Citrix SD-WAN 11.5

Machine translated content

Disclaimer

Contents

Citrix SD-WAN 11.5 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 11.5 に存在する拡張機能と変更、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。

新機能

SD-WAN 11.5 リリースで利用できる機能強化と変更。

その他

Citrix SD-WAN 11.5 リリース仕様

- Citrix SD-WAN 11.5.0 は限定可用性リリースであり、特定の顧客/本番環境でのみ推奨およびサポートされています。
- SD-WAN 11.5.0 リリースは、Advanced Edition（AE）、プレミアムエディション（PE）、WAN 最適化の展開をサポートしていません。
- SD-WAN 11.5.0 は、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に記載されているプラットフォームのみをサポートします。
- SD-WAN 11.5.0 は、オンプレミスの Citrix SD-WAN Center または Citrix SD-WAN Orchestrator をサポートしていません。
- SD-WAN 11.5.0 ファームウェアは、Citrix ダウンロードページでは利用できません。
- SD-WAN 11.5.0 リリースは、Citrix SD-WAN Orchestrator サービスを介してのみ利用可能で、選択した地理的 POP でのみ利用できます。
- 実稼働ネットワークに 11.5.0 を展開する前に、Citrix Product Management/Citrix サポートから必要な承認とガイダンスを取得してください。

[NSSDW-38486]

Citrix SD-WAN 構成エディターに代わる Citrix SD-WAN オーケストレーターサービス：

Citrix SD-WAN 11.5 リリースから、SD-WAN 構成エディターおよび SD-WAN Center は、Citrix SD-WAN オーケストレーターサービスに置き換えられました。Citrix SD-WAN Orchestrator サービスは、SD-WAN 構成エディターを介して現在行われているすべての構成をサポートします。Citrix SD-WAN Orchestrator サービスの詳細については、「Citrix SD-WAN Orchestrator サービス」を参照してください。

[NSSDW-33528]

IPv6 のサポート:

Citrix SD-WAN 11.5.0 リリース以降、Citrix SD-WAN アプライアンスの次のデータプレーン機能は IPv6 アドレスをサポートします。

- アプリケーションルート
- Citrix Cloud および Cloud サービスの最適化
- ドメイン名ベースのアプリケーション分類
- ダイナミック PAC ファイルのカスタマイズ
- 動的ルーティング
- ファイアウォールのデフォルト
- マルチキャスト
- Office 365 の最適化
- PPPoE
- サイトレポート-ルーティングプロトコル
- VRRP

上記の機能を構成した後、IPv4 または 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。

[SDW-23397、NSSDW-29150、NSSDW-29152、NSSDW-29154、NSSDW-29155、NSSDW-29156、NSSDW-29468、NSSDW-1940、NSSDW-1995]

監視機能の強化:

次の監視ダッシュボードが強化され、新しいアプライアンス UI で使用できます。

- DNS トランスペアレントフォワーダ
- ファイアウォール接続、ファイアウォールフィルタ、ファイアウォール NAT
- IGMP、IGMP プロキシ、IGMP 統計情報
- IKE、IPsec
- マルチキャストグループ、マルチキャストグループ送信元、マルチキャストグループ宛先
- PPPoE セッション

- VRRP

[NSSDW-33763]

プラットフォームとシステム

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-38209]

解決された問題

SD-WAN 11.5 リリースで対処されている問題。

その他

一部の SD-WAN アプライアンスの管理インターフェイスステータスが、UI の [イーサネットインターフェイス設定] ページに [ダウン] と表示されていました。この問題は、帯域内管理がサポートされている一部のアプライアンスで、帯域外を使用するオプションが使用できる場合に発生しました。したがって、アプライアンスは帯域外管理インターフェイスを使用して SD-WAN Orchestrator サービスにアクセスしました。

[NSSDW-37028]

既知の問題

SD-WAN 11.5 リリースに存在する問題。

いずれかのサイトまたは WAN リンクで設定変更時に展開が拡張された場合、ルーティングエンジンの再起動により BGP セッションがフラップします。

[SDWANHELP-2594]

SD-WAN アプライアンスが予期せずクラッシュしました。この問題は、次の場合に発生しました。

- ソフトウェアのアップグレード中に IPv6 マルチキャストトラフィックが流れていました。
- IPv6 マルチキャストトラフィックは、イントラネット GRE トンネルを使用して送信され、MLDv2 プロキシ設定を使用して仮想パスを介して複数のブランチにレプリケートされました。

回避策：ソフトウェアのアップグレード中は IPv6 マルチキャストトラフィックを無効にし、アップグレードが正常に完了したら有効にします。

[NSSDW-38495]

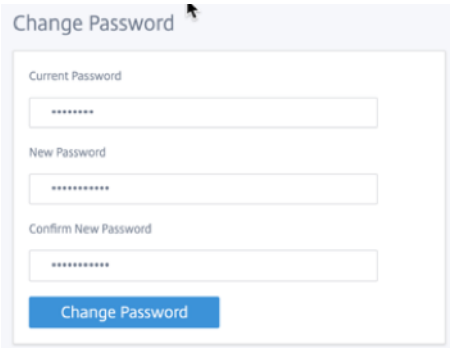
SD-WAN アプライアンスの新しいユーザーインターフェイス

August 30, 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** 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る。

> 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。

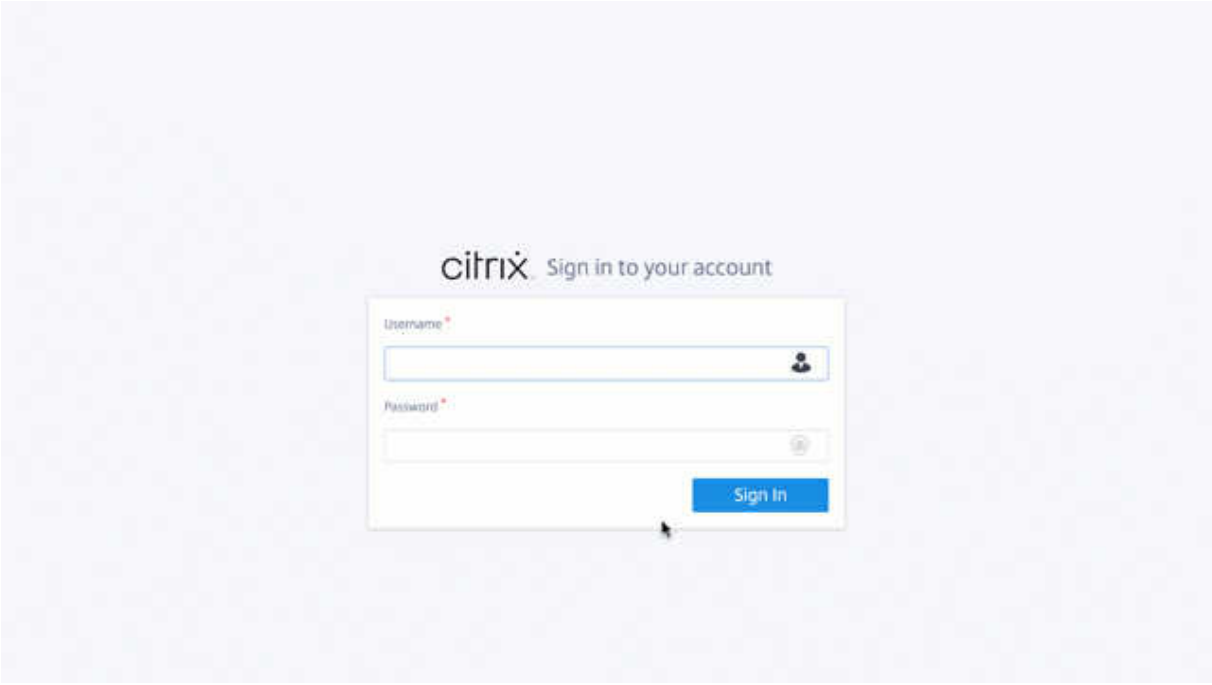
1. 新しいブラウザータブを開き、**https://** < management-ip > に移動し、SD-WAN アプライアンスの新しい UI にアクセスします。IPv6 アドレスにアクセスする場合は、`https://<[IPv6 address]>`と入力します。

   例: `https://[fd73:xxxx:yyyy:26::9]`

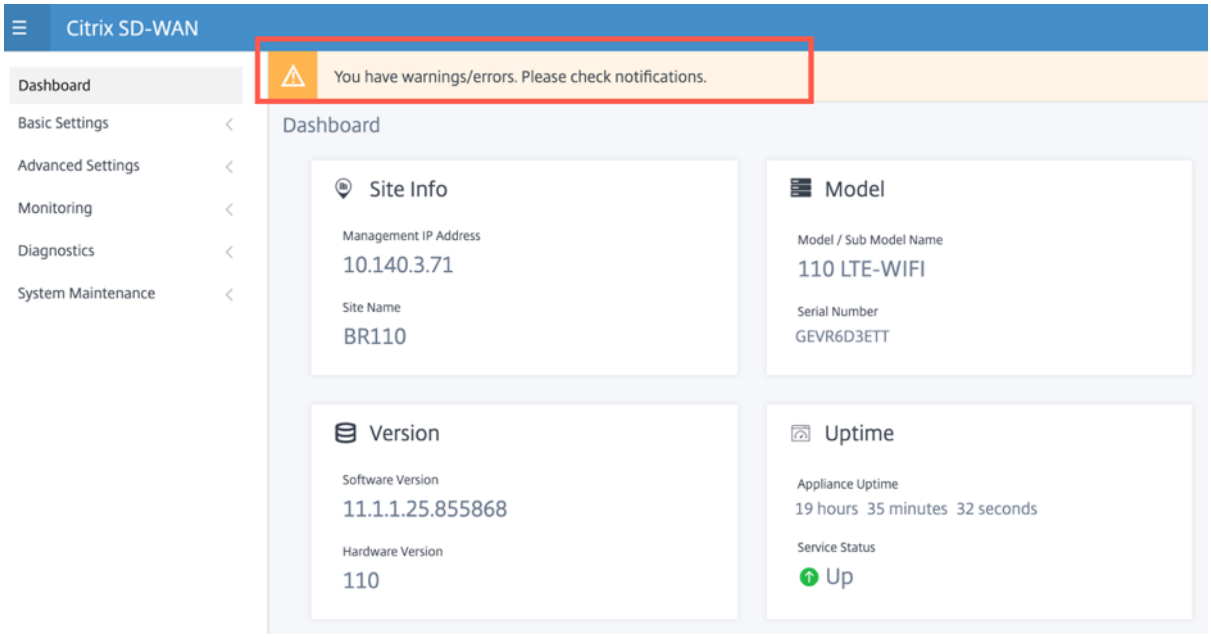
> 注:
>
> インバンド管理が有効になっているシナリオでは、インターフェイスの IP アドレス ** < management-ip > をで指定して、新しい UI にアクセスできます。インバンド管理は、IP サービスに使用できるように有効になっている複数の信頼できるインターフェイスで有効にできます。管理 IP とインバンド仮想 IP を使用して UI にアクセスできます。

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。

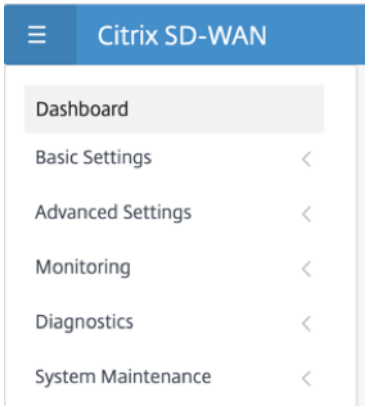


正常にログインすると、ナビゲーションパネルが左側にあることがわかります。また、警告やエラーがある場合は、ダッシュボードに通知バナーが表示されます。



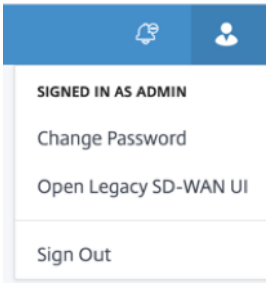
ナビゲーション

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。

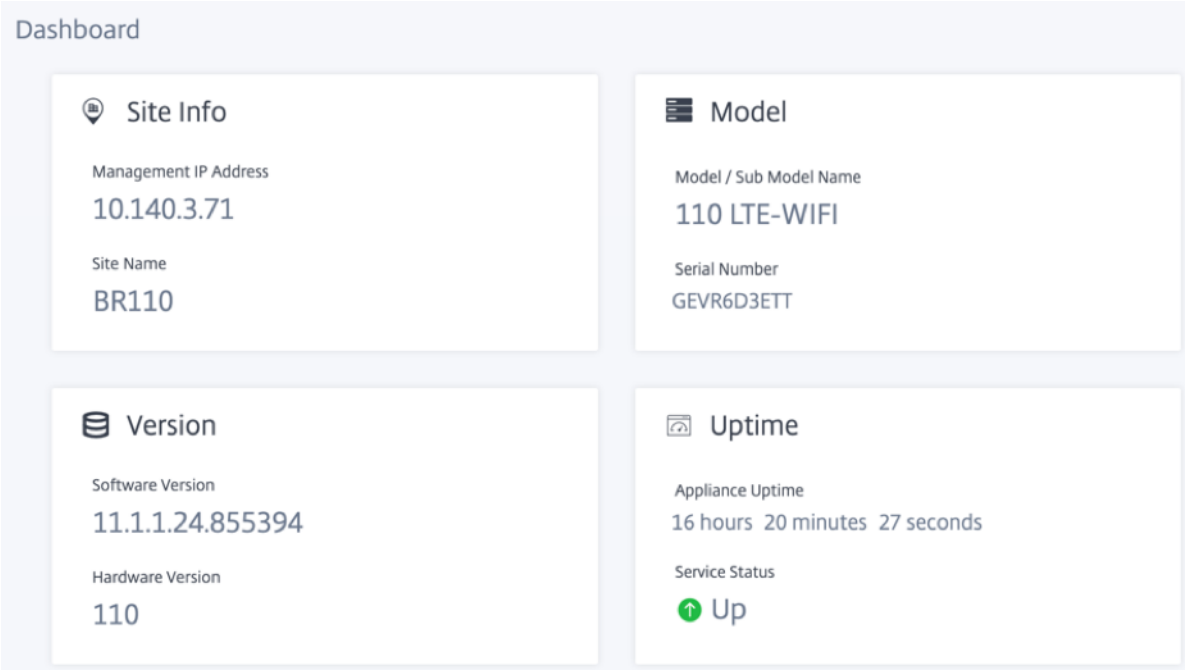


ダッシュボード

[**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 **。
- [**Version**]: 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

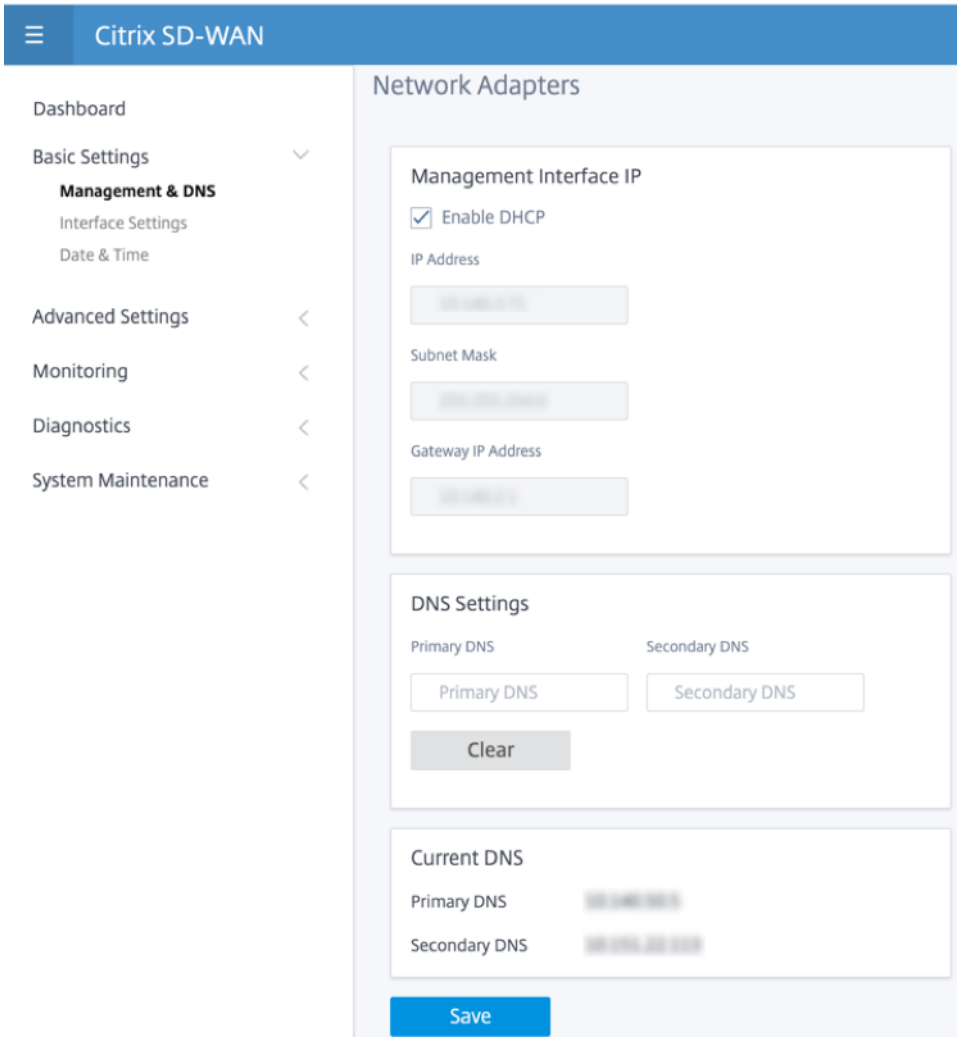
管理と **DNS**

[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

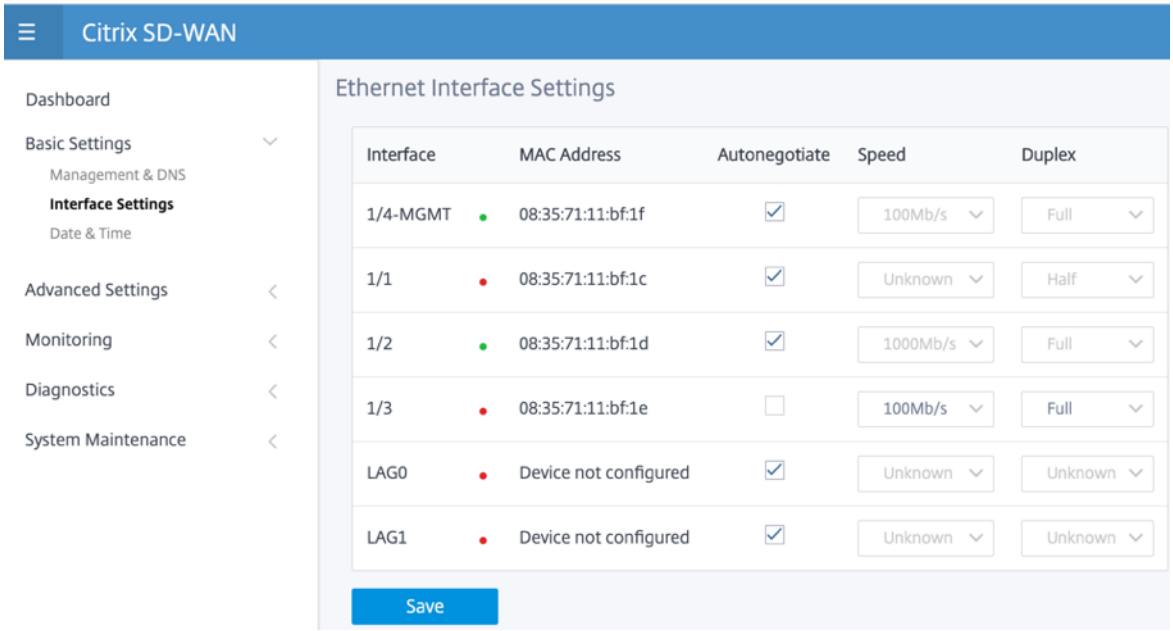
は、IPv6 アドレスのみを使用して SD-WAN アプライアンス管理インターフェイスにアクセスする必要があります



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。



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。

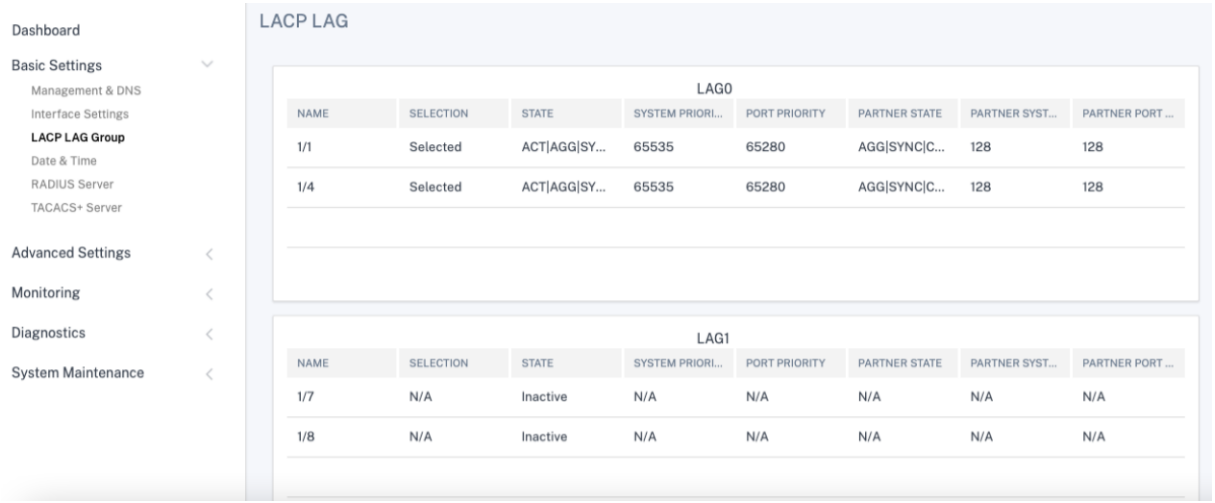
Citrix SD-WAN アプライアンスの各 LAG にグループ化された最大 4 つのポートを持つ最大 4 つの LAG を作成できます。

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。

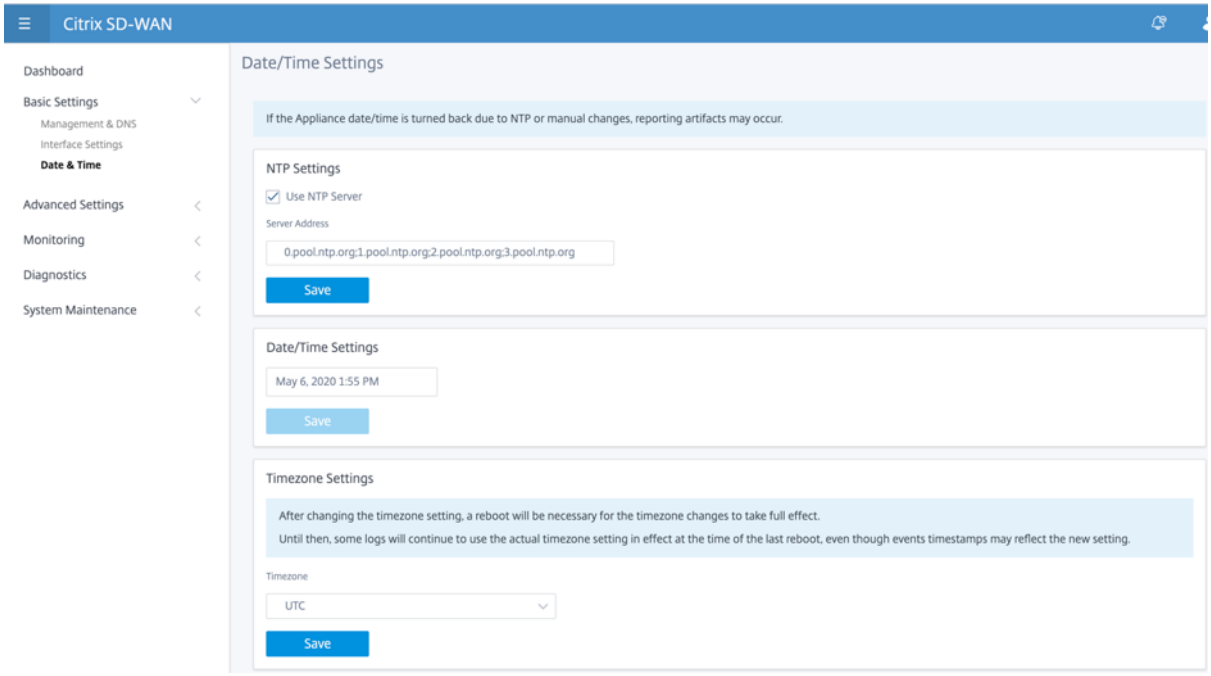
LAG の詳細を表示するには、[基本設定] > [**LACP LAG** グループ] に移動します。

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。



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。



RADIUS サーバ

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

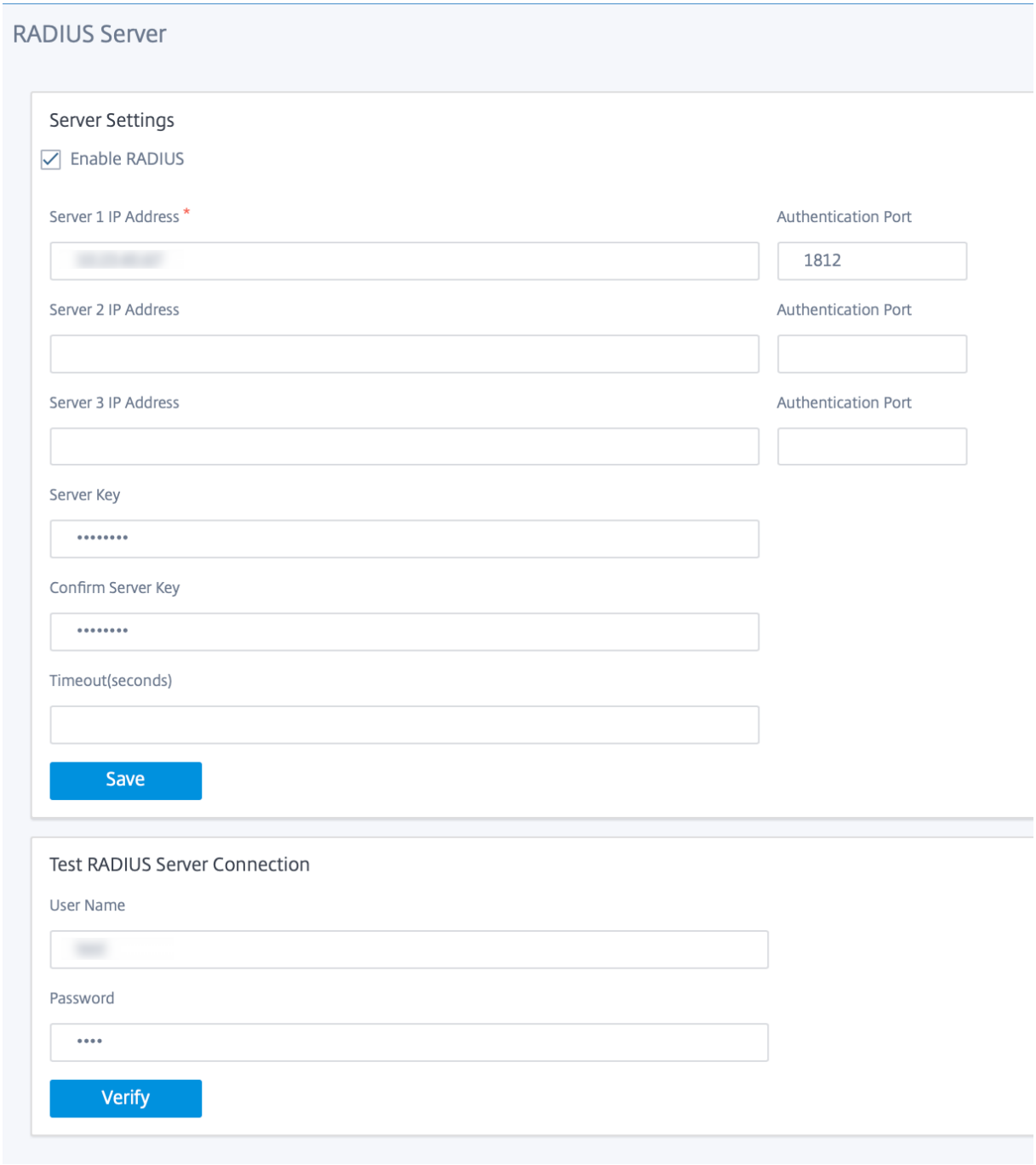
RADIUS サーバを構成するには、次の手順を実行します。

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。



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。

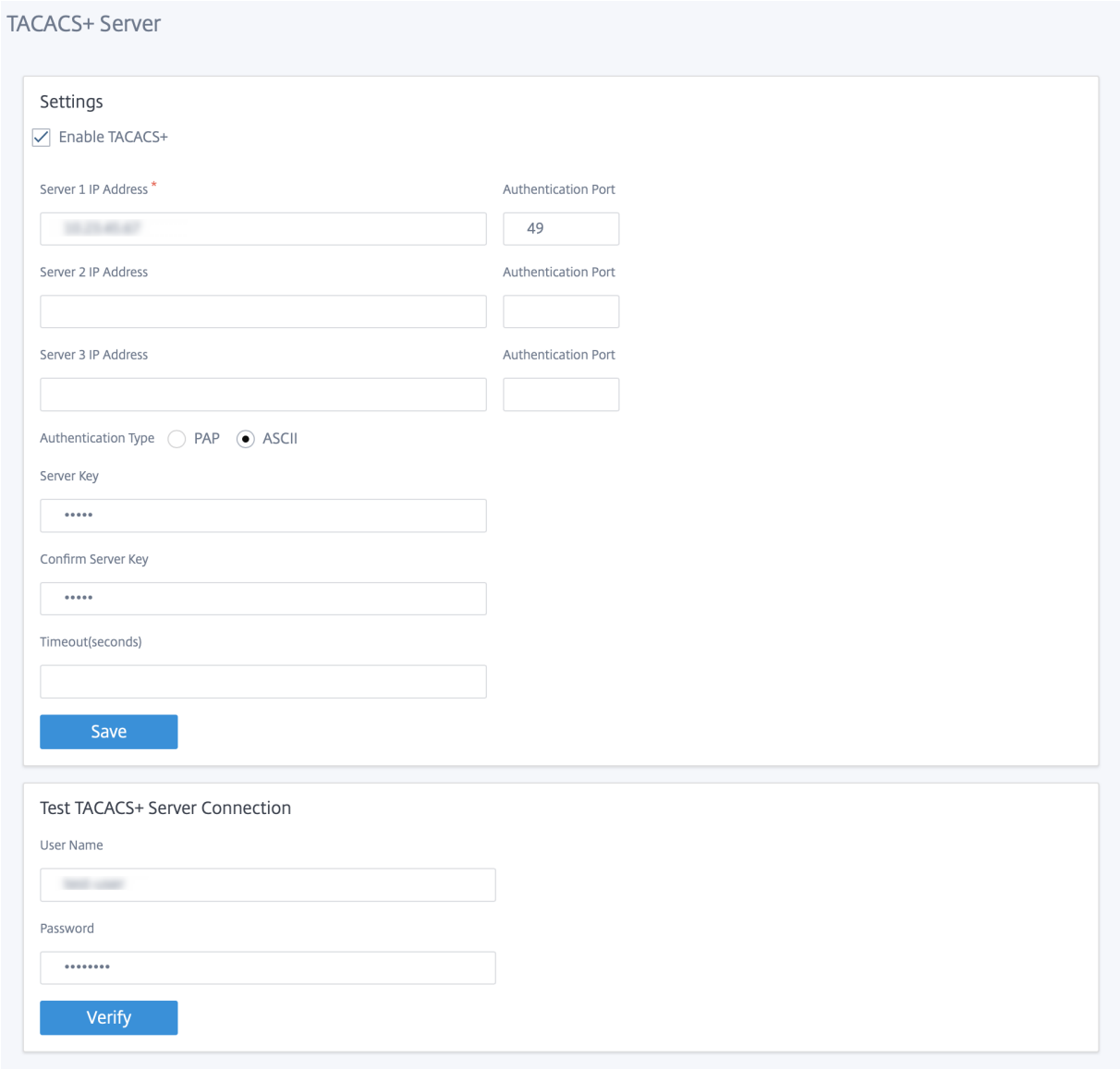
   > 注:
   >
   > IPv6 アドレスを設定するには、TACACS+ サーバにも IPv6 アドレスが設定されていることを確認します。

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。



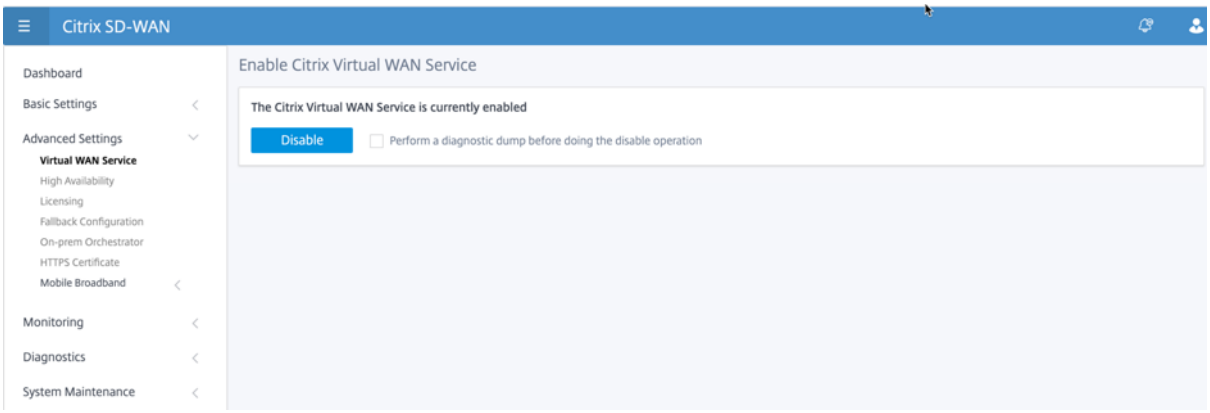
詳細設定

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
- ライセンス管理
- 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

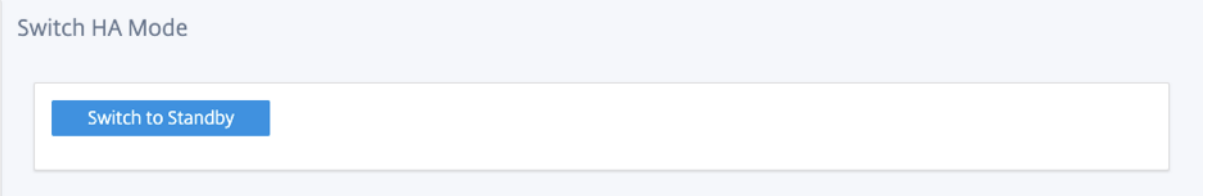
Citrix 仮想 **WAN** サービス

[**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 。

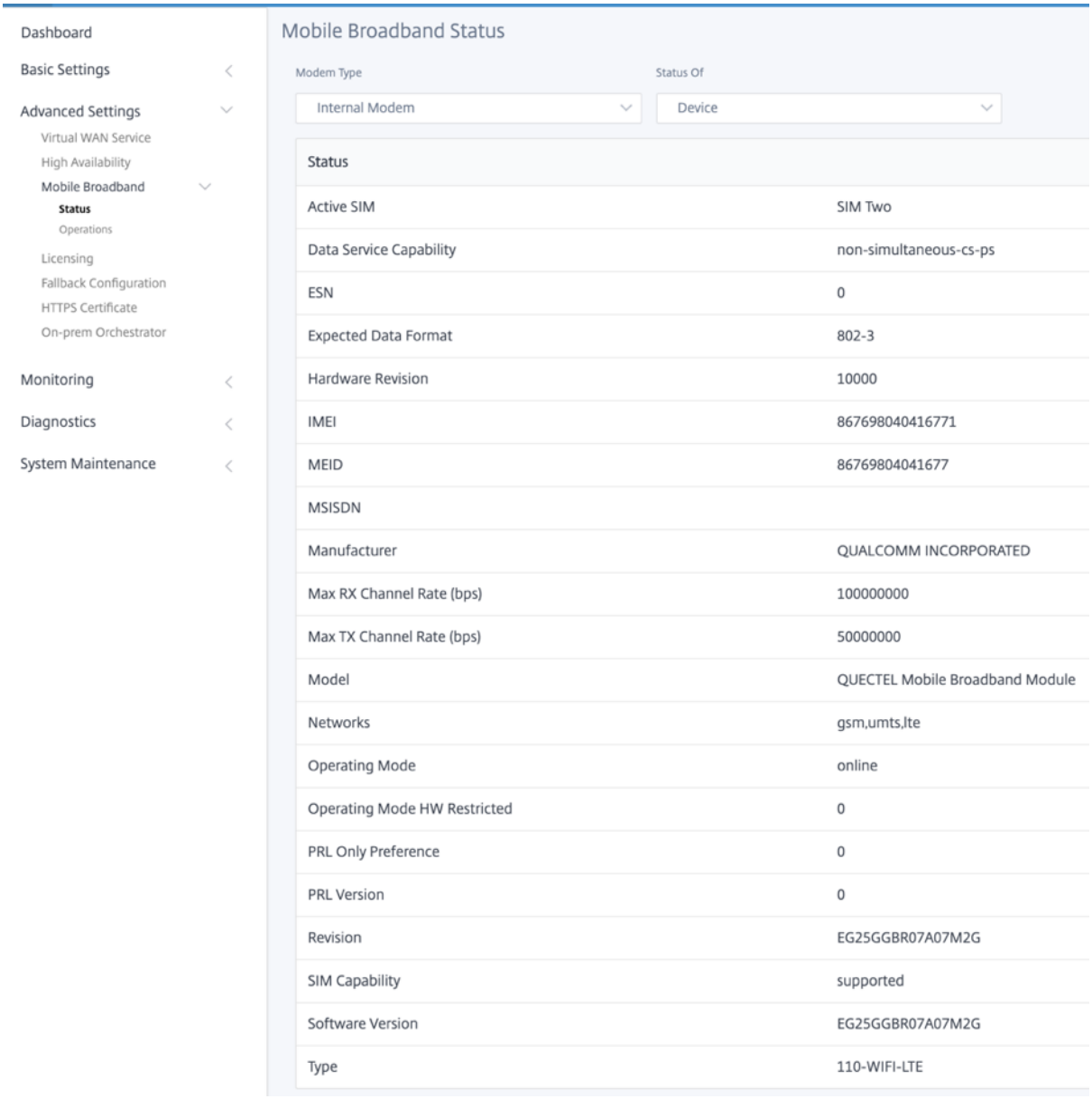
> 注:
>
> Citrix SD-WAN 110-LTE-WiFi アプライアンスには、2 つの標準（2FF）SIM スロットがあります。マイクロ（3FF）およびナノ（4FF）サイズの SIM を使用するには、SIM アダプタを使用します。小さい SIM をアダプタにスナップします。アダプタは、フィールド交換可能ユニット（FRU）として Citrix から入手するか、SIM プロバイダから入手できます。内部 LTE モデム用の SIM のホットスワップは、Citrix SD-WAN 110-LTE-WiFi アプライアンスでのみサポートされています。

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。

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。

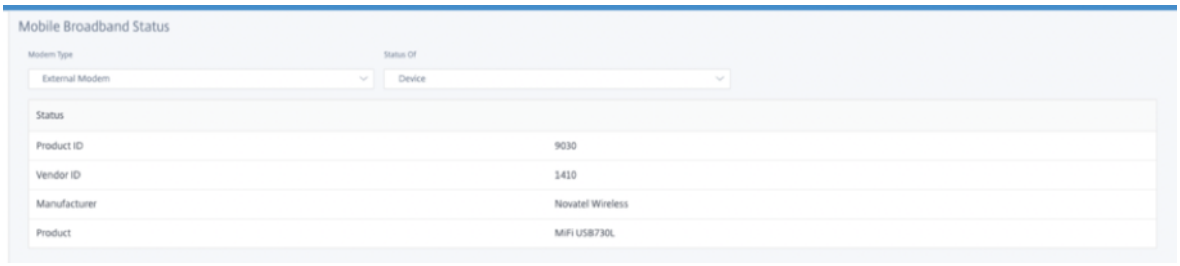


以下は、いくつかの有用なステータス情報です。

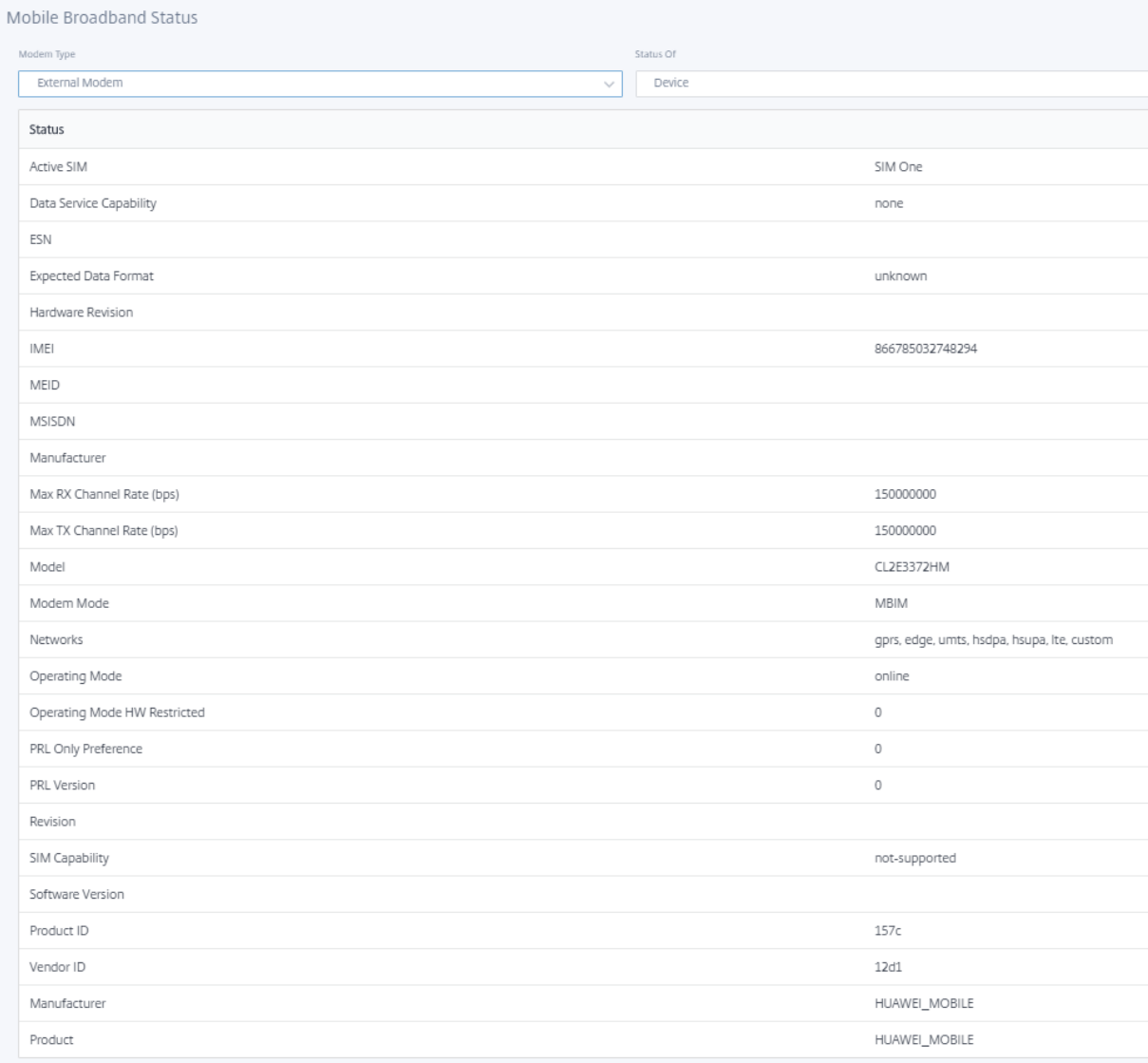
- モデムの種類: モデムの種類として [外部] または [内部] を選択します。内蔵モデムは、[モバイルブロードバンド**] > [**ステータス**]** ページにステータスを表示します。SIM 設定、APN 設定、モデムの有効化/無効化、モデムの再起動、SIM の更新などのその他のすべてのセクションは、[モバイルブロードバンド**] > [**操作] ページにあります。
- アクティブ **SIM**: アクティブになることができる SIM はいつでも、1 つのみです。現在アクティブな SIM を表示します。
- 動作モード: モデムの状態を表示します。
- **SIM** 機能:SIM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

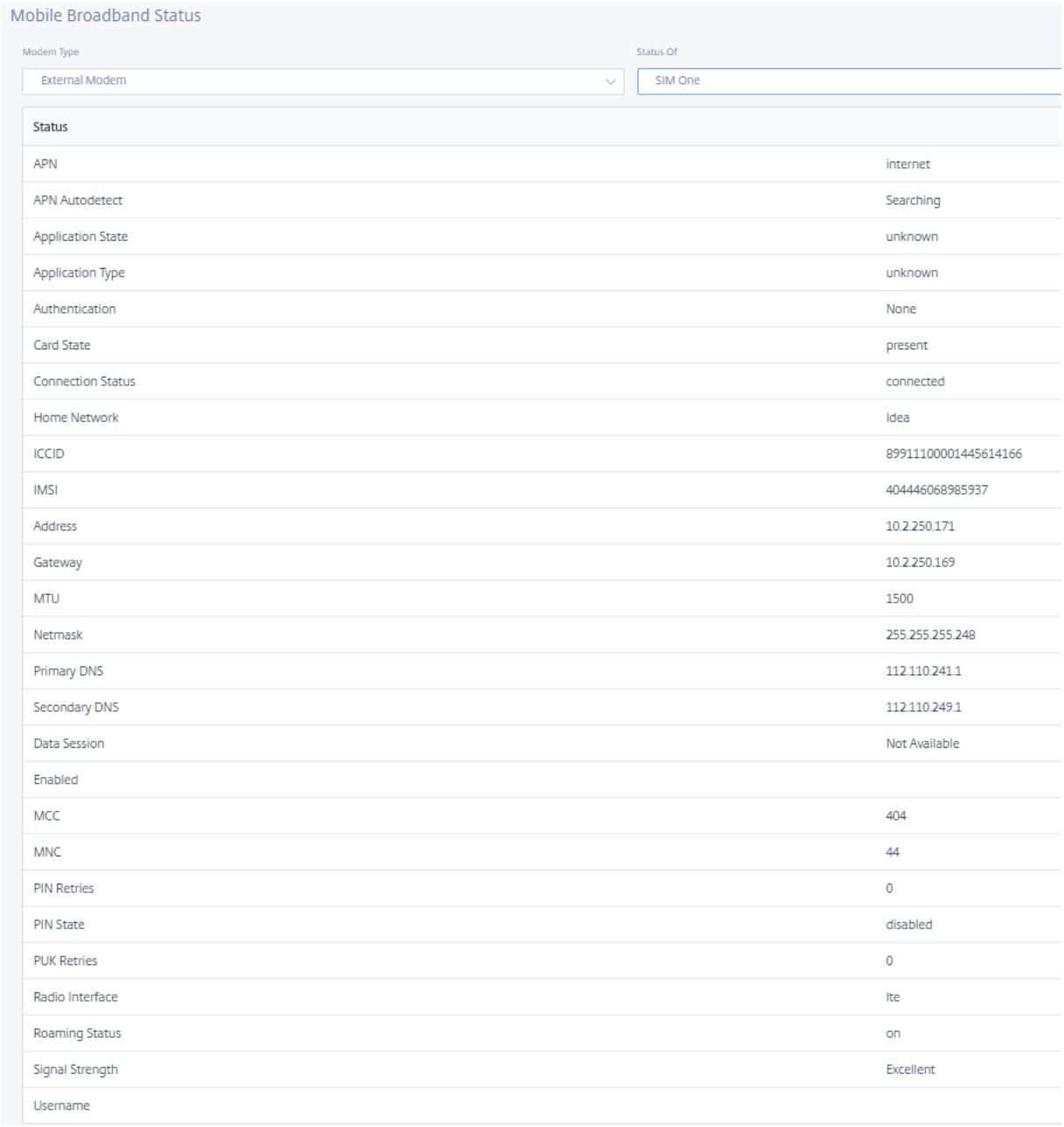
CDC イーサネット外部モデムのデバイスの詳細



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。



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。



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:

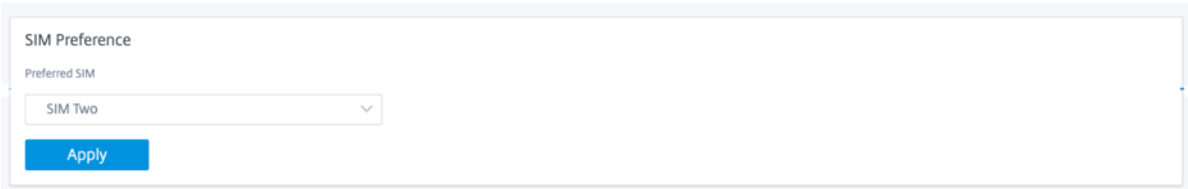
操作	内蔵モデム	外部モデム-CDC イーサネット	外部モデム-MBIM および NCM
SIM プリファレンス	はい-デュアル SIM をサポートするアプライアンスの場合	いいえ	いいえ
SIM ピン	はい	いいえ	いいえ

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。

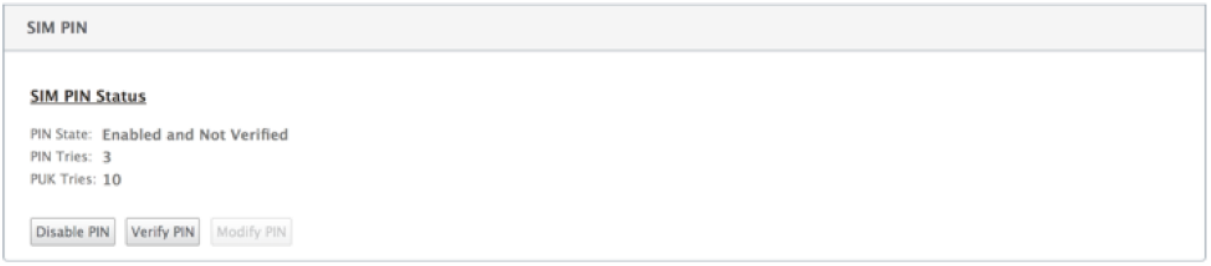
> 注:
>
> Citrix SD-WAN 210-SE LTE Wi-Fi アプライアンスには、SIM カードスロットが 1 つしかないため、［SIM 設定］オプションは使用できません。



SIM 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

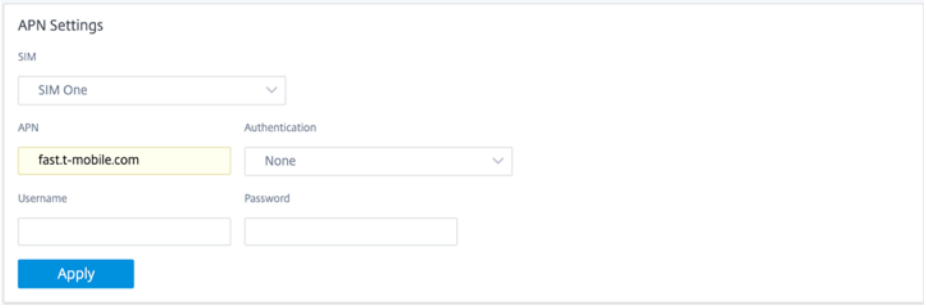
1. APN 設定を構成するには、[詳細設定] > [モバイルブロードバンド] > [オペレーション] の順に選択し、[**APN** 設定] セクションに移動します。

> 注
>
> キャリアから APN 情報を入手します。

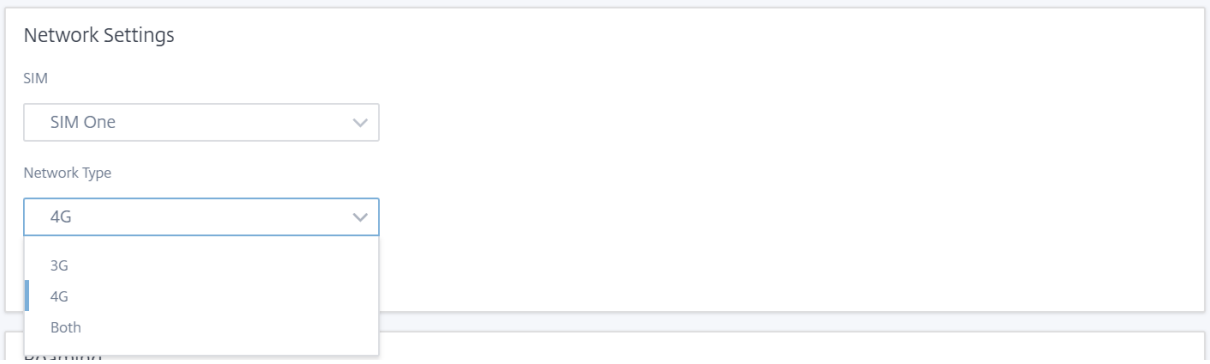
2. SIM カードを選択し、通信事業者から提供された **APN**、ユーザー名、パスワード、認証を入力します。PAP、CHAP、PAPCHAP 認証プロトコルから選択できます。通信事業者が認証タイプを提供していない場合は、[なし] に設定します。

   > (注
   >
   >) これらのフィールドはすべてオプションです。

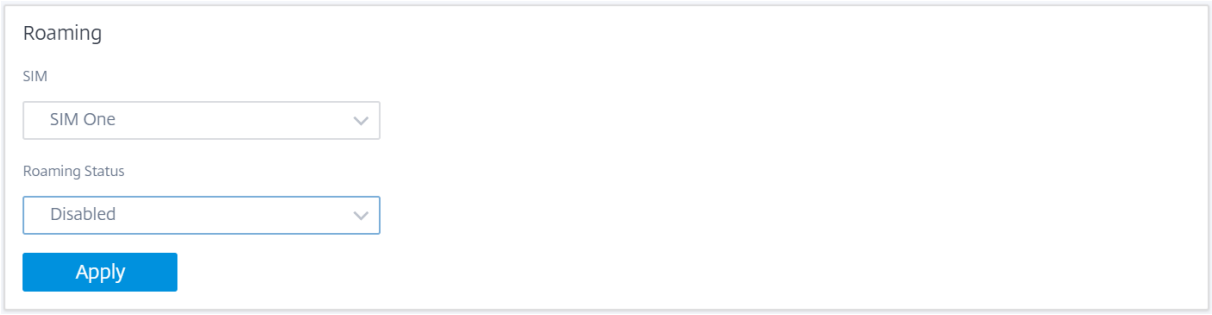
3. [適用] をクリックします。



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。



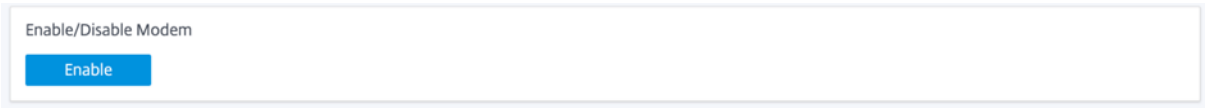
ローミング　ローミングオプションは、LTE アプライアンスではデフォルトで有効になっています。無効にすることもできます。



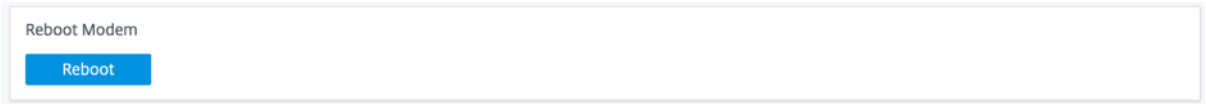
ファームウェアの管理

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。

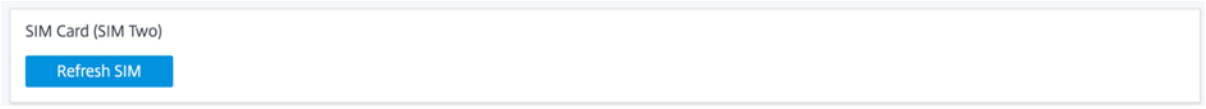


モデムの再起動　モデムをリブートします。再起動操作が完了するまで、最大で 7 分かかる場合があります。



SIM のリフレッシュ　**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。



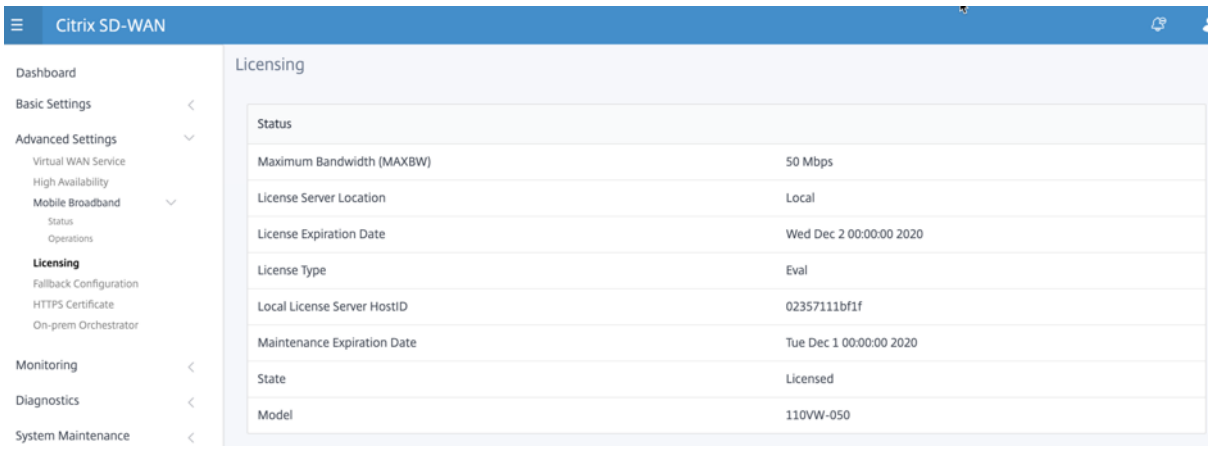
Citrix SD-WAN Center を使用して、ネットワーク内のすべての LTE サイトをリモートで表示および管理できます。詳細については、リモート LTE サイト管理を参照してください。

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。

ライセンス管理

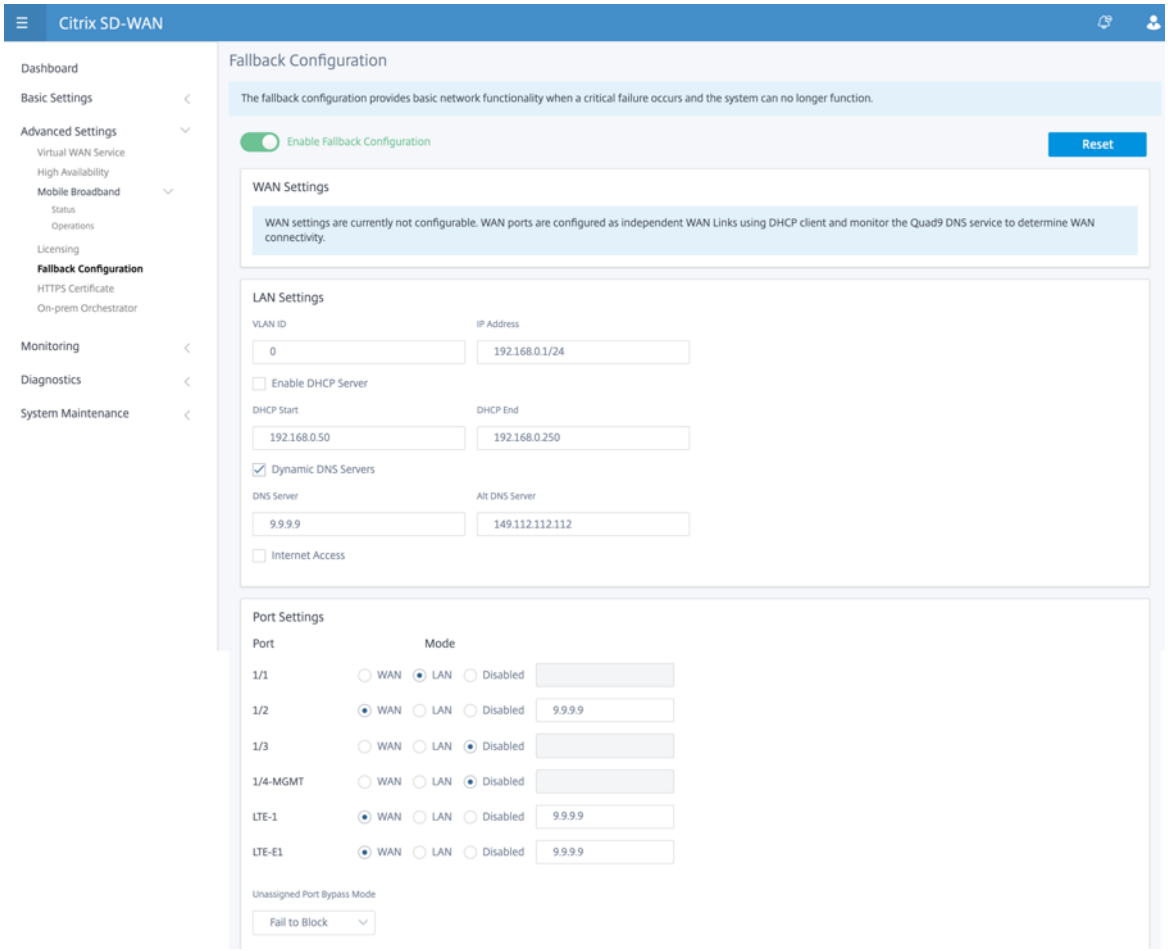
［ライセンス］ページには、サーバーの場所、モデル、ライセンスタイプなどのライセンスの詳細が表示されます。



> 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。

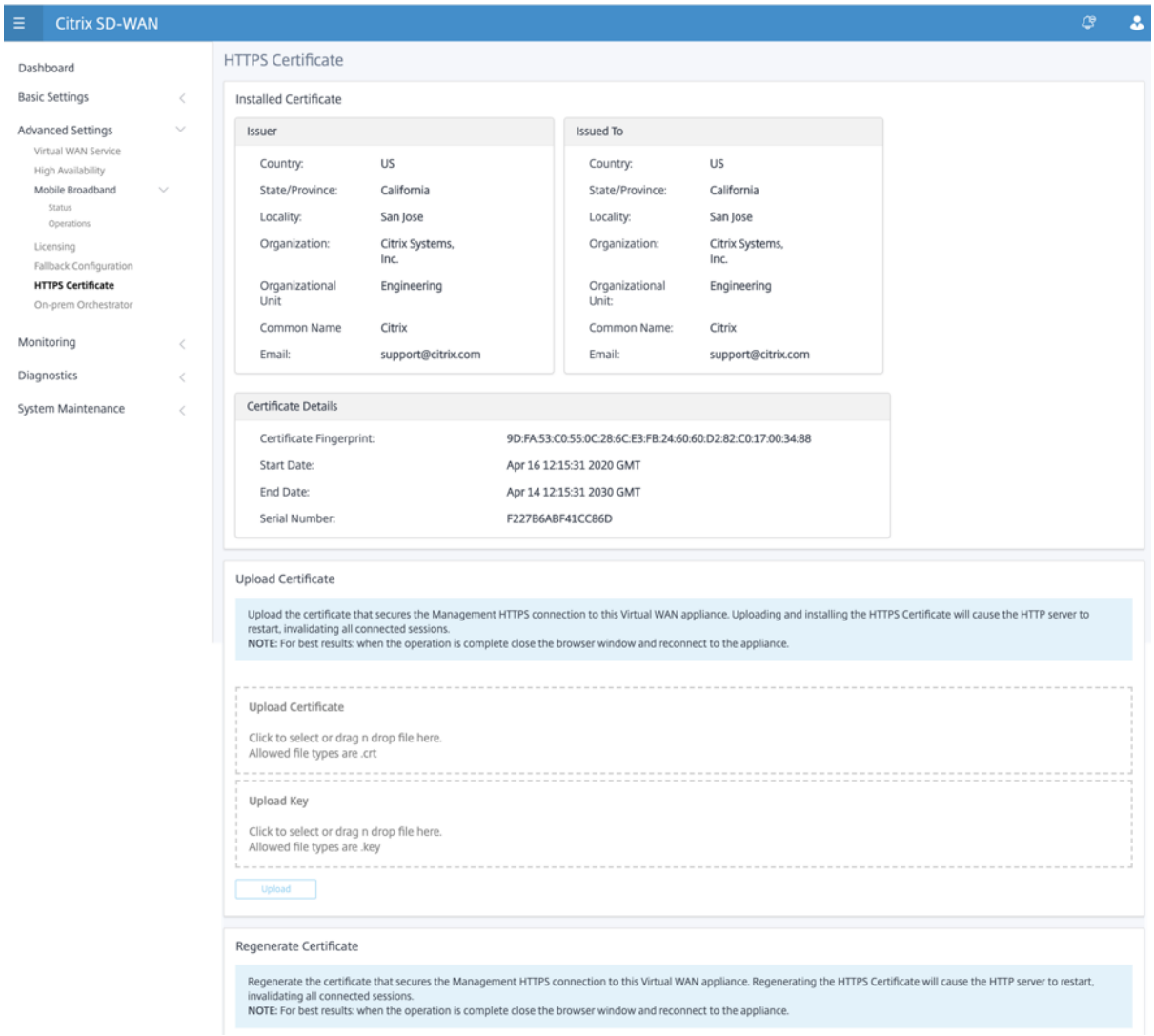


> 注
>
> LTE インターフェイスは、スタティック IP アドレスでは設定できません。

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。



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。

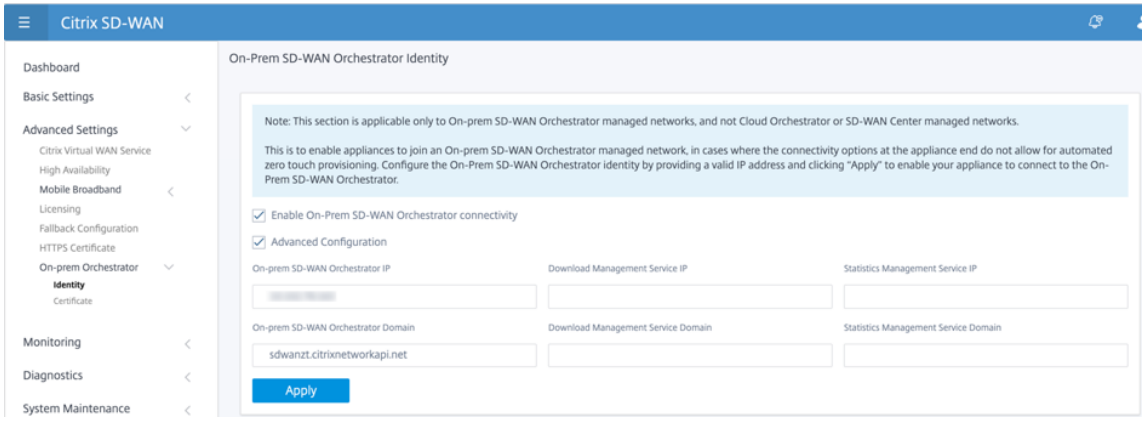
Orchestrator の接続を有効にし、オンプレミス SD-WAN オーケストレータの ID を指定することで、Citrix SD-WAN アプライアンスと Citrix オンプレミス SD-WAN オーケストレータ間の接続を確立できます。

> 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。



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ー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ー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ー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。

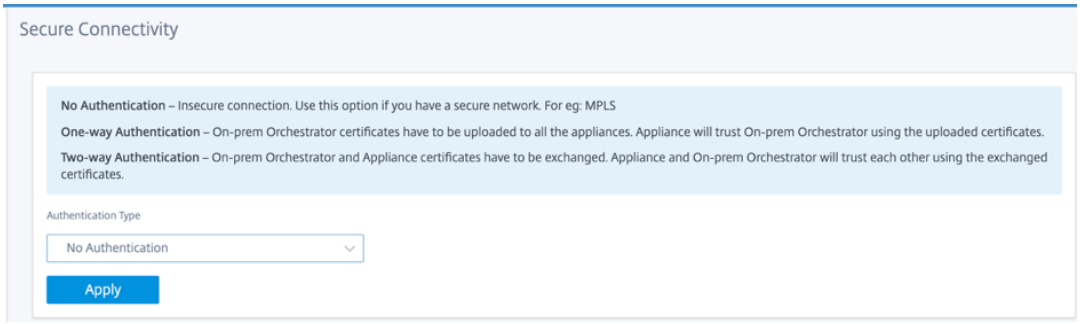
   オンプレミス **Orchestrator** 認証タイプが有効になっている場合、アプライアンスは双方向認証を介してオンプレミス **Orchestrator** にのみ接続できます。

   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。

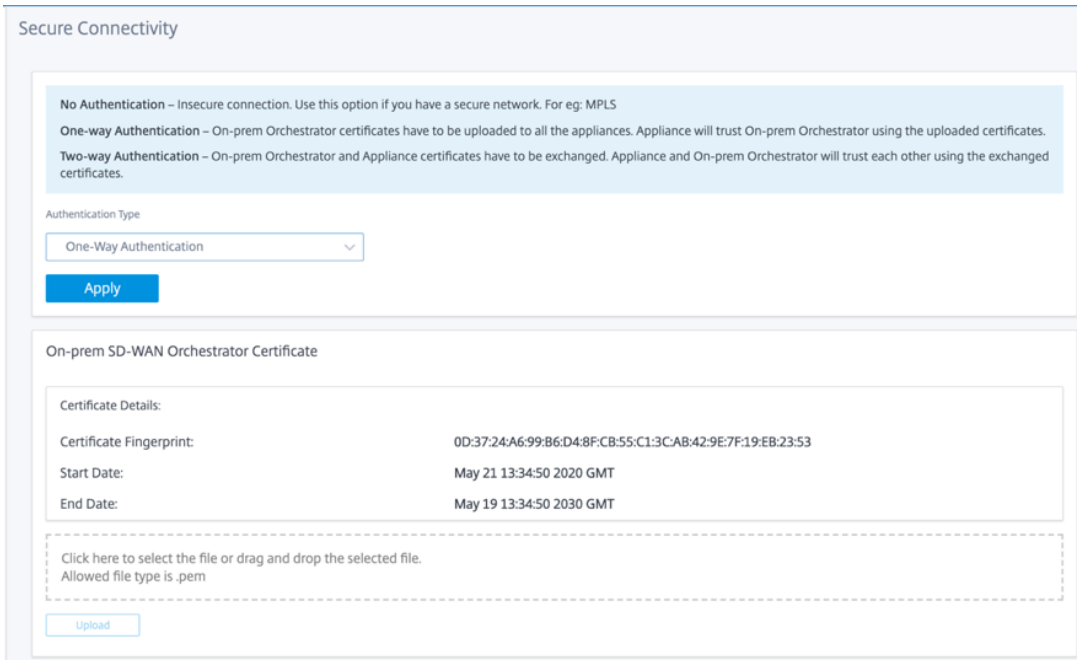
   > 注
   >
   > - 生成される証明書は X509 自己署名証明書です。
   > - 証明書の有効期限が切れたり、侵害されたりした場合は、証明書を再生成する必要があります。
   > - 証明書の有効期間は 10 年です。
   > - フィンガープリント、開始日、終了日などの証明書の詳細を表示できます。
   > - お客様は、On-Prem Orchestrator と SD-WAN アプライアンスの間で証明書が再生成され、交換されることを確認する必要があります。これにより、On-Prem Orchestrator とのアプライアンスの接続が切断されるのを防ぐことができます。

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。

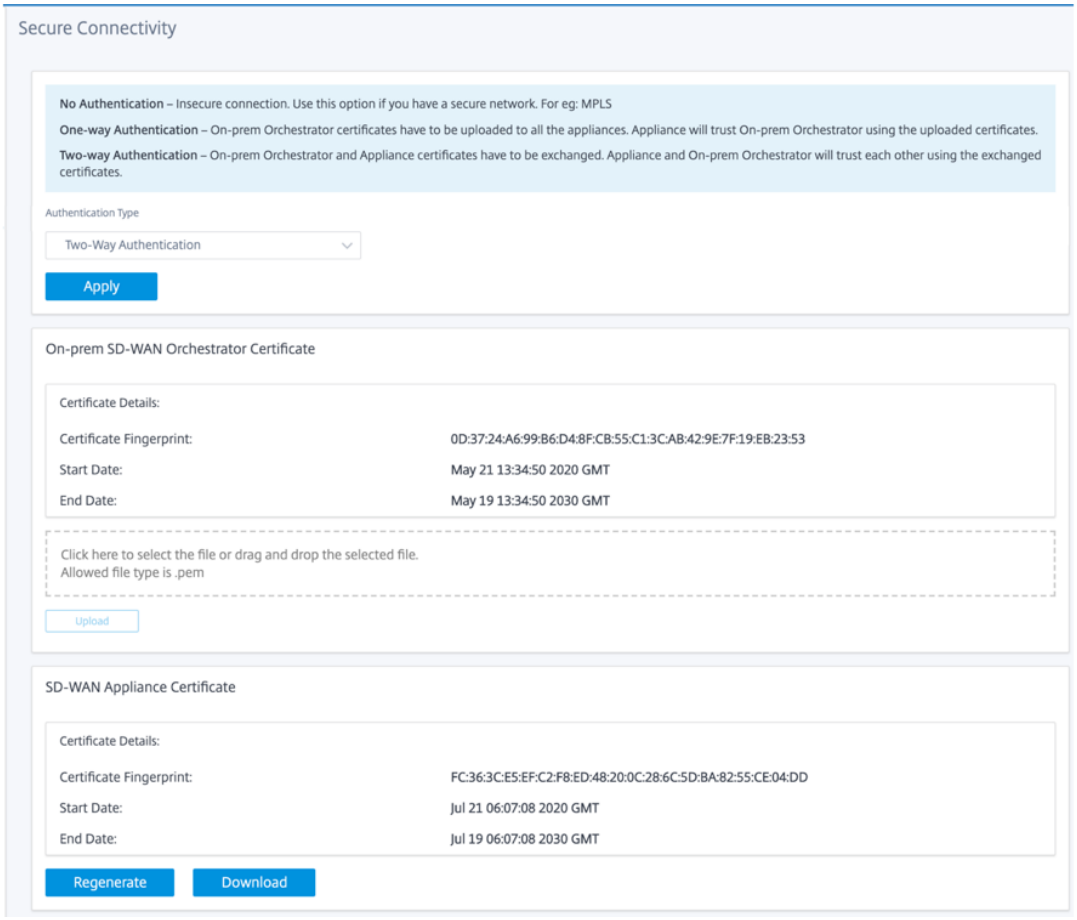
   - 認証なし—オンプレミスの SD-WAN Orchestrator と SD-WAN アプライアンスの間の認証は行われません。また、SD-WAN アプライアンスまたはオンプレミスの SD-WAN Orchestrator 証明書を使用する必要はありません。ただし、MPLS などのセキュアなネットワークがある場合は、このオプションを使用できます。



- 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使用して、オンプレミス Orchestrator を信頼します。



- 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 サーバー」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

Citrix SD-WAN 11.5 リリースアップグレードの影響

August 30, 2022

- Citrix SD-WAN 11.5.0 は限定可用性リリースであり、特定の顧客/本番環境でのみ推奨およびサポートされています。
- SD-WAN 11.5.0 リリースは、Advanced Edition（AE）、プレミアムエディション（PE）、WAN 最適化の展開をサポートしていません。
- SD-WAN 11.5.0 は、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に記載されているプラットフォームのみをサポートします。
- SD-WAN 11.5.0 は、オンプレミスの Citrix SD-WAN Center または Citrix SD-WAN Orchestrator をサポートしていません。
- SD-WAN 11.5.0 ファームウェアは、Citrix ダウンロードページでは利用できません。
- SD-WAN 11.5.0 リリースは、Citrix SD-WAN Orchestrator サービスを介してのみ利用可能で、選択した地理的 POP でのみ利用できます。
- 実稼働ネットワークに 11.5.0 を展開する前に、Citrix Product Management/Citrix サポートから必要な承認とガイダンスを取得してください。

システム要件

August 30, 2022

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 アプライアンスのセットアップ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

SD-WAN 11.5 リリース以降、SD-WAN アプライアンスのライセンスは、Citrix SD-WAN Orchestrator サービスを通じて管理されます。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

ブラウザーで 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 Edge 13+

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。

ハイパーバイザー

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

September 26, 2023

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

SD-WAN SE プラットフォームモデル	役割
210-SE/210-SE LTE	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
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 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。

アップグレード・パス

August 30, 2022

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。

構成

September 26, 2023

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。

初期セットアップ

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、構成パッケージの作成または変更、またはその他の複雑なタスクの実行時には、コンソールセッション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。

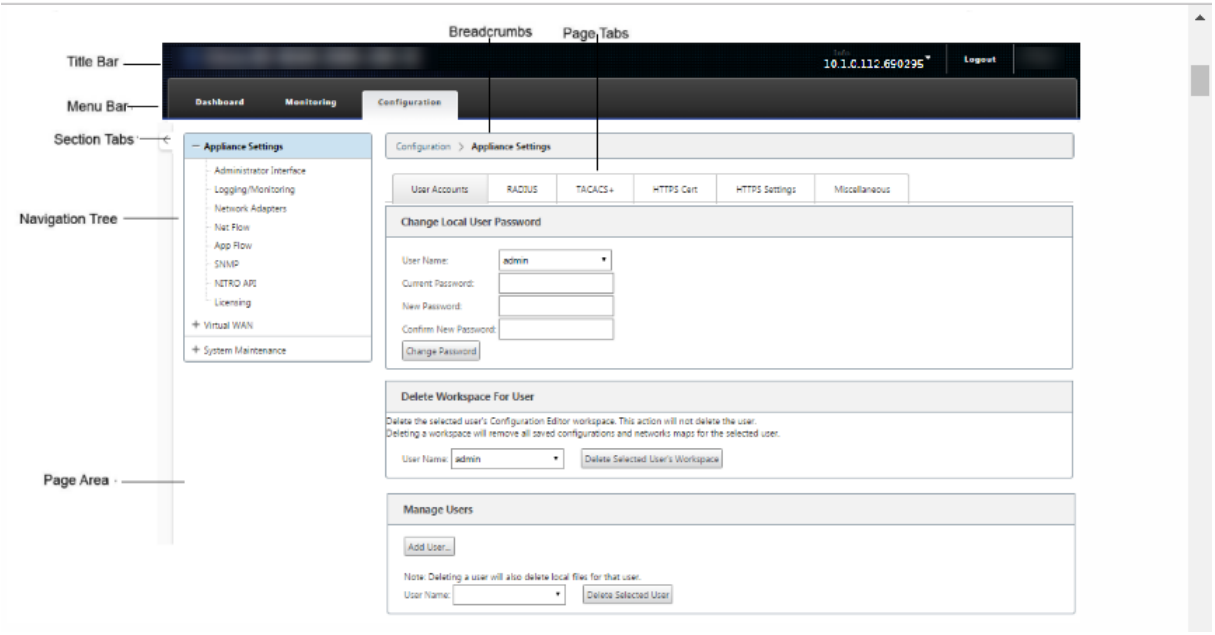
SD-WAN 仮想アプライアンス（SD-WAN VPX）のインストール手順については、次のセクションを参照してください。

- SD-WAN VPX について。
- ESXi での SD-WAN VPX-SE のインストールとデプロイ

Web インターフェイス **(UI)** レイアウトの概要

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。<! —構成エディタと変更管理ウィザードの特定のナビゲーション手順も表示されます。—>

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] ボタンも含まれています。
- メイン・メニュー・バー：これは、Management Web Interface の各画面のタイトル・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すると、そのセクションのナビゲーションツリーが表示されます。
- ナビゲーションツリー：ナビゲーションツリーは、左側のペインのメインメニューバーの下にあります。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すると、そのセクションのナビゲーションツリーが表示されます。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。

- ブレッドクラム -現在のページへのナビゲーションパスが表示されます。ブレッドクラムは、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および作業領域です。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さらに表示するためのタブがあります。これらは、ページ領域の上部、ブレッドクラム表示のすぐ下にあります。変更管理ウィザードの場合と同様に、タブがページ領域の左側の表示枠、ナビゲーションツリーとページの作業領域の間にある場合があります。
- 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より多くのフィールドを表示できます。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。

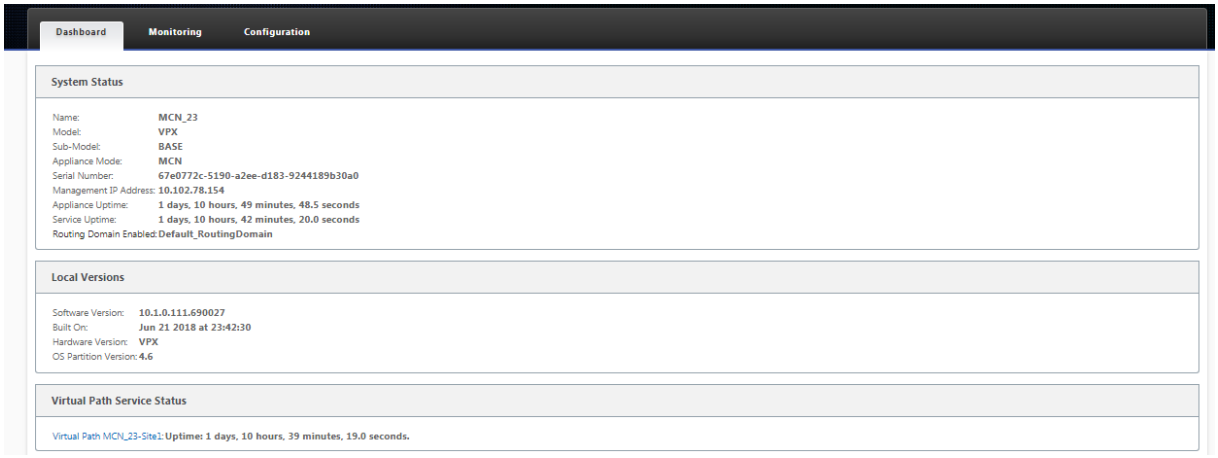
  ページでサイズ変更バーを使用できない場合は、ブラウザの右端をクリックしてドラッグし、ページ全体を表示できます。

Web 管理インターフェイスのダッシュボード　[**Dashboard**] 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。

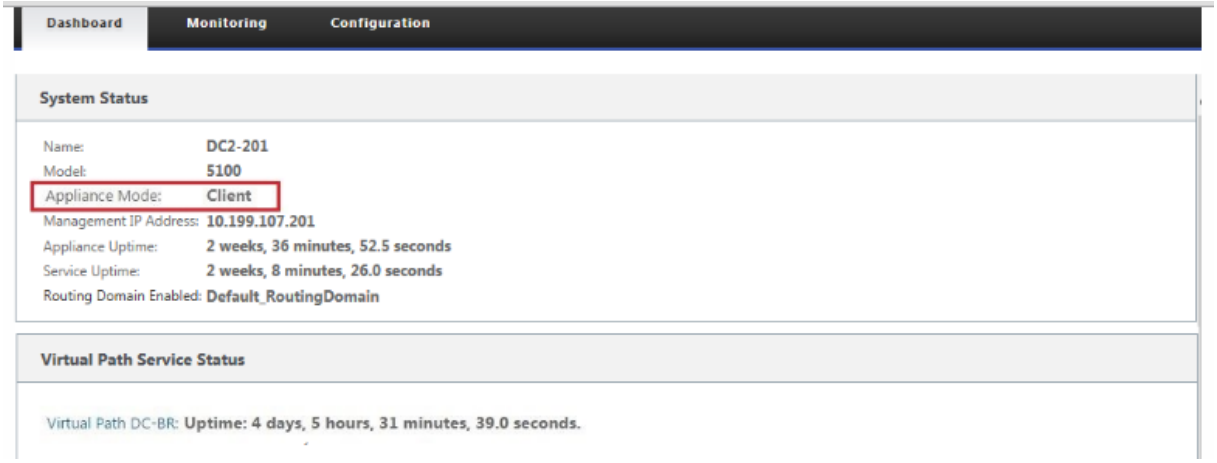
[ダッシュボード（Dashboard）] ページには、アプライアンスに関する次の基本情報が表示されます。

- 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の表示例を示しています。



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。



アプライアンスハードウェアの設定

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 アドレスを構成しなかった場合は、「SD-WAN VPX-SE の管理 IP アドレスの設定」セクション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 アドレスを構成しなかった場合は、「SD-WAN VPX-SE の管理 IP アドレスの設定」セクション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

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。

> 注
>
> - 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。

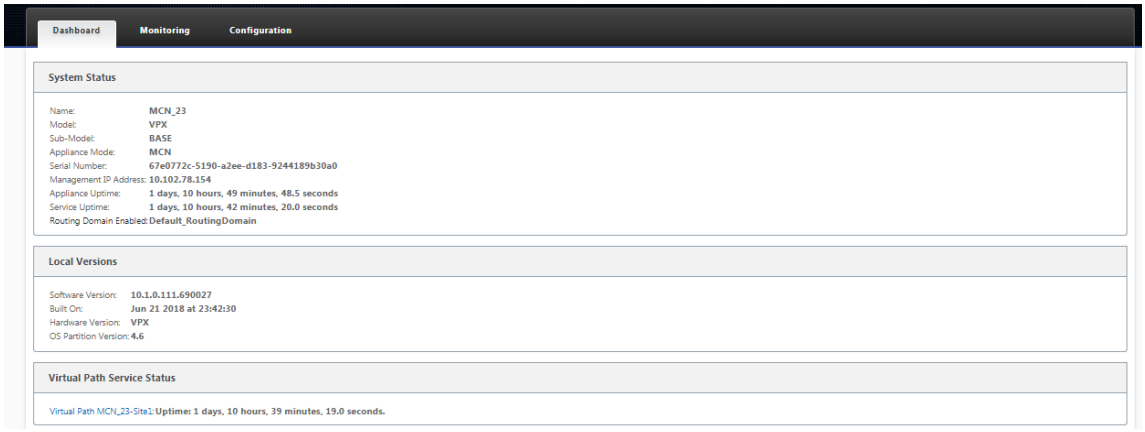
   これにより、接続されたアプライアンスで SD-WAN 管理 Web インターフェイスのログイン画面が開きます。

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。



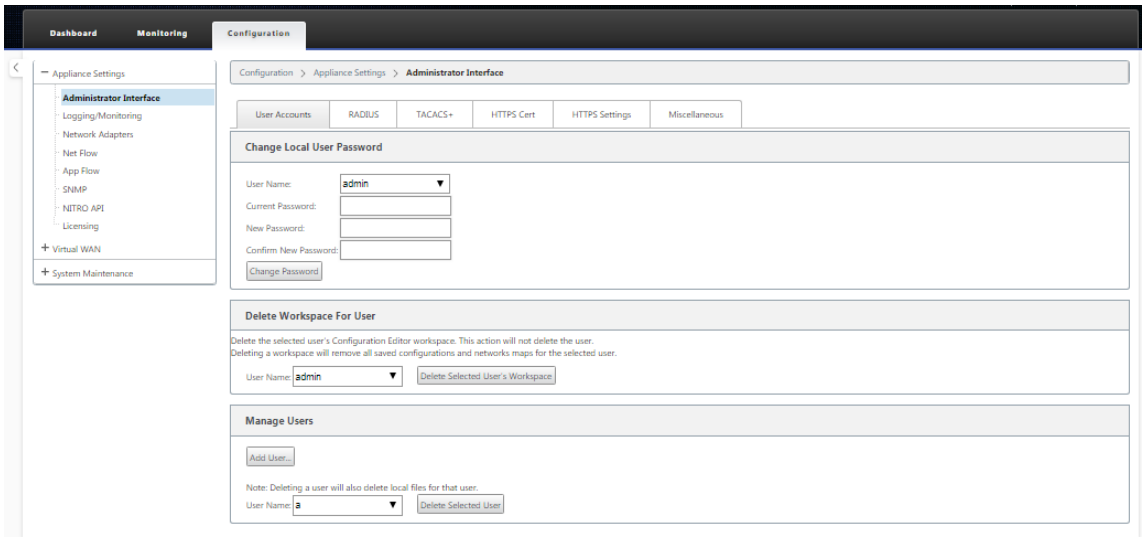
アプライアンスの管理 Web インターフェイスに初めてログインすると、ダッシュボードにアラートアイコン（ゴールデンロッドデルタ）と、SD-WAN サービスが無効になっており、ライセンスがインストールされていないことを示すアラートメッセージが表示されます。現時点では、このアラートは無視できます。このアラートは、ライセンスをインストールし、アプライアンスの構成および展開プロセスを完了した後に解決されます。

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。

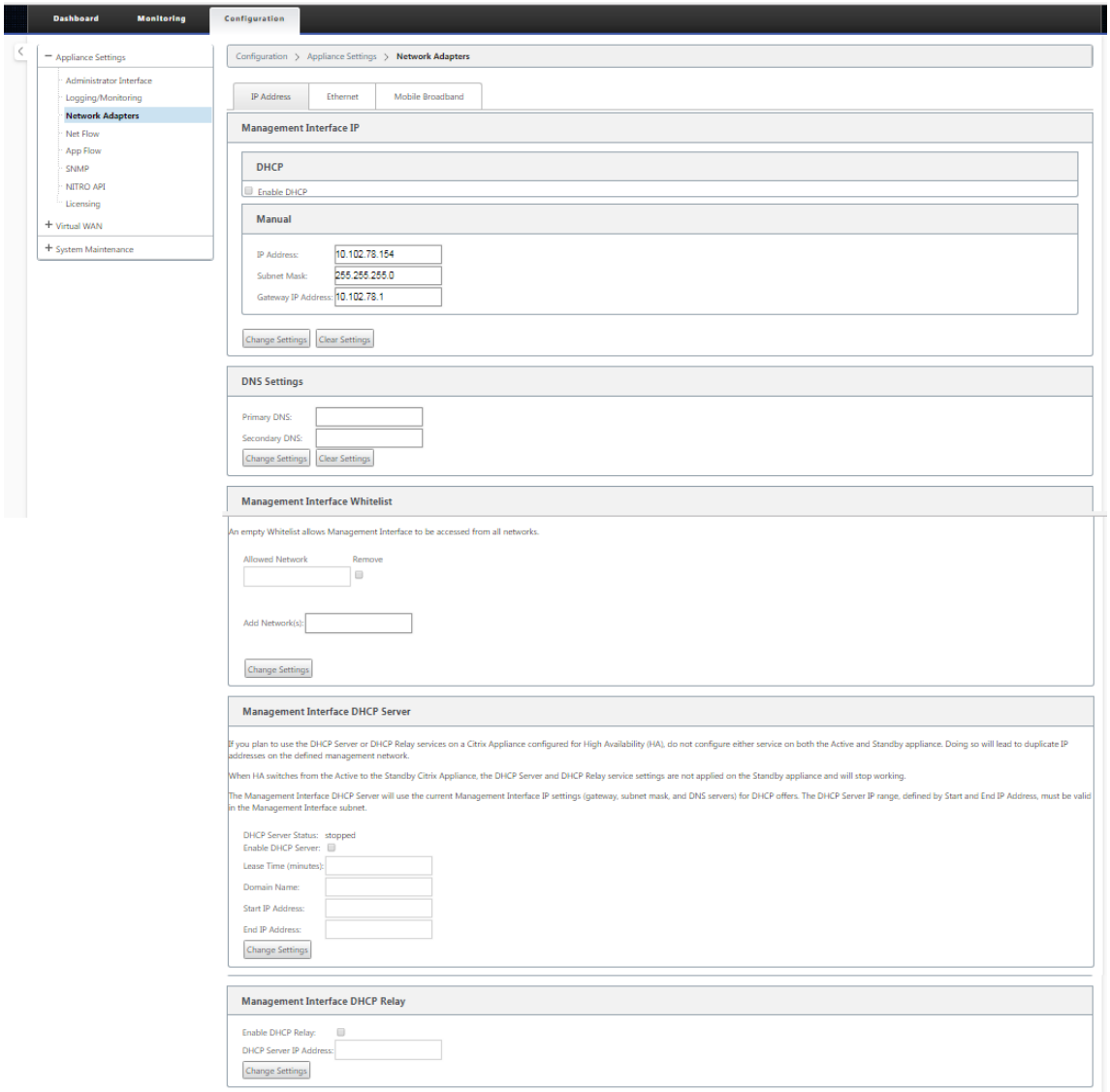
   これにより、画面の左ペインに [構成] ナビゲーションツリーが表示されます。[構成] ナビゲーションツリーには、次の 3 つの主要なブランチがあります。

   - 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。



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。



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。

> 注
>
> - 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]>`

    例: `https://[fd73:xxxx:yyyy:26::9]`

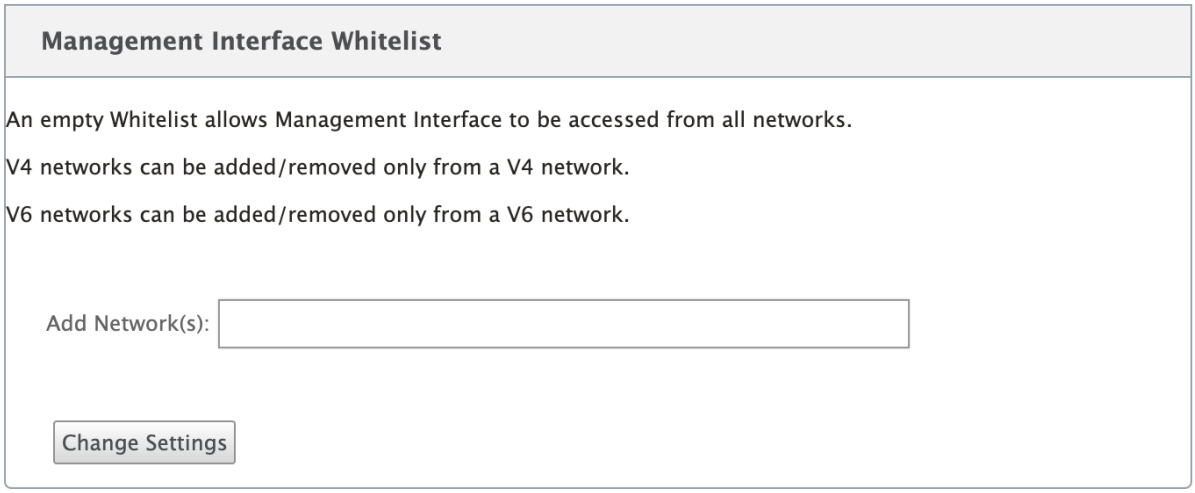
    接続に成功すると、構成したアプライアンスの SD-WAN 管理 Web インターフェイスの [ログイン] 画面が表示されます。

    > 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。



日付と時刻の設定

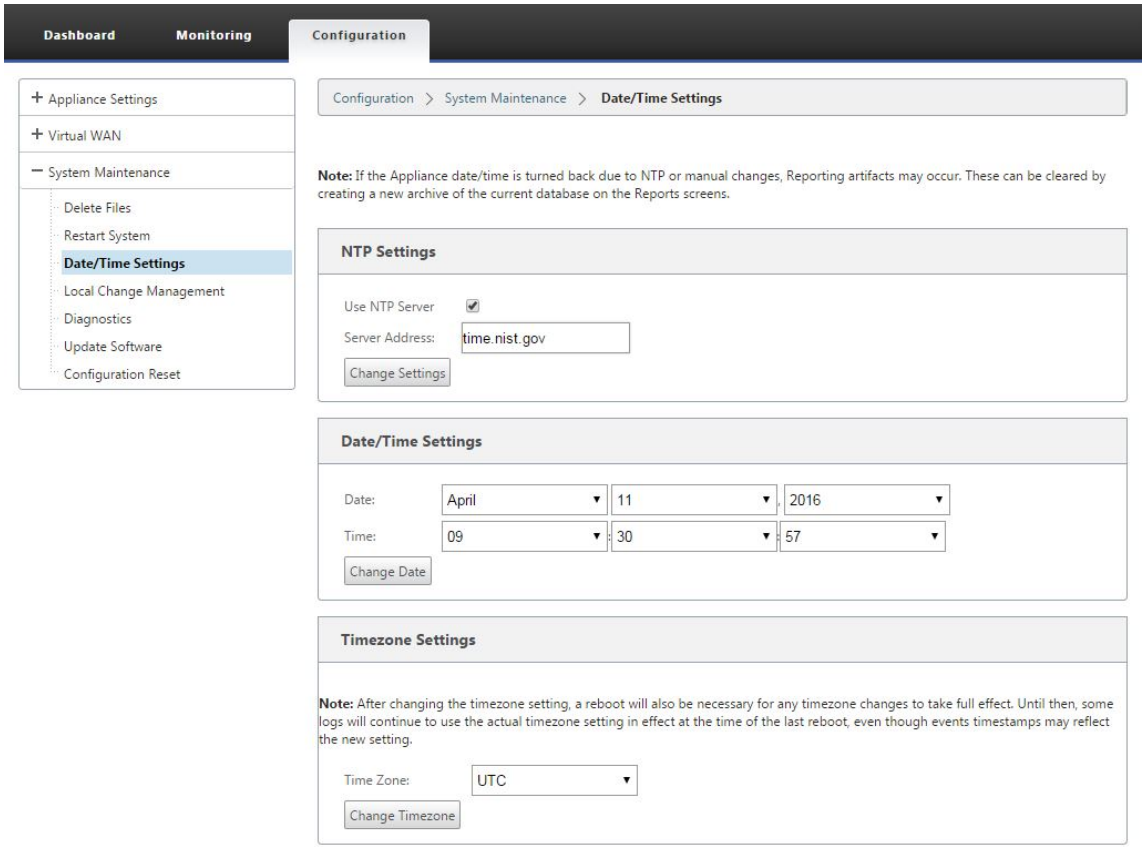
アプライアンスに SD-WAN ソフトウェア・ライセンスをインストールする前に、アプライアンスに日付と時刻を設定する必要があります。

> 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** サーバーを使用する] を選択します。
   b) [サーバアドレス（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（緑色のチェックマーク）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**]** 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、秒を選択します。

10. [日付の変更] 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。

次のステップは、コンソールセッションタイムアウトしきい値を最大値に設定することです。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の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、設定手順を最初から繰り返します。

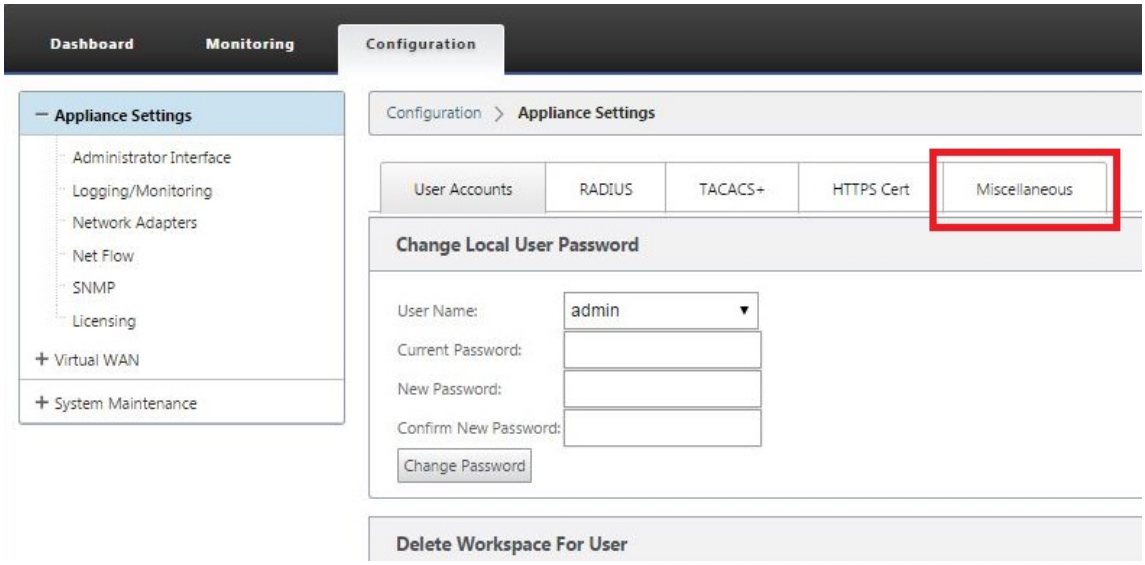
セッションのタイムアウト

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。

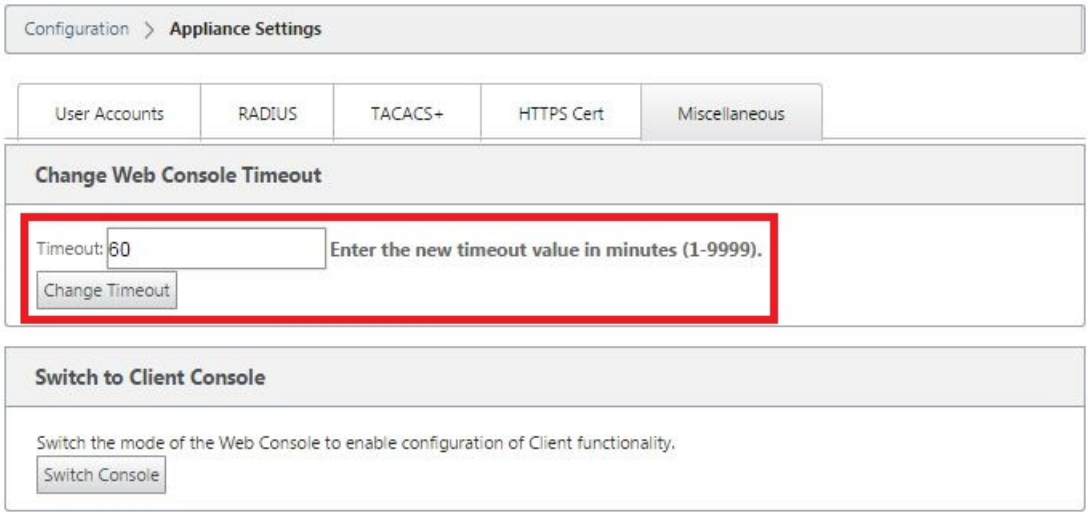
1. 「構成」タブを選択し、ナビゲーション・ツリーで「アプライアンスの設定」ブランチを選択します。

   「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」タブがあらかじめ選択されています。



2. [その他] タブ (右端) を選択します。

   これにより、[その他] タブページが表示されます。



3. コンソールの [タイムアウト] 値を入力します。

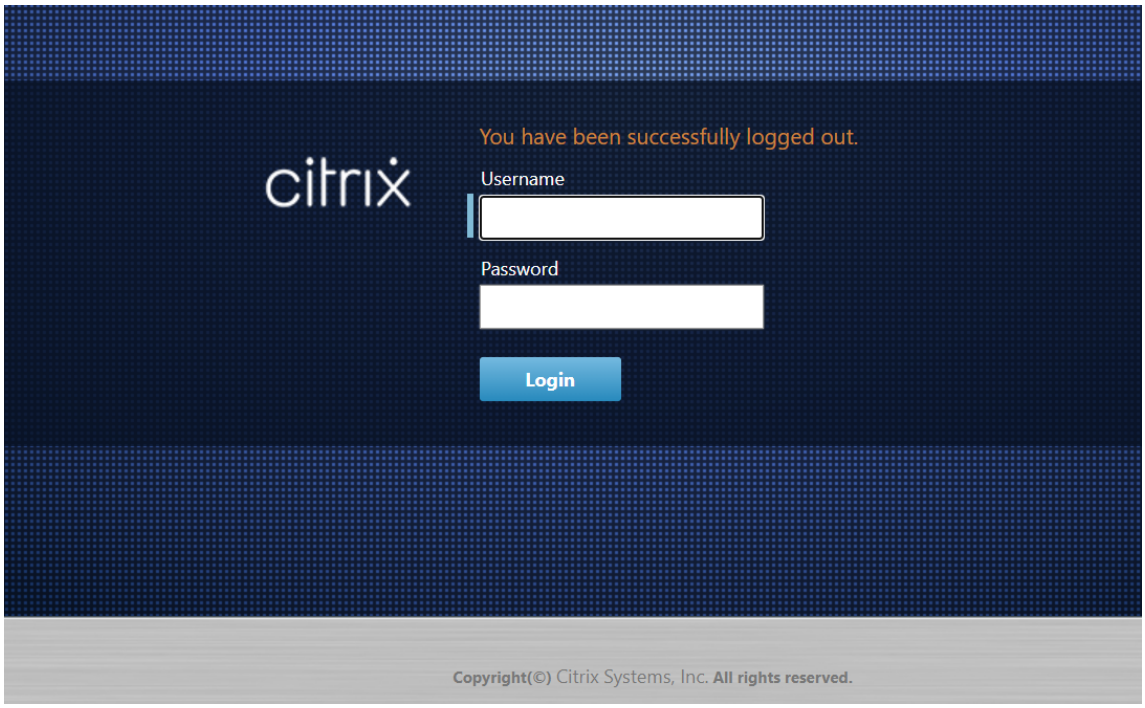
   [**Web **** コンソールのタイムアウトの変更 **] セクションの [タイムアウト] フィールドに、最大値 9999 までの大きい値 (分単位) を入力します。デフォルトは 60 で、初期設定セッションでは非常に短すぎます。

   > 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。

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。



5. 管理者ユーザー名 (*admin*) とパスワード (*password)* 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。

