグインを搭載したシステムをサーバーとして使用する場合、サーバー接続は高速化されません。一方、アプライアンス間のアクセラレーションは、どちらの側がクライアントでどちらがサーバーであるかに関係なく機能します。（アクティブモード FTP は、プラグインによって要求されたデータ転送を開始する接続がサーバーによって開かれるため、特殊なケースとして扱われます。）
- シグナリング接続-透過モードは、ステータス情報の送信にプラグインとアプライアンス間のシグナリング接続を使用します。アプライアンス間のアクセラレーションは、デフォルトで無効になっているセキュアなピア関係を除いて、シグナリング接続を必要としません。プラグインがシグナリング接続を開くことができない場合、アプライアンスを介した接続を高速化しようとはしません。
- デイジーチェーン接続-プラグインとその選択したターゲットアプライアンスの間のパスにあるアプライアンスの場合、[構成: チューニング] メニューでデイジーチェーンを有効にする必要があります。

透過モードは、VPN でよく使用されます。WANOP クライアントプラグインプラグインは、ほとんどの IPSec および PPTP VPN、および Citrix Access GatewayVPN と互換性があります。

次の図は、透過モードでのパケットフローを示しています。このパケットフローは、接続の高速化を試みるかどうかの決定がシグナリング接続を介してダウンロードされた高速化ルールに基づくことを除いて、アプライアンス間の高速化とほぼ同じです。

図 2: 透過モードでのパケットフロー



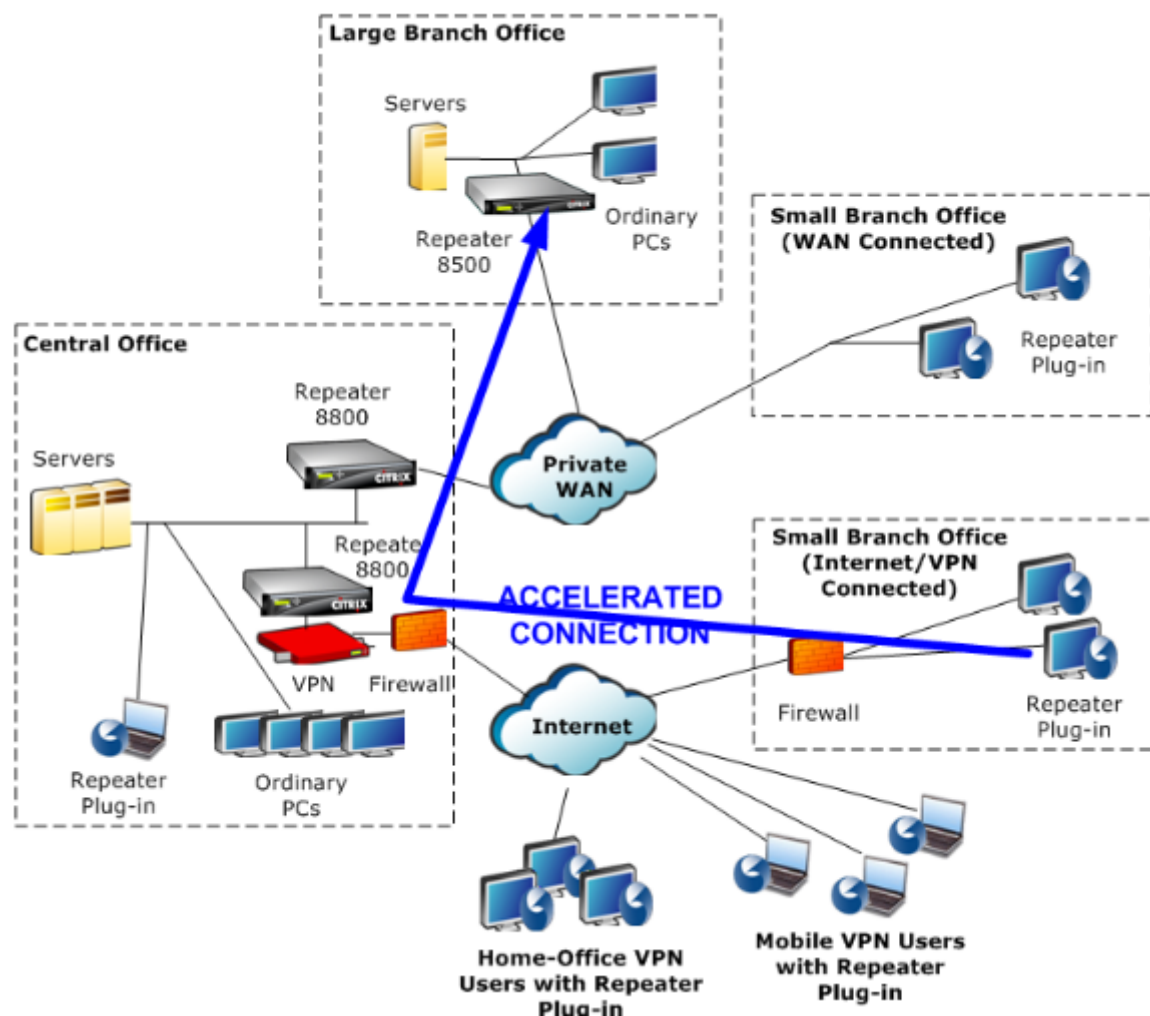
リダイレクタモード

リダイレクタモードは、次の点で透過モードとは動作が異なります。

- WANOP クライアントプラグインソフトウェアは、パケットをアプライアンスに明示的にアドレス指定することにより、パケットをリダイレクトします。
- したがって、リダイレクタモードアプライアンスは、すべての WAN リンクトラフィックを傍受する必要はありません。アクセラレーションされた接続は直接アドレス指定されるため、プラグインとサーバーの両方から到達できる限り、どこにでも配置できます。
- アプライアンスは最適化を実行してから、出力パケットをサーバーにリダイレクトし、パケット内の送信元 IP アドレスを独自のアドレスに置き換えます。サーバーの観点からは、接続はアプライアンスで開始されます。
- サーバーからのリターントラフィックはアプライアンスにアドレス指定されます。アプライアンスはリターン方向で最適化を実行し、出力パケットをプラグインに転送します。
- 宛先ポート番号は変更されないため、ネットワーク監視アプリケーションは引き続きトラフィックを分類できます。

次の図は、リダイレクタモードがどのように機能するかを示しています。

図 1: リダイレクタモード



次の図は、リダイレクタモードでのパケットフローとアドレスマッピングを示しています。

図 2: リダイレクタモードでのパケットフロー

- 1 The user's application opens a TCP connection to the server, sending a TCP SYN packet.

Src: 10.0.0.50, Dst: 10.200.0.10

- 2 The Repeater Plug-in looks up the dst address and decides to redirect the connection to the appliance at 10.200.0.201.

Src: 10.0.0.50, Dst: 10.200.0.201

(10.200.0.10 is preserved in a TCP option field. Options 24-31 are used for various parameters.)

- 3 The appliance accepts the connection and forwards the packet to the server (using the dst address from the TCP options field), and giving itself as the src.

Src: 10.200.0.201, Dst: 10.200.0.10

- 4 The server accepts the connection and responds with a TCP SYN-ACK packet.

Src: 10.200.0.10, Dst: 10.200.0.201

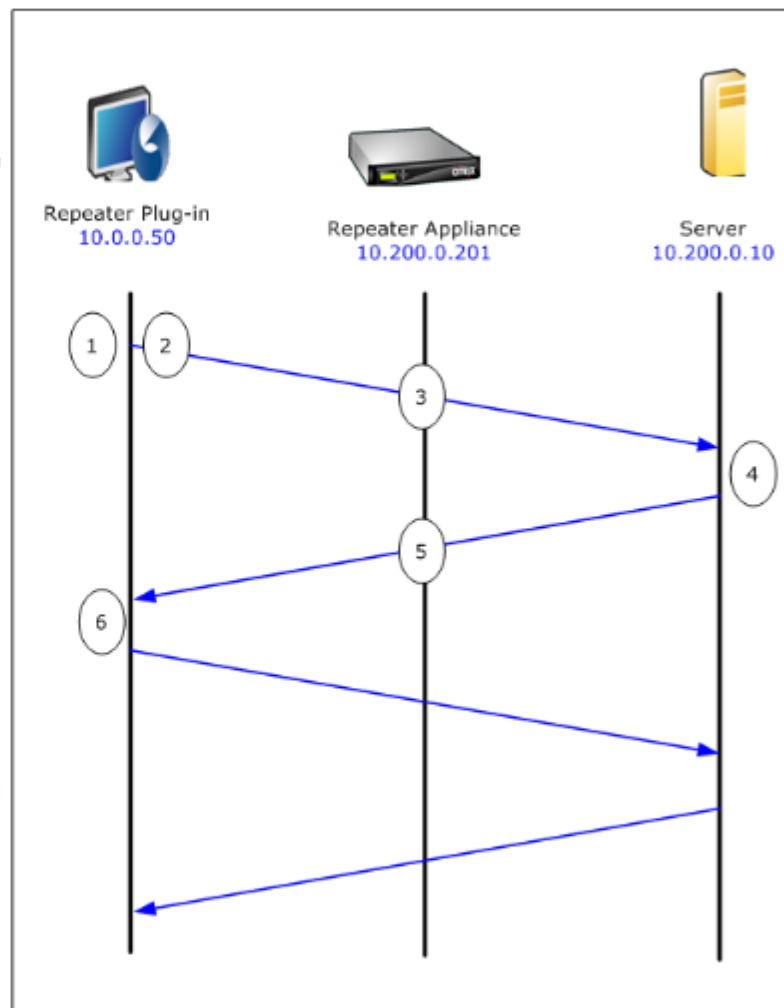
- 5 The appliance rewrites the addresses and forwards the packet to the Plug-in (placing the server address in an option field).

Src: 10.200.0.201, Dst: 10.0.0.50

- 6 The connection is now fully open. The client and server send packets back and forth via the appliance.

While the addresses are altered in Redirector mode, the destination port numbers are not (though the ephemeral port number may be). The data is not encapsulated. Redirector mode is a proxy, not a tunnel.

There is no 1:1 relationship between packets (though in the end, the data received is always identical to the data sent). Compression may reduce many input packets into a single output packet. CIFS acceleration will perform speculative read-ahead and write-behind operations. Also, if packets are dropped between appliance and the Repeater Plug-in, the retransmission is handled by the appliance, not the server, using advanced recovery algorithms.



プラグインがアプライアンスを選択する方法

各プラグインは、高速接続を要求するために接続できるアプライアンスのリストで構成されています。

アプライアンスにはそれぞれ、アクセラレーション規則のリストがあります。これは、アプライアンスがアクセラレーション接続を確立できるターゲット・アドレスまたはポートのリストです。プラグインはこれらのルールをアプライアンスからダウンロードし、各接続の宛先アドレスとポートを各アプライアンスのルールセットと照合します。特定の接続を高速化するアプライアンスが 1 つしかない場合、選択は簡単です。複数のアプライアンスが接続を高速化することを提案している場合、プラグインはアプライアンスの 1 つを選択する必要があります。

アプライアンスの選択のルールは次のとおりです。

- 接続を高速化するために提供しているすべてのアプライアンスがリダイレクタモードアプライアンスである場合、プラグインのアプライアンスリストの左端のアプライアンスが選択されます。(アプライアンスが DNS アドレスとして指定されていて、DNS レコードに複数の IP アドレスがある場合、これらも左から右にスキャンされます。)
- 接続を高速化するために提供しているアプライアンスの一部がリダイレクタモードを使用し、一部が透過モードを使用している場合、透過モードアプライアンスは無視され、リダイレクタモードアプライアンスから選択が行われます。
- 接続を高速化するために提供しているすべてのアプライアンスが透過モードを使用している場合、プラグインは特定のモードを選択しません appliance. WANOP クライアントプラグイン SYN オプションを使用して接続を開始し、返される SYN-ACK パケットに適切なオプションをアタッチする候補アプライアンスが使用されます。これにより、実際にトラフィックと一致しているアプライアンスがプラグインに対して自身を識別できるようになります。ただし、プラグインは応答するアプライアンスとのオープンなシグナリング接続を備えている必要があります。そうでない場合、アクセラレーションは行われません。
- 一部の構成情報はグローバルと見なされます。この構成情報は、シグナリング接続を開くことができるリストの左端のアプライアンスから取得されます。

プラグインで使用するためのアプライアンスのデプロイ

May 10, 2021

クライアントアクセラレーションには、WANOP クライアントプラグインアプライアンスでの特別な構成が必要です。その他の考慮事項には、アプライアンスの配置が含まれます。プラグインは通常、VPN 接続用に展開されます。

可能な場合は専用のアプライアンスを使用してください

プラグインアクセラレーションとリンクアクセラレーションの両方に同じアプライアンスを使用しようとすると、多くの場合困難になります。これは、2 つの用途でアプライアンスをデータセンターの異なるポイントに配置する必要

があり、2つの用途で異なるサービスクラスルールが必要になる場合があります。

さらに、単一のアプライアンスがプラグインアクセラレーションのエンドポイントまたはサイト間アクセラレーションのエンドポイントとして機能できますが、同じ接続に対して同時に両方の目的を果たすことはできません。したがって、VPNのプラグインアクセラレーションとリモートデータセンターへのサイト間アクセラレーションの両方にアプライアンスを使用する場合、プラグインユーザーはサイト間アクセラレーションを受信しません。この問題の深刻さは、プラグインユーザーが使用するデータのどれだけがリモートサイトからのものであるかによって異なります。

最後に、専用アプライアンスのリソースはプラグインとサイト間の要求に分割されないため、より多くのリソースを提供し、各プラグインユーザーにより高いパフォーマンスを提供します。

可能な場合はインラインモードを使用してください

アプライアンスは、サポートするVPNユニットと同じサイトに展開する必要があります。通常、2つのユニットは互いに一致しています。インライン展開は、最も単純な構成、ほとんどの機能、および最高のパフォーマンスを提供します。最良の結果を得るには、アプライアンスがVPNユニットと直接一致している必要があります。

ただし、アプライアンスは、グループモードまたは高可用性モードを除き、任意のデプロイモードを使用できます。これらのモードは、アプライアンスからアプライアンスへのアクセラレーションとクライアントからアプライアンスへのアクセラレーションの両方に適しています。単独で使用することも（透過モード）、リダイレクタモードと組み合わせ使用することもできます。

アプライアンスをネットワークの安全な部分に配置します

アプライアンスは、サーバーと同じように既存のセキュリティインフラストラクチャに依存します。ファイアウォール（および使用する場合はVPNユニット）のサーバーと同じ側に配置する必要があります。

NAT の問題を回避する

プラグイン側のネットワークアドレス変換（NAT）は透過的に処理され、問題にはなりません。アプライアンス側では、NATが面倒になる可能性があります。スムーズな展開を確実にするために、次のガイドラインを適用してください。

- アプライアンスをサーバーと同じアドレス空間に配置して、サーバーに到達するために使用されるアドレス変更もアプライアンスに適用されるようにします。
- アプライアンスがそれ自体に関連付けられていないアドレスを使用してアプライアンスにアクセスしないでください。
- アプライアンスは、プラグインユーザーが同じサーバーにアクセスするのと同じIPアドレスを使用してサーバーにアクセスする必要があります。
- つまり、サーバーやアプライアンスのアドレスにNATを適用しないでください。

ソフトブーストモードを選択します

[設定の構成: 帯域幅管理] ページで、[ソフトブーストモード] を選択します。Softboost は、WANOP クライアントプラグインプラグインでサポートされている唯一のタイプのアクセラレーションです。

プラグインアクセラレーションルールを定義する

アプライアンスは、どのトラフィックを加速するかをクライアントに指示する加速ルールのリストを維持します。各ルールは、アプライアンスが高速化できるアドレスまたはサブネットとポート範囲を指定します。

何を加速するか-どのトラフィックを加速するかを選択は、アプライアンスが使用されている用途によって異なります。

- VPN アクセラレータ-アプライアンスが VPN アクセラレータとして使用されており、すべての VPN トラフィックがアプライアンスを通過している場合、宛先に関係なく、すべての TCP トラフィックを高速化する必要があります。
- リダイレクタモード-トランスペアレントモードとは異なり、リダイレクタモードのアプライアンスは明示的なプロキシであるため、プラグインは、望ましくない場合でもトラフィックをリダイレクタモードアプライアンスに転送します。クライアントがサーバーから離れたアプライアンスにトラフィックを転送する場合、特にこの「三角形のルート」によって低速または信頼性の低いリンクが導入される場合、アクセラレーションは逆効果になる可能性があります。したがって、特定のアプライアンスが自身のサイトのみを高速化できるようにアクセラレーションルールを構成することをお勧めします。
- その他の用途-プラグインを VPN アクセラレータとしてもリダイレクタモードでも使用しない場合、アクセラレーションルールには、ユーザーからリモートでデータセンターからローカルのアドレスを含める必要があります。

Define the Rules- [構成] の [WANOP クライアントプラグイン] の [アクセラレーションルール] タブで、アクセラレーションルールを定義します。

ルールは順番に評価され、アクション（加速または除外）は最初に一致したルールから実行されます。接続を高速化するには、接続が高速化ルールに一致する必要があります。

デフォルトのアクションは加速しないことです。

図 1: アクセラレーションルールの設定

Signaling Channel Configuration
Acceleration Rules
General Configuration

Repeater Plug-In: Acceleration Rules

Apply
Cancel
Add
Delete
Up
Down

Rule	Rule Type	Destination IP/Mask	Port
1	Exclude	10.200.33.102	All
2	Exclude	10.200.33.100	All
3	Exclude	10.200.33.104	All
4	Exclude	10.200.33.105	All
5	Accelerate	10.0.0.0/8	All
Default	Exclude	All	All

1. 構成: WANOP プラグイン: アクセラレーションルールタブ:

- アプライアンスが到達できるローカル LAN サブネットごとに Accelerated ルールを追加します。つまり、[追加] をクリックし、[アクセラレート] を選択して、サブネットの IP アドレスとマスクを入力します。
 - アプライアンスに対してローカルなサブネットごとに繰り返します。
2. 含まれる範囲の一部を除外する必要がある場合は、除外ルールを追加して、より一般的なルールの上に移動します。たとえば、10.217.1.99 はローカルアドレスのように見えます。それが実際に VPN ユニットのローカルエンドポイントである場合は、次の Accelerate ルールの上の行に Exclude ルールを作成します。10.217.1.0/24.
 3. HTTP のポート 80 など、単一のポートのみにアクセラレーションを使用する場合（非推奨）、[ポート] フィールドのワイルドカード文字を特定のポート番号に置き換えます。ポートごとに 1 つずつルールを追加することで、追加のポートをサポートできます。
 4. 一般に、一般的なルールの前に狭いルール（通常は例外）をリストします。
 5. [適用] をクリックします。適用する前にこのページから移動した場合、変更は保存されません。

IP ポートの使用法

IP ポートの使用については、次のガイドラインを使用してください。

- **WANOP Client Plug-in Plug-in** との通信に使用されるポート: プラグインは、シグナリング接続を介してアプライアンスとのダイアログを保持します。デフォルトでは、ほとんどのファイアウォールで許可されているポート 443 (HTTPS) にあります。

- サーバーとの通信に使用されるポート：WANOP Client Plug-in Plug-in Appliance 間の通信では、プラグインとアプライアンスが存在しない場合、クライアントがサーバーとの通信に使用するポートと同じポートが使用されます。つまり、クライアントがポート 80 で HTTP 接続を開くと、ポート 80 でアプライアンスに接続します。次に、アプライアンスはポート 80 でサーバーに接続します。

リダイレクタモードでは、既知のポート（つまり、TCP SYN パケットの宛先ポート）のみが保持されます。エフェメラルポートは保持されません。透過モードでは、両方のポートが保持されます。

アプライアンスは、クライアントが要求した任意のポートでサーバーと通信できると想定し、クライアントは、任意のポートでアプライアンスと通信できると想定します。これは、アプライアンスがサーバーと同じファイアウォールルールの対象である場合にうまく機能します。このような場合、直接接続で成功する接続はすべて、高速接続で成功します。

TCP オプションの使用法とファイアウォール

WANOP クライアントプラグインパラメータは、TCP オプションで送信されます。TCP オプションは任意のパケットで発生する可能性があり、接続を確立する SYN および SYN-ACK パケットに存在することが保証されています。

ファイアウォールが 24~31（10 進数）の範囲の TCP オプションをブロックしてはなりません。ブロックしないと、アクセラレーションを実行できません。ほとんどのファイアウォールはこれらのオプションをブロックしません。ただし、リリース 7.x ファームウェアを搭載した Cisco PIX または ASA ファイアウォールはデフォルトでそうする可能性があるため、設定を調整する必要がある場合があります。

プラグイン MSI ファイルをカスタマイズする

May 10, 2021

WANOP クライアントプラグイン配布ファイルでパラメーターを変更できます。配布ファイルは、標準の Microsoft インストーラ (MSI) 形式です。カスタマイズには、MSI エディタを使用する必要があります。

注

編集したパラメータの変更。MSI ファイルは、新規インストールにのみ適用されます。既存のプラグインユーザーが新しいリリースに更新しても、既存の設定は保持されます。したがって、パラメータを変更した後は、新しいバージョンをインストールする前に、古いバージョンをアンインストールするようにユーザーにアドバイスする必要があります。

ベスト・プラクティス:

最も近いプラグイン対応アプライアンスに解決される DNS エントリを作成します。たとえば、アプライアンスが 1 つしかない場合は、「Repeater.mycompany.com」を定義して、アプライアンスに解決させます。または、たとえば 5 つのアプライアンスがある場合は、Repeater.mycompany.com を 5 つのアプライアンスの 1 つに解決し、ク

クライアントまたはVPN ユニットへの近さに基づいてアプライアンスを選択します。たとえば、特定のVPNに関連付けられたアドレスを使用しているクライアントは、`Repeater.mycompany.com` がそのVPNに接続されているWANOPクライアントプラグインアプライアンスのIPアドレスに解決されることを確認する必要があります。OrcaなどのMSIエディターを使用して、このアドレスをプラグインバイナリに組み込みます。アプライアンスを追加、移動、または削除するときに、DNSサーバーでこの単一のDNS定義を変更すると、プラグインのアプライアンスリストが自動的に更新されます。

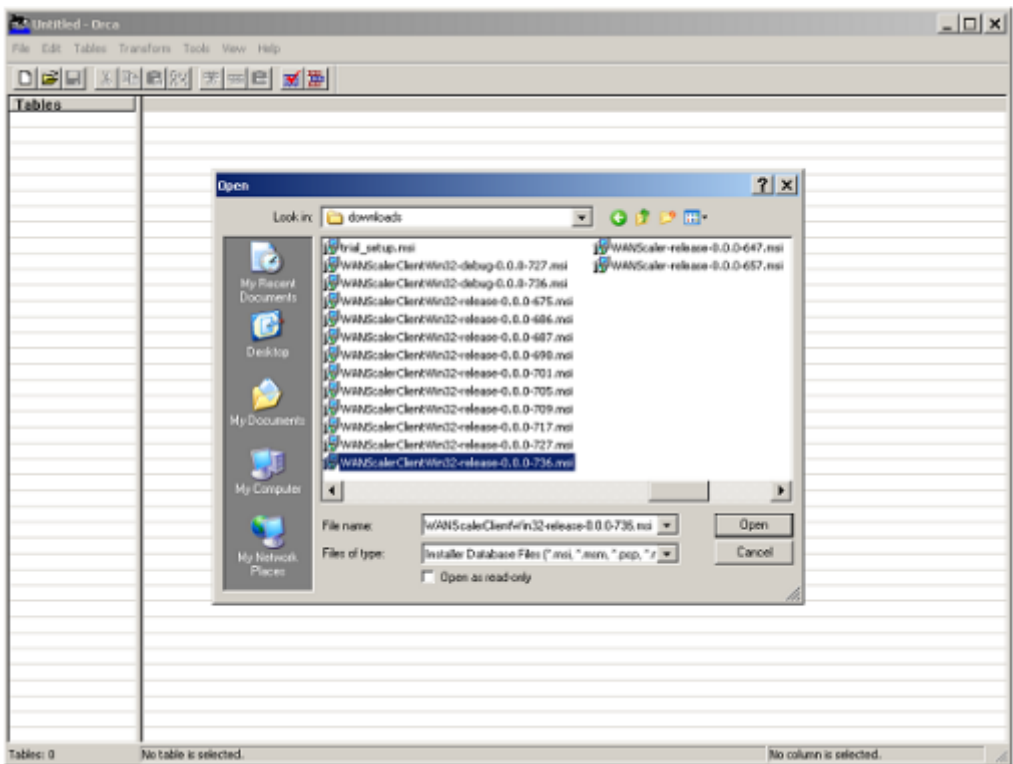
DNSエントリを複数のアプライアンスに解決することもできますが、プラグインはリストの左端のアプライアンスからその特性の一部を取得し、それらをグローバルに適用するため（SSL圧縮特性を含む）、すべてのアプライアンスが同じように構成されていない限り、これは望ましくありません。これは、特にDNSサーバーが各要求のIPアドレスの順序をローテーションする場合に、望ましくない混乱を招く結果につながる可能性があります。

Orca MSI エディタをインストールします。

Orca など多くの MSI エディタが存在する。Orca は Microsoft の無償の Platform SDK の一部であり、Microsoft からダウンロードできる。

- Orca MSI エディタをインストールするには
 1. SDK の PSDK-x86.exe バージョンをダウンロードして実行します。インストール手順に従います。
 2. SDK をインストールしたら、Orca エディタをインストールする必要があります。これは、Microsoft プラットフォーム SDK\ Bin\ Orca.Msi の下になります。Orca.msi を起動して、実際の Orca エディタ (orca.exe) をインストールします。
 3. **Orca** の実行: Microsoft は Orca のドキュメントをオンラインで提供しています。次の情報は、最も重要な WANOP クライアント・プラグイン・パラメータを編集する方法について説明します。
 4. [スタート]>[すべてのプログラム]>[オルカ]で**Orca**を起動します。空のOrcaウィンドウが表示されたら、[ファイル]>[開く]で**WANOP**クライアントプラグイン**MSI**ファイルを開きます。

図 1: **Orca** の使用



5. [テーブル] メニューの [プロパティ] をクリックします。.MSI ファイルの編集可能なすべてのプロパティのリストが表示されます。次の表に示すパラメーターを編集します。パラメータを編集するには、その値をダブルクリックし、新しい値を入力して **[Enter]** を押します。

パラメーター	説明	デフォルト	コメント
WSAPPLIANCES	アプライアンスの一覧	なし	ここでは、WANOP アプライアンスの IP アドレスまたは DNS アドレスをカンマで区切って入力します。{appliance1, appliance2, appliance3} の形式で入力します。シグナリング接続に使用されるポートがデフォルト（443）と異なる場合は、Appliance1: port_number の形式でポートを指定します。

パラメーター	説明	デフォルト	コメント
DBCMINSIZE	圧縮に使用するディスク領域の最小量（メガバイト単位）	250	これを大きな値（2000 など）に変更すると、圧縮のパフォーマンスは向上しますが、十分なディスク領域がない場合はインストールできなくなります。 DBCMINSIZE に指定した値に加えて、少なくとも 100 MB の空きディスク容量がない限り、プラグインはインストールされません。
EKEYPEM	プラグインの秘密キー。SSL 圧縮で使用する証明書/キーペアの一部	なし	Orca の [セルを貼り付け] コマンドを使用します。通常の [貼り付け] 機能では、キーの形式は保持されません。PEM 形式の秘密キーである必要があります（— BEGIN RSA プライベートキーで始まる）
X509CERTPEM	プラグインの証明書。SSL 圧縮で使用する証明書/キーペアの一部	なし	Orca の [セルを貼り付け] コマンドを使用します。通常の [貼り付け] 機能では、キーの形式は保持されません。PEM 形式の証明書である必要があります（— BEGIN Certificate —で始まる）
CACERTPEM	プラグインの証明機関証明書。SSL 圧縮で使用	なし	Orca の [セルを貼り付け] コマンドを使用します。通常の [貼り付け] 機能では、キーの形式は保持されません。PEM 形式の証明書である必要があります（— BEGIN Certificate —で始まる）

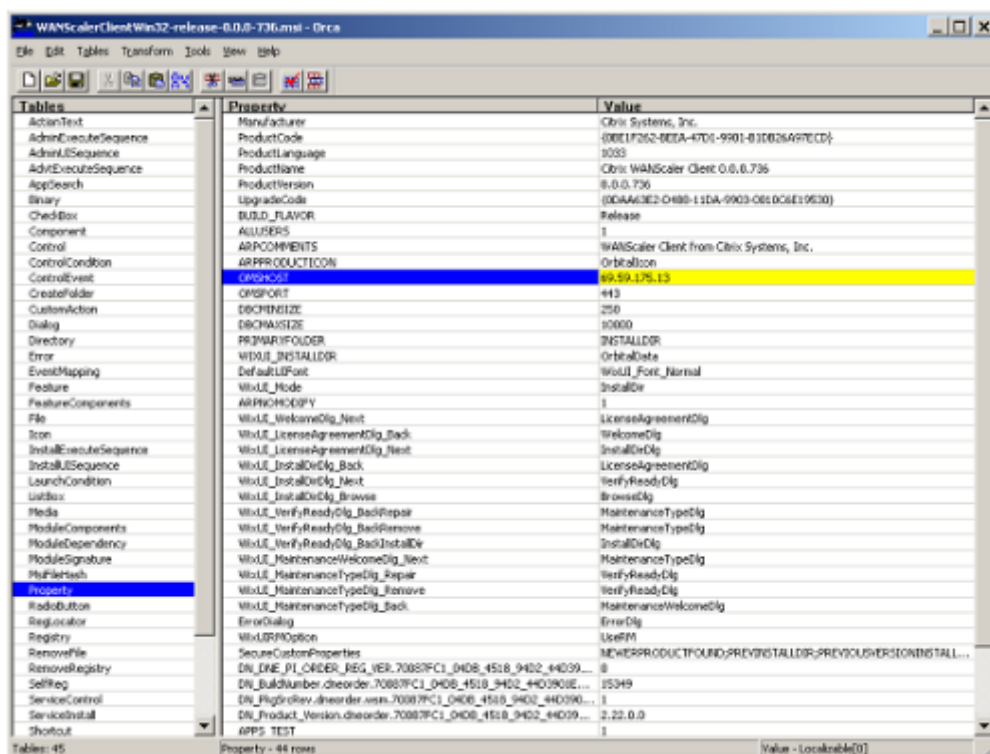
6. [テーブル] メニューで、[プロパティ] をクリックします。.MSI ファイルの編集可能なすべてのプロパティのリストが表示されます。次の表に示すパラメーターを編集します。パラメータを編集するには、その値をダブルクリックし、新しい値を入力して **[Enter]** を押します。

パラメーター	説明	デフォルト	コメント
WSAPPLIANCES	アプライアンスの一覧	なし	WANOP クライアント・プラグイン・アプライアンスの IP または DNS アドレスをここに入力します。 <i>{appliance1, appliance2, appliance3}</i> の形式でカンマ区切りのリストで入力します。シグナリング接続に使用されるポートがデフォルト (443) と異なる場合は、 <i>Appliance1: port_number</i> の形式でポートを指定します。
DBCMINSIZE	圧縮に使用するディスク領域の最小量 (メガバイト単位)	250	これを大きな値 (2000 など) に変更すると、圧縮のパフォーマンスは向上しますが、十分なディスク領域がない場合はインストールできなくなります。 DBCMINSIZE に指定した値に加えて、少なくとも 100 MB の空きディスク容量がない限り、プラグインはインストールされません。
PRIVATEKEYPEM	プラグインの秘密キー。SSL 圧縮で使用する証明書/キーペアの一部	なし	Orca の [セルを貼り付け] コマンドを使用します。通常の [貼り付け] 機能では、キーの形式は保持されません。PEM 形式の秘密キーである必要があります (—BEGIN RSA プライベートキーで始まる)

パラメーター	説明	デフォルト	コメント
X509CERTPEM	プラグインの証明書。SSL 圧縮で使用される証明書/キーペアの一部	なし	Orca の [セルを貼り付け] コマンドを使用します。通常の [貼り付け] 機能では、キーの形式は保持されません。PEM 形式の証明書である必要があります (— BEGIN Certificate —で始まる)
CACERTPEM	プラグインの証明機関証明書。SSL 圧縮で使用	なし	Orca の [セルを貼り付け] コマンドを使用します。通常の [貼り付け] 機能では、キーの形式は保持されません。PEM 形式の証明書である必要があります (— BEGIN Certificate —で始まる)

7. 完了したら、[ファイル]: [名前を付けて 保存] コマンドを使用して、編集したファイルを新しいファイル名 (test.msi など) で保存します。

図 2: Orca のパラメータの編集:



- 完了したら、[ファイル]: [名前を付けて 保存] コマンドを使用して、編集したファイルを新しいファイル名 (test.msi など) で保存します。

これで、プラグインソフトウェアがカスタマイズされました。

注

一部のユーザーは、ファイルを 1MB に切り捨てる orca のバグを確認しています。保存したファイルのサイズを確認してください。切り捨てられている場合は、元のファイルのコピーを作成し、[保存] コマンドを使用して元のファイルを上書きします。

Orca を使用してアプライアンスリストをカスタマイズし、カスタマイズした MSI ファイルをユーザーに配布すると、ユーザーはソフトウェアのインストール時に構成情報を入力する必要がなくなります。

Windows システムにプラグインを展開する

May 10, 2021

WANOP クライアントプラグインは、他の Web 配布プログラムと同様にダウンロードしてインストールする実行可能な Microsoft インストーラー (MSI) ファイルです。このファイルは、Citrix.com Web サイトの MyCitrix セクションから入手します。

注:

WANOP クライアントプラグインのユーザーインターフェイスは、それ自体を **Citrix** アクセラレーションプラグインマネージャーと呼んでいます。

プラグインに必要な唯一のユーザー構成は、アプライアンスアドレスのリストです。このリストは、IP アドレスまたは DNS アドレスのコンマ区切りのリストで構成できます。2 つの形式を混在させることができます。リストがデフォルトでアプライアンスを指すように、配布ファイルをカスタマイズできます。インストールすると、操作は透過的になります。アクセラレーションされたサブネットへのトラフィックは適切なアプライアンスを介して送信され、他のすべてのトラフィックはサーバーに直接送信されます。ユーザーアプリケーションは、これが発生していることに気づいていません。

インストール

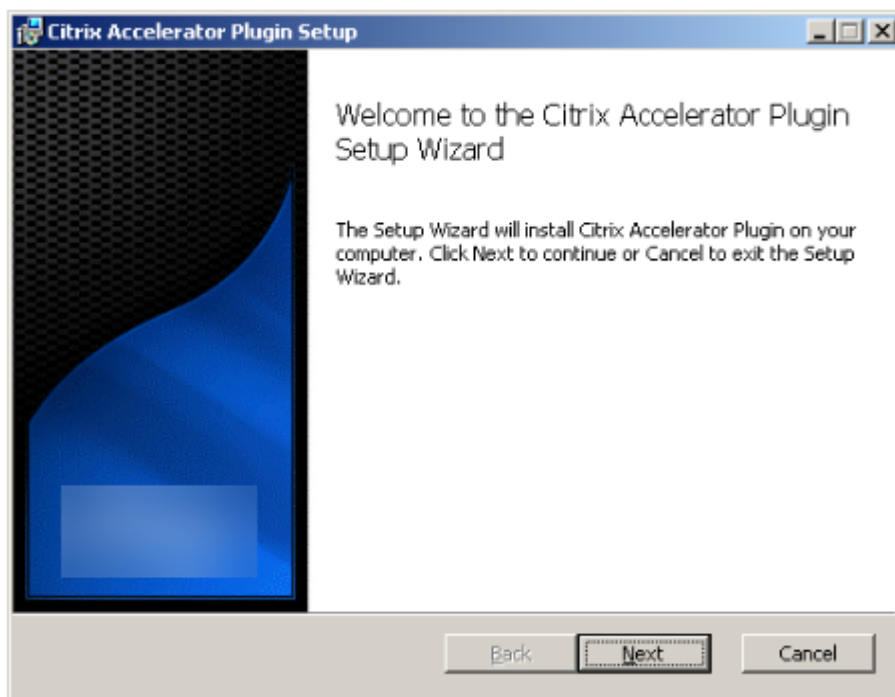
必須要件:

