Citrix SD-WAN WANOP 11.1

Machine translated content

Disclaimer

Contents

Citrix SD-WAN WANOP について

December 16, 2022

Citrix SD-WAN WANOP アプライアンスは WAN リンクを最適化し、ユーザーにあらゆる距離で最大の応答性とスループットを提供します。Citrix SD-WAN WANOP アプライアンスは、透過的に機能するため、簡単に導入できます。20 分のインストールにより、他の構成を必要とせずに WAN トラフィックが高速化されます。アプリケーション、サーバー、クライアント、またはネットワークインフラストラクチャを変更する必要はありません。ただし、Citrix SD-WAN WANOP のインストール後に、トラフィックの高速化に影響を与えることなく変更できます。Citrix SD-WAN WANOP アプライアンスは、WAN リンクが変更された場合にのみ再構成が必要です。

Citrix SD-WAN WANOP アプライアンスは、次のようなあらゆる最適化をサポートします。

- 最大圧縮率のマルチセッション圧縮 10,000:1.
- Windows ネットワークファイルシステム (CIFS)、仮想アプリ (ICA および CGP、新しいマルチセッション *ICA* 標準を含む)、Microsoft Outlook (MAPI)、および SSL のプロトコルアクセラレーション。
- 高優先度のインタラクティブトラフィックが低優先度またはバルクトラフィックよりも優先されるようにするためのトラフィックシェーピング。
- 高度な TCP プロトコルアクセラレーション。輻輳したリンクや待ち時間の長いリンクでの遅延を減らします。
- ビデオキャッシング。

Citrix SD-WAN WANOP はどのように機能しますか?

Citrix SD-WAN WANOP 製品は、リンクの両端に 1 つずつペアで動作し、リンク上のトラフィックを高速化します。送信者によって行われた変換は、受信者によって逆にされます。

ただし、1 つのアプライアンス（または仮想アプライアンス）で多くのリンクを処理できるため、各接続にペアを割り当てる必要はありません。

企業は通常、サイトごとに 1 つの Citrix SD-WAN WANOP アプライアンスを持っています（大きなサイトでは大きなアプライアンス、小さなサイトでは小さなアプライアンス）が、多数のブランチオフィスを持つ企業は、中央のデータセンターに複数のアプライアンスを持っている場合があります。

Citrix SD-WAN WANOP アプライアンスを備えたサイトから Citrix SD-WAN WANOP アプライアンスを備えていないサイトへのリンクは正常に機能しますが、トラフィックは加速されません。

Citrix SD-WAN WANOP の機能には、比較的低速なリンクでの高速パフォーマンスのための堅牢な圧縮と、輻輳に対処するためのロスレスフロー制御が含まれます。TCP 最適化は、問題のあるリンクの主な制限を克服し、アプリケーションの最適化は、高速のローカルネットワーク用に設計されたアプリケーションの制限を取り除きます。自動検出機能により、展開が迅速かつ簡単になります。

Citrix SD-WAN WANOP の機能と利点

労働者が自分のコンピューターが応答するのを待つのに費やす時間はすべて失われ、生産性が失われます。ユーザーがリモートで作業したり、オフサイトリソースを使用したりする場合、生産性はネットワーク接続の応答性に依存します。接続の応答性を保護するには、高度なネットワークアクセラレーションが必要です。

Citrix SD-WAN WANOP 製品ラインは、複数の連動する最適化のセットを通じて信頼性の高い WAN およびインターネットリンクのパフォーマンスを提供し、それぞれが相互に強化することで、生産性を保護します。企業全体で最大の生産性を提供するために、最大のデータセンターから最小のブランチオフィス、さらには個々のラップトップまで、あらゆるニーズに対応する Citrix SD-WAN WANOP 製品があります。

Citrix SD-WAN WANOP は、リンクのサイズが小さかったり劣化したりしても、堅牢なユーザビリティを提供します。

一目でわかる機能:

詳しくは、tableを参照してください。

機能と利点:

以下は、Citrix SD-WAN WANOP 製品ラインの主な利点の一部です。

圧縮は低いリンク速度を克服します。ワイドエリアネットワーク（WAN）リンクとインターネットリンクの最も明らかな問題は、ローカルエリアネットワーク（LAN）と比較して帯域幅が狭いことです。1 Mbps WAN には 100Mbps LAN のスループットの 1% 。低リンク帯域幅をどのように克服しますか? 圧縮あり。100:1 の圧縮比 は 1Mbps のリンクで 100Mbps の速度でデータを転送できます。このスピードアップ係数は、次の基準が満たされるたびに達成されます。

- 圧縮アルゴリズムは、高い圧縮率を提供できる必要があります。
- 圧縮アルゴリズムは非常に高速である必要があります（リンク帯域幅よりもはるかに高速で、理想的には LAN と同じくらい高速です）。
- 異なるセグメントは異なるレートでデータを処理するため、リンクの LAN セグメントは WAN セグメントから独立したフロー制御を備えている必要があります。
- さまざまな種類のトラフィックのさまざまなニーズを処理するには、複数の圧縮エンジンを使用する必要があります。インタラクティブトラフィックは比較的少ない帯域幅を必要としますが、遅延には非常に敏感です。一方、バルク転送は帯域幅に非常に敏感ですが、遅延には敏感ではありません。

TCP プロトコルアクセラレーションは輻輳を克服します。リンク速度よりも速くトラフィックを送信しようとすると、輻輳が発生し、高いパケット損失と高いキューイング遅延によって引き起こされる多くの問題が発生します。

ロスレスフロー制御。ザ・TCP/IP プロトコルには、送信者を直接遅くするフロー制御がありません。この必要な制御メカニズムがないため、ミッションクリティカルなリンクであっても、パケット損失と過度のキューイング遅延が正常になります。（どちらかといえば、**bufferbloat** の現象に関する論文が証明しているように、この問題は時間とともに悪化しています。）

Citrix SD-WAN WANOP アプライアンスは、TCP/IP プロトコルから省略されたフロー制御を提供することにより、この問題を解決します。単にパケット損失を再割り当てする通常のサービス品質（QoS）ソリューションとは異なり、Citrix SD-WAN WANOP は、送信者が好きな速度でデータを送信できるようにする代わりに、エンドポイント送信者がデータを送信する速度を制御するロスレスフロー制御を提供します。送信しすぎるとパケットをドロップします。各送信者は、Citrix SD-WAN WANOP が送信できるデータのみを送信し、パケットをドロップすることはありません。このデータは、オーバーフローすることなくリンクをいっぱいに保つために、正確に正しいレートでリンクに配置されます。余分なデータを排除することにより、Citrix SD-WAN WANOP はそれを破棄することを強制されません。Citrix SD-WAN WANOP がないと、ドロップされたパケットを再送信する必要があり、不要な遅延が発生します。ロスレスフロー制御は、過度のバッファリングによって引き起こされる遅延も排除します。ロスレスフロー制御は、ビジーリンクでの最大の応答性の鍵であり、40%の使用率で使用できなくなるまで混雑していたリンクが、95%の使用率で生産性と応答性を維持できるようにします。

距離に基づく不公平を排除します。待ち時間が長いリンクやパケット損失のあるリンクは、特に TCP Reno などの通常の TCP バリアントでは、全帯域幅で使用するのが困難です。その結果、過度の遅延が発生し、料金を支払っている帯域幅を取得するのが困難になります。リンク距離が長くなるほど、問題は悪化します。

Citrix SD-WAN WANOP TCP プロトコルアクセラレーションは、これらの影響を最小限に抑え、大陸間リンクや衛星リンクをフルスピードで実行できるようにします。

トラフィックシェーピングは帯域幅を自動的に管理します。出力側では、均等化キューイングのようなアルゴリズムにより、各接続が個別にキューに入れられ、リンク帯域幅の公平なシェアが与えられます。トラフィックシェーピングポリシーにより、さまざまなサービスに高い優先順位または低い優先順位を与えることができます。アプリケーションの最適化は設計上の制限を克服します。

ローカルエリアネットワークで使用するために設計されたアプリケーションとプロトコルは、設計者がプロトコルに対する長い光速遅延の影響を考慮していなかったため、ワイドエリアネットワークでのパフォーマンスの低下で有名です。たとえば、単純な Windows ファイルシステム（CIFS）の操作では、メッセージがネットワークを行き来するときに最大 50 回のラウンドトリップが必要になる場合があります。ラウンドトリップ時間が 100 ミリ秒のワイドエリアネットワークでは、ラウンドトリップが 50 回の場合、5 秒の遅延が発生します。

光速の遅延は基本的な制限ですが、アプリケーションの最適化では、通常は投機的な操作を通じて、より少ないラウンドトリップで同じ操作を実行できます。元のアプリケーションが一度に 1 つのコマンドを発行し、それが完了するのを待ってから次のコマンドを発行する場合、多くの場合、待たずに一連のコマンドを発行するのが完全に安全です。さらに、データ転送は、プリフェッチ、先読み、および後書き操作の組み合わせによって加速できます。できるだけ多くの操作を 1 回の往復にまとめることで、パフォーマンスを 10 倍以上向上させることができます。

Citrix SD-WAN WANOP の最適化は、特に CIFS/SMB（Windows ファイルシステム）、MAPI（Outlook/Exchange プロトコル）、および HTTP。

複数の最適化により、仮想アプリ/仮想デスクトップ（**Citrix HDX**）のパフォーマンスが向上します。Citrix SD-WAN WANOP アプライアンスはシトリックス製品であるため、特に Citrix Virtual Apps and Desktops などの Citrix プロトコルの高速化に有効です。Citrix SD-WAN WANOP アクセラレーションのあらゆる側面がこれらのプロトコルと連携して、リモートユーザーエクスペリエンスを可能な限り生産的にします。

Citrix SD-WAN WANOP アプライアンスは、Citrix Virtual Apps and Desktops サーバーとセッションオプショ

ンをネゴシエートします。これにより、Citrix SD-WAN WANOP アプライアンスで次の拡張機能を適用できます。

- サーバーのネイティブ圧縮をより高性能な Citrix SD-WAN WANOP 圧縮に置き換えます。
- 接続のトラフィックシェーピングの優先順位は、すべての Citrix Virtual Apps and Desktops tops 接続に組み込まれている優先度ビットに基づいて決まります。これにより、接続の優先度をトラフィックのタイプに応じて変えることができます。たとえば、インタラクティブタスクは優先度の高いタスクであり、印刷ジョブは優先度の低いタスクです。
- 使用されている仮想アプリまたは仮想デスクトップアプリケーションに基づいて、統計を収集してレポートします。
- 元の接続のエンドツーエンド暗号化を維持します。

最小限の構成のための自動検出。ソリューションはダブルエンドであり、リンクの両端に Citrix SD-WAN WANOP 製品が存在する必要があるため、展開はリモートオフィス、特に専任の IT スタッフがいないオフィスに負担をかけるように思われます。ただし、Citrix SD-WAN WANOP は、インストールと保守が非常に簡単になるように設計されています。通常のインストールには約 20 分かかります。必要なパラメータは、通常のネットワークパラメータ（IP アドレスやサブネットマスクなど）、Citrix ライセンスサーバーのアドレス、およびリンクの送受信速度のみです。

自動検出により、手動で構成しなくても、Citrix SD-WAN WANOP がどの接続を高速化できるか（どの接続を高速化できないか）を決定するため、最小限の構成のみが必要になります。リンクのもう一方の端にある Citrix SD-WAN WANOP が自動的に検出され、接続が高速化されます。Citrix SD-WAN WANOP アプライアンスをアドホックな方法でネットワークに追加できます。新しいアプライアンスの到着を既存のアプライアンスに通知する必要はありません。彼らは自分でそれを発見します。

TCP ヘッダーオプションは TCP 標準の一部であるため、Citrix SD-WAN WANOP は TCP ヘッダーオプションを使用してその存在を報告し、リモート Citrix SD-WAN WANOP とアクセラレーションパラメーターをネゴシエートします。この方法は、ファイアウォールが存在する場合を除いて、非常にうまく機能します。最も一般的なオプションを除くすべてを拒否するようにプログラムされています。このようなファイアウォールは存在しますが、Citrix SD-WAN WANOP で使用されるオプションが通過できるように構成できます。

Citrix SD-WAN WANOP の操作は、送信者と受信者の両方に対して透過的です。ネットワーク内の他のデバイスは、Citrix SD-WAN WANOP
が存在することを認識していません。これらは、Citrix SD-WAN WANOP のインストール前と同じように機能し続けます。この透過性により、Citrix SD-WAN WANOP アクセラレーションの恩恵を受けるために、サーバーまたはクライアントに特別なソフトウェアをインストールする必要もなくなります。すべてが透過的に機能します。

製品ライン機能:

Citrix SD-WAN WANOP 製品ラインのすべての製品は、基本的な Citrix SD-WAN WANOP アクセラレーション機能を提供します。ほとんどのモデルには、次のような追加機能もあります。

- ビデオキャッシング
- イーサネットバイパス機能を備えた複数の高速ブリッジ
- GUI、CLI、SNMP、AppFlow、および Citrix ADM を介した監視と管理。

Citrix SD-WAN WANOP 製品が異なれば、機能も異なります。より高い WAN 帯域幅をサポートする製品は、より多くのユーザーをサポートし、通常、より多くのリソース（より多くのパワー CPU、より多くのメモリ、より大きなディスク、より高速化されたブリッジ）を備えています。

Citrix SD-WAN WANOP プラグインや Citrix SD-WAN WANOP VPX など、独自のハードウェアで実行される製品の機能は、ハードウェアの速度と、アクセラレーション専用のシステムリソースの量によって異なります。

最新の仕様については、Citrix SD-WAN 製品データシートを参照してください。

Citrix SD-WAN WANOP アーキテクチャ

Citrix SD-WAN WANOP アプライアンスは、WAN リンクを介したトラフィックを高速化します。WAN を高速化するには、高速化するサイトごとに 1 つずつ、少なくとも 2 つの Citrix SD-WAN WANOP アプライアンスが必要です。

送信側の Citrix SD-WAN WANOP アプライアンスは、圧縮や暗号化など、一連の最適化と変換をトラフィックに適用します。多くの操作では、受信側の Citrix SD-WAN WANOP が解凍や復号化などの逆の操作を実行して、トラフィックを元の状態に復元する必要があります。

したがって、ほとんどの最適化では、トラフィックが 2 つの Citrix SD-WAN WANOP アプライアンスを通過する必要があります。一部の最適化はシングルエンドであり、単独で動作するローカルアプライアンスによって実行されます。これらの最適化には、トラフィックシェーピングとビデオキャッシングが含まれます。

Citrix SD-WAN WANOP アプライアンスは、ネットワークに対してほとんど透過的です。アプライアンス自体は、ルーター、ゲートウェイ、またはプロキシではなく、ブリッジのように見えます。この不可視性により、他のハードウェアを構成せずにアプライアンスをインストールできます。アプライアンスの最適化も透過的であり、リンクのもう一方の端にあるパートナーアプライアンスによってのみ検出されます。

Citrix SD-WAN WANOP アプライアンスは、自動検出および自動ネゴシエーション機能により、ネットワーク上の新しいアプライアンスが他のアプライアンスによって即座に検出され、アクセラレーションがすぐに開始されるため、ネットワークに自由に追加できます。

上の図はアプライアンスが 2 つしかないネットワークを示していますが、1 つの Citrix SD-WAN WANOP アプライアンスが任意の数のパートナーサイトと通信できます。ポイントツーポイント、ハブアンドスポーク、およびメッシュネットワークがすべてサポートされています。

スタンドアロンアプライアンスに加えて、Citrix SD-WAN WANOP アクセラレーション製品には、仮想マシン（Citrix SD-WAN WANOP VPX シリーズ）および Windows システム用のインストール可能なアクセラレーションサービス（Citrix SD-WAN WANOP プラグイン）が含まれます。

加速とは

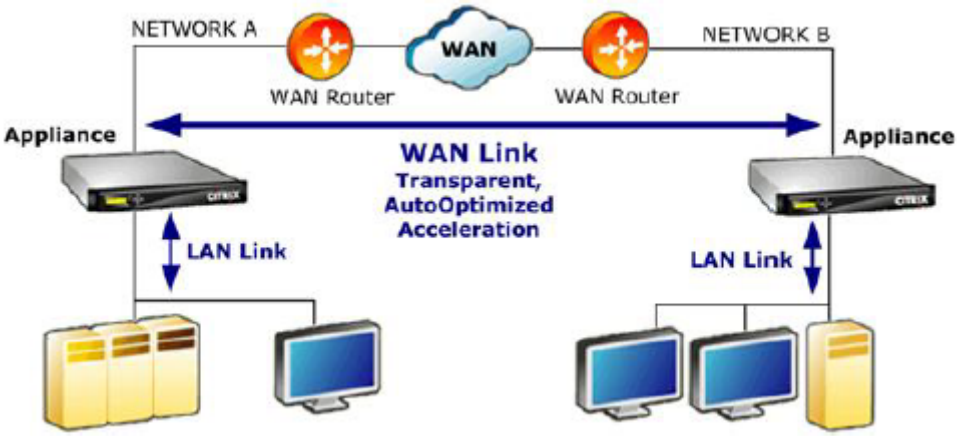
Citrix SD-WAN WANOP の用語では、「アクセラレーション」とはトランザクション時間の短縮であり、ユーザーが待機する時間を短縮します。ユーザーが待機に費やす時間は生産性の直接的な損失を表すため、アクセラレーションの主な利点は生産性の向上です。

ネットワークトラフィックでは、トランザクションは非常に小さいもの（Telnet または SSH ターミナルセッションの 1 バイトのデータ）から、FTP 転送のように非常に大きいものまであり、サイズがギガバイトを超えることがよくあります。実用的なアクセラレータは、インタラクティブトラフィックからバルクトラフィックまで、トランザクションサイズの全範囲を加速し、全体的に最高のパフォーマンスとユーザーエクスペリエンスを提供する必要があります。Citrix SD-WAN WANOP テクノロジーは、さまざまな方法でこれを実現します。

アクセラレーションの仕組み：パイプライン

Citrix SD-WAN WANOP アプライアンスがどのように機能するかを確認するには、トラフィックフローパイプラインの図をよく見てください。ご覧のとおり、2 つのパイプラインがあります。

1. ローカル LAN から WAN に入るデータを高速化する送信パイプライン。
2. WAN を出てローカル LAN に入るデータを加速する受信パイプライン。



パイプラインを送信

アプライアンスを理解するには、送信パイプラインを一度に 1 ユニットずつ検討します。

1. 入力バッファ。LAN からのパケットはアプライアンスによって受信されます。なぜなら non-TCP/IP トラフィックはトラフィックシェーパーによってのみ最適化され、非 TCP パケットはトラフィックシェーパーに直接転送されます。ザ・TCP/IP トラフィック（以降、TCP トラフィックと呼びます）は、パイプラインの残りの部分を通過します。
2. ビデオキャッシュ。TCP トラフィックがビデオキャッシュの設定と一致する場合、要求はビデオキャッシュユニットに渡されます。
3. LAN 側の自動検出。トラフィックシェーピング以外に、送信側の最適化では、ローカルアプライアンスだけでなくリモートアプライアンスも必要です。リモートアプライアンスを通過しない接続は、トラフィックシェーパーに転送されます。このアクションは、LAN 側の自動検出ロジックによって実行されます。リモートアプライアンスの実際のテストは、WAN 側の自動検出ユニットによって行われます。

4. LAN 側のフロー制御。Citrix SD-WAN WANOP は、透過的な TCP プロキシとして機能し、エンドポイント受信者に代わってエンドポイント送信者からパケットを受信および確認します。これにより、アプライアンスは、トラフィックが WAN 上を移動する速度に関係なく、ローカル送信者からの大量のデータを LAN のフルスピードで非常に迅速に受け入れることができます。（通常の TCP はエンドツーエンドの速度制御を使用しますが、これは最大のパフォーマンスを実現するのに十分な俊敏性ではありません。）さらに、Citrix SD-WAN WANOP フロー制御はロスレスです。つまり、ローカル送信者にはドロップされたパケットが表示されないため、信頼性と効率が向上。

5. アプリケーションエンジン：Citrix SD-WAN WANOP は、次のようないくつかのプロトコルに対して特定の最適化を実行します。

   - ICA プロトコルと CGP プロトコルを使用して、Citrix Virtual Apps and Desktops。
   - Windows ファイルシステム（SMB1 および SMB2 バージョンを含む CIFS）
   - Outlook/Exchange （MAPI）

     これらの最適化により、トランザクション時間が短縮されます。これは、コマンドの書き換え、結合、および並べ替え、先読みと後書きの使用、より高度なトラフィックシェーピングのためのプロトコルの知識の使用、および圧縮ヒントによって行われます。

6. 圧縮エンジン。圧縮によりトランザクションが小さくなり、リンクを介してデータを転送するのにかかる時間が短縮されます。Citrix SD-WAN WANOP コンプレッサーは、複数の圧縮アルゴリズムを使用します。一部は小規模トランザクションに非常に効率的で、一部はバルクトランザクションに最適化され、一部は中規模トランザクションに最適化されています。圧縮比 10,000:1 は Citrix SD-WAN WANOP コンプレッサーによって簡単に実現できます。コンプレッサーは非常に高速であるため、WAN のフルスピードで高い圧縮率を維持できます。Citrix SD-WAN WANOP 処理では、で圧縮されるファイル 100:1 比率は、100Mbps の全体的なスループットで 1Mbps のリンクを介して簡単に送信できます。

7. セキュリティエンジン。一部の Citrix SD-WAN WANOP 機能では、2 つのアプライアンスが相互におよびオリジンサーバーと安全なピア関係を結ぶ必要があります。セキュリティエンジンは、このピア関係を認証し、それらの間の高速データ接続を暗号化します。セキュアなピア関係により、SSL 圧縮と、暗号化された仮想アプリ/仮想デスクトップ（ICA/CGP）、Windows ファイルシステム（CIFS）、および Outlook/Exchange（MAPI）トラフィックの高速化を使用できます。

8. WAN 側のフロー制御と自動検出。WAN リンクはトラフィックの速度低下が発生する場所であり、リンクが混雑している場合、パケットは失われるため、再送信する必要があります。パケットを再送信すると、常に大幅な遅延が発生し、場合によっては 1 秒以上続くこともあります。WAN 側のフロー制御ユニットは、高度な再送信要素と高度な再送信要素を使用します TCP/IP 「クリーン」リンクと「問題のある」リンクの両方で最大のパフォーマンスを発揮するプロトコル。自動検出ユニットは、接続ごとにパートナーの Citrix SD-WAN WANOP ユニットの存在を識別します。これにより、最適化が不要な場所で使用されるのを防ぎ、既存のアプライアンスで新しいアプライアンスを次のように検出できます。それらがネットワークに追加されるとすぐに。自動検出は、TCP ヘッダーフィールドのオプションを使用します。これは通常透過的ですが、再構成が必要な一部のファイアウォールによってブロックされる可能性があります。

9. アプリケーション分類子。このユニットは、Citrix SD-WAN WANOP を通過するすべてのトラフィックを調べ、それが属するアプリケーションまたはプロトコルを識別します。この情報は、レポートおよびトラフィックシェーパーによって使用されます。
10. トラフィックシェーパー。輻輳、過度のキューイング、およびその他の回避可能な遅延の原因を回避するために、トラフィックシェーパーは、WAN のデータレートよりわずかに低い速度でトラフィックを WAN に注入し、WAN がオーバーランしないようにします。重み付き公平キューイングアルゴリズムを使用して、すべてのトラフィックがリンク帯域幅の公平なシェアを確実に取得できるようにします。トラフィックシェーピングポリシーでは、さまざまなトラフィックタイプがさまざまな重みを受け取ることができるため、一部のトラフィックは他のトラフィックよりも多くの帯域幅を取得します。

受信パイプライン

受信方向のパイプラインは送信方向と似ていますが、暗号化する代わりに復号化し、圧縮する代わりに解凍する点が異なります。また、受信方向にもトラフィックシェーパーがあり、着信 WAN トラフィックにトラフィックシェーピングポリシーを適用して、両方向が規制されていることに注意してください。

自動検出とパケットレベルの変換

自動検出アルゴリズムは、TCP ヘッダーオプションを挿入して、Citrix SD-WAN WANOP アプライアンスの存在を通知し、ネゴシエーションを容易にします。これらのオプションは 24〜31 の範囲です。次のパケットレベルの変換が使用されます。

- 接続の最初のパケット（SYN パケット）で、送信アプライアンスは、自身を Citrix SD-WAN WANOP アプライアンスとして識別し、圧縮などの他の機能も宣言するヘッダーオプションを添付します。これは「タグ付き SYN パケット」と呼ばれます。
- タグ付き SYN パケットを受信すると、受信アプライアンスはヘッダーオプションを SYN-ACK パケットに添付し、それ自体を識別してその機能をアナウンスします。
- 送信側アプライアンスがタグ付き SYN-ACK パケットを受信すると、両方のアプライアンスで共有されている機能に応じて接続を高速化できます。たとえば、両方のアプライアンスが圧縮のサポートを宣言した場合、接続は圧縮されます。
- 両方向の TCP 初期シーケンス番号（ISN）は、元の値に 2,000,000,000 を追加することによって変更されます。これは、1 つのアプライアンスに障害が発生した場合、または接続内のすべてのトラフィックを認識できないようにルーティングが変更された場合に、接続が続行されないようにするための予防措置です。接続が加速されると、その存続期間を通じて加速されたままでなければなりません。
- 各パケットに挿入された Citrix SD-WAN WANOP TCP ヘッダーオプション用のスペースを確保するために、MSS 値は通常 1380 バイトに削減されます。
- 接続の IP アドレスとポート番号は変更されません。

事前承認

SYN パケットと SYN-ACK パケットは、エンドツーエンドで流れます。

- SYN パケットは、エンドポイントクライアントから、クライアント側アプライアンス、WAN、サーバー側アプライアンス、そして最後にサーバーに流れます。
- SYN-ACK パケットは、サーバーからサーバー側アプライアンスを経由して、WAN 経由で、クライアント側アプライアンスを経由して、最後にクライアントに流れます。

接続の最後のパケット、FIN、FIN-ACK、および RST パケットについても同じことが言えます。

ただし、他のパケットは事前に確認されています。たとえば、サーバー側アプライアンスはサーバーからパケットを受信すると、LAN 経由ですぐにパケットを確認し、WAN 経由で最終的に送信できるようにバッファリングします。これにより、サーバー側アプライアンスのバッファーが非常に迅速にいっぱいになるため、圧縮やその他の最適化に使用するデータが常に十分にあります。（これは、すべての確認応答が WAN の反対側から送信され、確認応答が非常に遅くなり、接続のすべてのセグメントが最も遅いセグメントよりも速く移動しないようにする通常の TCP 操作とは大きく異なり、アクセラレーションの効果が大幅に低下します。）

トラフィックをアプライアンスに出し入れする

Citrix SD-WAN WANOP アプライアンスには、いくつかの「転送モード」があります。転送モードは、アプライアンスにトラフィックを出し入れする方法です。最も一般的なのはインラインモードで、Citrix SD-WAN WANOP がブリッジデバイスのように見えます。一方のブリッジポートに入るパケットは、もう一方のブリッジポートから出るように見えます。もちろん、Citrix SD-WAN WANOP はさまざまな方法でデータを変換するため、多くの場合、2 番目のポートを出るパケットは、最初のポートに入ったパケットと同じではありませんが、それがネットワークの他の部分に表示されます。。

インラインモードが実用的でない場合は、他のいくつかの方法、特に WCCP モードを使用できます。これらは、単一のインターフェイスケーブルを使用する「ワンアーム」モードです。

> ヒント
>
> Citrix ADM を使用して Citrix SD-WAN WANOP アプライアンスを管理および監視できます。詳細については、Citrix ADM を使用した Citrix SD-WAN インスタンスの管理を参照してください。

Citrix SD-WAN WANOP の使用を開始する

April 19, 2021

Citrix SD-WAN WANOP アプライアンスを正常に展開することは難しくありませんが、不適切な展開は問題を引き起こし、不十分なアクセラレーションを提供する可能性があります。加速させたいリンクに十分な容量のアプライア

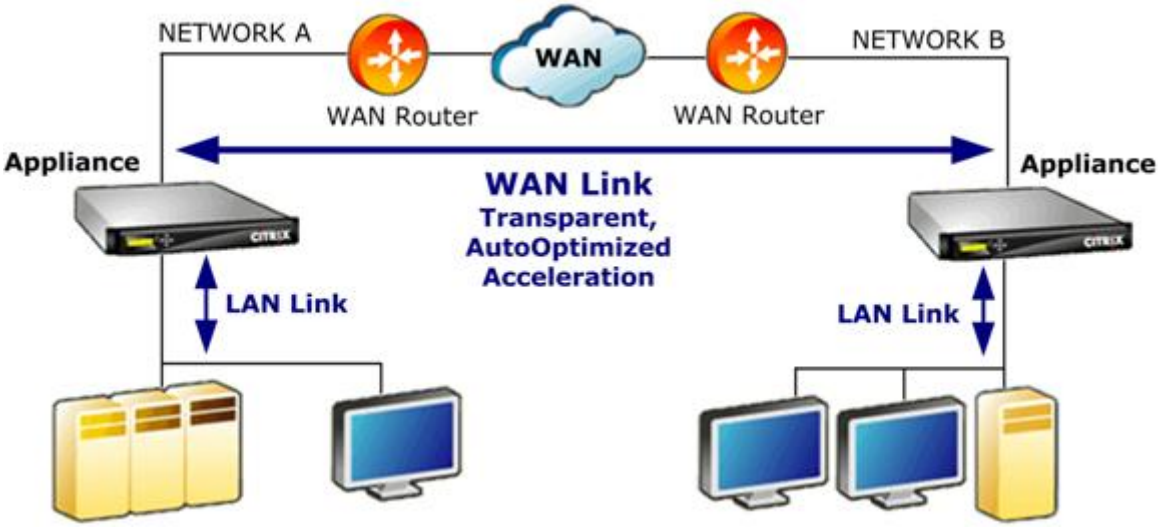
ンスを選択してください。製品の選択も、アプライアンスをトポロジに最適に適合させる方法を決定する際に考慮すべき要素の 1 つです。

最も基本的な展開基準は次のとおりです。

- TCP 接続内のすべてのパケットは、サポートされている 2 つの アクセラレーションユニット（Citrix SD-WAN WANOP アプライアンスまたはプラグイン）の組み合わせを通過する必要があります。
- トラフィックは、2 つの加速ユニットを両方向に通過する必要があります。

これらの基準が満たされると、加速は自動的に行われます。

トラフィックが 2 つのアプライアンスを通過するとき、アクセラレーションはパフォーマンスを向上させます



WAN ネットワークが 1 つしかないサイトの場合、Citrix SD-WAN WANOP アプライアンスを WAN とインラインに配置することで、これらの基準を満たすことができます。より複雑なサイトでは、他のオプションを利用できます。WCCP サポートなどの一部は、すべてのモデルで使用できます。その他は特定のモデルでのみ利用可能です。したがって、より複雑なサイトのニーズにより、アプライアンスの選択が制限される場合があります。

オプションを評価するときは、デバイスに障害が発生した場合や無効にする必要がある場合に備えて、ネットワークのさまざまなセグメントを稼働させ続けることの重要性を考慮してください。インライン展開の場合、Citrix は イーサネットバイパスカードを推奨します。このカードは Citrix SD-WAN WANOP アプライアンスではオプションであり、アプライアンスに障害が発生すると閉じるリレーがあり、電源が失われたり取り外されたりした場合でもパケットを通過させることができます。

冗長性は、すべてのタイプの展開で考慮されます。Citrix SD-WAN WANOP アプライアンスは、さまざまなタイプの冗長性を提供します。

- SD-WAN WANOP 4000/5000 アプライアンスにはデュアル電源があります。
- SD-WAN WANOP 4000/5000 アプライアンスには冗長ディスクドライブがあります。
- アプライアンスは、高可用性モードで使用できます（自動フェイルオーバーを備えた 2 つの冗長アプライアンス）。このモードはすべてのモデルでサポートされています。

> 注
>
> Citrix SD-WAN WANOP アプライアンスと展開モードの詳細については、SD-WAN WANOP プラットフォームのドキュメントを参照してください。

容量に基づいてアプライアンスを選択します

April 19, 2021

適切に動作させるには、Citrix SD-WAN WANOP アプライアンスに、高速化する WAN リンクの数をサポートし、それらのリンクのすべてのユーザーをサポートするための適切なリソースが必要です。Citrix SD-WAN WANOP アプライアンスを選択する場合、リンク容量（帯域幅）、ユーザー容量、およびディスク容量の 3 つの容量が重要です。

リンク容量

Citrix SD-WAN WANOP アプライアンスを選択する場合、最も重要な要素は、WAN リンクをサポートすることです。サイトに単一の WAN リンクがある場合、アプライアンスはリンク速度をサポートする必要があります。たとえば、Citrix SD-WAN WANOP 2000-010 は、最大 10 Mbps のリンクをサポートできます。これは、8 Mbps リンクには適していますが、12Mbps リンクには適していません。単一のアプライアンスによって高速化される複数のリンクがサイトにある場合、アプライアンスは、これらすべての WAN リンクを合計した合計速度をサポートする必要があります。

サポートされる最大速度は、アプライアンスのハードウェアと製品ライセンスの組み合わせによって決まります。ライセンスされた帯域幅制限は、ライセンスでサポートされている最大リンク速度です。

製品	ライセンス供与された **WAN BW** 範囲
現在の製品	
SD-WAN WANOP プラグイン	-
SD-WAN WANOP 400	2～6 Mbps
SD-WAN WANOP 800	2～10 Mbps
SD-WAN WANOP 2000、2000WS	10～50 Mbps
SD-WAN WANOP 3000	5 0-155
SD-WAN WANOP 4000	310～1,000 Mbps
SD-WAN WANOP 5000	1,500～2,000 Mbps

製品	ライセンス供与された **WAN BW** 範囲
SD-WAN WANOP VPX	1-45 Mbps

表 1. 製品ラインごとのライセンス帯域幅制限

Virtual Apps/Virtual Desktops. のユーザー容量

各アプライアンスは、XenApp または仮想デスクトップユーザーの最大数について評価されます。Virtual Apps または Virtual Desktops を使用する場合は、この値を超えないようにしてください。仮想アプリまたは仮想デスクトップを使用していない場合は、この数字を他のアプリケーションのユーザー数の大まかなガイドと考えてください。

製品	最大ユーザー数
SD-WAN WANOP プラグイン	1
SD-WAN WANOP 400	10-30
SD-WAN WANOP 800	20-100
SD-WAN WANOP 2000、2000WS	100-300
SD-WAN WANOP 3000	300-500
SD-WAN WANOP VPX	20-350
SD-WAN WANOP 4000	750-2,500
SD-WAN WANOP 5000	3,500-5,000

表 2。Virtual Apps/Virtual Desktops のユーザー容量

ディスクサイズ

ディスクスペースは主に圧縮履歴に使用され、ディスクスペースが多いほど圧縮パフォーマンスが向上します。

SD-WAN WANOP 4000/5000 シリーズは 1.8TB から 2.4TB のディスク容量を提供します。これは、SD-WAN WANOP 3000 の 2.1TB、SD-WAN WANOP 2000 の 470GB、SD-WAN WANOP 800 の 80GB、および SD-WAN WANOP 400 の 40GB と比較されます。SD-WAN WANOP VPX のディスク容量は 100～500GB です。理想的には、アプライアンスのディスク容量はリンクのデータのサイクルタイムよりも大きい必要があります。たとえば、ほとんど毎日の更新トラフィックを伝送するリンクには、24 時間以上のディスク容量が必要です。主にユーザーセッションを運ぶリンクでは、このウィンドウを小さくすることができます。（1 Mbps リンクは、フルスピードで 1 日あたり約 10 GB を転送できます。）

表 3. ディスクサイズのデータライフタイムの例

アプライアンスモデル	リンク速度**-1Mbps**	リンク速度**-10Mbps**	リンク速度**-100Mbps**	リンク速度**-1000Mbps**
リンク使用率 **33**% でのデータライフタイム				
SD-WAN WANOP 800	23 日	2.3 日	-	-
SD-WAN WANOP 2000、2000WS	141 日	14 日	-	-
SD-WAN WANOP 5000	717 日	72 日	7.2 日	17 時間
リンク使用率 **100**% でのデータライフタイム				
SD-WAN WANOP 800	8 日	19 時間	-	-
SD-WAN WANOP 2000、2000WS	47 日	4.7 日	-	-
SD-WAN WANOP 5000	239 日	24 日	2.4 日	6 時間

データセンタートポロジに基づいて展開モードを選択します

April 19, 2021

アプライアンスは、WAN リンクに沿って配置できます。アプライアンスは、インラインモードに 2 つのブリッジイーサネットポートを使用します。パケットは一方のイーサネットポートに入り、もう一方のイーサネットポートから出ます。このモードでは、アプライアンスを WAN ルーターと LAN の間に配置します。ネットワークの残りの部分では、アプライアンスがまったく存在しなかったかのようになります。その操作は完全に透過的です。

インラインモードには、他の展開モードに比べて次の利点があります。

- 最高性能。
- クイックインストールページのみを使用して、非常に簡単に構成できます。
- 他のネットワーク機器の再構成はありません。

他のモード（WCCP、仮想インライン、リダイレクタ）はセットアップが不便であり、通常はルータを再設定する必要があり、パフォーマンスがやや低下します。

基本的な展開の考慮事項は、サイトに単一の WAN ルーターがあるか複数の WAN ルーターがあるかです。また、どの機能をどのモードで使用できるかについても考慮する必要があります。VPN をサポートするための要件は、ネットワーク内のアプライアンスの配置に影響します。

Access Gateway アプライアンスは Citrix SD-WAN WANOP TCP 最適化をサポートし、Citrix SD-WAN WANOP アプライアンスが Access Gateway とともに展開されている場合に VPN 接続を高速化します。

展開モードの概要

アプライアンスは、次のモードで展開できます。

転送モード

- インラインモード**-**最高のパフォーマンス、最も透過的なモード。データは、一方の高速イーサネットポートに流入し、もう一方のポートに流出します。いかなる種類のルーターの再構成も必要ありません。
- デュアルブリッジとインライン—インラインと同じですが、2 つの独立したアクセラレーションブリッジがあります。
- **WCCP** モード-インラインモードが実用的でない場合に推奨されます。ほとんどのルーターでサポートされています。3 行のルーター構成のみが必要です。Cisco ルータで WCCP モードを使用するには、ルータが少なくとも IOS バージョン 12.0（11）S または 12.1（3）T を実行している必要があります。（WCCP は Web Cache Communications Protocol の略ですが、プロトコルはバージョン 2.0 で大幅に拡張され、さまざまなネットワークデバイスをサポートします。）
- 仮想インラインモード-WCCP モードと同様です。ポリシーベースのルーティングを使用します。通常、ルーターには専用の LAN ポートが必要です。イーサネットバイパスカードのないユニットでは推奨されません。Cisco ルータで仮想インラインモードを使用するには、ルータで IOS バージョン 12.3（4）T 以降が実行されている必要があります。
- グループモード：サイト内で、リンクごとに 1 つずつ、2 つ以上のインラインアプライアンスで使用されます。複数のブリッジ、WCCP、および仮想インラインモードがすべて実用的でない場合にのみ推奨されます。
- ハイアベイラビリティモード—2 つのインラインまたは仮想インラインアプライアンスを primary/secondary ペアに透過的に組み合わせます。プライマリアプライアンスがすべてのトラフィックを処理します。失敗した場合は、セカンダリアプライアンスが引き継ぎます。ルーターの設定は必要ありません。イーサネットバイパスカードを備えたアプライアンスが必要です。
- 透過モード—Citrix SD-WAN WANOP プラグインとの通信に推奨されるモード。透過モードでは、プラグインは Citrix SD-WAN WANOP アプライアンスと基本的に同じ方法で接続を開始し、接続の元の IP アドレスとポート番号を保持し、Citrix SD-WAN WANOP オプションを TCP/IP 選択したパケットのヘッダーに追加

します。対照的に、リダイレクタモード（非推奨）では、プラグインはパケットの宛先 IP とポート番号を変更して、アプライアンスのシグナリング IP（およびポート）と一致させます。

- リダイレクタモード（非推奨）-Citrix SD-WAN WANOP プラグインがトラフィックをアプライアンスに転送するために使用します。スタンドアロンモードとして使用することも、他の展開の 1 つと組み合わせて使用することもできます。ルーターの設定は必要ありません。

加速モード

- **Softboost** モード：ほとんどのリンクに推奨される高性能 TCP バリアント。ハードブーストモードよりもパフォーマンスは低くなりますが、どの展開でも機能します。通常の TCP と同じように動作しますが、より高速です。
- ハードブーストモード—高速リンク、大陸間リンク、衛星リンク、およびフルリンク速度を達成することが難しいその他の固定速度リンクに役立つ、非常にアグレッシブで帯域幅が制限された TCP バリアント。トラフィックシェーピングが不要な固定速度のポイントツーポイントリンクに推奨されます。

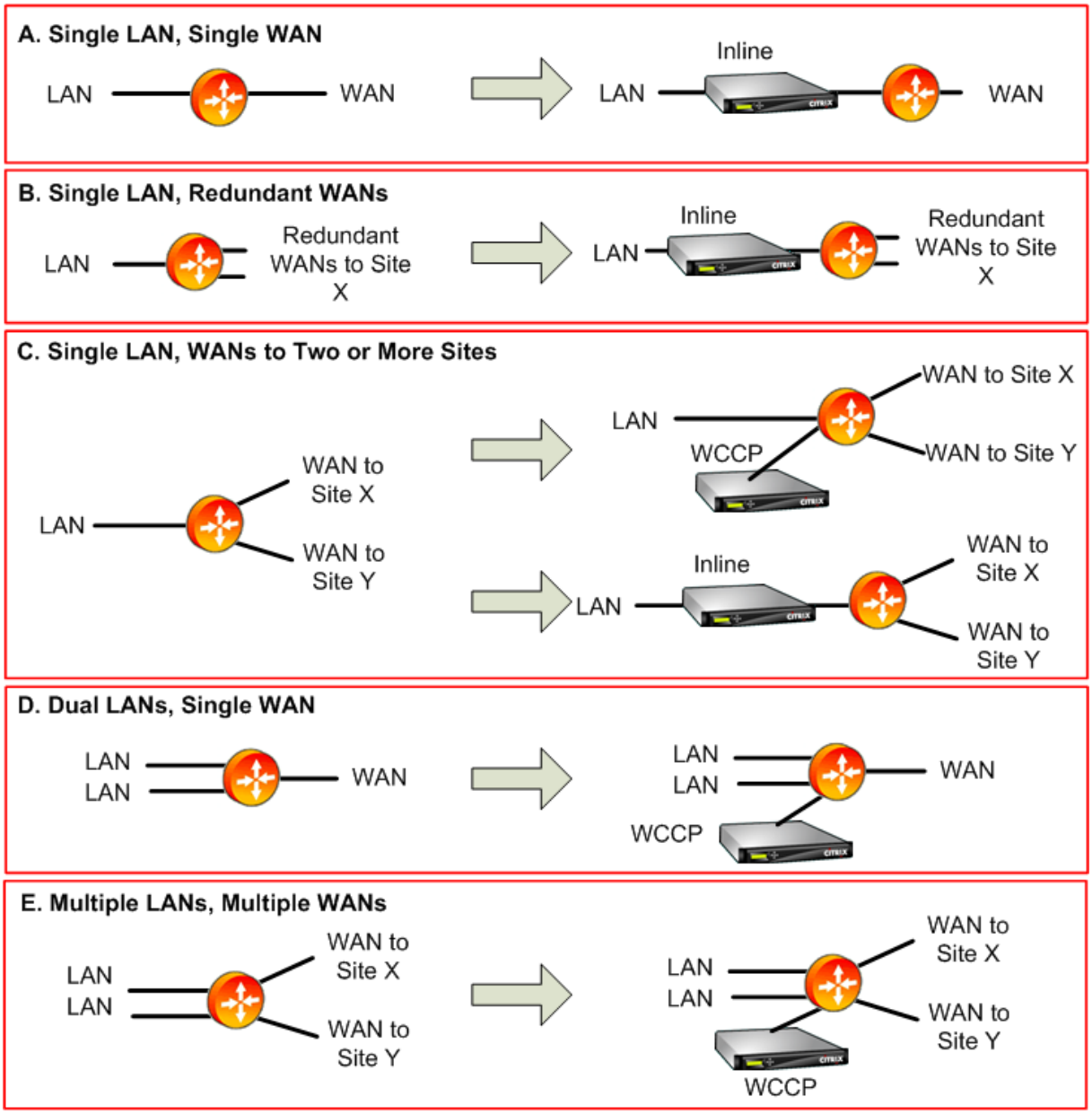
> 注
>
> Citrix SD-WAN WANOP アプライアンスと展開モードの詳細については、Citrix SD-WAN WANOP プラットフォームのドキュメントを参照してください。

WAN ルーターが 1 つあるサイト

April 19, 2021

WAN ルーターが 1 つしかないサイトの場合、展開における主な問題は、Citrix SD-WAN WANOP アプライアンスがルーターと調和して機能できるようにすることです。次の図は、単一ルーターの推奨される展開モードを示しています。ルーターのケーブル接続と比較して、ご使用の環境に最適なモードを見つけてください。

WAN ルータートポロジに基づく推奨される展開モード



推奨される展開モードに関するコメント:

1. シングル **LAN**、シングル **WAN**: インラインモード。ルータには、単一のアクティブ LAN インターフェイスと単一のアクティブ WAN インターフェイスがあります。この場合の推奨モードはインラインモードです。これは、どのモードよりも簡単なインストール、ほとんどの機能、および最高のパフォーマンスを提供します。
2. 単一 **LAN**、冗長 **WAN**: インラインモード。この構成にもインラインモードが最適です。
3. 単一 **LAN**、複数 **WAN**: インラインまたは **WCCP**。このトポロジは、ハブアンドスポークまたはマルチホップの 2 つのカテゴリに分類されます。ハブアンドスポーク展開では、接続は主にスポークサイトとハブサイトの間で行われます。マルチホップ展開では、多くの接続が 2 つのスポークサイト間にあり、データはハブサイトを通過します。したがって、ハブサイトのアプライアンスがトラフィックフローのどこに配置されているか

の詳細に応じて、単一のマルチホップ接続には最大 3 つのアプライアンスが含まれる可能性があります。

マルチホップ展開で適切なトラフィックシェーピングを行うには、ハブサイトの WAN ルーター上のすべての WAN トラフィックも、WAN インターフェイス間でルーターを直接通過させるのではなく、アプライアンスを通過する必要があります。この場合、WCCP が優先モードです。展開がハブアンドスポークであり、ほとんどのトラフィックがハブサイトで終了する場合は、インライン展開が推奨されます。

4. デュアル **LAN**、シングル **WAN**：インライン（デュアルブリッジ付き）または **WCCP**。このモードは、デュアルアクセラレーションブリッジ、WCCP モード、または仮想インラインモードでサポートされています。
5. 複数の **LAN**、複数の **WAN**：インライン（デュアルブリッジ）または **WCCP**。これはケース C に似ていますが、複数の LAN インターフェイスと複数の WAN が存在するため複雑です。ここではいつでも WCCP を使用できます。2 LAN の場合、デュアルブリッジを備えたアプライアンスをインラインモードで使用することもできます。

   詳細については、table を参照してください。

複数の **WAN** ルーターがあるサイト

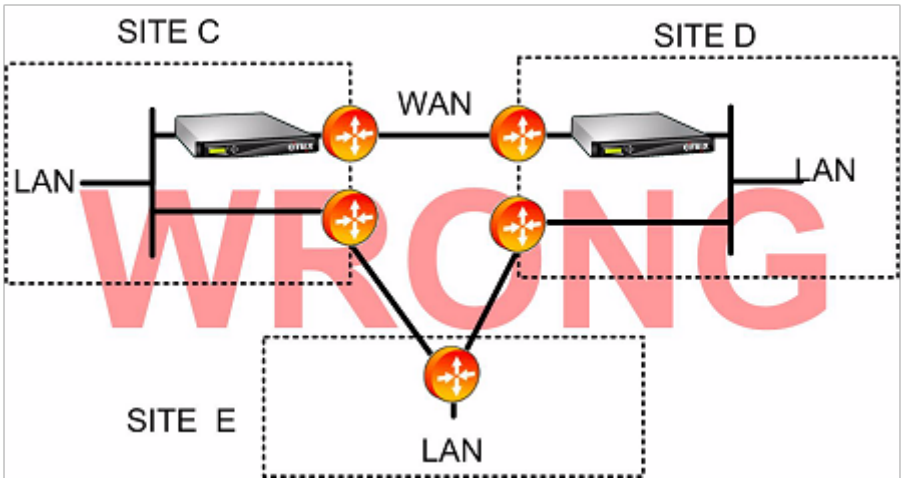
April 19, 2021

同じサイトに複数の WAN ルーターがあると、非対称ルーティングの可能性が高くなります。通常、IP ネットワークは、パケットが宛先に到着する限り、パケットがたどるパスの影響を受けません。ただし、アプライアンスは、内のすべてのパケットを確認することに依存しています。connection. 「エンドアラウンド」パケットは受け入れられません。

WAN ルーターが 1 つしかないサイトでは、アプライアンスをルーターとサイトの他の部分との間のパスに配置できるため、非対称ルーティングは問題になりません。ルーターに出入りするトラフィックもアプライアンスを通過します。ただし、WAN ルーターが 2 つあると、非対称ルーティングが問題になる可能性があります。

非対称ルーティングの問題は、インストール中またはその後に、セカンダリリンクへのフェイルオーバー、または他の形式の動的ルーティングと負荷分散の結果として発生する可能性があります。次の図は、非対称ルーティングの影響を受ける可能性のあるサイトの例を示しています。サイト C と D が常にダイレクトパス（CD または DC）を使用している場合、トラフィックを相互に送信するときは、すべて問題ありません。ただし、CED または DEC の長いパスを使用するパケットはアプライアンスをバイパスするため、新しい接続が加速されず、既存の接続がハングします。

非対称ルーティング

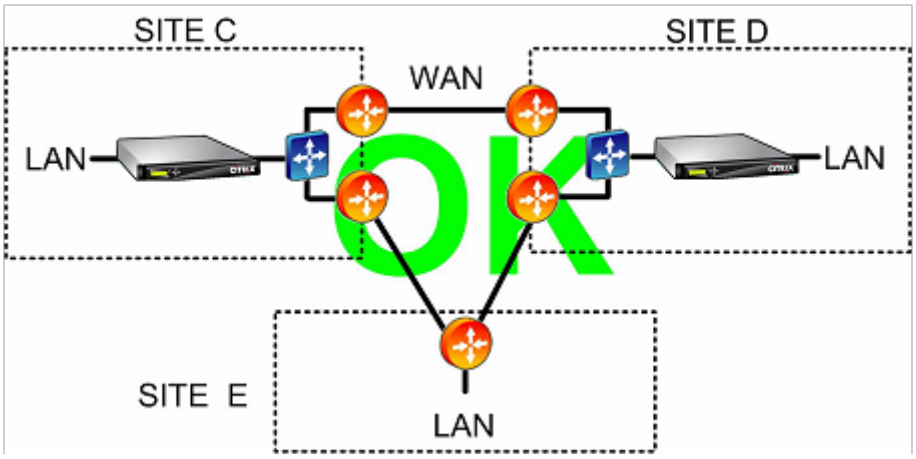


非対称ルーティングは、ルーター構成、アプライアンス配置、またはアプライアンス構成によって対処できます。

特定の接続のすべてのパケットが常にアプライアンスを両方向に通過するようにルーターが構成されている場合、非対称性はありません。

次の図に示すように、アプライアンスがすべての WAN ストリームが結合されたポイントの後に配置されている場合、非対称性が回避され、すべてのトラフィックが加速されます。