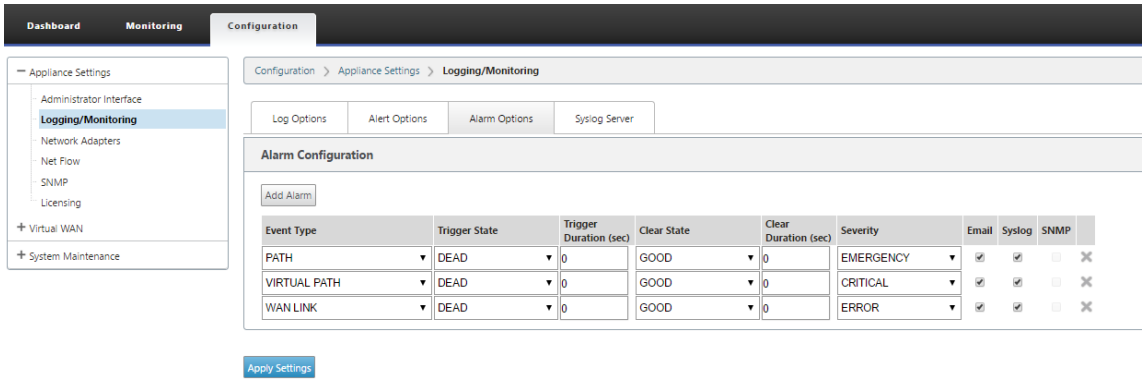
アラームの設定

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、設定 > ** アプライアンスの設定 ** > ロギング/モニタリングにナビゲートし、アラームオプションをクリックして下さい。
2. [**Add Alarm**] をクリックして、新しいアラームを追加します。



3. 次のフィールドの値を選択または入力します。

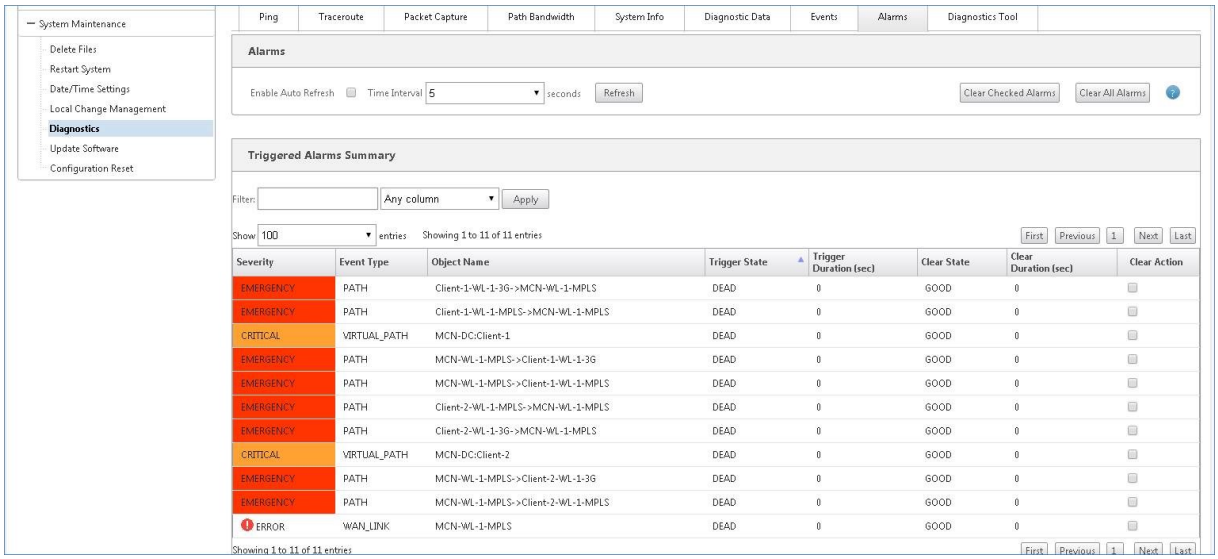
   - イベントタイプ:SD-WAN アプライアンスは、ネットワーク内の特定のサブシステムまたはオブジェクトに対してアラームをトリガーできます。これらはイベントタイプと呼ばれます。使用可能なイベントタイプは、SERVICE、VIRTUAL_PATH、WANLINK、PATH、DYNAMIC_VIRTUAL_PATH、WAN_LINK_CONGESTION、USAGE_CONGESTION、FAN、POWER_SUPPLY、PROXY_ARP、ETHERNET、DISCOVERED_MTU、GRE_TUNNEL、IPSEC_TUNNEL です。
   - トリガー状態**:** イベントタイプのアラ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。
   - クリア期間**:** 秒単位の時間。これにより、アラームがクリアされるまでの待機時間が決まります。「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とクリアアラートは、Syslog を介して送信されます。
   - **SNMP**: イベントタイプのアラームトリガーとクリアアラートは、SNMP トラップを介して送信されます。

4. 必要に応じて、引き続きアラームを追加します。
5. [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要約を表示するには、次の手順を実行します。

SD-WAN Web 管理インターフェイスでは、設定 > システムメンテナンス **>** 診断 **** アラームにナビゲートして下さい **。

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。



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。

1. SD-WAN Web 管理インターフェイスでは、設定 > システムメンテナンス **>** 診断 **** アラームにナビゲートして下さい **。
2. [アクションのクリア（Clear Action）] 列で、クリアするアラームを選択します。
3. [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。

マスター制御ノードの設定

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、これはデータセンターにデプロイされた仮想 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。

Citrix SD-WAN 11.5 リリース以降、Citrix SD-WAN Orchestrator サービスを介して MCN をセットアップできま

す。詳細については、「[展開とサイト構成](/ja-jp/citrix-sd-wan-orchestrator/site-level-configuration/basic-settings.html)」を参照してください。

クライアントアプライアンスのネットワークへの接続

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。

CloudInit を使用して **OpenStack** で **Citrix SD-WAN Standard Edition** を展開する

OpenStack 環境に Citrix SD-WANStandard 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。

> 注
>
> 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。

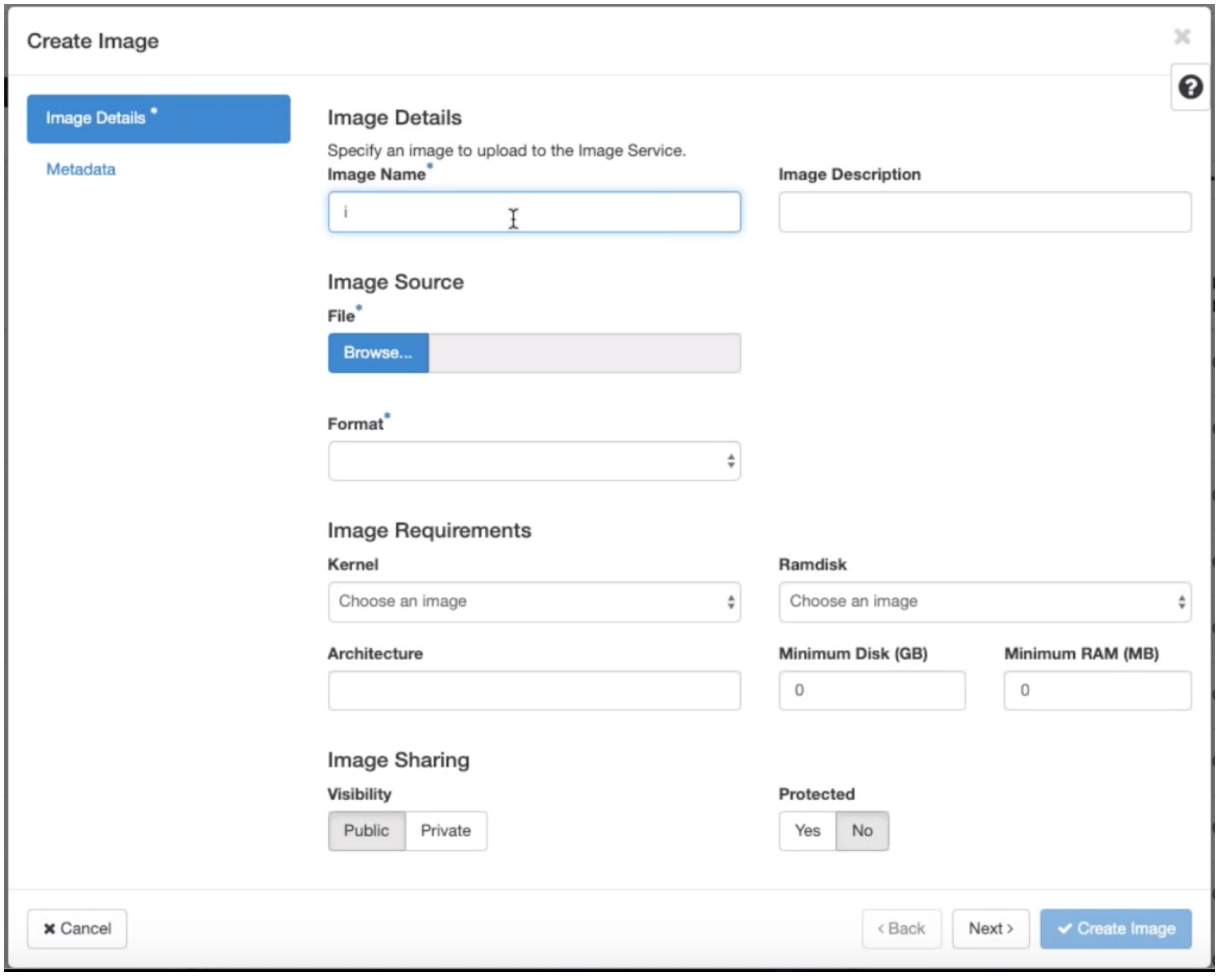
OpenStack の SD-WAN インスタンスの場合、ユーザーからの管理 IP、DNS、およびシリアル番号に必要な入力。Cloudinit スクリプトはこれらの入力を解析し、指定された情報を使用してインスタンスをプロビジョニングします。

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、[イメージの作成] をクリックします。

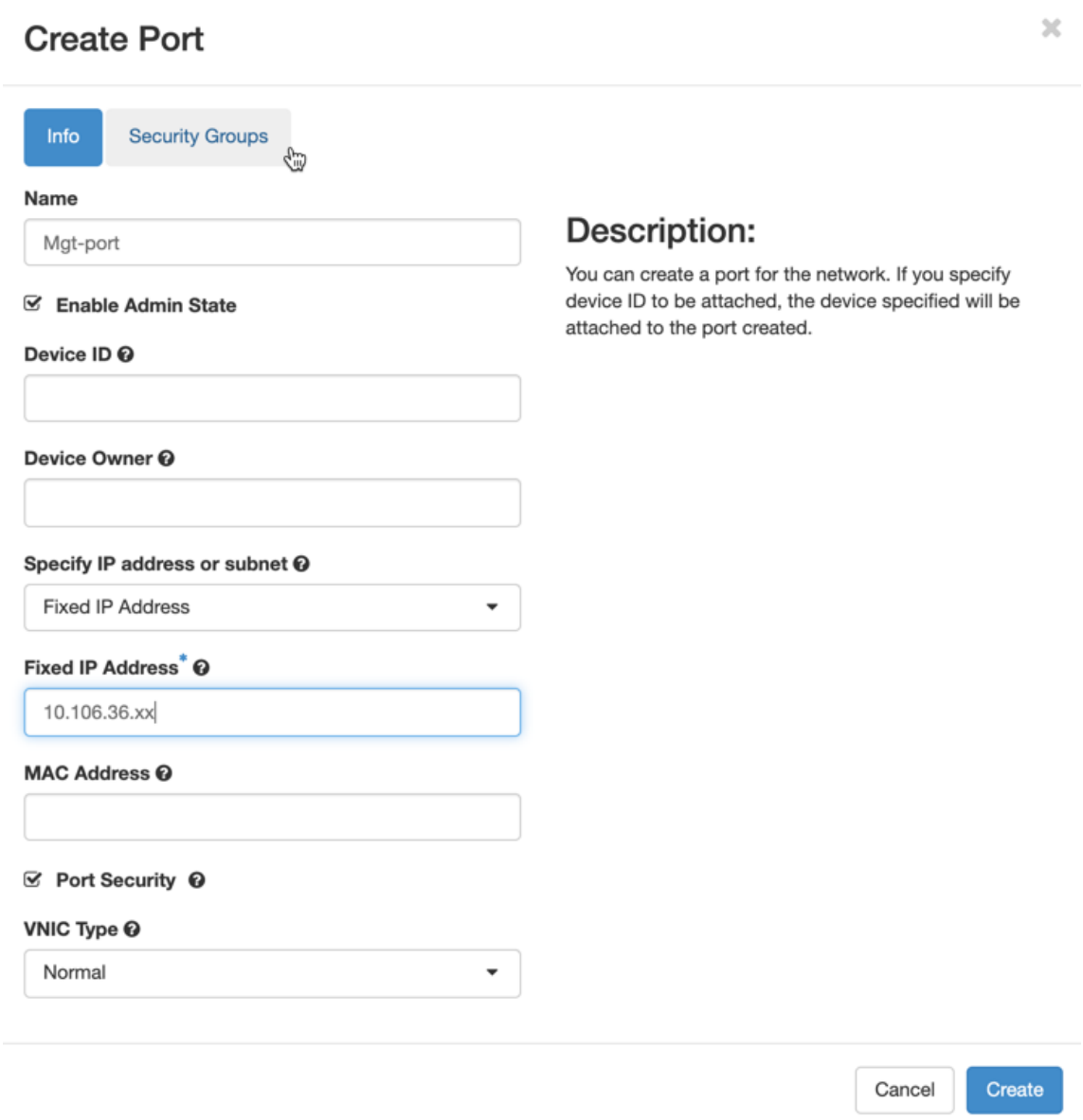


- イメージ名 -イメージ名を指定します。
- イメージの説明—イメージの説明を追加します。
- **File** -ローカルドライブから kvm.qcow2 イメージファイルを参照して選択します。
- フォーマット—ドロップダウンリストから QCOW2 —QEMU エミュレータのディスクフォーマットを選択します。

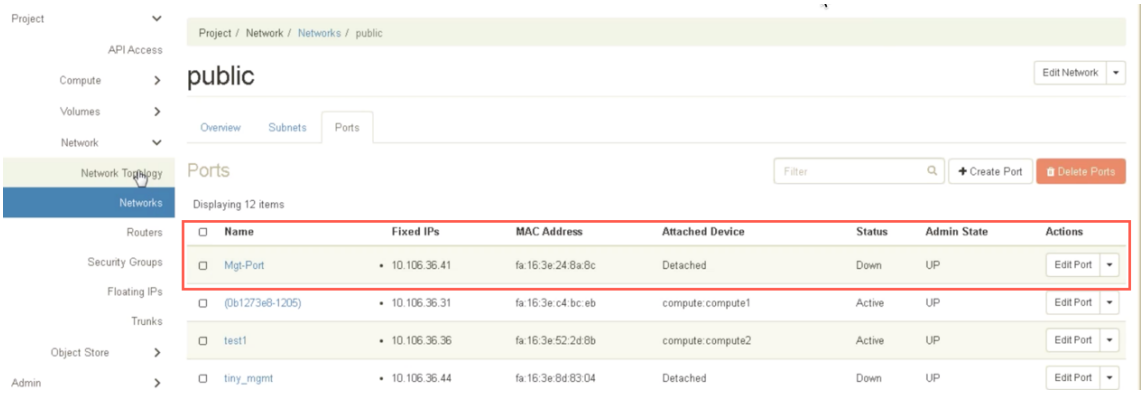
[**Create Image**] をクリックします。

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] の [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て [作成] をクリックします。



[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。

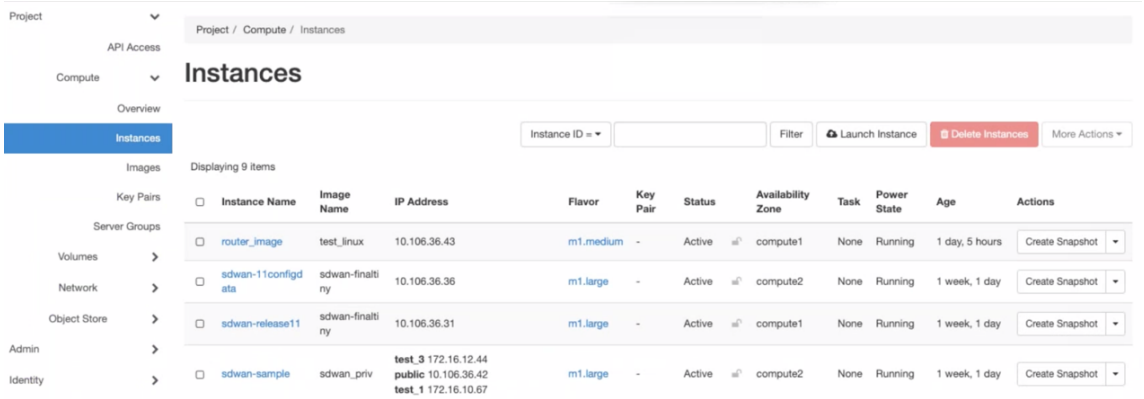


ポートが作成され、どのデバイスにも接続されていないので、現在のステータスは [Detached] と表示されま

す。

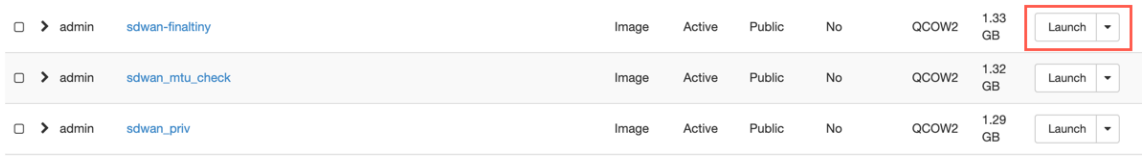
OpenStack インスタンスを作成して、config-drive を有効にし、user_data を渡します。

3. OpenStack にログインし、インスタンスを設定します。



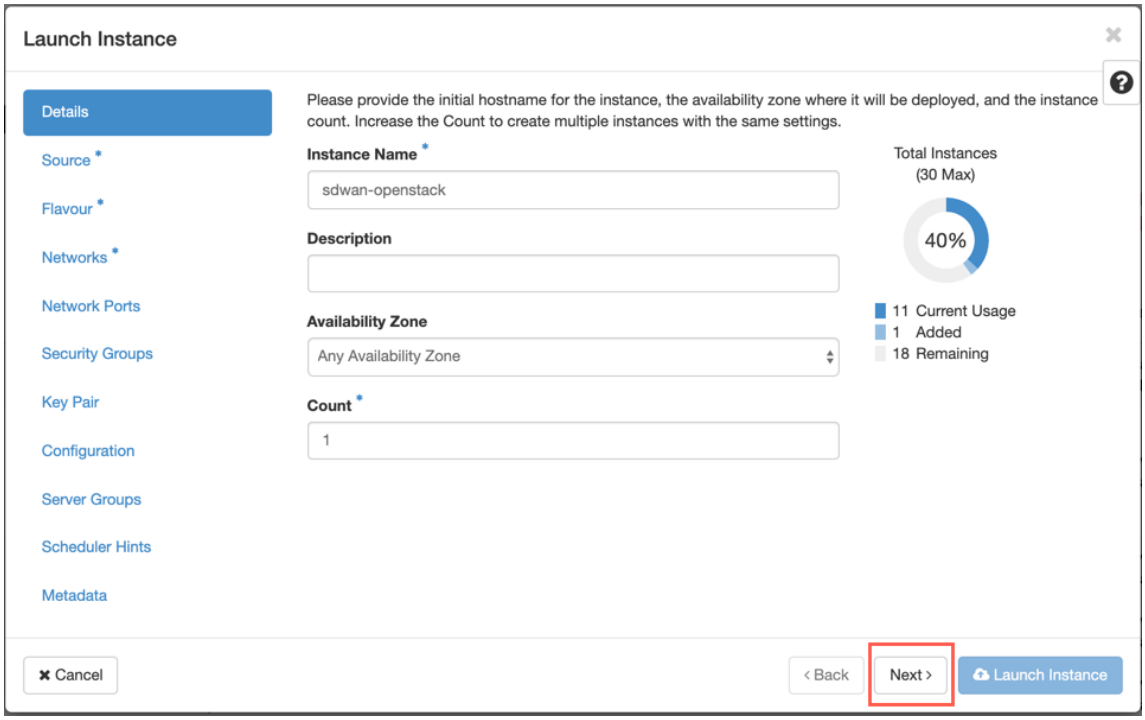
4. **kvm.qcow2.gz** ファイルをダウンロードし、解凍します。
5. [インスタンス] に移動し、[インスタンスの起動] をクリックします。

> 注:
>
> [インスタンス] に戻り、[** インスタンスの起動 **] をクリックするか、イメージが作成されたら [イメージ] 画面から [**Launch**] をクリックします。

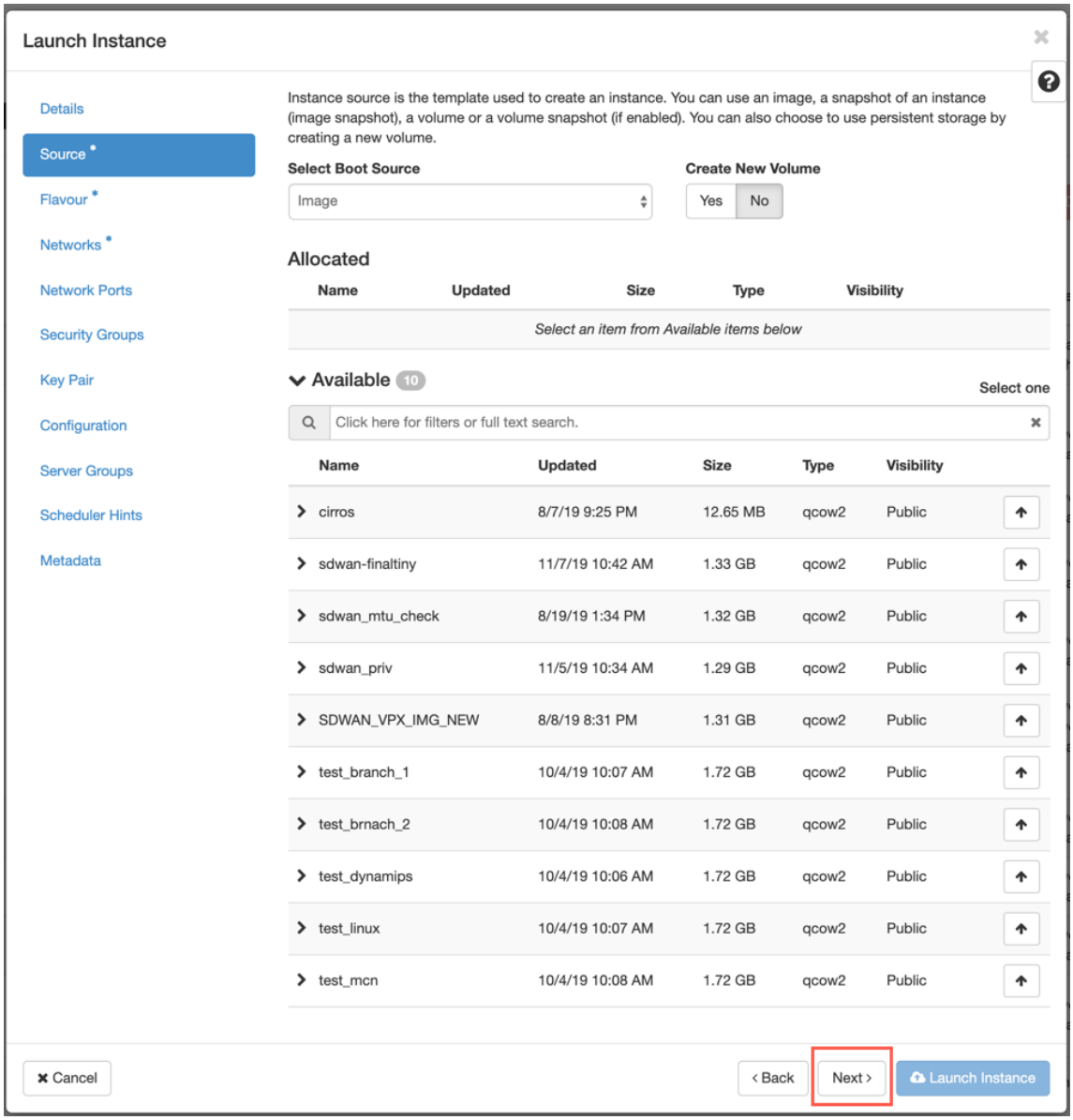


6. [詳細] タブで、次の情報を入力します。

   - 「インスタンス名」—インスタンスのホスト名を指定します。
   - 説明—インスタンスの説明を追加します。
   - [**Availability** Zone] —インスタンスをデプロイするアベイラビリティー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] —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。



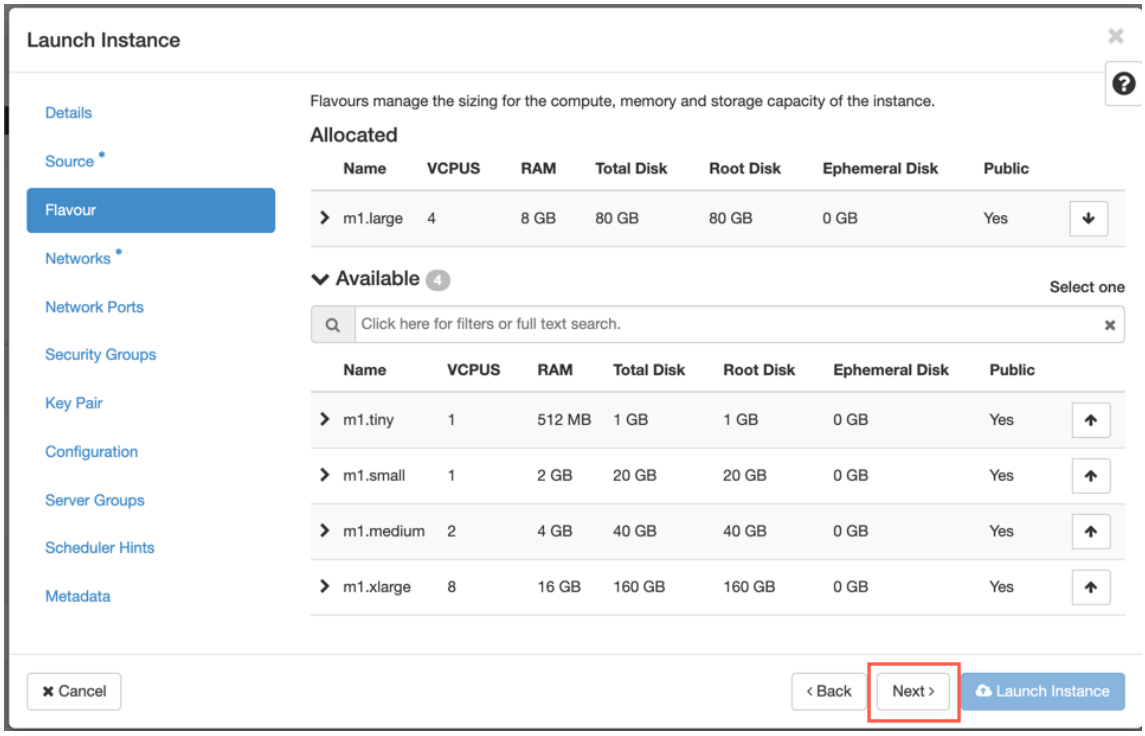
7. [ソース] タブで、[新しいボリュームの作成] で [いいえ] を選択し、[次へ] をクリックします。インスタンスソースは、インスタンスの作成に使用されるテンプレートです。



8. インスタンスの [**Flavour**] を選択し、[Next] 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。

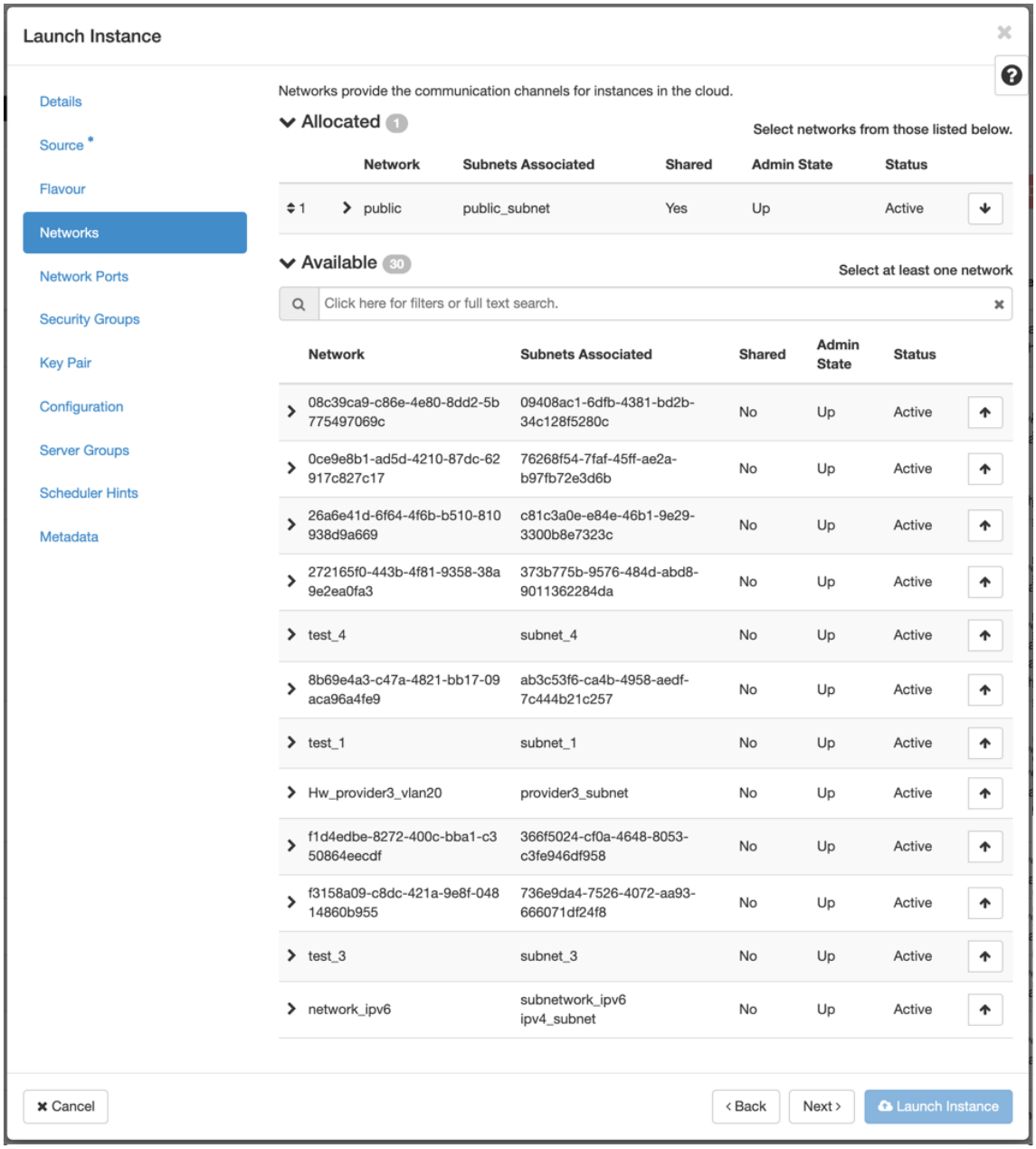
> 注
>
> 選択するフレーバーには、作成しようとしているインスタンスのタイプをサポートするのに十分なリソースが割り当てられている必要があります。インスタンスに十分なリソースを提供していないフレーバーが、使用可能なテーブルで黄色の警告アイコンで識別されます。

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。



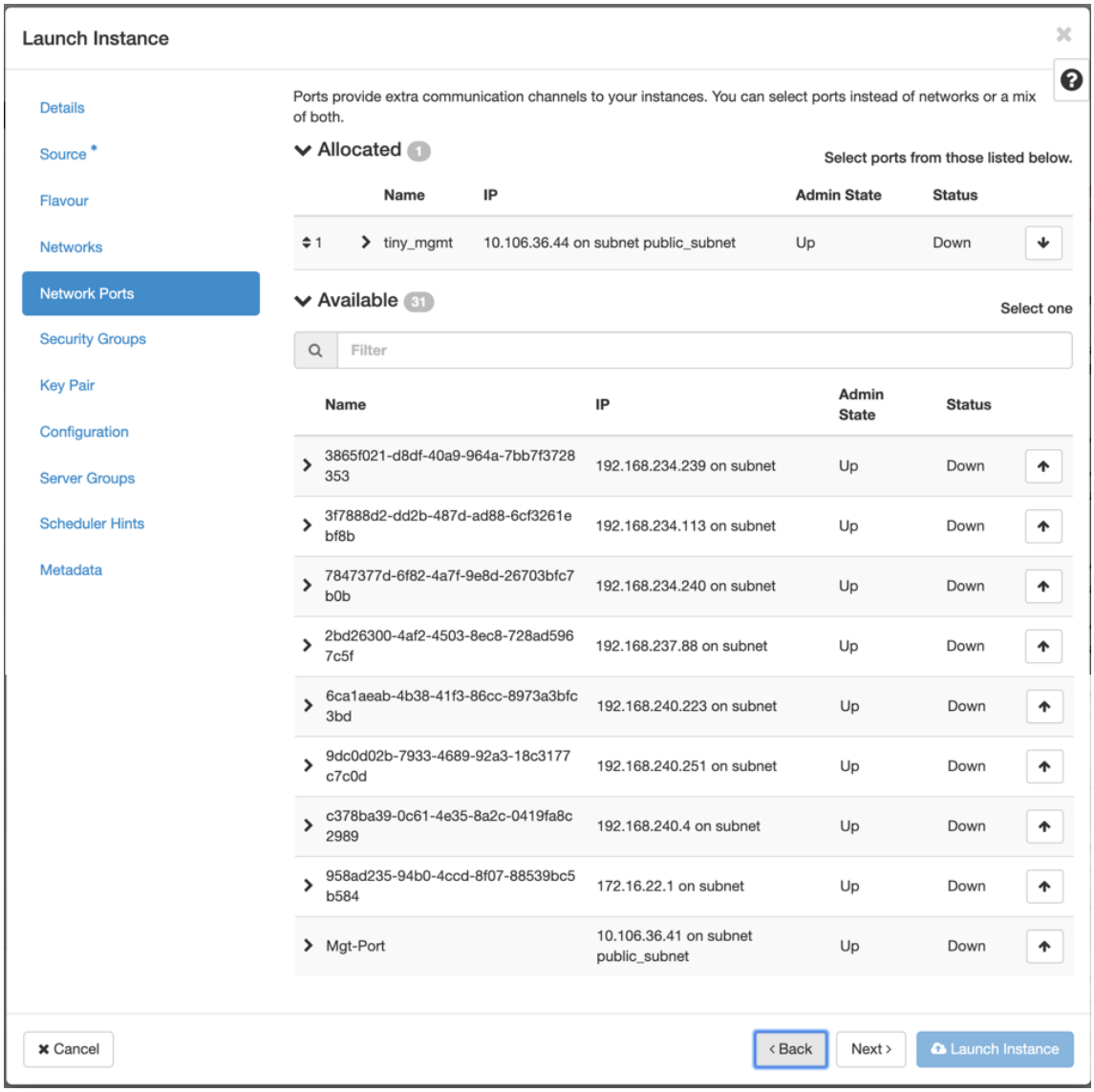
9. ネットワークを選択し、[次へ] をクリックします。ネットワークは、インスタンスの通信チャネルを提供します。

> 注
>
> 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。

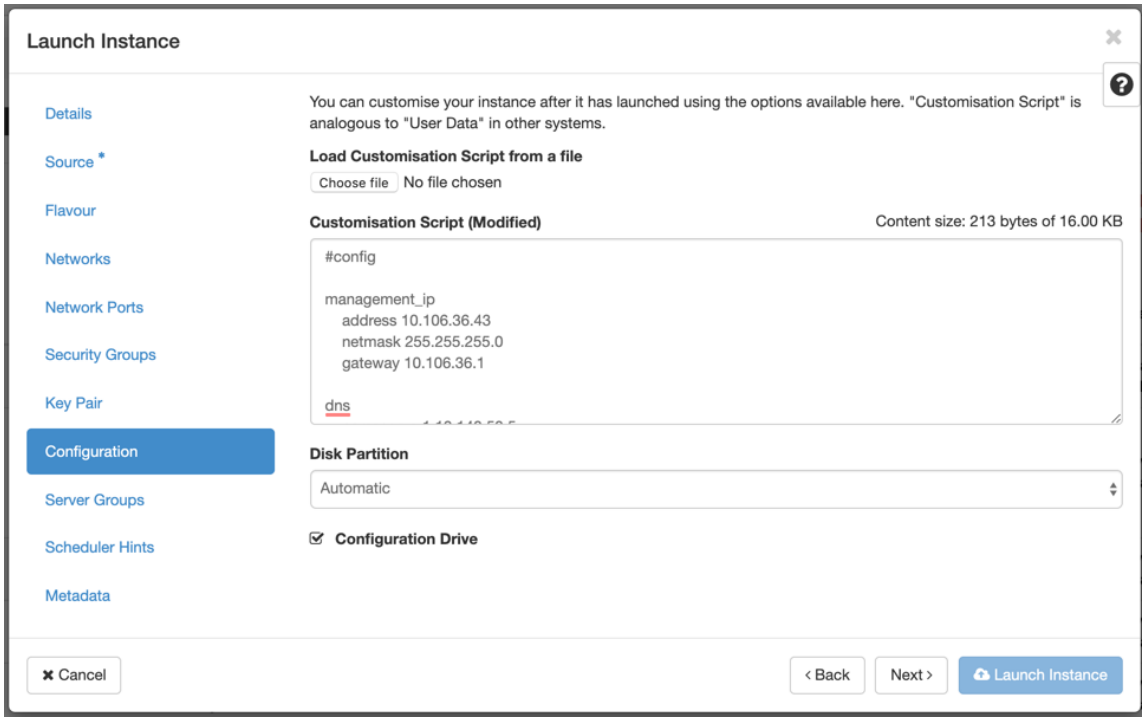


10. インスタンスのネットワークポートを選択し、[**Next**] をクリックします。ネットワークポートは、インスタンスへの追加の通信チャネルを提供します。

> 注
>
> 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。



11. [構成] に移動し、[ファイルの選択] をクリックします。user_data ファイルを選択します。user_data ファイルでは、管理 **IP**、**DNS**、およびシリアル番号の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。



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

August 30, 2022

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。ネットワークで LTE サイトを構成および管理する方法については、「LTE ファームウェアのアップグレード」を参照してください。

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。

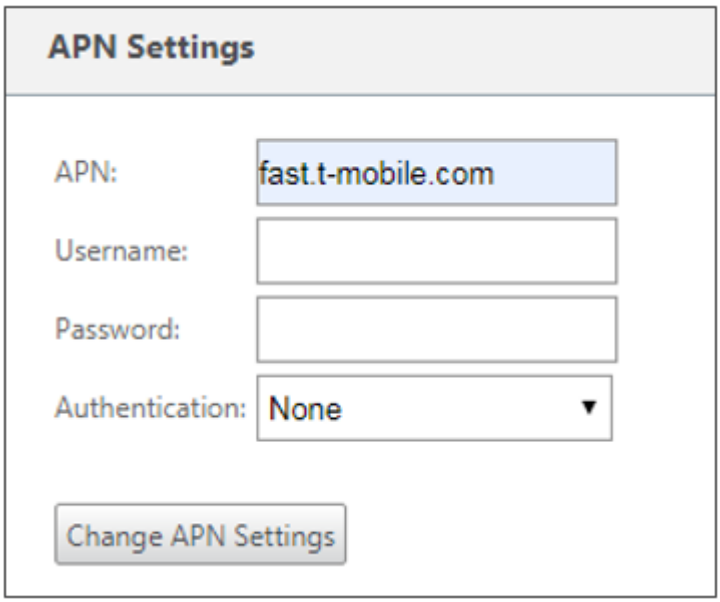
> 注:
> 標準または 2FF SIM カード (15x25 mm) のみがサポートされています。

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。

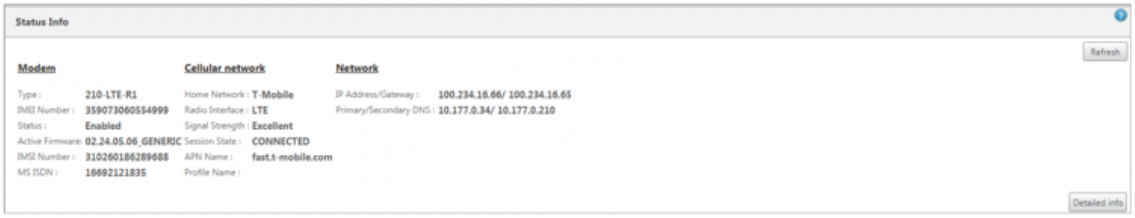
> 注:
> APN 情報をキャリアから入手します。



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。

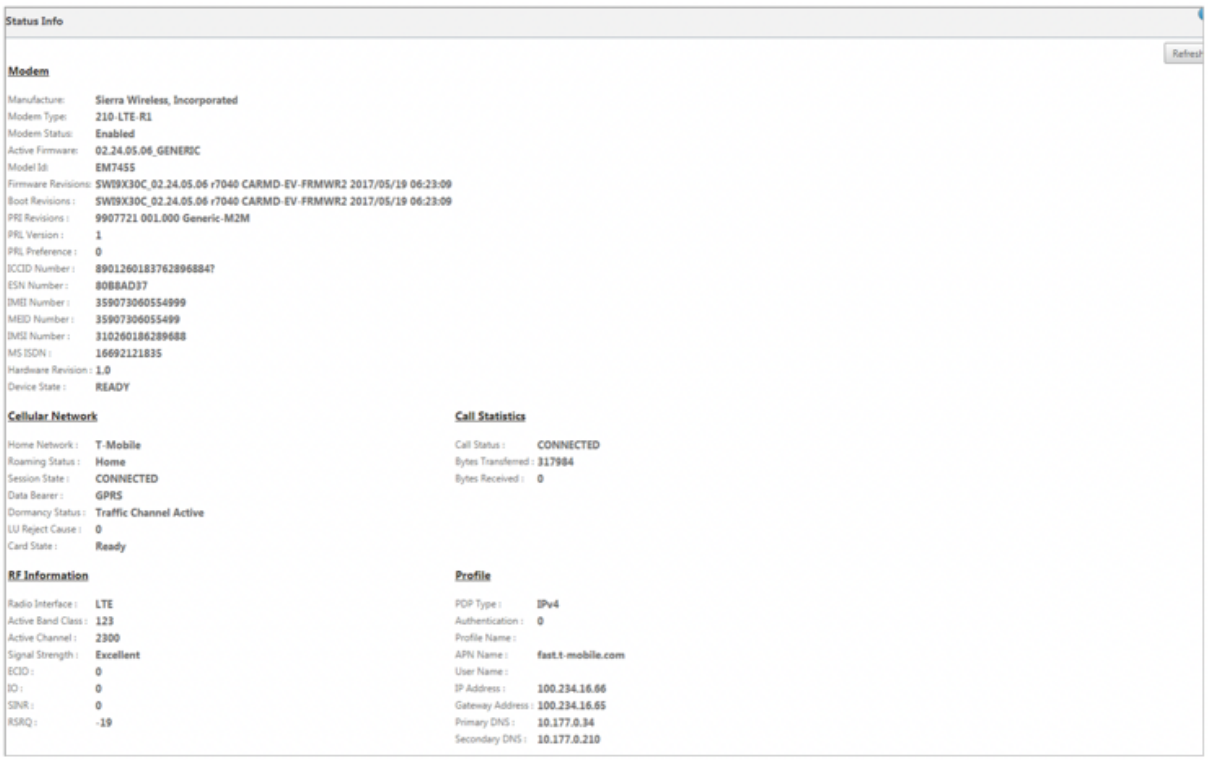
7. SD-WAN アプライアンス GUI で、設定 **>** アプライアンス設定 **>** ネットワークアダプタ **>** モバイルブロードバンドにナビゲートして下さい。

   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。

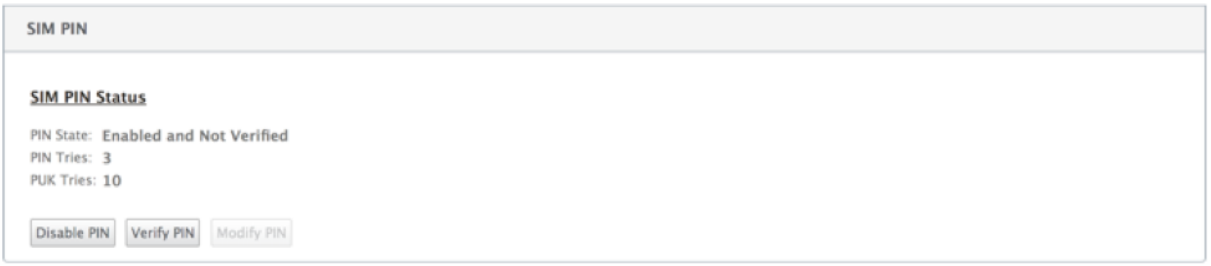
- 動作モード：モデムの状態を表示します。
- アクティブ **SIM**：アクティブになることができる SIM はいつでも、1 つのみです。現在アクティブになっている SIM を表示した。
- カードの状態：Present は SIM が正しく挿入されていることを示します。
- 信号強度: 信号強度の品質-優秀、良好、公正、不良、または信号なし。
- ホームネットワーク: 挿入された SIM のキャリア。
- **APN** 名:LTE モデムが使用するアクセスポイント名。
- セッション状態：Connected は、デバイスがネットワークに参加したことを示します。セッション状態が切断されている場合は、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。



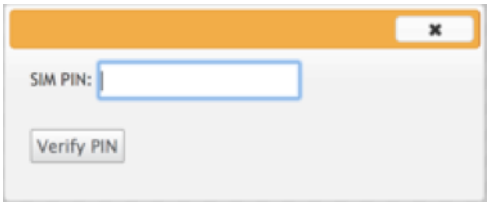
SIM ピン

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。

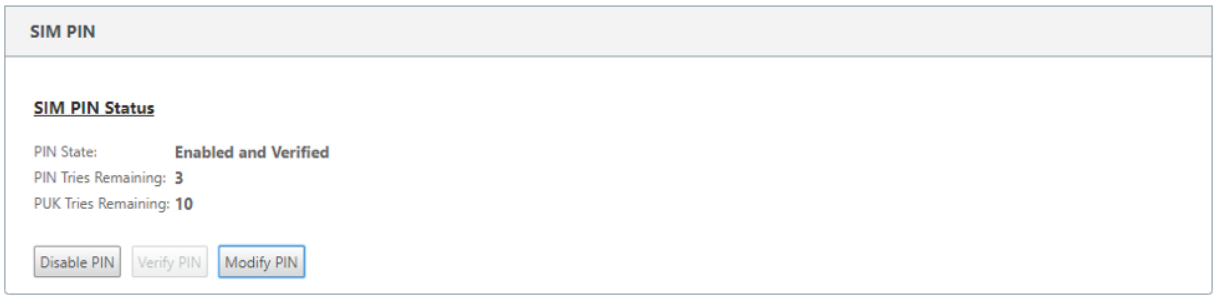
SIM PIN 操作を実行するには、[構成] **>** [アプライアンスの設定] **>** [ネットワークアダプタ] **>** [モバイルブロードバンド] **>** [**SIM PIN**] に移動します。



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。

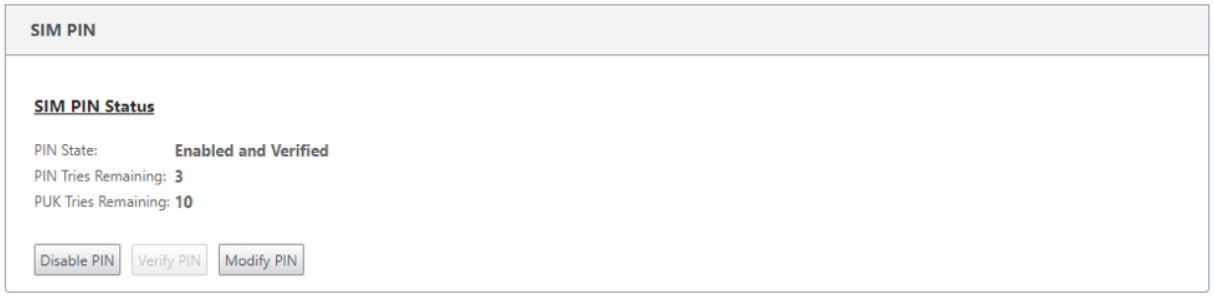


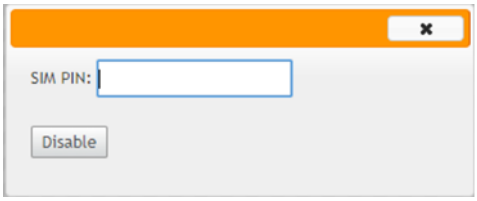
ステータスが [有効] および [確認済み] に変わります。



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。

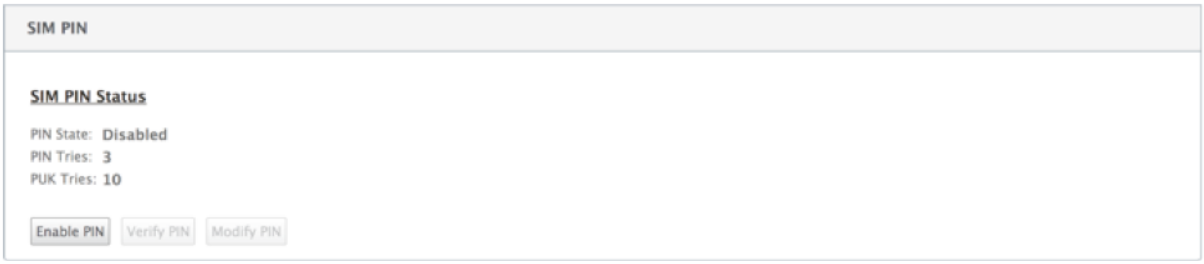




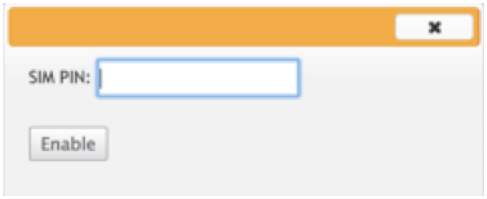
PIN を無効にするをクリックします。**SIM PIN** を入力し、[無効] をクリックします。

SIM PIN を有効にする

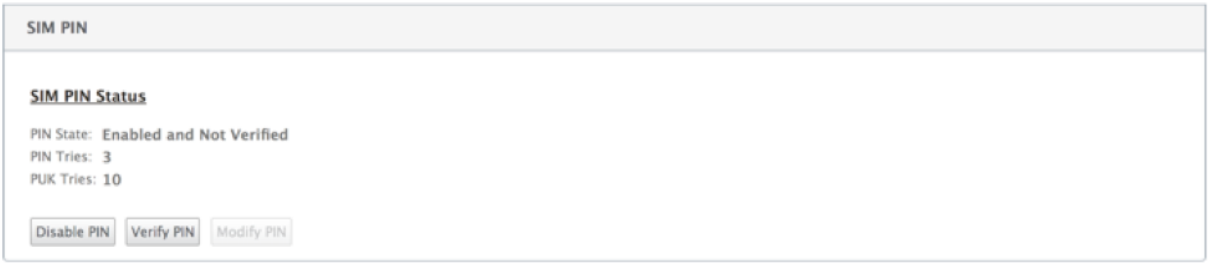
SIM PIN は、無効になっている SIM に対して有効にすることができます。



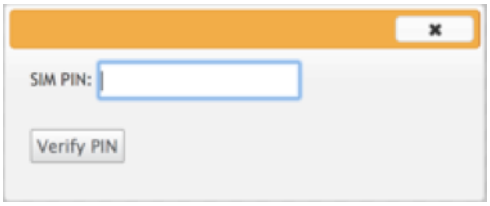
PIN を有効にするをクリックします。通信事業者から提供された SIM PIN を入力し、[有効] をクリックします。



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。

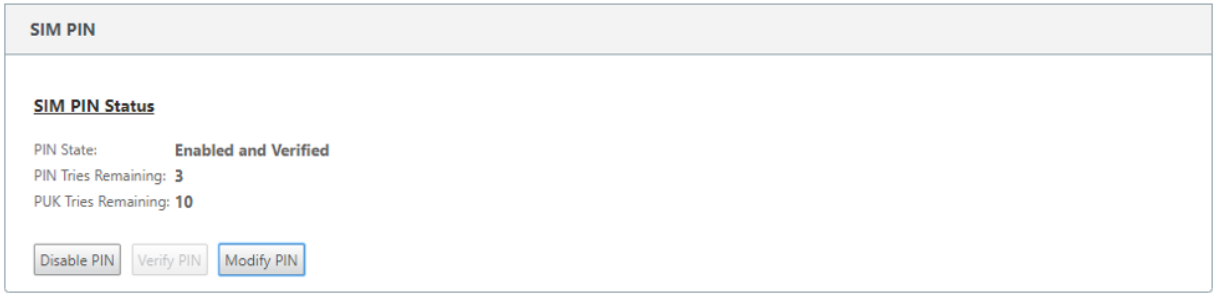


PIN を確認をクリックします。通信事業者から提供された SIM PIN を入力し、[**PIN** の確認] をクリックします。

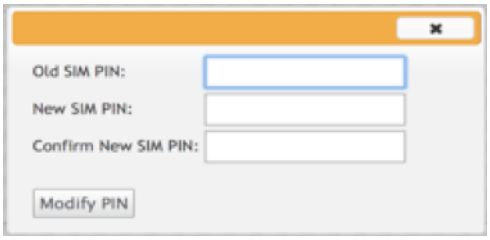


SIM PIN の変更

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。



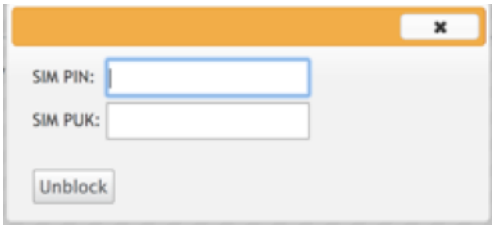
PIN の変更をクリックします。通信事業者から提供された SIM PIN を入力します。新しい SIM PIN を入力し、確認します。**PIN** の変更をクリックします。



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。

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。通信事業者から入手した **SIM PIN** と **SIM PUK** を入力し、[ブロック解除] をクリックします。

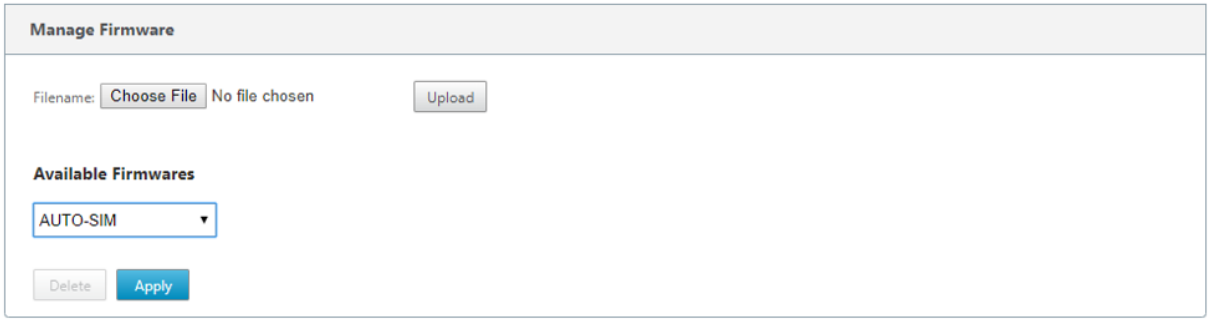


> 注:
> SIM カードは、SIM のブロックを解除しながら、PUK の 10 回の試行に失敗して永久にブロックされます。新しい SIM カードについては、通信事業者のサービスプロバイダーにお問い合わせください。

ファームウェアの管理

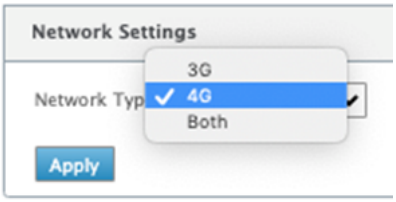
LTE が有効になっているすべてのアプライアンスには、使用可能なファームウェアのセットがあります。既存のファームウェアのリストから選択するか、ファームウェアをアップロードして適用することができます。

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。



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。



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

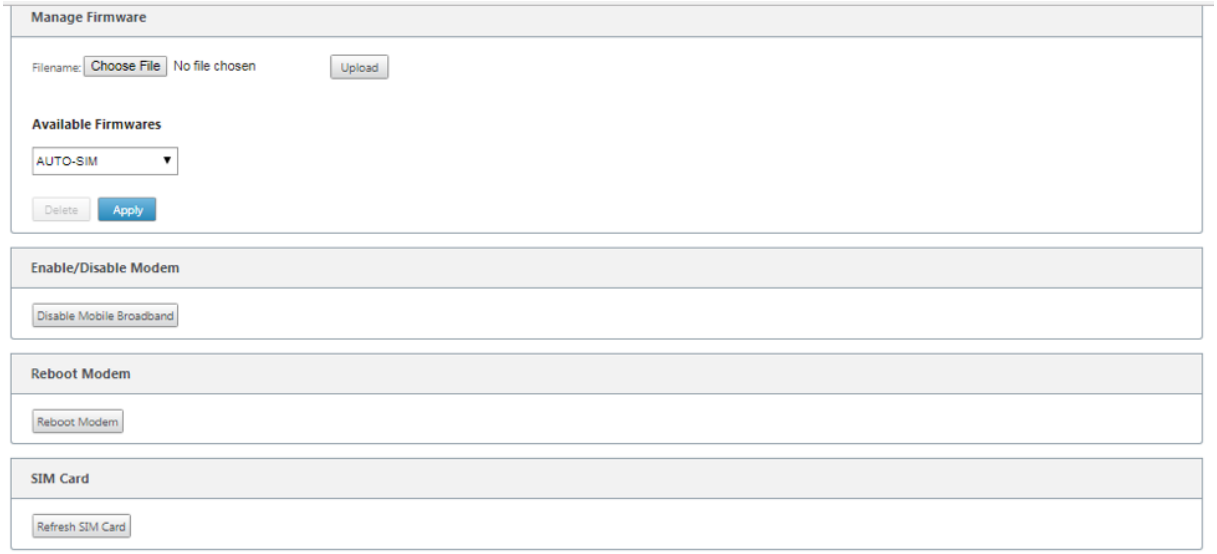
LTE 機能を使用する目的に応じて、モデムを有効または無効にします。デフォルトでは、LTE モデムは有効になっています。

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。



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 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

1. 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。
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。

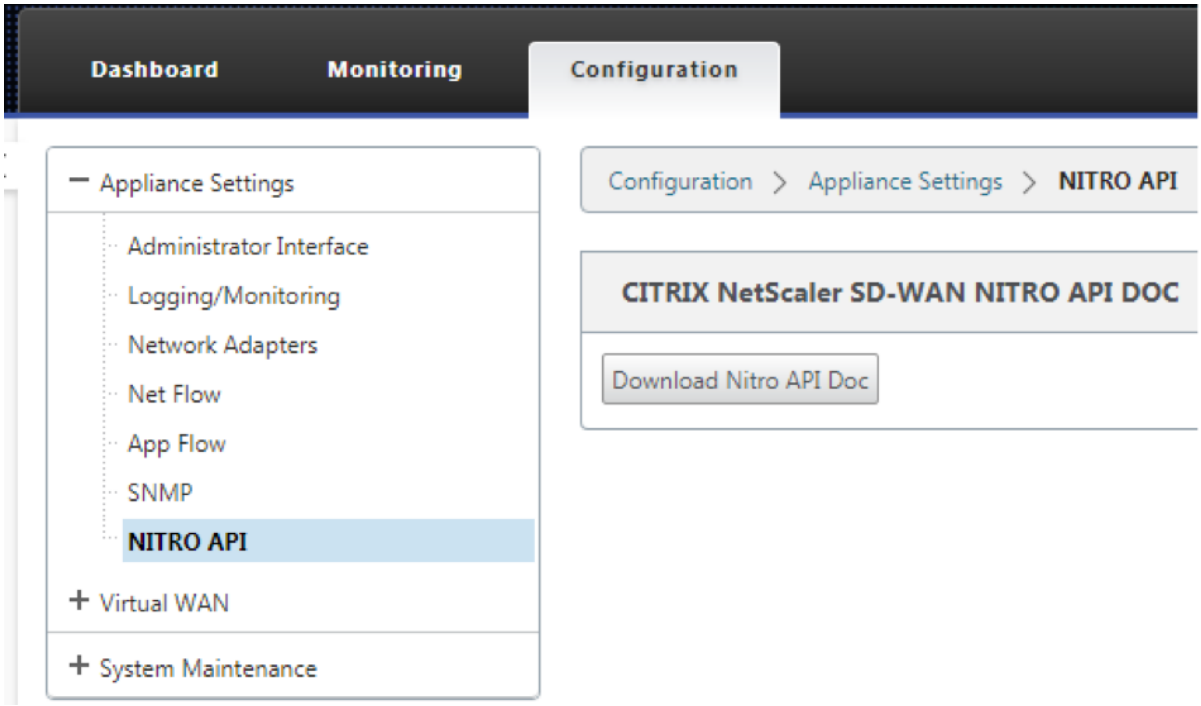
アプライアンスの電源がオンになると、ゼロタッチ展開サービスは LTE ポートを使用して、管理ポートが接続されていない場合にのみ、最新の SD-WAN ソフトウェアおよび SD-WAN 構成を取得します。

210-SE LTE アプライアンスの管理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

August 30, 2022

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。
> - ネットワーク内のすべての LTE サイトを構成および管理する方法については、「LTE ファームウェアテンプレート」を参照してください。

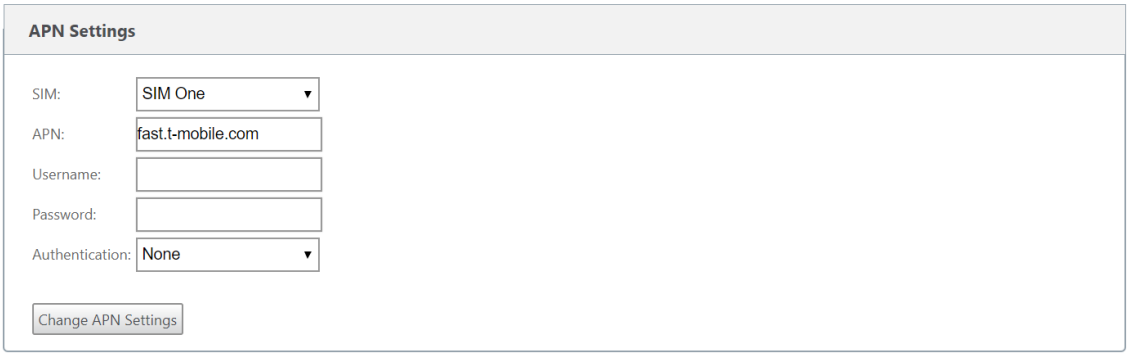
Citrix SD-WAN 110-LTE-WiFi の使用を開始する

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。

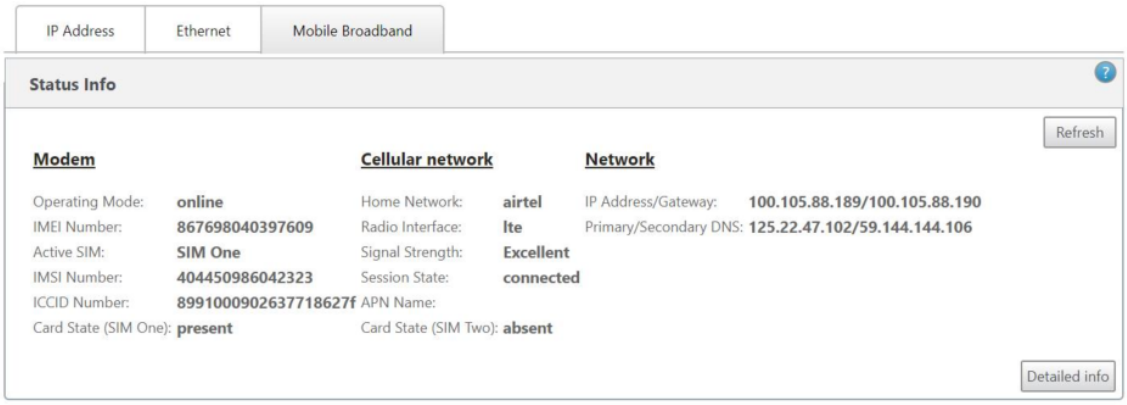


5. SIM カードを選択し、通信事業者から提供された **APN**、ユーザー名、パスワード、および認証を入力します。PAP、CHAP、PAPCHAP 認証プロトコルから選択できます。通信事業者が認証タイプを提供していない場合は、[なし] に設定します。

   > 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。



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。

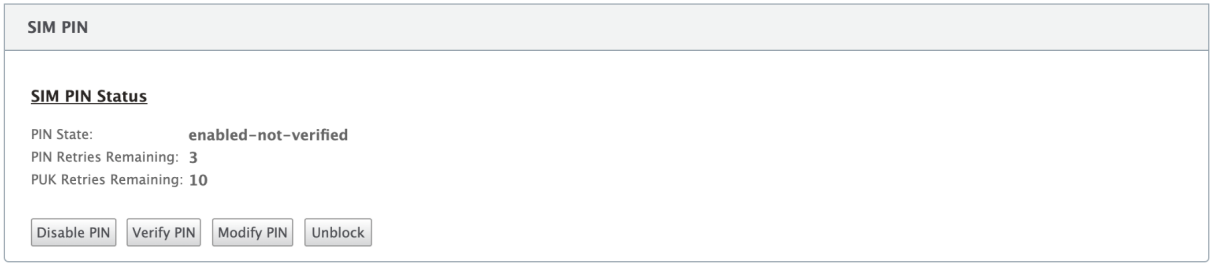
- **SIM One** 推奨:2 つの SIM が挿入されている場合、ブートアップ時に LTE モデムは SIM One (使用可能な場合) を使用します。LTE モデムが起動して実行されると、その時点で使用可能な SIM（SIM 1 または SIM 2）が使用されます。SIM がアクティブになるまで使用し続けます。
- **SIM Two** 推奨：SIM が 2 台挿入されている場合、LTE モデムは SIMTwo を使用します（利用可能な場合）。LTE モデムが起動して実行されると、その時点で使用可能な SIM（SIM 1 または SIM 2）が使用されます。SIM がアクティブにな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 ピン

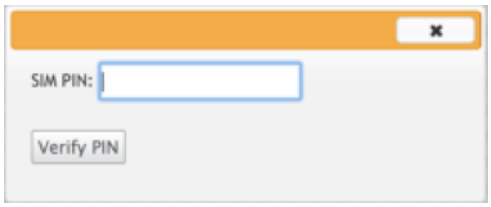
PIN でロックされている SIM カードを挿入した場合、SIM ステータスは 有効化-検証されていない 状態になります。SIM PIN で認証されるまで、SIM カードは使用できません。SIM PIN は通信事業者から入手できます。

> 注
>
> SIM PIN 操作は、アクティブな SIM にのみ適用されます。

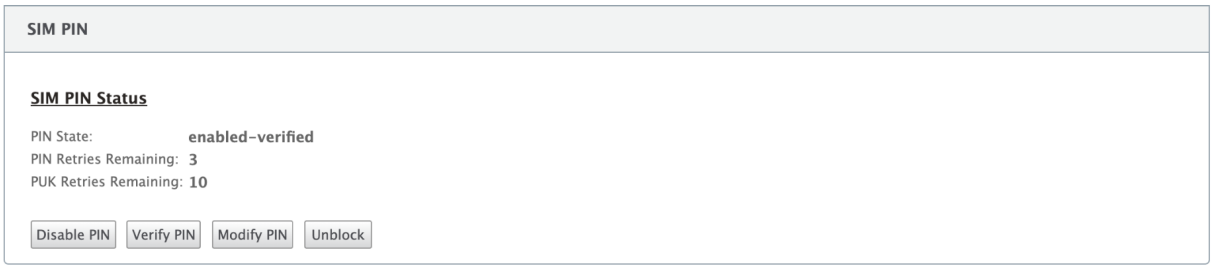
SIM PIN 操作を実行するには、[構成] **>** [アプライアンスの設定] **>** [ネットワークアダプタ] **>** [モバイルブロードバンド] **>** **[SIM PIN]** に移動します。



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。

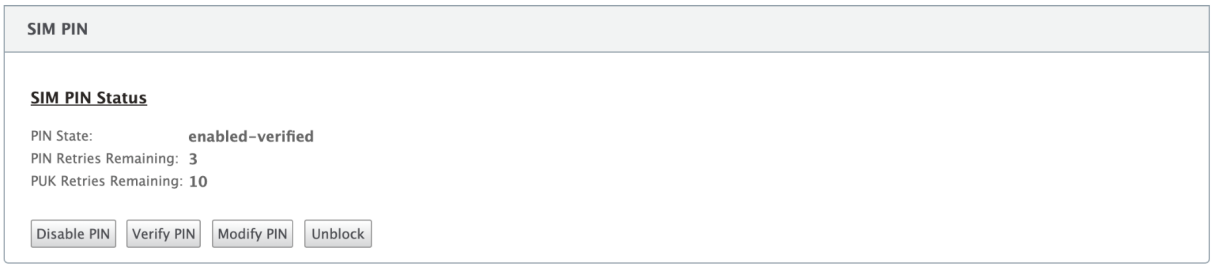


ステータスは [有効化検証済み] に変わります。

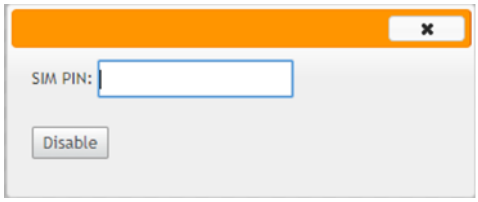


SIM PIN を無効にする

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。

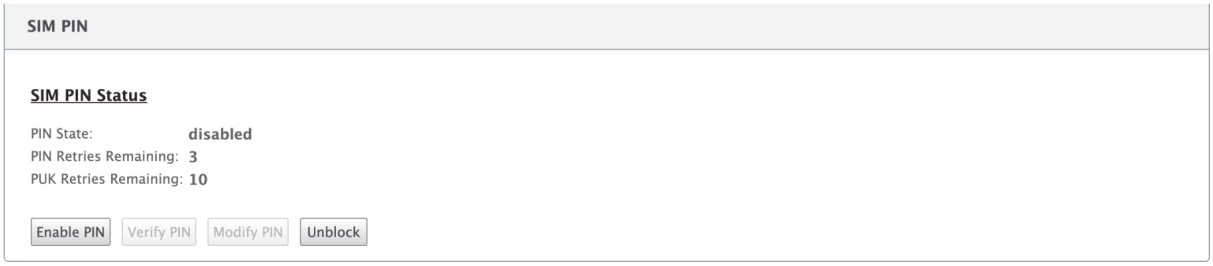


PIN を無効にするをクリックします。**SIM PIN** を入力し、[無効] をクリックします。

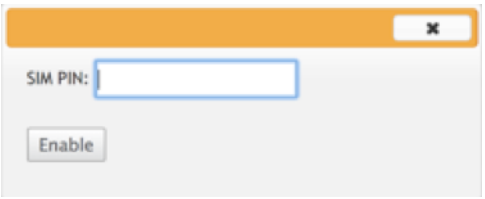


SIM PIN を有効にする

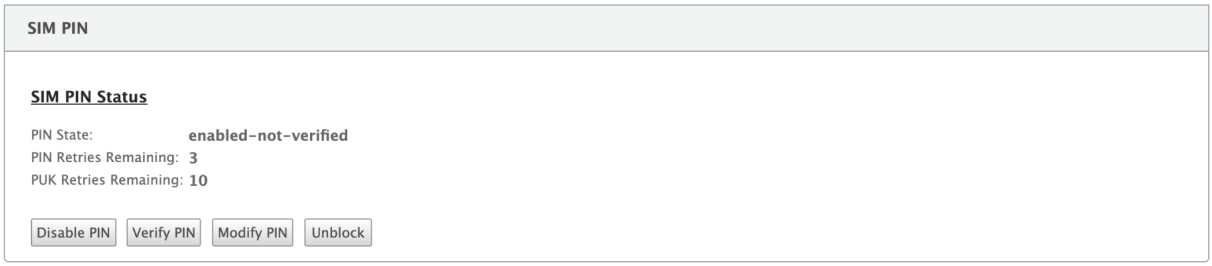
SIM PIN は、無効になっている SIM に対して有効にすることができます。



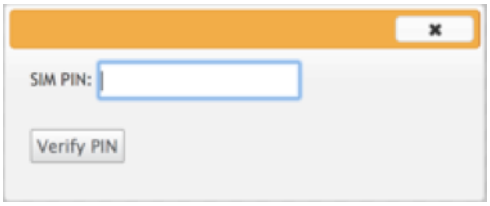
PIN を有効にするをクリックします。通信事業者から提供された SIM PIN を入力し、[有効] をクリックします。



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。

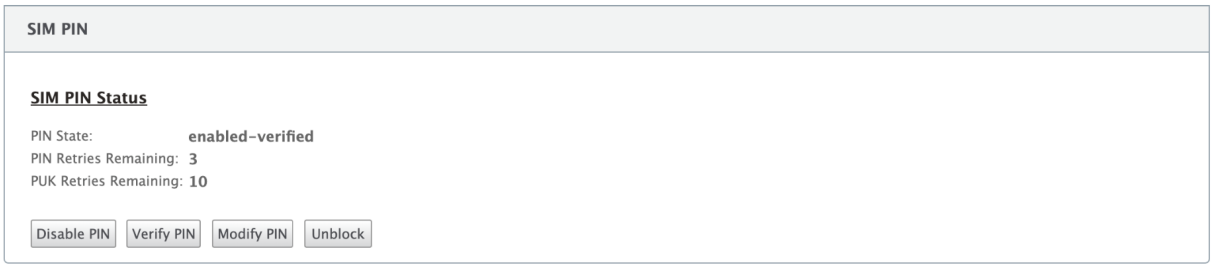


PIN を確認をクリックします。通信事業者から提供された SIM PIN を入力し、[**PIN** の確認] をクリックします。

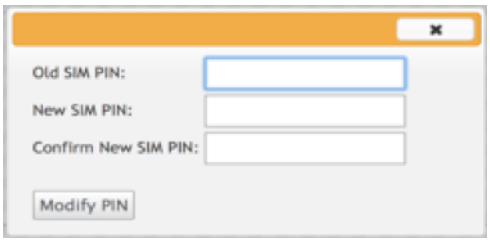


SIM PIN の変更

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。



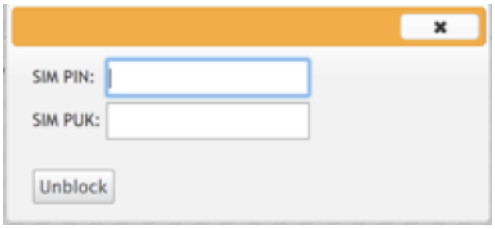
PIN の変更をクリックします。通信事業者から提供された SIM PIN を入力します。新しい SIM PIN を入力し、確認します。**PIN** の変更をクリックします。



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。

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。



> 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。

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。

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。

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 <unblock> <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

コマンド	説明
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> 選択 [1|2] [1|2]}	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 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。

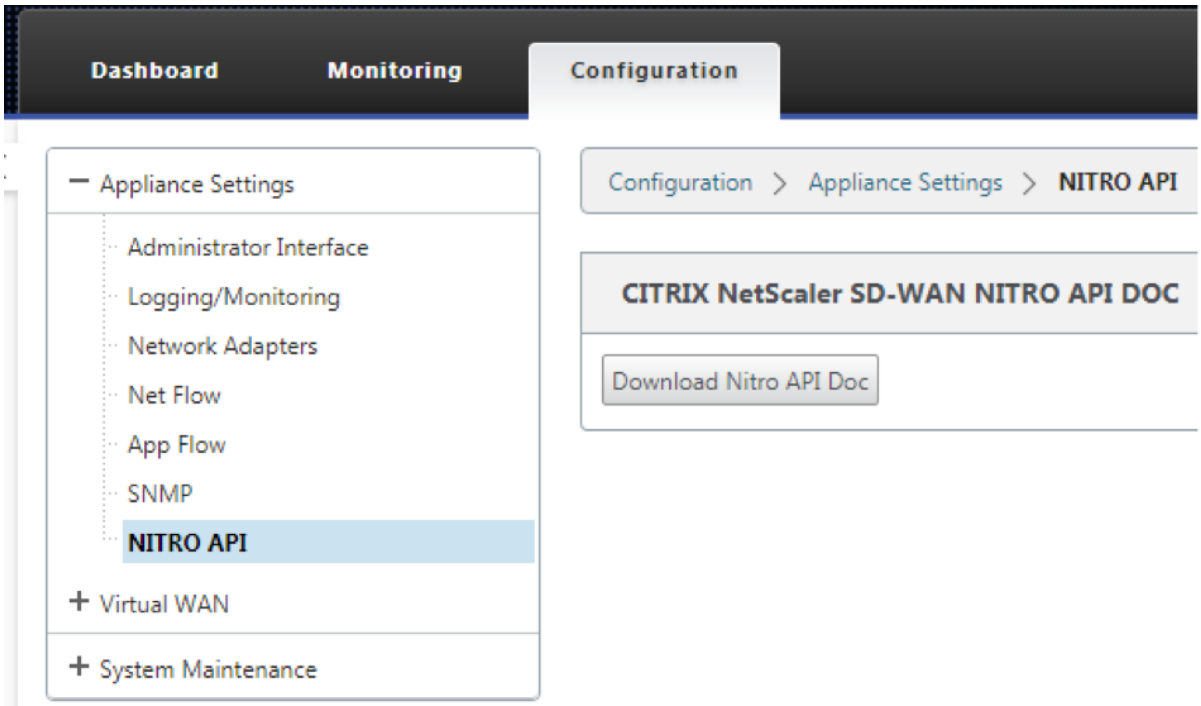
アプライアンスの電源がオンになると、ゼロタッチ展開サービスは LTE ポートを使用して、最新の SD-WAN ソフトウェアと SD-WAN 構成を取得します。

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 。

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

August 30, 2022

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
- 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
- Citrix SD-WAN 2100 SE

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。

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

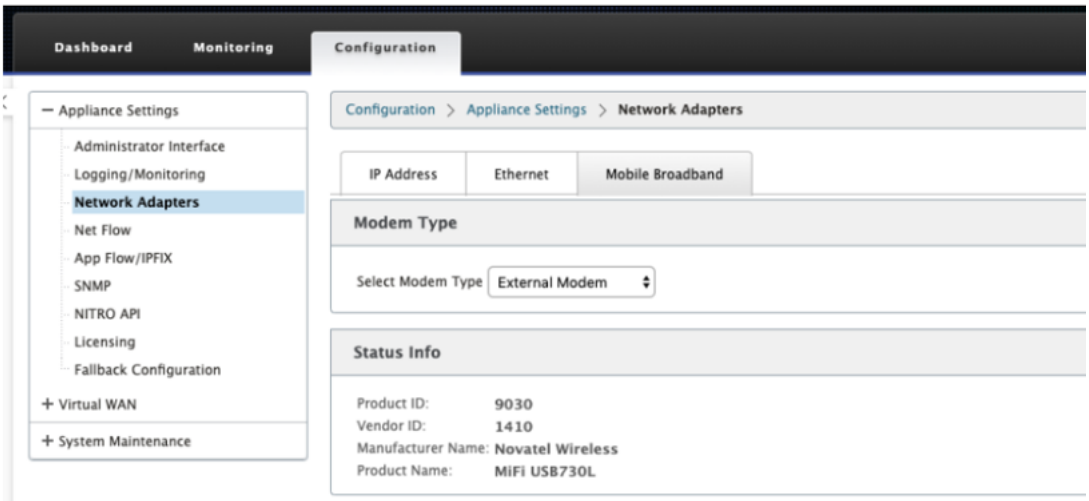
ワイヤレスキャリアのガイドラインに従って、USB モデムを有効にしてテストします。

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

外部 **USB** モデムの設定

Citrix SD-WAN Orchestrator サービスを介して外部 USB モデムを使用して LTE サイトを構成できます。詳細については、「LTE ファームウェアのアップグレード」を参照してください。