Windows 10 では、エラーなしでインストールを実行するには、すべてのドライバに有効なデジタル署名が必要です。

WANOP クライアントプラグインプラグインアクセラレータを Windows システムにインストールするには:

1. Repeater*.msi ファイルはインストールファイルです。開いているすべてのアプリケーションとウィンドウを閉じて、通常の方法でインストーラを起動します（ファイルウィンドウをダブルクリックするか、run コマンドを使用します）。

図 1: 初期インストール画面:

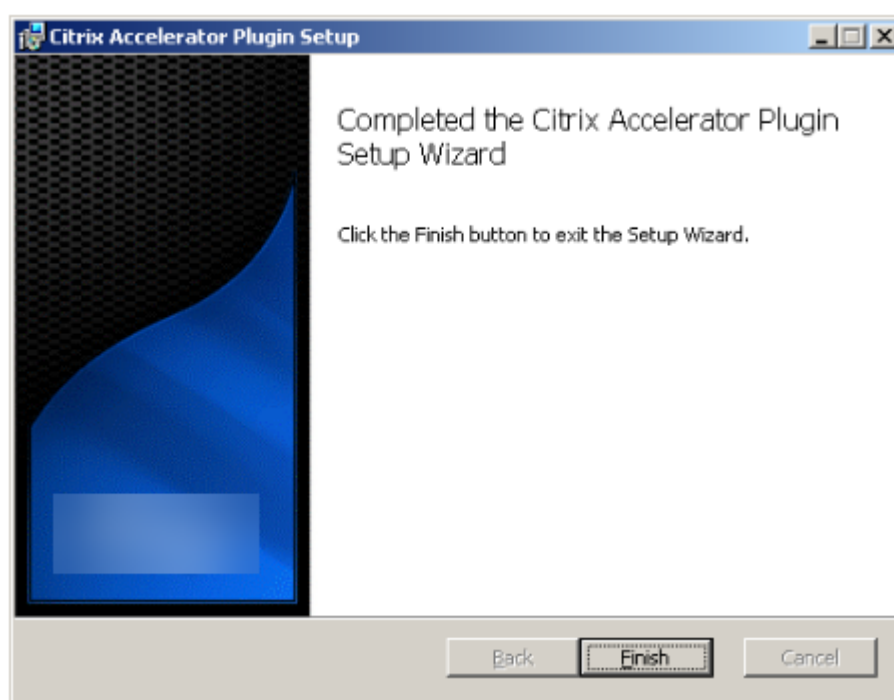


以下の手順は、インタラクティブインストール用です。サイレントインストールは、次のコマンドで実行できます。

「**msiexec /i client_msi_file /qn**」

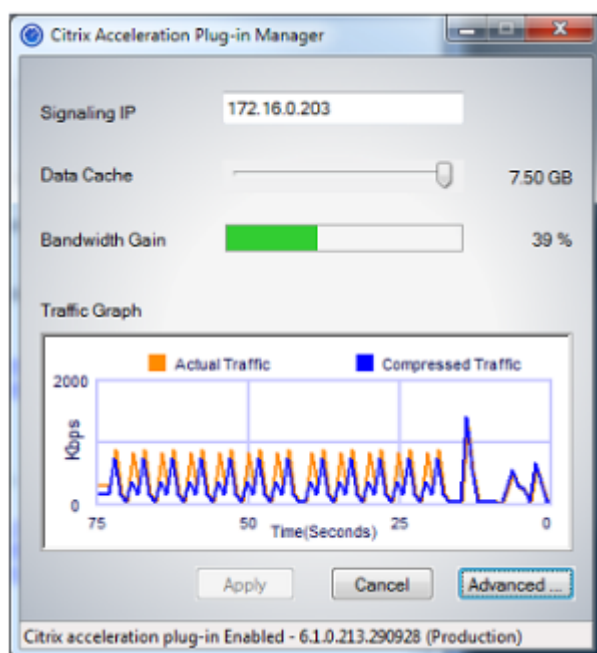
2. インストールプログラムは、ソフトウェアをインストールする場所の入力を求めます。指定したディレクトリは、クライアントソフトウェアとデータベースの圧縮履歴の両方に使用されます。これらを合わせると、最低 500MB のディスク容量が必要です。
3. インストーラーが終了すると、システムを再起動するように求められる場合があります。再起動後、WANOP クライアントプラグインプラグインが自動的に起動します。

図 2: 最終インストール画面



4. タスクバーのアクセラレータアイコンを右クリックし、[アクセラレータの管理] を選択して、Citrix Plug-in Accelerator Manager を起動します。

図 3: Citrix アクセラレータプラグインマネージャー、初期（基本）表示



5. .MSI ファイルがユーザー向けにカスタマイズされていない場合は、シグナリングアドレスと圧縮に使用するディスク容量を指定します。

- [アプライアンス: シグナリングアドレス] フィールドに、アプライアンスのシグナリング IP アドレスを入力します。プラグイン対応アプライアンスが複数ある場合は、それらすべてをコンマで区切ってリストします。IP アドレスまたは DNS アドレスのいずれかを使用できます。
- [データキャッシュ] スライダーを使用して、圧縮に使用するディスク容量を選択します。多いほど良いです。利用可能なディスク容量が多ければ、7.5GB はそれほど多くありません。
- [適用] を押します。

これで、WANOP クライアントプラグインアクセラレータが実行されます。加速されたサブネットへの今後のすべての接続は加速されます

プラグインの [AdvancedRules] タブで、[Acceleration Rules] リストに、各アプライアンスが Connected として表示され、各アプライアンスの Accelerated サブネットが Accelerated として表示されます。そうでない場合は、Signaling Addresses IP フィールドと一般的なネットワーク接続を確認してください。

プラグインのトラブルシューティング

プラグインのインストールは一般的にスムーズに進みます。そうでない場合は、次の問題を確認してください。

一般的な問題:

- システムを再起動しないと、WANOP クライアントプラグインが正しく実行されません。

- 高度に断片化されたディスクは、圧縮パフォーマンスを低下させる可能性があります。
- アクセラレーションの失敗（[**Diagnostics**] タブにアクセラレーション接続が表示されない）は、通常、何かがアプライアンスとの通信を妨げていることを示します。プラグインの [構成: アクセラレーション規則] の一覧をチェックして、アプライアンスに正常に接続され、ターゲットアドレスがアクセラレーション規則の 1 つに含まれていることを確認します。接続障害の一般的な原因は次のとおりです。
 - アプライアンスが実行されていないか、アクセラレーションが無効になっています。
 - ファイアウォールは、プラグインとアプライアンスの間のある時点で WANOP クライアントプラグイン TCP オプションを削除しています。
 - プラグインはサポートされていない VPN を使用しています。

確定的ネットワークエンハンサーロックエラー

まれに、プラグインをインストールしてコンピューターを再起動した後、次のエラーメッセージが 2 回表示されます。

確定的ネットワークエンハンサーのインストールでは、ロックされたリソースを解放するために、最初に再起動する必要があります。コンピュータを再起動した後、このインストールを再度実行してください。

これが発生した場合は、次のようにします。

1. [プログラムの追加と削除] に移動し、WANOP クライアントプラグインがあれば削除します。
2. [コントロールパネル] > [ネットワークアダプタ] > [ローカルエリア接続] > [プロパティ] に移動し、[決定論的ネットワークエンハンサー] のエントリを探し、チェックボックスをオフにして、[**OK**] をクリックします。（ネットワークアダプタが「ローカルエリア接続」以外の名前呼び出されることがあります。）
3. コマンドウィンドウを開き、c:\windows\inf (Windows を標準以外の場所にインストールしている場合は、同等のディレクトリ) に移動します。
4. 次のコマンドを入力します。

「`dne2000.cat`」を見つける `oem*.inf`
5. 一致する行（一致する行は `CatalogFile= dne2000.cat`）を返した最も高い番号の `oem*.inf` ファイルを検索し、編集します。次に例を示します：

`notepad oem13.inf`
6. セミコロンで始まる上部の 3 行を除くすべてを削除してから、ファイルを保存します。これにより、不適切または廃止された設定がすべてクリアされ、次のインストールではデフォルト値が使用されます。
7. インストールを再試行してください。

その他のインストールの問題

WANOP クライアントプラグインのインストールに関する問題は、通常、既存のネットワーク、ファイアウォール、またはウイルス対策ソフトウェアがインストールを妨害した結果です。通常、インストールが完了すると、それ以上の問題は発生しません。

インストールが失敗した場合は、次の手順を試してください。

1. プラグインインストールファイルがローカルシステムにコピーされていることを確認してください。
2. アクティブなものをすべて切断します VPN/remote ネットワーククライアント。
3. ファイアウォールとウイルス対策ソフトウェアを一時的に無効にします。
4. これのいくつかが難しい場合は、できることをしてください。
5. WANOP クライアントプラグインを再インストールします。
6. それでも問題が解決しない場合は、システムを再起動してもう一度試してください。

WANOP プラグイン GUI コマンド

May 10, 2021

[Citrix アクセラレータプラグイン] アイコンを右クリックし、[アクセラレータの管理] を選択すると、**WANOP** クライアントプラグイン GUI が表示されます。GUI の基本画面が最初に表示されます。必要に応じて使用できる高度なディスプレイもあります。

基本表示

[基本] ページでは、次の 2 つのパラメーターを設定できます。

- Signaling Addresses フィールドは、プラグインが接続できる各アプライアンスの IP アドレスを指定します。アプライアンスを 1 つだけリストすることをお勧めしますが、コンマ区切りのリストを作成することもできます。これは順序付きリストであり、左端のアプライアンスが他のアプライアンスよりも優先されます。信号接続を確立できる左端のアプライアンスで加速が試行されます。DNS アドレスと IP アドレスの両方を使用できます。

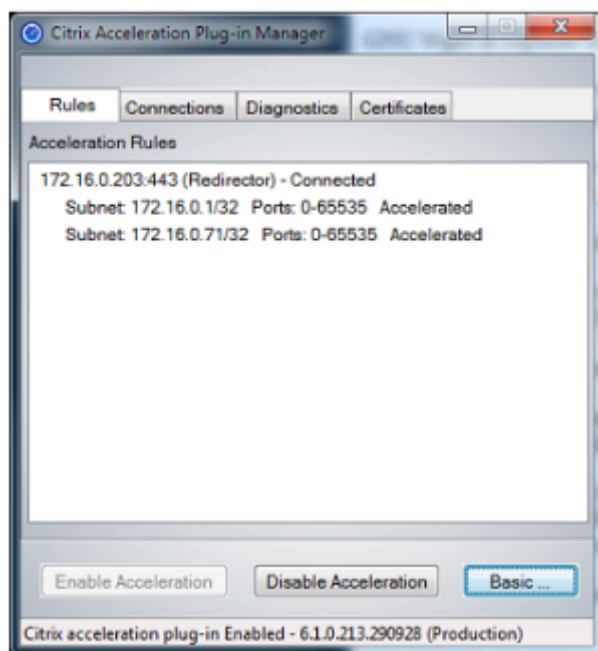
例: 10.200.33.200、ws.mycompany.com、ws2.mycompany.com

- データキャッシュスライダーは、プラグインのディスクベースの圧縮履歴に割り当てられるディスクスペースの量を調整します。多いほど良いです。

さらに、詳細表示に移動するためのボタンがあります。

高度な表示

[詳細設定] ページには、[ルール]、[接続]、[診断]、および [証明書] の 4 つのタブがあります。



ディスプレイの下部には、アクセラレーションを有効にしたり、アクセラレーションを無効にしたり、基本ページに戻ったりするためのボタンがあります。

[ルール] タブ

[ルール] タブには、アプライアンスからダウンロードされたアクセラレーションルールの簡略リストが表示されます。各リスト項目には、アプライアンスのシグナリングアドレスとポート、アクセラレーションモード（リダイレクタまたはトランスペアレント）、接続状態が表示され、その後にアプライアンスのルールの概要が表示されます。

[接続] タブ

[接続] タブには、さまざまなタイプの開いている接続の数が表示されます。

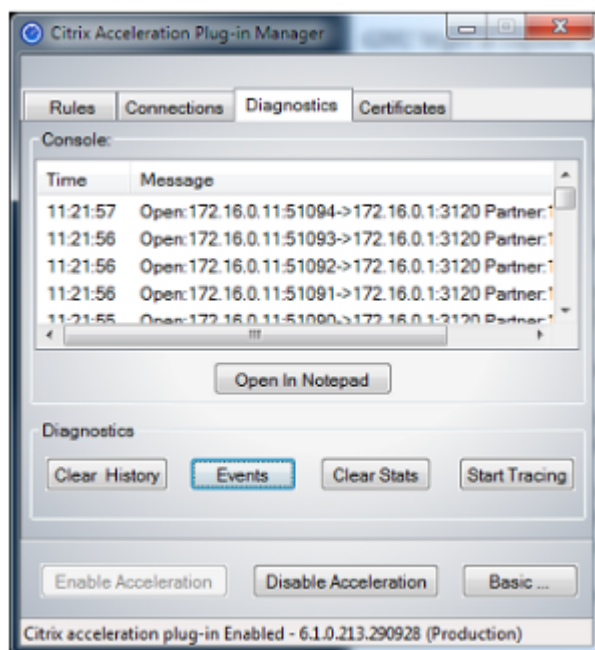
- **アクセラレーテッド接続**: WANOP クライアント・プラグインとアプライアンス間のオープン接続の数。この数には、アプライアンスごとに 1 つのシグナリング接続が含まれますが、高速化された CIFS 接続は含まれません。[詳細] をクリックすると、各接続の簡単な概要を示すウィンドウが開きます。（[その他] ボタンはすべて、サポートと共有する場合に、ウィンドウ内の情報をクリップボードにコピーできます。）
- **CIFS 接続の高速化**: CIFS（Windows ファイル・システム）サーバとのオープンで高速化された接続の数。これは通常、マウントされたネットワークファイルシステムの数と同じです。[詳細] をクリックすると、高速接続の場合と同じ情報に加えて、CIFS 接続が WANOP クライアントプラグインの特別な CIFS 最適化で実行されている場合にアクティブを報告するステータスフィールドが表示されます。

- 高速化された **MAPI** 接続: オープンで高速化された Outlook/Exchange 接続の数。
- アクセラレーション **ICA** 接続: ICA プロトコルまたは CGP プロトコルを使用して、オープンでアクセラレーションされた XenApp および XenDesktop 接続の数。
- アクセラレーションされていない接続: アクセラレーションされていない接続を開きます。[詳細] をクリックすると、接続が高速化されなかった理由の簡単な説明が表示されます。通常、この理由は、宛先アドレスを加速させるアプライアンスがないためです。このアドレスは、サービスポリシールールとして報告されます。
- 接続のオープン/クローズ: 完全にオープンではないが、オープンまたはクローズ処理中の接続 (TCP「ハーフオープン」または「ハーフクローズ」接続)。[詳細] ボタンには、これらの接続に関する追加情報が表示されます。

[診断] タブ

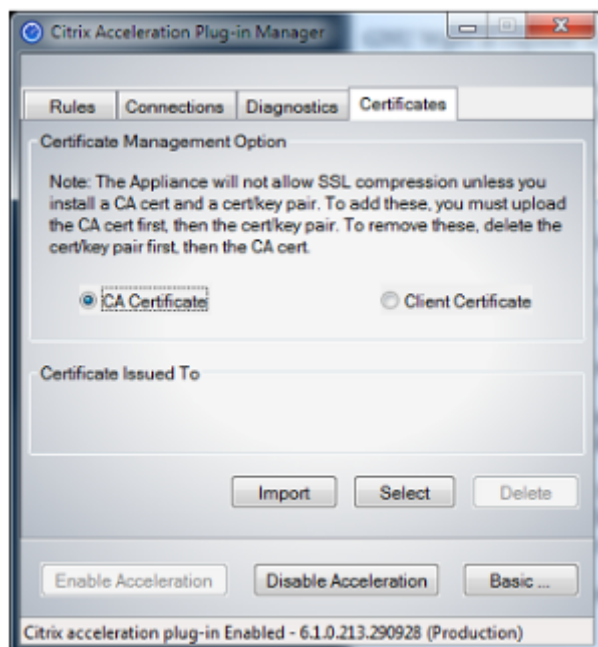
[診断] ページには、さまざまなカテゴリの接続数やその他の役立つ情報が報告されます。

- トレースの開始/トレースの停止: 問題を報告した場合、Citrix の担当者が問題を特定するために接続トレースの実行を依頼することがあります。このボタンは、トレースを開始および停止します。トレースを停止すると、ポップアップウィンドウにトレースファイルが表示されます。Citrix の担当者が推奨する方法でそれらを送信します。
- 履歴のクリア: この機能は使用しないでください。
- **Clear Statistics**-このボタンを押すと、[Performance] タブの統計情報がクリアされます。
- **Console**: スクロール可能なウィンドウで、最近のステータスメッセージ (ほとんど接続オープンメッセージと接続クローズメッセージ、エラーメッセージやその他のステータスメッセージなど) が表示されます。



【証明書】タブ

【証明書】タブで、オプションのセキュアピアリング機能のセキュリティ資格情報をインストールできます。これらのセキュリティ資格情報の目的は、プラグインが信頼できるクライアントであるかどうかをアプライアンスが確認できるようにすることです。



CA 証明書と証明書とキーのペアをアップロードするには:

1. [CA 証明書管理] を選択します。
2. [インポート] をクリックします。
3. CA 証明書をアップロードします。証明書ファイルは、サポートされているファイルタイプ（.pem、.crt、.cer、または.spc）のいずれかを使用する必要があります。使用する証明書ストアを選択するように求めるダイアログボックスが表示され、キーワードのリストが表示される場合があります。リストの最初のキーワードを選択します。
4. [クライアント証明書の管理] を選択します。
5. [インポート] をクリックします。
6. 証明書とキーのペアの形式を選択します（PKCS12 または PEM/DER）。
7. [Submit] をクリックします。

注

の場合 PEM/DER, 証明書とキー用に別々のアップロードボックスがあります。証明書とキーのペアが 1 つのファイルに結合されている場合は、ファイルを 2 回、各ボックスに 1 回指定します。

WANOP プラグインの更新

May 10, 2021

新しいバージョンの WANOP クライアントプラグインをインストールするには、プラグインを初めてインストールするときに使用したのと同じ手順に従います。

WANOP クライアントプラグインをアンインストールします

WANOP クライアントプラグインをアンインストールするには、Windows の [プログラムの追加と削除] ユーティリティを使用します。WANOP クライアントプラグインは、現在インストールされているプログラムのリストに、**Citrix** アクセラレーションプラグイン として表示されます。それを選択し、[削除] をクリックします。

クライアントのアンインストールを完了するには、システムを再起動する必要があります。

WANOP プラグインのトラブルシューティング

May 10, 2021

- 問題: シグナリングチャネルの接続の問題に直面しています。これらの問題を解決するにはどうすればよいですか？

解決策: シグナリングチャネルの接続の問題を解決するには、次のトラブルシューティング手順を実行します。

- シグナリング IP アドレスが正しく構成されていることを確認します。これを行うには、シグナリング IP アドレスに ping を実行し、応答を確認します。
 - WANOP アプライアンスでシグナリングステータスが有効になっていることを確認します。
 - ネットワークにインストールされているファイアウォールが WANOP TCP オプションを削除しないことを確認します。
 - 有効な WANOP プラグインライセンスが WANOP アプライアンスにインストールされていることを確認します。
 - シグナリングチャネルソースフィルタリング構成がクライアントソース IP アドレスをブロックしないことを確認します。
 - LAN 検出を有効にしている場合は、WANOP プラグインと WANOP アプライアンス間のラウンドトリップ時間が許容値であることを確認してください。
- 問題: WANOP 4000 アプライアンスで、WANOP プラグインを無効にできません。
- 原因: これは既知の問題です。

解決策: なし。WANOP4000 アプライアンスで WANOP プラグインを無効にすることはできません。

- 問題: WANOP プラグインを使用して WANOP アプライアンスに接続すると、次のエラーメッセージエントリが [Alerts] タブに記録されます。

<Number> このアプライアンスに接続しようとした WANOP プラグインの現在の制限を超えています。

原因: WANOP アプライアンスへの接続数が、ライセンスされたユーザー制限を超えました。

解決策: ユーザーが接続を切断するのを待つか、接続を終了します。

- 問題: WANOP 4000 または 5000 アプライアンスで正しくないシグナリング IP アドレスが設定されています。

解決策: WANOP 4000 または 5000 アプライアンスのシグナリング IP アドレスを更新するには、次の手順を実行します。

1. WANOP アプライアンスの NetScaler インスタンスにログオンします。
2. [トラフィック管理] > [負荷分散] > [仮想サーバー] > [BR_LB_VIP_SIG] ページに移動します。
3. シグナリング IP アドレスを更新します。
4. 構成を保存します。

- 問題: CIFS と ICA のトラフィックが加速されない。

解決策: この問題を解決するには、次のトラブルシューティング手順を実行します。

- IP アドレスとポート番号のアクセラレーションルールが WANOP プラグインに対して正しく定義されていることを確認します。
- シグナリング接続が成功した後、CIFS または ICA 接続が確立されていることを確認します。
- 使用されているサービスクラスのアクセラレーションポリシーを確認します。

SMB 3.1.1 接続

May 10, 2021

サーバーメッセージブロック (SMB) プロトコルは、ネットワークファイル共有プロトコルです。プロトコルの特定のバージョンを定義するメッセージパケットは、ダイレクトと呼ばれます。共通インターネットファイルシステム (CIFS) プロトコルは、SMB の方言です。

Citrix SD-WAN リリース 10 バージョン 1 では、SMB 3.1.1 プロトコルが Citrix SD-WAN WANOP および Premium エディションプラットフォームで導入されています。

Citrix SD-WAN WANOP は、SMB 3.1.1 接続をサポートします。SMB 3.1.1 接続は、クライアントが Windows 10 で、サーバーが Windows Server 2016 の場合に適用されます。

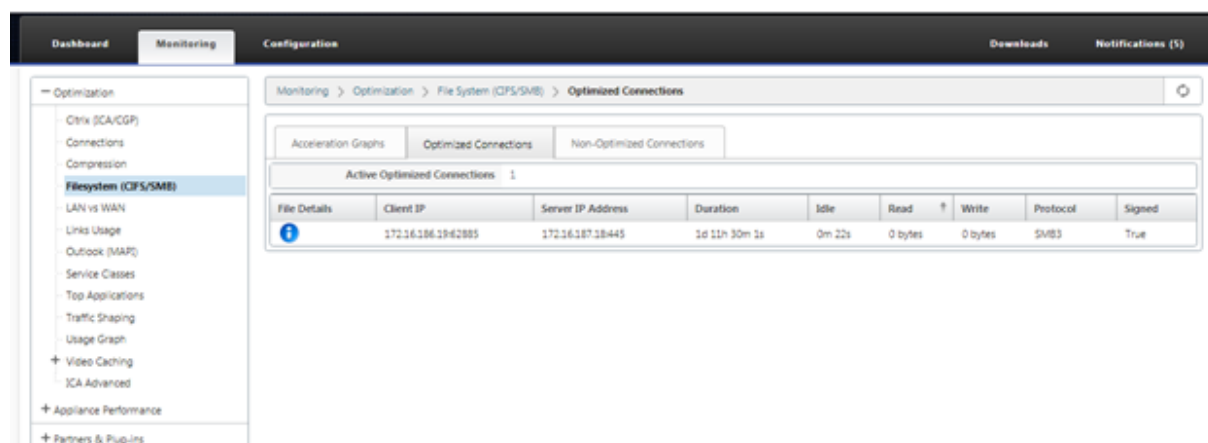
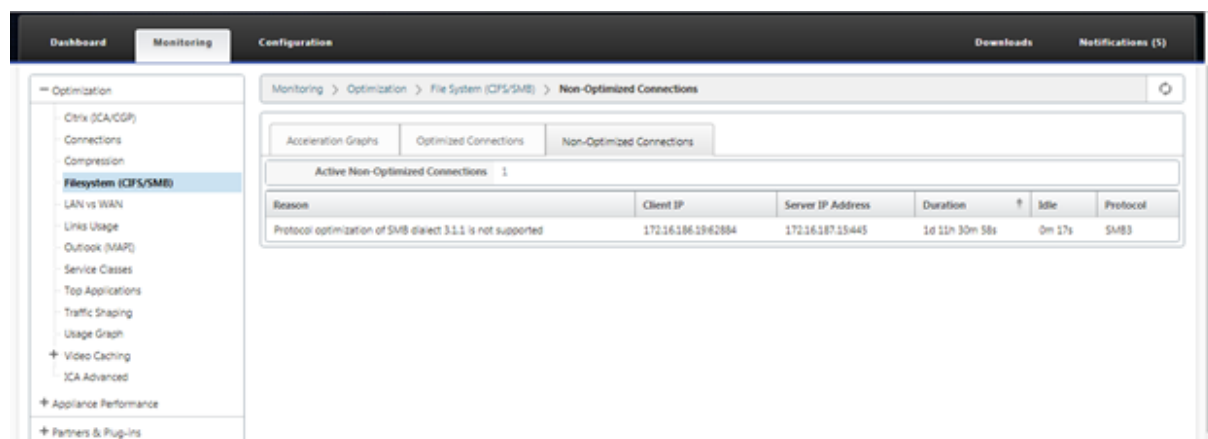
SMB 3.1.1 トラフィックが WANOP モジュールを通過する場合:

- SMB 3.1 CIFS 最適化されていない接続の一部としてカウント/認識可能
- 次のトレースメッセージが表示されます、「SMB 3.1.1 としてこの接続を渡すはサポートされていません」。

クライアント	サーバー	SMB バージョン
Windows 10	Win 2016, 2012R2	SMB 3.1.1, 3.0.2
Windows 8.1	SMB 3.0	SMB 3.0
Windows 7	SMB 3.0	SMB 3.0

最適化されていない接続の場合、Citrix SD-WAN WANOP アプライアンスの GUI に SMB 3.1.1 のメッセージが表示されます。

Citrix SD-WAN WANOP アプライアンスの GUI で、[監視] > [ファイルシステム (**CIFS/SMB**)] に移動します。[非最適化された接続] タブをクリックすると、次のメッセージが表示されます。*SMB* ダイアレクト 3.1.1 のプロトコル最適化はサポートされていません。使用可能なログエントリはありません。また、SD-WAN WANOP では、これをサポートするための新しい設定は必要ありません。



ハウツー記事

August 30, 2022

「How-to-Articles」では、Citrix SD-WAN でサポートされる機能を構成する手順について説明します。これらの記事には、次の重要な機能の一部に関する情報が含まれています。

以下の機能名をクリックすると、その機能に関するハウツー記事のリストが表示されます。

- [仮想ルーティングと転送](#)
- [QoS 公平性のための RED の有効化](#)
- [構成](#)
- [動的ルーティング](#)
- [DHCP サーバーと DHCP リレー](#)
- [ルートフィルタ](#)
- [IPSec の終了とモニタリング](#)
- [Secure Web Gateway](#)
- [QoS](#)
- [FIPS 準拠の動作-IPSec トンネル](#)
- [ダイナミック NAT 設定](#)
- [適応型帯域幅検出](#)
- [アクティブ帯域幅テスト](#)
- [BGP の拡張機能](#)
- [SSL プロファイルとサービスクラスの関連付け](#)
- [セキュアピアリングと手動セキュアピアリング](#)
- [ゼロタッチ展開](#)
- [ツートップモードの展開](#)

インターフェイスグループ

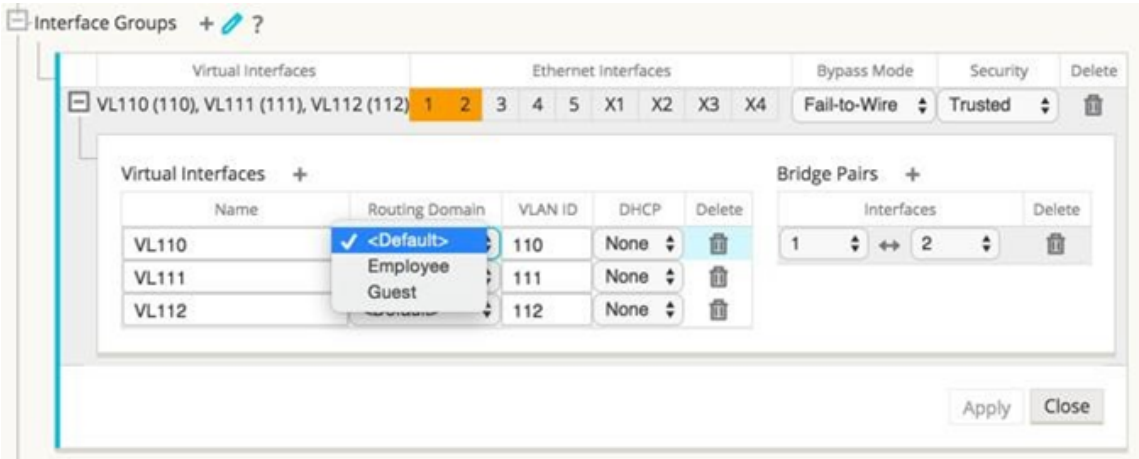
May 10, 2021

インターフェイスグループを設定するには、次の手順を実行します。

1. 構成エディターで、[サイト] > [[クライアントサイト名]] > [インターフェイスグループ] に移動し、仮想インターフェイスを設定するときにドロップダウンメニューから ルーティングドメイン を選択します。詳しい手順については、[設定, インターフェイスグループ](#)を参照してください。

注

仮想インターフェイスが特定のルーティングドメインに関連付けられると、そのルーティングドメインを使用する場合、それらのインターフェイスだけが使用可能になります。



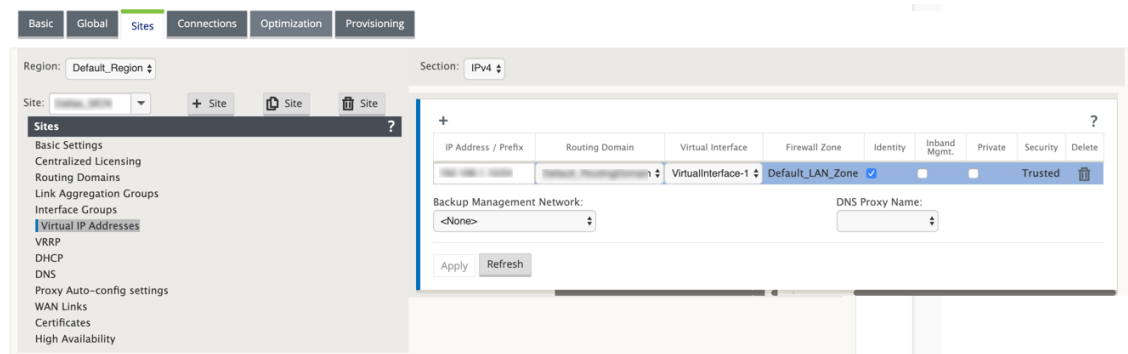
仮想 IP アドレス ID の設定

May 10, 2021

仮想ネットワークインターフェイスは、同じサブネットまたは異なるサブネットで複数の IP アドレスをホストできます。ただし、ID が true に設定されている仮想 IP は 1 つだけ選択できます。仮想 IP は、BGP/OSPF、DHCP サーバ/リレー、およびインバンド管理などのダイナミックルーティングプロトコルに使用できます。

仮想 IP アドレス ID を構成するには、次の手順を実行します。

1. 構成エディターで、[サイト] > [サイト [名]] > [仮想 IP アドレス] に移動します。
2. 仮想 IP アドレスの [Identity] チェックボックスをクリックして、IP サービスに使用します。



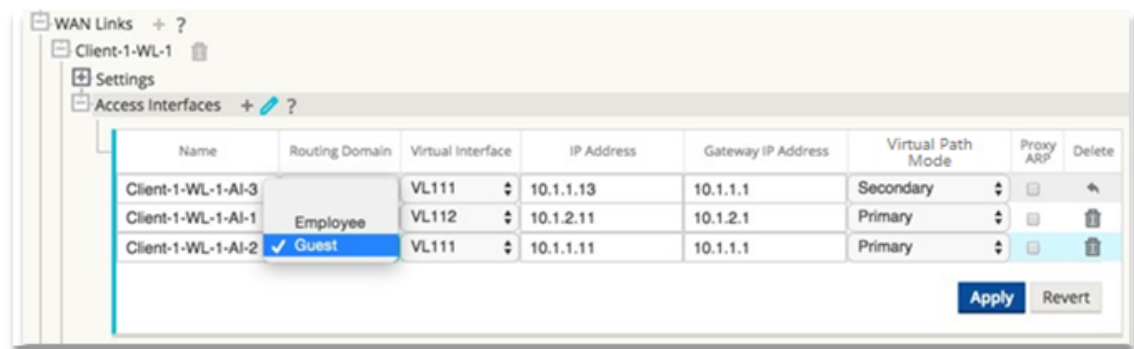
アクセスインターフェイスの設定

September 26, 2023

アクセスインターフェイスを構成するには、次の手順を実行します。

1. 構成エディターで、[サイト]>[クライアント ****[サイト] 名 ****]>[**WAN** リンク]>[W **[AN リンク名]**]>[アクセスインターフェイス]に移動します。
2. アクセスインターフェイスを設定するときに、ドロップダウンメニューから ルーティングドメイン を選択します。

詳細な手順については、[MCN の設定](#)トピックの「アクセスインターフェイスの構成方法」を参照してください。



仮想 IP アドレスの構成

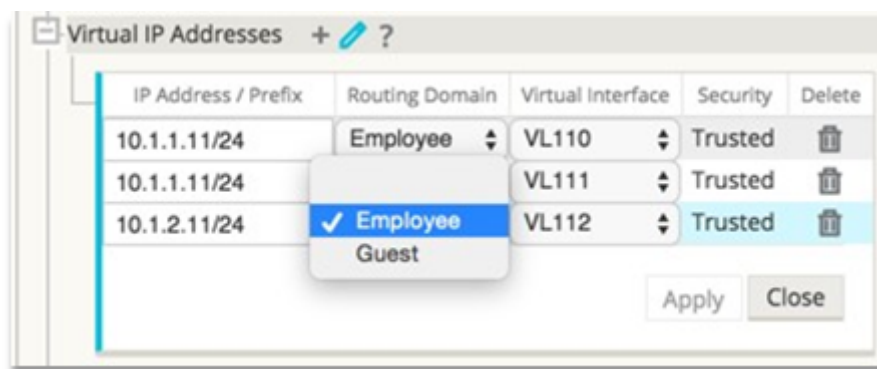
May 10, 2021

仮想 IP アドレスを構成するには

1. 構成エディターで、[サイト] > [[クライアントサイト名]] > [仮想 IP アドレス] に移動します。
2. 仮想 IP アドレスを設定するときに、ドロップダウンメニューから ルーティングドメイン を選択します。