アプライアンスを適切に配置することで非対称ルーティングを回避する

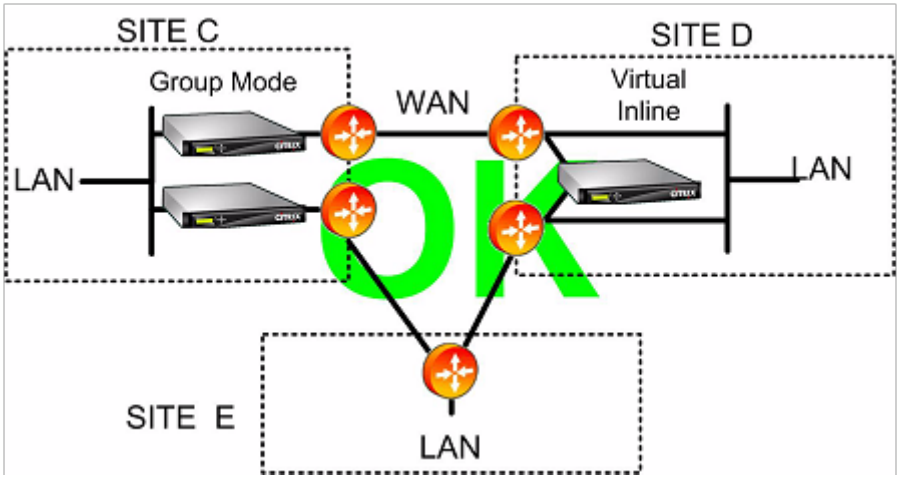


次の非対称転送モードのいずれかを使用するようにアプライアンスを構成すると、問題を解決できます。

- 複数のブリッジ。2 つの加速ブリッジまたは 加速ペア（たとえば、apA と apB）を備えたアプライアンスでは、2 つのリンクをインラインモードで加速できます。2 つのリンクは、完全に独立している、負荷分散されている、または primary/backup リンク。
- *WCCP* モードで は、単一のアプライアンスを複数の WAN ルーター間で共有できるため、どのリンクに到達するかに関係なく、すべての WAN トラフィックを処理できます。
- 仮想インラインモードで は、単一のアプライアンスを複数の WAN ルーター間で共有できるため、どのリンクに到達するかに関係なく、すべての WAN トラフィックを処理できます。

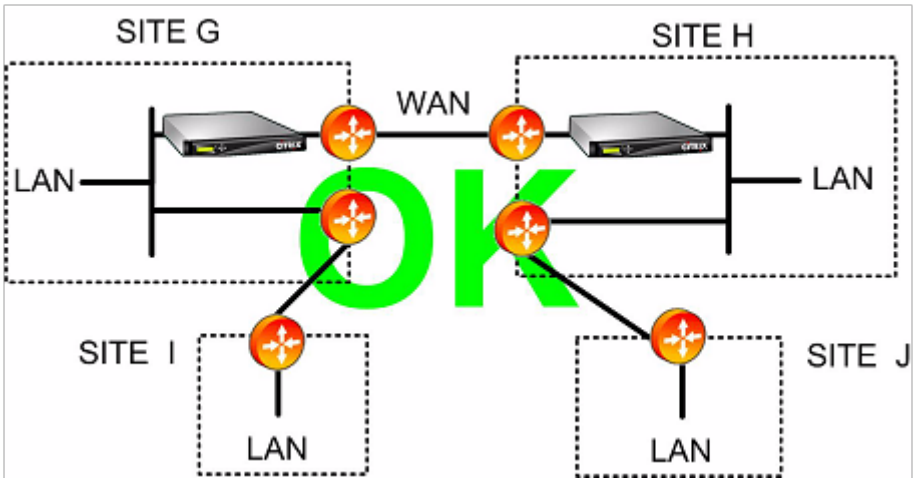
- グループモードで は、2 つ以上のインラインアプライアンスが互いにトラフィックを共有できるため、間違ったリンクに到着したトラフィックが適切にハンドオフされます。グループモードには複数のアプライアンスが必要なため、高速リンクの物理的な分離が広く、他の代替手段が困難な設置に最適な高価なソリューションです。たとえば、2 つの WAN リンクが同じ都市の異なるオフィスにある場合（ただし、キャンパスは LAN スピードリンクで接続されている場合）、グループモードが唯一の選択肢となる可能性があります。

グループモードまたは仮想インラインモードを使用した非対称ルーティングの排除



> 注
>
> リンクの一方の端は仮想インラインモードを使用でき、もう一方の端はグループモードを使用できます。リンクの両端は、同じ転送モードを使用する必要はありません。

WAN リンクが 1 つしかないサイトでは、非対称ルーティングの問題は発生しません。



さまざまな展開モードで処理されるアプライアンスの障害

April 19, 2021

Citrix SD-WAN WANOP アプライアンスには、ソフトウェア、ハードウェア、および電源障害が発生した場合の接続の喪失に対する保護手段があります。これらのセーフガードはモードに依存します。

インラインモードでは、アプライアンスは、ハードウェア、ソフトウェア、または電源障害が発生した場合でもネットワークの継続性を維持します。存在する場合、電源が失われたり、その他の障害が発生したりすると、アプライアンスのバイパスリレーが閉じます。バイパスカードのないインラインアプライアンスは通常、重大な障害が発生した場合にトラフィックをブロックしますが、ネットワークスタックは実行されているが、アクセラレーションソフトウェアが無効になっているか、永続的であるためにシャットダウンした場合など、特定の条件下でトラフィックを転送し続けます。エラー。

通常、既存の高速接続は障害後に応答しなくなり、最終的にはエンドポイントの 1 つでアプリケーションまたはネットワークスタックによって終了します。一部の加速接続は、障害後も加速されていない接続として継続する場合があります。新しい接続は非高速モードで実行されます。

アプライアンスがオンラインに戻ると、既存の接続は高速化されていない接続として継続されます。新しい接続が加速されます。

WCCP モードでは、ルータは応答を停止するアプライアンスをバイパスし、アプライアンスが再び応答を開始すると接続を再開します。WCCP プロトコルには、統合されたヘルスチェックがあります。

「verify-availability」オプションを 仮想インラインモードで使用すると、ルータは WCCP モードの場合と同じように動作し、使用できない場合はアプライアンスをバイパスし、使用できる場合は再接続します。「verify-availability」が使用されていない場合、アプライアンスが使用できないと、アプライアンスに転送されたすべてのパケットがドロップされます。

グループモードでは、アプライアンスは「オープン」（ブリッジングが無効）または「クローズド」（ブリッジングまたはバイパスリレーが有効）に失敗するように構成できます。

高可用性 モードでは、一方の HA アプライアンスに障害が発生すると、もう一方が自動的に引き継ぎます。アプライアンスのバイパスカードは HA モードでは無効になっているため、HA アプライアンスがインラインモードで両方のアプライアンスに障害が発生すると、接続が失われます。

リダイレクタモードでは、Citrix SD-WAN WANOP プラグインがリダイレクタモードアプライアンスのヘルスチェックを実行し、応答しないアプライアンスをバイパスして、代わりにエンドポイントサーバーにトラフィックを直接送信します。

サポートされているモードと機能マトリックス

April 19, 2021

通常、すべてのモードが同時にアクティブになります。ただし、次の表に示すように、一部の組み合わせは一緒に使用しないでください。

サポートされている組み合わせ、イーサネットバイパスカードを備えたユニット							
構成	インライン	仮想インライン	**WCCP-GRE**	**WCCP- L2**	複数ブリッジ	高可用性。	グループモード
Citrix SD-WAN WANOP プラグイン	o	o	o	o	o	o	×
インライン	o	×	×	×	o	o	o
仮想インライン		o	o	o	o	o	×
WCCP-GRE			o	o	o	o	×
WCCP- L2				o	o	o	×
複数ブリッジ					o	o	×
高可用性。						o	o
サポートされている組み合わせ、イーサネットバイパスカードのないユニット							
構成	インライン	仮想インライン	**WCCP-GRE**	**WCCP- L2**	複数ブリッジ	高可用性。	グループモード

サポートされている組み合わせ、イーサネットバイパスカードを備えたユニット							
Citrix SD-WAN WANOP プラグイン	×	×	×	×	×	×	×
インライン	O	×	×	×	×	×	×
仮想インライン		O	O	O	×	×	×
WCCP-GRE			O	O	×	×	×
WCCP- L2				O	×	×	×
複数ブリッジ					×	×	O
高可用性。						×	×

Y = はい、サポートされています。**N =** サポートされていません。

Access GatewayVPN を使用して **Citrix SD-WAN WANOP** プラグインを構成する

April 19, 2021

Access Gateway Standard Edition VPN は、Citrix SD-WAN WANOP アプライアンスが Access Gateway アプライアンスとともに展開され、Access Gateway アプライアンスがそれをサポートするように構成されている場合、Citrix SD-WAN WANOP プラグインアクセラレーションをサポートします。

他の VPN での Citrix SD-WAN WANOP プラグインのサポートについては、VPN のドキュメントを参照するか、Citrix の担当者にお問い合わせください。

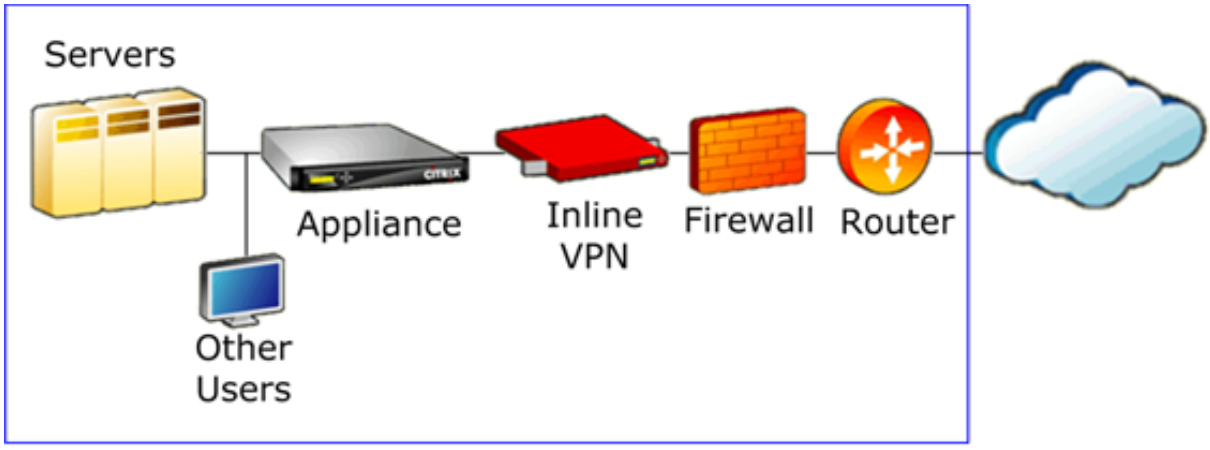
Citrix SD-WAN WANOP サポートを構成するには、次のように Access Gateway 管理ツールを使用します。

1. [グローバルクラスターポリシー] ページの [詳細オプション] で、[**Citrix SD-WAN WANOP** プラグインを使用して **TCP** 最適化を有効に する] チェックボックスをオンにします。
2. Citrix SD-WAN WANOP で使用される IP アドレス（リダイレクタ IP および管理 IP）で、[アクセスポリシーマネージャ] ページの [ネットワークリソース] セクションでアクセスが有効になっていることを確認してください。
3. これらのアドレスごとに、すべてのプロトコル（TCP、UDP、ICMP）を有効にし、[TCP オプションの保持] を有効にします。
4. これらの同じアドレスが [アクセスポリシーマネージャー] ページの [ユーザーグループ：デフォルト：ネットワークポリシー] に含まれていることを確認してください。

VPN サポートオプション

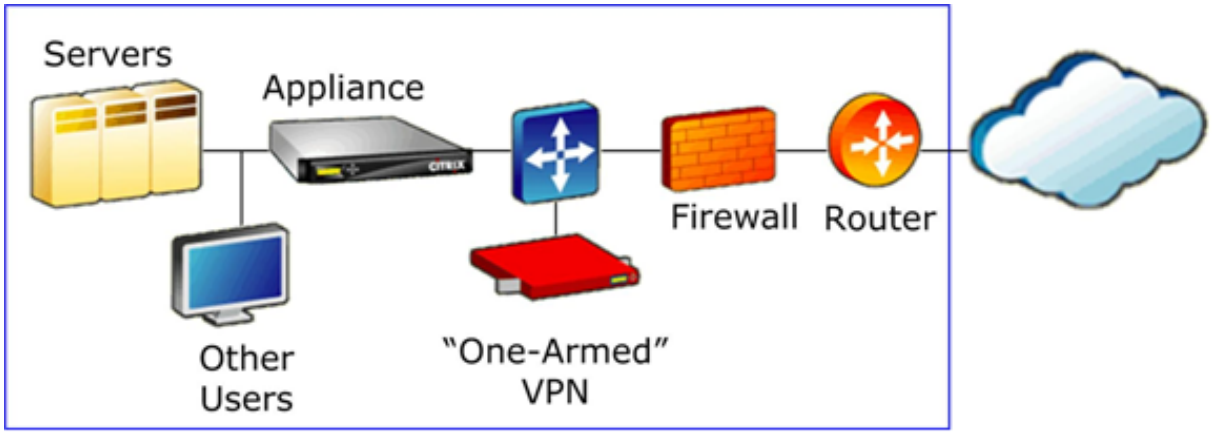
次の図に示すように、VPN のサポートは、アプライアンスを VPN の LAN 側に配置するだけです。この配置により、アプライアンスは、カプセル化が解除され、復号化されたプレーンテキストバージョンのリンクトラフィックを確実に送受信し、圧縮とアプリケーションアクセラレーションを機能させることができます。（アプリケーションの高速化と圧縮は、暗号化されたトラフィックには影響しません。ただし、TCP プロトコルアクセラレーションは暗号化されたトラフィックで機能します。）

インライン VPN の VPN ケーブル接続



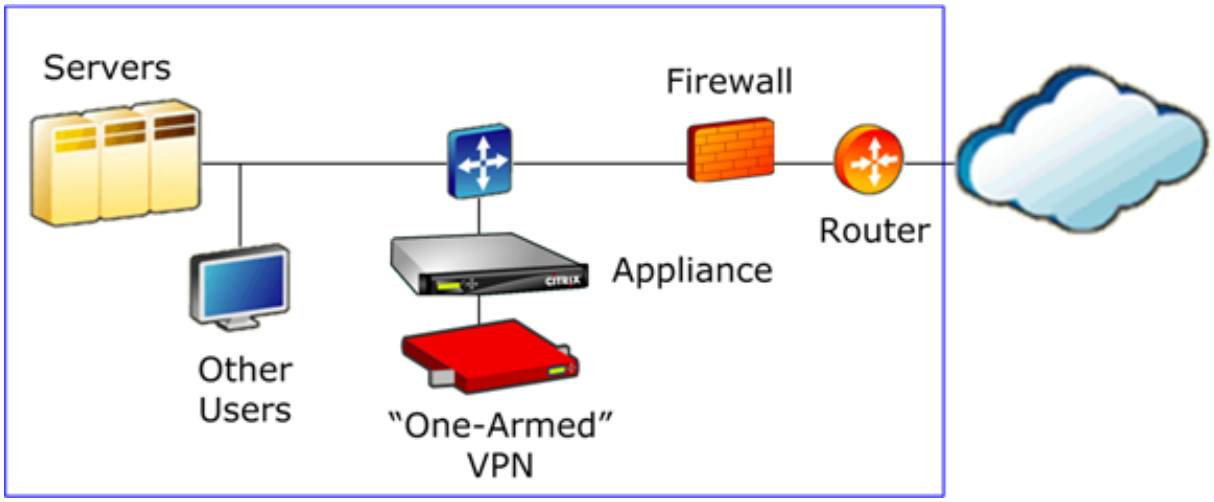
次の図は、ワンアーム VPN を高速化するための 1 つのオプションを示しています。アプライアンスは VPN のサーバー側にあります。ローカル宛先とのすべての VPN トラフィックが高速化されます。リモート宛先との VPN トラフィックは加速されません。VPN 以外のトラフィックも加速できます。

ワンアーム VPN アクセラレーション、オプション A



次の図は、ワンアーム VPN を高速化するための別のオプションを示しています。アプライアンスは VPN のサーバー側にあります。ローカル宛先とのすべての VPN トラフィックが高速化されます。リモート宛先との VPN トラフィックは加速されません。VPN 以外のトラフィックも加速できます。

ワンアーム VPN アクセラレーション、オプション B



> 重要
>
> アクセラレーションを有効にするには、VPN で TCP ヘッダーオプションを保持する必要があります。ほとんどの VPN はそうします。

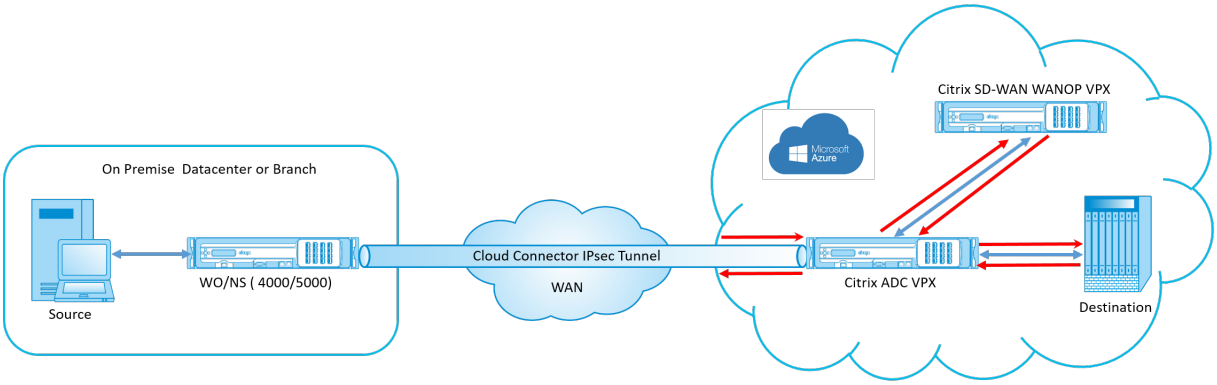
Microsoft Azure に SD-WAN WANOP VPX をデプロイする

April 19, 2021

Citrix SD-WAN WANOP Edition が Azure マーケットプレイスで利用可能になり、企業間の WAN 最適化が可能になりました datacenter/branch および Azure クラウド。L2 モードのサポートはクラウドインフラストラクチャでは利用できないため、Citrix SD-WAN WANOP をスタンドアロン VPX として Azure Cloud にデプロイすることは

できません。ただし、Citrix クラウドインフラストラクチャに Citrix SD-WAN WANOP VPX を Citrix ADC VPX と一緒にデプロイできます。Citrix ADC は Cloud Connector を使用して IPsec トンネルを作成し、Citrix SD-WAN WANOP VPX は接続を高速化し、アプリケーションに LAN のようなパフォーマンスを提供します。

Azure クラウドトポロジでの **Citrix SD-WAN WANOP**



トポロジ図は、Citrix SD-WAN を示しています 4000/5000 データセンターまたはブランチ構内に展開されます。Citrix SD-WAN WANOP と Citrix ADC アプライアンスを 2 ボックスモードで展開することも、両方を VPX にすることもできます。Azure クラウド VNET では、Citrix SD-WAN WANOP VPX は、Citrix ADC VPX を使用してワンアーム（PBR）モードで展開されます。

展開の概要

SD-WAN WANOP を MicrosoftAzure に展開するには:

1. Citrix ADC VPX インスタンスを Azure クラウドにデプロイします。詳しくは、「Microsoft Azure で Citrix ADC VPX インスタンスを展開する」を参照してください。4 つの異なるサブネットに 4 つのネットワークインターフェイスを構成し、すべてのネットワークインターフェイスで IP 転送を有効にします。4 つのネットワークインターフェイスは次のように使用されます。
   - 管理インターフェイス
   - WAN 側インターフェース、IPsec トンネル用
   - サーバーに接続するための LAN 側インターフェース
   - Azure クラウド上の Citrix SD-WAN WANOP VPX と通信するための WANOP 通信インターフェイス。
2. Citrix SD-WAN WANOP VPX を Azure クラウドにデプロイします。詳細については、以下の展開手順を参照してください。

   > 注意: WANOP インターフェースで IP 転送を有効にします。

3. Citrix ADC WAN インターフェイスのパブリック IP アドレスを使用して、オンプレミスアプライアンスと Azure クラウド上の Citrix ADC VPX の間に IPsec トンネルを構成します。IP トンネルの設定の詳細については、IP トンネルを参照してください。

4. パケットを Citrix SD-WAN WANOP VPX にリダイレクトするように Citrix ADC VPX を構成します。WANOP 通信インターフェースのプライベート IP アドレスを使用して、負荷分散仮想サーバーを作成します。詳しくは、「負荷分散仮想サーバーの作成」を参照してください。
5. Azure で次のルートテーブルを構成します。
   - Citrix ADC VPX の WANOP に面したインターフェイスのルートテーブル–ルートテーブルエントリには、クライアントサブネットとサーバーサブネットとしてそれぞれ送信元アドレスと宛先アドレスが必要です。Citrix ADC VPX の WANOP 対応インターフェイス IP アドレスはネクストホップです。
   - Citrix SD-WAN WANOP インターフェイスのルートテーブル-ルートテーブルエントリには、クライアントサブネットとサーバーサブネットとしてそれぞれ送信元アドレスと宛先アドレスが必要です。Citrix SD-WAN WANOP インターフェイスの IP アドレスはネクストホップです。

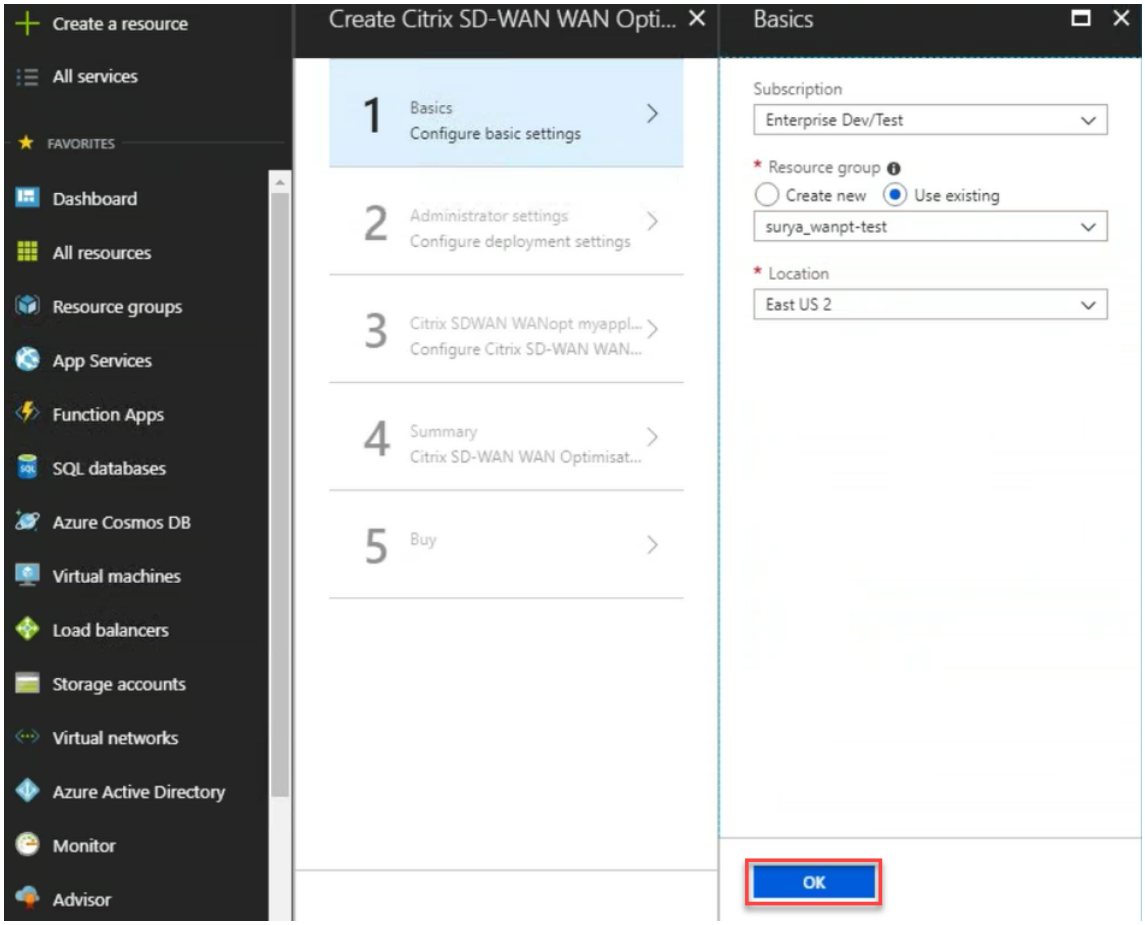
上記の例では、送信元がクラウドの宛先上のアプリケーションにアクセスしようとすると、パケットは確立された IPsec トンネルを通過します。Azure クラウド VNET 側で、Citrix ADC VPX はパケットを受信し、復号化して、Citrix SD-WAN WANOP VPX に転送します。Citrix SD-WAN WANOP VPX は、パケットを処理して最適化し、Citrix ADC VPX に送り返します。Citrix ADC VPX はパケットを宛先に送信します。リターンパスでは、Citrix ADC VPX がパケットを Citrix SD-WAN WANOP VPX に転送して最適化します。最適化されたパケットは、確立された IPsec トンネルを介して送信元に返送されます。

Microsoft Azure に Citrix SD-WAN OP VPX をデプロイする

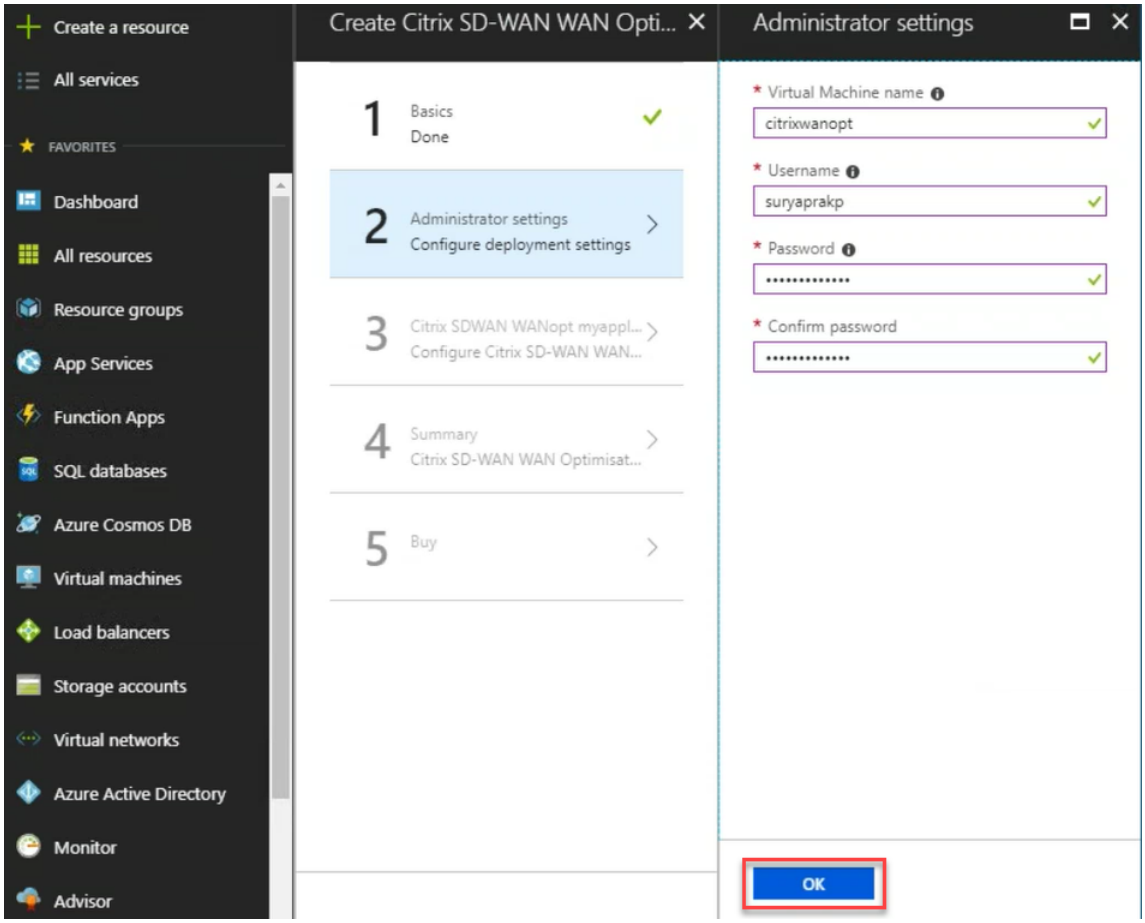
Citrix SD-WAN WANOP VPX を Microsoft Azure に展開するには:

1. Microsoft Azure で、[ホーム]> 市場 > ネットワークに移動し、**Citrix SD-WAN WANOP** を検索してインストールします。
2. Citrix SD-WAN WAN OP ページで、ドロップダウンリストから [リソースマネージャー] を選択し、[作成] をクリックします。[**Citrix SD-WANWAN** 最適化 の作成] ページが表示されます。
3. [基本] セクションで、サブスクリプションの種類、リソースグループ、および場所を選択します。[OK] をクリックします。

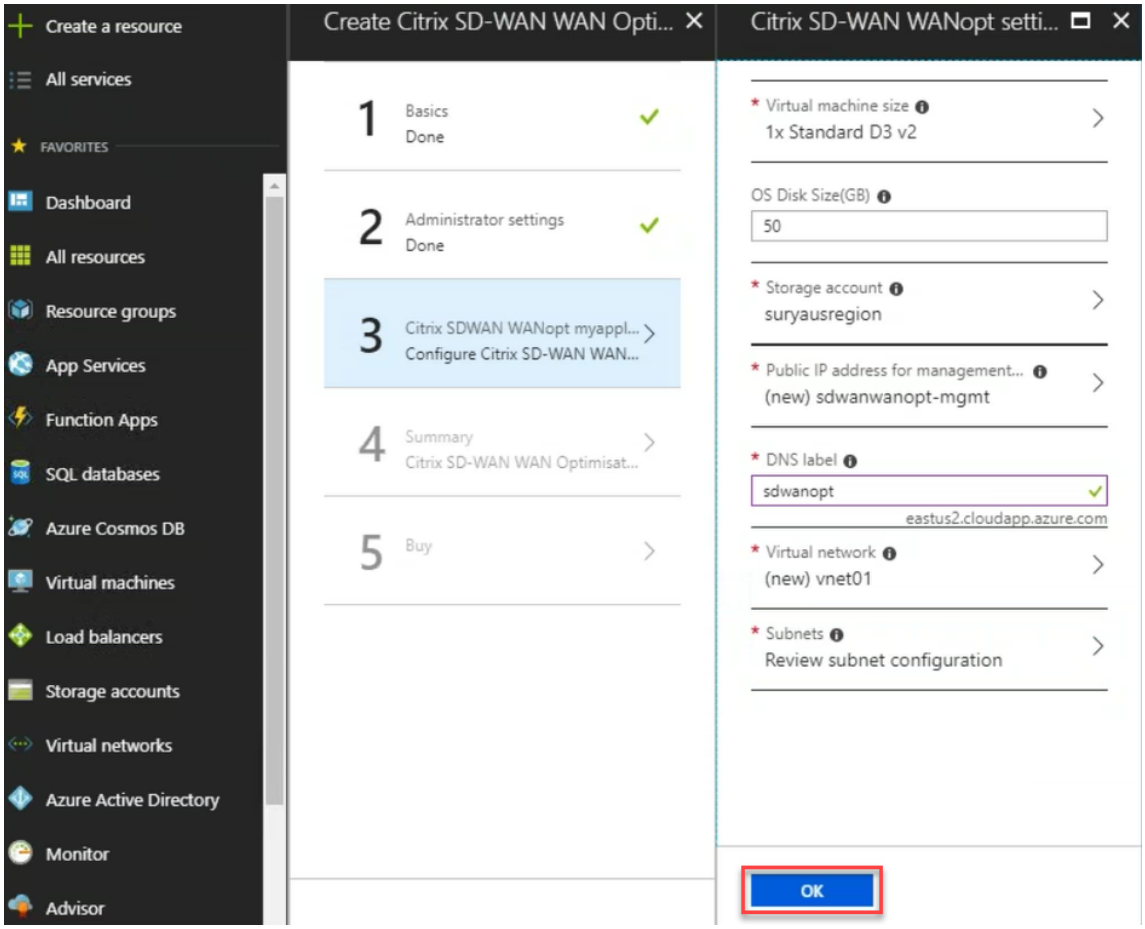
   > 注:
   >
   > リソースグループの作成を選択できます。リソースグループは、Azure ソリューションの関連リソースを保持するコンテナーです。リソースグループには、ソリューションのすべてのリソースを含めることも、グループとして管理するリソースのみを含めることもできます。



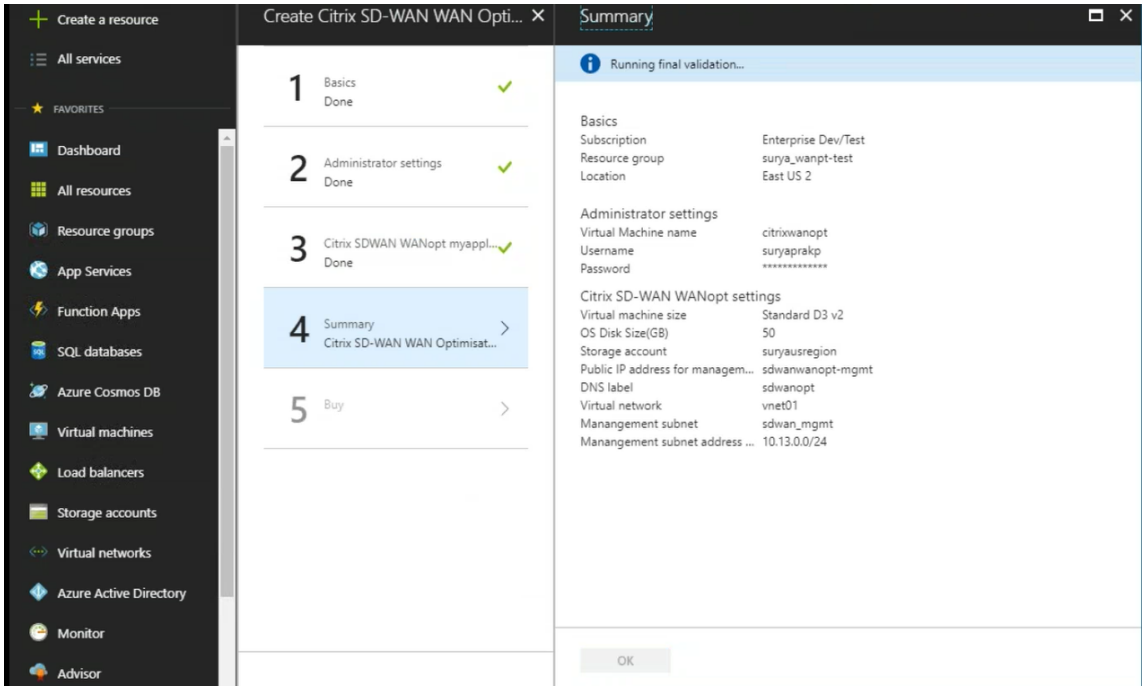
4. [管理者] セクションで、Citrix SD-WAN WANOP 仮想マシンの名前と資格情報を入力します。[**OK**] をクリックします。



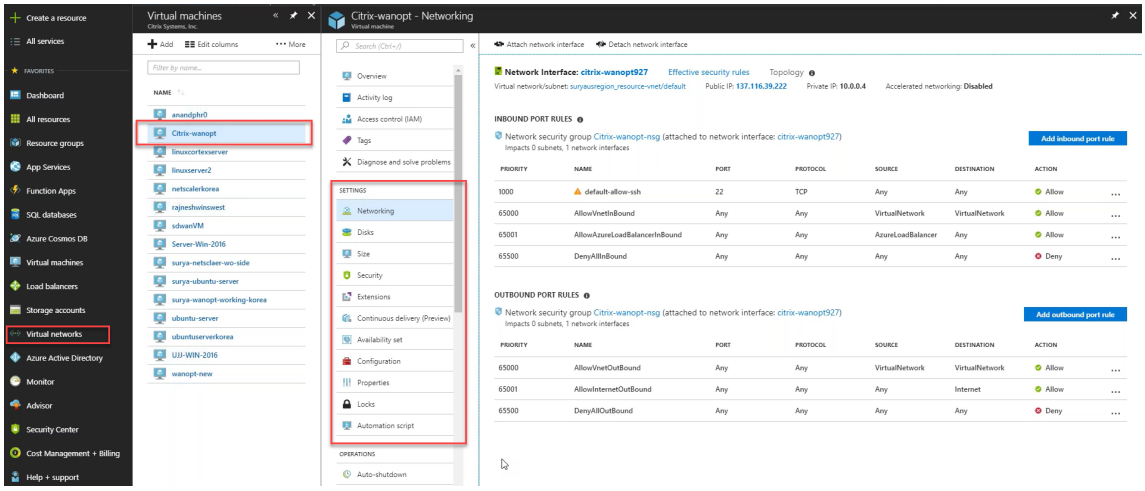
5. [**Citrix SD-WAN WANOP** 設定] セクションで、要件に応じて Citrix SD-WAN WANOP VPX の設定を構成します。[**OK**] をクリックします。



6. 前の手順で指定した構成が検証され、適用されます。正しく構成した場合、検証に合格したメッセージが表示されます。［**OK**］をクリックします。



7. 導入が成功したら、仮想ネットワーク に移動して Citrix SD-WAN WANOP VPX を表示します。設定オプションを使用して、仮想マシンのパラメーターをさらに構成できます。



SD-WAN WANOP のアップグレード手順

April 19, 2021

このセクションでは、Citrix SD-WAN WAN 最適化（WANOP）ソフトウェアパッケージのダウンロードとアップグレードに関する情報を提供します。

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

ソフトウェアパッケージをダウンロードする

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

Citrix SD-WAN WANOP ソフトウェアパッケージをダウンロードするには:

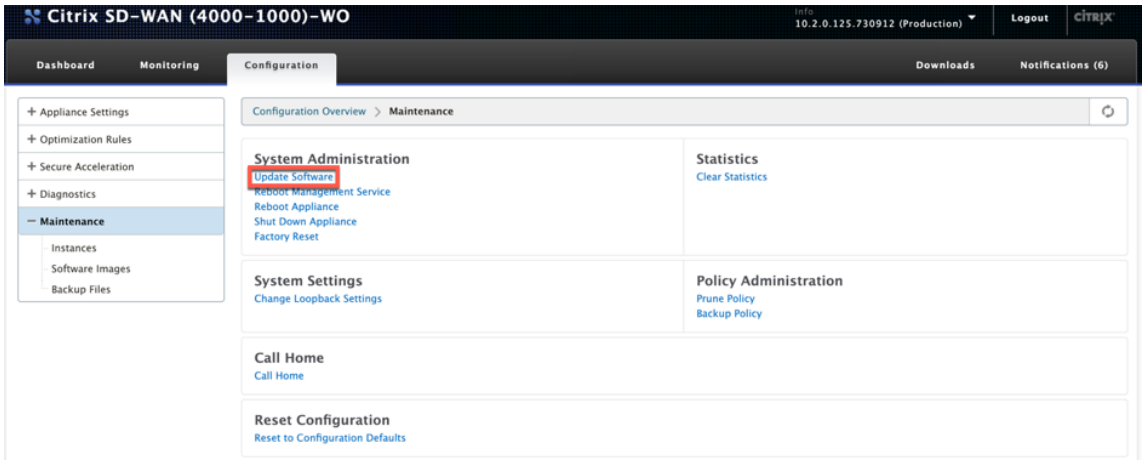
1. Google アカウントの資格情報を使用してcitrix.comにログインします。
2. ダウンロードページに移動し、ドロップダウンリストから製品（Citrix SD-WAN）を選択します。
3. **Citrix SD-WAN WANOP** エディション を展開し、必要なソフトウェアリリースを選択します。
4. 次のダウンロードオプションを使用できます。必要なソフトウェアをダウンロードします。
   - SD-WAN WANOP 400/800/1000/1000WS/2000/2000WS/3000/4000/4100/5000/5100 アプライアンスの.upg アップグレードファイルをダウンロードします。
   - SD-WAN WANOP VPX アプライアンスの.bin アップグレードファイルをダウンロードします。

SD-WAN WANOP がサポートするプラットフォームの詳細については、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を参照してください。

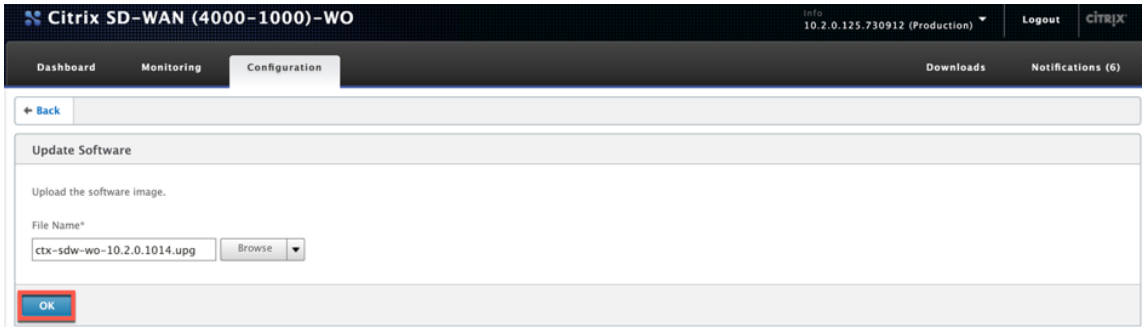
アップグレード手順

ソフトウェアを更新するには、次の手順を実行します。

1. 構成 **>** メンテナンス **>** システム管理 > [ソフトウェアの更新] をクリックします。

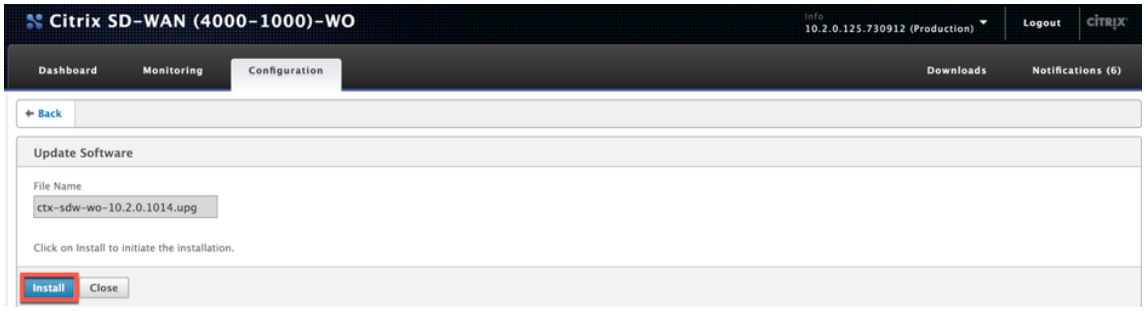


2. [参照] をクリックして、**ctx-sdw-wo-10.2.X.upg** ファイルを提供します。[**OK**] をクリックします。



アップロードステータスバーが表示されます。

3. アップロードが成功したことを通知するメッセージが表示されたら、[インストール] をクリックします。



4. アプライアンスはアップグレードを実行します。これには、プラットフォームモデルに基づいて 10～40 分かかります。アップグレードの準備から 始まり、アップグレードが正常に完了したまでの一連のステータスメッセージが表示されます。

5. [**OK]** をクリックして、更新されたユーザーインターフェイスを表示します。

初期構成

April 19, 2021

接続を確認したら、SD-WAN アプライアンスをネットワークに展開する準備が整います。

Citrix から出荷されたアプライアンスには、デフォルトの IP アドレスが構成されています。アプライアンスをネットワークに展開するには、アプライアンスに適切な IP アドレスを構成して、ネットワークトラフィックを高速化する必

要があります。

初期構成は、次のタスクで構成されています。

- 初期構成の前提条件を特定します。
- 初期構成手順で必要なさまざまな値を記録します。
- アプライアンスをイーサネットポートに接続して構成します。
- シリアルコンソールから管理 IP アドレスを割り当てます。

デフォルトでは、初期構成はアプライアンスをインラインモードで展開します。

前提条件

April 19, 2021

Citrix SD-WAN 4100 または 5100 アプライアンスを展開するには、アプライアンスを構成する前に、次の前提条件のセットアップを完了する必要があります。

ソフトウェアバージョン

このドキュメントでは、SD-WAN ソフトウェアのリリースについて説明します。SD-WAN ソフトウェアの目的のリリースに対応する NetScaler ソフトウェアの推奨バージョンについては、リリースノートを参照してください。SD-WAN4100 および 5100 アプライアンスに推奨されているバージョン以外のバージョンは絶対に使用しないでください。

ライセンス ファイル

アクセラレータアプライアンスの数は、ハードウェアプラットフォームと、アプライアンスに適用するライセンスの種類によって異なります。次のリストは、構成ウィザードによって自動的にプロビジョニングされるアクセラレータの数を示しています。

- Model 310: 2
- Model 500: 3
- Models 1000 および 1500: 6
- Model 2000: 8

アプライアンスの Provisioning を開始する前に、ライセンスファイルを用意することをお勧めします。これは、構成プロセスの早い段階で必要です。ライセンスファイルをダウンロードするには、「My Account All Licensing Tools-User Guide」で説明されている手順を完了します。

ハードウェアのインストール

Citrix からハードウェアアプライアンスを受け取ったら、ネットワークにインストールする必要があります。SD-WAN 4100/5100 アプライアンスハードウェアをインストールするには、ハードウェアのインストールのインストール手順に従います。

導入ワークシート

April 19, 2021

> 注
>
> このワークシートは、リリース 9.3 構成ウィザードを使用して出荷時設定にリセットされたアプライアンスをプロビジョニングする場合にのみ使用してください。以前に構成したシステムをリリース 9.3 にアップグレードするだけの場合、アプライアンスは以前の構成を保持しますが、これは異なります。

アプライアンスは少なくとも 2 つのポートを使用します: 管理ポート (通常は 0/1) およびトラフィックポート (10/1 など)。インラインモードでは、ポートなどのトラフィックポートをペアで使用します 10/1 そして 10/2. 構成はポートの ID に依存するため、ポートは事前に選択する必要があります。

アプライアンスは、管理サブネット、外部トラフィックサブネット、および内部トラフィックサブネットの 3 つのサブネットを直接使用します。各サブネットで複数の IP アドレスが使用されます。各サブネットは、正しいサブネットマスクとともに指定する必要があります。

次の図は、これらのパラメーターのワークシートです。高可用性の有無にかかわらず、インラインモードと WCCP モードをサポートします。図の下の表は、各エントリの意味を示しています。

表 **1** 展開ワークシートのパラメーター

	パラメーター	例	あなたの価値	説明
管理サブネット				
M2.	ゲートウェイの IP アドレス	10.199.79.254		管理サブネットにサービスを提供するデフォルトゲートウェイ。
M3.	サブネット マスク	255.255.255.128		管理サブネットのサブネットマスク。
M4.	Xen Hypervisor の IP アドレス	10.199.79.225		Xen Hypervisor の IP アドレス。

	パラメーター	例	あなたの価値	説明
M5.	サービス VM の IP アドレス	10.199.79.226		構成を制御する管理サービス VM の IP アドレス。
M6.	アクセラレータ UI	10.199.79.227		インスタンスを 1 つの単位として管理する、ブローカー UI とも呼ばれるアクセラレータ GUI。
M7.	NetScaler ManagementIP アドレス	10.199.79.245		NetScaler インスタンスの GUI および CLI インターフェースの IP アドレス。
外部トラフィックサブネット				
T1.	Router IP address	172.17.17.1		外部トラフィックサブネット上のルーターの IP アドレス。
T2.	サブネット マスク	255.255.255.0		外部トラフィックサブネットのサブネットマスク。
T3.	NetScaler の IP アドレス	172.17.17.2		外部トラフィックサブネット上の NetScalerIP アドレス。
T4.	外部シグナリング IP アドレス	172.17.17.10		この IP アドレスへのトラフィックは、アクセラレータのシグナリング IP アドレス間で負荷分散されます。
T5.	外部 WCCPIP アドレス #1	172.17.17.11		NAT を介してアクセラレータ上の WCCPVIP にマップします #1.
T6.	外部 WCCPIP アドレス #2	172.17.17.12		NAT を介してアクセラレータ上の WCCPVIP にマップします #2.