LTE 経由のゼロタッチ展開

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 Orchestrator サービスを介した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
```

デプロイメント

August 30, 2022

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。

- Gateway 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
- ゼロタッチ展開
- 単一リージョン展開
- マルチリージョンの配備
- 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

次のリストは、SD-WAN Standard Editions の展開に関連する手順と手順の概要を示しています。

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

August 30, 2022

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

Gateway モードの展開に関する推奨事項を次に示します。

1. Gateway 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:
>
> Gateway 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

Gateway 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 アドレッシ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/容量のアカウンティングを含め、ブレークアウト、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 ボックスがデイジーチェーン接続され、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、ブレー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

Gateway 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 -Gateway 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。
- セキュリティポスチャー -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、ブレークアウト/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 以降）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ー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/Gateway 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で推奨される方法
    - 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）。

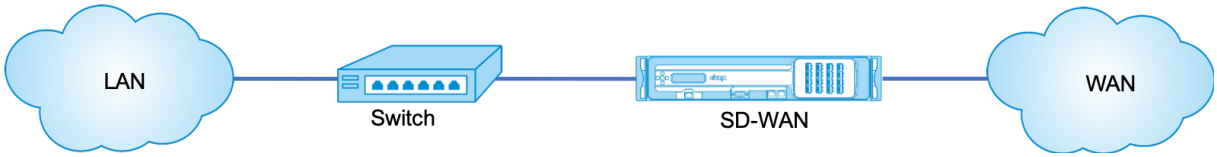
Gateway モード

August 30, 2022

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（ツーアーム配置）。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 Gateway 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 Gateway モード。Gateway 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

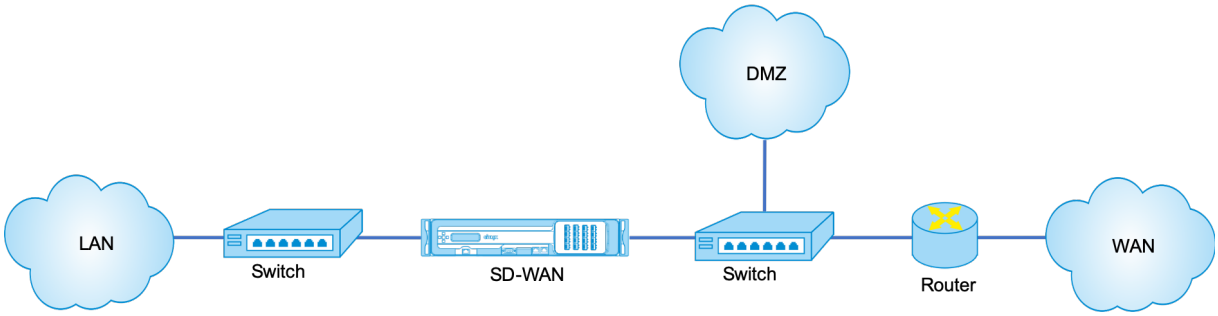
ゲートウェイ展開モードは、Citrix SD-WAN Orchestrator サービスでサポートされています。詳細については、「インターフェイス」を参照してください。



> 注
>
> Gateway 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気的に接続され、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。

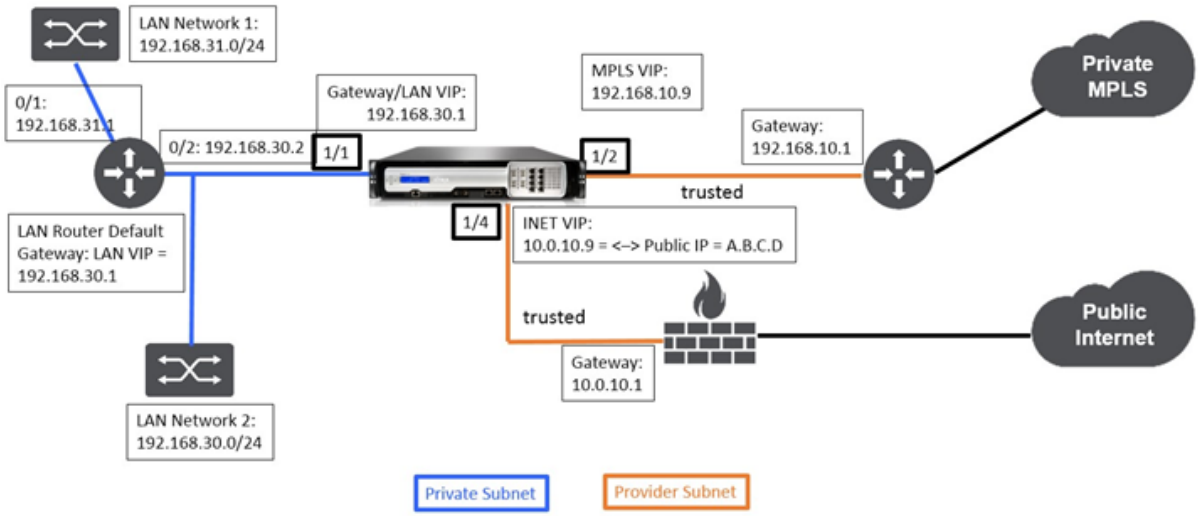


この記事では、ネットワーク設定のサンプルで SD-WAN アプライアンスを Gateway モードで構成する手順を順を追って説明します。インライン展開は、ブランチ側で設定を完了するためにも説明されています。Inline デバイスが削除されても、ネットワークは引き続き機能しますが、Gateway デバイスが削除されるとすべてのアクセスが失われます。

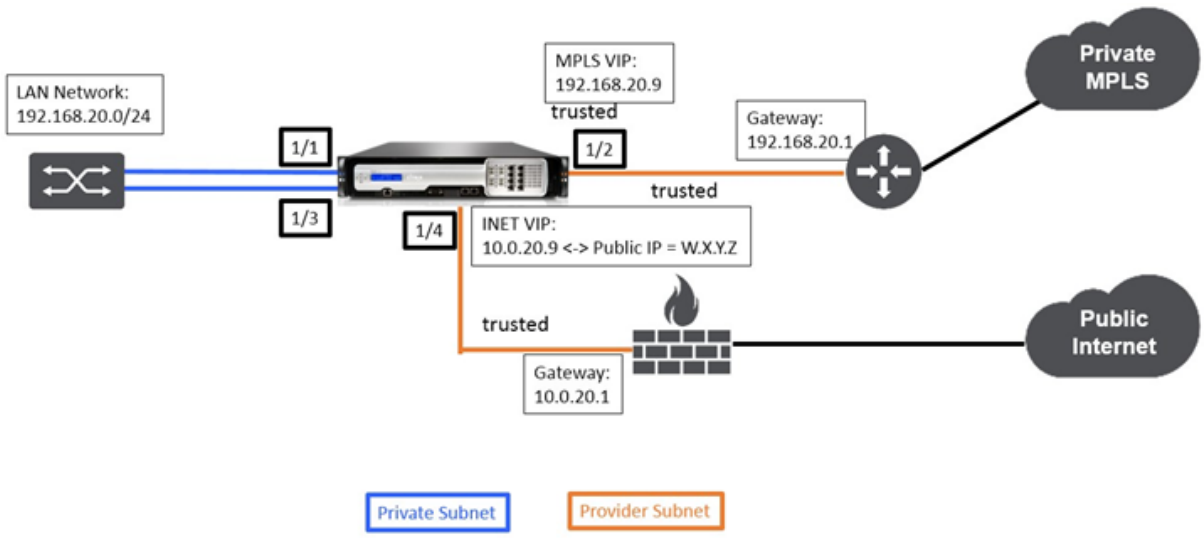
トポロジ

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



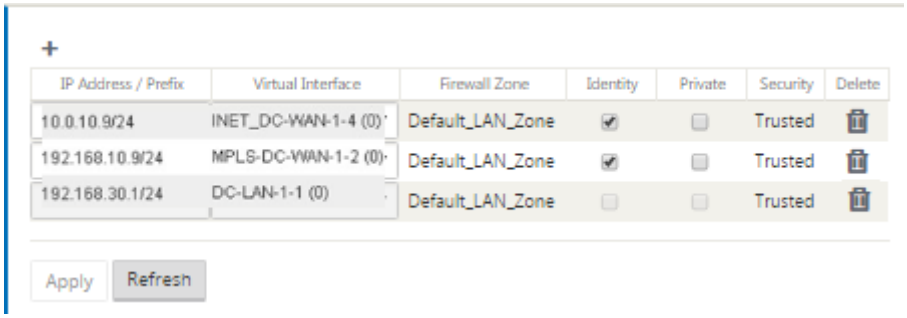
データセンターサイト **Gateway** モードの設定

データセンターサイト Gateway 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。

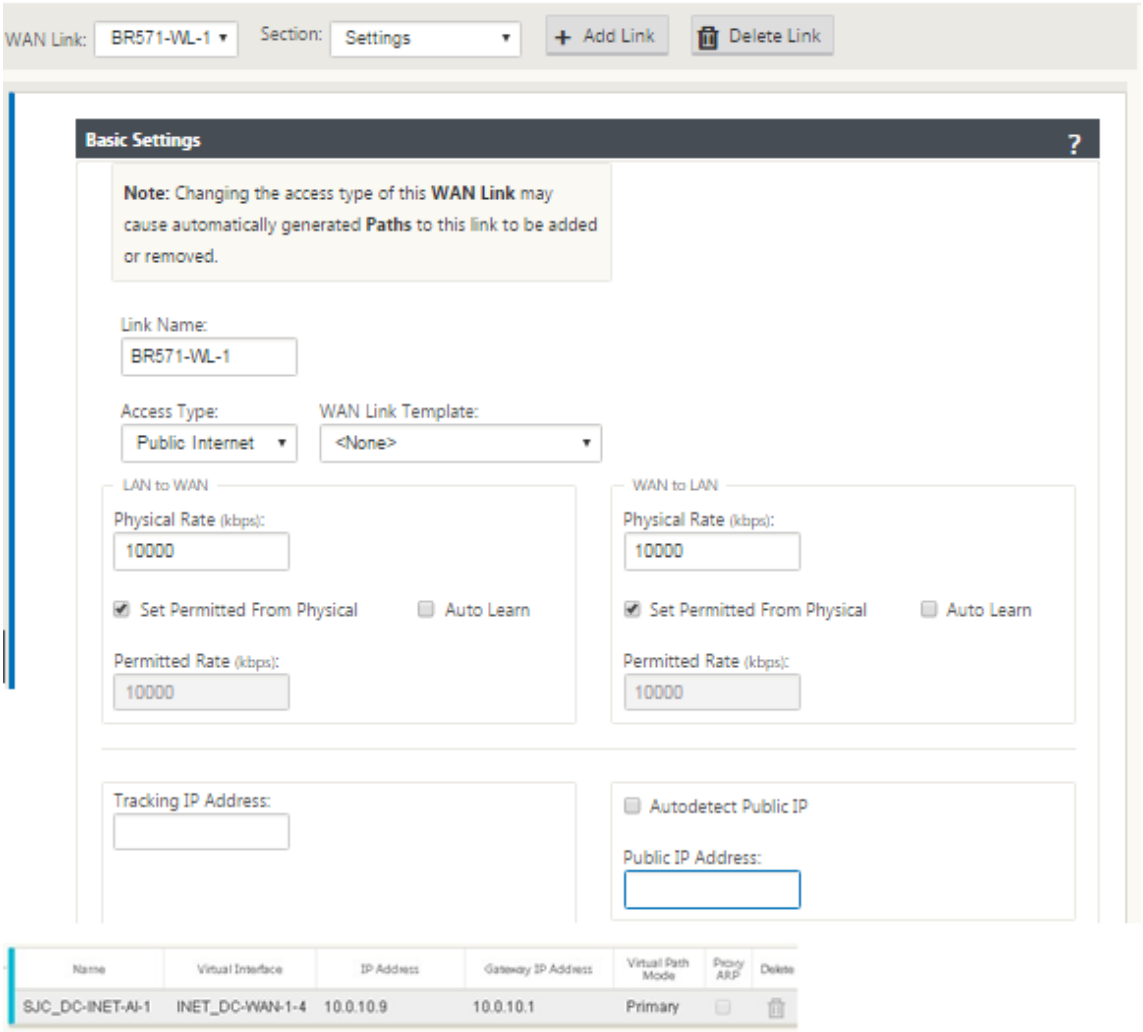
仮想インターフェイスごとに仮想 **IP**（**VIP**）アドレスを作成するには

1. 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。
2. LAN ネットワークの Gateway アドレスとして使用する仮想 IP アドレスを作成します。



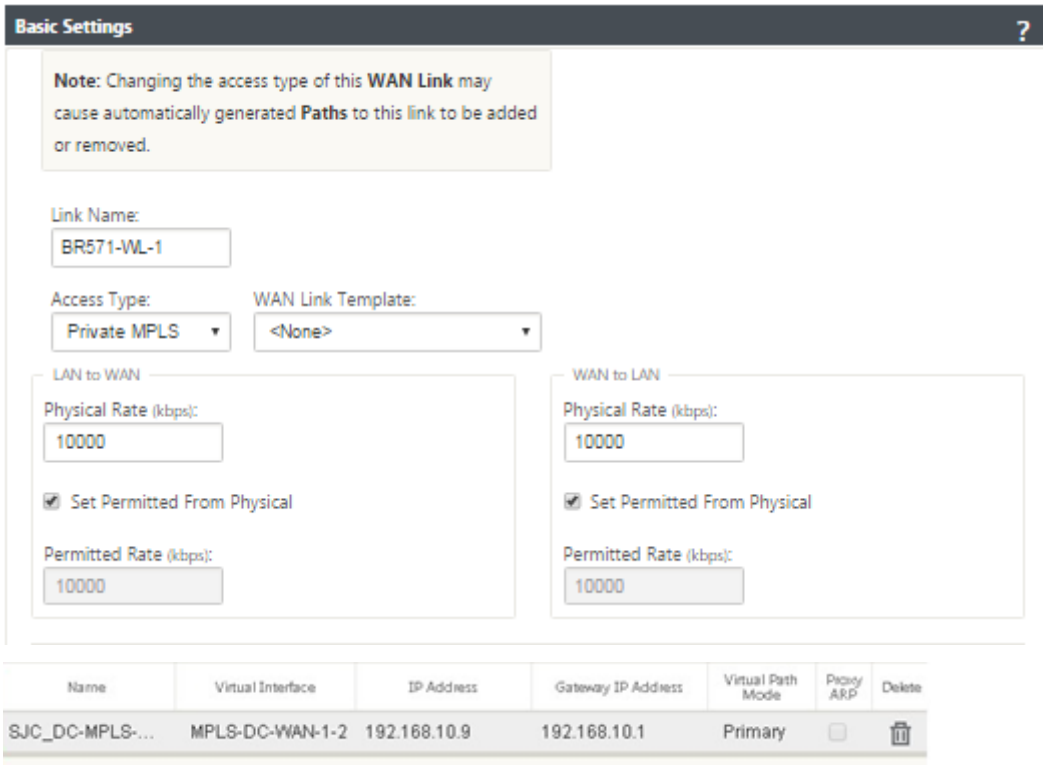
インターネットリンクを使用して、バースト速度ではなく、物理レートに基づいて WAN リンクを設定するには、次の手順を実行します。

1. [**WAN** リンク] に移動し、[**+** 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。



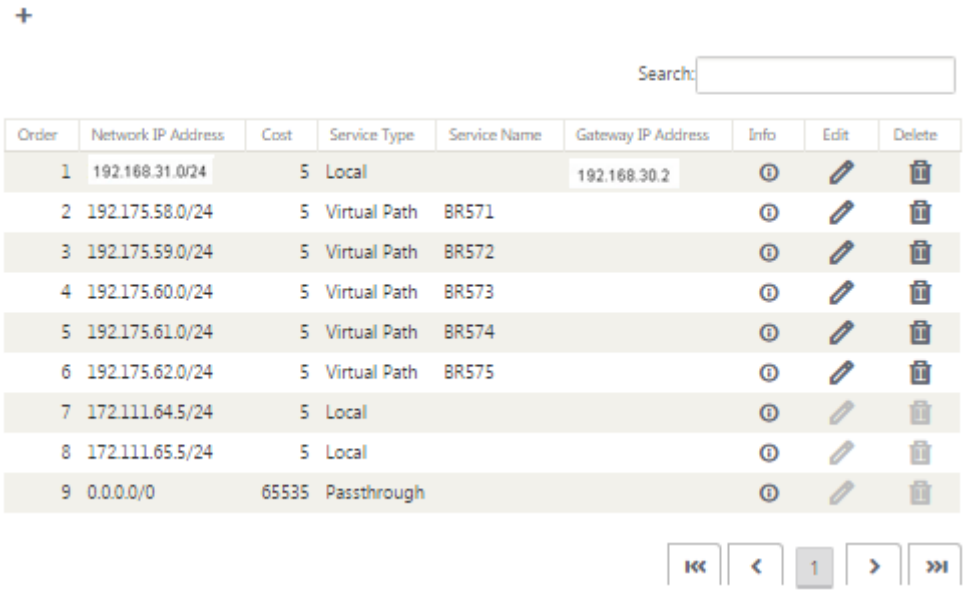
MPLS リンクを作成するには

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（**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。



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** という余分な 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。Gateway 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。



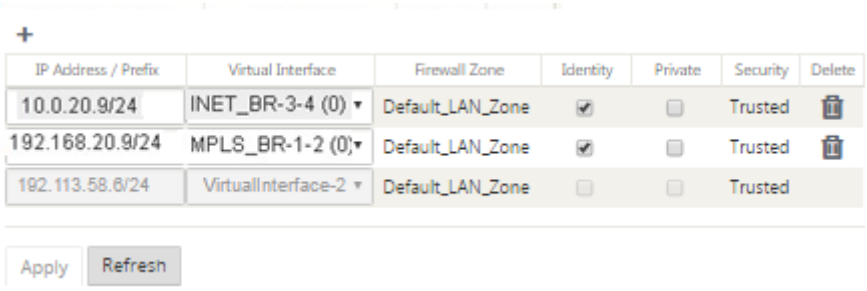
ブランチサイトのインライン展開設定

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。

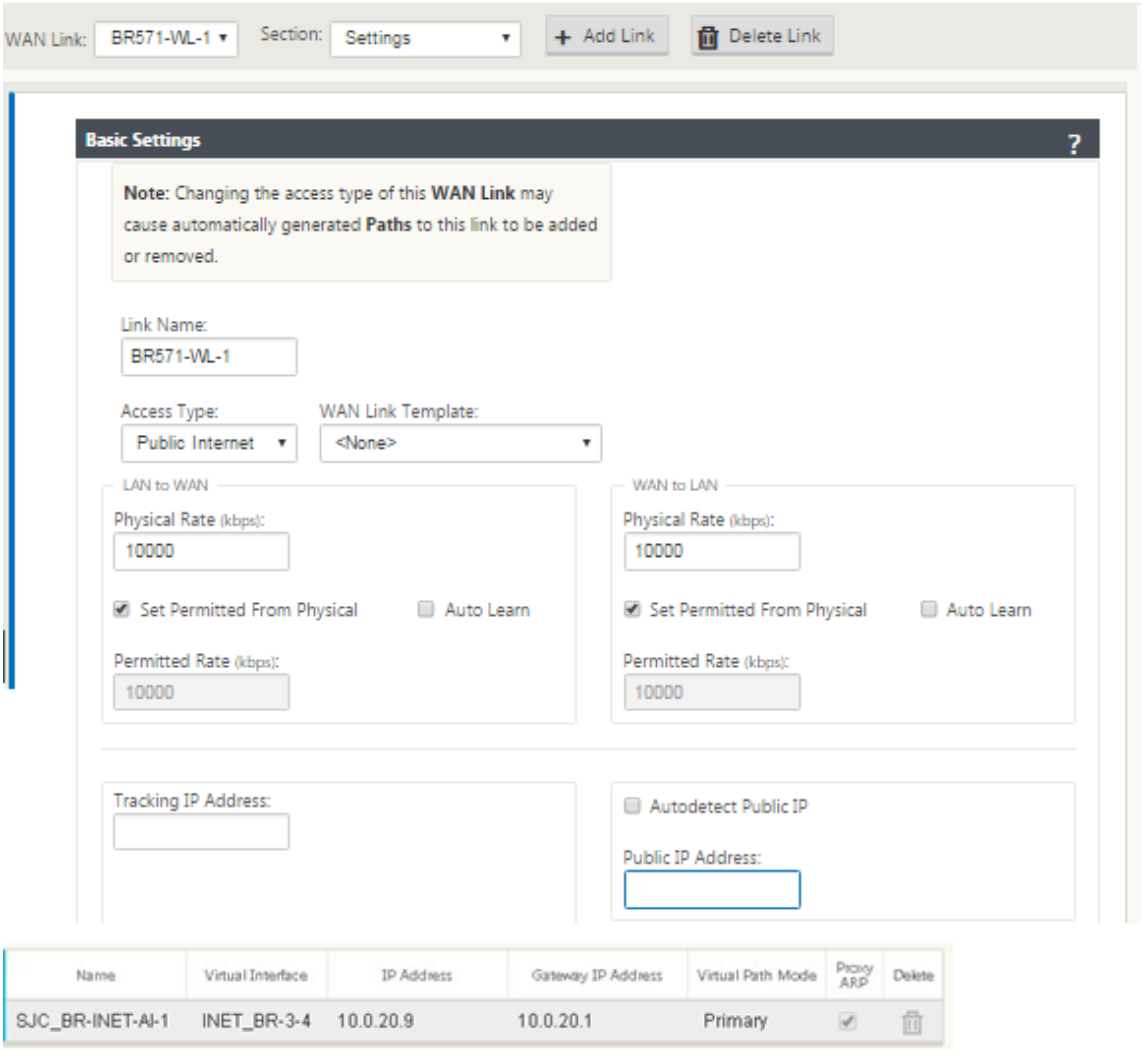
仮想インターフェイスごとに仮想 **IP**（**VIP**）アドレスを作成するには

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。



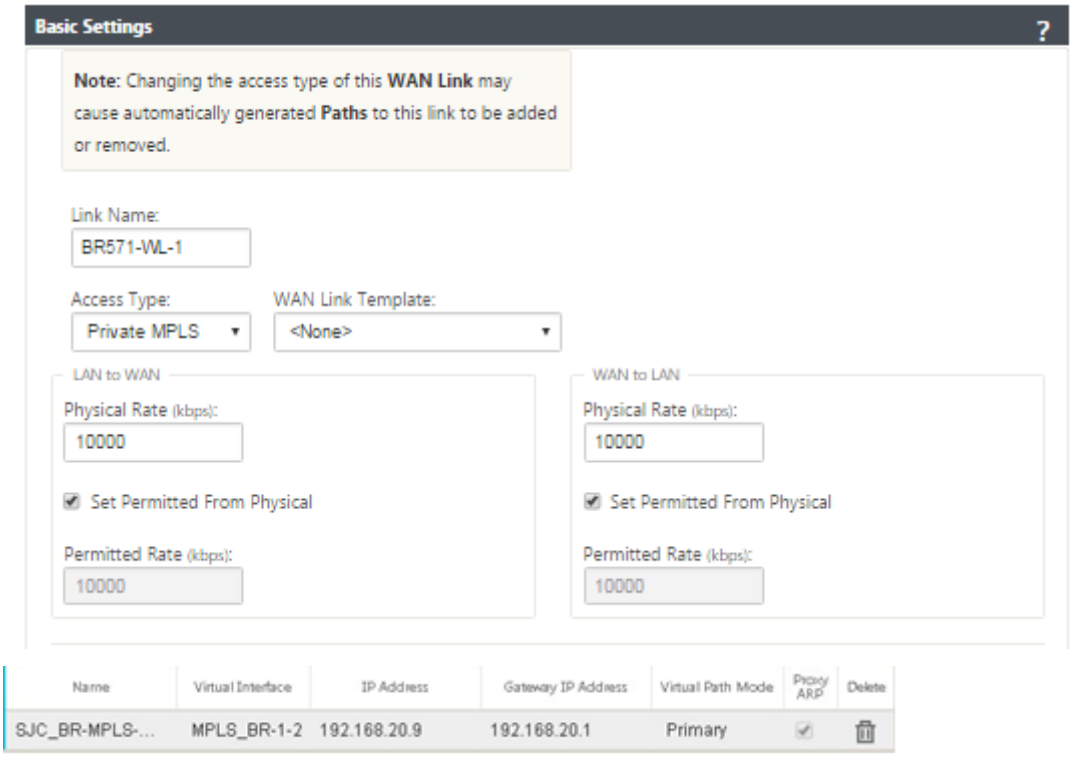
インターネットリンクを使用して、バースト速度ではなく、物理レートに基づいて WAN リンクを設定するには、次の手順を実行します。

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 のアクセスインタフェースを設定します。



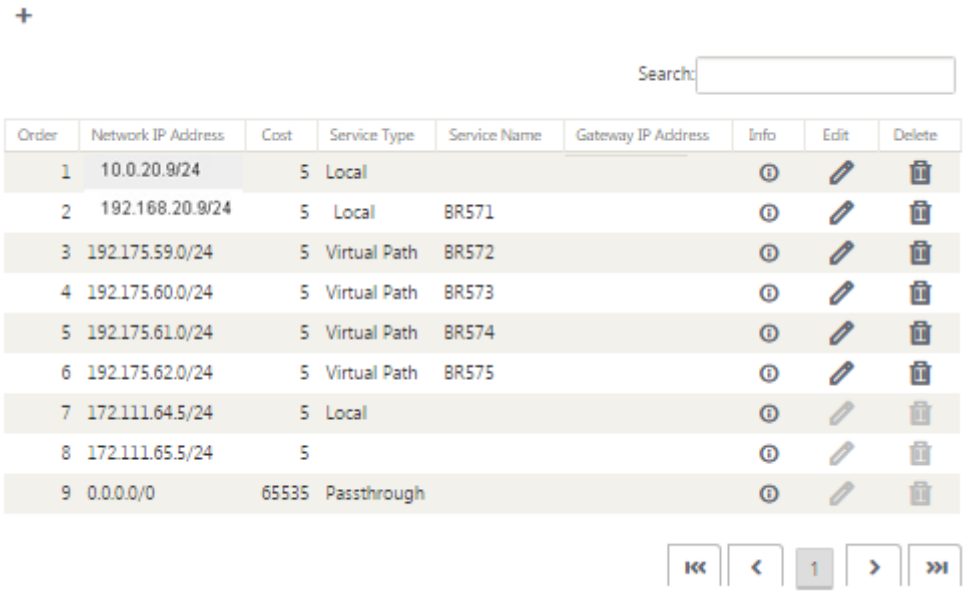
MPLS リンクを作成するには

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（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。



ルートを設定するには

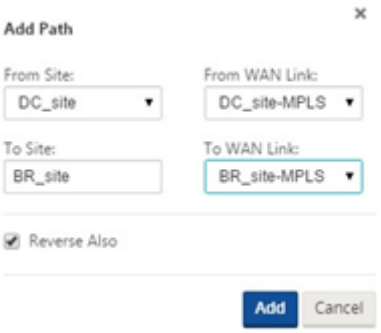
ルートは、上記の設定に基づいて自動作成されます。このリモートブランチオフィスに固有のサブネットが増える場合は、それらのバックエンドサブネットに到達するためにトラフィックを誘導する Gateway を特定する特定のルートを追加する必要があります。



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。



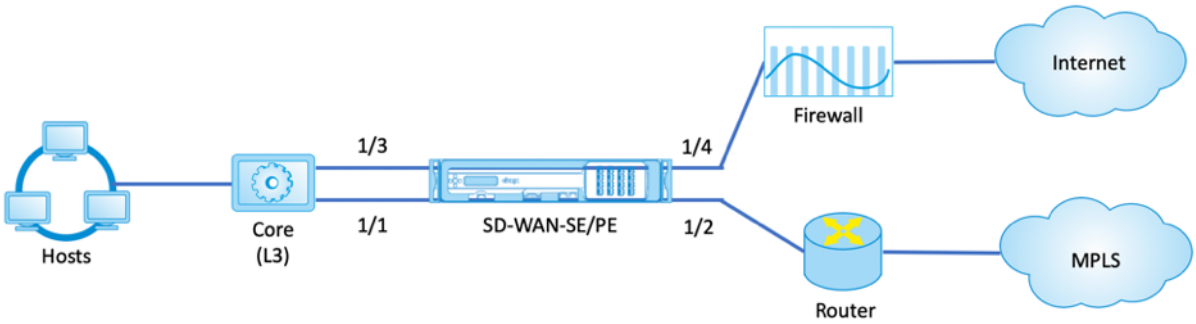
上記の手順をすべて完了したら、SD-WAN アプライアンスパッケージの準備に進みます。—>

インラインモード

August 30, 2022

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気的に接続され、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。SD-WAN Orchestrator サービスベースのインラインモード展開の詳細については、「インターフェイス」を参照してください。



仮想インラインモード

August 30, 2022

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、コアスイッチで設定するか、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

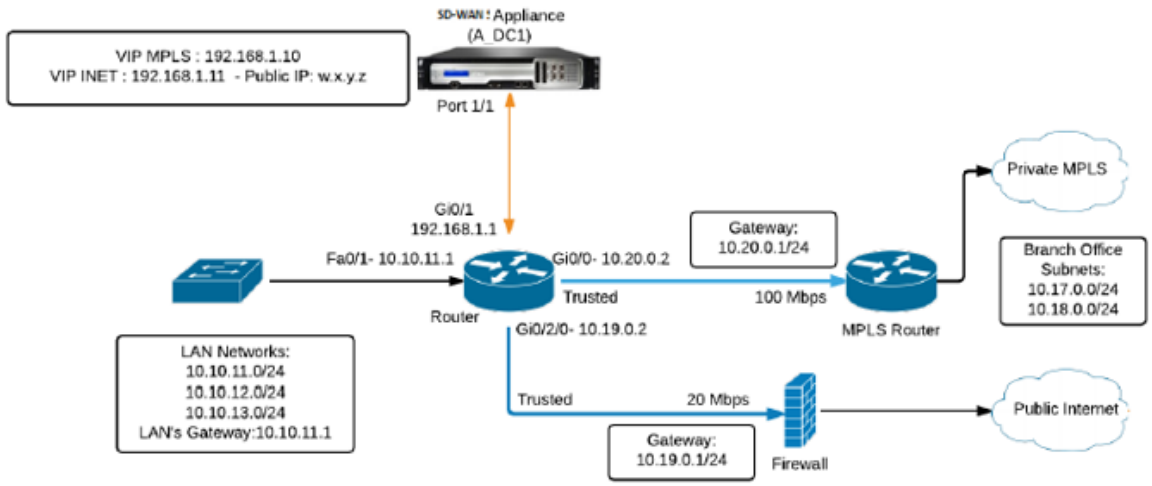
仮想インラインモードの設定に必要な次の情報を収集します。

- 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

SD-WAN Orchestrator サービスベースの仮想インラインモードの展開については、「インターフェイス」を参照してください。

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—仮想インラインモード



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

August 30, 2022

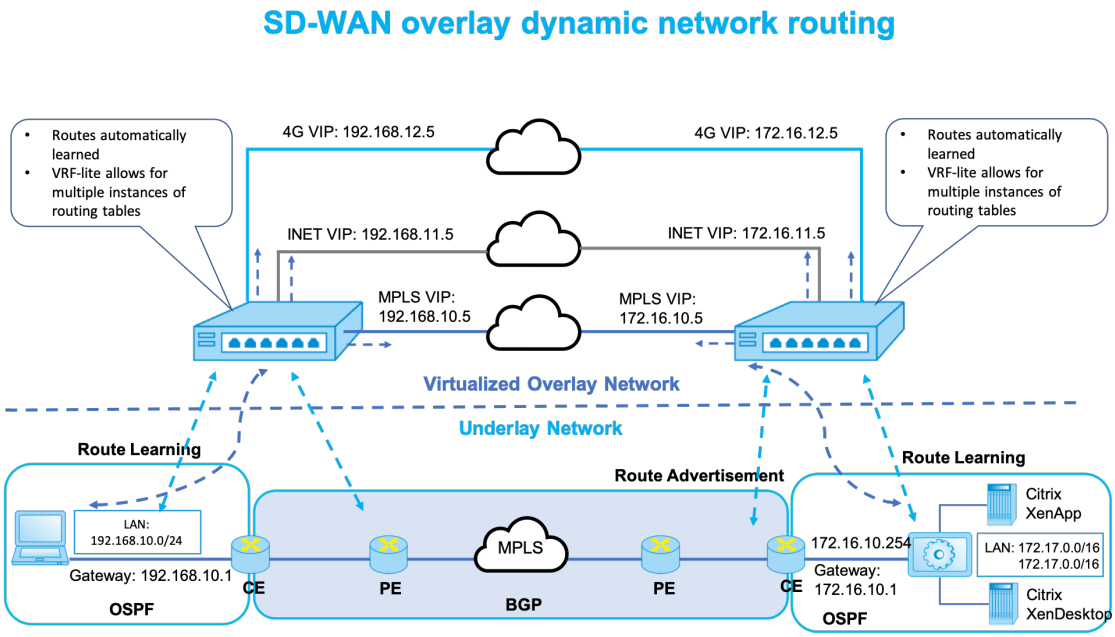
SD-WAN オーバーレイルートテーブルを構築せずに SD-WAN オーバーレイネットワークを構築するには、次の手順を実行します。

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トポロジ

- Local：サブネットがこのサイトに存在する（SD-WAN 環境にアドバタイズされる）
- 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。



高可用性

August 30, 2022

このトピックでは、SD-WAN アプライアンス (Standard 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:

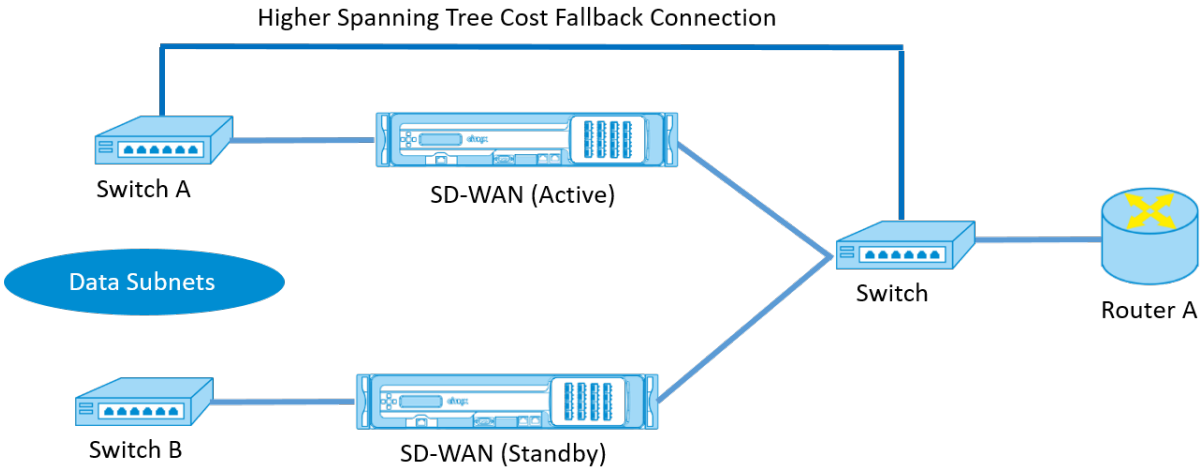
  SD-WAN アプライアンスの 1 つがアクティブである限り、仮想パスがダウンしていても、アクティブトラフィックはフローします。SD-WAN アプライアンスは、トラフィックをイントラネットトラフィックとしてルータにリダイレクトします。ただし、アクティブ/スタンバイ SD-WAN アプライアンスの両方が非アクティブになると、ルータはトラフィックをアプライアンスにリダイレクトしようとします。次のアプライアンスに到達できない場合、ルータで IP SLA モニタリングを設定して PBR を無効にすることができます。これにより、ルータがフォールバックしてルート検索を実行し、パケットを適切に転送できます。

並列インライン高可用性モード:

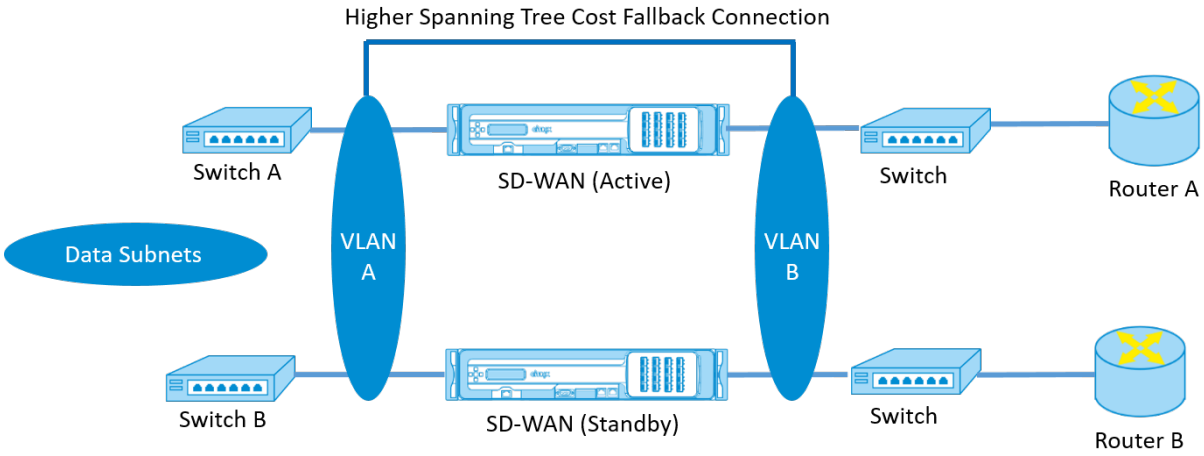
パラレルインライン高可用性モードでは、SD-WAN アプライアンスはデータパスにインラインで配置されます。アクティブアプライアンスを経由するパスは 1 つだけ使用されます。バイパスインターフェイスグループは、フェールオーバー中のブリッジングループを回避するために fail-to-block に設定されることに注意してください。

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。



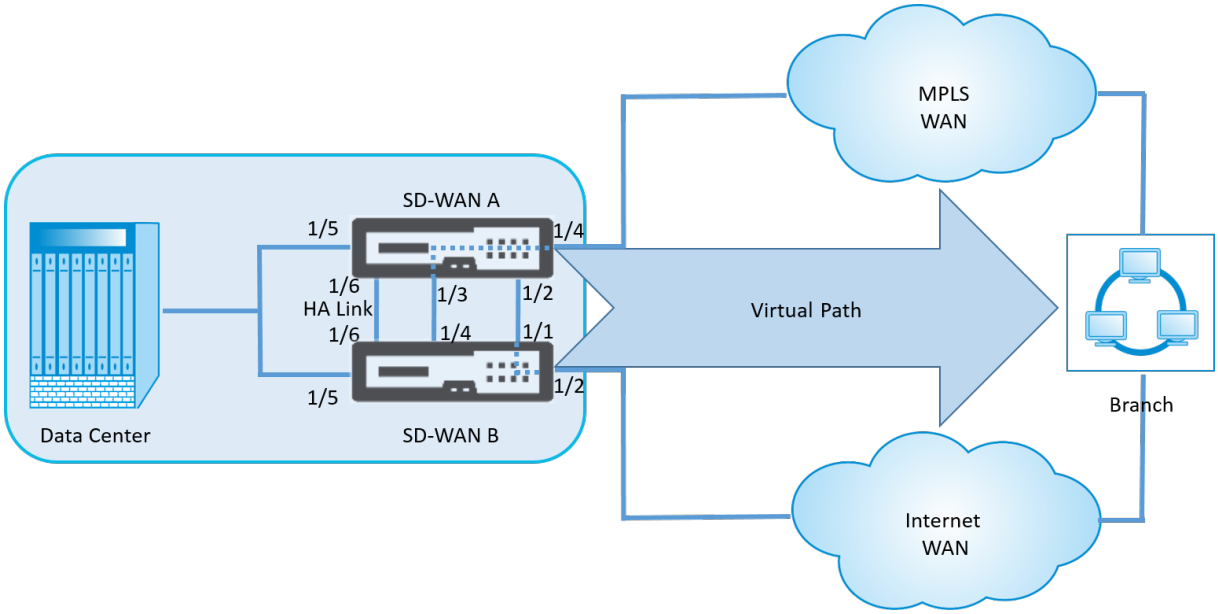
フェール・ツー・ワイヤ・モード:

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ステートである状態で、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とき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。

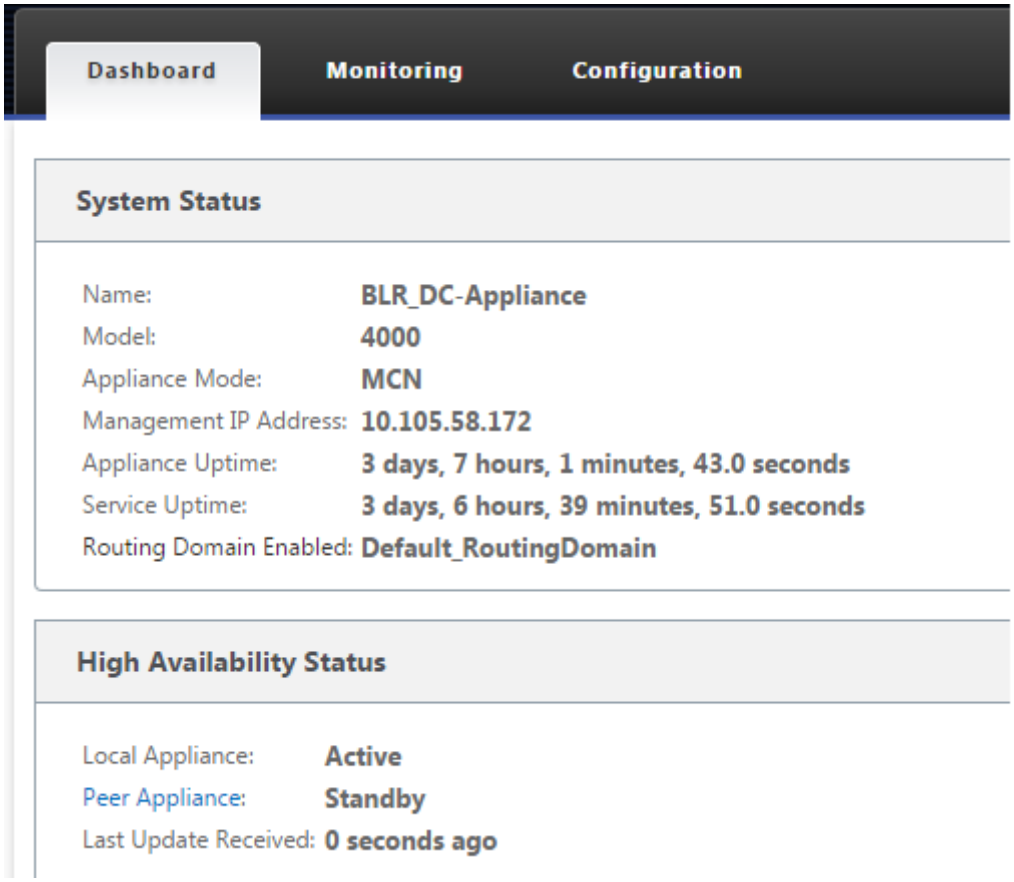
フェールオーバー中に最小限のサービス損失が許容できる場合は、Fail-to-Wire 高可用性モードが適しています。Fail-to-Wire 高可用性モードは、アプライアンスの障害から保護し、パラレルインライン高可用性はすべての障害から保護します。すべてのシナリオにおいて、高可用性は、システム障害時に SD-WAN ネットワークの継続性を維持するために有用です。

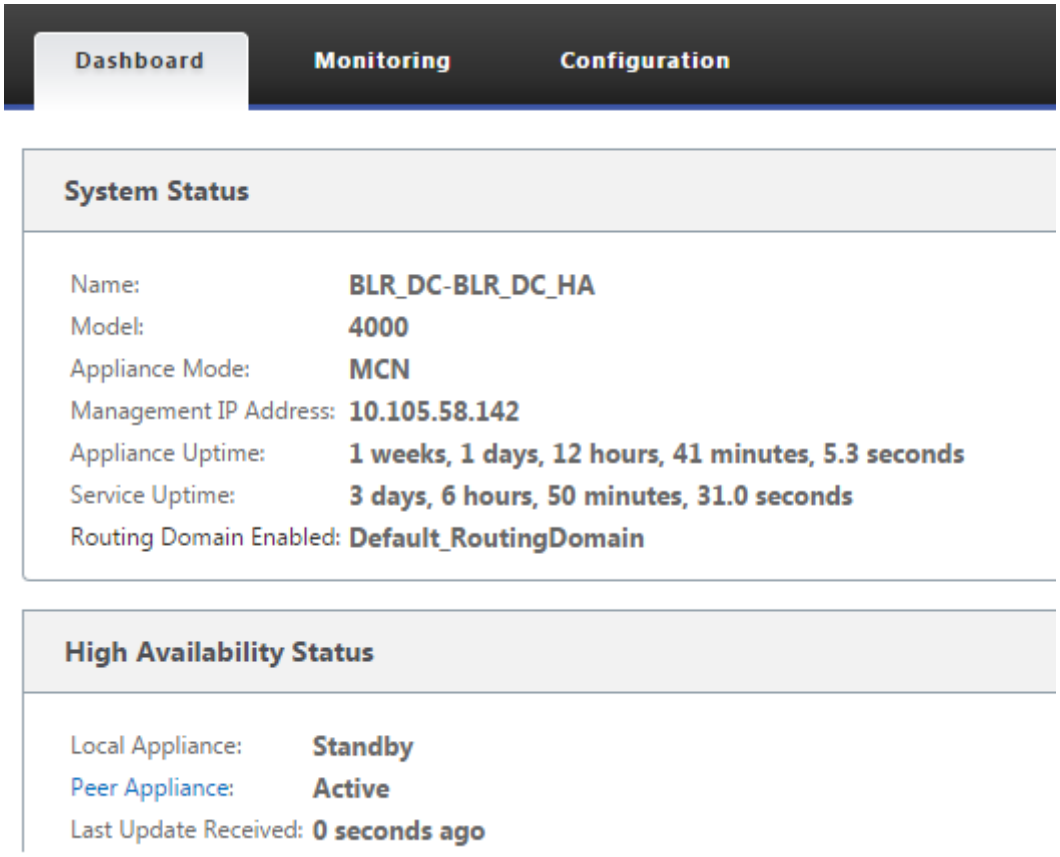
SD-WAN Orchestrator サービスベースの HA 展開の詳細については、「デバイスの詳細」を参照してください。

監視

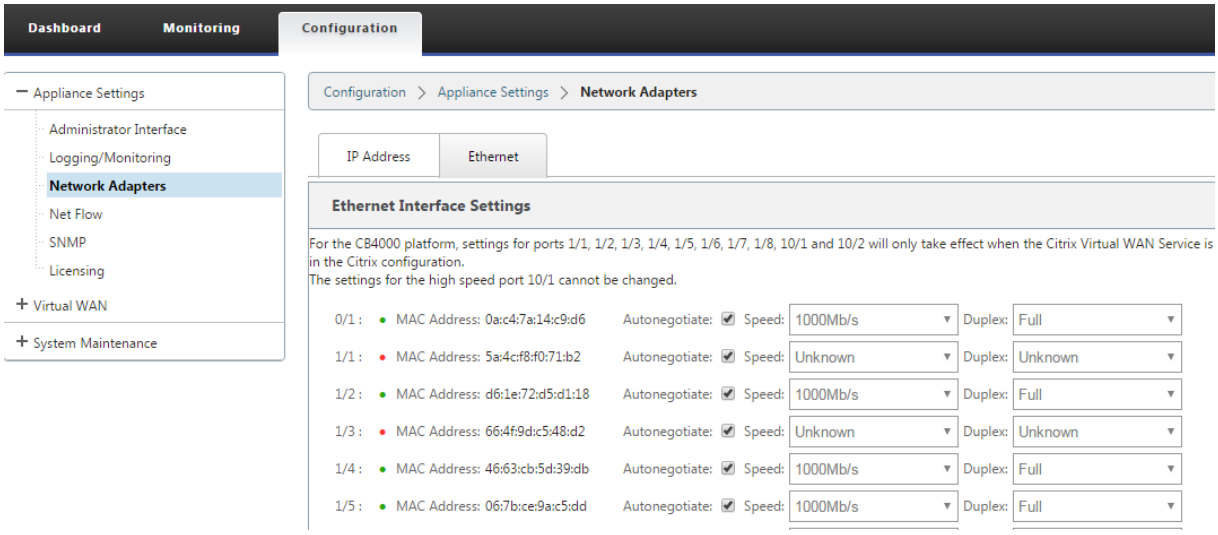
高可用性構成を監視するには、次の手順を実行します。

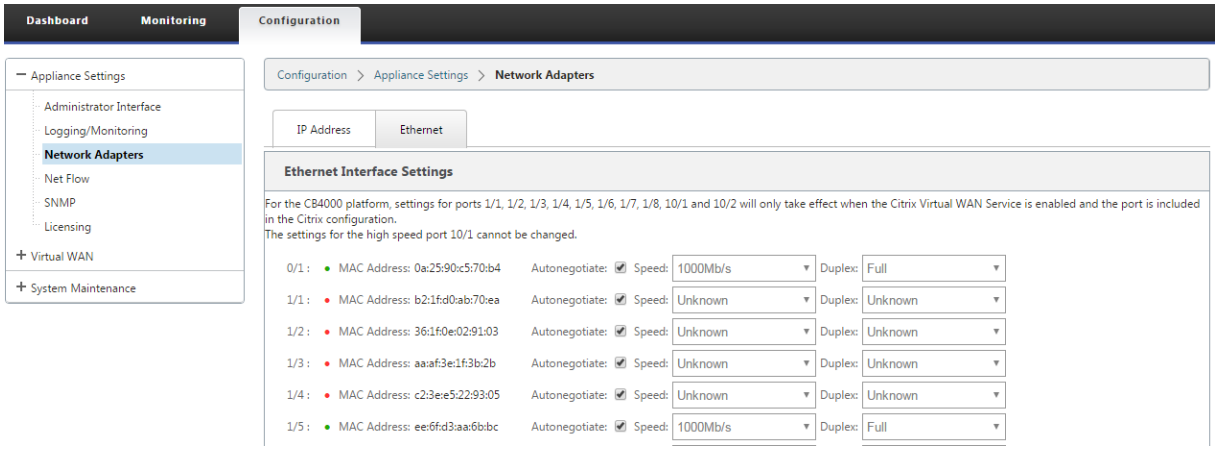
高可用性が実装されているアクティブおよびスタンバイアプライアンスの SD-WAN Web 管理インターフェイスにログインします。［ダッシュボード］タブに高可用性ステータスを表示します。





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。





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。

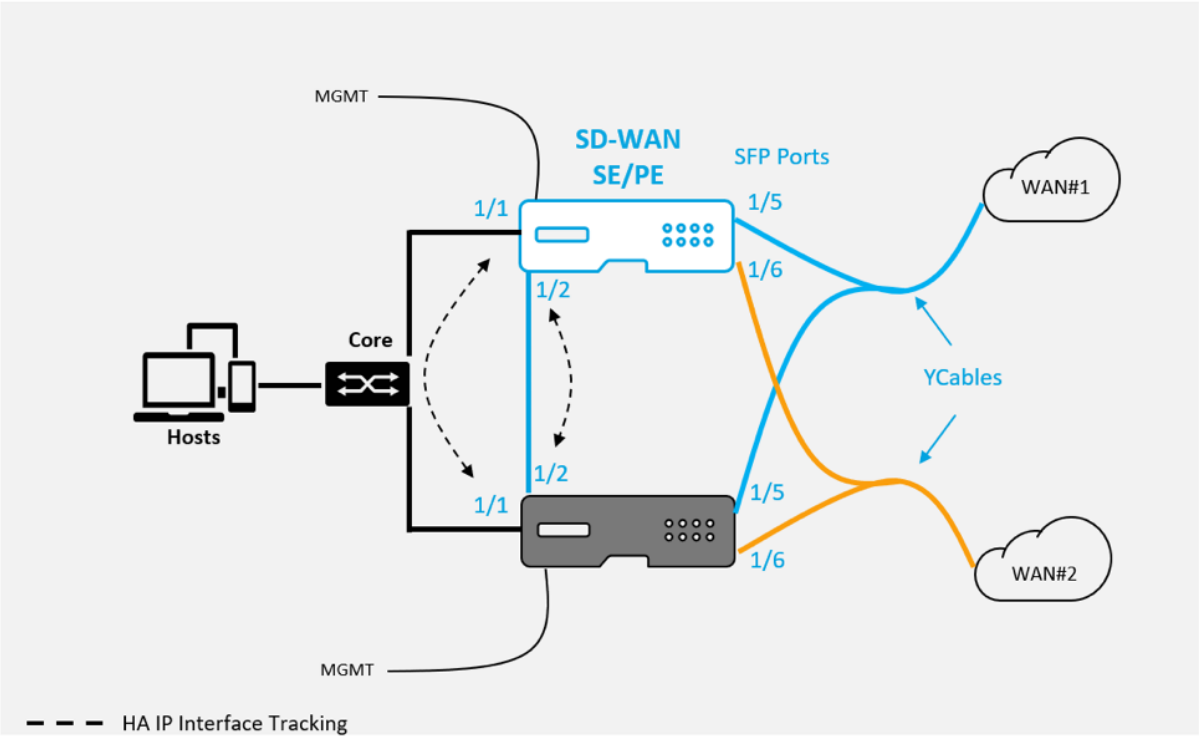
光ファイバ Y ケーブルを使用したエッジモードの高可用性の有効化

August 30, 2022

> 注：リリース 10.2 バージョン 2 では、この機能は 1100 SE アプライアンスにのみ適用できます。

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ーであるエッジモードで展開された 1100 SE アプライアンスで高可用性（HA）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ことで、エッジ・モード導入の高可用性機能を実現できます。
1100 SE アプライアンスでは、スプリッタケーブルのスプリットエンドは、HA ペアで構成された 2 台の 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ーのファイバハンドオフに接続され、もう一方の端は HA ペアで展開された 2 台の 1100 SE アプライアンスの 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。

SD-WAN Orchestrator サービスベースのエッジモード HA 展開については、「デバイスの詳細」を参照してください。



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

August 30, 2022

> 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 1100 Standard Edition
> - SD-WAN 2100 Standard 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。

ゼロタッチ展開のクラウドサービスは、ゼロタッチ対応デバイス（2100-SE など）を購入した Citrix 顧客の保存された ID をホストするバックエンド 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。

詳しくは、Citrix SD-WAN Orchestrator サービスのゼロタッチ展開のトピックを参照してください 。

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。

- 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。

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。

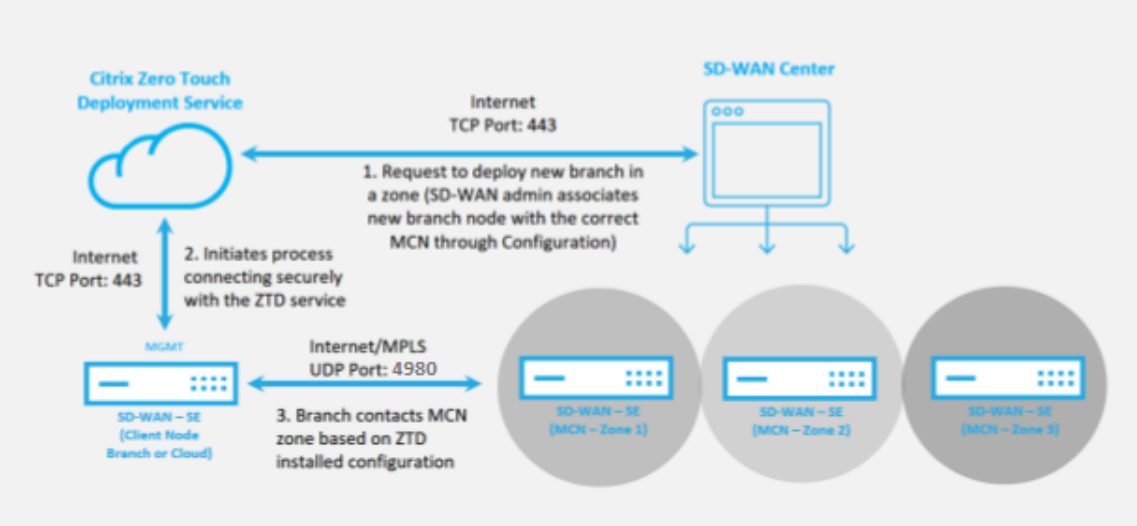
リモート・サイト:

オンサイト・インストーラ—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。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。

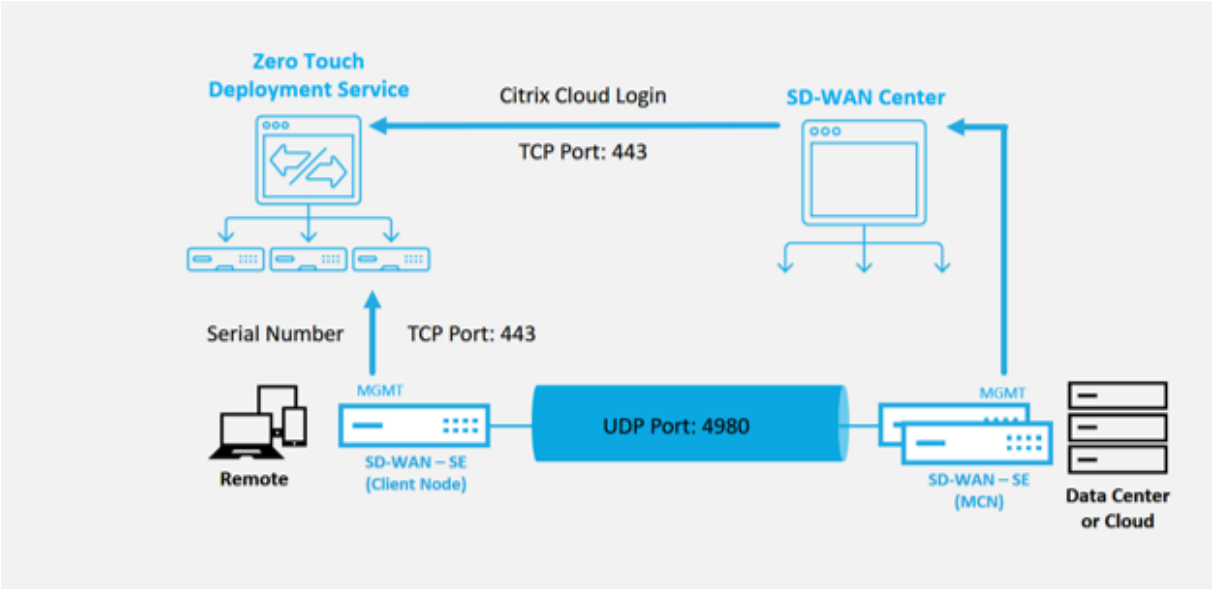
> 注
>
> インタフェースのレイアウトはモデルごとに異なるため、データおよび管理ポートの識別に関するドキュメントを参照してください。



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。
- 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）。
- 直接またはプロキシサーバーを介して、ポート 443 でインターネットへの管理ネットワーク接続 (SD-WAN Appliance)。
- （オプション）既存のアンダーレイネットワーク全体で正常なパス確立を検証するために、MCN への有効な仮想パス接続を備えたクライアントモードのブランチオフィスで動作してい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:

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、管理者は環境に最初の SD-WAN デバイスを展開することから始める必要があります。

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。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。

ゼロタッチ展開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。

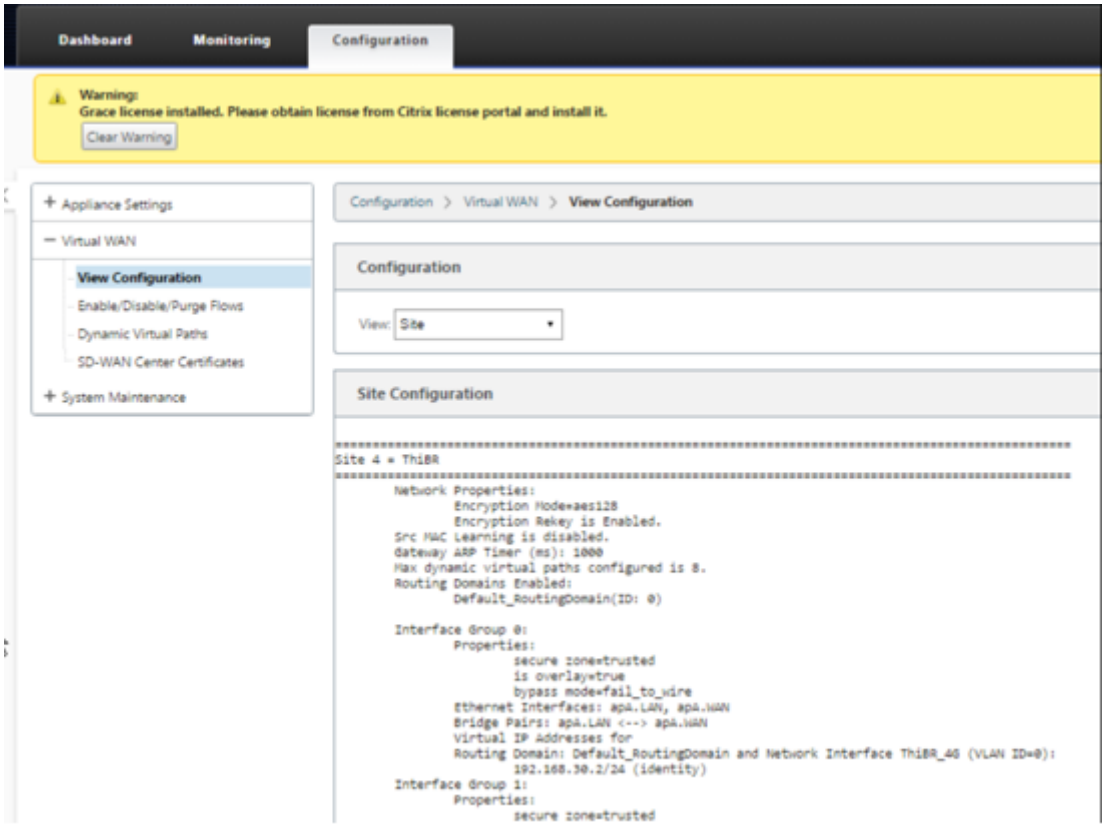
- シリアル番号を検証して、ブランチアプライアンスを認証します。
- 対象のアプライアンスに固有の構成ファイルをブランチアプライアンスにプッシュします。
- ブランチアプライアンスに構成ファイルをインストールします。

- 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。

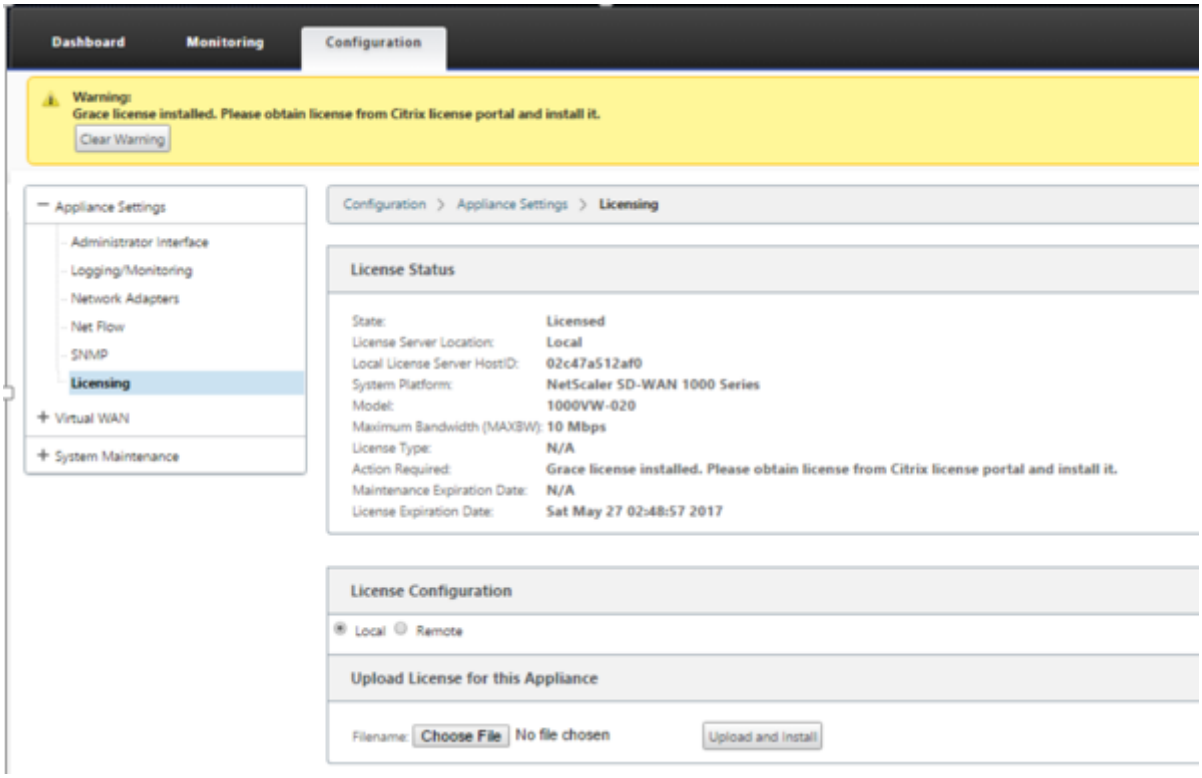
SD-WAN 管理者がアプライアンスに永久ライセンスファイルをインストールするには、さらに多くの手順が必要です。

> (
> 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。

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。



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。



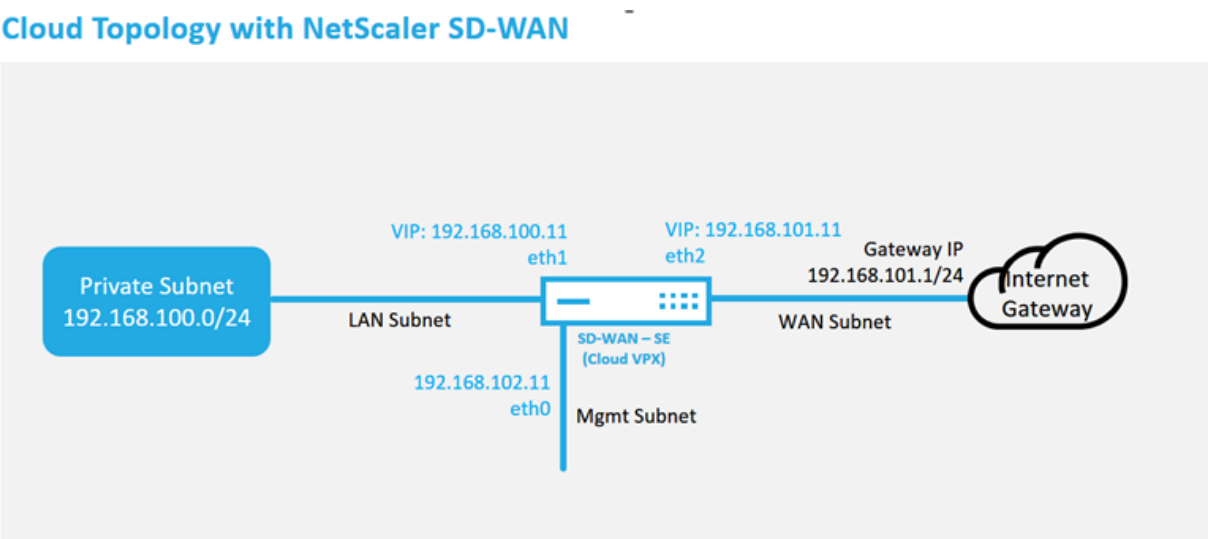
永続ライセンスファイルをアップロードしてインストールすると、Grace License 警告バナーが消え、ライセンスのインストールプロセス中にリモートサイトへの接続が失われることはありません（ping はドロップされません）。

AWS

August 30, 2022

SD-WAN リリース 11.5 では、AWS 環境でのゼロタッチデプロイが SD-WAN Orchestrator サービスを通じてサポートされています。

> 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 で利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。



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。

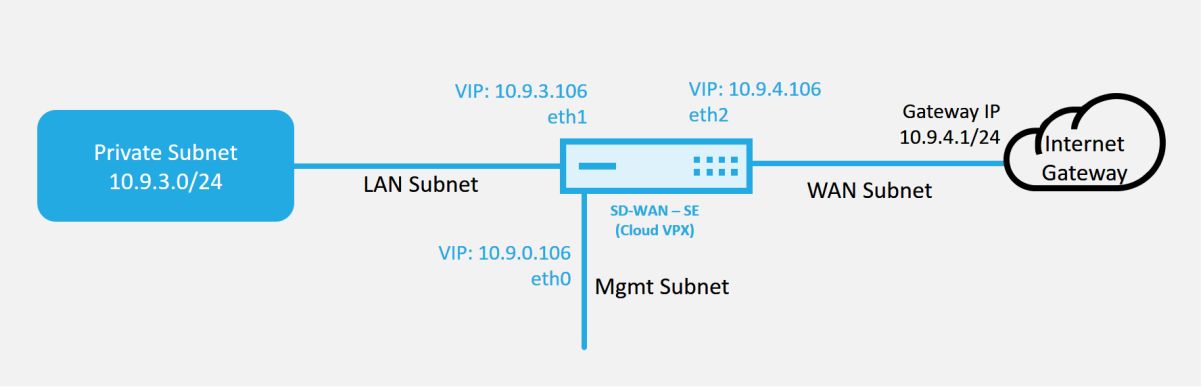
Azure

August 30, 2022

SD-WAN リリース 11.5 では、SD-WAN Orchestrator サービスを通じて Azure 環境でのゼロタッチ展開がサポートされます。

> 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。ゼロ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 リンクに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。

単一リージョンの展開

August 30, 2022

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。

Citrix SD-WAN Orchestrator サービスによる単一リージョン展開の詳細については、「リージョン」を参照してください。

マルチリージョンの展開

August 30, 2022

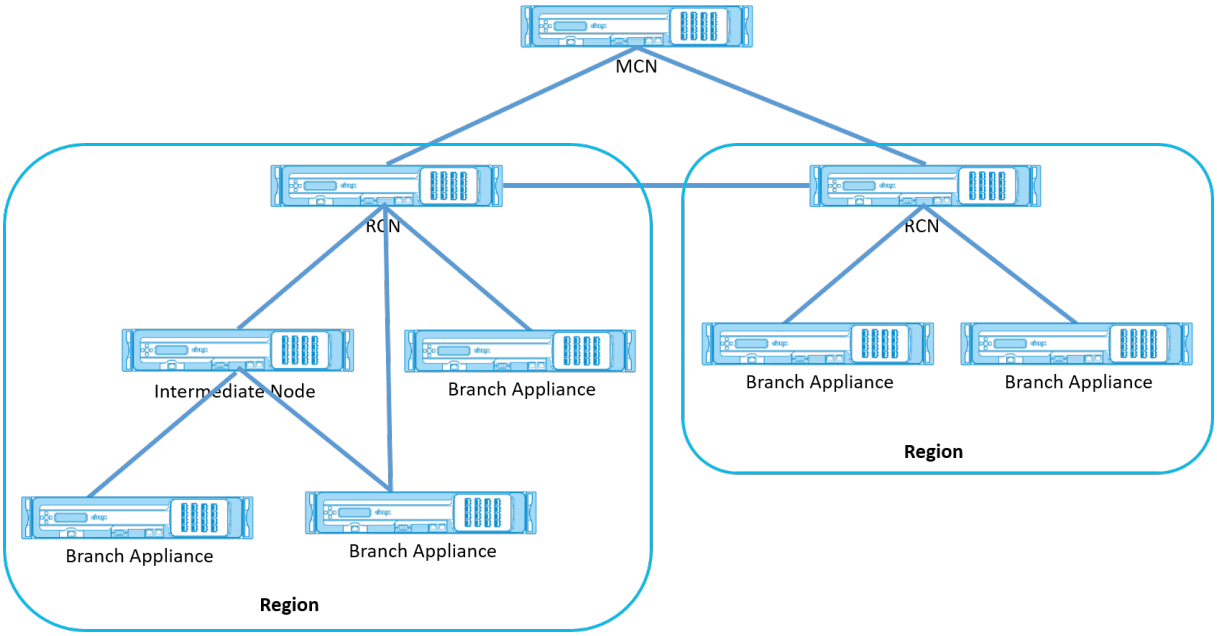
マスターコントロールノード (MCN) として構成された SD-WAN アプライアンスは、マルチリージョンの展開をサポートします。MCN は、複数の地域制御ノード (RCN) を管理します。各 RCN は、複数のクライアントサイトを管理します。MCN を使用して、一部のクライアントサイトを直接管理することもできます。

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。

Citrix SD-WAN Orchestrator サービスによるマルチリージョン展開の詳細については、「リージョン」を参照してください。



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。

> 注
>
> 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
1100-SE	はい	はい
VPX-SE、VPXL-SE	はい	はい

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
2100-SE, 4100-SE, 5100-SE, 6100-SE	はい	はい

Citrix Virtual Apps and Desktops のワークロードの構成ガイド

August 30, 2022

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

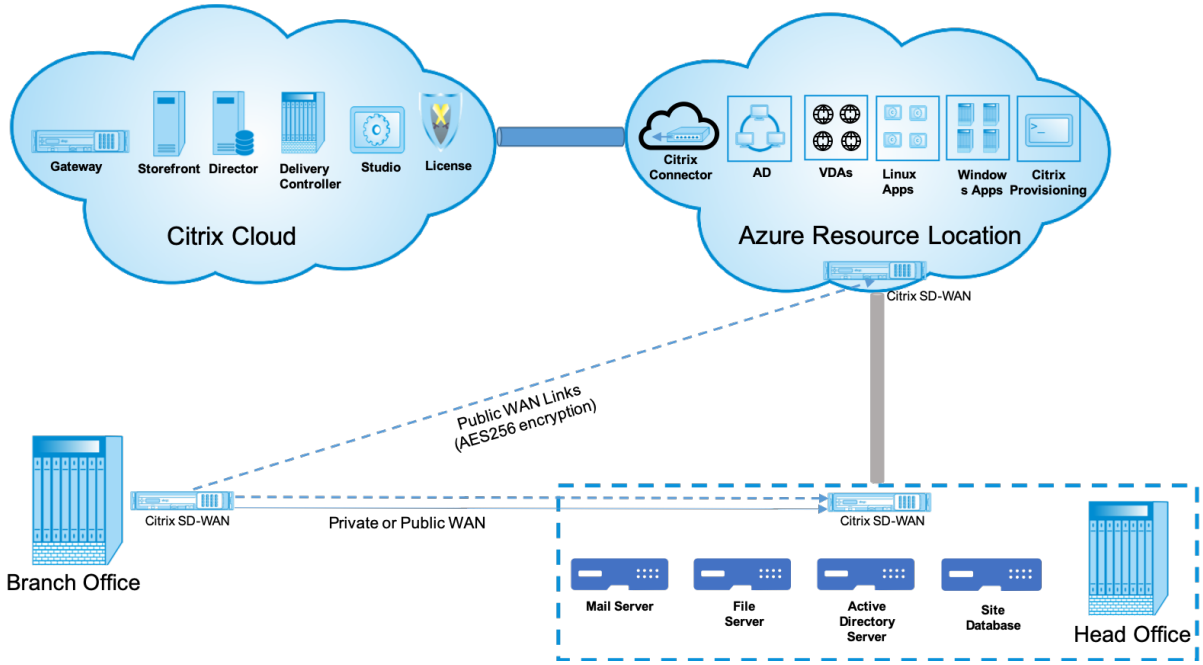
- ガイド付きワークフローにより、Citrix Virtual Apps and Desktops で SD-WAN を簡単にセットアップ
- 高度な SD-WAN テクノロジーにより、常時オンで高性能な接続を実現
- すべての接続（VDA から DC、ユーザーから VDA、VDA からクラウド、ユーザーからクラウド）にわたるメリット
- データセンターへのトラフィックのバックホールに比べてレイテンシを低減
- QoS（サービス品質）を確保するためのトラフィック管理
  - HDX/ICA トラフィックストリーム間の QoS（シングルポートマルチストリーム HDX 自動 QoS）
  - HDX 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ス、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

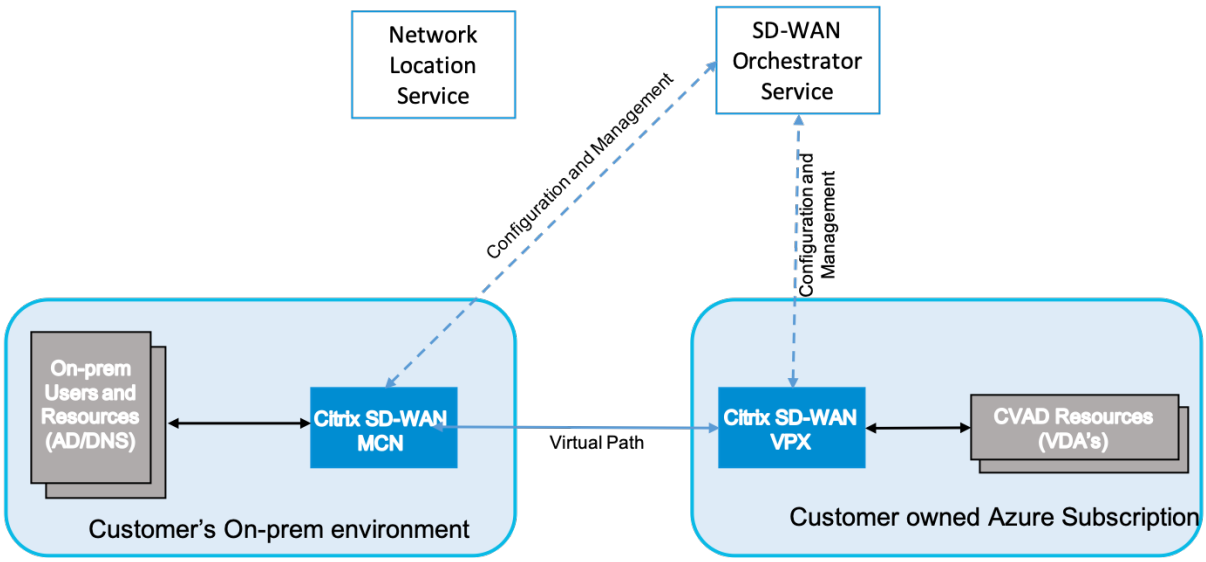


デプロイメントには、次のエンティティが必要です。

- 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 Cloud Connector/Cloud Connector** -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 とリソースの場所の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。

導入と構成



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。

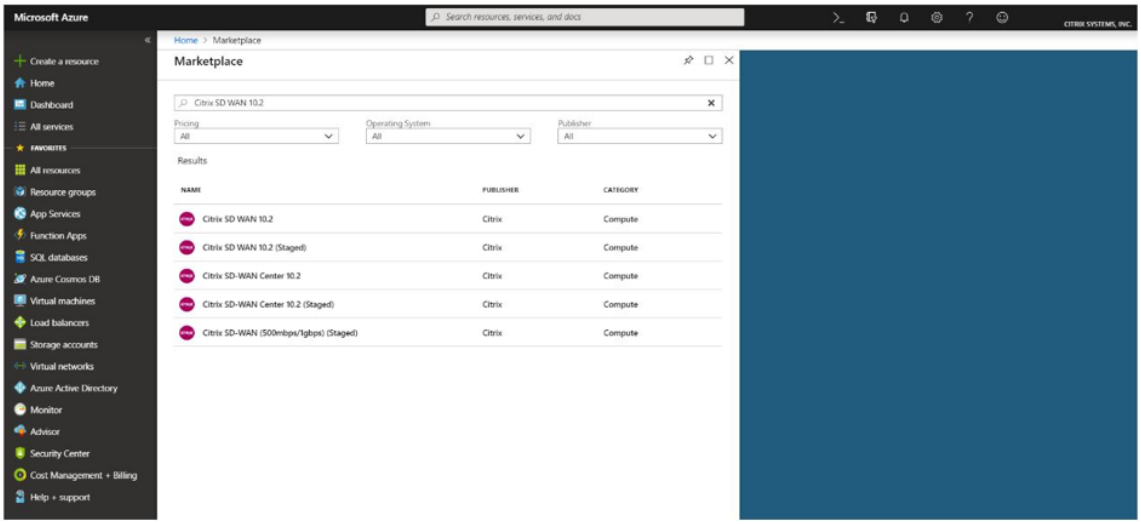
この統合の第 3 のコンポーネントは、内部ユーザーが Gateway をバイパスして VDA に直接接続できるようにするネットワークロケーションサービス（**NLS**）です。これにより、内部ネットワークトラフィックの待ち時間が短縮されます。NLS は、手動または Citrix SD-WAN Orchestrator を使用して構成できます。詳細については、「NLS」を参照してください。

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-WANStandard Edition を検索します。

2. 検索結果で、Citrix SD-WANStandard 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ら、[作成] をクリックします。

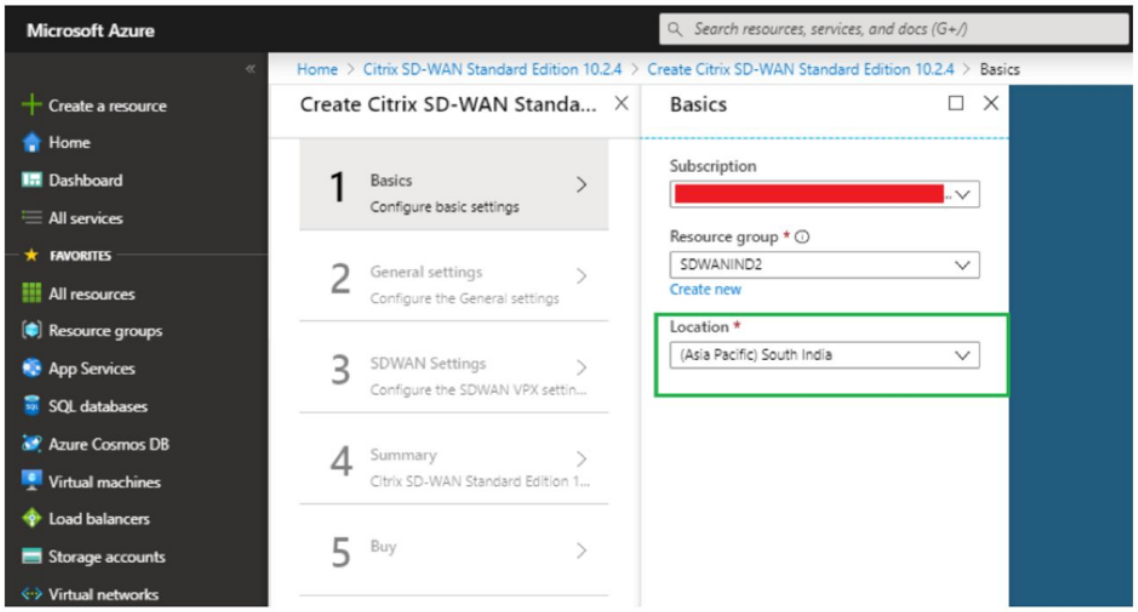


[**Create**] をクリックすると、仮想マシンを作成するために必要な詳細情報を入力するウィザードが表示されます。

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ーです。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。

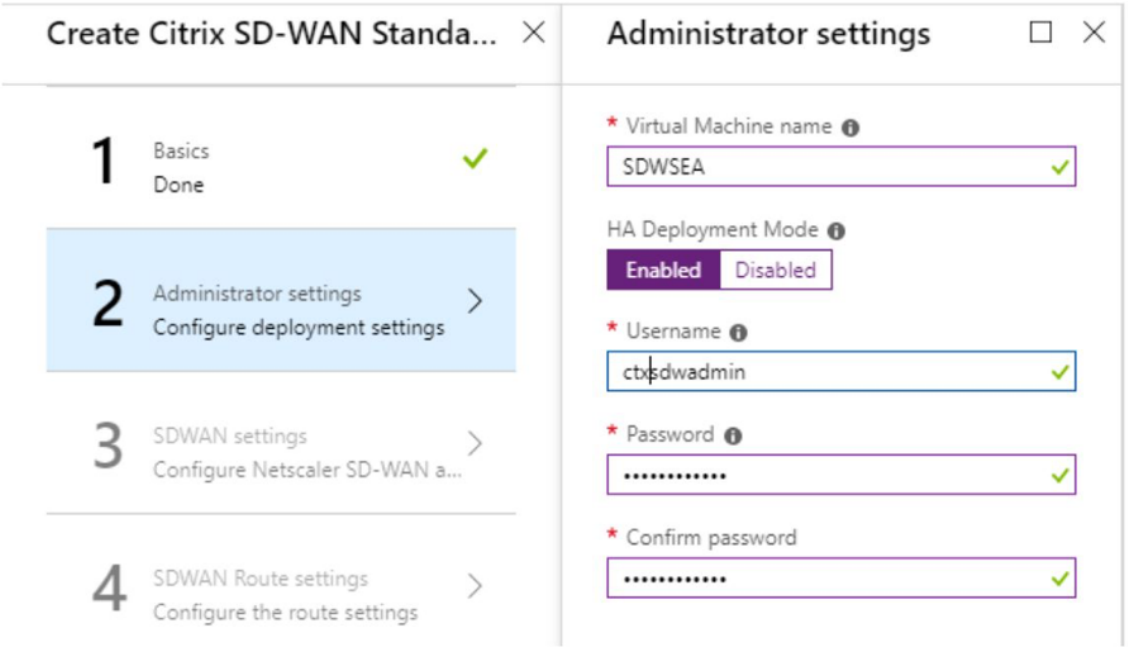
Citrix SD-WAN の場合は、選択するリソースグループを空にする必要があります。同様に、SD-WAN インスタンスをデプロイする Azure リージョンを選択します。リージョンは、Citrix Virtual Apps and Desktops リソースが展開されるリージョンと同じである必要があります。



4. [管理者設定] ページで、仮想マシンの名前を入力します。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。

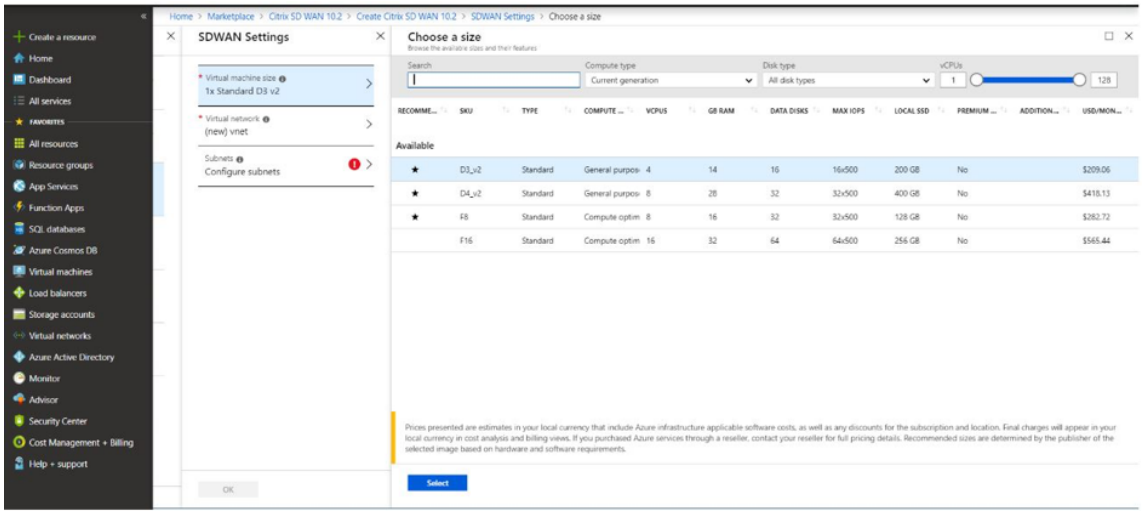
   このパスワードは、インスタンスの管理インターフェイスにゲストユーザーとしてログインするために必要です。インスタンスへの管理者アクセスを取得するには、インスタンスの Provisioning 中に作成されたユーザー名およびパスワードとして admin を使用します。インスタンスの Provisioning 中に作成されたユーザー名を使用すると、読み取り専用アクセスが取得されます。また、ここで展開の種類を選択します。

   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。

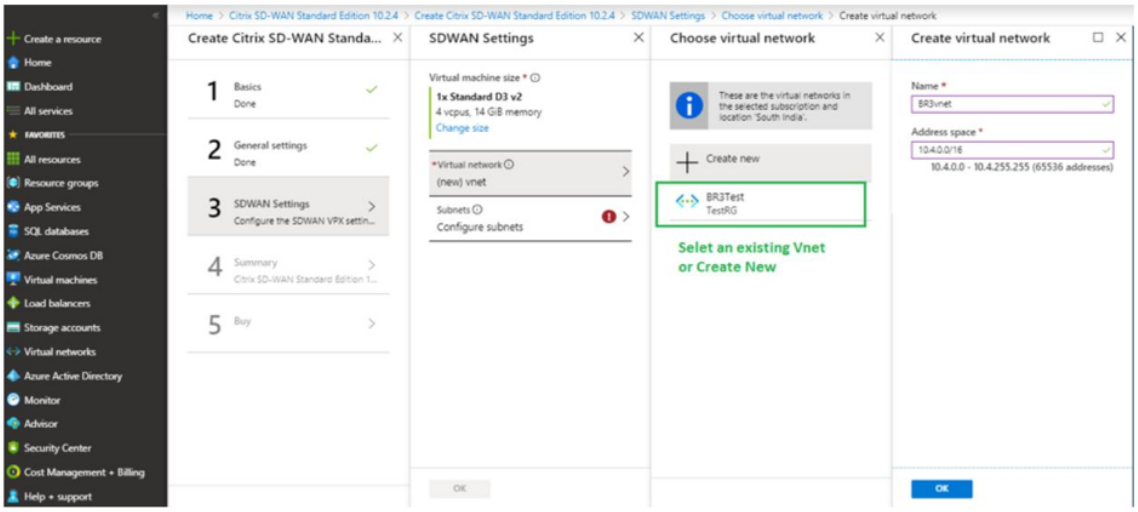


5. [**SD-WAN** 設定] ページで、イメージを実行するインスタンスを選択します。要件に応じて、次のインスタンスタイプを選択します。

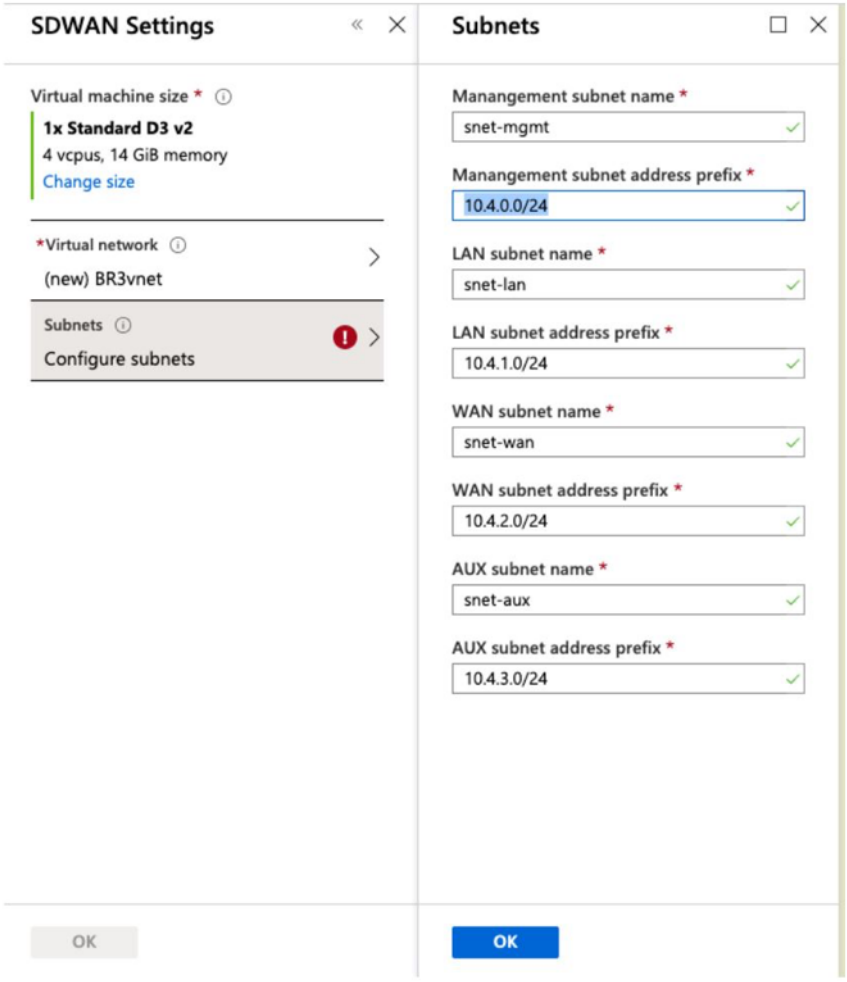
   - インスタンスタイプ D3_V2。最大単一方向スループットが 200 Mbps で、最大 16 のブランチに直接接続できます。
   - インスタンスタイプ D4_V2。最大単一方向スループットが 500 Mbps で、最大 16 のブランチに直接接続できます。
   - インスタンスタイプ F8 標準。最大単一方向スループットが 1 Gbps で、最大 64 のブランチに直接接続できます。
   - インスタンスタイプ F16 標準。最大単一方向スループットが 1 Gbps で、最大 128 のブランチに直接接続できます。



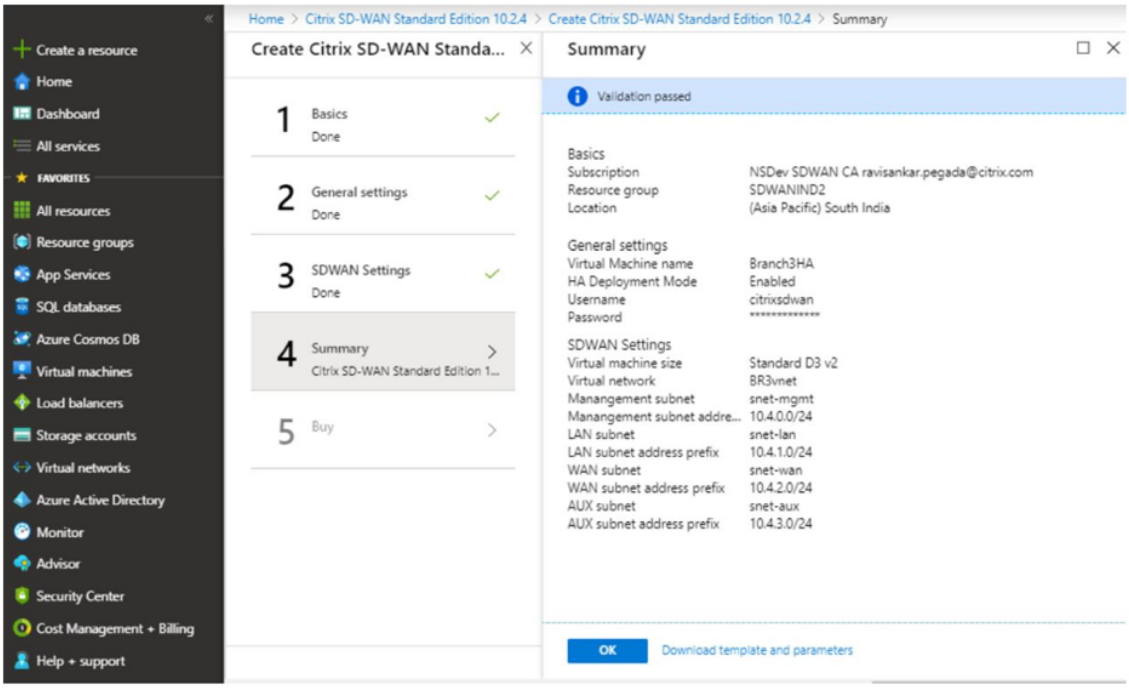
6. 新しい仮想ネットワーク (VNet) を作成するか、既存の VNet を使用します。このステップでは、SD-WAN VPX VM のインターフェイスに割り当てるサブネットを選択するため、これは展開にとって最も重要なステップです。



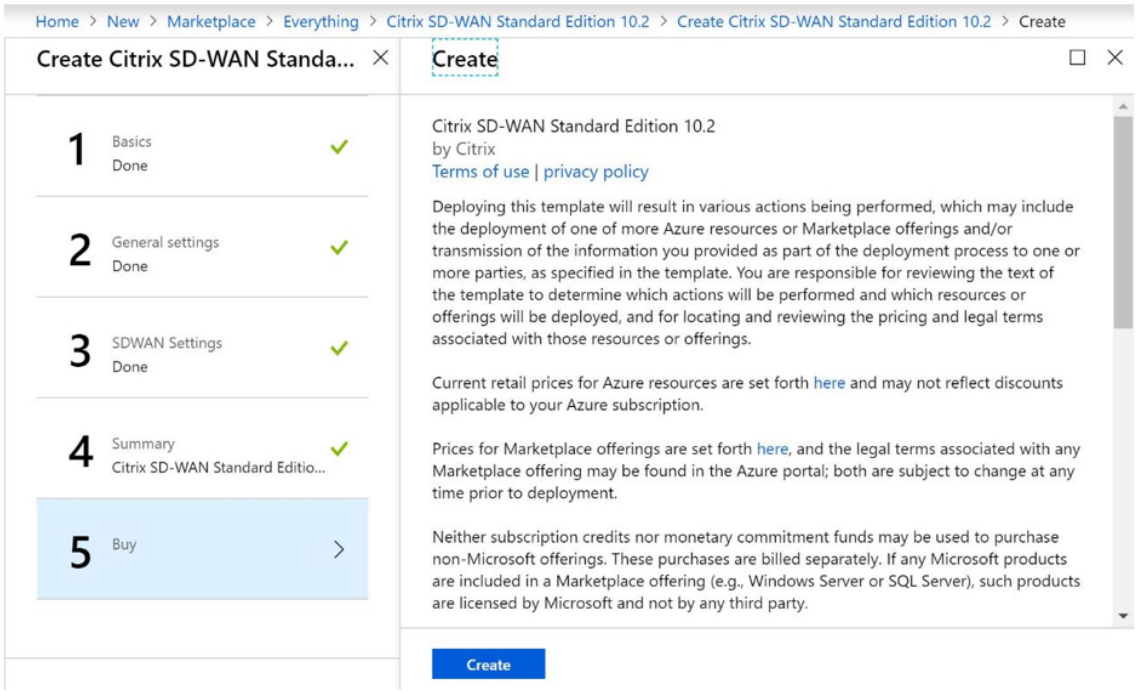
AUX サブネットは、HA モードでインスタンスをデプロイする場合のみ必要です。SD-WAN インスタンスが Citrix Virtual Apps and Desktops リソースと同じ VNet にデプロイされ、SD-WAN VPX アプライアンスの LAN インターフェイスと同じサブネット上にあることを確認します。



7. ［概要］ページで設定を確認し、［**OK**］をクリックします。



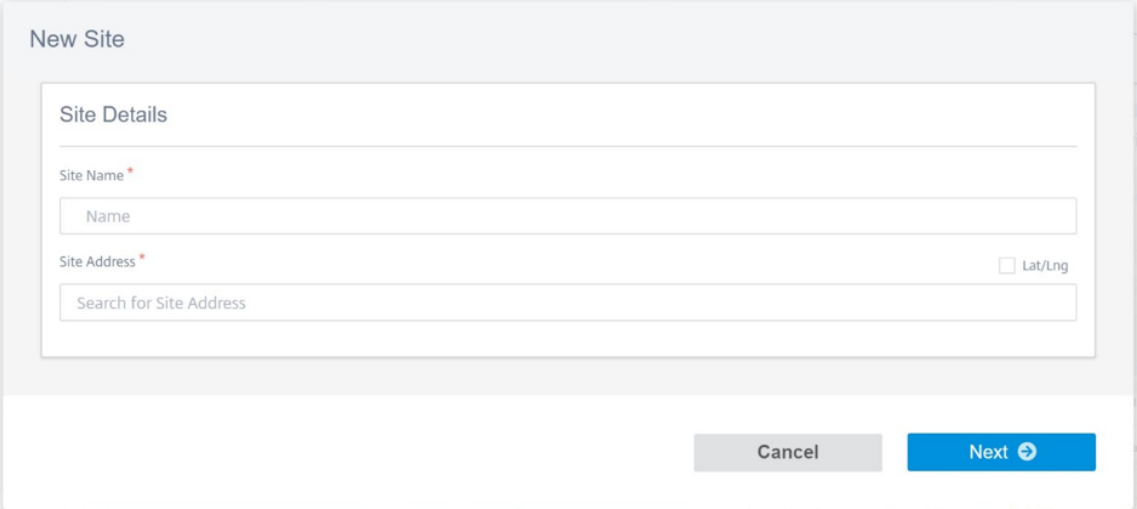
8. [**Buy**] ページで [**Create**] をクリックして、インスタンスのプロビジョニングプロセスを開始します。インスタンスがプロビジョニングされるまでに約 10 分かかる場合があります。Azure 管理ポータルに、インスタンスの作成の成功/失敗を示す通知が表示されます。



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
>
> ）管理者アクセスの場合、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。

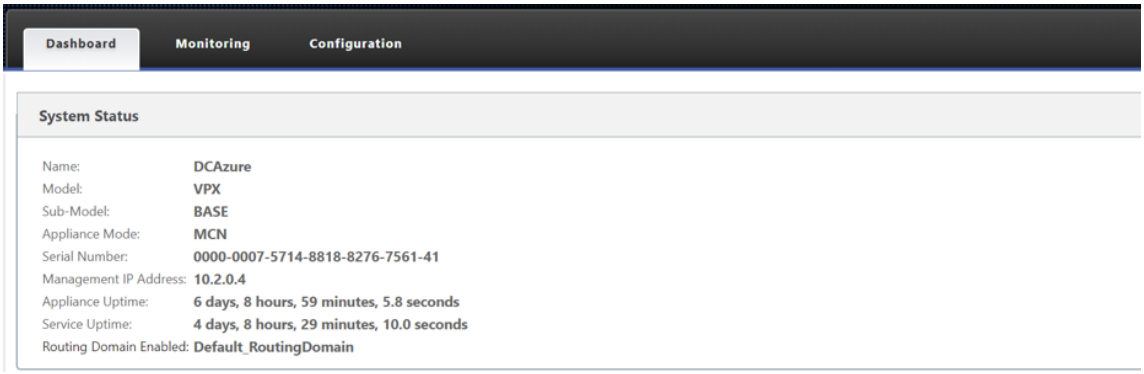
9. サイトがプロビジョニングされたら、SD-WAN Orchestrator にログインして構成します。前提条件で説明したように、サイトを構成するには SD-WAN Orchestrator のエンタイトルメントが必要です。まだお持ちでない場合は、Citrix SD-WAN Orchestrator のオンボーディングを参照してください。
10. SD-WAN ネットワークが既にある場合は、Azure でプロビジョニングしたサイトの構成の作成に進みます。それ以外の場合は、MCN を作成する必要があります。詳細については、「ネットワーク構成」を参照してください。
11. SD-WAN Orchestrator へのアクセス権があり、すでに MCN を設定したら、SD-WAN オーケストレータにログインし、[**+ New]** サイトをクリックして (Azure でプロビジョニングした) SD-WAN VPX アプライアンスの構成を開始します。



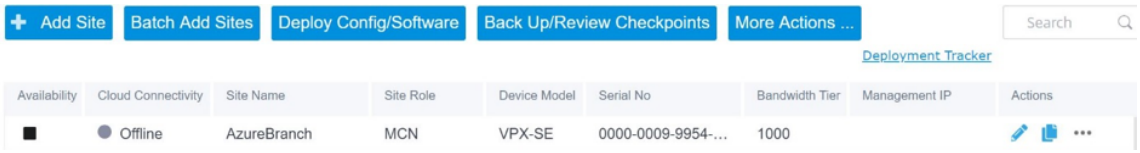
12. 一意のサイト名を指定し、イメージを Provisioning するリージョンに基づいてアドレスを入力します。Azure でインスタンスをセットアップするには、基本設定を参照してください。

> 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** 仮想マシン**] > [**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 **。

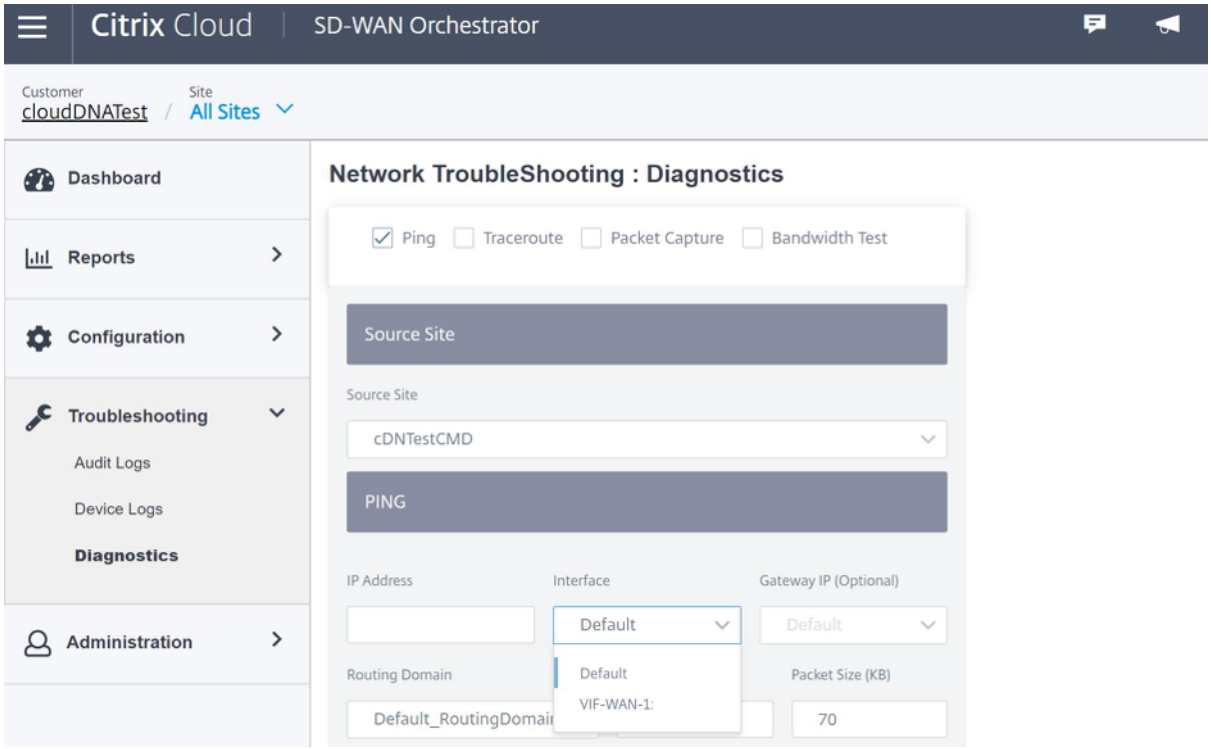


15. 問題がなく、構成が正確である場合は、構成展開を実行した後、Azure のインスタンスと MCN の間の仮想パスを作成する必要があります。

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 を備えた展開では、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 を使用している場合は、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、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。



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利用でき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、内部ユーザーはゲートウェイをバイパスして 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遅延が軽減されます。

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 の構成について詳しくは、「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た NLS の構成について詳しくは、「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

August 30, 2022

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マシンが読み取ることができる 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

次の種類の DNS サービスを使用して、Citrix SD-WAN Orchestrator サービスを介した DNS プロキシまたは DNS 透過的な転送を構成できます。

- 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 Orchestrator サービスを介して DNS プロキシを構成する方法については、「DNS プロキシ」を参照してください。

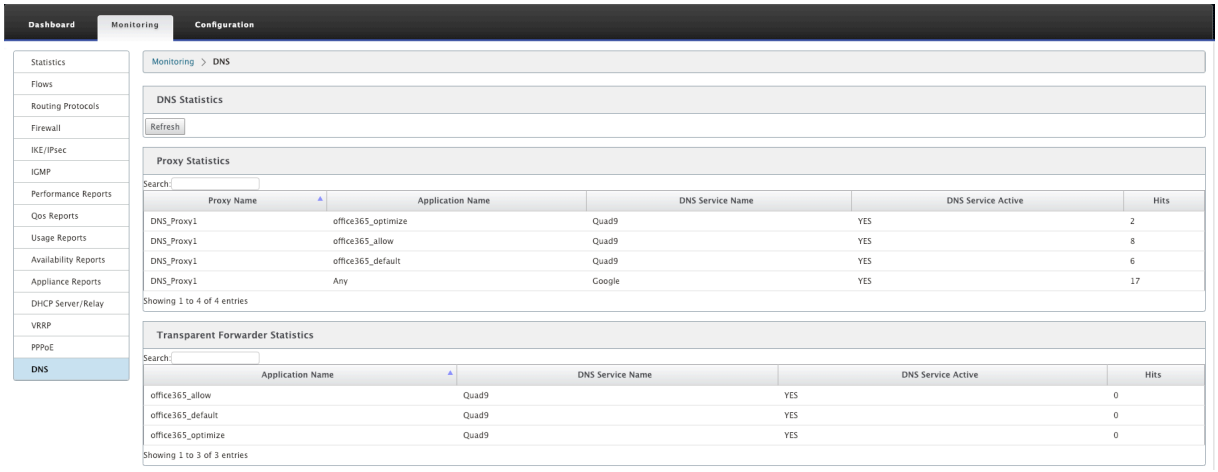
DNS トランスペアレントフォワーダ

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 Orchestrator サービスを介して DNS トランスペアレントフォワーダーを構成する方法については、「DNS トランスペアレントフォワーダー」を参照してください。

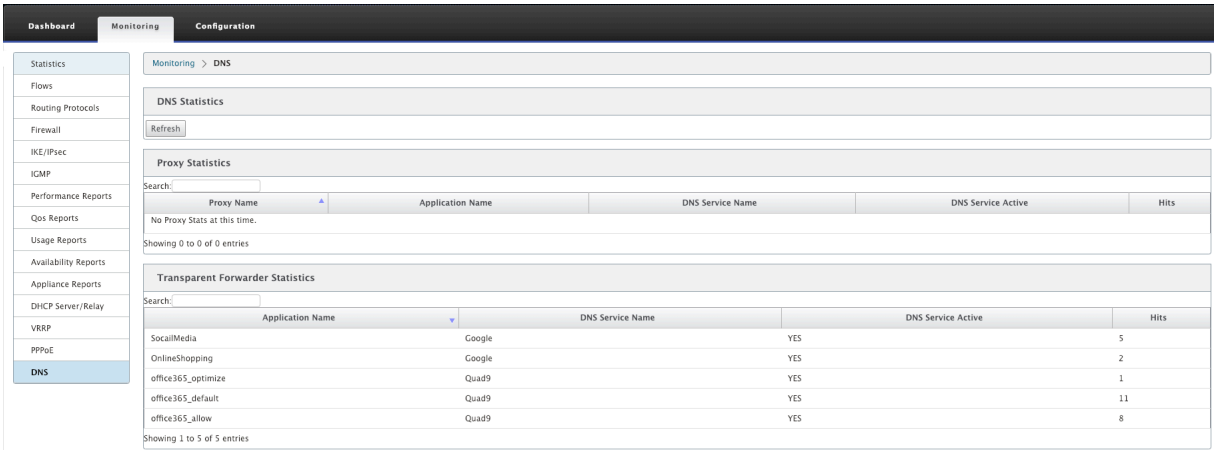
監視

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



トランスペアレントフォワーダの統計



DHCP

November 17, 2022

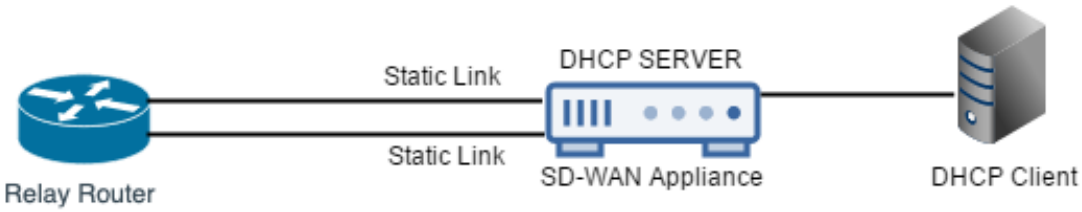
Citrix SD-WAN には、Standard Edition アプライアンスを DHCP サーバーまたは DHCP リレーエージェントとして使用する機能が導入されています。DHCP サーバー機能を使用すると、SD-WAN アプライアンスの LAN/WAN インターフェイスと同じネットワーク上のデバイスが、SD-WAN アプライアンスから IP 設定を取得できます。DHCP リレー機能を使用すると、SD-WAN アプライアンスは DHCP クライアントとサーバ間で DHCP パケットを転送できます。

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。

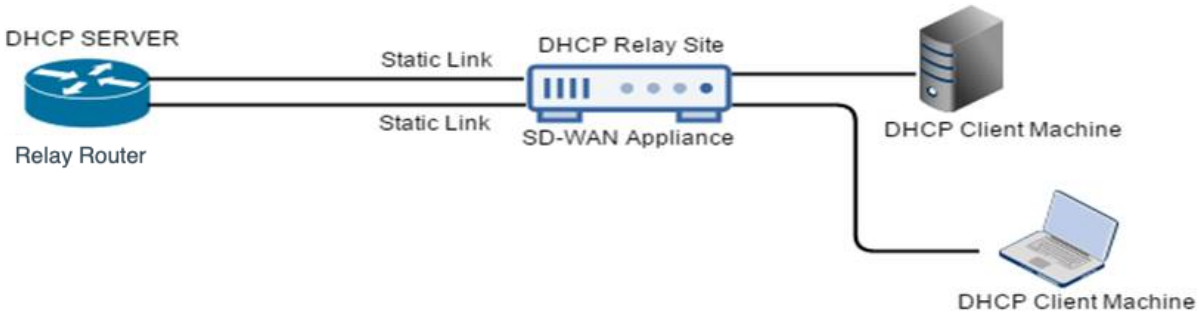
DHCP サーバ

Citrix SD-WAN アプライアンスは、DHCP サーバー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プールの 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 クライアントによる WAN リンク IP アドレスの学習

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にのみ、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。

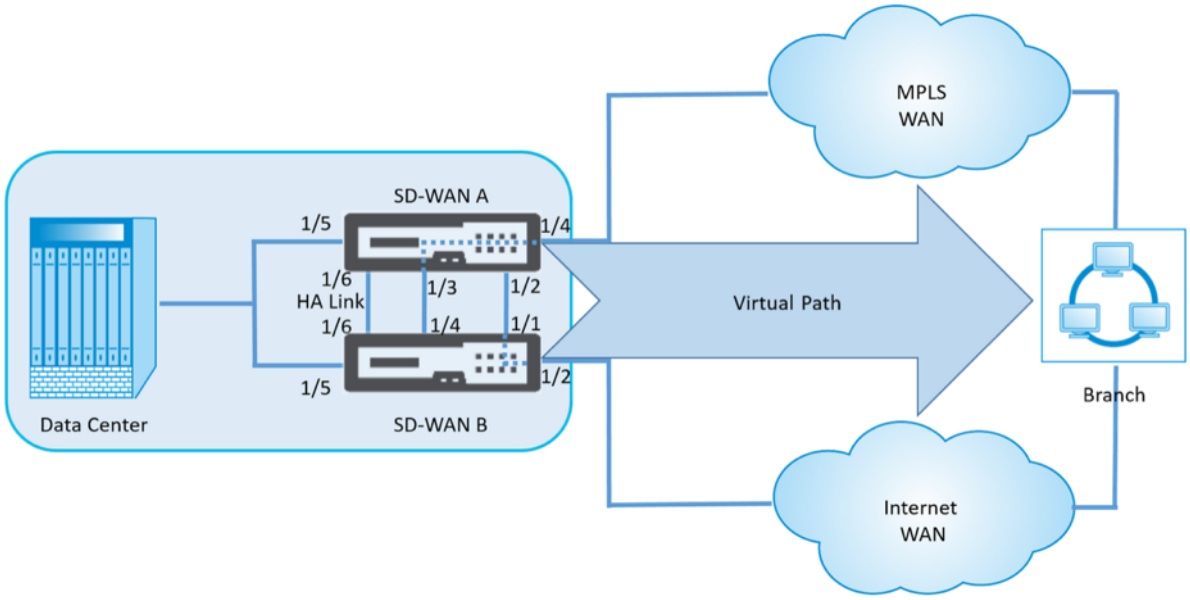
Citrix SD-WAN 11.5 リリース以降、Citrix SD-WAN Orchestrator サービスを介して、フェールツーブロックモードで信頼できない仮想インターフェイスの DHCP を構成できます。詳細については、「DHCP クライアントによる WAN リンク IP アドレスの学習」を参照してください。

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。
- DHCP インターフェイスをプライベートイントラネット **WAN** リンクの一部として選択できます。

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。



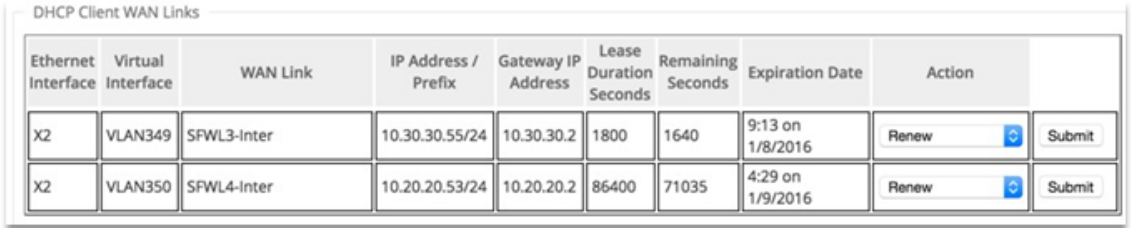
> 注:
>
> パケットはインターフェイス間でブリッジングされる可能性があるため、LAN インターフェイスをフェールツーワイヤペアに接続しないでください。

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の仮想 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。

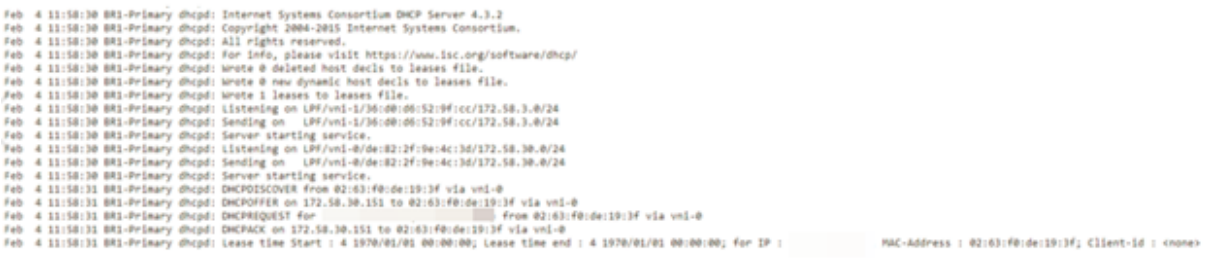

DHCP Client WAN Links

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。



> 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

August 30, 2022

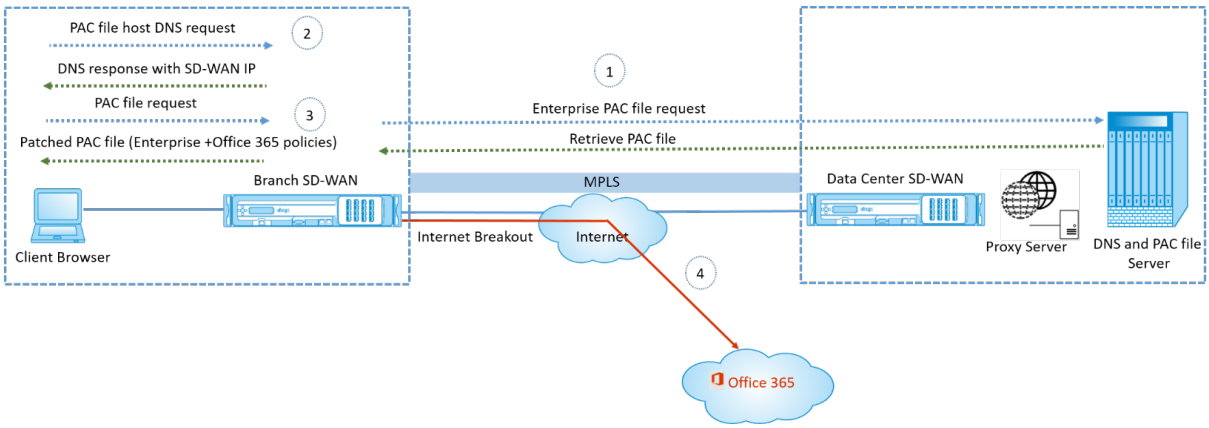
ミッションクリティカルな SaaS アプリケーションと分散型ワークフォースの企業導入の増加に伴い、レイテンシーと輻輳を低減することが非常に重要になります。レイテンシーと輻輳は、データセンターを通過するトラフィックをバックホールする従来の方法に固有のものです。Citrix SD-WAN では、Office 365 などの SaaS アプリケーションを直接インターネットから抜け出すことができます。詳細については、「Office 365 の最適化」を参照してください。

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ー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 ブレー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プレースホルダ (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

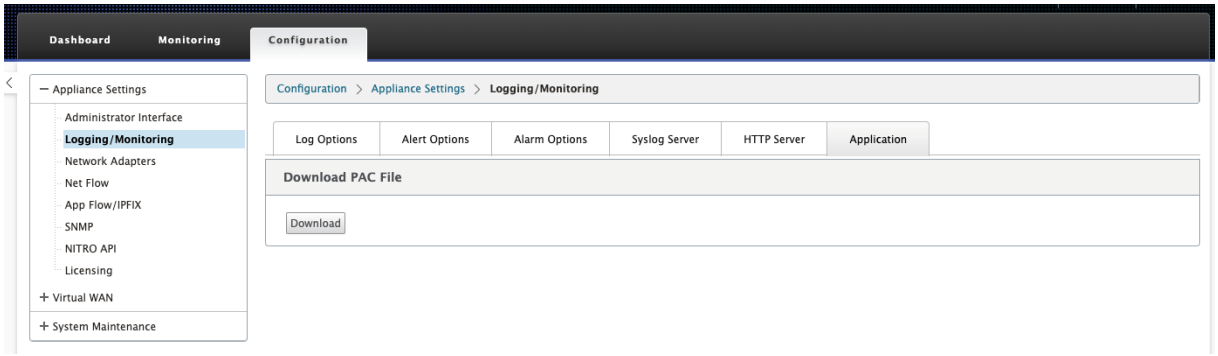
1. 企業は、PAC ファイルをホストする必要があります。
2. PAC ファイルには、プレースホルダー *SDWAN_TAG* 、または Office 365 の URL にパッチを適用するための *findproxyforurl* 関数の 1 つの出現が含まれている必要があります。
3. PAC ファイルの URL は、IP ベースではなく、ドメインベースである必要があります。
4. PAC ファイルは、信頼されたアイデンティティ VIP を介してのみ提供されます。
5. Citrix SD-WAN アプライアンスは、管理インターフェイス経由でエンタープライズ PAC ファイルをダウンロー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

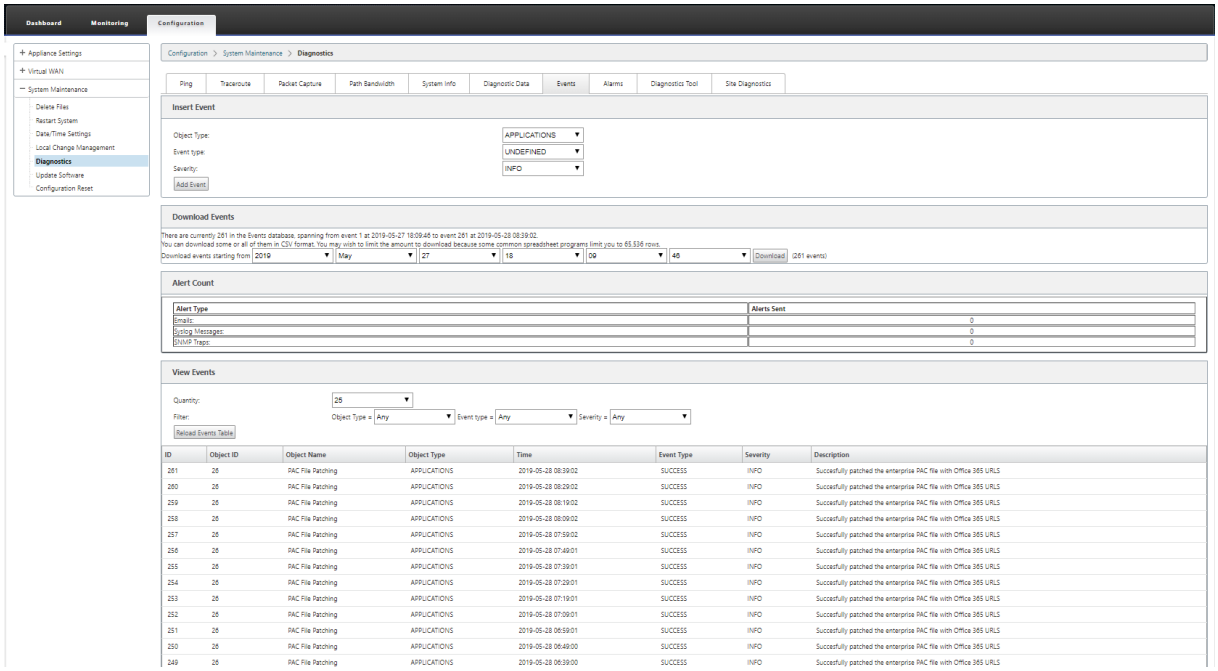
Citrix SD-WAN Orchestrator サービスを使用して PAC ファイルのカスタマイズを有効にできます。詳細については、「プロキシ自動設定」を参照してください。

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 > ロギング/監視 > アプリケーションに移動し、ダウンロードをクリックします。



また、［イベント］セクションで PAC ファイルのパッチ適用ステータスを表示し、［構成］>［システムメンテナンス］>［診断］に移動し、［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 経由の WPAD はサポートされていません。

GRE トンネル

August 30, 2022

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。SD-WAN Orchestrator サービスを使用して GRE トンネルを構成するには、「GRE サービス」を参照してください。

帯域内およびバックアップ管理

August 30, 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、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には、インバンド管理を構成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 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。

Citrix SD-WAN 11.5 以降では、Citrix SD-WAN Orchestrator サービスを介してのみ仮想 IP のインバンド管理を有効にできます。詳細については、「インバンド管理」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。

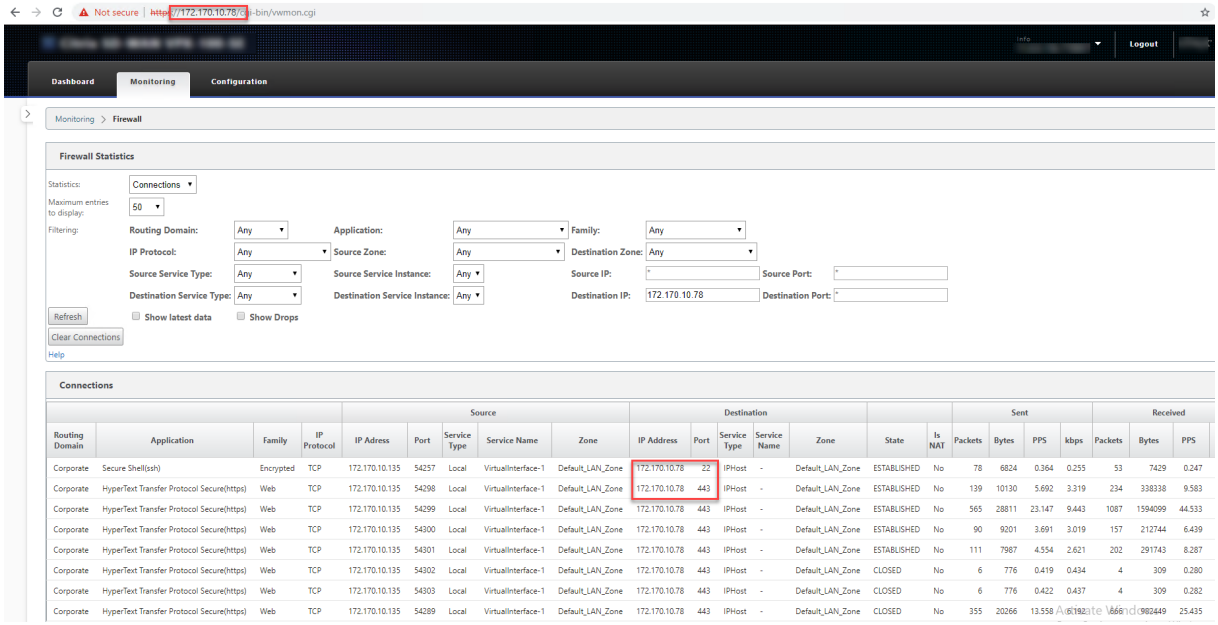
たとえば、アプライアンスへのアクセスには、次のインバンド IP アドレスが使用されます。

- 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。



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。

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。

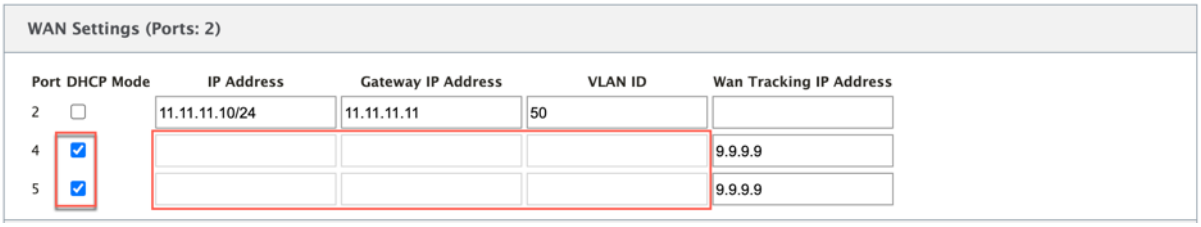
次の表に、異なるプラットフォームでのフォールバック構成用に事前に指定された WAN ポートおよび LAN ポートの詳細を示します。

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
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。



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。

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

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。

バックアップ管理ネットワーク

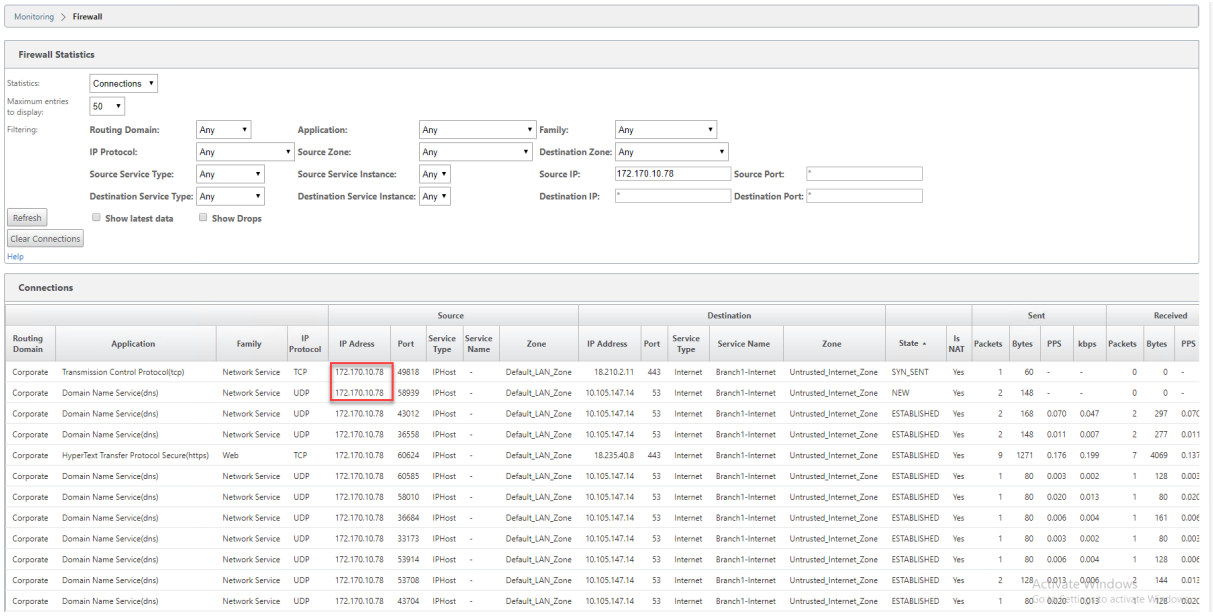
仮想 IP アドレスをバックアップ管理ネットワークとして設定できます。管理ポートにデフォルト Gateway が設定されていない場合、管理 IP アドレスとして使用されます。

> 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。

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。



インターネットアクセス

November 17, 2022

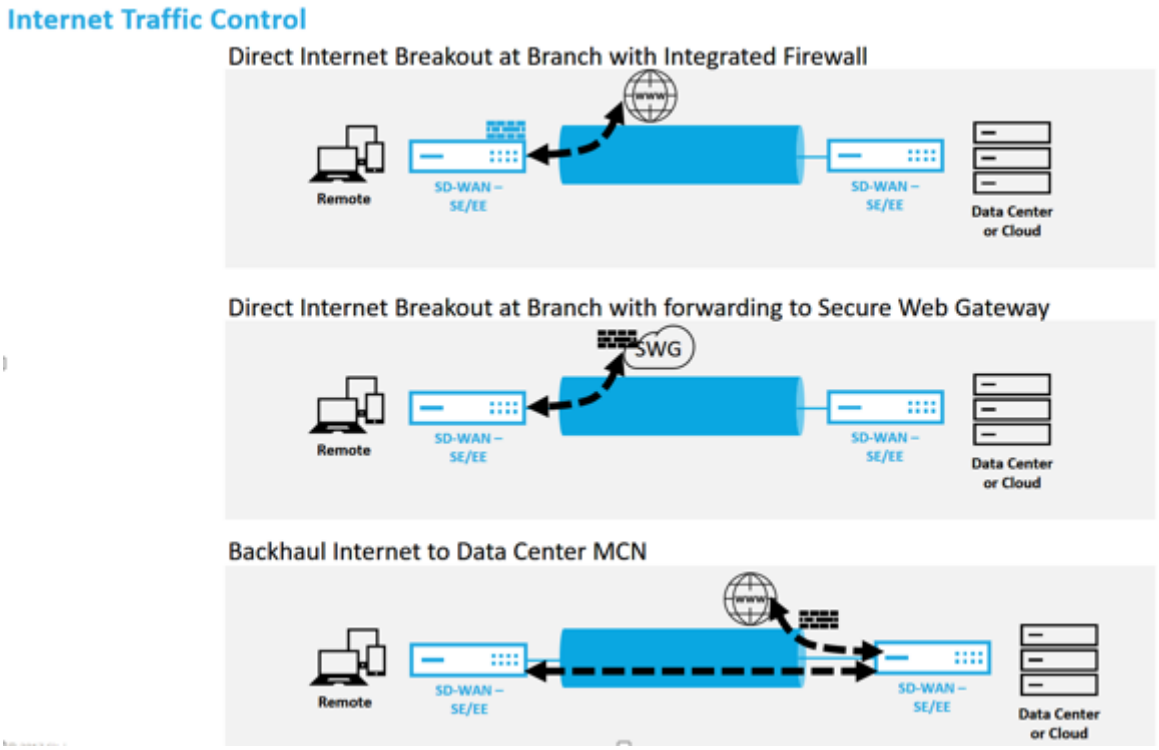
インターネットサービスは、エンドユーザーサイトとパブリックインターネット上のサイト間のトラフィックに使用されます。インターネットサービストラフィックは SD-WAN によってカプセル化されず、仮想パスサービス経由で配信されるトラフィックと同じ機能はありません。ただし、SD-WAN 上でこのトラフィックを分類して考慮することが重要です。インターネットサービスとして識別されるトラフィックにより、管理者が設定した構成に従って、仮

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

Citrix SD-WAN Orchestrator サービスを介してインターネットサービスを構成する方法については、「インターネットサービス」を参照してください。



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

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）

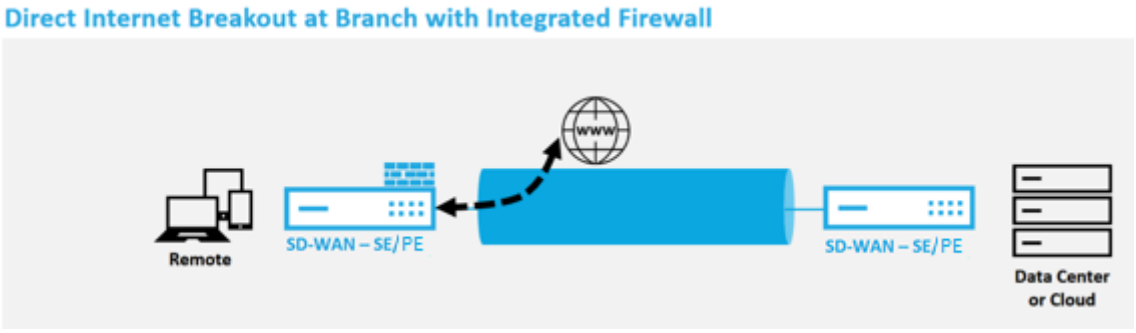
Citrix SD-WAN は、どのネットワークでもオーバーレイソリューションとして導入できます。オーバーレイソリューションとして、SD-WAN は通常、既存の Edge ルータやファイアウォールの背後に展開されます。SD-WAN がネッ

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。

- Edge モードまたは Gateway モード

Citrix SD-WAN を Edge デバイスとして展開し、既存の Edge 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。

Citrix SD-WAN Orchestrator サービスを介してインターネットサービスを構成する方法については、「インターネットサービス」を参照してください。



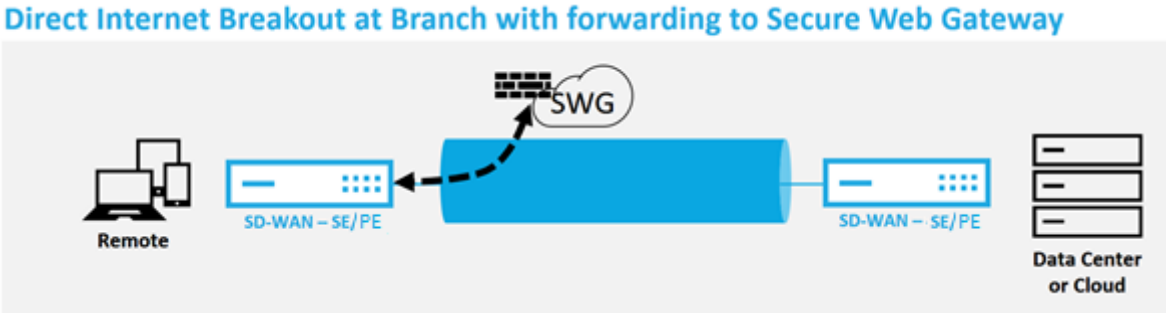
Secure Web Gateway による直接インターネットアクセス

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。

Citrix SD-WAN Orchestrator サービスを介してインターネットサービスを構成する方法については、「インターネットサービス」を参照してください。



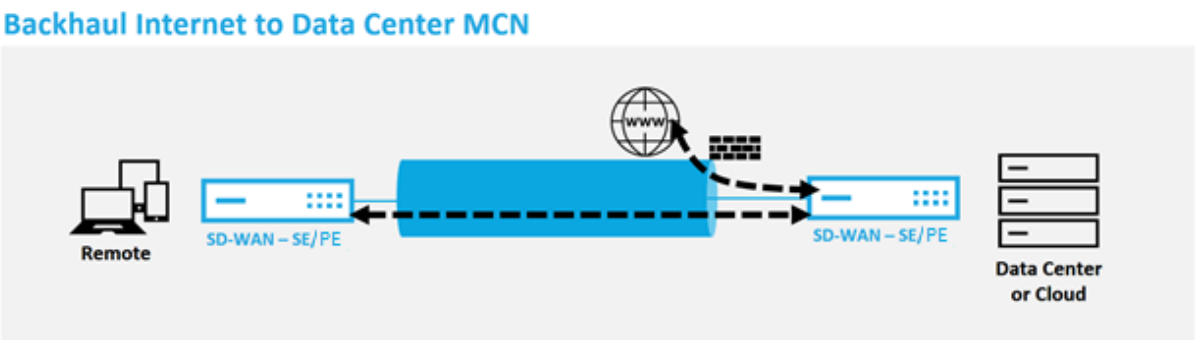
Citrix SD-WAN は、次のサードパーティの Secure Web Gateway ソリューションをサポートしています。

- Zscaler
- Forcepoint
- パロ・アルト
- Citrix Secure Internet Access

バックホールインターネット

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トポロジが原因で、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ライブする可能性があります。

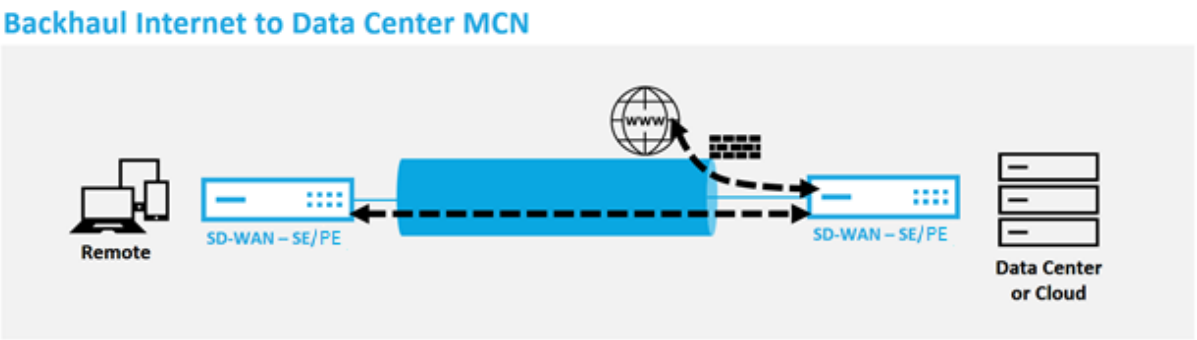


すべての Citrix SD-WAN デバイスは、1 つのデバイスに最大 8 つの異なるインターネット WAN リンクを終了できます。集約された WAN リンクのライセンスされたスループット機能は、Citrix SD-WAN のデータシートに各アプライアンスごとに一覧表示されます。

ヘアピンモード

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。



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 のルートを認識します。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 および VPX（仮想）アプライアンスは、ヘアピン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ニングを使用する場合、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。

ホストされたファイアウォール

November 17, 2022

Citrix SD-WAN Orchestrator サービスは、次のホストされたファイアウォールをサポートします。

- 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

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。ファイアウォールの仮想マシンは、2 つのデータ仮想インターフェイスが接続された状態で仮想ワイヤーモードで統合されています。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。

SD-WAN Orchestrator サービスを介してファイアウォール仮想マシンをプロビジョニングする方法については、ホストされたファイアウォールを参照してください。

長所

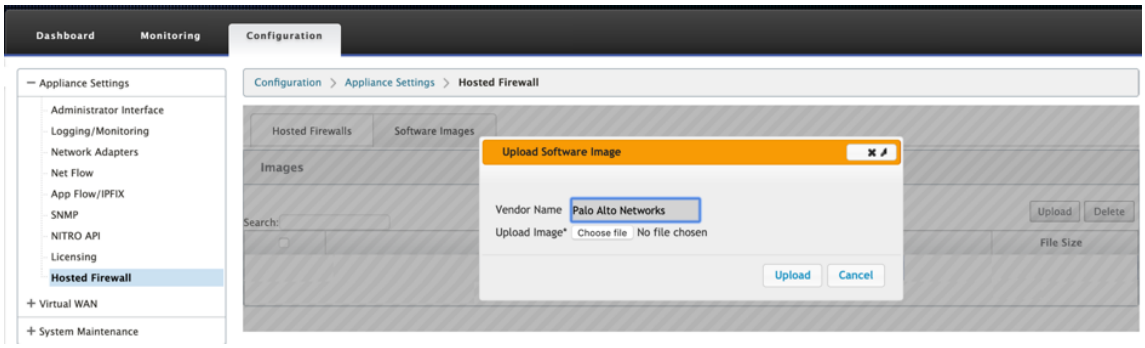
以下は、SD-WAN 1100 プラットフォームでの Palo Alto Networks 統合の主な目標または利点です。

- ブランチデバイスの統合: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 からインターネット、およびインターネットから LAN へのトラフィックを保護するオンプレミスの 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。

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。

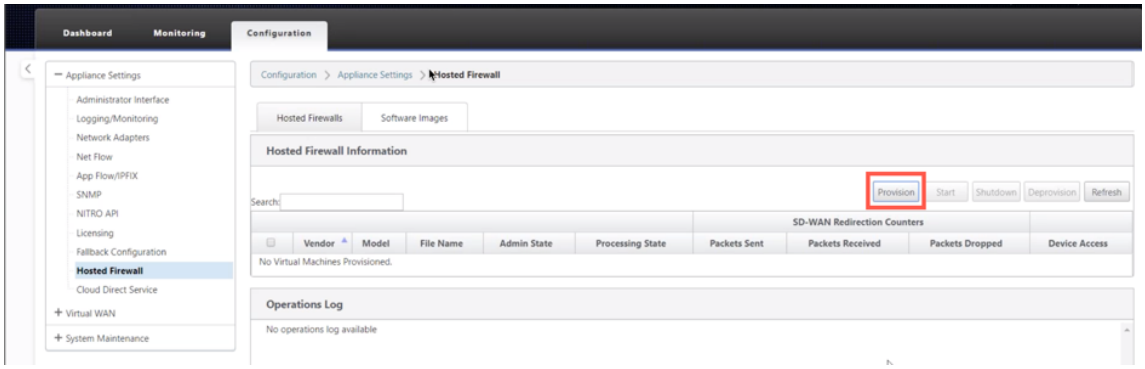
1. Citrix SD-WAN GUI で、［構成］**>**［アプライアンスの設定］の順に 展開し、［ホストされたファイアウォール］を選択します。
2. ソフトウェアイメージをアップロードします。
   - ［ソフトウェアイメージ］タブを選択します。[**Palo Alto Networks**] としてベンダー名を選択します。
   - ソフトウェアイメージファイルを選択します。
   - ［アップロード］をクリックします。



> 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と表示されるまで、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。

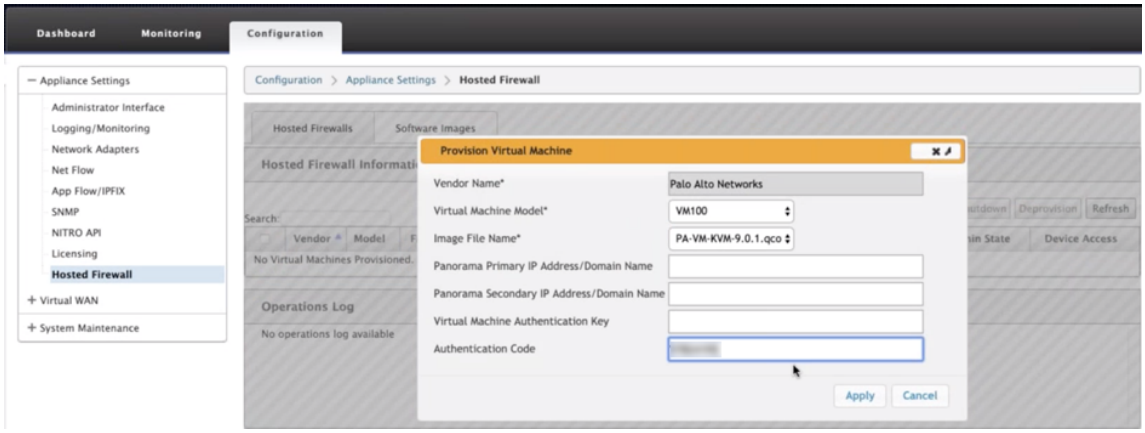
3. プロビジョニングの場合は、[ホストされたファイアウォール] タブを選択し、[プロビジョニング] ボタンをクリックします。



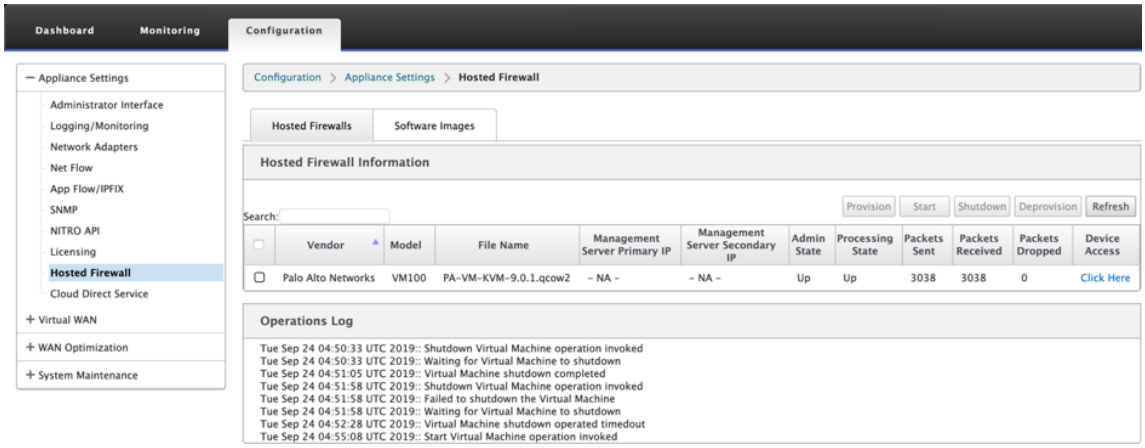
4. Provisioning について次の詳細を入力します。

   - 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 (オプション) を指定します。
   - 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 (オプション) を指定します。
   - 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。



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、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パス処理状態。
- 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、パロアルトネットワーク仮想マシン GUI にアクセスするか、管理 IP を 4100 ポート (管理 IP: 4100) とともに使用します。

> 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。

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

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 SE プラットフォーム上で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ブリッジモードで統合され、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。

SD-WAN Orchestrator サービスを介してファイアウォール仮想マシンをプロビジョニングする方法については、ホストされたファイアウォールを参照してください。

> 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 以降がサポートされています。

長所

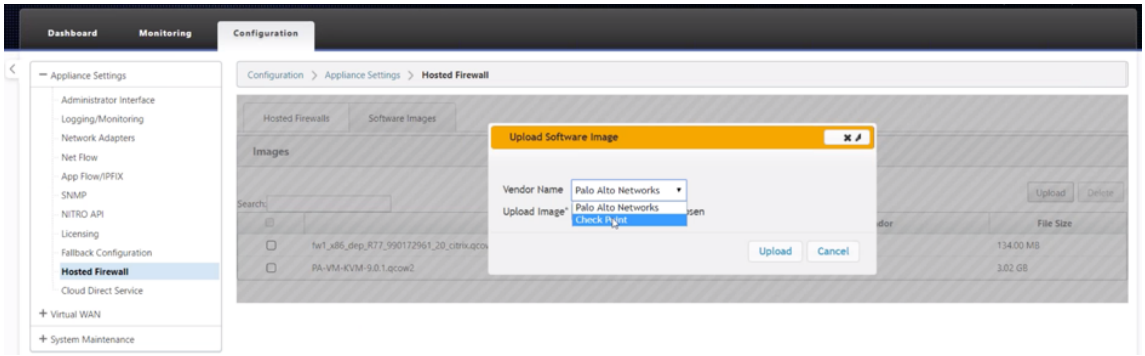
次に、SD-WAN 1100 プラットフォームでの Check Point 統合の主な目標または利点を示します。

- 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

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。

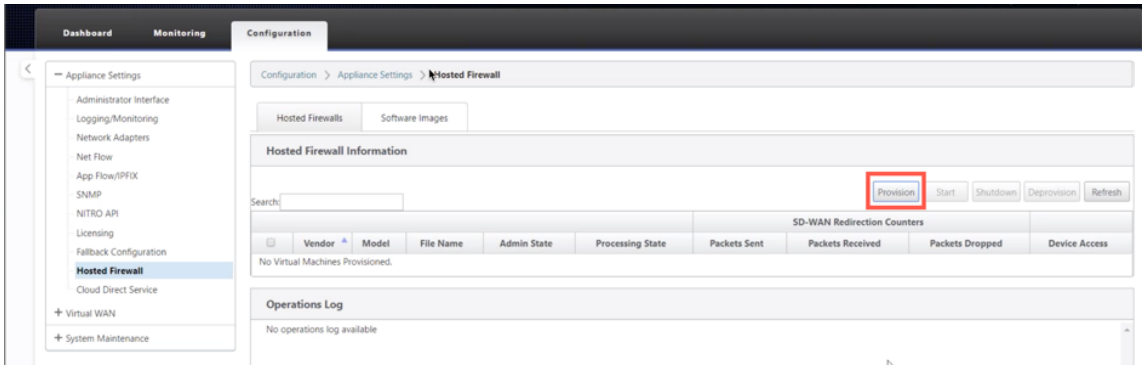
1. Citrix SD-WAN GUI から、［構成］**>>**［アプライアンスの設定］［ホストされたファイアウォール］を選択します。
2. ソフトウェアイメージをアップロードします。
   - ［ソフトウェアイメージ］タブを選択します。**Check Point** としてベンダー名を選択します。
   - ソフトウェアイメージファイルを選択します。
   - ［アップロード］をクリックします。



> 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。

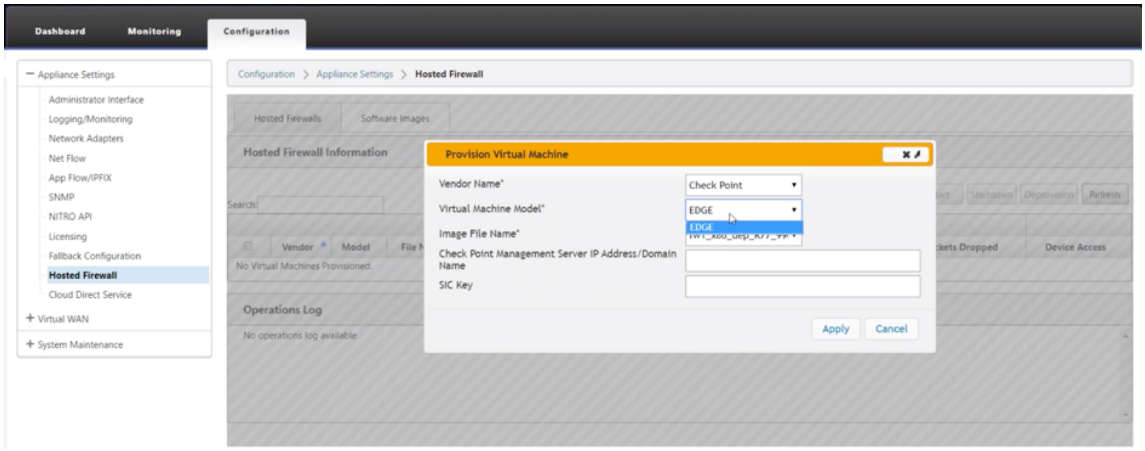
アップロードプロセスを追跡するステータスバーが表示されます。画像が正常にアップロードされると、ファイルの詳細が反映されます。Provisioning に使用されるイメージは削除できません。画像ファイルに 100% アップロードされたと表示されるまで、アクションを実行したり、他のページに戻ったりしないでください。

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。

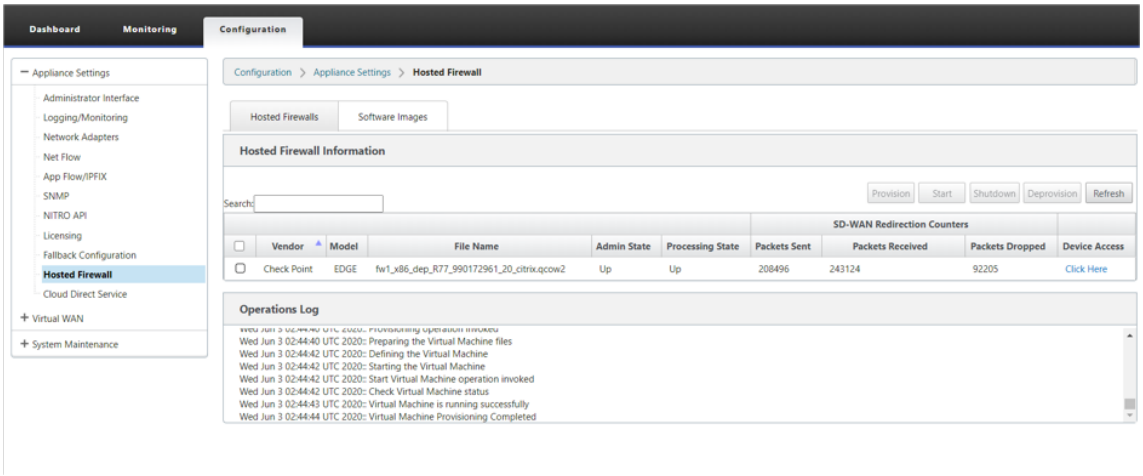


4. Provisioning について次の詳細を入力します。

   - 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。［適用］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。

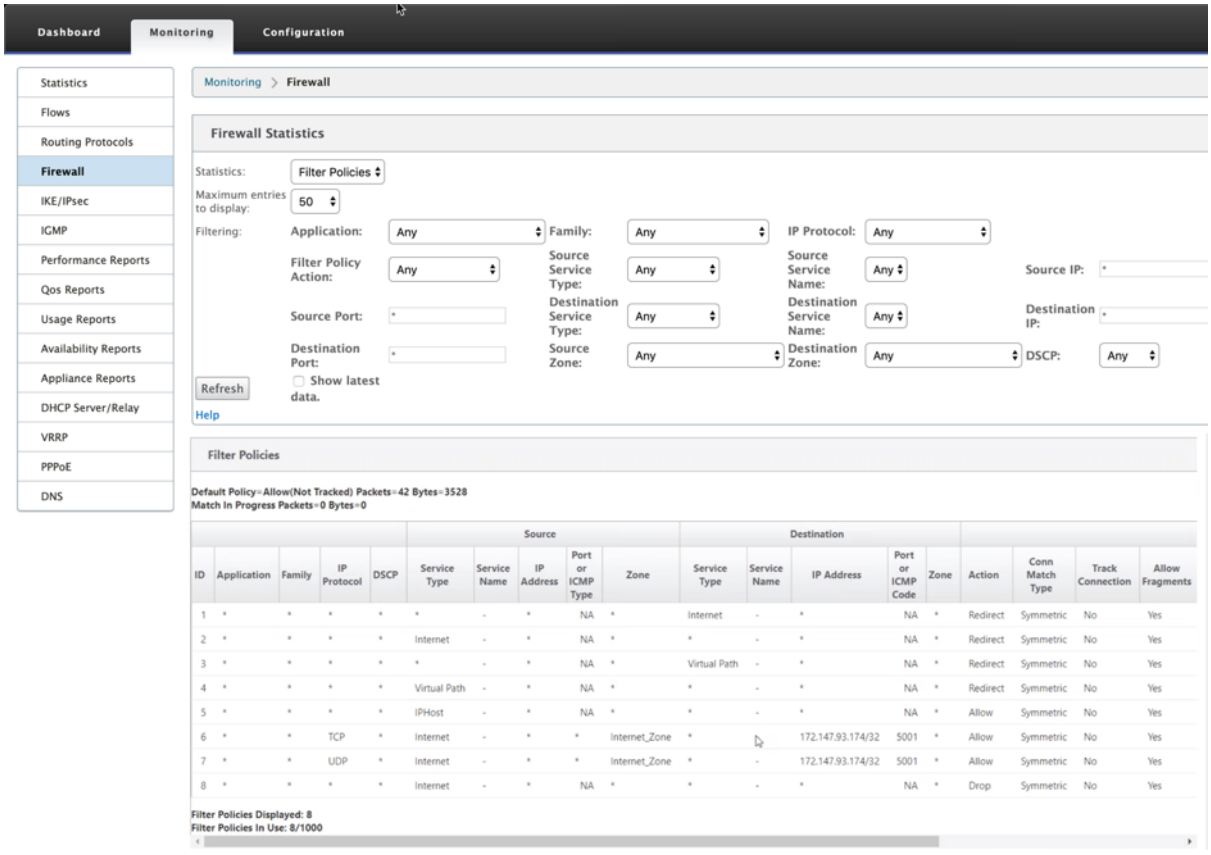


- 管理状態：仮想マシンが起動中か停止中かを示します。
- 処理状態: 仮想マシンのデータパス処理状態。
- パケット送信:SD-WAN からセキュリティ仮想マシンに送信されたパケット。
- 受信パケット:SD-WAN がセキュリティ仮想マシンから受信したパケット。
- パケットドロップ：SD-WAN によってドロップされたパケット（セキュリティ仮想マシンがダウンしている場合など）。
- デバイスアクセス: セキュリティ仮想マシンへの GUI アクセスを取得するには、リンクをクリックします。

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。

すべてのネットワーク設定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**] > [**フィルタポリシー] で接続を監視できます。



リンク集約グループ

August 30, 2022

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 1100 SE
- Citrix SD-WAN 2100 SE
- Citrix SD-WAN 4100 SE
- Citrix SD-WAN 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。

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。

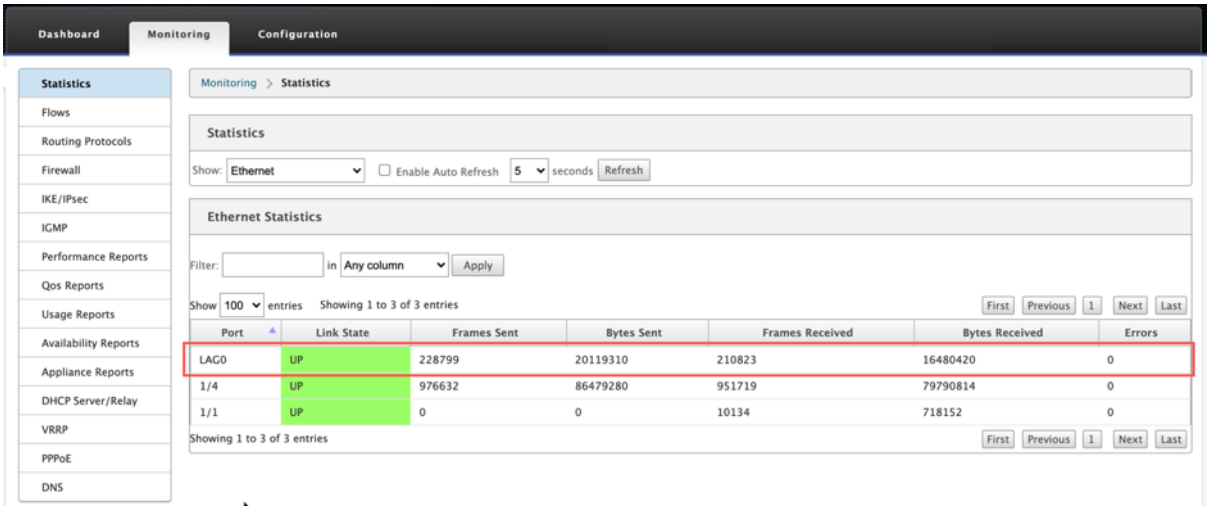
11.3 リリース以降、LACP 実装の SD-WAN では、ポートは常にアクティブモードになります。つまり、SD-WAN は常にネゴシエーションを開始できます。

> 注
>
> - Citrix SD-WAN 210 SE 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。
> - 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 LAG が使用されている場合、Link State Propagation（LSP; リンクステートプロパゲーション） 機能はサポートされません。

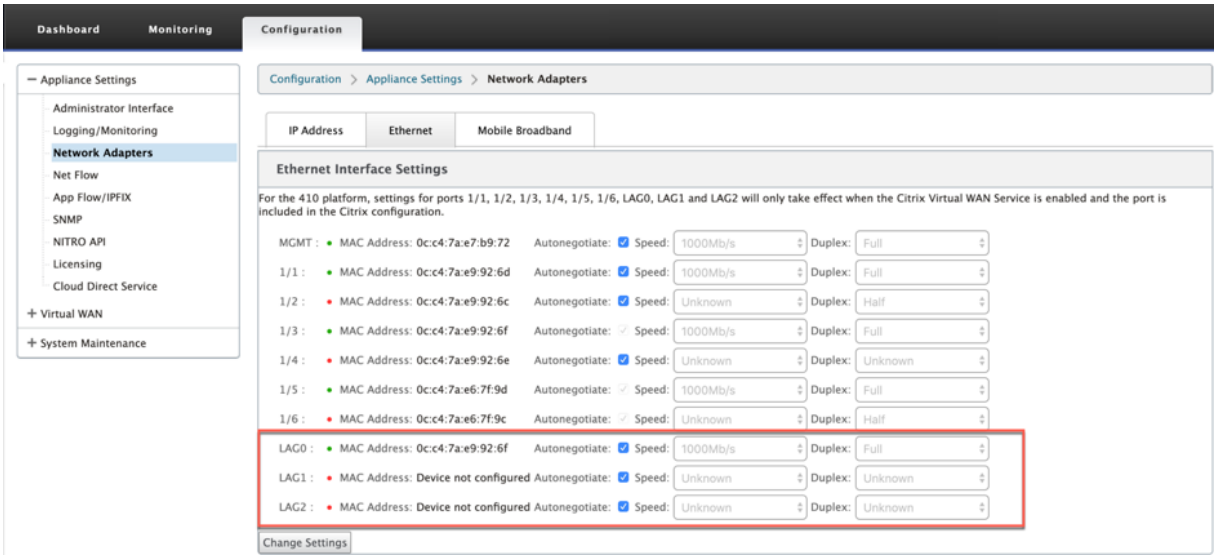
Citrix SD-WAN 11.5 以降では、SD-WAN Orchestrator サービスを介してリンクアグリゲーショングループを構成できます。詳細については、「リンクアグリゲーショングループ」を参照してください。

監視とトラブルシューティング

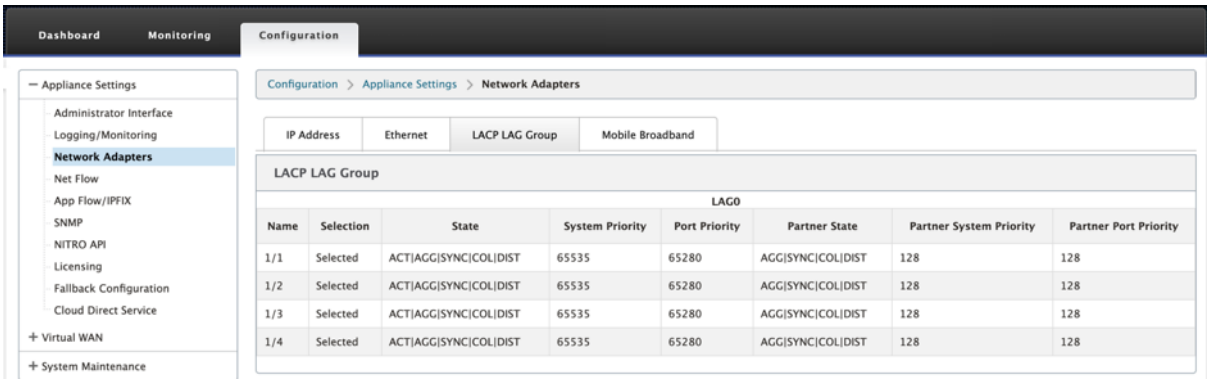
統計またはリンクの状態を表示するには、[監視] **>** [統計] に移動します。[**Show**] ドロップダウンリストから [**Ethernet**] を選択します。



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。

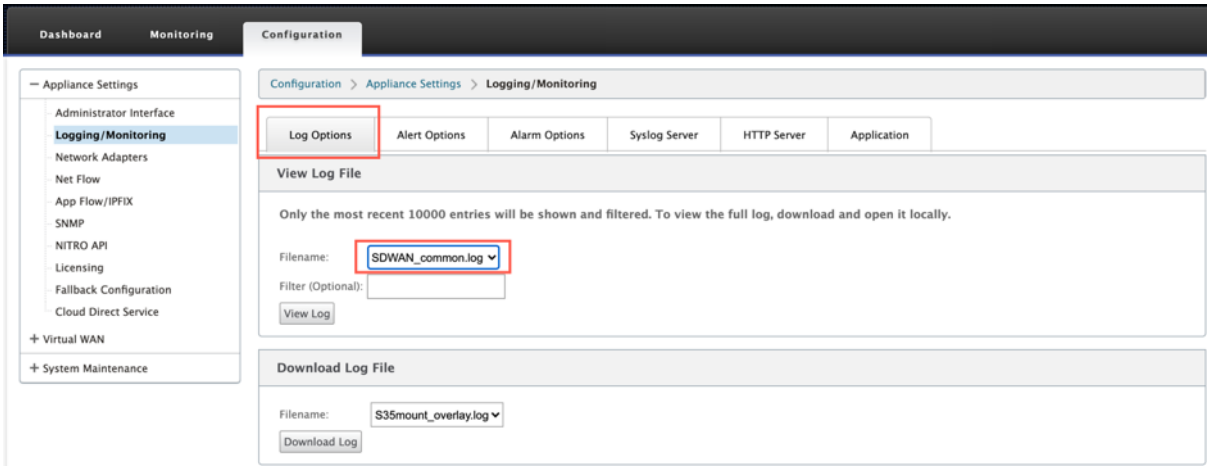


[**LACP LAG** グループ] タブを選択して、LACP LAG グループに関連するさまざまな詳細を表示します。



> 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。



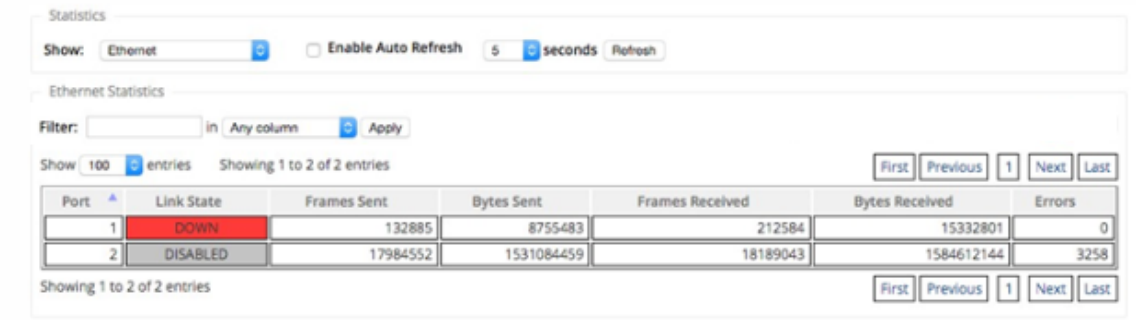
リンク状態の伝播

August 30, 2022

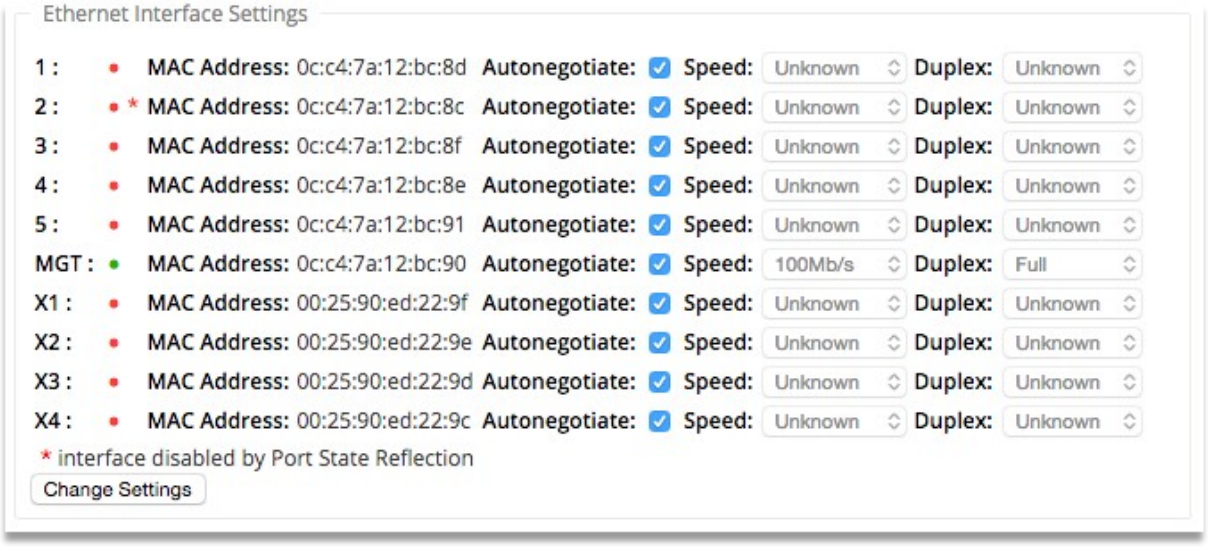
リンクステート伝播（LSP）機能を使用すると、ネットワーク管理者はバイパスペアのリンク状態を同期させることができます。デバイスを表示して、リンクが非アクティブであるときに表示します。バイパスペアの 1 つのポートが非アクティブになると、結合されたリンクは管理上非アクティブになります。ネットワークアーキテクチャに並列フェールオーバーネットワークが含まれている場合は、トラフィックがそのネットワークに移行します。中断されたリンクが復元されると、対応するリンクが自動的にアクティブになります。

リンク統計情報のモニタリング

1. [モニタ**] > [**統計（**Statistics** ）] ページで、[表示（**Show** ）] ドロップダウンメニューから [イーサネット（Ethernet）] を選択し、リンクステート伝播が有効になっている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。



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、[イーサネットインターフェイス設定（**Ethernet Interface Settings**）] リストで赤いアスタリスク（*）で示されます。



メータリングおよびスタンバイ **WAN** リンク

November 17, 2022

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/コントロール）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。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（デフォルトは 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。

- オンデマンド -オンデマンド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に送信されます。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。

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、非アクティブの間は良好であると見なされ、[モニタリング] 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。

SD-WAN 11.5 以降では、Citrix SD-WAN Orchestrator サービスを使用して、従量制課金およびスタンバイ WAN リンクを構成できます。詳細については、「メータリングとスタンバイ WAN リンク」を参照してください。

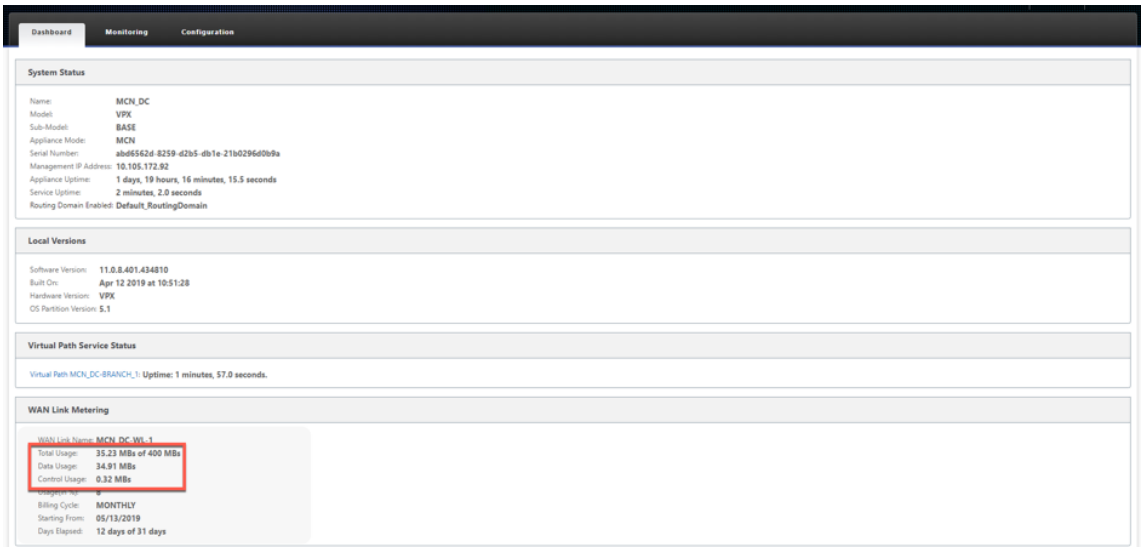
構成の前提条件:

- 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。

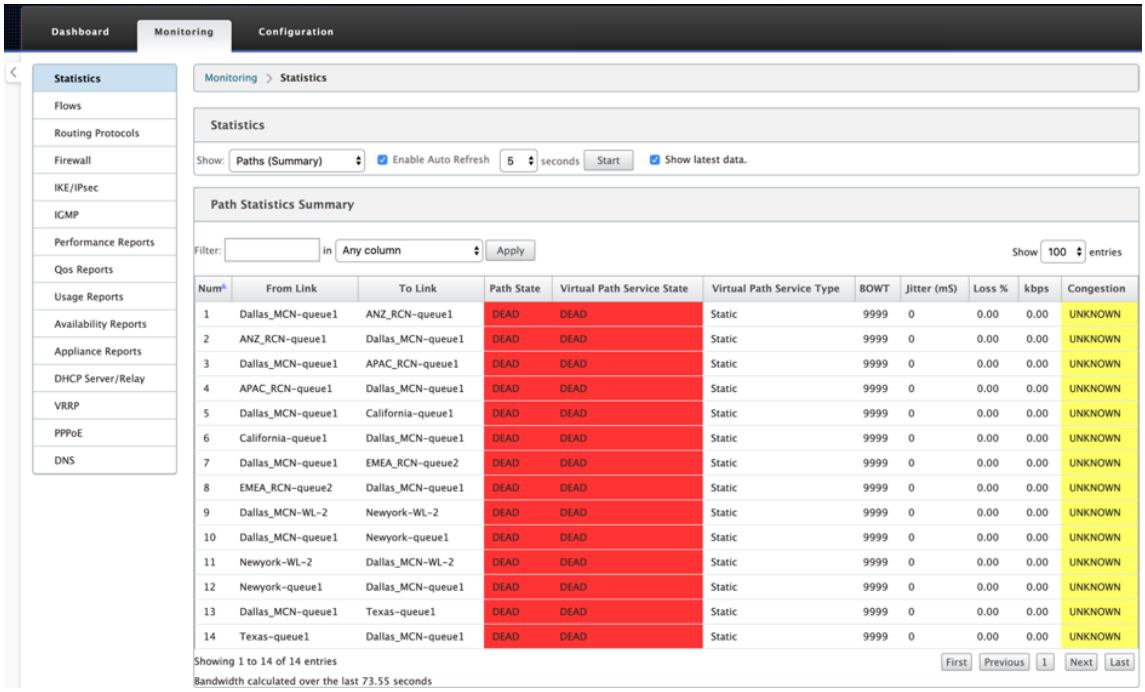
- サイトごとに少なくとも 1 つの非スタンバイリンクを設定する必要があります。サイトごとに最大 3 つのスタンバイリンクがサポートされます。
- インターネット/イントラネットサービスは、オンデマンドスタンバイリンクで構成されていない可能性があります。オンデマンドスタンバイリンクは、仮想パスサービスのみをサポートします。
- インターネットサービスは、last-resort スタンバイリンクで設定されている場合がありますが、サポートされているのは負荷分散モードだけです。
- イントラネットサービスは、ラストリゾートスタンバイリンクで構成されている可能性がありますが、サポートされているのはセカ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。

従量制課金およびスタンバイ **WAN** リンクの監視

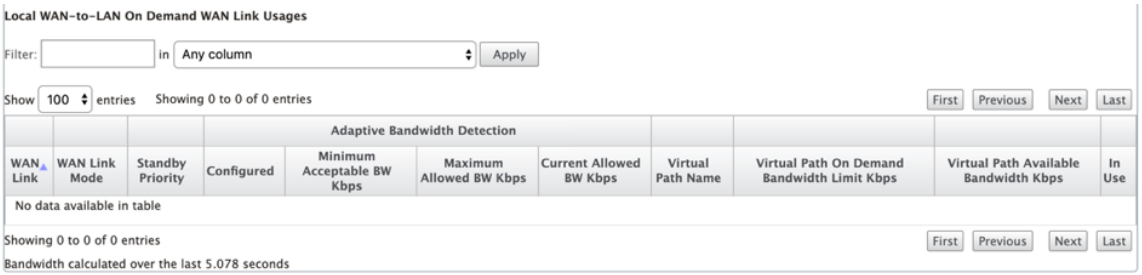
- [ダッシュボード（Dashboard）] ページには、次の **WAN** リンクメータリング情報が使用値とともに表示されます。
  - **WAN** リンク名：WAN リンク名を表示します。
  - 合計使用量: トラフィック使用量の合計を表示します (データ使用量 + 制御使用量)。
  - データ使用量: ユーザトラフィック別の使用状況を表示します。
  - 制御使用量：制御トラフィックごとの使用状況を表示します。
  - 使用量 **(**単位**:%)**: 使用されたデータ上限値をパーセンテージ (合計使用量/データ上限) x 100 で表示します。
  - 請求サイクル: 請求頻度 (毎週/毎月)
  - 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)



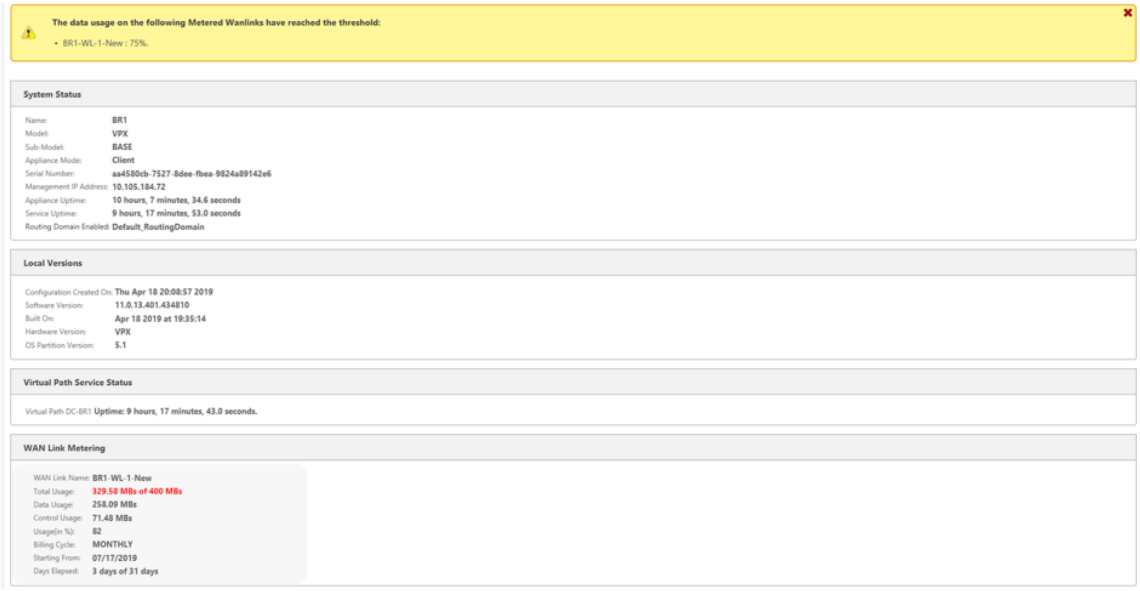
- パス統計情報（[**Monitoring] > [Statistics] > [Paths**]）が表示されている場合、従量制課金リンクとスタンバイリンクは、スクリーンショットのようにマークされます。



- アプライアンスに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がある仮想パスがある場合、WAN リンク使用状況の統計情報を表示すると、オンデマンド帯域幅を示す追加のテーブルがページの下部に表示されます（[モニタリング（Monitoring）]**> [**統計（**Monitoring**）**] > [**統計（**Statistics**）**] > [WAN** リンク使用状況（WAN



- 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、使用量が設定されたデータ上限の 75% を超える場合、ダッシュボードの下部に向けた数値メータリング情報が強調表示されます。



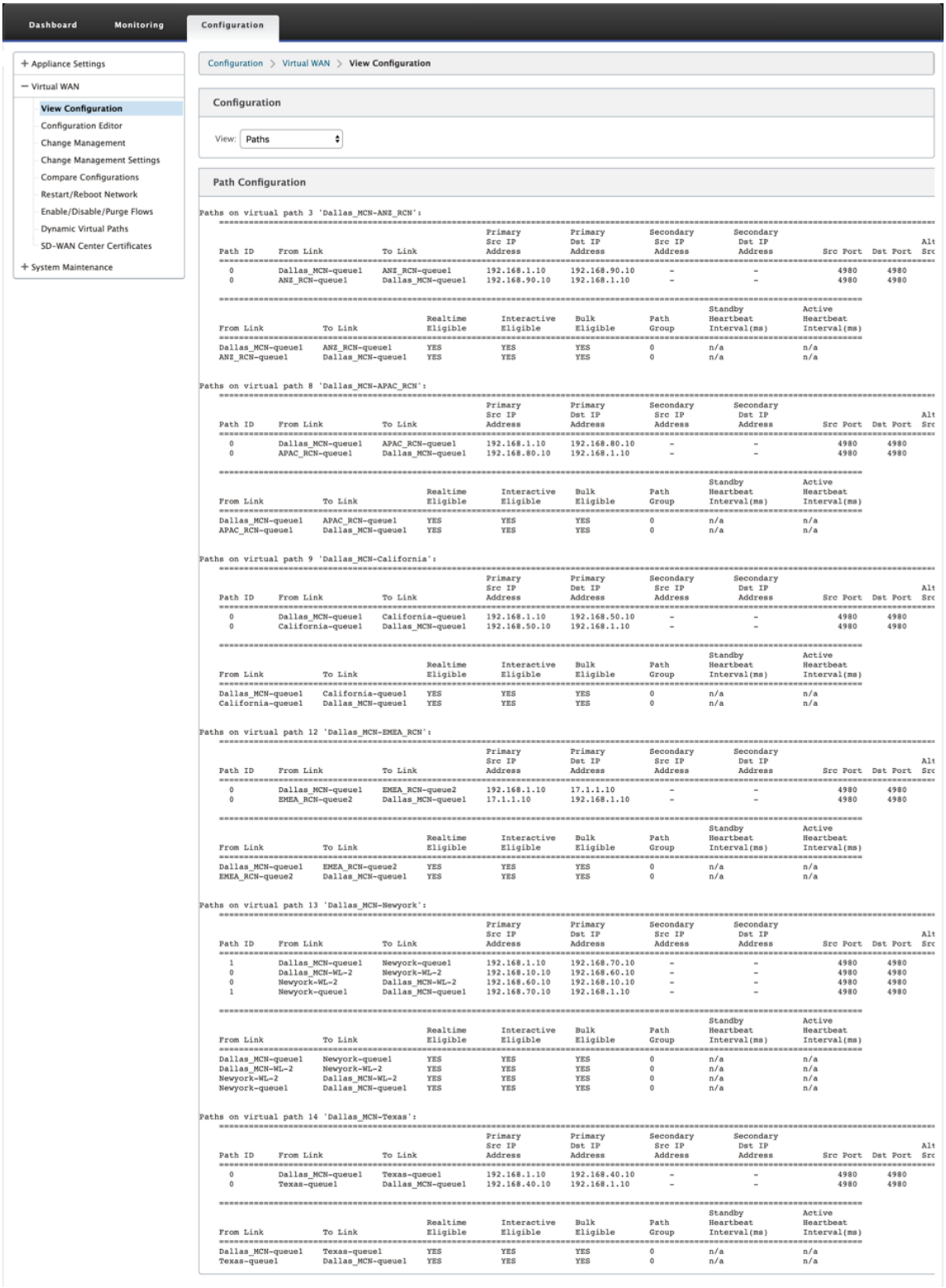
WAN リンク使用イベントは、設定済みデータ上限の 50%、75%、および 90% を超えると、アプライアンスでも生成されます。

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

1. 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。



Office 365 の最適化

November 17, 2022

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場所にある 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だけの場合と比べて、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ー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。