詳しい手順については、[構成](#), [仮想 IP アドレス](#)を参照してください。

選択したルーティングドメインによって、ドロップダウンメニューから使用できる仮想インターフェイスが決まります。



GRE トンネルの設定

May 10, 2021

GRE トンネルを設定するには、次の手順を実行します。

1. 構成エディタで、[接続] > [サイト] > [GRE トンネル] に移動します。送信元 IP アドレスは、信頼できるリンクの仮想ネットワークインターフェイスからのみ選択できます。
2. GRE トンネルの名前を入力します。
3. ドロップダウンメニューから使用可能な送信元 IP アドレスを選択します。ルーティングドメインは、ドロップダウンメニューから使用できる送信元 IP アドレスを決定します。
4. (オプション) パブリックソース IP を選択します。このアドレスが送信元 IP と同じ場合、このフィールドは空にできます。
5. GRE トンネルの宛先 IP アドレスを入力します。
6. GRE トンネルのトンネル IP/プレフィクス アドレスを入力します。
7. GRE トンネルヘッダーでチェックサムを使用する場合は、[チェックサム] をクリックします。
8. キープアライブ期間の値を秒単位で入力します。0 を設定すると、キープアライブパケットは送信されませんが、GRE トンネルはアクティブになります。
9. キープアライブの再試行値を入力します。この値は、SD-WAN アプライアンスが GRE トンネルを非アクティブにするまでにキープアライブの再試行回数を決めます。

詳細については、MCN サイトの[GRE トンネルの設定](#)を参照してください。

Name	Source IP	Public Source IP	Destination IP	Tunnel IP / Prefix	Checksum	Keepalive Period (s)	Keepalive Retries	Delete
Appliance-Tunnel-1	*		*	*	MD5	10	3	

GRE トンネルを使用した Web Gateway のセキュリティ保護の詳細については、[Secure Web Gateway](#)を参照してください。

ブランチ間通信用の動的パスを設定する

May 10, 2021

VoIP とビデオ会議の需要により、トラフィックはオフィス間を移動するようになっています。データセンターを介して完全なメッシュ接続を設定することは効率的ではありません。これには時間がかかることがあります。

Citrix SD-WAN では、すべてのオフィス間のパスを構成する必要はありません。ダイナミックパス機能を有効にすると、SD-WAN ソリューションは必要に応じてオフィス間のパスを自動的に作成します。セッションでは、最初に既存の固定パスが使用されます。また、帯域幅と時間のしきい値が満たされると、新しいパスが固定パスよりも優れたパフォーマンス特性を持つ場合、パスは動的に作成されます。セッショントラフィックは、新しいパスを介して送信されます。これにより、リソースの効率的な使用が可能になります。パスは、必要な場合にのみ存在し、データセンターとの間で送受信されるトラフィックの量を削減します。

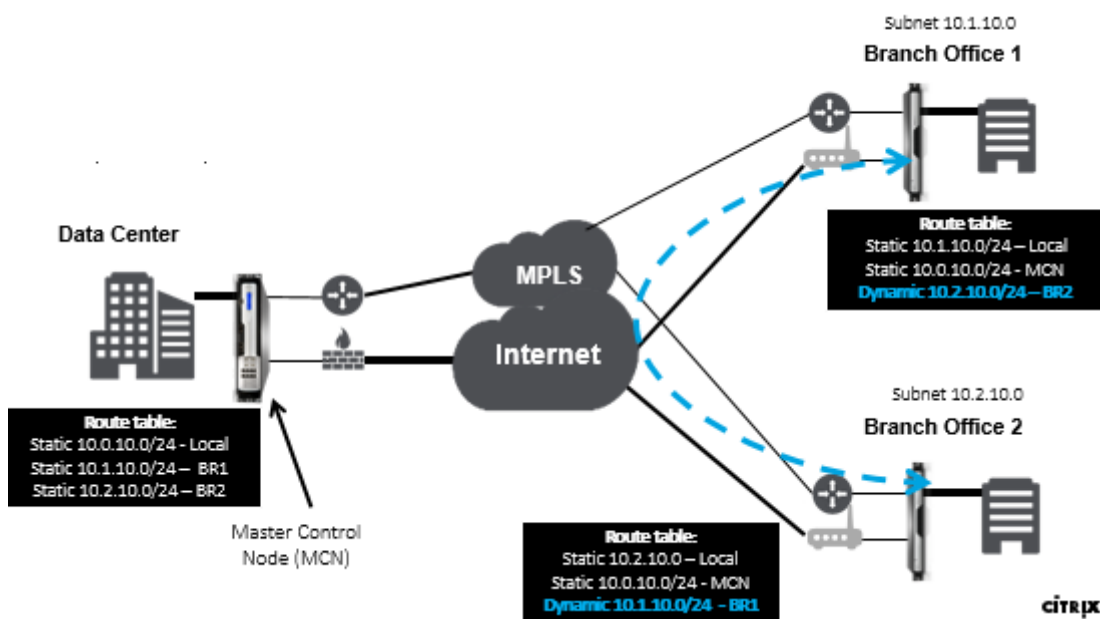
SD-WAN ネットワークのその他の利点は次のとおりです。

- ブランチ間の接続を許可する帯域幅と PPS のしきい値
- レイテンシーを最小限に抑えながら、データセンター内外の帯域幅要件を軽減
- オンデマンドで作成されるパスは、設定されたしきい値に依存
- 必要のない場合にネットワークリソースを動的に解放する
- マスターコントロールノードの負荷とレイテンシーを軽減

動的仮想パスを使用したブランチとブランチ間の通信：



動的パスを持つ SD-WAN ネットワーク：

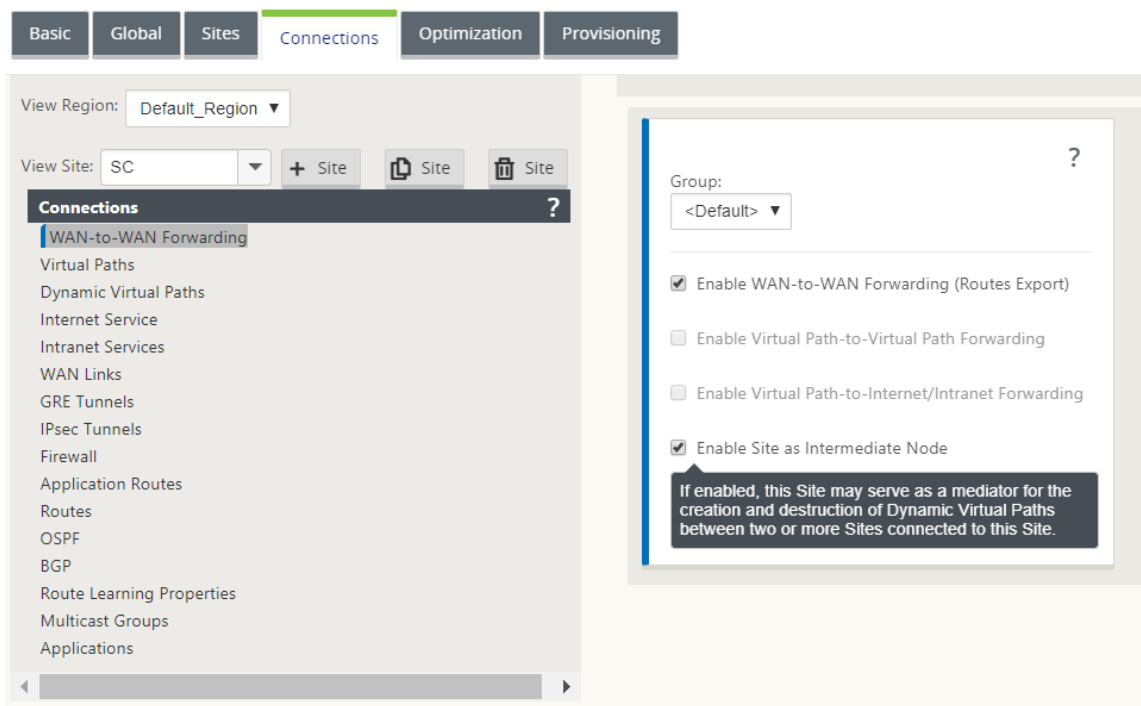


- 動的仮想パスは、エンタープライズなどの大規模な展開に使用されます。
- 小規模な展開では、静的仮想パスと Any-to-any 仮想パスを使用する
- 2 つのデータセンター間 (DC から DC へ) の静的仮想パスを常に使用
- 動的仮想パスを使用するためにすべての WAN パスを構成する必要はありません
- 各 SD-WAN アプライアンスには、構成可能な動的仮想パスの数が制限されています (動的最小制限 8 個、静的最小制限 8 個 = 合計 16 個)。

SD-WAN GUI で動的仮想パスを有効にする方法

動的仮想パスを有効にする手順は、次のとおりです。

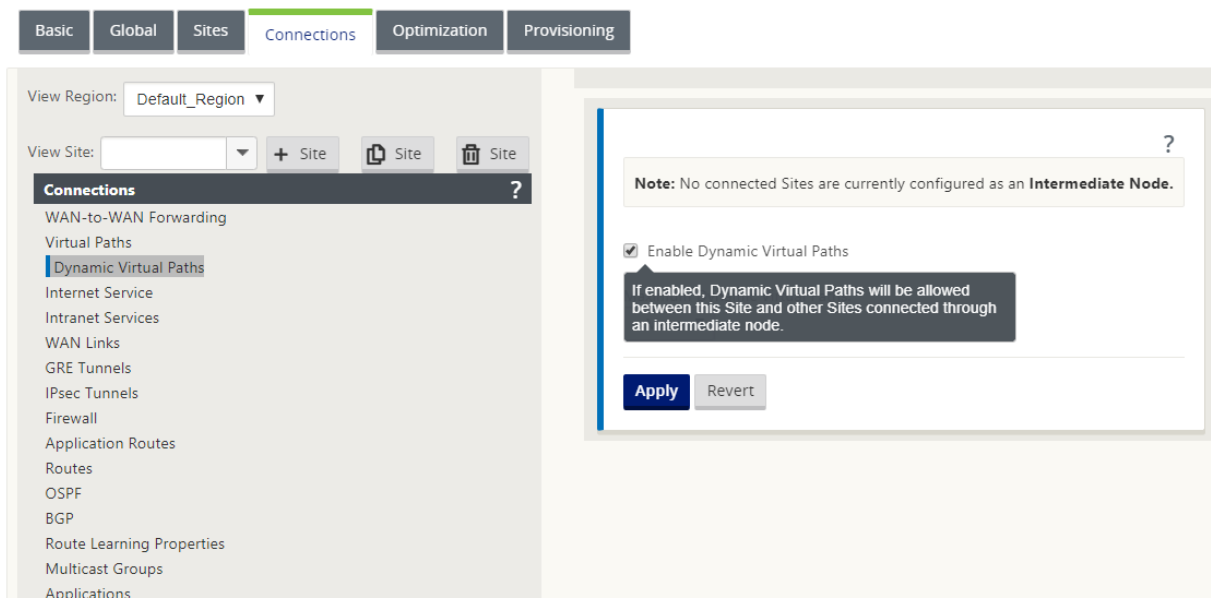
1. Citrix SD-WAN GUI の [接続] ペインで、WAN から WAN への転送グループを作成します。
2. [接続] > [クライアントサイト名] > [WAN から WAN への転送] に移動します。
3. **WAN** から **WAN** への転送を有効にして、サイトがマルチホップサイト間プロキシとして機能できるようにします。
4. サイトを中間ノードとして有効にする
5. [接続] > [リモートサイト] > [WAN から WAN への転送] に移動します。
6. サイトがマルチホップサイト間プロキシとして機能できるようにするには、WAN から WAN への転送を有効にします。



7. [接続]>[リモートサイト]>[仮想パス]>[動的仮想パス]に移動します。

8. 動的仮想パスを有効にします。

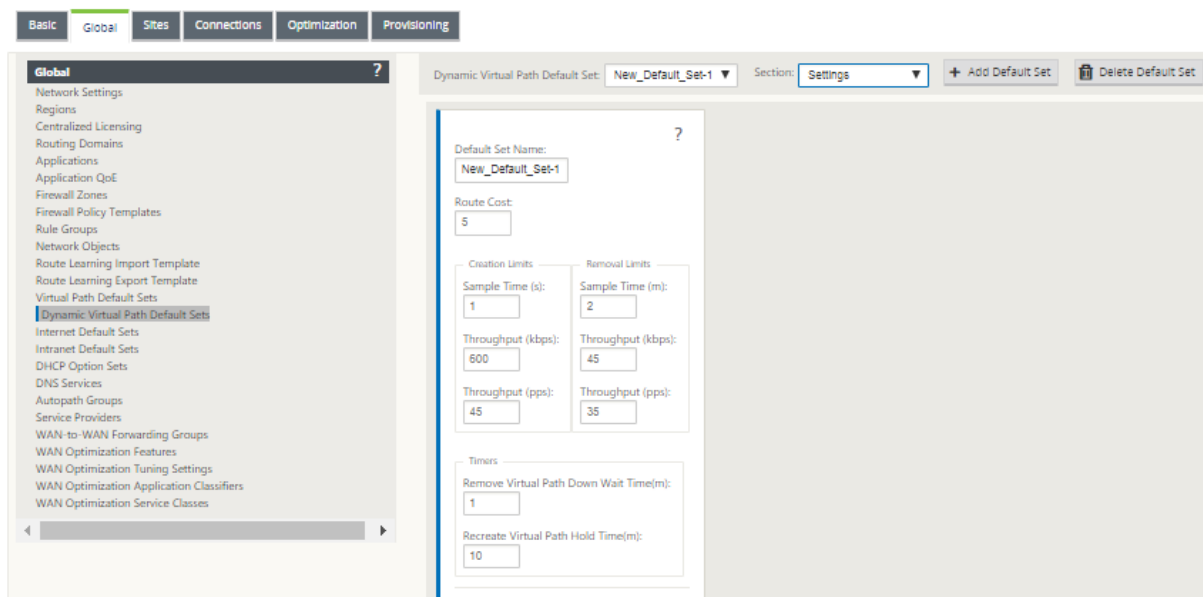
9. ダイナミックパスの最大数を設定します。



動的仮想パスの作成方法

- 構成では、動的仮想パスがアクティブかダウンするかを決定します。

- 時間枠内のサンプルパケットカウント（pps）または帯域幅（kbps）を設定します。
- グローバルに設定することも、中間ノードで WAN リンクを設定することもできます。



監視とトラブルシューティング

May 10, 2021

Citrix SD-WAN アプライアンスの Web 管理インターフェイスを使用して、サポートされている機能を監視およびトラブルシューティングできます。以下は、Citrix SD-WAN アプライアンスに適用される監視およびトラブルシューティングのトピックへのリンクです。

[仮想 WAN の監視](#)

[統計情報の表示](#)

[フロー情報の表示](#)

[レポートの表示](#)

[ファイアウォールの統計情報の表示](#)

[診断ツール](#)

[パス・マッピングと帯域幅の向上](#)

[管理 IP のトラブルシューティング](#)

[アクティブ帯域幅テスト](#)

[適応型帯域幅検出](#)

仮想 WAN の監視

May 10, 2021

アプライアンスの基本情報の表示

ブラウザを使用して、監視するアプライアンスの管理 Web インターフェイスに接続し、[ダッシュボード] タブをクリックして、そのアプライアンスの基本情報を表示します。

[ダッシュボード] ページには、ローカルアプライアンスの次の基本情報が表示されます。

システムステータス:

- 名前—アプライアンスをシステムに追加したときに割り当てた名前です。
- モデル—これは仮想 WAN アプライアンスのモデル番号です。
- **Appliance Mode** : このアプライアンスがプライマリ MCN またはセカンダリ MCN として構成されているか、またはクライアントアプライアンスとして構成されているかを示します。
- 管理 IP アドレス—アプライアンスの管理 IP アドレスです。
- **Appliance Uptime** —前回の再起動以降、アプライアンスが稼働していた期間を指定します。
- **[Service Uptime]** : 前回の再起動以降、仮想 WAN サービスが実行されている期間を指定します。

仮想パスサービスのステータス:

仮想パス [サイト名]—このアプライアンスに関連付けられているすべての仮想パスのステータスが表示されます。仮想 WAN サービスが有効になっている場合は、このセクションがページに含まれます。Virtual WAN サービスが無効な場合、このセクションの代わりに、アラートアイコン（ゴールデンロッドのデルタ）とアラートメッセージが表示されます。

ローカルバージョン情報:

- ソフトウェアのバージョン—これは、アプライアンス上で現在アクティブになっている CloudBridge Virtual Path ソフトウェアパッケージのバージョンです。
- **Build on** —ローカルアプライアンス上で現在実行されている製品バージョンのビルド日です。
- ハードウェアバージョン—これは、アプライアンスのハードウェアモデル番号とバージョンです。
- **OS** パーティションのバージョン—アプライアンス上で現在アクティブな OS パーティションのバージョンです。

下の図は、サンプルのダッシュボードページを示しています。

Dashboard	Monitoring	Configuration
System Status		
Name: MCN_23		
Model: VPX		
Sub-Model: BASE		
Appliance Mode: MCN		
Serial Number: 67e0772c-5190-a2ee-d183-9244189b30a0		
Management IP Address: 10.102.78.154		
Appliance Uptime: 6 days, 13 hours, 22 minutes, 23.0 seconds		
Service Uptime: 6 days, 13 hours, 14 minutes, 46.0 seconds		
Routing Domain Enabled: Default_RoutingDomain		
Local Versions		
Software Version: 10.1.0.111.690027		
Built On: Jun 21 2018 at 23:42:30		
Hardware Version: VPX		
OS Partition Version: 4.6		
Virtual Path Service Status		
Virtual Path MCN_23-Site1: Uptime: 6 days, 13 hours, 11 minutes, 45.0 seconds.		

統計情報の表示

May 10, 2021

ここでは、仮想 WAN 統計情報を表示する基本的な手順について説明します。

1. MCN の管理 Web インターフェイスにログインします。
2. [モニタリング] タブを選択します。

これにより、左側のペインに [**Monitoring**] ナビゲーションツリーが開きます。デフォルトでは、[表示] フィールドで [パス] があらかじめ選択された [統計] ページも表示されます。これには、パスの統計情報の詳細なテーブルが含まれます。

注

別の [**Monitoring**] ページ ([**Flows**] など) に移動した場合は、[**Monitoring**] ナビゲーション・ツリー (左側のペイン) で [**Statistics**] を選択することで、このページに戻ることができます。

Dashboard

Monitoring

Configuration

Statistics

Flows

Routing Protocols

Firewall

IKE/Ipsec

IGMP

Performance Reports

Qos Reports

Usage Reports

Availability Reports

Appliance Reports

DHCP Server/Relay

VRRP Protocol

Monitoring > Statistics

Statistics

Show: Paths (Summary) ☐ Enable Auto Refresh 5 seconds Refresh ☒ Show latest data.

Path Statistics Summary

Filter: in Any column Apply Show 100 entries

Num	From Link	To Link	Path State	Virtual Path Service State	Virtual Path Service Type	BOWT	Jitter (mS)	Loss %	kbps	Congestion
1	MCN-DC-WL-1	Branch1-WL-1	GOOD	GOOD	Static	2	3	0.00	59.95	NO
2	MCN-DC-WL-1	Branch1-WL-2	GOOD	GOOD	Static	2	3	0.00	8.72	NO
3	MCN-DC-WL-2	Branch1-WL-1	GOOD	GOOD	Static	2	3	0.00	8.72	NO
4	MCN-DC-WL-2	Branch1-WL-2	GOOD	GOOD	Static	2	3	0.00	11.82	NO
5	Branch1-WL-1	MCN-DC-WL-1	GOOD	GOOD	Static	2	3	0.00	8.89	NO
6	Branch1-WL-1	MCN-DC-WL-2	GOOD	GOOD	Static	2	3	0.00	25.19	NO
7	Branch1-WL-2	MCN-DC-WL-1	GOOD	GOOD	Static	2	3	0.00	11.84	NO
8	Branch1-WL-2	MCN-DC-WL-2	GOOD	GOOD	Static	2	3	0.00	8.73	NO

Showing 1 to 8 of 8 entries
Bandwidth calculated over the last 41278.42 seconds

FirstPrevious1NextLast

11.1.0 リリースでは、近隣探索の問題をデバッグするために、近隣探索プロトコル（NDP）オプションが追加されました。

1. [Show] ドロップダウンメニューから [NDP] オプションを選択すると、NDP の状態を IPv6 アドレスとともに表示できます。

Statistics

Show: NDP ☐ Enable Auto Refresh 5 seconds Refresh

NDP Statistics

Filter: in Any column

Show 100 entries Showing 1 to 2 of 2 entries

Num	Interface	VLAN	IP Addr	MAC Addr	Type	State	Is Router	Clear NDP Entry
0	2	0	2607:f0d0:2001:a::20	02:63:d7:64:85:4e	PERSISTENT	NDP_STATE_REACHABLE	Y	
1	2	0	fe80::63:d7ff:fe64:854e	02:63:d7:64:85:4e	END_USER	NDP_STATE_STALE	N	<input type="button" value="Clear"/>

Showing 1 to 2 of 2 entries

FirstPrevious1NextLast

FirstPrevious1NextLast

2. ドロップダウンメニューから [WAN リンク] を選択します。[IP Address] タブで設定した場合は、IPv6 アドレスも表示できます。

Statistics

Show: WAN Link

☐ Enable Auto Refresh

 5 seconds

Refresh

☒ Show latest data.

WAN Link Statistics

Filter: in Any column

Apply

Show 100 entries Showing 1 to 6 of 6 entries

First

Previous

1

Next

Last

WAN Link	Access Interface	IP Address	Proxy Address	Proxy ARP State	MAC	Last ARP Reply Age (ms)
demo_cl1_inet	N/A	2607:f0d0:2001:b::10	N/A	N/A	N/A	N/A
demo_cl1_inet2	N/A	172.16.100.1	N/A	N/A	N/A	N/A
demo_cl2_inet	N/A	2607:f0d0:2001:c::10	N/A	N/A	N/A	N/A
demo_cl2_inet2	N/A	172.16.150.1	N/A	N/A	N/A	N/A
demo_mcn_inet	demo_mcn_inet-AI-1	2607:f0d0:2001:a::10	N/A	N/A	N/A	N/A
demo_mcn_inet2	demo_mcn_inet2-AI-1	172.16.200.1	N/A	DISABLED	N/A	N/A

Showing 1 to 6 of 6 entries

First

Previous

1

Next

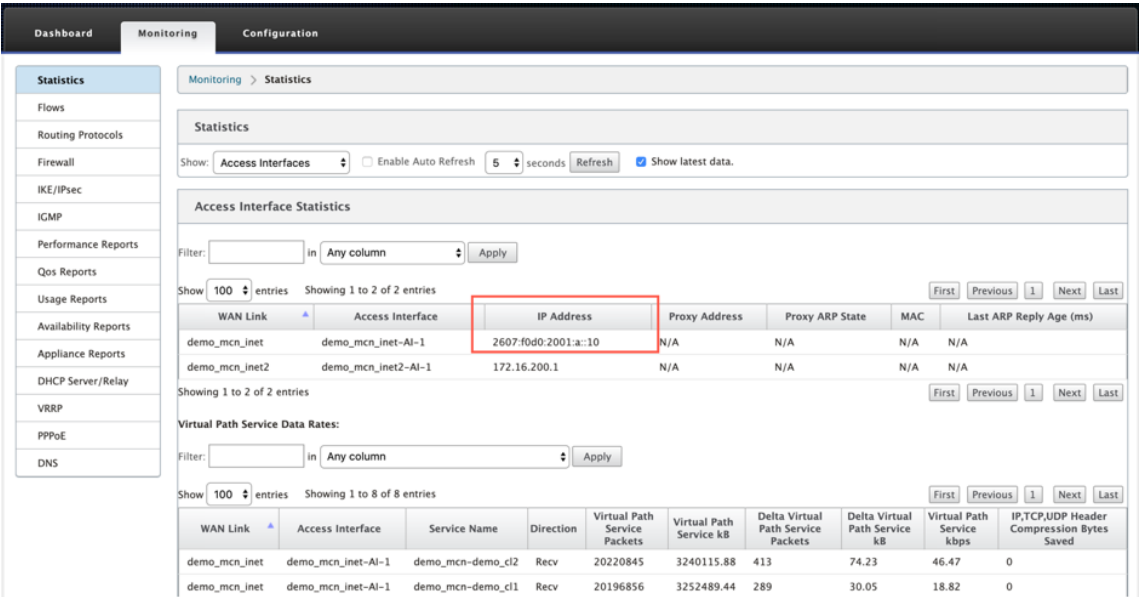
Last

Virtual Path Service Data Rates

Filter: in Any column

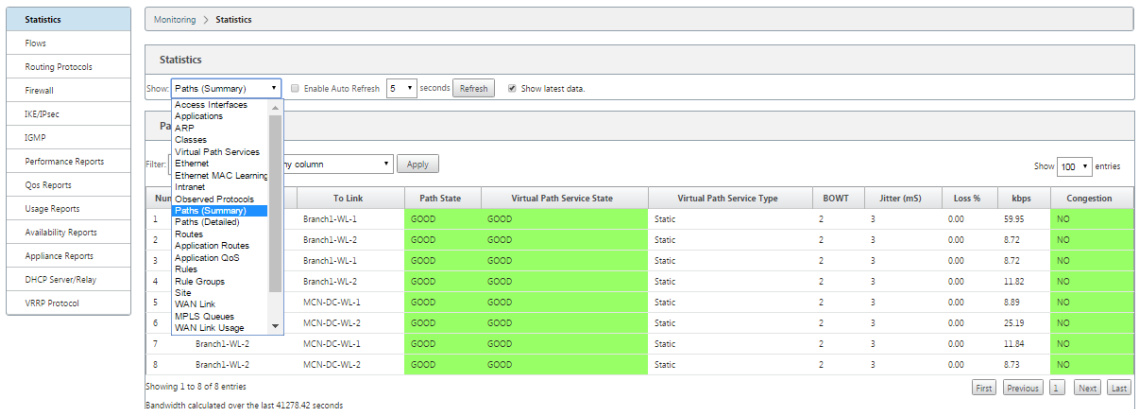
Apply

3. アクセスインターフェースの統計情報も表示できます。



4. [表示] ドロップダウンメニューを開きます。

[表示] メニューには、パス、NDP、アクセスインターフェイス、および WAN リンクの統計情報に加えて、統計情報のフィルタリングおよび表示のためのオプションがいくつか用意されています。



「表示」メニューからフィルタを選択して、そのトピックの統計情報の表を表示します。

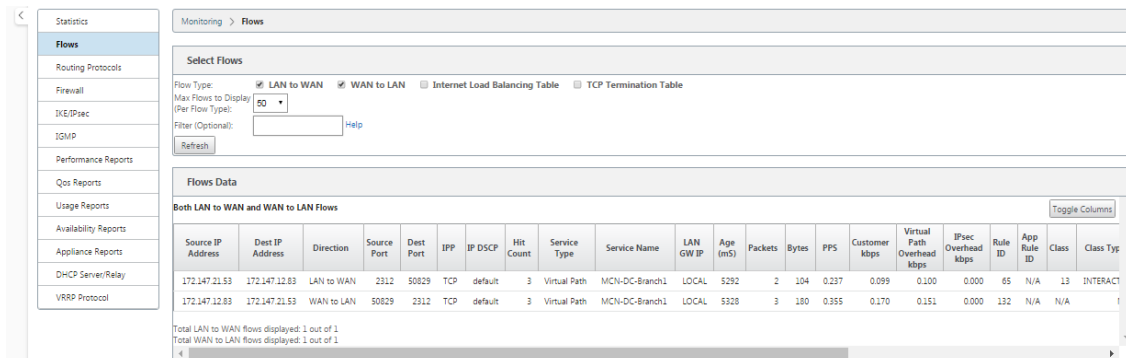
フロー情報の表示

February 8, 2022

ここでは、仮想 WAN フロー情報を表示する基本的な手順について説明します。

フロー情報を表示するには、次の手順を実行します。

1. MCN の管理 Web インターフェイスにログインし、[モニタリング] タブを選択します。左側のペインに [**Monitoring**] ナビゲーションツリーが開きます。
2. ナビゲーションツリーで [フロー] ブランチを選択します。[**Flow Type**] フィールドで事前選択された ****LAN** から **WAN** への [フロー ** (Flows)] ページが表示されます。



3. フロータイプを選択します。[フロータイプ] フィールドは、[フロー] ページの上部にある [**** フローの選択**]** セクションにあります。[**Flow Type**] フィールドの横には、表示するフロー情報を選択するためのチェックボックスオプションの行があります。1 つまたは複数のチェックボックスをオンにして、表示する情報をフィルタできます。
4. そのフィールドの横にあるドロップダウンメニューから [表示する最大フロー数] を選択します。
5. これは、[フロー (Flows)] テーブルに表示するエントリの数を決めます。オプションは、**50**、**100**、**1000** です。
6. (オプション) [フィルタ (Filter)] フィールドに検索テキストを入力します。検索テキストを含むエントリのみがテーブルに表示されるように、テーブルの結果をフィルタリングします。

ヒント

フィルタを使用してフローテーブルの結果を調整する詳細な手順を表示するには、[フィルタ] フィールドの右側にある [**** ヘルプ**] をクリックします。 **** ヘルプ** 表示を閉じるには、[フローの選択] セクションの左下隅にある [更新] をクリックします。

7. [**Refresh**] をクリックして、フィルタ結果を表示します。この図は、すべてのフロータイプが選択された [フロー] ページのフィルタ表示の例を示しています。

Select Flows

Flow Type:

☒ LAN to WAN☒ WAN to LAN☒ Internet Load Balancing Table☒ TCP Termination Table

Max Flows to Display (Per Flow Type):

50

Filter (Optional):

172.79.2.83

Help

Refresh

Flows Data

Toggle Columns

Both LAN to WAN and WAN to LAN Flows

Source IP Address	Dest IP Address	Direction	Source Port	Dest Port	IPP	IP DSCP	Hit Count	Service Type	Service Name	LAN GW IP	Age (mS)	Packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps
172.79.2.83	172.79.1.42	LAN to WAN	9281	58689	TCP	default	9577	Virtual Path	DC-BR	LOCAL	5332	12038	1020734	0.079	0.033	0.031
172.79.2.83	172.79.1.42	LAN to WAN	9281	58690	TCP	default	9631	Virtual Path	DC-BR	LOCAL	5346	12199	1075706	0.079	0.033	0.031
172.79.1.42	172.79.2.83	WAN to LAN	58689	9281	TCP	default	18025	Virtual Path	DC-BR	LOCAL	5346	18025	1294598	0.157	0.052	0.062
172.79.1.42	172.79.2.83	WAN to LAN	58690	9281	TCP	default	18244	Virtual Path	DC-BR	LOCAL	5360	18244	1389118	0.157	0.052	0.062

Total LAN to WAN flows displayed: 2 out of 305

Total WAN to LAN flows displayed: 2 out of 305

Internet Load Balancing Flows

LAN IP	WAN IP	Age (mS)	WAN Link	Flow Count
--------	--------	----------	----------	------------

Note: Only the active flows will be displayed and the total number of flows include active and inactive flows.