	パラメーター	例	あなたの価値	説明
T7.	ローカル LAN サブネット	10.200.0.0/16		加速されるローカル LAN サブネット。これは、アクセラレーションを受信する唯一のサブネットです。
T8.	GRE ルーターのホスト ID	-		WCCP-GRE のみ。GRE ルーターのホスト ID。
T9.	トラフィックポート	10/1		加速トラフィックに使用されるポート。
T10+.	（インライン）より多くのトラフィックポート			ペアの他のトラフィックポート。
T11, T12	（WCCP）サービスグループ：TCP、UDP	71, 72		アクセラレータ #1 が使用するサービスグループ WCCP の場合。1 つ目は TCP トラフィック用、2 つ目は UDP 用です。
T13, T14	（使用されていない）			
T15, T16	（インライン）リンク #2 で使用されるポート	10/5, 10/6		インラインモードで複数のリンクが使用されている場合、これらのポートはリンク #2 に使用されます
T17, T18	（インライン）リンク #3 で使用されるポート	10/7, 10/8		インラインモードで複数のリンクが使用されている場合、これらのポートはリンク #3 に使用されます
VLAN1.1、VLAN1.2、VLAN1.3、VLAN1.4	ブリッジ #1 の外部 VLAN	412		VLAN トランキングが使用されている場合、これらはブリッジ #1 を通過するタグ付き VLAN です。

	パラメーター	例	あなたの価値	説明
VLAN2.1、VLAN2.2、VLAN2.3、VLAN2.4				VLAN トランキングが使用されている場合、これらはブリッジ #2 を通過するタグ付き VLAN です。
VLAN3.1、VLAN3.2、VLAN3.3、VLAN3.4	ブリッジ #1 の外部 VLAN			VLAN トランキングが使用されている場合、これらはブリッジ #3 を通過するタグ付き VLAN です。

アプライアンスの構成

April 19, 2021

アプライアンスの構成を開始する前に、管理サービスの IP アドレスを管理ネットワーク内の IP アドレスに変更して、ネットワーク経由でアプライアンスにアクセスできるようにする必要があります。管理 IP アドレスは、イーサネットポートまたはシリアルコンソールを介してコンピューターをアプライアンスに接続することで変更できます。

イーサネットポートを介した管理 **IP** アドレスの割り当て

April 19, 2021

WindowsServer を使用するすべての SD-WAN1000 または 2000 アプライアンスの初期構成には、次の手順を使用します。この手順により、次のタスクが実行されます。

- サイトで使用するようにアプライアンスを構成します。
- Citrix ライセンスをインストールします。
- アクセラレーションを有効にします。
- トラフィックシェーピングを有効にします（インラインモードのみ）。

インライン展開では、ほとんどのアクセラレーション機能がデフォルトで有効になっており、追加の構成を必要としないため、この構成で十分な場合があります。

シリアルコンソールを使用してアプライアンスをコンピューターに接続して構成する場合は、シリアルコンソールを介した管理 IP アドレスの割り当て 手順を完了してワークシートから管理サービスの IP アドレスを割り当てて、次の手順の手順 4 ～15 を実行します。

> 注:
>
> アプライアンスに物理的にアクセスできる必要があります。

コンピューターを **SD-WAN** アプライアンスのイーサネットポートに接続してアプライアンスを構成するには **0/1**

1. コンピューター（またはイーサネットポートを備えた他のブラウザー搭載デバイス）のイーサネットポートアドレスを 192.168.100.50 に設定し、ネットワークマスクを 255.255.0.0 にします。Windows デバイスでは、これは、以下に示すように、LAN 接続のインターネットプロトコルバージョン 4 のプロパティを変更することによって行われます。ゲートウェイと DNS サーバーのフィールドは空白のままにすることができます。

2. イーサネットケーブルを使用して、このコンピューターを SD-WAN アプライアンスの PRI というラベルの付いたポートに接続します。
3. アプライアンスの電源を入れます。コンピュータの Web ブラウザを使用して、デフォルトの管理サービスの IP アドレス（つまりhttp://192.168.100.1）を使用してアプライアンスにアクセスします。
4. ログインページで、次のデフォルトの資格情報を使用してアプライアンスにログオンします。

- ユーザー名: nsroot
- パスワード: nsroot

1. 始めましょクリックして設定ウィザードを起動します。
2. 次の例に示すように、**[**プラットフォームの構成**]** ページで、ワークシートからそれぞれの値を入力します。

3. ［完了］をクリックします。インストール中…メッセージを示す画面が表示されます。このプロセスには、ネットワーク速度にもよりますが、約 2～5 分かかります。
4. 新しい管理 IP へのリダイレクトメッセージが表示されます。
5. ［**OK**］をクリックします。
6. コンピューターをイーサネットポートから取り外し、ポートを管理ネットワークに接続します。
7. コンピュータの IP アドレスを以前の設定にリセットします。
8. 管理ネットワーク上のコンピュータから、新しい管理サービス IP アドレス（`https://<Managemnt_IP_Address>`など）を Web ブラウザに入力して、アプライアンスにログオンします。
9. 構成を続行するには、証明書を受け入れて続行します。続行するオプションは、使用している Web ブラウザーによって異なります。
10. ワークシートの **nsroot** ユーザー名およびパスワードを使用して、アプライアンスにログオンします。
11. 設定プロセスを完了するには、アプライアンスのプロビジョニングを参照してください。

シリアルポートを介した管理 **IP** アドレスの割り当て

April 19, 2021

コンピューターの設定を変更したくない場合は、シリアルヌルモデムケーブルを使用してアプライアンスをコンピューターに接続することにより、アプライアンスを構成できます。アプライアンスに物理的にアクセスできる必要があります。

シリアルコンソールからアプライアンスを構成するには

1. シリアルヌルモデムケーブルをアプライアンスのコンソールポートに接続します。
2. ケーブルのもう一方の端を、Microsoft HyperTerminal などのターミナルエミュレーターを実行しているコンピューターのシリアル COM ポートに、設定 9600、N、8、1、p で接続します。
3. HyperTerminal 出力で、**Enter** キーを押します。ターミナル画面にログオンプロンプトが表示されます。注意: 使用している端末プログラムによっては、**Enter** キーを 2〜3 回押す必要がある場合があります。
4. ログオンプロンプトで、次のデフォルトの資格情報を使用してアプライアンスにログオンします。

- ユーザー名: nsroot
- パスワード: nsroot

1. **$** プロンプトで次のコマンドを実行して、アプライアンスのシェルプロンプトに切り替えます。`$ ssh 169.254.0.10`
2. [はい] を入力して、管理サービスへの接続を続行します。
3. 次のデフォルトの資格情報を使用して、アプライアンスのシェルプロンプトにログオンします。
   パスワード: nsroot。
4. ログオンプロンプトで、次のコマンドを実行して、管理サービスの初期ネットワークアドレス構成メニューを開きます。`# networkconfig`
5. **1** と入力し、**Enter** キーを押してオプション 1 を選択し、管理サービスの新しい管理 IP アドレスを指定します。
6. **2** を入力し、**Enter** キーを押してオプション 2 を選択し、Citrix Hypervisor の新しい管理 IP アドレスを指定します。
7. **3** と入力し、**Enter** キーを押してオプション 3 を選択し、IP アドレスのネットワークマスクを指定します。
8. **4** と入力し、**Enter** キーを押してオプション 4 を選択し、管理サービス IP アドレスのデフォルトゲートウェイを指定します。
9. **8** と入力し、**Enter** キーを押して設定を保存し、終了します。
10. SD-WAN アプライアンスにアクセスするには、管理ネットワーク上のコンピュータの Web ブラウザで、アプライアンスの新しい管理サービス IP アドレス（`https://<Management_Service_IP_Address>`など）を入力します。
11. 構成を続行するには、証明書を受け入れて続行します。続行するオプションは、使用している Web ブラウザーによって異なります。

12. 設定プロセスを完了するには、アプライアンスのプロビジョニングを参照してください。

アプライアンスのプロビジョニング

April 19, 2021

管理サービスに IP アドレスを割り当てたら、NetScaler およびアクセラレータインスタンスをプロビジョニングする準備が整います。アプライアンスにログオンすると、構成ウィザードが表示されます。

構成ウィザードを使用するときは、次の点に注意してください。

- 次の手順は、構成ワークシートにすでに記入していることを前提としています。
- 管理ネットワークの IP アドレスを変更した場合、またはデフォルトゲートウェイを管理ネットワーク上にないアドレスに変更した場合、管理ポートと同じイーサネットセグメントを使用していない限り、アプライアンスへの接続が失われます。
- 構成ウィザードを使用するときは、エントリを注意深く確認してください。ウィザードには [戻る] ボタンはありません。前の画面を変更する必要がある場合は、ブラウザの [戻る] ボタンを使用してください。これにより、ログオンページに移動し、次に前の画面に移動します。
- 構成ウィザードは、アプライアンスを構成するために初めてアプライアンスにログオンしたときにのみ表示されます。アプライアンスの構成が完了すると、このウィザードにアクセスできなくなり、工場出荷時のリセット後にのみ再表示されます。エントリを注意深く確認してください。

このウィザードは、アプライアンスの新しい構成を案内します。

> 注:
>
> あなたが受け取った場合 #SESS_CORRUPTED これらの手順中はいつでもエラーが発生します。
> [ログアウト] をクリックし、ブラウザのキャッシュをクリアして、ブラウザを閉じてから、もう一度開いてください。

構成ウィザードを使用してアプライアンスを構成するには、次のようにします。

1. [ようこそ] ページで、[開始] をクリックします。

   > 注:
   >
   > はじめにページの後のすべてのページには、「展開モード：Inline/L2 モード」というヘッダーが付きますが、このウィザードはすべての展開モードで使用されます。

2. 7.3 に完全に準拠したシステムを構成するには、次の手順に従います。

   - MyCitrix のリリース 7.3 ダウンロードページから次のリリース 7.3 ソフトウェア配布を入手します。
     - 管理サービス（.tgz ファイルとして）

  - NetScaler VM（.xva ファイルとして）
  - アクセラレータ VM（.xva ファイルとして）
  - バンドル（.upg として）ファイルをアップグレードする
- システム **>** 構成 **>** 管理サービス **\ > [**ソフトウェアイメージ**]** ページで、[アクション] リストから **[** アップロード**]** を選択します。
- リリース 7.3 管理サービスイメージをアップロードします（.tgz ファイルとして配布されます）。
- システム **>** 構成 **> NetScaler \ > [**ソフトウェアイメージ**]** ページに移動し、リリース 7.3 NetScalerXVA イメージをアップロードします。
- システム **>** 構成 **> SD-WAN \ > [**ソフトウェアイメージ**]** ページで、アクセラレーター XVA イメージをアップロードします。
- システム **>** 構成 **\ >** その後、管理サービスのページに移動し、アップグレード管理サービスのリンクをクリックしてください。
- 最近アップロードした管理サービスイメージを選択し、[**OK**] をクリックします。
- 画面の左下隅に「管理サービスが正常に更新されました」と表示されたら、ログオフしてブラウザのキャッシュをクリアします。管理サービスの再起動後（数分）にログオンします。
- [ようこそ] 画面で、[開始] をクリックします。

3. [管理アクセス設定] で、ネットワーク設定に従ってさまざまなフィールドに値を指定します。次のスクリーンショットは、このドキュメントで使用されているサンプル値を示しています。次のように値を入力します。

   - **Citrix Hypervisor IP** アドレス：（ワークシートの項目 M4、高可用性ペアの 2 番目のアプライアンスの場合は H4）。組み込みの Citrix Hypervisor の管理アドレス。これは、管理ネットワーク上の有効なアドレスである必要があります。

   - 管理サービスの **IP** アドレス—（ワークシートのアイテム M5、またはこれが高可用性ペアの 2 番目のアプライアンスである場合は H5）。ほとんどのシステム管理タスクを実行するために使用する管理サービス VM のアドレス。これは、管理ネットワーク上の有効なアドレスである必要があります。

   - ネットマスク—（ワークシートのアイテム M3）。管理ネットワークのサブネットマスク。

   - ゲートウェイ—（ワークシートのアイテム M2）。管理ネットワークのデフォルトゲートウェイ。

   - **DNS** サーバ：DNS サーバの IP アドレス。これは必須パラメーターです。

   - **NTP** サーバー-タイムサーバーの IP アドレスまたは FQDN アドレス。これは、アプライアンス内のすべての仮想マシンで使用されます。> 注 あなたは、高度な CIFS や MAPI アクセラレーションを使用する場合は、アプライアンスのシステム時刻で、あなたの Windows ドメインサーバ上の時間に密接な関係を維持して NTP サーバを選択し、近くに Windows ドメインサーバのものに し ておく必要があります。

     > 注:
     >
     > NTP サーバーが IP アドレスとして指定されていない限り、アクセラレータは使用しません。

   - タイムゾーン—プルダウンメニューからタイムゾーンを選択します。

- **[Change Password]**：このチェックボックスをオンにして、新しい nsroot パスワードを 2 回入力します。パスワードを変更します。これと同じパスワードが、アカウント nsroot の管理サービスと NetScaler インスタンス、および管理者アカウントのアクセラレータで使用されます。パスワードを変更しない場合は、nsroot（デフォルト）に設定されたままになります。
  図 1 構成の [管理アクセス設定] ページのフィールドのサンプル値

4. 設定を確認して、[続行] をクリックします。
5. **[**ライセンス の管理] セクションで、適切なライセンスが [名前**]** フィールドに既にリストされているかどうかを確認します。その場合は、それを選択して手順 8 に進みます。
6. [ライセンス の更新] セクションで [アップロード**]** をクリックします。
7. ライセンスファイルが含まれているフォルダーに移動し、ファイルを開きます。
8. [ライセンスの追加**]** をクリックして、Citrix が提供するライセンスファイルをアップロードします。次の図に示すように、ライセンスがアプライアンスに追加されます。
   図 2：構成ウィザードの [ライセンスファイルの管理] ページでアプライアンスに追加されたサンプルライセンス

   ここのリンクをクリックし、My Citrix 資格情報を使用して、Citrix.comWeb サイトからライセンスファイルを取得することもできます。
9. [名前**]** フィールドでライセンスを選択し、[続行] をクリックします。SD-WAN セットアップページが表示されます。次のようにフィールドに入力します。

   a) ネットワーク設定-このセクションは、管理ネットワークのアクセラレータに通知します。

      - **SD-WAN** アクセラレータの **IP** アドレス-ワークシートから M6 の値を入力します。これはアクセラレータの IP アドレスです
      - **NetScalerIP** アドレス-ワークシートから M7 の値を入力します。これは、NetScalerGUI の IP アドレスです。
      - **[**システムネットマスクとゲートウェイを使用する]-[プラットフォーム構成] ページで指定したネットワークマスクとゲートウェイの IP アドレスを使用する場合は、このオプションを選択します。
      - ネットマスク—ワークシートから M3 の値を入力します。これは、管理ネットワークのサブネットマスク（ネットマスク）です（前のページですでに入力していることに注意してください）。
      - ゲートウェイ-ワークシートから M2 の値を再入力します。
      - シグナリング **IP** アドレス-ワークシートから T4 の値を入力します。これは、アクセラレータの外部シグナリング IP アドレスであり、SD-WAN プラグインがアプライアンスに接続するために使用します。
      - シグナリングネットマスク—ワークシートから T2 の値を入力します。これは、外部トラフィックネットワークのサブネットマスク（ネットマスク）です。

   b) **XVA** ファイル-このセクションでは、NetScaler およびアクセラレータインスタンス用に以前にアップ

ロードされた XVA ファイル（Xen 仮想マシン）を指定できます。手順 2 の一部としてアップロードした XVA 画像を選択します。

図 3：SD-WAN セットアップページ

10. ［続行］をクリックします。次の図に示すように、ウィザードは必要なインスタンスのプロビジョニングを開始します。

    図 4：プロビジョニングの進行状況インジケーター

11. 次の図に示すように、インスタンスがプロビジョニングされたら、ワークシートのリスト T7 の [リンク構成] セクションにローカル LAN サブネットの 1 つを追加します。このサブネットは、アクセラレータでローカル LAN サブネットとして追加されます。複数の LAN サブネットがある場合は、構成ウィザードの完了後に、それらをアクセラレータ GUI の **LAN** リンク定義に追加できます。[追加] をクリックしてサブネットを追加します。

    図 5：リンク構成はこのページの下部にあります

12. ログオフしてから、再度ログオンします。「バージョンの非互換性が検出されました」というメッセージが表示された場合は、手順 2 でダウンロードしたアップグレードバンドルをインストールします。

基本設定が完了しました。次に、展開モード固有の設定（WCCP モードなど）を実行します。

> 注:
>
> ウィザードが完了すると、アプライアンスは基本セットアップ用に構成されます。アプライアンスを特定の展開シナリオ用に構成するには、
> 展開モードを参照してください。

展開モード

April 19, 2021

SD-WAN アプライアンスは仮想ゲートウェイとして機能します。TCP エンドポイントでもルーターでもありません。他のゲートウェイと同様に、その仕事は着信パケットをバッファリングし、適切な速度で発信リンクに配置することです。このパケット転送は、インラインモード、仮想インラインモード、WCCP モードなどのさまざまな方法で実行できます。これらのメソッドは モードと呼ばれますが、別の転送モードを有効にするために無効にする必要はありません。展開が複数のモードをサポートしている場合、アプライアンスが使用するモードは、各パケットのイーサネットおよび IP 形式によって自動的に決定されます。

アプライアンスはさまざまな転送モードとさまざまな種類の非転送接続をサポートしているため、ある種類のトラフィックを別の種類のトラフィックと区別する方法が必要です。これは、次の表に示すように、宛先 IP アドレスと宛先イーサネットアドレス（MAC アドレス）を調べることによって行われます。たとえば、インラインモードでは、アプ

ライアンスはブリッジとして機能します。他のトラフィックとは異なり、ブリッジパケットは、アプライアンス自体ではなく、アプライアンスを超えたシステムにアドレス指定されます。アドレスフィールドには、アプライアンスの IP アドレスもアプライアンスのイーサネット MAC アドレスも含まれていません。

純粋な転送モードに加えて、アプライアンスは、GUI への管理接続や、高可用性ペアのメンバー間で通過するハートビート信号など、追加の接続タイプを考慮する必要があります。完全を期すために、これらの追加のトラフィックモードも以下の表にリストされています。

表 **1.** イーサネットアドレスと **IP** アドレスがモードを決定する方法

宛先 IP アドレス	宛先イーサネットアドレス	モード
アプライアンスではありません	アプライアンスではありません	インラインまたはパススルー
アプライアンスではありません	アプライアンス	仮想インラインまたは L2WCCP
アプライアンス	アプライアンス	直接（UI アクセス）
アプライアンス（VIP）	アプライアンス	高可用性。プロキシモード
アプライアンス（WCCP GRE パケット）	アプライアンス	WCCP GRE モード
アプライアンス（シグナリング IP）	アプライアンス	シグナリング接続（SD-WAN プラグインシグナリング接続（SD-WAN プラグイン、セキュアピア）またはリダイレクタモード接続（SD-WAN プラグイン）

すべてのモードを同時にアクティブにすることができます。特定のパケットに使用されるモードは、イーサネットヘッダーと IP ヘッダーによって決定されます。

転送モードは次のとおりです。

- インラインモード。アプライアンスは、2 つのイーサネットポート間を流れるトラフィックを透過的に加速します。このモードでは、アプライアンスは（ネットワークの残りの部分からは）イーサネットブリッジのように見えます。最小限の構成で済むため、インラインモードをお勧めします。
- **WCCP** モード。WCCPv。2.0 プロトコルを使用してルーターと通信します。このモードは、ほとんどのルーターで簡単に構成できます。WCCP には、WCCP-GRE と WCCP-L2 の 2 つのバリアントがあります。WCCP-GRE は、WCCP トラフィックを Generic Routing Encapsulation（GRE）トンネル内にカプセル化します。WCCP-L2 は、カプセル化されていないネットワークレイヤ 2（イーサネット）トランスポートを使用します。
- 仮想インラインモード。ルーターが WAN トラフィックをアプライアンスに送信し、アプライアンスがそれをルーターに返します。このモードでは、アプライアンスはルーターのように見えますが、ルーティングテー

ブルを使用していません。リターントラフィックを実際のルーターに送信します。インラインモードと高速 WCCP 動作が実用的でない場合は、仮想インラインモードをお勧めします。
- グループモード。2 つのアプライアンスが一緒に動作して、広く分離された WAN リンクのペアを高速化します。
- 高可用性モード：アプライアンスがアクティブ/スタンバイの高アベイラビリティペアとして動作できるようにします。プライマリアプライアンスが停止するとセカンダリアプライアンスが処理を引き継ぎます。

完全を期すために、追加のトラフィックタイプをここに示します。

- パススルー トラフィックとは、アプライアンスが加速を試みないトラフィックを指します。これはトラフィックカテゴリであり、転送モードではありません。
- アプライアンスが通常のサーバーまたはクライアントとして機能する直接アクセス。GUI および CLI は、HTTP、HTTPS、SSH、または SFTP プロトコルを使用した直接アクセスの例です。直接アクセストラフィックには、NTP および SNMP プロトコルを含めることもできます。
- アプライアンス間の通信。シグナリング接続（セキュアピアリングおよび SD-WAN プラグインで使用）、VRRP ハートビート（高可用性モードで使用）、暗号化 GRE トンネル（グループモードで使用）が含まれます。
- 非推奨のモード。プロキシモードとリダイレクタモードはレガシー転送モードであり、新規インストールでは使用しないでください。

SD-WAN 4100/5100 アプライアンスには、WCCP とインラインの 2 つの推奨展開モードがあります。これらのモードは、通常、高可用性（ハイアベイラビリティ）なしで使用され、高可用性ではあまり使用されません。

現在、Citrix は、ほとんどの展開で、ルーターが 1 つで、高可用性がない WCCP モードを推奨しています。WCCP が使用できない場合は、インラインモードを使用してください。

現在、次のモードのすべてが推奨されているわけではありませんが、すべてサポートされています。

- 単一ルータの WCCP モード
- 1 台のルータと高可用性を使用した WCCP モード
- NetScaler MPX アプライアンスを使用した WCCP モードの 2 つ以上のアプライアンスのカスケード
- WCCP モードの 2 つ以上のアプライアンスと高可用性の NetScaler MPX アプライアンスのカスケード
- インラインモード
- 高可用性のインラインモード
- 仮想インラインモード
- 高可用性の仮想インラインモード

> 注
>
> WCCP およびインライン以外のモードはサポートされていますが、それらは完全に文書化されていないため、通常のインストールには推奨されません。これらのモードのいずれかを検討する場合は、Citrix の担当者にお問い合わせください。

イーサネットポートのカスタマイズ

April 19, 2021

一般的なアプライアンスには、4 つのイーサネットポートがあります。バイパス（配線に失敗）リレーを備えた 加速ペア *A* （apA.1 および apA.2）と呼ばれる 2 つの加速ブリッジポートと、プライマリおよび Aux1 と呼ばれる 2 つの加速されていないマザーボードポートです。ブリッジポートは加速を提供しますが、マザーボードポートは二次的な目的で使用されることもあります。ほとんどのインストールでは、ブリッジポートのみが使用されます。

一部の SD-WAN ユニットには、マザーボードポートしかありません。この場合、2 つのマザーボードポートがブリッジされます。

アプライアンスのユーザーインターフェイスには、VLAN または非 VLAN ネットワークからアクセスできます。管理目的で、アプライアンスのブリッジポートまたはマザーボードポートのいずれかに VLAN を割り当てることができます。

図 1：イーサネットポート

ポートリスト

ポートの名前は次のとおりです。

イーサネット ポート	名前
マザーボードポート 1	プライマリ（またはバイパスカードが存在しない場合は apA.1）
マザーボードポート 2	Auxiliary1 または Aux1（またはバイパスカードが存在しない場合は apA.2）
ブリッジ #1	加速ペア A（apA、ポート apA.1 および apA.2）
ブリッジ #2	加速ペア B（apB、ポート apB.1 および apB.2）

表 1. イーサネットポート名

ポートパラメータ

April 19, 2021

各ブリッジとマザーボードポートは次のようになります。

- 有効または無効
- 割り当てられた IP アドレスとサブネットマスク
- デフォルトゲートウェイを割り当てました
- VLAN に割り当てられています
- 1000 Mbps、100 Mbps、または 10Mbps に設定
- 全二重、半二重、または自動に設定（SD-WAN WANOP の場合）4000/5000 アプライアンス、一部のポートは 10 Gbps に設定できます）

を除くこれらすべてのパラメータ speed/duplex 設定は、[構成：IP アドレス] ページで設定します。ザ・speed/duplex 設定は、「構成：インターフェース」ページで設定します。

> パラメータに関する注意：

- 無効にしたポートは、どのトラフィックにも応答しません。
- ブラウザベースの UI は、すべてのポートで個別に有効または無効にできます。
- IP アドレスを持つポートの UI を保護するには、[構成：管理者インターフェイス：Web アクセス] ページで HTTP ではなく HTTPS を選択します。
- インラインモードは、ブリッジに IP アドレスがない場合でも機能します。他のすべてのモードでは、IP アドレスをポートに割り当てる必要があります。
- トラフィックはインターフェイス間でルーティングされません。たとえば、ブリッジ apA の接続は、プライマリポートまたは Aux1 ポートにクロスオーバーしませんが、ブリッジ apA には残ります。ルーティングの問題はすべてルーターに任されています。

アクセラレーションブリッジ（**apA** および **apB**）

April 19, 2021

すべてのアプライアンスには、*apA*（加速ペア *A* の場合）と呼ばれる加速ブリッジとして機能するイーサネットポートのペアが少なくとも 1 つあります。橋はインラインで機能できます mode, イーサネットスイッチのように、透過的なブリッジとして機能します。パケットは一方のポートに流入し、もう一方のポートから流出します。橋は片方の腕で行動することもできます mode, パケットは 1 つのポートを流れ、同じポートからバックアウトします。

バイパスカードを備えたアプライアンスは、ブリッジまたはアプライアンスが誤動作した場合でもネットワークの継続性を維持します。

一部のユニットには複数の加速ペアがあり、これらの追加の加速ペアには apB、apC などの名前が付けられます。

バイパスカード

アプライアンスの電源が切れたり、その他の方法で障害が発生した場合、内部リレーが閉じ、2 つのブリッジポートが電気的に接続されます。この接続はネットワークの継続性を維持しますが、ブリッジポートにアクセスできなくな

ります。したがって、管理アクセスにマザーボードポートの 1 つを使用することをお勧めします。

注意：プライマリポートがネットワークに接続されていない場合は、プライマリポートを有効にしないでください。そうしないと、アプライアンスにアクセスできません。詳細については、「イーサネットバイパスとリンクダウン伝搬」を参照してください。

バイパスカードは、一部のモデルでは標準であり、他のモデルではオプションです。すべてのインライン展開では、バイパスカード付きのアプライアンスを購入することをお勧めします。

バイパス機能は、クロスケーブルが 2 つのポートを接続しているかのように配線されます。これは、適切に配線された設置での正しい動作です。

重要：バイパスの設置をテストする必要があります-不適切なケーブル接続は通常の操作では機能する可能性がありますが、バイパスモードでは機能しない可能性があります。イーサネットポートは不適切なケーブル接続に耐性があり、多くの場合、サイレントに調整します。バイパスモードはハードワイヤードであり、そのような適応性はありません。アプライアンスをオフにしてインラインインストールをテストし、ケーブル接続がバイパスモードに対して正しいことを確認します。

複数のブリッジを使用する

アプライアンスに 2 つの加速ブリッジが装備されている場合、それらを使用して 2 つの異なるリンクを加速できます。これらのリンクは、完全に独立している場合もあれば、同じサイトに接続する冗長リンクの場合もあります。冗長リンクは、負荷分散することも、メインリンクおよびフェイルオーバーリンクとして使用することもできます。

図 1：デュアルブリッジの使用

アプライアンスが特定の接続のパケットを送信する時間になると、パケットは、アプライアンスがその接続の最新の入力パケットを受信したのと同じブリッジを介して送信されます。したがって、アプライアンスは、ルータによって行われたリンクの決定をすべて尊重し、一般的な負荷分散または main-link/failover-link リアルタイムのアルゴリズム。負荷分散されていないリンクの場合、後者のアルゴリズムは、パケットが常に正しいブリッジを使用することも保証します。

WCCP および仮想インラインモード

複数のブリッジは、WCCP モードと仮想インラインモードの両方でサポートされています。使用法はシングルブリッジの場合と同じですが、WCCP には、特定の WCCP サービスグループのすべてのトラフィックが同じブリッジに到着する必要があるという追加の制限があります。

複数のブリッジによる高可用性

複数のブリッジを持つ 2 台のユニットを、高可用性ペアで使用できます。すべてのリンクが両方のアプライアンスを通過するように、ブリッジを一致させるだけです。

マザーボードポート

April 19, 2021

バイパスリレーが閉じている場合、バイパスカードのイーサネットポートにはアクセスできませんが、マザーボードポートはアクティブのままです。ブリッジポートにアクセスできない場合は、マザーボードポートを介して障害のあるアプライアンスにアクセスできることがあります。

プライマリポート

プライマリポートが有効で、IP アドレスが割り当てられている場合、アプライアンスはその IP アドレスを使用して、他のアクセラレーションユニットに対して自身を識別します。このアドレスは、さまざまな目的で内部的に使用され、[監視：最適化：接続] ページの [パートナーユニット] フィールドとしてユーザーに最もよく表示されます。マザーボードポートが有効になっていない場合、アプライアンスは Accelerated PairA の IP アドレスを使用します。

プライマリポートは次の目的で使用されます。

- Web ベースの UI による管理
- グループモードのバックチャネル
- 高可用性モードのバックチャネル

AUX1 ポート

Aux1 ポートはプライマリポートと同じです。Aux1 ポートが有効になっていて、プライマリポートが有効になっていない場合、アプライアンスは Aux1 ポートの IP アドレスから ID を取得します。両方が有効になっている場合、プライマリポートの IP アドレスはユニットの ID です。

VLAN のサポート

April 19, 2021

仮想ローカルエリアネットワーク（VLAN）は、イーサネットヘッダーの一部を使用して、特定のイーサネットフレームが属する仮想ネットワークを示します。SD-WAN アプライアンスは、すべての転送モード（インライン、WCCP、仮想インライン、およびグループモード）で VLAN トランキングをサポートします。VLAN タグの任意の組み合わせを持つトラフィックは、正しく処理および加速されます。

たとえば、高速化されたブリッジを通過する 1 つのトラフィックストリームが 10.0.0.1、VLAN 100 にアドレス指定され、別のトラフィックストリームが 10.0.0.1、VLAN 111 にアドレス指定されている場合、アプライアンスは、2 つの VLAN が持っていても、これらが 2 つの異なる宛先であることを認識します。同じ IP アドレス。

VLAN は、アプライアンスのイーサネットポートのすべて、一部、またはまったく割り当てられません。VLAN がポートに割り当てられている場合、管理インターフェイス（GUI および CLI）はその VLAN 上のトラフィックのみをリッスンします。VLAN が割り当てられていない場合、管理インターフェイスは VLAN のないトラフィックのみをリッスンします。この選択は、[構成]: [アプライアンス設定]: [ネットワークアダプター]: [IP アドレス] タブで行います。

イーサネットポートのカスタマイズ

April 19, 2021

一般的なアプライアンスには、4 つのイーサネットポートがあります。バイパス（配線に失敗）リレーを備えた 加速ペア *A* （apA.1 および apA.2）と呼ばれる 2 つの加速ブリッジポートと、プライマリおよび Aux1 と呼ばれる 2 つの加速されていないマザーボードポートです。ブリッジポートは加速を提供しますが、マザーボードポートは二次的な目的で使用されることもあります。ほとんどのインストールでは、ブリッジポートのみが使用されます。

一部の SD-WAN ユニットには、マザーボードポートしかありません。この場合、2 つのマザーボードポートがブリッジされます。

アプライアンスのユーザーインターフェイスには、VLAN または非 VLAN ネットワークからアクセスできます。管理目的で、アプライアンスのブリッジポートまたはマザーボードポートのいずれかに VLAN を割り当てることができます。

図 1: イーサネットポート

ポートリスト

ポートの名前は次のとおりです。

イーサネット ポート	名前
マザーボードポート 1	プライマリ（またはバイパスカードが存在しない場合は apA.1）
マザーボードポート 2	Auxiliary1 または Aux1（またはバイパスカードが存在しない場合は apA.2）
ブリッジ #1	加速ペア A（apA、ポート apA.1 および apA.2）
ブリッジ #2	加速ペア B（apB、ポート apB.1 および apB.2）

表 1. イーサネットポート名

イーサネットバイパスとリンクダウン伝搬

April 19, 2021

注: リンクダウン伝播は、7.2.1 リリースで SD-WAN（以前の SD-WAN）1000、2000、3000、4000、および 5000 アプライアンスに追加されました。

ほとんどのアプライアンスモデルには、インラインモード用の「配線失敗」（イーサネットバイパス）機能が含まれています。電源に障害が発生すると、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、アプライアンスがないかのようにイーサネット信号が一方のポートからもう一方のポートに通過できるようになります。フェイルトゥワイヤモードでは、アプライアンスは 2 つのポートを接続するクロスケーブルのように見えます。

アプライアンスのハードウェアまたはソフトウェアに障害が発生すると、リレーも閉じます。アプライアンスを再起動すると、アプライアンスが完全に初期化されるまでバイパスリレーは閉じたままになり、ネットワークの継続性が常に維持されます。この機能は自動であり、ユーザー設定は必要ありません。

バイパスリレーが閉じていると、アプライアンスのブリッジポートにアクセスできなくなります。

キャリアが一方のブリッジポートで失われた場合、キャリアはもう一方のブリッジポートにドロップされ、リンクダウン状態がアプライアンスの反対側のデバイスに確実に伝播されます。したがって、リンク状態を監視するユニット（ルーターなど）には、ブリッジの反対側の状態が通知されます。

リンクダウン伝播には、次の 2 つの動作モードがあります。

- プライマリポートが有効になっていない場合、一方のブリッジポート上のリンクダウンステートは、もう一方のブリッジポート上で一時的にミラーリングされ、その後再び有効になります。これにより、管理、高可用性ハートビート、およびその他のタスクのために、接続されたままのポートを介してアプライアンスに到達できます。
- プライマリポートが有効になっている場合、アプライアンスは、プライマリポートが管理、高可用性ハートビート、およびその他のタスクに使用されていると（チェックせずに）想定します。一方のブリッジポートのリンクダウン状態は、キャリアが復元されるか、ユニットが再起動されるまで、もう一方のポートに永続的にミラーリングされます。これは、プライマリポートが GUI で有効になっていても、ネットワークに接続されていない場合でも当てはまります。したがって、使用していないときは、プライマリポートを無効（デフォルト）にする必要があります。

サイト全体を加速する

April 19, 2021

インラインモード、WAN 上のすべてのトラフィックを高速化 は、インラインモードの一般的な構成を示しています。どちらのサイトでも、アプライアンスは LAN と WAN の間に配置されるため、高速化できるすべての WAN トラフィ

ックが高速化されます。これはアクセラレーションを実装するための最も簡単な方法であり、実用的な場合に使用する必要があります。

すべてのリンクトラフィックがアプライアンスを通過しているため、均等化キューイングとフロー制御の利点により、リンクがオーバーランするのを防ぎます。

IP ネットワークでは、ボトルネックゲートウェイがリンク全体のキューイング動作を決定します。ボトルネックゲートウェイになることで、アプライアンスはリンクを制御し、インテリジェントに管理できます。これは、帯域幅制限をリンク速度よりわずかに低く設定することによって行われます。これが行われると、リンクのパフォーマンスが理想的であり、完全なリンク使用率でも遅延と損失が最小限に抑えられます。

部分的なサイトの加速

April 19, 2021

リモートバックアップサーバーなどの特定のシステムグループ用にアプライアンスの高速帯域幅を予約するには、それらのシステムのみを含むブランチネットワークにアプライアンスをインストールします。これを次の図に示します。

図 1：インラインモード、選択したシステムのみを高速化

SD-WAN トラフィックシェーピングはリンク全体の制御に依存しているため、アプライアンスはリンクトラフィックの一部しか認識しないため、このトポロジではトラフィックシェーピングは効果的ではありません。レイテンシー制御はボトルネックゲートウェイ次第であり、インタラクティブな応答性が損なわれる可能性があります。

WCCP モード

April 19, 2021

Web キャッシュ通信プロトコル（WCCP）は、Cisco によって導入されたダイナミックルーティングプロトコルです。WCCP バージョン 2 は、もともと Web キャッシングのみを目的としていましたが、より汎用的なプロトコルになり、Citrix SD-WAN アプライアンスなどのアクセラレータでの使用に適しています。

WCCP モードは、インライン操作が実用的でない場合に SD-WAN アプライアンスをインストールする最も簡単な方法です。また、非対称ルーティングが発生する場合、つまり、同じ接続からのパケットが異なる WAN リンクを介して到着する場合にも役立ちます。WCCP モードでは、ルータは WCCP 2.0 プロトコルを使用して、アプライアンスを介してトラフィックを迂回させます。アプライアンスによって受信されると、トラフィックは、インラインモードで受信されたかのように、アクセラレーションエンジンとトラフィックシェーパーによって処理されます。

> 注
>
> - この説明では、WCCP バージョン 1 は廃止されたと見なされ、WCCP バージョン 2 のみが示されています。
> - 標準の WCCP ドキュメントでは、WCCP クライアントを「キャッシュ」と呼んでいます。実際のキャッシュとの混同を避けるために、Citrix は通常、WCCP クライアントを「キャッシュ」と呼ぶことを避けています。代わりに、WCCP クライアントは通常「アプライアンス」と呼ばれます。
> - この説明では、「ルーター」という用語を使用して、WCCP 対応ルーターおよび WCCP 対応スイッチを示します。ここでは「ルーター」という用語が使用されていますが、一部のハイエンドスイッチは WCCP もサポートしており、SD-WAN アプライアンスで使用できます。
>
> SD-WAN アプライアンスは 2 つの WCCP モードをサポートします：
>
> - WCCP は、リリース 3.x 以降でサポートされている元の SD-WAN WCCP オファリングです。単一のアプライアンスサービスグループをサポートします（クラスタリングなし）。
> - リリース 7.2 で導入された WCCP クラスタリングにより、ルータは複数のアプライアンス間でトラフィックの負荷を分散できます。

WCCP モードのしくみ

SD-WAN アプライアンスの WCCP 展開の物理モードは、アプライアンスが WAN ルーターの専用ポートに直接接続されるワンアームモードです。WCCP 標準には、アプライアンスがルーターに自身を登録するプロトコルネゴシエーションが含まれており、2 つは共通にサポートする機能の使用をネゴシエートします。このネゴシエーションが成功すると、トラフィックは WCCP ルータとルータで定義されたリダイレクションルールに従ってルータとアプライアンスの間でルーティングされます。

WCCP モードのアプライアンスには、イーサネットポートが 1 つだけ必要です。アプライアンスは、専用ルーターポート（または WCCP 対応スイッチポート）に展開するか、VLAN を介して他のトラフィックから分離する必要があります。インラインモードと WCCP モードを混在させないでください。

次の図は、選択したインターフェイス上のトラフィックを傍受し、それを WCCP 対応アプライアンスに転送するようにルータを設定する方法を示しています。WCCP 対応アプライアンスが使用できない場合は常に、トラフィックは傍受されず、通常どおり転送されます。

図 1：WCCP トラフィックフロー

トラフィックのカプセル化

WCCP を使用すると、次のいずれかのモードでルータとアプライアンス間でトラフィックを転送できます。

- L2 モード：ルータとアプライアンスが同じ L2 セグメント（通常はイーサネットセグメント）上にある必要があります。IP パケットは変更されず、パケットを転送するために L2 アドレス指定のみが変更されます。多く

のデバイスでは、L2 転送はハードウェア層で実行され、最大のパフォーマンスを提供します。パフォーマンス上の利点があるため、L2 転送が推奨されるモードですが、すべての WCCP 対応デバイスが L2 転送をサポートしているわけではありません。

- GRE モード-GenericRouting Encapsulation（GRE）はルーティングされたプロトコルであり、アプライアンスは理論的にはどこにでも配置できますが、パフォーマンスを向上させるには、ルーターの近く、できるだけ少ないスイッチとルーターを通過する高速で混雑していないパスに配置する必要があります。。GRE は元の WCCP モードです。GRE ヘッダーが作成され、データパケットが追加されます。受信デバイスは GRE ヘッダーを削除します。カプセル化を使用すると、アプライアンスは、ルーターに直接接続されていないサブネット上に配置できます。ただし、カプセル化プロセスとそれに続くルーティングの両方で、ルーターに CPU オーバーヘッドが追加され、28 バイトの GRE ヘッダーを追加すると、パケットの断片化が発生し、オーバーヘッドが追加される可能性があります。

WCCP モードは、複数のルーターと GRE との両方をサポートします。L2 転送。各ルーターは複数の WAN リンクを持つことができます。各リンクは、独自の WCCP サービスグループを持つことができます。

アプライアンスが TCP トラフィックだけでなく UDP トラフィックも管理しない限り、トラフィックシェーピングは効果的ではありません。トラフィックシェーピングが必要な場合は、WAN リンクごとに UDP サービスグループを持つ 2 番目のサービスグループをお勧めします。

登録とステータスの更新

WCCP クライアント（アプライアンス）は、UDP ポート 2048 を使用して、ルーターに自身を登録し、ルーターに送信する必要のあるトラフィックと、このトラフィックに使用する必要のある WCCP 機能をネゴシエートします。アプライアンスはこのトラフィックで動作し、結果のトラフィックを元のエンドポイントに転送します。アプライアンスのステータスは、WCCP 登録プロセスとハートビートプロトコルを通じて追跡されます。アプライアンスは最初に WCCP 制御チャネル（UDP ポート 2048）を介してルーターに接続し、アプライアンスとルーターは次の名前のパケットと情報を交換します。それぞれ “Here_I_Am” そして “I_See_You”。デフォルトでは、このプロセスは 10 秒ごとに繰り返されます。ルーターがこれらの間隔の 3 つでアプライアンスからのメッセージの受信に失敗した場合、ルーターはアプライアンスに障害が発生したと見なし、接続が再確立されるまでトラフィックの転送を停止します。

サービスとサービスグループ

同じルーターを使用する異なるアプライアンスは、異なるサービスを提供できます。どのサービスがどのアプライアンスに割り当てられているかを追跡するために、WCCP プロトコルはサービスグループ識別子（1 バイト整数）を使用します。アプライアンスがそれ自体をルーターに登録すると、サービスグループ番号も含まれます。

- 1 つのアプライアンスで複数のサービスグループをサポートできます。
- 1 つのルーターで複数のサービスグループをサポートできます。
- 1 つのアプライアンスで、複数のルーターで同じサービスグループを使用できます。

- 1 つのルーターで、複数のアプライアンスで同じサービスグループを使用できます。SD-WAN アプライアンスの場合、WCCP クラスターモードでは複数のアプライアンスがサポートされ、WCCP モードでは単一のアプライアンスがサポートされます。
- 各アプライアンスは、各方向および各サービスグループに対して個別に「戻り値の型」（L2 または GRE）を指定します。SD-WAN 4000/5000 アプライアンスは、常に両方向に同じ戻り値の型を指定します。他の SD-WAN アプライアンスでは、戻り値の型を変えることができます。

図 2：さまざまなサービスにさまざまな WCCP サービスグループを使用する

同じアプライアンス上の WCCP で複数のサービスグループ を使用できます。たとえば、アプライアンスは、ある WAN リンクからサービスグループ 51 のトラフィックを受信し、別の WAN リンクからサービスグループ 62 のトラフィックを受信できます。アプライアンスは複数のルーターもサポートしています。すべてのルーターが同じサービスグループを使用するか、異なるルーターが異なるサービスグループを使用するかは関係ありません。

サービスグループの追跡。パケットが 1 つのサービスグループに到着した場合、同じ接続の出力パケットは同じサービスグループに送信されます。パケットが複数のサービスグループの同じ接続に到着した場合、出力パケットはその接続で最後に確認されたサービスグループを追跡します。

高可用性の動作

WCCP を高可用性モードで使用する場合、プライマリアプライアンスはルータに接続するときに、高可用性ペアの仮想アドレスではなく、独自の APA または APB 管理 IP アドレスを送信します。フェールオーバーが発生すると、新しいプライマリアプライアンスが自動的にルータに接続し、WCCP チャネルを再確立します。ほとんどの場合、WCCP タイムアウト時間および高可用性フェールオーバー時間が重複しています。その結果、ネットワークの停止は 2 つの遅延の合計よりも少なくなります。

標準の WCCP では、WCCP サービスグループ内のアプライアンスは 1 つだけです。新しいアプライアンスがルーターに接続しようとすると、他のアプライアンスがサービスグループを処理していることを検出し、新しいアプライアンスがアラートを設定します。サービスグループが他のアプライアンスでまだアクティブであるかどうかを定期的にチェックし、他のアプライアンスが非アクティブになると、新しいアプライアンスがサービスグループを処理します。WCCP クラスタリングでは、サービスグループごとに複数のアプライアンスを使用できます。

展開トポロジ表示

次の図は、L2 または GRE のいずれかに適した単純な WCCP 展開を示しています。トラフィックポート (1/1) 専用ルーターポートに直接接続されています（ギグ 4/12)。

図 3：単純な WCCP 展開

この例では、SD-WAN 4000/5000 トラフィックポートを使用して、ワンアームモードで展開されます (1/1) および管理ポート (0/1) それぞれが専用のルーターポートに接続します。

ルータでは、WCCP は、WAN ポートと LAN ポートのステートメントで同一の ipwccp リダイレクトを使用して設定されています。71 と 72 の 2 つのサービスグループが使用されます。サービスグループ 71 は TCP トラフィック

に使用され、サービスグループ 72 は UDP トラフィックに使用されます。アプライアンスは UDP トラフィックを加速しませんが、トラフィックシェーピングポリシーを適用できます。

> 注意: WCCP 仕様では、TCP と UDP 以外のプロトコルの転送は許可されていないため、ICMP や GRE などのプロトコルは常にアプライアンスをバイパスします。

WCCP クラスタリング

SD-WAN アプライアンスは WCCP クラスタリングをサポートします。これにより、ルーターは複数のアプライアンス間でトラフィックの負荷を分散できます。SD-WAN アプライアンスをクラスタとして展開する方法の詳細については、WCCP クラスタリングを参照してください。

WCCP 仕様

WCCP の詳細については、Web キャッシュ通信プロトコル V2、リビジョン 1、http://tools.ietf.org/html/draft-mclaggan-wccp-v2rev1-00を参照してください。

> 注
>
> スイッチの冗長性のために SD-WAN を WCCP に展開する場合、スイッチ 2 を apB に接続できます。apB 用に別の SG を作成し、apA 用の SG よりも優先度を低くします。apA の高い SG がアップしている場合、それはリダイレクトに使用されます。それがダウンしている場合は、apBSG が使用されます。apA と apB は異なるサブネット上にある必要があることに注意してください。

WCCP モード（非クラスター化）

April 19, 2021

WCCP モードでは、WCCP サービスグループ内の単一のアプライアンスのみが許可されます。新しいアプライアンスがルーターに接続しようとすると、他のアプライアンスがサービスグループを処理していることを検出し、新しいアプライアンスがアラートを設定します。サービスグループが他のアプライアンスでまだアクティブであるかどうかを定期的にチェックし、他のアプライアンスが非アクティブになると、新しいアプライアンスがサービスグループを処理します。

> 注:
> WCCP クラスタリングでは、サービスグループごとに複数のアプライアンスを使用できます。

制限とベストプラクティス

以下は、（クラスター化されていない）WCCP モードの制限とベストプラクティスです。

- 複数のアクセラレーションペアを備えたアプライアンスでは、特定の WCCP サービスグループのすべてのトラフィックが同じアクセラレーションペアに到着する必要があります。
- 同じアプライアンスでインライントラフィックと WCCP トラフィックを混在させないでください。アプライアンスはこのガイドラインを強制しませんが、違反すると加速が困難になる可能性があります。（WCCP モードと仮想インラインモードを混在させることができますが、WCCP と仮想インライントラフィックが異なるルーターから送信されている場合に限ります。）
- WAN ルーターが 1 つしかないサイトでは、インラインモードが実用的でない場合は常に WCCP を使用してください。
- サービスグループごとにサポートされるアプライアンスは 1 つだけです。複数のアプライアンスが同じサービスグループの同じルーターに接続しようとすると、ネゴシエーションは最初のアプライアンスに対してのみ成功します。
- 同じアプライアンスでサービスを提供する複数の WAN ルーターがあるサイトの場合、WCCP を使用して、WAN ルーターの 1 つ、一部、またはすべてをサポートできます。他のルーターは仮想インラインモードを使用できます。

WCCP のルーターサポート

WCCP 用のルータの設定は非常に簡単です。WCCP バージョン 2 のサポートは、リリース 12.0（11）S および 12.1（3）T で Cisco IOS に追加された、すべての最新のルータに含まれています。最適なルーター構成戦略は、ルーターとスイッチの特性によって決まります。トラフィックシェーピングには、2 つのサービスグループが必要です。

ルータがリバースパスフォワーディングをサポートしている場合は、WCCP トラフィックとスプーフィングトラフィックが混同される可能性があるため、すべてのポートで無効にする必要があります。この機能は、Cisco 7600 などの新しい Cisco ルータにあります。

ルーター構成戦略

ルーターからアプライアンスにトラフィックをリダイレクトするには、2 つの基本的なアプローチがあります。

WAN ポートでのみ、「WCCP リダイレクトイン」ステートメントと「WCCP リダイレクトアウト」ステートメントを追加します。
アプライアンスに接続されているポートを除く、ルーターのすべてのポートに、「WCCP リダイレクトイン」ステートメントを追加します。

最初の方法は、WAN トラフィックのみをアプライアンスにリダイレクトし、2 番目の方法は、WAN に関連しているかどうかに関係なく、すべてのルートラフィックをアプライアンスにリダイレクトします。複数の LAN ポートと大量の LAN-to-LAN トラフィックがあるルーターでは、すべてのトラフィックをアプライアンスに送信すると、LAN セグメントが過負荷になり、アプライアンスにこの不要な負荷がかかる可能性があります。GRE が使用されている場合、不要なトラフィックがルータに負荷をかける可能性もあります。

一部のルーターでは、「リダイレクトイン」パスの方が「リダイレクトアウト」パスよりも高速で、ルーターの CPU にかかる負荷が少なくなります。必要に応じて、ルーターで直接実験することでこれを判断できます。ネットワーク

全体の負荷の下で両方のリダイレクト方法を試して、どちらが最高の転送速度を提供するかを確認します。

一部のルーターおよび WCCP 対応スイッチは、「WCCP リダイレクトアウト」をサポートしていないため、2 番目の方法を使用する必要があります。ルーターの過負荷を回避するには、アプライアンスを介して多数のルーターポートをリダイレクトしないようにするためのベストプラクティスです。おそらく、WAN ルーティング用と LAN-to-LAN ルーティング用の 2 つのルーターを使用します。

一般に、方法 1 の方が単純ですが、方法 2 の方がパフォーマンスが向上する場合があります。

トラフィックシェーピングと **WCCP**

サービスグループは TCP または UDP のいずれかですが、両方にすることはできません。トラフィックシェーパーを有効にするには、両方の種類の WAN トラフィックがアプライアンスを通過する必要があります。したがって、次のようになります。

アクセラレーションには、TCP トラフィック用に 1 つのサービスグループが必要です。
トラフィックシェーピングには、TCP トラフィック用と UDP トラフィック用の 2 つのサービスグループが必要です。2 つの違いはアプライアンスで構成され、ルーターはこの構成を受け入れます。

ルーターを構成する

アプライアンスは、WCCP-GRE または WCCP-L2 を自動的にネゴシエートします。主な選択肢は、ユニキャスト操作（アプライアンスが各ルーターの IP アドレスで構成されている）または マルチキャスト操作（アプライアンスとルーターの両方がマルチキャストアドレスで構成されている）のいずれかです。

標準（ユニキャスト）動作: 通常の動作では、ルータ全体の WCCP バージョン 2 と WCCP グループ ID を宣言し、各 WAN インターフェイスでリダイレクションを有効にします。次に、Cisco IOS の例を示します。

```
config term
ip wccp version 2
! We will configure the appliance to use group 51 for TCP and 52 for
   UDP.
ip wccp 51
ip wccp 52

! Repeat the following three lines for each WAN interface
! you wish to accelerate:
interface your_wan_interface
! If Reverse Path Forwarding is enabled (with an ip verify unicast
! source reachable”  statement), delete or comment out the statement:
! ip verify unicast source reachable-via any
! Repeat on all ports.

ip wccp 51 redirect out
ip wccp 51 redirect in
ip wccp 52 redirect out
ip wccp 52 redirect in
```



```
19
20 ! If the appliance is inline with one of the router interfaces
21 ! (NOT SUPPORTED), add the following line for that interface
22 ! to prevent loops:
23 ip wccp redirect exclude in
24 ^Z
```

複数のルーターが同じアプライアンスを使用する場合、それぞれが上記のように構成され、同じサービスグループまたは異なるサービスグループを使用します。

マルチキャスト操作：アプライアンスと各ルーターにマルチキャストアドレスを与える場合、構成は通常の操作とは少し異なります。次に、Cisco IOS の例を示します。

```
1  config term
2  ip wccp version 2
3  ip wccp 51 group-address 225.0.0.1
4
5  ! Repeat the following three lines for each WAN interface
6  ! you wish to accelerate:
7  interface your_wan_interface
8  ! If Reverse Path Forwarding is enabled (with an ip verify unicast
9  ! source reachable”  statement), delete or comment out the statement:
10 ! ip verify unicast source reachable-via any
11
12 ip wccp 51 redirect out
13 ip wccp 51 redirect in
14 !
15 ! The following line is needed only on the interface facing the other
      router,
16 ! if there is another router participating in this service group.
17 ip wccp 51 group-listen
18
19 !If the appliance is inline with one of the router interfaces,
20 !(which is supported but not recommended), add
21 !the following line for that interface to prevent loops:
22 ip wccp redirect exclude in
23 ^Z
```

SD-WAN アプライアンスでの WCCP モードの基本的な構成手順

ほとんどのサイトでは、次の手順を使用して、アプライアンスで WCCP モードを構成できます。この手順では、いくつかのパラメーターを適切なデフォルト値に設定します。高度な展開では、これらのパラメーターを他の値に設定する必要がある場合があります。たとえば、WCCP サービスグループ 51 がすでにルータで使用されている場合は、アプライアンスに別の値を使用する必要があります。

アプライアンスで WCCP モードを構成するには：

1. [構成：アプライアンス設定：WCCP] ページ。

2. サービスグループが定義されていない場合は、[モードの選択] ページが表示されます。オプションは、単一の SD-WAN とクラスター（複数の SD-WAN）です。[シングル SD-WAN] を選択します。WCCP ページに移動します。
   注：モードラベルは誤解を招く恐れがあります。「シングル SD-WAN」モードは、SD-WAN 高可用性ペアにも使用されます。
3. WCCP モードが有効でない場合は、[En **able**] をクリックします。
4. [サービスグループの追加] をクリックします。
5. デフォルトのインターフェイス（apA）、プロトコル（TCP）、WCCP 優先度（0）、ルーター通信（ユニキャスト）、（パスワードブランク）、および存続可能時間（1）の値は、通常、最初のサービスグループで変更する必要はありません。作成しますが、作成する場合は、表示されたフィールドに新しい値を入力します。
6. [ルーターアドレス指定] フィールド（ユニキャストを使用している場合）または [マルチキャストアドレス] フィールド（マルチキャストを使用している場合）に、ルーターの IP アドレスを入力します。アプライアンスとの WCCP 通信に使用されるルーターポートの IP を使用します。
7. 複数のルーターが WCCP を使用してこのアプライアンスと通信している場合は、ここでルーターを追加します。
8. ルーターに特別な要件がある場合は、ルーター転送を設定します (Auto/GRE/Level-2), ルーターパケットリターン (Auto/GRE/Level-2), およびルーターの割り当て (Mask/Hash) それに応じてフィールド。デフォルトでは、ほとんどのルーターで最適な結果が得られます。
9. ［追加］をクリックします。
10. 上記の手順を繰り返して、UDP トラフィック用に別のサービスグループを作成します（たとえば、サービスグループ ID 52 とプロトコル UDP）。
11. [監視：アプライアンスのパフォーマンス：WCCP] ページに移動します。[ステータス] フィールドは 60 秒以内に [接続済み] に変わります。
12. リンクを介してトラフィックを送信し、[接続] ページで、接続が到着して加速されていることを確認します。