```
- Teams Realtime
- Exchange Online
- 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ークアウトしたり、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。

```
- Teams TCP Fallback
- Exchange Mail
- SharePoint Allow
- 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 ブレー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。

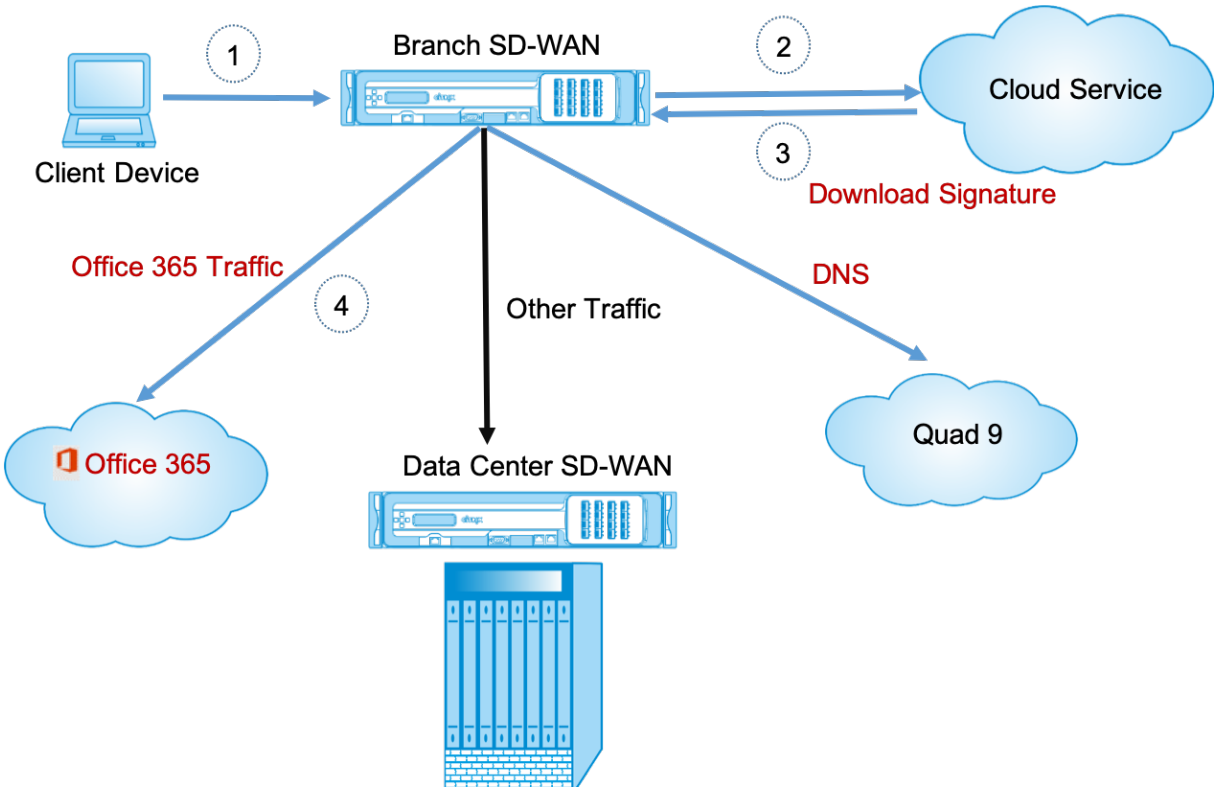
Office 365 の最適化の仕組み

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。

Citrix SD-WAN 11.5 以降では、Citrix SD-WAN Orchestrator サービスを使用してオフィス 365 ブレークアウトを構成できます。詳細については、「Office 365 の最適化」を参照してください。

Office 365 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ー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

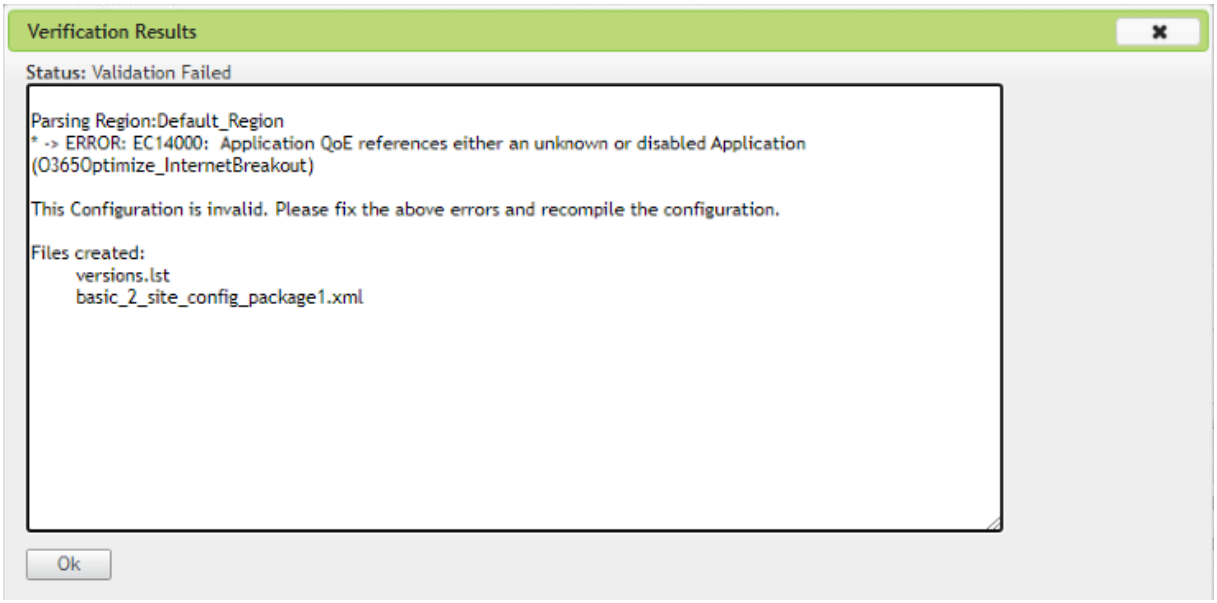
［Office **365** の最適化］および［許可］カテゴリでインターネットブレークアウトポリシーを有効にした場合、Citrix SD-WAN 11.4.0 へのアップグレード時に、対応するサブカテゴリのインターネットブレークアウトポリシーが自動的に有効になります。

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ー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 透過フォワーダ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。

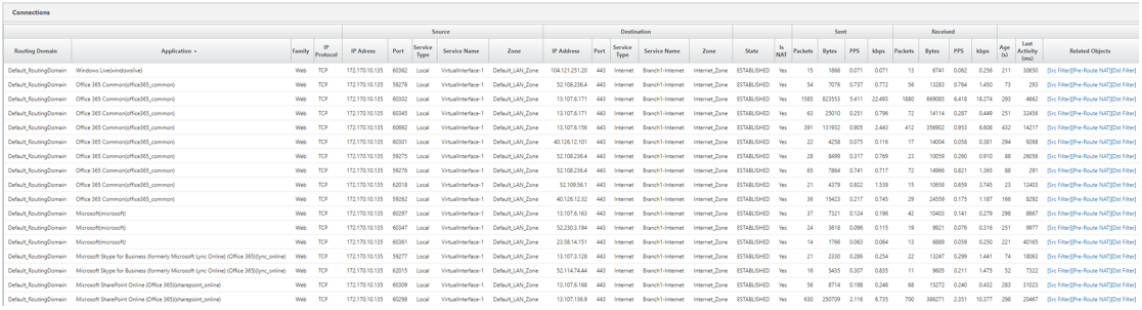
古い DNS プロキシまたは透過フォワーダルールを削除せずに Citrix SD-WAN 11.4.0 のアップグレードを続行すると、エラーは表示されず、アップグレードも成功します。ただし、Citrix SD-WAN 11.4.0 では、DNS プロキシルールと透過転送ルールは有効になりません。

> 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。

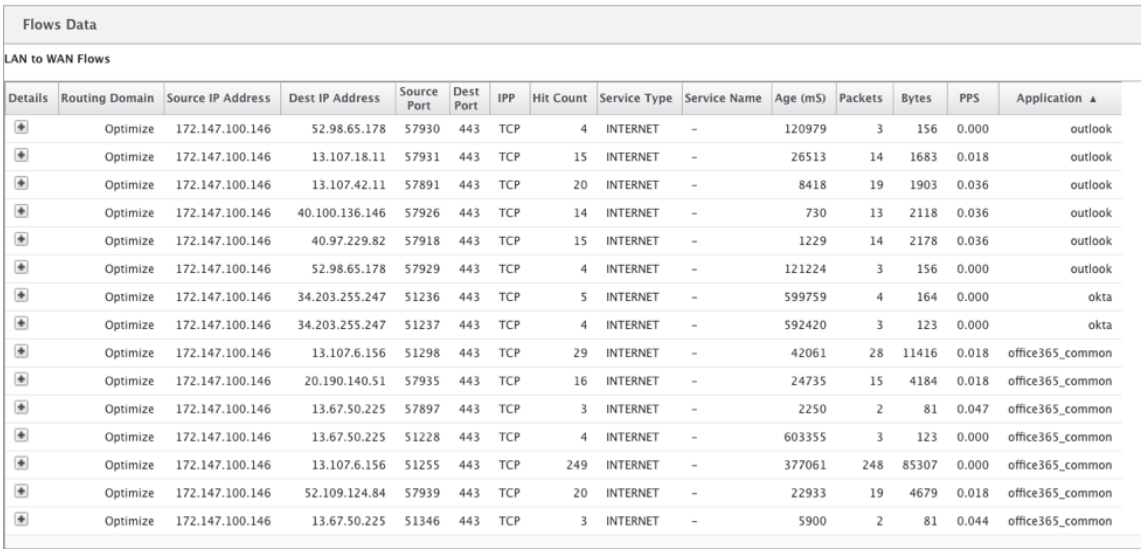
監視

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。

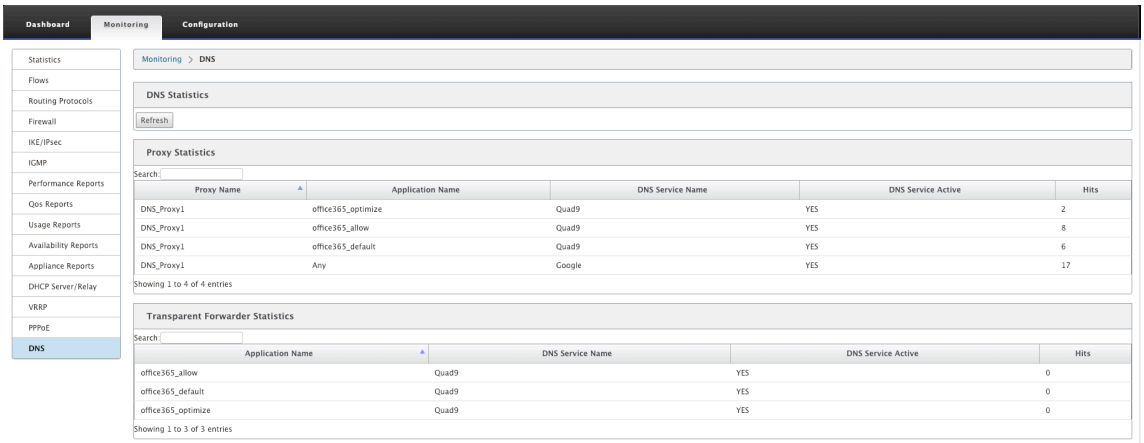
- ファイアウォールの統計情報



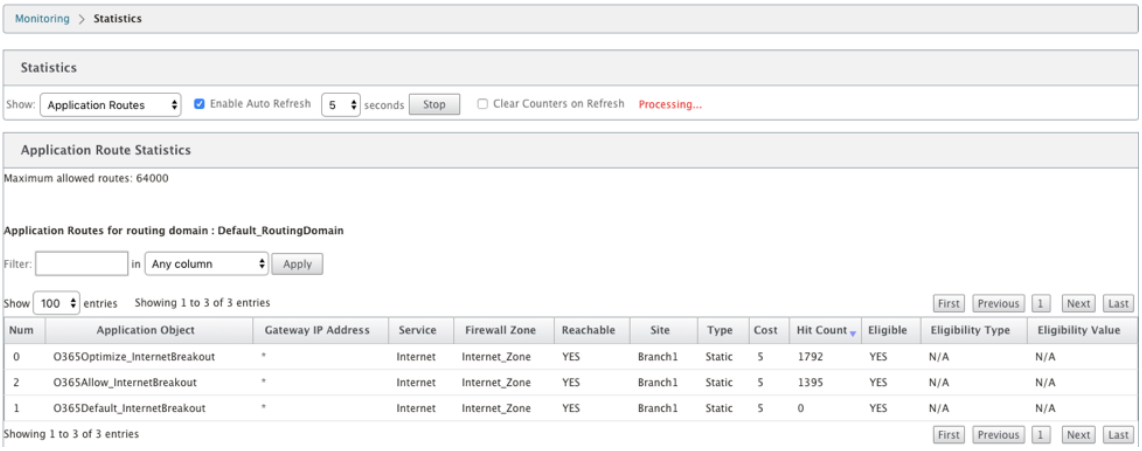
- フロー



- DNS 統計情報



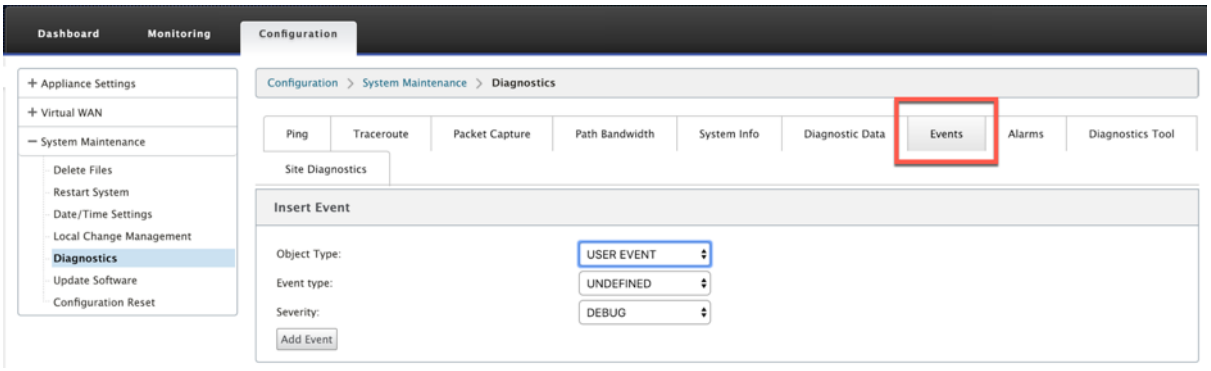
- アプリケーションルート統計情報



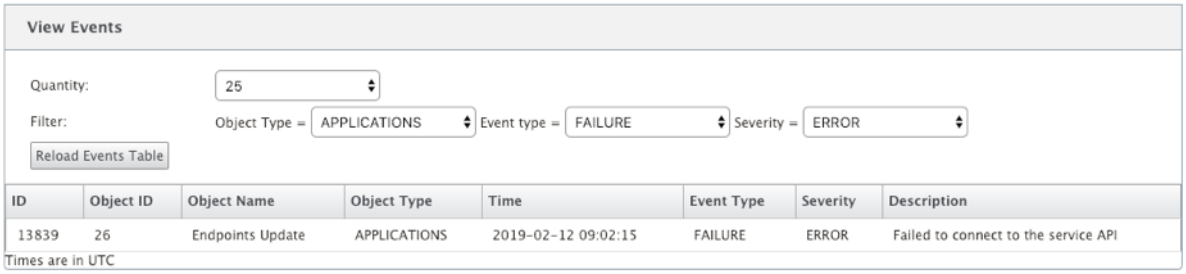
トラブルシューティング

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。

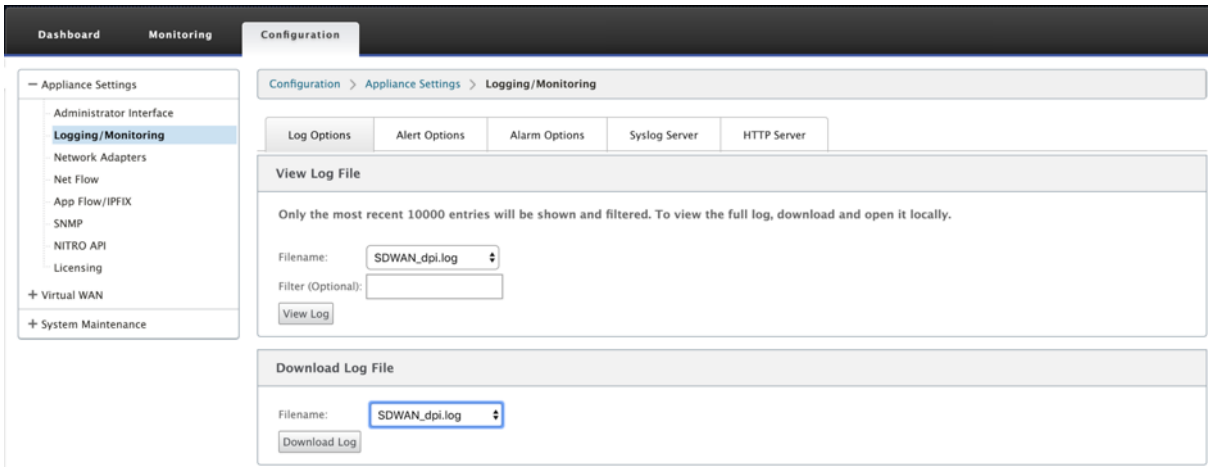


Citrix サービス（sdwan-app-routing.citrixnetworkapi.net）への接続に問題がある場合、エラーメッセージは［イベントの表示］テーブルに表示されます。



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

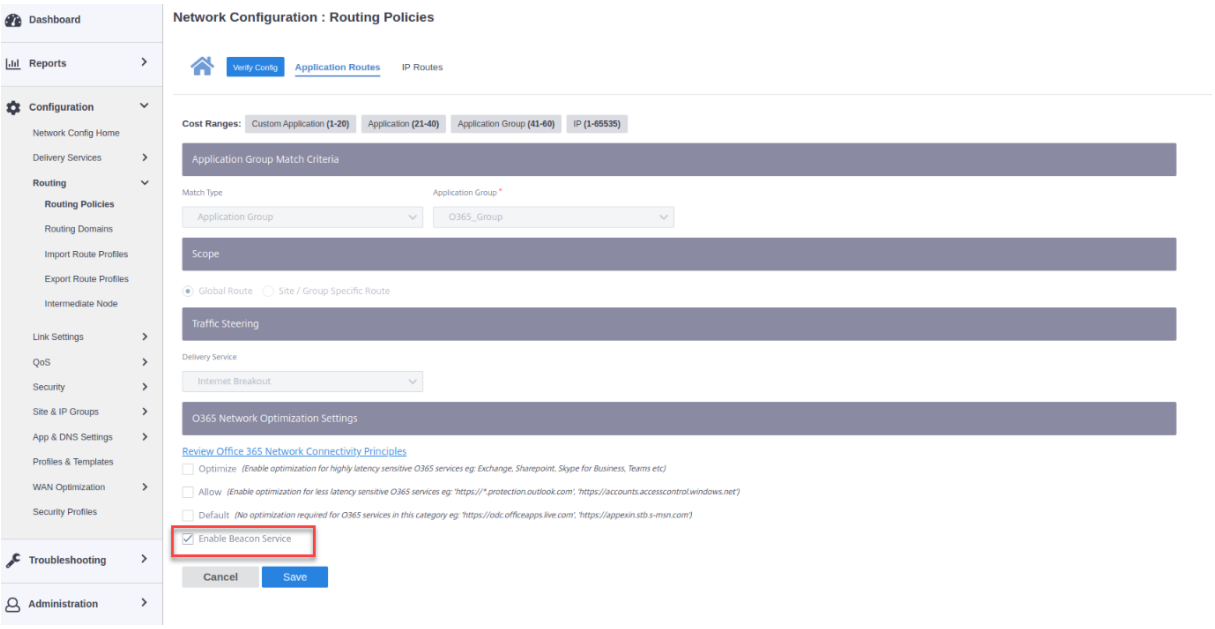
Microsoft は、WAN リンクを介した Office 365 の到達可能性を測定する Office 365 ビーコンサービスを提供しています。ビーコンサービスは、基本的に URL です-sdwan.measure.office.com/apc/trans.png は、定期的にプローブされます。プローブは、インターネット対応のすべての WAN リンクについて、各アプライアンス上で実行されます。プローブごとに HTTP 要求がビーコンサービスに送信され、HTTP 応答が予期されます。HTTP 応答は、Office 365 サービスの可用性と到達可能性を確認します。

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 ブレー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。

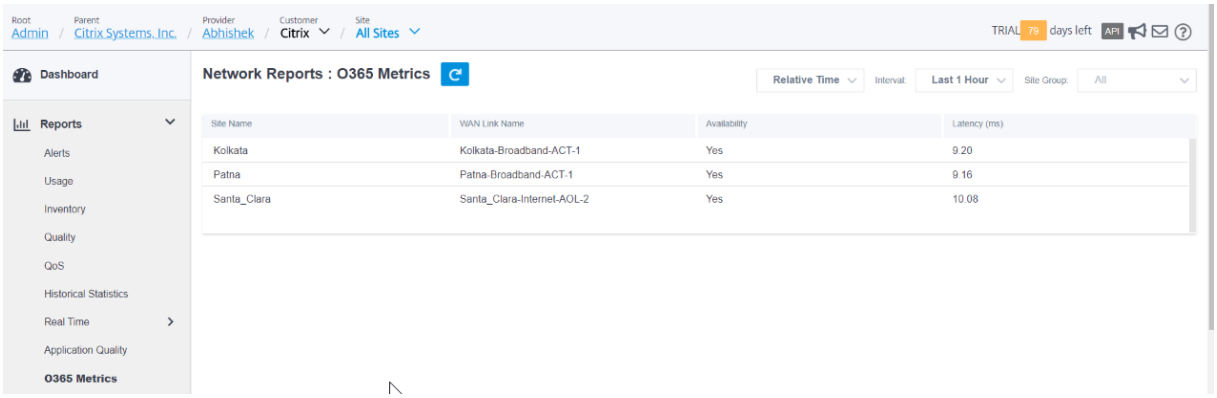
> 注
>
> 従量制課金リンクでは、Office 365 ビーコンプローブが有効になっていません。

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。

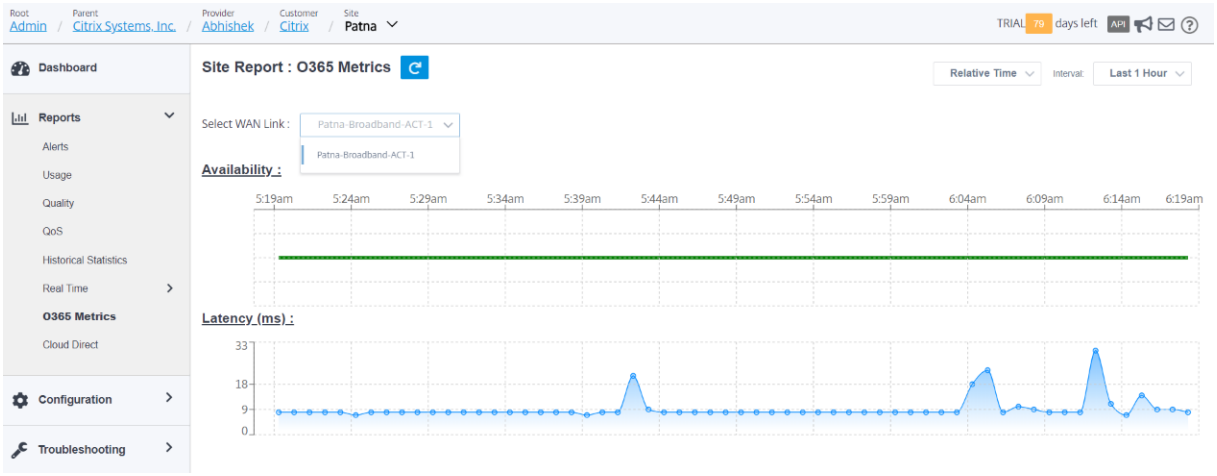
Office 365 ビーコンサービスを無効にするには、SD-WAN Orchestrator で、ネットワークレベルで [構成] > [ルーティング] **> [**** ルーティングポリシー **] > [**O365** ネットワーク最適化の設定] に移動し、[ビーコンサービスを有効にする] をオフにします。



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 宛て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 サービスのブレー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 サービスのブレー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 サービスのブレー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ー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 Cloud および **Cloud** サービスのカテゴリ

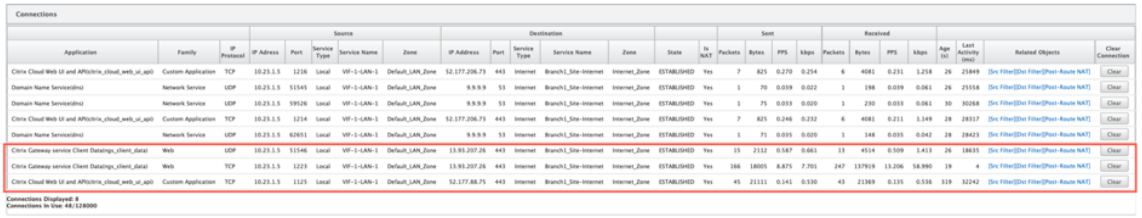
分類および最適化の目的で使用されるトラフィックカテゴリを次に示します。

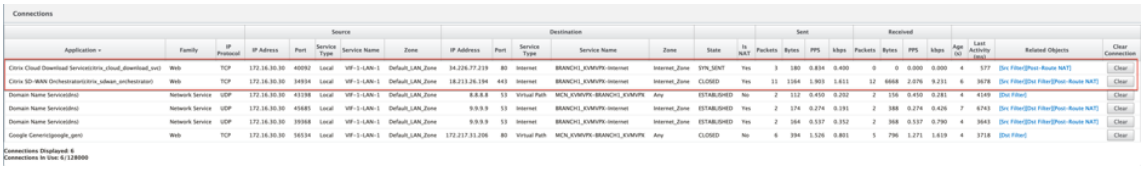
- **Citrix Cloud**：Citrix Cloud Web UI および API 宛てのトラフィックを検出してルーティングできるようにします。
  - Citrix SD-WAN Orchestrator と依存する重要なサービス：
    - **Citrix SD-WAN Orchestrator**：Citrix SD-WAN アプライアンスと Citrix SD-WAN Orchestrator 間の接続を確立し、維持するために必要なハートビートやその他のトラフィックからインターネットに直接ブレイクアウトできます。
    - **Citrix Cloud** ダウンロードサービス：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 データトンネルの直接インターネットブレー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ー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ー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

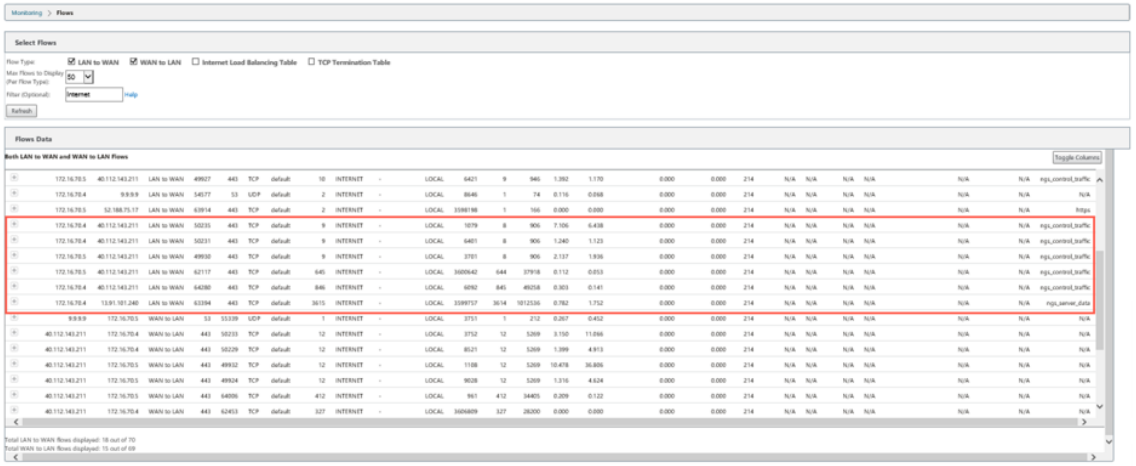
Gateway サービスの統計情報は、次の SD-WAN 統計レポートで監視できます。

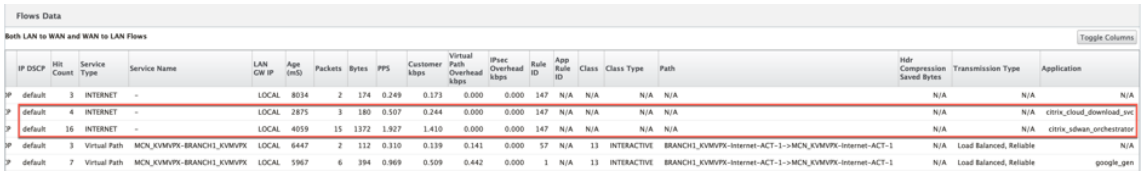
- ファイアウォールの統計情報



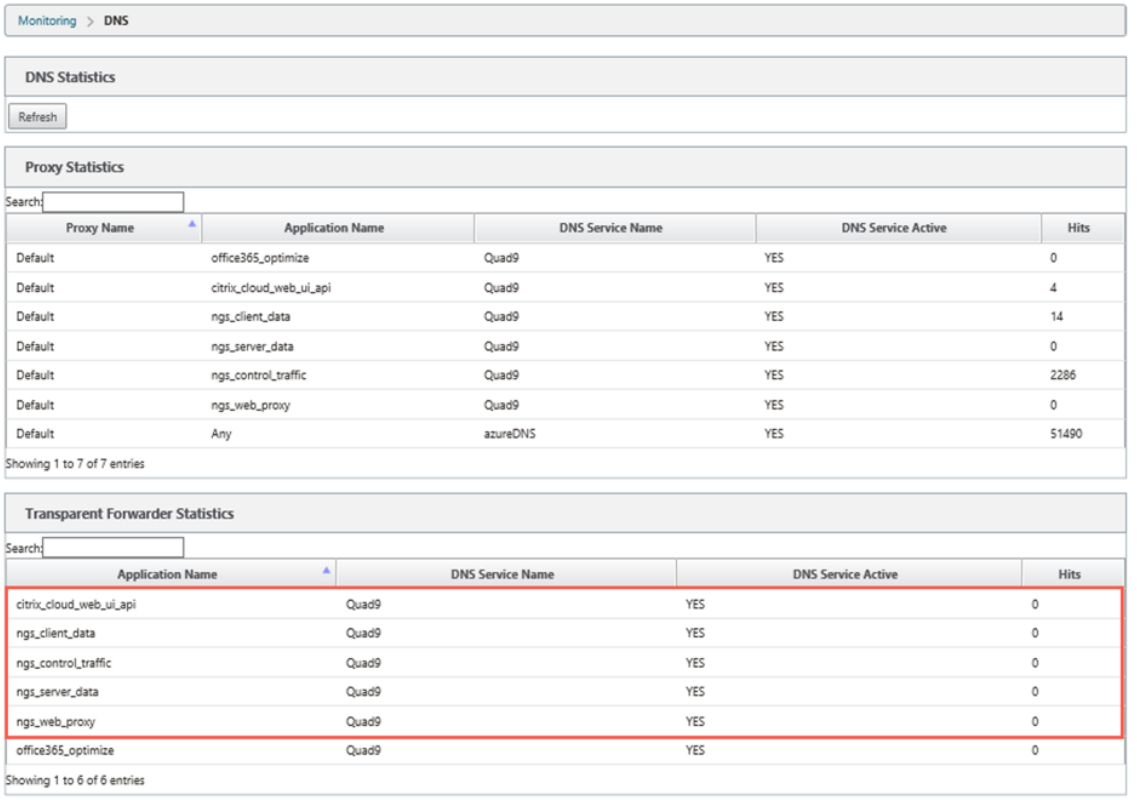


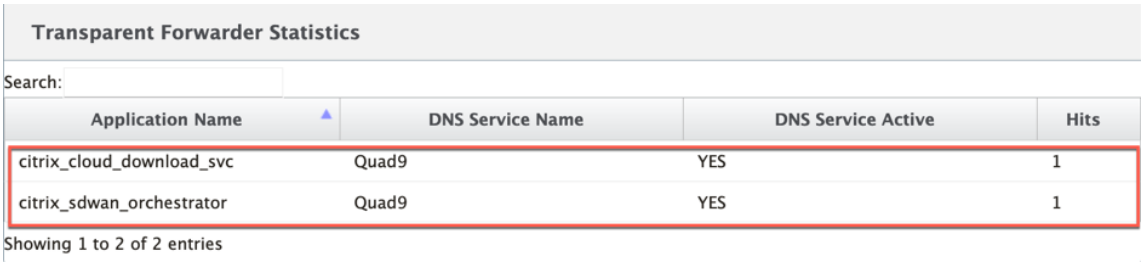
- フロー



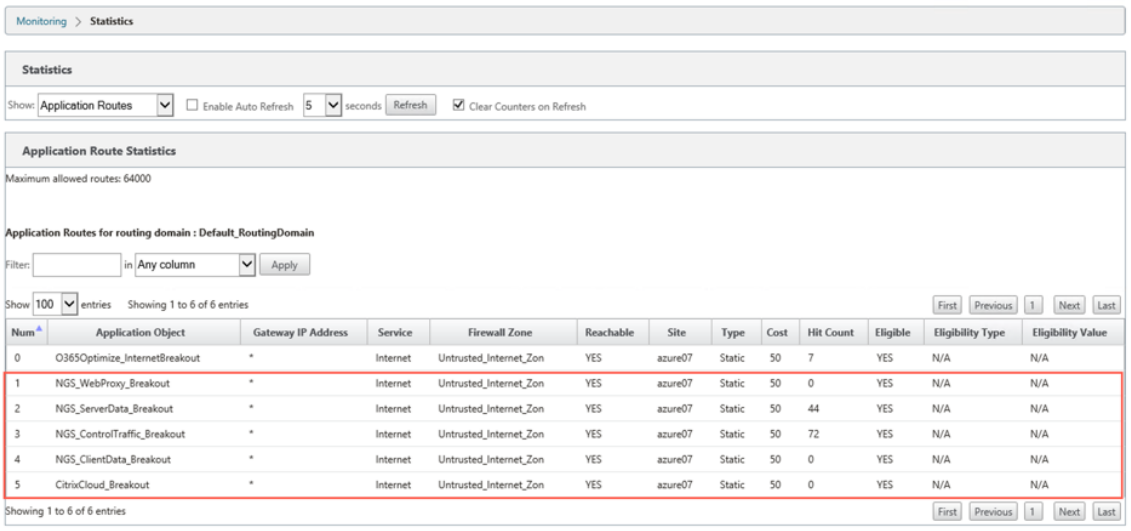


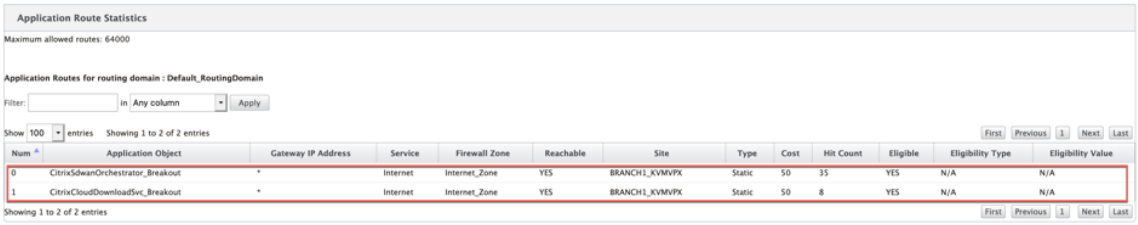
- DNS 統計情報





- アプリケーションルート統計情報

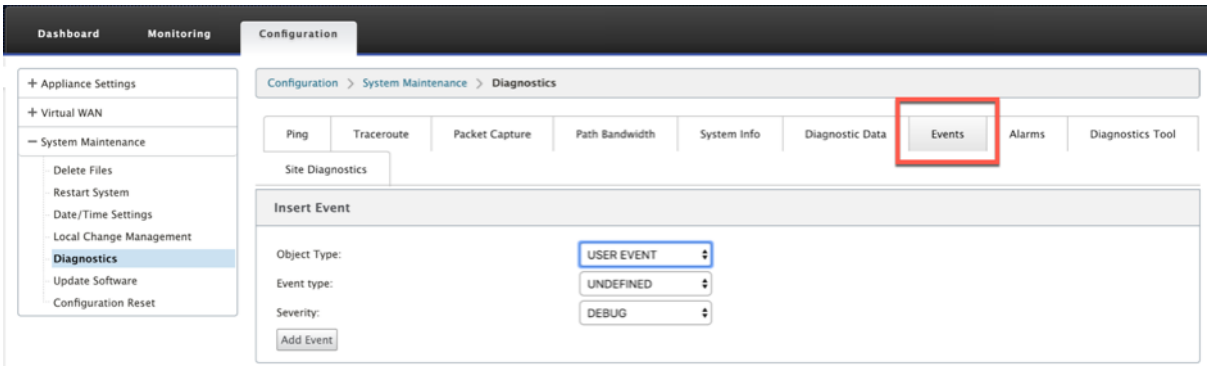




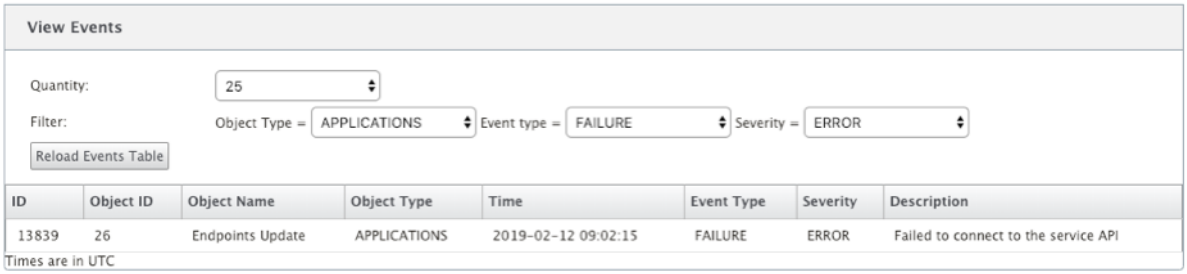
トラブルシューティング

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。

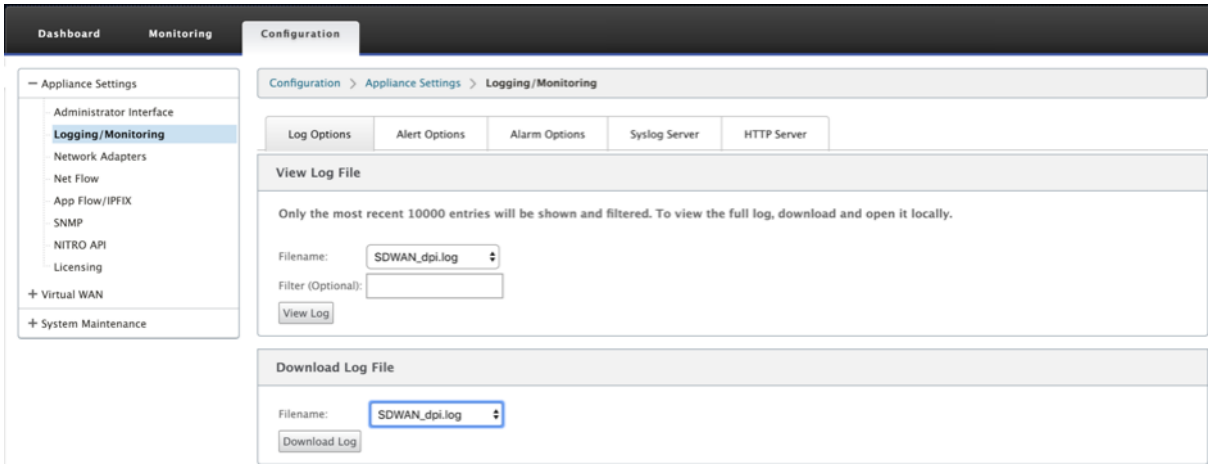


Citrix サービス（sdwan-app-routing.citrixnetworkapi.net）への接続に問題がある場合、エラーメッセージは［イベントの表示］テーブルに表示されます。



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 Lo**g] をクリックします。



PPPoE セッション

August 30, 2022

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 サーバーとの認証を行い、動的 IP アドレスを取得するか、静的 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、以下が必要です。

- 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:
  >
  > 複数の VNI は、同じ 802.1Q > VLAN タグで作成できます。

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。
- 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。

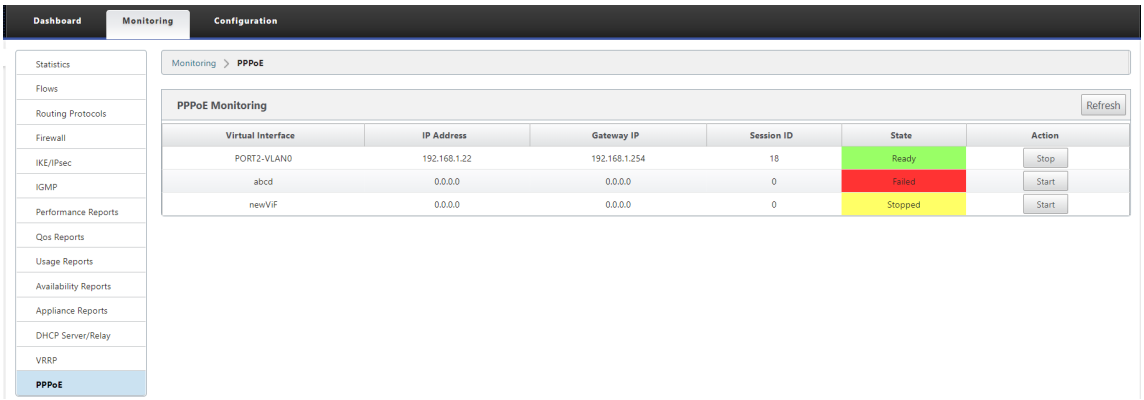
Citrix SD-WAN Orchestrator サービスを介して PPPoE を構成する方法については、「インターフェイス」を参照してください。

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 で [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。これにより、トラブルシューティングの目的で、Citrix SD-WAN Orchestrator サービスからセッションを手動で開始および停止できます。

- VNI が起動して準備ができている場合は、[**IP]** 列と **[Gateway IP**] 列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。



[**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。

PPPoE セッションタイプ	色	説明
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。
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。

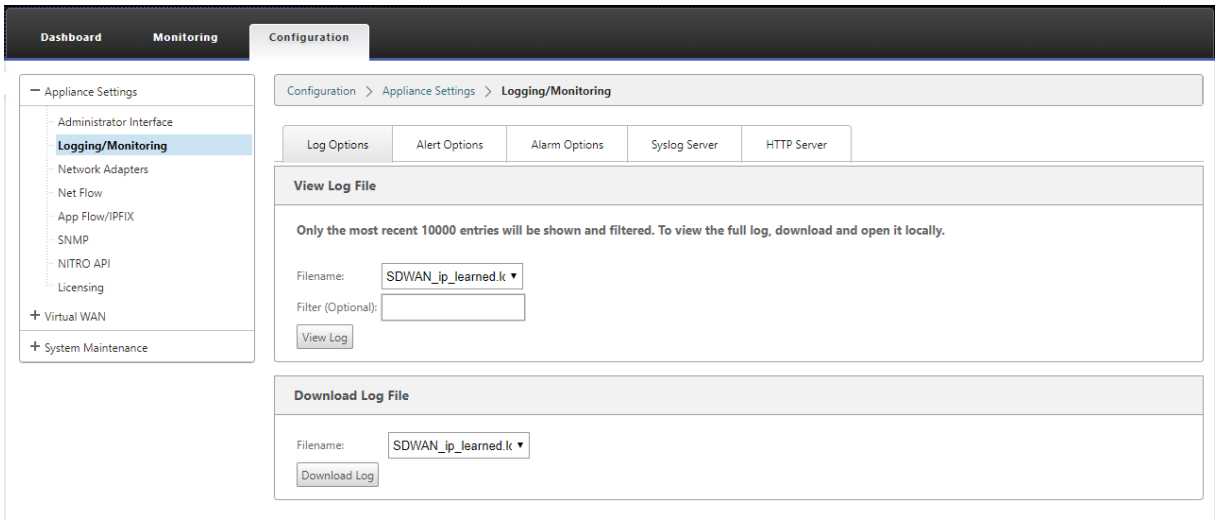
- 障害が正常であれば、すぐに再起動します。
- 失敗がエラーの場合、再起動は 10 秒間戻ります。
- 失敗が致命的である場合、再起動は 30 秒間戻ってから再起動します。

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* ファイルを表示するか、またはダウンロードするために、アプライアンスの設定 > ロギング/監視 > ログオプションにナビゲートして下さい。*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。

SD-WAN 11.5 リリース以降、QoS 機能は Citrix SD-WAN Orchestrator サービスを通じて構成できます。詳細については、「サービス品質」を参照してください。

クラス

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。

Citrix SD-WAN Orchestrator サービスは 13 のクラスをサポートしています。詳細については、「クラス」を参照してください。

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、時間に敏感な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。
- インタラクティブ: 低から中程度のレイテンシーが必要で、帯域幅要件が低から中程度のインタラクティブ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%。

帯域幅配分の結果は次のとおりです。

- リアルタイムトラフィックは、必要に応じて 10Mbs（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。

IP アドレスとポート番号による規則

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。

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。

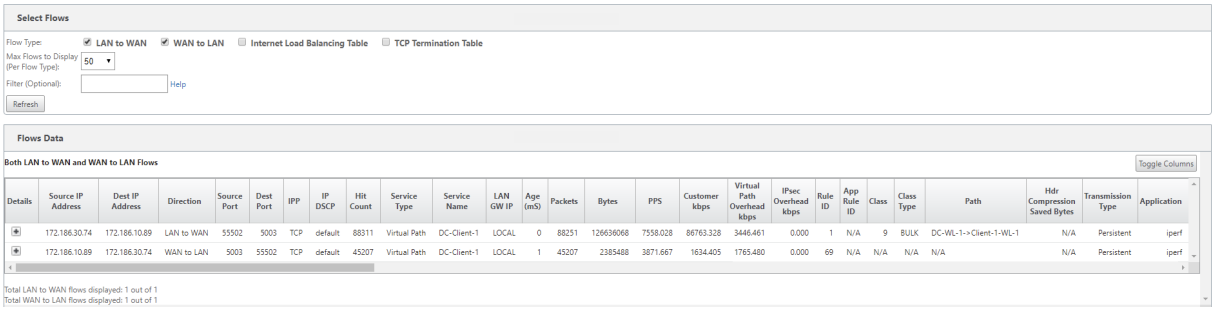
Citrix SD-WAN 11.5 リリース以降、Citrix SD-WAN Orchestrator サービスを使用して IP ルールを作成できます。詳細については、「IP ルール」を参照してください。

規則の確認

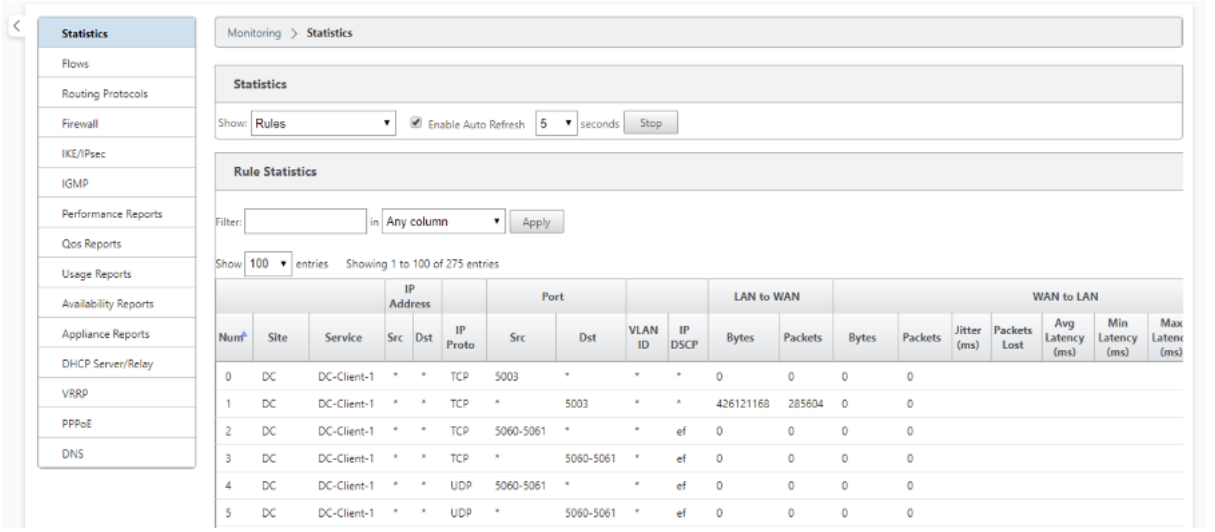
監視 **>** フローに移動します。「フロー」ページの上部にある「フローの選択」セクションにある「フロータイプ ****** 」フィールドを選択します。**[**Flow Type**] フィールドの横には、表示するフロー情報を選択するためのチェックボックスが並んでいます。フロー情報が設定された規則に従っているかどうかを確認します。

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。



[監視] **>** [統計] に移動し、構成されたルールを確認します。



アプリケーション名別のルール

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の一致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、それらに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 ルールの詳細については、IP アドレスとポート番号によるルール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。

- **Load Balance Path**: フローのアプリケーショントラフィックは、複数のパスにまたがって分散されます。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	送信モード	失われたパケットの再送信	パケット集約を有効にする	パケット再シーケンシングの有効化	リシーケンスの保持時間（ミリ秒）	レイトリシーケンスパケットの破棄	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	無効限界 (ミリ秒)	深度の無効化 (バイト)
HDX_Priority_0 (HDX_priority_tag_0)	10	負荷分散パス	True	False	True	250	True	350	30000	True	0	128000
HDX_Priority_1 (HDX_priority_tag_1)	9	負荷分散パス	True	False	True	250	True	350	30000	True	0	128000
HDX_Priority_2 (HDX_priority_tag_2)	8	負荷分散パス	True	False	True	250	True	350	30000	True	0	128000
HDX_Priority_3 (HDX_priority_tag_3)	7	負荷分散パス	True	False	True	250	True	350	30000	True	0	128000
HDX	11 (interactive_high_class)	負荷分散パス	True	False	True	250	True	350	30000	True	0	128000

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。

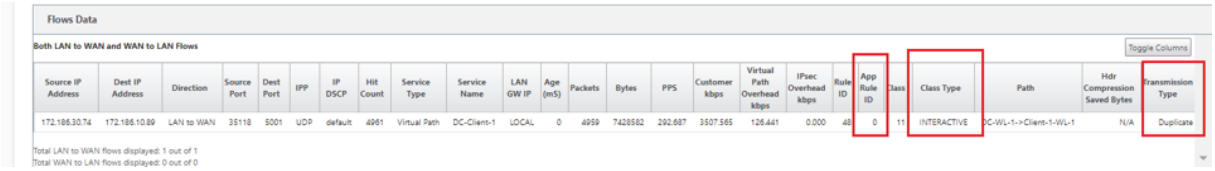
IP ルールは、アプリケーションルールと比較して、属性のより多くの数を持っています。アプリケーションルールはいくつかの IP ルール属性だけを上書きし、残りの IP ルール属性はパケットで処理されたままになります。

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。

Citrix SD-WAN Orchestrator を使用してアプリケーションルールを作成するには、「アプリケーションルール」を参照してください。

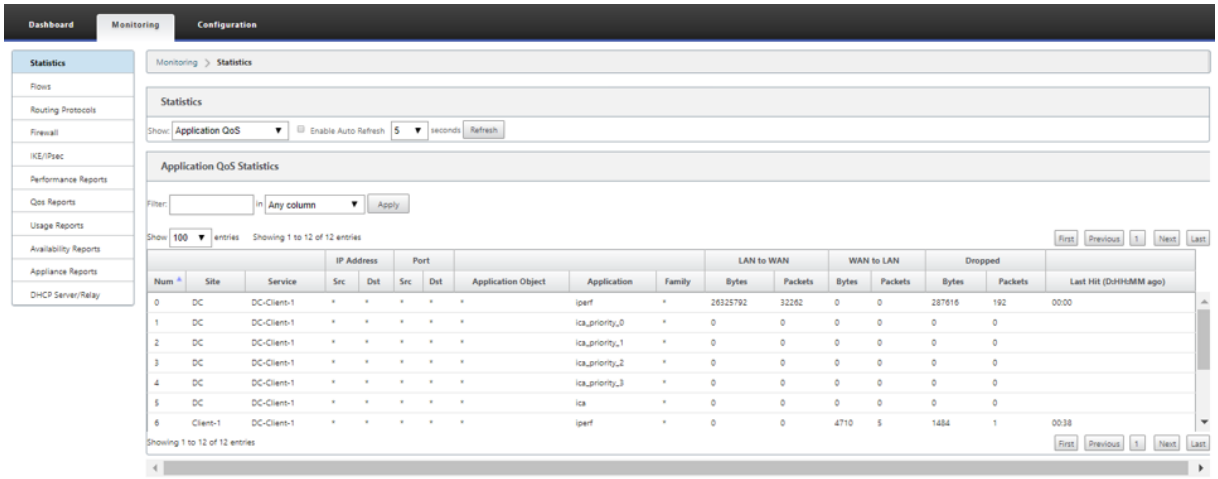
アプリケーションルールがトラフィックフローに適用されているかどうかを確認するには、[**Monitoring**] > [**Flows**] に移動します。

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。



[Monitoring] > [**Statistics**] > [Application QoS] に移動して、各サイトでアップロード、ダウンロード、またはドロップされたパケット数/バイト数などのアプリケーション **QoS** をモニタできます。

Num パラメータは、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。



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。

アプリケーション分類

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。

Citrix SD-WAN Orchestrator サービスで DPI ライブラリ分類を有効にするには、「DPI ライブラリの分類」を参照してください。

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 を介して配信される ICA トラフィックの分類は、SD-WAN Standard Edition ではサポートされていません。
>
> 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 以降が必要です。
> - HDX ユーザーベースのレポートを SDWAN-Center に表示するには、SD-WAN Standard 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_prority_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。

Citrix SD-WAN Orchestrator サービスで ICA ベースの分類を有効にするには、ICA 分類を参照してください。

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。

Citrix SD-WAN Orchestrator サービスでドメイン名ベースのアプリケーションを定義するには、「ドメイン名ベースのアプリケーション分類」を参照してください。

> 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。
> - Citrix SD-WAN 11.5.0 以降のリリース以降、AAAA レコードは Citrix SD-WAN Orchestrator サービスでサポートされています。

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。
- 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 エンジンは 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 エンジンは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 エンジンは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 エンジンは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

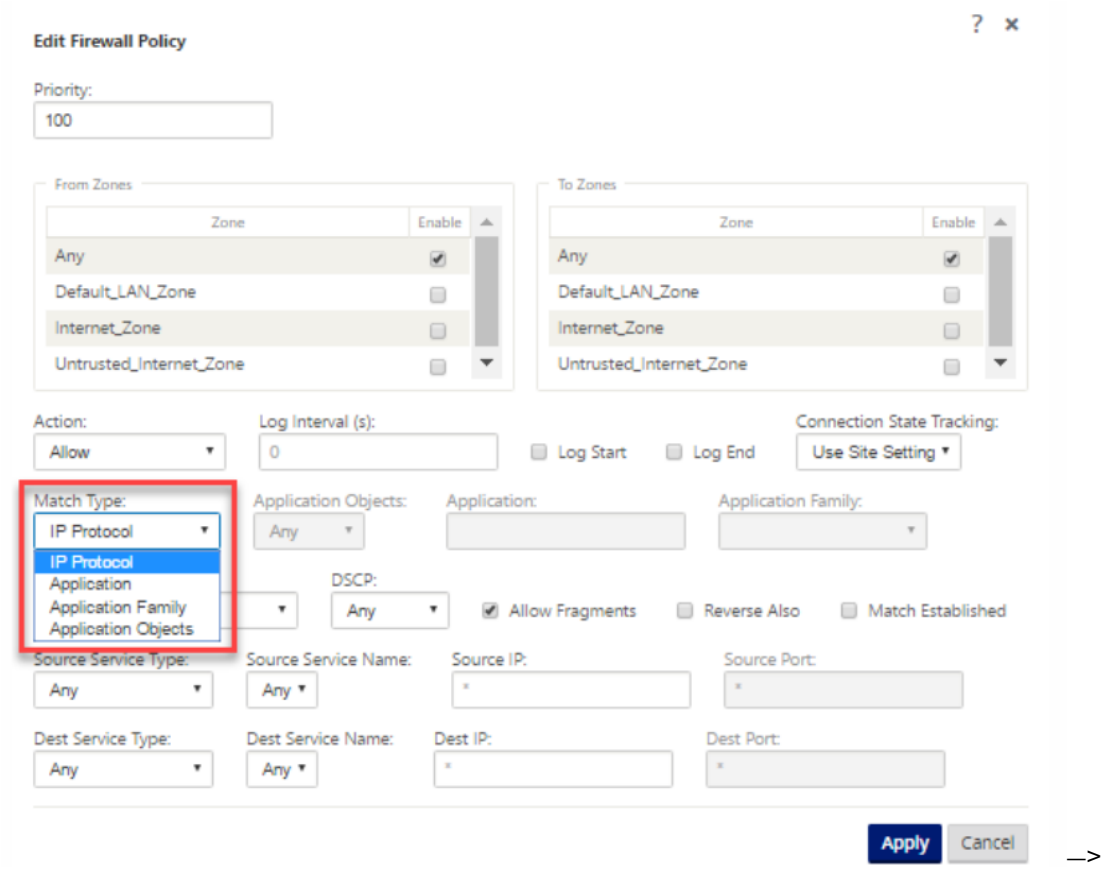
アプリケーションオブジェクトを使用すると、異なるタイプの一致基準を 1 つのオブジェクトにグループ化できます。このオブジェクトは、ファイアウォールポリシーおよびアプリケーションステアリングで使用できます。IP プロトコル、アプリケーション、およびアプリケーションファミリは、使用可能な一致タイプです。

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

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、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、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。

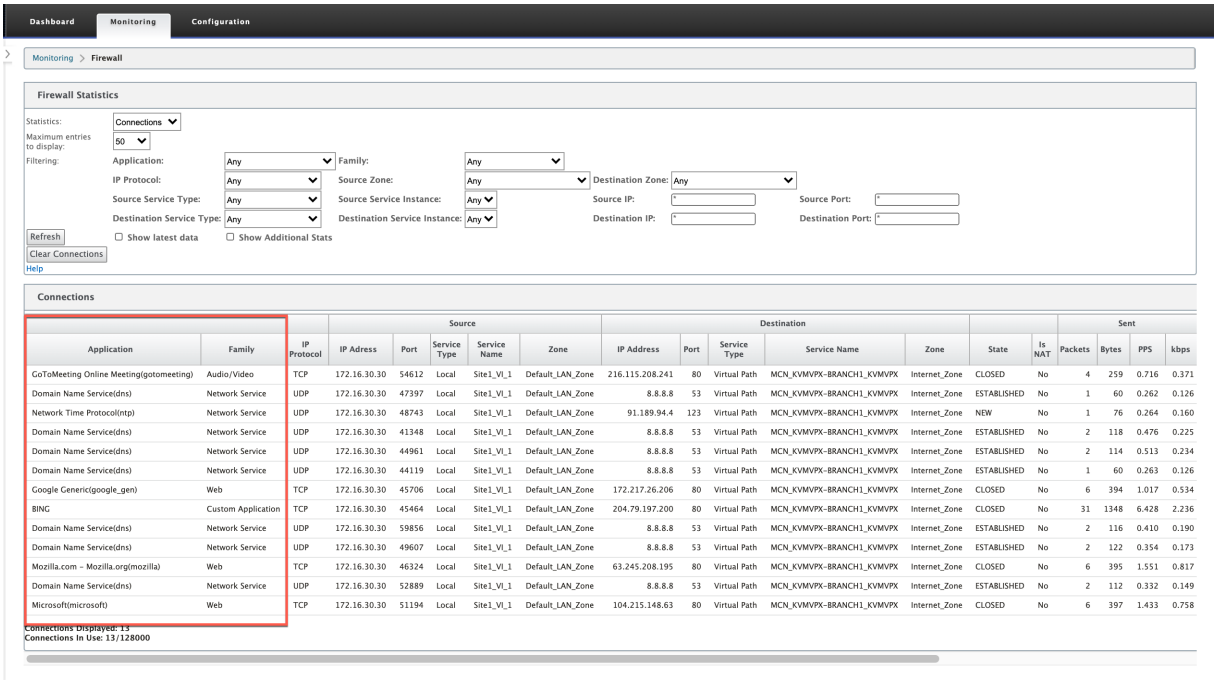


アプリケーション分類の表示

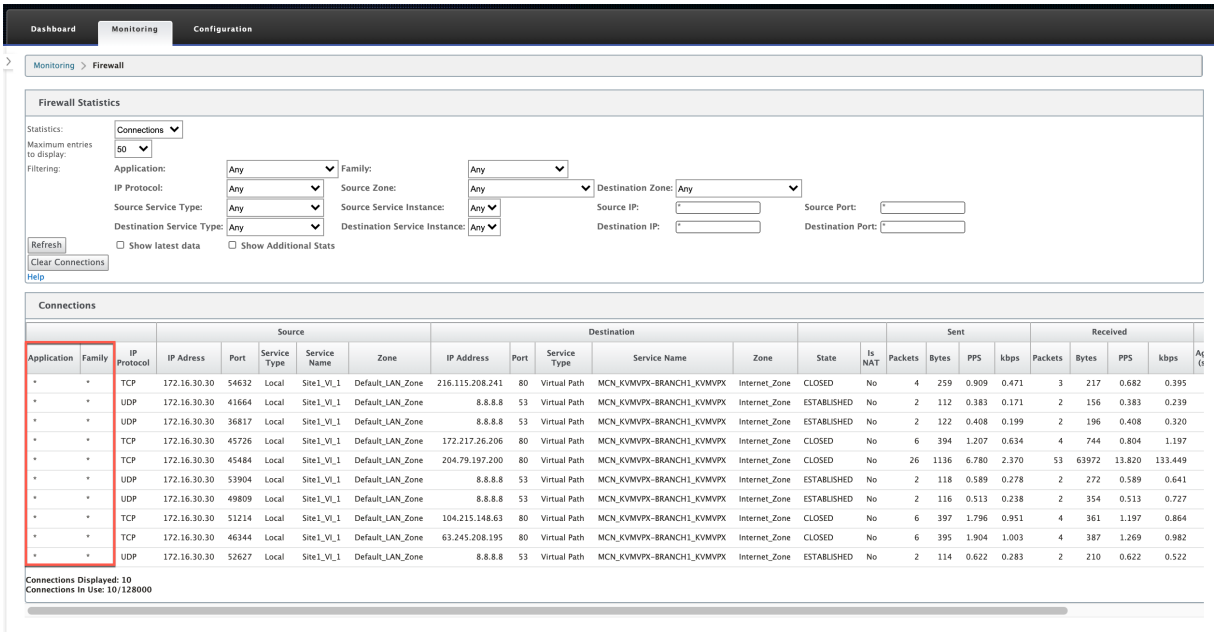
アプリケーションの分類を有効にすると、次のレポートでアプリケーション名とアプリケーション・ファミリの詳細を表示できます。

- 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

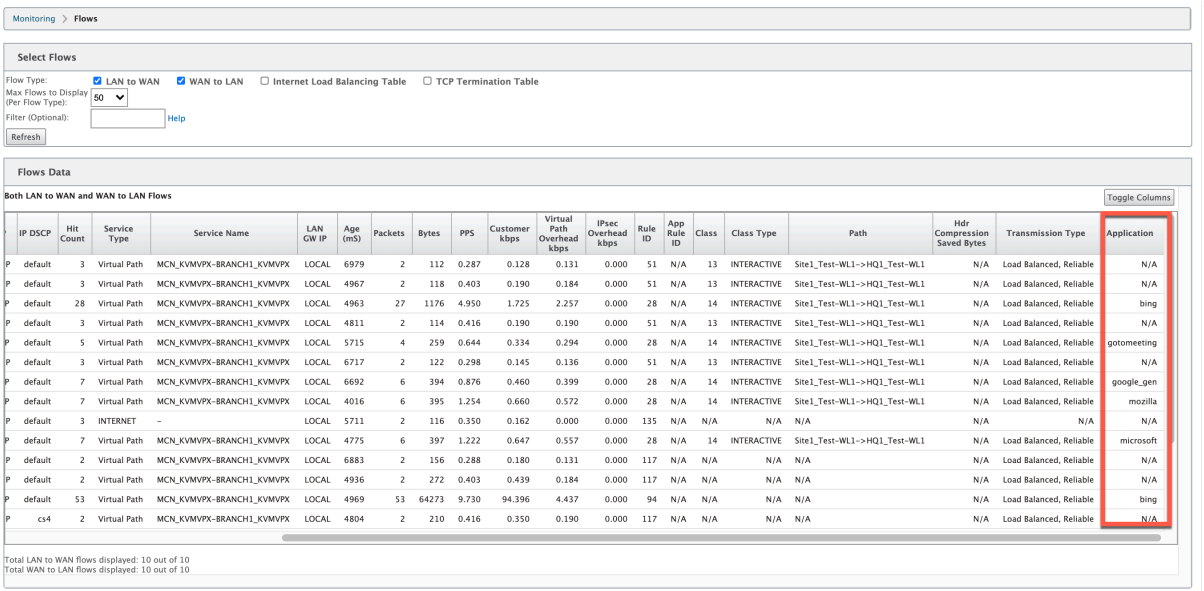
ファイアウォール接続の統計情報　監視 > ファイアウォールに移動します。[接続] セクションの [アプリケーション] 列と [ファミリ] 列には、アプリケーションとその関連ファミリが一覧表示されます。



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」列にはデータが表示されません。



フロー情報　監視 **>** 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。



アプリケーション統計　[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。

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**）

QoS 公平性機能は、QoS クラスとランダム早期検出（RED）を使用して、複数の仮想パスフローの公平性を改善します。仮想パスは、16 の異なる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、階層的公正サービス曲線 (HFSC) アルゴリズムを使用して、クラス間の公平性を実現します。

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を保持し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フローが仮想パスを満たすため、新しい TCP 接続では帯域幅を均等に割り当てることが困難になります。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 の使用方法と有効化方法については、RED の使用方法を参照してください。

MPLS キュー

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 Differented 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。Citrix SD-WAN Orchestrator サービスを使用して MPLS を構成する方法については、「MPLS キュー」を参照してください。

> 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。

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。

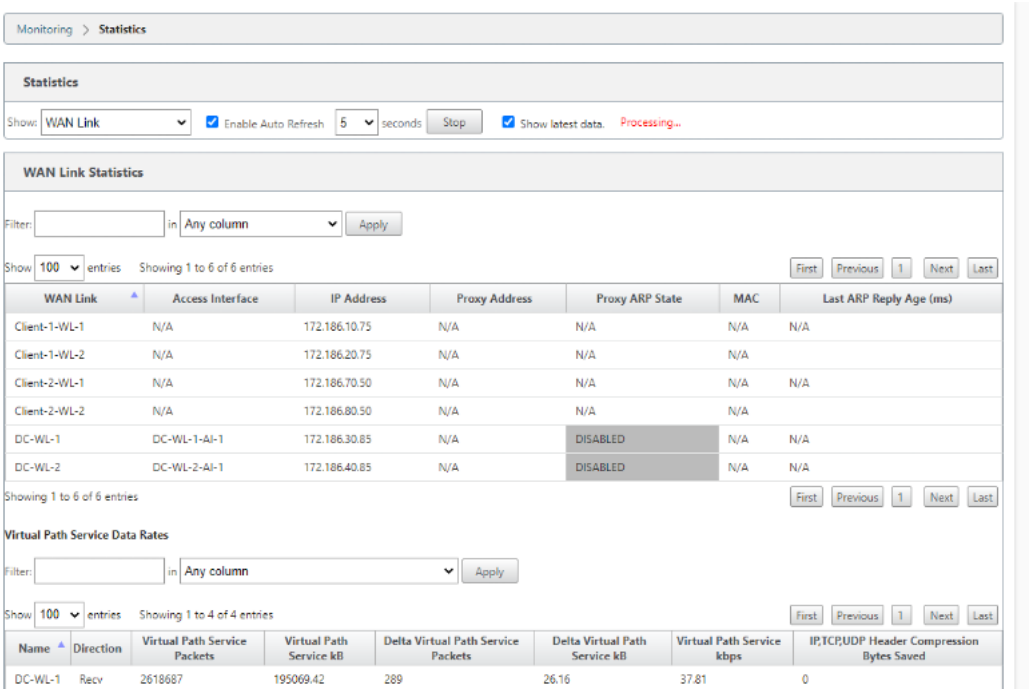
WAN リンクの許可レートと輻輳の表示

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。

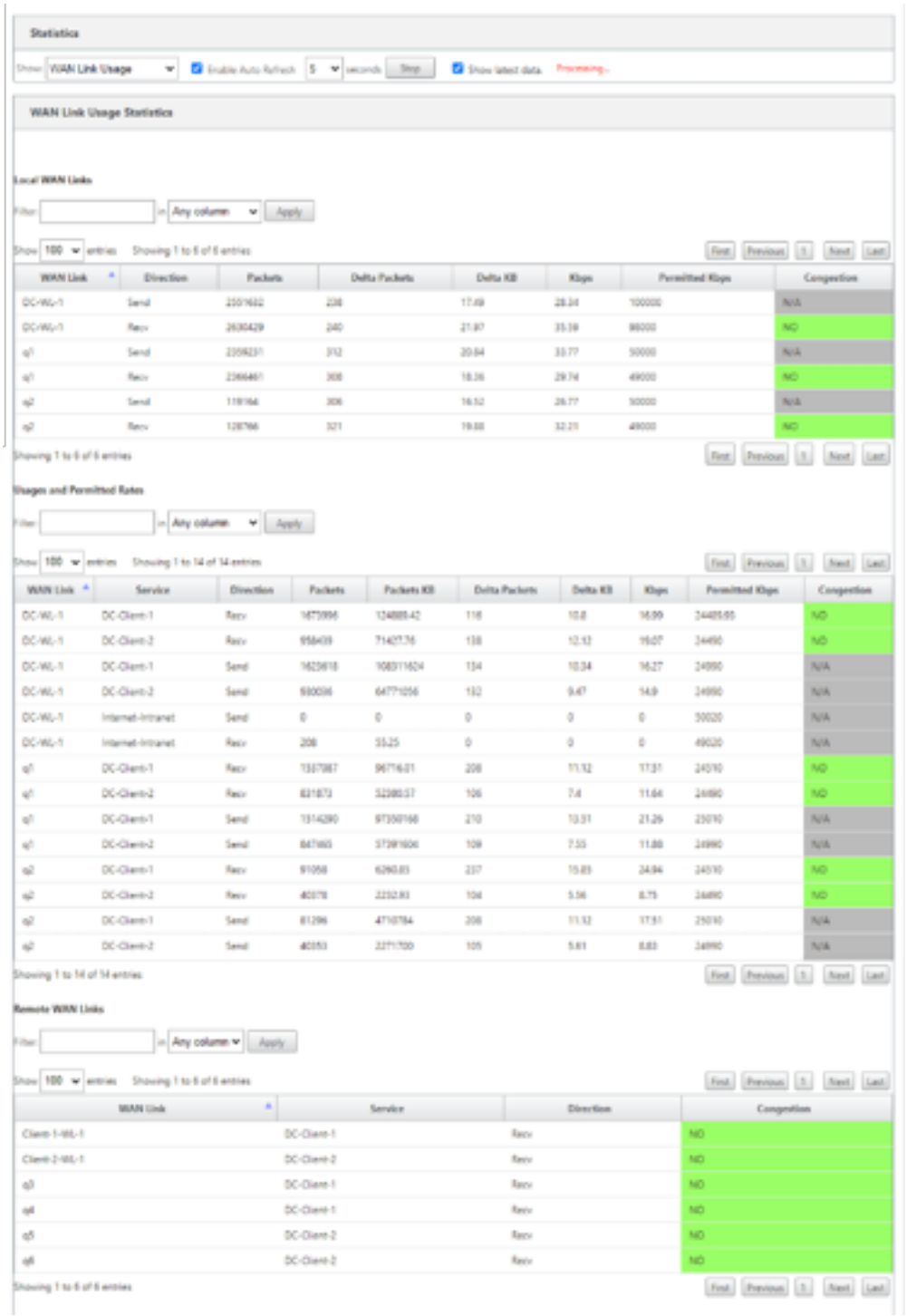
許可された料金を表示　許可レートは、特定の WAN リンク、仮想パスサービス、イントラネットサービス、またはインターネットサービスが、特定の時点で使用できる帯域幅の量です。WAN リンクの許可レートはスタティックで、SD-WAN 設定で明示的に定義されます。仮想パスサービス、イントラネットサービス、またはインターネットサービスの許可率は、輻輳、ユーザーの要求、公正な共有に応じて時間の経過とともに変動しますが、常にサービスの最小予約帯域幅以上になります。

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。

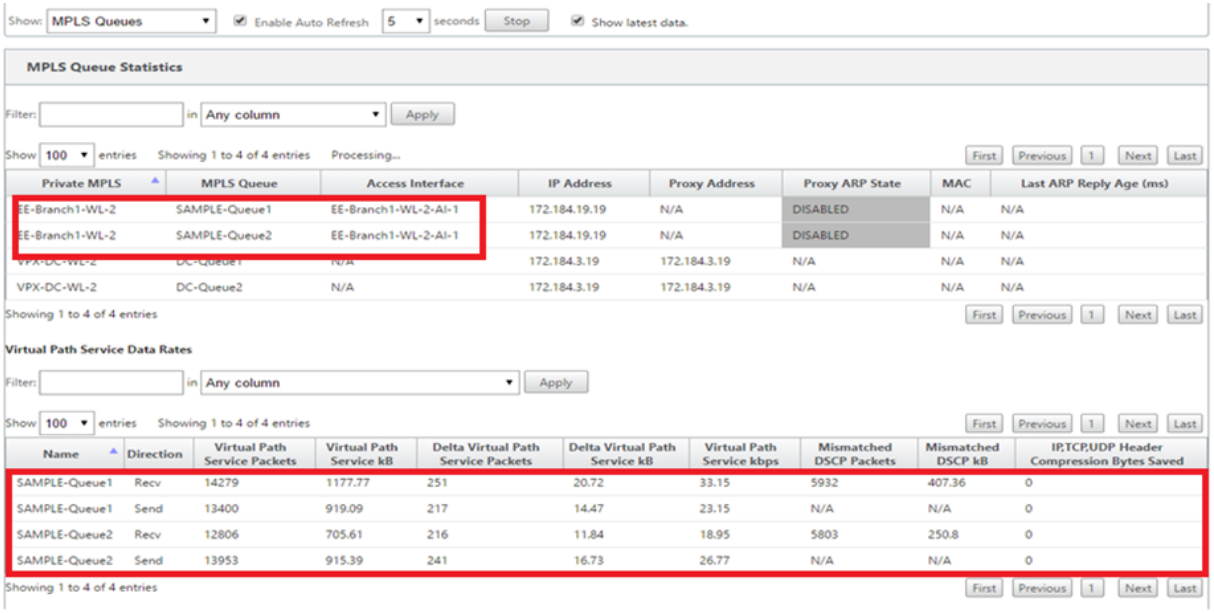


[モニター**] > [**統計] の順に選択し、[表示] ドロップダウンリストから [**WAN** リンクの使用状況] を選択します。



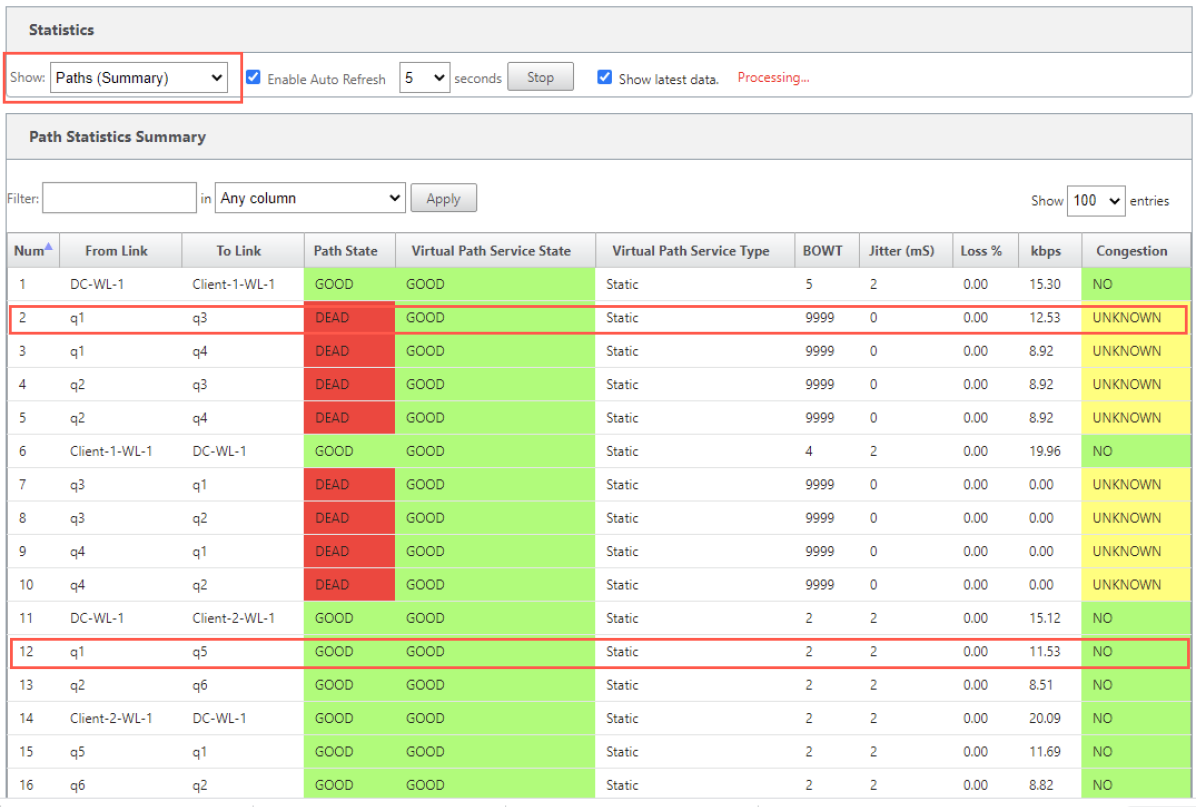
MPLS キューの監視

[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。



MPLS キューのトラブルシューティング

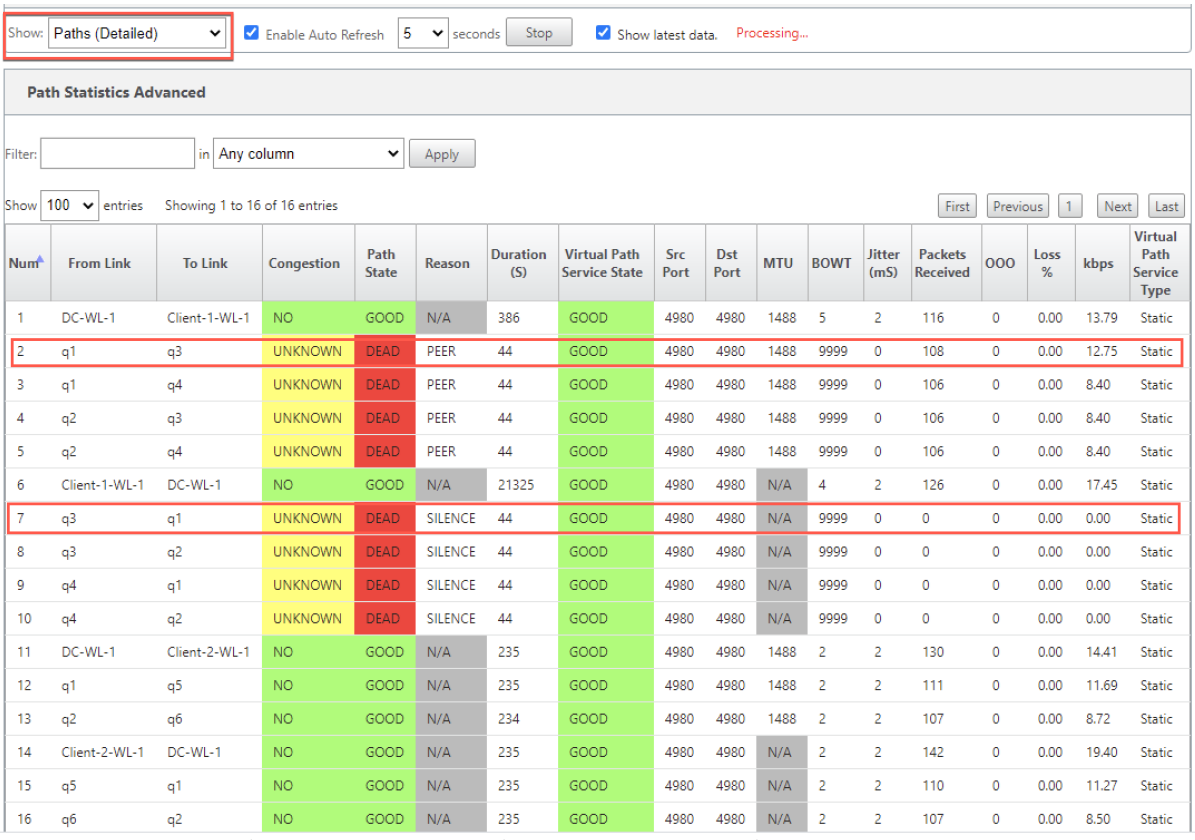
MPLS キューのステータスを確認するには、[モニタ**] > [**統計] に移動し、[表示] ドロップダウンリストから [パス（要約）] を選択します。次の例では、MPLS キュー「q1」から「q3」へのパスが DEAD 状態であり、赤色で示されています。MPLS キュー「q1」から「q5」へのパスは GOOD 状態であり、緑色で表示されます。



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、

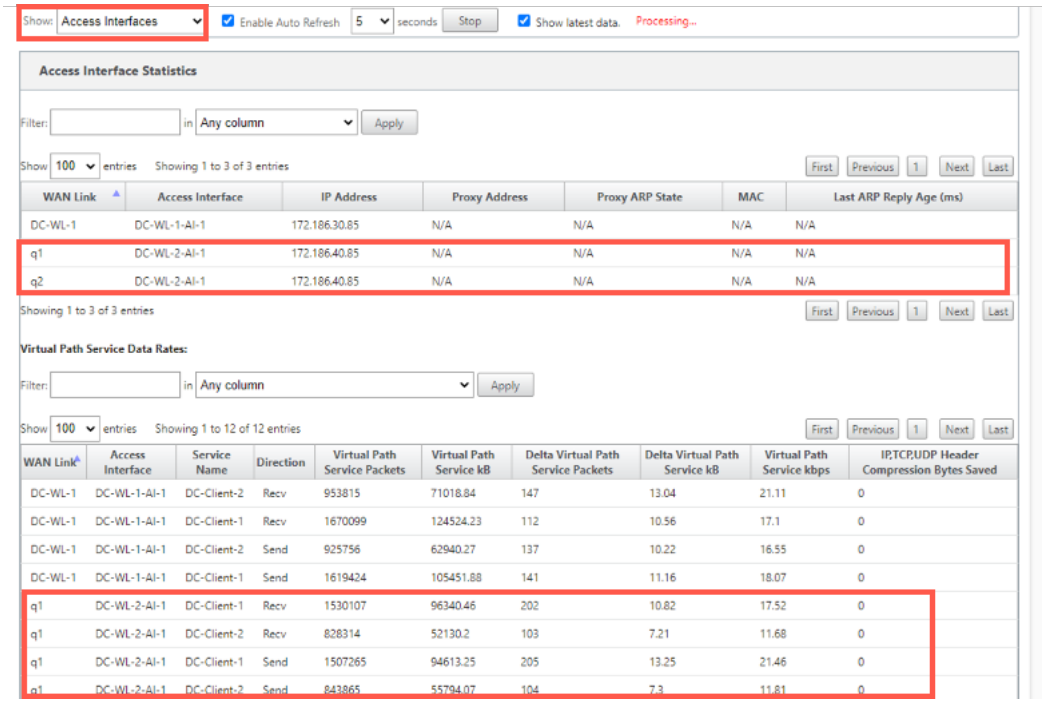
次の例では、MPLS キュー「q1」から「q3」へのパスが DEAD 状態であり、その理由は PEER です。MPLS キュー「q3」から「q1」へのパスは停止しており、その理由は SILENCE です。次の表に、利用可能な理由のリストとその説明を示します。

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

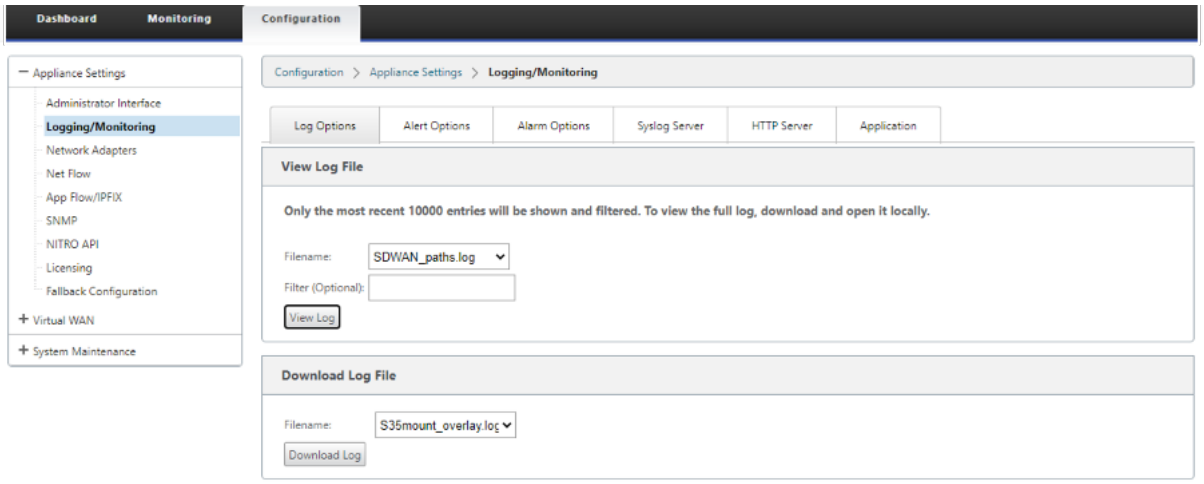


Num	From Link	To Link	Congestion	Path State	Reason	Duration (S)	Virtual Path Service State	Src Port	Dst Port	MTU	BOWT	Jitter (mS)	Packets Received	OOO	Loss %	kbps	Virtual Path Service Type
1	DC-WL-1	Client-1-WL-1	NO	GOOD	N/A	386	GOOD	4980	4980	1488	5	2	116	0	0.00	13.79	Static
2	q1	q3	UNKNOWN	DEAD	PEER	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。



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。



レポート

November 17, 2022

アプリケーション **QoE**

アプリケーション **QoE** は、SD-WAN ネットワーク内のアプリケーションのエクスペリエンス品質の尺度です。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

アプリケーションの **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。

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インタラクティブトラフィック用のカスタム QoE プロファイルを作成し、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 QoE プロファイルでマッピングできます。

Citrix SD-WAN Orchestrator サービスを介してカスタム QoE プロファイルを作成するには、「アプリケーション QoE プロファイル」を参照してください。

HDX QoE

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。

Citrix SD-WAN Orchestrator サービスを使用して HDX QoE を構成する方法について詳しくは、「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、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に常に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* パケット損失に関連しますが、アプリケーションの損失は再送信後のもので、*WAN* リンク損失よりも低くなります。
> - *GUI* に表示される *WAN* リンクの遅延は、*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、リンクの最適なメトリックです。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 *1MSI* ではなく *4SSI* 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* 分かかることがあります。
> - *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。

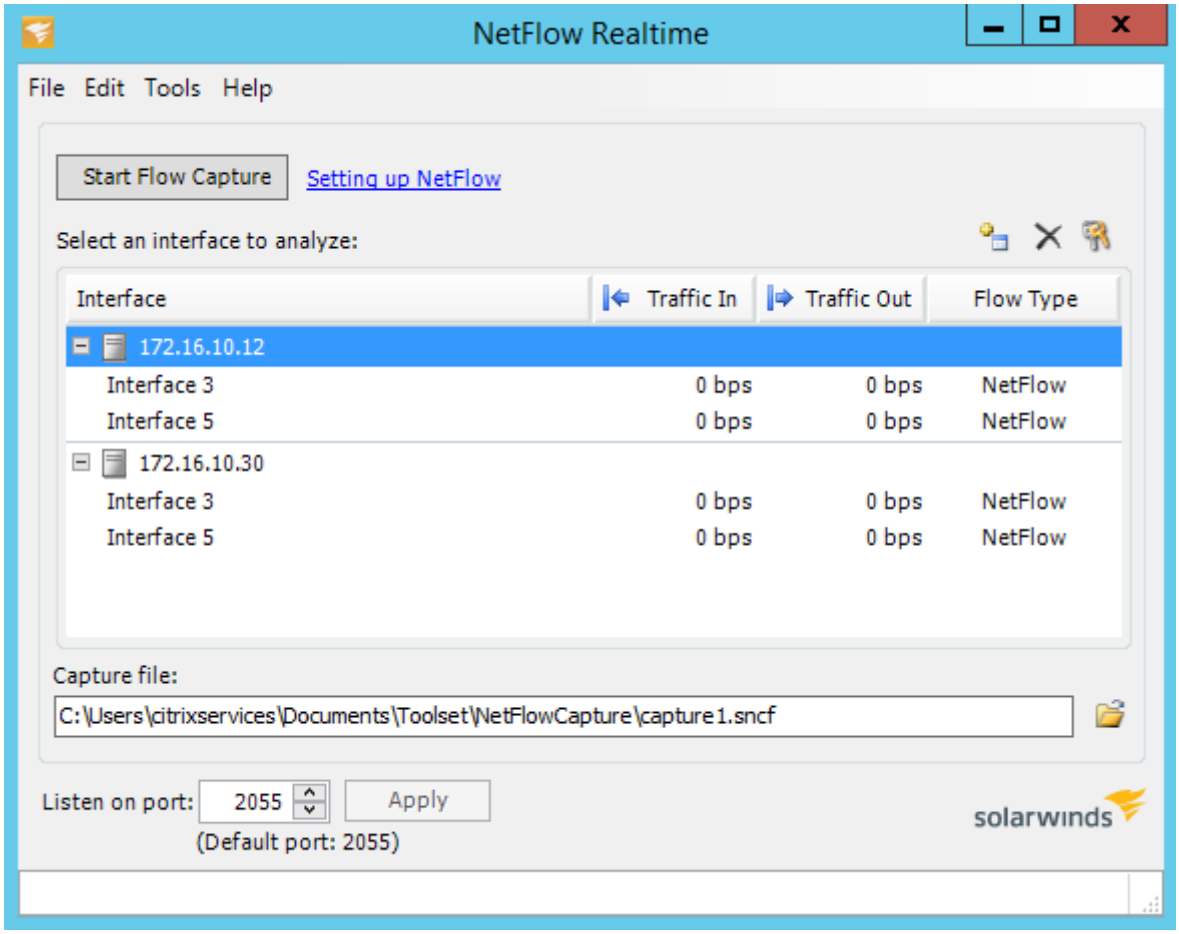
複数のネットフローコレクタ

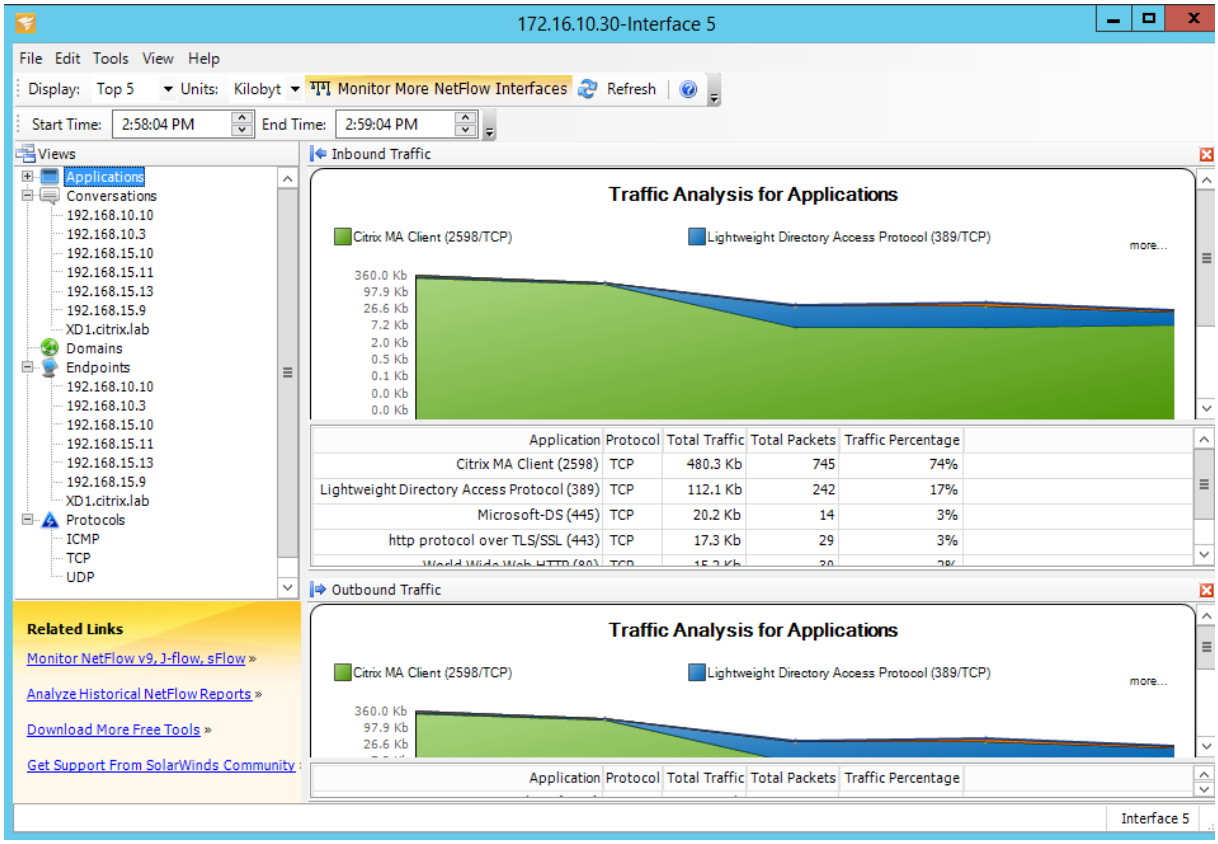
ネットフローコレクタは、SD-WAN インターフェイスに出入りすると、IP ネットワークトラフィックを収集します。Net Flow によって提供されるデータを分析することで、トラフィックの送信元と宛先、サービスクラス、およびトラフィックの輻輳の原因を特定できます。Citrix SD-WAN デバイスは、構成済みの Net フローコレクターに基本的な Net フローバージョン 5 の統計データを送信するように構成できます。Citrix SD-WAN は、信頼できるトランスポートプロトコルによって隠されるトラフィックフローに対する Net Flow サポートを提供します。ソリューションの WAN 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。Net Flow は、Citrix SD-WAN Standard Edition アプライアンスでサポートされています。

Citrix SD-WAN Orchestrator サービスを使用して Net Flow ホストを構成する方法については、「Netflow ホスト設定」を参照してください。

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。



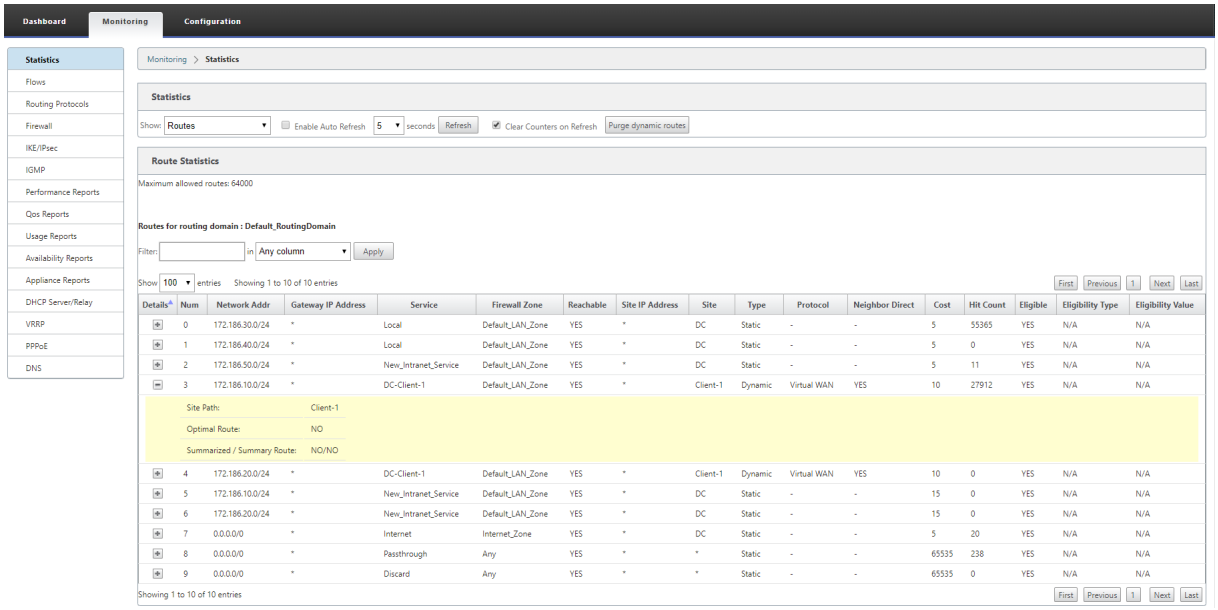


NetFlow の制限事項

- SD-WAN Standard Edition アプライアンスで Netflow が有効になっていると、仮想パスデータは指定された 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

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 > 統計情報 > ルートに移動します。



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、受信したプレフィクスの信頼できる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、その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ための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：サマリルートは、スーパーネットに含まれる複数のプレフィクスを集約するために管理者によって明示的に設定されたルートです。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 Gateway/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: ルートで使用されるファイアウォールゾーン。
- 到達可能: ルートは到達可能かどうか。
- 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、ルートラーニング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したプレフィクス。
  - **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パスを決定するために使用されるコスト。
- **Hit Count**: 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：ルートが適格であり、トラフィック処理中にパケットをプレフィックスヒットに転送またはルーティングするために使用されることを示します。
- 適格タイプ: 次の 2 つの資格タイプがあります。
  - **Gateway** 適格性:Gateway が到達可能かどうかを決定します。
  - パスの適格性: パスが死んでいるか死んでいないかを決定します。
- 適格性の値: システムでルートが作成されるときに、ゲートウェイまたは構成内のパスに選択された値。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

November 17, 2022

> 注
>
> SD-WAN 11.5 リリース以降、すべてのルーティング構成は Citrix SD-WAN Orchestrator サービスを介してのみサポートされます。Citrix SD-WAN Orchestrator サービスのルーティング構成については、「ルーティング」を参照してください。

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の数が減少します。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

August 30, 2022

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 では、特定のサイトのスタティックルートエントリと、OSPF、eBGP、iBGP などのサポートされているルーティングプロトコル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、仮想パスを通っ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。
- イントラネット：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：これは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 リンクへのトラフィックフロー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。

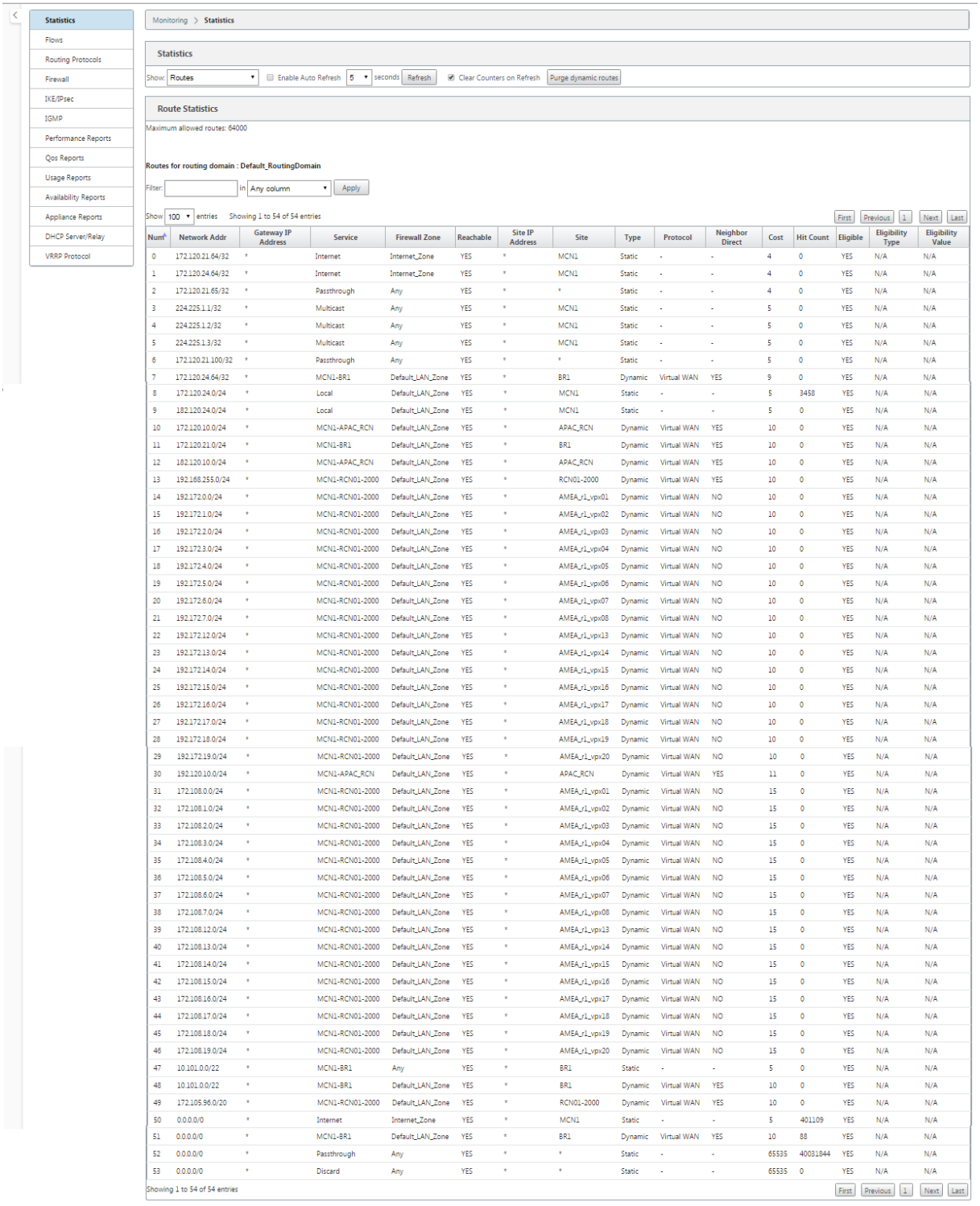
> 注
>
> インターネットサービスルートは、仮想パスを介してインターネットアクセスをバックホールしているかどうかに応じて、他の SD-WAN アプライアンスにアドバタイズしたり、エクスポートできないようにしたりできます。

- パススルー—このサービスは、アプライアンスがインラインモードの場合の最後の手段またはオーバーライド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 パススルール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/Gateway 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)。

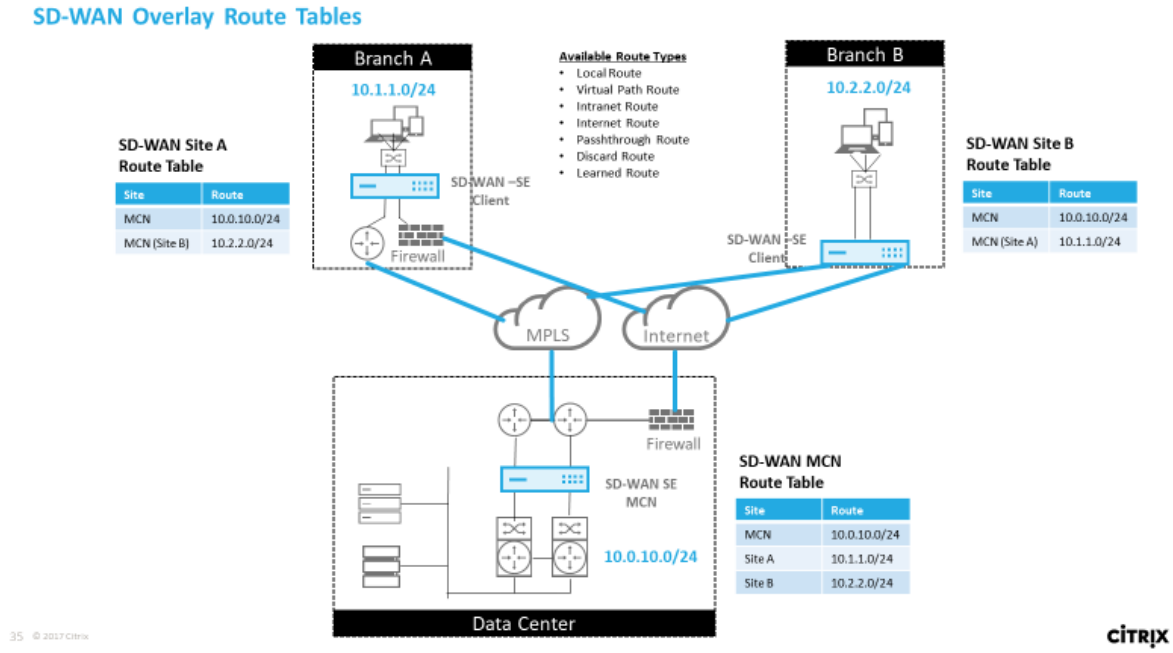
ローカルクライアントノードのルートテーブルは、[**Monitoring] > [**Statistics**] ページで、[**Show**] ドロップダウンリストで [ルート] を選択して監視できます ** 。



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。



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. 最長プレフィクス一致
2. コスト
3. Service

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の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。SD-WAN Orchestrator サービスで同じルーティングプロトコルを有効にすると、SD-WAN オーバーレイを使用するように示されているサブネットの構成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/Gateway 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。

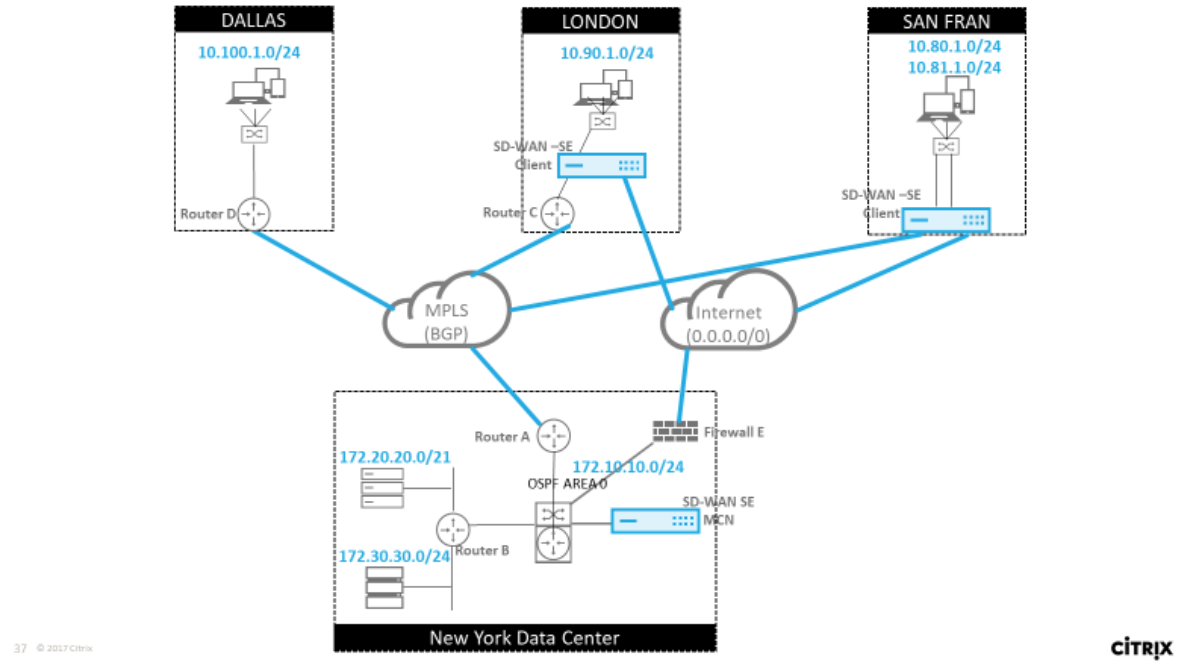
> 重要
>
> 気をつけなければ、不要なルートを漏らすのは簡単です。

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 Gateway 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：



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 Gateway 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 Gateway 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/Gateway 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。

ダラスルーター **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。

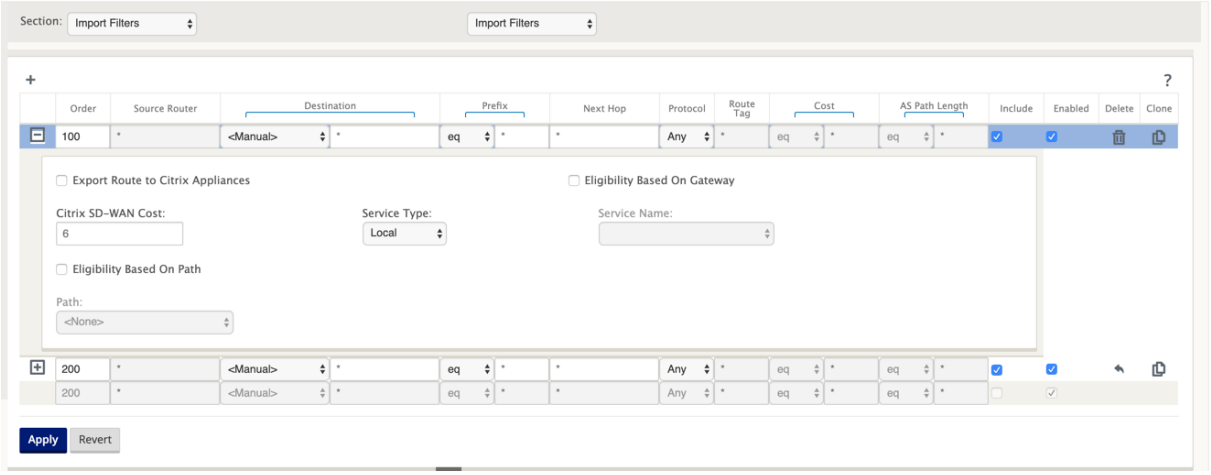
```
vyos@VYATTA-ROUTER-D:~$ show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - ISIS, B - BGP, > - selected route, * - FIB route