TCP Terminated Flows

Source IP Address	Dest IP Address	Source Port	Dest Port	IPP	Age (mS)	From Wan kbps	To Wan kbps	Bytes Pending To LAN	Bytes Pending To WAN	State
-------------------	-----------------	-------------	-----------	-----	----------	---------------	-------------	----------------------	----------------------	-------

Total TCP Terminated flows displayed: 0 out of 305

8. (オプション) テーブルに含める列を選択します。以下を実行します：

9. [フローデータ] テーブルの右上隅にある [列の切り替え] をクリックします。選択されていない列が表示され、各列の上にあるチェックボックスが開き、その列を選択または選択解除できます。選択解除された列は、図に示すように、グレー表示されます。

注

デフォルトでは、すべての列が選択されています。これにより、テーブルが切り捨てられ、[列の切り替え] ボタンが表示されなくなる場合があります。その場合は、テーブルの下に水平スクロールバーが表示されます。スクロールバーを右にスライドすると、テーブルの切り詰められたセクションが表示され、[列の切り替え] ボタンが表示されます。スクロールバーが利用できない場合は、スクロールバーが表示されるまでブラウザウィンドウの幅を変更してみてください。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

911

Monitoring > Flows

Balancing Table TCP Termination Table

Apply

<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Hit Count	Service Type	Service Name	LAN GW IP	Age (mS)	Packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type
9598	Virtual Path	DC-BR	LOCAL	2435	12065	1023038	0.033	0.023	0.013	0.000	12	9	REALTIME	DC-WL-2->BR-WL-1	N/A	Duplicate, Reliable
9652	Virtual Path	DC-BR	LOCAL	2434	12226	1078010	0.033	0.023	0.013	0.000	12	9	REALTIME	DC-WL-2->BR-WL-1	N/A	Duplicate, Reliable
18064	Virtual Path	DC-BR	LOCAL	2448	18064	1287454	0.048	0.028	0.019	0.000	89	N/A	N/A	N/A	N/A	Duplicate, Reliable
18283	Virtual Path	DC-BR	LOCAL	2447	18283	1391974	0.048	0.028	0.019	0.000	89	N/A	N/A	N/A	N/A	Duplicate, Reliable

10. チェックボックスをクリックして、列を選択または選択解除します。

- 送信元 **IP** アドレス: このフロー上のパケットの送信元 IP アドレス。
- Dest IP Address**: このフロー上のパケットの宛先 IP アドレス。
- 方向-このフロー上のパケットの方向 (LAN から WAN または WAN から LAN)。
- [Source Port]**: このフロー上のパケットの送信元ポート。
- Dest Port**: このフロー上のパケットの宛先ポート。
- IPP**-このフロー上のパケットの IP プロトコル番号。
- IP DSCP**-このフロー上のパケットの IP DSCP タグ設定。
- Hit Count**-このフローが検索され、見つかった回数。
- [サービスの種類]**-このフローの種類が [仮想パス]、[インターネット]、[イントラネットトラフィック] のいずれであるかを示します。
- [Service Name]**: 仮想パストラフィックが使用している仮想パスの名前。
- LAN GW IP**: LAN ゲートウェイの IP アドレス (指定されている場合)。
- Age (ms)**-このフローでパケットが分類されてからの経過時間 (ミリ秒)。
- Packets**: フローの存続期間中に送信されたパケット数。
- Bytes**: フローの存続期間中に送信されたバイト数。
- PPS**-前回の更新以降の 1 秒あたりのパケット数。
- 顧客 **kbps**/ 仮想パスオーバーヘッド **kbps** / **IPsec** オーバーヘッド **kbps**-最後の更新以降の 1 秒あたりのキロビット数。
- Rule ID**: このフローのトラフィックが一致したルールの ID。
- App Rule ID**-このフローのトラフィックが一致したルールのアプリの ID。
- Class**: トラフィックが使用している仮想パスクラスの ID。
- [Class Type]**: トラフィックが使用している仮想パスクラスのタイプ (リアルタイム、インタラクティブ)

ブ、バルク)。

- **Path** -トラフィックが使用しているパス。
- **HDR** 圧縮保存バイト数 -ヘッダー圧縮によって保存されたバイト数です。
- **Transmission Type**： トラフィックが使用している伝送タイプ。
- **Application** -使用中のアプリケーションの名前。

11. [適用] (テーブルの右上隅の上) をクリックします。選択オプションが解除され、選択した列のみが含まれるようにテーブルが更新されます。

Select Flows

Flow Type: ☒ LAN to WAN ☒ WAN to LAN ☐ Internet Load Balancing Table ☐ TCP Termination Table

Max Flows to Display (Per Flow Type): 50

Filter (Optional): 172.79.2.83 [Help](#)

Refresh

Flows Data

Toggle Columns

Both LAN to WAN and WAN to LAN Flows

Source IP Address	Dest IP Address	Direction	Source Port	Dest Port	Hit Count	Service Type	Service Name	LAN GW IP	Age (mS)	Packets	Bytes
172.79.2.83	172.79.1.42	LAN to WAN	9281	58689	9613	Virtual Path	DC-BR	LOCAL	12022	12084	1024626
172.79.2.83	172.79.1.42	LAN to WAN	9281	58690	9667	Virtual Path	DC-BR	LOCAL	12040	12246	1080066
172.79.1.42	172.79.2.83	WAN to LAN	58689	9281	18092	Virtual Path	DC-BR	LOCAL	12040	18092	1299440
172.79.1.42	172.79.2.83	WAN to LAN	58690	9281	18312	Virtual Path	DC-BR	LOCAL	12056	18312	1394758

Total LAN to WAN flows displayed: 2 out of 306
Total WAN to LAN flows displayed: 2 out of 306

SD-WAN Center の DPI アプリケーション

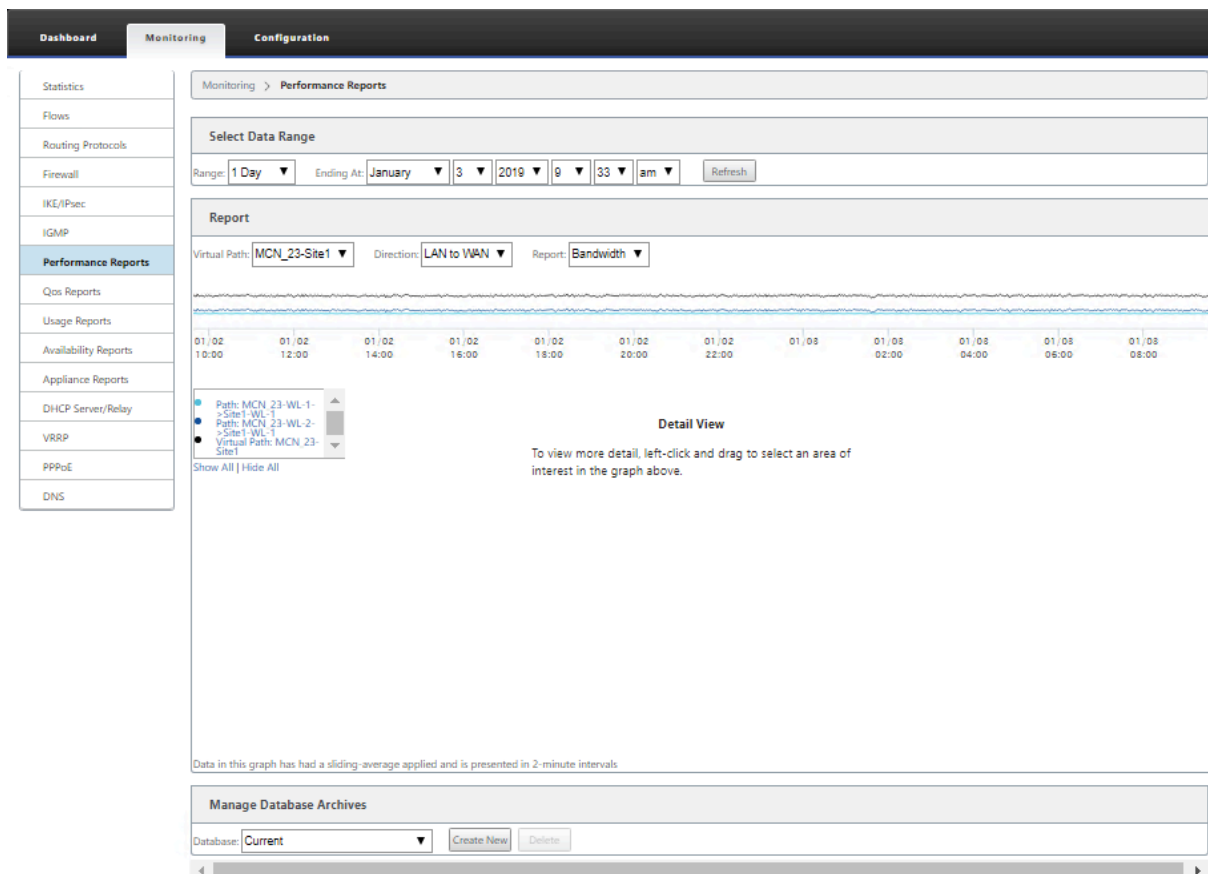
以前のリリースでは、約 4,000 のアプリケーションを識別し、800 のサービス (550 の仮想パス、256 のイントラネットサービス) で構成しました。このデータを格納すると、システム全体のパフォーマンス (データの格納に必要な CPU サイクルとディスク容量) に影響します。また、使用量またはパスごとのデータに関するレポートがサポートされる場合にも影響があります。

データ・パスは 1 分で収集されたすべてのアプリケーションに関する情報を提供しますが、1 分単位の統計レポートによって上位 100 個のアプリケーションが決定され、他のすべてのアプリケーションの集計が「その他」とレポートされます。ネットワーク内に追跡可能なアプリケーションの多様性が高い場合、データの明瞭さに影響を与える可能性があります。特に、アプリケーションの使用状況を追跡/グラフ化したい場合に、アプリケーションが上位 100 の制限から外れることがあります。

レポートの表示

May 10, 2021

このセクションでは、管理 Web Interface を使用してローカルアプライアンスに関する仮想 WAN レポートを生成および表示する基本的な手順について説明します。アプライアンスは、最大 30 個のアーカイブを保持し、30 個のエントリを超える最も古いアーカイブをパージできます。



注

管理 Web インターフェイスで生成されたレポートは、ローカルアプライアンスにのみ適用されます。仮想 WAN のレポートを生成および表示するには、仮想 WAN センター Web インターフェイスを使用します。

仮想 WAN レポートを生成および表示するには、次の手順を実行します。

1. MCN の管理 Web インターフェイスにログインし、[モニタリング] タブを選択します。

これにより、左側のペインに [**Monitoring**] ナビゲーションツリーが開きます。

2. ナビゲーション・ツリーからレポート・タイプを選択します。

レポートタイプは、ナビゲーションツリーの [**Flow s**] ブランチのすぐ下にブランチとして表示されます。



使用可能なレポートタイプは次のとおりです。

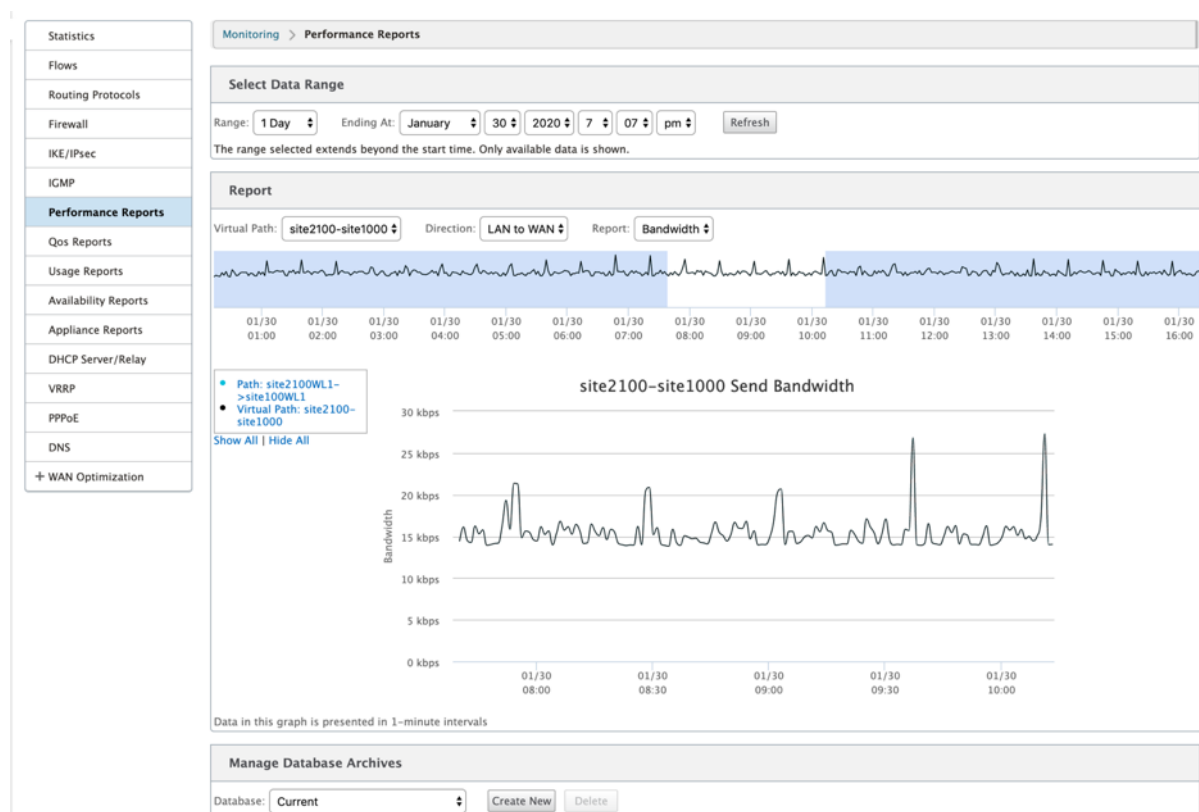
- パフォーマンスレポート
- **QoS** レポート
- 使用状況レポート
- 可用性レポート
- アプライアンス・レポート

3. レポートオプションを選択します。

さまざまなタイプのレポートに加えて、各レポートタイプには、レポート結果を絞り込むための多数のオプションとフィルタがあります。

パフォーマンス・レポート

Citrix SD-WAN では、サイト、仮想パス、または方向（LAN から WAN および WAN から LAN）レベルでパフォーマンス統計を表示できます。Citrix SD-WAN を使用すると、各リンクの効率をミリ秒単位で示すメトリックを収集できます。詳細を表示するには、左クリックしてグラフィック内のパスまたは時間枠の特定の領域を選択します。

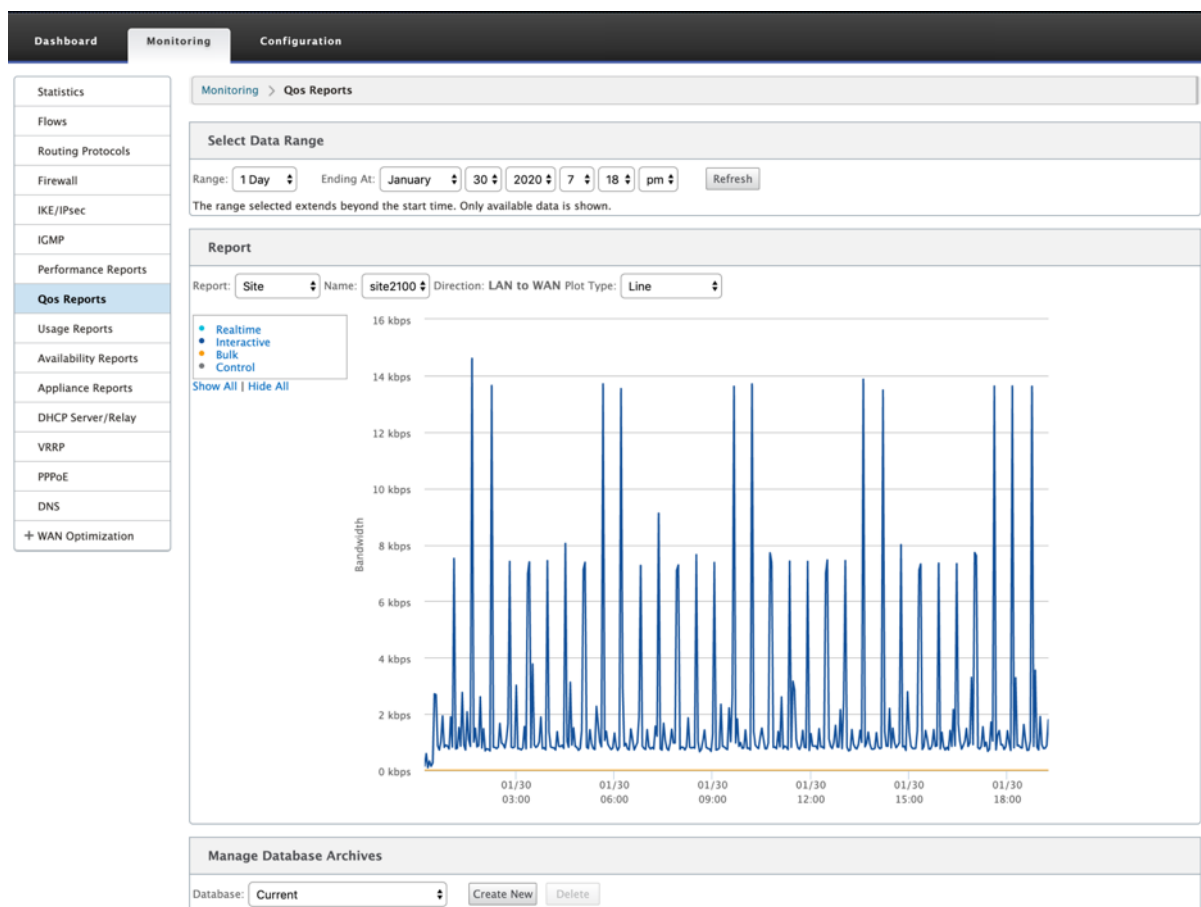


必要に応じてデータ範囲を選択し、次のフィールドを使用してパフォーマンス・レポートを表示できます。

- 仮想パス: ドロップダウンリストから仮想パスを選択します。
- 方向: 必要に応じて [方向] を選択します ([LAN から WAN へ] または [WAN から LAN へ])。
- レポート: レポートを表示するには、次のネットワークパラメータを選択します。
 - 帯域幅
 - 遅延
 - ジッター
 - 損失
 - 品質

QoS レポート

アプリケーション QoS レポートは、各サイト、WAN リンク、仮想パス、パスレベルでアップロード、ダウンロード、ドロップされたパケット数またはバイト数などの監視できます。

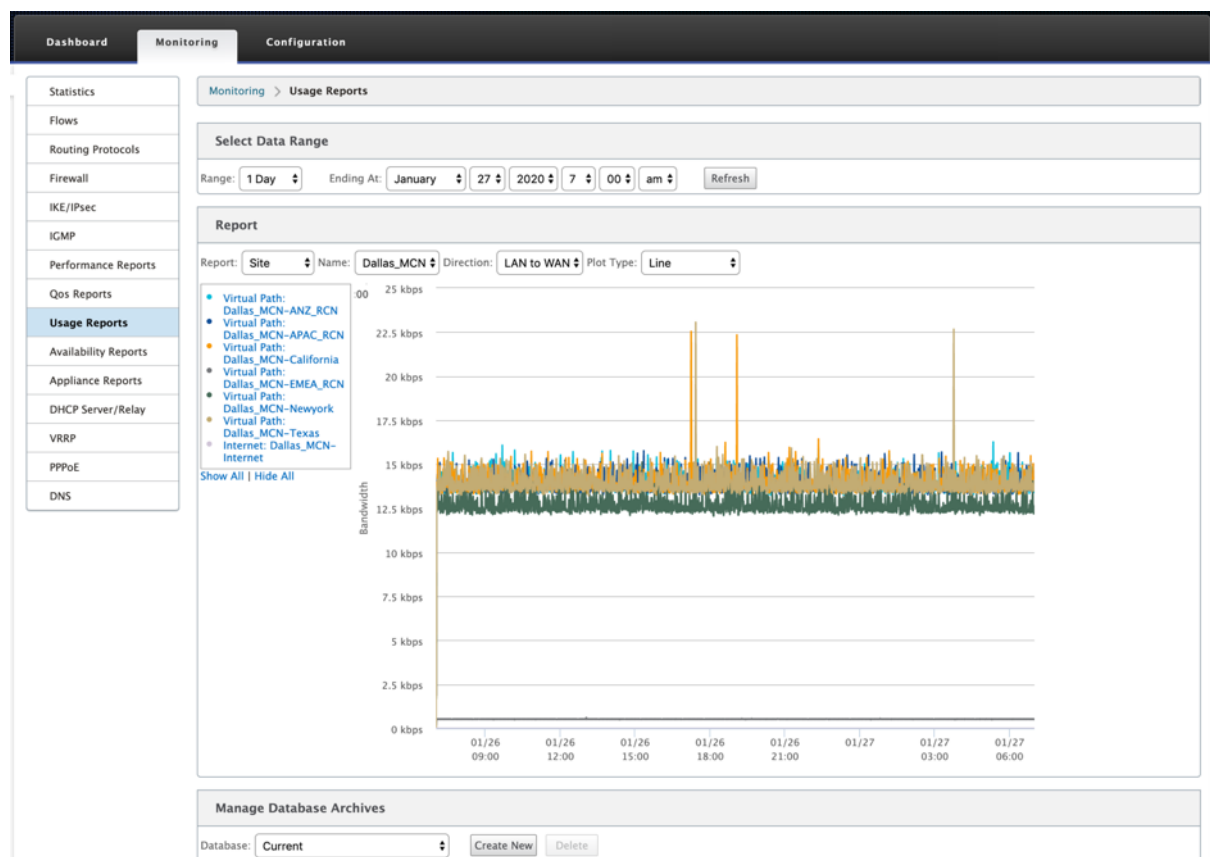


次のメトリックを表示できます。

- リアルタイム: Citrix SD-WAN 構成でリアルタイムクラスの種類に属するアプリケーションによって消費される帯域幅。このようなアプリケーションのパフォーマンスは、ネットワーク遅延に大きく依存します。遅延したパケットは、失われたパケットよりも劣ります（たとえば、VoIP、Skype for Business）。
- インタラクティブ: Citrix SD-WAN 構成の対話型クラスの種類に属するアプリケーションによって消費される帯域幅。このようなアプリケーションのパフォーマンスは、ネットワーク遅延とパケット損失に大きく依存します（たとえば、XenDesktop、XenApp）。
- Bulk:** Citrix SD-WAN 構成でバルククラスタイプに属するアプリケーションによって消費される帯域幅。これらのアプリケーションは、人的介入がほとんどなく、ほとんどがシステム自体（FTP、バックアップ操作など）によって処理されます。
- コントロール: ルーティング、スケジューリング、およびリンクの統計情報を含む制御パケットの転送に使用される帯域幅。

使用状況レポート

使用状況レポートは、仮想バスの使用状況情報を提供します。



- レポート: ドロップダウンリストから [サイト] または [**WAN** リンク] を選択して、レポートを表示します。
- [名前]: ドロップダウンリストからサイトまたは WAN リンクの名前を選択します。
- 方向: 必要に応じて方向を選択します (LAN から WAN または WAN から LAN)。
- [プロットタイプ]: ドロップダウンリストから [プロットタイプ] を選択します ([線分] または [面積])。

可用性レポート

このレポートでは、WAN リンク、パス、仮想パスの可用性データを表示できます。また、1 時間、24 時間、7 日などの特定の時間枠に切り替えたり、選択して、利用可能なデータを表示することもできます。パスと仮想パスのデータは、**DD: HH: MM: SS** 形式で表されます。

Dashboard

Monitoring

Configuration

Statistics

Flows

Routing Protocols

Firewall

IKE/IPsec

ICMP

Performance Reports

Qos Reports

Usage Reports

Availability Reports

Appliance Reports

DHCP Server/Relay

VRRP

PPPoE

DNS

Monitoring > Availability Reports

Select Timeframe

For the period from 7:01 on 1/26/2020 to 7:01 on 1/27/2020 | Switch to: 1 hour | 24 hours | 7 days | All Available Data

All times are represented in days (if available), hours (if available), minutes and seconds. DD:HH:MM:SS

Paths and Virtual Paths

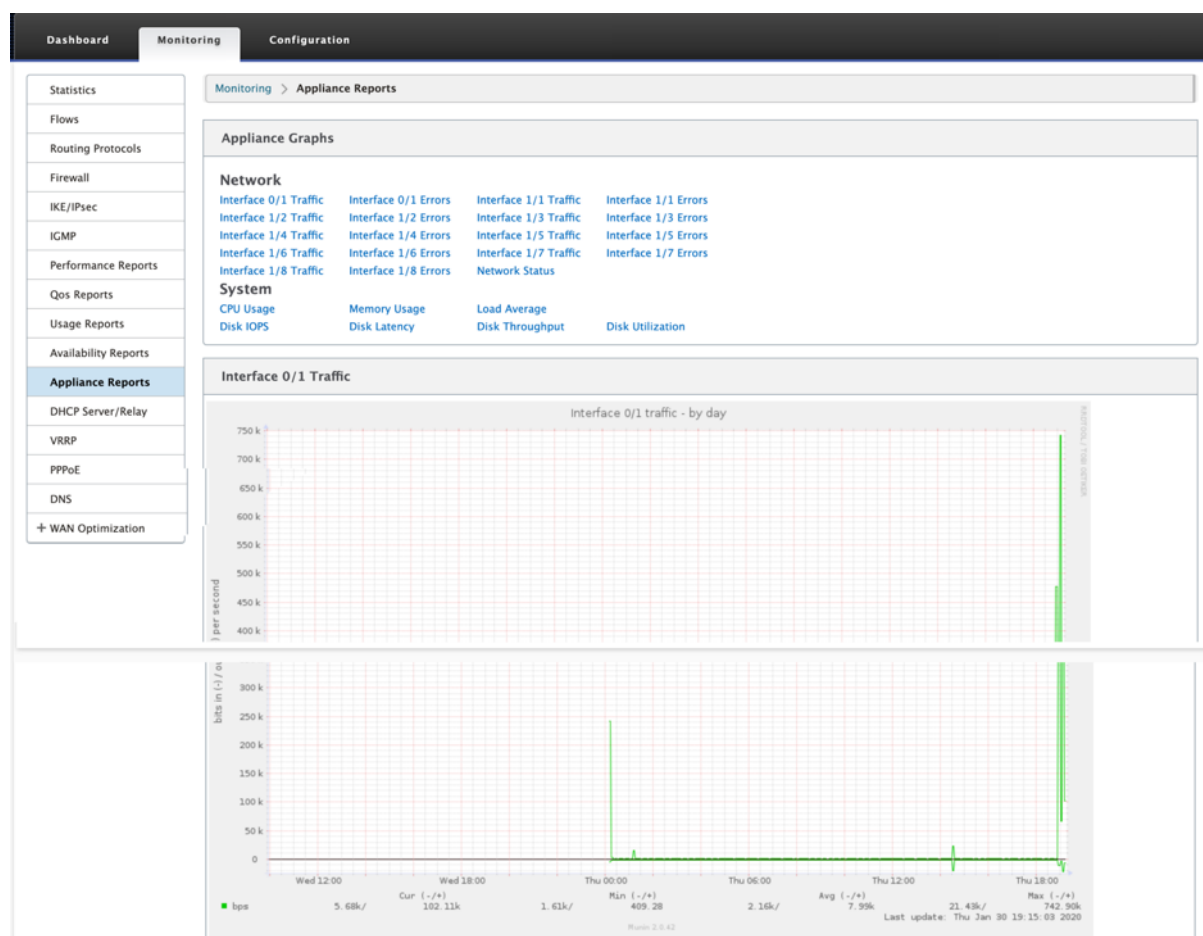
	Uptime	Goodtime	Badtime				Downtime			Incidents			
			Total	Loss	Silence	Peer	Total	Silence	Peer	Total	Loss	Silence	Peer
Virtual Path Dallas_MCN-ANZ_RCN	1:00:00:00	1:00:00:00	0:00	0:00	5								
Dallas_MCN-queue1->ANZ_RCN-queue1	1:00:00:00	1:00:00:00	0:00	---	0:00	0:00	0:00	0:00	0:00	0	---	0	0
ANZ_RCN-queue1->Dallas_MCN-queue1	1:00:00:00	23:59:10	0:50	0:00	0:50	---	0:00	0:00	---	5	0	5	---
Virtual Path Dallas_MCN-APAC_RCN	1:00:00:00	1:00:00:00	0:00	0:00	14								
Dallas_MCN-queue1->APAC_RCN-queue1	1:00:00:00	1:00:00:00	0:00	---	0:00	0:00	0:00	0:00	0:00	0	---	0	0
APAC_RCN-queue1->Dallas_MCN-queue1	1:00:00:00	23:57:40	2:20	0:00	2:20	---	0:00	0:00	---	14	0	14	---
Virtual Path Dallas_MCN-California	1:00:00:00	23:59:42	0:18	0:00	2								
Dallas_MCN-queue1->California-queue1	23:58:36	23:58:36	0:00	---	0:00	0:00	0:00	0:00	0:00	2	---	0	2
California-queue1->Dallas_MCN-queue1	1:00:00:00	23:59:40	0:20	0:00	0:20	---	0:00	0:00	---	2	0	2	---
Virtual Path Dallas_MCN-EMEA_RCN	0:00	0:00	0:00	1:00:00:00	0								
Dallas_MCN-queue1->EMEA_RCN-queue2	0:00	0:00	0:00	---	0:00	0:00	1:00:03:45	1:00:03:45	0:00	0	---	0	0
EMEA_RCN-queue2->Dallas_MCN-queue1	0:00	0:00	0:00	0:00	0:00	---	1:00:03:45	1:00:03:45	---	0	0	0	---
Virtual Path Dallas_MCN-Newyork	1:00:00:00	1:00:00:00	0:00	0:00	8								
Dallas_MCN-WL-2->Newyork-WL-2	0:00	0:00	0:00	---	0:00	0:00	0:00	0:00	0:00	0	---	0	0
Dallas_MCN-queue1->Newyork-queue1	1:00:00:00	1:00:00:00	0:00	---	0:00	0:00	0:00	0:00	0:00	0	---	0	0
Newyork-WL-2->Dallas_MCN-WL-2	0:00	0:00	0:00	0:00	0:00	---	1:00:03:45	1:00:03:45	---	0	0	0	---
Newyork-queue1->Dallas_MCN-queue1	1:00:00:00	23:58:40	1:20	0:00	1:20	---	0:00	0:00	---	8	0	8	---
Virtual Path Dallas_MCN-Texas	1:00:00:00	23:59:42	0:18	0:00	12								
Dallas_MCN-queue1->Texas-queue1	23:58:35	23:58:35	0:00	---	0:00	0:00	0:00	0:00	0:00	2	---	0	2
Texas-queue1->Dallas_MCN-queue1	1:00:00:00	23:58:00	2:00	0:00	2:00	---	0:00	0:00	---	12	0	12	---

WAN Links

	Uptime	Downtime	Incidents
Dallas_MCN-WL-2	0:00	1:00:00:00	1
Dallas_MCN-queue1	1:00:00:00	0:00	No downtime

アプライアンス・レポート

アプライアンス・レポートは、ネットワーク・トラフィックとシステム使用状況レポートを提供します。各リンクをクリックして、アプライアンスのグラフを日、週、月、年単位で表示または監視します。



ファイアウォールの統計情報の表示

May 10, 2021

ファイアウォールポリシーと NAT ポリシーを設定したら、接続、ファイアウォールポリシー、および NAT ポリシーの統計情報をレポートとして表示できます。さまざまなフィルタリングパラメータを使用して、レポートをフィルタリングできます。

ファイアウォールおよび NAT ポリシーの設定については、[ステートフルファイアウォールと NAT のサポート](#)を参照してください。

接続

ファイアウォールポリシーのアプリケーションの統計情報を確認できます。これにより、選択したアプリケーションと一致するすべての接続、接続元、接続先、および生成しているトラフィックの量を確認できます。ファイアウォールポリシーが、各アプリケーションのトラフィックに対してどのように動作しているかを確認できます。

次のパラメータを使用して、接続統計をフィルタリングできます。

- アプリケーション-接続のフィルタ条件として使用されるアプリケーション。
- ファミリー-接続のフィルタ条件として使用されるアプリケーションファミリー。
- IP プロトコル-接続によって使用される IP プロトコル。
- ソースゾーン-接続の発信元のゾーン。
- 宛先ゾーン-応答トラフィックの発信元ゾーン。
- ソースサービスタイプ-接続の発信元のサービス。
- ソースサービスインスタンス-接続の発信元であるサービスのインスタンス。
- [Source IP]: 接続の発信元の IP アドレス。ドット付き 10 進表記で入力し、オプションのサブネットマスクを使用します。
- [Source Port]: 接続元のポートまたはポートの範囲。「-」文字を使用して、単一のポートまたはポートの範囲を受け入れます。
- 宛先サービスタイプ: 応答トラフィックの発信元となるサービス。
- 宛先サービスインスタンス-応答トラフィックの発信元となるサービスのインスタンス。
- Destination IP: 応答デバイスの IP アドレス。ドット付き 10 進表記で入力し、オプションのサブネットマスクを使用します。
- 宛先ポート: 応答するデバイスで使用されるポートまたはポートの範囲。「-」文字を使用して、単一のポートまたはポートの範囲を受け入れます。

フィルタポリシー

ポリシーを使用すると、トラフィックフローのアクションを指定できます。ファイアウォールフィルタのグループは、ファイアウォールポリシーテンプレートを使用して作成され、ネットワーク内のすべてのサイトに適用することも、特定のサイトにのみ適用することもできます。

すべてのフィルタポリシーの統計レポートを表示し、次のパラメータを使用してフィルタリングできます。

- アプリケーションオブジェクト-ファイアウォールポリシーのフィルタ条件として使用される Application オブジェクト。
- Application-ファイアウォールポリシーでフィルタ条件として使用されるアプリケーション
- Family-ファイアウォールポリシーでフィルタ条件として使用されるアプリケーションファミリー。
- [IP プロトコル]-フィルタポリシーが一致する IP プロトコル。
- DSCP: フィルタポリシーが一致する DSCP タグ。
- [フィルタポリシーアクション]-パケットがフィルタに一致したときにポリシーが実行するアクション。
- ソースサービスタイプ-接続の発信元のサービス。
- [ソースサービス名]-接続の発信元であるサービスのインスタンス。
- [Source IP]: 接続の発信元の IP アドレス。ドット付き 10 進表記で入力し、オプションのサブネットマスクを使用します。
- [Source Port]: 接続元のポートまたはポートの範囲。「-」文字を使用して、単一のポートまたはポートの範囲を受け入れます。

- 宛先サービスタイプ: 応答するトラフィックが宛先となるサービス。
- [宛先サービス名]: 該当する場合、応答トラフィックが宛先となるサービス。
- Destination IP: 応答デバイスの IP アドレス。ドット付き 10 進表記で入力し、オプションのサブネットマスクを使用します。
- 宛先ポート: 応答するデバイスで使用するポートまたはポートの範囲。「-」文字を使用して、単一のポートまたはポートの範囲を受け入れます。
- [Source Zone]: フィルタポリシーに一致する発信元ゾーン。
- 宛先ゾーン-フィルタポリシーに一致する応答ゾーン。

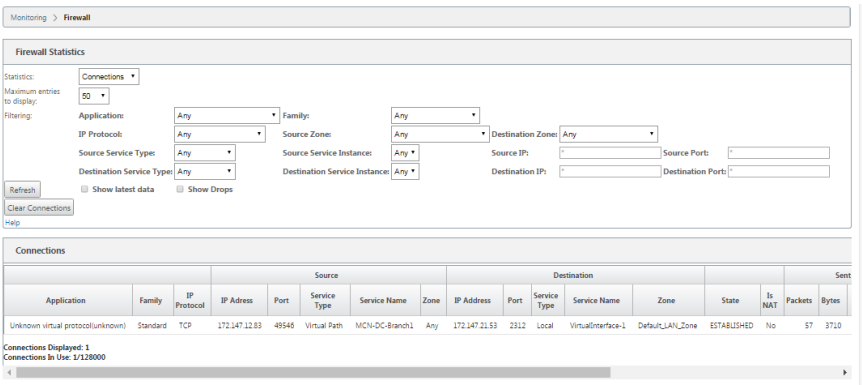
NAT ポリシー

すべてのネットワークアドレス変換 (NAT) ポリシーの統計情報を表示し、次のパラメータを使用してレポートをフィルタリングできます。

- IP プロトコル-NAT ポリシーが一致する IP プロトコル。
- NAT タイプ-NAT ポリシーで使用されている NAT のタイプ。
- ダイナミック NAT タイプ: NAT ポリシーで使用中のダイナミック NAT のタイプ。
- サービスタイプ-NAT ポリシーで使用するサービスタイプ。
- サービス名-NAT ポリシーで使用するサービスのインスタンス。
- Inside IP-内部 IP アドレス。ドット付き 10 進表記で入力し、オプションのサブネットマスクを使用します。
- 内部ポート: NAT ポリシーで使用する内部ポート範囲。「-」文字を使用して、単一のポートまたはポートの範囲を受け入れます。
- Outside IP-外部 IP アドレス。ドット付き 10 進表記で入力し、オプションのサブネットマスクを使用します。
- [Outside Port]: NAT ポリシーで使用する外部ポート範囲。「-」文字を使用して、単一のポートまたはポートの範囲を受け入れます。

ファイアウォールの統計情報を表示するには

1. [監視] > [ファイアウォール] に移動します。
2. [Statistics] フィールドで、必要に応じて [接続]、[フィルタポリシー]、または **[NAT ポリシー]** を選択します。
3. フィルタ条件を必要として設定します。



4. [更新] をクリックします。

診断

August 30, 2022

Citrix SD-WAN 診断ユーティリティには、接続の問題をテストおよび調査するための次のオプションが用意されています。

- Ping
- Traceroute
- パケットキャプチャ
- バス帯域幅
- システム情報
- 診断データ
- イベント
- alarms
- 診断ツール
- サイト診断

Citrix SD-WAN ダッシュボードの診断オプションは、データ収集を制御します。

Ping

Ping オプションを使用するには、[構成] > [診断] に移動し、[Ping] を選択します。Ping を使用して、ホストの到達可能性とネットワーク接続を確認できます。

ルーティングドメインを選択します。有効な IP アドレス、ping カウント数 (ping 要求を送信する回数)、およびパケットサイズ (データバイト数) を指定します。[**Ping** の停止] をクリックして、進行中の ping 検索を停止します。

特定のインターフェイスから ping を実行できます。ルーティングドメインを選択し、IP アドレスと ping カウント、パケットサイズを指定し、ドロップダウンリストから仮想インターフェイスを選択します。

Traceroute

Traceroute オプションを使用するには、[構成] > [システムメンテナンス] > [診断] を展開し、[**traceroute**] を選択します。

traceroute は、リモートサーバーへのパスまたはルートの検出と表示に役立ちます。**Traceroute** オプションをデバッグツールとして使用して、ネットワーク内の障害点を検出します。

ドロップダウンリストからパスを選択し、[トレース] をクリックします。[結果] セクションで詳細を表示できます。

Packet capture

[パケットキャプチャ (**Packet Capture**)] オプションを使用すると、選択したサイトに存在する選択したアクティブインターフェイスを通過するリアルタイムデータパケットを代行受信できます。パケットキャプチャは、ネットワークの問題の分析とトラブルシューティングに役立ちます。

Dashboard

Monitoring

Configuration

+

Appliance Settings

+

Virtual WAN

−

System Maintenance

- Delete Files
- Restart System
- Date/Time Settings
- Local Change Management
- Diagnostics**
- Update Software
- Configuration Reset
- Factory Reset

Configuration > System Maintenance > Diagnostics

Ping

Traceroute

Packet Capture

Path Bandwidth

System Info

Diagnostic Data

Events

Alarms

Diagnostics Tool

Site Diagnostics

Packet Capture

Interfaces:

X 1/1 X 1/2 X 1/4 X 1/6

Duration (seconds):

30

Max # of packets to view:

5000

Capture Filter (Optional):

Capture

Note: Capture file size will not exceed 575 MB. Once the packet capture file reaches this size, packet capturing will be stopped. Atleast 1 interface needs to be selected to trigger a packet capture.