WCCP サービスグループ構成の詳細

サービスグループでは、WCCP ルーターと SD-WAN アプライアンス（WCCP 用語では「WCCP キャッシュ」）が通信属性（機能）をネゴシエートします。ルータは、「ISeeYou」メッセージでその機能をアドバタイズします。通信属性は次のとおりです。

- 転送方法：GRE またはレベル 2
- パケットリターン方式（マルチキャストのみ）：GRE またはレベル 2
- 割り当て方法：ハッシュまたはマスク
- パスワード（デフォルトは none）

アプライアンスは、その属性とルーターの属性の間に非互換性を検出すると、アラートをトリガーします。サービスグループの特定の属性（GRE やレベル 2 など）が原因で、アプライアンスに互換性がない可能性があります。ごくまれに、マルチキャストサービスグループでは、「自動」選択が特定のルーターが接続されている特定の属性を選択したときにアラートがトリガーされることがありますが、その属性は後続のルーターと互換性がありません。

以下は、SD-WAN アプライアンス内の通信属性の基本的なルールです。

ルーター転送の場合:

- 「自動」が選択されている場合、ルーターとアプライアンスの両方でより効率的であるため、レベル 2 が優先されます。レベル 2 は、ルーターがそれをサポートし、ルーターがアプライアンスと同じサブネット上にある場合にネゴシエートされます。
- 「自動」が選択されている場合、ユニキャストサービスグループ内のルーターはさまざまな方法をネゴシエートできます。
- マルチキャストサービスグループ内のルーターは、「GRE」または「レベル 2」で強制されるか、「自動」で強制されるかにかかわらず、接続するサービスグループ内の最初のルーターによって決定されるすべての同じ方法を使用する必要があります。
- 互換性がない場合、アラートはルーターに「互換性のないルーター転送がある」ことを通知します。

ルーター割り当ての場合:

- デフォルトはハッシュです。
- 「自動」を選択すると、モードはルーターとネゴシエートされます。
- サービスグループ内のすべてのルーターは、同じ割り当て方法（ハッシュまたはマスク）をサポートする必要があります。
- どのサービスグループでも、この属性が「自動」として構成されている場合、アプライアンスは最初のルーターが接続されたときに「ハッシュ」または「マスク」を選択します。「ハッシュ」は、ルーターがサポートしている場合に選択されます。それ以外の場合は、「マスク」が選択されます。後続のルーターが自動的に選択された方法と互換性がないという問題は、サービスグループ内のすべてのルーターに共通の方法を手動で選択することで最小限に抑えることができます。
- 互換性がない場合、アラートはルーターに「互換性のないルーター割り当て方法がある」ことを通知します。
- どちらの方法でも、サービスグループ内の単一のアプライアンスは、サービスグループ内のすべてのルーターにすべての TCP または UDP パケットをアプライアンスに送信するように指示します。ルーターは、アクセスリストを使用するか、サービスグループにリダイレクトするインターフェイスを選択することにより、この動作を変更できます。

  マスク方式の場合、アプライアンスは「送信元 IP アドレス」マスクをネゴシエートします。アプライアンスには、送信元または宛先のいずれかの「宛先 IP アドレス」またはポートを選択するメカニズムはありません。「送信元 IP アドレス」マスクは、特定の IP アドレスまたは範囲を具体的に識別しません。このプロトコルは、特定の IP アドレスを指定する手段を提供していません。デフォルトでは、サービスグループにはアプライアンスが 1 つしかないため、ルーターのリソースを節約するために 1 ビットのマスクが使用されます。（リリース 6.0 はより大きなマスクを使用しました。）

パスワードの場合:

- ルータにパスワードが必要な場合は、アプライアンスで定義されているパスワードが一致している必要があり

ます。ルータがパスワードを必要としない場合、アプライアンスのパスワードフィールドは空白である必要があります。

WCCP のテストとトラブルシューティング

WCCP を使用する場合、アプライアンスは WCCP インターフェイスのステータスを監視するさまざまな方法を提供し、ルータも情報を提供する必要があります。

監視：アプライアンスのパフォーマンス：**WCCP** ページ-WCCP ページは、WCCP リンクの現在の状態を報告し、ほとんどの問題を報告します。

ログエントリ-[監視：アプライアンスのパフォーマンス：ログ] ページには、WCCP モードが確立または失われるたびに新しいエントリが表示されます。

図 1：WCCP ログエントリ（形式はリリースによって多少異なります）

ルータステータス：ルータで、「showipwccp」コマンドは WCCP リンクのステータスを表示します。

```
Router>enable
Password:
Router#show ip wccp
Global WCCP information:
    Router information:
        Router Identifier:                   172.16.2.4
        Protocol Version:                    2.0

    Service Identifier: 51
        Number of Cache Engines:             0
        Number of routers:                   0
        Total Packets Redirected:            19951
        Redirect access-list:                -none-
        Total Packets Denied Redirect:       0
        Total Packets Unassigned:            0
        Group access-list:                   -none-
        Total Messages Denied to Group:      0
        Total Authentication failures:       0
```

WCCP モードを確認する

SD-WAN GUI から WCCP 設定を監視できます。

WCCP 設定を監視するには

1. モニタリング **>** アプライアンスのパフォーマンス **> WCCP** ページに移動します。
2. キャッシュを選択し、[情報を見る] をクリックします。次の図に示すように、[キャッシュステータス] ページに WCCP 構成が表示されます。

3. SD-WAN アプライアンスを介して転送する必要のあるトラフィックを開始し、監視 **>** 最適化 **>** 接続ページで接続を監視します。

   - [加速接続] タブに接続が表示されている場合は、すべてが機能していることを示しています。
   - 接続が [加速さ れていない接続] タブにある場合は、[詳細] 列を確認してください。ルーティングの非対称性が検出されたメッセージは、ルータの ip wccp リダイレクト回線の 1 つが欠落しているかエラーがあるか、クライアントサーバートラフィックとサーバークライアントトラフィックによって異なるパスが使用されていることを示します。
   - 接続が表示されていないが、アプライアンスがルーターに接続されていることを報告し、WCCP 監視ページにエラーが表示されない場合は、ルーターの構成に問題がある可能性があります。

WCCP クラスタリング

December 16, 2022

WCCP クラスタリング機能を使用すると、同じリンクに複数の SD-WAN アプライアンスを割り当てることで、アクセラレーション容量を増やすことができます。最大 32 倍の容量で、最大 32 個の同一のアプライアンスをクラスター化できます。WCCP 2.0 標準を使用しているため、WCCP クラスタリングは、ほとんどのルーターと一部のスマートスイッチで機能します。ほとんどの場合、既に使用しているものも含まれます。

分散型プロトコルを使用しているため、WCCP クラスタリングでは SD-WAN アプライアンスを自由に追加または削除できます。アプライアンスに障害が発生した場合、そのトラフィックは存続しているアプライアンスに再ルーティングされます。

SD-WAN 高可用性とは異なり、2 つのアプライアンスを使用して 1 つのアプライアンスのパフォーマンスを提供するアクティブ/パッシブペアです。WCCP クラスタとしてデプロイされた同じアプライアンスは、1 つのアプライアンスの 2 倍のパフォーマンスを発揮し、冗長性とパフォーマンスの向上を実現します。

サイトのニーズの増加に応じてアプライアンスを追加するだけでなく、Citrix の「Payas You Grow」機能を使用して、ライセンスのアップグレードを通じてアプライアンスの機能を向上させることができます。

WCCP クラスターの管理には Citrix Command Center をお勧めします。次の図は、Citrix Command Center を使用して管理される WCCP モードの SD-WAN アプライアンスのクラスターの基本的なネットワークを示しています。

図 1: Citrix Command Center を使用して管理される SD-WAN クラスター

負荷分散された **WCCP** クラスター

WCCP プロトコルは、クラスターと呼ばれるフォールトトレラントで負荷分散されたアレイで最大 32 台のアプライアンスをサポートします。以下の例では、3 つの同一のアプライアンス（同じモデル、同じソフトウェアバージョン）が同じようにケーブル接続され、IP アドレスを除いて同じように構成されています。同じルータで同じサービスグル

ープを使用するアプライアンスは、負荷分散された WCCP クラスタになることができます。新しいアプライアンスがルーターに登録されると、アプライアンスの既存のプールに参加して、トラフィックのシェアを受け取ることができます。アプライアンスがネットワークを離れると（ハートビート信号がないことで示されます）、クラスターは再調整され、残りのアプライアンスのみが使用されます。

図 2: 3 つのアプライアンスを備えた負荷分散された WCCP クラスター

クラスタ内の 1 つのアプライアンスが指定されたキャッシュとして選択され、クラスタ内のアプライアンスの負荷分散動作を制御します。指定されたキャッシュは、IP アドレスが最も小さいアプライアンスです。アプライアンスの構成は同じであるため、どちらが指定されたキャッシュであるかは関係ありません。現在の指定キャッシュがオフラインになると、別のアプライアンスが指定キャッシュになります。

指定されたキャッシュは、負荷分散されたトラフィックの割り当て方法を決定し、これらの決定をルーターに通知します。ルーターはクラスターのすべてのメンバーと情報を共有するため、指定されたキャッシュがオフラインになってもクラスターは動作できます。

> 注意: 通常の構成では、SD-WAN 4000/5000 アプライアンスは、ルータからは 2 つの WCCP キャッシュとして表示されます。

負荷分散アルゴリズム

WCCP の負荷分散は静的です。ただし、アプライアンスがクラスタに出入りする場合を除きます。これにより、クラスタは現在のメンバー間で再分散されます。

WCCP 標準は、マスクまたはハッシュに基づく負荷分散をサポートします。たとえば、SD-WAN WCCP クラスタリングは、32 ビット IP アドレスの 1～6 ビットのマスクを使用して、マスク方式のみを使用します。これらのアドレスビットは連続していない可能性があります。マスクされたときに同じ結果をもたらすすべてのアドレスは、同じアプライアンスに送信されます。負荷分散の効果は、適切なマスク値の選択に依存します。マスクの選択が不十分な場合、すべてのトラフィックが単一のアプライアンスに送信され、負荷分散が不十分になるか、まったく発生しない可能性があります。

展開トポロジ表示

ネットワークトポロジに応じて、WCCP クラスタを単一のルータまたは複数のルータのいずれかで展開できます。単一のルーターに接続する場合でも、複数のルーターに接続する場合でも、クラスター内の各アプライアンスは、使用中のすべてのルーターに同じように接続する必要があります。

単一ルーターの展開

次の図では、3 つの SD-WAN アプライアンスがデータセンターの 200 MbpsWAN を高速化します。このサイトは 750 の仮想アプリユーザーをサポートしています。

SD-WAN データシートに示すように、SD-WAN 3000-100 は 100 Mbps および 400 ユーザをサポートできます。したがって、これらのアプライアンスのペアは 200 Mbps および 800 ユーザをサポートします。これは、200 Mbps リンクおよび 750 というデータセンターの要件を満たします。ユーザー。

ただし、フォールトトレランスのために、1 つのアプライアンスに障害が発生しても、WCCP クラスターは過負荷になることなく動作し続ける必要があります。これは、計算で 2 つ必要な場合に、3 つのアプライアンスを使用することで実現できます。これは、N+1 ルール。

障害は異常なイベントであるため、通常、3 つのアプライアンスすべてが動作しています。この場合、各アプライアンスは 67 Mbps と 250 ユーザーのみをサポートし、十分なヘッドルームを残し、クラスターの CPU パワーが 1 つのアプライアンスの 3 倍、圧縮履歴が 3 倍であるという事実をうまく利用しています。

WCCP クラスタリングを使用しない場合、多くの容量とフォールトトレランスを実現するには、高可用性モードで SD-WAN 4000-500 アプライアンスのペアが必要になります。これらのアプライアンスの 1 つだけが一度にアクティブになります。

複数のルーターの展開

複数の WAN ルーターを使用することは、単一の WAN ルーターを使用することに似ています。前の例を変更して、1 つの 200Mbps リンクではなく 2 つの 100Mbps リンクを含めると、トポロジは変更されますが、計算は変更されません。

制限事項

WCCP クラスターでのアプライアンスの構成には、次の制限があります。

- クラスタ内のすべてのアプライアンスは同じモデルであり、同じソフトウェアリリースを使用する必要があります。
- クラスター内のアプライアンス間のパラメーター同期は自動ではありません。Command Center を使用して、アプライアンスをグループとして管理します。
- SD-WAN トラフィックシェーピングは、リンク全体を 1 つの単位として制御することに依存しており、どのアプライアンスもこれを実行できる位置にないため、効果的ではありません。代わりにルーター QoS を使用できます。
- WCCP ベースの負荷分散アルゴリズムは負荷によって動的に変化しないため、良好な負荷分散を実現するには、ある程度の調整が必要になる場合があります。
- キャッシュ割り当てのハッシュ方式はサポートされていません。マスク割り当てはサポートされている方法です。
- WCCP 標準では 1～7 ビットのマスク長が許可されていますが、アプライアンスは 1～6 ビットのマスクをサポートしています。
- マルチキャストサービスグループはサポートされていません。ユニキャストサービスグループのみがサポートされています。

- 同じサービスグループペアを使用するすべてのルーターは、同じ転送方法（GRE または L2）をサポートする必要があります。
- ルータとネゴシエートされた転送およびリターン方式は一致する必要があります。両方が GRE であるか、両方が L2 である必要があります。一部のルータは両方向で L2 をサポートしていないため、「ルータのフォワードまたはリターン、または割り当て機能が不一致というエラーになります。」この場合、サービスグループは GRE として設定する必要があります。
- SD-WAN VPX は、WCCP クラスタリングをサポートしていません。
- アプライアンスは、重み付けされていない（等しい）キャッシュ割り当てのみをサポート（およびネゴシエート）します。加重割り当てはサポートされていません。
- SD-WAN 700 などの一部の古いアプライアンスは、WCCP クラスタリングをサポートしていません。
- （SD-WAN 4000/5000 のみ）L2 モードでは、インターフェイスごとに 2 つのアクセラレータインスタンスが必要です。アプライアンスごとに 3 つのインターフェイスがサポートされます（その後、6 つ以上のアクセラレータインスタンスを備えたアプライアンスでのみサポートされます）。
- （SD-WAN 4000/5000 のみ）ルータからの WCCP 制御パケットは、サービスグループ用にアプライアンスで設定されたルータ IP アドレスの 1 つと一致する必要があります。実際には、ルーターをアプライアンスに接続するインターフェイスのルーターの IP アドレスを使用する必要があります。ルータのループバック IP は使用できません。

デプロイメントワークシートとクラスターの制限

次のワークシートで、インストールに必要なアプライアンスの数と推奨されるマスクフィールドサイズを計算できます。推奨されるマスクサイズは、インストールの最小マスクサイズよりも 1〜2 ビット大きくなります。

パラメーター	値	メモ
使用したアプライアンスモデル		いいえ
アプライアンスごとにサポートされる Citrix Virtual Apps and Desktops ユーザー	Uspec =	データシートから
WAN 上の Citrix Virtual Apps and Desktops ユーザーリンク	Uwan =	いいえ
ユーザー過負荷係数	Uoverload = Uwan/Uspec =	いいえ
アプライアンスごとにサポートされる BW	BWspec =	データシートから
WAN リンク BW	BWwan =	いいえ
BW 過負荷係数	BWoverload = BWwan/BWspec =	いいえ

必要なアプライアンスの数	N = max(Uoverload, BWoverload) +1 =	スペアが 1 つ含まれています いいえ
バケットの最小数	ロ短調 = N、2 の累乗を切り上げ =	いいえ
SD-WAN 4000 または 5000 の場合、	ロ短調 = 2N、2 の累乗に切り上げ =	いいえ
推奨値	B = 4 \Bmin Bmin の場合 < = 16、その他 2 \Bmin =	いいえ
アドレスマスクの「1」ビットの数	M = log2（B）	場合 B=16, M=4.

マスク値：マスク値は、前に提供されたワークシートの M に等しいいくつかの「1」ビットを持つ 32 ビットアドレスマスクです。多くの場合、これらのビットは、リモートサイトで使用される WAN サブネットマスクの最下位ビットである可能性があります。リモートサイトのマスクが異なる場合は、中央値マスクを使用してください。（例：あり /24 サブネットの場合、サブネットの最下位ビットは 0x00 00 nn00 です。1 に設定するビット数は log2（マスクサイズ）です。マスクサイズが 16 の場合、4 ビットを 1 に設定します。したがって、マスクサイズが 16 で、/24 サブネットの場合、マスク値を 0x00 00 0f 00 に設定します。）

上記のガイドラインは、選択したサブネットフィールドがトラフィックに均等に分散されている場合、つまり、マスクによって選択された各アドレスビットがリモートホストの半分に対して 1 であり、残りの半分に対して 0 である場合にのみ機能します。そうしないと、負荷分散が損なわれます。この均等な分布は、ネットワークフィールドの数ビット（2 ビットのみ）にのみ当てはまる可能性があります。ネットワークでそうであれば、サブネットフィールドの問題のある領域のビットをマスクする代わりに、それらのビットをホストアドレスフィールドの 50/50 プロパティ。たとえば、サブネットビットが 3 つしかない場合 /24 サブネットには 50/50 プロパティであり、4 つのマスクビットを使用している場合、0x00 00 07 10 のマスクは、0x00 00 0800 の問題のあるビットを回避し、それを 0x00 00 00 10 に置き換えます。これは、アドレスフィールドの一部である可能性があります。50/50 リモートサブネットが通常、それぞれ少なくとも 32 個の IP アドレスを使用する場合はプロパティ。

パラメーター	値	メモ
Final Mask Value		いいえ
Accelerated Bridge		通常 apA
WAN Service Group		ルーターでまだ使用されていないサービスグループ（51-255）
LAN Service Group		別の未使用のサービスグループ

Router IP address	アプライアンスに面しているポートのルーターインターフェイスの IP アドレス
WCCP Protocol（通常は「自動」）	いいえ
DC Algorithm	アプライアンスが 2 つしかない場合、または HSRP や GSLB などの動的負荷分散を使用している場合は、「決定論的」を使用します。それ以外の場合は、「最低破壊的」を使用します。

WCCP クラスターでのアプライアンスの構成には、次の制限があります。

- クラスタ内のすべてのアプライアンスは同じモデルであり、同じソフトウェアリリースを使用する必要があります。
- クラスター内のアプライアンス間のパラメーター同期は自動ではありません。Command Center を使用して、アプライアンスをグループとして管理します。
- SD-WAN トラフィックシェーピングは、リンク全体を 1 つの単位として制御することに依存しており、どのアプライアンスもこれを実行できる位置にないため、効果的ではありません。代わりにルーター QoS を使用できます。
- WCCP ベースの負荷分散アルゴリズムは負荷によって動的に変化しないため、良好な負荷分散を実現するには、ある程度の調整が必要になる場合があります。
- キャッシュ割り当てのハッシュ方式はサポートされていません。マスク割り当てはサポートされている方法です。
- WCCP 標準では 1～7 ビットのマスク長が許可されていますが、アプライアンスは 1～6 ビットのマスクをサポートしています。
- マルチキャストサービスグループはサポートされていません。ユニキャストサービスグループのみがサポートされています。
- 同じサービスグループペアを使用するすべてのルーターは、同じ転送方法（GRE または L2）をサポートする必要があります。
- ルータとネゴシエートされた転送およびリターン方式は一致する必要があります。両方が GRE であるか、両方が L2 である必要があります。一部のルータは両方向で L2 をサポートしていないため、「ルータのフォワードまたはリターン、または割り当て機能が不一致というエラーになります。」この場合、サービスグループは GRE として設定する必要があります。
- SD-WAN VPX は、WCCP クラスタリングをサポートしていません。
- アプライアンスは、重み付けされていない（等しい）キャッシュ割り当てのみをサポート（およびネゴシエート）します。加重割り当てはサポートされていません。
- SD-WAN 700 などの一部の古いアプライアンスは、WCCP クラスタリングをサポートしていません。

- （SD-WAN WANOP 4000/5000 のみ）L2 モードでは、インターフェイスごとに 2 つのアクセラレータインスタンスが必要です。アプライアンスごとにサポートされるインターフェイスは 3 つまでです（その後、6 つ以上のアクセラレータインスタンスを備えたアプライアンスでサポートされます）。
- （SD-WAN 4000/5000 のみ）ルータからの WCCP 制御パケットは、サービスグループ用にアプライアンスで設定されたルータ IP アドレスの 1 つと一致する必要があります。実際には、ルーターをアプライアンスに接続するインターフェイスのルーターの IP アドレスを使用する必要があります。ルータのループバック IP は使用できません。

テストとトラブルシューティング

モニタリング > アプライアンス > アプリケーションのパフォーマンス > **WCCP** ページには、ローカルアプライアンスだけでなく、クラスタに参加している他のすべてのアプライアンスの現在の状態が表示されます。WCCP キャッシュを選択し、[情報を見る] をクリックします。

[キャッシュステータス**]** タブに は、ローカルアプライアンスのステータスが表示されます。すべてが順調な場合、ステータスは「25：割り当てあり」です。ステータスの変化を監視するには、ページを手動で更新する必要があります。アプライアンスがタイムアウト期間内に「25：割り当てあり」のステータスに達しない場合、他の有益なステータスメッセージが表示されます。

[サービスグループ**]** または **[**ルーター**]** タブをクリックすると、追加情報が表示されます。

[クラスターの概要**]** タブに は、WCCP クラスター全体に関する情報が表示されます。WCCP プロトコルの副作用として、クラスターの各メンバーは他のすべての情報を持っているため、この情報はクラスター内の任意のアプライアンスから監視できます。

ルーターはステータス情報を提供することもできます。ルーターのドキュメントを参照してください。

WCCP クラスタリングを構成する

展開トポロジを完成させ、すべての制限を考慮し、展開ワークシートに記入したら、アプライアンスを WCCP クラスターに展開する準備が整います。WCCP クラスターを構成するには、次のタスクを実行する必要があります。

- NetScaler インスタンスの構成
- ルーターの構成
- アプライアンスの構成

仮想インラインモード

April 19, 2021

> 注:
>
> 仮想インラインモードは、インラインモードと WCCP モードの両方が実用的でない場合にのみ使用してください。同じアプライアンス内でインラインモードと仮想インラインモードを混在させないでください。ただし、同じアプライアンス内で仮想インラインモードと WCCP モードを混在させることができます。Citrix は、ヘルスモニタリングをサポートしていないルーターでの仮想インラインモードを推奨していません。

仮想インラインモードでは、ルータはポリシーベースルーティング（PBR）ルールを使用して、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て加速し、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。ほとんどすべての構成タスクはルーターで実行されます。アプライアンスで構成する必要があるのは転送方法だけであり、デフォルトの方法をお勧めします。

WCCP と同様に、仮想インライン展開では再配線やダウンタイムが不要であり、2 つ以上の WAN リンクを使用した展開で直面する非対称ルーティングの問題に対するソリューションを提供します。WCCP とは異なり、ステータスモニタリングやヘルスチェックが組み込まれていないため、トラブルシューティングが困難です。したがって、WCCP が推奨モードであり、仮想インラインは、インラインモードと WCCP モードの両方が実用的でない場合にのみ推奨されます。

例

次の図は、リモートサイト宛てまたはリモートサイトから受信したすべてのトラフィックがアプライアンスにリダイレクトされる単純なネットワークを示しています。この例では、ローカルサイトとリモートサイトの両方が仮想インラインモードを使用しています。

図 1：仮想インラインの例

この例のネットワークの構成の詳細は次のとおりです。

- エンドポイントシステムでは、ゲートウェイがローカルルーターに設定されています（これは仮想インラインモードに固有ではありません）。
- 各ルーターは、着信 WAN トラフィックと発信 WAN トラフィックの両方をローカルアプライアンスにリダイレクトするように構成されています。
- 各アプライアンスは、ローカルルーターから受信したトラフィックを処理し、ルーターに転送します。
- ルーターに構成された PBR ルールは、パケットがアプライアンスとの間で 1 回だけトリップできるようにすることで、ルーティングループを防止します。アプライアンスがルーターに転送するパケットは、元の（ローカルまたはリモートの）宛先に送信されます。
- 各アプライアンスでは、通常どおり、デフォルトゲートウェイがローカルルーターのアドレスに設定されています（[構成：ネットワークアダプター] ページ）。パケットをルーターに転送するためのオプションは、「イーサネット送信者に戻る」と「ゲートウェイに送信」です。

アプライアンスでのパケット転送の構成

April 19, 2021

仮想インラインモードには、2 つのパケット転送オプションがあります。

イーサネット送信側に戻る（デフォルト）：このモードでは、複数のルータがアプライアンスを共有できます。アプライアンスは、着信パケットのイーサネットアドレスで示されるように、仮想インライン出力パケットを元の場所に転送します。2 つのルーターが 1 つのアプライアンスを共有している場合、それぞれが独自のトラフィックを取得しますが、他のルーターからのトラフィックは取得しません。このモードは、単一のルーターでも機能します。

ゲートウェイに送信（非推奨）：このモードでは、仮想インライン出力パケットは、ローカルサブネット上のホスト宛てであっても、デフォルトゲートウェイに転送されて配信されます。このオプションは、ルーティング構造に複雑さの忘れがちな要素を追加するため、通常、[イーサネット送信者に戻る] オプションよりも望ましくありません。

パケット転送オプションを指定するには—**[**構成：最適化ルール：チューニング] ページの [仮想インライン] の横で、[イーサネット送信者に戻る] または [ゲートウェイに送信] を選択します。

ルーター構成

April 19, 2021

仮想インラインモードをサポートする場合、ルータには 3 つのタスクがあります。

1. 着信 WAN トラフィックと発信 WAN トラフィックの両方を SD-WAN アプライアンスに転送する必要があります。
2. SD-WAN トラフィックを宛先（WAN または LAN）に転送する必要があります。
3. アプライアンスに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、アプライアンスの状態を監視する必要があります。

ポリシーベースのルール

仮想インラインモードでは、ルーティングルールがアプライアンスによって転送されたパケットと転送されていないパケットを区別しない場合、パケット転送メソッドはルーティングループを作成できます。その区別をする任意の方法を使用できます。

一般的な方法では、ルーターのイーサネットポートの 1 つをアプライアンス専用にし、パケットが到着するイーサネットポートに基づいたルーティングルールを作成します。アプライアンス専用のインターフェイスに到着したパケットがアプライアンスに転送されることはありませんが、他のインターフェイスに到着したパケットは転送される可能性があります。

基本的なルーティングアルゴリズムは次のとおりです。

- アプライアンスからアプライアンスにパケットを転送しないでください。
- パケットが WAN から到着した場合は、アプライアンスに転送します。
- パケットが WAN 宛ての場合は、アプライアンスに転送します。
- LAN-to-LAN トラフィックをアプライアンスに転送しないでください。
- すべての WAN トラフィックがアプライアンスを通過しない限り、トラフィックシェーピングは効果的ではありません。

> 注意: ルーティングオプションを検討するときは、送信データだけでなく、返されるデータもアプライアンスを通過する必要があることに注意してください。たとえば、アプライアンスをローカルサブネットに配置し、それをローカルシステムのデフォルトルーターとして指定することは、仮想インライン展開では機能しません。送信データはアプライアンスを通過しますが、受信データはそれをバイパスします。ルーターを再構成せずにアプライアンスを介してデータを強制するには、インラインモードを使用します。

動作状態監視

アプライアンスに障害が発生した場合、データをアプライアンスにルーティングしないでください。デフォルトでは、Cisco ポリシーベースルーティングはヘルスモニタリングを行いません。ヘルスモニタリングを有効にするには、アプライアンスの可用性をモニタリングするルールを定義し、「setipnext-hop」コマンドに「verify-availability」オプションを指定します。この構成では、アプライアンスが使用できない場合、ルートは適用されず、アプライアンスはバイパスされます。

重要：仮想インラインモードは、正常性監視とともに使用する場合のみお勧めします。ポリシーベースのルーティングをサポートする多くのルーターは、ヘルスチェックをサポートしていません。ヘルスモニタリング機能は比較的新しいものです。Cisco IOS リリース 12.3（4）T で利用可能になりました。

以下は、アプライアンスの可用性を監視するためのルールの例です。

“‘ pre codeblock
!- Use a ping (ICMP echo) to see if appliance is connected track 123 rtr 1 reachabilit y ! rtr 1 type echo protocol IpIcmpecho 192.168.1.200 schedule 1 life forever start-time now

```
このルールは、192.168.1.200でアプライアンスに定期的にpingを実行します。123に対してテストして、ユニットが稼働しているかどうかを確認できます。

## ルーティングの例

次に、[仮想インラインの例](/ja-jp/citrix-sd-wan-wanop/11-1/cb-deployment-modes-con/br-adv-virt-inline-mode-con.html)に示すローカルサイトおよびリモートサイトの Cisco ルータの設定例を示します。ヘルスモニタリングを説明するために、ローカルサイトの構成にはヘルスモニタリングが含まれていますが、リモートサイトの構成には含まれていません。

注：ローカルサイトの構成では、pingモニターが既に構成されていることを前提としています。

```



```
例は、Cisco IOS CLIに準拠しています。他のベンダーのルーターには適用できない場合があります。

ローカルサイト、ヘルスチェックが有効:

``` pre codeblock
!
! For health-checking to work, do not forget to start
! the monitoring process.
!
! Original configuration is in normal type.
! appliance-specific configuration is in bold.
!
ip cef
!
interface FastEthernet0/0
ip address 10.10.10.5 255.255.255.0
ip policy route-map client_side_map
!
interface FastEthernet0/1
ip address 172.68.1.5 255.255.255.0
ip policy route-map wan_side_map
!
interface FastEthernet1/0
ip address 192.168.1.5 255.255.255.0
!
ip classless
ip route 0.0.0.0 0.0.0.0 171.68.1.1
!
ip access-list extended client_side
permit ip 10.10.10.0 0.0.0.255 10.16.20.0 0.0.0.255
ip access-list extended wan_side
permit ip 10.16.20.0 0.0.0.255 10.10.10.0 0.0.0.255
!
route-map wan_side_map permit 20
match ip address wan_side
!- Now set the appliance as the next hop, if it’ s up.
set ip next-hop verify-availability 192.168.1.200 20 track 123
!
route-map client_side_map permit 10
match ip address client_side
set ip next-hop verify-availability 192.168.1.200 10 track 123
```

リモートサイト（ヘルスチェックなし）:

“‘ pre codeblock

! This example does not use health-checking.

! Remember, health-checking is always recommended,

! so this is a configuration of last resort.

!

!


```

ip cef
!
interface FastEthernet0/0
ip address 20.20.20.5 255.255.255.0
ip policy route-map client_side_map
!
interface FastEthernet0/1
ip address 171.68.2.5 255.255.255.0
ip policy route-map wan_side_map
!
interface FastEthernet1/0
ip address 192.168.2.5 255.255.255.0
!
ip classless
ip route 0.0.0.0 0.0.0.0 171.68.2.1
!
ip access-list extended client_side
permit ip 10.16.20.0 0.0.0.255 10.10.10.0 0.0.0.255
ip access-list extended wan_side
permit ip 10.10.10.0 0.0.0.255 10.16.20.0 0.0.0.255
!
route-map wan_side_map permit 20
match ip address wan_side
set ip next-hop 192.168.2.200
!
route-map client_side_map permit 10
match ip address client_side
set ip next-hop 192.168.2.200
!_

```
上記の各例では、アクセスリストをルートマップに適用し、ルートマップをインターフェイスにアタッチします。アクセスリストは、一方の高速化されたサイトで発信され、もう一方のサイトで終了するすべてのトラフィックを識別します（ 10.10.10.0/24 と目的地 20.20.20.0/24 またはその逆）。アクセスリストとルートマップの詳細については、ルーターのドキュメントを参照してください。

この構成は、一致するすべてのIPトラフィックをアプライアンスにリダイレクトします。TCPトラフィックのみをリダイレクトする場合は、アクセスリストの設定を次のように変更できます（リモート側の設定のみがここに表示されます）。

``` pre codeblock
```


```

```
!
 ip access-list extended client_side
 permit tcp 10.16.20.0 0.0.0.255 10.10.10.0 0.0.0.255
 ip access-list extended wan_side
 permit tcp 10.10.10.0 0.0.0.255 10.16.20.0 0.0.0.255
!
```

アクセスリストの場合、通常のマスクは使用されないことに注意してください。代わりにワイルドカードマスクが使用されます。ワイルドカードマスクをバイナリで読み込む場合、「1」は「気にしない」ビットと見なされます。

マルチ **WAN** 環境向けの仮想インライン

April 19, 2021

複数の WAN リンクを持つ企業は、多くの場合、非対称ルーティングポリシーを採用しており、インラインアプライアンスを一度に 2 か所に配置する必要があるようです。仮想インラインモードは、使用されている WAN リンクに関係なく、ルーター構成を使用してアプライアンスを介してすべての WAN トラフィックを送信することにより、非対称ルーティングの問題を解決します。次の図は、単純な複数 WAN リンクの展開例を示しています。

2 つのローカル側ルーターは、トラフィックをローカルアプライアンスにリダイレクトします。FE 0/0 両方のルーターのポートは、アプライアンスと同じブロードキャストドメインにあります。ローカルアプライアンスは、デフォルトの仮想インライン構成（イーサネットセンダーに戻る）を使用する必要があります。

図 1：2 つの WAN ルーターを備えた仮想インラインモード

仮想インラインモードと高可用性

April 19, 2021

仮想インラインモードは、高可用性（ハイアベイラビリティ）設定で使用できます。次の図は、単純な高可用性の展開を示しています。仮想インラインモードでは、アプライアンスのペアが 1 つの仮想アプライアンスとして機能します。ルータの設定は、単一アプライアンスの場合と同じですが、個々のアプライアンスの IP アドレスではなく、高可用性ペアの仮想 IP アドレスがルータ設定テーブルで使用される点が異なります。この例では、ローカルアプライアンスはデフォルトの仮想インライン構成（イーサネットセンダーに戻る）を使用する必要があります。

図 1：高可用性の例

監視とトラブルシューティング

April 19, 2021

仮想インラインモードでは、WCCP モードとは異なり、アプライアンスは仮想インライン固有の監視を提供しません。仮想インライン展開のトラブルシューティングを行うには、アプライアンスにログインし、[ダッシュボード] ページを使用して、トラフィックがアプライアンスに出入りしていることを確認します。トラフィック転送の失敗は、通常、ルーター構成のエラーが原因で発生します。

[監視：使用状況] または [監視：接続] ページにトラフィックが転送されているがアクセラレーションが行われていないことが示されている場合（アプライアンスが WAN リンクのもう一方の端にすでにインストールされていると想定）、着信 WAN トラフィックと発信 WAN トラフィックはアプライアンスに転送されています。一方向のみ前進すると加速できません。

ヘルスチェックをテストするには、アプライアンスの電源を切ります。ヘルスチェックアルゴリズムがタイムアウトした後、ルータはトラフィックの転送を停止する必要があります。

グループモード

April 19, 2021

グループモードでは、2 つ以上のアプライアンスが単一の仮想アプライアンスになります。このモードは、非対称ルーティングの問題に対する 1 つの解決策です。これは、特定の接続の一部のパケットが特定のアプライアンスを通過するが、他のパケットは通過しない場合として定義されます。アプライアンスアーキテクチャの制限は、特定の接続内のすべてのパケットが同じ 2 つのアプライアンスを通過しない限り、アクセラレーションを実行できないことです。グループモードはこの制限を克服します。

グループモードは、ルーターを再構成せずに、複数のリンクまたは冗長リンクで使用できます。

> 注
>
> グループモードは、SD-WAN 4000 または 5000 アプライアンスではサポートされていません。

グループモードは、WAN リンクの片側にあるアプライアンスにのみ適用されます。ローカルアプライアンスは、リモートアプライアンスがグループモードを使用しているかどうかを認識も気にしません。

グループモードでは、ハートビートメカニズムを使用して、グループの他のメンバーがアクティブであることを確認します。パケットはアクティブなグループメンバーにのみ転送されます。

非対称ルーティングを回避することがグループモードを使用する主な理由ですが、その目的で使用できる方法はグループモードだけではありません。ご使用の環境に最適な方法であると判断した場合は、いくつかのパラメーターを設定することで有効にできます。特定の接続を担当するアプライアンスを決定するためのデフォルトのメカニズムで最適なアクセラレーションが提供されない場合は、転送ルールを変更できます。

図 1：冗長リンクのあるグループモード

図 2：非対称ルーティングの可能性がある非冗長リンクのグループモード

図 3：近くのキャンパスのグループモード

グループモードを使用する場合

April 19, 2021

次の一連の状況でグループモードを使用します。

- 複数の WAN リンクがあります。
- 非対称ルーティングの可能性があります（特定の接続上のパケットがいずれかのリンクを通過する可能性があります）。
- グループモードは、単一のアプライアンスを使用する代替モードよりもシンプルで実用的です。

代替手段は次のとおりです。

- 2 つ以上のリンクからのトラフィックが WCCP プロトコルを使用して WAN ルーターによって同じアプライアンスに送信される WCCP モード。
- 仮想インラインモード。ルータは、同じアプライアンス（または高可用性ペア）を介して 2 つ以上のリンクからトラフィックを送信します。
- 複数のブリッジ。各リンクは、同じアプライアンス内の異なるアクセラレーションブリッジを通過します。
- LAN レベルの集約。WAN トラフィックが 2 つ以上のパスに分割されるポイントより前に、アプライアンス（または高可用性ペア）を LAN に近づけます。

グループモードのしくみ

April 19, 2021

グループモードでは、グループの一部であるアプライアンスはそれぞれ、グループの接続の一部の所有権を取得します。特定のアプライアンスが接続の所有者である場合、そのアプライアンスはその接続に関するすべてのアクセラレーション決定を行い、圧縮、フロー制御、パケット再送信などを担当します。

アプライアンスは、所有者ではない接続のパケットを受信すると、所有者であるアプライアンスにパケットを転送します。所有者はパケットを調べ、適切なアクセラレーションの決定を行い、出力パケットを所有していないアプライアンスに転送します。このプロセスは、ルーターによって行われたリンクの選択を保持し、接続内のすべてのパケットを所有するアプライアンスで管理できるようにします。ルーターの場合、アプライアンスの導入による影響はあり

ません。ルーターを再構成する必要はなく、アプライアンスはルーティングメカニズムを理解する必要もありません。それらは単にルーターの転送決定を受け入れます。

図 1：グループモードでの送信側トラフィック

図 2：グループモードでの受信側のトラフィックフロー

グループモードには、ユーザーが選択できる 2 つの障害モードがあり、そのうちの 1 つに障害が発生した場合に、グループメンバーが相互に対話する方法を制御します。障害モードは、障害が発生したアプライアンスのバイパスカードが開く（アプライアンスを通過するトラフィックをブロックする）か、閉じたままにする（トラフィックが通過できるようにする）かを決定します。故障モードは次のとおりです。

加速を続ける**-** グループメンバーに障害が発生した場合、そのバイパスカードが開かれ、障害が発生したアプライアンスを通過するトラフィックはありません。冗長リンクが使用されている場合、結果はおそらくフェイルオーバーです。そうしないと、リンクにアクセスできなくなります。グループ内の他のアプライアンスは加速し続けています。通常のハッシュアルゴリズムは、変更された条件を処理します。（つまり、古いハッシュアルゴリズムが使用され、障害が発生したユニットが所有者として示されている場合は、新しい、より小さなグループに基づくハッシュアルゴリズムが適用されます。これにより、できるだけ多くの古い接続が保持されます。）

加速しない**-** グループメンバーに障害が発生すると、そのバイパスカードが閉じ、トラフィックが加速せずに通過できるようになります。加速されていないパスは非対称ルーティングを導入するため、グループの他のメンバーも障害を検出するとパススルーモードになります。

グループモードの有効化

April 19, 2021

グループモードを有効にするには、2 つ以上のアプライアンスのグループを作成します。アプライアンスは、1 つのグループのメンバーになることができます。グループメンバーは、アプライアンスライセンスの IP アドレスと SSL 共通名で識別されます。

すべてのグループモードパラメータは、[設定：グループモード] ページの [設定の構成：グループモード] テーブルにあります。

図 1：グループモードページ

グループモードを有効にするには

1. グループ通信に使用するアドレスを選択します。[構成: 高度な展開: グループモード] タブの [グループモード構成] テーブルの上部にある [メンバー VIP] の下のテーブルセルには、他のグループメンバーとの通信に使用されるポートの管理アドレスが含まれています。（ラベルのない）ドロップダウンメニューを使用して、正しいアドレスを選択します（たとえば、Aux1 ポートを使用するには、Aux1 ポートに割り当てた IP アドレスを選択します）。次に、[VIP の変更] をクリックします。

2. リストに少なくとももう 1 人のグループメンバーを追加します。（3 つ以上のグループがサポートされていますが、ほとんど使用されません。）[メンバー VIP] 列の次のセルに、他のアプライアンスがグループモード通信に使用するポートの IP アドレスを入力します。
3. 他のグループメンバーの SSL 共通名を [SSL 共通名] 列に入力します。SSL 共通名は、他のアプライアンスの「構成：高度なデプロイメント：高可用性」タブにリストされています。他のグループメンバーが高可用性ペアである場合、リストされている名前はプライマリアプライアンスの SSL 共通名です。

   > 注:
   >
   > ローカルアプライアンスが高可用性ペアの一部でない場合、高可用性セカンダリ SSL 共通名の最初のセルは空白です。他のグループメンバーが高可用性ペアである場合は、高可用性の SSL 共通名を指定します。高可用性セカンダリ SSL 共通名列の可用性セカンダリアプライアンス。

4. [追加] をクリックしてください。
5. グループ内の追加のアプライアンスまたは高可用性ペアに対して、手順 2 〜4 を繰り返します。
6. グループメンバーのリストの下にある 3 つのボタンはトグルであるため、それぞれが現在の設定の反対としてラベル付けされています。

   a) 上部のボタンには、「メンバーの障害が検出されたときに加速しない」または 「メンバーの障害が検出されたときに加速を続行する」のいずれかが表示されます。「加速しない…」設定は常に機能し、トラフィックをブロックしませんが、いずれかのメンバーに障害が発生すると、他のグループメンバーがバイパスモードになり、加速が完全に失われます。「続行して加速」オプションを使用すると、障害が発生したアプライアンスのブリッジが開回路になり、リンクに障害が発生します。このオプションは、WAN ルーターがフェイルオーバーを引き起こして応答する場合に適しています。新しい接続、および存続しているアプライアンスに属するオープン接続が高速化されます。
   b) 下のボタンには、[グループモードを無効にする] というラベルが付いているはずです。そうでない場合は、ボタンをクリックしてグループモードを有効にします。

7. 画面を更新します。ページの上部にはグループモードのパートナーが一覧表示されますが、グループモードのパートナーはまだ構成されていないため、ステータスに関する警告が表示されます。たとえば、パートナーが見つからないか、別のソフトウェアリリースを実行していることを示している可能性があります。
8. グループの他のメンバーでこの手順を繰り返します。グループの最後のメンバーを有効にしてから 20 秒以内に、[グループモードステータス] 行に NORMAL が表示され、他のグループモードメンバーが [ステータス：オンライン] および [構成：OK] と表示されます。

転送ルール

April 19, 2021

デフォルトでは、グループモード接続の 所有者 は、送信元 IP アドレスと宛先 IP アドレスのハッシュによって設定されます。グループ内の各アプライアンスは、同じアルゴリズムを使用して、特定の接続を所有しているグループメンバーを判別します。この方法は設定を必要としません。所有者は、オプションでユーザー設定可能なルールを介して指定できます。

グループモードハッシュはロードバランサーで使用されるものと同じではないため、トラフィックの約半分が 2 アプライアンスグループの所有アプライアンスに転送される傾向があります。最悪の場合、転送によって LAN 側のインターフェイスの負荷が 2 倍になり、実際の WAN トラフィックに対するアプライアンスのピーク転送速度が半分になります。

プライマリまたは Aux1 イーサネットポートがグループメンバー間のトラフィックに使用される場合、この速度ペナルティを減らすことができます。たとえば、2 つのアプライアンスのグループがある場合、イーサネットケーブルを使用して 2 つのユニットのプライマリポートを接続し、各ユニットの [グループモード] ページでプライマリポートを指定できます。ただし、グループモードメンバー間で転送されるトラフィックの量を最小限に抑えると、最大のパフォーマンスが得られます。

所有者は、特定のオプションに従って設定できます IP/port-based ルール。これらのルールは、グループ内のすべてのアプライアンスで同一である必要があります。グループの各メンバーは、そのグループモード構成が他のメンバーと同一であることを確認します。すべての構成が同一でない場合、どのメンバーアプライアンスもグループモードになりません。

トラフィックが接続を所有するアプライアンスに最初に到着した場合、トラフィックは加速され、通常どおり転送されます。グループ内の別のアプライアンスに最初に到着した場合、GRE トンネルを介して所有者に転送され、GRE トンネルによって高速化され、転送のために元のアプライアンスに戻されます。したがって、グループモードでは、ルータのリンク選択は変更されません。

明示的な IP ベースの転送ルールを使用すると、グループモード転送の量を減らすことができます。これは特に便利です primary-link/backup-link 各リンクが特定の範囲の IP アドレスを処理するが、他のリンクがダウンしているときにバックアップとして機能できるシナリオ。

図 1：IP ベースの所有者の選択

転送ルールにより、グループメンバーが「自然な」トラフィックのみを処理できるようになります。トラフィックが通常通常のリンクを介してルーティングされ、他のリンクを通過することはめったにない多くのインストールでは、これらのルールによってオーバーヘッドを大幅に削減できます。

ルールは上から下の順に評価され、最初に一致するルールが使用されます。ルールはオプションの IP と照合されます address/mask ペア（送信元アドレスと宛先アドレスの両方に対して比較されます）、およびオプションのポート範囲に対して。

ルールの順序に関係なく、パートナーアプライアンスが使用できない場合、ルールが一致するかどうかに関係なく、トラフィックはパートナーアプライアンスに転送されません。

たとえば、次の図では、メンバー 172.16.1.102 は、自身のサブネットとの間のすべてのトラフィックの所有者です。(172.16.1.0/24), メンバー 172.16.0.184 は、他のすべてのトラフィックの所有者です。

パケットがユニット 172.16.1.102 に到着し、アドレス指定されていない場合 to/from ネット 172.16.1.0/24, 172.16.0.184 に転送されます。

ただし、ユニット 172.16.0.184 に障害が発生した場合、ユニット 172.16.1.102 はパケットを転送しなくなります。トラフィック自体を処理しようとします。この動作は、[グループモード] タブの [メンバー障害が検出さ れたときに加速しない] をクリックすることで禁止できます。

プライマリ WAN リンクとバックアップ WAN リンクを使用するセットアップでは、転送ルールを記述して、すべてのトラフィックをプライマリリンクでアプライアンスに送信します。プライマリ WAN リンクに障害が発生したが、プライマリアプライアンスに障害が発生しなかった場合、WAN ルーターはフェイルオーバーし、セカンダリリンクを介してトラフィックを送信します。セカンダリリンク上のアプライアンスはトラフィックをプライマリリンクアプライアンスに転送し、アクセラレーションは中断されずに続行されます。この構成は、リンクフェイルオーバー後も高速接続を維持します。

図 2：転送ルール

グループモードの監視とトラブルシューティング

April 19, 2021

グループモードのインストールでは、次の 2 つのことを確認する必要があります。

- 2 つのアプライアンスがグループモードに入ったこと。これは、いずれかのアプライアンスの [構成：高度な展開：グループモード] ページで確認できます。
- グループモードペアの動作は、他のメンバーに障害が発生した場合、およびリンクの 1 つに障害が発生した場合に、他のアプライアンスを無効にし、リンクの 1 つを一時的に切断することによって決定されます。

イーサネットポートのカスタマイズ

April 19, 2021

一般的なアプライアンスには、4 つのイーサネットポートがあります。バイパス（配線に失敗）リレーを備えた 加速ペア *A* （apA.1 および apA.2）と呼ばれる 2 つの加速ブリッジポートと、プライマリおよび Aux1 と呼ばれる 2 つの加速されていないマザーボードポートです。ブリッジポートは加速を提供しますが、マザーボードポートは二次的な目的で使用されることもあります。ほとんどのインストールでは、ブリッジポートのみが使用されます。

一部の SD-WAN ユニットには、マザーボードポートしかありません。この場合、2 つのマザーボードポートがブリッジされます。

アプライアンスのユーザーインターフェイスには、VLAN または非 VLAN ネットワークからアクセスできます。管理目的で、アプライアンスのブリッジポートまたはマザーボードポートのいずれかに VLAN を割り当てることができます。

図 1: イーサネットポート

ポートリスト

ポートの名前は次のとおりです。

イーサネット ポート	名前
マザーボードポート 1	プライマリ（またはバイパスカードが存在しない場合は apA.1）
マザーボードポート 2	Auxiliary1 または Aux1（またはバイパスカードが存在しない場合は apA.2）
ブリッジ #1	加速ペア A（apA、ポート apA.1 および apA.2）
ブリッジ #2	加速ペア B（apB、ポート apB.1 および apB.2）

表 1. イーサネットポート名

高可用性モードの動作

April 19, 2021

高可用性（ハイアベイラビリティ）ペアでは、1 つのアプライアンスはプライマリ、もう 1 つのアプライアンスはセカンダリです。プライマリは、自身とセカンダリのステータスを監視します。問題が検出されると、トラフィック処理はセカンダリアプライアンスにフェイルオーバーします。既存の TCP 接続は終了します。フェイルオーバーを成功させるために、2 つのアプライアンスは構成の同期を維持します。WCCP モードの高可用性構成では、トラフィックを処理しているアプライアンスがアップストリームルーターとの通信を維持します。

ステータスの監視 高可用性が有効になっている場合、プライマリアプライアンスは VRRP プロトコルを使用して、ハートビート信号をセカンダリアプライアンスに 1 秒に 1 回送信します。さらに、プライマリアプライアンスは、イーサネットポートのキャリアステータスを監視します。以前にアクティブだったポートでキャリアが失われると、接続が失われます。

フェイルオーバー プライマリアプライアンスのハートビート信号に障害が発生した場合、またはプライマリアプライアンスが以前にアクティブだったイーサネットポートでキャリアを 5 秒間失った場合、セカンダリアプライアンスが引き継ぎ、プライマリになります。障害が発生したアプライアンスが再起動すると、セカンダリになります。新しい

プライマリは、ARP ブロードキャストを使用してネットワーク上で自身をアナウンスします。MAC スプーフィングは使用されません。イーサネットブリッジングはセカンダリアプライアンスで無効になり、プライマリアプライアンスをインライントラフィックの唯一のパスとして残します。ループを防ぐために、両方のアプライアンスで配線の失敗が禁止されています。

> 警告
>
> イーサネットバイパス機能は、高可用性モードで無効になります。インライン高可用性ペアの両方のアプライアンスの電源が切れた場合、接続が失われます。停電時に WAN 接続が必要な場合は、少なくとも 1 つのアプライアンスをバックアップ電源に接続する必要があります。
> 注
>
> 高可用性ペアのセカンダリアプライアンスには、フォワーディングループを防ぐために、ブリッジポートの 1 つであるポート APA.1 が無効になっています。アプライアンスにデュアルブリッジがある場合、apB.1 も無効になります。片腕設置では、ポート apA.2 を使用します。そうしないと、高可用性が有効になっていると、セカンダリアプライアンスにアクセスできなくなります。