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。

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。

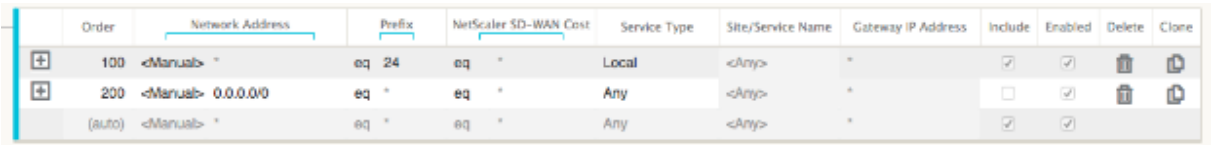
仮想パスルーティングテーブルと、使用中のダイナミックルートプロトコルの間でルートがどのように渡されるかを理解することが重要です。ルーティングループを作成したり、ルートをアドバタイズしたりするのは簡単です。フィルタメカニズムは、ルーティングテーブルに出入りする内容を制御する機能を提供します。各場所を順番に検討します。

- サンフランシスコのロケーションには、**10.80.1.0/24** と 10.81.1.0/24** の 2 つのローカルサブネットがあります。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。



- 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、仮想パスを通って学習しました。



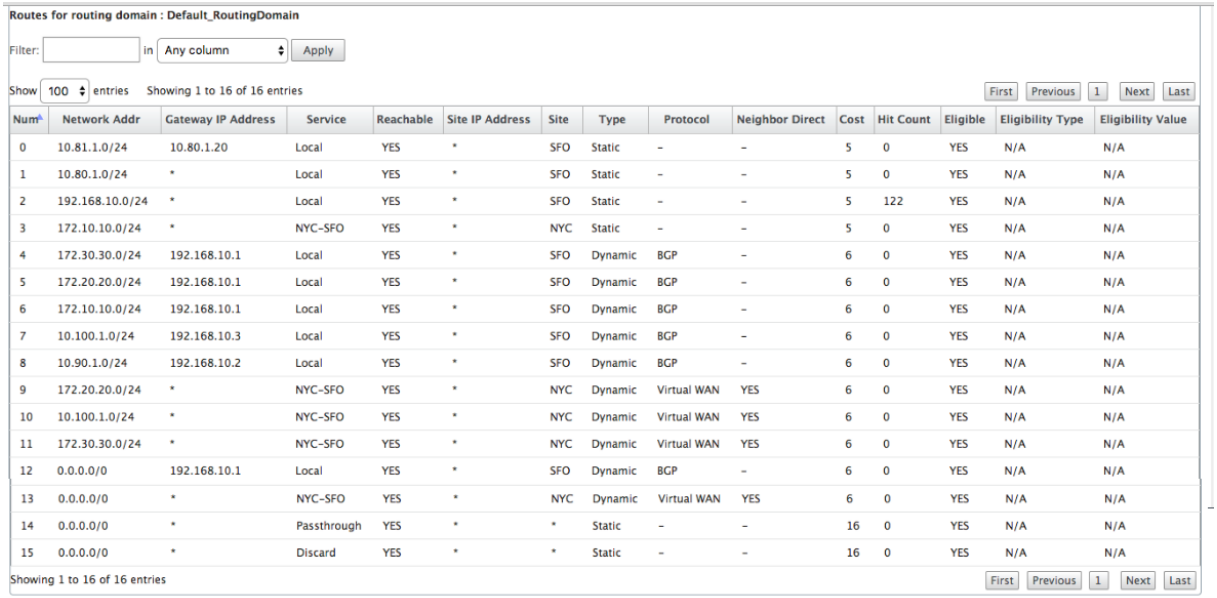
Citrix SD-WAN アプライアンスを展開した後、ダラスサイトにある BGP ルータのルートテーブルをリフレッシュできます。10.80.1.0/24 および 10.81.1.0/24 サブネットが、サンフランシスコ SD-WAN からの eBGP を介して正しく認識されていることがわかります。

ダラス・ルーター **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。

San Francisco Citrix SD-WAN:



Routes for routing domain : Default_RoutingDomain

Filter: in Any column Apply

Show 100 entries Showing 1 to 16 of 16 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	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 First Previous 1 Next Last

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。

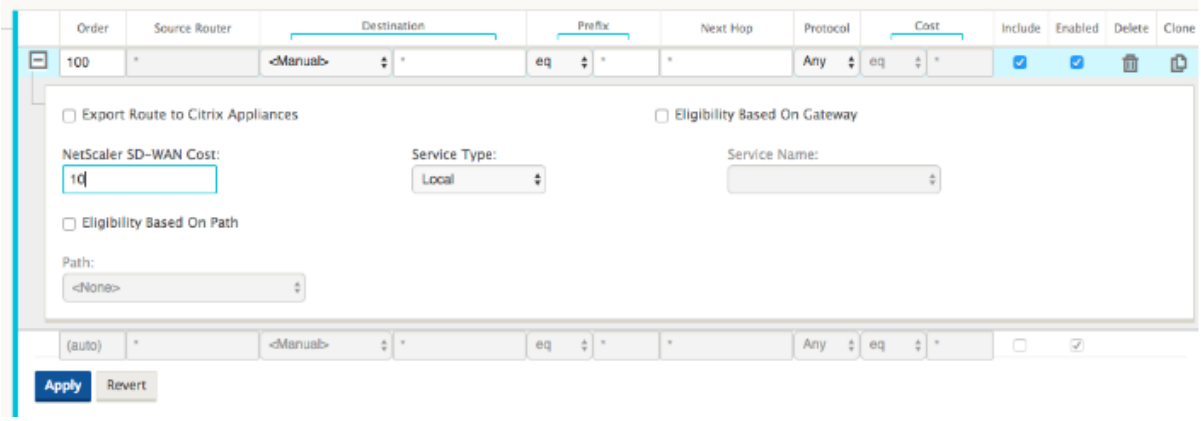
- BGP（番号 6）を介してアドバタイズされたルートとして、コストは 6 です。これは現在、フォールバックルートと見なされます。

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。

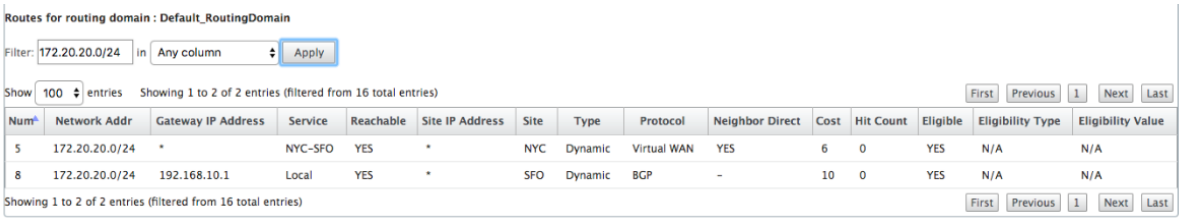
さて、ルート 172.20.20.0/24 を考えてみましょう。

- 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。

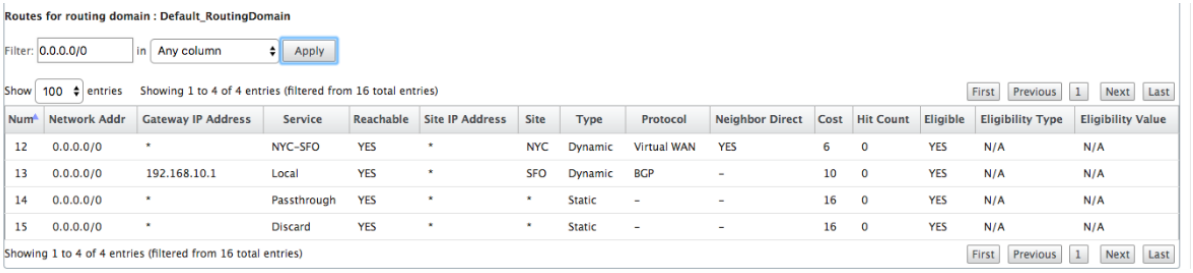
正しいルーティングを確保するには、BGP ルートコストを増やして、仮想パスルートがあり、それが優先ルートであるかどうかを確認する必要があります。これは、インポートフィルタのルートウェイトをデフォルトの 6 よりも大きく調整することで実行できます。



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。



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) 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
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) First Previous 1 Next Last

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。

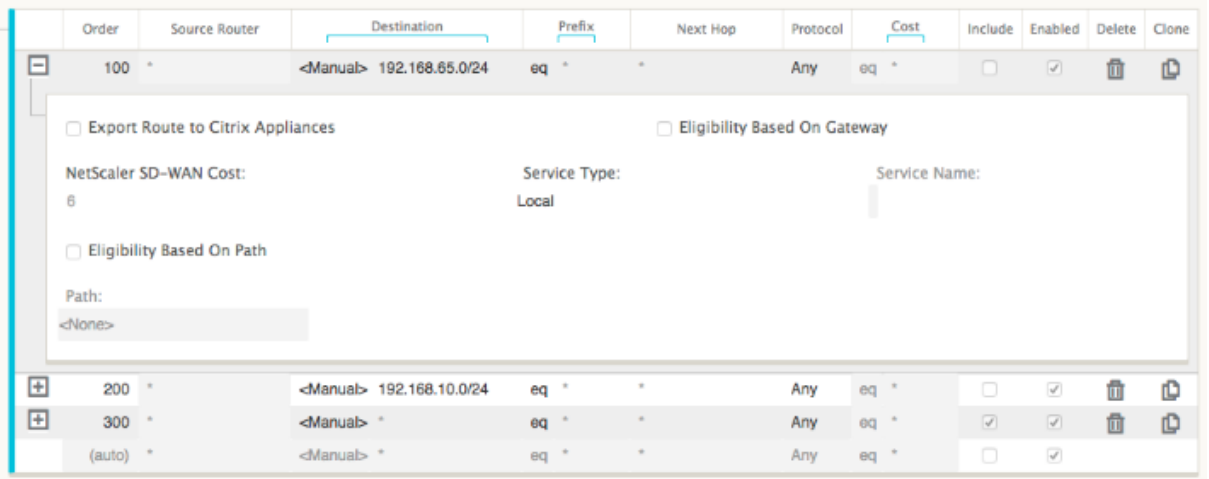
ここでは、ニューヨークのサイトに焦点を当て、仮想パスがアクティブなときに、リモートサイト（ロンドンとサンフランシスコ）宛てのトラフィックを SD-WAN アプライアンスに転送します。

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 *				
200	*	<Manual> 192.168.10.0/24	eq *	*	Any	eq *				
300	*	<Manual> *	eq *	*	Any	eq *				
(auto)	*	<Manual> *	eq *	*	Any	eq *				

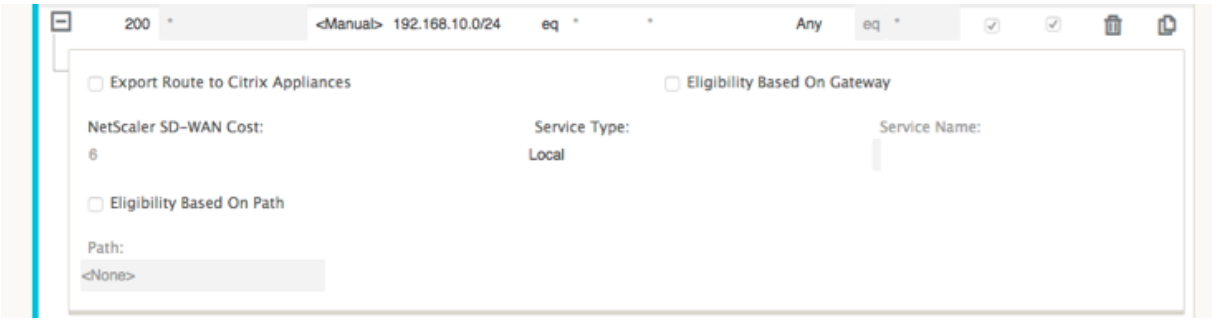
Export Route to Citrix Appliances　Eligibility Based On Gateway

NetScaler SD-WAN Cost: 6　Service Type: Local　Service Name:

Eligibility Based On Path

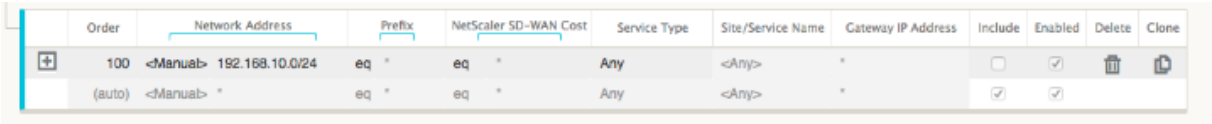
Path: <None>

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。



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。



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 Apply

Show 100 entries Showing 1 to 11 of 11 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	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

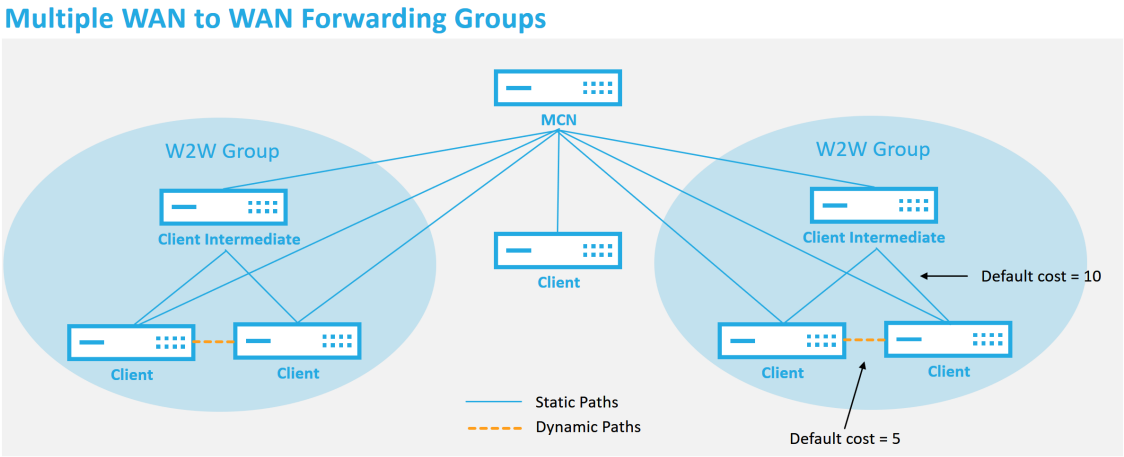
動的仮想パスは、2 つのクライアントノード間で許可され、2 つのサイト間で直接通信するためのオンデマンド仮想パスを構築できます。動的仮想パスの利点は、MCN または 2 つの仮想パスを通過することなく、トラフィックが 1 つのクライアントノードから 2 番目のクライアントノードに直接フローできることです。これにより、トラフィックフローにレイテンシーが増える可能性があります。動的仮想パスは、ユーザー定義のトラフィックしきい値に基づいて動的に構築および削除されます。これらのしきい値は、パケット/秒（pps）または帯域幅（kbps）のいずれかとして定義されます。この機能により、ダイナミックフルメッシュ 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。

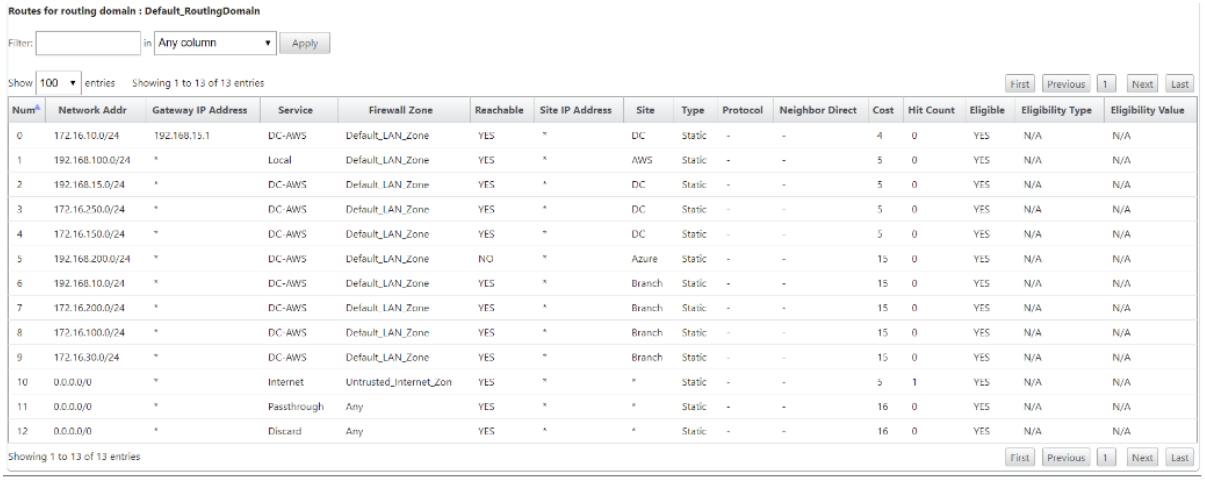
SD-WAN では複数の WAN-to-WAN 転送グループが許可され、特定のクライアントノードと他のクライアントノード間のパス確立を完全に制御できます。



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 Gateway
- 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ての 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

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—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
- イントラネット・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

August 30, 2022

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を作成できます。

ルーティングドメインの構成

August 30, 2022

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。

11.0.2 リリースでは、ルーティング可能な仮想 **IP**（**VIP**）の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、ブランチ間の通信を許可します。

CLI を使用してルーティングにアクセスする

August 30, 2022

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、コマンドのリストを表示します。

```
dynamic_routing?
<!--NeedCopy-->
```


動的ルーティング

August 30, 2022

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 の安定したコンバージェンスを使用して、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。

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。

> 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。

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。

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

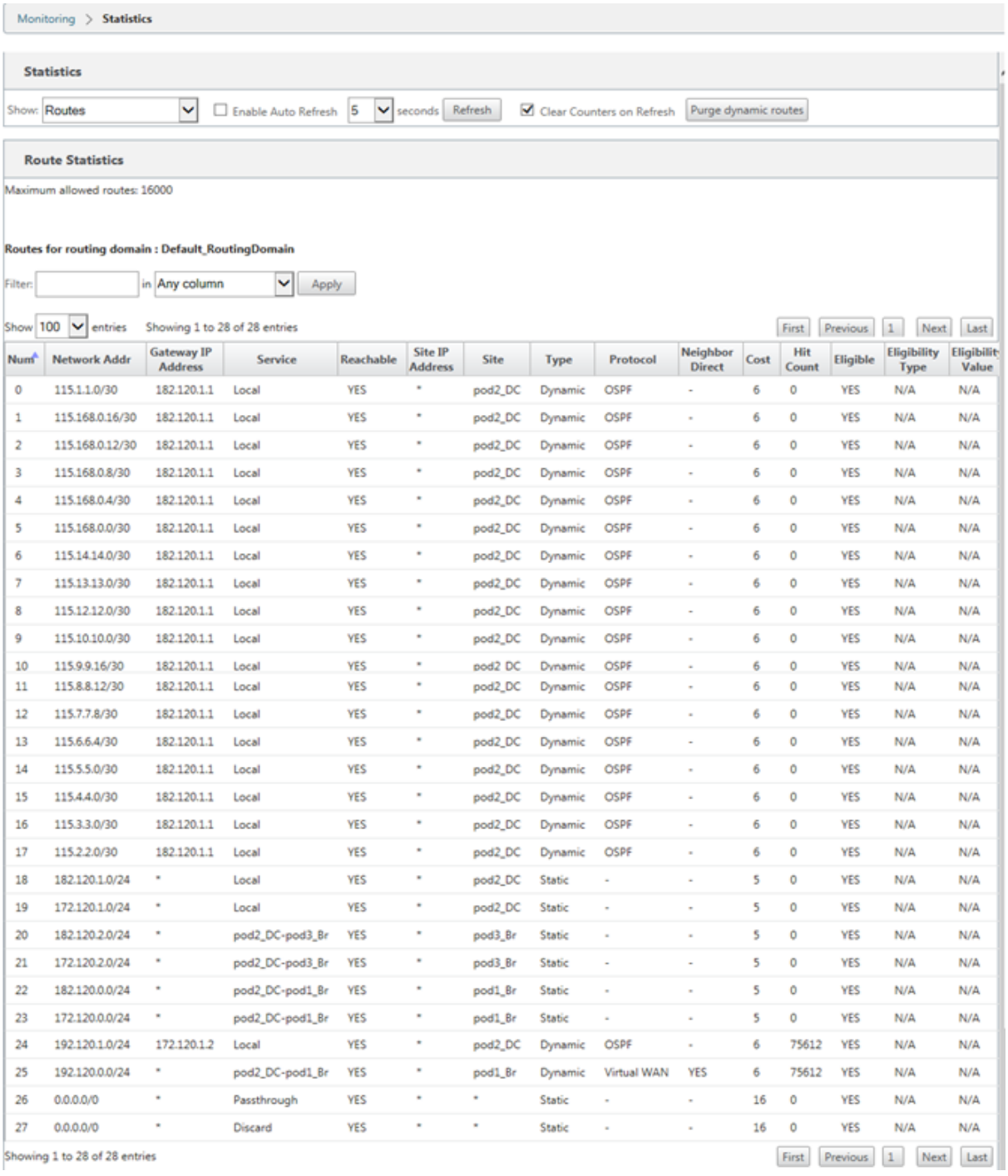
BGP プロトコルは、**AS** パス長属性を使用して最適ルートを決定します。AS パスの長さは、ルート内で通過する自律システムの数を示します。Citrix SD-WAN は、**BGP AS** パス長 属性を使用してルートをフィルタリングおよびインポートします。

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。

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かにかかわらず、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

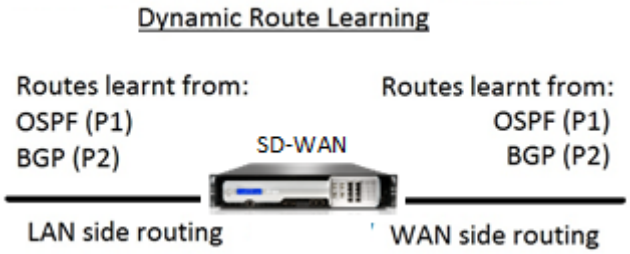
August 30, 2022

LAN 側：ダイナミックルートラーニング

Gateway 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 ルーティングアドバ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。

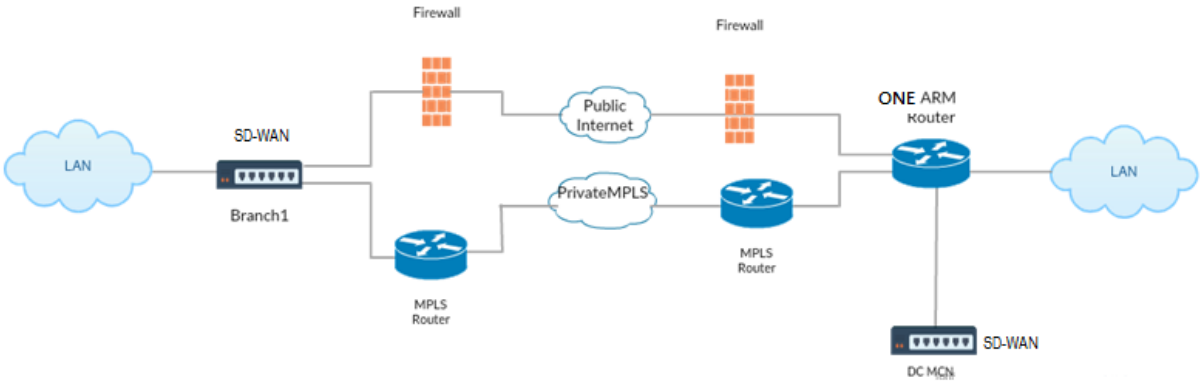
ワンアームトポロジでの **OSPF** の実装

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。

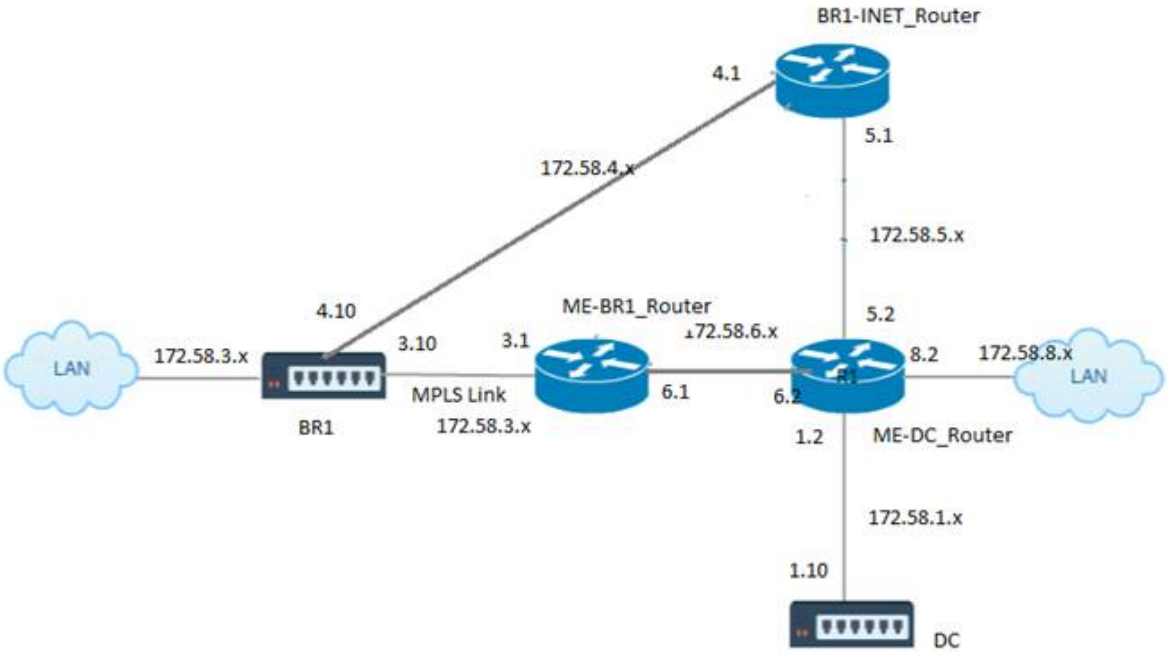


上の図に示すように、DC MCN はワンアームトポロジで展開されます。DC サイトがアップしている場合、ワンアームルータは、ローカル LAN から他のサイト（宛先 IP アドレスが同じサブネット内にある支店のローカル LAN など）にすべてのトラフィックを転送します。次に、SD-WAN アプライアンスはすべてのパケットをラップし、すべてのパケットの宛先 IP でルータに送信します。アドレスを、ブランチ仮想 IP アドレスに入力します。ルータは、これらのパケットを WAN に転送します。

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。

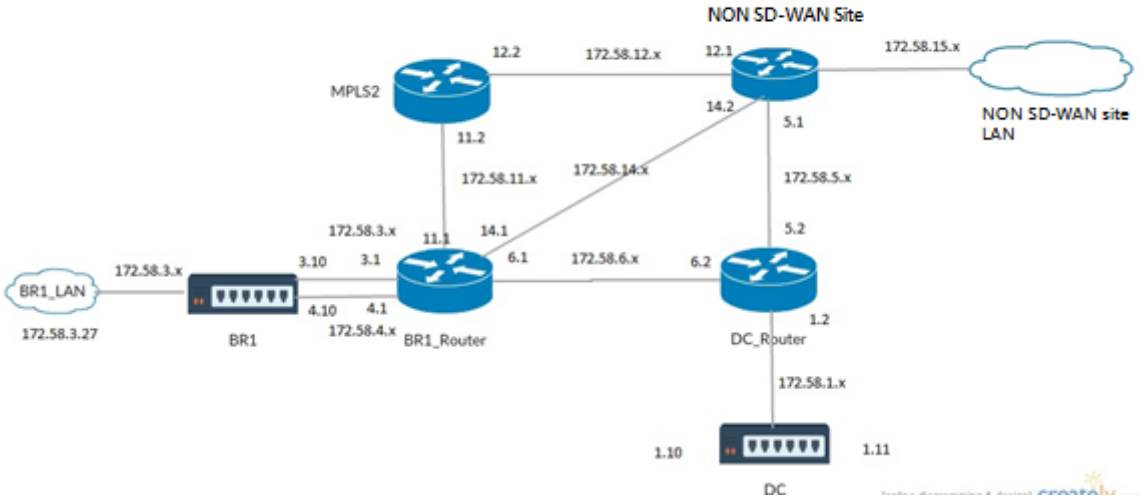
ME-DC_router は、172.58.8.0/24 ネットワークを DC SD-WAN と ME-BR1_router の両方にアドバタイズするための送信元として使用します。

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。

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

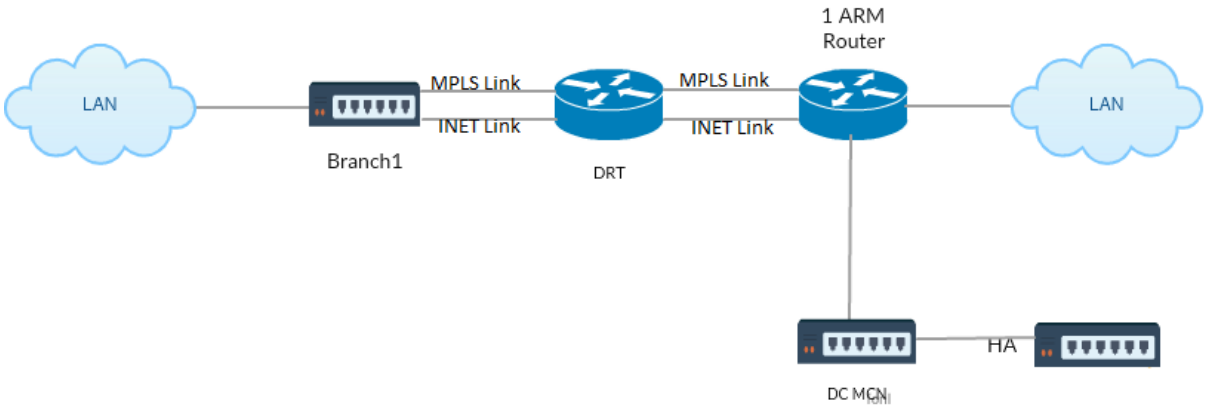
下の図に示すように、サードパーティのアプライアンスサイトは、サイト B に直接トラフィックを送信することで、サイト B の LAN にアクセスすることができます。トラフィックを直接送信できない場合、フォールバックルート

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。



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。

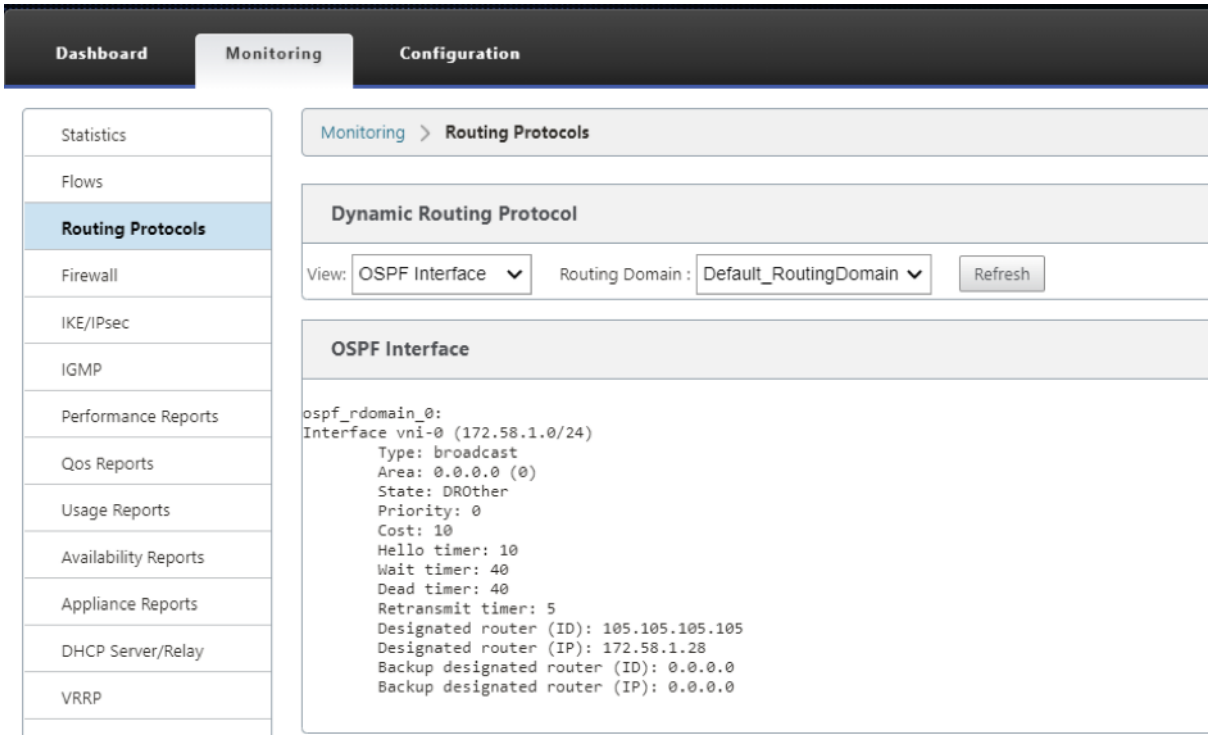
高可用性セットアップでの **SD-WAN** ネットワークでの **OSPF** の実装

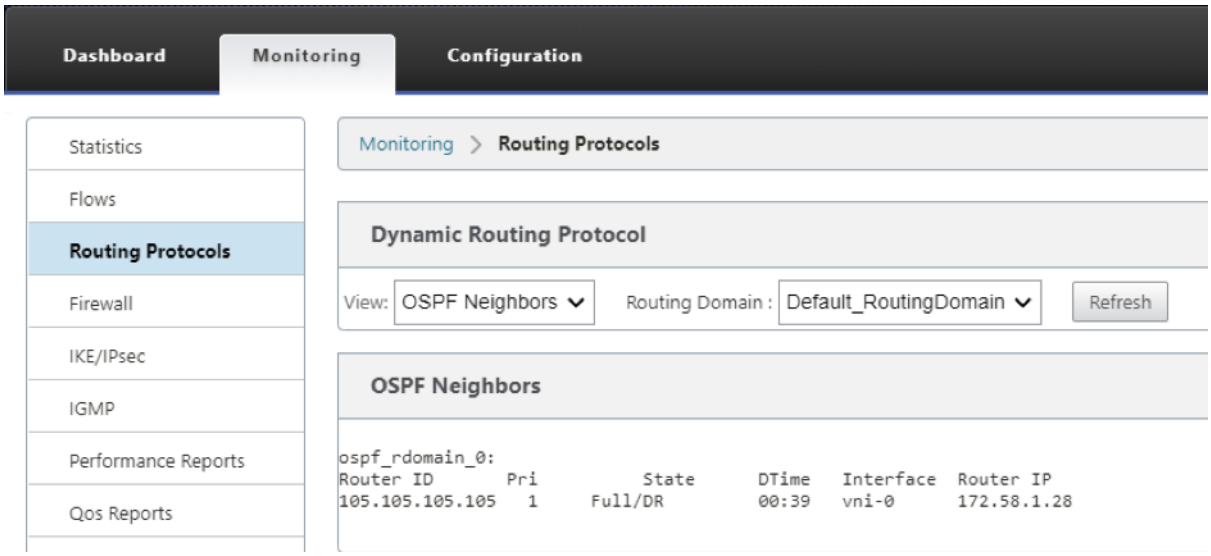


スタンバイアプライアンスへのフェールオーバー中に高可用性サイトを持つ OSPF Type-5 から Type-1 への高可用性セットアップで展開されます。

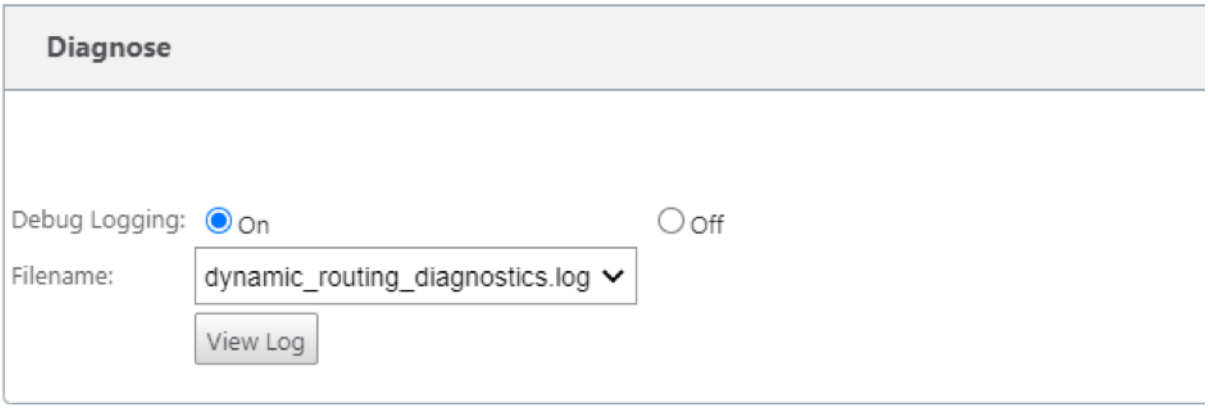
トラブルシューティング

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。





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。



BGP

August 30, 2022

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。

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。

1. [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、ルーティングのログファイルを表示するには、[モニタ（Monitor）] > [ルーティングプロトコル（Routing Protocol 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。標準のルーティング情報は *dynamic_routing.log* に保存され、動的ルーティングの問題は *dynamic_routing_diagnostics.log* にキャプチャされます。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

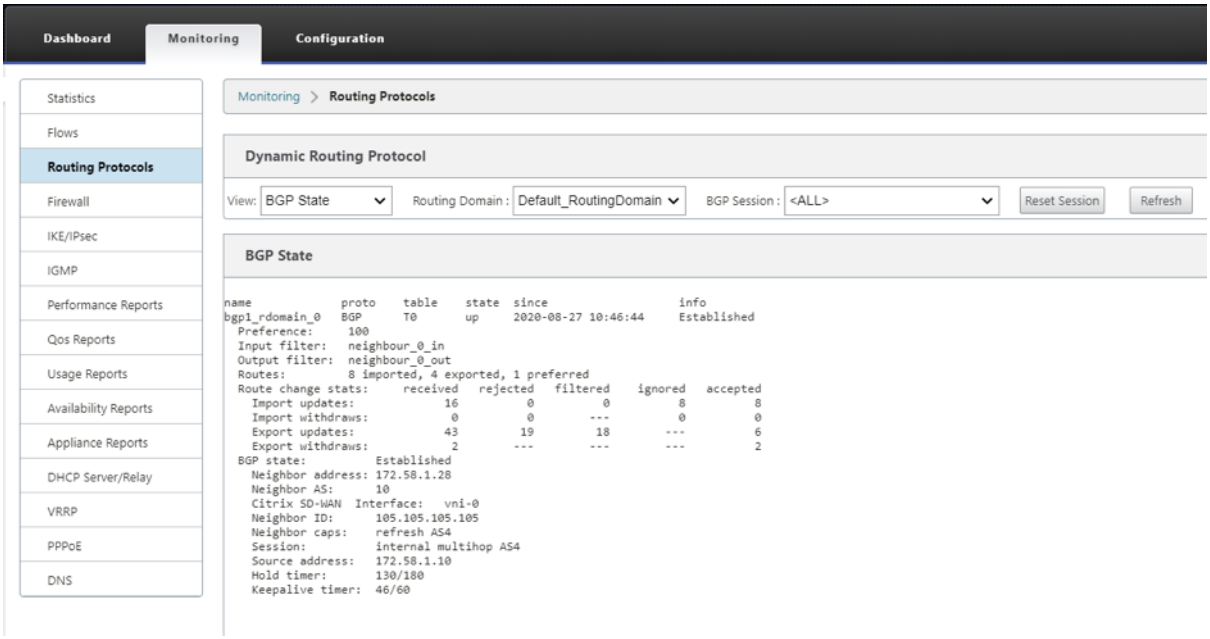
BGP ピアのルーティングポリシーには、インバウンドまたはアウトバウンドルーティングテーブルの更新に影響する可能性のあるルートマップ、配布リスト、プレフィクスリスト、フィルタリストなどの設定が含まれます。ルーティングポリシーに変更があった場合、新しいポリシーを有効にするには、BGP セッションをクリアまたはリセットする必要があります。

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。

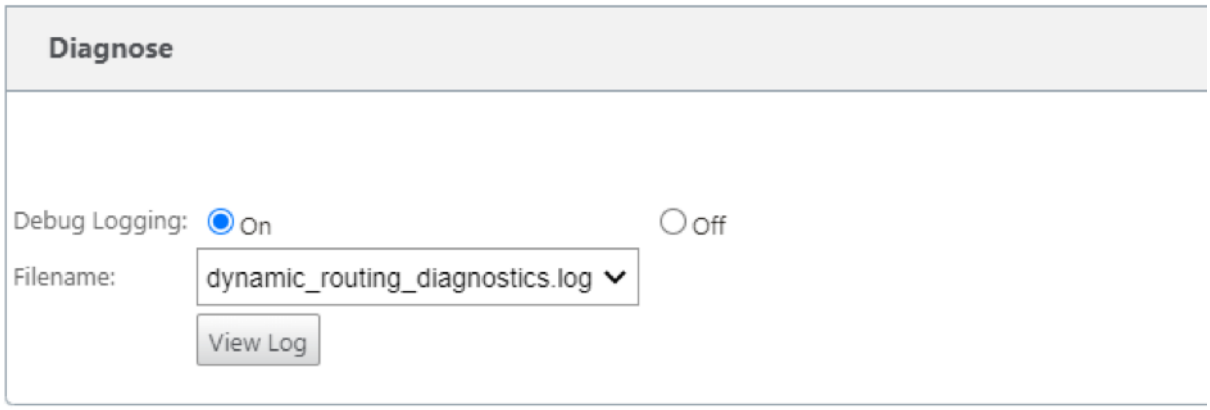
BGP ソフトリセット拡張機能は、格納されているルーティングテーブルの更新情報に依存しない着信 BGP ルーティングテーブルアップデートのダイナミックソフトリセットを自動的にサポートします。

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。



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。



iBGP

August 30, 2022

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トポロジー内の複数の 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

August 30, 2022

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

仮想 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た場合に、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学習を提供します。

アプリケーションルート

August 30, 2022

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と、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、仮想パス間の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

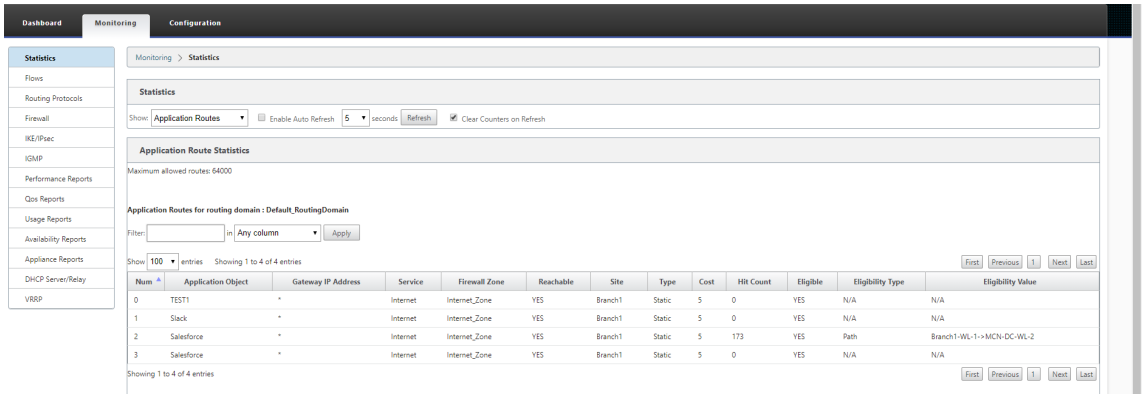
ク（2 つの SD-WAN アプライアンス間のトラフィックが設定されたしきい値に達した場合のみ存在）のいずれかになります。

- 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、仮想パスを介した伝送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 > 統計情報へのナビゲート。
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によって使用される Gateway 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るサービスタイプ。
- ファイアウォールゾーン: このルートが該当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**: ルートがスタティックかダイナミックかを示します。
- コスト: ルートの優先順位。
- **Hit Count**: トラフィックを操縦するためにアプリケーションルートが使用された回数。
- 適格: アプリケーションルートはトラフィックを送信する資格があるか。
- 適格性タイプ: このルートに適用されるルート適格条件のタイプ。適格性タイプは、パス、ゲートウェイ、またはトンネルです。
- 適格性値: ルート適格条件に指定された値。