Gathering Requested Data

Generating packet capture information...

Packet Capture Successful!

Packet Capture File

A binary file containing the packet data captured during the last successful packet capture. This file can be opened in Wireshark for analysis.

The downloaded Packet capture file displays internal labels for interface names. Here are the mappings for this platform:
MGMT -> tn-mgt0
1/1 -> dpdk-1_1
1/4 -> dpdk-1_4
1/2 -> dpdk-1_2
1/6 -> dpdk-1_6

Download

Packet View

#	Interface Name	Protocol	Time	Length	Source	Destination	Src
1.	1/2	UDP	May 8, 2019 06:06:30.415518572 UTC	1442	172.168.1.10	152.168.1.10	4980
2.	1/2	UDP	May 8, 2019 06:06:30.415524972 UTC	1442	152.168.1.10	172.168.1.10	4980
3.	1/2	UDP	May 8, 2019 06:06:30.415628324 UTC	1442	152.168.1.10	172.168.1.10	4980
4.	1/2	UDP	May 8, 2019 06:06:30.415648675 UTC	1442	172.168.1.10	152.168.1.10	4980
5.	1/2	UDP	May 8, 2019 06:06:30.415858329 UTC	1442	152.168.1.10	172.168.1.10	4980
6.	1/2	UDP	May 8, 2019 06:06:30.415873459 UTC	1442	172.168.1.10	152.168.2.10	4980
7.	1/2	UDP	May 8, 2019 06:06:30.416073413 UTC	1442	172.168.1.10	152.168.2.10	4980
8.	1/2	UDP	May 8, 2019 06:06:30.416232216 UTC	1442	152.168.1.10	172.168.1.10	4980
9.	1/1	TCP	May 8, 2019 06:06:30.321504133 UTC	1384	152.168.1.51	172.168.1.52	80
10.	1/2	UDP	May 8, 2019 06:06:30.416266227 UTC	1442	152.168.1.10	172.168.1.10	4980
11.	1/2	UDP	May 8, 2019 06:06:30.416435190 UTC	1442	172.168.1.10	152.168.1.10	4980
12.	1/2	UDP	May 8, 2019 06:06:30.416525402 UTC	114	172.168.1.10	152.168.2.10	4980
13.	1/1	TCP	May 8, 2019 06:06:30.321511153 UTC	54	152.168.1.52	172.168.1.51	2307
14.	1/2	UDP	May 8, 2019 06:06:30.416529932 UTC	114	172.168.1.10	152.168.2.10	4980
15.	1/1	TCP	May 8, 2019 06:06:30.321514773 UTC	54	152.168.1.52	172.168.1.51	2163
16.	1/2	UDP	May 8, 2019 06:06:30.416651685 UTC	1442	152.168.1.10	172.168.1.10	4980
17.	1/2	UDP	May 8, 2019 06:06:30.416693075 UTC	1442	152.168.1.10	172.168.1.10	4980
18.	1/2	UDP	May 8, 2019 06:06:30.416783167 UTC	1442	172.168.1.10	152.168.2.10	4980
19.	1/2	UDP	May 8, 2019 06:06:30.416881149 UTC	1442	172.168.1.10	152.168.2.10	4980
20.	1/2	UDP	May 8, 2019 06:06:30.417039802 UTC	1442	152.168.1.10	172.168.1.10	4980
21.	1/2	UDP	May 8, 2019 06:06:30.417127644 UTC	114	172.168.1.10	152.168.2.10	4980
22.	1/2	UDP	May 8, 2019 06:06:30.417132114 UTC	114	172.168.1.10	152.168.1.10	4980
23.	1/2	UDP	May 8, 2019 06:06:30.417135804 UTC	1442	172.168.1.10	152.168.2.10	4980
24.	1/1	TCP	May 8, 2019 06:06:30.321517954 UTC	54	152.168.1.52	172.168.1.51	6265
25.	1/2	UDP	May 8, 2019 06:06:30.417178605 UTC	114	172.168.1.10	152.168.1.10	4980
26.	1/1	TCP	May 8, 2019 06:06:30.321648046 UTC	1384	172.168.1.51	152.168.1.52	80

パケットキャプチャ操作に次の入力を提供します。

- インターフェイス - アクティブなインターフェイスは、SD-WAN アプライアンスのパケットキャプチャに使用できます。ドロップダウンリストからインターフェイスを選択するか、インターフェイスを追加します。パケットキャプチャをトリガーするには、少なくとも 1 つのインターフェイスを選択する必要があります。

注:

すべてのインターフェイスで同時にパケットキャプチャを実行する機能は、トラブルシューティングタスクのスピードアップに役立ちます。

- **Duration (秒)** - データをキャプチャする必要がある期間 (秒単位)。
- 表示するパケットの最大数: パケットキャプチャ結果に表示されるパケットの最大制限。
- **Capture Filter** (オプション): オプションの Capture Filter フィールドは、キャプチャされるパケットを決定するために使用されるフィルタ文字列を受け入れます。パケットはフィルタ文字列と比較され、比較結果が true の場合、パケットがキャプチャされます。フィルタが空の場合、すべてのパケットがキャプチャされます。詳細については、[キャプチャフィルタを参照してください](#)。

このキャプチャフィルターの例を以下に示します。

- **Ether proto\ ARP**: ARP パケットだけをキャプチャします。
- **Ether proto\ IP**: IPv4 パケットのみをキャプチャします
- **VLAN 100**: VLAN が 100 のパケットのみをキャプチャします。
- ホスト **10.40.10.20** - アドレスが 10.40.10.20 のホストとの間で送受信される IPv4 パケットのみをキャプチャします
- ネット **10.40.10.0** マスク **255.255.255.0** - 10.40.10.0/24 サブネット内の IPv4 パケットだけをキャプチャします
- **IP プロト ¥TCP** - IPv4/TCP パケットのみをキャプチャします。
- ポート **80**: ポート 80 との間で送受信される IP パケットのみをキャプチャします。
- ポート範囲 **20 ~30**: ポート 20 ~30 との間で送受信される IP パケットだけをキャプチャします。

注

キャプチャファイルの最大サイズ制限は最大 575 MB です。パケットキャプチャファイルがこのサイズに達すると、パケットキャプチャは停止します。

[**Capture**] をクリックして、パケットキャプチャ結果を表示します。最後に成功したパケットキャプチャ中にキャプチャされたパケットデータを含むバイナリファイルをダウンロードすることもできます。

リクエストされたデータの収集

この表では、パケットキャプチャ情報の生成のステータス（パケットキャプチャが成功したかどうか、パケットキャプチャがないかどうか）を確認できます。

パケットキャプチャファイル

パケットは、最後に成功したパケットキャプチャ中に、バイナリデータとしてキャプチャされます。バイナリファイルをダウンロードして、パケット情報をオフラインで分析できます。インタフェース名は、GUI インタフェースと比較して、ダウンロードしたファイルでは異なります。内部インターフェイスのマッピングを表示するには、[Help] オプションをクリックします。

Packet Capture File

A binary file containing the packet data captured during the last successful packet capture. This file can be opened in Wireshark for analysis. [Help](#)

The downloaded packet capture file displays internal labels for interface names. Here are the mappings for this platform:

```

MGMT -> tn-mgt0
1/4 -> dpdk-1_4
1/1 -> dpdk-1_1
1/5 -> dpdk-1_5
1/2 -> dpdk-1_2
LTE-1 -> dpdk-lte_1

```

[Download](#)

バイナリファイルを開いて読み込むには、**Wireshark** ソフトウェア 2.4.13 バージョン以上が必要です。

The screenshot shows the Wireshark interface. The top toolbar includes icons for file operations, network analysis, and search. The main pane displays a list of captured packets with columns for Time, Source, Destination, Protocol, Length, Interface name, and Src Mac. The details pane on the right shows the selected packet's structure, including Ethernet II, Internet Protocol Version 4, and Hypertext Transfer Protocol.

Time	Source	Destination	Protocol	Length	Interface name	Src Mac
1 2019-04-26 05:53:09.403929649	10.103.40.80	192.168.60.15	UDP	306	dpdk-lte_1	9e:15:
2 2019-04-26 05:53:09.808203024	10.103.40.80	192.168.60.15	UDP	226	dpdk-lte_1	9e:15:
3 2019-04-26 05:53:09.808215048	10.103.40.80	192.168.60.15	UDP	226	dpdk-lte_1	9e:15:
4 2019-04-26 05:53:10.026787042	fe80::5834:4eff:fe...	ff02::2	ICMPv6	70	dpdk-1_1	5a:34:
5 2019-04-26 05:53:10.811549725	10.103.40.80	192.168.60.15	UDP	226	dpdk-lte_1	9e:15:
6 2019-04-26 05:53:10.811561358	10.103.40.80	192.168.60.15	UDP	226	dpdk-lte_1	9e:15:
7 2019-04-26 05:53:11.404405624	10.103.40.80	192.168.60.15	UDP	306	dpdk-lte_1	9e:15:
8 2019-04-26 05:53:11.815088189	10.103.40.80	192.168.60.15	UDP	226	dpdk-lte_1	9e:15:
9 2019-04-26 05:53:11.815100522	10.103.40.80	192.168.60.15	UDP	226	dpdk-lte_1	9e:15:
10 2019-04-26 05:53:12.818065232	10.103.40.80	192.168.60.15	UDP	226	dpdk-lte_1	9e:15:
11 2019-04-26 05:53:12.818156899	10.103.40.80	192.168.60.15	UDP	226	dpdk-lte_1	9e:15:
12 2019-04-26 05:53:13.405512485	10.103.40.80	192.168.60.15	UDP	306	dpdk-lte_1	9e:15:
13 2019-04-26 05:53:13.821801944	10.103.40.80	192.168.60.15	UDP	226	dpdk-lte_1	9e:15:
14 2019-04-26 05:53:13.821813477	10.103.40.80	192.168.60.15	UDP	226	dpdk-lte_1	9e:15:
15 2019-04-26 05:53:14.834919479	10.103.40.80	192.168.60.15	UDP	226	dpdk-lte_1	9e:15:
16 2019-04-26 05:53:14.834931891	10.103.40.80	192.168.60.15	UDP	226	dpdk-lte_1	9e:15:
17 2019-04-26 05:53:15.406160515	10.103.40.80	192.168.60.15	UDP	306	dpdk-lte_1	9e:15:
18 2019-04-26 05:53:15.838934651	10.103.40.80	192.168.60.15	UDP	226	dpdk-lte_1	9e:15:
19 2019-04-26 05:53:15.838946928	10.103.40.80	192.168.60.15	UDP	226	dpdk-lte_1	9e:15:
20 2019-04-26 05:53:16.842346703	10.103.40.80	192.168.60.15	UDP	226	dpdk-lte_1	9e:15:
21 2019-04-26 05:53:16.842358521	10.103.40.80	192.168.60.15	UDP	226	dpdk-lte_1	9e:15:
22 2019-04-26 05:53:17.406642988	10.103.40.80	192.168.60.15	UDP	306	dpdk-lte_1	9e:15:
23 2019-04-26 05:53:17.845891359	10.103.40.80	192.168.60.15	UDP	226	dpdk-lte_1	9e:15:
24 2019-04-26 05:53:17.845903254	10.103.40.80	192.168.60.15	UDP	226	dpdk-lte_1	9e:15:
25 2019-04-26 05:53:18.850000114	10.103.40.80	192.168.60.15	UDP	226	dpdk-lte_1	9e:15:
26 2019-04-26 05:53:18.850012213	10.103.40.80	192.168.60.15	UDP	226	dpdk-lte_1	9e:15:
27 2019-04-26 05:53:19.407464852	10.103.40.80	192.168.60.15	UDP	306	dpdk-lte_1	9e:15:
28 2019-04-26 05:53:19.867551012	10.103.40.80	192.168.60.15	UDP	226	dpdk-lte_1	9e:15:
29 2019-04-26 05:53:19.867562750	10.103.40.80	192.168.60.15	UDP	226	dpdk-lte_1	9e:15:

▼ Frame 1: 306 bytes on wire (2448 bits), 306 bytes captured (2448 bits) on interface 0

- Interface id: 0 (dpdk-lte_1)
- Encapsulation type: Ethernet (1)
- Arrival Time: Apr 26, 2019 11:23:09.403929649 IST
- [Time shift for this packet: 0.000000000 seconds]
- Epoch Time: 1556257989.403929649 seconds
- [Time delta from previous captured frame: 0.000000000 seconds]
- [Time delta from previous displayed frame: 0.000000000 seconds]
- [Time since reference or first frame: 0.000000000 seconds]
- Frame Number: 1

パケットビュー

パケットキャプチャファイルのサイズが大きければ、パケットビューのレンダリングプロセスを完了するのに時間がかかります。この場合、パケットビューの結果に頼るのではなく、ファイルをダウンロードして分析に **Wireshark** を使用することを推奨します。

パス帯域幅

パス帯域幅機能を使用するには、[設定] > [システムメンテナンス] > [診断] を展開し、[パス帯域幅] を選択します。

DashboardMonitoringConfiguration

+

Appliance Settings

+

Virtual WAN

-

System Maintenance

- Delete Files
- Restart System
- Data/Time Settings
- Local Change Management
- Diagnostics**
- Update Software
- Configuration Reset
- Factory Reset

Configuration > System Maintenance > Diagnostics

Ping

Traceroute

Packet Capture

Path Bandwidth

System Info

Diagnostic Data

Events

Alarms

Diagnostics Tool

Instant Path Bandwidth Testing

Path:MCN-5100-WL-2>BR572-1

Test

Results

Minimum Bandwidth: 936564 kbps
Maximum Bandwidth: 1213883 kbps
Average Bandwidth: 1189846 kbps

Schedule Path Bandwidth Testing

Add

Path Name

Frequency

Day of Week

Hour

Minute

Apply Settings

History Path Bandwidth Testing Result

Show50entriesShowing 1 to 27 of 27 entries

First

Previous

1

Next

Last

Num	From Link	To Link	Test Time	Min Bandwidth (kbps)	Max Bandwidth (kbps)	Avg Bandwidth (kbps)
1	RCN1-5100-WL-1	MCN-5100-WL-1	2/17/2018, 2:01:03 PM	2883972	5099707	4357330
2	RCN1-5100-WL-1	MCN-5100-WL-1	2/17/2018, 4:01:03 PM	3109115	3872000	3616157
3	RCN1-5100-WL-1	MCN-5100-WL-1	2/17/2018, 6:01:04 PM	3041280	4119960	3518949
4	RCN1-5100-WL-1	MCN-5100-WL-1	2/17/2018, 8:01:04 PM	2769377	3700672	3276124
5	RCN1-5100-WL-1	MCN-5100-WL-1	2/17/2018, 10:01:04 PM	409245	3574153	2489269
6	RCN1-5100-WL-1	MCN-5100-WL-1	2/18/2018, 12:01:04 AM	2481756	4001694	3198224
7	RCN1-5100-WL-1	MCN-5100-WL-1	2/18/2018, 2:01:04 AM	2548653	3872000	3236546
8	RCN1-5100-WL-1	MCN-5100-WL-1	2/18/2018, 4:01:03 AM	3204413	3982628	3642643
9	RCN1-5100-WL-1	MCN-5100-WL-1	2/18/2018, 6:01:03 AM	2997677	4672357	3664018
10	RCN1-5100-WL-1	MCN-5100-WL-1	2/18/2018, 8:01:04 AM	2248259	6288360	3612666
11	RCN1-5100-WL-1	MCN-5100-WL-1	2/18/2018, 10:01:04 AM	2410236	3372387	2816032
12	RCN1-5100-WL-1	MCN-5100-WL-1	2/18/2018, 12:01:03 PM	2613600	4401852	3563752
13	RCN1-5100-WL-1	MCN-5100-WL-1	2/18/2018, 2:01:04 PM	2324266	4059961	3101910
14	RCN1-5100-WL-1	MCN-5100-WL-1	2/18/2018, 4:01:03 PM	2173340	3684370	2929146
15	RCN1-5100-WL-1	MCN-5100-WL-1	2/18/2018, 6:01:03 PM	2613600	3589498	3021890
16	RCN1-5100-WL-1	MCN-5100-WL-1	2/18/2018, 8:01:03 PM	1678056	3499380	2655280
17	RCN1-5100-WL-1	MCN-5100-WL-1	2/18/2018, 10:01:03 PM	1954093	3558944	2975804
18	RCN1-5100-WL-1	MCN-5100-WL-1	2/19/2018, 12:01:03 AM	2161116	3784398	2902068
19	RCN1-5100-WL-1	MCN-5100-WL-1	2/19/2018, 2:01:04 AM	2986971	4079765	3821158
20	RCN1-5100-WL-1	MCN-5100-WL-1	2/19/2018, 4:01:04 AM	3514084	4181760	3893381
21	RCN1-5100-WL-1	MCN-5100-WL-1	2/19/2018, 6:01:03 AM	3958843	4059961	3756691
22	RCN1-5100-WL-1	MCN-5100-WL-1	2/19/2018, 8:01:03 AM	3216738	4245441	3716551
23	RCN1-5100-WL-1	MCN-5100-WL-1	2/19/2018, 10:01:04 AM	3558944	4202773	3932908
24	RCN1-5100-WL-1	MCN-5100-WL-1	2/19/2018, 12:01:03 PM	3427872	4267102	3838552
25	RCN1-5100-WL-1	MCN-5100-WL-1	2/19/2018, 2:01:04 PM	2874061	4224000	3608676
26	RCN1-5100-WL-1	MCN-5100-WL-1	2/19/2018, 4:01:03 PM	2816000	6288360	4165337
27	MCN-5100-WL-2	BR572-WL-1	2/19/2018, 5:23:04 PM	936564	1213883	1109046

Showing 1 to 27 of 27 entries

First

Previous

1

Next

Last

アクティブ帯域幅テストを使用すると、パブリックインターネット WAN リンクを介してインスタントパス帯域幅テストを発行したり、パブリックインターネット WAN リンク帯域幅テストを特定の時間に繰り返して完了するように

スケジュールしたりできます。

パス帯域幅機能は、新規および既存のインストール時に、2つのロケーション間で使用可能な帯域幅の量を示すのに役立ちます。[パス帯域幅]の値は、可能な最大帯域幅を示します。正確な許可された帯域幅に関しては、設定>システムメンテナンス>診断>** サイト診断 **>帯域幅テストにナビゲートして下さい。詳細については、[アクティブ帯域幅テストを参照してください](#)。

システム情報

[システム情報 (System Info)] ページには、システム情報、イーサネットポートの詳細、およびライセンスステータスが表示されます。

システム情報を表示するには、[構成]>[システムメンテナンス]>[診断]の順に展開し、[システム情報]を選択します。

DashboardMonitoringConfiguration

+ Appliance Settings

+ Virtual WAN

- System Maintenance

- Delete Files
- Restart System
- Date/Time Settings
- Local Change Management
- Diagnostics**
- Update Software
- Configuration Reset
- Factory Reset

Configuration > System Maintenance > Diagnostics

PingTraceroutePacket CapturePath BandwidthSystem InfoDiagnostic DataEventsAlarmsDiagnostics Tool

Site Diagnostics

System Information

Name: Dallas_MCN

Appliance Mode: MCN

Hardware Model: 4000

Software Version: 11.0.0.72.760315

Built On: Apr 10 2019 at 19:08:49

OS Partition Version: 5.1

Serial Number: HNXCJCRGJX

BIOS version: 4.2a

Hard Disk Usage

Partition	Usage
Active OS	51%
/home	18%

[View Details](#)

Ethernet Ports

0/1:	mgt0	0a:c4:7a:85:ce:62
1/1:	la0	be:0a:f7:be:76:3d
1/2:	wa0	e6:18:31:22:b9:84
1/3:	la1	86:c0:b7:3c:03:5d
1/4:	wa1	8e:4b:f2:fd:86:75
1/5:	la2	da:6c:7c:73:d4:84
1/6:	wa2	be:e3:26:7e:2b:99
1/7:	la3	82:af:6a:d8:74:72
1/8:	wa3	a2:af:76:6f:90:a2
10/1:	la4	96:9a:df:97:77:eb
10/2:	wa4	76:5d:15:d9:f0:26

License Status

State:	Licensed
License Server HostID:	02c47a85ce62
Model:	4000VW-2000
Maximum Bandwidth (MAXBW):	2000 Mbps
License Type:	Retail
Maintenance Expiration Date:	Sun Dec 1 00:00:00 2019
License Expiration Date:	Mon Dec 2 00:00:00 2019

[システム情報 (System Info)] には、デフォルトに設定されていないすべてのパラメータが一覧表示されます。この情報は読み取り専用です。なんらかの設定ミスが疑われる場合にサポートが使用します。問題を報告すると、このページで1つ以上の値を確認するように求められる場合があります。

診断データ

診断データを使用すると、Citrix サポートチームが分析する診断データパッケージを生成できます。診断ログファイルパッケージをダウンロードして、Citrix サポートチームと共有できます。

診断データを表示するには、[構成] > [システムメンテナンス] > [診断] の順に展開し、[診断データ] を選択します。

The screenshot displays the Citrix SD-WAN 11.4 web interface, specifically the **Configuration > System Maintenance > Diagnostics** section. The left sidebar shows the navigation menu with **Diagnostics** selected. The main content area is divided into several sections:

- FTP Information:** Contains fields for Customer, Username, Password, and FTP Server, with an **FTP Apply** button. A note states: "Note: All fields are required in order to FTP Apply."
- Diagnostic Information:** Includes a note: "NOTE: To enable Upload option, please configure DNS settings and an FTP Customer Name for this appliance." It lists **Diagnostic Log Files** and provides a **Create New...** button, a **Filename:** dropdown, and buttons for **Download Selected**, **Upload Selected**, and **Delete Selected**.
- Memory Dumps:** Includes a note: "NOTE: To enable Upload option, please configure DNS settings and an FTP Customer Name for this appliance." It lists **System Error Memory Dumps** and provides a **Download**, **Upload**, and **Delete** button.
- Configuration Diagnostic Information:** Includes a note: "NOTE: To enable Upload option, please configure DNS settings and an FTP Customer Name for this appliance." It lists **Configuration Diagnostic Files** and provides a **Create New...** button, a **Filename:** dropdown, and buttons for **Download Selected**, **Upload**, and **Delete Selected**.

診断データには次のものが含まれます。

- 「**FTP 情報**」—FTP パラメータの詳細を入力し、「**FTP 適用**」をクリックします。診断情報パッケージをアップロードするために FTP サーバーに接続するのに必要な FTP 情報。
- 診断情報: 診断ログファイルパッケージには、ブラウザからダウンロードしたり、FTP 経由で FTP サーバにアップロードしたりできるリアルタイムのシステム情報が含まれています。

注:

システムに同時に存在できる診断パッケージは 5 つだけです。

- 構成診断情報 -Citrix SD-WAN 11.0 リリースでは、ブランチ用に収集された診断情報でネットワーク構成ファイルを使用できません。サポートケースの場合は、ブランチの診断情報と、ブランチの接続先のコントロールノードからの構成診断情報を入力します。

Control Node GUI から設定診断情報を収集するには、[構成] > [システムメンテナンス] > [診断] > [診断データ] > [構成診断情報] の下に移動し、[新規作成] をクリックします。

The screenshot shows the 'Configuration Diagnostic Information' section of the Citrix SD-WAN GUI. It includes a note about enabling the upload option by configuring DNS settings and an FTP customer name. Below this, there's a section for 'Configuration Diagnostic Files' with two bullet points explaining the package contents and the limit of 5 packages. At the bottom, there's a 'Create New...' button (highlighted with a red box), a 'Filename:' input field, and buttons for 'Download Selected', 'Upload', and 'Delete Selected'.

構成診断情報の作成が完了したら、[選択したファイルのダウンロード] をクリックしてこのファイルを Citrix サポートに提供するか、同じページにある FTP 適用操作を使用してこのファイルを FTP 処理します。

- メモリダンプシステムエラーメモリダンプファイルをダウンロードまたはアップロードして、Citrix サポートチームと共有できます。必要でない場合は、ファイルを削除することもできます。

注:

デフォルトでは、[アップロード] オプションは無効モードになっています。これを有効にするには、このアプライアンスの **DNS** 設定と **FTP** カスタマー名を設定します。

イベント

イベント機能を使用して、生成されたイベントを追加、監視、および管理します。リアルタイムでイベントを特定し、問題を即座に解決し、Citrix SD-WAN アプライアンスを効果的に実行し続けるのに役立ちます。イベントは CSV 形式でダウンロードできます。

イベントを追加するには、ドロップダウンリストからオブジェクトタイプ、イベントタイプ、および重大度を選択し、**[Add Event]** をクリックします。

イベントを表示するには、**[構成] > [システムメンテナンス] **[診断]** の順に展開し **、**[イベント]** を選択します。

DashboardMonitoringConfiguration

+ Appliance Settings

+ Virtual WAN

- System Maintenance

Delete Files

Restart System

Date/Time Settings

Local Change Management

Diagnostics

Update Software

Configuration Reset

Factory Reset

Configuration > System Maintenance > Diagnostics

PingTraceroutePacket CapturePath BandwidthSystem InfoDiagnostic Data**Events**AlarmsDiagnostics Tool

Site Diagnostics

Insert Event

Object Type:USER EVENT

Event type:UNDEFINED

Severity:DEBUG

Add Event

Download Events

There are currently 85 in the Events database, spanning from event 245471 at 2019-03-24 05:35:54 to event 245555 at 2019-04-21 06:23:16. You can download some or all of them in CSV format. You may wish to limit the amount to download because some common spreadsheet programs limit you to 65,536 rows.

Download events starting from2019March24535

54Download (85 events)

Alert Count

Alert Type	Alerts Sent
Emails:	0
Syslog Messages:	0
SNMP Traps:	5

View Events

Quantity:1000

Filter: Object Type = AnyEvent type = AnySeverity = Any

Reload Events Table

ID	Object ID	Object Name	Object Type	Time	Event Type	Severity	Description
245555	25	License_Alert	LICENSE_EVENT	2019-04-21 06:23:16	WARNING	CRITICAL	The total configured permitted rate (WAN to LAN) 13670000 (Kbps) must not exceed twice the License Rate which is 4000000 (Kbps).
245554	25	License_Alert	LICENSE_EVENT	2019-04-20 06:23:01	WARNING	CRITICAL	The total configured permitted rate (WAN to LAN) 13670000 (Kbps) must not exceed twice the License Rate which is 4000000 (Kbps).
245553	25	License_Alert	LICENSE_EVENT	2019-04-19 06:22:46	WARNING	CRITICAL	The total configured permitted rate (WAN to LAN) 13670000 (Kbps) must not exceed twice the License Rate which is 4000000 (Kbps).
245552	25	License_Alert	LICENSE_EVENT	2019-04-18 06:22:31	WARNING	CRITICAL	The total configured permitted rate (WAN to LAN) 13670000 (Kbps) must not exceed twice the License Rate which is 4000000 (Kbps).
245551	25	License_Alert	LICENSE_EVENT	2019-04-17 06:22:15	WARNING	CRITICAL	The total configured permitted rate (WAN to LAN) 13670000 (Kbps) must not exceed twice the License Rate which is 4000000 (Kbps).
245550	25	License_Alert	LICENSE_EVENT	2019-04-16 06:22:00	WARNING	CRITICAL	The total configured permitted rate (WAN to LAN) 13670000 (Kbps) must not exceed twice the License Rate which is 4000000 (Kbps).
245549	25	License_Alert	LICENSE_EVENT	2019-04-15 06:21:44	WARNING	CRITICAL	The total configured permitted rate (WAN to LAN) 13670000 (Kbps) must not exceed twice the License Rate which is 4000000 (Kbps).
245548	25	License_Alert	LICENSE_EVENT	2019-04-14 06:21:29	WARNING	CRITICAL	The total configured permitted rate (WAN to LAN) 13670000 (Kbps) must not exceed twice the License Rate which is 4000000 (Kbps).

Citrix SD-WAN を構成して、さまざまなイベントタイプのイベント通知を電子メール、**SNMP** トラップ、または Syslog メッセージとして送信できます **。

電子メール、SNMP、および syslog 通知の設定が完了したら、さまざまなイベントタイプの重大度を選択し、イベント通知を送信するモード（電子メール、SNMP、syslog）を選択できます。

通知は、イベントタイプに指定された重大度レベル以上のイベントに対して生成されます。

イベントの詳細は、**[View Events]** テーブルで確認できます。イベントの詳細には、次の情報が含まれます。

- **ID** – イベント ID。

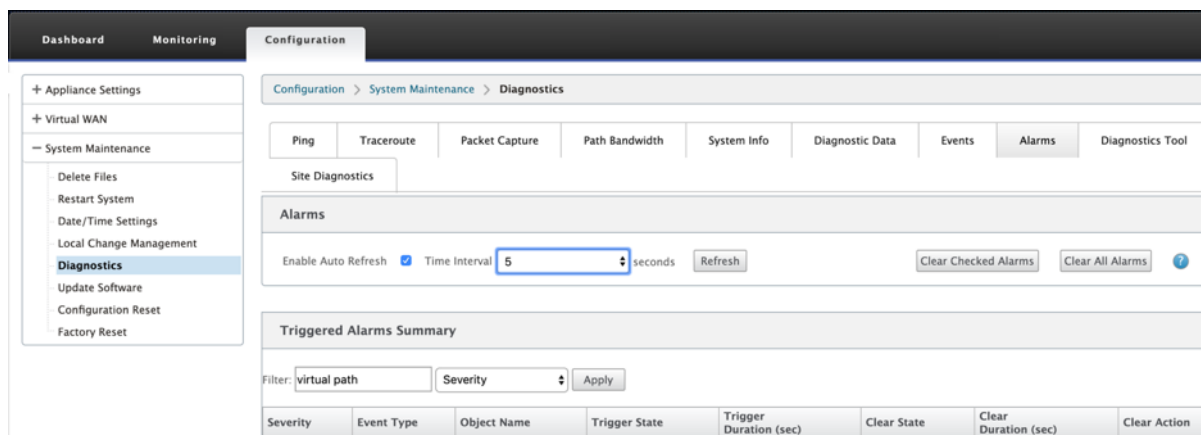
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

932

- オブジェクト **ID** - イベントを生成するオブジェクトの ID。
- オブジェクト名 - イベントを生成するオブジェクトの名前。
- オブジェクトタイプ - イベントを生成するオブジェクトのタイプ。
- **Time** - イベントが生成された時刻。
- **Event Type** - イベント発生時のオブジェクトの状態。
- 重大度 - イベントの重大度レベル。
- 説明 - イベントの説明文です。

alarms

トリガーされたアラームを表示およびクリアできます。アラームを表示するには、[構成]に移動し、[システムメンテナンス]>[診断]を展開し、[アラーム]を選択します。



クリアするアラームを選択し、[チェック済みアラームのクリア (**Clear Alarms**)] をクリックするか、[すべてのアラームをクリア (**Clear All Alarms**)] をクリックしてすべてのアラームをクリアします。

トリガーされたすべてのアラームの次のサマリーを表示できます。

- 重大度: 重大度は、アラームがトリガーまたはクリアされたときに送信されるアラート、およびトリガーされたアラームの概要に表示されます。
- **Event Type**: SD-WAN アプライアンスは、ネットワーク内の特定のサブシステムまたはオブジェクトに対してアラームをトリガーできます。これらのアラームは、イベントタイプと呼ばれます。
- [オブジェクト名] - イベントを生成するオブジェクトの名前。
- [**Trigger State**]: イベントタイプのアラームをトリガーするイベント状態。
- トリガー期間 (秒) - 一秒単位の期間によって、アプライアンスがアラームをトリガーする速度が決まります。
- [**Clear State**]: アラームがトリガーされた後にイベントタイプのアラームをクリアするイベント状態。
- [**Clear Duration (sec)**]: アラームをクリアするまでの待機時間を秒単位で指定します。
- [**Clear Action**]: アラームのクリア中に実行されるアクション。

診断ツール

診断ツールは、テストトラフィックを生成するために使用します。これにより、次のような結果になる可能性のあるネットワーク上の問題をトラブルシューティングできます。

- パス状態が良好から不良に頻繁に変化する。
- アプリケーションのパフォーマンスが低下します。
- パケット損失の増加

ほとんどの場合、これらの問題は、ファイアウォールとルータで設定されたレート制限、誤った帯域幅設定、低いリンク速度、ネットワークプロバイダーによって設定されたプライオリティキューなどが原因で発生します。診断ツールを使用すると、このような問題の根本原因を特定し、トラブルシューティングを行うことができます。

診断ツールは、データセンターおよびブランチホストに手動でインストールする必要がある iPerf などのサードパーティ製ツールへの依存性を排除します。これにより、送信される診断トラフィックのタイプ、診断トラフィックが流れる方向、および診断トラフィックが流れるパスをより詳細に制御できます。

診断ツールでは、次の 2 種類のトラフィックを生成できます。

- 制御：パケットに QoS/スケジューリングが適用されていないトラフィックを生成します。その結果、そのパスが最適でない場合でも、UI で選択したパスでパケットが送信されます。このトラフィックは、特定のパスをテストするために使用され、ISP 関連の問題の特定に役立ちます。これを使用して、選択したパスの帯域幅を決定することもできます。
- データ:SD-WAN トラフィック処理でホストから生成されたトラフィックをシミュレートします。QoS/Scheduling がパケットに適用されるため、パケットは利用可能な最良のパスで送信されます。負荷分散が有効の場合、トラフィックは複数のパスで送信されます。このトラフィックは、QoS /スケジューラ関連の問題のトラブルシューティングに使用されます。

注

パスで診断テストを実行するには、パスの両端でアプライアンスでテストを開始する必要があります。診断テストは、一方のアプライアンスのサーバとして、もう一方のアプライアンスのクライアントとして開始します。

診断ツールを使用するには、次の手順に従います。

1. 両方のアプライアンスで、構成 > システムメンテナンス > 診断 > 診断ツールをクリックします。

The screenshot shows the 'Diagnostics Tool' window. In the 'Tool Mode' dropdown, 'Server' is selected. 'Traffic Type' is set to 'Data'. The 'Port' field contains '10'. The 'Iperf' field is empty. The 'WAN to LAN Paths' dropdown shows 'DC-INET-1->BR1-INET-1'. A 'Start' button is at the bottom left of the tool section. Below this is the 'Results' section, which contains a 'stop' button and a text area showing 'Server listening on TCP port 10' and 'TCP window size: 85.3 KByte (default)'.