Primary/secondary 割り当て-両方のアプライアンスが再起動された場合、それ自体を完全に初期化した最初のアプライアンスがプライマリになります。つまり、アプライアンスには役割が割り当てられておらず、最初に使用可能になったアプライアンスがプライマリとして引き継ぎます。VRRP ハートビートに使用されるインターフェイスで IP アドレスが最も高いアプライアンスは、両方が同時に使用可能になった場合にタイブレーカーとして使用されます。

フェイルオーバー中の接続の終了：フェイルオーバーの副作用として、加速された TCP 接続と加速されていない TCP 接続の両方が終了します。非 TCP セッションは、プライマリアプライアンスの障害からセカンダリアプライアンスへのフェイルオーバーまでの短い期間（数秒）によって引き起こされる遅延を除いて、影響を受けません。ユーザーは開いている接続が閉じられることを経験しますが、新しい接続を開くことはできます。

構成の同期—2 つのアプライアンスは設定を同期して、セカンダリがプライマリを引き継ぐ準備ができていることを確認します。ペアの構成がブラウザベースのインターフェイスを介して変更された場合、プライマリアプライアンスはセカンダリアプライアンスをすぐに更新します。

高可用性は、両方のアプライアンスが同じソフトウェアリリースを実行していない限り有効にできません。

WCCP モードでの高可用性：WCCP を高可用性ペアとともに使用すると、プライマリアプライアンスはルータとの通信を確立します。アプライアンスは、仮想 IP アドレスではなく、apA または apB の管理 IP アドレスを使用してルーターと通信します。フェールオーバー時に、新しいプライマリアプライアンスはルータとの WCCP 通信を確立します。

ケーブル接続の要件

April 19, 2021

高可用性ペアの 2 つのアプライアンスは、パラレル配置またはワンアーム配置のいずれかで、同じサブネット上にインストールされます。両方とも次の図に示します。ワンアーム構成では、apA.1 ポートではなく、apA.2 ポート（およびオプションで apB.2 ポート）を使用します。一部のモデルでは、インラインモードまたはワンアームモードのどちらで展開する場合でも、個別の管理 LAN が必要です。これは、中央の図にのみ示されています。

図 1：高可用性ペアのケーブル接続

追加のスイッチで上記のトポロジーを壊さないでください。ランダムスイッチの配置はサポートされていません。各スイッチは、単一のモノリシックスイッチ、単一の論理スイッチ、または同じシャーシの一部である必要があります。

アプライアンスに接続されているルータまたはスイッチポートでスパニングツリープロトコル（STP）が有効になっている場合、フェールオーバーは機能しますが、フェールオーバー時間は約 30 秒に増加する可能性があります。STP がない場合、フェイルオーバー時間は約 5 秒です。したがって、可能な限りブリーフィールオーバー間隔を実現するには、アプライアンスに接続するポートで STP を無効にします。

そのほかの要件

April 19, 2021

高可用性ペアの両方のアプライアンスは、次の基準を満たしている必要があります。

- ダッシュボードページのシステムハードウェアエントリに示されているように、同一のハードウェアを使用します。
- まったく同じソフトウェアリリースを実行します。
- イーサネットバイパスカードを装備します。アプライアンスに何がインストールされているかを確認するには、ダッシュボードページを参照してください。

高可用性をサポートしないアプライアンスは、[構成：高可用性] ページに警告を表示します。

高可用性ペアへの管理アクセス

April 19, 2021

高可用性（ハイアベイラビリティ）ペアを設定する場合は、ペアに仮想 IP（VIP）アドレスを割り当てます。これにより、2 つのアプライアンスを単一のユニットであるかのように管理できます。高可用性モードを有効にすると、セカンダリアプライアンスの IP アドレスを介して管理することはほとんど無効になり、ほとんどのパラメータはグレー表示されます。警告メッセージは、すべてのページに理由を表示します。すべての管理タスクに高可用性 VIP を使用します。ただし、セカンダリアプライアンスの高可用性状態は、管理 UI から無効にできます。

高可用性ペアの設定

April 19, 2021

新しくインストールした 2 つのアプライアンスを高可用性ペアとして設定することも、既存のインストールに 2 台目のアプライアンスを追加して高可用性ペアを作成することもできます。

前提条件：物理的なインストールと基本的な構成手順

高可用性を構成するには

1. （加速されたブリッジ上で）トラフィックネットワークに接続されているアプライアンスが 1 つだけであることを確認してください。両方が接続されている場合は、1 つのブリッジケーブルを 2 番目のアプライアンスのアクティブなブリッジから外します。これにより、転送ループが防止されます。
2. 最初のアプライアンスの [機能] ページで、トラフィック処理を無効にします。これにより、高可用性ペアが設定されるまで、アクセラレーションが無効になります。
3. 2 番目のアプライアンスについても繰り返します。
4. 最初のアプライアンスで、以下に示す [構成：高度な展開：高可用性] タブに移動します。
5. [有効] チェックボックスを選択します。
6. [高可用性仮想 IP アドレスの構成] リンクをクリックして、仮想 IP アドレスを apA インターフェイスに割り当てます。このアドレスは、後で両方のアプライアンスを 1 つのユニットとして制御するために使用されます。
7. [高可用性] ページに戻り、[VRRP VRID] フィールドで VRRP ID をペアに割り当てます。値のデフォルトはゼロですが、VRRPID 番号の有効な範囲は 1～255 です。この範囲内で、ネットワーク上の別の VRRP デバイスに属していない任意の値を指定できます。
8. [パートナー SSL 共通名] フィールドに、他のアプライアンスの SSL 共通名を入力します。これは、そのアプライアンスの [構成：高度な展開：高可用性] タブの [パートナー SSL 共通名] フィールドに表示されます。ここで使用される SSL 資格情報は、工場でインストールされています。
9. ［更新］をクリックします。
10. 2 番目のアプライアンスで手順 3～8 を繰り返します。アクセラレーションブリッジ（apA など）を介してアプライアンスを管理している場合、2 番目のアプライアンスに接続するには、手順 1 で取り外したイーサネットケーブルを再接続する必要がある場合があります。その場合は、このケーブルを接続し、最初のアプライアンスの対応するケーブルを外します。
11. ブラウザで、高可用性ペアの仮想 IP アドレスに移動します。[機能] ページでトラフィック処理を有効にします。それ以上の構成は、この仮想アドレスから実行されます。
12. 切断したままのケーブルを差し込みます。
13. 各アプライアンスで、[構成：高度な展開：高可用性] ページに、高可用性がアクティブであり、一方のアプライアンスがプライマリで、もう一方がセカンダリであることが表示されます。そうでない場合は、問題の性質を示す警告バナーが画面の上部に表示されます。

図 1：高可用性構成ページ

高可用性ペアでのソフトウェアの更新

April 19, 2021

高可用性ペアで SD-WAN ソフトウェアをアップデートすると、アップデート中の一時点でフェールオーバーが発生します。

注：[更新] ボタンをクリックすると、開いているすべての TCP 接続が終了します。

高可用性ペアのソフトウェアを更新するには

1. 両方のアプライアンスにログオンします。
2. セカンダリアプライアンスで、ソフトウェアを更新して再起動します。再起動後も、アプライアンスはセカンダリのままです。インストールが成功したことを確認します。プライマリアプライアンスは、セカンダリアプライアンスが存在するが、バージョンの不一致が原因で自動パラメータ同期が機能していないことを示す必要があります。
3. プライマリアプライアンスで、ソフトウェアを更新してから再起動します。再起動するとフェイルオーバーが発生し、セカンダリアプライアンスがプライマリになります。再起動が完了すると、両方のアプライアンスが同じソフトウェアを実行しているため、高可用性が完全に確立されます。

高可用性ペアのパラメータの保存/復元

April 19, 2021

システムメンテナンス：Backup/Restore 関数を使用して、次のように高可用性ペアのパラメーターを保存および復元できます。

パラメータをバックアップするには

通常どおりバックアップ機能を使用します。つまり、高可用性 VIP アドレス（高可用性ペアを管理する場合と同様）を使用して GUI にログオンし、[システム管理: バックアップ/復元] ページで [Download Settings] をクリックします。

パラメータを復元するには

1. [構成：高度な展開：高可用性（高可用性）] タブの [有効] チェックボックスをオフにして、両方のアプライアンスで高可用性を無効にします。

2. 1 つのアプライアンスのブリッジからネットワークケーブルを抜きます。(「アプライアンス A」と呼びます。)
3. アプライアンス A から電源コードを抜きます。
4. 以前に保存したパラメータのセットをシステムメンテナンスにアップロードして、他のアプライアンス（アプライアンス B）のパラメータを復元します。Backup/Restore ページをクリックし、[設定の復元] をクリックします。(この操作を完了するには、再起動が必要です。再起動すると、高可用性が再び有効になります)。
5. アプライアンス B が再起動するのを待ちます。プライマリになります。
6. アプライアンス A を再起動します。
7. アプライアンス A の GUI にログオンし、[構成：高度な展開：高可用性（高可用性）] タブで高可用性を再度有効にします。アプライアンスは、プライマリからパラメータを取得します。
8. 手順 2 で取り外したネットワークケーブルを差し込みます。

これで、両方のアプライアンスが復元され、同期されます。

高可用性ペアのトラブルシューティング

April 19, 2021

アプライアンスが高可用性モードへの失敗を報告した場合は、エラーメッセージに原因も記載されます。高可用性モードを妨げる可能性のある問題には、次のようなものがあります。

- 他のアプライアンスは実行されていません。
- 2 つのアプライアンスの高可用性パラメータは同一ではありません。
- 2 つのアプライアンスは同じソフトウェアリリースを実行していません。
- 2 つのアプライアンスのモデル番号は同じではありません。
- アプライアンス間のケーブル接続が不適切または不完全な場合、高可用性ハートビートがアプライアンス間で通過できません。
- 高い availability/Group 一方または両方のアプライアンスのモード SSL 証明書が破損しているか、欠落しています。

2 ボックスモード

April 19, 2021

2 ボックスモードは、SD-WAN SE アプライアンスが WCCP ルーターおよび SDWAN-WANOP として機能する WCCP ワンアームベースの展開です。(4000/5000) アプライアンスは WCCP クライアントとして機能し、WCCP コンバージェンスの確立を支援します。このようにすべての仮想 path/Intranet SD-WAN SE アプライアンスに到達するサービス指向 TCP パケットは、SD-WAN SE と WANOP の両方の利点を顧客のトラフィックに提供することにより、最適化の利点のために SDWAN-WANOP アプライアンスにリダイレクトされます。

2 ボックスモードは、次のアプライアンスモデルでのみサポートされます。

- SD-WAN SE アプライアンス–4000、4100、および 5100
- SD-WAN WANOP アプライアンス–4000、4100、5000、および 5100

> 注
>
> Two Box モードが有効の場合、高可用性および WCCP 配置モードにアクセスできません。ただし、これらの展開モードは、ユーザーが管理するために使用できます。
>
> 重要
>
> - Two Box Mode が有効の場合、レガシー WCCP 配置は無効になりますが、サービスグループのコンバージェンスは WCCP モニタリングページからしか確認できません。Two BoxMode の監視セクションの下に個別の GUI ページはありません。
> - Standard Edition アプライアンスで実行されている WCCP プロセスが、短い時間間隔内に複数回、たとえば 1 分間に 3 回再起動すると、サービスグループは自動的にシャットダウンします。このようなシナリオでは、WANOP アプライアンスで WCCP コンバージェンスを取得するには、WANOP アプライアンスの Web GUI で WCCP 機能を再度有効にします。
> - Standard Edition アプライアンスの構成に関連する WCCP 構成または WAN 最適化に変更があると、外部 WANOP アプライアンスがリブートします。例えば、enabling/disabling 構成エディターのインターフェースグループの WCCP チェックボックスに続いて変更管理プロセスを実行すると、WANOP アプライアンスも再起動します。
>
> 注
>
> また、2 ボックスモードを実装する際に考慮すべき次の点に注意してください。
>
> - 構成エディタから WANOP アプライアンスにリダイレクトするようにルーティングドメインを選択した場合は、WCCP が有効になっているインターフェイスグループに追加する必要があります。
> - パートナーサイトでも同じルーティングドメインのトラフィックを選択する必要があります。たとえば、**MCN** > **Branch01** は、WAN 最適化のメリットを確認します。
> - WCCP が有効になっているインターフェイスグループでルーティングドメインが選択されている場合、ブリッジドインターフェイスを含む別のインターフェイスグループには、同じルーティングドメインが設定されている必要があります。WCCP 対応のインターフェイスグループにルーティングドメインが設定されている場合にのみ、WAN 最適化の利点を備えたエンドツーエンドのトラフィックフローを送信するだけでは不十分です。

Citrix SD-WAN 標準版

DC またはブランチサイトの StandardEdition アプライアンスで 2 ボックスモードソリューションを構成するには、次の手順に従います。

1. SD-WAN SE Web 管理インターフェイスで、[構成]> 仮想 **WAN**> 構成エディターに移動します。既存の構成パッケージを開くか、パッケージを作成します。
2. 選択した構成のパッケージでは、構成の詳細を表示する 高度なタブ に移動します。
3. グローバル 設定を開き、ルーティングドメイン を展開して、**[WANOP** にリダイレクト**]** チェックボックスが有効になっていることを確認します。
4. DC を展開して、アプライアンスが有効になっている仮想ネットワークインターフェイスを示す [インターフェイスグループ**]** 設定で、仮想インターフェイスの **WCCP** を有効にします。
5. [サイト **+** 追加**]** を展開して、ブランチルーティングドメインとインターフェイスグループの設定を表示します。ブランチサイトで、ルーティングドメインの **[WANOP** にリダイレクト**]** チェックボックスが有効になっています。

> 注
>
> WCCP リスナーは、イーサネットインターフェイスが 1 つだけ設定されている仮想ネットワークインターフェイスに対してだけ有効にする必要があります。ブリッジドペアで WCCP リスナーを有効にしないでください。SD-WAN SE アプライアンスと SD-WAN WANOP アプライアンス間の ONE-ARM インターフェイスで有効にすることを意図しています。

Citrix SD-WAN WANOP 構成

SD-WAN WANOP アプライアンスの WebGUI で 2 ボックス展開モードを設定するには:

1. SD-WAN WANOP Web 管理インターフェースで、「構成」 > アプライアンスの設定 > 高度な展開 > **2** ボックスソリューションに移動します。
2. 編集 アイコンをクリックして、2 つのボックスモード設定を編集します。キャッシュ **IP** に関する情報ダイアログが表示されます。[**OK**] をクリックします。
3. [**2** つのボックスを有効にする**]** チェックボックスを有効にします。
4. ピア **IP** を入力します。ピア IP は、SD-WAN StandardEdition アプライアンスの IP アドレスです。
5. ユーザー資格情報を入力し、[適用] をクリックします。

2 ボックスモードの構成と管理性

以下は、展開のために考慮すべき 2 つのボックスモード構成と管理性のポイントの一部です。

- SD-WAN WANOP 設定は、SD-WAN SE 構成エディタから統合ペインとして設定できます。
  - サービスクラス
  - アプリケーション分類子

  - 特徴
  - システムチューニング

監視

SD-WAN SE アプライアンスの WebUI の [監視] ページを使用して、SD-WAN WANOP トラフィックを直接監視できます。これにより、データトラフィックの処理中に、SDWAN-SE アプライアンスと SDWAN-WO アプライアンスの両方を単一ペインで監視できます。SDWAN-SE UI の [WAN Optimization] ノードで、接続の詳細、セキュアパートナーの詳細などを表示できます。

構成

APPFLOW は、**APPFLOW** ノードの SDWAN-SE 構成 ページから直接構成できます。これにより、SDWAN-SE は、APPFLOW の構成、およびサービスクラス、アプリケーション分類子などの他のデータ処理構成属性の単一ペインとして機能できます。SDWAN-SE で行われた構成は、SDWAN-WO 構成に反映され、シームレスな APPFLOW 機能のサポートを維持します。

Citrix Application Delivery Management（ADM）によってすでに検出されている SD-WAN WANOP を 2 ボックスモードで使用する場合は、このモードをオフにするまで、Citrix ADM を使用して分離して構成しないでください。これは、トラフィック処理用の WANOP の構成が、2 ボックスモードの SD-WAN SE アプライアンスによって管理されるためです。

高度な Optimization またはセキュアアクセラレーションは、SDWAN-WO アプライアンスで設定する場合と同様に、SDWAN-SE アプライアンス上で直接構成する必要があります。これは、ドメイン参加やセキュア Acceleration/SSL 高度な最適化または SSL プロキシ用のプロファイル作成などの構成の単一ペインの構成を維持するのに役立ちます。

- ライセンスは、SD-WAN SE および SD-WAN WANOP アプライアンスごとに個別に管理する必要があります。
- ソフトウェアアップグレードは、SD-WAN SE および SD-WAN WANOP アプライアンスごとに、それぞれのソフトウェアパッケージで個別に管理する必要があります。たとえば、SD-WAN SE の場合は tar.gz、SD-WAN WANOP の場合は upg をアップグレードします。
- データパス統合は、WCCP 展開モードを介して SD-WAN SE と外部 WANOP アプライアンス間で構成する必要があります。
  - データパスレベルでは、WCCP と仮想 WAN の両方の機能が、WANOP と SE の間のデータパス統合を通じてワンアームモードで外部的に提供され、最適化のメリットが得られます。

統一された構成と監視

SD-WAN SE および SDWAN-WANOP アプライアンスでツーボックスモードを有効にすると、SD-WAN-EE アプライアンスでのツーボックス構成の表示と同様に、SD-WAN SE アプライアンスで設定を表示できます。

1. 構成 > 仮想 **WAN** > **WAN Optimization**
2. 構成 下の Appflow ノード > アプライアンスの設定
3. [構成] の [WAN Optimization] ノード。

   この情報は、SD-WAN SE アプライアンスで 2 ボックスモードになっている SD-WAN WANOP アプライアンスからリダイレクトされます。

   SSL アクセラレーションや AppFlow などの WANOP に関連する構成を、SD-WAN SE Web GUI から実行できるようになりました。

   接続、圧縮、CIFS/SMB、ICA Advanced、MAPI、パートナーなどのトラフィック関連の統計情報を、SD-WAN SE Web GUI の [監視] > [WAN 最適化**]** の **[SD-WAN** Premium Edition] アプライアンスと同様に監視できるようになりました。

2 ボックスモードでの **SD-WAN WANOP** アプライアンスの管理 **IP** アドレスの変更

2 ボックスモードで SDWAN-WANOP アプライアンスの管理 IP アドレスを変更するには:

1. SD-WAN SE アプライアンス上コマンド *clear_wo_sync* を実行する。これにより、GUI リダイレクトのために SD-WAN WANOP IP アドレス情報が確実にクリアされます。
2. SD-WAN WANOP アプライアンスで 2 ボックスモード構成を無効または有効にします。SD-WAN WANOP アプライアンスの新しい IP アドレス（変更された IP）が SD-WAN SE に送信されます。新しく変更された IP アドレスが URL リダイレクトページに表示されます。

管理 IP アドレスは、ピア IP アドレスの構成に使用されます。

SD-WAN WANOP アプライアンスで **2** ボックスモードを無効にする

SD-WAN WANOP および SD-WAN SE アプライアンスを無効にするか 2 ボックスモードから切り離すには:

1. SD-WAN WANOP アプライアンスから TwoBox モードを無効にします。
2. SD-WAN SE WebGUI に SD-WAN WANOP アプライアンスの 2 つのボックスモードページが表示されることが期待されます。これらのページをクリアするには、次のコマンドを実行します。*clear_wo_sync* 。

よくあるご質問

April 19, 2021

アクセラレーション

April 19, 2021

加速はトンネルを使用しますか?

いいえ、アクセラレーションは透過的であり、元の接続と同じ IP アドレスとポート番号を使用します。これにより、現在の監視方法を引き続き正常に機能させることができます。

アクセラレーションはパケットストリームをどのように変更しますか?

非圧縮接続の場合、アクセラレーションはパケットの TCP ヘッダーにオプションを追加しますが、パケットペイロードはそのまま残します。これらのオプションにより、接続の両端にある Citrix SD-WAN WANOP デバイスが相互に通信できるようになります。さらに、TCP シーケンス番号は、ルーティングの問題やアプライアンスの障害が同じ接続で加速されたパケットと加速されていないパケットを混合することを防ぐために調整されます。

圧縮接続では、もちろんペイロードが圧縮され、コンプレッサーの出力がフルサイズのパケットに蓄積されます。結果は、たとえば、3:1 圧縮すると、同じ数のパケットではなく、3 分の 1 の数のパケットが送信され、それぞれが 3 分

の 1 のサイズに縮小されます。圧縮では、Citrix SD-WAN WANOPTCP ヘッダーオプションとシーケンス番号の調整も使用されます。

加速の基本的な要件は何ですか?

アクセラレーションには、接続の両端に Citrix SD-WAN WANOP デバイスが必要であり、接続は TCP プロトコルを使用する必要があり、接続のすべてのパケットは両方の Citrix SD-WAN WANOP デバイスを通過する必要があります。

CIFS と MAPI

April 19, 2021

Citrix SD-WAN WANOP アプライアンスで **MAPI** と署名付き **SMB** を構成する前に、どのような前提条件が必要ですか?

Citrix SD-WAN WANOP アプライアンスで MAPI と署名付き SMB を構成する前に、次の条件を満たす必要があります。

- Secure Peer オプションは、サーバー側アプライアンスだけでなくクライアントでも True に設定する必要があります。
- デリゲートユーザーをデータセンター側のアプライアンスに追加し、そのステータスを「成功」としてマークする必要があります。
- データセンター側のアプライアンスは、ドメインに正常に参加する必要があります。
- サーバー側アプライアンスで構成された DNS IP アドレスは到達可能である必要があります。

  詳しくは、「安全な Windows トラフィックを最適化するように Citrix SD-WAN WANOP アプライアンスを構成する」を参照してください。

デリゲートユーザーのドメインコントローラーで何を構成する必要がありますか?

Citrix SD-WAN WANOP アプライアンスでユーザーの委任を構成する前に、ドメインコントローラーでユーザーを作成する必要があります。

DNS サーバーで何かを構成する必要がありますか?

はい。DNS サーバーで、ドメインコントローラーのすべての IP アドレスの順方向および逆方向のルックアップを構成する必要があります。

Citrix SD-WAN WANOP アプライアンスをドメインに参加させる前に何を確認する必要がありますか?

アプライアンスをドメインに参加させる前に、以下を確認してください。

- プライマリまたはセカンダリ DNS サーバーに構成された IP アドレスに到達できる必要があります。

- ドメインに到達できる必要があります。
- 解決されたドメイン IP アドレスに到達できる必要があります。
- オプションで、Pre Domain JoinCheck ユーティリティのステータスに合格する必要があります。

Citrix SD-WAN WANOP アプライアンスがユーザーを代理ユーザーとして追加する準備ができているかどうかを確認するにはどうすればよいですか?

Windows ドメインページの [デリゲートユーザーの確認] ユーティリティを使用して、ユーザーを確認できます。すべてのパラメータのステータスにエラーメッセージがない場合、アプライアンスはユーザーをデリゲートユーザーとして追加する準備ができています。

ユーティリティに障害が表示された場合は、ユーザーを代理ユーザーとして追加する前に、これらに対処する必要があります。ログを参照して、テスト結果を理解できます。

サーバー側の **Citrix SD-WAN WANOP** アプライアンスのホスト名とホスト名の長さに関する要件はありますか?

サーバー側の Citrix SD-WAN WANOP アプライアンスで、ホスト名がネットワーク内で一意であることを確認してください。さらに、ホスト名の長さは 15 文字を超えてはなりません。

ドメインで一方向の信頼を構成できますか?

いいえ。クライアントとサーバーは、サーバー側の Citrix SD-WAN WANOP アプライアンスのドメインと双方向の信頼関係を持つドメインのメンバーである必要があります。アプライアンスは一方向の信頼をサポートしていません。

Macintosh Outlook クライアントを使用して、**Citrix SD-WAN WANOP** アプライアンスの高速化のメリットを得ることができますか?

いいえ。MacintoshOutlook は通信プロトコルとして MAPI を使用しません。したがって、この設定では Macintosh Outlook を使用できません。

暗号化された **MAPI** を高速化するために、ブランチ側の **Citrix SD-WAN WANOP** アプライアンスをドメインに参加させる必要がありますか?

いいえ。暗号化された MAPI を高速化するために、ブランチ側の Citrix SD-WAN WANOP アプライアンスをドメインに参加させる必要はありません。

暗号化された **MAPI** 用にデータセンター側の **Windows-Server** で **Citrix SD-WAN WANOP 2000** アプライアンスを構成できますか?

はい。暗号化された MAPI 用にデータセンター側の Windows-Server で Citrix SD-WAN WANOP2000 アプライアンスを構成できます。

Citrix SD-WAN WANOP アプライアンスをドメインに参加させ、異なるタイムゾーンで構成された **NTP** サーバーがネットワーク上に存在する場合、アプライアンスはドメインコントローラーまたは **NTP** サーバーと時刻を同期しますか?

Citrix SD-WAN WANOP アプライアンスをドメインに参加させると、アプライアンスは常に NTP サーバーではなくドメインコントローラーと時刻を同期します。

Citrix SD-WAN WANOP アプライアンスで、ブラックリストに記載されている接続をクリアするためのデフォルトの期間はどれくらいですか?

デフォルトでは、ブラックリストにある接続は 900 秒でクリアされます。

Citrix SD-WAN WANOP アプライアンスでサポートされている **Outlook** 認証メカニズムはどれですか?

リリース 6.2.4 以降、アプライアンスはネゴシエート（デフォルト）および NTLM v2 Outlook 認証をサポートしますが、Kerberos 認証はサポートされていません。ただし、リリース 6.2.3 以前のリリースでは、NegotiateOutlook 認証のみがサポートされています。

Citrix SD-WAN WANOP は **Outlook Anywhere**、**RPC over HTTPS** をサポートしていますか?

はい、リリース 7.3 以降です。

圧縮

April 19, 2021

Citrix SD-WAN WANOP 圧縮の利点は何ですか?

圧縮の基本的なメカニズムはデータストリームを小さくすることですが、これの利点は物事を速くすることです。小さいファイル（または小さいトランザクション）は、転送にかかる時間が短くなります。サイズは関係ありません。圧縮のポイントは速度です。

圧縮効果はどのように測定されますか?

圧縮効果を測定するには、時間と圧縮率の 2 つの方法があります。WAN リンクが主要なボトルネックである場合、この 2 つは関連しています。Citrix SD-WAN WANOP コンプレッサーは非常に高速であるため、データをリアルタイムで圧縮します。5:1 5 分の 1 の時間で転送します。これは、二次的なボトルネックが発生するまで当てはまります。たとえば、クライアントが遅すぎてフルスピードの転送を処理できない場合、5:1 圧縮率は、5:1 スピードアップ。

圧縮はどのように機能しますか?

圧縮エンジンは、以前にリンクを介して転送されたデータを保持し、最新のデータはメモリに保持され、ディスクにははるかに大量に保持されます。以前に転送された文字列が再び検出されると、前のコピーへの参照に置き換えられます。この参照は実際の文字列ではなく WAN を介して送信され、もう一方の端のアプライアンスは参照を検索して出力ストリームにコピーします。

達成可能な最大圧縮率はどれくらいですか?

Citrix SD-WAN WANOP アプライアンスで達成可能な最大圧縮率は約 10,000:1。

予想される圧縮率はどれくらいですか?

全体的な圧縮率は、リンク上のデータストリームを圧縮しようとするすべての試みの平均です。圧縮率が高いものもあれば、まったく圧縮されないものもあります。アプライアンスはサービスクラスを使用して、明らかに圧縮不可能なストリームをコンプレッサーに送信しないようにします。さまざまなタイプのデータに対する圧縮の影響は、次のように異なります。

暗号化された SSH トンネルやリアルタイムのビデオカメラ監視など、一度だけ圧縮または暗号化されたデータ（二度と表示されることはなく、すでに圧縮または暗号化されているストリーム）は、データストリームが 2 回同じになることはないため、圧縮されません。。

圧縮されたバイナリデータまたは複数回表示される暗号化されたデータは、2 回目以降の転送で非常によく圧縮され、これらの以降の転送では圧縮率が数百から数千対 1 の範囲になります。最初の転送では、圧縮されません。このようなデータの平均圧縮率は、データが複数回表示される頻度によって異なります。個々の転送では、圧縮率が 1,000:1, リンク上の圧縮されたバイナリデータの平均 1.5:1 そして 5:1 ほとんどのリンクで、平均以上 10:1 トラフィックの性質に応じて、一部のリンクで。

テキストストリームと uncompressed/unencrypted バイナリデータは最初のパスでも圧縮されます。無関係なテキストでも多くの部分文字列が共通しているため、テキストストリームは適切に圧縮されます。これは、ドキュメント、ソースコード、HTML ページなどに当てはまります。のオーダーの初回通過圧縮 1.5:1 に 4:1 共通しています。2 回目以降のパスでは、圧縮されたバイナリデータとほぼ同じように圧縮されます。(100:1 以上)。非圧縮のバイナリデータは可変ですが、多くの場合、テキストよりも圧縮率が高くなります。非圧縮バイナリデータの例には、CD イメージ、実行可能ファイル、および非圧縮イメージ、オーディオ、およびビデオ形式が含まれます。2 回目以降のパスでは、圧縮されたバイナリデータと同様に圧縮されます。

Citrix Virtual Apps and Desktops のデータは、ファイル転送、プリンター出力、およびビデオで特に圧縮されます。ただし、同じデータストリームが以前にリンクを通過していれば、プロトコルのオーバーヘッドのため、ピーク圧縮はおよそ 40:1, そして平均的な圧縮はの近くにある可能性が高い 3:1。画面の更新などのインタラクティブなデータストリームは、次のオーダーの圧縮結果を提供します。2:1。

キャッシュと圧縮の違いは何ですか?

キャッシュは、名前付きオブジェクト全体をクライアント側アプライアンスに保存します。名前は、ファイルシステムキャッシングの場合はパスとファイル名、Web キャッシングの場合は URL です。同じオブジェクトを別の名前で転送する場合、キャッシュにはメリットがありません。キャッシュされたオブジェクトと同じ名前で、内容がわずかに異なるオブジェクトを転送する場合、キャッシュにはメリットがありません。オブジェクトをキャッシュから提供できる場合、サーバーからフェッチされません。

一方、圧縮にはオブジェクト名の概念がなく、転送内の文字列がすでに圧縮履歴にある文字列と一致する場合は常に利点があります。これは、ファイルをダウンロードする場合、変更することを意味します 1% そのコンテンツの、そして新しいファイルをアップロードすると、あなたは 99:1 アップロード時の圧縮を達成するかもしれません。ファイルをダウンロードしてからリモートサイトの別のディレクトリにアップロードすると、高い圧縮率も達成される可能性があります。圧縮はファイルロックを必要とせず、「古さ」の影響を受けません。オブジェクトは常にサーバーからフェッチされるため、常にバイト単位で正確です。

HTTPS 経由の **RPC**

April 19, 2021

HTTPS 接続を介して **RPC** を高速化するサービスクラスを作成する必要がありますか?

新しいサービスクラスの作成はオプションのタスクです。既存の HTTPS サービスクラスを使用できます。ただし、RPC over HTTPS 接続専用のレポートを作成するには、新しいサービスクラスを作成し、SSL プロファイルをそれにバインドする必要があります。RPC over HTTPS 接続のサービスクラスを作成したくない場合は、作成した SSL プロファイルを Web（Private-Secure）サービスクラスにバインドできます。

RPC over HTTPS アプリケーションのサービスクラスを作成していません。これは、**HTTPS** 接続を介した **RPC** のレポートにどのように影響しますか?

アプライアンスをリリース 7.3 にアップグレードすると、作成された RPC over HTTPS アプリケーションはどのサービスクラスにも属しません。その結果、すべての RPC over HTTPS 接続は、レポートに TCP その他の接続としてリストされます。これらの接続を RPC over HTTPS 接続として分類する場合は、これらのアプリケーションのサービスクラスを作成する必要があります。

アプライアンスに **RPC over HTTPS** のデフォルトのサービスクラスはありますか?

いいえ。アプライアンスにはデフォルトのアプリケーションのみがあり、デフォルトのサービスクラスはありません。アプリケーションのサービスクラスを作成する必要があります。

アプライアンスは、**HTTPS** 接続を介して **RPC** に **SSL** 圧縮の利点を提供しますか?

いいえ。アプライアンスは、HTTP 接続を介した RPC に SSL 圧縮の利点を提供しません。圧縮の利点は、HTTPS トラフィックの暗号化と復号化でのみ利用できます。

MAPI と同様に、アプライアンスは **HTTPS** 接続を介した **RPC** の遅延を最適化しますか?

いいえ。アプライアンスは、RPC over HTTPS の遅延を最適化しません。

MAPI over HTTP は **RPC over HTTPS** とは異なりますか?

はい。MAPI over HTTP は、Microsoft Exchange Server 2013SP1 以降でサポートされる新しいプロトコルです。

クライアント側とサーバー側の **Citrix SD-WAN WANOP** アプライアンスの **RPC over HTTPS** 設定の違いは何ですか?

サービスクラスを作成し、RPC over HTTPS アプリケーションを追加することを除いて、クライアント側の Citrix SD-WAN WANOP アプライアンスで追加の構成を行う必要はありません。

SSL プロファイルを透過プロキシモードで構成するとどうなりますか?

一部の Exchange サーバーでは、TLS セッションチケットのサポートが必要です。透過プロキシモードは TLS セッションチケットをサポートしていないため、これらのサーバーへの接続を高速化するには、分割プロキシを使用して SSL プロファイルを作成する必要があります。

Microsoft Exchange Server に負荷分散の設定を使用する場合、**RPC over HTTPS** サービスクラスを作成するときに、どの宛先 **IP** アドレスをフィルタールールに追加する必要がありますか?

負荷分散アプライアンスを使用している場合は、RPC over HTTP サービスクラスを作成するときに、その仮想 IP（VIP）アドレスをフィルタールールに追加します。

Outlook（**MAPI**）ページで **HTTP** トラフィックを介して **MAP** と **RPC** を区別するにはどうすればよいですか?

Outlook（MAPI）ページに表示されるアプリケーションに基づいてトラフィックを区別できます。たとえば、MAPI および RPC over HTTPS は、次のアプリケーションに使用されます。

- **MAPI**: MAPI および eMAPI
- **HTTPS** 経由の **RPC**: HTTP MAPI、HTTP eMAPI、HTTPS MAPI、および HTTPS eMAPI

SCPS

April 19, 2021

SCPS プロトコルとは何ですか?

Space Communications Protocol Standard（SCPS）プロトコルは、TCP プロトコルの変形です。

SCPS プロトコルの用途は何ですか?

SCPS プロトコルは、衛星通信および同様のアプリケーションで使用されます。

SCPS プロトコルは **Citrix SD-WAN WANOP** アプライアンスでサポートされていますか?

はい。Citrix SD-WAN WANOP アプライアンスは SCPS プロトコルをサポートし、このプロトコルを使用して転送されるデータを高速化します。

SCPS 対応アプライアンスを非 **SCPS** 対応アプライアンスで使用できますか?

はい。SCPS 対応アプライアンスと非 SCPS 対応アプライアンスを混在させる必要がある場合は、不一致が発生しないように展開してください。IP ベースのサービスクラスルールを使用するか、各パスに一致するアプライアンスが含まれるように展開を調整できます。

リンクの一方の端で **SCPS** 対応アプライアンスを使用し、もう一方の端で非 **SCPS** 対応アプライアンスを使用するとどうなりますか?

接続の一方の端にあるアプライアンスで SCPS が有効になっていて、有効になっていない場合、再送信のパフォーマンスが低下します。この状態は、「SCPS モードの不一致」アラートも引き起こします。

SCPS 対応アプライアンスとデフォルトアプライアンスの動作の違いは何ですか?

SCPS 対応とデフォルトのアプライアンスの動作の主な違いは、標準の選択的確認応答（SACK）の代わりに SCPS スタイルの「選択的否定確認応答」（SNACK）が使用されることです。

安全なピアリング

April 19, 2021

安全なピアリングが必要な **Citrix SD-WAN WANOP** 機能はどれですか?

次の機能のいずれかを使用する場合は、リンクの両端で Citrix SD-WAN WANOP アプライアンス間に安全なピアリングを確立する必要があります。

- SSL 圧縮
- 署名された CIFS サポート
- 暗号化された MAPI のサポート

安全なトンネルを構成する前に何かを考慮する必要がありますか?

はい。リンクの両端にある Citrix SD-WAN WANOP アプライアンス間に安全なトンネルを構成する前に、暗号化ライセンスを注文して受け取る必要があります。

リンクの一方の端にあるアプライアンスでセキュアピアリングを有効にするとどうなりますか?

リンクの一方の端にある Citrix SD-WAN WANOP アプライアンスでセキュアピアリングを有効にすると、もう一方のアプライアンスがそれを検出し、SSL シグナリングトンネルを開こうとします。2 つのアプライアンスがこのトンネルを介して相互に正常に認証された場合、アプライアンスは安全なピアリング関係にあります。2 つのアプライアンス間のすべての高速接続は暗号化され、圧縮が有効になります。

パートナーアプライアンスでセキュアピアリングを有効にしないとどうなりますか?

アプライアンスでセキュアピアリングが有効になっている場合、セキュアピア関係がないパートナーとの接続は暗号化または圧縮されませんが、TCP フロー制御アクセラレーションは引き続き使用できます。保護されたパートナーからの圧縮履歴に保存されたデータを保護されていないパートナーと共有できないようにするために、圧縮は無効になっています。

キーストアのパスワードが必要なのはなぜですか?

セキュリティパラメータにアクセスするには、キーストアのパスワードが必要です。このパスワードは管理者のパスワードとは異なり、セキュリティ管理を他のタスクから分離することができます。キーストアのパスワードがリセットされると、既存の暗号化されたデータと秘密鍵はすべて失われます。

アプライアンスが盗まれた場合でもデータを保護するには、アプライアンスを再起動するたびにキーストアのパスワードを再入力する必要があります。これが行われるまで、セキュアピアリングと圧縮は無効になります。

Citrix から受け取った **Citrix SD-WAN WANOP** アプライアンスには、安全なトンネルをセットアップするためのキーと証明書が含まれていますか?

いいえ。Citrix SD-WAN WANOP 製品は、SSL シグナリングトンネルに必要なキーと証明書なしで出荷されます。自分で生成する必要があります。

SSL アクセラレーション

April 19, 2021

加速はトンネルを使用しますか?

いいえ、アクセラレーションは透過的であり、元の接続と同じ IP アドレスとポート番号を使用します。これにより、現在の監視方法を引き続き正常に機能させることができます。

アクセラレーションはパケットストリームをどのように変更しますか?

非圧縮接続の場合、アクセラレーションはパケットの TCP ヘッダーにオプションを追加しますが、パケットペイロードはそのまま残します。これらのオプションにより、接続の両端にある Citrix SD-WAN WANOP デバイスが相互に通信できるようになります。さらに、TCP シーケンス番号は、ルーティングの問題やアプライアンスの障害が同じ接続で加速されたパケットと加速されていないパケットを混合することを防ぐために調整されます。

圧縮接続では、もちろんペイロードが圧縮され、コンプレッサーの出力がフルサイズのパケットに蓄積されます。結果は、たとえば、3:1 圧縮すると、同じ数のパケットではなく、3 分の 1 の数のパケットが送信され、それぞれが 3 分の 1 のサイズに縮小されます。圧縮では、Citrix SD-WAN WANOPTCP ヘッダーオプションとシーケンス番号の調整も使用されます。

加速の基本的な要件は何ですか?

アクセラレーションには、接続の両端に Citrix SD-WAN WANOP デバイスが必要であり、接続は TCP プロトコルを使用する必要があり、接続のすべてのパケットは両方の Citrix SD-WAN WANOP デバイスを通過する必要があります。

Citrix SD-WAN WANOP プラグイン

April 19, 2021

Citrix SD-WAN WANOP プラグインをコンピューターにインストールするためにどのような方法を使用できますか?

次のいずれかの方法を使用して、Citrix SD-WAN WANOP プラグインをコンピューターにインストールできます。

- スタンドアロンインストール：Microsoft インストーラー（msi）ファイルを実行します。
- サイレントインストール：次のコマンドを実行します。

  ```
  *\> msiexec.exe /i path\\CitrixSD-WANWANOPPluginReleasex64-\<
  Release\\_Nunmer\> /qn*
  ```

- リモートインストール：Citrix SD-WAN WANOP プラグインを Citrix Receiver からリモートでインストールします。このインストールは、マーチャンダイジングサーバーを使用して行われます。

Citrix SD-WAN WANOP プラグインインストーラーをカスタマイズできますか?

はい。Citrix SD-WAN WANOP プラグインの msi ファイルを使用して、シグナリング IP アドレスとディスクベースの圧縮（DBC）サイズをカスタマイズできます。

Citrix SD-WAN WANOP プラグインをインストールするための最小ハードウェア要件は何ですか?

Citrix SD-WAN WANOP プラグインの場合、コンピューターは次の要件を満たしている必要があります。

- Pentium4 クラス CPU
- 最小 4GB の RAM
- ハードディスクの空き容量として最低 2GB

Citrix SD-WAN WANOP プラグインをインストールできるオペレーティングシステムはどれですか?

Citrix SD-WAN WANOP プラグインは、次のオペレーティングシステムにインストールできます。

オペレーティングシステム	エディション	バージョン
Windows XP	Home, Professional	32 ビット
Windows Vista	Home Basic, Home Premium, Business, Enterprise, Ultimate	32 ビット
Windows 7	Home Basic, Home Premium, Business, Enterprise, Ultimate	32 ビット、64 ビット
Windows 8	Professional, Enterprise	32 ビット、64 ビット
Windows 10	Professional, Enterprise	32 ビット、64 ビット

Citrix SD-WAN WANOP プラグインをインストールする前に、どのような予防措置を講じる必要がありますか?

Citrix SD-WAN WANOP プラグインをコンピューターにインストールする前に、次の予防措置を講じてください。

- オペレーティングシステムのバージョンに応じて、32 ビットまたは 64 ビットの Citrix SD-WAN WANOP インストーラーバージョンをダウンロードします。
- Citrix SD-WAN WANOP プラグインを圧縮ドライブまたはフォルダーにインストールすることはできません。
- コンピュータに十分な空きディスク容量があることを確認してください。
- Citrix SD-WAN WANOP プラグインリリースをダウングレードすることはできません。以前の Citrix SD-WAN WANOP リリースを使用する場合は、現在のリリースをアンインストールしてから、以前のリリースをインストールする必要があります。

どの **Citrix SD-WAN WANOP** アプライアンスが **Citrix SD-WAN WANOP** プラグインをサポートしていますか?

次の Citrix SD-WAN WANOP アプライアンスは、Citrix SD-WAN WANOP プラグインをサポートしています。

- SD-WAN WANOP 2000
- Windows Server を搭載した SD-WAN WANOP 2000 アプライアンス
- SD-WAN WANOP 3000
- SD-WAN WANOP 4000
- SD-WAN WANOP 5000

どの **Citrix SD-WAN WANOP** アプライアンスが **Citrix SD-WAN WANOP** プラグインをサポートしていませんか?

次の Citrix SD-WAN WANOP アプライアンスは、Citrix SD-WAN WANOP プラグインをサポートしていません。

- SD-WAN WANOP 400
- SD-WAN WANOP 700
- SD-WAN WANOP 800
- Windows Server を搭載した SD-WAN WANOP 1000

Citrix SD-WAN WANOP プラグインを使用するには、**Citrix SD-WAN WANOP 2000**、**3000**、および **VPX** アプライアンスにコンカレント（**CCU**）ライセンスをインストールする必要がありますか?

はい。Citrix SD-WAN WANOP プラグインを使用するには、Citrix SD-WAN WANOP 2000、3000、および VPX アプライアンスに CCU ライセンスをインストールする必要があります。

Citrix SD-WAN WANOP プラグインを使用するには、**Citrix SD-WAN WANOP 4000** および **5000** アプライアンスに **CCU** ライセンスをインストールする必要がありますか?

いいえ。Citrix SD-WAN WANOP プラグインを使用するために、Citrix SD-WAN WANOP4000 および 5000 アプライアンスに CCU ライセンスをインストールする必要はありません。アプライアンスの基本ライセンスは、Citrix SD-WAN WANOP プラグインがこれらのアプライアンスに接続するのに十分です。

サブネットを高速化するための **Citrix** の推奨事項は何ですか?

サブネットを高速化するには、次のことをお勧めします。

- 絶対に使用しないでください ALL/ALL 加速構成用。要件に基づいてサブネットを指定します。
- Citrix Gateway VIP アドレスのアクセラレーションを構成しないでください。

Citrix SD-WAN WANOP プラグインは **Windows** シンクライアントでサポートされていますか?

いいえ。Citrix SD-WAN WANOP プラグインは、Windows シンクライアントではサポートされていません。

Citrix SD-WAN WANOP プラグインでサポートされている **Citrix Receiver** および **Citrix Gateway** のリリースはどれですか?

Citrix SD-WAN WANOP プラグインは、Citrix Receiver 4.1 および Citrix Gateway10.5 リリースをサポートします。

Citrix SD-WAN WANOP プラグインでサポートされていない **Citrix SD-WAN WANOP** 機能はどれですか?

Citrix SD-WAN WANOP プラグインは、次の Citrix SD-WAN WANOP 機能をサポートしていません。

- ビデオキャッシング
- トラフィックシェーピング
- IPv6

Citrix SD-WAN WANOP プラグインを使用するには、**Citrix SD-WAN WANOP 4000** または **5000** アプライアンスでアクセラレーションルールを構成する必要がありますか?

はい。Citrix SD-WAN WANOP プラグインを使用するには、Citrix SD-WAN WANOP4000 または 5000 アプライアンスでアクセラレーションルールを構成する必要があります。

シグナリングチャネルソースフィルタリングの重要性は何ですか?

シグナリングチャネルソースフィルタリングを使用することにより、特定のサブネットまたは IP アドレスがアプライアンスに接続してアクセラレーションルールをフェッチする機能を許可または拒否できます。拒否された送信元サブネットは、シグナリング接続を確立してトラフィックを高速化できません。

LAN 検出の意義は何ですか?

LAN 検出を有効にすると、Citrix SD-WAN WANOP プラグインとアプライアンスが同じ LAN 上にある場合のトラフィックアクセラレーションが防止されます。アプライアンスの帯域幅制限をローカル接続に適用すると、ローカルトラフィックの速度が低下する可能性があるため、ローカルアクセラレーションは望ましくありません。

トラフィックを加速するために、**Citrix SD-WAN WANOP** プラグインとアプライアンスの間で推奨される最小 **RTT** 値はどれくらいですか?

ローカル LAN 上の RTT（ping 時間）よりも大きいが、リモートユーザーの RTT よりも小さい RTT 値を構成することをお勧めします。ほとんどのネットワークでは、デフォルト値の 20 ミリ秒で十分です。

Citrix SD-WAN WANOP プラグインのアクセラレーションルールを定義する際に考慮すべき条件は何ですか?

Citrix SD-WAN WANOP プラグインのアクセラレーションルールを定義するときは、次の条件を考慮してください。

- アプライアンスに対してローカルであるすべてのサブネットのアクセラレーションルールを定義します。これらのサブネットは、アプライアンスがインストールされているサイトの LAN サブネットです。
- LAN の一部ではない宛先 IP アドレスがある場合は、これらの IP アドレスの除外ルールを追加します。IP アドレスを除外するためのルールが、サブネットのトラフィックを高速化するためのルールよりも前にあることを確認してください。これには、ローカルに見える IP アドレスを持つリモートサイトのサブネットが含まれます。
- VPN を使用してアプライアンスをインラインモードでインストールし、透過モードで動作している場合は、ローカルサイトから発信されたトラフィックやローカルサイト宛てのトラフィックだけでなく、すべてのエンタープライズトラフィックを高速化するようにアプライアンスを構成できます。この場合、高速化された接続は、

Citrix SD-WAN WANOP プラグインと VPN の間のみです。Citrix SD-WAN WANOP プラグインと VPN 間のトラフィックの高速化が最適です。

Citrix SD-WAN WANOP プラグインのクラッシュおよびトレースファイルはコンピューターのどこに保存されますか?

Citrix SD-WAN WANOP プラグインのクラッシュファイルとトレースファイルは、次のフォルダーに保存されます。

- クラッシュファイル：C:/ProgramFiles/Citrix/Citrix SD-WAN WANOP
- トレースファイル：C:/Users/admin/AppData/Local/Temp

Citrix SD-WAN WANOP プラグインはどのようにして高可用性ペアに接続しますか?

Citrix SD-WAN WANOP プラグインは、常に同じシグナリング IP アドレスに接続します。シグナリング IP アドレスは、セカンダリアプライアンスではなく、ハイアベイラビリティペアのプライマリアプライアンスにのみバインドされます。したがって、Citrix SD-WAN WANOP プラグインは、常に高可用性ペアのプライマリアプライアンスに接続します。

Citrix SD-WAN WANOP プラグインはどの展開モードをサポートしていますか?

Citrix SD-WAN WANOP プラグインは、次の展開モードをサポートします。

- インライン。
- WCCP。
- 高可用性。
- NAT 展開の Citrix SD-WAN WANOP プラグイン。
- ICA プロキシを使用した WCCP モードの Citrix SD-WAN WANOP アプライアンスを備えた Citrix SD-WAN WANOP プラグイン。
- Citrix SD-WAN WANOP 4000 または 5000 アプライアンスを備えた Citrix SD-WAN WANOP プラグイン。この展開では、管理ポート (0/1) は管理ネットワークに接続されており、シグナリング IP アドレスは別のネットワーク上にあります。

パケットは透過モードとリダイレクタモードでどのように流れますか?

透過モードでは、Citrix SD-WAN WANOP アプライアンスはパケットの送信元 IP アドレスを変更しません。リダイレクタモードでは、Citrix SD-WAN WANOP アプライアンスがサーバーをプロキシし、パケットの IP アドレスを変更します。

> 注
>
> 実稼働環境では、透過モードをお勧めします。

Citrix SD-WAN WANOP プラグインとアプライアンスの間に安全なトンネルを確立するにはどうすればよいですか?

Citrix SD-WAN WANOP プラグインとアプライアンスの間に安全なトンネルを確立するには、次の手順を実行します。

1. Citrix SD-WAN WANOP プラグインのユーザーインターフェイスで、[証明書] タブを開きます。
2. **CA** 証明書 オプションを選択します。
3. [インポート] をクリックして、関連する CA 証明書をアップロードします。
4. 証明書を保存する証明書ストアを選択します。
5. [クライアント証明書] オプションを選択します。
6. [インポート] をクリックします。
7. 適切な証明書形式を選択し、関連する証明書をアップロードします。
8. 証明書を証明書ストアに保存します。
9. 秘密鍵がパスワードで保護されている場合は、パスワードを入力して秘密鍵を復号化します。
10. 安全なトンネルを確立するには、同じ CA 証明書とキーペアをアプライアンスにアップロードする必要があります。

安全なトンネルが確立されていることを確認するにはどうすればよいですか?

安全なトンネルが確立されていることを確認するには、次の手順を実行します。

1. Citrix SD-WAN WANOP プラグインをインストールしたコンピューターで、次のコマンドを実行します。

   \> telnet localhost 1362

2. コンソールで、次のコマンドを実行します。

   \> showtunnels

   以下は、コマンドの出力例です。[Connected Available] セクションに「secure」というテキストが出力に含まれている場合、セキュアトンネルが確立されています。安全なトンネルが確立されていない場合、テキストはクリアテキストになります。

   ```
   ```
   Showtunnels
   Message Tunnels:
   Connected Available:
   172.16.9.100 auto,secure,client,initiator,configured
   CN: mike.199.130
   ```

   Connected Available : 1
   Clients: 1 peers: 0

   “‘

   Citrix SD-WAN WANOP プラグインの詳細については、[Citrix SD-WAN WANOP プラグイン] (/en-us/citrix-sd-wan-wanop/11-1/wanopt-plug-in.html) を参照してください。

 
   ```

トラフィックシェーピング

April 19, 2021

Citrix SD-WAN WANOP トラフィックシェーピングとは何ですか?