> 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

August 30, 2022

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。

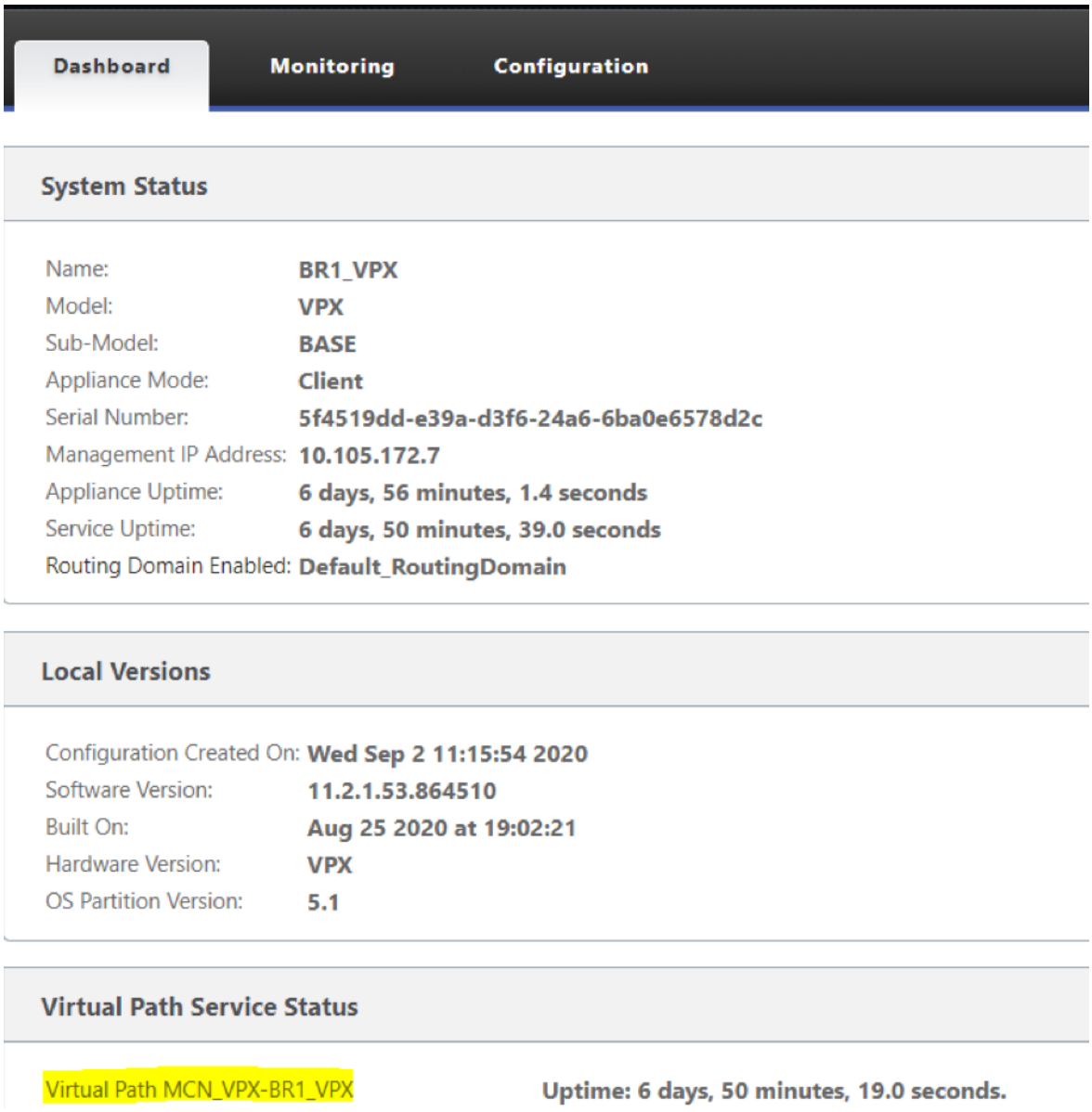
ルート集約

August 30, 2022

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。

トラブルシューティング

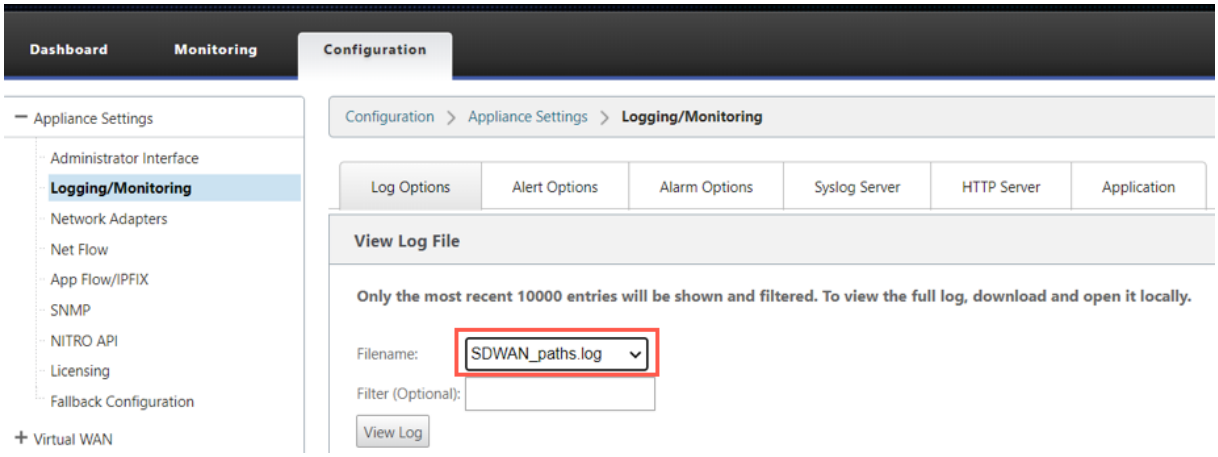
MCN で設定された集約ルートは、仮想パスを経由してブランチに送信されます。ブランチのルートテーブルに仮想パスの詳細が表示されない場合は、ブランチダッシュボードを確認します。ダッシュボードには、MCN とブランチ間の仮想パスのステータスが表示されます。



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

August 30, 2022

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。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。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

August 30, 2022

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。

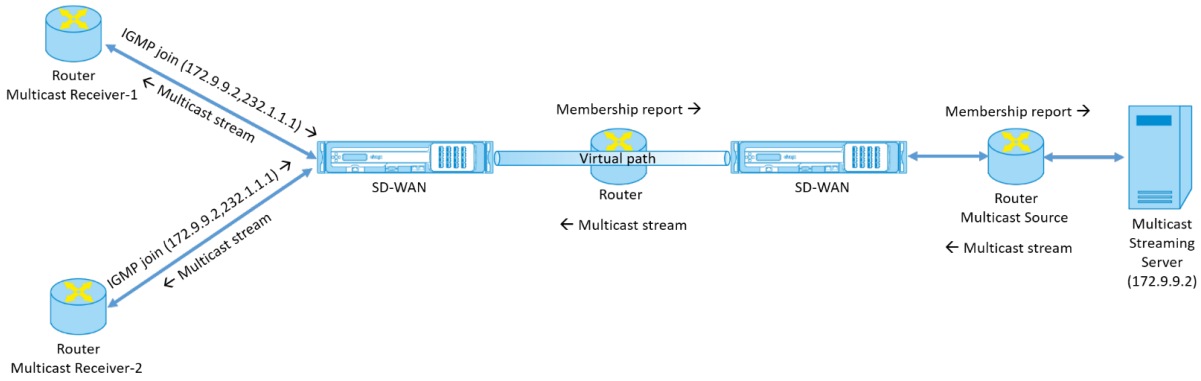
送信元固有のマルチキャスト

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ッ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 要求をリッスンし、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。

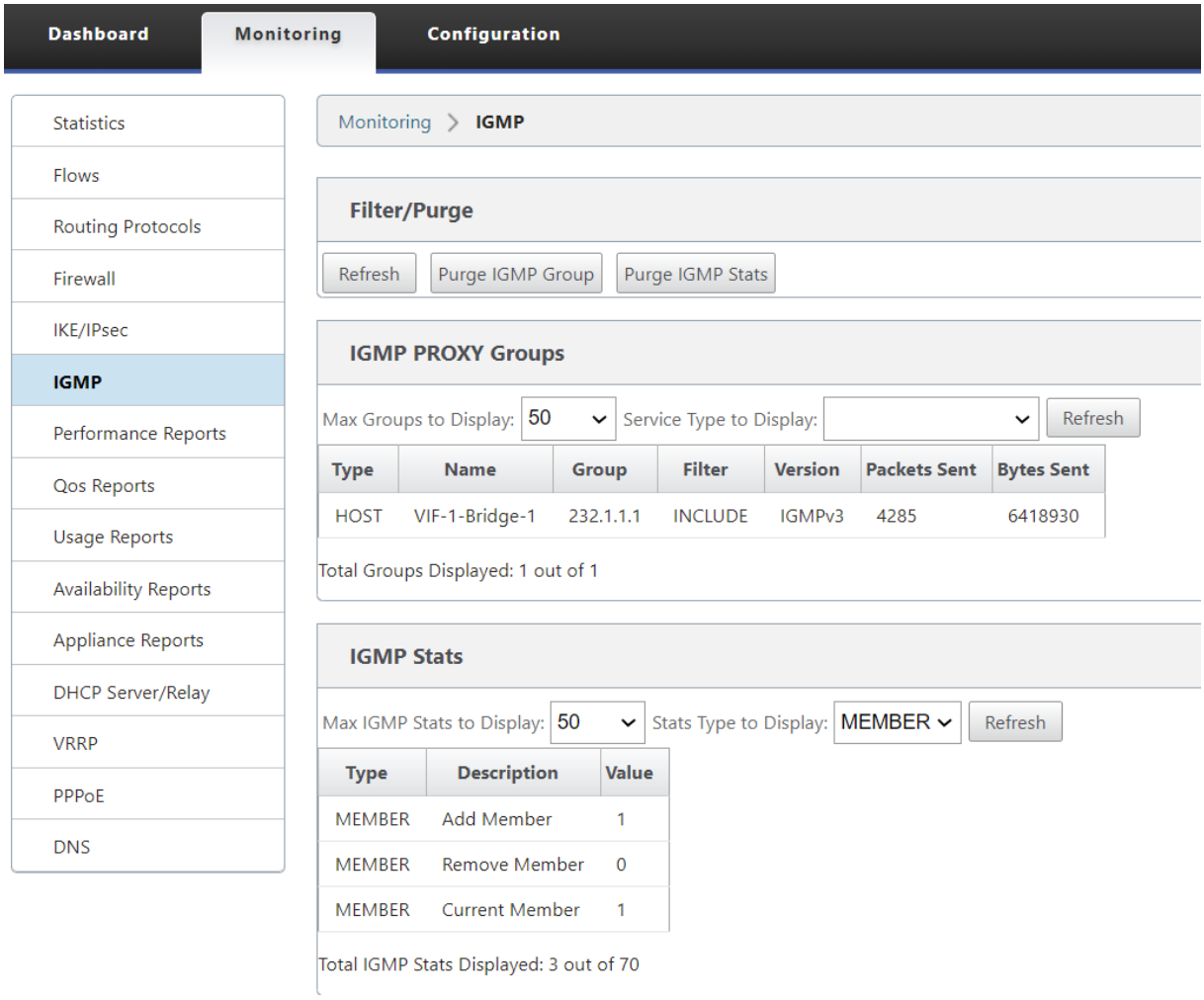
1. マルチキャストグループの作成：マルチキャストグループの名前と IP アドレスを指定します。マルチキャストグループ IP は、送信元固有のマルチキャストに対して 232.0.0.0/8 の範囲内にある必要があります。
2. IGMP プロキシを有効にする—Citrix SD-WAN アプライアンスを IGMP プロキシとして構成し、マルチキャストルーティング用の IGMP 制御チャネル情報を伝送できます。IGMP V3 は、単一送信元マルチキャストに必要です。
3. アップストリームおよびダウンストリームサービスの定義：アップストリームインターフェイスにより、IGMP PROXY は、トラ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。
   アップストリームサービスとダウンストリームサービスは、ソースのアプライアンスと宛先のアプライアンスで異なります。

監視

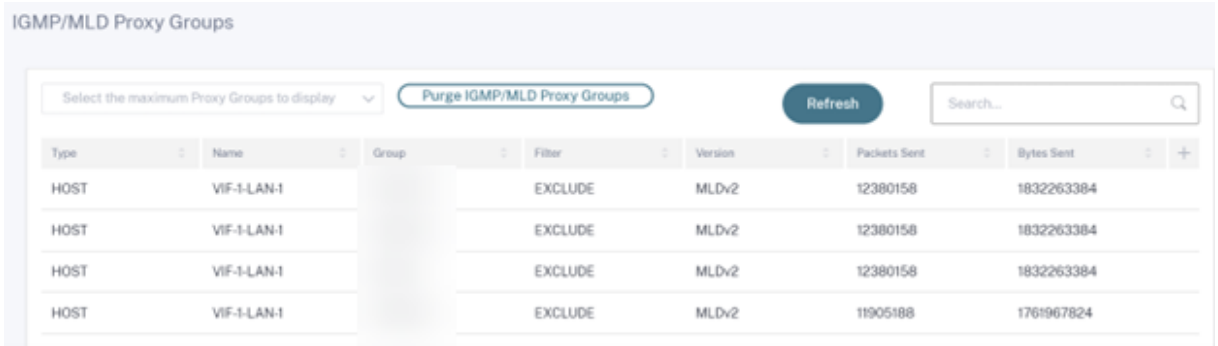
IGMP 統計情報

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、MLD 加入が開始され、メッセージタイプ RECV がマルチキャストグループアドレスの受信に使用されることを示しています。また、以下の IGMP/MLD メッセージの統計情報も確認できます。



次の図は、IGMP/MLD プロキシグループに関する情報を示しています。また、IGMP/MLD プロキシグループの統計情報と使用されているバージョンも確認できます。



仮想パスルートコストの構成

August 30, 2022

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。これまでは、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。

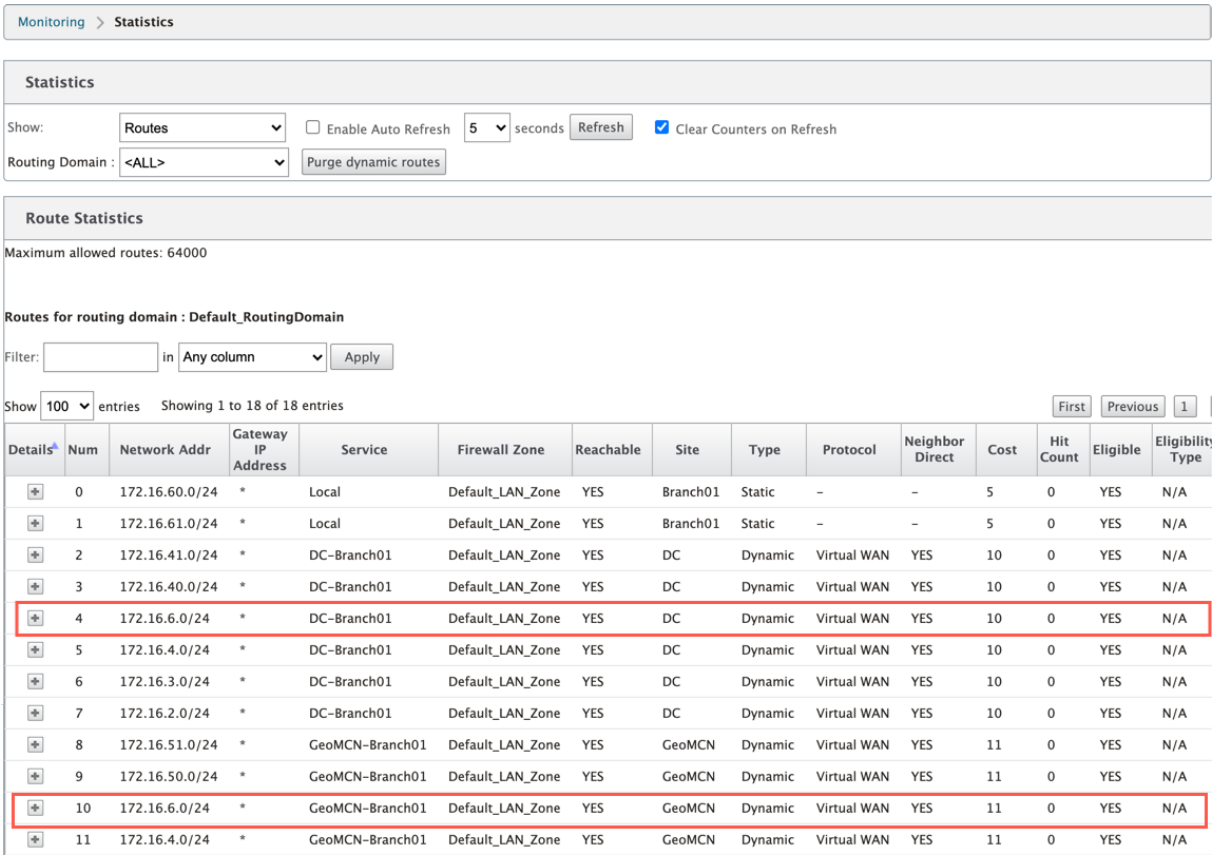
> 注
>
> VP ルートコストは、リリースバージョン 10.0 より前のリリースバージョンに存在した WAN から WAN への転送コストを非推奨にします。WAN から WAN への転送コストに基づくルーティング決定は、VP ルートコストを使用して再影響を受ける必要があります。リリースバージョン 10.0 に移行すると、WAN から WAN への転送コストは重要ではないためです。

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。



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

仮想ルータの冗長性プロトコルの構成

August 30, 2022

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。

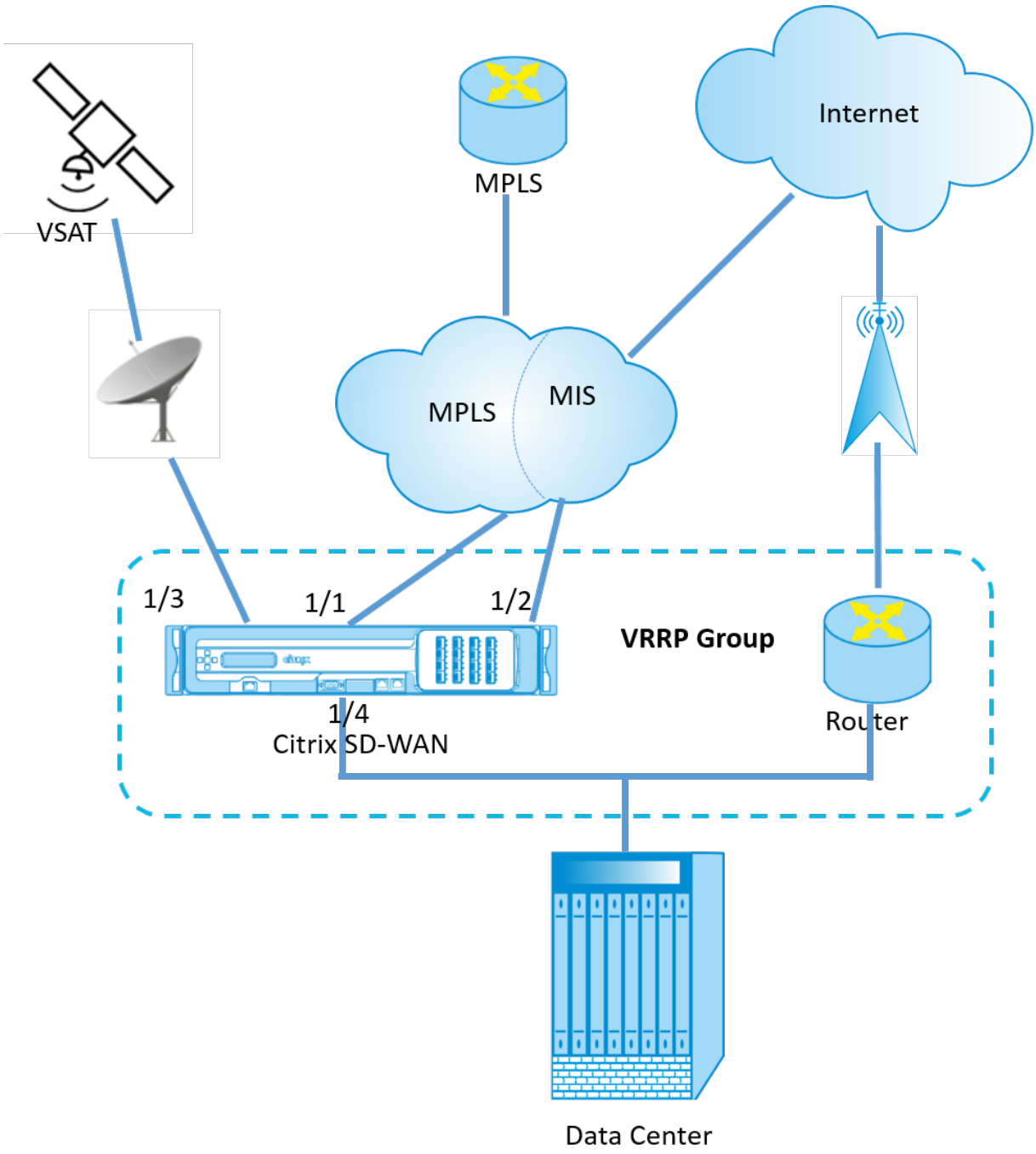
プライマリ/マスタールータに障害が発生すると、バックアップルータが自動的に引き継ぎます。VRRP 設定では、マスタールータは、アドバタイズメントと呼ばれる VRRP パケットをバックアップルータに送信します。マスタールータがアドバタイズメントの送信を停止すると、バックアップルータはインターバルタイマーを設定します。この保留期間内にアドバタイズメントが受信されない場合、バックアップルータはフェールオーバールーチンを開始します。

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。

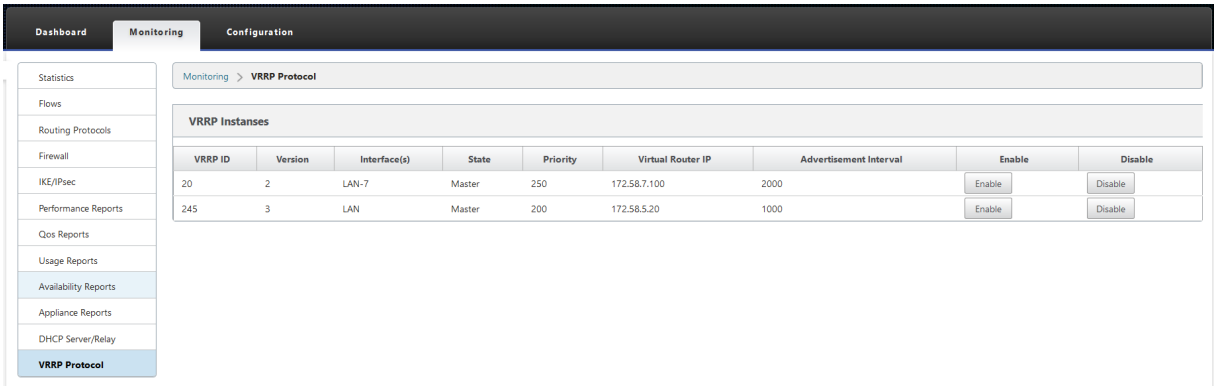
Citrix SD-WAN リリースバージョン 10.1 では、VRRP バージョン 2 およびバージョン 3 がサポートされ、サードパーティ製のルーターとの相互動作が可能です。SD-WAN アプライアンスはマスタールータとして機能し、サイト間で仮想パスサービスを使用するようにトラフィックを誘導します。仮想インターフェイス IP を VRRP IP として設定し、手動でプライオリティをピアルータよりも高い値に設定することで、SD-WAN アプライアンスを VRRP マスターとして設定できます。アドバタイズメント間隔と preempt オプションを設定できます。

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 統計情報

VRRP 統計は、[監視] > [**VRRP**] で確認できます。



次の統計データを表示できます。

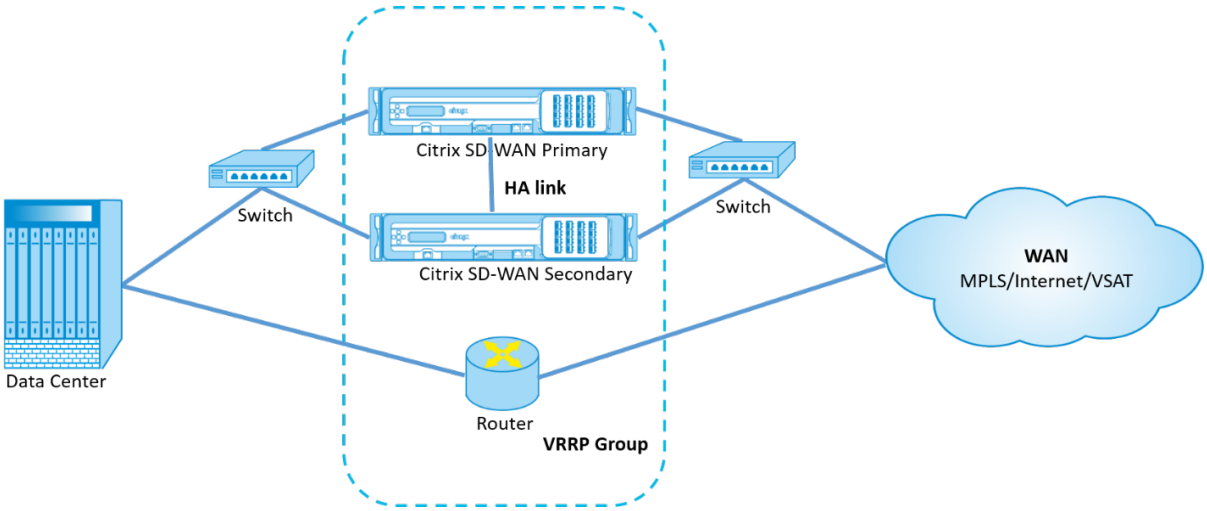
- **VRRP ID:** VRRP グループ ID
- バージョン**:** VRRP プロトコルのバージョン。
- インターフェイス： VRRP に使用される仮想インターフェイス。
- 状態**:** SD-WAN アプライアンスの VRRP 状態。アプライアンスがマスターかバックアップかを示します。
- 優先順位**:** VRRP グループに対する SD-WAN アプライアンスの優先順位
- 仮想ルータ **IP**： VRRP グループの仮想ルータ IP アドレス。
- アドバタイズメント間隔： VRRP アドバタイズメントの頻度。
- 有効**:** SD-WAN アプライアンスで VRRP インスタンスを有効にする場合に選択します。
- 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に選択します。

制限事項

- VRRP は、Gateway 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。

高可用性展開モードの詳細については、「高可用性」を参照してください。

LAN セグメンテーションのルーティングサポート

August 30, 2022

SD-WAN Standard 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に 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 側の VLAN を認識して記録を維持し、別の SD-WAN Standard Edition アプライアンスを使用してリモートロケーションで他の LAN セグメント（VLAN）に接続できる他の 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 Edition アプライアンスで維持される仮想ルーティングおよび転送（VRF）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 セグメントがアクセスできるリモート 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。

ルーティング間ドメインサービス

August 30, 2022

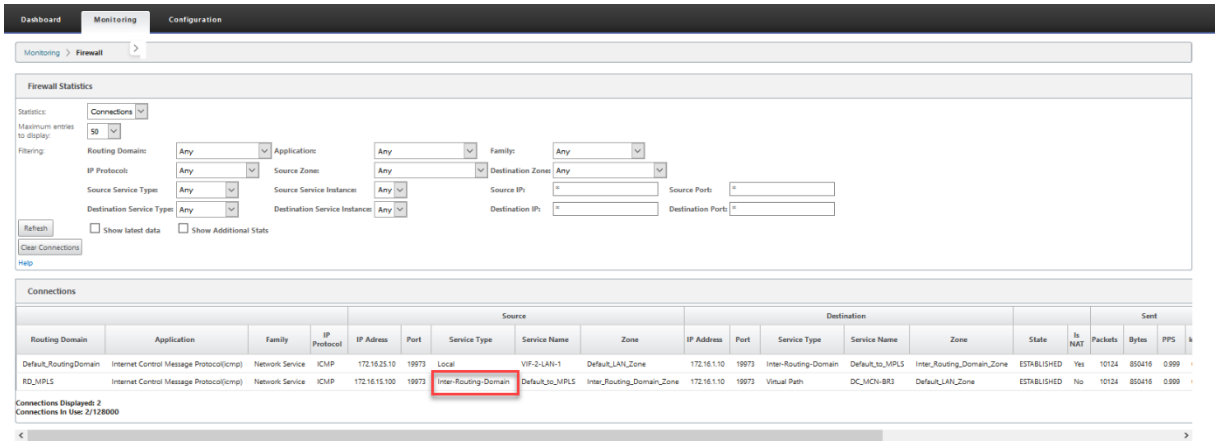
Citrix SD-WAN を使用すると、ルーティングドメインを使用してネットワークをセグメント化できるため、高いセキュリティと容易な管理が可能になります。ルーティングドメインを使用すると、トラフィックはオーバーレイネットワーク内で互いに隔離されます。各ルーティングドメインは、独自のルーティングテーブルを保持します。ただし、ルーティングドメイン間でトラフィックをルーティングする必要がある場合もあります。たとえば、プリンタ、スキャナ、メールサーバーなどの共有サービスが、個別のルーティングドメインとしてプロビジョニングされる場合などです。ルーティング間ドメインは、異なるルーティングドメインのユーザ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。

監視

ルーティングドメイン間サービスを使用する接続のモニタリング統計情報は、[モニタリング] > [ファイアウォール統計] > [接続] で確認できます。



ECMP 負荷分散

August 30, 2022

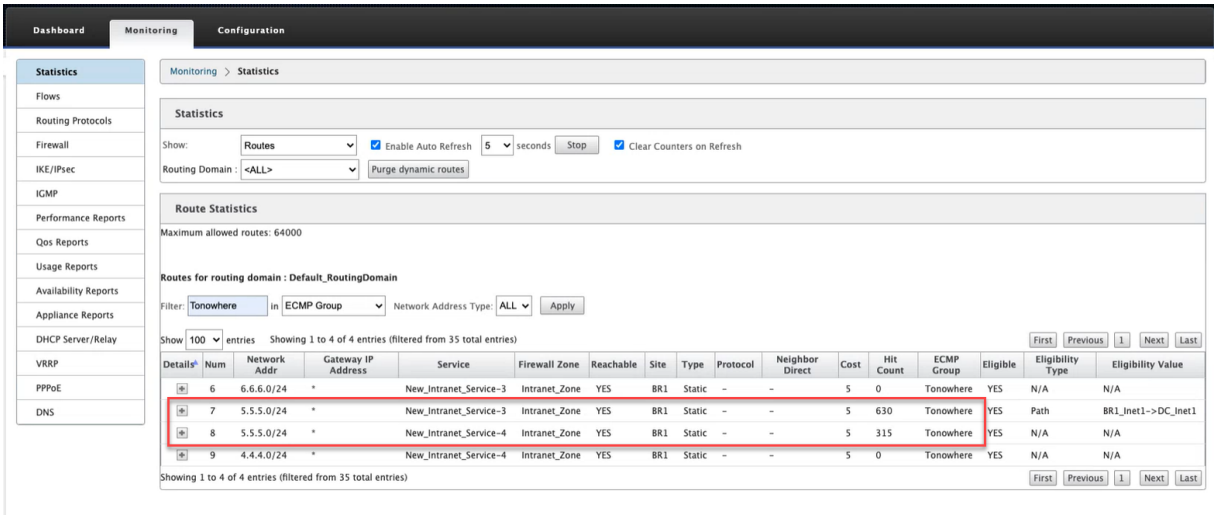
ECMP（等コストマルチパス）グループを使用すると、同じコスト、宛先、サービスで複数のパスをグループ化できます。接続またはセッション・データは、ECMP グループのタイプに応じて、ECMP グループ内のすべてのパスでロード・バランシングされます。たとえば、同じルートコストを持つブランチとデータセンターの間に 2 つの WAN リンクを持つネットワークがあるとします。従来、WAN リンクの 1 つはアクティブで、もう 1 つはフォールバックリンクとして機能している状態のままでした。ECMP グループを使用すると、これらの WAN リンクをグループ化して、両方の WAN リンクを通じてトラフィック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 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。



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。

セキュリティ

August 30, 2022

このセクションのトピックでは、Citrix SD-WAN 展開の一般的なセキュリティガイダンスについて説明します。

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

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。

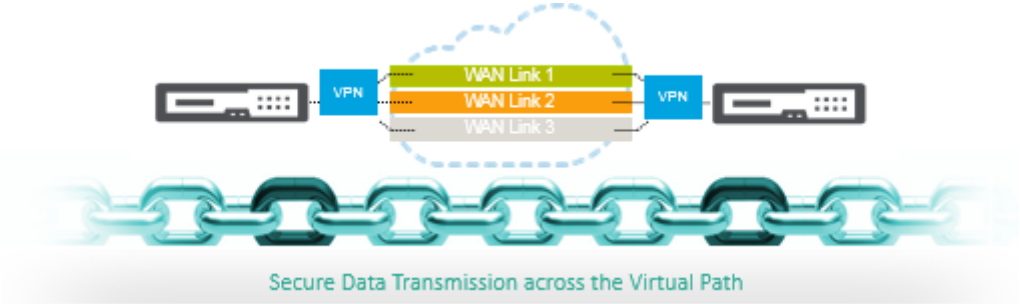
- IPSec トンネル
- Firewall

IPsec トンネル終了

August 30, 2022

Citrix SD-WAN は IPsec 仮想パスをサポートし、サードパーティデバイスが Citrix SD-WAN WAN アプライアンスの LAN 側または WAN 側で IPsec VPN トンネルを終了できるようにします。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。



> 重要な注意:
>
> - SD-WAN 11.5 リリース以降、すべての IPsec トンネル構成と IKE 設定は、Citrix SD-WAN Orchestrator サービスを介してのみサポートされます。Citrix SD-WAN Orchestrator サービス IPsec/IKE 構成の詳細については、「IPsec サービス」を参照してください。
> - 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。

Citrix SD-WAN と AWS トランジットゲートウェイとの統合

November 17, 2022

Amazon Web Service (AWS) Transit Gateway サービスを使用すると、Amazon Virtual Private Clouds (VPC) とオンプレミスネットワークを単一の Gateway 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、セントラルゲートウェイからネットワーク上の各 Amazon VPC、オンプレミスデータセンター、またはリモートオフィスへの単一の接続を作成して管理するだけで済みます。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 Transit Gateway 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 Transit Gateway に接続され、Transit Gateway 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 Transit Gateway** ネットワークマネージャーはこのパラダイムを変えます。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 Transit Gateway とともに使用できるようになりました。これにより、Transit Gateway 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 Transit Gateway（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 Transit Gateway 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 Gateway プロトコル（BGP）ピアリングを確立し、Transit Gateway に接続されたネットワーク（VPC）を学習します。

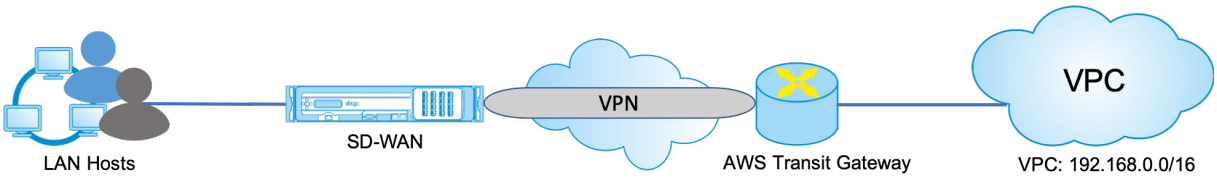
使用例

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 Transit Gateway 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。

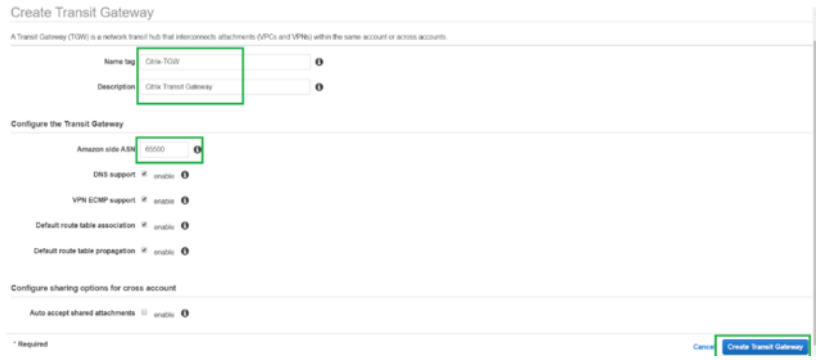
どちらの方法を選択しても、トラフィックは、AWS インフラストラクチャ内のルーティングを手動で管理することなく、Transit Gateway に接続されている VPC に到達します。



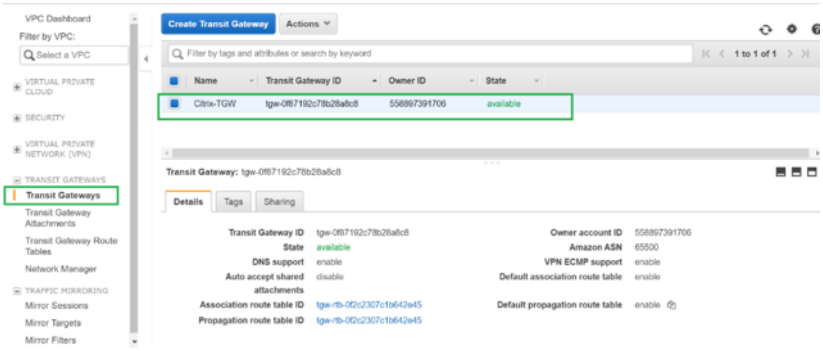
AWS Transit Gateway の設定

AWS Transit Gateway を作成するには、VPC ダッシュボードに移動して、**Transit Gateway** セクションに移動します。

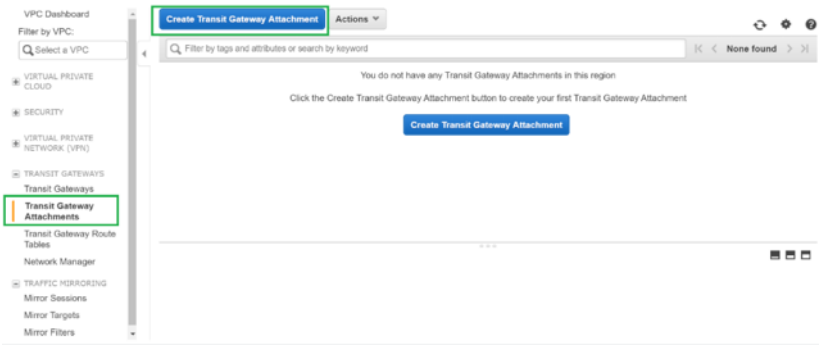
1. 次のスクリーンショットで強調表示されているように、Transit Gateway 名、説明、および Amazon ASN 番号を入力し、[**Create Transit Gateway**] をクリックします。



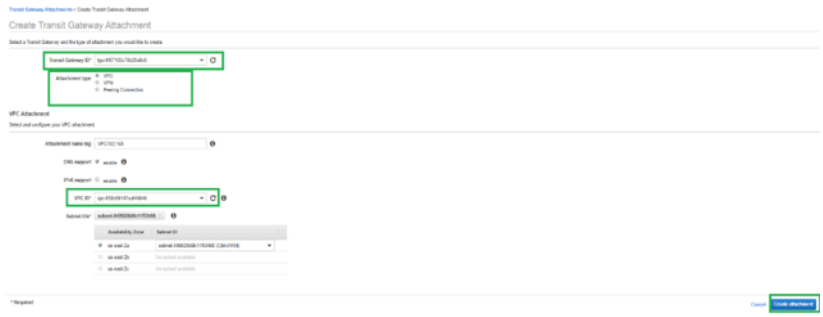
Transit Gateway の作成が完了すると、ステータスが [使用可能] として表示されます。



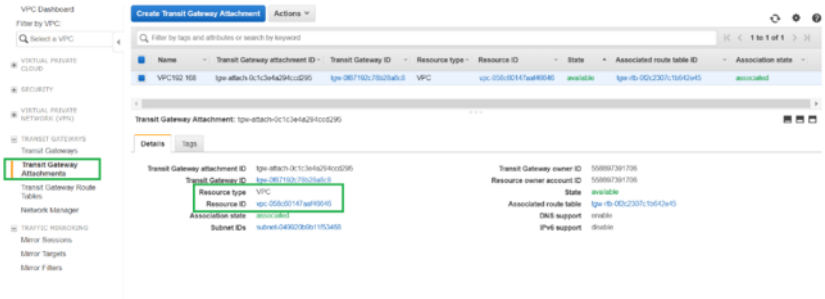
2. **Transit Gateway** 添付ファイルを作成するには、[Transit Gateway] **> [Transit Gateway** 添付ファイル] に移動し、[**Transit Gateway** 添付ファイルの作成] をクリックします。



3. ドロップダウンリストで作成した Transit Gateway を選択し、アタッチメントタイプとして **VPC** を選択します。添付ファイル名タグを指定し、作成した Transit Gateway 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。[アタッチメントの作成] をクリックして、VPC を Transit Gateway にアタッチします。

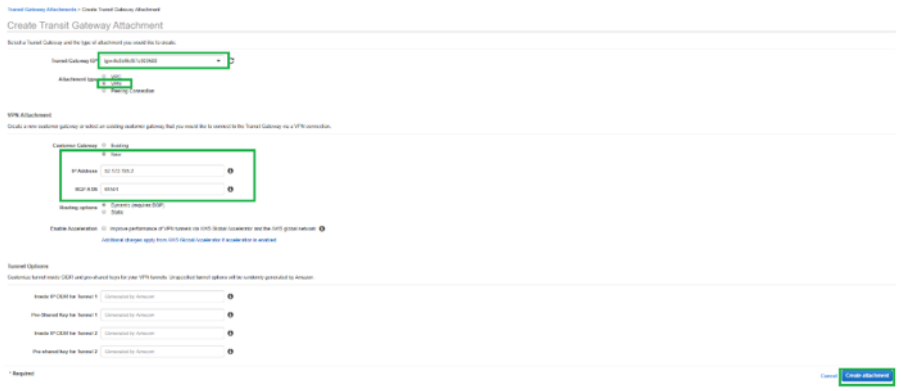


4. VPC を Transit Gateway にアタッチすると、リソースタイプ **VPC** がトランジットゲートウェイに関連付けられていることがわかります。

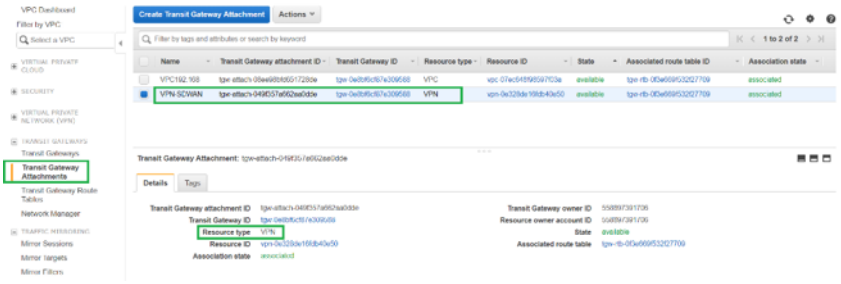


5. VPN を使用して SD-WAN を Transit Gateway に接続するには、ドロップダウンリストから [**Transit Gateway ID**] を選択し、[アタッチメントタイプ] として [**VPN**] を選択します。正しい Transit Gateway ID を選択していることを確認します。

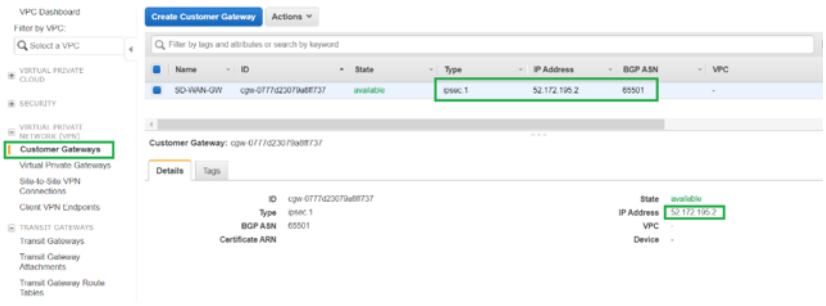
   SD-WAN リンクのパブリック IP アドレスと BGP ASN 番号を指定して、新しい VPN カスタマー Gateway を接続します。[添付ファイルの作成] をクリックして、Transit Gateway に VPN をアタッチします。



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。

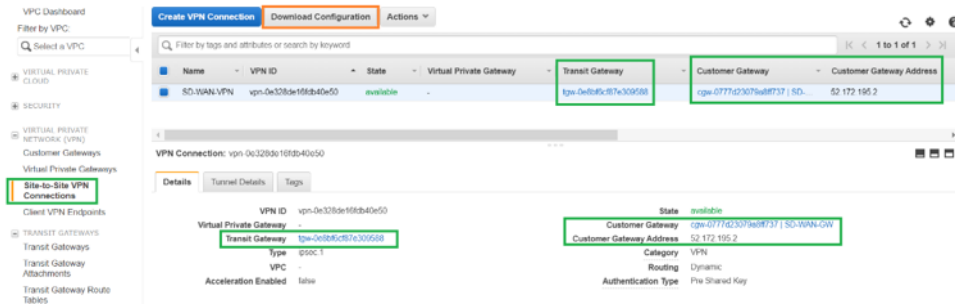


7. [カスタマー **Gateway**] では、SD-WAN カスタマー Gateway とサイト間 VPN 接続が、Transit Gateway への VPN アタッチメントの一部として作成されます。SD-WAN カスタマー Gateway が、SD-WAN の WAN リンクパブリック IP アドレスを表すこのカスタマー Gateway の IP アドレスとともに作成されていることがわかります。

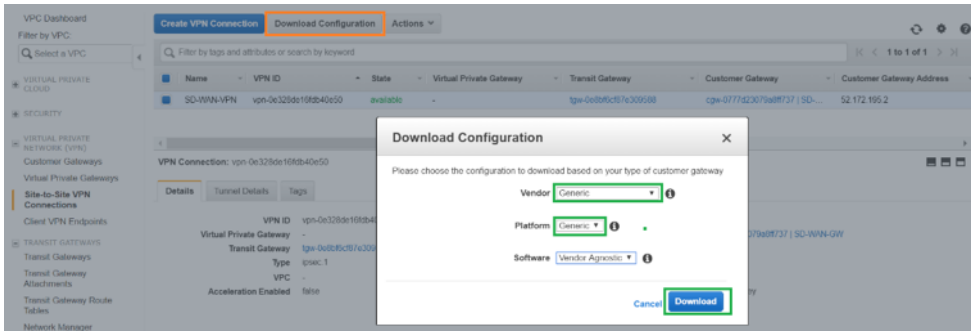


8. [サイト間 **VPN** 接続] に移動して、**SD-WAN** カスタマー **Gateway VPN** 設定をダウンロードします。この構成ファイルには、BGP ピア情報とともに 2 つの IPsec トンネル詳細があります。冗長性のために、SD-WAN から Transit Gateway への 2 つのトンネルが作成されます。

   SD-WAN リンクのパブリック IP アドレスがカスタマー Gateway 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 設定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] を [汎用]、[ソフトウェア] を [ベンダーに依存しない] として選択します。



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。

![2 つの IPsec トンネル] (/en-us/citrix-sd-wan/current-release/media/two-ipsec-tunnels.png)

SD-WAN でイントラネットサービスを構成する

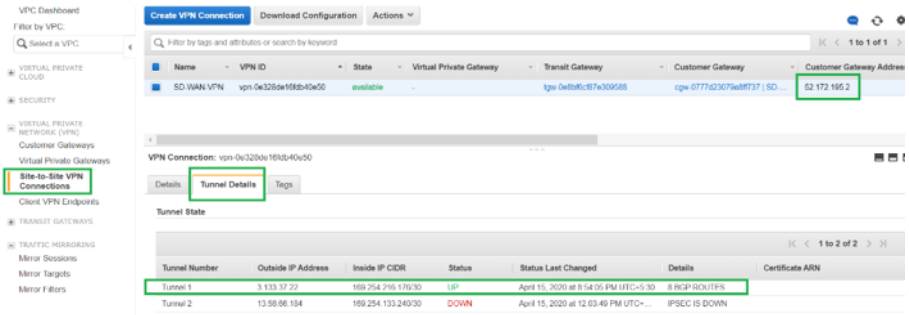
Citrix SD-WAN Orchestrator サービスを介してイントラネットサービスを構成するには、[デリバリーサービス] に移動します。

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 Gateway アドレスは、あなたがト

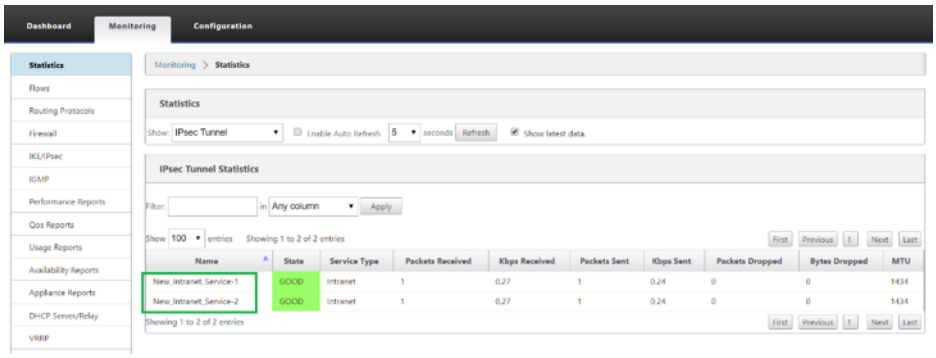
ンネルを確立している使用して SD-WAN リンクのパブリック IP アドレスを表していることを確認することができます。

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** ルートを学習したことも確認できます。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。

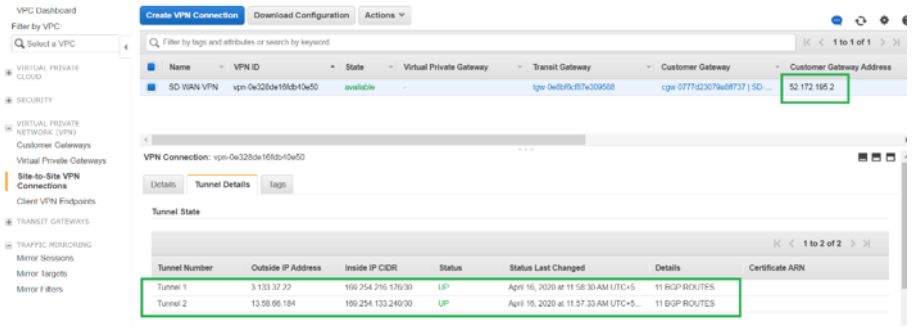


2. SD-WAN にダウンロードした構成ファイルに基づいて、2 番目のトンネルに関連する IPSec および BGP の詳細を設定します。

   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。



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。

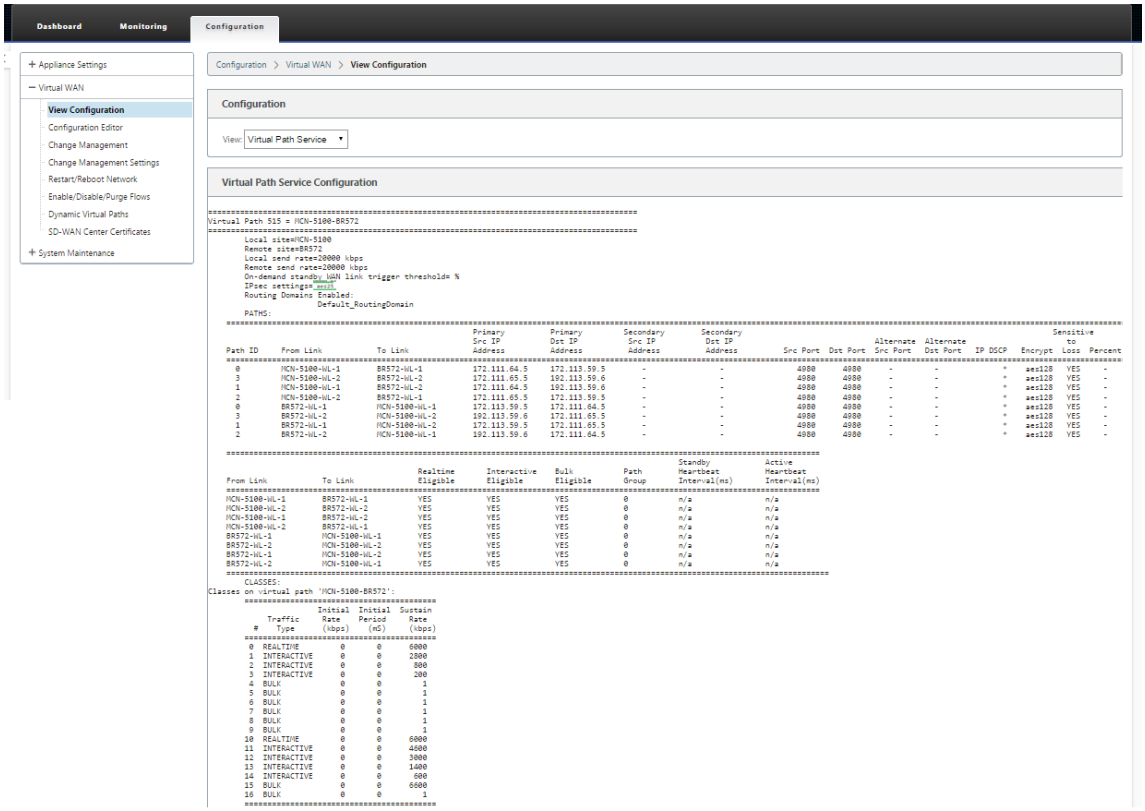


IPsec トンネルの設定を表示する方法

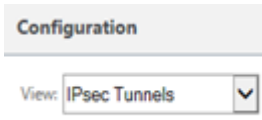
August 30, 2022

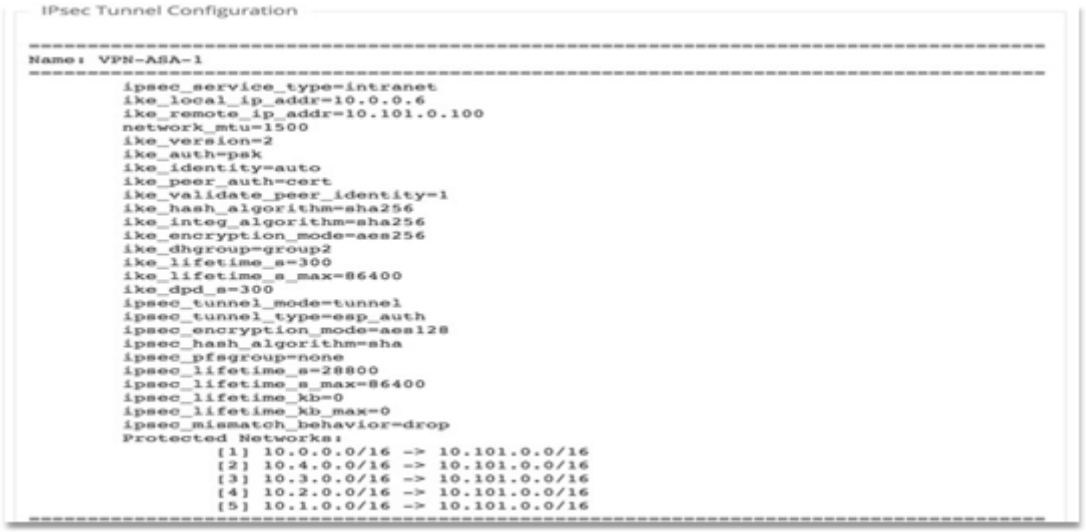
ipsec トンネルの設定を表示するには、次の手順を実行します。

1. 設定 **>** 仮想 **WAN** > ビュー設定に移動します。
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、IPsec が有効になっている場合にのみ表示されます。

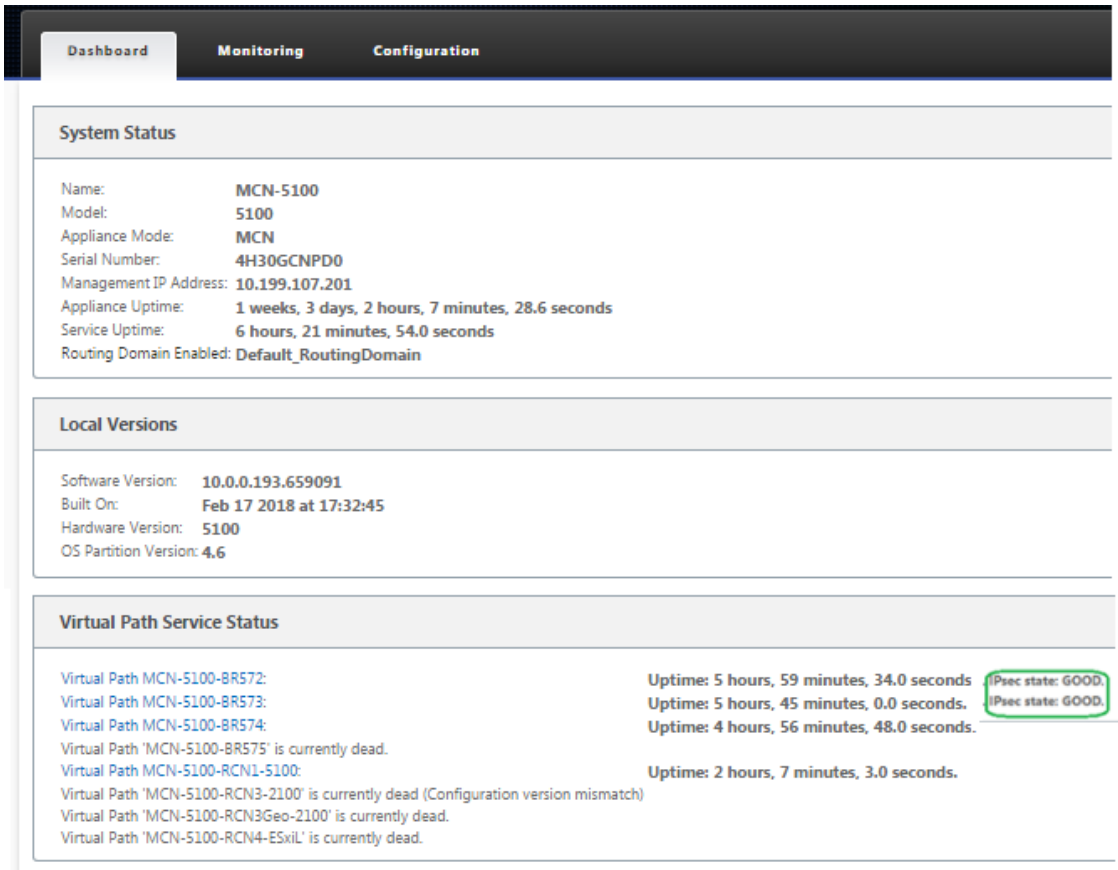


3. ドロップダウンメニューから [**IPsec** トンネル] を選択して、IPsec トンネルの構成を表示します。





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。

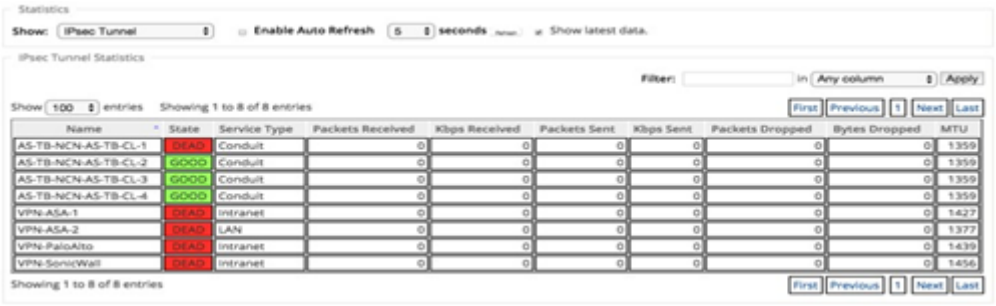


IPsec の監視とログ

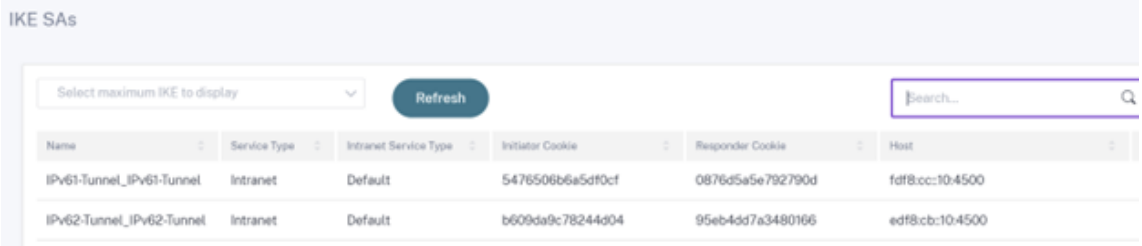
August 30, 2022

IPSec/IKE SA の統計情報を監視するには

1. [監視**] > [IPsec**] に移動します。**IPsec SA** を選択します。



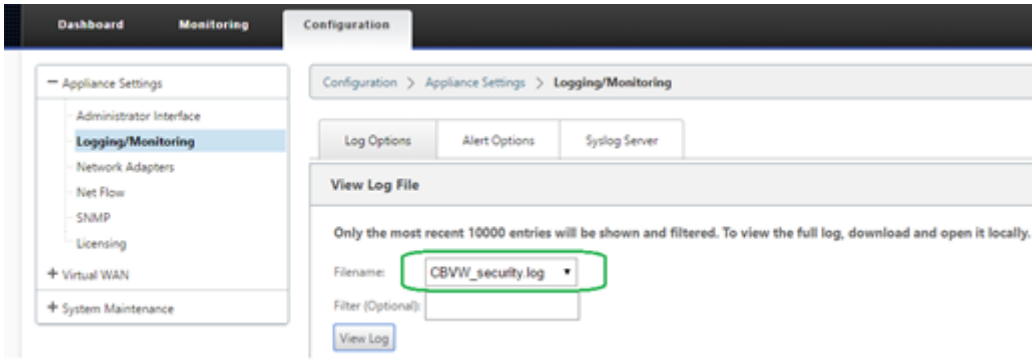
2. 監視 > **IKE SA** に移動します。設定された IPSec トンネル、SD-WAN ネットワーク内に設定された 2 つのエンドポイントまたはモード VPN エンドポイント間の IKE および IPSec サービスアソシエーションを確認します。

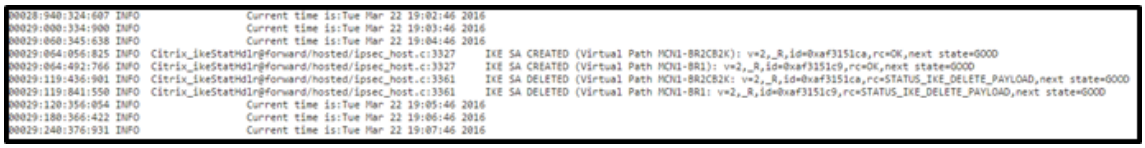


IPSec ログを監視する方法

1. 構成 > アプライアンスの設定 > ロギング/モニタリングに移動します。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。

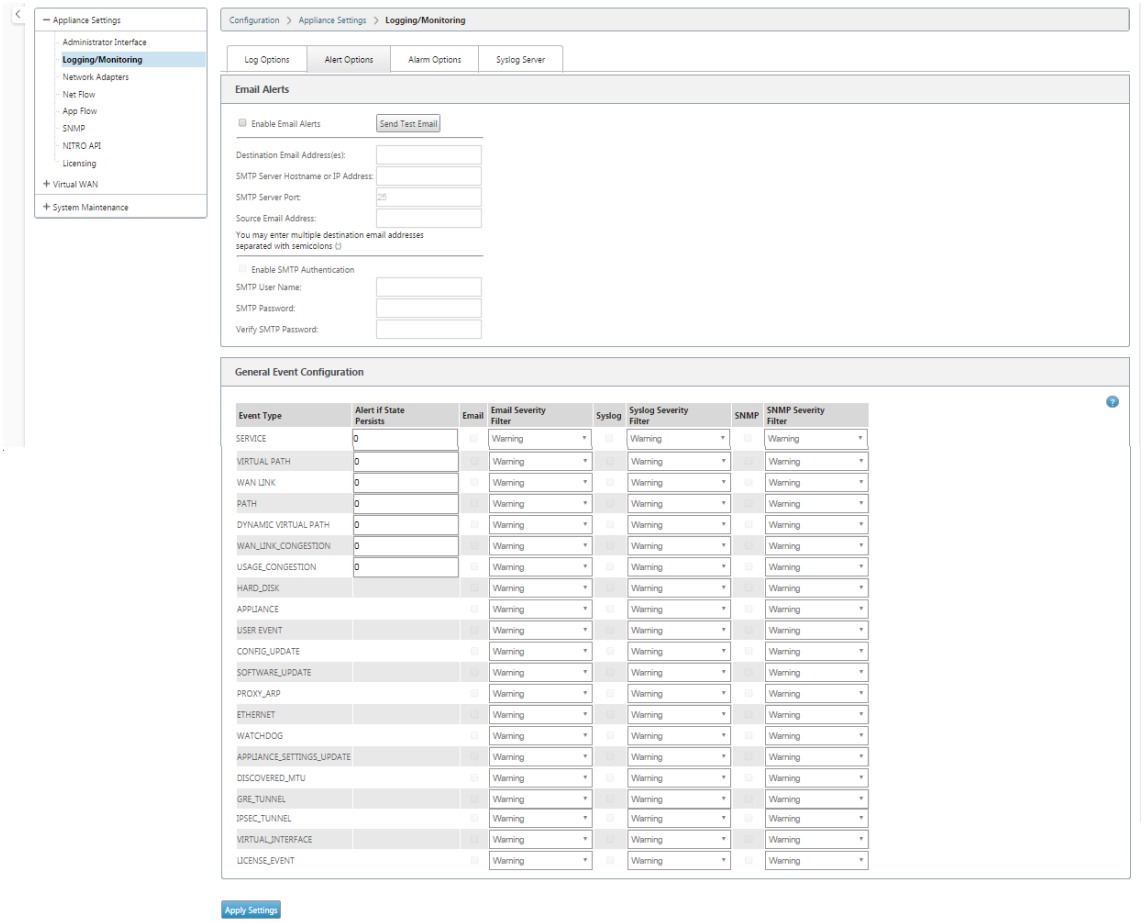
   - IPsec トンネルの作成と削除
   - IPsec トンネルステータスの変更





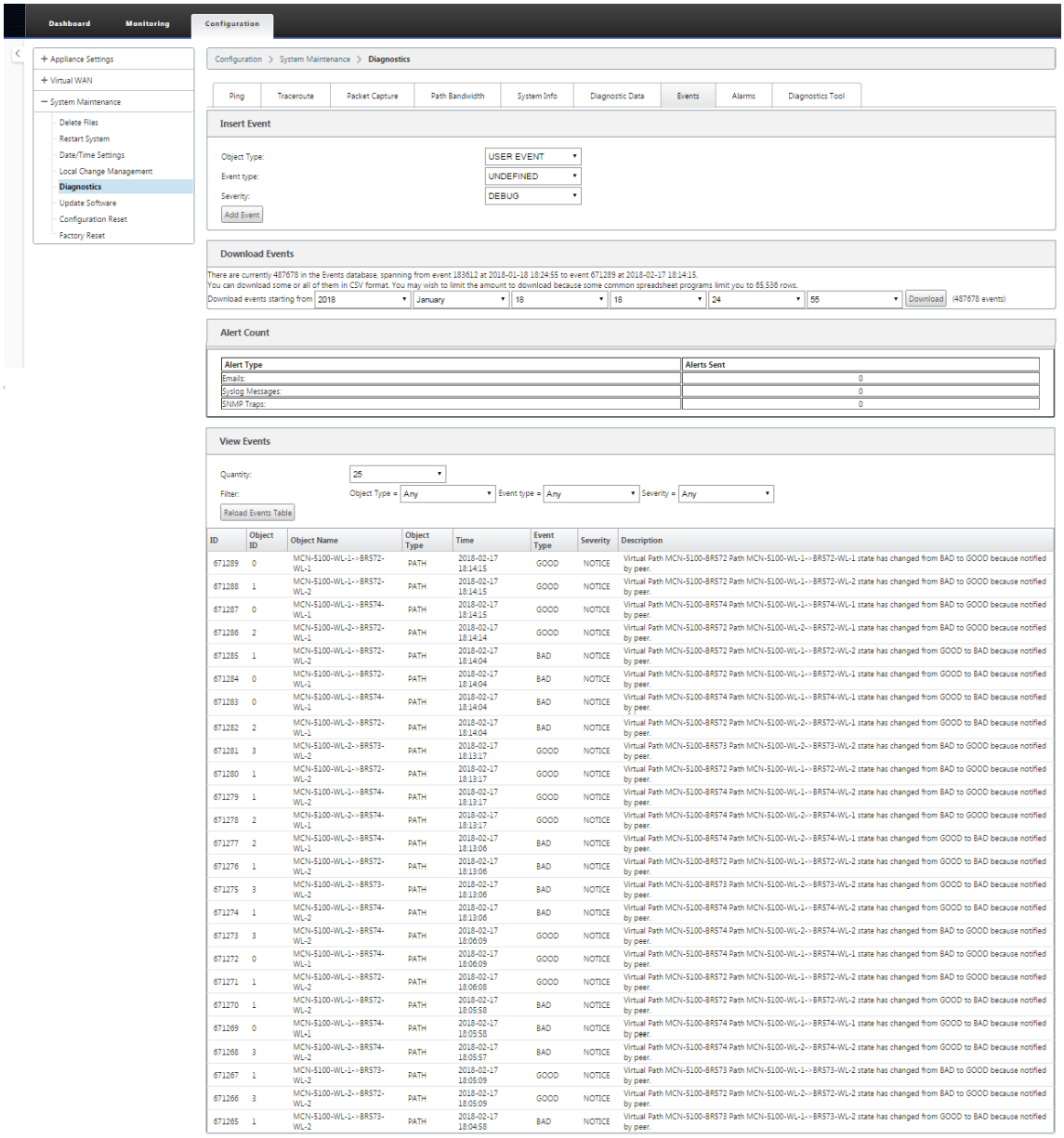
IPSec トンネル警告を表示する方法

1. 構成 > アプライアンスの設定 **>** ロギング**/**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。



IPSec トンネルイベントを監視する方法

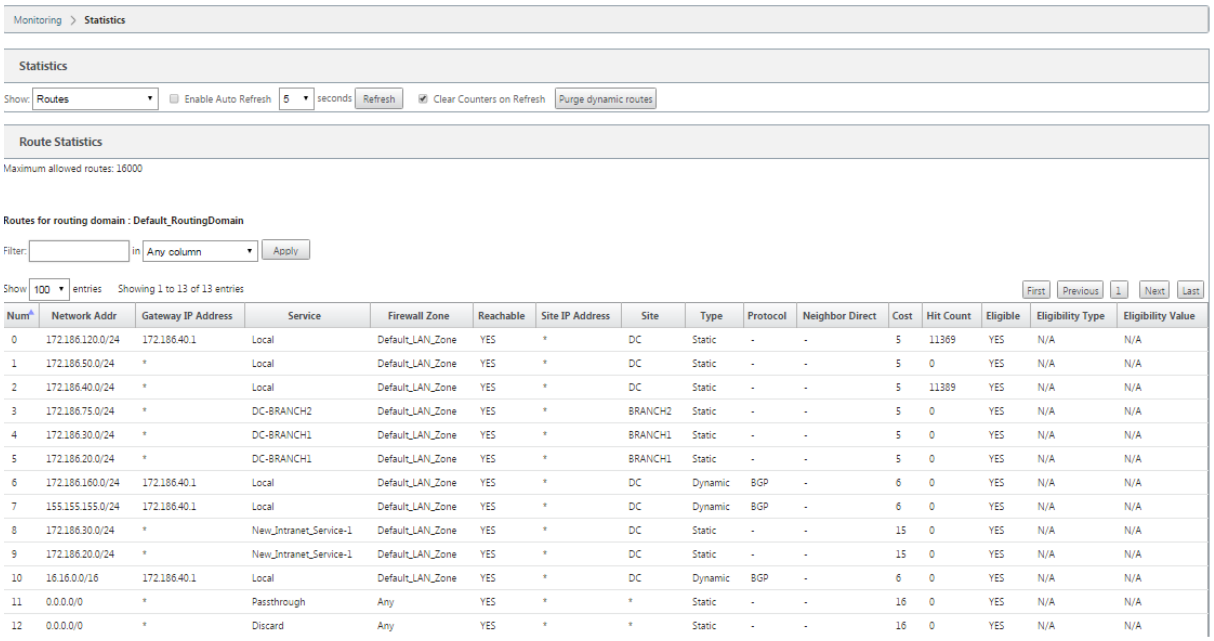
1. [構成] **>** [システムメンテナンス] **>** [診断] > [イベント] に移動します。
2. **IPSEC_TUNNEL** オブジェクトタイプに基づいてイベントを追加します。すべての IPSec 関連イベントのフィルタを作成します。



IPsec 非仮想パスルートの適格性

August 30, 2022

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。



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

FIPS 準拠

August 30, 2022

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 Orchestrator サービスを使用して FIPS コンプライアンスを有効にするには、「FIPS モード」を参照してください。

Citrix SD-WAN Secure Web Gateway

August 30, 2022

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、レイテンシーを加え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、すべての支店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 Security Platform 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。Citrix SD-WAN アプライアンスによって実行される処理にこれらのセキュリティ標準を適用するには、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、ファイアウォールのリダイレクト（宛先 NAT による透過プロキシ）機能を使用して、インターネット（HTTP および HTTPS）トラフィックをエンタープライズエッジの SD-WAN アプライアンスから Forcepoint クラウドホストセキュリティモジュールに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 17, 2022

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。

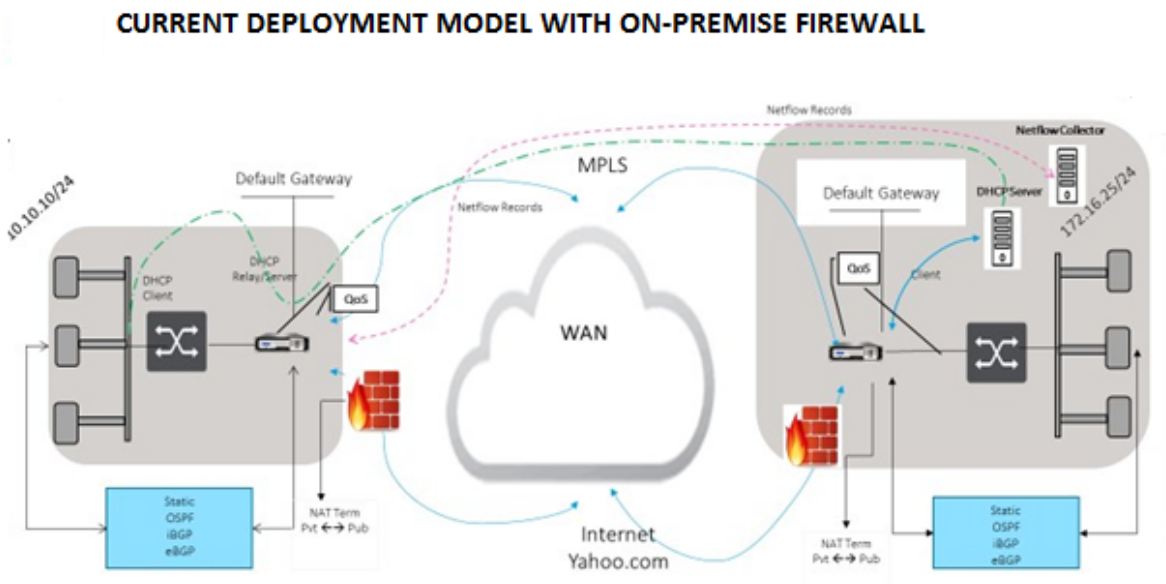
Citrix SD-WAN アプライアンスは、お客様のサイトの GRE トンネルを介して Zscaler クラウドネットワークに接続できます。SD-WAN アプライアンスを使用した Zscaler の展開では、次の機能がサポートされています。

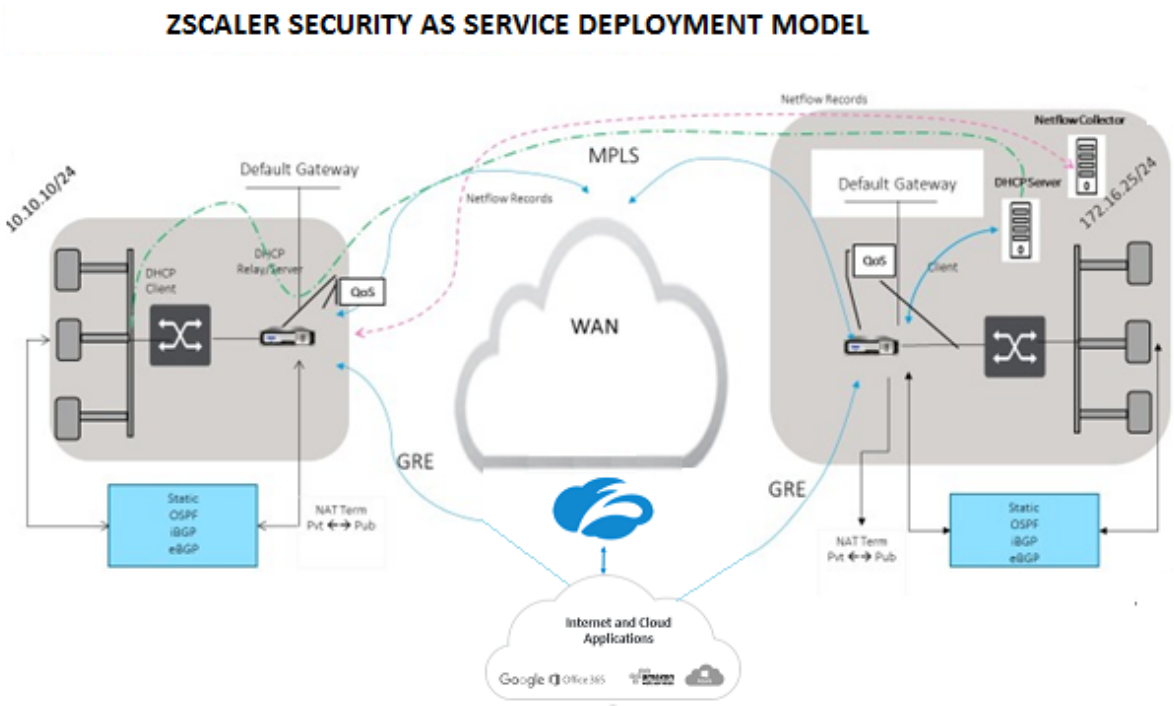
- すべての GRE トラフィックを Zscaler に転送することで、直接インターネットブレイクアウトが可能になります。
- 顧客サイトごとに Zscaler を使用した直接インターネットアクセス（DIA）。
  - 一部のサイトでは、DIA にオンプレミスのセキュリティ機器を提供し、Zscaler を使用しない場合があります。
  - 一部のサイトでは、インターネットアクセス用に別の顧客サイトへのトラフィックのバックホールを選択する場合があります。
- 仮想ルーティングと転送の展開。
- インターネットサービスの一部としての 1 つの WAN リンク。

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





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、トラフィックをリダイレクトする 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

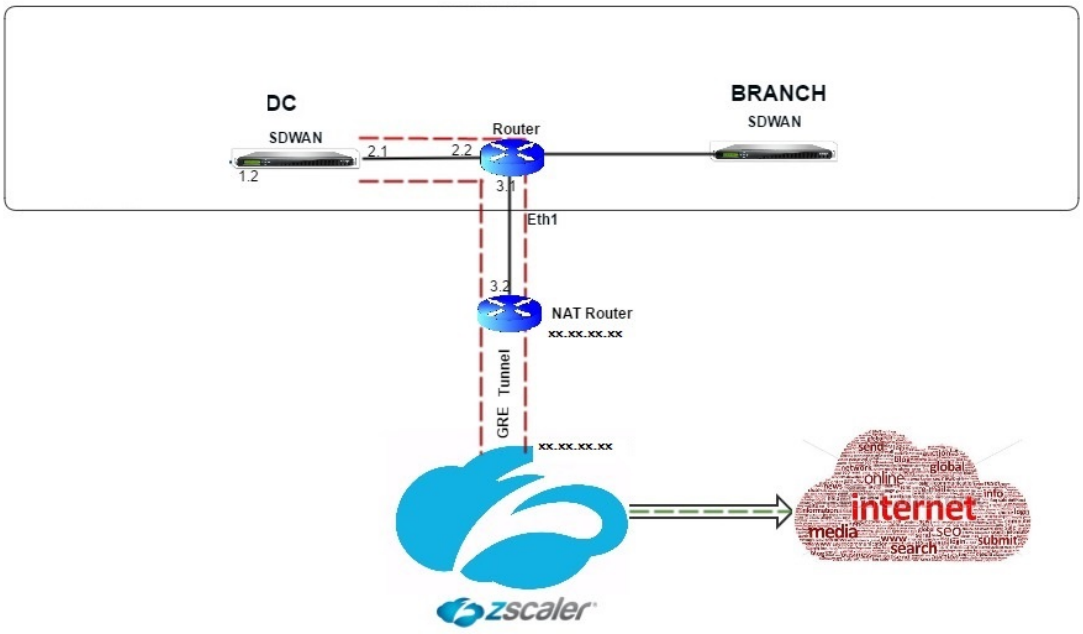
内部ルーター IP アドレス:172.17.6.245/30
内部 ZEN IP アドレス:172.17.6.246/30

インターネットサービスの設定

Citrix SD-WAN Orchestrator サービスを介してインターネットサービスを構成するには、「デリバリーサービス」を参照してください。サイトで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、「ダイレクトインターネットブレイクアウト」を参照してください。

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。



Cirix SD-WAN Orchestrator サービスを介して GRE トンネルを構成するには、GRE トンネル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。

> 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。

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

August 30, 2022

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。

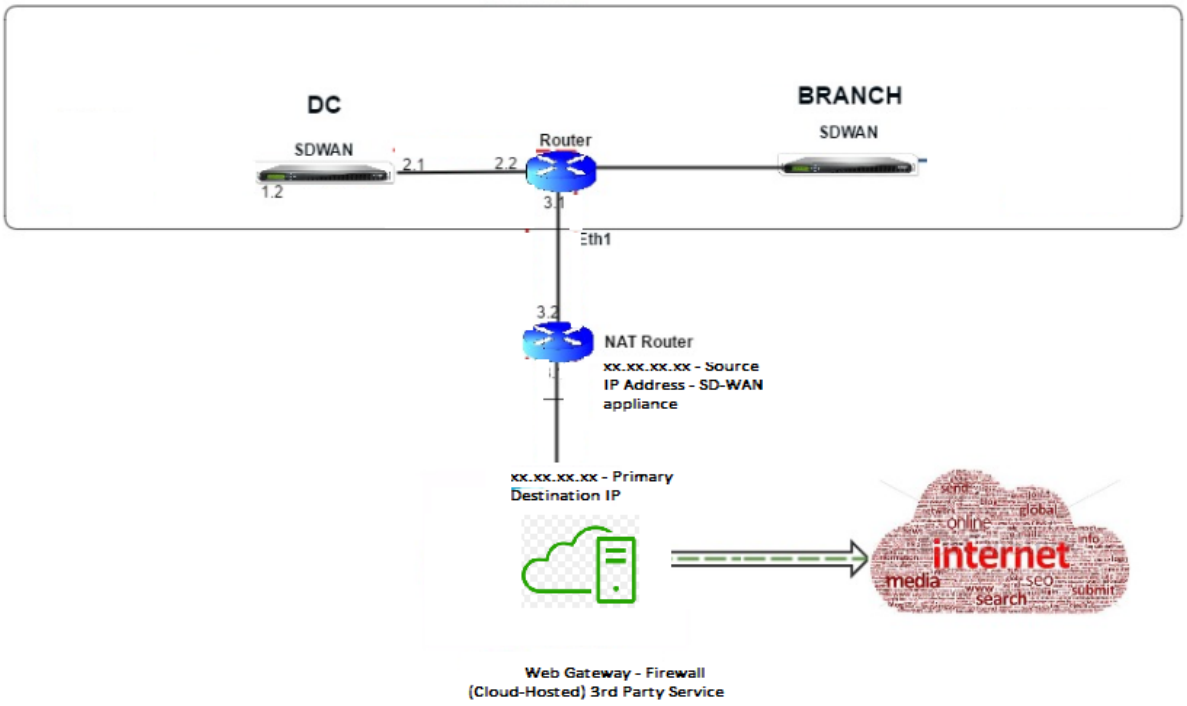
前提条件:

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。

NAT は、Citrix SD-WAN Orchestrator サービスを使用して構成できます。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。

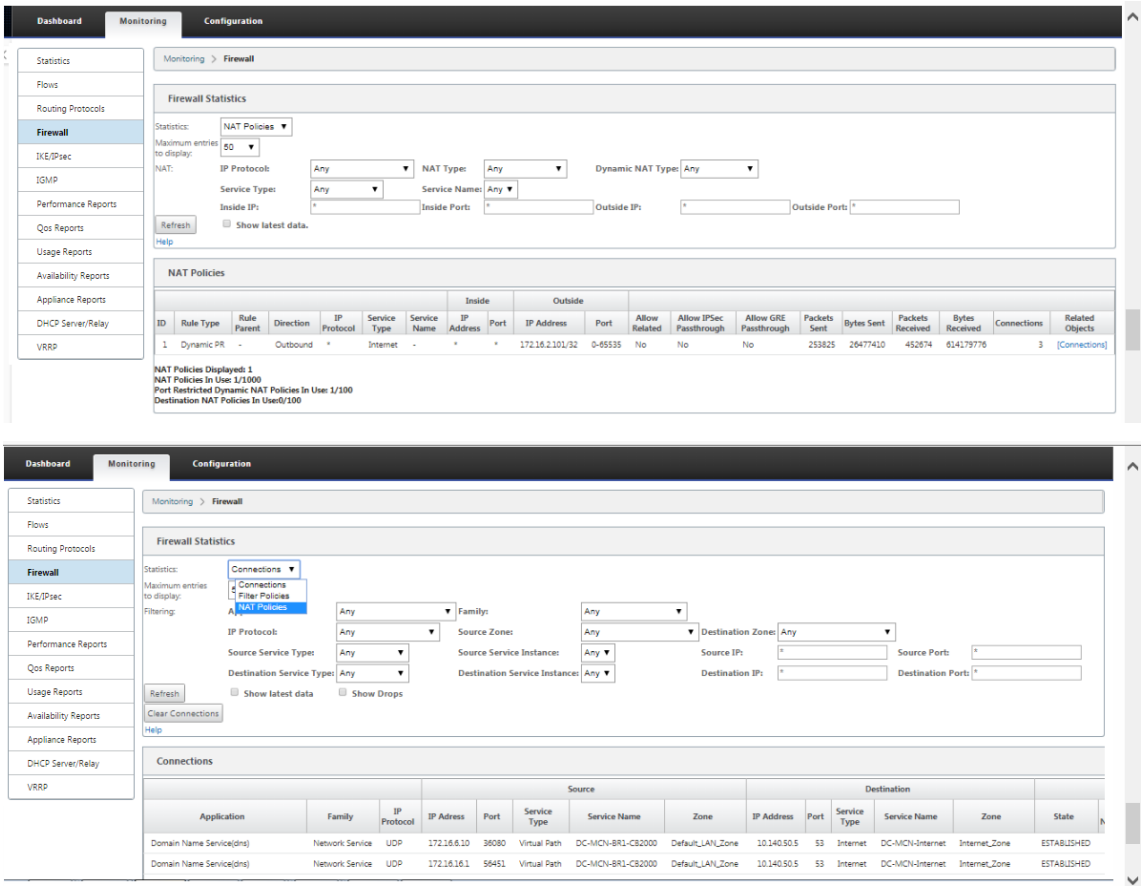


宛先 **NAT** ポリシー（ファイアウォール）のモニタリング

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。



IPsec トンネルを使用した **Palo Alto** 統合

August 30, 2022

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ドし、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の場所を簡単に追加して運用上の課題を最小限に抑える効率的な方法を提供し、これらの場所のユーザーが常に接続されて安全であることを保証します。また、Panorama からポリシーを一元管理して、リモートネットワークの一貫した合理的なセキュリティを実現できます。場所。

リモートネットワークロケーションを 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、またはサービスへの IPsec トンネルを確立できる
SD-WAN を含むサードパーティの IPSec 準拠デバイスを使用できます。

- リモートネットワーク用の Prisma アクセスサービスを計画する
- 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。

ステートフルファイアウォールと **NAT** のサポート

August 30, 2022

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）
- 複数のカスタマーに同じ 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

> 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。

グローバルファイアウォールの設定

August 30, 2022

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 Citrix SD-WAN Network 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。

ファイアウォールの詳細設定

November 17, 2022

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す。

サイトレベルでファイアウォールの詳細設定を構成するには、「ファイアウォール設定」を参照してください。

ゾーン

August 30, 2022

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。

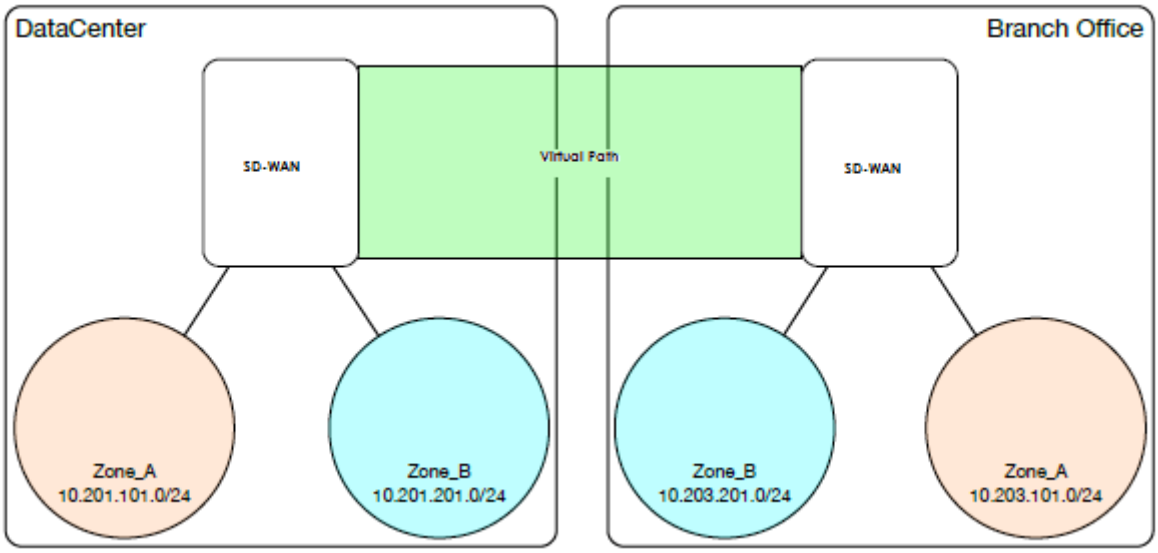
- 仮想ネットワークインターフェイス（VNI）
- イントラネットサービス
- GRE トンネル
- LAN IPsec トンネル

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。



ポリシー

August 30, 2022

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。ファイアウォールポリシーは、Citrix SD-WAN Orchestrator サービスを介して構成できます。詳細については、「ファイアウォールポリシー」を参照してください。

ネットワークアドレス変換 **(NAT)**

August 30, 2022

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 Citrix SD-WAN Orchestrator サービスを介してのみ構成できます。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。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。

静的 **NAT**

August 30, 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、同じであってはなりません。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。

IPv6 インターネットサービスのスタティック **NAT** ポリシー

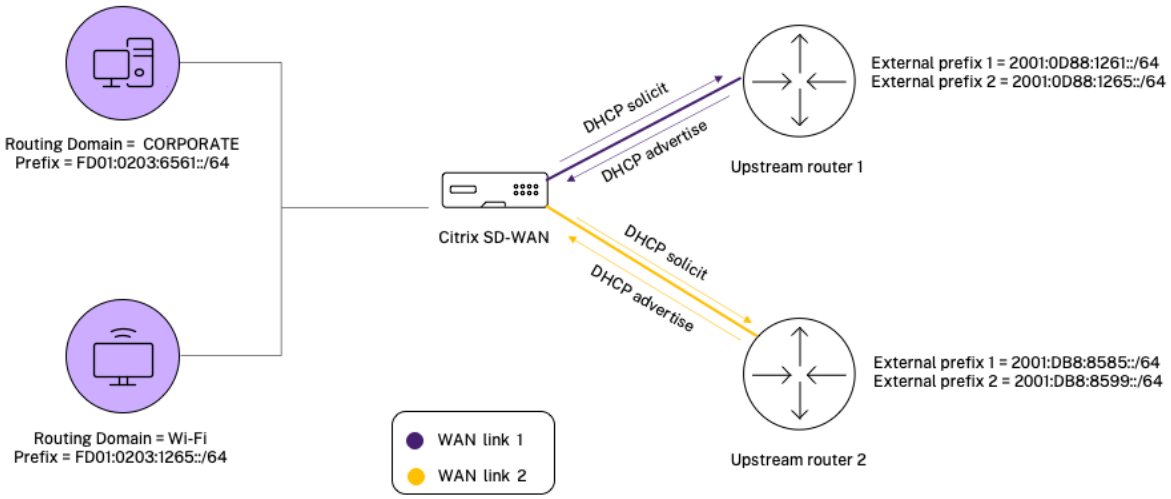
Citrix SD-WAN は、リリース 11.4.0 以降の IPv6 インターネットサービスの静的 NAT ポリシーをサポートします。IPv6 インターネットサービスのスタティック NAT ポリシーは、内部ネットワークプレフィクスと外部ネットワークプレフィクスのマッピングを指定します。必要なスタティック NAT ポリシーの数は、内部ネットワークの数と外部ネットワーク（WAN リンク）の数によって異なります。**M** 個の内部ネットワークと **N** 個の **WAN** リンクがある場合、必要なスタティック NAT ポリシーの数は **M x N** です。

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。

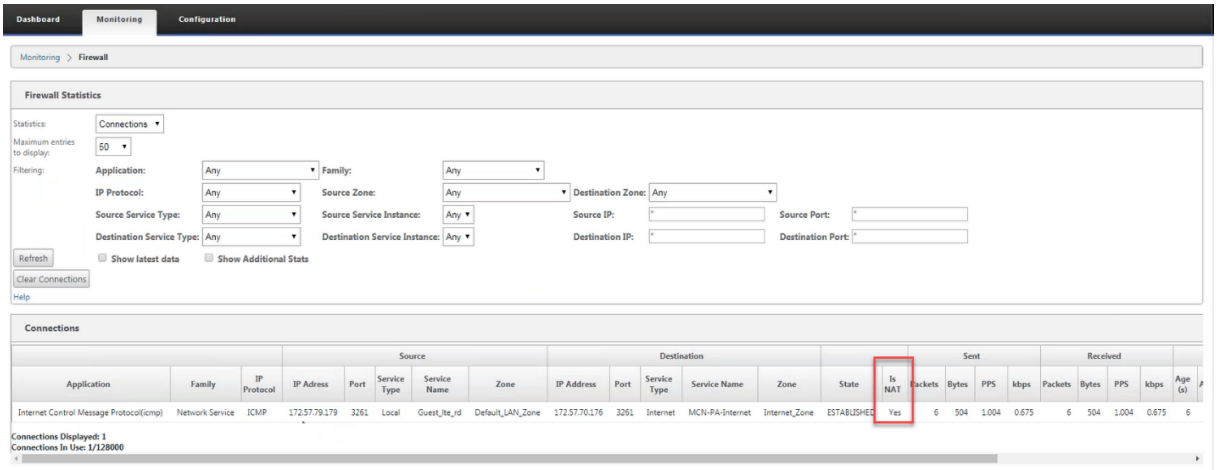


このシナリオでは、M=2 内部ネットワークと N=2 WAN リンクがあります。したがって、IPv6 インターネットサービスの適切な展開に必要なスタティック NAT ポリシーの数は 2 x 2 = 4 です。次の 4 つのスタティック NAT ポリシーは、次のアドレス変換を指定します。

- 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

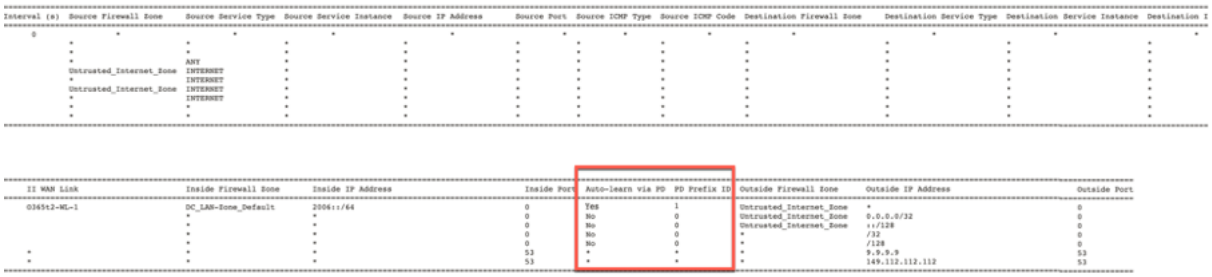
監視

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。



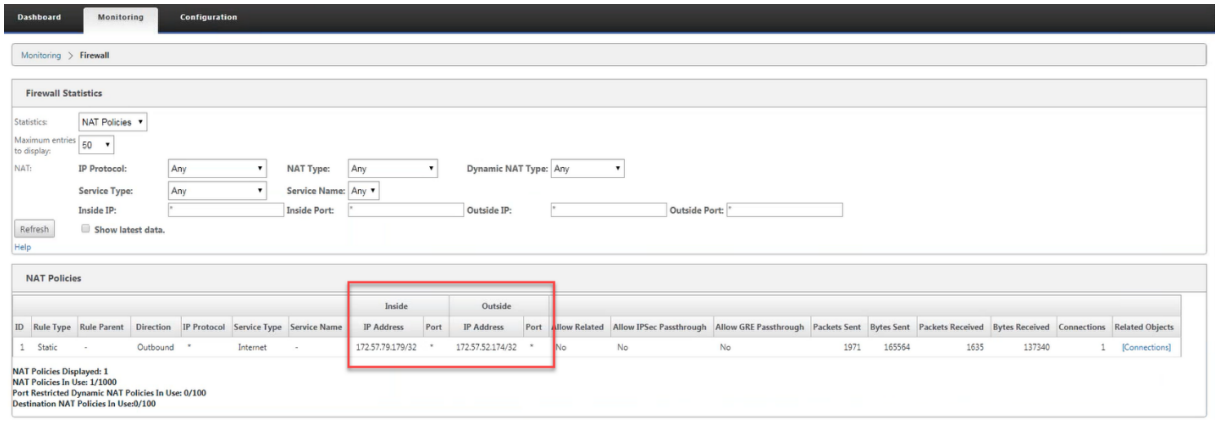
任意の NAT ルールに PD 経由の自動学習が設定されているかどうかを確認するには、[構成] **> [**仮想 **WAN] > [**設定の表示] に移動し、[表示] ドロップダウンリストから [ファイアウォール] を選択します。[**PD** による自動学習] およ

び [**PD** プレフィックス **ID**] 列に詳細が表示されます。

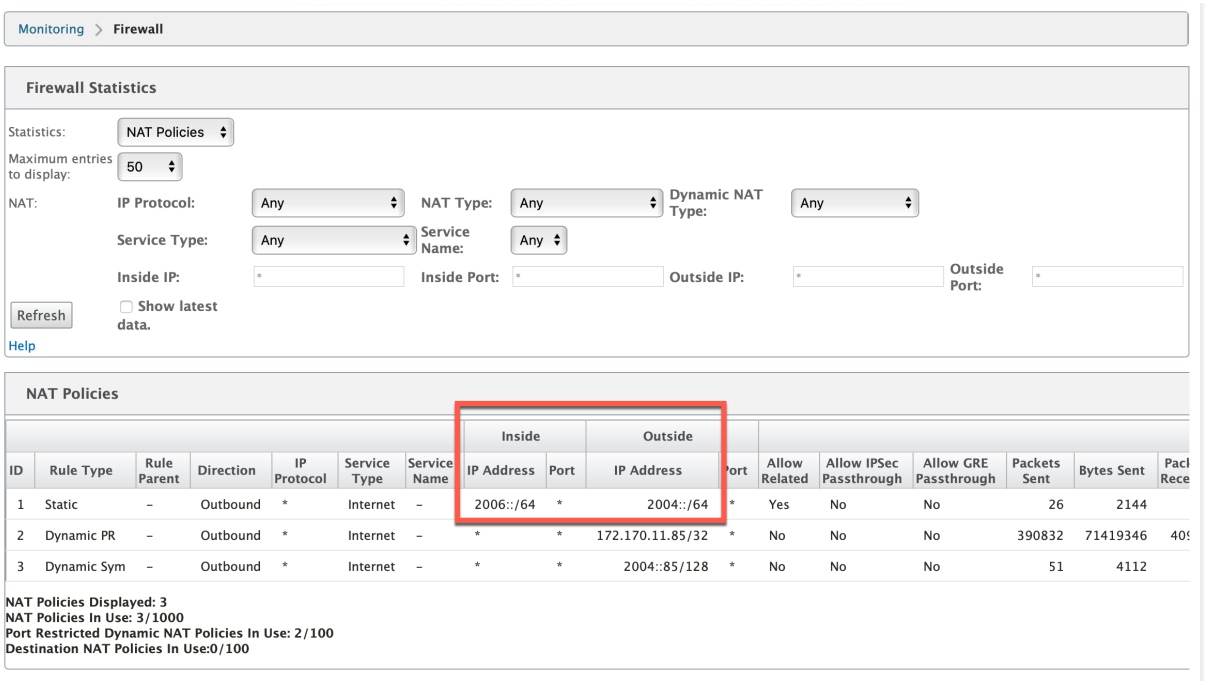


内部 IP アドレスと外部 IP アドレスのマッピングをさらに確認するには、[関連オブジェクト] の [ルート後 **NAT**] をクリックするか、[モニタリング] > [ファイアウォール統計] > [**NAT** ポリシー] に移動します。

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。



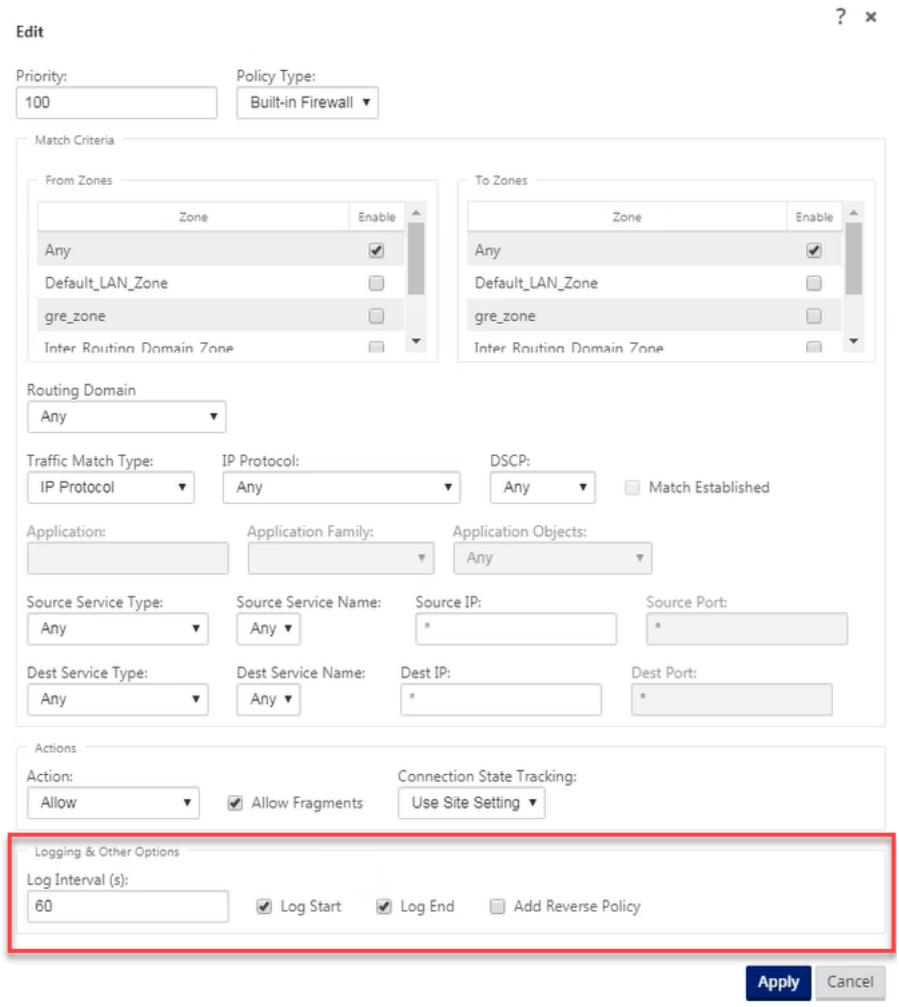
次のスクリーンショットは、IPv6 スタティック NAT ポリシーにおける内部アドレスと外部アドレスのマッピングを示しています。