2. 「ツールモード」フィールドで、「アプライアンス上のサーバ」を選択し、選択したパスのリモートエンドに存在するアプライアンスで「クライアント」を選択します。
3. [トラフィックタイプ (Traffic Type)] フィールドで、診断トラフィックの種類 ([制御] または [データ]) を選択します。両方のアプライアンスで同じトラフィックタイプを選択します。
4. [ポート (**Port**)] フィールドで、診断トラフィックを送信する **TCP/UDP** ポート番号を指定します。両方のアプライアンスで同じポート番号を指定します。
5. [**Iperf**] フィールドに、IPERF コマンドラインオプションがあれば指定します。

注

次の IPERF コマンドラインオプションを指定する必要はありません。

- -c: 診断ツールによってクライアントモードオプションが追加されます。
- -s: 診断ツールによってサーバ・モード・オプションが追加されます。
- -B: IPERF を特定の IP/インターフェイスにバインドするには、選択したパスに応じて診断ツールを実行します。
 - -p: ポート番号は診断ツールで提供されます。
- -i: 出力間隔 (秒)。
- -t: テストの合計時間 (秒)。

6. 診断トラフィックを送信する WAN から LAN へのパスを選択します。両方のアプライアンスで同じパスを選択します。
7. 両方のアプライアンスで [**Start**] をクリックします。

結果には、選択したアプライアンスのモード（クライアントまたはサーバ）と、テストが実行された TCP または UDP ポートが表示されます。テストの合計期間に達するまで、指定された間隔で転送されたデータおよび使用された帯域幅が定期的に表示されます。

Configuration > System Maintenance > Diagnostics

PingTraceroutePacket CapturePath BandwidthSystem InfoDiagnostic DataEventsAlarmsDiagnostics Tool

Site Diagnostics

Diagnostics Tool

Tool Mode: ClientTraffic Type: DataPort: 10

Iperf:LAN to WAN Paths: MCN_184_78-Broadband

Start

Results

stop

Client connecting to 172.16.31.10, TCP port 10
Binding to local address 172.16.21.10
TCP window size: 112 KByte (default)

[3] local 172.16.21.10 port 39993 connected with 172.16.31.10 port 10
[ID] Interval Transfer Bandwidth
[3] 0.0~ 1.0 sec 10.1 MBytes 84.9 Mbits/sec
[3] 1.0~ 2.0 sec 11.9 MBytes 99.6 Mbits/sec
[3] 2.0~ 3.0 sec 13.4 MBytes 112 Mbits/sec
[3] 3.0~ 4.0 sec 15.1 MBytes 127 Mbits/sec
[3] 4.0~ 5.0 sec 14.5 MBytes 122 Mbits/sec
[3] 5.0~ 6.0 sec 14.5 MBytes 122 Mbits/sec
[3] 6.0~ 7.0 sec 15.1 MBytes 127 Mbits/sec
[3] 7.0~ 8.0 sec 15.1 MBytes 127 Mbits/sec
[3] 8.0~ 9.0 sec 15.6 MBytes 131 Mbits/sec
[3] 9.0~10.0 sec 16.0 MBytes 134 Mbits/sec
[3] 0.0~10.0 sec 141 MBytes 118 Mbits/sec

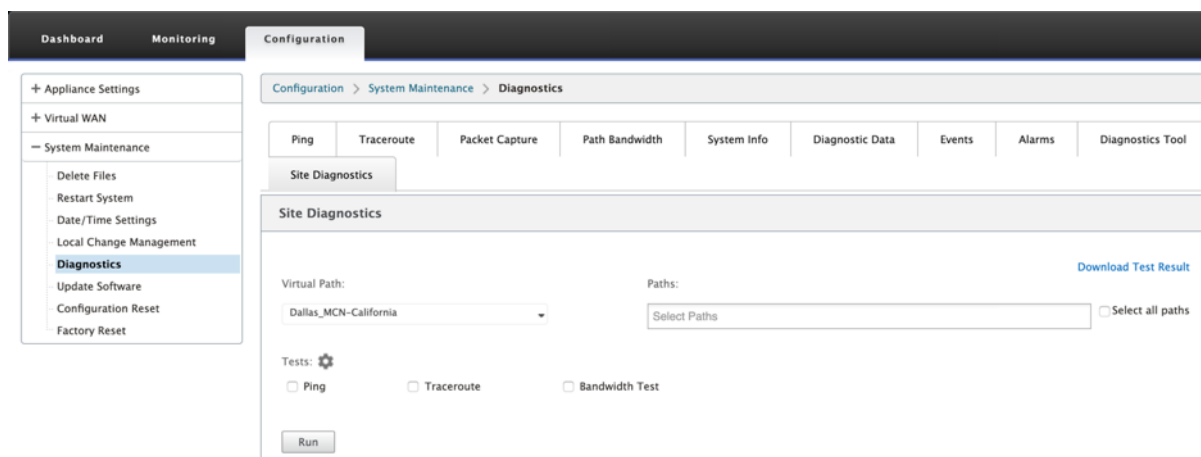
サイト診断

Citrix SD-WAN ネットワークの異なるサイトで構成された WAN リンクの帯域幅使用状況、ping をテストし、トレースルートを実行することができます。既存の設定の問題のトラブルシューティングに役立つ情報を提供します。

サイト診断を使用するには、[構成] > [システムメンテナンス] **[診断 **] を展開し、[診断ツール] を選択します。

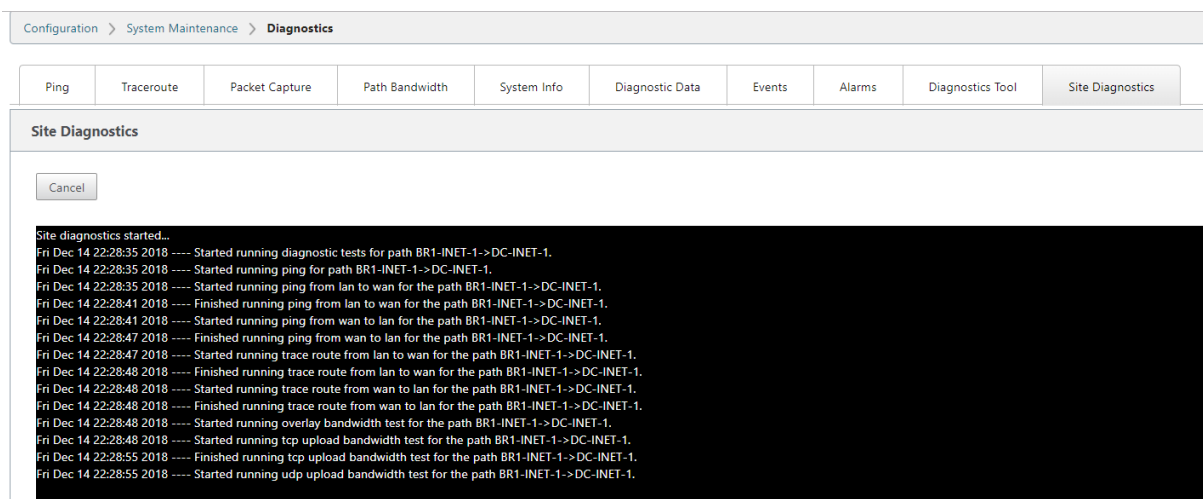
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

936



[結果] セクションには次の情報が表示されます。

- **[Interface Status]:** インターフェイスの名前、インターフェイスに関連付けられているファイアウォールゾーンの数、VLAN ID、および関連付けられているポートが表示されます。
- **[パスステータス]:** ターゲットプライベート IP、ゲートウェイ IP、ターゲットパブリック IP、パートナー IP、パートナーパブリック IP アドレスの詳細が表示されます。また、ゲートウェイ ARP とパス MTU のステータスも表示されます。
- **Ping Result: ping** の方向、ステータス、回数 (試行回数と失敗回数を含む)、および RTT が表示されます。
- **traceroute Result:** ホップの方向、ステータス、ホップ数、IP アドレスまたは RTT が表示されます。
- **帯域幅の結果:** TCP と UDP のステータスと、オーバーレイおよびアンダーレイネットワークに使用されている帯域幅 (kbps 単位) が表示されます。UDP は帯域幅ベースであり、設定された帯域幅のみを使用するため、UDP と比較して TCP で使用される帯域幅は大きくなります。TCP はランプアッププロトコルです。基盤となるネットワーク構成によっては、使用状況によって、設定された帯域幅よりも高い帯域幅が報告される場合があります。



パス・マッピングと帯域幅の使用率の向上

May 10, 2021

[Monitoring] タブでは、パスマッピングと帯域幅使用率の拡張が実装され、トラフィックフローが表示されます。たとえば、1 つの仮想パスだけがネットワーク接続を提供していて、その仮想パスが非アクティブになると、新しい最適パスが選択され、最初のパスが最後の最適パスになります。このシナリオは、帯域幅の需要が少なく、パスが 1 つしか選択されていない場合に実装されます。

複数の仮想パスが 1 つの接続を提供している場合、1 つの現在の最適パスと次の最適パス (使用可能な場合) が表示されます。トラフィックを処理するパスが 1 つだけ存在する場合、トラフィックを処理するパスが 3 つ以上存在し、パスステابلが 2 つのパスで更新されている場合、フローの SD-WAN GUI の [Monitoring] タブには、現在の最適パスが最初のパスとして表示され、次のカンマで区切られたパスが最後の最適パスとして表示されます。このシナリオは、帯域幅を必要とするパスを増やす必要がある場合に実装されます。

SD-WAN GUI による DPI アプリケーション情報の監視

モニタリングフローの DPI アプリケーションオブジェクト名は、SD-WAN GUI モニタリング -> フロー ページに格納され、表示されます。DPI アプリケーションを識別するためのツールチップが表示されます。

Statistics

Flows

Routing Protocols

Firewall

IKE/IPsec

IGMP

Performance Reports

Qos Reports

Usage Reports

Availability Reports

Appliance Reports

DHCP Server/Relay

+ WAN Optimization

Monitoring > Flows

Select Flows

Flow Type: ☒ LAN to WAN ☒ WAN to LAN ☐ Internet Load Balancing Table ☐ TCP Termination Table

Max Flows to Display (Per Flow Type): 50

Filter (Optional): [Help](#)

Refresh

Flows Data

Both LAN to WAN and WAN to LAN Flows

Source IP Address	Dest IP Address	Direction	Source Port	Dest Port	IPP	IP DSCP	Hit Count	Service Type	Service Name	LAN GW IP	Age (mS)	Packets	Bytes	PPS	Customer kbps	Virtu Path Overhe kbps
172.16.14.99	172.16.19.167	LAN to WAN	80	2189	TCP	default	41572	Virtual Path	DC-BR	LOCAL	758	41571	14527110	2.072	6.337	0.8
172.16.14.99	172.16.19.162	LAN to WAN	80	3161	TCP	Override = NO Demote on Large Packets = NO Separate TCP ACK Class = NO Packet Sequence Inorder = YES Inorder Holdtime: 900 Late Packet Action = DISCARD					361	41525	14427708	2.099	6.488	0.5
172.16.14.99	172.16.19.161	LAN to WAN	80	6310	TCP						60	41827	14468200	2.115	6.341	0.5
172.16.14.99	172.16.19.170	LAN to WAN	80	10844	TCP						360	41863	14393387	2.110	6.285	0.5

Availability Reports

Appliance Reports

DHCP Server/Relay

+ WAN Optimization

Both LAN to WAN and WAN to LAN Flows

Toggle Columns

Source IP Address	Dest IP Address	Direction	Source Port	Dest Port	IPP	IP DSCP	Hit Count	Service Type	Service Name	LAN GW IP	Age (mS)	Packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps
172.16.14.99	172.16.19.167	LAN to WAN	80	2189	TCP	default	41572	Virtual Path	DC-BR	LOCAL	758	41571	14527110	2.072	6.337	0.6
172.16.14.99	172.16.19.162	LAN to WAN	80	3161	TCP	Override = NO Demote on Large Packets = NO Separate TCP ACK Class = NO Packet Sequence Inorder = YES Inorder Holdtime: 900 Late Packet Action = DISCARD					361	41525	14427708	2.099	6.488	0.6
172.16.14.99	172.16.19.161	LAN to WAN	80	6310	TCP	Persistent Paths = NO					60	41827	14468200	2.115	6.341	0.6
172.16.14.99	172.16.19.170	LAN to WAN	80	10844	TCP	Reliable = YES					360	41863	14393387	2.110	6.285	0.6
172.16.14.99	172.16.19.164	LAN to WAN	80	3387	TCP	TCP Standalone ACKs = NO Check Flow TOS = NO Deep Packet Inspection = NO IP,TCP,UDP Header Compression = NO GRE Header Compression = NO Packet Aggregation = NO TCP Termination = NO Rule ID = 1 VLAN ID = 0 App Rule ID = N/A					358	41798	14472656	2.070	6.284	0.6
172.16.14.215	172.16.19.99	LAN to WAN	9321	80	TCP						14	43483	2592802	2.145	1.022	0.6
172.16.14.99	172.16.19.167	LAN to WAN	80	4200	TCP						312	41705	14426227	2.114	6.348	0.6
172.16.14.99	172.16.19.169	LAN to WAN	80	3161	TCP						356	40970	14508376	2.054	6.299	0.6
172.16.14.218	172.16.19.99	LAN to WAN	3371	80	TCP						407	42980	2552820	2.043	0.967	0.6
172.16.14.99	172.16.19.166	LAN to WAN	80	1116	TCP						313	41286	14568312	2.047	6.220	0.6
172.16.14.213	172.16.19.99	LAN to WAN	17082	80	TCP						361	42915	2556999	2.114	1.006	0.6
172.16.14.217	172.16.19.99	LAN to WAN	4090	80	TCP	BPI Application = http					364	42530	2540882	2.059	0.983	0.6

SD-WAN GUI でのトラフィックフローのパス情報のモニタリング

帯域幅を要求する着信トラフィックレートに基づいて、トラフィックを処理するために 1 つ以上のパスが必要になることがあります。

パスマッピングの実行方法を決定するには、次のシナリオを確認してください。

負荷分散伝送モード：

次の図は、トラフィックが開始され、すべてのパスが良好である場合、帯域幅需要が 1 つのパスによって処理されるのに十分なので、最適なパスが 1 つ選択されるシナリオを示しています。 **DC-MCN-internet-> BR1-VPX-internet** のパスが **1** つだけ選択され、伝送タイプのタイプが **Load Balanced** と表示されます。

Select Flows

Flow Type:

☒ LAN to WAN

☒ WAN to LAN

☐ Internet Load Balancing Table

☐ TCP Termination Table

Max Flows to Display (Per Flow Type):

50

Filter (Optional):

Help

Refresh

Flows Data

Toggle Columns

Service Name	LAN GW IP	Age (mS)	Packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	App Rule ID	Class	Type	Path	Hdr Compression Saved Bytes	Transmission Type	Application
DC-MCN-BR1-VPX	LOCAL	3	291	435918	85.373	1023.106	36.881	0.000	52	N/A	15	BULK	DC-MCN-Internet->BR1-VPX-Internet	N/A	Load Balanced, Reliable	iperf

次の図は、トラフィックが流れていて、そのパスの WAN 属性が低下しているときに、中断せずにトラフィックを処理するために新しいパスが選択されていることを示しています。この場合、パスマッピング機能を使用すると、トラフィックを処理する現在の最適パスが **DC-MCN-Internet2-> BR1-VPX-Internet** であり、トラフィックを処理した最後の最適パスが **DC-MCN-internet-> BR1-VPX-Internet** であることを指定できます。

この例の最後の最適パスは、どのパスが以前に接続したかを示すインジケータです。

Select Flows

Flow Type:

☒ LAN to WAN☒ WAN to LAN☐ Internet Load Balancing Table☐ TCP Termination Table

Max Flows to Display

(Per Flow Type):

50

Filter (Optional):

Help

Refresh

Flows Data

Toggle Columns

ackets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	App Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type	Application
728	1090544	0.983	11.778	0.425	0.000	52	N/A	15	BULK	DC-MCN-Internet-2->BR1-VPX-Internet, DC-MCN-Internet->BR1-VPX-Internet	N/A	Load Balanced, Reliable	iperf

次の図は、トラフィックが継続中であり、帯域幅の需要によりトラフィック処理用に複数のパスが選択されている場合に、トラフィックの送信時に複数のパスが選択されていることを示しています。上記の場合とは異なり、ここではトラフィックを処理するパスが3つ以上ある場合がありますが、GUIでは現在トラフィックを処理している最適なパスが2つだけ表示されます。

DC-MCN-インターネット-> BR1-VPX-インターネット、DC-MCN-インターネット 2-> BR1-VPX-インターネットが、フローデータ テーブルに示されている2つのパスであることを確認します。

注

示されているように、フローテーブル内の最大2つのパスだけが表示されます。

Select Flows

Flow Type:

☒ LAN to WAN☒ WAN to LAN☐ Internet Load Balancing Table☐ TCP Termination Table

Max Flows to Display

(Per Flow Type):

50

Filter (Optional):

Help

Refresh

Flows Data

Toggle Columns

ets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	App Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type	Application
355	1280790	318.598	3818.082	137.634	0.000	52	N/A	15	BULK	DC-MCN-Internet->BR1-VPX-Internet, DC-MCN-Internet-2->BR1-VPX-Internet	N/A	Load Balanced, Reliable	iperf

次の図は、トラフィックが依然として流れているときに、**DC-MCN-Internet->BR1-VPX-Internet**である現在の最適パスがWAN アトリビュートで利用不可/非アクティブ/劣化している場合、選択された現在の最適パスが**Flows Data** テーブルのパスセクションで最初に表示されることを示しています。の後に、トラフィックを処理している最後の最適パスが続きます。

DC-MCN-インターネット->BR1-VPX-インターネット はもはや最適ではなかったので、新しい現在の最適パスが**DC-MCN-MPLS->BR1-VPX-MPLS**としてシステムによって選択されました。現在の最適パスとともにアクティブに接続を提供している最後の最適パスは、**DC-MCN-インターネット 2->BR1-VPX**です。両方のインターネットは、帯域幅の現在のトラフィック需要のために必要です。

Select Flows

Flow Type:

☒ LAN to WAN☒ WAN to LAN☐ Internet Load Balancing Table☐ TCP Termination Table

Max Flows to Display (Per Flow Type):

50

Filter (Optional):

Help

Refresh

Flows Data

Toggle Columns

packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	App Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type	Application
2764	4140472	170.434	2042.476	73.627	0.000	52	N/A	15	BULK	DC-MCN-MPLS->BR1-VPX-MPLS, DC-MCN-Internet-2->BR1-VPX-Internet	N/A	Load Balanced, Reliable	iperf

重複送信モード

一般的なパケット複製モードでは、2つのパスが同じ接続のパケットを処理するために最初に使用され、2つの別々のパス間でパケットを複製することによって信頼性の高い配信を保証します。

パスマッピングでは、フローテーブルの path セクションに2つのパスがある限り、複製によってフローを処理するパスが2つあることがわかります。

次の図は、wen トラフィックが流れていることを示しています。2つのパスがトラフィックを処理していることがわかります。他のモードとは異なり、トラフィックが1つのパスだけで提供できる帯域幅が少なくても、このモードは常に2つのパス間でトラフィックを複製し、信頼性の高いアプリケーション配信を実現します。

次の図では、[フローデータ] テーブルのパスセクションに2つのパス（**DC-MCN-Internet2-> BR-VPX-インターネット**、**DC-MCN-MPLS-> BR1-VPX-MPLS**）があります。

Select Flows

Flow Type:

☒ LAN to WAN☒ WAN to LAN☐ Internet Load Balancing Table☐ TCP Termination Table

Max Flows to Display (Per Flow Type):

50

Filter (Optional):

Help

Refresh

Flows Data

Toggle Columns

ie S)	Packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	App Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type	Application
3	551	32640	88.836	42.100	38.377	0.000	0	N/A	9	BULK	DC-MCN-Internet-2->BR1-VPX-Internet, DC-MCN-MPLS->BR1-VPX-MPLS	N/A	Duplicate, Reliable	iperf
4	1651	2362062	262.860	3008.560	113.555	0.000	72	N/A	N/A	N/A	N/A	N/A	Duplicate, Reliable	iperf

次の図は、トラフィックが流れているときに、現在の最適パスの1つが非アクティブになった場合に、別のパスが選択され、[**Flows Data**] テーブルのパスセクションの一部として2つのパスが残っていることを示しています。

Select Flows

Flow Type: ☒ LAN to WAN ☒ WAN to LAN ☐ Internet Load Balancing Table ☐ TCP Termination Table

Max Flows to Display (Per Flow Type): 50

Filter (Optional): [Help](#)

Refresh

Flows Data

Toggle Columns

IN IP	Age (mS)	Packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	App Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type
CAL	10	9692	530732	75.025	32.705	32.411	0.000	0	N/A	9	BULK	DC-MCN-MPLS->BR1-VPX-MPLS, DC-MCN-Internet->BR1-VPX-Internet	N/A	Duplicate, Reliable
CAL	0	34213	4905970	267.264	3066.058	115.458	0.000	72	N/A	N/A	N/A	N/A	N/A	Duplicate, Reliable

永続パス送信モード

永続パス送信モードは、パス遅延インピーダンスに基づいてフローのパケットを保持するのに役立ちます。

次の図は、フローとそのパケットを現在処理している最適なパスである 1 つのパスだけを示しています。帯域幅の需要はなく、1 つのパスがすべてを供給します。現在、**DC-MCN-インターネット->BR1-VPX-インターネット**である最適なパスは **1** だけです。

Flows Data

Toggle Columns

Service type	Service Name	LAN GW IP	Age (mS)	Packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	App Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type	Application
Local Path	DC-MCN-BR1-VPX	LOCAL	662	3	4494	1.127	13.511	0.487	0.000	4	N/A	9	BULK	DC-MCN-Internet->BR1-VPX-Internet	N/A	Persistent	iperf

次の図は、パス **DC-MCN-internet->BR1-VPX-internet** が遅延が発生しやすくなったり、無効になったりすると、新しいパスが有効になり、現在のパス **DC-MCN-internet->BR1-VPX-inter net** が最後の最適パスになることを示しています。

したがって、新しいパスセクションには、**DC-MCN-MPLS->BR1-VPX-MPLS**、**DC-MCN-インターネット->BR1-VPX-インターネット**が表示されます。

Flows Data

Toggle Columns

IN IP	Age (mS)	Packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	App Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type	Application
CAL	950	41	61418	0.992	11.894	0.429	0.000	4	N/A	9	BULK	DC-MCN-MPLS->BR1-VPX-MPLS, DC-MCN-Internet->BR1-VPX-Internet	N/A	Persistent	iperf

永続モードでは、トラフィックを処理するために複数のパスを選択することができます。この場合、GUI は、トラフィックフローの先頭からフローテーブルの path セクションに、ベストパスとネクストベストパスの両方を表示します。

次の図は、最初は 3 つ以上のパスしか必要とせず、パス遅延インピーダンスの交差 (50 ms) がない限り、フローは永続的であることを示しています。次の 2 つのパスは、**DC-MCN-インターネット->BR1-VPX-インターネット**、**DC-MCN-MPLS->BR1-VPX-MPLS** のように表示されます。

Flows Data

Toggle Columns

	Age (mS)	Packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	App Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type	Application
L	51	6368	367504	128.449	59.303	55.490	0.000	2	N/A	9	BULK	DC-MCN-Internet->BR1-VPX-Internet, DC-MCN-MPLS->BR1-VPX-MPLS	N/A	Persistent	iperf
L	1	9694	13894396	195.491	2241.576	84.452	0.000	74	N/A	N/A	N/A	N/A	N/A	Persistent	iperf

DC-MCN-internet の最良パスの 1 つが高遅延になるか、無効になっていると仮定します。これにより、新しいパスが表示され、その時点でのパス選択の決定に基づいて、新しいパスが最適パスになるか、2 番目の最適パスになることができます。

Flows Data														
Toggle Columns														
Age (mS)	Packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	App Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type	Application
2	79540	4709572	147.475	73.223	63.709	0.000	2	N/A	9	BULK	DC-MCN-MPLS->BR1-VPX-MPLS, DC-MCN-Internet-2->BR1-VPX-Internet	N/A	Persistent	iperf
0	119720	171655210	195.634	2233.531	84.514	0.000	74	N/A	N/A	N/A	N/A	N/A	Persistent	iperf

管理 IP のトラブルシューティング

May 10, 2021

DHCP IP アドレスを構成するときに発生する可能性のあるシナリオを次に示します。また、SD-WAN アプライアンスの展開時に DHCP 管理 IP アドレスを構成するためのベストプラクティスと推奨事項についても説明します。

これらの推奨事項は、SD-WAN のすべてのプラットフォームモデル（Standard Edition、WANOP、Premium (Enterprise) Edition（物理アプライアンスと仮想アプライアンス））に適用されます。

注

SD-WAN アプライアンスのすべてのハードウェアモデルには、工場出荷時のデフォルトの管理 IP アドレスが付属しています。セットアッププロセス中に、アプライアンスに必要な DHCP IP アドレスを設定してください。

SD-WAN アプライアンス（VPX モデル）および AWS 環境にデプロイできるアプライアンスのすべての仮想モデルには、工場出荷時のデフォルト IP アドレスが割り当てられていません。

DHCP サーバに到達できない状態でアプライアンスの電源を入れます。

- 原因:
 - イーサネット管理ケーブルが切断されている
 - 接続されているネットワークの DHCP サービスがダウンしています。
- 正常な動作
 - DHCP サービスを有効にしたアプライアンスは、300 秒ごとに DHCP 要求を再試行します（デフォルト値）。実際の間隔は約 7 分です

- したがって、DHCP サービスを有効にしたアプライアンスは、DHCP サーバーが使用可能になってから 7 分以内に DHCP アドレスを取得します。遅延の範囲は 0 ～7 分

割り当てられた **DHCP** アドレスの有効期限が切れます。

- 予想される動作:
 - DHCP サービスを有効にしたアプライアンスは、アドレスの有効期限が切れる前にリースの更新を試みます
 - アプライアンスは新しい DHCP 検出で開始します（更新に失敗した場合）

DHCP サービスが有効になっているアプライアンスは、**DHCP** が有効なサブネットから別のサブネットに移動します。

- 原因: アプライアンスが割り当てられた DHCP サブネットから別の DHCP サブネットに移動する
- 予想される動作:
 - 永続的なリースの DHCP IP アドレスの割り当てでは、新しい DHCP サーバから IP アドレスを取得するために、アプライアンスの再起動が必要になる場合があります。
 - DHCP リースの有効期限が切れると、現在の DHCP サーバーに到達できない場合、アプライアンスが DHCP 検出プロトコルを再開することがあります。
 - アプライアンスは、8 分の遅延で新しい IP アドレスを取得します。Gateway IP アドレスは、GUI および CLI では変更されません。再起動プロセスが完了した後に更新されます。

推奨:

- Citrix SD-WAN アプライアンス（物理/仮想）に割り当てられた DHCP アドレスには、常に永続的なリースを割り当てます。これにより、アプライアンスは予測可能な管理 IP アドレスを持つことができます。

セッションベースの **HTTP** 通知

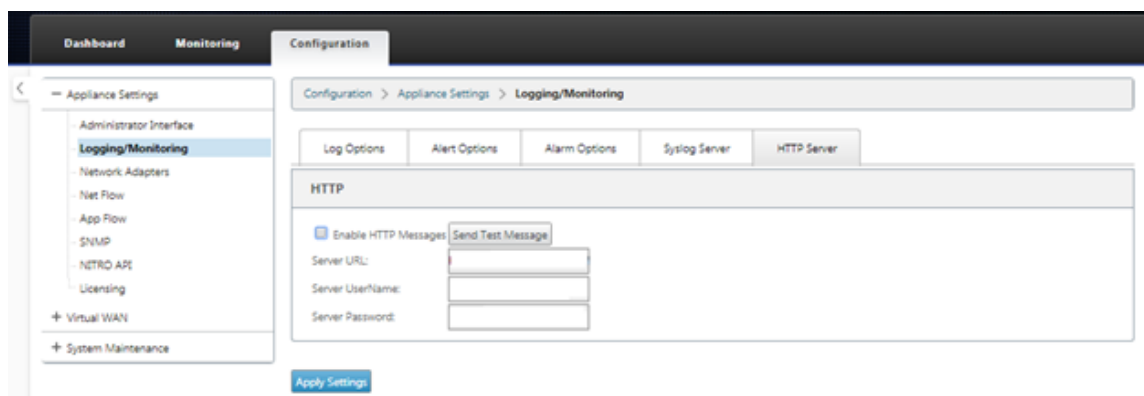
May 10, 2021

Citrix SD-WAN アプライアンスの GUI で、汎用 HTTP POST API サービス要求のイベントレポートとアラームレポートを構成できるようになりました。HTTP アラームおよびイベント通知の設定は、SD-WAN でサポートされるイベントおよびアラームの電子メールイベントおよび SNMP イベントに似ています。

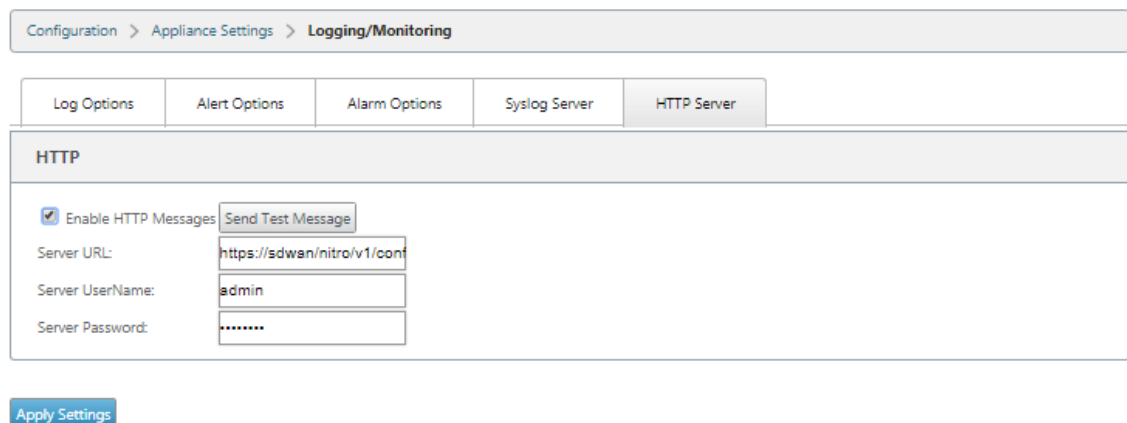
セッションベースの HTTP ポスト通知は、[Service Now] などの外部サービスに送信されます。HTTP サーバーのイベント通知は、Citrix SD-WAN アプライアンス GUI および Citrix SD-WAN Center で構成できます。

Citrix SD-WAN アプライアンス GUI で HTTP POST 通知を構成するには、以下の手順に従ってください。

1. [構成] > [ログ作成/監視] > [**HTTP** サーバー] に移動します。



2. [**HTTP** メッセージを有効にする] をクリックします。
3. 通知を受信する HTTP サーバのサーバ **URL** を入力します。サーバのユーザ名とサーバのパスワードを入力します。



4. [設定の適用] をクリックします。HTTP サーバー通知設定が適用されると、ページが更新されます。

注

[テストメッセージの送信] オプションを使用して、HTTP サーバー接続が成功したことを確認します。

HTTP サーバセッションにアラーム通知を追加するには、次の手順を実行します。

1. [ロギング/モニタリング] ページで、[アラームオプション] タブページに移動します。
2. [アラームの追加] をクリックします。

Configuration > Appliance Settings > Logging/Monitoring

Log Options | Alert Options | Alarm Options | Syslog Server | HTTP Server

Alarm Configuration

Add Alarm

Event Type	Trigger State	Trigger Duration (sec)	Clear State	Clear Duration (sec)	Severity	Email	Syslog
						<input type="checkbox"/>	<input type="checkbox"/>

Apply Settings

3. ドロップダウンリストから [イベントタイプ] を選択します。

Dashboard | Monitoring | Configuration

Appliance Settings

- Administrator Interface
- Logging/Monitoring
- Network Adapters
- Net Flow
- App Flow
- SNMP
- NITRO API
- Licensing
- + Virtual WAN
- + System Maintenance

Configuration > Appliance Settings > Logging/Monitoring

Log Options | Alert Options | Alarm Options | Syslog Server | HTTP Server

Alarm Configuration

Add Alarm

Event Type	Trigger State	Trigger Duration (sec)	Clear State	Clear Duration (sec)	Severity	Email	Syslog
						<input type="checkbox"/>	<input type="checkbox"/>

Apply Settings

4. 選択した イベントタイプについて、次のアラーム通知状態を選択します。トリガー状態とクリア状態は、選択したイベントタイプに応じて変化します。

- トリガー状態-GOOD, DISABLED, BAD, DEAD
- トリガー時間—秒単位の時間
- クリア状態 - GOOD, DISABLED, BAD, DEAD
- クリア期間—秒単位の時間
- 重大度—デバッグ、情報、通知、警告、エラー、重大、イベント、緊急

Dashboard | Monitoring | Configuration

Appliance Settings

- Administrator Interface
- Logging/Monitoring
- Network Adapters
- Net Flow
- App Flow
- SNMP
- NITRO API
- Licensing
- + Virtual WAN
- + System Maintenance

Configuration > Appliance Settings > Logging/Monitoring

Log Options | Alert Options | Alarm Options | Syslog Server | HTTP Server

Alarm Configuration

Add Alarm

Event Type	Trigger State	Trigger Duration (sec)	Clear State	Clear Duration (sec)	Severity	Email	Syslog
VIRTUAL_PATH	GOOD	0	GOOD	0		<input type="checkbox"/>	<input type="checkbox"/>

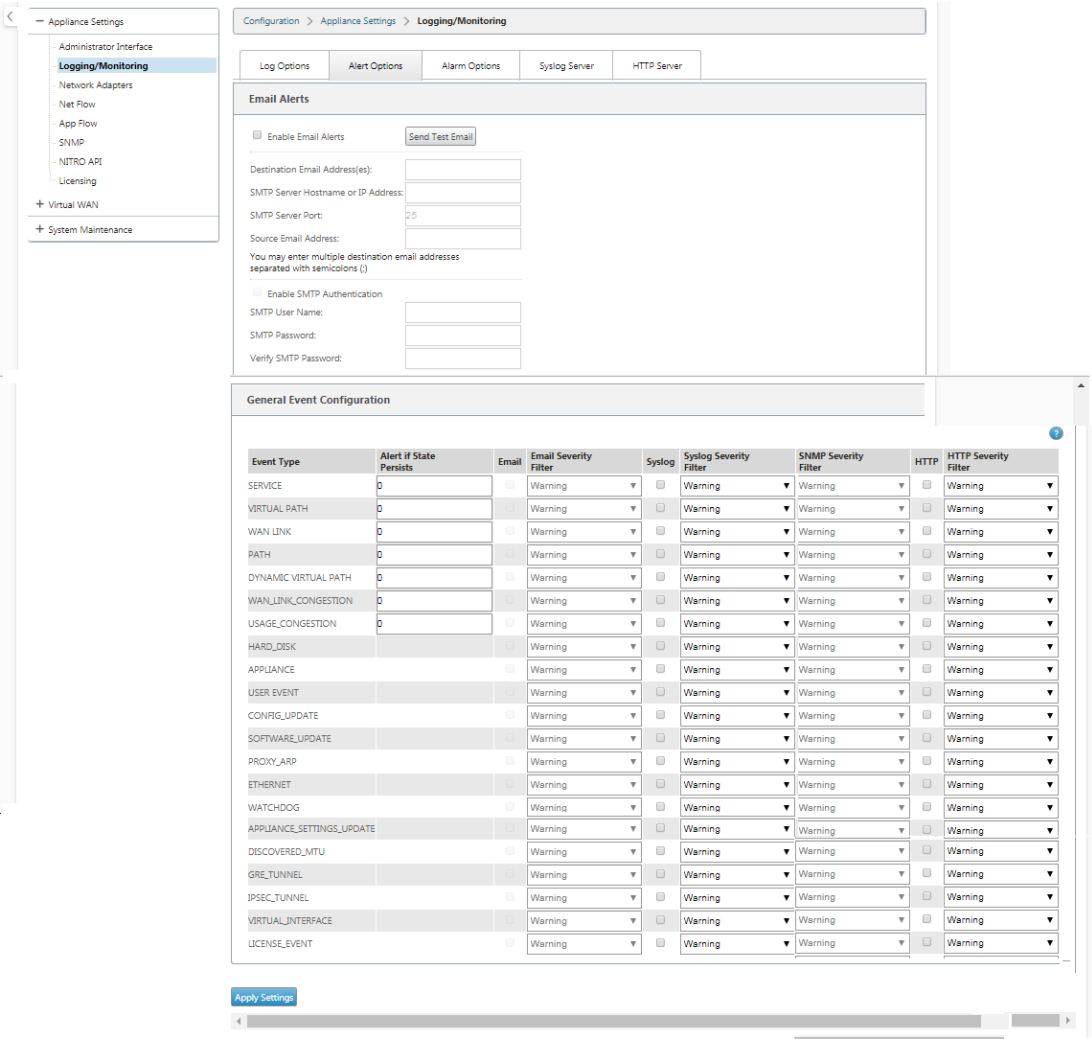
Apply Settings

5. **Syslog** および **HTTP** サーバイベントに固有の通知を受信するには、[Syslog] および [HTTP] チェックボックスをオンにします。[設定の適用] をクリックします。

イベント・オプションを構成するには、次の手順に従います。

[アラートオプション] タブ・ページに移動します。[一般的なイベント構成] ページで、イベントタイプの HTTP サーバー通知フィルタを選択し、[設定の適用] をクリックします。

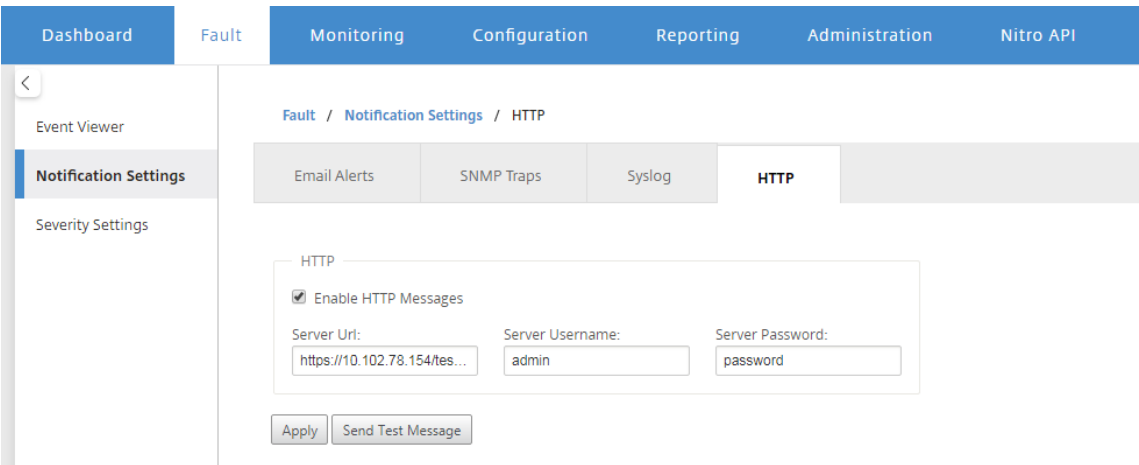
- HTTP
- HTTP 重大度フィルタ



Citrix SD-WAN Center で HTTP 通知を構成する

HTTP 通知を構成するには、次の手順を実行します。

1. [障害] > [通知設定] > [HTTP] に移動します。



2. HTTP サーバのサーバ **URL**、サーバユーザ名、サーバパスワード を入力します。
3. [適用] をクリックします。

重大度設定を構成するには、次の手順に従います。

1. 重大度の設定 ページに移動します。[**Enable**] をクリックして、選択したイベントタイプの HTTP 通知の監視を開始します。

		Email		Syslog		SNMP		HTTP	
Event Type	Alert if State Persists	Enable	Severity Filter	Enable	Severity Filter	Enable	Severity Filter	Enable	Severity Filter
SERVICE	Alert Immediately ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
VIRTUAL PATH	Alert Immediately ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
WANLINK	Alert Immediately ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
PATH	Alert Immediately ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
DYNAMIC VIRTUAL PATH	Alert Immediately ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
WAN LINK CONGESTION	Alert Immediately ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
USAGE CONGESTION	Alert Immediately ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼

Enable sending event notifications via HTTP Notifications for the current Event Type.