Citrix SD-WAN WANOP トラフィックシェーピングは、ポリシーのグループを使用して、さまざまなリンクトラフィックの優先度を設定し、リンク速度に近いがそれ以下の速度でトラフィックをリンクに送信します。にのみ適用される加速とは異なり TCP/IP トラフィック、トラフィックシェーパーは、リンク上のすべてのトラフィックを処理します。

トラフィックシェーピングの利点は何ですか?

トラフィックシェーピングは、設定したポリシーに従って希少なリンクリソースを使用するため、重要であることがわかっているトラフィックは、重要でないことがわかっているトラフィックよりも多くの帯域幅を受け取ります。

トラフィックシェーパーは **Citrix Virtual Apps and Desktops** のトラフィックとどのように相互作用しますか?

Citrix SD-WAN WANOP デバイスは、Virtual Apps/Virtual Desktops データストリームを解析し、さまざまな種類のトラフィックとその優先度を認識し、優先度の高いトラフィックを優先します。これは、暗号化された ICA ストリームに優先順位を付け、MultiStream ICA のネイティブサポートを提供できる唯一の製品であり、ユーザーのセッションを異なる優先順位の最大 4 つの接続に分割します。

重み付き公平キューイングとは何ですか?

Citrix SD-WAN WANOP アプライアンスは、重み付き公平キューイングを 使用します。これにより、接続ごとに個別のキューが提供されます。均等化キューイングでは、接続が速すぎると、それ自体のキューのみがオーバーフローする可能性があります。他の接続には影響しません。

重み付き公平キューイングと非重み付き公平キューイングの違いは何ですか?

重み付き公平キューイングには、一部のトラフィックに他のトラフィックよりも高い優先度（重み）を与えるオプションが含まれています。重みが 2 のトラフィックは、重みが 1 のトラフィックの 2 倍の帯域幅を受信します。Citrix SD-WAN WANOP 構成では、重みはトラフィックシェーピングポリシーで割り当てられます。

リンク定義とは何ですか?

リンク定義は、定義されたリンクに関連付けられているトラフィック、リンクで受信されるトラフィックを許可する最大帯域幅、およびリンクを介して送信されるトラフィックの最大帯域幅を指定します。この定義では、トラフィックをインバウンドまたはアウトバウンド、および WAN 側または LAN 側のトラフィックとしても識別します。

リンク定義の利点は何ですか?

リンク定義により、アプライアンスは WAN リンクの輻輳と損失を防ぎ、トラフィックシェーピングを実行できます。この定義では、トラフィックをインバウンドまたはアウトバウンド、および WAN 側または LAN 側のトラフィックとしても識別します。アプライアンスを流れるすべてのトラフィックがリンク定義のリストと比較され、最初に一致する定義がトラフィックが属するリンクを識別します。

デフォルトポリシーでサービスクラスを構成していません。ただし、トラフィックシェーピングレポートには、デフォルトポリシーで表される大量のトラフィックが表示されます。何かを間違って構成しましたか?

いいえ。構成に問題はありません。トラフィックシェーピングは、WAN リンクにのみ適用できます。LAN またはその他のリンク上のトラフィックは、デフォルトポリシーで表されます。

たとえば、次のようなサービスクラスを作成する構成について考えてみます。Management_Service_Class, 宛先 IP アドレスとして管理サブネットを持ち、カスタムトラフィックシェーピングポリシーをこのサービスクラスにバインドします。この場合、WAN にトラフィックがない場合、管理トラフィックは次のように分類されます。Management_Service_Class サービスクラスレポートで。ただし、トラフィックシェーピングポリシーレポートには、カスタムトラフィックシェーピングポリシーとして存在すると予想されるデフォルトポリシーのエントリが引き続き存在します。

トラフィックシェーピングポリシーレポートでは、アプライアンスはカスタマイズされたトラフィックシェーピングポリシーを使用しません。Management_Service_Class ポリシーを適用し、デフォルトポリシーを適用します。この混乱を避けるために、他のすべてのオプションをクリアするか、管理インターフェイスの LAN タイプリンクを定義できます。

アップグレード（**OS**）プロセス

April 19, 2021

新しい **WANOP OS** カーネルのアップグレードは、どの **SD-WAN** リリースからサポートされていますか?

Citrix SD-WAN リリース 10.1 以降。

新しい **OS** はすべての **SD-WAN** プラットフォームでサポートされていますか?

はい。OS のアップグレードは、すべての SD-WAN WANOP (VPX、物理、クラウド)、および Premium/Enterprise エディションアプライアンス。

WANOP VPX プロファイルとは (RAM/Disk/vCPU) リリース 10.1 でサポートされていますか?

- 6GB RAM、100GB ディスクおよび 2 つの vCPU
- 6GB RAM、250GB ディスクおよび 2 つの vCPU
- 8GB RAM、500GB ディスクおよび 4 つの vCPU
- 16GB RAM、500GB ディスクおよび 4 つの vCPU

リリース **10.0** 以下で実行されている **WANOP** と **10.1** で実行されている **WANOP** の主な機能の違いは何ですか?

機能	10.0 以前	10.1 以降	コメント
WANOP でのビデオキャッシングのサポート	サポートされています	未サポート	なし
WANOP VPX の最小 RAM 要件	4GB RAM	6GB RAM	なし
WANOP VPX 展開ウィザード	サポートされています	未サポート	なし
プライマリ / WANOP VPX の apA アダプター管理 IP アドレス	DHCP はデフォルトで無効になっています	DHCP はデフォルトで有効になっています	なし
Citrix Hypervisor 上の既存のスタンドアロン WANOP VPX でのアップグレードサポート	サポートされています	サポートされません。新しい SD-WAN10.1XVA イメージをインポートする必要があります	なし
Citrix Hypervisor 6.0 ハイパーバイザーバージョン（7.2.2 以前の出荷時ベースイメージバージョンに同梱されているプラットフォーム）リリース 10.1 を持つ物理 WANOP プラットフォームでのアップグレードサポート	サポートされています	Citrix Hypervisor を 6.5 バージョン（WANOP Citrix Hypervisor 6.5 アップグレードバンドルを使用）にアップグレードし、WANOP 10.1 アップグレードを実行する必要があります。	「構成」GUI をクリックすると、Citrix Hypervisor のバージョンが表示されます。

スタンドアロンの **Citrix Hypervisor**（**WO** ビルド **10.0** 以前）で実行されている **WANOP VPX** を **10.1** バージョンにアップグレードすることはサポートされていますが、そうでない場合はなぜですか?

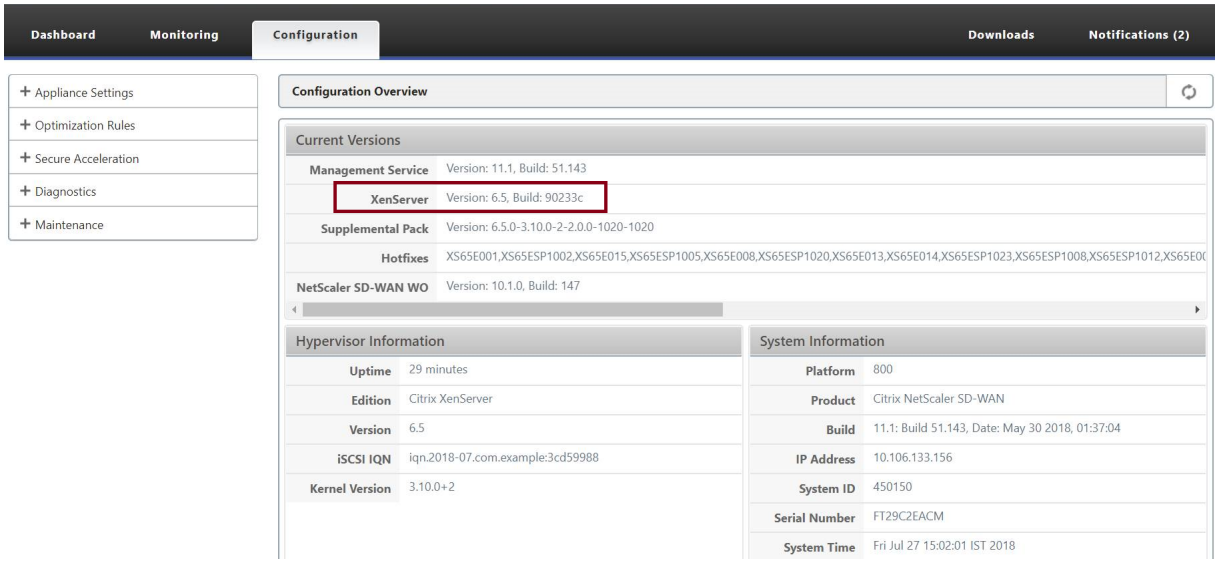
PV から HVM への変換のため、このアップグレードはサポートされていません。XVA イメージを使用して、10.1 Citrix Hypervisor WANOP VPX 上で新しい SD-WAN リリースをプロビジョニングする必要があります。

スタンドアロン **ESXi** で実行されている **WANOP VPX** のアップグレード/ Hyper-V（WO ビルド 10.0 以前）から 10.1 バージョンまでがサポートされていますが、サポートされていない場合は、なぜですか?

このアップグレードはサポートされています。アップグレードする前に、新しい RAM リソース要件の変更に注意してください。

物理アプライアンス（**WANOP** ビルド **10.0** 以前）の **WANOP** を **10.1** バージョンにアップグレードすることはサポートされていますが、サポートされていない場合は、なぜですか?

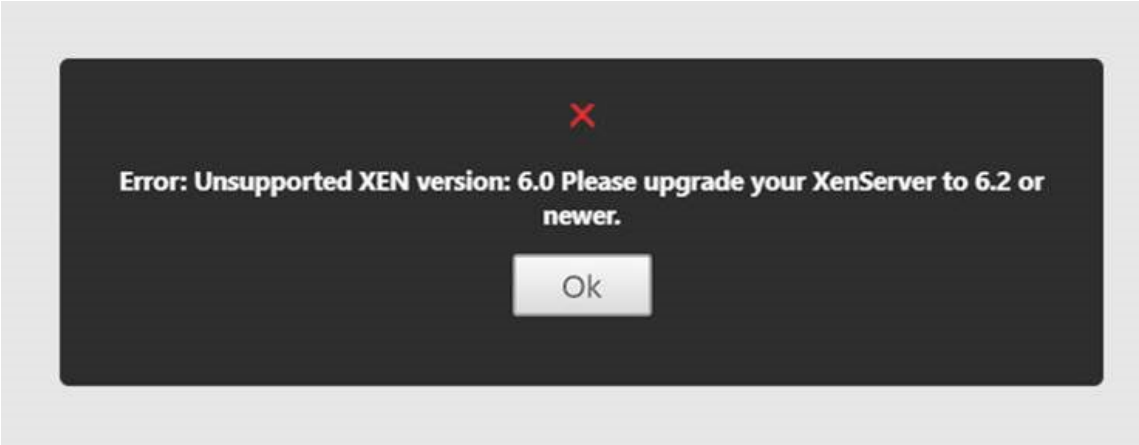
このアップグレードはサポートされています。このアップグレードの前提条件は、（物理 SD-WAN アプライアンス上）をホストする Citrix Hypervisor のバージョン 6.2/6.5 以上のバージョンの Citrix Hypervisor をインストールすることです。これは、[構成] タブを使用して確認できます。



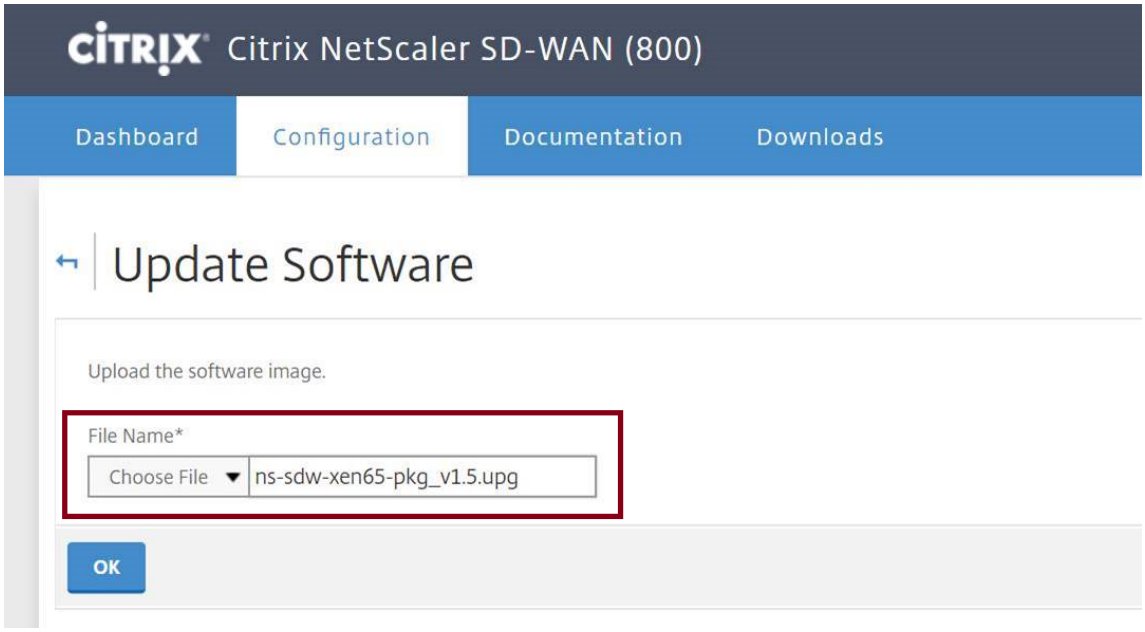
物理 **WANOP** アプライアンスが **Citrix Hypervisor 6.2/6.5** 以降で実行されていない場合、ユーザーは何を実行する必要がありますか?

SD-WAN WO バージョンをアップグレードする前に、Citrix Hypervisor をアップグレードする必要があります。たとえば、以下のユースケースでは、7.2.2（Citrix Hypervisor 6.0 バージョンを持つ）で動作する SD-WAN 800 WANOP プラットフォームをアップグレードすることを計画することを検討しましょう。

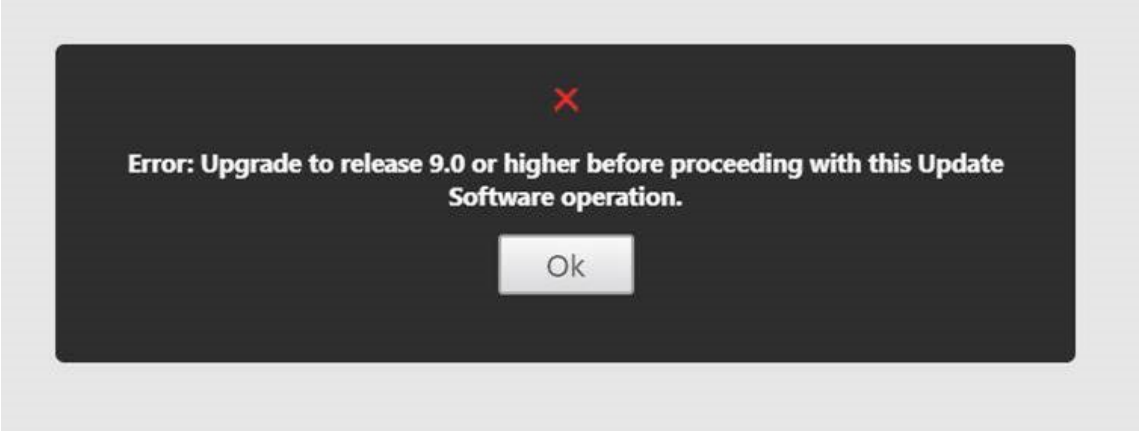
1. このアプライアンスを SD-WAN 10.1 リリースにアップグレードしているときに、次のエラーメッセージが表示されます。



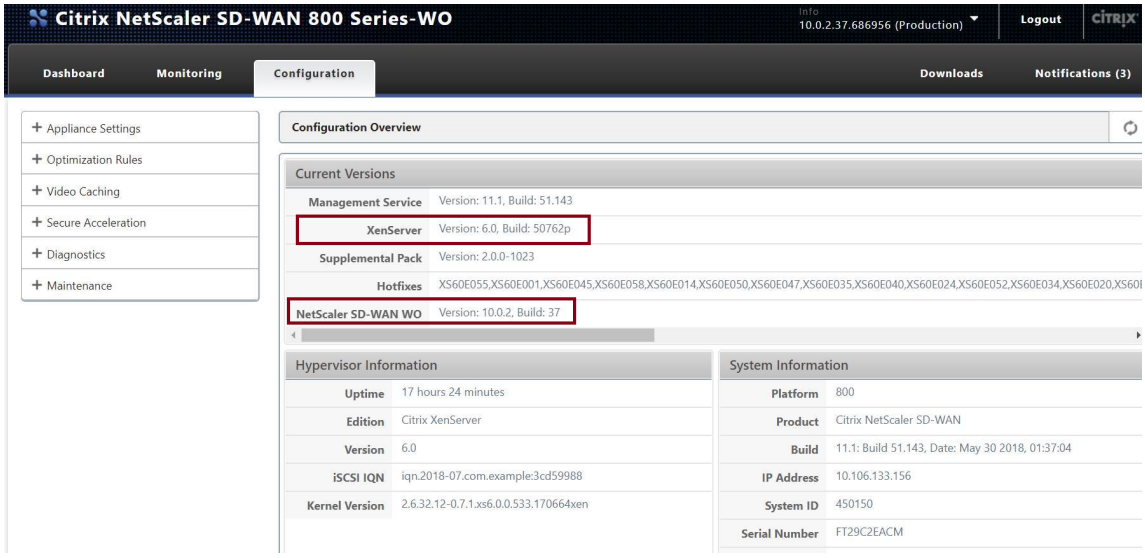
2. 「ns-sdw-xen65-pkg_v1.5.upg」を使用して、Citrix Hypervisor を 6.5 にアップグレードします（これは、Citrix ダウンロード Web サイトからダウンロードできます。



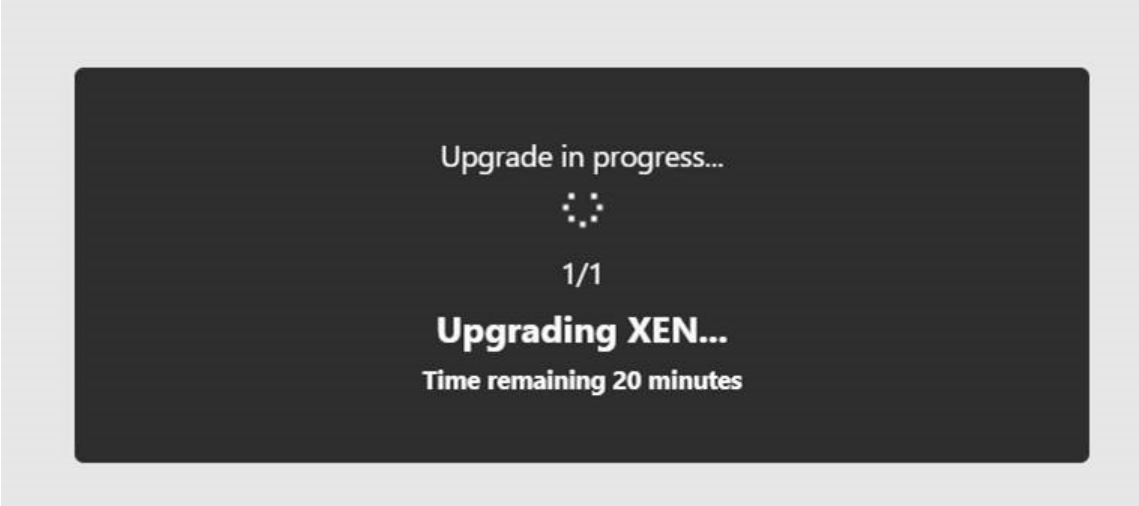
3. SD-WAN WO に 9.0 以降のバージョンがない場合は、Citrix Hypervisor 6.5 へのアップグレードは行われません。以下のエラーメッセージが表示されます。

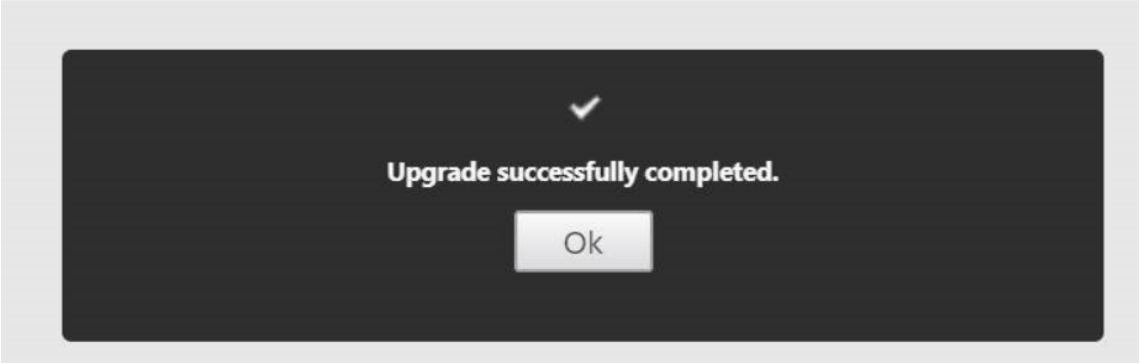


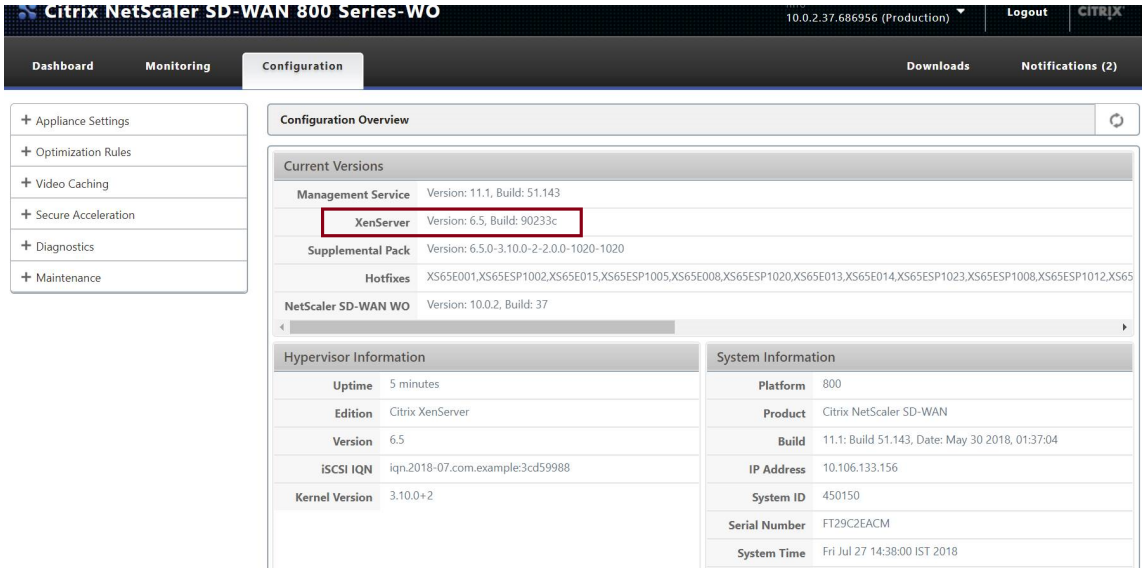
4. ユーザーが WO バージョンを 10.0.2 にアップグレードしたと仮定します。



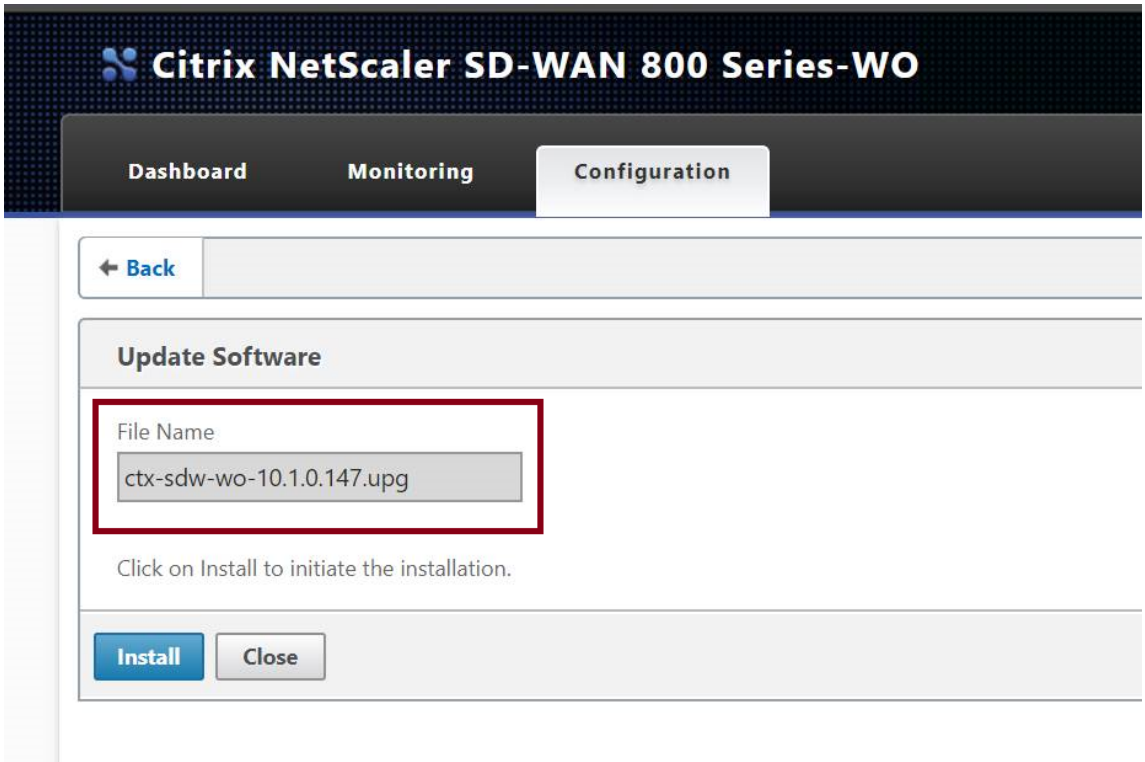
5. ここで、「ns-sdw-xen65-pkg_v1.5.upg」を使用して、Citrix Hypervisor を 6.5 にアップグレードします。

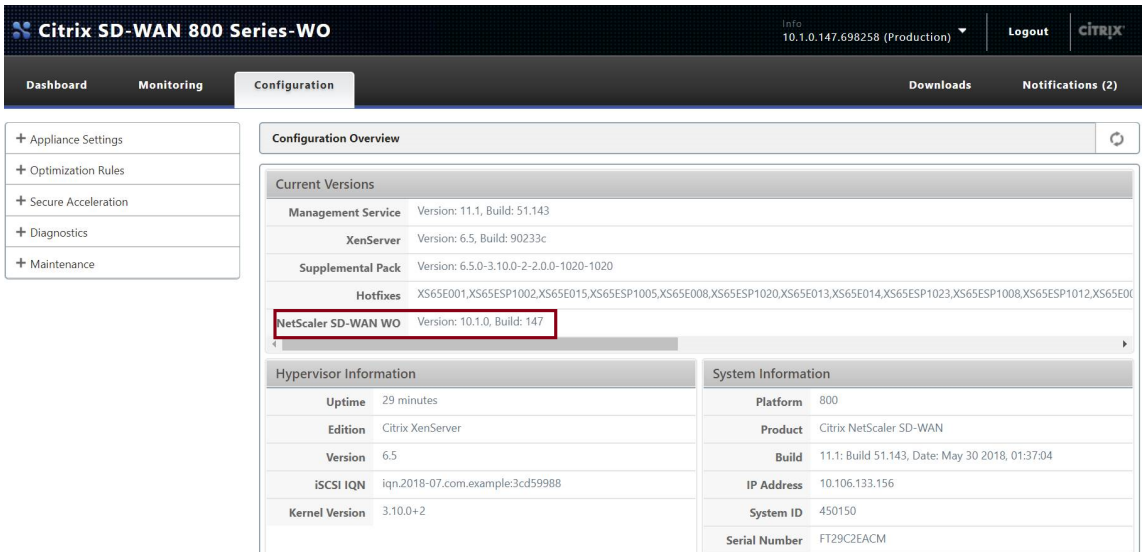






6. 次に、SD-WAN を 10.1 リリースにアップグレードします。





クライアントからサーバーへの **ICMPPing** は正常に機能していますが、**TCP** トラフィックが **WANOP VPX** アプライアンスを通過していません（**WANOP** トラフィック処理を無効にすると正常に機能します）?

クライアント、サーバー、ルーターのファイアウォール設定を確認してください。
WANOP VPX または Client/Server が VM としてホストされている場合は、エンドホスト VM でチェックサムが無効になっていることを確認してください。

```
Linuxコマンドの例：
ethtool -K eth0 tx off
ethtool -K eth0 rx off
```



```
ethtool --offload eth0 tx off
ethtool --offload eth0 rx off
```

両方の WO VPX で「Checksum.SendForceSW」パラメータを有効にして「ON」にする必要があります。

```
例：
Checksum.SendForceSW on
```

SDWAN に変更はありますか SE/EE/WO 新しい WO OS カーネルによるアプライアンスのアップグレードプロセス?

いいえ。

ビデオキャッシング

April 19, 2021

ビデオキャッシングはディスクベースの圧縮とどう違うのですか?

キャッシュを使用すると、キャッシュされたオブジェクトのローカルコピーは、リモートサーバーから再度ダウンロードすることなく、ローカルアプライアンスによって提供されます。キャッシングでは、リンクの両端にアプライアンスは必要ありません。ローカルエンドだけにあります。圧縮を使用すると、オブジェクトのリモートコピーがリモートサーバーによって提供されます。リモート（サーバー側）アプライアンスはそれを圧縮してサイズを縮小し、その結果、伝送速度を上げ、ローカル（クライアント側）アプライアンスはそれを解凍します。

圧縮は、変更されたオブジェクトと変更されていないオブジェクトの両方で機能します。ファイルが変更された場合 1% サーバー上で、次の転送は最大 99:1 圧縮。

キャッシングは、変更されていないオブジェクトでのみ機能します。ファイルが変更された場合 1% サーバーでは、新しいバージョン全体をダウンロードする必要があります。キャッシュされていないものはすべて圧縮され、両方の利点を実現するため、キャッシングと圧縮は補完的なテクノロジーです。

アプライアンスの合計メモリをビデオキャッシュと他の **Citrix SD-WAN WANOP** 機能の間で分割できますか?

いいえ。必要なキャッシュパーティションとメモリは構成できません。

サポートされているビデオコンテナ形式は何ですか?

ビデオキャッシングはコーデック形式に依存せず、すべての主要なコンテナ形式をサポートします。

自分のサイトで内部および外部のエンタープライズビデオのキャッシュをアクティブ化できますか?

はい。これらのビデオへのアクセスが HTTP を介している場合は、これらのサイトをキャッシュ用に構成できます。

キャッシュされたオブジェクトの最大サイズを構成できますか?

はい。構成した制限よりも大きいオブジェクトはキャッシュされません。この制限を設定するには、[構成]> 最適化ルール > ビデオキャッシング と利用可能な制限から値を選択します。

ビデオキャッシングはユーザーエクスペリエンスをどのように改善しますか?

キャッシングにより、特に低速のリンクで複数回表示されるビデオのユーザーエクスペリエンスが向上します。特定のビデオストリームの最初の視聴者はビデオキャッシュ機能の恩恵を受けませんが、その後の視聴は Citrix SD-WAN WANOP アプライアンスから LAN 速度で配信され、WAN の使用量が削減されるという追加のメリットがあります。

さらに、2 番目のユーザーが最初のユーザーにストリーミングされている間に同じビデオを要求すると、2 番目のユーザーはキャッシュされたコピーを受け取ります。

アプライアンスが元の送信元および宛先 IP アドレスを保持する通常の Citrix SD-WAN WANOP TCP 操作とは異なり、アプライアンスはクライアントの送信元アドレスをアクセラレーションブリッジに割り当てられた IP アドレスに置き換えるため、アプライアンスを通過するすべての HTTP トラフィックはアプライアンス自体。

どの **Citrix SD-WAN WANOP** アプライアンスがビデオキャッシングをサポートしていますか?

次のアプライアンスは、ビデオキャッシング機能をサポートしています。

- すべての帯域幅ライセンスモデルを備えた SD-WAN WANOP 800 アプライアンス。
- すべての帯域幅ライセンスモデルを備えた、Windows Server を備えた SD-WAN WANOP1000 アプライアンス。
- すべての帯域幅ライセンスモデルを備えた SD-WAN WANOP 2000 アプライアンス。
- すべての帯域幅ライセンスモデルを備えた、Windows Server を備えた SD-WAN WANOP 2000 アプライアンス。
- すべての帯域幅ライセンスモデルを備えた SD-WAN WANOP 3000 アプライアンス。

ビデオキャッシングの場合、**Citrix SD-WAN WANOP** アプライアンスでサポートされている展開モードはどれですか?

- サポートされている展開-インライン仮想インライン、VLAN、および WCCP
- サポートされていない機能-Citrix SD-WAN WANOP の高可用性、グループモード、およびデイジーチェーン

ビデオキャッシュでサポートされているファイル拡張子はどれですか?

ビデオファイル名には、.3gp、.avi、.dat、.divx、.dvx、.dv-avi、.flv、.fmv、.h264、.hdmov、.m15、.m1v のいずれかの拡張子が必要です。.m21、.m2a、.m2v、.m4e .m4v、.m75、.moov、.mov、.movie、.mp21、mp2v、.mp4、.mp4v、.mpe、.mpeg、mpeg4、mpg、mpg2、。mpv、.mts、.ogg、.ogv、.qt、.qtm、.ra、.rm、.ram、.rmd、.rms、rmvb、.rp、rv、.swf、.ts、.vfw、.vob 、.webm、.wm、.wma、.wmv、および.wtv。

サポートされていない **Citrix SD-WAN WANOP** プラットフォームでビデオキャッシュ機能を有効にできますか?

いいえ。サポートされていないプラットフォームでは、ビデオキャッシュ機能を使用できません。

ビデオキャッシュ機能を有効にするための最小構成およびその他の前提条件は何ですか?

ビデオキャッシュ機能を有効にするには、次のことを行う必要があります。

- 有効な IP アドレスとゲートウェイを apA インターフェイスに割り当て、存在する場合は apB インターフェイスに割り当てます。
- アプライアンスで、www.citrix.com に解決できる有効な DNS サーバーを構成します。
- [選択したビデオキャッシュアプリケーション] リストに少なくとも 1 つのアプリケーションがあります。
- Citrix SD-WAN WANOP GUI 既存の構成アラートの alerts/notification を確認してください。

Citrix SD-WAN WANOP プラグインはビデオキャッシュ機能を使用できますか?

いいえ。Citrix SD-WAN WANOP プラグインでビデオキャッシュ機能を使用することはできません。

サポートされているブラウザとデバイスは何ですか?

ビデオキャッシュは、Internet Explorer、Firefox、および Chrome ブラウザをサポートします。ビデオは、Windows 7 または 8、Apple iPad、および Android iOS デバイスで表示できます。

Citrix SD-WAN WANOP アプライアンスは、すべてのビデオ **Web** サイトのビデオキャッシュをサポートしていますか?

いいえ。ビデオ Web サイトは、ビデオキャッシュ構成ページの [サポートされているアプリケーション] リストから利用でき、追加されます。デフォルトでサポートされているアプリケーションには、YouTube、Vimeo、Youku、Dailymotion、Metacafe が含まれます。URL にランダムな文字を追加するなど、キャッシュ回避メカニズムを使用していない場合は、IP アドレスを指定して他の Web サイトを追加できます。

SNMP 監視はビデオキャッシングでサポートされていますか?

はい。SNMP MIB を使用して、ビデオキャッシング固有のタスクを監視できます。

ビデオキャッシングは非 **HTTP** トラフィックでサポートされていますか?

いいえ。ビデオキャッシングは、HTTP、RTSP、RTMP などの非 HTTP トラフィックではサポートされていません。

ポート **80** 以外のポートに送信された **HTTP** トラフィックでビデオキャッシュを使用できますか?

はい。ビデオキャッシングの場合、カスタマイズされたポートをアプライアンスに追加できます。ビデオキャッシング用にカスタマイズされたポートを追加するには、[構成**]**> 最適化ルール > [ビデオキャッシュ] ページで、[設定] タブの [グローバル設定**]** リンクをクリックします。

Citrix SD-WAN WANOP 圧縮（**HTTP** サービスクラスポリシーを使用）をビデオキャッシングで使用できますか?

はい。キャッシュされたオブジェクトが Citrix SD-WAN WANOP 圧縮履歴とビデオキャッシュの両方に存在する場合、コンテンツはキャッシュヒット時にキャッシュから提供され、キャッシュミス時にサーバーからフェッチ（および圧縮）されます。

透過プロキシがある場合に **IP** アドレス構成を必要とする既存の **HTTP** アプリケーションに変更が必要ですか?

はい。Citrix SD-WAN WANOP は、HTTP 透過プロキシを実行し、パケットの送信元 IP アドレスを置き換えます。したがって、既存の HTTP アプリケーションに特定のポリシー（特定の IP アドレスやプロキシメカニズムをブロックするなど）がある場合は、それらのポリシーを変更する必要があります。

HTTP プロキシ接続のシステムメモリと接続制限は何ですか?

制限を決定するには、Video Caching Debug ページ（support.html）でグラフと統計を確認してください。さらに、Videocaching.cmd statsinfo コマンドに次の情報が表示されることを確認します。

	SD-WAN WANOP 800	Widows サーバーを備えた SD-WAN 1000	Widows サーバーを備えた SD-WAN 2000	SD-WAN 2000	SD-WAN 3000
ディスク	25 GB	25 GB	50 GB	50 GB	99 GB
RAM	375 MB	375 MB	700 MB	700 MB	1024MB
HTTP 接続の合計制限	1000	1000	1500	1500	3000
HTTP 書き込みの最大制限	200	200	300	300	600

上記の HTTP 接続制限に達すると、新しい接続はバイパスされます。

> 注
>
> 上記の構成を変更しないでください。

ビデオキャッシュの監視ページには、ビデオトラフィックのみが含まれていますか?

はい。非ビデオ HTTP トラフィック（プロキシによってインターセプトされた場合でも）は、ビデオキャッシング GUI 統計に含まれません。

Citrix SD-WAN WANOP アプライアンスで有効な **IP** アドレスを使用して **apA** および **apB** インターフェイスを構成する必要がありますか?

いいえ。両方のインターフェースに有効な IP アドレスを割り当てる必要はありません。apA インターフェイスから受信した HTTP パケットは apAIP アドレスでプロキシされ、apB インターフェイスから受信した HTTP パケットは apBIP アドレスでプロキシされます。

インターフェイスの IP アドレスを設定しない場合、そのインターフェイスで受信された HTTP パケットはキャッシュのメリットを享受できません。

キャッシュできるビデオファイルのサイズの最小および最大制限は何ですか?

- 最小：100 KB

- 最大：300 MB
- デフォルト：100 MB

ビデオキャッシングディスクはどのようにクリアされますか?

キャッシュされたオブジェクトは、最近使用されていないアルゴリズムで指定されたとおりにクリアされます。

Citrix SD-WAN WANOP アプライアンスをリリース **6.x** から **7.y** にアップグレードし、ビデオキャッシュを有効にするとどうなりますか?

既存の Citrix SD-WAN WANOP DBC 履歴が失われ、ビデオキャッシュ用の個別のパーティションが作成されます。

Citrix SD-WAN WANOP アプライアンスをリリース **7.y** から **6.x** にダウングレードし、ビデオキャッシュを有効にするとどうなりますか?

Citrix SD-WAN WANOP DBC およびビデオキャッシングの履歴が保持されます。ただし、ビデオキャッシュ機能はリリース 6.x では使用できません。

Citrix SD-WAN WANOP アプライアンスをリリース **7.x** から **7.y** にアップグレードし、ビデオキャッシュを有効にするとどうなりますか?

Citrix SD-WAN WANOP DBC およびビデオキャッシュの履歴が保持されます。

ブランチオフィスに、管理とデータトラフィックを共有する単一のネットワークがあります。このネットワークでビデオキャッシュを構成するにはどうすればよいですか?

管理およびデータトラフィック用の単一ネットワークがある場合は、アクセラレーションブリッジポートの LAN 側にプライマリ IP アドレスを追加することをお勧めします。

同時に実行できる事前入力タスクの最大数はいくつですか?

1。複数の事前入力タスクを同時に開始しようとすると、アプライアンスは先入れ先出し法でタスクのキューを作成します。

アプライアンスで構成できるビデオソースの最大数はいくつですか?

100

アプライアンスに追加できる事前入力エントリの最大数はいくつですか?

50

ディレクトリにリストされたフォルダからダウンロードおよびキャッシュされるビデオファイルの最大数はいくつですか?

300

事前入力機能によって開始されたビデオのダウンロードとキャッシュには、ディスクベースの圧縮（**DBC**）の利点がありますか?

はい。ビデオファイルはキャッシュされているため、ビデオへのアクセスの試行はキャッシュから提供されます。

Office365 アクセラレーション

April 19, 2021

1. なぜ SAN を解析するのですか?

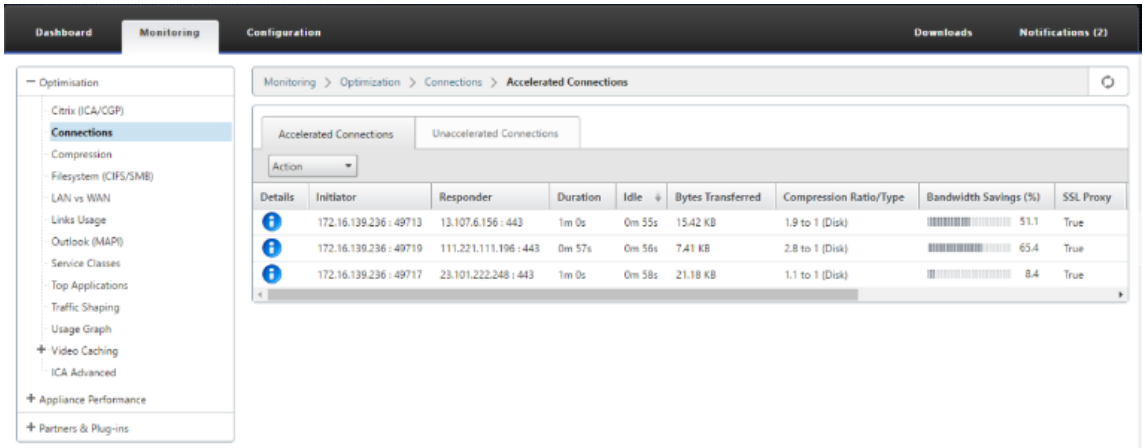
   ドメインごとに FQDN の複数のプロファイルを作成するのは面倒です。これを克服するために、証明書から SAN を解析します。

2. 除外リストとは何ですか?

   エラーまたは警告メッセージが表示されますブラウザまたはアプリに CA 証明書が含まれていない場合、そのような場合、ブラウザまたはアプリからの接続を数回（2〜3 回）試行すると、クライアントの IP アドレスが除外リストに追加されます。次の試行では、接続は SSL プロキシされておらず、エラーや警告なしにページが読み込まれます。クライアント IP アドレスは 48 時間除外リストに残ります。除外リストは、分割プロキシに対してのみ維持されます。

3. Office 365 アクセラレーション接続情報はどこで確認できますか?

   監視 > 接続 > 加速接続に移動し SSL プロキシの状態を確認します。接続の詳細については、詳細アイコンをクリックしてください。



4. SSL プロファイル構成の一部としてリストの除外オプションがデフォルトで有効になっていない場合はどうなりますか?

   ブラウザまたはアプリに CA 証明書が含まれていない場合、エラーまたは警告が表示され、そのクライアントまたはアプリからの接続がブロックされます。このような問題を回避するには、SSL プロファイル構成の一部として [リスト を除外] オプションを選択します。

5. 必要な SAN が configured/created プロキシ証明書の一部でない場合はどうなりますか?

   接続は SSL プロキシされません。また、プロキシされていない SSL 接続のアクセラレーションの利点はありません。

6. クライアントがドメインの一部ではない場合、またはクライアントがドメインのルート証明書を持っていない場合はどうなりますか?

   除外リストが有効になっていない場合、接続はブロックされます。

7. データセンター側の Citrix SD-WAN WANOP にルート CA または中間 CA がない場合はどうなりますか?

   接続がブロックされているか、不足しているルート CA または中間 CA を必要とする Office365 アプリケーションページが部分的に読み込まれています。接続のブロックを解除するか、これらのページを完全にロードするには、適切な CA 証明書を追加するか、SSL プロファイルのアクセラレーションを無効にします。

8. どのクライアントがアクセラレーションから除外されているかを知る方法は?

   除外されたクライアント情報は、ログから、または CLI コマンド *show ssl-exclude-list* を使用して知ることができます。

9. クライアントが除外された場合はどうすればよいですか?

   デフォルトでは、アプライアンスから除外リスト情報は 48 時間後にクリアされます。ユーザーは、CLI コマンド `*clear ssl-exclude-list -\<all\>/\<Client\\_IP\>*`を使用して除外リスト情報を強制的にクリアできます。

10. どの SSL 接続（SNI）がプロキシされていないかを知る方法は?

    ログから、または CLI コマンド *show ssl-non-proxied-sni* を使用して、プロキシされていない SNI のリストを知ることができます。

11. プロキシされていない SNI をクリアする方法は?

    CLI コマンド `*clear ssl-non-proxied-sni -\<all\>/\<server name identifier\>*`を使用します。

12. 除外状態のクライアントのデフォルトの時間はどれくらいですか?

    クライアントは 48 時間除外状態のままです。

13. 特定のサービスクラスに複数のプロファイルを適用できますか?

    はい、複数の SSL プロファイルを持つサービスクラスを適用できます。

    これを行うには、仮想 WAN アプライアンスで [構成**]>** サービスクラス **>Web**（インターネット**-**セキュア）> 編集 > （アプリケーション）を編集し、利用可能なプロファイルを追加します。

14. プロキシされていない接続の理由をどのように確認しますか?