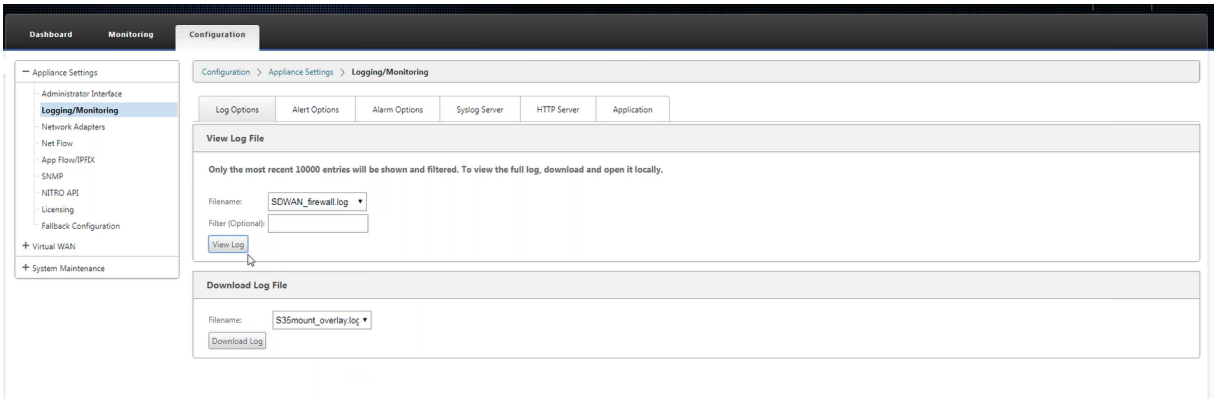
ログ

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。

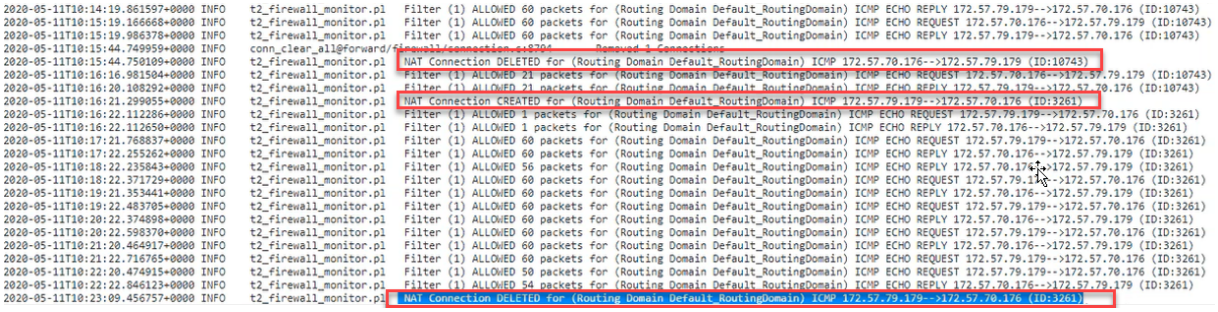
- 日付と時刻
- ルーティングドメイン
- IP プロトコル
- 送信元ポート
- 送信元 IP アドレス
- 翻訳された IP アドレス
- 翻訳されたポート
- 宛先 IP アドレス
- Destination port



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。



NAT 接続の詳細がログファイルに表示されます。



ダイナミック **NAT**

November 17, 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。

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。

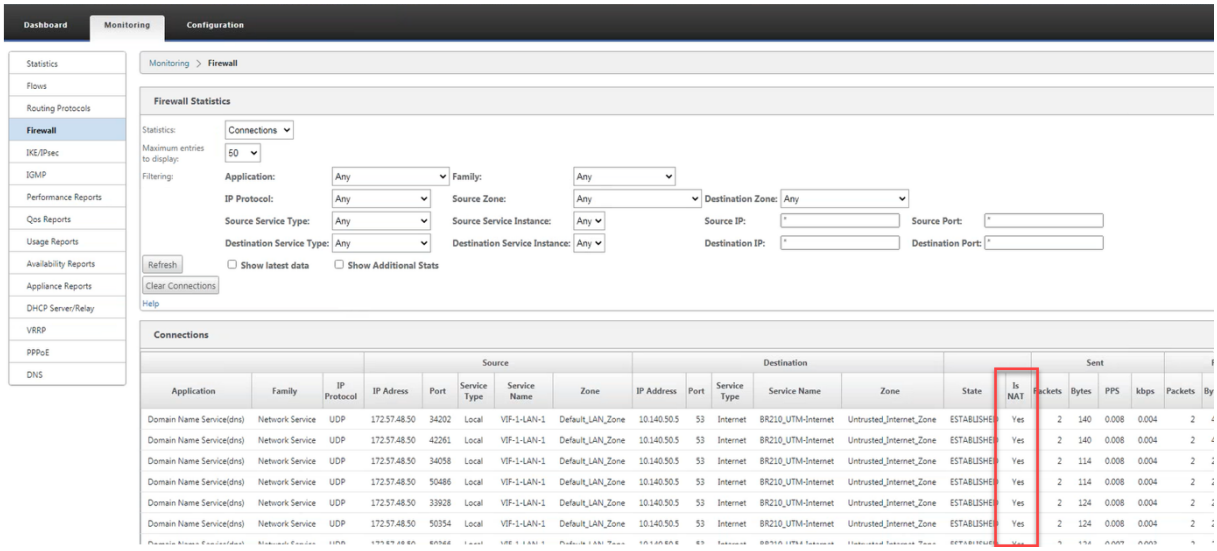
自動作成されたダイナミック **NAT** ポリシー

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
- Citrix SD-WAN Orchestrator サービスを使用して、単一の WAN リンク上の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 Orchestrator サービスで DNS フォワーダーまたは DNS プロキシを構成します。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。

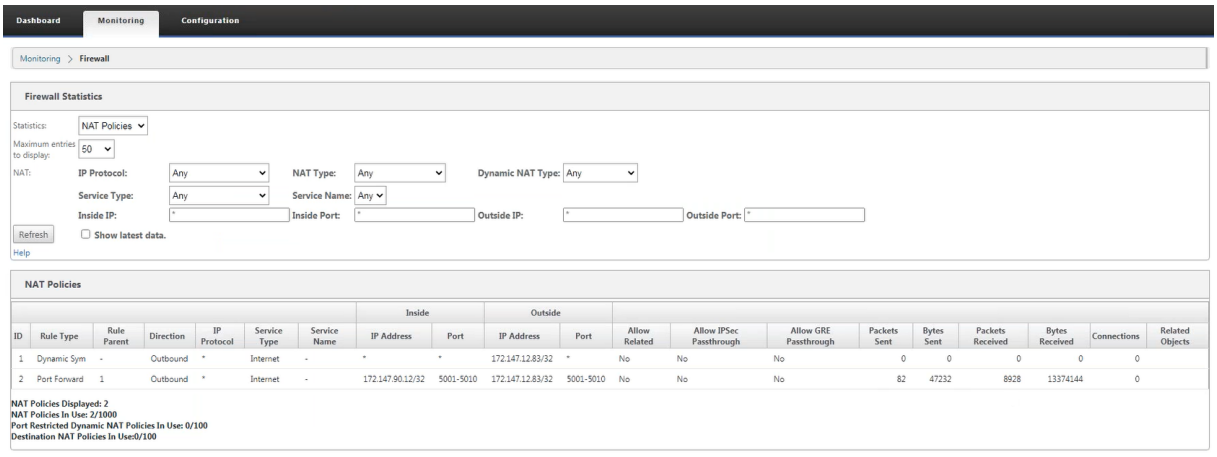
監視

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。

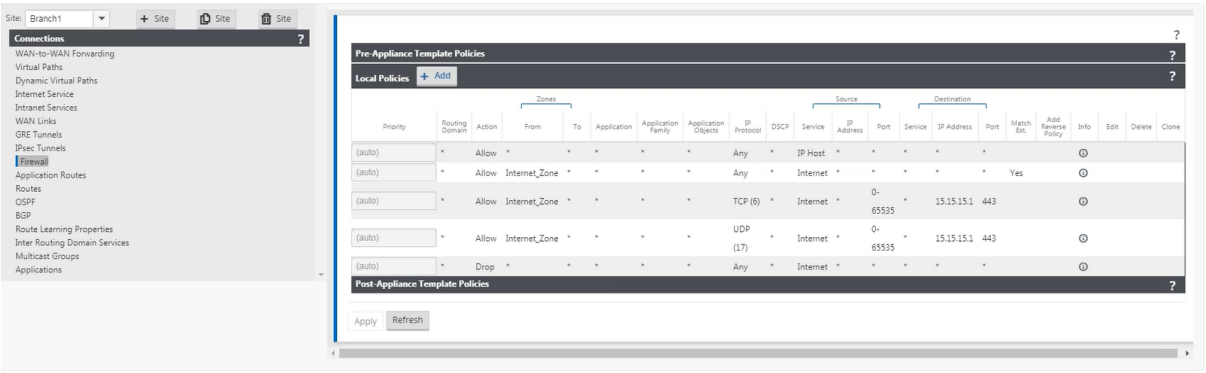


内部 IP アドレスと外部 IP アドレスのマッピングをさらに確認するには、**[** 関連オブジェクト**]** の **[** ルーティング前 **NAT]** または **[** ポストルート **NAT]** をクリックするか、**[** モニタリング**]** > **[** ファイアウォール統計**]** > **[NAT** ポリシー**]** に移動します。

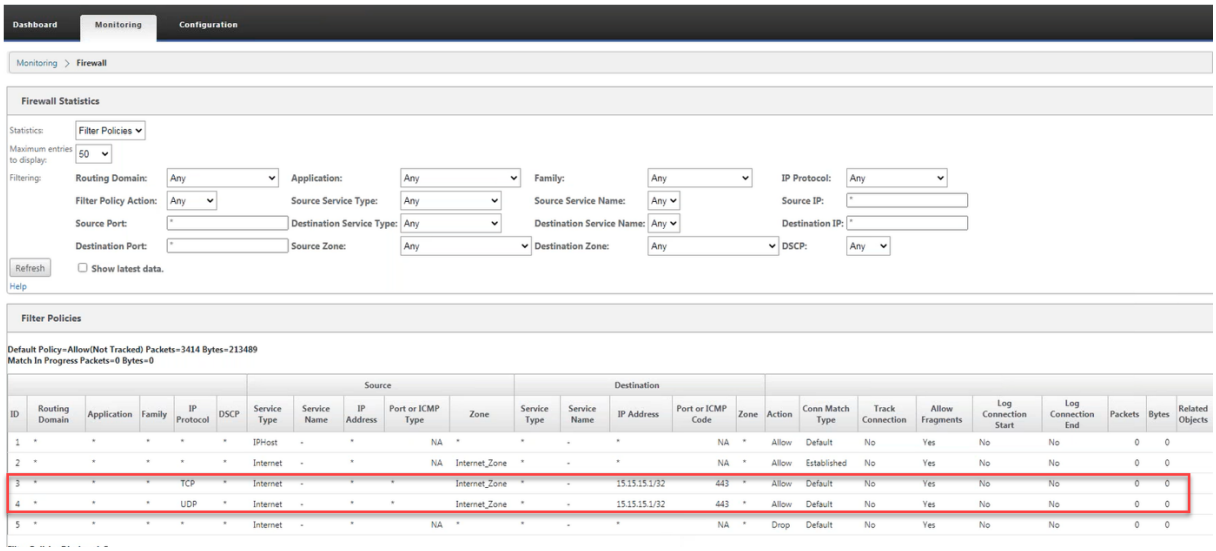
次のスクリーンショットは、タイプシンメトリックダイナミック NAT 規則とそれに対応するポート転送規則の統計を示しています。



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。



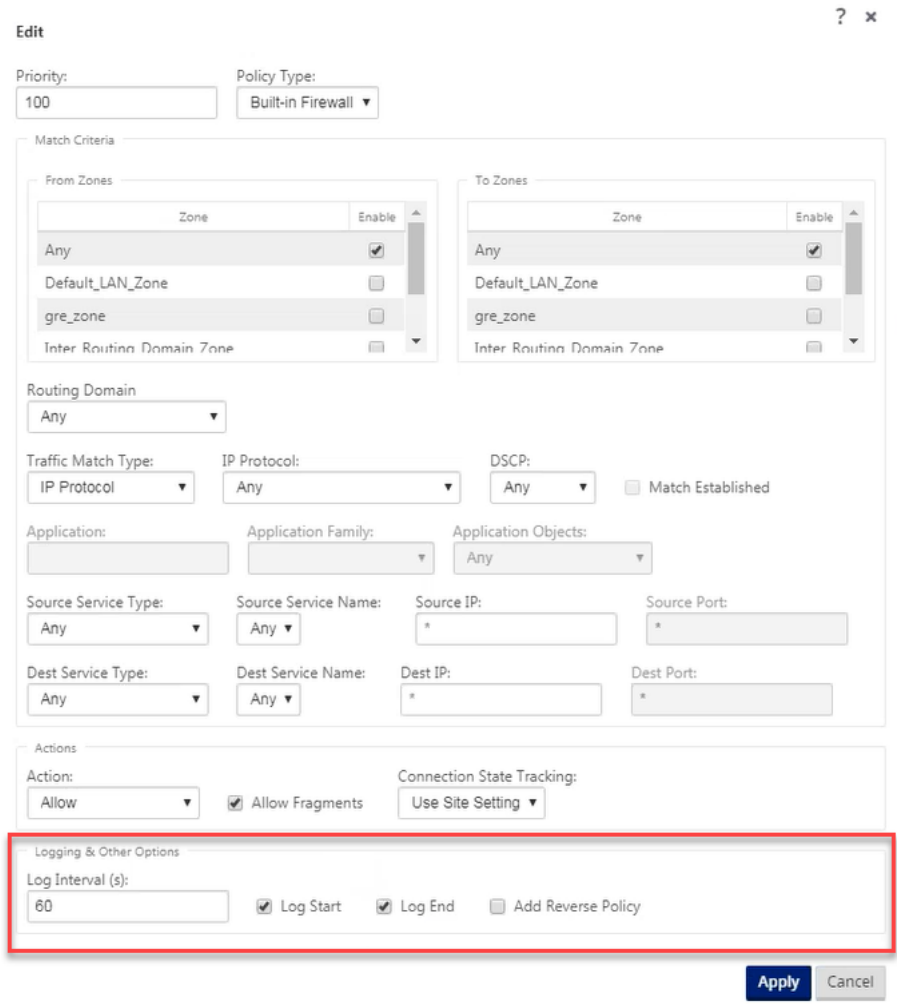
[監視] > [ファイアウォール統計] > [フィルタポリシー] に移動すると、フィルタポリシーの統計を表示できます。



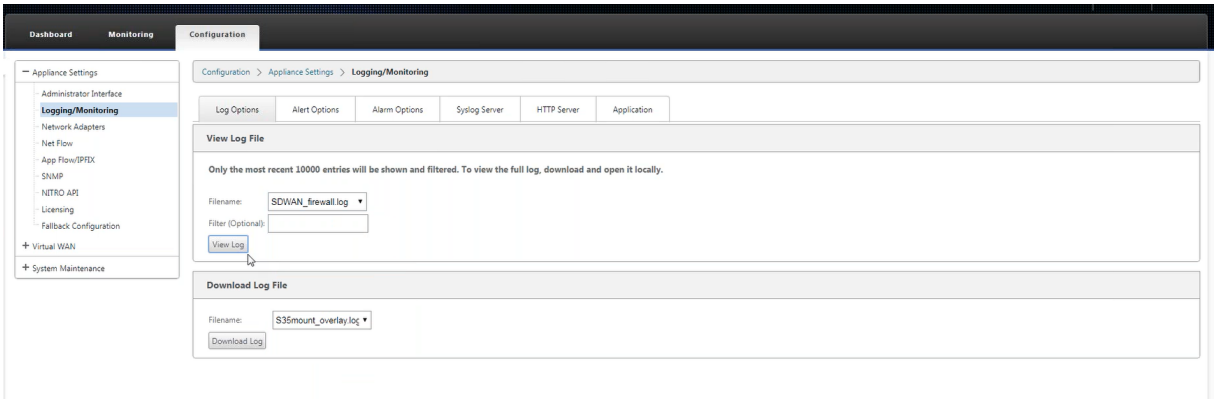
ログ

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。

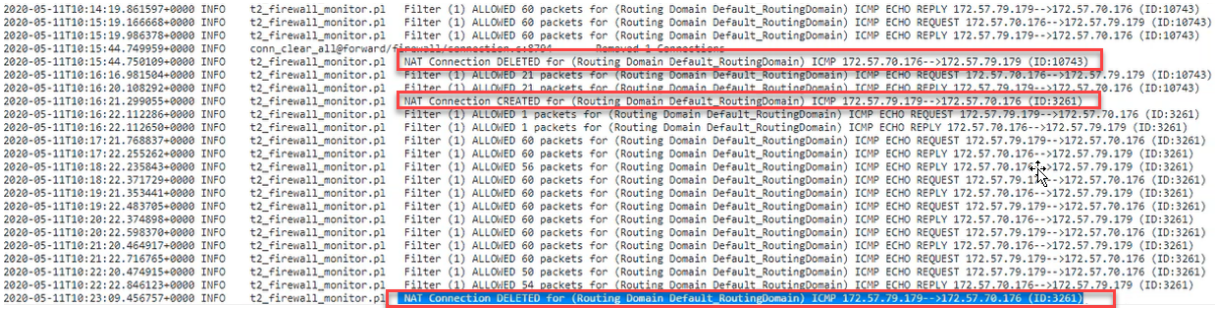
- 日付と時刻
- ルーティングドメイン
- IP プロトコル
- 送信元ポート
- 送信元 IP アドレス
- 翻訳された IP アドレス
- 翻訳されたポート
- 宛先 IP アドレス
- Destination port



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。



NAT 接続の詳細がログファイルに表示されます。



仮想 **WAN** サービスの構成

August 30, 2022

Citrix SD-WAN 構成では、Citrix SD-WAN ネットワークのトポロジについて説明し、定義します。Citrix SD-WAN Orchestrator サービスを使用して仮想 WAN サービスを構成する方法については、「フロー」を参照してください。

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。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。

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て、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。

ファイアウォールセグメンテーションの構成

November 17, 2022

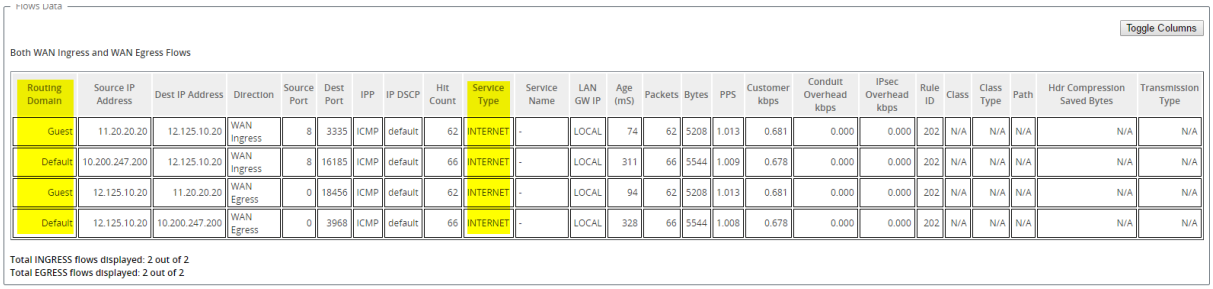
Virtual Route Forwarding（VRF; Virtual Route Forwarding）ファイアウォールセグメンテーションでは、複数のルーティングドメインが共通のインターフェイスを介してインターネットにアクセスでき、各ドメインのトラフィックは他のドメインのトラフィックから分離されます。たとえば、従業員とゲストは、互いのトラフィックにアクセスすることなく、同じインターフェイスを介してインターネットにアクセスできます。SD-WAN 11.5 リリース以降、Citrix SD-WAN Orchestrator サービスを使用してファイアウォールのセグメンテーションを構成できます。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」を参照してください。

- ローカルゲストユーザインターネットアクセス

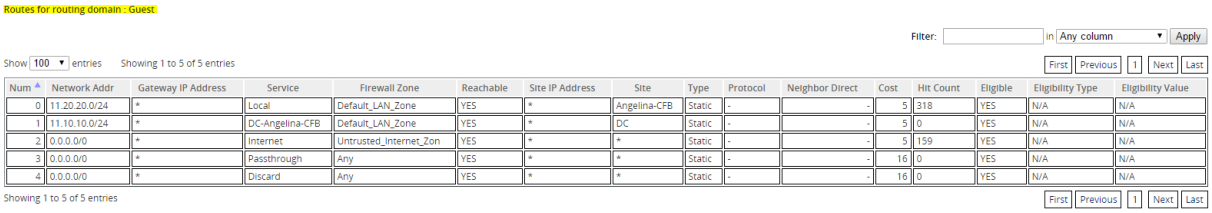
- 定義されたアプリケーションに対する従業員とユーザーのインターネットアクセス
- 従業員ユーザーは、MCN に他のすべてのトラフィックをヘアピンし続けることができます
- 特定のルーティングドメインに特定のルートを追加することをユーザーに許可します。
- 有効にすると、この機能はすべてのルーティングドメインに適用されます。

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。

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、**Web** 管理インターフェイスの **[**フロー（****Monitor** ）] > [フロー（Flows）] の [フロー（Flows）] テーブルの [ルーティングドメイン（Routing Domain）**



また、[モニタ] > [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。



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次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。

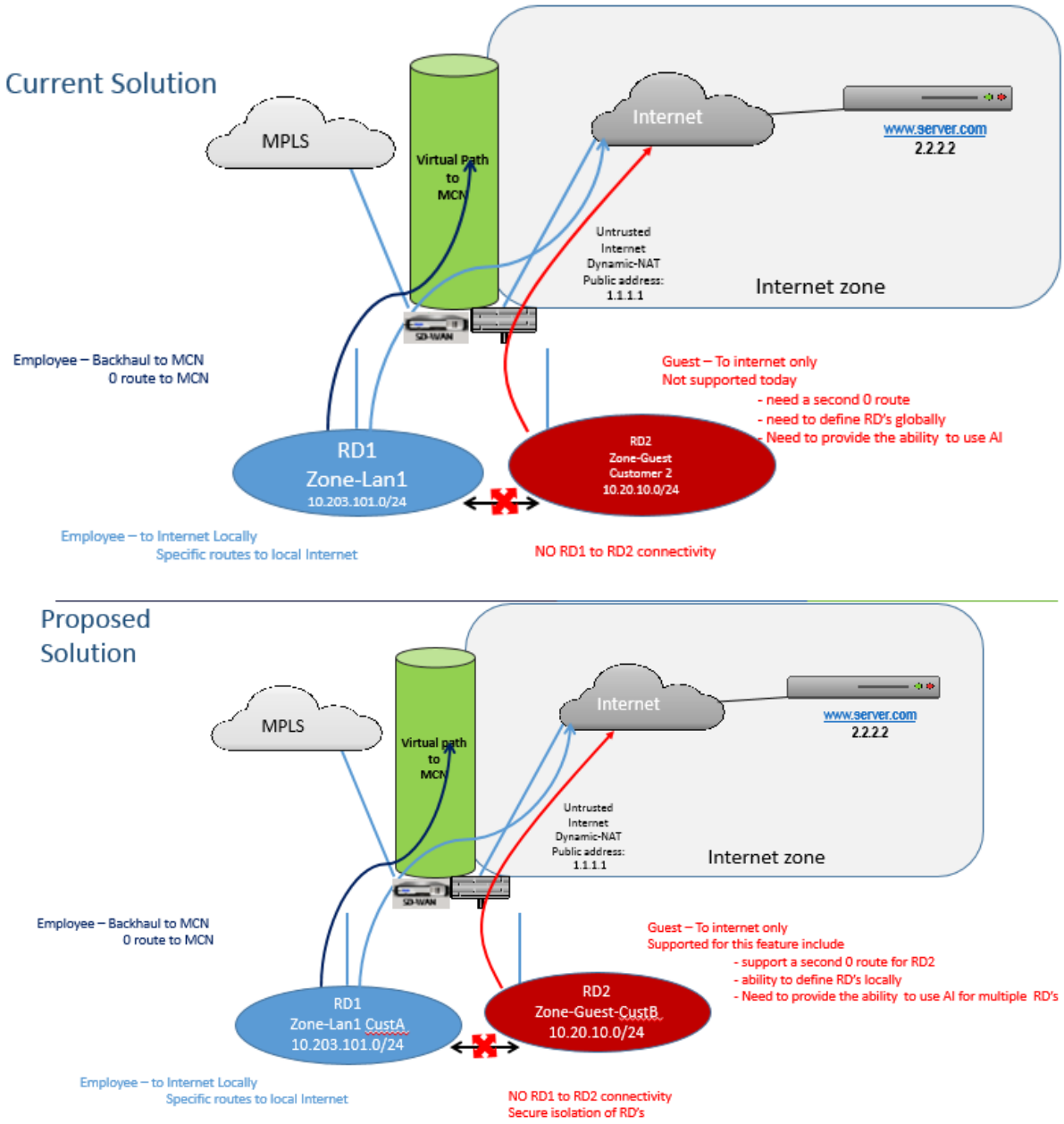
- 従業員やゲストなど、少なくとも 2 つのユーザーグループの安全な接続をサポートするインフラストラクチャをブランチサイトで提供します。このインフラストラクチャは、最大 16 のルーティングドメインをサポートできます。
- 各ルーティングドメインのトラフィックを、他のルーティングドメインのトラフィックから分離します。
- 各ルーティングドメインにインターネットアクセスを提供し、
  - 共通のアクセスインターフェイスが必要であり、許容される
  - 個別のパブリック向け IP アドレスを持つ各グループのアクセスインターフェイス
- 従業員のトラフィックは、ローカルインターネット（特定のアプリケーション）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。
- 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。

展開シナリオ



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に QoS はありません。先着順です。

証明書の認証

August 30, 2022

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。

証明書認証により、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。

Citrix SD-WAN Orchestrator サービスを使用して、SD-WAN アプライアンスの証明書認証を有効にすることができます。証明書認証の詳細については、「証明書認証」を参照してください。

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 データセットの TCP は、マルチホップデータを提供します。HDX データセットは HDX インサイトデータを提供します。

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** 名 **&ID**	タイプと **len**	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	destinationIpv4Addres, 12	Ipv4address, 4	
Ipversion	ipVersion, 60	Unsigned8, 1	4 に設定します。
IP プロトコル番号	protocoldentifier,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** 名 **&ID**	タイプと **len**	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	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。
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	flowKeyIndicator, 173	Unsigned64, 8	Set to 0x1E037F.
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変更されます。

テンプレート **ID**：**615**（**IPv6** フロー）　| 情報要素 (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|destinationIpv6Addres, 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|Unsigned8, 1|0x00: 入力フロー 0x01: 出力フロー WAN-WAN および 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** 名 **&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** 名 **&ID**	タイプと **len**	コメント
Ipv4 SRC IP	sourceIPv4Address, 8	Ipv4address, 4	
Ipv4 DST IP	destinationIpv4Addres, 12	Ipv4address, 4	
Ipversion	ipVersion, 60	Unsigned8, 1	
IP プロトコル番号	プロトコル識別子, 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	デスティネーション TransportPort, 11	Unsigned16, 2	
Pkt カウント	packetDeltaCount, 2	Unsigned64, 8	

情報要素 **(IE)**	**IE** 名 **&ID**	タイプと **len**	コメント
バイト数	octetDeltaCount, 1	Unsigned64, 8	
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	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。
入力 VLAN ID	vlanId, 58	Unsigned16, 2	
出力 VLAN ID	postVlanId, 59	Unsigned16, 2	

テンプレート **ID**：**616**（**IPv6** フロー）　| 情報要素 (IE)|IE 名と ID| タイプと len| コメント |
|-|-|-|-|
|Ipv6 SRC IP|sourceIPv6Address, 27|Ipv6address, 16|
|Ipv6 DST IP|destinationIpv6Addres, 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: 出力フローワン 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|
入力インターフェイス |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|

制限事項

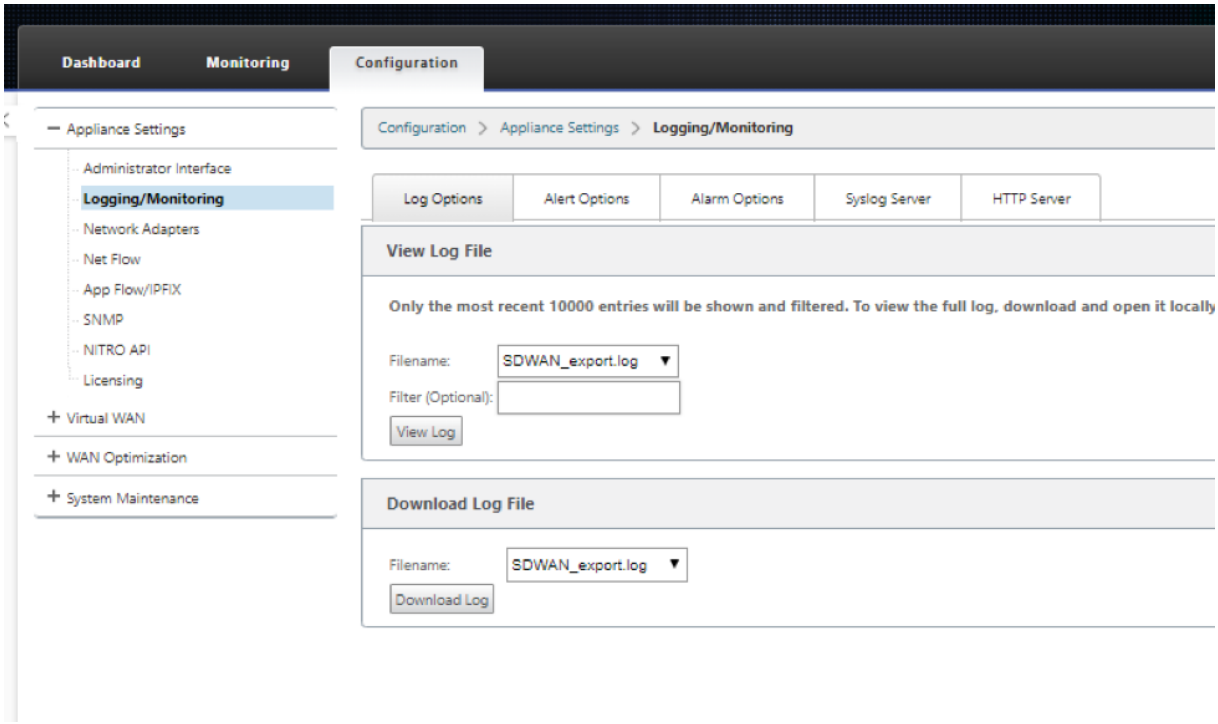
- AppFlow は、IPv6 コレクタおよびフローレコードをサポートしていません。
- Net Flow のエクスポート間隔が 15 秒から 60 秒に増加します。
- AppFlow/IPfix フローは UDP 経由で送信され、接続が失われた場合、すべてのデータが再送信されるわけではありません。エクスポート間隔が X 分に設定されている場合、アプライアンスは X 分のデータのみを保存します。接続損失の X 分後に再送信されます。
- Citrix SD-WAN、リリース 10 バージョン 2 では、**AppFlow** 設定はすべてのアプライアンスに対してローカルになりますが、以前の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 は、Citrix SD-WAN Orchestrator サービスを介してのみ構成できます。詳細については、「AppFlow と IPFIX」を参照してください。

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

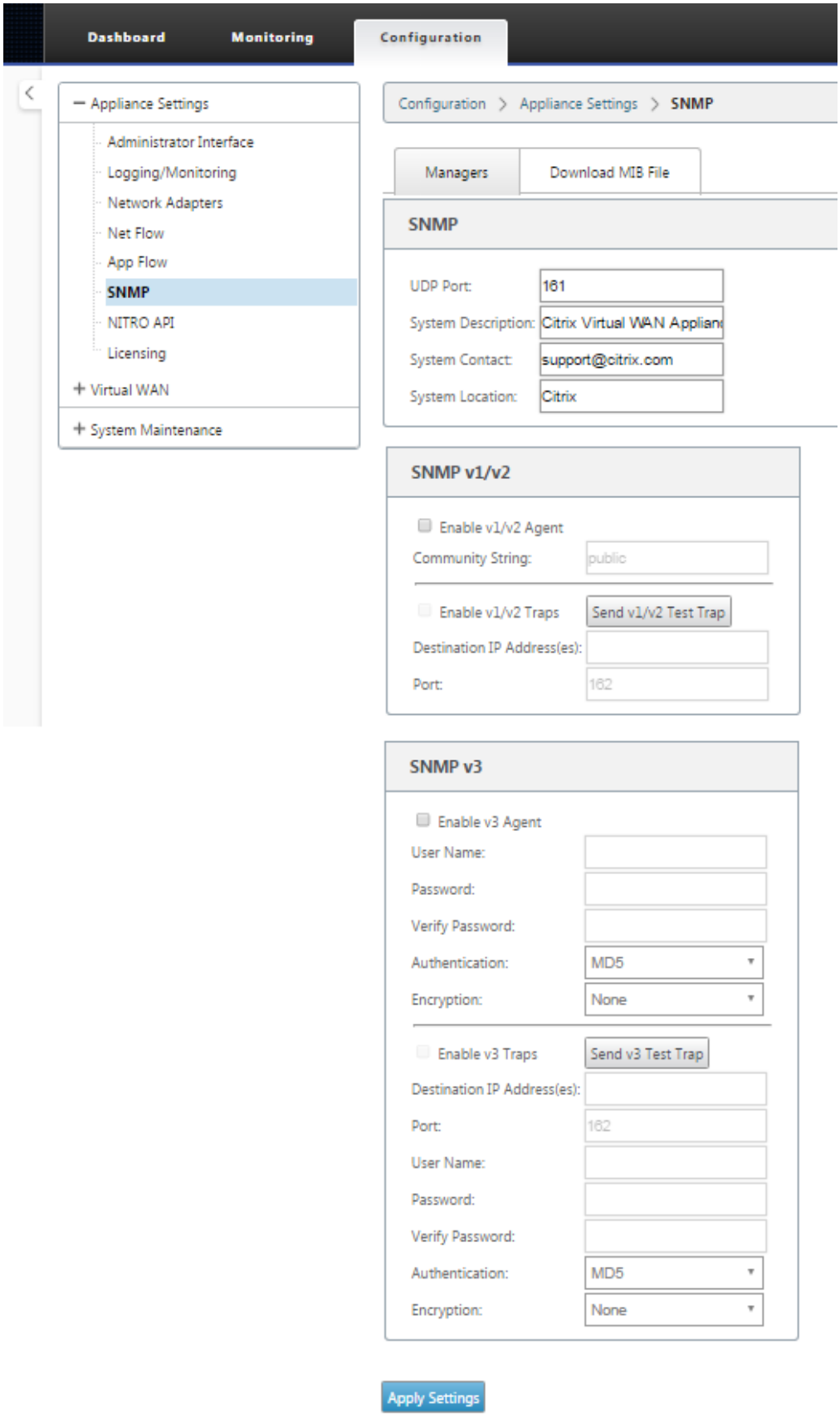
November 17, 2022

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。



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

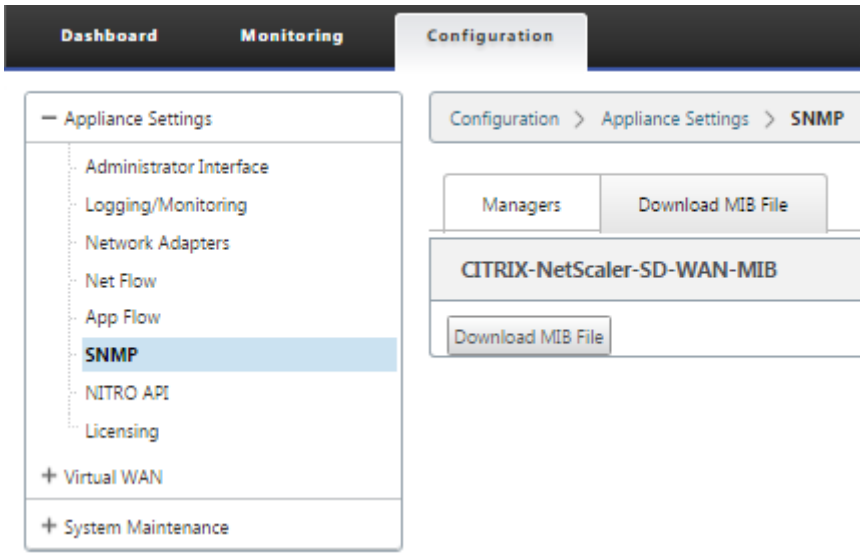
Citrix SD-WAN アプライアンスの監視を開始する前に、次の SNMP ファイルをダウンロードする必要があります。

- 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

August 30, 2022

Citrix SD-WAN Orchestrator サービスを使用して、次の管理オプションを使用して、Citrix SD-WAN アプライアンスを管理および保守できます。詳細については、「アプライアンスの設定」を参照してください。

- 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。

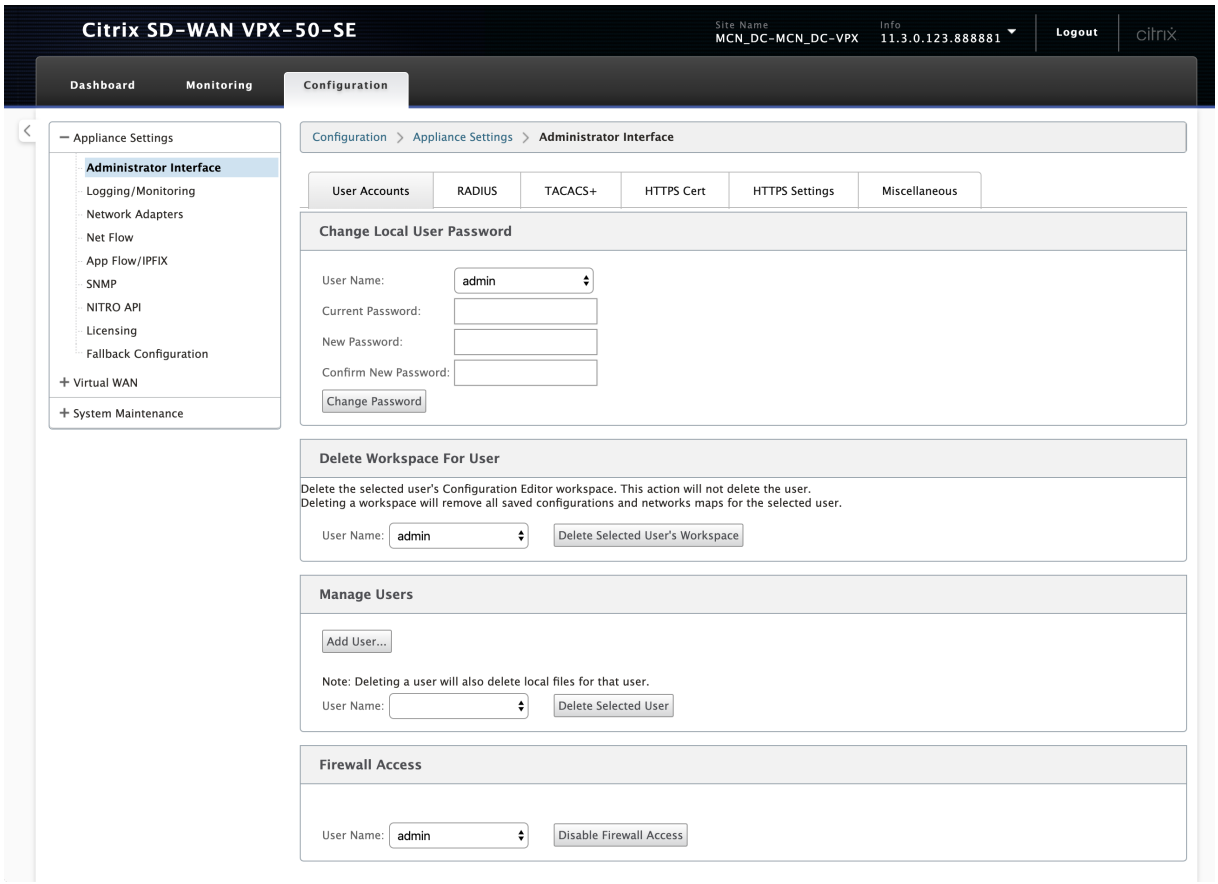
  特権管理者（admin）には以下の特権があります。

  - 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、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、ファイアウォールとセキュリティ関連の設定を除いて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。

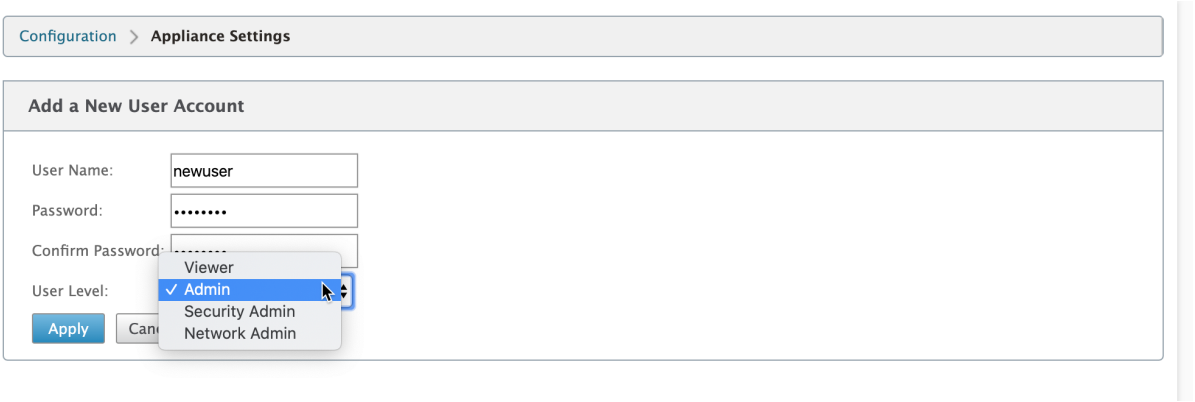
> 注
>
> ネットワーク管理者およびセキュリティ管理者は、ユーザーアカウントを追加または削除できません。編集できるのは自分のアカウントのパスワードのみです。



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。

RADIUS サーバー

1 台または 3 台の RADIUS サーバでユーザ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。

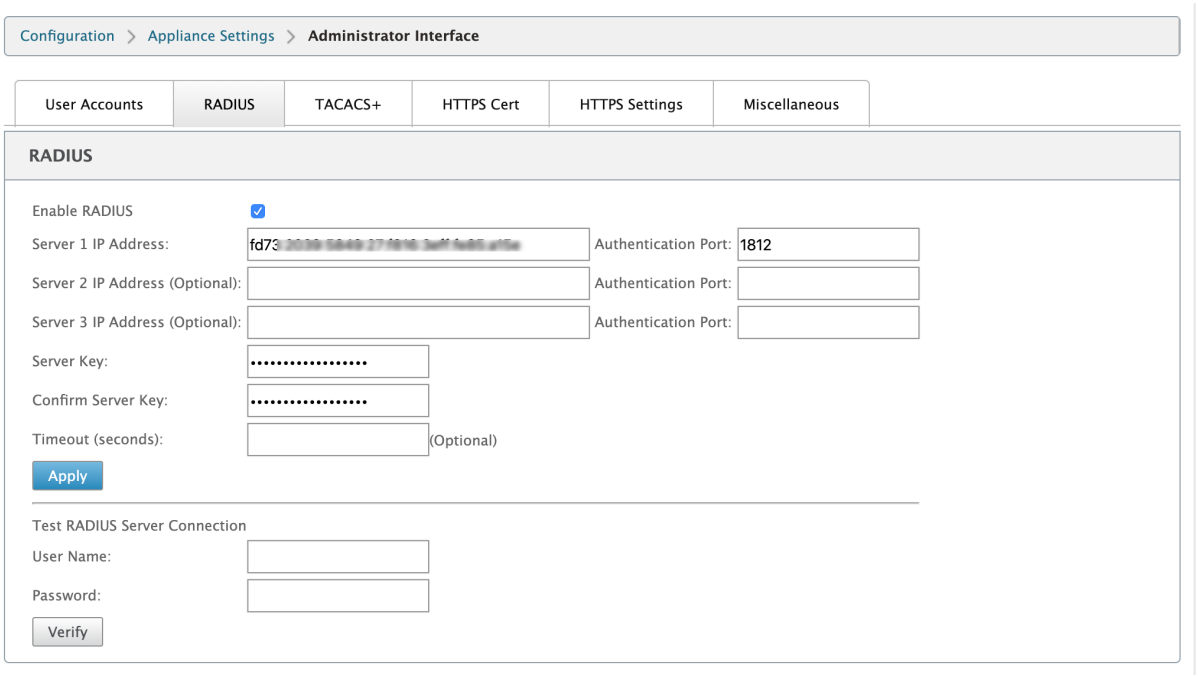
RADIUS サーバを構成するには、次の手順を実行します。

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。



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。

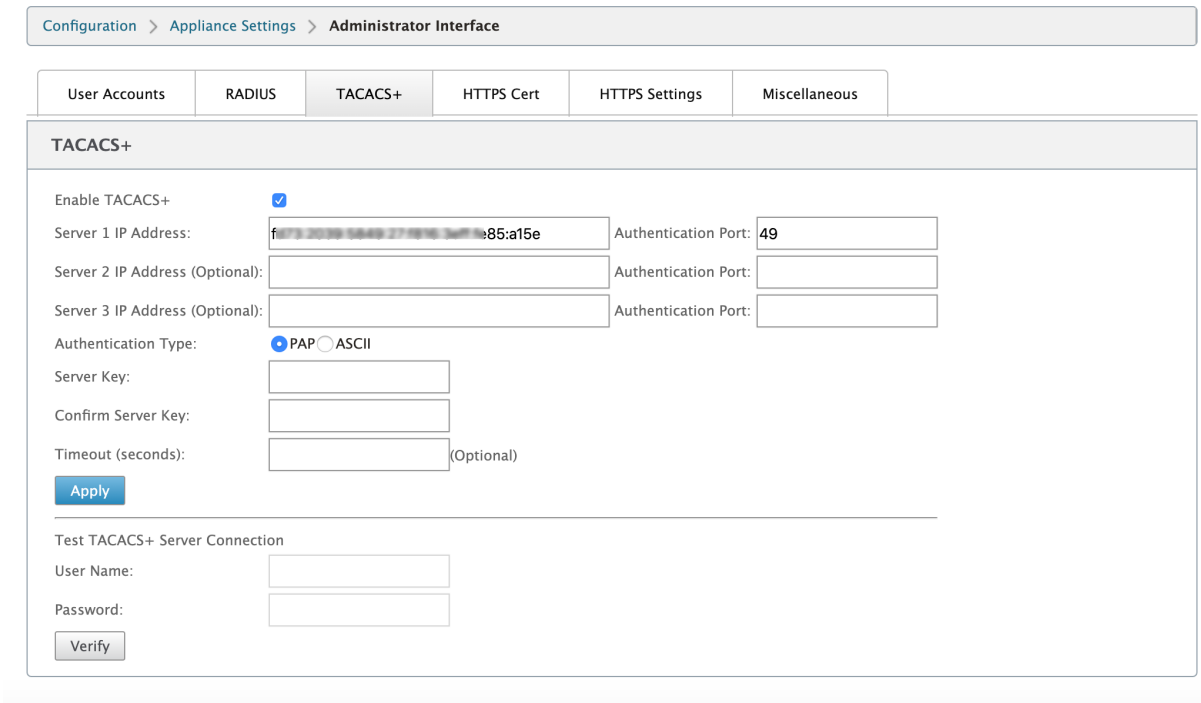
4. [認証タイプ] として [**PAP**] または [**ASCII**] を選択します。

   - 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。
   -

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。



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

November 17, 2022

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。

Citrix SD-WAN Orchestrator サービスを使用して NDP ルーターアドバタイズメントを構成できます。詳細については、NDP ルーターアドバタイズメントを参照してください。

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は、Citrix SD-WAN Orchestrator サービスを介して構成できます詳細については、「委任グループにプレフィックスを付ける」を参照してください。

ハウツー記事

August 30, 2022

「ハウツー記事」には、Citrix SD-WAN でサポートされている機能を構成する手順が記載されています。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。

- 仮想ルーティングおよび転送
- QoS 公平性のための RED の有効化
- Configuration
- 動的ルーティング
- DHCP サーバと 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 拡張機能
- SSL プロファイルとのサービスクラスの関連付け
- ゼロタッチ展開

アクセスインターフェイスの設定

August 30, 2022

Citrix SD-WAN Orchestrator サービスを介してアクセスインターフェイスを構成するには、「WAN リンク」を参照してください。

仮想 **IP** アドレスの構成

August 30, 2022

Citrix SD-WAN Orchestrator サービスを介して仮想 IP アドレスを構成するには、「WAN リンク」を参照してください。

GRE トンネルの設定

August 30, 2022

Citrix SD-WAN Orchestrator サービスを使用して GRE トンネルを構成するには、「GRE サービス」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

November 17, 2022

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。

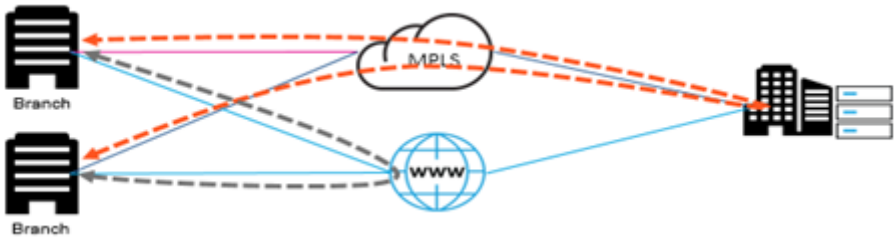
Citrix SD-WAN では、すべてのオフィス間のパスを構成する必要はありません。ダイナミックパス機能を有効にすると、SD-WAN ソリューションは必要に応じてオフィス間のパスを自動的に作成します。セッションでは、最初に既存

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。

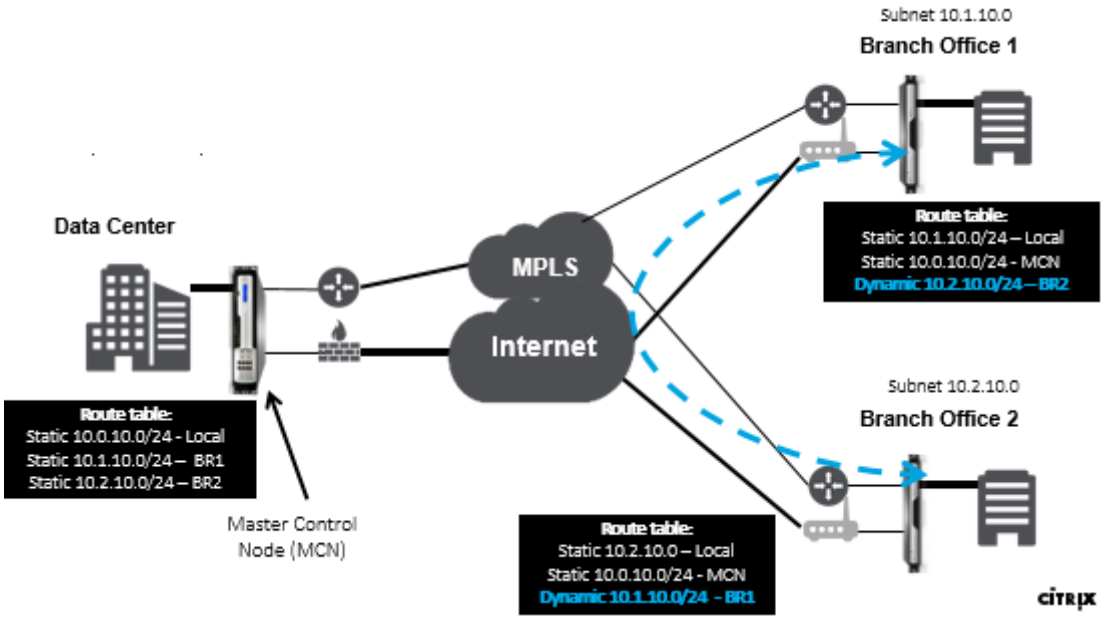
SD-WAN ネットワークのその他の利点は次のとおりです。

- ブランチ間の接続を許可する帯域幅と PPS のしきい値
- レー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

Citrix SD-WAN Orchestrator サービスを使用して動的仮想パスを有効にするには、「仮想パス」を参照してください。

WAN から **WAN** への転送

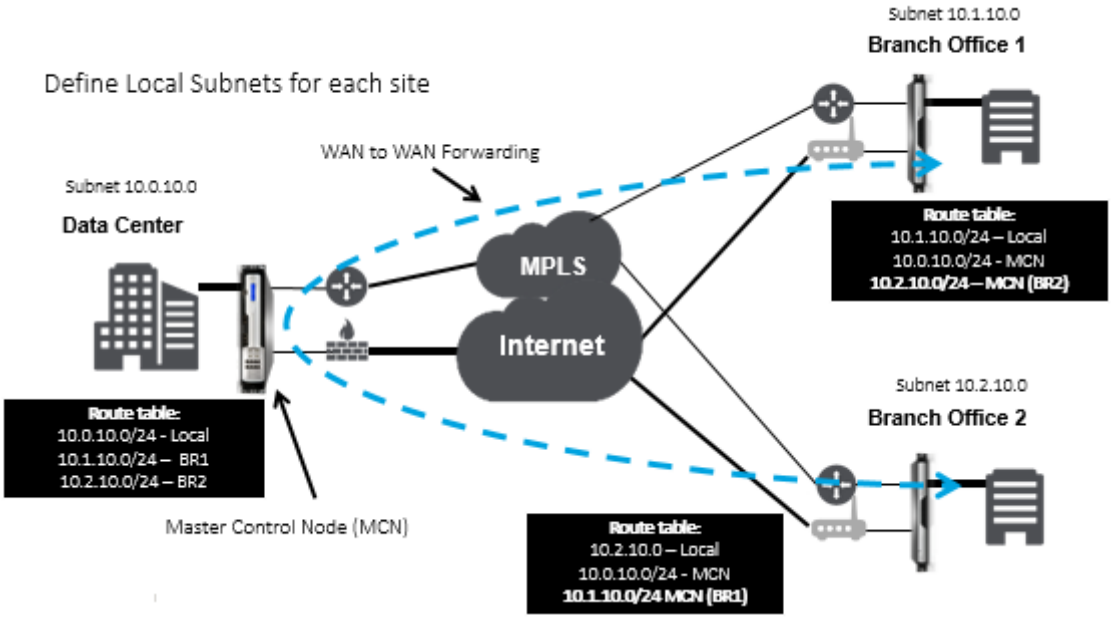
August 30, 2022

MCN で WAN から WAN への転送を有効にすると、MCN がリモートサイトルートをアドバタイズできるようになります。

- クライアントは MCN ローカルルートおよびその他のクライアントサイトルートを認識している
- クライアントの観点からは、すべてのルートは MCN ルートと見なされます

MCN で WAN-to-WAN 転送が有効になっていない場合、カスタマーネットワークでブランチ間通信の問題が発生します。

クライアントモードで実行されているアプライアンスは、MCN で WAN-to-WAN 転送が有効になるまで、他のブランチサブネットを認識しません。このオプションを有効にすると、ブランチ SD-WAN ノードは他のブランチサブネットを認識します。他のブランチ宛てのトラフィックは MCN に転送されます。MCN は正しい宛先にルーティングします。



監視とトラブルシューティング

August 30, 2022

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

August 30, 2022

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（**Dashboard**）] 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。

[**Dashboard**] ページには、ローカルアプライアンスに関する次の基本情報が表示されます。

システムステータス:

- 名前—これは、アプライアンスをシステムに追加したときにアプライアンス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。
- アプライアンスモード—これは、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 として設定されているか、またはクライアントアプライアンスとして設定されているかを示します。
- 管理 **IP** アドレス—これはアプライアンスの管理 IP アドレスです。
- **Appliance Uptime** —これは、前回の再起動以降にアプライアンスが実行されている期間を指定します。
- [**Service Uptime**]：これは、前回の再起動以降に仮想 WAN サービスが実行されている期間を指定します。

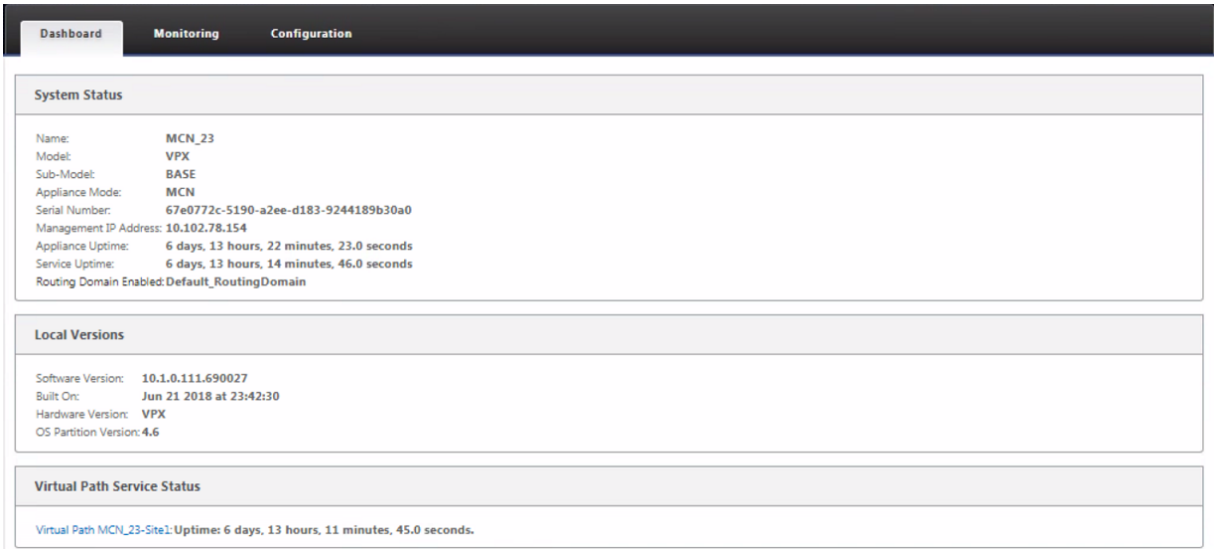
仮想パスサービスのステータス**:**

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**:**

- ソフトウェアバージョン—これは、アプライアンスで現在アクティブ化されている CloudBridge Virtual Path ソフトウェアパッケージのバージョンです。
- **Build on** —これは、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** パーティションバージョン—これは、アプライアンス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。

以下の図は、サンプルのダッシュボードページを示しています。



統計情報の表示

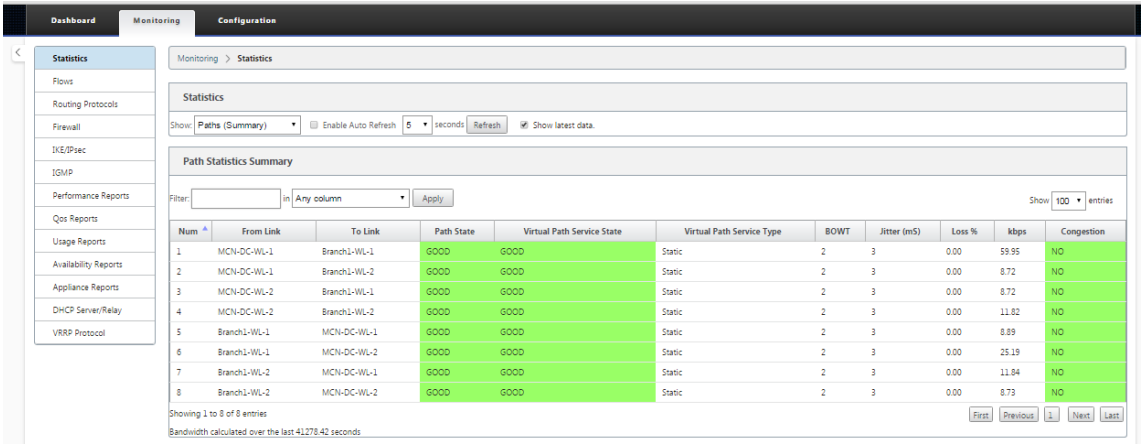
August 30, 2022

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。

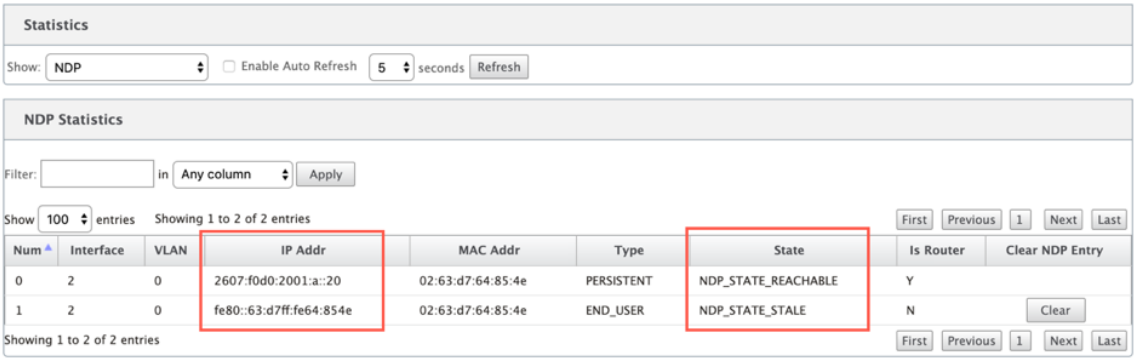
   これにより、左側のペインに [**Monitoring**] ナビゲーションツリーが開きます。デフォルトでは、[**Show**] フィールドでパスが事前に選択された状態の [**Statistics**] ページも表示されます。これには、パスの統計情報の詳細なテーブルが含まれます。

   > 注
   >
   > 別の [**Monitoring**] ページ（[**Flow**s] など）に移動した場合は、[Monit **or** ing] 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。

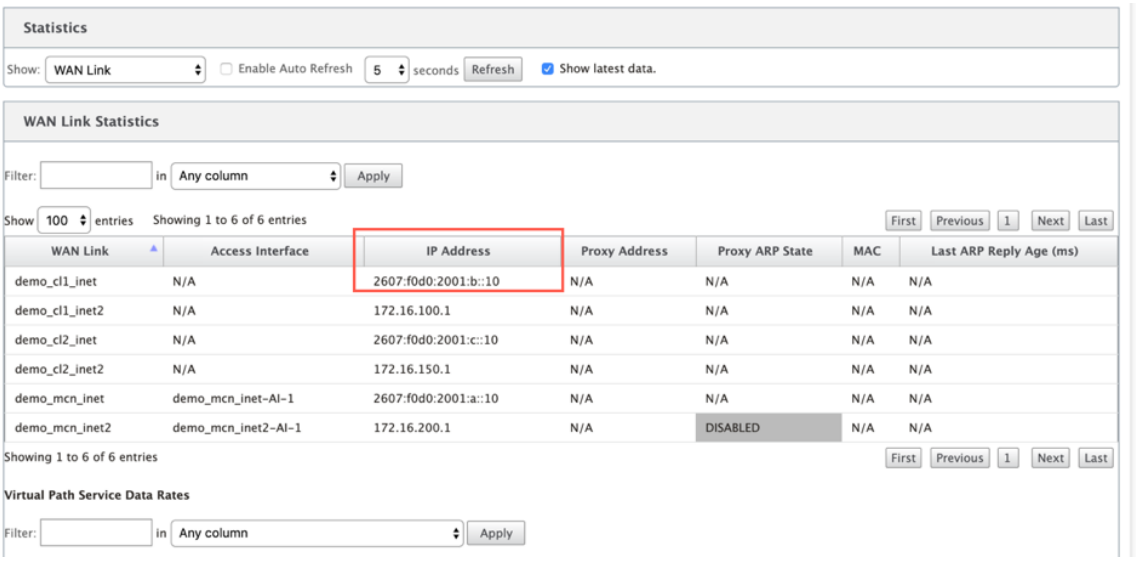


11.1.0 リリースでは、近隣探索の問題をデバッグするために、近隣探索プロトコル（NDP）オプションが追加されました。

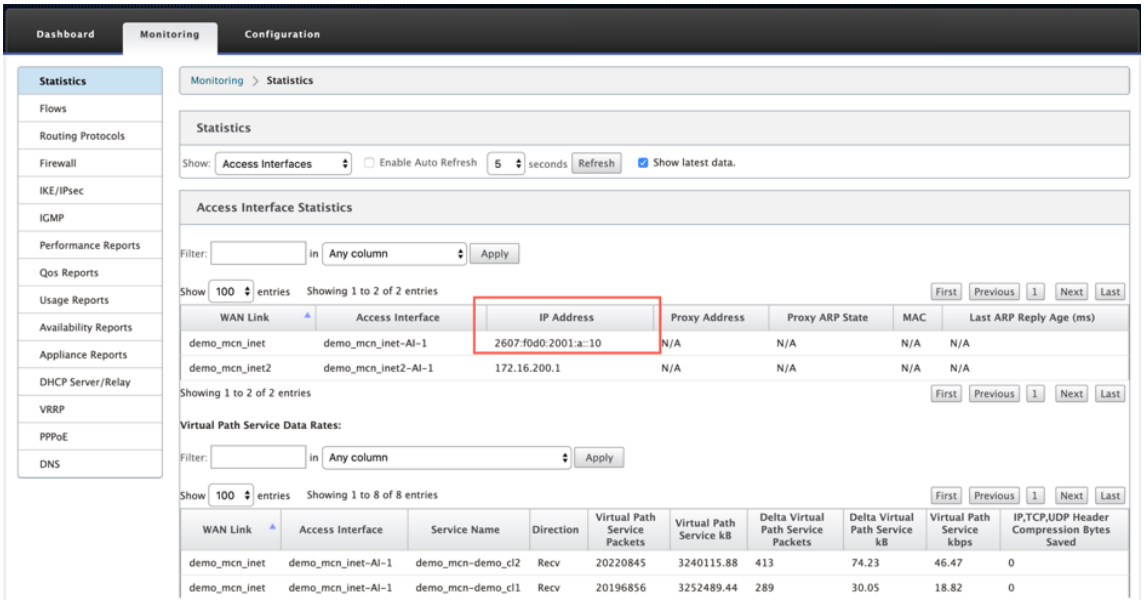
1. [Show] ドロップダウンメニューから [NDP] オプションを選択すると、NDP の状態を IPv6 アドレスとともに表示できます。



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。

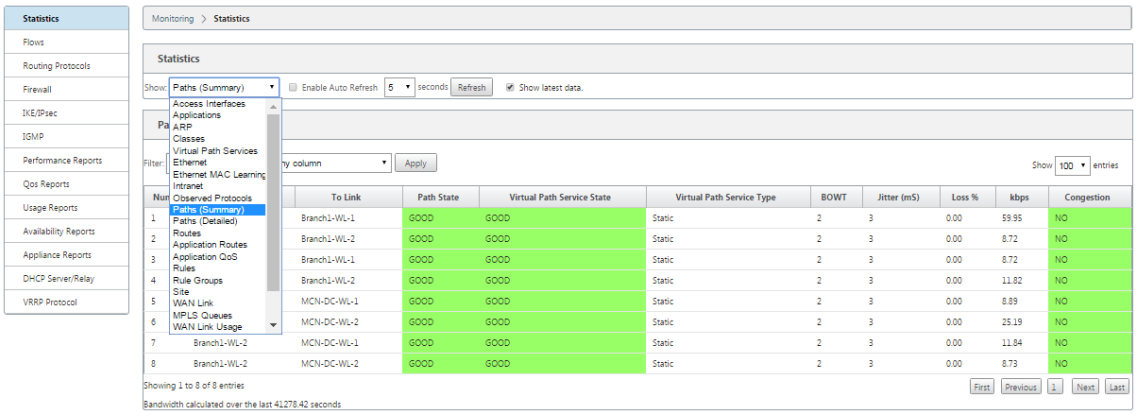


3. アクセスインターフェイスの統計情報も表示できます。



4. [表示] ドロップダウンメニューを開きます。

   [**Show**] 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、統計情報をフィルタリングおよび表示する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。

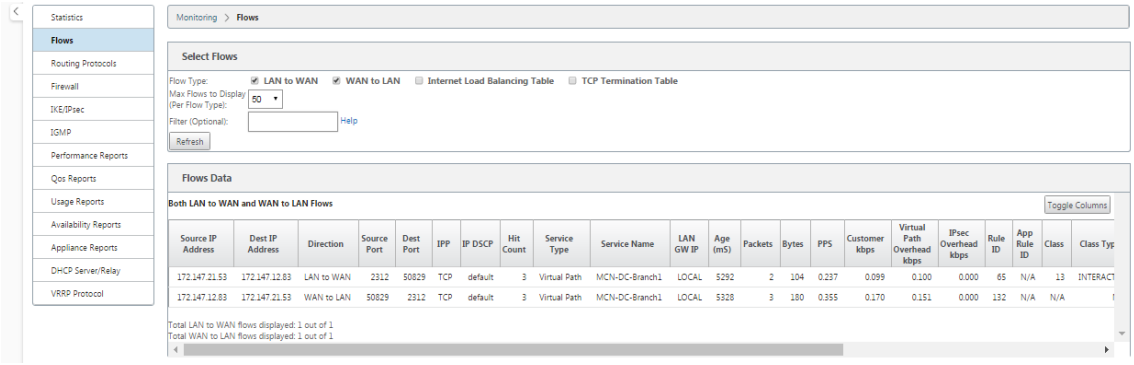
フロー情報の表示

August 30, 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。

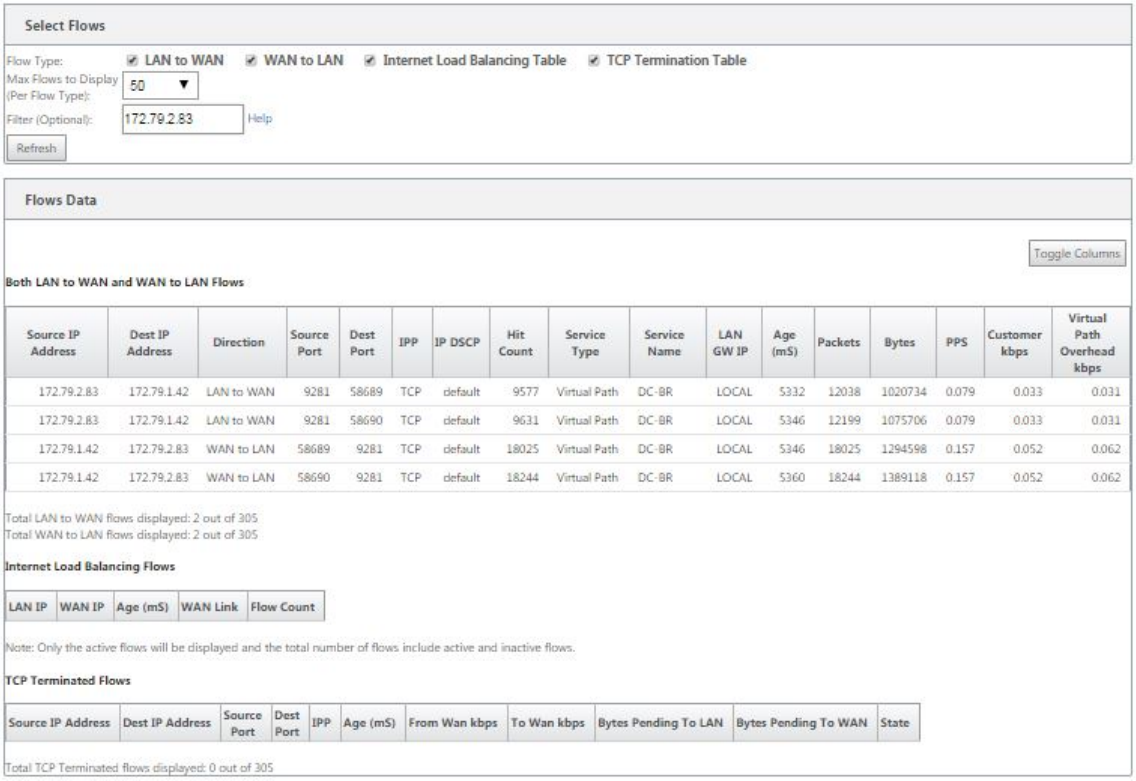
1. MCN の管理 Web インターフェイスにログインし、[モニタリング] タブを選択します。左側のペインに [**Monitoring**] ナビゲーションツリーが開きます。
2. ナビゲーションツリーで [フロー] ブランチを選択します。[Flow **Type]** フィールドで事前選択された ****LAN** から **WAN** への [フロー ** （**Flows**）] ページが表示されます。



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定します。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。

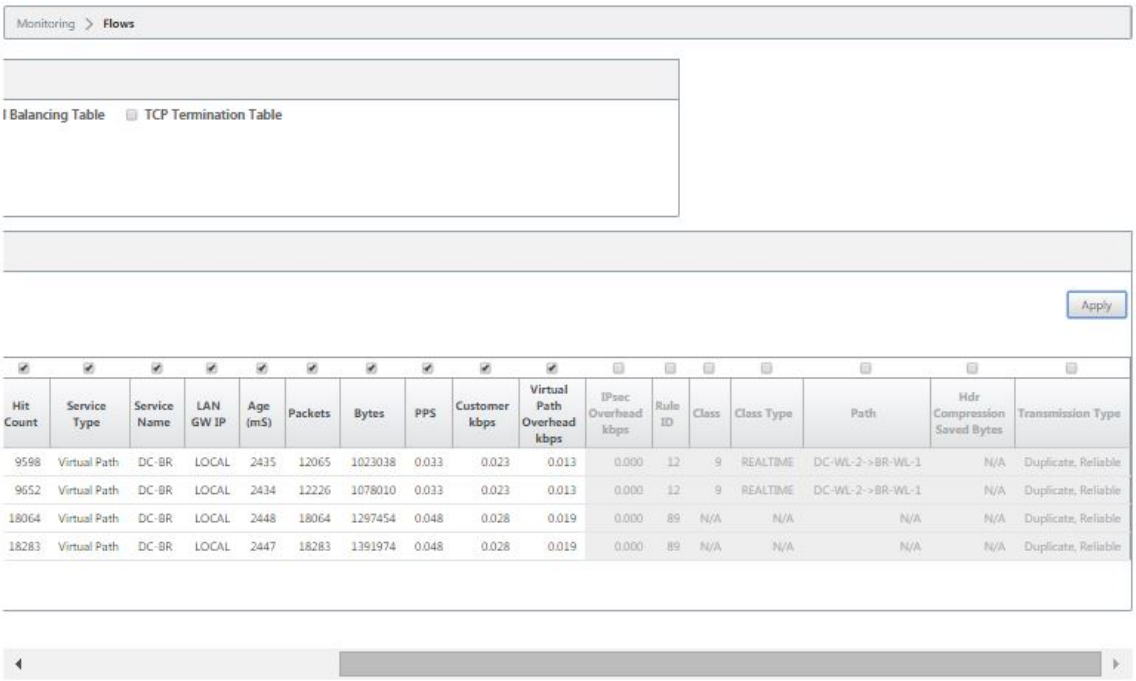
7. [**Refresh**] をクリックして、フィルタ結果を表示します。この図は、すべてのフロータイプが選択された **[**フロー**]** ページのフィルタ表示の例を示しています。



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。



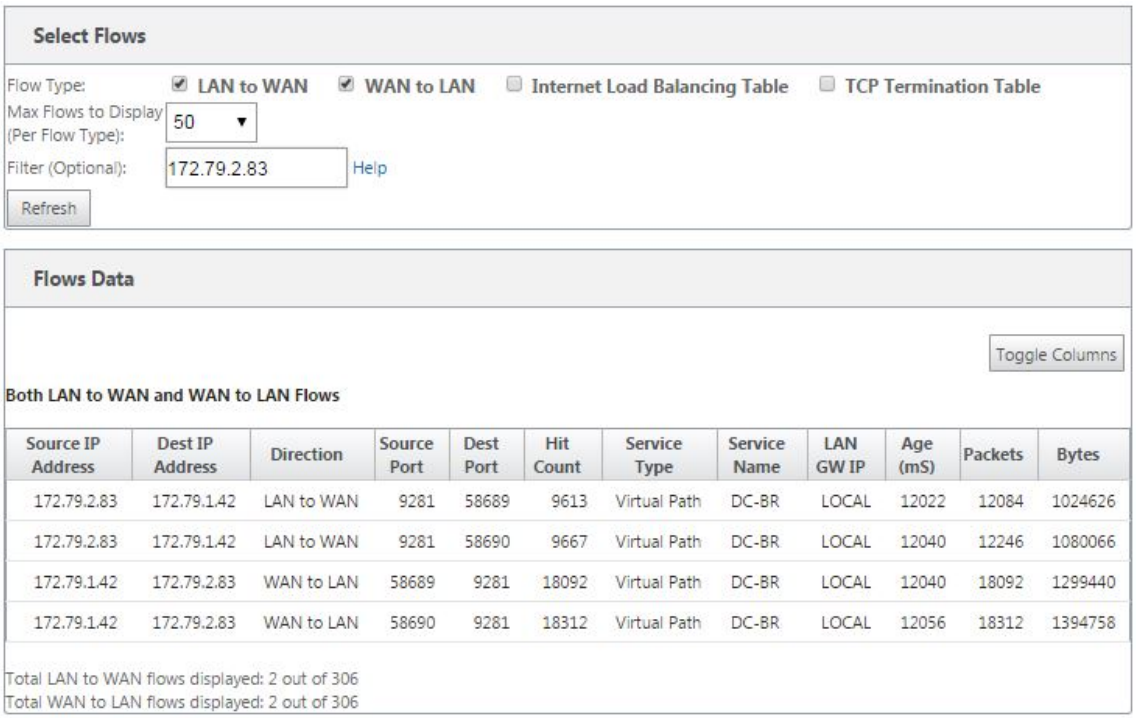
10. チェックボックスをクリックして、列を選択または選択解除します。

- 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、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。



SD-WAN Center の **DPI** アプリケーション

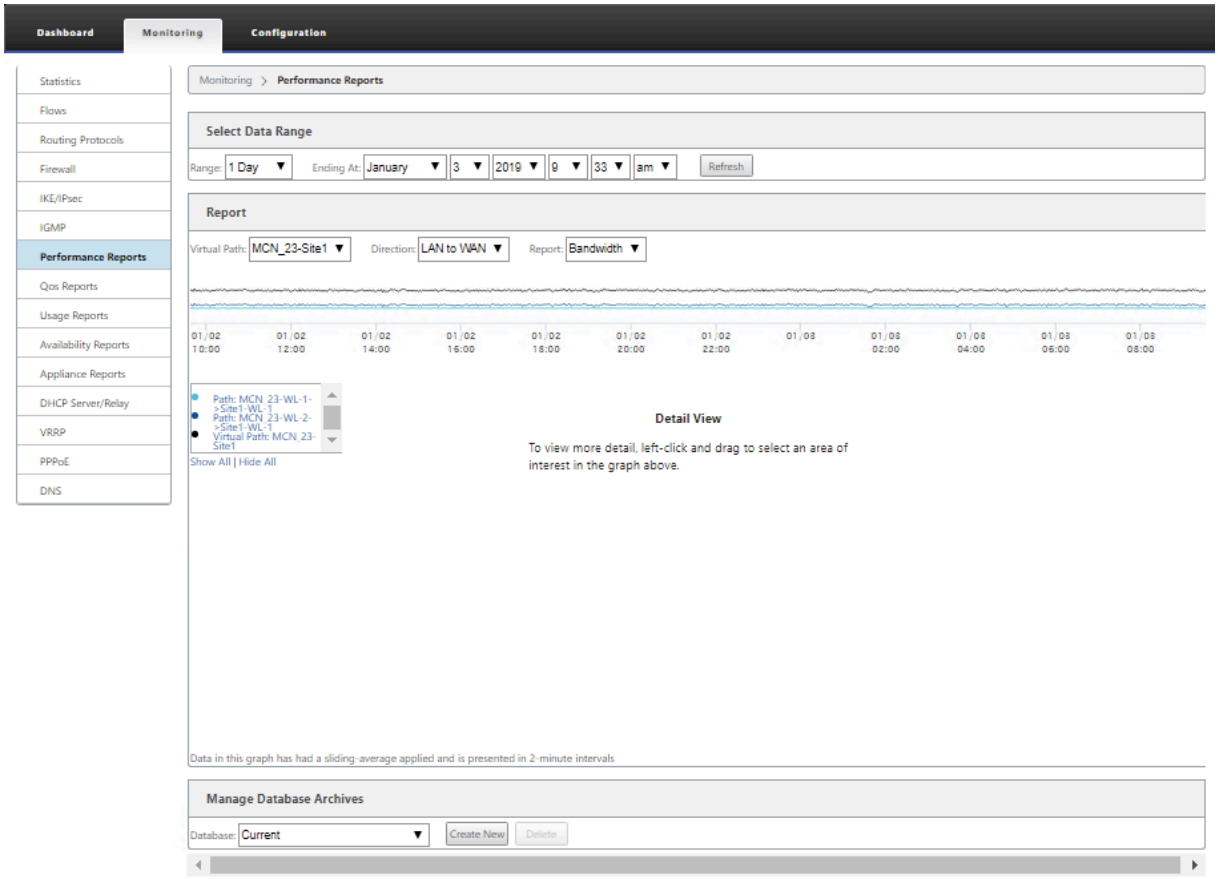
以前のリリースでは、約 4,000 のアプリケーションを識別し、800 のサービス (550 の仮想パス、256 のイントラネットサービス) で構成しました。このデータを格納すると、システム全体のパフォーマンス（データの格納に必要な CPU サイクルとディスク容量）に影響します。また、使用量またはパスごとのデータに関するレポートがサポートされる場合にも影響があります。

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

August 30, 2022

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。

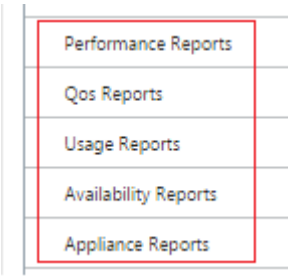
仮想 WAN レポートを生成および表示するには、次の手順を実行します。

1. MCN の管理 Web インターフェイスにログオンし、[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 [フロー（**Flows**）] ブランチのすぐ下にブランチとしてリストされます。



使用可能なレポートタイプは次のとおりです。

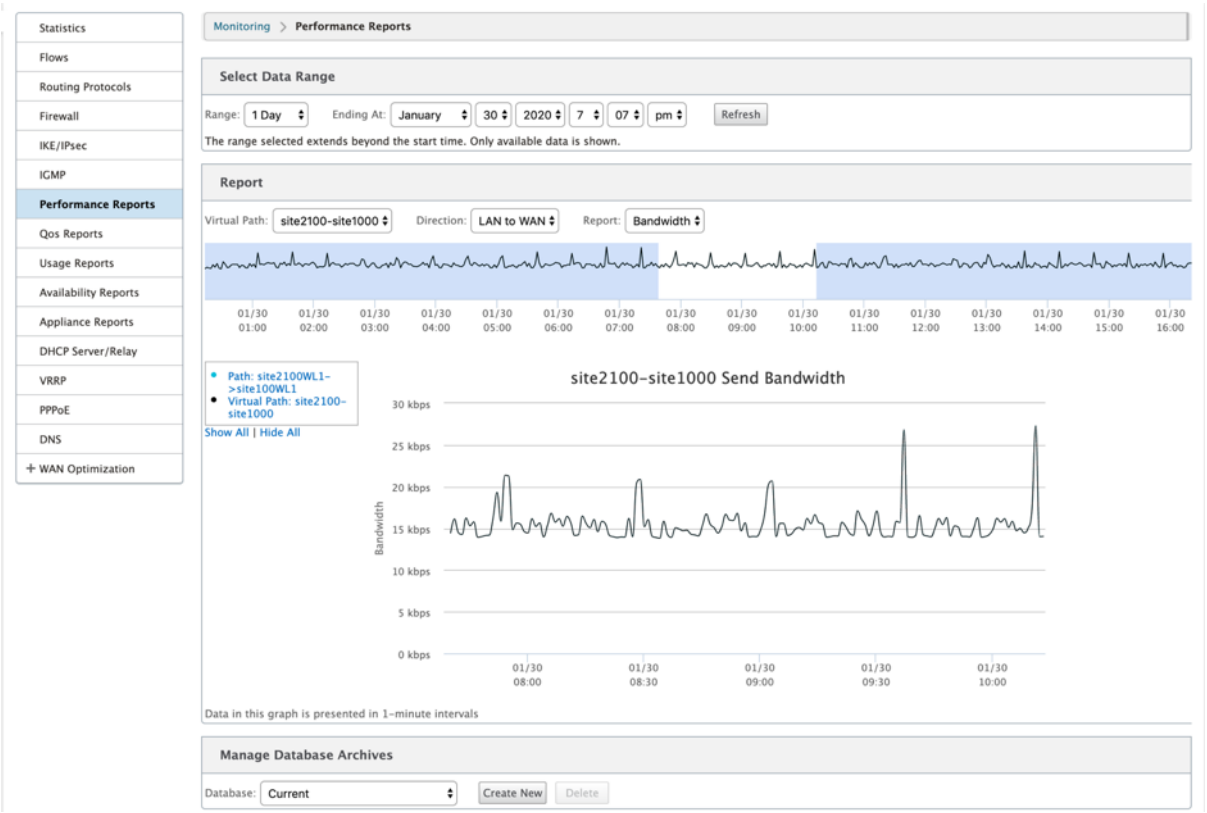
- パフォーマンス・レポート
- **QoS** レポート
- 使用状況レポート
- 可用性レポート
- アプライアンスレポート

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ライン内のパスまたは時間枠の特定の領域を選択します。

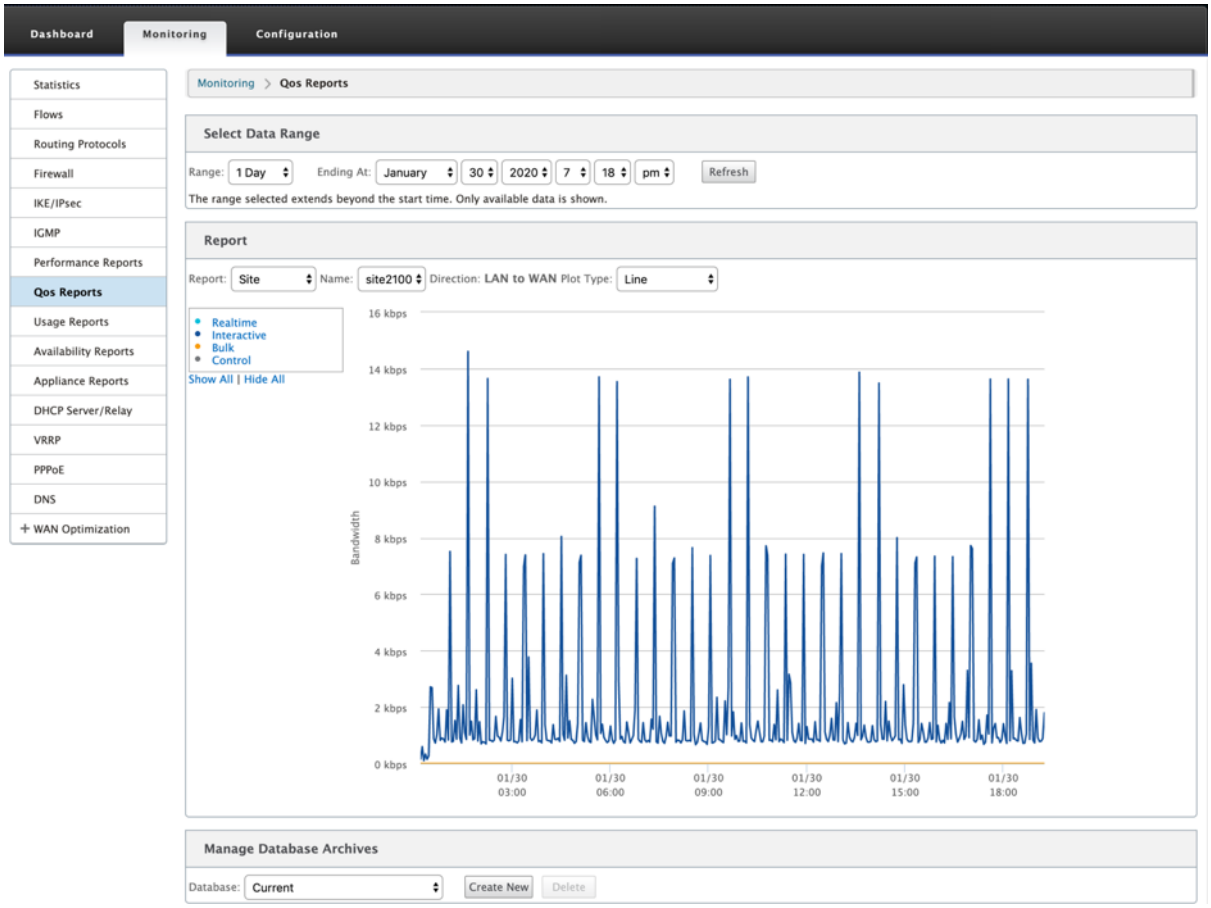


必要に応じてデータ範囲を選択し、次のフィールドを使用してパフォーマンス・レポートを表示できます。

- 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] または [WAN から LAN])。
- 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 ―
  - 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。

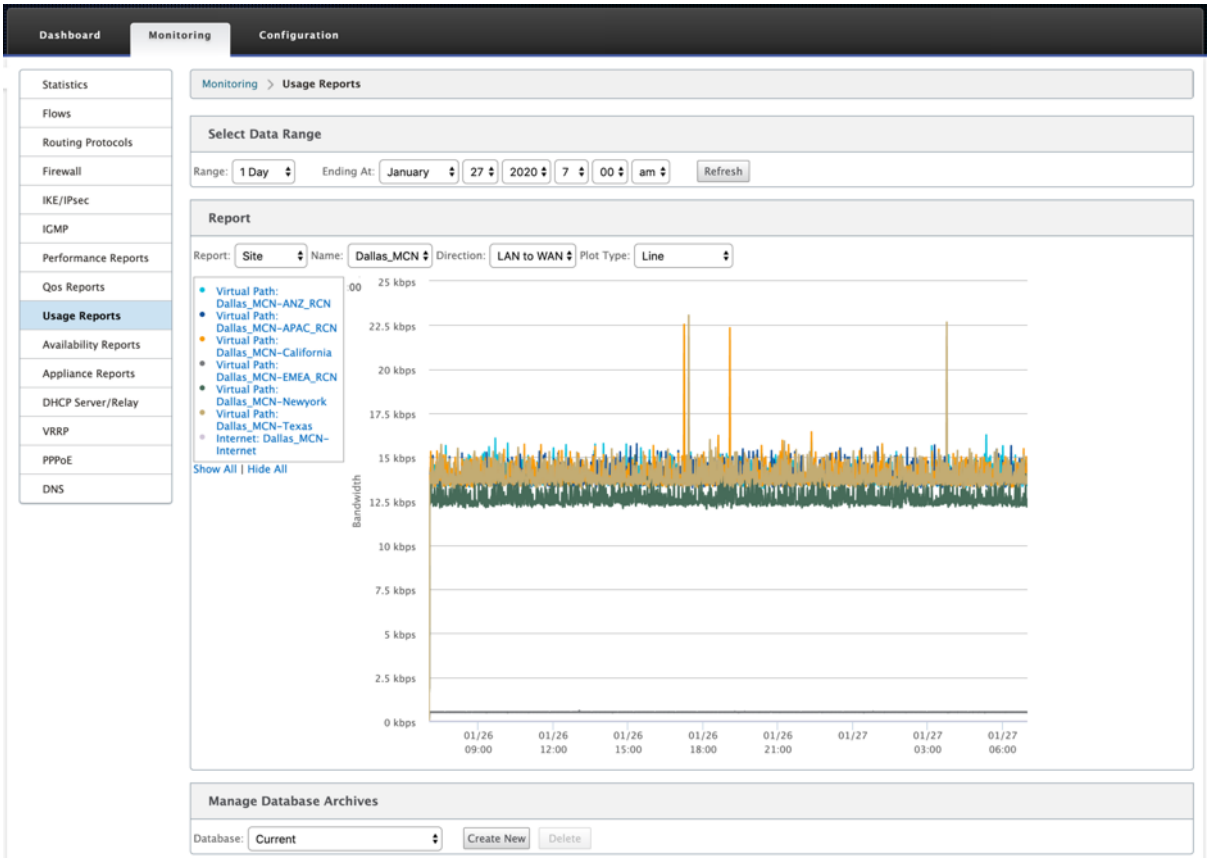


次のメトリックを表示できます。

- リアルタイム： Citrix SD-WAN 構成のリアルタイム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 構成のインタラクティブ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）。
- バルク： Citrix SD-WAN 構成の一括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。
- 制御：ルーティング、スケジューリング、およびリンク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

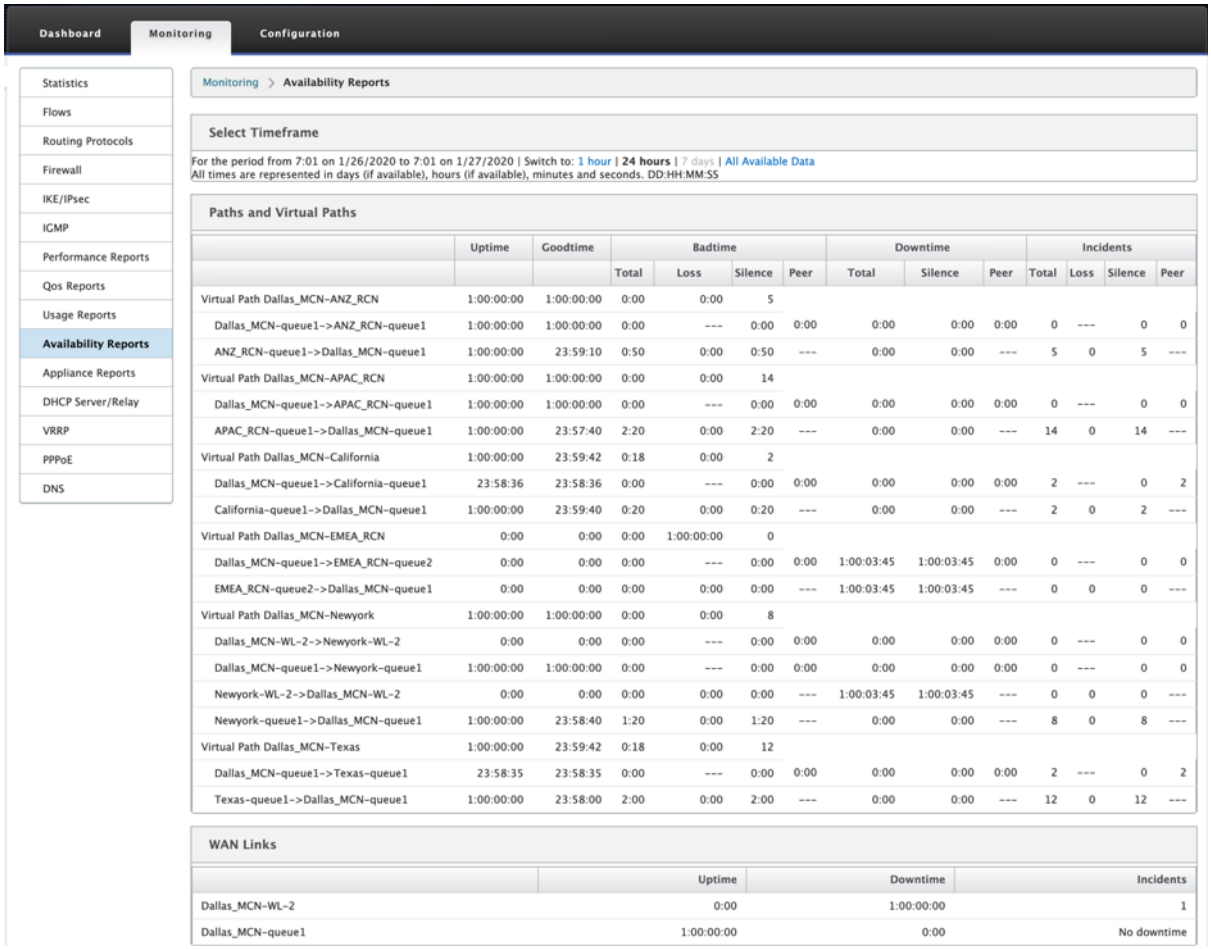
使用状況レポートは、仮想パスの使用状況情報を提供します。



- 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。
-
- 方向**:** 必要に応じて方向 (LAN から WAN または WAN から LAN) を選択します。
-

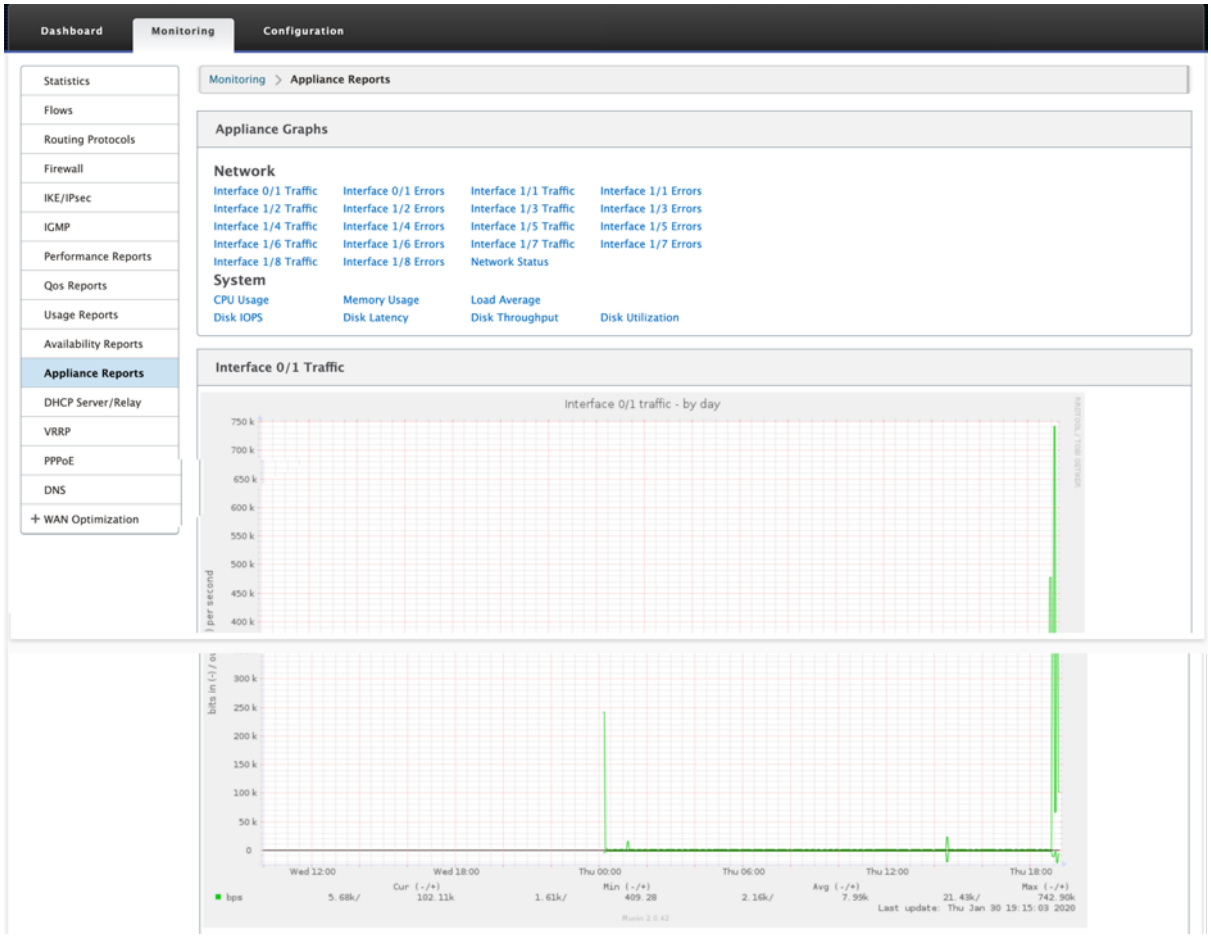
可用性レポート

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。



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

August 30, 2022

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。

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. 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. 必要に応じてフィルタリング基準を設定します。
4. [更新] をクリックします。

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-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。
- 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。
- [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。
- [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 ポリシーで使用されるサービスタイプ。
- サービス名-NAT ポリシーで使用され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 ポリシーで使用される内部ポート範囲。「-」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 ポリシーで使用される外部ポート範囲。「-」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。

診断

August 30, 2022

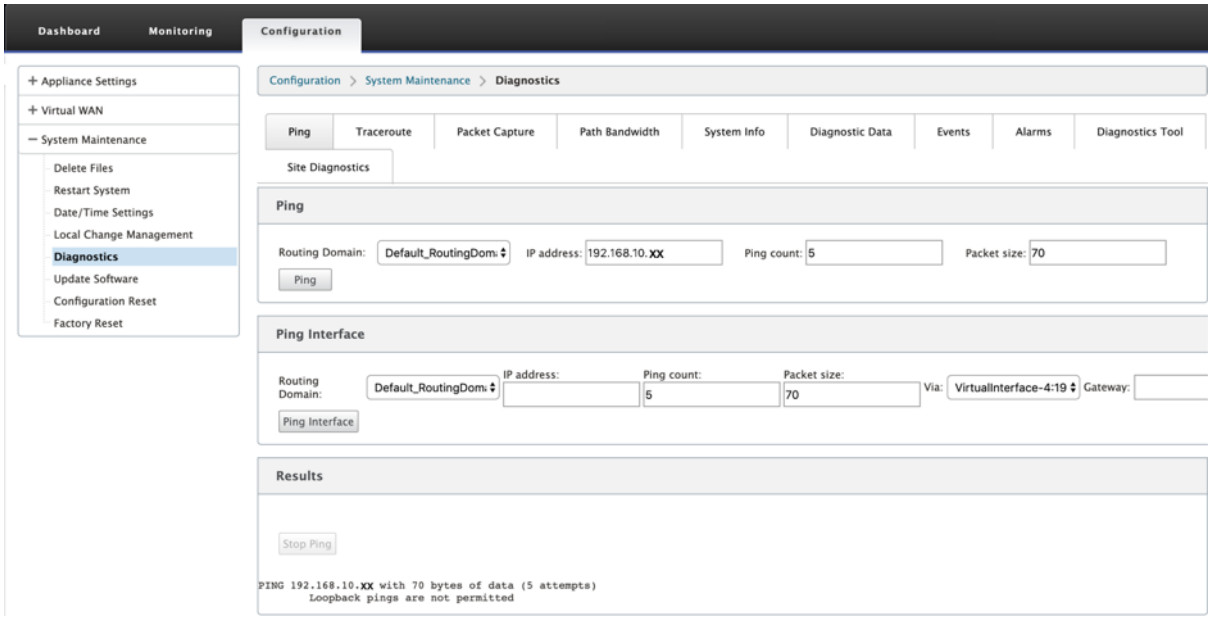
Citrix SD-WAN 診断ユーティリティには、接続の問題をテストおよび調査するための次のオプションが用意されています。

- Ping
- Traceroute
- パケットキャプチャ
- パス帯域幅
- 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。

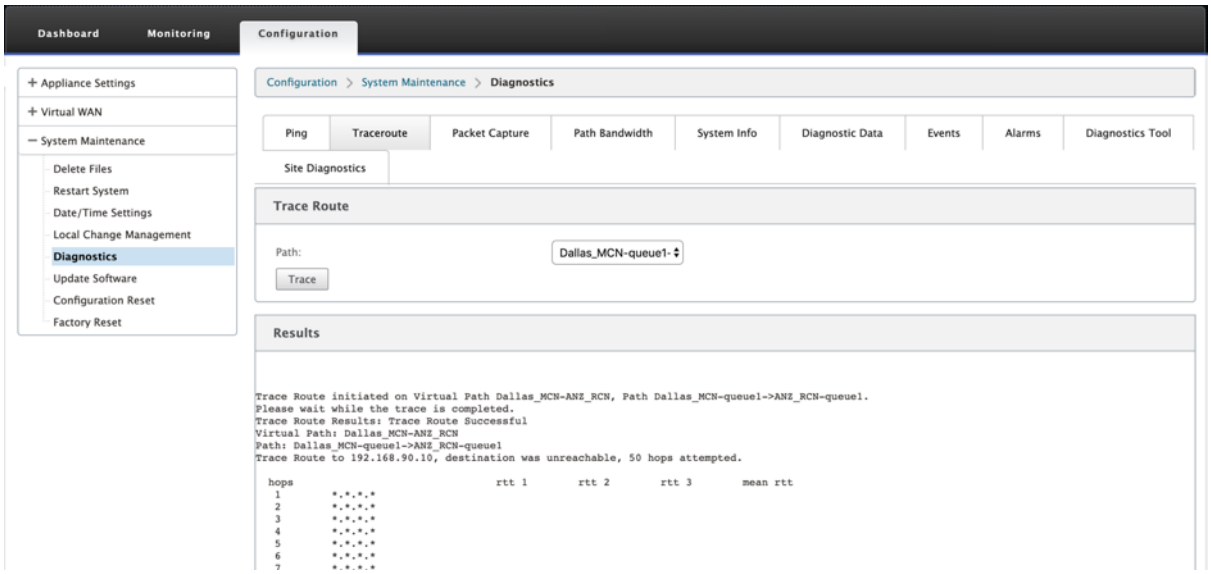


ルーティングドメインを選択します。有効な IP アドレス、ping カウント数 (ping 要求を送信する回数)、およびパケットサイズ (データバイト数) を指定します。[**Ping** の停止] をクリックして、進行中の ping 検索を停止します。