2. 次のイベントタイプについて、電子メール、Syslog、SNMP、および HTTP イベント通知を監視するように選択できます。[適用] をクリックします。

Dashboard

Fault

Monitoring

Configuration

Reporting

Administration

Nitro API

<

Event Viewer

Notification Settings

Severity Settings

Fault / Severity Settings

Event Type	Alert If State Persists	Email		Syslog		SNMP		HTTP	
		Enable	Severity Filter	Enable	Severity Filter	Enable	Severity Filter	Enable	Severity Filter
SERVICE	Alert Immediately ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
VIRTUAL PATH	Alert Immediately ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
WANLINK	Alert Immediately ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
PATH	Alert Immediately ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
DYNAMIC VIRTUAL PATH	Alert Immediately ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
WAN LINK CONGESTION	Alert Immediately ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
USAGE CONGESTION	Alert Immediately ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
HARD DISK		<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
APPLIANCE		<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
USER EVENT		<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
CONFIG UPDATE		<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
SOFTWARE UPDATE		<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
PROXY ARP		<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
ETHERNET		<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
WATCHDOG		<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
SD WAN CENTER SYSTEM		<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
APPLIANCE SETTINGS UPDATE		<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
SD WAN CENTER USER		<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
SD WAN CENTER STORAGE		<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
SD WAN CENTER DATABASE		<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
CONNECTION TO VIRTUAL WAN		<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
DISCOVERED MTU		<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
GRE TUNNEL		<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
IPSEC TUNNEL		<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
VIRTUAL INTERFACE		<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼
LICENSE EVENT		<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼	<input type="checkbox"/>	WARNING ▼

Apply

アクティブ帯域幅テスト

May 10, 2021

アクティブ帯域幅テストを使用すると、パブリックインターネット WAN リンクを介してインスタントパス帯域幅テストを発行したり、パブリックインターネット WAN リンク帯域幅テストを特定の時間に繰り返して完了するようにスケジュールしたりできます。この機能は、新規および既存のインストール中に 2 つのロケーション間で利用可能な

帯域幅の量を示す場合に便利です。また、DSCP タグ設定や帯域幅許可レートの調整など、設定および確認の変更の結果を判断するためのパスをテストする場合にも役立ちます。

アクティブ帯域幅テスト機能を使用するには、次の手順を実行します。

1. [システムメンテナンス] > [診断] > [パス帯域幅] に移動します。
2. 目的の パス を 選択し、[テスト] をクリックします。

The screenshot displays the Citrix SD-WAN Configuration > System Maintenance > Diagnostics > Path Bandwidth Testing interface. The sidebar on the left contains navigation options: Appliance Settings, Virtual WAN, System Maintenance, and Diagnostics (selected). The main panel is divided into several sections:

- Instant Path Bandwidth Testing:** A section for performing a single test. It includes a "Path:" dropdown menu with the selected path "MCN-5100-WL-2->BR572-1" and a "Test:" button.
- Results:** A section displaying the results of the instant test. It shows:
 - Minimum Bandwidth: 936564 kbps
 - Maximum Bandwidth: 1213863 kbps
 - Average Bandwidth: 1189846 kbps
- Schedule Path Bandwidth Testing:** A section for scheduling recurring tests. It includes an "Add" button and a table with columns: Path Name, Frequency, Day of Week, Hour, and Minute. An "Apply Settings" button is at the bottom.
- History Path Bandwidth Testing Result:** A section showing a table of test results. The table has columns: Num, From Link, To Link, Test Time, Min Bandwidth (kbps), Max Bandwidth (kbps), and Avg Bandwidth (kbps). The table displays 27 entries, with the first 26 entries showing results for the path "MCN-5100-WL-1" and the last entry showing results for the path "BR572-WL-1".

出力には、テストの WAN リンクの最小帯域幅および最大帯域幅結果の許可レートとして設定する値として使用された平均帯域幅が表示されます。帯域幅をテストする機能に加えて、学習した帯域幅を使用するように構成ファイルを変更できるようになりました。これは、[サイト] > [**WAN** リンク] [サイト名] > [WAN リンク名] [設定] の下にある [自動学習] オプションによって実現されます。有効にすると、システムは学習した帯域幅を使用します。

また、毎週、毎日、または毎時間の間隔で、パス帯域幅の繰り返しテストをスケジュールすることもできます。

Schedule Path Bandwidth Testing

Add

Path Name	Frequency	Day of Week	Hour	Minute	
DC_MPLS2->Branch_	every day	Sunday	0	0	X
	every day	Sunday	0	0	↶

Apply Settings

注

このページの下部にパス帯域幅テスト結果の履歴が表示され、結果は7日ごとにアーカイブされます。

Schedule Path Bandwidth Testing

Add

Path Name	Frequency	Day of Week	Hour	Minute	

Apply Settings

History Path Bandwidth Testing Result

show 50 entries Showing 1 to 14 of 14 entries Search

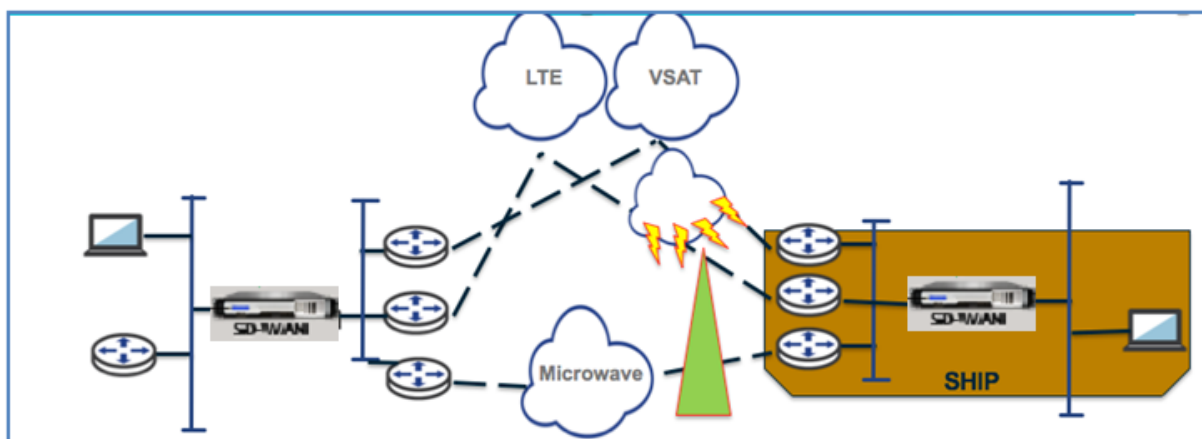
Num	From Link	To Link	Test Time	Min Bandwidth (kbps)	Max Bandwidth (kbps)	Avg Bandwidth (kbps)
1	BR_1-INET-1*	DC_MCN-INET-1	3/29/2017, 1:29:54 AM	363140	780616	525927
2	BR_1-INET-1*	DC_MCN-INET-1	3/29/2017, 1:30:00 AM	281995	573073	430345
3	BR_1-INET-1*	DC_MCN-INET-1	3/29/2017, 1:30:06 AM	317568	636640	480818
4	BR_1-MPLS-1	DC_MCN-MPLS-1	3/29/2017, 1:34:00 AM	440056	1083357	725514
5	DC_MCN-INET-1	BR_1-INET-1*	3/29/2017, 1:34:10 AM	506768	786784	638673
6	DC_MCN-INET-1	BR_1-INET-1*	3/29/2017, 1:34:18 AM	462584	1388712	669232
7	DC_MCN-INET-1	BR_1-WL-1	3/29/2017, 1:34:27 AM	380679	727895	533286
8	DC_MCN-MPLS-1	BR_1-MPLS-1	3/29/2017, 1:35:12 AM	26823	35495	30578
9	DC_MCN-INET-1	BR_1-INET-1*	3/29/2017, 1:36:09 AM	350097	733929	591542
10	DC_MCN-INET-1	BR_1-INET-1*	3/29/2017, 1:36:47 AM	476024	789756	639048
11	DC_MCN-INET-1	BR_1-WL-1	3/29/2017, 1:36:56 AM	446292	777674	608533

適応型帯域幅検出

May 10, 2021

この機能は、VSAT、LOS、マイクロ波、3G/4G/LTE WAN リンクを持つネットワークに適用できます。使用可能な帯域幅は、気象と大気の状態、場所、およびサイトの障害物によって異なります。これにより、SD-WAN アプライアンスは、定義された帯域幅範囲（最小および最大 WAN リンクレート）に基づいて WAN リンクの帯域幅レートを動的に調整し、パスに BAD マークを付けずに、使用可能な帯域幅の最大量を使用できます。

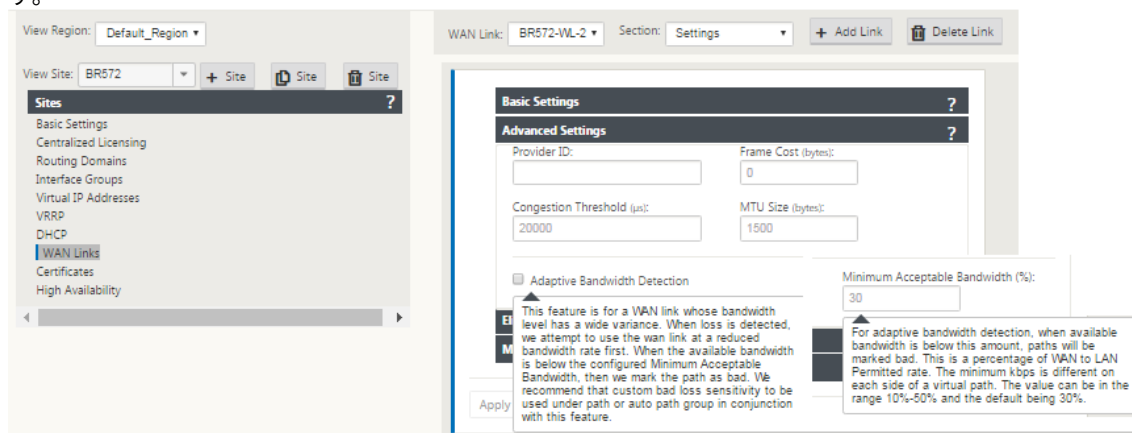
- 帯域幅の信頼性（VSAT 以上、マイクロ波、3G/4G、LTE 以上）
- ユーザーが構成した設定よりも適応型帯域幅の予測性が向上



適応型帯域幅検出を有効にするには、次の手順を実行します。

この機能を使用するには、前提条件として [Bad Loss sensitivity] オプションを有効にする必要があります (デフォルト/カスタム)。【グローバル】>【自動パスグループ】>【自動パスグループ名】>【不良ロスセンシティブ】で有効にすることができます。

1. 【グローバル】>【自動パスグループ】>【自動パスグループ名】>【不良ロスセンシティブ】で、【適応帯域幅検出】を有効にします。
2. 【構成エディタ】>【サイト】>【サイト名】>【WAN リンク】>【WAN リンク名】>【設定】>【詳細設定】に移動します。



3. 【適応帯域幅検出】チェックボックスをオンにし、【最小許容帯域幅】フィールドに値を入力します。
4. 【監視】>【統計】>【WAN リンク ** の使用状況】>【使用量と許可されたレート】の順に移動して、【使用 ** 量と許可されたレート】テーブルを表示します。

Usages and Permitted Rates

Filter: in Any column Apply

Show 100 entries Showing 1 to 4 of 4 entries

First Previous 1 Next Last

WAN Link	Service	Direction	Packets	Packets KB	Delta Packets	Delta KB	Kbps	Permitted Kbps	Congestion
BR1_VPX-WL-INET	MCN_VPX-BR1_VPX	Recv	5437658	3467411.62	0	0	0	25	NO
BR1_VPX-WL-INET	MCN_VPX-BR1_VPX	Send	7598365	559484464	118	8.39	12.69	5905	N/A
BR1_VPX-WL-MPLS	MCN_VPX-BR1_VPX	Recv	58537274	41745181.34	6562	5203.86	7872.71	8105	NO
BR1_VPX-WL-MPLS	MCN_VPX-BR1_VPX	Send	20640095	1497892080	229	17.25	26.1	5880	N/A

Showing 1 to 4 of 4 entries

First Previous 1 Next Last

ベストプラクティス

May 10, 2021

以下のトピックでは、ネットワークで Citrix SD-WAN ソリューションの設計、計画、実行を行う際に従うべきベストプラクティスを示します。

[セキュリティ](#)

[ルーティング](#)

[QoS](#)

[WAN リンク](#)

セキュリティ

February 8, 2022

この記事では、Citrix SD-WAN ソリューションのセキュリティのベストプラクティスについて説明します。Citrix SD-WAN 展開に関する一般的なセキュリティガイダンスを提供します。

Citrix SD-WAN 展開のガイドライン

展開ライフサイクルを通じてセキュリティを維持するには、次のセキュリティを考慮することをお勧めします。

- 物理的セキュリティ
- アプライアンスのセキュリティ
- Network Security
- 管理と管理

物理的セキュリティ

セキュアサーバールームへの Citrix SD-WAN アプライアンスの展開-Citrix SD-WAN がインストールされているアプライアンスまたはサーバーは、セキュアなサーバールームまたは制限付きデータセンター施設に配置する必要があります。これにより、アプライアンスが不正アクセスから保護されます。少なくとも、アクセスは電子カードリーダーによって制御される必要があります。アプライアンスへのアクセスは、監査目的ですべてのアクティビティを継続的に記録する CCTV によって監視されます。侵入した場合、電子監視システムはセキュリティ担当者にアラームを送信してすぐに対応する必要があります。

フロントパネルとコンソールポートを不正アクセスから保護-物理キーのアクセス制御により、アプライアンスを大きなケージまたはラックに保護します。

電源の保護-アプライアンスが無停電電源装置で保護されていることを確認します。

アプライアンスセキュリティ

アプライアンスのセキュリティを確保するには、Citrix SD-WAN 仮想アプライアンス (VPX) をホストするサーバーのオペレーティングシステムを保護し、リモートソフトウェアアップデートを実行し、次の安全なライフサイクル管理方法を実行します。

- Citrix SD-WAN VPX アプライアンスをホストするサーバーのオペレーティングシステムの保護-Citrix SD-WAN VPX アプライアンスは、標準サーバー上で仮想アプライアンスとして実行されます。標準サーバーへのアクセスは、ロールベースのアクセス制御と強力なパスワード管理で保護する必要があります。また、オペレーティングシステムの最新のセキュリティパッチを使用してサーバーを定期的に更新し、サーバー上の最新のウイルス対策ソフトウェアを更新することをお勧めします。
- リモートソフトウェア更新の実行-すべてのセキュリティ更新プログラムをインストールして、既知の問題を解決します。サインアップして最新のセキュリティアラートを受け取るには、セキュリティ情報 Web ページを参照してください。
- Secure Lifecycle Management Practice に従う-RMA の再デプロイ時または開始時、機密データの廃棄時にアプライアンスを管理するには、アプライアンスから永続データを削除してデータ追従対策を完了します。
- DMZ の背後にアプライアンスの管理インターフェイスを展開し、管理インターフェイスへの直接インターネットアクセスがないことを確認します。保護を強化するには、管理ネットワークがインターネットから隔離され、承認された管理アプリケーションを持つ承認されたユーザーだけがネットワーク内で実行されていることを確認します。

Network Security

ネットワークセキュリティのために、デフォルトの SSL 証明書は使用しないでください。管理者インターフェイスにアクセスするときはトランスポート層セキュリティ (TLS) を使用し、アプライアンスのルーティング不可能な管理 IP アドレスを保護し、高可用性セットアップを構成し、展開に適した管理と管理の保護手段を実装します。

- デフォルトの SSL 証明書を使用しない-信頼できる認証局からの SSL 証明書を使用すると、インターネットに直接接続する Web アプリケーションのユーザーエクスペリエンスを簡素化できます。自己署名証明書や評判の良い証明機関からの証明書の場合とは異なり、Web ブラウザーでは、Web サーバーへの安全な通信を開始するために、ユーザーは評判の良い証明機関からの証明書をインストールする必要はありません。
- 管理者インターフェイスにアクセスするときにトランスポート層セキュリティを使用する-管理 IP アドレスがインターネットからアクセスできないか、少なくともセキュリティで保護されたファイアウォールで保護されていることを確認してください。LOM IP アドレスがインターネットからアクセスできないか、少なくともセキュリティで保護されたファイアウォールで保護されていることを確認してください。
- 管理アカウントと管理アカウントの保護—別の管理者アカウントを作成し、管理者アカウントとビューアのアカウントに強力なパスワードを設定します。リモートアカウントアクセスを設定する場合は、RADIUS および TACAS を使用してアカウントの外部認証管理を設定することを検討してください。admin ユーザーアカウントのデフォルトパスワードの変更、NTP の設定、デフォルトのセッションタイムアウト値の使用、SNMPv3 と SHA 認証および AES 暗号化を使用します。

Citrix SD-WAN オーバーレイネットワークは、SD-WAN オーバーレイネットワークを通過するデータを保護します。

セキュアな管理者インターフェイス

安全な Web 管理アクセスを実現するには、信頼できる認証局から証明書をアップロードおよびインストールして、デフォルトのシステム証明書を置き換えます。**SD-WAN** アプライアンスの **GUI** で、**[構成] > [アプライアンスの設定] > [管理者インターフェイス]** に移動します。

ユーザーアカウント:

- ローカルユーザーパスワードの変更
- ユーザーの管理

HTTPS 証明書:

- 証明書
- キー

その他:

- Web コンソールのタイムアウト

The screenshot displays the Citrix SD-WAN 11.4 Administrator Interface. On the left is a navigation pane with a tree view containing: Appliance Settings, Administrator Interface (selected), Logging/Monitoring, Network Adapters, Net Flow, App Flow, SNMP, NITRO API, Licensing, + Virtual WAN, and + System Maintenance. The main content area is titled 'Configuration > Appliance Settings > Administrator Interface'. It features a tabbed interface with tabs for User Accounts, RADIUS, TACACS+, HTTPS Cert (active), HTTPS Settings, and Miscellaneous. The 'Installed Certificate' section shows two columns: 'Issued to:' and 'Issuer:'. Both columns list the same information: Country: US, State/Province: California, Locality: San Jose, Organization: Citrix Systems, Inc., Organizational Unit: Engineering, Common Name: Citrix, and Email: support@citrix.com. Below this is the 'Certificate Details' section, which includes the Certificate Fingerprint (24:8F:11:86:0F:32:AE:6A:D4:86:32:E3:F7:C3:D3:9B:30:51:A2:D5), Start Date (Mar 20 03:35:15 2017 GMT), End Date (Mar 18 03:35:15 2027 GMT), and Serial Number (C5586E258899CF6). The 'Upload HTTPS Certificate Files' section contains a note about the impact of uploading a certificate and fields for Certificate Filename and Key Filename, each with a 'Choose File' button and 'No file chosen' text. The 'Regenerate HTTPS Certificate' section contains a similar note and a 'Regenerate HTTPS Certificate' button.

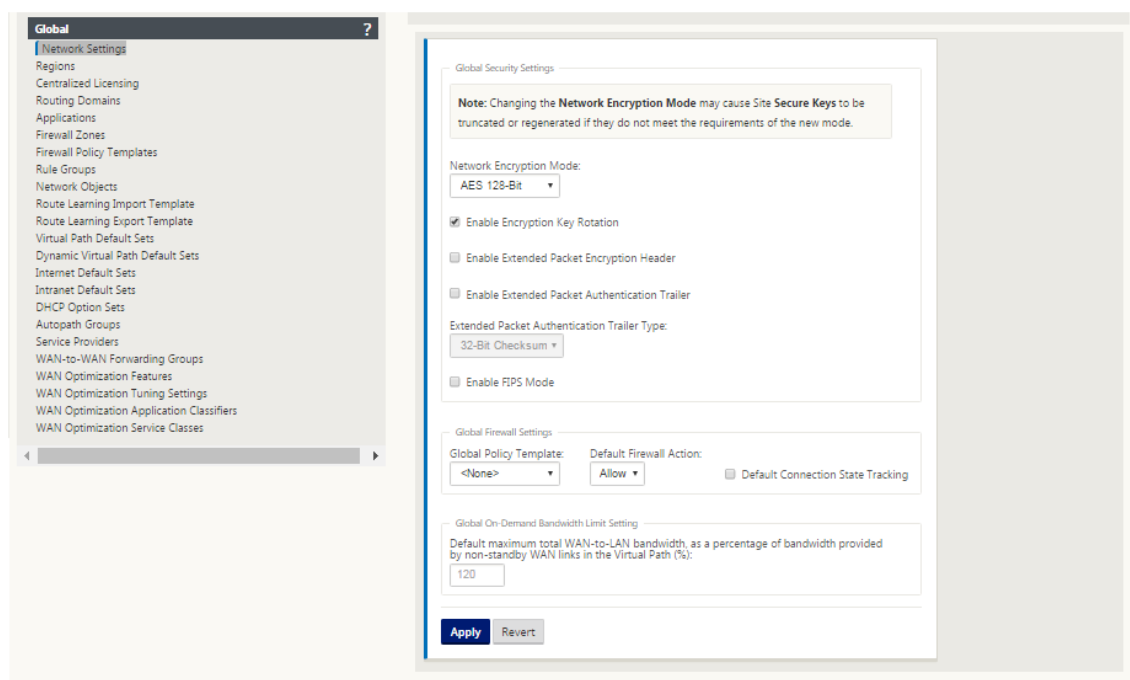
設定エディタ > グローバル > ネットワーク設定

グローバルファイアウォールの設定:

- グローバルポリシーテンプレート
- デフォルトのファイアウォールのアクション
- デフォルトの接続状態トラッキング

グローバル仮想パス暗号化設定:

- AES 128 ビット (デフォルト)
- 暗号化キーのローテーション (デフォルト)
- 拡張パケット暗号化ヘッダー
- 拡張パケット認証トレーラ



Citrix Web App Firewall 使用を検討する

Citrix ADC ライセンスアプライアンスは、ポジティブセキュリティモデルを使用し、コマンドインジェクション、SQL インジェクション、クロスサイトスクリプティングなどの脅威から保護するために、アプリケーションの適切な動作を自動的に学習する組み込みの Citrix Web App Firewall を提供します。

Citrix Web App Firewall を使用すると、ユーザーはコードを変更することなく、構成をほとんど変更することなく、Web アプリケーションにセキュリティを強化できます。詳しくは、「[Citrix Web アプリケーションファイアウォールの概要](#)」を参照してください。

グローバル仮想パス暗号化設定

- AES-128 データ暗号化はデフォルトで有効になっています。パス暗号化には、AES-128 以上の保護を使用して AES-256 暗号化レベルを使用することを推奨します。「Enable Encrypted Key Rotation」が設定されており、楕円曲線 Diffie-Hellman 鍵交換を使用して、暗号化が有効になっているすべての仮想パスに対して鍵の再生成が 10 ～15 分間隔で行われるようにします。

ネットワークで機密性（つまりタンパープロテクション）に加えてメッセージ認証が必要な場合は、IPsec データ暗号化することをお勧めします。機密性のみが必要な場合は、拡張ヘッダーを使用することをお勧めします。

- Extended Packet Encryption Header を使用すると、暗号化されたメッセージの先頭にランダムにシードされたカウンタを追加できるようになります。暗号化されると、このカウンタはランダムな初期化ベクトルとして機能し、暗号化キーでのみ決定論的です。これにより、暗号化の出力がランダム化され、区別がつかない

ほど強力なメッセージが出力されます。このオプションを有効にすると、パケットのオーバーヘッドが 16 バイト増加することに注意してください。

- 拡張パケット認証トレーラーは、暗号化されたすべてのメッセージの最後に認証コードを追加します。このトレーラーを使用すると、パケットが転送中に変更されていないことを確認できます。このオプションでは、パケットのオーバーヘッドが増加することに注意してください。

ファイアウォールのセキュリティ

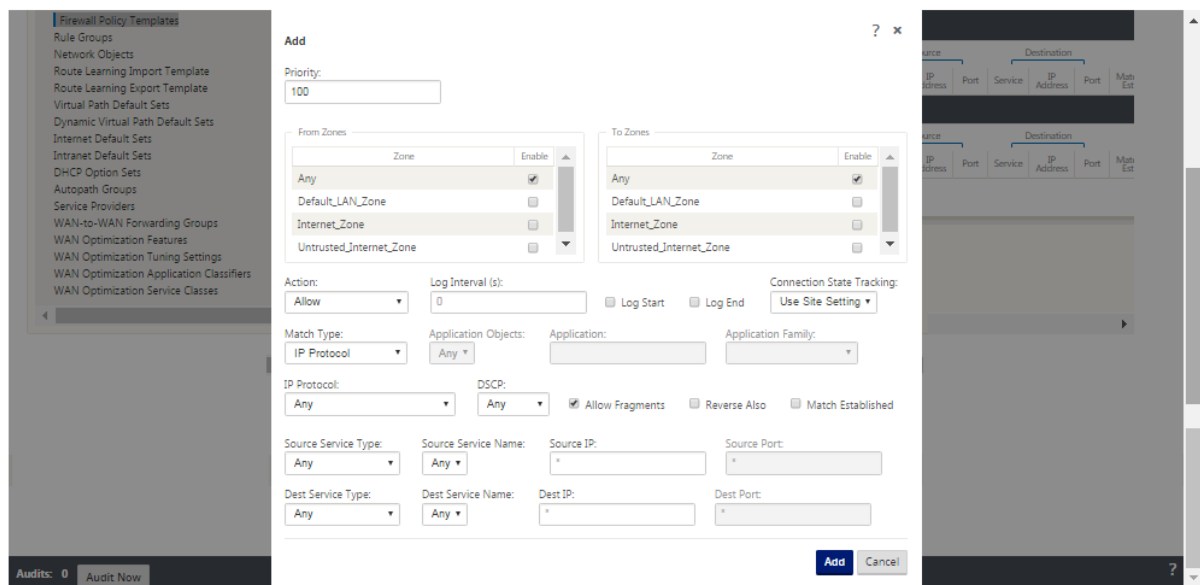
推奨されるファイアウォールの構成では、まず「すべて拒否」というデフォルトのファイアウォールアクションが使用され、次に例外が追加されます。ルールを追加する前に、ファイアウォールルールの目的を文書化および確認します。可能な場合は、ステートフル検査とアプリケーションレベル検査を使用します。ルールを簡素化し、冗長なルールを排除します。ファイアウォール設定の変更を追跡して確認できる変更管理プロセスを定義し、遵守します。グローバル設定を使用してアプライアンスを経由する接続を追跡するように、すべてのアプライアンスのファイアウォールを設定します。接続のトラッキングは、パケットが適切に形成され、接続状態に適していることを確認します。組織のネットワークまたは機能領域の論理階層に適したゾーンを作成します。ゾーンは世界的に重要であり、地理的に異なるネットワークを同じセキュリティゾーンとして扱うことができることに注意してください。セキュリティホールリスクを軽減する最も具体的なポリシーを作成し、許可ルールで [Any] を使用しないようにします。グローバルポリシーテンプレートを設定および管理して、ネットワーク内のすべてのアプライアンスの基本レベルのセキュリティレベルを作成します。ネットワーク内のアプライアンスの機能的役割に基づいてポリシーテンプレートを定義し、必要に応じて適用します。必要な場合のみ、個々のサイトでポリシーを定義します。

グローバルファイアウォールテンプレート - ファイアウォールテンプレートを使用すると、SD-WAN オーバーレイ環境で動作する個々のアプライアンスのファイアウォールの動作に影響を与えるグローバルパラメータを設定できます。

デフォルトのファイアウォールアクション - 許可を有効にすると、どのフィルタポリシーにも一致しないパケットが許可されます。Deny は、どのフィルタポリシーにも一致しないパケットをドロップすることを有効にします。

【デフォルトの接続状態トラッキング (Default Connection State Tracking)】: フィルタポリシーまたは NAT ルールと一致しない TCP、UDP、および ICMP フローの双方向接続状態トラッキングを有効にします。非対称フローは、ファイアウォールポリシーが定義されていない場合でも、これを有効にすると、ブロックされます。この設定は、グローバル設定よりも優先されるサイトレベルで定義できます。サイトで非対称フローが発生する可能性がある場合は、グローバルではなくサイトまたはポリシーレベルでこれを有効にすることをお勧めします。

ゾーン - ファイアウォールゾーンは、Citrix SD-WAN に接続されているネットワークの論理的なセキュリティグループを定義します。ゾーンは、仮想インターフェイス、イントラネットサービス、GRE トンネル、および LAN IPsec トンネルに適用できます。



WAN リンクセキュリティゾーン

信頼できないセキュリティゾーンは、パブリック (セキュリティで保護されていない) ネットワークに直接接続された WAN リンクで構成する必要があります。Untrusted は、WAN リンクを最も安全な状態に設定し、インターフェイスグループで暗号化、認証、および許可されたトラフィックだけを許可します。仮想 IP アドレスへの ARP および ICMP は、他に許可されるトラフィックタイプだけです。この設定により、暗号化されたトラフィックだけが、Interface グループに関連付けられたインターフェイスから送信されるようになります。

ルーティングドメイン

ルーティングドメインは、ネットワークトラフィックのセグメント化に使用される一連のルータを含むネットワークシステムです。新しく作成されたサイアーは、デフォルトのルーティングドメインに自動的に関連付けられます。