    TCP 接続ページを確認してください。詳細については、ログを確認してください。プロキシされていない接続の問題をデバッグするには、次の手順を実行します。

    a) ログに有効な構成が表示されない場合-有効な構成を設定します。Office 365 機能の構成の詳細については、Office365 アクセラレーションを参照してください。

    b) ログに認証検証が失敗したことが示されている場合-有効な CA 証明書をデータセンター側の Citrix SD-WAN WANOP アプライアンスに追加します。

c) ログにクライアントが除外されていることが示されている場合-除外されたクライアントに関する情報は、CLI コマンド *`clear ssl-exclude-list -\<all\>/\<Client\\_IP\>`*を使用してアプライアンスからクリアできます。

その他の注意事項

- OneDrive クライアントにログを記録すると、「誤った警告」という警告メッセージが表示されることがあります。これは Microsoft（https://support.microsoft.com/en-us/kb/3097938 ）の既知の問題であり、Citrix SD-WAN WANOP アプライアンスに固有のものではありません。
- プロキシされる Office365 リダイレクトページの場合、リダイレクトされたページの証明書に対応する SAN リストを含む別のプロキシ証明書を作成することをお勧めします。このプロキシ証明書を使用して別のプロファイルを作成し、サービスクラスに適用します。また、Citrix SD-WAN WANOP アプライアンスに関連する CA を追加します。
- ブラウザに正しい CA 証明書が表示されない場合があります。そのような場合は、Wireshark または OpenSSL を使用してルートおよび中間 CA 名を取得し、「本物の」ソース（たとえば、Windows SSL ストア）から証明書を取得します。
- ブラウザーの動作の違いは、必要な証明書がなく、[リストの除外] オプションが無効になっているさまざまなブラウザーから Office365 アプリケーションにアクセスするときに観察されます。
- Office 365 接続が SSL プロキシされ（つまり、SSL プロキシが True に設定されている）、ブラウザーでプロキシ証明書の代わりに Office 365 証明書が表示される場合は、ブラウザーを非認識モードで開き、動作を確認するか、キャッシュをクリアすることをお勧めします。その後、動作を再度確認します。
- Microsoft Office 365 には、OneDrive、Outlook、SharePoint、Word、PPT、Excel、OneNote などの多くのコンポーネントとアプリケーションが含まれています。これらのアプリケーションはすべてテスト済みであり、問題なく動作することがわかっています。他のアプリケーションも問題なく動作することが期待されます。ただし、このステータスは時間の経過とともに変化する可能性があり、不明な問題が発生する可能性があります。

圧縮

April 19, 2021

Citrix SD-WAN WANOP 圧縮は、画期的なテクノロジーを使用して、透過的なマルチレベル圧縮を提供します。任意のバイトストリームに作用するのは真の圧縮です。これはアプリケーションに対応しておらず、接続境界に影響されず、データに 2 回目に表示されるときに文字列を最適に圧縮できます。Citrix SD-WAN WANOP 圧縮は、任意のリンク速度で機能します。

圧縮エンジンは非常に高速であるため、圧縮のスピードアップ係数を圧縮比に近づけることができます。たとえば、1.5 Mbps の T1 リンクを独占し、100:1 WAN 帯域幅が転送の唯一のボトルネックである場合、圧縮率はほぼ 100 倍、つまり 150Mbps のスピードアップ率を実現できます。

ほとんどの圧縮方法とは異なり、Citrix SD-WAN WANOP の圧縮履歴は、同じ 2 つのアプライアンス間を通過するすべての接続間で共有されます。接続 A によって数時間、数日、または数週間前に送信されたデータは、後で接続 B によって参照され、圧縮による完全な高速化のメリットを享受できます。結果として得られるパフォーマンスは、従来の方法で達成できるよりもはるかに高くなります。

圧縮では、アプライアンスのディスクとメモリを使用して、最大テラバイトの圧縮履歴を提供できます。

圧縮のしくみ

すべての圧縮アルゴリズムは、圧縮するデータをスキャンして、以前に送信された文字列と一致するデータの文字列を検索します。そのような一致が見つからない場合、リテラルデータが送信されます。一致するものが見つかった場合、一致するデータは前のオカレンスへのポインターに置き換えられます。非常に大きな一致する文字列では、メガバイトまたはギガバイトのデータを数バイトのみを含むポインターで表すことができ、それらの数バイトのみをリンク経由で送信する必要があります。

圧縮エンジンは、圧縮履歴のサイズによって制限されます。LZS や ZLIB などの従来の圧縮アルゴリズムは、64KB 以下の圧縮履歴を使用します。Citrix SD-WAN WANOP アプライアンスは、少なくとも 100GB の圧縮履歴を維持します。Citrix SD-WAN WANOP アルゴリズムは、従来のアルゴリズムの 100 万倍を超える圧縮履歴を使用して、より多くの一致とより長い一致を検出し、優れた圧縮率を実現します。

Citrix SD-WAN WANOP 圧縮アルゴリズムは非常に高速であるため、エントリーレベルのアプライアンスでもコンプレッサーの出力で 100 MbpsLAN を飽和させることができます。最高性能のモデルは、1Gbps をはるかに超えるスループットを実現できます。

ペイロードデータのみが圧縮されます。ただし、ヘッダーは間接的に圧縮されます。たとえば、接続が達成された場合 4:1 圧縮では、4 つのフルサイズの入力パケットごとに 1 つのフルサイズの出力パケットのみが送信されます。したがって、ヘッダーデータの量も次のように削減されます。4:1。

汎用最適化としての圧縮:

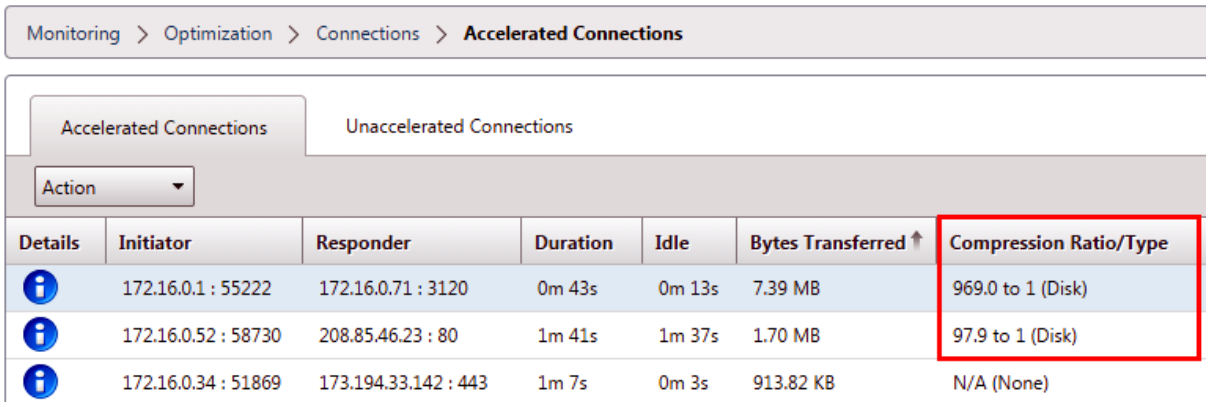
Citrix SD-WAN WANOP 圧縮は、アプリケーションに依存しません。暗号化されていない TCP 接続からのデータを圧縮できます。

キャッシングとは異なり、圧縮パフォーマンスはデータの変更に直面しても堅牢です。キャッシュでは、ファイルの 1 バイトを変更すると、キャッシュ内のコピー全体が無効になります。圧縮では、ファイルの途中で 1 バイトを変更すると、1 バイトの不一致データで区切られた 2 つの大きな一致が作成されるだけで、結果の転送時間は以前よりわずかに長くなります。そのため、変化量に応じて圧縮率が緩やかに低下します。ファイルをダウンロードする場合は、1% それの、そしてそれをもう一度アップロードして、99:1 アップロード時の圧縮率を期待してください。

大きな圧縮履歴のもう 1 つの利点は、事前に圧縮されたデータが Citrix SD-WAN WANOP テクノロジで簡単に圧縮されることです。たとえば、JPEG 画像や YouTube ビデオは事前に圧縮されているため、リンクを介して最初に送

信されるときに追加の圧縮が行われる可能性はほとんどありません。ただし、最初に FTP で送信され、次に HTTP で送信されるなど、異なるユーザーまたは異なるプロトコルで送信された場合でも、再送信されるたびに、転送全体がほんの数バイトに削減されます。

実際には、圧縮パフォーマンスは、リンクを通過するデータの量が、以前にリンクを通過したデータと同じであるかどうかに依存します。金額は、アプリケーションごと、日ごと、さらには瞬間ごとに異なります。アクティブな加速接続のリストを見るときは、1:1 から 10,000:1 の比率が表示されることを期待してください

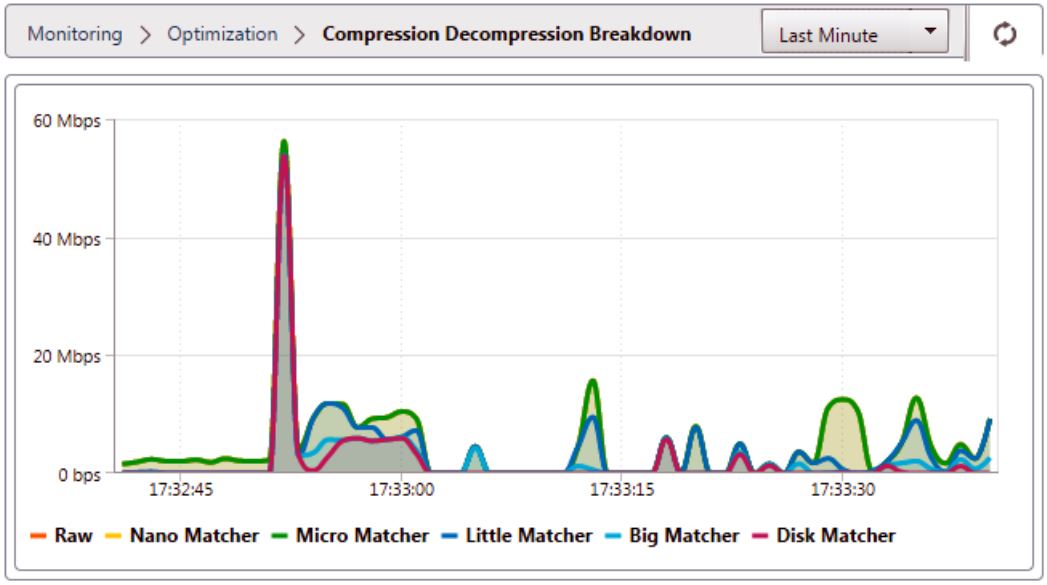


暗号化されたプロトコルを圧縮する:

圧縮パフォーマンスが低いことを示す多くの接続は、暗号化されているためにそうなります。暗号化されたトラフィックは通常圧縮できませんが、Citrix SD-WAN WANOP アプライアンスは、アプライアンスがセキュリティインフラストラクチャに参加するときに暗号化された接続を圧縮できます。Citrix SD-WAN WANOP アプライアンスは、Citrix Virtual Apps and Desktops とセキュリティインフラストラクチャに自動的に結合し、手動構成で SSL、Windows ファイルシステム（CIFS/SMB）、および Outlook/Exchange（MAPI）サーバーのセキュリティインフラストラクチャに参加できます。

適応型のゼロ構成操作:

さまざまな種類のトラフィックのさまざまなニーズに対応するために、Citrix SD-WAN WANOP アプライアンスは 1 つではなく 5 つの圧縮エンジンを使用するため、最も大規模なバルク転送から最も遅延の影響を受けやすいインタラクティブトラフィックまですべてのニーズに簡単に対応できます。圧縮エンジンは、個々の接続の変化するニーズに動的に一致するため、圧縮は自動的に最適化されます。追加の利点は、圧縮エンジンが構成を必要としないことです。



メモリベースの圧縮

ほとんどの圧縮エンジンは、RAM を使用して圧縮履歴を保存します。これは、メモリベースの圧縮と呼ばれます。一部のアプライアンスは、これらの圧縮エンジンにギガバイトのメモリを割り当てます。メモリベースの圧縮はレイテンシーが低く、仮想アプリ/仮想デスクトップトラフィックなどの対話型タスクでは自動的に選択されます。

ディスクベースの圧縮

ディスクベースの圧縮エンジンは、数十ギガバイトからテラバイトのメモリを使用して圧縮履歴を保存し、より多くのより良い圧縮の一致を可能にします。ディスクベースの圧縮エンジンは非常に高速ですが、メモリベースのエンジンよりも待ち時間が長くなることがあり、バルク転送用に自動的に選択されることがよくあります。

圧縮を有効または無効にする

圧縮は、サービスクラスごとに、[構成：サービスクラス] ページで有効になります。このページには、各サービスクラスのプルダウンメニューがあり、次のオプションがあります。

- ディスク。これは、ディスクベースの圧縮とメモリベースの圧縮の両方が有効になっていることを意味します。このオプションを無効にする特別な理由がない限り、このオプションを選択する必要があります。
- メモリ。つまり、メモリベースの圧縮は有効になっていますが、ディスクベースの圧縮は有効になっていません。両方のタイプの圧縮が有効になっている場合、アプライアンスはメモリまたはディスクを自動的に選択するため、この設定が使用されることはめったにありません。
- **Flow-Control Only**。これは圧縮を無効にしますが、フロー制御の加速は有効にします。常に暗号化されるサービス、および FTP 制御チャネルの場合は、このオプションを選択します。

- なし。つまり、圧縮とフロー制御の両方が無効になっています。

詳しくは、「サービスクラス」を参照してください。

ディスクベースの圧縮パフォーマンスを測定する

レポート：圧縮ページの圧縮ステータス] タブには、システムが起動してから、または [クリア] ボタンを使用して統計をリセットしてからのシステム圧縮パフォーマンスが報告されます。個々の接続の圧縮は、システムログの接続閉鎖メッセージで報告されます。

圧縮パフォーマンスは、データストリームの冗長性の量や、程度は低いもののデータプロトコルの構造など、さまざまな要因によって異なります。

FTP などの一部のアプリケーションは、純粋なデータストリームを送信します。TCP 接続ペイロードは、常に元のデータファイルとバイト単位で同一です。CIFS や NFS などの他のものは、純粋なデータストリームを送信しませんが、コマンド、メタデータ、およびデータを同じストリームに混在させます。圧縮エンジンは、接続ペイロードをリアルタイムで解析することにより、ファイルデータを区別します。このようなデータストリームは、次の圧縮率を簡単に生成できます。2 回目のパスで 100:1 および 10,000:1 。

リンクの平均圧縮率は、長い一致、短い一致、および一致なしの相対的な普及率によって異なります。この比率はトラフィックに依存し、実際に予測することは困難です。

テスト結果は、全体としてマルチレベル圧縮の効果を示しており、メモリベースとディスクベースの圧縮がそれぞれ貢献しています。

ディスクベースの圧縮に使用できるストレージスペースがいっぱいになり、新しいデータと一致する以前のデータの最大量が提供されるまで、最大の圧縮パフォーマンスは達成されません。完璧な世界では、定常状態の動作に到達したことを確認するために、アプライアンスのディスクがいっぱいになるだけでなく、少なくとも 1 回はいっぱいになり、上書きされるまで、テストは終了しません。ただし、これほど多くの代表的なデータを自由に使用できる管理者はほとんどいません。

パフォーマンステストのもう 1 つの問題は、アクセラレーションによってネットワーク内の弱いリンク、通常はクライアント、サーバー、または LAN のパフォーマンスが明らかになることが多く、これらが期待外れのアクセラレーションパフォーマンスと誤診されることがあることです。

予備テストと初期テストには、Iperf または FTP を使用できます。Iperf は予備テストに役立ちます。非常に圧縮性が高く（最初のパスでも）、2 つのエンドポイントシステムで CPU を比較的少なく使用し、ディスクリソースを使用しません。Iperf を使用した圧縮パフォーマンスでは、両側の LAN がギガビットイーサネットを使用している場合は T1 リンクを介して 200 Mbps 以上、エンドポイントとアプライアンス間の LAN パスにファストイーサネット機器がある場合は 100Mbps 未満を送信する必要があります。

Iperf はアプライアンスにプリインストールされており（[診断] メニューの下）、http://iperf.sourceforge.net/から入手できます。理想的には、エンドポイントシステムからインストールして実行し、アプライアンス間だけでなく、エンドツーエンドでネットワークをテストする必要があります。

FTP は、Iperf で可能なテストよりも現実的なテストに役立ちます。FTP はシンプルでなじみがあり、その結果は簡単に解釈できます。2 回目のパスのパフォーマンスは、Iperf の場合とほぼ同じである必要があります。そうでない場合、制限要因はおそらくエンドポイントシステムの 1 つのディスクサブシステムです。

ディスクベースの圧縮システムをテストするには:

1. ディスクベースの圧縮を有効にして、2 つのアプライアンス間で数ギガバイトのデータストリームを転送します。この転送中に達成された圧縮に注意してください。データの性質によっては、最初のパスでかなりの圧縮が見られる場合があります。
2. 同じデータストリームをもう一度転送し、圧縮への影響に注意してください。

プレミアムエディションの圧縮レポート

Citrix SD-WAN Premium（Enterprise）エディションには、プロトコルまたはアプリケーションの関連付けがある WANOP サービスクラスを介して、プロトコルまたはアプリケーションごとに圧縮レポートを表示するためのビューがありません。Premium（Enterprise）エディションのアプライアンスを使用している場合、圧縮に使用できるレポートは、プロトコルが最適化または圧縮されている範囲を可視化しない接続レベルの圧縮レポートのみです。圧縮レポートは、WAN 最適化 GUI で利用できます。この GUI には、すべての固有のプロトコルの内訳と、一定期間にレポートがどのように最適化されたかが表示されます。

Citrix SD-WAN Premium（Enterprise）Edition アプライアンス GUI では、WAN 最適化のために、WAN 最適化ダッシュボードの下に次のウィジェットが追加されています。

- 統合された圧縮率–WANOP アプライアンスを通過するすべてのトラフィックと、加速および非加速接続の総数。これにより、LAN から WAN に送信されるトラフィックの合計を監視できます。
- 圧縮率-上位 10 のサービスクラス。
- 集約リンクスループット–LAN および WAN。

統合圧縮率:

このレポートには、WANOP に送信されたすべてのトラフィックの統合された圧縮率と、加速された接続と加速されていない接続の総数が表示されます。また、アプライアンスの WANOP サービスの稼働時間を示します。

集約されたリンクスループット:

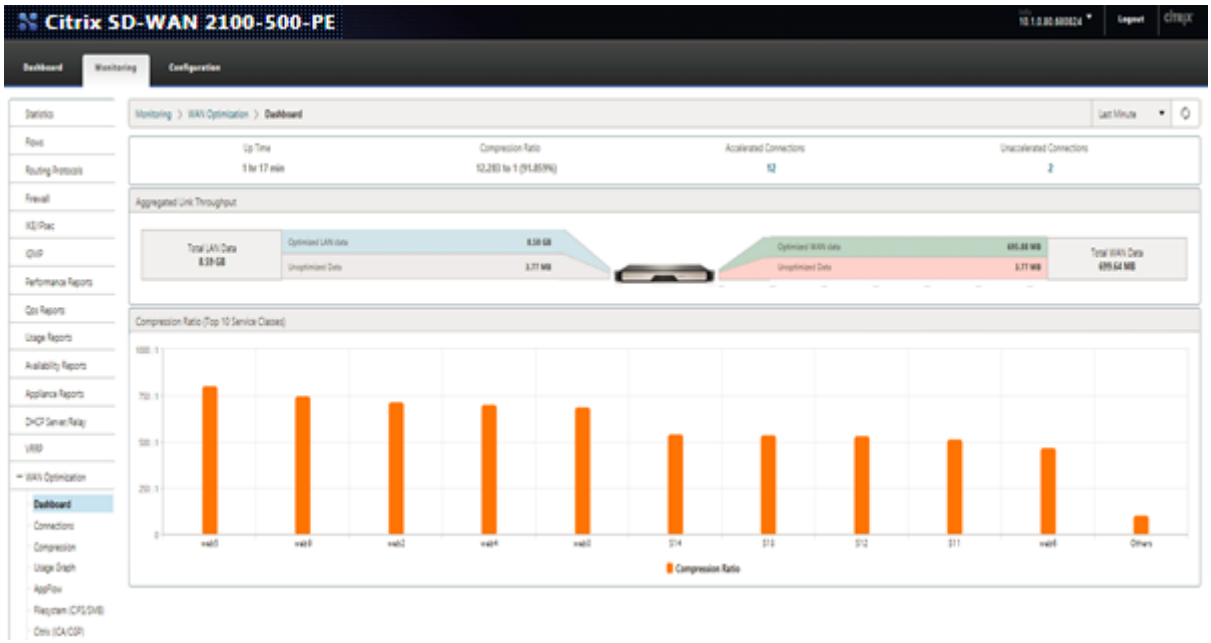
このレポートには、WANOP に送信される合計トラフィックと、両端の最適化されたデータと最適化されていないデータのカテゴリに分割して送信される合計トラフィックが表示されます。

圧縮率（上位 **10** のサービスクラス）:

Citrix SD-WAN アプライアンス GUI で、[監視]>**WAN** 最適化に移動して、接続の詳細と圧縮率（サービスクラスダッシュボードごと）を確認できます。この自動はダッシュボードノードを選択し、ダッシュボードの形式で概要を提供します。

グラフには、サービスクラス別に分類されたトラフィックの圧縮率の上位 10 個の値が表示されます。

追加の「その他」バーが表示されます。これは、上位 10 のサービスクラスの圧縮率レポートに加えて、システムの一部である他のすべての高速接続の圧縮率を示します。



HTTP アクセラレーション

April 19, 2021

Citrix SD-WAN WANOP アクセラレーターは、さまざまなゼロ構成最適化を使用して HTTP トラフィックを高速化します。これにより、HTTP プロトコル（ファイルのダウンロード、ビデオストリーミング、自動更新など）を使用して Web ページやその他のアプリケーションが高速化されます。

HTTP を加速する最適化には、圧縮、トラフィックシェーピング、フロー制御、およびキャッシングが含まれます。

圧縮

HTTP は、Citrix SD-WAN WANOP マルチレベル圧縮に最適なアプリケーションです。

標準の HTML ページ、画像、ビデオ、バイナリファイルなどの静的コンテンツは、通常、さまざまな量の初回通過圧縮を受け取ります。事前に圧縮されたバイナリコンテンツ 1:1 、およびテキストベースのコンテンツについては 2:1 かそれ以上。オブジェクトが 2 回目に表示されたときから、2 つの最大の圧縮エンジン（メモリベースの圧縮とディ

スクベースの圧縮）は非常に高い圧縮率を提供し、より大きなオブジェクトは次の圧縮率を受け取ります。1,000:1 以上。このような高い圧縮率では、WAN リンクが制限要因ではなくなり、サーバー、クライアント、または LAN がボトルネックになります。

アプライアンスはコンプレッサーを動的に切り替えて、最大のパフォーマンスを提供します。たとえば、アプライアンスは HTTP ヘッダーで小さいコンプレッサーを使用し、HTTP ボディで大きいコンプレッサーを使用します。

HTTP ヘッダーや動的に生成されたページ（2 回同じになることはないが、互いに類似しているページ）を含む動的コンテンツは、より小さな一致を処理する 3 つの圧縮エンジンによって圧縮されます。ページを初めて表示するときは、圧縮が適切です。前のページのバリアントが見られる場合は、圧縮の方が優れています。

トラフィックシェーピング

HTTP は、インタラクティブトラフィックとバルクトラフィックの組み合わせで構成されています。すべてのユーザーのトラフィックは両方が混在しており、同じ接続に両方が混在している場合があります。トラフィックシェーパーは、各 HTTP 接続がリンク帯域幅の公平なシェアを取得することをシームレスかつ動的に保証し、バルク転送がインタラクティブユーザーを犠牲にしてリンクを独占することを防ぎます。また、バルク転送がインタラクティブ接続が使用しない帯域幅を取得することを保証します。

フロー制御

高度な再送信アルゴリズムおよびその他の TCP レベルの最適化により、応答性が維持され、遅延や損失が発生しても転送速度が維持されます。

ビデオキャッシング

ビデオファイルの HTTP キャッシングは、リリース 7.0 で導入されました。キャッシングには、HTTP オブジェクトをローカルストレージに保存し、サーバーからリロードせずにローカルクライアントに提供することが含まれます。

キャッシュと圧縮の違いは何ですか? キャッシングは圧縮と同様のスピードアップを提供しますが、2 つの方法は異なり、補完的です。

- 圧縮により、リモートサーバーからの転送が高速化されます。圧縮が存在しない場合、この高いデータレートにより、サーバーに高い負荷がかかる可能性があります。キャッシュはサーバーからの転送を防ぎ、サーバーの負荷を軽減します。
- 圧縮は、以前の転送と同様に、どのデータストリームでも機能します。リモートサーバー上のファイルの名前を変更して再度転送すると、圧縮は完全に機能します。キャッシュは、クライアントによって要求されているオブジェクトとディスク上のオブジェクトが同一であることがわかっている場合にのみ機能します。リモートサーバー上のファイルの名前を変更して再度転送すると、キャッシュされたコピーは使用されません。

- 圧縮されたデータは、サーバーが送信できるよりも速く配信することはできません。キャッシュされたデータは、クライアント側のアプライアンスの速度にのみ依存します。
- 圧縮は CPU に負荷がかかります。キャッシングはそうではありません。

HTML5 のしくみ

April 19, 2021

HTML5 は HTTP を使用します。これは request/response クライアントとサーバー間の通信用のプロトコル。クライアントは TCP 接続を開始し、それを使用して HTTP 要求をサーバーに送信します。サーバーは、使用可能なリソースへのアクセス権を付与することにより、これらの要求に応答します。クライアントとサーバーが接続を確立した後、それらの間で交換されるメッセージには WebSocket ヘッダーのみが含まれ、HTTP ヘッダーは含まれません。

HTML5 のインフラストラクチャは WebSocket で構成されており、WebSocket は、既存の HTTP インフラストラクチャをさらに使用して、クライアントと Web サーバー間の通信のための軽量メカニズムを提供します。通常、WebSocket プロトコルはブラウザーと Web サーバーに実装します。ただし、このプロトコルは任意のクライアントまたはサーバーアプリケーションで使用できます。

クライアントが WebSockes を使用して接続を確立しようとすると、Web サーバーは WebSocket ハンドシェイクをアップグレード要求として扱い、サーバーは WebSocket プロトコルに切り替えます。WebSocket プロトコルにより、ブラウザーと Web サーバー間の頻繁な対話が可能になります。したがって、このプロトコルは、株価指数やスコアカードなどのライブ更新、さらにはライブゲームにも使用できます。これは、クライアントブラウザとサーバー間の双方向の継続的な通信のためのオープン接続を維持しながら、サーバーが一方的な応答をクライアントに送信するための標準化された方法のために可能です。

> 注
>
> また、Comet などの他のさまざまなテクノロジーを使用して、標準化されていない方法でこの効果を実現することもできます。Comet の詳細については、http://en.wikipedia.org/wiki/Comet_(programming)を参照してください。

WebSocket プロトコルは、TCP ポート 80 および 443 を介して通信します。これにより、ファイアウォールを使用して Web 以外のインターネット接続をブロックする環境での通信が容易になります。さらに、WebSocket には独自の断片化メカニズムがあります。WebSocket メッセージは、複数の WebSocket フレームとして送信できます。

> 注
>
> サーバー上の Web アプリケーションが WebSocket をサポートしていない場合、WebSocket を使用することはできません。

HTML5 が webSocket セッションを確立する方法

HTML5 をサポートするブラウザーは、JavaScriptAPI を使用して次のタスクを実行します。

- WebSocket 接続を開きます。
- WebSocket 接続を介して通信します。
- WebSocket 接続を閉じます。

WebSocket 接続を開くために、ブラウザーは WebSocket プロトコルに切り替えるための HTTP アップグレードメッセージをサーバーに送信します。サーバーは、この要求を受け入れるか拒否します。以下は、サンプルのクライアント要求とサーバー応答のスニペットです。

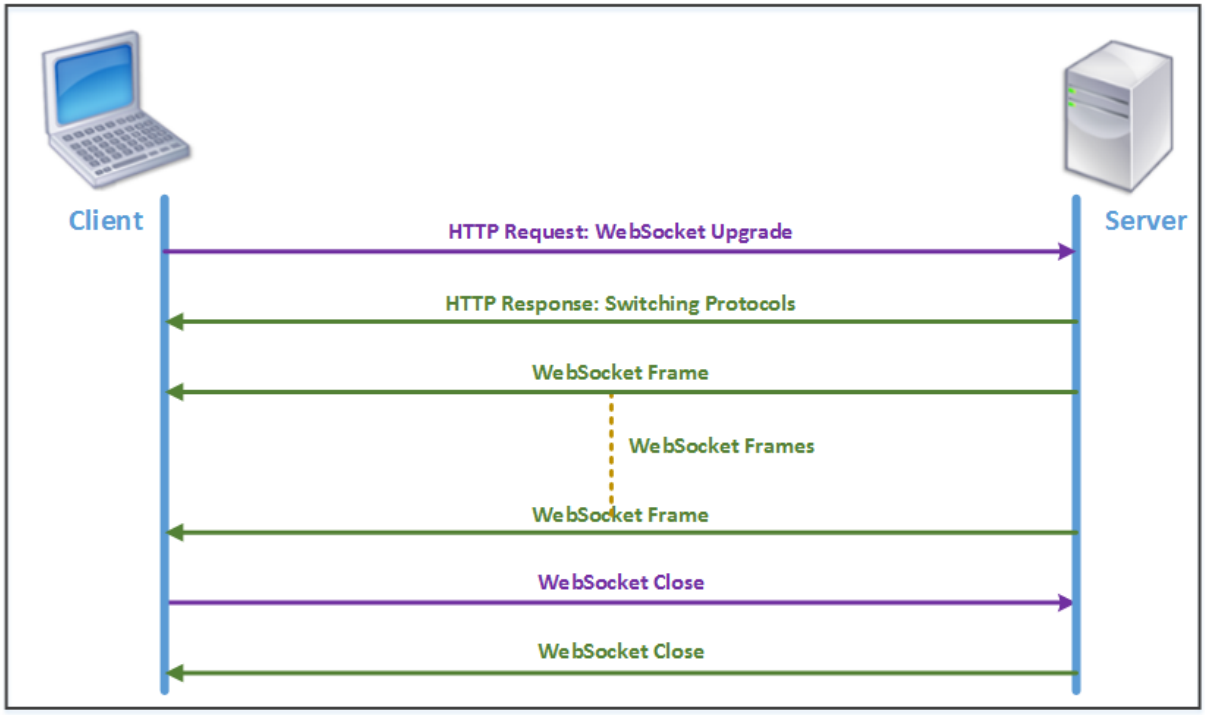
- サンプルクライアントリクエスト

```
pre codeblock GET /HTTP/1.1 Upgrade: websocket Sec-websocket-
protocol: <List of protocols that the client supports over this
 websocket session, such as an application level protocol, for
 example ICA.> Sec-websocket-extensions: <List of extensions
client wants applied to this session, such as compression.> Sec-
Websocket-version: <Version of websocket protocol that the client
 intends to use.>
```

- サンプルサーバーの応答

```
pre codeblock HTTP/1.1 101 Switching Protocols Upgrade: websocket
 Connection: Upgrade Sec-Websocket-Protocol: <One from the list
of protocols in the client request.> Sec-Websocket-extensions:
<List of extensions server accepts for session.> Sec-Websocket-
version: <Version of websocket protocol that the server supports
.>
```

次の図は、クライアントとサーバー間で交換されるメッセージのシーケンスを示しています。



HTML5 接続中に、次のメッセージがクライアントとサーバーの間で交換されます。

- クライアントは、WebSocket をアップグレードするための HTTP リクエストを送信します。
- サーバーはクライアントの要求に応答し、WebSocket プロトコルに切り替えます。
- サーバーは WebSocket フレームをクライアントに送信します。
- クライアントは、WebSocket を閉じる要求を送信します。
- サーバーは WebSocket を閉じます。

インターネットプロトコルバージョン 6（IPv6）アクセラレーション

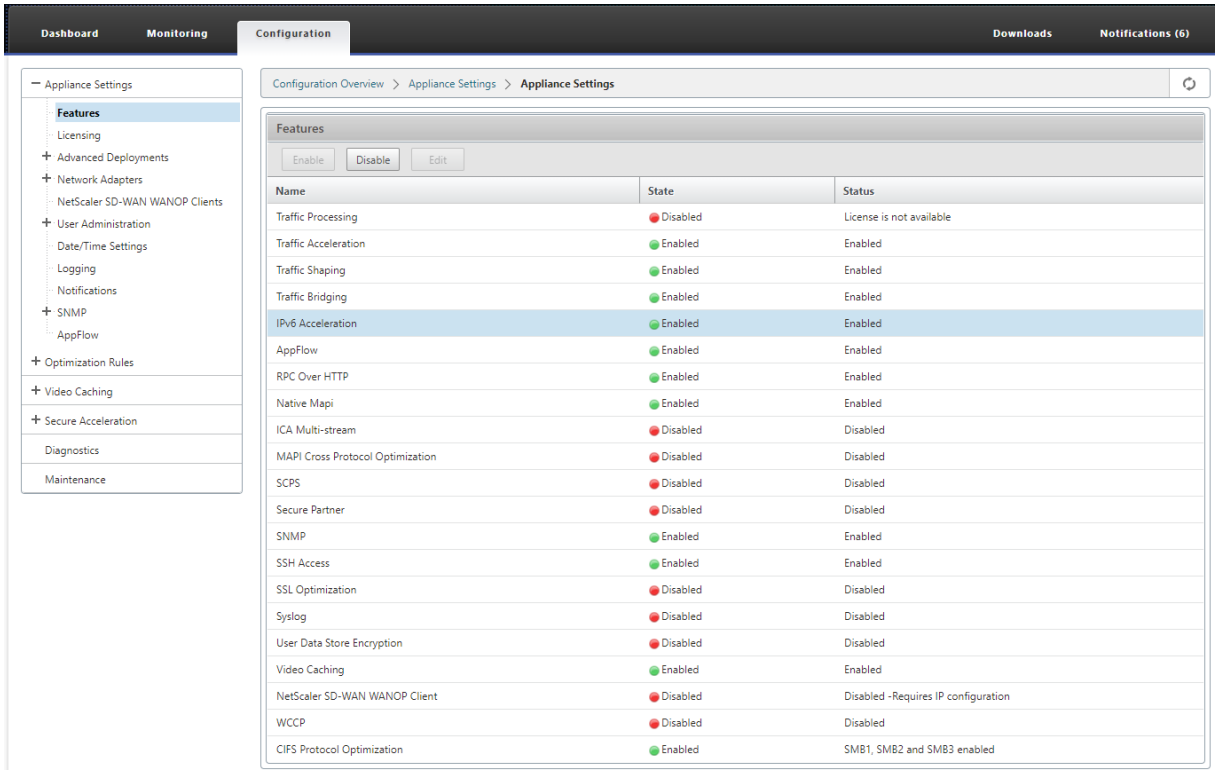
April 19, 2021

デバイスを介してインターネットに接続すると、デバイスに IP アドレスが割り当てられます。IP アドレスはアプライアンスを識別し、その場所を示します。インターネットに接続するデバイスの数は急速に増加しています。その結果、32 ビットアドレスを使用する既存のバージョンのインターネットプロトコル（IP）である IPv4 では、IP アドレスの要求を管理することは困難です。IPv4 を使用することにより、インターネットに接続するデバイスに約 43 億のアドレスを割り当てることができます。

IPv6 は、128 ビットアドレスと 16 進ラベルを使用して IPv6 ネットワーク上のデバイスのネットワークインターフェイスを識別することにより、この問題に対処します。IPv6 は IPv4 よりもはるかに多くの IP アドレスをサポートしているため、組織やアプリケーションは徐々に IPv6 プロトコルのサポートを導入しています。

IPv4 プロトコルと IPv6 プロトコルは相互運用できないため、移行が困難です。Citrix SD-WAN WANOP アプライアンスでサポートされているさまざまなアプリケーションからの IPv6 トラフィックの増加を加速するために、IPv6 加速機能を有効にすることができます。

デフォルトでは、IPv6 はアプライアンスで無効になっています。Citrix SD-WAN WANOP アプライアンスで IPv6 アクセラレーションを有効にするには、**[** 構成**]>** アプライアンスの設定 > 機能 ページを開き、**IPv6** アクセラレーション 機能を有効にします。

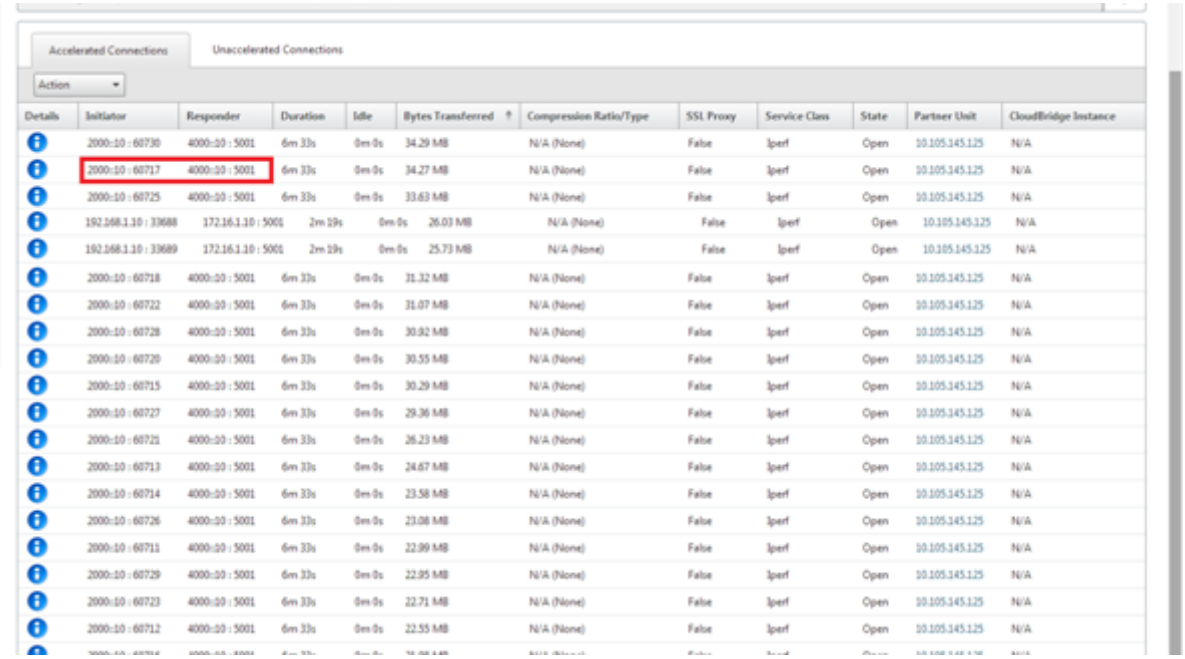


IPv6 接続を確認する

アプライアンスで IPv6 アクセラレーションを有効にした後、アプライアンスは IPv6 プロトコルを使用してアプリケーションのトラフィックのアクセラレーションを開始します。アプライアンスが IPv6 トラフィックを加速していることを確認するために、アプライアンスでそのような接続を監視できます。

IPv6 接続を監視するには、[監視] タブに移動します。[監視] タブの [接続] ページには、IPv6 プロトコルのトラフィック関連の統計が表示されます。

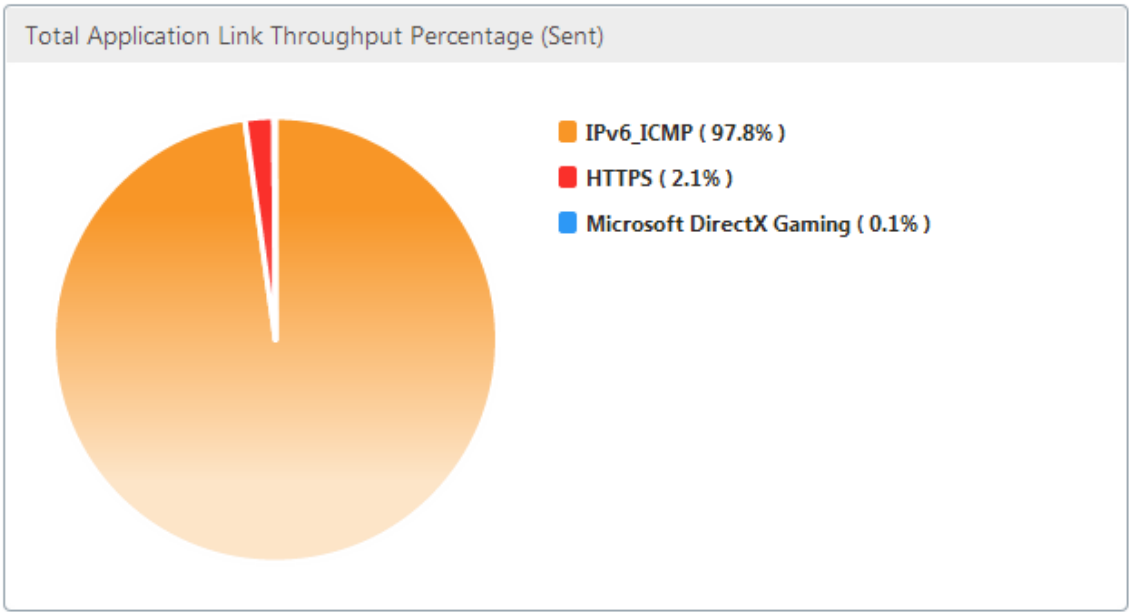
接続: [接続] ページには、アプライアンスで確立されたすべての接続の詳細が一覧表示されます。このページは、AcceleratedConnections と UnacceleratedConnections の 2 つのタブで構成されています。[Accelerated Connections] タブには、アプライアンスが加速しているすべての接続が一覧表示されます。このタブでは、各エントリの [イニシエーター] 列と [レスポンダー] 列を参照して、IPv6 トラフィックを識別できます。これらの列に 16 進数の IP アドレス値が含まれている場合、次のスクリーンショットに示すように、エントリは IPv6 接続を表します。



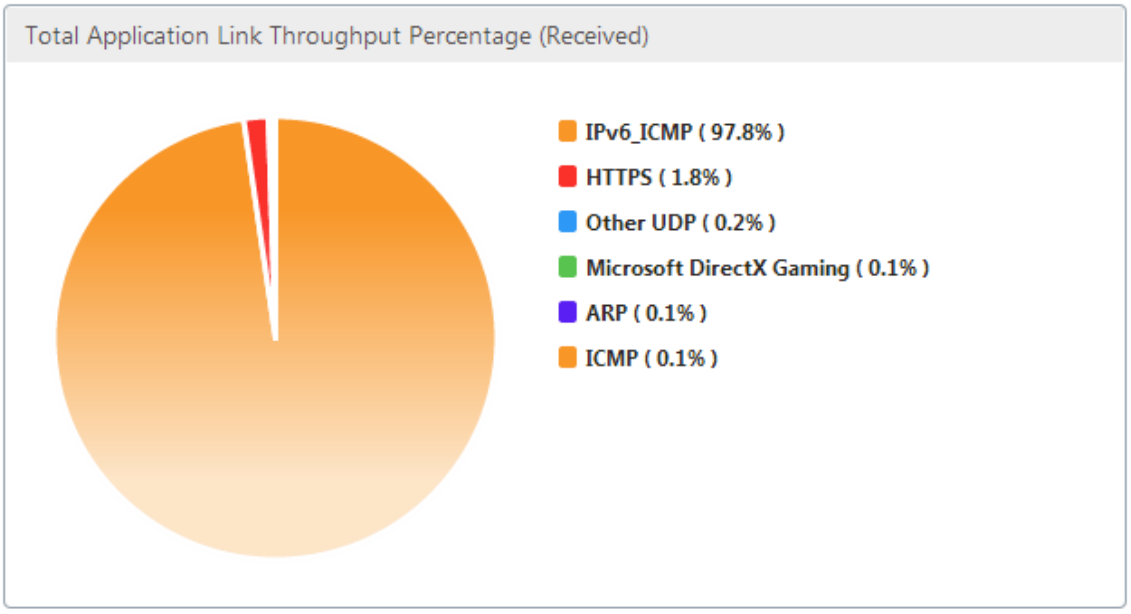
加速されていない IPv6 接続は、[加速されていない接続] タブに一覧表示されます。これらの接続を高速化したい場合は、アプライアンスのアプリケーションパラメータのトラブルシューティングと微調整が必要になる場合があります。**[Accelerated Connections]** タブと同様に、このタブでは、各エントリの **[Initiator]** 列と **[Responder]** 列を参照して IPv6 接続を識別できます。

トップアプリケーション: [トップアプリケーション] ページには、Citrix SD-WAN アプライアンスによって提供されるさまざまなアプリケーションのトラフィックスループットをグラフィカルに表すために使用できる時間枠の粒度が表示されます。デフォルトでは、トラフィックスループットは直前までに表示されます。ただし、ページのタイトルバーにあるリストから [直前]、[前回]、[前回]、[先週]、または [先月] を選択して、時間枠を変更できます。このページには、**[** トップアプリケーショングラフ**]**、**[**最後の再起動以降**]**、および **[** アクティブなアプリケーション（最後の再起動以降）**]** の 3 つのタブがあります。[トップアプリケーショングラフ] タブには、次の統計が含まれています。

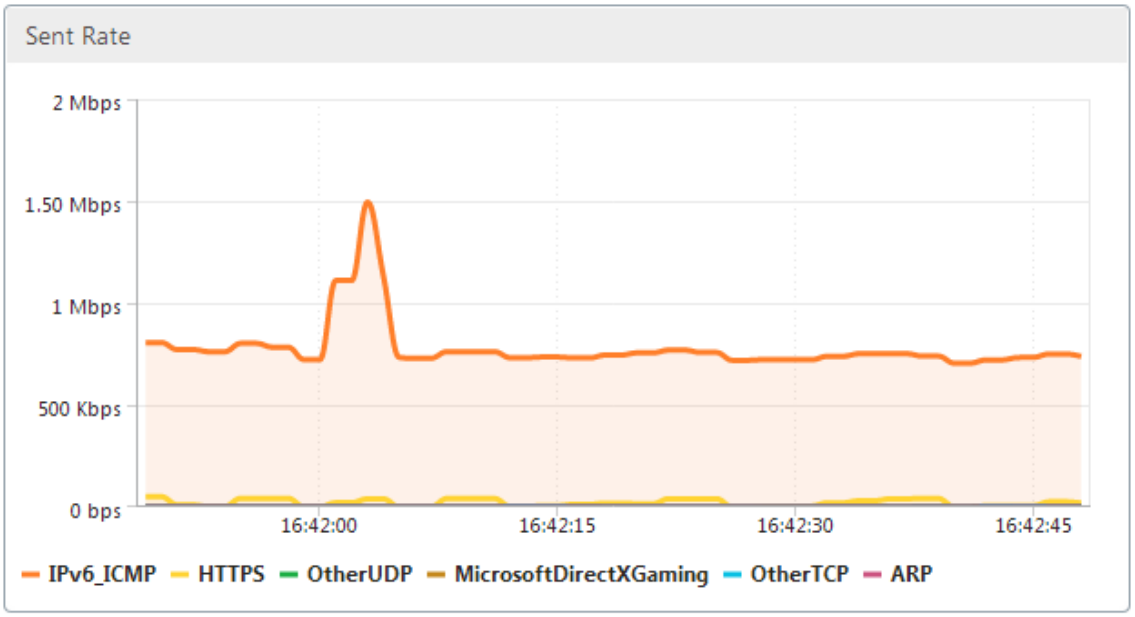
- 合計アプリケーションリンクスループットのパーセンテージ（送信済み）：これは、アプライアンスが各アプリケーションに送信したトラフィックの割合を示す円グラフです。アプライアンスが IPv6 プロトコルを使用するアプリケーションにかなりの割合のトラフィックを送信した場合、アプリケーションのトラフィックの割合はこのグラフに示されます。



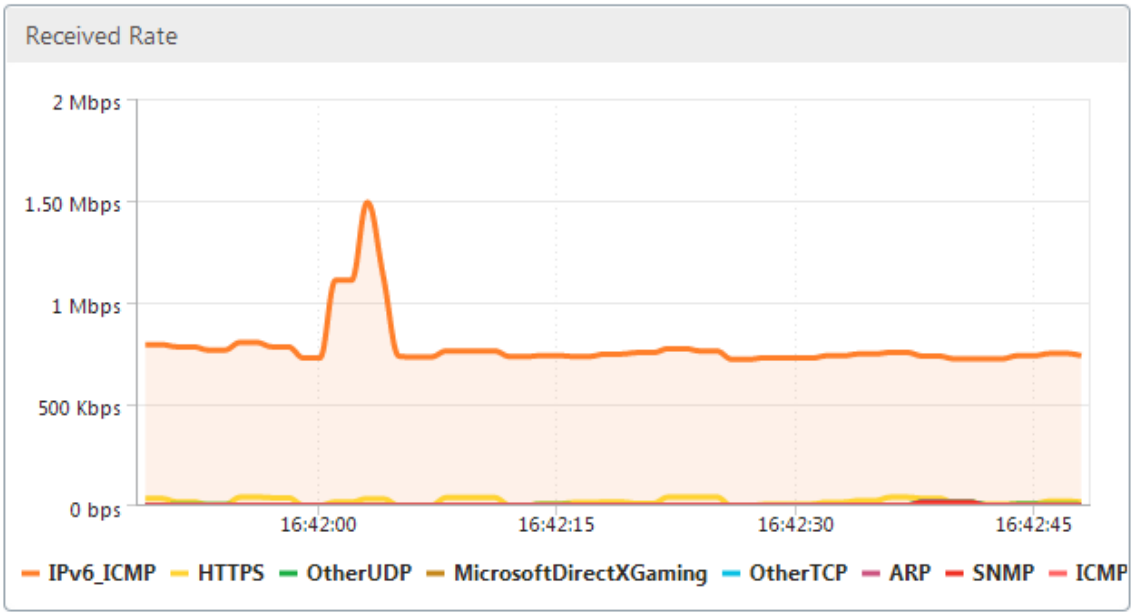
- 合計アプリケーションリンクスループットのパーセンテージ（受信済み）：これは、アプライアンスが各アプリケーションから受信したトラフィックの割合を示す円グラフです。アプライアンスが IPv6 プロトコルを使用するアプリケーションからかなりの割合のトラフィックを受信した場合、グラフにはアプリケーションによって生成されたトラフィックの割合が表示されます。



- 送信レート: これは、アプライアンスが各アプリケーションにトラフィックを送信した速度をビット/秒で表す一連のデータのスタックグラフです。アプライアンスが IPv6 プロトコルを使用してアプリケーションにデータを送信した場合、IPv6 プロトコルを使用して各アプリケーションを示す一連のデータもこのグラフにプロットされます。



- 受領率: これは、アプライアンスが各アプリケーションからトラフィックを受信した速度をビット/秒で表す一連のデータのスタックグラフです。アプライアンスが IPv6 プロトコルを使用するアプリケーションからデータを受信した場合、IPv6 プロトコルを使用する各アプリケーションを示す一連のデータもこのグラフにプロットされます。



- トップアプリケーションテーブル: これは、各アプリケーションの統計の表です。この表には、アプライアンスがトラフィックを処理したすべてのアプリケーションが、ビット/秒単位の送受信レート、送受信された合計バイト数、アプリケーションのトラフィックの割合、およびアプライアンスがトラフィックを処理したレートとともに一覧表示されます。応用。アプライアンスが IPv6 プロトコルを使用してアプリケーションのトラフィックを処理した場合、アプリケーションはその統計とともにこの表にリストされます。

Top Applications

Application	Sent Rate (bps)	Received Rate (bps)	Total Bytes Sent	Total Bytes Received	Total %	Order
IPv6_ICMP	719.56 K	719.56 K	5.4 M	5.4 M	98.3	1
HTTPS	10.57 K	9.64 K	79.3 K	72.35 K	1.38	2
Microsoft DirectX Gaming	416	416	3.14 K	3.14 K	0.06	4
Other TCP	312	312	2.35 K	2.35 K	0.04	5
Other UDP	128	1.7 K	984	12.73 K	0.12	3
ARP	24	488	232	3.66 K	0.04	6
SNMP	0	496	0	3.76 K	0.03	7
ICMP	0	376	0	2.84 K	0.03	8

- アプリケーショングループ: これは、各アプリケーションの統計の表であり、そのアプリケーショングループと親アプリケーション（存在する場合）も含まれます。この表は、アプリケーションに対して送受信されたバイトを示しています。各アプリケーション、およびそのアプリケーショングループと親アプリケーションは、ハイパーリンクとして表示されます。ハイパーリンクをクリックすると、クリックしたリンクの統計の詳細が表示されます。アプライアンスが IPv6 プロトコルを使用してアプリケーションのトラフィックを処理した場合、アプリケーションはその統計とともにこの表にリストされます。

Application Groups

Application	Application Group	Parent Application	Bytes Sent	Bytes Received
IPv6_ICMP	IP Protocols	IPv4	5.4 M	5.4 M
HTTPS	Web, Security Protocols	TCP	79.3 K	72.35 K
Microsoft DirectX Gaming	Games	TCP	3.14 K	3.14 K
Other TCP	N/A	N/A	2.35 K	2.35 K
Other UDP	N/A	N/A	984	12.73 K
ARP	Legacy Or Non-IP	N/A	232	3.66 K
SNMP	Network Management, Infrastructure	UDP	0	3.76 K
ICMP	Infrastructure, IP Protocols	IPv4	0	2.84 K

[最後の再起動以降] タブには、アプライアンスを再起動してからのアプリケーショントラフィックに関する統計が含まれています。このタブには、[Total Application Link Throughput Percentage（Sent）] および [Total Application Link Throughput Percentage（Received）] グラフと、[Top Applications Graphs] タブと同様の統計が示されていますが、アプライアンスの再起動以降のデータが含まれています。[アクティブなアプリケーション（最後の再起動以降）] タブには、アプライアンスが再起動されてからのすべてのアクティブなアプリケーションを一覧表示するテーブルが含まれています。このテーブルには、アプリケーションの送受信レート、送受信された合計バイト数、および送受信された合計パケット数に関する詳細が含まれています。

リンクの定義

April 19, 2021

リンク定義により、アプライアンスは WAN リンクの輻輳と損失を防ぎ、トラフィックシェーピングを実行できます。リンク定義は、定義されたリンクに関連付けられているトラフィック、リンクで受信されるトラフィックを許可する最大帯域幅、およびリンクを介して送信されるトラフィックの最大帯域幅を指定します。この定義では、トラフィックをインバウンドまたはアウトバウンド、および WAN 側または LAN 側のトラフィックとしても識別します。アプラ

イアンスを流れるすべてのトラフィックがリンク定義のリストと比較され、最初に一致する定義がトラフィックが属するリンクを識別します。

クイックインストール手順を実行することにより、アプライアンスのデフォルトのリンク定義をカスタマイズします。次に、アプライアンスの WAN へのリンクと LAN へのリンクを定義しました。単純なインライン展開の場合、リンク定義をさらに構成する必要はありません。他のタイプのデプロイメントでは、リンク定義の追加構成が必要です。

すべてのリンクには、送信速度と受信速度を表す 2 つの帯域幅制限があります。リンク速度がわかっている場合にのみ、アプライアンスは正確に適切な速度でトラフィックをリンクに注入できるため、送信を試みすぎることによる輻輳やパケット損失、または送信が少なすぎることによるパフォーマンスの低下を排除できます。高速 LAN と低速 WAN の間に配置され、仮想ゲートウェイ として機能する場合、アプライアンスは、WAN が受け入れるよりも速くトラフィックを受信する機能を備えており、トラフィックのバックログを作成します。このバックログの存在により、アプライアンスは次に送信するパケットを選択でき、この選択によりトラフィックシェーピングが可能になります。複数のストリームから選択できるパケットがない限り、一方のストリームをもう一方のストリームよりも優先することはできません。したがって、トラフィックシェーピングは、仮想ゲートウェイの存在に依存し、帯域幅制限を正しく設定します。

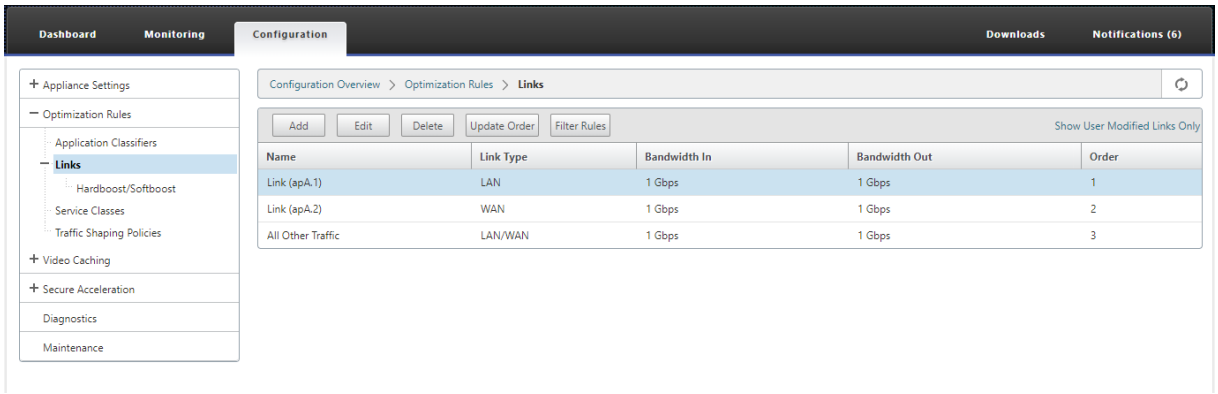
> 注
>
> リンク定義は通常、高速化されたブリッジポートのペアへの接続に適用されます。プライマリと Aux1 の 2 つのマザーボードポートもリンクとして定義できますが、WAN トラフィックではなく、管理および高可用性モードとグループモードのバックチャネルとして使用されるため、リンクとして定義することはほとんどありません。
>
> 重要
>
> 重要：リンク定義の目的では、リンク は物理リンクであり、独自の帯域幅容量があります。通常、建物から出るケーブルです。次の点に注意してください。
>
> - VLAN はリンクではありません。
> - 仮想リンクはリンクではありません。
> - トンネルはリンクではありません。