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。

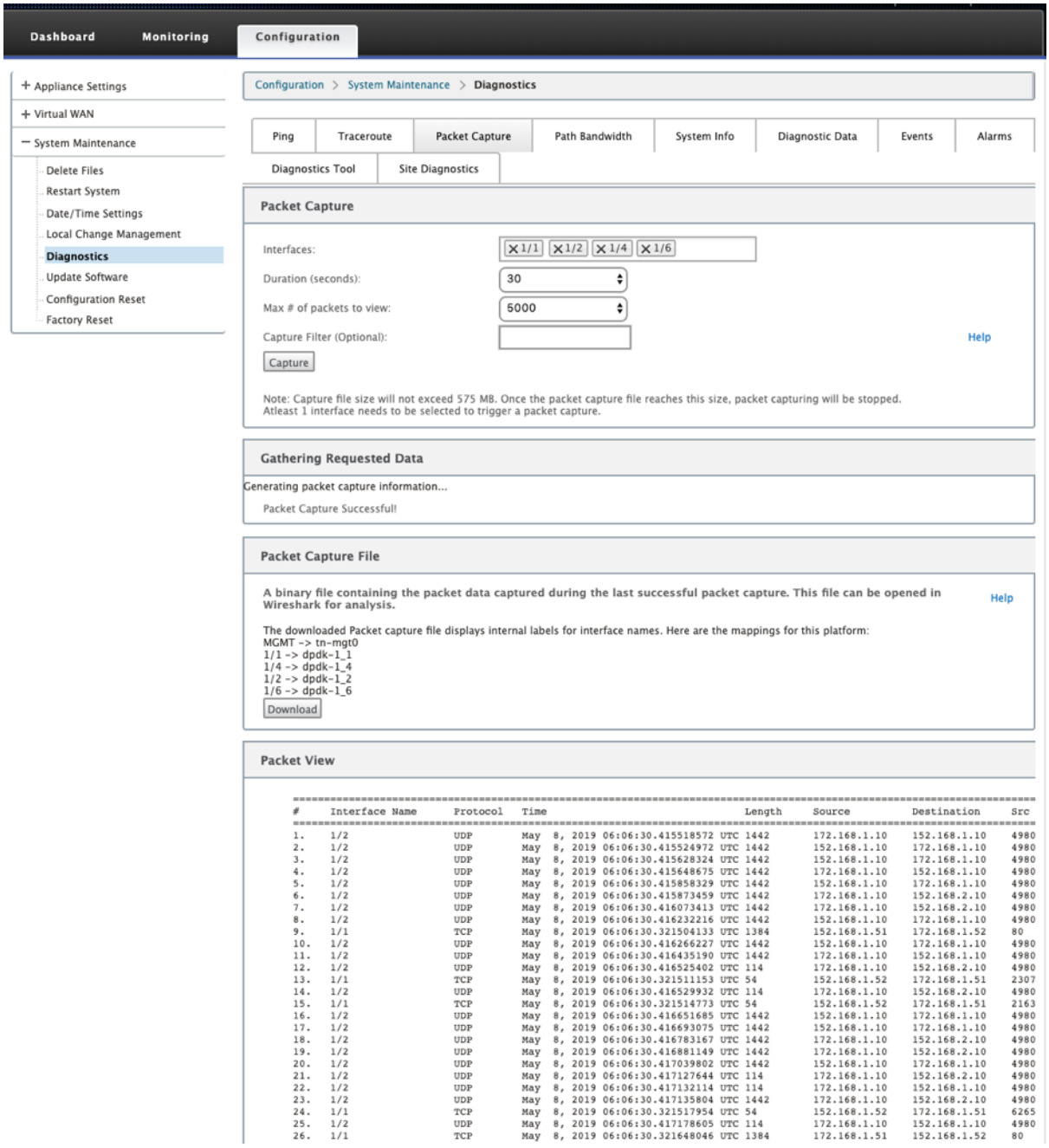


traceroute は、リモートサーバーへのパスまたはルートの検出と表示に役立ちます。**Traceroute** オプションをデバッグツールとして使用して、ネットワーク内の障害点を検出します。

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。



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 (seconds**) —データをキャプチャする必要がある時間の長さ (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] フィールドには、キャプチャす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指定できます。パケットはフィルター文字列と比較され、比較結果が true の場合、パケットがキャプチャされます。フィルターが空の場合、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。

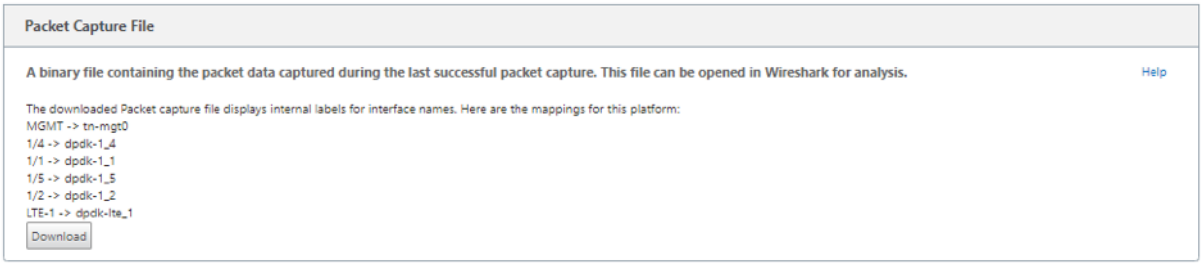
[**Capture**] をクリックして、パケットキャプチャ結果を表示します。最後に成功したパケットキャプチャ中にキャプチャされたパケットデータを含むバイナリファイルをダウンロードすることもできます。

リクエストされたデータの収集

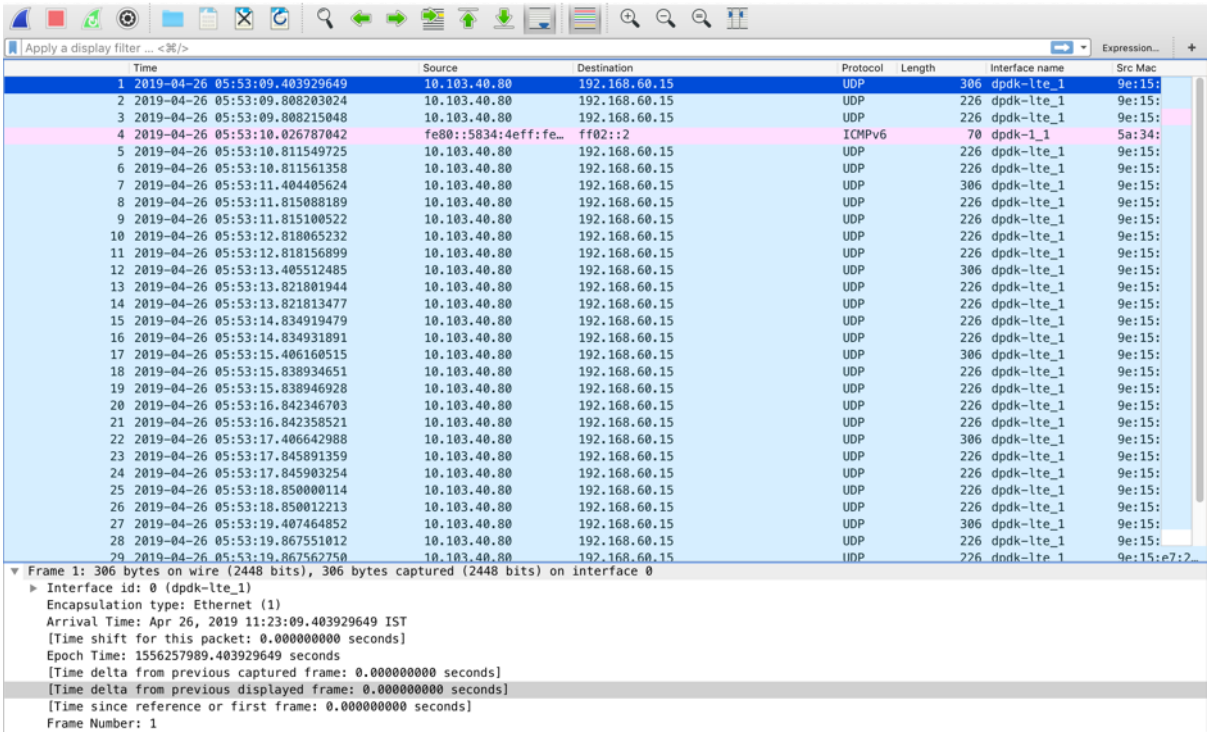
この表では、パケットキャプチャ情報の生成のステータス（パケットキャプチャが成功したかどうか、パケットキャプチャがないかどうか）を確認できます。

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。



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。

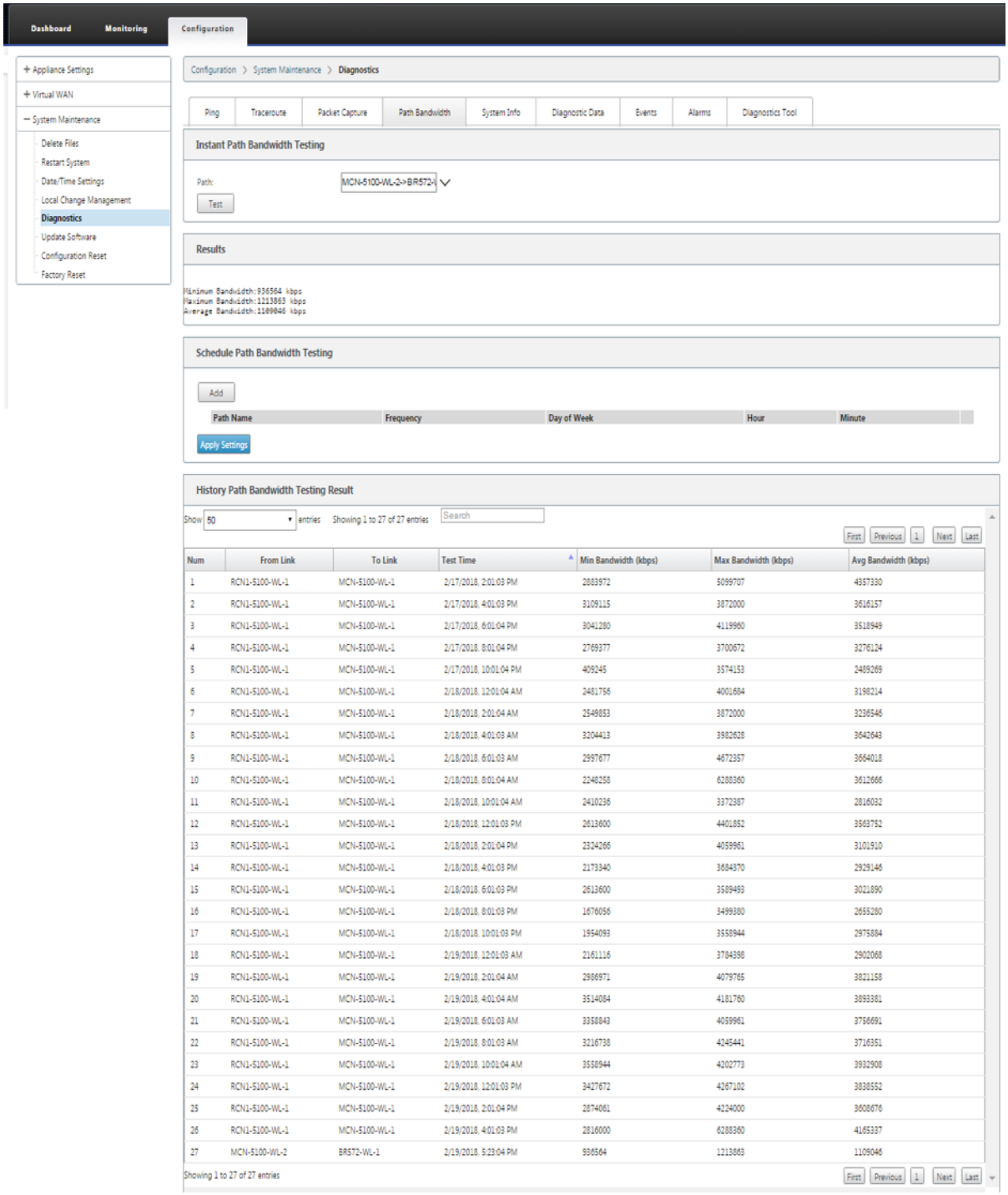


パケットビュー

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。



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

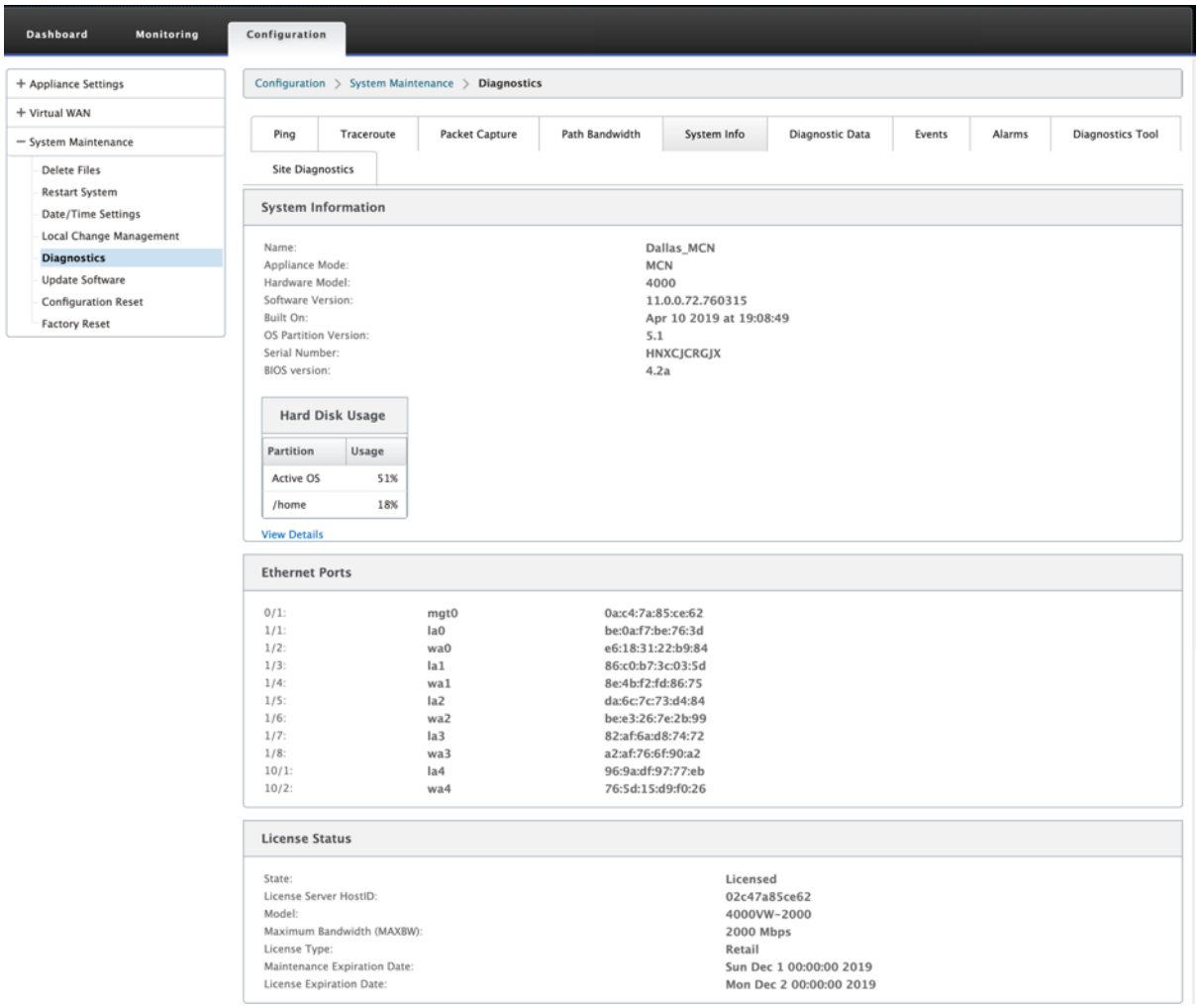
スケジュールしたりできます。

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。

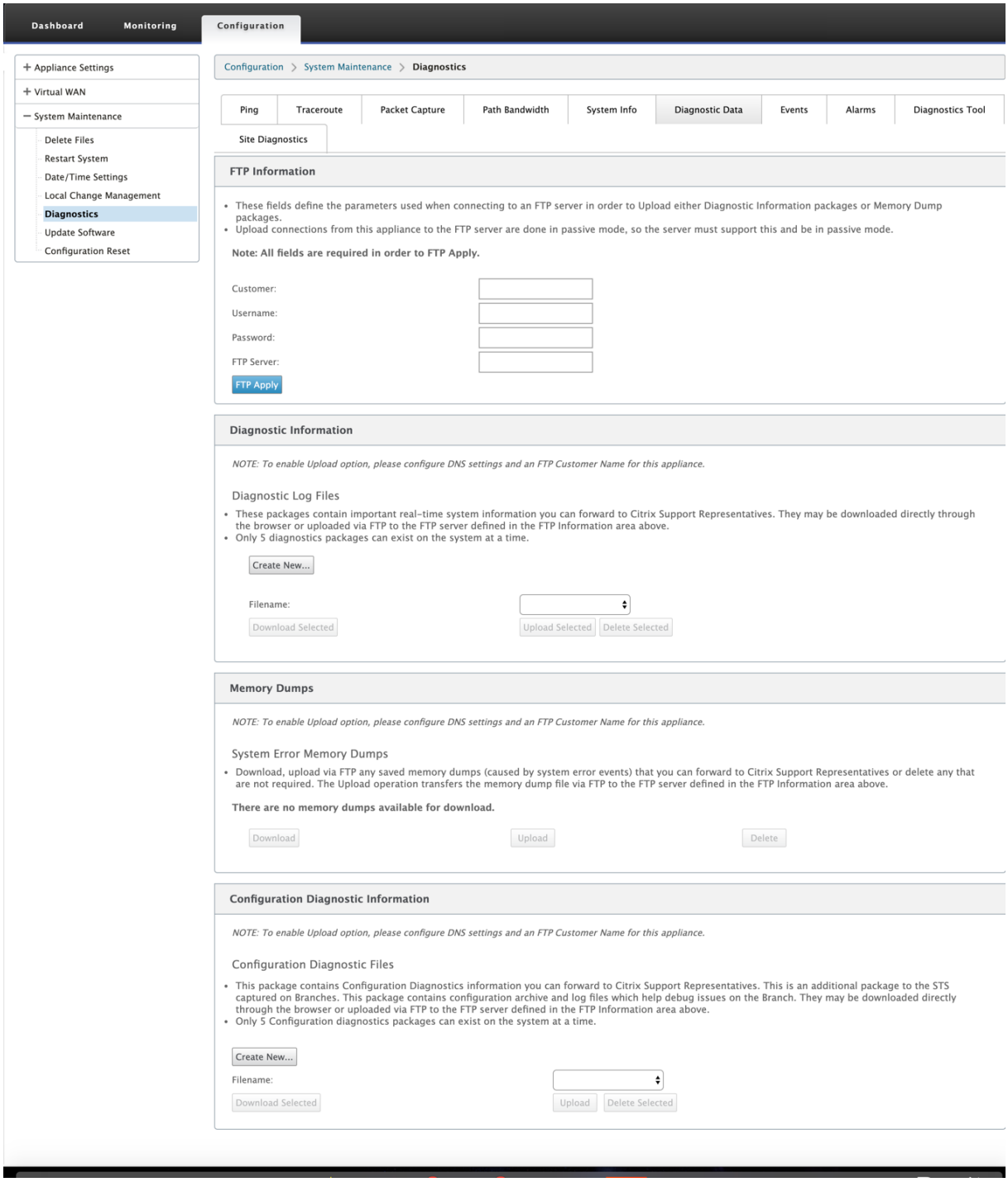


[システム情報（**System Info** ）] には、デフォルトに設定されていないすべてのパラメータが一覧表示されます。この情報は読み取り専用です。なんらかの設定ミスが疑われる場合にサポートが使用します。問題を報告すると、このページで 1 つ以上の値を確認するように求められる場合があります。

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。



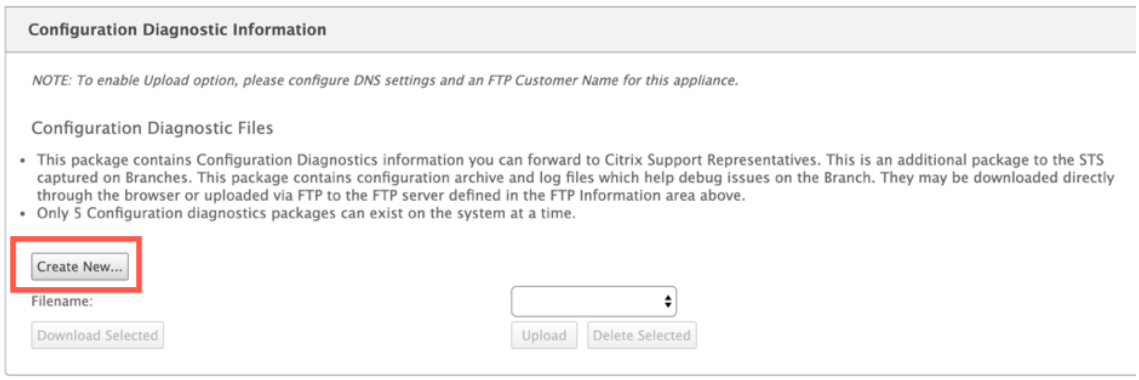
診断データには次のものが含まれます。

- 「**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。

  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。

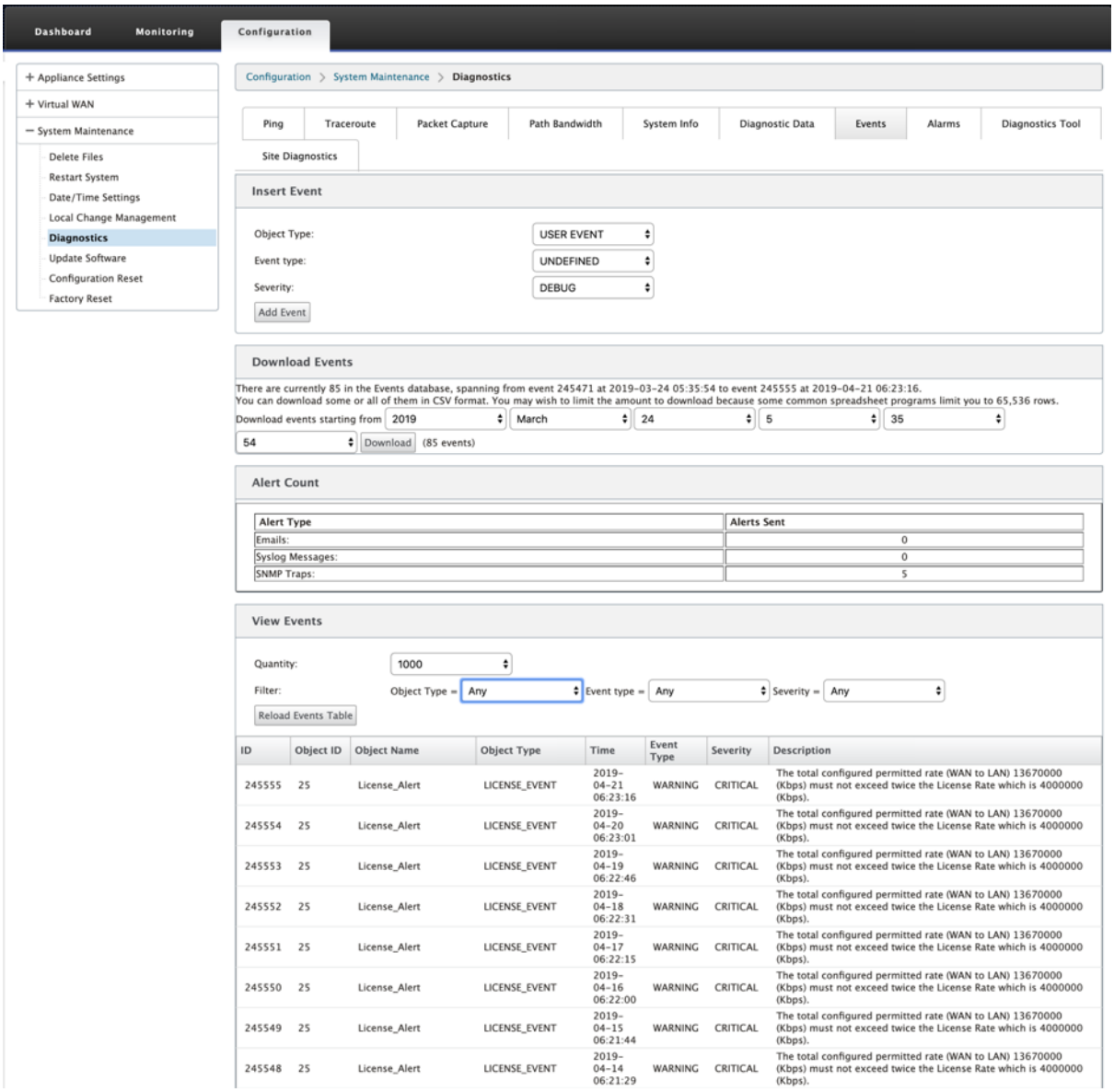
  > 注：
  >
  > デフォルトでは、[アップロード] オプションは無効モードになっています。これを有効にするには、このアプライアンスの **DNS** 設定と **FTP** カスタマー名を設定します。

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。



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。

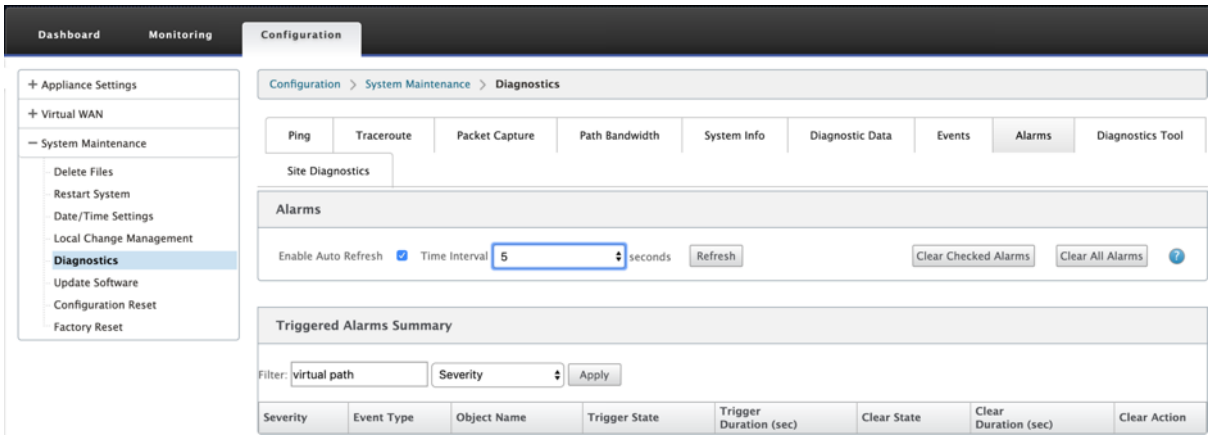
イベントの詳細は、[View **Events**] テーブルで確認できます。イベントの詳細には、次の情報が含まれます。

- **ID** —イベント ID。

- 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**)** —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。

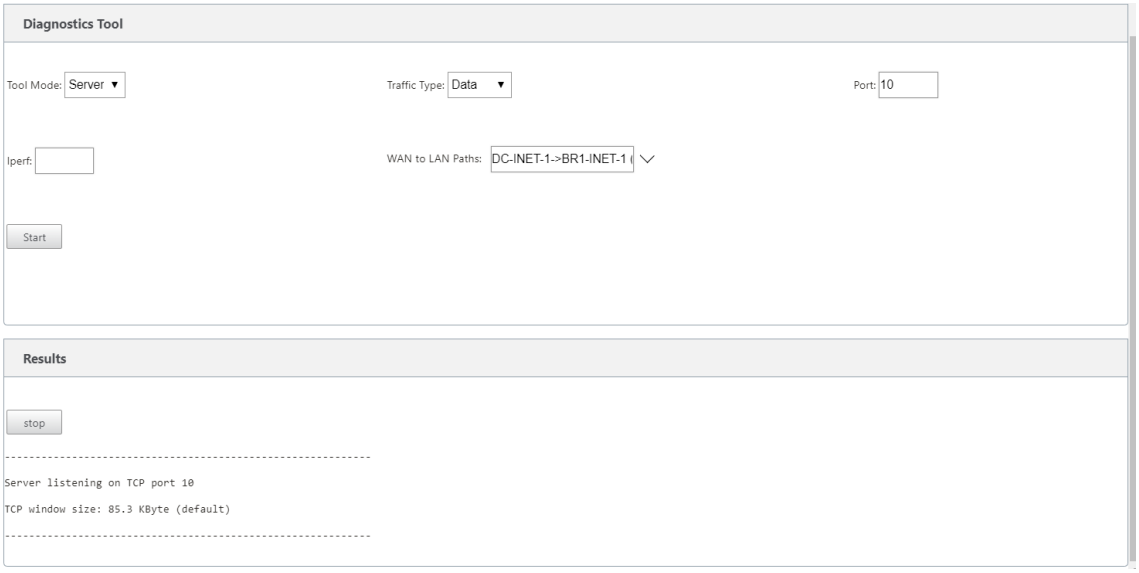
診断ツールでは、次の 2 種類のトラフィックを生成できます。

- 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。

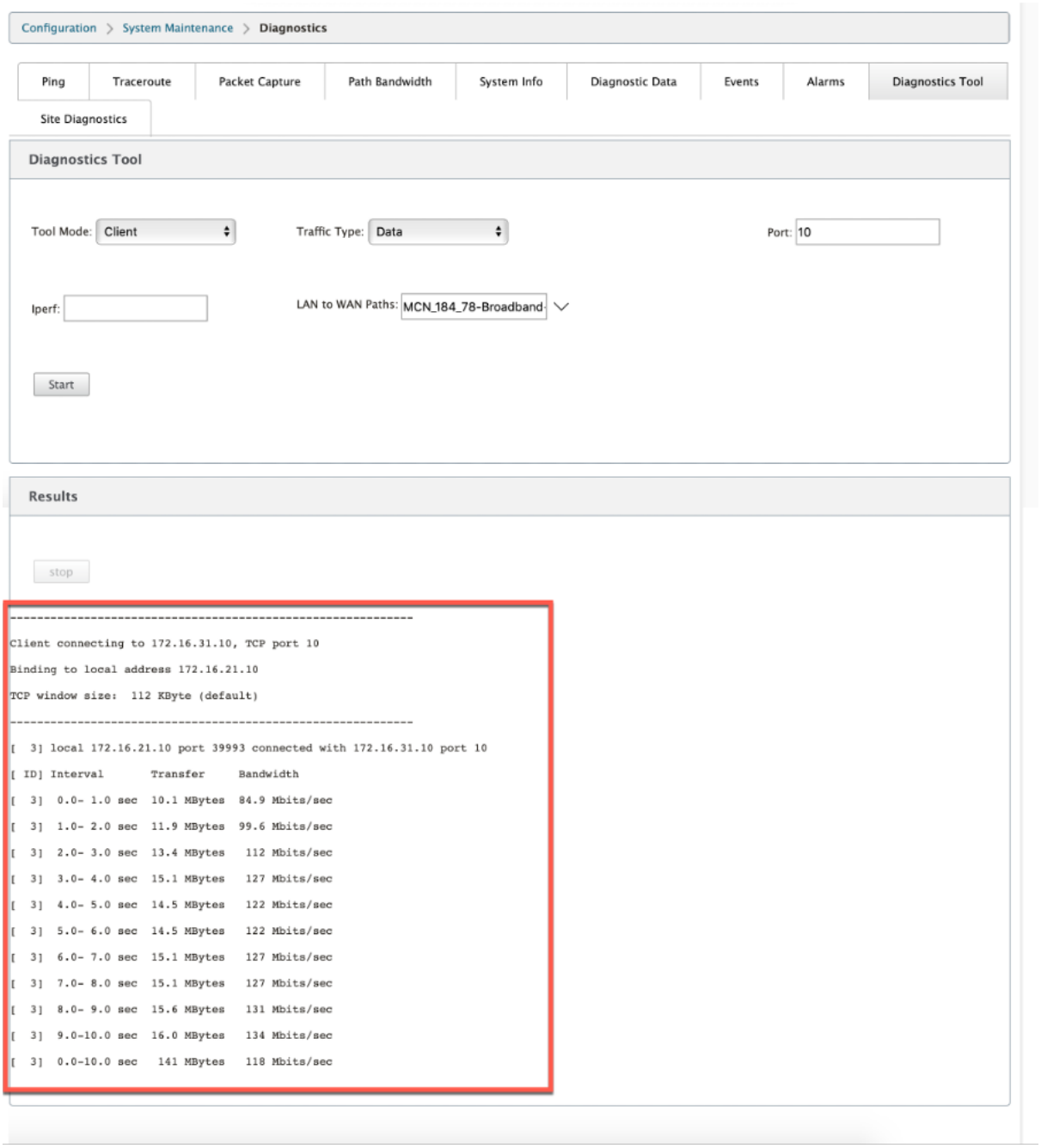


2. 「ツールモード」フィールドで、「アプライアンス上のサーバ」を選択し、選択したパスのリモートエンドに存在するアプライアンスで「クライアント」を選択します。
3. [トラフィックタイプ（Traffic Type）] フィールドで、診断トラフィックの種類（[制御] または [データ]）を選択します。両方のアプライアンスで同じトラフィックタイプを選択します。
4. [ポート（**Port**）] フィールドで、診断トラフィックを送信する **TCP/UDP** ポート番号を指定します。両方のアプライアンスで同じポート番号を指定します。
5. [**Iperf**] フィールドに、IPERF コマ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。

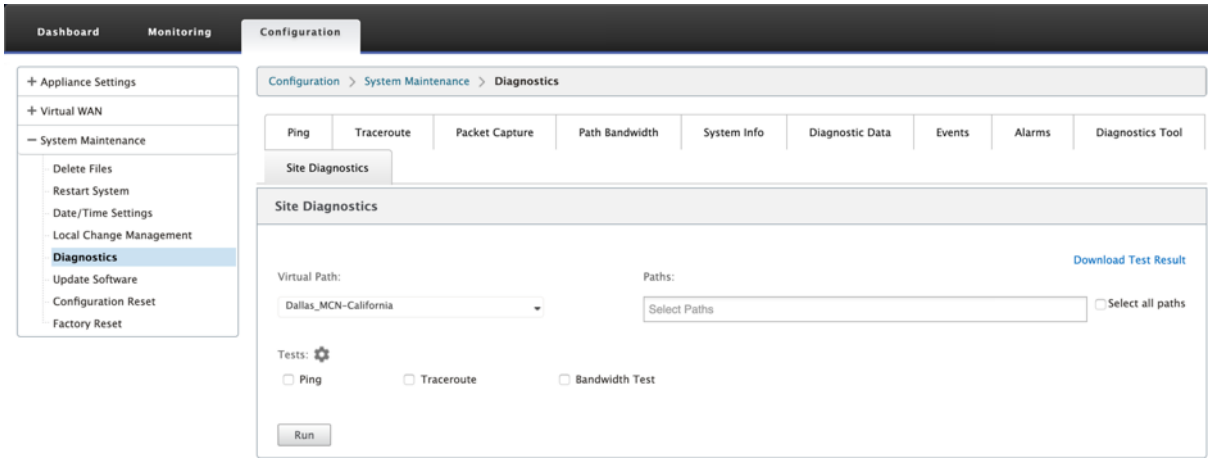
結果には、選択したアプライアンスのモード（クライアントまたはサーバー）と、テストが実行された TCP または UDP ポートが表示されます。テストの合計期間に達するまで、指定された間隔で転送されたデータおよび使用された帯域幅が定期的に表示されます。



サイト診断

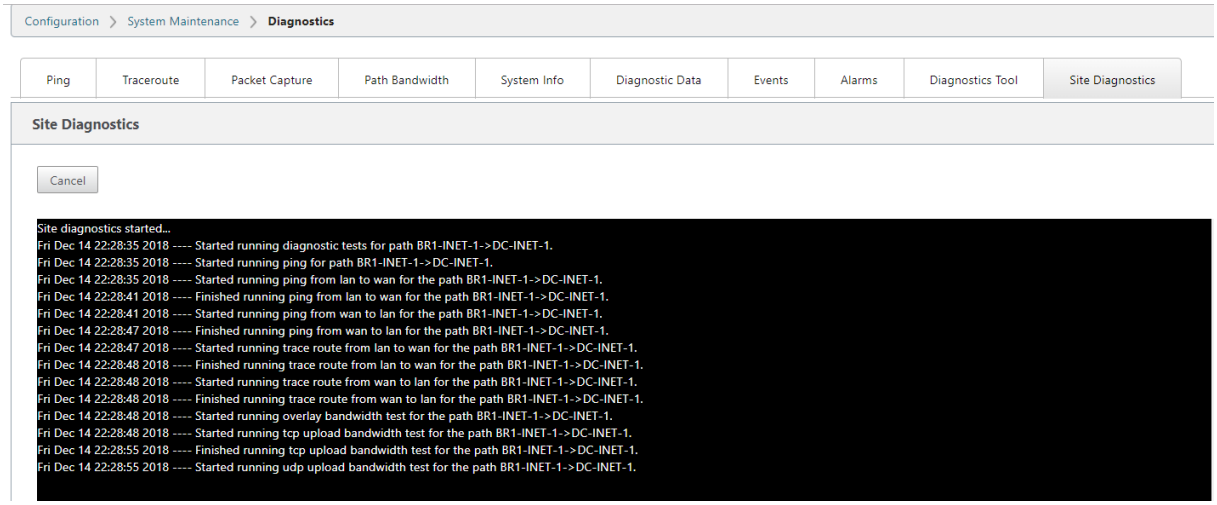
Citrix SD-WAN ネットワークの異なるサイトで構成された WAN リンクの帯域幅使用状況、ping をテストし、トレースルートを実行することができます。既存の設定の問題のトラブルシューティングに役立つ情報を提供します。

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。



[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

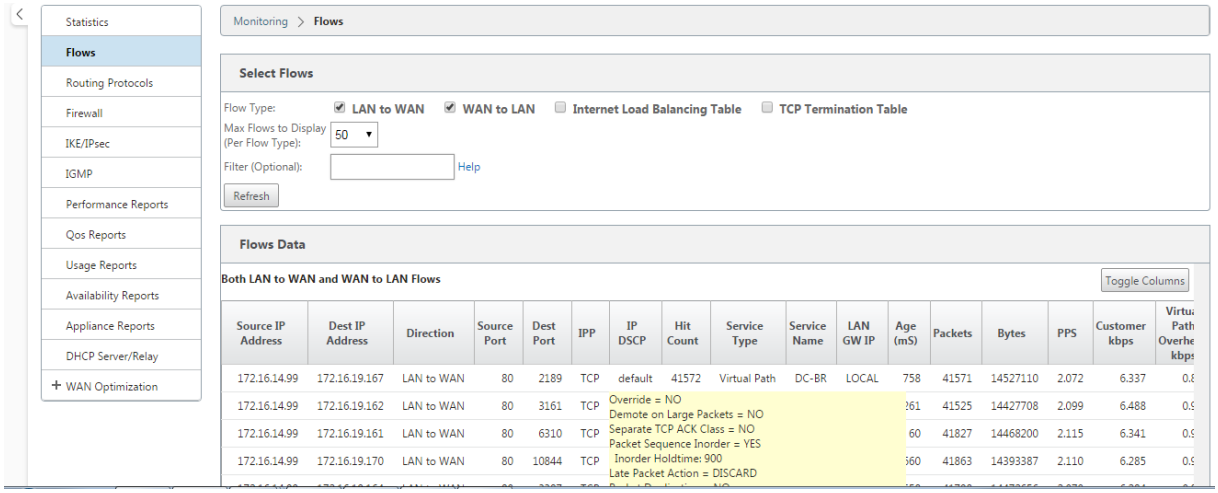
August 30, 2022

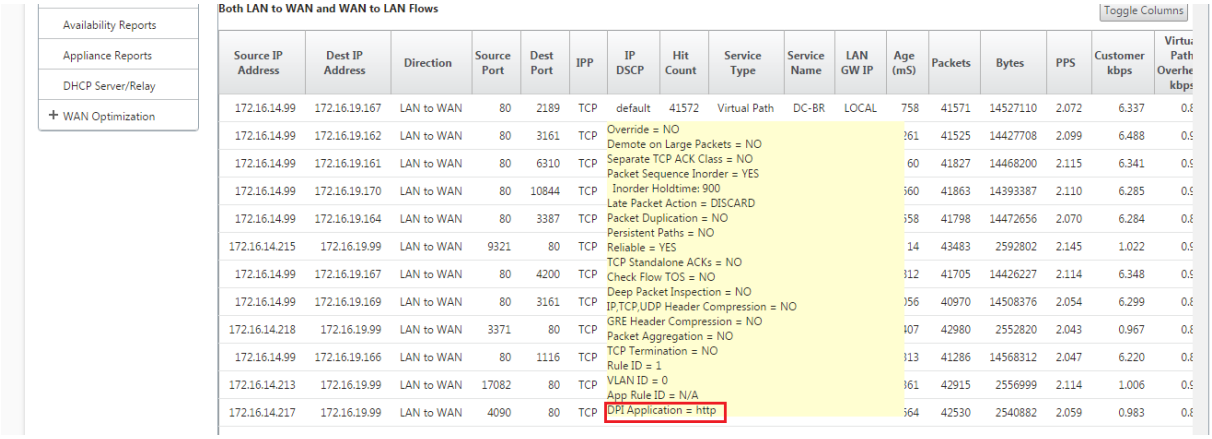
[Monitoring] タブでは、パスマッピングと帯域幅使用率の拡張が実装され、トラフィックフローが表示されます。たとえば、1 つの仮想パスだけがネットワーク接続を提供していて、その仮想パスが非アクティブになると、新しい最適パスが選択され、最初のパスが最後の最適パスになります。このシナリオは、帯域幅の需要が少なく、パスが 1 つしか選択されていない場合に実装されます。

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、パステーブルが 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が保存され、[SD-WAN GUI **Monitoring**]-> [**Flows**] ページに表示されます。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。





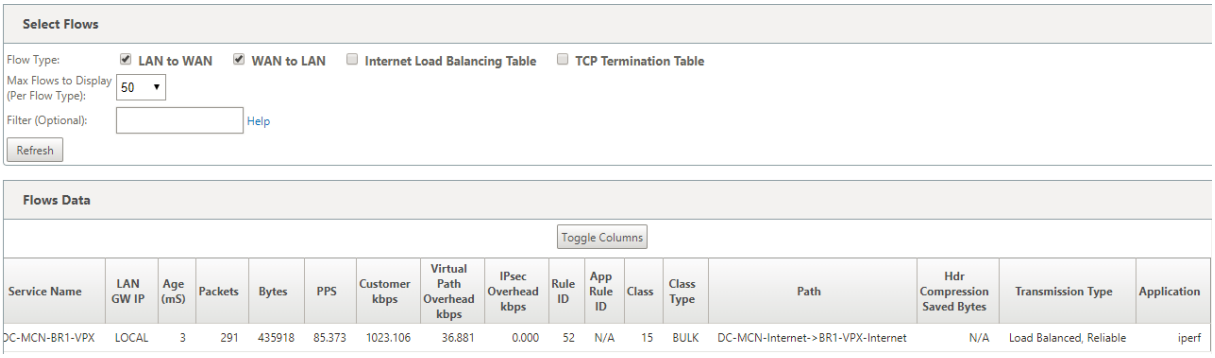
SD-WAN GUI でのトラフィックフローのパス情報のモニタリング

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。

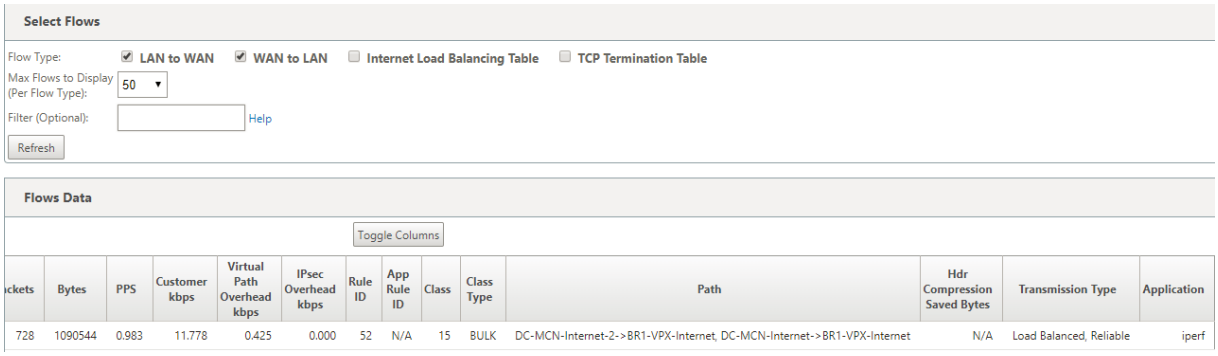
負荷分散伝送モード**:**

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**** パスが 1** つだけ選択され、伝送タイプのタイプが [負荷分散] として表示されます。



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により、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-**インターネットであることを示すことができます。

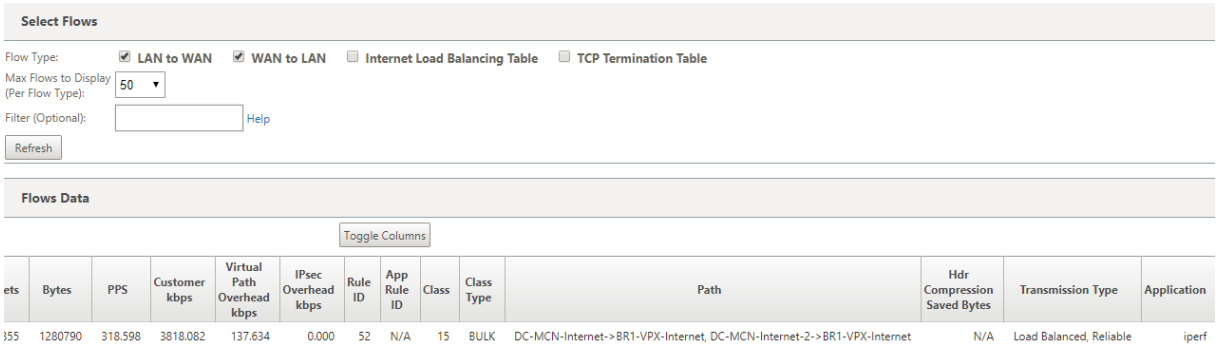
この例の最後の最適パスは、どのパスが以前に接続したかを示すインジケータです。



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。

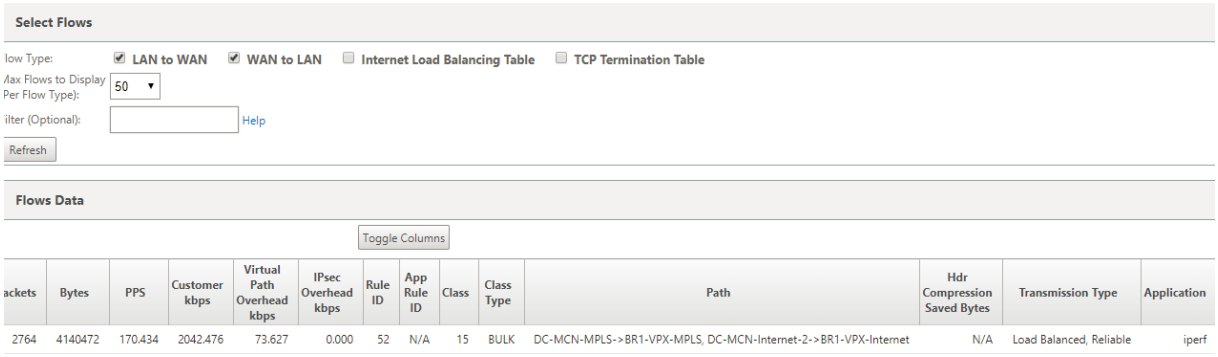
DC-MCN-インターネット**->BR1-VPX** インターネット、**DC-MCN-Internet2->BR1-VPX-Internet** が、フローデータテーブルに示されている 2 つのパスであることを確認して下さい。

> 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。



次の図は、トラフィックがまだ流れているときに、現在のベストパス（**DC-MCN-Internet->BR1-VPX-Internet**）が WAN 属性で利用不可/非アクティブ/劣化している場合、選択された現在のベストパスがフローデータテーブルのパスセクションの最初に表示されることを示しています。トラフィックを処理している最後の最適パスで指定します。

DC-MCN-Internet->BR1-VPX-Internet はもう最適ではなかったので、システムによって新しい現在のベストパスが **DC-MCN-MPLS->BR1-VPX-MPLS** として選択され、現在のベストパスと共にアクティブに接続を提供している最後のベストパスは **DC-MCN-Internet2->BR1-VPX-Internet** です。両方とも帯域幅の現在のトラフィック需要に必要です。



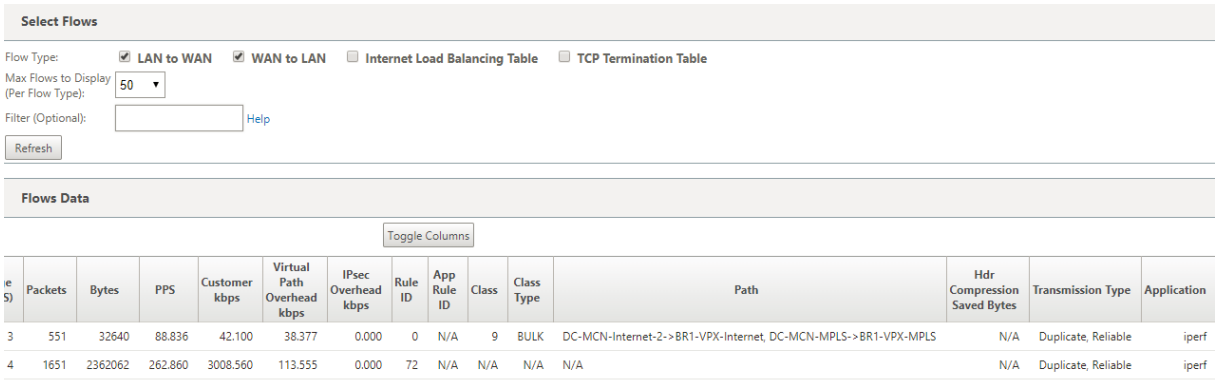
重複送信モード

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。

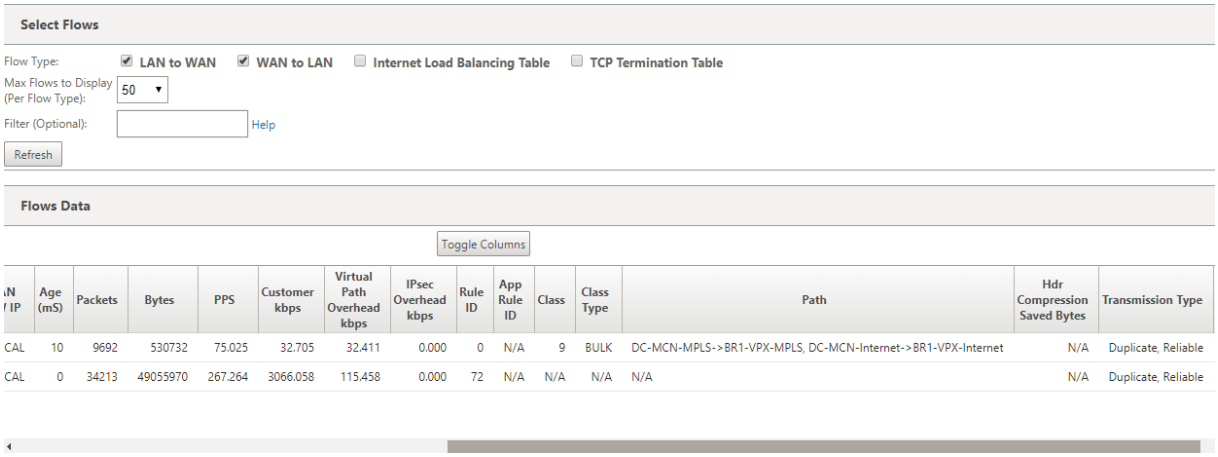
パスマッピングでは、フローテーブルの path セクションに 2 つのパスがある限り、複製によってフローを処理するパスが 2 つあることがわかります。

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。

下の図では、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-Internet**、**DC-MCN-MPLS->BR1-VPX-MPLS**）があります。



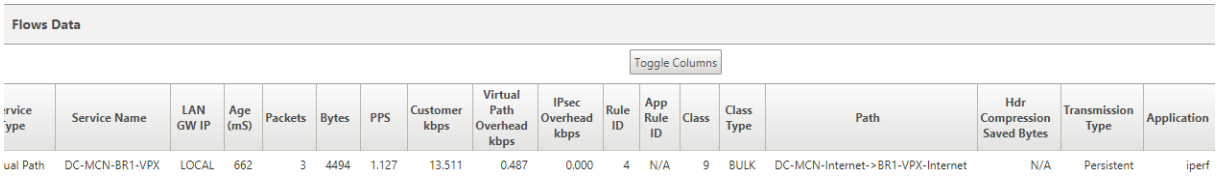
次の図は、トラフィックが流れるときに、現在の最適パスの 1 つが非アクティブになった場合、別のパスが選択され、[**Flows Data**] テーブルのパスセクションの一部として 2 つのパスが残っていることを示しています。



永続パス送信モード

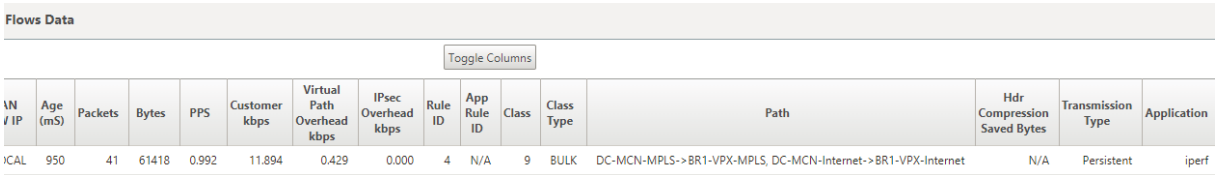
永続パス送信モードは、パス遅延インピーダンスに基づいてフローのパケットを保持するのに役立ちます。

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ベストパスは **1** つだけあります。



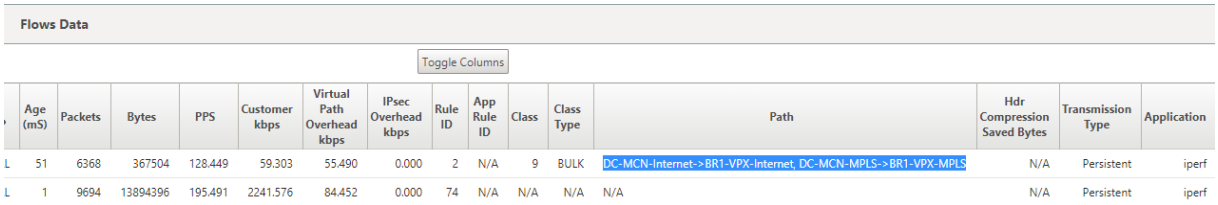
次の図は、**DC-MCN-Internet->BR1-VPX-Internet** パスが遅延傾向になるか無効になっている場合、新しいパスが有効になり、現在のパス **DC-MCN-Internet->BR1-VPX-Internet** が最後の最適パスになることに気付くことを示しています。

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。



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。

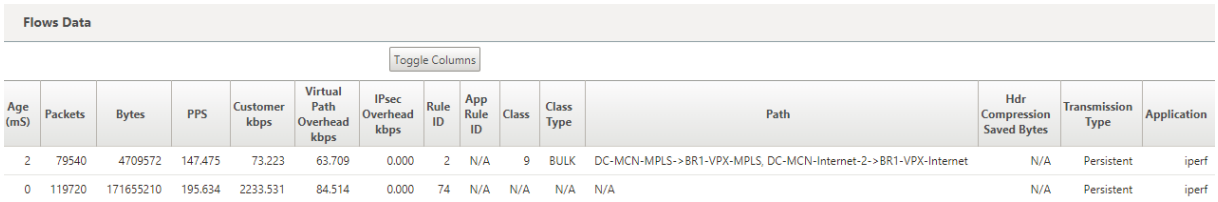
次の図は、最初は 3 つ以上のパスしか必要とせず、パス遅延インピーダンスの交差（50 ms）がない限り、フローは永続的であることを示しています。取られる 2 つのパスは、**DC-MCN-**インターネット**->BR1-VPX-**インターネット、**DC-MCN-MPLS->BR1-VPX-MPLS** として示されます。


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 のベストパスの 1 つが高遅延になるか、または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

August 30, 2022

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 Standard Edition（物理アプライアンスと仮想アプライアンス）のすべてのプラットフォームモデルに適用されます。

> 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。

アプライアンスは **DHCP** サーバに到達できない状態で電源を入れます。

- 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

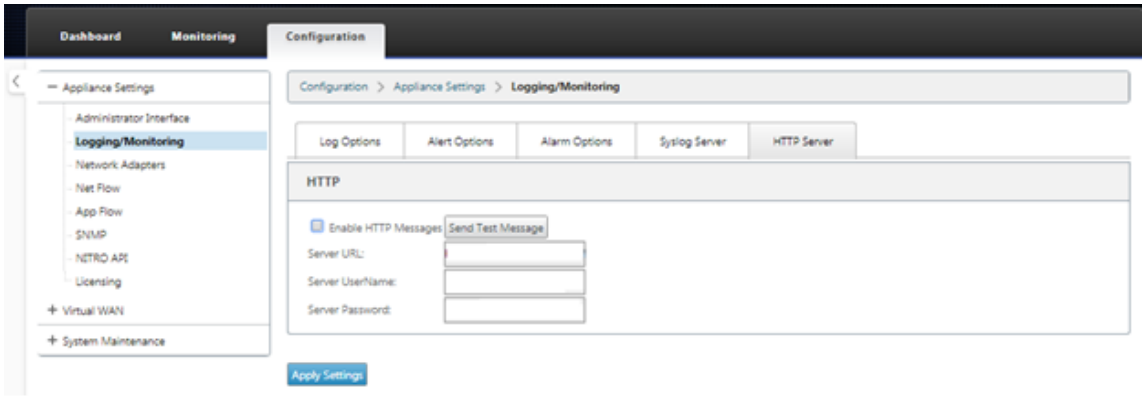
August 30, 2022

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 E メールおよび SNMP イベントに似ています。

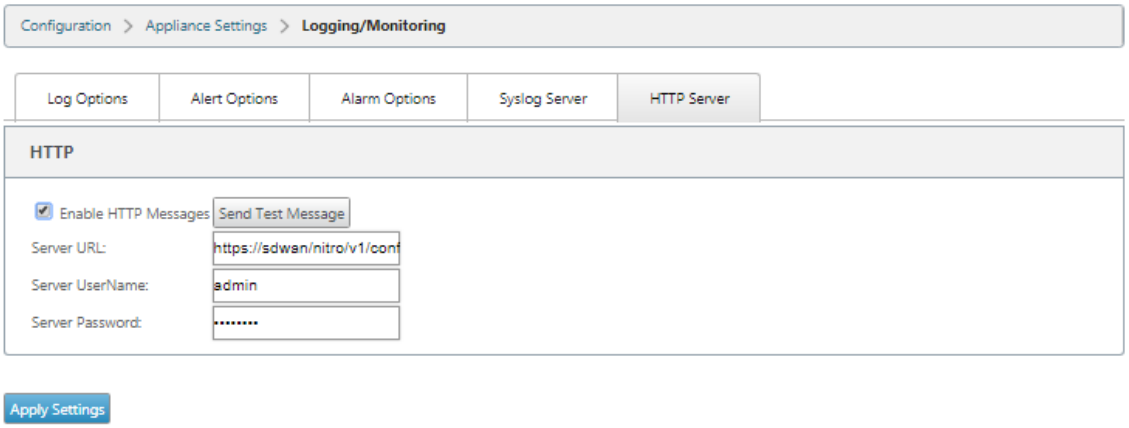
セッションベースの HTTP ポスト通知は、[Service Now] などの外部サービスに送信されます。HTTP サーバーのイベント通知は、Citrix SD-WAN アプライアンス GUI および Citrix SD-WAN Center で構成できます。

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. 設定 > ロギング/モニタリング > **HTTP** サーバにナビゲートして下さい。



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。** サーバユーザ名とサーバパスワードを入力します **。

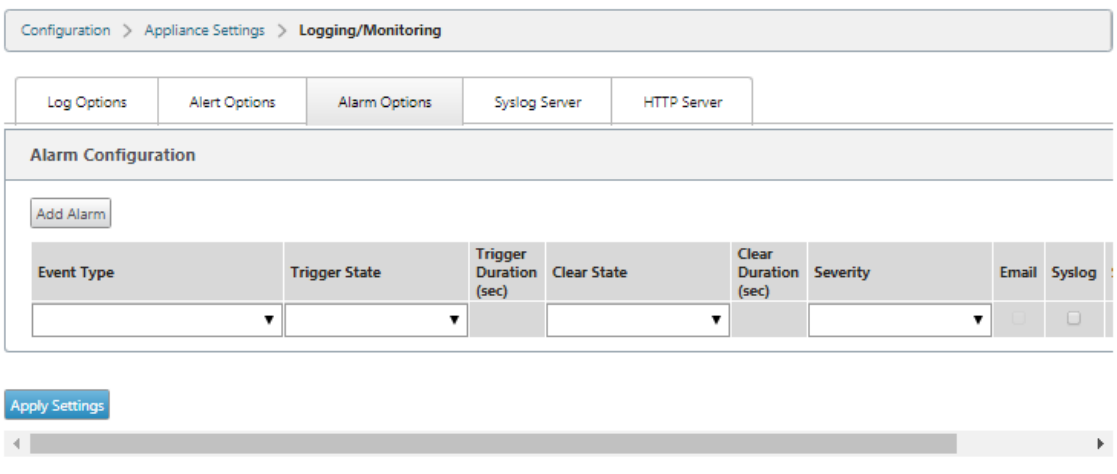


4. [設定の適用] をクリックします。HTTP サーバー通知設定が適用されると、ページが更新されます。

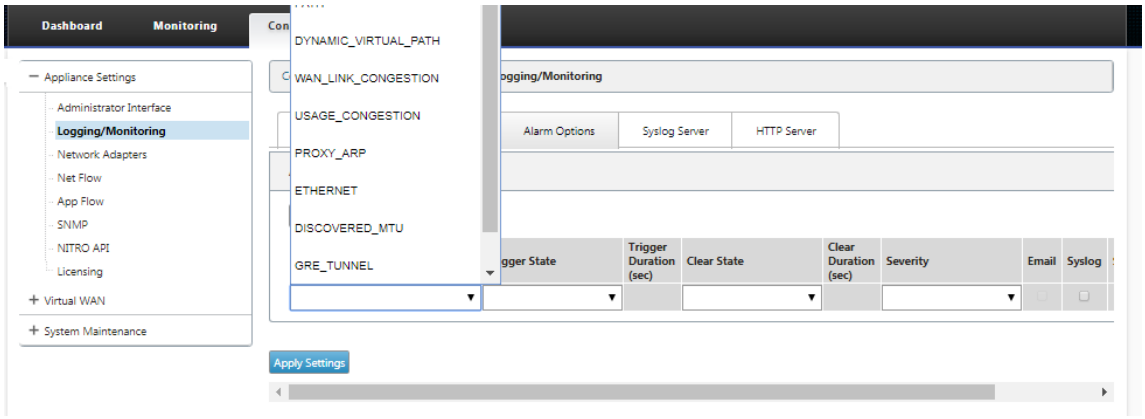
> 注
>
> [テストメッセージの送信（Send Test Message）] オプションを使用して、HTTP サーバ接続が成功したことを確認します。

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。

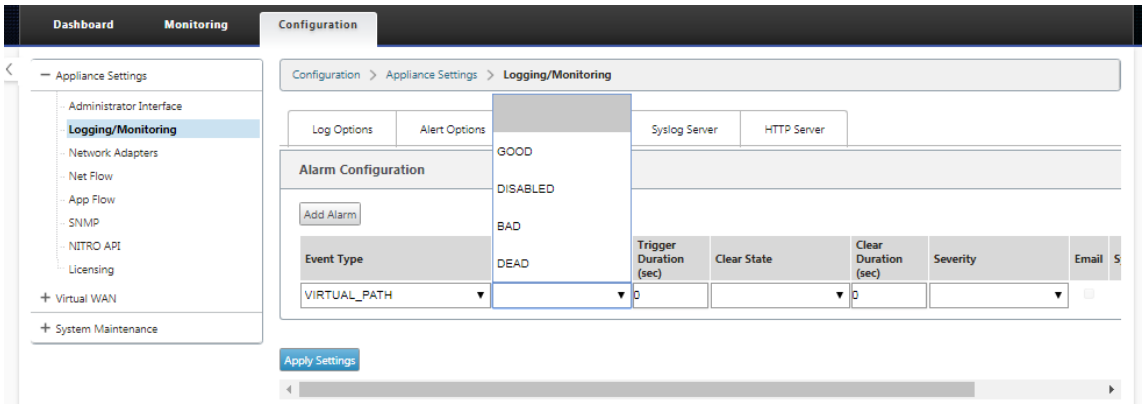


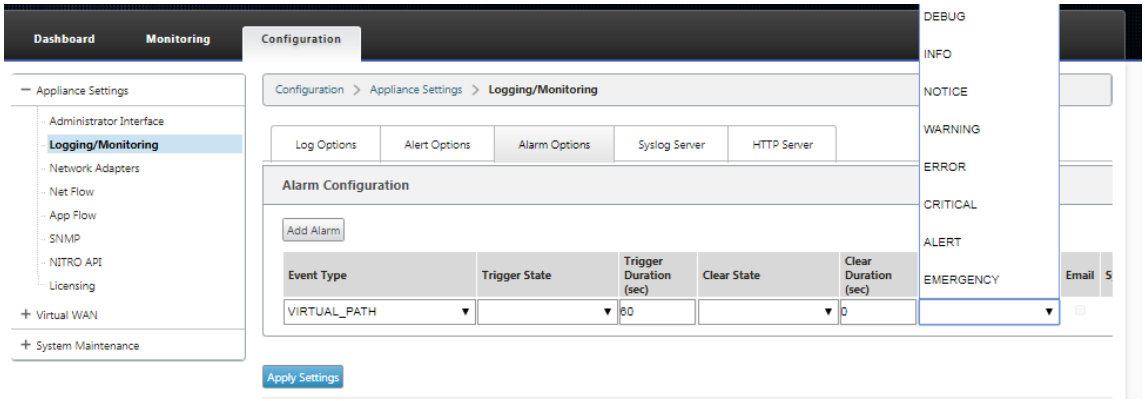
3. ドロップダウンリストから [イベントタイプ] を選択します。



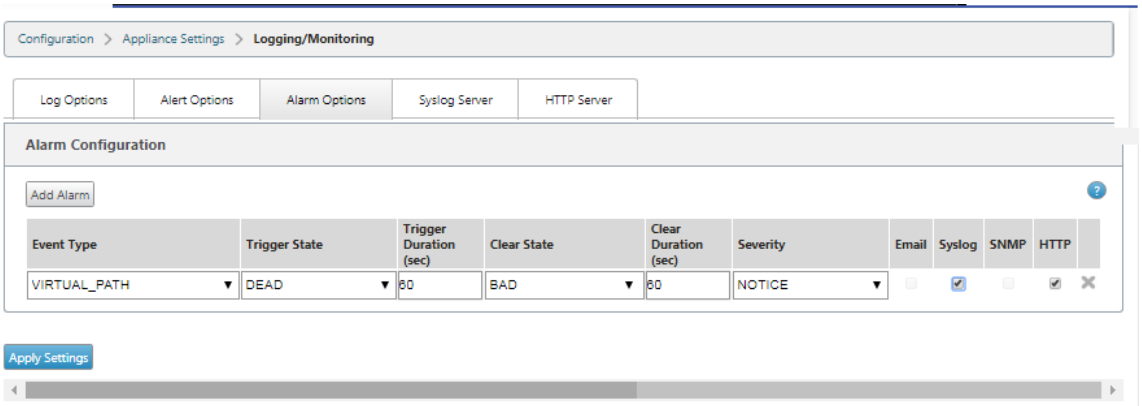
4. 選択したイベントタイプについて、次のアラーム通知状態を選択します。トリガー状態とクリア状態は、選択したイベントタイプに応じて変化します。

   - 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





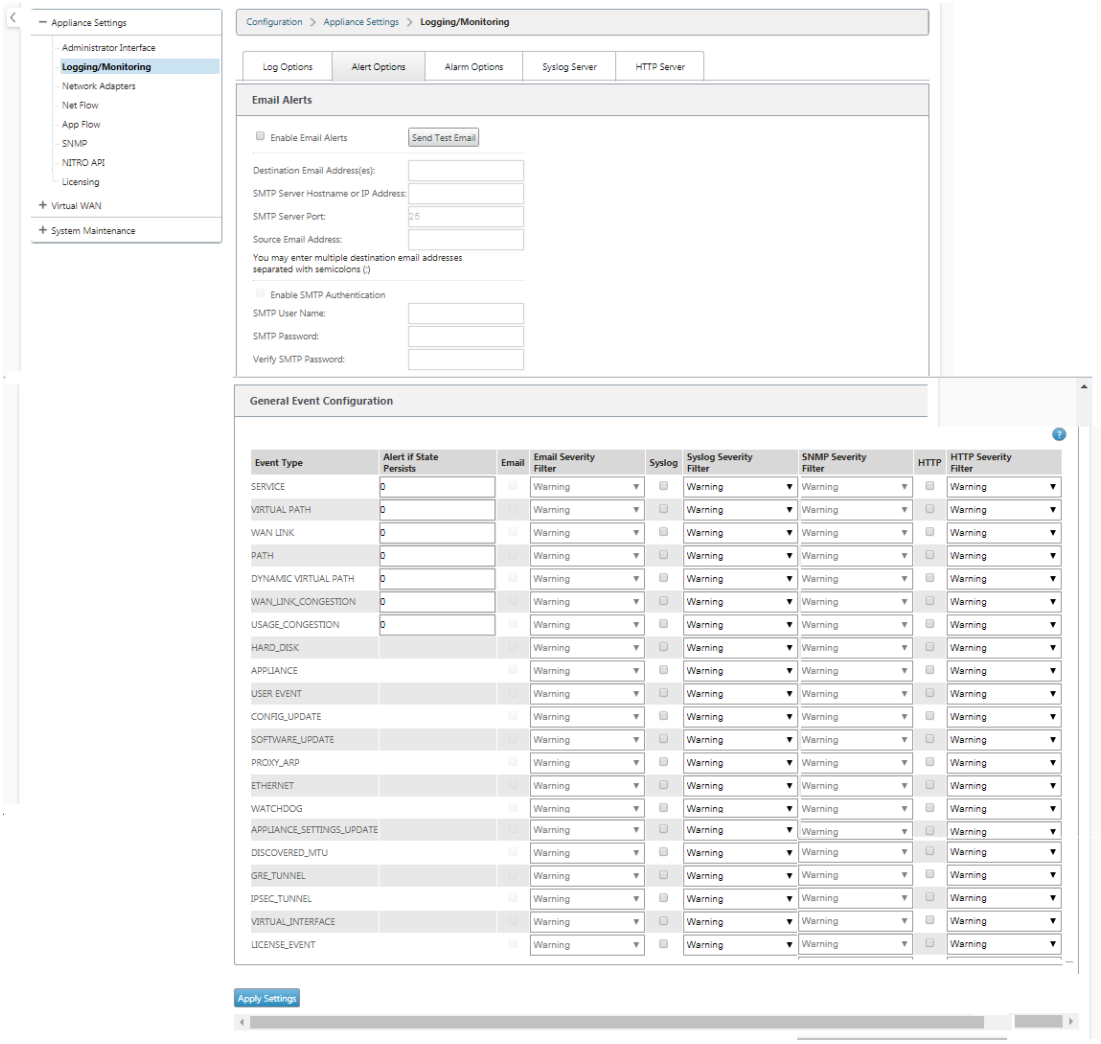
5. **Syslog** および **HTTP** サーバイベントに固有の通知を受信するには、[Syslog] および [HTTP] チェックボックスをオンにします。[設定の適用] をクリックします。



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。[一般イベント設定] ページで、[イベントタイプ] の [HTTP サーバ通知フィルタ] を選択し、[設定の適用] をクリックします。

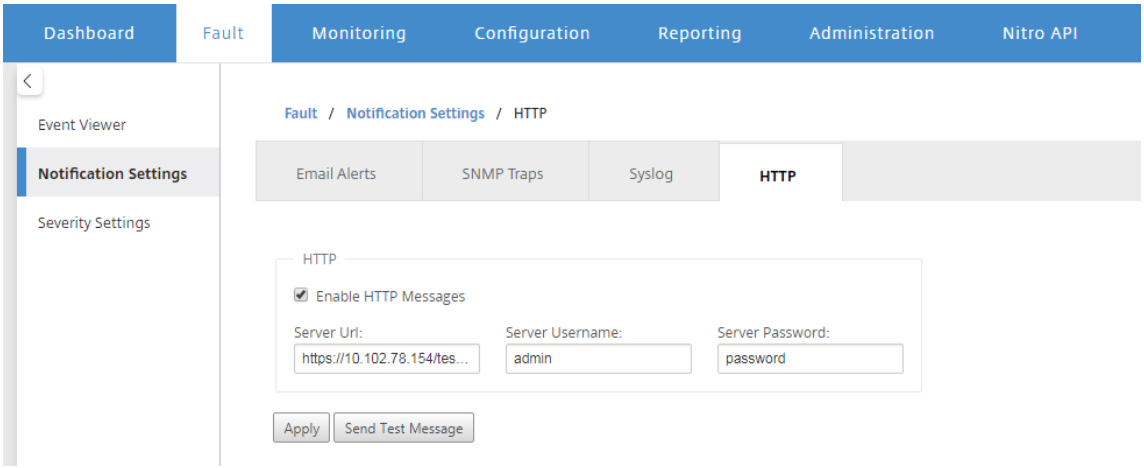
- HTTP
- HTTP 重大度フィルタ



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。

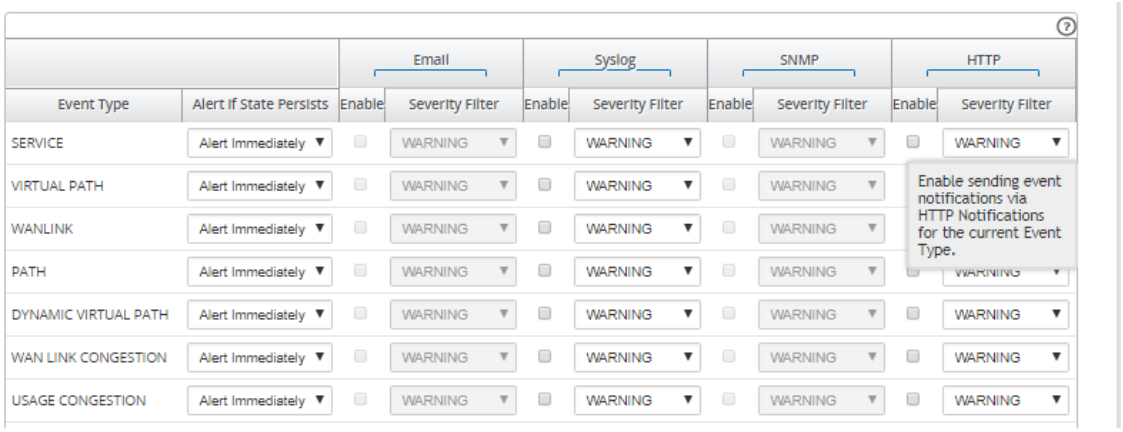
1. [障害] > [通知設定**] > [HTTP**] に移動します。



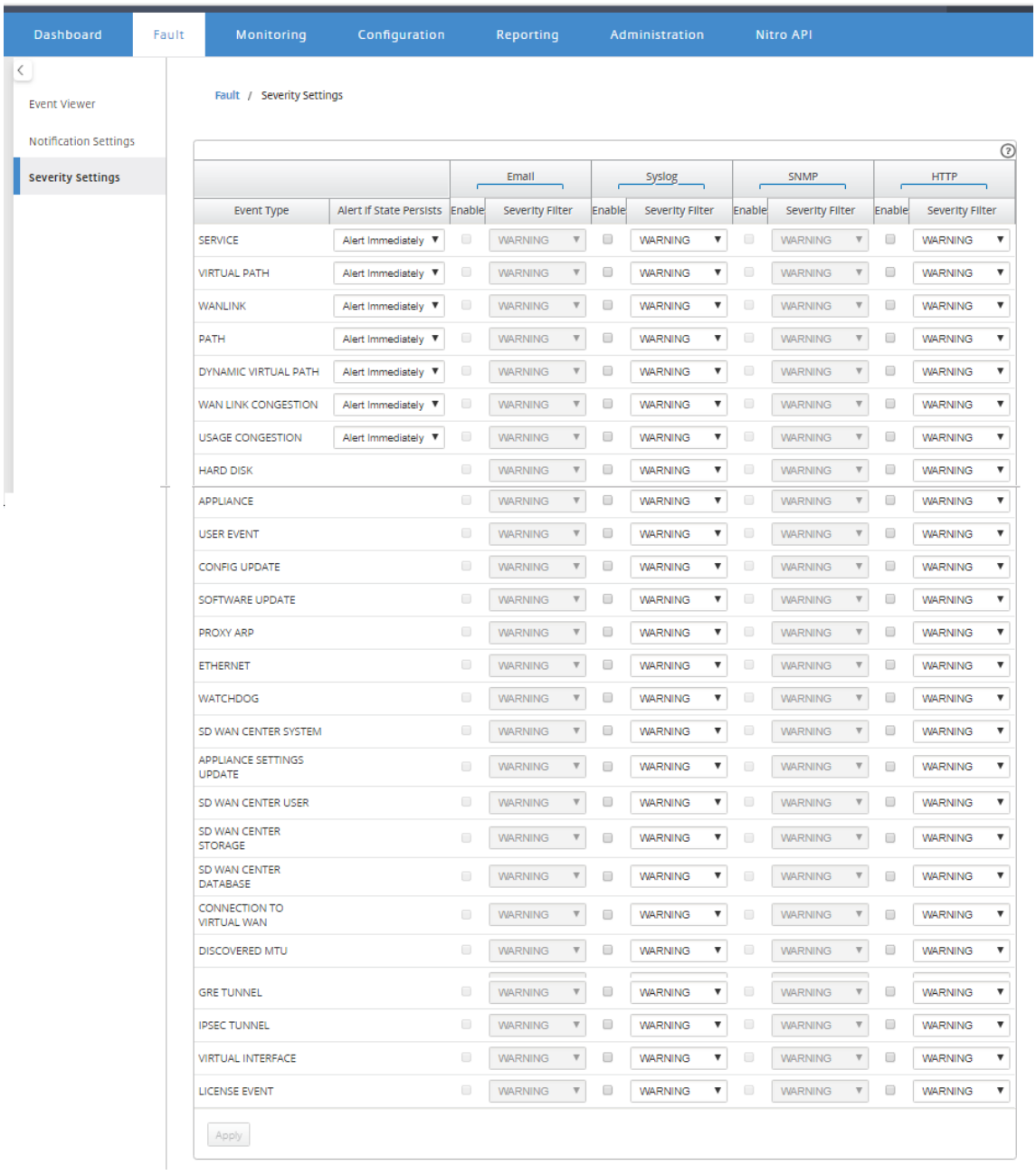
2. HTTP サーバのサーバ **URL**、サーバユーザ名、およびサーバパスワードを入力します。
3. [適用] をクリックします。

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 通知のモニタリングを開始します。



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。



アクティブ帯域幅テスト

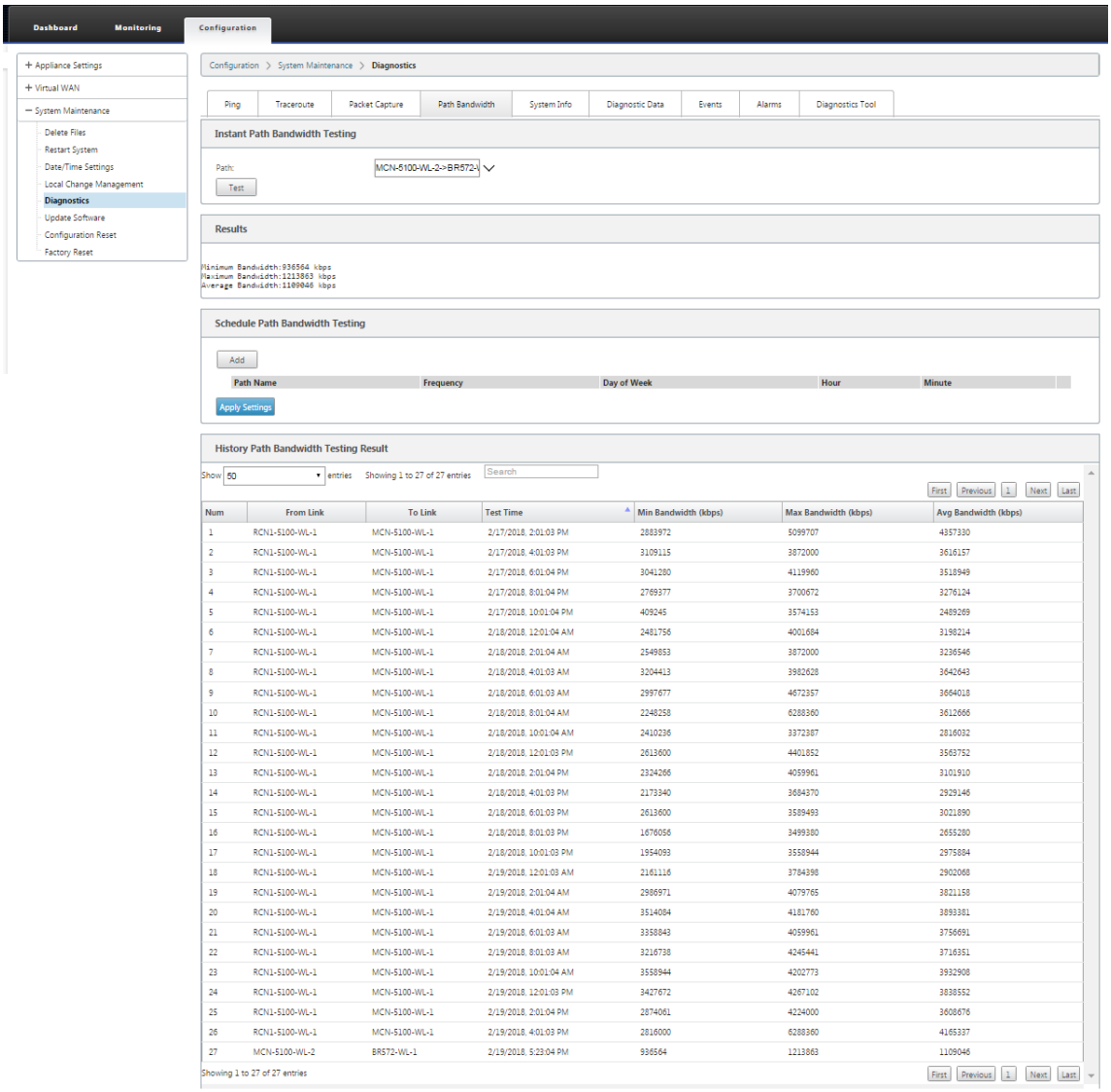
August 30, 2022

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。

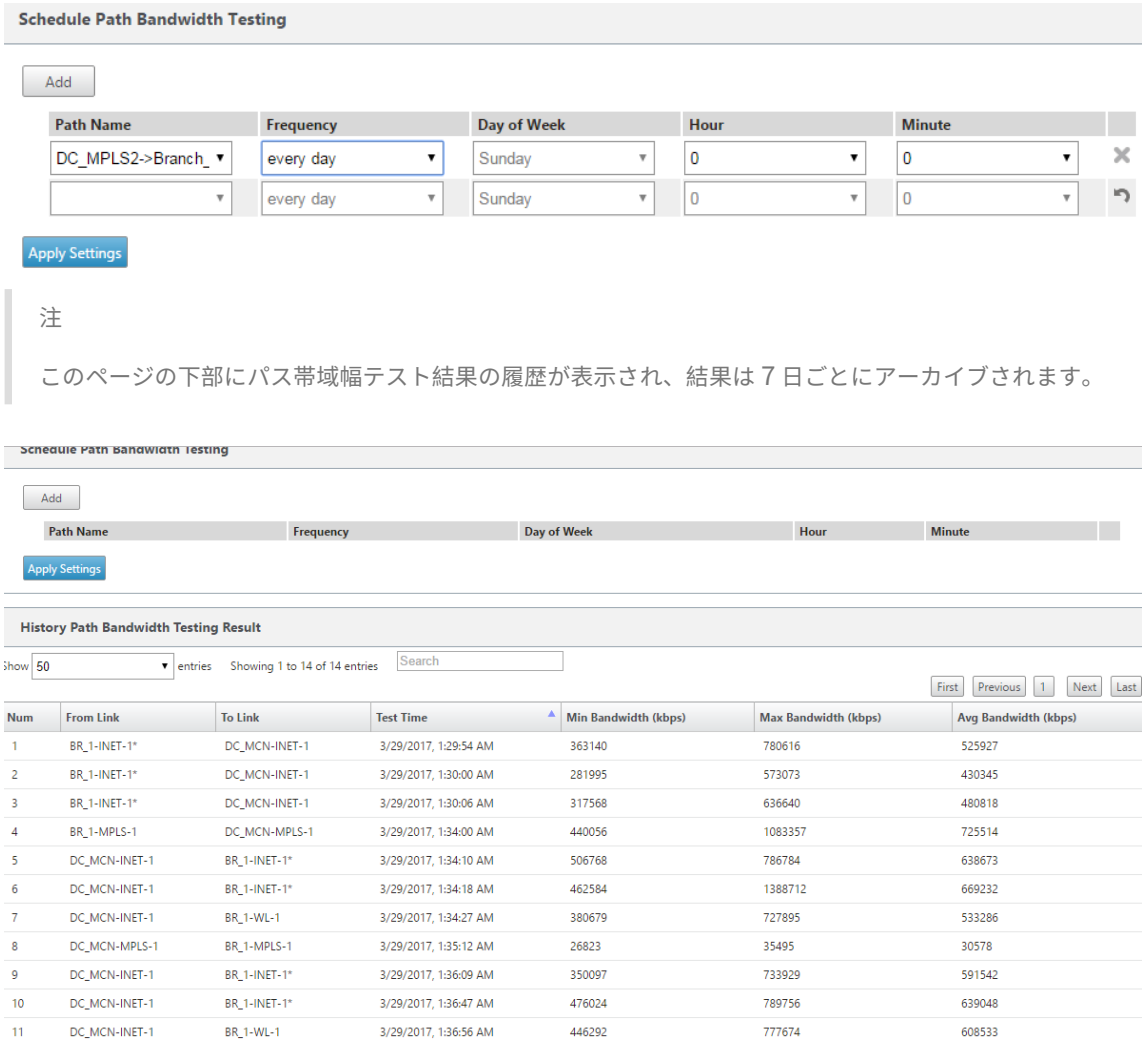
アクティブ帯域幅テスト機能を使用するには、次の手順を実行します。

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。



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] > [サイト名] > [WAN リンク] > [**WAN** リンク名] > [設定] にある [自動学習] オプションによって実現され、有効になっている場合、システムは学習され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。



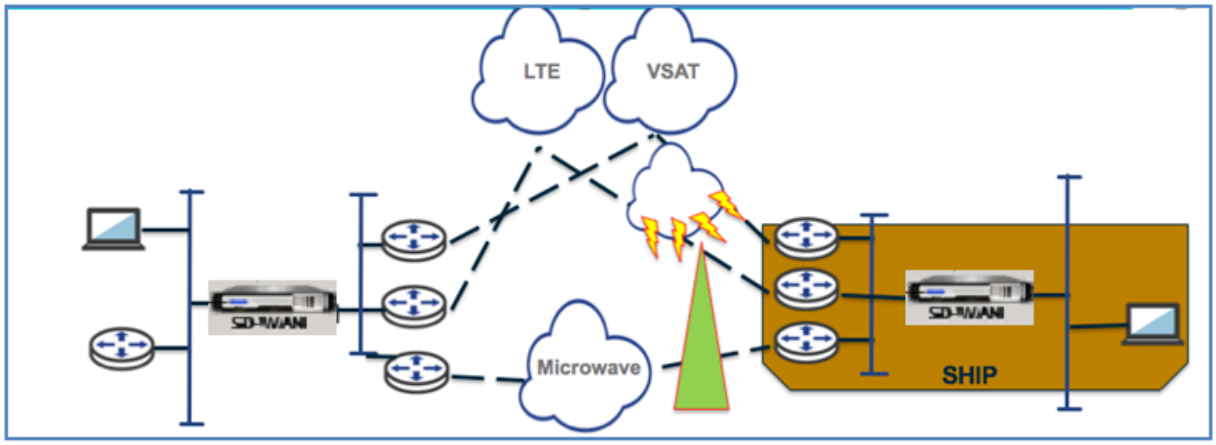
> 注
>
> このページの下部にパス帯域幅テスト結果の履歴が表示され、結果は 7 日ごとにアーカイブされます。

適応型帯域幅検出

November 17, 2022

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、気象と大気の条件、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、パスを BAD としてマークすることなく、使用可能な最大帯域幅を使用できます。

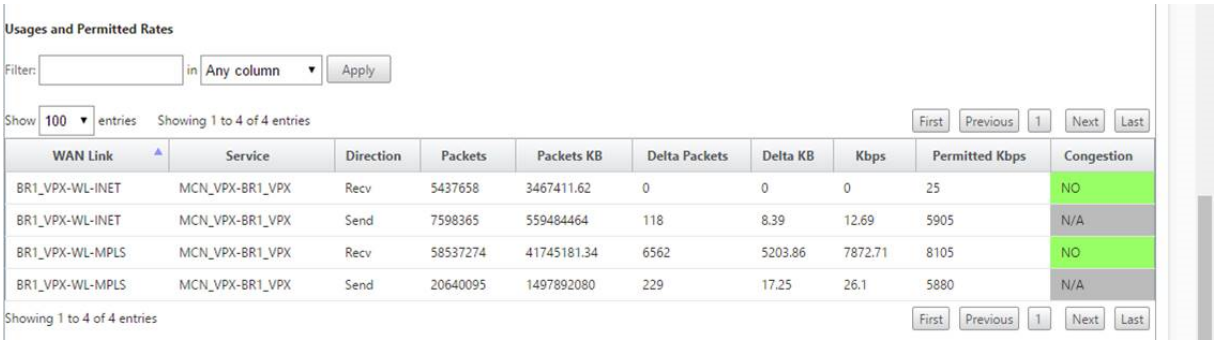
- 帯域幅の信頼性（VSAT 以上、マイクロ波、3G/4G、LTE 以上）
- ユーザーが構成した設定よりも適応型帯域幅の予測性が向上



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)。SD-WAN 11.5 リリース以降、Citrix SD-WAN Orchestrator サービスで有効にできます。詳細については、「適応型帯域幅検出」を参照してください。

[監視] > [統計] > [**WAN **** リンク使用状況**] > [**使用率と許可レート] に移動して、[****** 使用率と許可レート **] 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

August 30, 2022

以下のトピックでは、ネットワークで Citrix SD-WAN ソリューションを設計、計画、実行するときに従うべきベストプラクティスについて説明します。

Security

Routing

QoS

WAN リンク

セキュリティ

August 30, 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フェース

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:

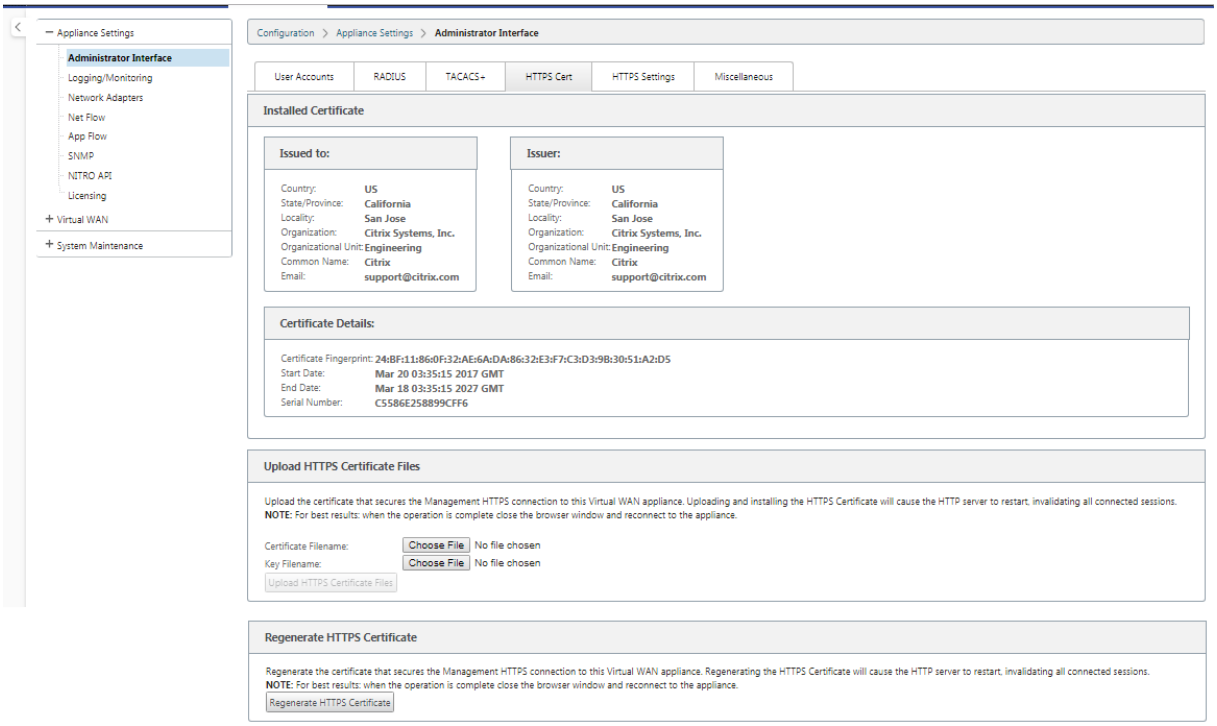
- ローカルユーザーパスワードの変更
- ユーザーの管理

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



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 Encryptic 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の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。

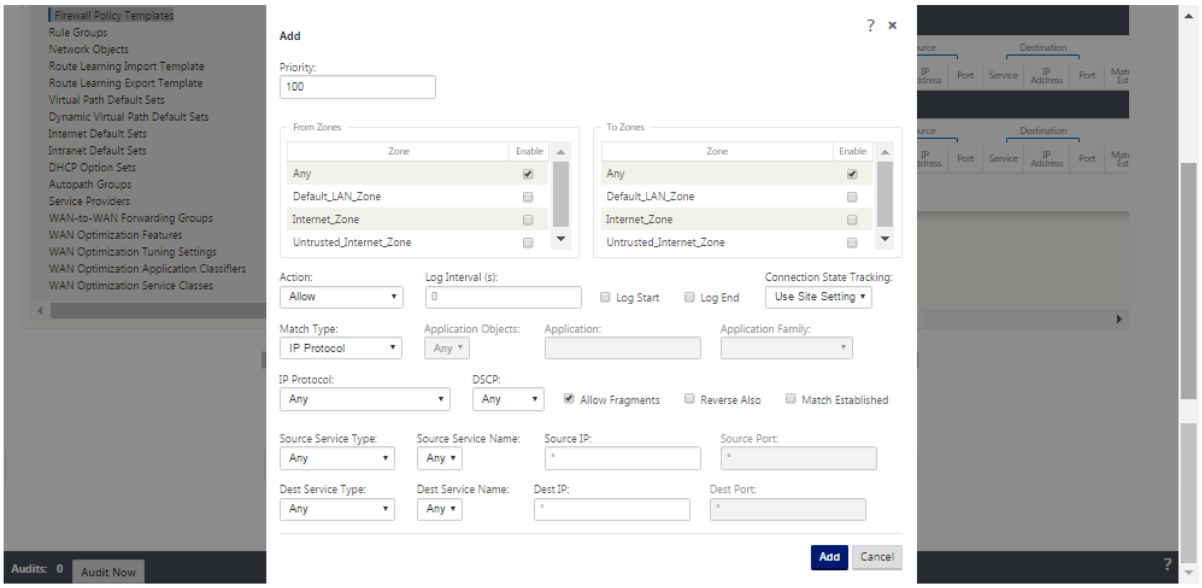
グローバルファイアウォールテンプレート -ファイアウォールテンプレートを使用すると、SD-WAN オーバーレイ環境で動作する個々のアプライアンスのファイアウォールの動作に影響を与えるグローバルパラメータを設定できます。

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。

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

August 30, 2022

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バウンドトラフィックに設定されておらず、****** 代わりにローカルルートまたはパススルールートがゲートウェイルータに到達するように設定されている場合 ****** 。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ローカルとして設定されている場合、そのルートはすべてのブランチ 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

August 30, 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

August 30, 2022

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

- 許可レートと物理レートを実際の WAN リンク帯域幅として設定します。WAN リンクキャパシティ全体が SD-WAN アプライアンスによって使用されるはずでない場合は、それに応じて許可レートを変更します。
- 帯域幅が不明で、リンクの信頼性が低い場合は、自動学習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のみを学習し、将来同じ値を使用します。
- 基礎と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、リンクのヘルス/キャパシティを確認します。
- SD-WAN がワンアームモードで展開されている場合は、基礎となるリンクの物理容量を超過しないようにします。

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 ネットワークを設定するのに役立ちます。

ネットワークトポロジ

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。

よくある質問

August 30, 2022

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 サプリメンタル/HFS 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***、またはシングルステップアップグレードの*.zip* パッケージを使用する必要がありますか?

SD-WAN ソフトウェアを 9.3.x にアップグレードするには、該当するプラットフォームの*.tar.gz* ファイルを使用します。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アップグレードしますか?

いいえ。OS ソフトウェアのアップデート/アップグレードは、シングルステップアップグレード*.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で提供されるスケジュールの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*** の後に*.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* パッケージが変更管理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 以降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* アップグレードは実行されませんか?

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 コンポーネントのソフトウェアパッケージを転送/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 コンポーネントをインスタント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、アプライアンスがサイトに必要なすべてのパッケージを受信したとき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?

[変更管理の設定**]** ページには、デフォルトのスケジューリング情報 (「開始」*:*「*2016-05-21 21:20:00*」、「ウィンドウ」*: 1*、「繰り返し」*: 1*、「単位」*:*「日」) が表示されます。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は「*2016-05-21 at 21:20:00*（メンテナンスウィンドウは *1* 時間、*1* 日おきに繰り返す）」に設定されています。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?

[変更管理の設定］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?

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、現在のソフトウェアバージョン 9.3.x 以降の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** などのハイパーバイザ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、スケジュールの詳細は *2016-05-21 21:20:00*（メンテナンスウィンドウは *1* 時間、*1* 日おきに繰り返す）として設定されており、繰り返し値が **1** 日に設定されており、メンテナンスが行われているため、新しいソフトウェアが毎日インストールできるかどうかをシステムがチェックすることを意味します。ウィンドウは **1** 時間で、**2016-05-21** から **21:20:00**（ローカルアプライアンス時間）にインストールが開始/試行（新しいソフトウェアが利用可能な場合）

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?

[**Status**] 列には、緑色のチェックマークが表示されます。その上にマウスカーソルを置くと、「アップグレードに成功しました」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?

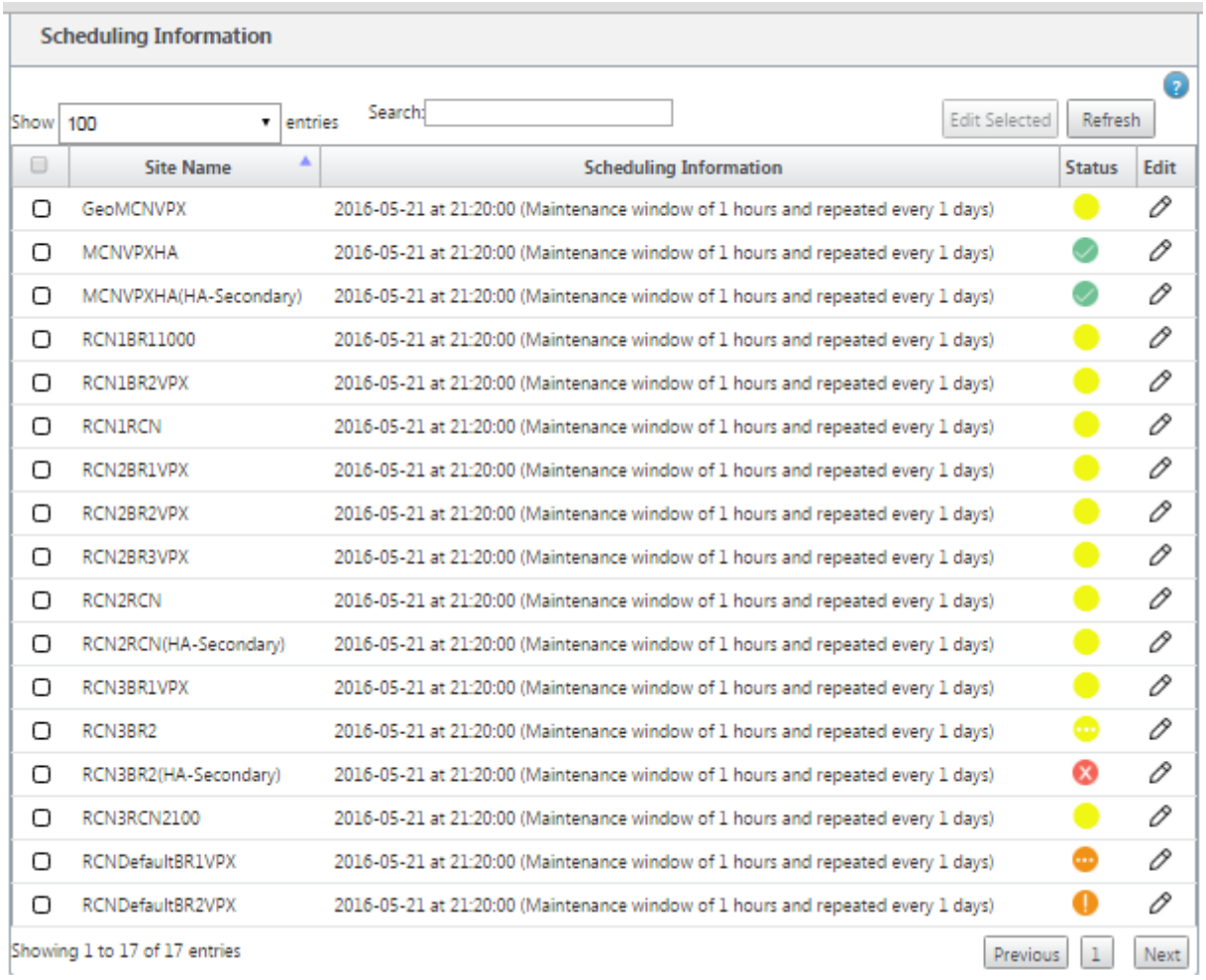
RCN のスケジューリングは、MCN 変更管理の設定ページから実行します。RCN ブランチの場合は、各 RCN にログインし、スケジュールの詳細を設定する必要があります。

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 変更管理の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。



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 を取得して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に関して 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 MCN で*.zip* パッケージを使用して変更管理をもう一度実行するか、アクティブ MCN の役割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 OS コンポーネントパッケージの役割を引き継ぐことができ、他のパッケージにステージングできます。ブランチ。

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。この場合は、アクティブな MCN で*.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。

多層ネットワークへのアップグレード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 ファイルをアップロードした後 <release-version>、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。その他のアプライア

ンスパッケージは、** アプライアンスの検証ボタンまたはステージングボタンを選択すると ** 、一覧表示、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。

RCNs ブランチは任意のプラットフォームモデルであることができるため、パッケージは RCN にステージングされます。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 アプライアンスであり、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の場合、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はどのような影響がありますか。

はい、[未完了を無視] 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 [ローカル変更管理（**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 でチェックボックスが有効になっていることを確認してください。

- 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] > [変更管理設定] ページのチェックボックスを有効にして、部分的なサイトの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でき、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ができますか?

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動作している必要があります。

MCN から Partial Software Upgrade オプションが無効になっていて、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場合はどうなりますか。

MCN は、部分的なソフトウェアアップグレード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、ネットワーク内のすべてのアプライアンスは MCN によって自動修正され、アクティブおよびステージングされたバージョンと一致します。ただし、MCN では、[変更管理] の [アクティベーション] ページから [ステージをアクティブ化] オプションがクリックされることを想定しています。[Activate **Staged]** ボタンをクリックしてネットワークをアクティブにするか、[**Change Preparation**] 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では、構成の更新後に 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非アクティブになった場合に、作業構成へのロールバックが有効になります。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。

再起動するための構成のロールバックの基準は何ですか

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、障害のある設定/ソフトウェアは段階的な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はユーザーにどのように通知されますか?

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、変更管理ステータステーブルであることもわかります。** 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、ソフトウェアのアップグレードも構成とともに実行され、ロールバックシナリオが発生した場合、ソフトウェアもロールバックされます。

MCN に問題があり、クラッシュまたはすべてのサイトとの接続が失われた場合はどうなりますか。

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、すべてのサイトが変更管理セクションにロールバックステータスとして表示されます。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された場合、問題のあるリージョンはロールバックされ、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。ロールバックされたリージョンの 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られ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 に反映されません。その結果、MCN は地域を離れます。MCN にはロールバックバナーが表示されず、MCN 自体またはネットワークはロールバックされません。

どちらのシナリオでも、RCN はロールバックバナーを却下するまで表示されます。MCN によって自動却下できないためです。

参考資料

August 30, 2022

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。