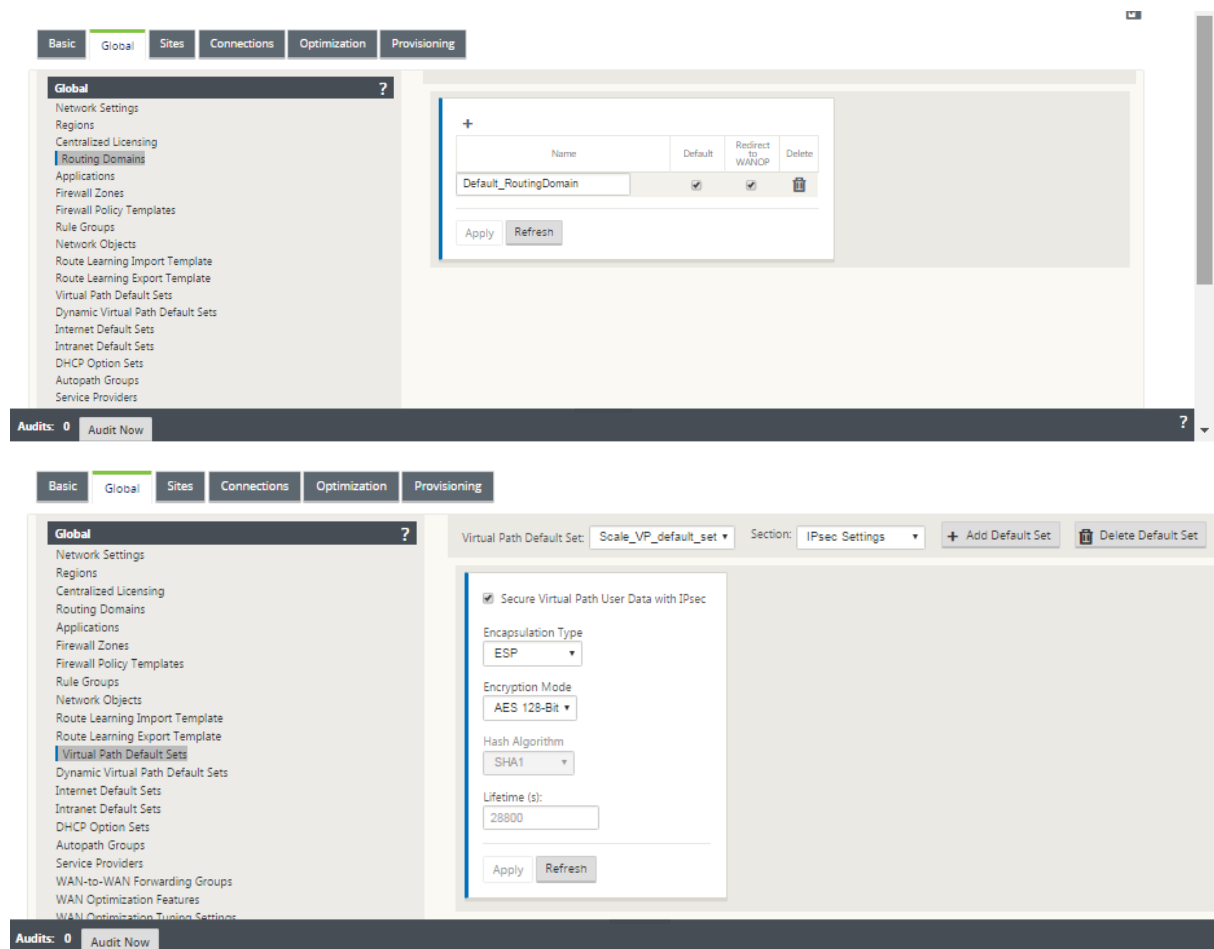
設定エディター > グローバル

ルーティングドメイン

- RoutingDomain

IPsec トンネル

- デフォルト・セット
- IPsec による仮想パスユーザーデータのセキュリティ保護



IPsec トンネル

IPsec トンネルは、ユーザデータとヘッダー情報の両方を保護します。Citrix SD-WAN アプライアンスは、LAN または WAN 側の固定 IPsec トンネルを非 SD-WAN ピアとネゴシエートできます。LAN 経由の IPsec トンネルでは、ルーティングドメインを選択する必要があります。IPsec トンネルがイントラネットサービスを使用する場合、ルーティングドメインは選択されたイントラネットサービスによって事前に決定されます。

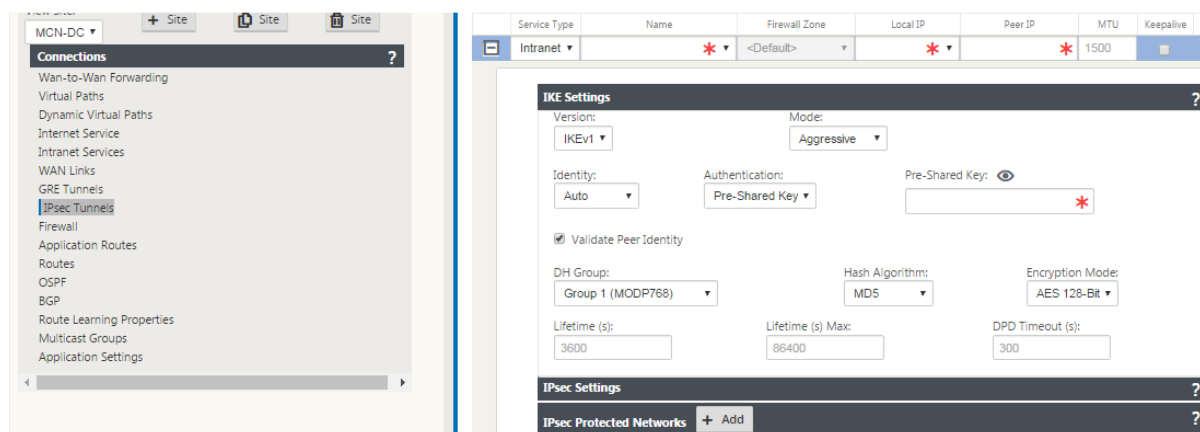
IPsec トンネルは、SD-WAN オーバーレイネットワークを介してデータが流れる前に仮想パス上に確立されます。

- [カプセル化タイプ] オプションには、ESP-データはカプセル化および暗号化、ESP+auth-データはカプセル化、暗号化、および HMAC で検証され、AH-データは HMAC で検証されます。
- 暗号化モードは、ESP が有効な場合に使用される暗号化アルゴリズムです。
- ハッシュアルゴリズムは、HMAC を生成するために使用されます。
- ライフタイムは、IPsec セキュリティアソシエーションが存在する場合に推奨される期間（秒単位）です。0 は無制限に使用できます。

IKE 設定

インターネットキーエクスチェンジ (IKE) は、セキュリティアソシエーション (SA) の作成に使用される IPSec プロトコルです。Citrix SD-WAN アプライアンスは、IKEv1 と IKEv2 の両方のプロトコルをサポートします。

- モードは、メインモードまたはアグレッシブモードのいずれかです。
- ID は、ピアを識別するために自動的に指定することも、IP アドレスを使用してピアの IP アドレスを手動で指定することもできます。
- 認証では、認証方法として事前共有キー認証または証明書が有効になります。
- [ピア ID の検証] は、ピアの ID タイプがサポートされている場合に IKE のピア ID の検証を有効にします。サポートされていない場合は、この機能を有効にしないでください。
- Diffie-Hellman グループは、グループ 1 が 768 ビット、グループ 2 が 1024 ビット、グループ 5 が 1536 ビットグループで IKE キー生成に使用できます。
- ハッシュアルゴリズムには、MD5、SHA1、および SHA-256 には、IKE メッセージ用のアルゴリズムが用意されています。
- 暗号化モードには、IKE メッセージに対して AES-128、AES-192、および AES-256 暗号化モードがあります。
- IKEv2 の設定には、ピア認証と整合性アルゴリズムが含まれます。



ファイアウォールの設定

アップストリームのルータとファイアウォールの設定を確認することで、次の一般的な問題を特定できます。

- MPLS キュー/QoS 設定: SD-WAN 仮想 IP アドレス間の UDP カプセル化トラフィックが、ネットワークの中間アプライアンスの **QoS** 設定によって影響を受けないことを確認します。
- SD-WAN ネットワーク上に構成された WAN リンク上のすべてのトラフィックは、適切なサービスタイプ（仮想パス、インターネット、イントラネット、ローカル）を使用して Citrix SD-WAN アプライアンスによって処理される必要があります。
- トラフィックが Citrix SD-WAN アプライアンスをバイパスし、同じ基になるリンクを使用する必要がある場合は、SD-WAN トラフィックの適切な帯域幅予約をルーター上で行う必要があります。また、SD-WAN 構成

では、それに応じてリンク容量を設定する必要があります。

- 中間ルータ/ファイアウォールに UDP フラッディングや PPS の制限が適用されていないことを確認します。これにより、仮想パス（UDP カプセル化）を介して送信されるトラフィックが抑制されます。

ルーティング

May 10, 2021

この記事では、Citrix SD-WAN ソリューションのルーティングのベストプラクティスについて説明します。

インターネット/イントラネットルーティングサービス

インターネットサービスがインターネットにバインドされたトラフィックに対して構成されていない場合、ローカルルートまたはパススルー ルートのいずれかが Gateway ルータに到達するように構成されます。ルータは SD-WAN アプライアンスに設定された WAN リンクを使用し、リンクのオーバーサブスクリプションの問題につながります。

MCN でインターネットルートが **Local** として設定されている場合、すべてのブランチ SD-WAN サイトで学習され、デフォルトで仮想パスルートとして設定されます。これは、ブランチアプライアンスでインターネットにバインドされたトラフィックが、仮想パスを経由して MCN にルーティングされることを意味します。

ルーティングの優先順位

ルーティングの優先順位：

- プレフィックス一致：最長プレフィックス一致。
- サービス: ローカル、仮想パスサービス、インターネット、イントラネット、パススルー
- ルートコスト

ルーティングの非対称性

ネットワークにルーティングの非対称性がないことを確認します（NetScaler SD-WAN アプライアンスがトラフィックを一方向のみ送信しています）。これにより、ファイアウォールの接続追跡とディープパケットインスペクションで問題が発生します。

QoS

June 8, 2022

QoS を設定する場合は、次の点を考慮してください。

- ネットワークトラフィックのパターンと要件を理解します。QoS 統計情報に示すように、テールドロップを回避するために、**QoS** クラスの統計情報を確認し、キューの深度を変更したり、デフォルトの QoS クラスシェアの割合を変更したりする必要がある場合があります。
- 場合によっては、特定のアプリケーション IP アドレス用のルールを作成する代わりに、設定を簡単にするためにサブネット全体がルールに追加されることがあります。サブネット全体をルールに追加すると、サブネット内のすべてのトラフィックが 1 つのルールに誤ってマッピングされます。したがって、そのルールに関連付けられた QoS クラスによって、テールドロップが発生し、アプリケーションのパフォーマンスやユーザーエクスペリエンスが低下する可能性があります。

WAN リンク

May 10, 2021

Citrix SD-WAN プラットフォームは、最大 8 つのパブリックインターネット接続と 32 のプライベート MPLS 接続をサポートします。この記事では、Citrix SD-WAN ソリューションの WAN リンク構成のベストプラクティスについて説明します。

WAN リンクの設定時に覚えておくべきポイント

- 実際の WAN リンク帯域幅として、許可レートと物理 レートを設定します。WAN リンク容量全体が SD-WAN アプライアンスによって使用されることが想定されていない場合は、それに応じて 許可 レートを変更します。
- 帯域幅が不明な場合、およびリンクが信頼できない場合には、**Auto Learn** 機能を有効にできます。自動学習機能は、基礎となるリンク容量だけを学習し、今後同じ値を使用します。
- 基になるリンクが安定しておらず、固定帯域幅（4G リンクなど）を保証しない場合は、適応型帯域幅検出 機能を使用します。
- 同じ WAN リンク上で、自動学習 と 適応帯域幅検出 を有効にすることは推奨されません。
- すべての WAN リンクの入力/出力物理レートを使用して MCN/RCN を手動で設定します。これは、MCN/RCN が複数のブランチ間の帯域幅分散の中心的なポイントであるためです。
- 重要なデータセンターのワークロード/サービスの信頼性を高めるために、自動学習を使用しない場合は、容量がランダムに変化しない SLA との信頼性の高いリンクを使用します。
- 基になるリンクが安定していない場合は、次の [パス] 設定を変更します。
 - 損失の設定
 - 不安定性のセンシティブを無効にする
 - 沈黙の時間

- 診断ツールを使用して、リンクの正常性/容量を確認します。
- SD-WAN がワンアーム モードで配置されている場合は、基礎となるリンクの物理容量を超過しないようにしてください。

ISP リンクのヘルスの確認

新しい展開の場合、SD-WAN 展開より前で、既存の SD-WAN 展開に新しい ISP リンクを追加する場合、次の手順を実行します。

- リンクタイプを確認します。たとえば、MPLS、ADSL、4G。
- ネットワーク特性たとえば、帯域幅、損失、遅延、ジッタなどです。

この情報は、要件に従って SD-WAN ネットワークを構成するのに役立ちます。

ネットワークポロジ

通常、特定のネットワークトラフィックは Citrix SD-WAN アプライアンスをバイパスし、SD-WAN ネットワークで構成されているのと同じ基になるリンクを使用することが観察されます。SD-WAN では、リンク使用率を完全に可視化できないため、SD-WAN がリンクをオーバーサブスクライブし、パフォーマンスと PATH の問題が発生する可能性があります。

プロビジョニング

SD-WAN の Provisioning 時に考慮すべきポイント

- デフォルトでは、すべてのブランチと WAN サービス (仮想パス/インターネット/イントラネット) は、同じ帯域幅のシェアを受け取ります。
- 接続するサイト間の帯域幅要件または可用性の面で大きな格差がある場合、プロビジョニングサイトを変更する必要があります。
- 使用可能な最大サイト間で動的仮想パスを有効にすると、DC への静的仮想パスと動的仮想パスの間で WAN リンク容量が共有されます。

よくあるご質問

May 10, 2021

高可用性

高可用性アプライアンスとセカンダリ (Geo) アプライアンスの違いは何ですか。

- 高可用性は、フォールトトレランスを保証しますセカンダリ (Geo) アプライアンスにより、ディザスタリカバリが可能になります。
- 高可用性は、MCN、RCN、およびブランチアプライアンスに対して設定できます。セカンダリ (Geo) アプライアンスは、MCN および RCN に対してのみ構成できます。
- 高可用性アプライアンスは、同じサイトまたは地理的な場所内で構成されます。地理的に異なる場所にあるブランチアプライアンスは、セカンダリ (Geo) MCN/RCN アプライアンスとして設定されます。
- 高可用性のプライマリアプライアンスとセカンダリアプライアンスは、同じプラットフォームモデルである必要があります。セカンダリ (Geo) アプライアンスは、プライマリ MCN/RCN と同じプラットフォームモデルである場合とそうでない場合があります。
- 高可用性は、セカンダリ (Geo) よりも高い優先順位です。アプライアンス (MCN/RCN) が高可用性およびセカンダリ (Geo) アプライアンスで構成されている場合、アプライアンスに障害が発生すると、セカンダリ高可用性アプライアンスがアクティブになります。両方の高可用性アプライアンスに障害が発生した場合や、データセンターサイトがクラッシュした場合は、セカンダリ (Geo) アプライアンスがアクティブになります。
- 高可用性では、プライマリ/セカンダリスイッチオーバーは、高可用性の展開に応じて、即座に、または 10 ～ 12 秒以内に発生します。プライマリ MCN/RCN からセカンダリ (Geo) MCN/RCN へのスイッチオーバーは、プライマリが非アクティブ状態の 15 秒後に発生します。
- 高可用性設定では、プライマリ再要求を設定できます。セカンダリ (Geo) アプライアンスのプライマリ再要求を設定することはできません。プライマリ再要求は、プライマリアプライアンスが戻り、ホールドタイマーが期限切れになると、自動的に行われます。

シングルステップアップグレード

注

WANOP、SVM、および XenServer サブリメンタル/HF は、OS コンポーネントとして表示されます。

現在のバージョン (8.1.x、9.1.x、9.2.x) から 9.3.x にアップグレードするには、*.tar.gz*** を使用するか、*.zip* パッケージをシングルステップアップグレードする必要がありますか？

関連するプラットフォームの *.tar.gz* ファイルを使用して、SD-WAN ソフトウェアを 9.3.x にアップグレードします。SD-WAN ソフトウェアを 9.3.x バージョンにアップグレードしたら、*.zip* パッケージを使用して変更管理を実行し、OS コンポーネントソフトウェアパッケージを転送またはステージングします。アクティベーション後、MCN は関連するすべてのブランチの OS コンポーネントを転送/ステージングします。

シングルステップアップグレードパッケージ (.zip ファイル) を使用して 9.3.0 にアップグレードした後、実行する必要があります。各アプライアンスで *upg* アップグレードしますか？

いいえ。OS ソフトウェアの更新/アップグレードは、1 ステップのアップグレード *.zip* パッケージによって処理され、各サイトの変更管理設定に記載されているスケジュール詳細に従ってインストールされます。

9.3 より前のバージョンから 9.3.x にアップグレードするために、*.tar.gz*** に続いて *.zip* パッケージを使用する必要があるのはなぜですか？ また、9.3.x の *.zip* パッケージを直接使用しないのはなぜですか？

シングルステップアップグレードパッケージは 9.3.0.161 以降でサポートされており、以前のリリースバージョン (リリース 9.3 以前) では、このパッケージは認識されません。シングルステップアップグレード *.zip* パッケージが Change Management の受信トレイにアップロードされると、パッケージが認識されないことを示すエラーがスローされます。したがって、まず SD-WAN ソフトウェアを 9.3 以上のバージョンにアップグレードしてから、を使用して変更管理を実行します。 *.zip* パッケージ。

OS コンポーネントは、1 ステップアップグレードでどのようにインストールされるのですか？ *upg* のアップグレードが実行されませんか？

MCN は、シングルステップアップグレード *.zip* パッケージを使用して変更管理が完了した後、アプライアンスモデルに基づいて OS コンポーネントソフトウェアパッケージを転送またはステージングします。アクティベーション後、MCN は、スケジュールされた更新/アップグレードに必要なブランチの OS コンポーネントソフトウェアパッケージの転送/ステージングを開始します。

後でインストールするスケジュールを設定せずに、OS コンポーネントをインストールするにはどうすればよいですか？

OS コンポーネントをすぐにインストールするには、メンテナンスウィンドウ の値を「0」に設定します。

注

インストールは、メンテナンスウィンドウ の値が「0」に設定されている場合でも、サイトに必要なすべてのパッケージがアプライアンスで受信された場合にのみ開始されます。

インストールのスケジュール設定にはどのようなものがありますか？ スケジュール指示を使用して VW 単体でアップグレードすることはできますか？

スケジュールされたインストールは SD-WAN リリース 9.3 で導入され、OS コンポーネントにのみ適用され、VW ソフトウェアのアップグレードには適用されません。シングルステップアップグレードでは、OS コンポーネントのアップグレードを実行するために各アプライアンスにログインする必要はありません。スケジュールリングオプションを使用すると、VW ソフトウェアバージョンアップグレード以外の時間に OS コンポーネントのインストールをスケジュールできます。

[変更管理設定] ページのスケジュール情報が、既定でスケジュール日を過ぎているのはなぜですか？

「変更管理設定」ページには、デフォルトのスケジュール情報が表示されます。「開始」：「2016-05-21 21:20:00」、「ウィンドウ」：1、「繰り返し」：1、「単位」：「日」です。日付が過去の日付の場合、スケジュールされたインストールは、日付ではなく、メンテナンスウィンドウ、リピートウィンドウ、ユニットなどの時間およびその他のパラメータに基づきます。

デフォルトのスケジュールインストール日時は何に設定されていますか。汎用アプライアンスとローカルアプライアンスに依存していますか。

デフォルトでは、スケジュールの詳細が 21:20:00 に「2016-05-21」に設定されています (メンテナンス期間は 1 時間で、1 日ごとに繰り返されます)。この詳細は、ローカルアプライアンスサイトによって異なります。

メンテナンス/スケジュールされたウィンドウを待たずに、OS Components をすぐにインストールするにはどうすればよいですか？

「変更管理設定」ページで「メンテナンスウィンドウ」の値を「**0**」に設定します。これにより、スケジュールされたインストール時間が上書きされます。

現在のソフトウェアバージョンが 9.3.x 以降の場合、アップグレードに使用するパッケージはどれですか？

現在のソフトウェアバージョン 9.3.x 以上の場合、シングルステップアップグレード .zip パッケージを使用して、より高いバージョンにアップグレードします。

OS コンポーネントファイルはいつブランチに転送/ステージングされますか？

シングルステップアップグレード .zip パッケージを使用して Change Management を実行すると、アクティベーションが完了した後、OS コンポーネントファイルは関連するブランチに転送/ステージングされます。

どのアプライアンスが OS Components ファイルを受信するか、プラットフォームに依存するか、すべてのブランチがそれを受信しますか？

EE ライセンスで実行されている **SD-WAN-400、800、1000、2000 SE**、ベアメタル **SD-WAN-2100** などの Hypervisor ベースのアプライアンスは、アップグレードする OS コンポーネントを受け取ります。

スケジューリングはどのように機能しますか？

デフォルトでは、スケジューリングの詳細は 2016-05-21 21:20:00 に設定されています（メンテナンスウィンドウは 1 時間で、1 日ごとに繰り返されます）。リピート値が 1 日に設定され、メンテナンス期間を 1 時間とし、**2016-05-21** から **21:20:00**（ローカルアプライアンス時間）にインストールがトリガー/試行（新しいソフトウェアが利用できる場合）されます。

OS コンポーネントがアップグレードされたかどうかを知るにはどうすればよいですか？

[ステータス] 列には、緑色のチェックマークが表示されます。その上にカーソルを合わせると、「アップグレードは成功しました」というメッセージが表示されます。

RCN とそのブランチ用の OS コンポーネントのインストールをスケジュールするにはどうすればよいですか？

RCN のスケジューリングは、[MCN 変更管理設定] ページから実行されます。RCN ブランチの場合は、各 RCN にログインし、スケジュールの詳細を設定する必要があります。

スケジュールされたインストールのステータスはどこから入手できますか。

RCN のスケジュールされたインストールのステータスは、[MCN 変更管理設定] ページから取得できます。RCN ブランチの場合、ステータスを取得するには、各 RCN にログインする必要があります。

スケジュールされたインストールのステータスを取得するにはどうすればよいですか。

「変更管理設定」ページにある更新ボタンを使用して、MCN からステータスを取得し、デフォルトリージョンおよび RCN のブランチについては RCN からステータスを取得します。

Scheduling Information

Show100▼entries

Search:

Edit Selected

Refresh

<input type="checkbox"/>	Site Name ▲	Scheduling Information	Status	Edit
<input type="checkbox"/>	GeoMCNVPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
<input type="checkbox"/>	MCNVPXHA	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
<input type="checkbox"/>	MCNVPXHA(HA-Secondary)	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
<input type="checkbox"/>	RCN1BR11000	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
<input type="checkbox"/>	RCN1BR2VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
<input type="checkbox"/>	RCN1RCN	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
<input type="checkbox"/>	RCN2BR1VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
<input type="checkbox"/>	RCN2BR2VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
<input type="checkbox"/>	RCN2BR3VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
<input type="checkbox"/>	RCN2RCN	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
<input type="checkbox"/>	RCN2RCN(HA-Secondary)	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
<input type="checkbox"/>	RCN3BR1VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
<input type="checkbox"/>	RCN3BR2	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
<input type="checkbox"/>	RCN3BR2(HA-Secondary)	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
<input type="checkbox"/>	RCN3RCN2100	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
<input type="checkbox"/>	RCNDefaultBR1VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
<input type="checkbox"/>	RCNDefaultBR2VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		

Showing 1 to 17 of 17 entries

Previous1Next

以前のソフトウェアアップグレードでシングルステップアップグレードが使用されたときに、tar.gz ファイルを使用して次のリリースにアップグレードできますか。

tar.gz ファイルを使用してアップグレードできますが、を使用してソフトウェアアップグレードを実行できるため、推奨されません。upg file. 該当する各アプライアンスにログインして、オペレーティングシステム (OS) コンポーネントソフトウェアをアップグレードするためにアップロードします。リリース 9.3 バージョン 1 から、「オペレーティングシステムソフトウェアの更新」ページは減価償却されます。その結果、.zip パッケージを使用して OS コンポーネントをアップグレードすることで、変更管理を実行できます。

現在実行中の OS コンポーネントのバージョンをどのように検証できますか？

現在、UI から OS コンポーネントの現在実行中のバージョンを検証できません。各コンソールからログインするか、STS にこの情報を表示できます。

ネットワークにベアメタルアプライアンスがある場合、どのような違いがありますか？ スケジューリングはベアメタル/仮想アプライアンスに影響しますか？

SD-WAN のようなベアメタルアプライアンス—**410,2100,4100,5100 SD-WAN** は、SD-WAN ソフトウェアのみを実行します。ベアメタルアプライアンスには OS コンポーネントパッケージは必要ありません。これらのプラットフォームは、ソフトウェアの必要性の観点から、SD-WAN VPX-SE アプライアンスと同等の扱いを受けます。MCN

は OS コンポーネントパッケージをこれらのアプライアンスに転送しません。これらのアプライアンスには、アップグレードが必要な OS コンポーネントがないため、スケジュール情報の設定は有効になりません。

SSU は、高可用性環境/デプロイメントでどのように機能しますか？

MCN での高可用性展開では、変更管理中にアクティブな MCN スイッチがプライマリ MCN の役割を切り替え、スタンバイ/セカンダリ MCN が引き継ぐという制限があります。この場合、パッケージのアクティブな MCN 上の .zip パッケージを使用して変更管理を再度実行するか、アクティブな MCN のロールを切り替えてプライマリ MCN に切り替えて、元のプライマリ MCN が他の OS コンポーネントパッケージにステージングされる OS コンポーネントパッケージのロールを引き継ぐことができるように、プライマリ MCN に戻すことができます。枝。

高可用性環境/導入では、シングルステップアップグレードはどのように機能しますか？

高可用性展開でシングルステップアップグレードを実行すると、プライマリ MCN とスタンバイ MCN の役割が切り替わります。これは制限です。このような場合は、アクティブな MCN の .zip パッケージを使用して変更管理を再度実行します。または、アクティブ MCN の役割を切り替えて、元のプライマリ MCN が OS コンポーネントパッケージをブランチにステージングできるように、プライマリ MCN に切り替えることもできます。

アプライアンスを再起動するために、ゼロタッチ導入をワンステップでアップグレードできますか？

はい、使用できます。

スタンドアロン WANOP アプライアンスをアップグレードするためにシングルステップアップグレードを使用できますか？

いいえ。

シングルステップアップグレードを使用して、2 ボックスモードで展開されたスタンドアロン WANOP アプライアンスをアップグレードできますか？

なし 2 ボックスモードの一部である SD-WAN アプライアンスのみがアップグレードされ、WANOP スタンドアロンアプライアンスはアップグレードされません。

多層ネットワークにアップグレードするには、どのパッケージを使用すればよいですか？

<release-version> 現在のソフトウェアバージョンが 9.3.x 以上の場合は、シングルステップアップグレードパッケージ *ns-sdw-sw-.zip* ファイルを使用します。MCN は、それぞれのブランチに RCN と RCN ステージングソフトウェアパッケージにステージングパッケージの世話をします。

ns-sdw-sw-.zip <release-version> ファイルをアップロードした後、現在のソフトウェアでは 1 つのプラットフォームモデルしか表示されていませんか？

リリース 10.0 から、スケールアーキテクチャのサポートが導入され、シングルステップアップグレードの処理が高速化されました。現在のソフトウェアでは、MCN プラットフォームモデルのみを表示できます。[**Verify**] ボタンまたは [**Stage Appliance**] ボタンを選択すると、その他のアプライアンス・パッケージがリスト/表示/処理されます。

VPX/VPXL/ベアメタルアプライアンスの場合、RCN 用にステージングされるパッケージはどれですか？

パッケージは RCN にステージングされます。RCN ブランチはどのプラットフォームモデルでもかまいません。したがって、彼らはすべてのパッケージを必要とします。

RCN が VPX アプライアンスで、ブランチがこれらのパッケージを必要とするアプライアンスである場合、RCN の背後にあるブランチサイトはどのように OS コンポーネントパッケージを取得しますか？

RCN は、SD-WAN VW ソフトウェアパッケージをアクティブ化した後、OS コンポーネントパッケージを必要とするブランチに、関連するパッケージをステージングします。

ステージング中に「未完了を無視」を選択し、変更管理の次のステージに進むことはできますか？ このボタンを選択すると、ステージングが完了していないサイトに対してどのような影響がありますか。

はい、[不完全無視] をクリックできます。これにより、[次へ] ボタンが有効になり、進行状況バーが表示されます。このオプションは、サイトにアクセスできず、変更管理がこれらのサイトのステージングが完了するのを待っている場合に提供されます。そのため、ユーザーはステージの状態を無視して次のステージに進み、アクティブ化に進むことができます。サイトが起動すると、MCN はアクティベーション完了後にパッケージをステージングします。

部分的なソフトウェアアップグレード

部分的なサイトアップグレードとは何ですか？ どのように使用できますか？

サイトソフトウェアの部分的なアップグレードは、リリース 10.0 で導入された新機能です。MCN からリリース 10.x の新しいバージョンをステージングし、選択したサイト/ブランチの **Local Change Management** ページからステージングされたソフトウェアバージョンをアクティブ化できます。サイト/ブランチでステージングされたソフトウェアをアクティブ化する前に、MCN のチェックボックスがオンになっていることを確認します。

- この機能はデフォルトでは無効になっています。既存の補正メカニズムにより、ネットワークの同期が維持されます。ユーザーは、[構成] > [管理設定の変更] ページでチェックボックスをオンにして、サイトの部分的なアップグレードを許可する必要があります。
- 部分的なソフトウェアアップグレードは、ブランチまたは RCN でのみ実行でき、MCN では実行できません。

サイトソフトウェアの部分的なアップグレードを使用できる場合のユースケース/シナリオを次に示します。

関連する変更を含むソフトウェアパッチが、特定のサイト (サイトの部分的なアップグレードが実行されている) に対して互換性があり、機能しているかどうかを検証します。アップグレードされたソフトウェアが予期したとおりに動作していることを確認します。これにより、ネットワーク全体を新しいソフトウェアでアップグレードする前に、新しいソフトウェアを検証し、特定のサイトで修正できます。

この機能を使用して次のものからアップグレードすることは可能ですが、

- 10.0 から 10.x
- 10.0.x から 10.0.y
- 11.0~11.y
- 11.0.x~11.0.y
- 上記のすべて

サイトソフトウェアの部分的なアップグレードは、アプライアンスがソフトウェアリリース 10.x 以降を実行している場合にのみ適用され、同じメジャーバージョンのソフトウェア内で使用できます。リリース 10.0 から 10.0.x/10.x の間で使用できます。サイトソフトウェアの部分的なアップグレードの一環として、構成を変更することはできません。

設定から機能を有効にすることで、部分的なソフトウェアアップグレードの一部としてテストする新機能をテストできますか。

いいえ。部分的なソフトウェアアップグレードでは、アクティブ構成とステージング構成を同一にする必要があります。変更できるのはソフトウェアバージョンのみです。

RCN の部分的なソフトウェアアップグレードを無効にすることはできますか。

いいえ。部分的なソフトウェアアップグレードは、MCN からのみ有効または無効にできます。RCN では、この機能は読み取り専用モードです。

9.3.x および 10.0.x をステージングした状態でアクティブになっている場合、部分的なソフトウェアアップグレードを使用できますか。

いいえ。アプライアンスはリリース 10.0 でアクティブなソフトウェアとして実行されている必要があります。

一部のブランチがこの機能を使用してすでにアップグレードされているときに、MCN から [Partial Software Upgrade] オプションが無効になっている場合はどうなりますか。

MCN は、Partial Software Upgrade 機能が無効になっているという通知をネットワーク内のすべてのアプライアンスに送信します。その後、ネットワーク内のすべてのアプライアンスが MCN によってアクティブおよびステージングされたバージョンに一致するように自動修正されます。ただし、MCN では、変更管理の [有効化] ページで [段階的有效化] オプションをクリックすることを期待しています。[Activate **Staged**] ボタンをクリックしてネットワークをアクティブ化するか、[****Change Prepared****] をクリックして確認を承認して状態をキャンセルするかを選択できます。

変更管理のロールバック

変更管理プロセスのロールバック機能とは何ですか？

リリース 9.3 から、変更管理ロールバック機能を使用すると、t2-app クラッシュや仮想パスの状態などの予期しないイベントが設定更新後に非アクティブになった場合に、作業構成にロールバックできます。ネットワークとアプライアンスは、設定の更新後 10 分間監視されます。この間、次の条件が満たされた場合（ユーザーがこの機能を有効にしている場合）、ステージングされた構成がアクティブになります。アクティブソフトウェアが [ステージング] にロールバックされます。

構成をロールバックして再起動するには、どのような基準がありますか。

ロールバックは、次のシナリオが発生した場合に発生します。

1. MCN-設定/ソフトウェアの変更後、30 分間隔でクラッシュにより t2_app サービスが無効になった場合。

2. MCN-構成/ソフトウェアの変更後、アクティベーション後 30 分以上仮想パスサービスがダウンしている場合。ロールバック機能は、サイトで開始されます。
3. サイト：構成/ソフトウェアの変更後、サイトが MCN との通信を失った場合、ロールバック機能が開始されます。
4. サイト-設定/ソフトウェア変更後、30 分間隔内にクラッシュしたため、t2_app サービスが無効になります。

ロールバック後はどうなりますか？

構成のロールバック後、障害のある構成/ソフトウェアが Staged ソフトウェアとして表示されます。

ロールバックが発生したことをユーザーにどのように通知しますか？

GUI の上部に、それぞれのエラーのために Config がロールバックされたという黄色のバナーが表示されます。また、あなたはそれが変更管理ステータステーブルである見ることができます。ロールバックが発生したサイトに対応する構成エラーまたはソフトウェアエラーが表示されます。

設定とソフトウェアの両方がロールバックされますか？

はい。構成とともにソフトウェアのアップグレードも実行され、ロールバックシナリオが発生すると、ソフトウェアもロールバックされます。

MCN に問題があり、すべてのサイトとの接続がクラッシュまたは切断された場合、どうなりますか？

MCN 以外のネットワーク全体がロールバックされます。通知が表示され、すべてのサイトの変更管理セクションにロールバック状態が表示されます。MCN の問題は手動で解決できます。

この機能を無効にすることはできますか？

はい、アクティブ化する直前にこの機能を無効にすることができます。ただし、この機能はデフォルトで有効になっています。

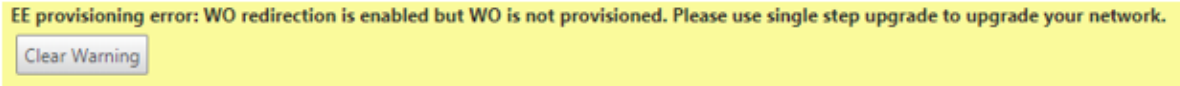
多層ネットワークがある場合、ロールバックは部分的なソフトウェアアップグレードとどのように相互作用しますか？

- 部分的なソフトウェアアップグレードが無効で、リージョン（または RCN）のサイトがロールバックすると、問題のあるリージョンがロールバックされ、完了すると、ロールバックは MCN に伝播されます。その結果、MCN とネットワークの残りの部分がロールバックされます。ロールバックしたリージョンの RCN と MCN の両方に、MCN が RCN でロールバックバナーを自動的に閉じることができないロールバックバナーが表示されます。
- 部分的なソフトウェアアップグレードが有効で、リージョン（または RCN）のサイトがロールバックされると、そのリージョンだけがロールバックされます。ロールバックイベントは MCN に伝播されません。その結果、MCN は地域を離れます。MCN はロールバックバナーを表示せず、自身またはネットワークをロールバックしません。

どちらのシナリオでも、RCN はロールバックのバナーを表示します。なぜなら、MCN では自動解除できないからです。

2100 Premium（エンタープライズ）エディション

2100 EE アプライアンスがリリース 10.0 にアップグレードされた場合、次のメッセージは何を示していますか。



アプライアンスに EE ライセンスがあるか、MCN から WANOP リダイレクトが有効になっています。WANOP コンポーネントのインストールをスケジュールして、このプラットフォームで WANOP 機能の Provisioning を開始できます。

関連情報

- [LTE を介したゼロタッチ展開](#)
- [HA でのセカンダリ MCN の設定](#)

参考資料

May 10, 2021

[アプリケーション署名ライブラリ](#)

Citrix SD-WAN アプライアンスがディープパケットインスペクションを使用して識別できるアプリケーションのリストです。



© 2024 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).