デフォルトのリンク定義

構成 > 最適化ルール > リンク に移動し現在定義されているリンクを表示。次のリンクはデフォルトで定義されています。

1. **apA.1**、加速ブリッジの 2 つのポートの 1 つ。
2. **apA.2**、加速ブリッジのもう 1 つのポート。
3. システムにデュアルアクセラレーションブリッジがある場合、apB.1 と apB.2 も存在します。
4. 他のすべてのトラフィック。これは実際のリンクではありませんが、実際のリンク定義と一致しないトラフィックのキャッチオールです。

このページにリンクが表示される順序は重要です。パケットが属するリンクを決定するとき、アプライアンスはリンクを順番にテストし、最初に一致するリンクが選択されます。これは、重複する定義が許可され、リンクの最後の定義がすべてのトラフィックに一致し、デフォルトのリンクとして機能することを意味します。注文を変更するには、[注文の 更新] をクリックします。



トラフィックシェーピングでリンク定義を管理する

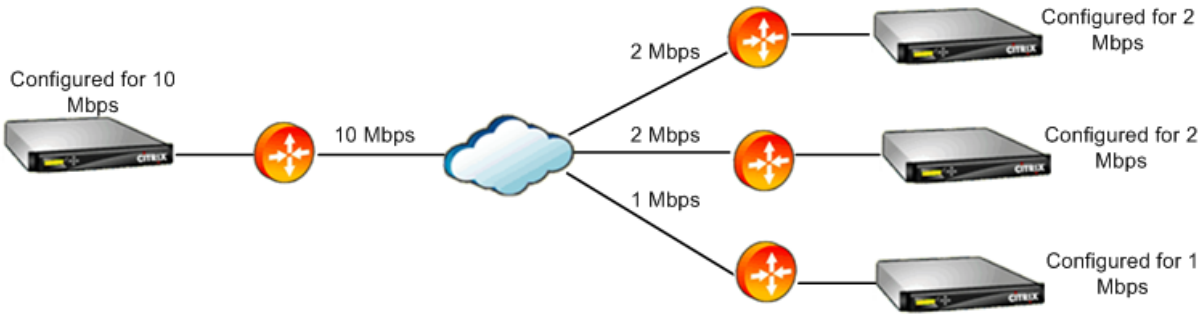
April 19, 2021

リンクを管理するには、トラフィックシェーパーに次の情報が必要です。

- 送信方向と受信方向の両方でのリンクの速度。
- リンクが WAN リンクであるか LAN ネットワークであるか。
- リンクトラフィックを他のトラフィックから区別する方法。
- トラフィックがリンク上を流れる方向。

リンク速度—リンク速度は 常に物理リンクの速度を指します。WAN リンクの場合、Citrix SD-WAN WANOP アプライアンスとの構築で終了するのは WAN セグメントの速度です。リンクのもう一方の端の速度は考慮されません。たとえば、次の図は 4 つのアプライアンスのネットワークを示しています。各アプライアンスの着信帯域幅と発信帯域幅は、リモートエンドポイントの速度に関係なく、独自のローカル WAN セグメントの速度の 95%に設定されています。

図 1：ローカル帯域幅制限はローカルリンク速度を追跡します



帯域幅の制限をリンク速度の 100%ではなく 95%に設定する理由は、リンクオーバーヘッドを考慮し（公開された速度の 100%でデータを伝送できるリンクはほとんどない）、アプライアンスがリンクよりもわずかに遅いことを確認するためです。、わずかなボトルネックになります。トラフィックシェーパーが接続のボトルネックでない限り、トラフィックシェーピングは効果的ではありません。

さまざまなタイプのトラフィックを区別する-各リンク定義で、定義が WAN リンクまたは LAN ネットワークのどちらに適用されるかを宣言する必要があります。

トラフィックシェーパーは、パケットが WAN 上を移動しているかどうか、移動している場合はどの方向に移動しているかを知る必要があります。この情報を提供するには:

- 単純なインライン展開の場合、アクセラレーションブリッジの一方のポートが WAN リンクに属し、もう一方のポートが LAN に属することを宣言します。
- 他の展開モードでは、アプライアンスは IP アドレス、MAC アドレス、VLAN、または WCCP サービスグループを調べます。（WCCP サービスグループのテストはまだサポートされていないことに注意してください。）
- サイトに複数の WAN がある場合、ローカルリンク定義には、アプライアンスが異なる WAN からのトラフィックを区別できるようにするルールを含める必要があります。

リンク定義を構成する

April 19, 2021

リンク定義は、リンクごとに 1 つのエントリの順序付きリストに配置され、アプライアンスに出入りするすべてのパケットについて上から下にテストされます。最初に一致する定義によって、パケットが属するリンクが決まります。各リンク定義内には、ルールの順序付きリストがあり、これも上から下にテストされます。各パケットはこれらのルールと比較され、いずれかのルールに一致する場合、パケットはそのリンクを通過していると見なされます。

単一のルール内では、フィールドはすべて AND で結合されるため、指定されたすべての値が一致する必要があります。すべてのフィールドのデフォルトは Any で、常に一致するワイルドカードエントリです。フィールドが IP サブネットのリストなどのリストで構成されている場合、リストエントリは OR 演算されます。つまり、いずれかの要素が一致する場合、リスト全体が一致すると見なされます。

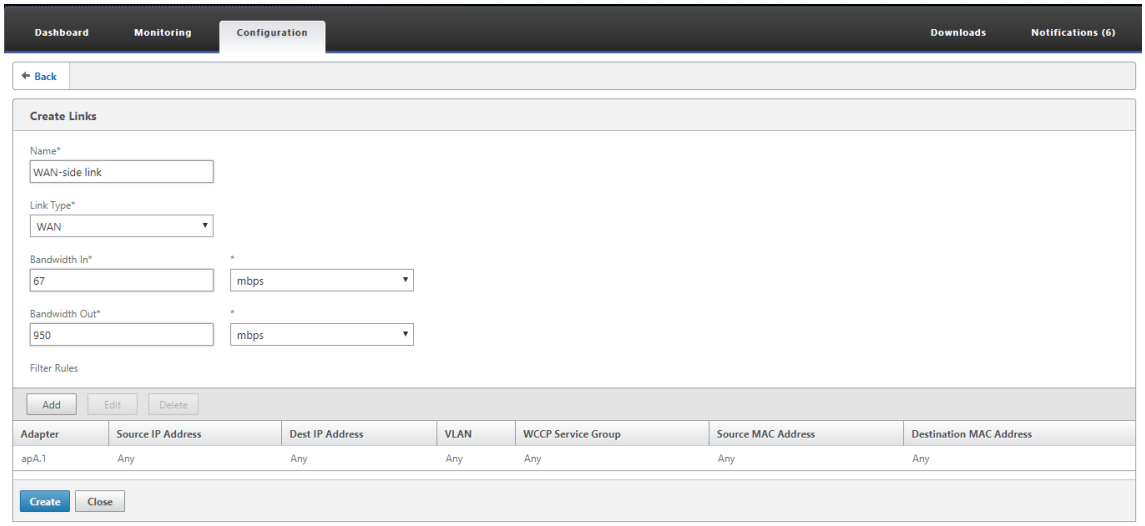
リンクは、トラフィックに関連付けられたイーサネットアダプタ、送信元と宛先の IP アドレス、VLAN タグ、WCCP サービスグループ（WCCP-GRE の場合のみ）、および送信元と宛先のイーサネット MAC アドレスに基づくことができます。単純なインライン展開では、LAN 側と WAN 側の高速ブリッジポート（apA.1 と apA.2）のみを識別できますが、複雑なデータセンター展開では、トラフィックを明確にするために提供されているオプションのほとんどを使用する必要があります。

冗長リンクが使用されている場合を除いて、IP アドレスの観点からリンクを定義することは可能です。特定のパケットは、アクティブスタンバイまたはアクティブアクティブデュアルリンク展開のいずれかのリンクを通過する可能性があるため、パケットが使用しているリンクを判別するには、他の方法を使用する必要があります。デュアルブリッジが使用されている場合、一方のリンクのトラフィックは apA を経由し、もう一方のリンクは apB を経由し、リンクはアダプターの観点から定義できます。2 つのリンクが異なるルーターによって提供されている場合、ルーターの MAC アドレスを使用してトラフィックを区別できます。他のすべてが失敗した場合、WCCP-GRE を使用でき、ルーターは WAN リンクごとに異なるサービスグループを使用できるため、Citrix SD-WAN WANOP ユニットはサービスグループごとにリンクトラフィックを区別できます。

Citrix では、単純なインライン展開にはポートベースのリンク定義を、その他すべての展開には IP ベースのリンク定義を推奨しています。

リンク定義を設定するには:

1. 構成 > 最適化ルール > リンクをクリックし、追加をクリックします。



2. 次のパラメーターの値を入力します。

   - 名前: リンクの説明的な名前。LAN 側のリンクなのか WAN 側のリンクなのかを説明することもできます。
   - リンクタイプ: リンクタイプ（LAN または WAN）。
   - 帯域幅: 着信帯域幅の制限。
   - 帯域幅出力: 発信帯域幅の制限。

3. [フィルタールール] セクションで、[追加] をクリックして、次のパラメーターの値を入力します。

   - アダプタ：これは、アダプタ（イーサネットポート）のリストを指定します。イーサネットアダプタでリンクを識別できる場合、これにより設定が簡単になります。
   - 送信元 **IP** アドレス：送信元 IP ルールは、ユニットに入るパケットに対して考慮されます（ユニットから出るパケットは無視されます）。これらのパケットでは、SrcIP フィールドのルールが IP ヘッダーの SourceAddress フィールドと比較されます。このルールは、IP アドレスまたはサブネットのリストを指定します。「Exclude10.0.0.1」などの負の一致もサポートされています。
   - 宛先 **IP** アドレス：宛先 IP ルールは、ユニットを出るパケットに対して考慮されます（ユニットに入るパケットは無視されます）。これらのパケットでは、DstIP フィールドのルールが IP ヘッダーの DestinationAddress フィールドと比較されます。このルールは、IP アドレスまたはサブネットのリストを指定します。「Exclude10.0.0.1」などの負の一致もサポートされています。
   - **VLAN**： VLAN ルールは、ユニットに出入りするパケットの VLAN ヘッダーに適用されます。
   - **WCCP** サービスグループ： WCCP サービスグループルールは、ユニットに出入りする GRE カプセル化 WCCP パケットに適用されます。（これは L2 WCCP では機能しません。）
   - 送信元 **MAC** アドレス：フィルター基準として使用される送信元 MAC アドレス。
   - 宛先 **MAC** アドレス: ディルター基準として使用される宛先 MAC アドレス。

4. ［作成］をクリックします。

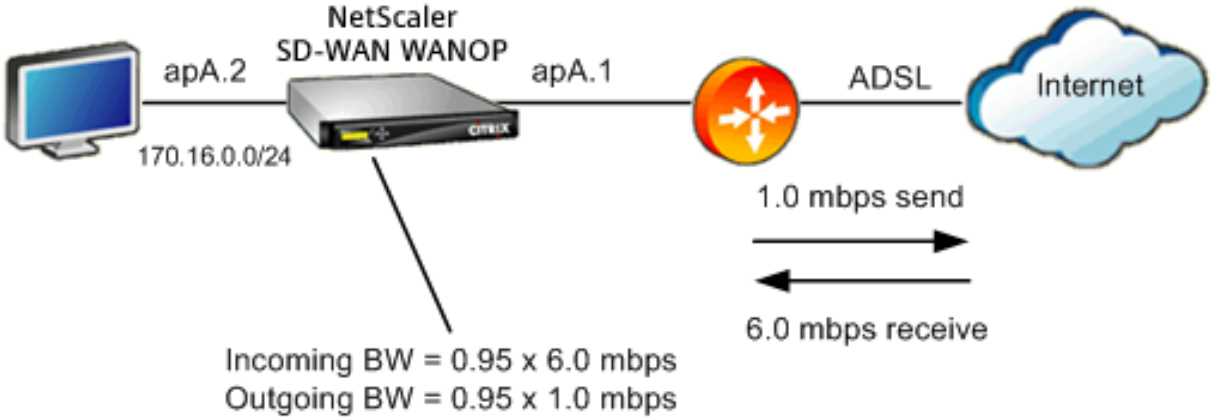
   トラフィック分類子は、SrcIP フィールドと DestIP フィールドを特殊な方法で使用します（同じことが SrcMAC と DstMAC にも当てはまります）。

   - Src フィールドは、アプライアンスに入るパケットでのみ検査されます。
   - Dst は、アプライアンスを出るパケットでのみ検査されます。

インラインリンク

ほとんどの Citrix SD-WAN WANOP アプライアンスは、単純なインライン展開を使用しており、各アクセラレーションブリッジは 1 つの WAN リンクのみを提供します。これは、構成するのに最も簡単なモードです。

シンプルなインラインリンク



上の図では、高速化されたブリッジを通過するすべてのトラフィックが WAN トラフィックであると想定されています。このリンクは、送信速度と受信速度が異なる ADSL リンクです（6.0 mbps ダウン、1.0 mbps アップ）。WAN は加速ブリッジポート apA.1 に接続され、LAN は加速ブリッジポート apA.2 に接続されます。

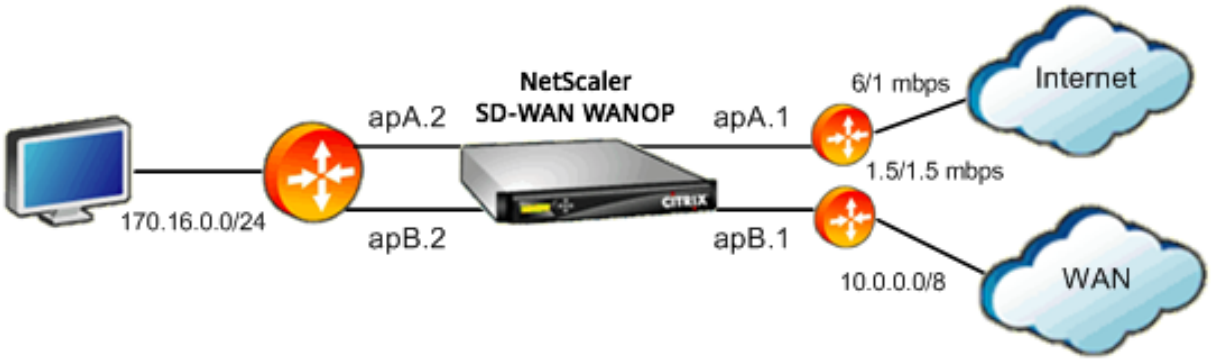
WAN 側リンク（apA.1）を定義するためのタスクは次のとおりです。

1. WAN に「WANtoHQ（apA.1）」などのわかりやすい名前を付けます。
2. タイプを「WAN」に設定します。
3. 着信および発信帯域幅の制限を公称リンク速度の 95%に設定します。
4. WAN イーサネットアダプタ（この例では apA）を指定するルールが定義されていることを確認します。
5. ［作成］をクリックします。

LAN 側リンク（apA.2）のタスクは類似しています。

1. 「ローカル LAN（apA.2）」などのわかりやすい名前を付けます。
2. タイプを「LAN」に設定します。
3. 着信および発信帯域幅の制限を、公称イーサネット速度の 95%（95mbps または 950mbps）に設定します。
4. LAN イーサネットアダプタ（この例では apA.2）を指定するルールが存在することを確認します。
5. ［作成］をクリックします。

デュアルブリッジによるインライン展開



構成は単純なインラインリンク構成に似ていますが、サイトには、ADSL インターネットリンクに加えて、2 番目のリンクである企業 WAN への T1 リンクがあります。Citrix SD-WAN WANOP アプライアンスには、WAN リンクごとに 1 つずつ、合計 2 つの高速ブリッジがあります。

構成はシングルブリッジの場合とほぼ同じくらい簡単で、次の追加手順があります。

1. apB の 2 番目の WAN リンク（この場合は apB.1）を編集します。タイプを「WAN」に設定します。リンク帯域幅を 1.5mbps T1 速度の 95%に設定し、リンクに「WANtoHQ」などの新しい名前を付けます。
2. 「LAN」定義に apB.2 を指定するルールを追加し、apB.2 のデフォルトのリンク定義を削除します。（または、apA.2 の場合と同様に、apB.2 のデフォルトのリンク定義を編集して LAN リンクとして指定することもできます。）

非インラインリンク

単純なインライン展開（高速化されたブリッジごとに 1 つの WAN のみにサービスを提供する）以外の場合は、ブリッジポートの代わりに IP サブネットを使用して、LAN トラフィックと WAN トラフィックを区別します。このアプローチは、単一のブリッジポートのみを使用するワンアーム展開に不可欠です。IP サブネットは、特にアプライアンスが複数の WAN にサービスを提供する場合に、インライン展開にも役立つことがあります。ただし、単純なインライン展開の場合、ポートベースのリンクを定義する方が簡単です。

トラフィック分類子は、SrcIP と DstIP を調べるときに特殊な規則を適用します。

- Src IP フィールドは、アプライアンスに入るパケットでのみ検査されます。
- Dst IP フィールドは、アプライアンスを出るパケットでのみ検査されます。

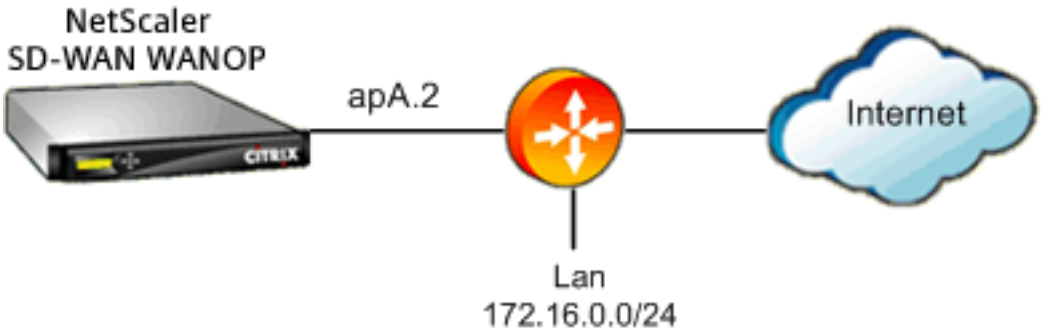
この規則は混乱を招く場合がありますが、パケットの移動方向を定義の一部として暗黙的に考慮することができます。

リンク定義で **IP** アドレスを使用する

IP ベースのルールを使用して単純なインライン LAN 定義を構成するには、イーサネットポートをまったく指定せずに、代わりに LAN サブネットを使用して LAN および WAN リンクを定義できます。

- LAN リンク定義のルールを作成し、[SrcIP] フィールドに LAN サブネットを指定します。
- WAN リンク定義のルールを作成し、[Dst IP] フィールドに LAN サブネット（WAN サブネットではない）を指定します。

WCCP および仮想インラインモード



LAN と WAN の IP サブネットは同一であるため、IP ベースのルールを使用した構成 WCCP または仮想インライン展開は、リンク定義で IP アドレスを使用する場合と同じです。

WCCP-GRE が使用される場合、GRE ヘッダーは無視され、カプセル化されたデータパケット内の IP ヘッダーが使用されます。したがって、この同じリンク定義は、WCCP-L2、WCCP-GRE、インライン、および仮想インラインモードで機能します。

(WCCP および仮想インラインモードでは、ルータを設定する必要があります。WCCP では、[構成：高度な展開] ページでも構成が必要です。)

Citrix Application Delivery Management を使用した管理と監視

December 16, 2022

Citrix SD-WAN WANOP AppFlow のサポートにより、Citrix SD-WAN WANOP アプライアンスの柔軟でカスタマイズされた監視が可能になります。

AppFlow インターフェースは、Citrix Application Delivery Management（ADM）と連携します。Citrix ADM は、AppFlow オープンスタンダードを使用してアプライアンスから詳細情報を受け取ります。Citrix ADM を使用すると、ネットワーク内の Citrix SD-WAN アプライアンスの分析を監視、管理、および表示できます。

Citrix ADM は、さまざまなデバイスをサポートしており、ネットワークのより完全なビューを表示できます。Citrix SD-WAN WANOP アプライアンスは、Virtual Apps/Virtual Desktops. トラフィックに関する詳細な統計を含む、WAN トラフィックに関する広範なビューを備えており、WAN ユーザーエクスペリエンスに関する重要な洞察を提供します。

詳しくは、「Citrix Application Delivery Management を使用した Citrix SD-WAN インスタンスの管理」を参照してください。

Virtual Apps/Virtual Desktops. の例

Citrix Virtual Apps and Desktops 環境では、ブランチユーザーのパフォーマンスが低下した場合、管理者は Virtual Apps または Virtual Desktops でホストされているネットワーク、ユーザー、およびアプリケーションを監視する必要があります。管理者は、次の質問をする必要がある場合があります。

- ネットワークのどの部分が悪いユーザーエクスペリエンスを引き起こしていますか?
- 公開されたアプリケーションの速度低下を特定する簡単な方法は何ですか?
- 特定の期間に最も多くの帯域幅を消費している仮想チャネルはどれですか?
- 特定の期間に最も多くの帯域幅を消費している Virtual Apps または Virtual Desktops ユーザーはどれですか。
- 特定の Virtual Desktops ユーザーについて、クライアント側とサーバー側の平均待ち時間、および平均ジッタはどれくらいですか。
- 特定の期間における稼働時間および起動の合計数によって、すべての Virtual Apps ユーザーの上位アプリケーションは何ですか?
- データセンターのレイテンシーとは何ですか?

Citrix SD-WAN WANOP AppFlow サポートは、上記のすべての質問に対する回答を提供します。これにより、たとえば、混雑した WAN リンクを低速のサーバーまたは低速のクライアントと区別できます。

Citrix Cloud Connector

April 19, 2021

Citrix SD-WAN WANOP アプライアンスの Citrix Cloud Connector 機能は、エンタープライズデータセンターを外部クラウドおよびホスティング環境に接続し、クラウドをエンタープライズネットワークのセキュアな拡張にします。クラウドでホストされるアプリケーションは、1 つの連続したエンタープライズネットワークで実行されているかのように見えます。Citrix Cloud Connector を使用すると、クラウドプロバイダーが提供する容量と効率でデータセンターを拡張できます。

Citrix Cloud Connector を使用すると、アプリケーションをクラウドに移動して、コストを削減し、信頼性を高めることができます。

Citrix SD-WAN WANOP アプライアンスの WAN 最適化機能は、トラフィックを高速化し、エンタープライズデータセンターとクラウドで実行されているアプリケーションに LAN のようなパフォーマンスを提供します。

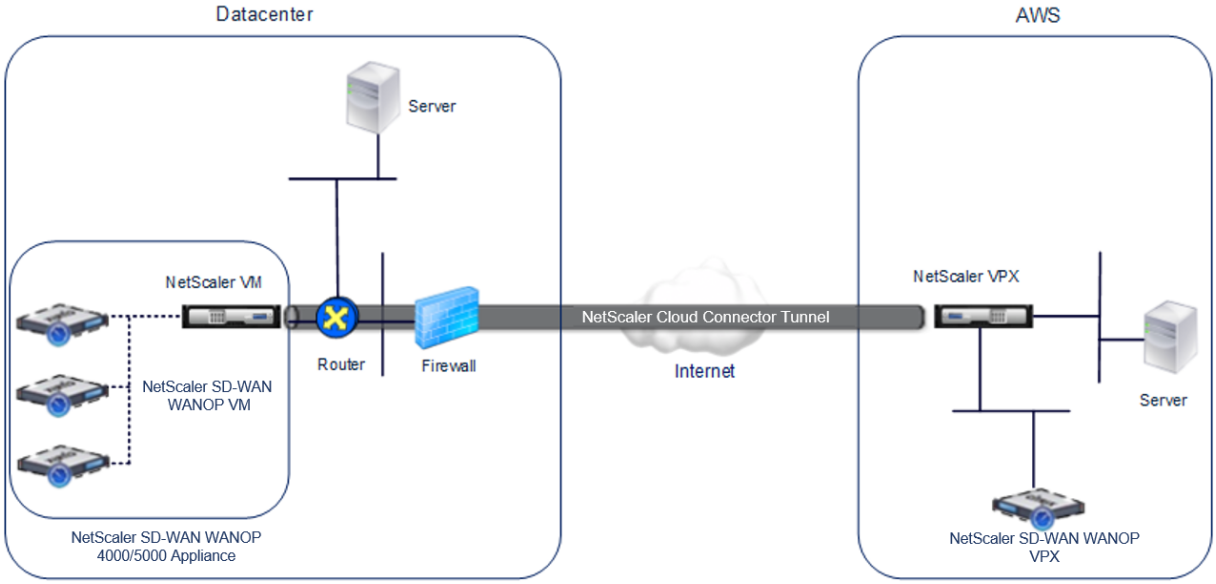
データセンターとクラウド間で Citrix Cloud Connector を使用することに加えて、これを使用して 2 つのデータセンターを接続し、大容量の安全で高速なリンクを実現できます。

Citrix Cloud Connector ソリューションを実装するには、Citrix Cloud Connector トンネルと呼ばれるトンネルを設定して、データセンターを別のデータセンターまたは外部クラウドに接続します。

データセンターを別のデータセンターに接続するには、各データセンターに 1 つずつ、2 つのアプライアンス間に Citrix Cloud Connector
トンネルを設定します。

データセンターを外部クラウド（Amazon AWS クラウドなど）に接続するには、データセンター内の Citrix SD-WAN WANOP アプライアンスとクラウド内にある仮想アプライアンス（VPX）の間に Citrix Cloud Connector トンネルを設定します。リモートエンドポイントは、Citrix Cloud Connector またはプラチナライセンスの Citrix VPX にすることができます。

次の図は、データセンターと外部クラウドの間に設定された Citrix Cloud Connector トンネルを示しています。



Citrix Cloud Connector トンネルがセットアップされているアプライアンスは、Citrix Cloud Connector トンネルの エンドポイント または ピア と呼ばれます。

Citrix Cloud Connector トンネルは次のプロトコルを使用します。

- 汎用ルーティングカプセル化（GRE）プロトコル
- オープン標準の IPSec プロトコルスイート（トランスポートモード）

GRE プロトコルは、さまざまなネットワークプロトコルからのパケットをカプセル化し、別のプロトコル経由で転送するメカニズムを提供します。GRE は次の目的で使用されます。

- 非 IP プロトコルおよびルーティング不可能なプロトコルを実行するネットワークを接続します。
- ワイドエリアネットワーク (WAN) を経由するブリッジ。
- 異なるネットワーク上で変更せずに送信する必要があるあらゆる種類のトラフィックに対して、トランスポートトンネルを作成します。

GRE プロトコルは、GRE ヘッダーと GRE IP ヘッダーをパケットに追加することによって、パケットをカプセル化します。

インターネットプロトコルセキュリティ（IPSec）プロトコルスイートは、Citrix Cloud Connector トンネル内のピア間の通信を保護します。

Citrix Cloud Connector トンネルでは、IPSec は次のことを保証します。

- データの整合性
- データ発信元認証
- データの機密性 (暗号化)
- リプレイ攻撃に対する保護

IPSec は、GRE カプセル化パケットが暗号化されるトランスポートモードを使用します。暗号化は、カプセル化セキュリティペイロード (ESP) プロトコルによって行われます。ESP プロトコルは、HMAC ハッシュ関数を使用してパケットの整合性を保証し、暗号化アルゴリズムを使用して機密性を保証します。パケットが暗号化され、HMAC が計算されると、ESP ヘッダーが生成されます。ESP ヘッダーは GRE IP ヘッダーの後に挿入され、ESP トレーラーは暗号化されたペイロードの最後に挿入されます。

Citrix Cloud Connector トンネル内のピアは、次のように、インターネットキー交換バージョン（IKE）プロトコル（IPSec プロトコルスイートの一部）を使用して、安全な通信をネゴシエートします。

- 2 つのピアは、次の認証方法のいずれかを使用して、相互に認証を行います。
  - 事前共有キー認証。事前共有キーと呼ばれるテキスト文字列は、各ピアに手動で設定されます。ピアの事前共有キーは、認証のために相互に照合されます。したがって、認証を成功させるには、各ピアで同じ事前共有キーを設定する必要があります。
  - デジタル証明書認証。発信側（送信者）ピアは、秘密キーを使用してメッセージ交換データに署名し、もう一方の受信側ピアは送信者の公開キーを使用して署名を検証します。通常、公開キーは X.509v3 証明書を含むメッセージで交換されます。この証明書は、証明書に示されているピアのアイデンティティが特定の公開キーに関連付けられていることを保証します。

- ピアは、次の上で合意に達するために交渉します。
  - 暗号化アルゴリズム。
  - 1 つのピアでデータを暗号化し、もう 1 つのピアでデータを復号化する暗号化キー。

セキュリティプロトコル、暗号化アルゴリズム、および暗号化キーに関する本契約は、セキュリティアソシエーション (SA) と呼ばれます。SA は一方向（単方向）です。たとえば、CB1 と CB2 の 2 つのピアがコネクタトンネルを介して通信している場合、CB1 には 2 つのセキュリティアソシエーションがあります。一方の SA は発信パケットの処理に使用され、もう一方の SA は着信パケットの処理に使用されます。

SA は、ライフタイムと呼ばれる指定された時間が経過すると期限切れになります。2 つのピアは、インターネットキー交換（IKE）プロトコル（IPSec プロトコルスイートの一部）を使用して、新しい暗号化キーをネゴシエートし、新しい SA を確立します。限られた寿命の目的は、攻撃者が鍵をクラックするのを防ぐことです。

また、Citrix Cloud Connector
トンネルエンドポイント上の Citrix SD-WAN WANOP インスタンスは、トンネルを介した WAN 最適化を提供します。

Citrix Cloud Connector トンネルを構成するための前提条件

AWS クラウドとデータセンターでワンアームモード用に構成された Citrix SD-WAN WANOP アプライアンスの間に Citrix Cloud Connector トンネルを設定する前に、次のタスクが完了していることを確認してください。

1. データセンターの Citrix SD-WAN WANOP アプライアンスが正しくセットアップされていることを確認してください。WCCP/Virtual インラインプロトコルを使用するワンアームモードでの Citrix SD-WAN アプライアンスの展開の詳細については、WAN ルーターが 1 つあるサイトを参照してください。
2. AWS クラウドに Citrix 仮想アプライアンス（VPX インスタンス）をインストール、設定、起動します。詳しくは、「AWS での NetScaler VPX のインストール」を参照してください。
3. AWS クラウドに Citrix SD-WAN WANOP 仮想アプライアンス（VPX）のインスタンスをインストール、構成、および起動します。詳しくは、「AmazonAWS への SD-WAN VPX SAMI のインストール」を参照してください。
4. AWS で、AWS 上の Citrix SD-WAN WANOP VPX インスタンスを AWS 上の Citrix VPX インスタンスの負荷分散仮想サーバーにバインドします。このバインディングは、Citrix SD-WAN WANOP VPX インスタンスを介してトラフィックを送信し、Citrix Cloud Connector トンネルを介して WAN を最適化するために必要です。

コマンドラインインターフェイスを使用して負荷分散仮想サーバーを作成するには:

コマンドプロンプトで、次のように入力します。

- **ns** モード **l2** を有効にする
- **add lb vserver** <cbvpxonaws_vs_name> ANY * * -**l2Conn** ON -**m** MAC

AWS に **Citrix SD-WAN WANOP VPX** インスタンスをサービスとして追加し、コマンドラインインターフェイスを使用して負荷分散仮想サーバーにバインドするには:

コマンドプロンプトで、次のように入力します。

- **add service** < cbvpxonaws_service_name> <cbvpxonaws_IP> ANY * -**cltTimeou**t 14400 -**svrTimeout** 14400
- **bind lb vserver** <cbvpxonaws_vs_name> <cbvpxonaws_service_name>

Cloud Connector トンネルを構成する

April 19, 2021

Citrix Cloud Connector トンネルを構成するには、両方の CitrixVPX アプライアンスの構成ユーティリティを使用して次のタスクを実行します。

- **IPSec** プロファイルの作成-IPSec プロファイルエンティティは、Citrix Cloud Connector トンネルの IPSec プロトコルで使用される IKE バージョン、暗号化アルゴリズム、ハッシュアルゴリズム、PSK などの IPSec プロトコルパラメータを指定します。
- **IP** トンネルを作成し、**IPSec** プロファイルをそれに関連付けます-IP トンネルは、ローカル IP アドレス、リモート IP アドレス、Citrix Cloud Connector トンネルのセットアップに使用されるプロトコル、および IPSec プロファイルエンティティを指定します。作成された IP トンネルエンティティは、Citrix Cloud Connector トンネルエンティティとも呼ばれます。
- **PBR** ルールを作成し、**IP** トンネルをそれに関連付けます-PBR エンティティは、一連の条件と IP トンネル（Citrix Cloud Connector トンネル）エンティティを指定します。送信元 IP アドレスの範囲と宛先 IP の範囲は、PBR エンティティの条件です。トラフィックが Citrix Cloud Connector トンネルを通過するサブネットを指定するには、送信元 IP アドレス範囲と宛先 IP アドレス範囲を設定する必要があります。たとえば、データセンター内のサブネット上のクライアントから発信され、AWS クラウド内のサブネット上のサーバー宛てのリクエストパケットがあるとします。このパケットが、データセンター内の Citrix SD-WAN WANOP アプライアンス上の Citrix 仮想アプライアンス上の PBR エンティティの送信元および宛先 IP 範囲と一致する場合、PBR エンティティに関連付けられた Citrix Cloud Connector トンネルを介してパケットを送信する Citrix SD-WAN WANOP 処理の対象と見なされます。

コマンドラインインターフェイスを使用して **IPSEC** プロファイルを作成するには:

コマンドプロンプトで、次のように入力します。

- `**add ipsec profile** \<ipsec\\_profile\\_name\> -**encAlgo** AES -**hashAlgo** HMAC\\_SHA1 -**lifetime** 500 -**psk** \<password \>`

コマンドラインインターフェイスを使用して **IP** トンネルを作成し、**IPSEC** プロファイルをそれにバインドするには:

コマンドプロンプトで、次のように入力します。

- `**add iptunnel** \<tunnel\\_name\> \<Remote CBC Public IP\> \<remote\\_cbs\\_Netmask\> \<lan\\_subnet\\_IP\> -**protocol** GRE -**ipsecProfileName** \<ipsec\\_profile\>`

コマンドラインインターフェイスを使用して、**PBR** ルールを作成し、**IPSEC** トンネルをそれにバインドするには:

コマンドプロンプトで、次のように入力します。

- `**add ns pbr** \<pbr\\_name\> ALLOW -**srcIP** = \<local\\_lan\\_subnet\> -**destIP** = \<remote\\_lan\\_subnet\> -**ipTunnel** \<tunnel\\_name\>`
- **apply ns pbrs**

構成ユーティリティを使用して **IPSEC** プロファイルを作成するには:

1. システム > **Citrix Cloud Connector** > **IPSec** プロファイルに移動。
2. 詳細ペインで、[追加] をクリックします。
3. [IPSec プロファイルの追加] ダイアログボックスで、次のパラメータを設定します。
   - 名前
   - 暗号化アルゴリズム
   - ハッシュアルゴリズム
   - IKE プロトコルバージョン（V2 を選択）
4. 次の IPSec 認証方法のいずれかを使用して、2 つのピアが相互認証に使用します。
   - Pre-Shared Key 認証方式の場合、Pre-Shared KeyExists パラメーターを設定します。
   - デジタル証明書の認証方法については、次のパラメータを設定します。
     - 公開キー
     - 秘密キー
     - ピア公開鍵
5. **Create**、**Close** の順にクリックします。

構成ユーティリティを使用して **IP** トンネルを作成し、**IPSEC** プロファイルをそれにバインドするには:

1. システム > **Citrix Cloud Connector** > **IP** トンネルに移動。

2. [IPv4 トンネル] タブで、[追加] をクリックします。
3. [Add IP Tunnel] ダイアログボックスで、次のパラメータを設定します。
   - 名前
   - リモート IP
   - リモートマスク
   - ローカル IP タイプ ([ローカル IP タイプ] ドロップダウンリストで、[サブネット IP] を選択します)。
   - ローカル IP（選択した IP タイプの構成済み IP はすべて、[ローカル IP] ドロップダウンリストに入力されます。リストから目的の IP を選択します）。
   - プロトコル
   - IPSec プロファイル
4. **Create**、**Close** の順にクリックします。

PBR ルールを作成し、構成ユーティリティを使用して **IPSEC** トンネルをそれにバインドするには:

1. [システム] > [ネットワーク] > [**PBR**] に移動します。
2. [PBR] タブで、[追加] をクリックします。
3. [PBR の作成] ダイアログボックスで、次のパラメータを設定します。
   - 名前
   - 操作（アクション）
   - ネクストホップタイプ（IP トンネルの選択）
   - IP トンネル名
   - 送信元 IP の低
   - 送信元 IP 高
   - 宛先 IP の低
   - 宛先 IP 高
4. **Create**、**Close** の順にクリックします。

   データセンターの Citrix SD-WAN WANOP アプライアンスの新しい Citrix Cloud Connector トンネル構成が、管理サービスのユーザーインターフェイスの [ホーム] タブに表示されます。

   AWS クラウドの CitrixVPX アプライアンス上の対応する新しい Citrix Cloud Connector トンネル構成が、構成ユーティリティに表示されます。

   Citrix Cloud Connector トンネルの現在のステータスは、[構成済み Citrix SD-WAN WANOP] ペインに表示されます。緑色のドットは、トンネルがアップしていることを示します。赤い点は、トンネルがダウンしていることを示します。

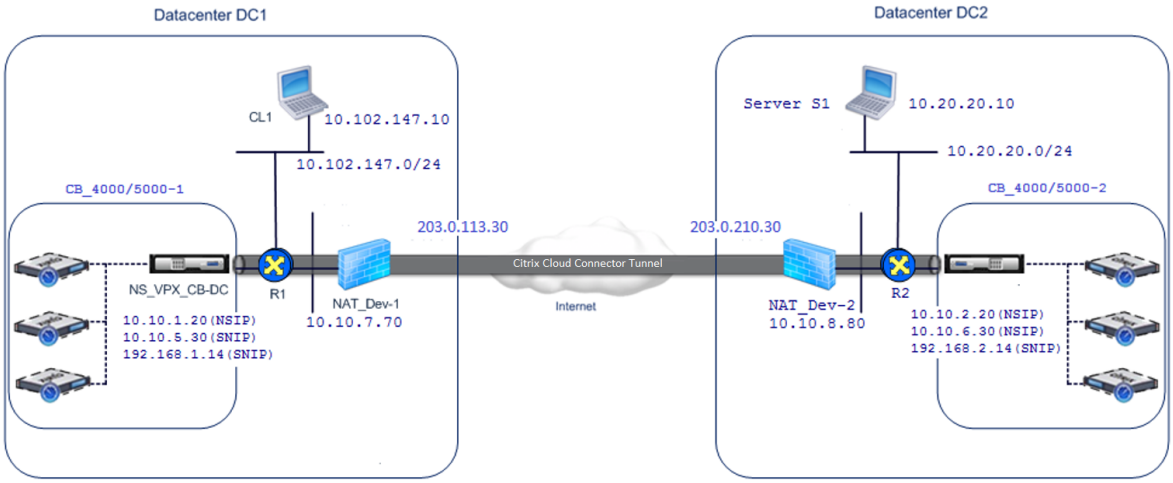
2 つのデータセンター間に Cloud Connector トンネルを構成する

April 19, 2021

2 つの異なるデータセンター間に Citrix Cloud Connector トンネルを構成して、ネットワークを再構成せずに拡張し、2 つのデータセンターの機能を活用できます。地理的に離れた 2 つのデータセンター間の Citrix Cloud Connector トンネルを使用すると、冗長性を実装し、セットアップを障害から保護できます。Citrix Cloud Connector トンネルは、2 つのデータセンター間でインフラストラクチャとリソースの最適な利用を実現するのに役立ちます。2 つのデータセンターで利用可能なアプリケーションは、ユーザーに対してローカルとして表示されます。

データセンターを別のデータセンターに接続するには、SD-WAN WANOP 間に Citrix Cloud
コネクタトンネルを設定します 4000/5000 1 つのデータセンターと別の SD-WAN WANOP に存在するアプライアンス 4000/5000 他のデータセンターにあるアプライアンス。

2 つの異なるデータセンター間で Citrix Cloud Connector トンネルがどのように構成されているかを理解するために、Citrix アプライアンス間に Cloud Connector トンネルが設定されている例を検討してください。CB_4000/5000-1 データセンター DC1 および Citrix アプライアンス CB_4000/5000-2 データセンター DC2 で。



両方の CB_4000/5000-1 そして CB_4000/5000-2 片腕モードで機能 (WCCP/PBR)。これにより、データセンター DC1 と DC2 のプライベートネットワーク間の通信が可能になります。たとえば、CB_4000/5000-1 そして CB_4000/5000-2 Citrix Cloud Connector トンネルを介したデータセンター DC1 のクライアント CL1 とデータセンター DC2 のサーバー S1 間の通信を有効にします。クライアント CL1 とサーバー S1 は、異なるプライベートネットワーク上にあります。

CL1 と S1 の間の適切な通信のために、L3 モードが有効になっています NS_VPX_CB_4000/5000-1 そして NS_VPX_CB_4000/5000-2, ルートは次のように構成されます。

- ルータ R1 には、NS_VPX_CB_4000/5000-1 経由で S1 に到達するためのルートがあります。

- NS_VPX_CB_4000/5000_1 には R1 を介して NS_VPX-CB_4000/5000-2 に到達するためのルートがあります。
- S1 には、NS_VPX-CB_4000/5000-2 経由で CL1 に到達するルートが必要です。
- NS_VPX-CB_4000/5000-2 は R2 を介して NS_VPX_CB_4000/5000-1 に到達するためのルートがあります。

次の表に、データセンター DC1 内 CB_4000/5000-1 の設定を示します。

エンティティ	名前	詳細
クライアント CL1 の IP アドレス		10.102.147.10
NAT デバイスの設定 **NAT-Dev-1**		
パブリック側の NAT IP アドレス		203.0.113.30 *
プライベート側の NAT IP アドレス		10.10.7.70
CB_4000/5000-1 の設定		
CB_4000/5000-1 の管理サービス IP アドレス **CB_4000/5000-1** で実行中の **NS_VPX_CB_4000/5000-1** の設定		10.10.1.10
NSIP アドレス		10.10.1.20
SNIP アドレス		10.10.5.30
Cloud Connector トンネル	Cloud_Connector_DC1-DC2	Citrix Cloud Connector トンネルのローカルエンドポイント IP アドレス = 10.10.5.30、Citrix Cloud Connector トンネルのリモートエンドポイント IP アドレス = 203.0.210.30 * **GRE** トンネルの詳細 名前 = Cloud_Connector_DC1-DC2 **IPSec** プロファイルの詳細 名前 = Cloud_Connector_DC1-DC2, 暗号化アルゴリズム = AES、ハッシュアルゴリズム = HMAC SHA1

エンティティ	名前	詳細
ポリシーベースのルート	CBC_DC1_DC2_PBR	ソース IP 範囲 = datacenter1 のサブネット = 10.102.147.0-10.102.147.255、宛先 IP 範囲 = datacenter2 のサブネット = 10.20.20.0-10.20.20.255、ネクストホップタイプ = IP トンネル、IP トンネル名 = CBC_DC1_DC2

* パブリック IP アドレスである必要があります。

次の表に、データセンター DC2 で CB-4000/5000-2 の設定を示します。

エンティティ	名前	詳細
サーバー S1 の IP アドレス		10.20.20.10
NAT デバイスの設定 **NAT-Dev-2**		
パブリック側の NAT IP アドレス		203.0.210.30 *
プライベート側の NAT IP アドレス		10.10.8.80
CB_4000/5000-2 の設定		
CB_SDX-1 の管理サービス IP アドレス		10.10.2.10
CB_4000/5000-2 で実行中の **NS_VPX_CB_4000/5000-2** の設定		
NSIP アドレス		10.10.2.20
SNIP アドレス		10.10.6.30
Citrix Cloud Connector トンネル	Cloud_Connector_DC1-DC2	Citrix Cloud Connector トンネルのローカルエンドポイント IP アドレス = 10.10.6.30、Citrix Cloud Connector トンネルのリモートエンドポイント IP アドレス = 203.0.113.30 * **GRE** トンネルの詳細 名前 = Cloud_Connector_DC1-DC2

エンティティ	名前	詳細
ポリシーベースのルート	CBC_DC1_DC2_PBR	**IPSec** プロファイルの詳細 名前 = Cloud_Connector_DC1-DC2, 暗号化アルゴリズム = AES、ハッシュアルゴリズム = HMAC SHA1 ソース IP 範囲 = datacenter2 のサブネット = 10.20.20.0-10.20.20.255、宛先 IP 範囲 = datacenter1 のサブネット = 10.102.147.0-10.102.147.255、ネクストホップタイプ = IP トンネル、IP トンネル名 = CBC_DC1_DC2

* パブリック IP アドレスである必要があります。

Citrix Cloud Connector トンネルのトラフィックフローは次のとおりです。

1. クライアント CL1 はサーバー S1 に要求を送信します。
2. リクエストは Citrix SD-WAN WANOP アプライアンス CB_4000/5000-1 で実行 されている Citrix 仮想アプライアンス NS_VPX_CB_4000/5000-1 に到達します。
3. NS_VPX_CB_4000/5000-1 は、Citrix SD-WAN WANOP アプライアンス CB_DC-1 WAN 最適化用で実行されている SD-WAN WANOP インスタンスの 1 つにパケットを転送します。パケットを処理した後、SD-WAN WANOP インスタンスはパケットを NS_VPX_CB_4000/5000-1 に返します。
4. 要求パケットは、PBR エンティティで指定された条件に一致します CBC_DC1_DC2_PBR （で構成 NS_VPX_CB_4000/5000-1), 要求パケットの送信元 IP アドレスと宛先 IP アドレスは、それぞれ、CBC_DC1_DC2_PBR で設定された送信元 IP 範囲と宛先 IP 範囲に属しているためです。
5. トンネルだから CBC_DC1_DC2_PBR にバインドされています CBC_DC1_DC2_PBR, アプライアンスは、Cloud_Connector_DC1-DC2 トンネル。を介して送信されるパケットを準備します
6. NS_VPX_CB_4000/5000-1 GRE プロトコルを使用して、GRE ヘッダーと GRE IP ヘッダーをパケットに追加することにより、各要求パケットをカプセル化します。GRE IP ヘッダーでは、宛先 IP アドレスは Cloud Connector トンネル (Cloud_Connector_DC1-DC2) データセンター DC2 のエンドポイントのアドレスです。
7. Cloud Connector トンネルの場合 Cloud_Connector_DC1-DC2, NS_VPX_CB_4000/5000-1 そして NS_VPX_CB_4000/5000-2. の間で合意されたように、NS_VPX_CB_4000/5000-1 はアウトバウンドパケットを処理するために storedIPSec セキュリティアソシエーション（SA）パラメータをチェックしますの

IPSec カプセル化セキュリティペイロード（ESP）プロトコル NS_VPX_CB_4000/5000-1 アウトバウンドパケットにこれらの SA パラメータを使用して、GRE カプセル化パケットのペイロードを暗号化します。

8. ESP プロトコルは、HMAC ハッシュ関数と Citrix Cloud Connector トンネル Cloud_Connector_DC1-DC2 に指定された暗号化アルゴリズムを使用して、パケットの整合性と機密性を保証します。ESP プロトコルは、GRE ペイロードを暗号化して HMAC を計算した後、ESP ヘッダーと ESP トレーラーを生成し、暗号化された GRE ペイロードの前と最後にそれぞれ挿入します。
9. NS_VPX_CB_4000/5000-1 は 結果のパケット NS_VPX_CB_4000/5000-2 を送信します
10. CB_DC-1 そして NS_VPX-AWS Cloud Connector トンネル用 Cloud_Connector_DC1-DC2 で合意されたとおり、NS_VPX_CB_4000/5000-2 は受信パケットを処理するために、保存されている IPSec セキュリティアソシエーション（SA）パラメータをチェックします。上の IPSecESP プロトコル NS_VPX_CB_4000/5000-2 インバウンドパケットにこれらの SA パラメータを使用し、要求パケットの ESP ヘッダーを使用して、パケットを復号化します。
11. NS_VPX_CB_4000/5000-2 次に、GRE ヘッダーを削除してパケットのカプセル化を解除します。
12. NS_VPX_CB_4000/5000-2 結果のパケットを CB_VPX_CB_4000/5000-2 に転送します。これは、WAN 最適化関連の処理をパケットに適用します。CB_VPX_CB_4000/5000-2 は 次に、結果のパケットを NS_VPX_CB_4000/5000-2 に返します。
13. 結果のパケットは、CB_VPX_CB_4000/5000-2 ステップ 2 で受信されたものと同じです。このパケットの宛先 IP アドレスは、サーバー S1 の IP アドレスに設定されています。NS_VPX_CB_4000/5000-2 このパケットをサーバー S1 に転送します。
14. S1 は要求パケットを処理し、応答パケットを送信します。応答パケットの宛先 IP アドレスはクライアント CL1 の IP アドレスであり、送信元 IP アドレスはサーバー S1 の IP アドレスです。

データセンターと **AWS/Azure** の間の **Cloud Connector** トンネルを構成する

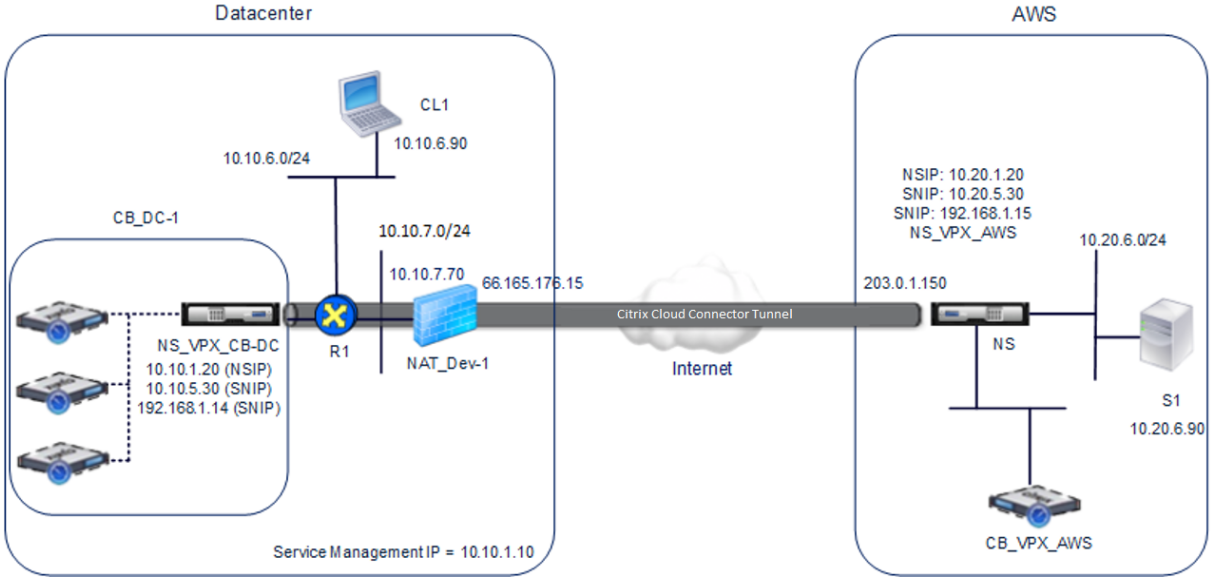
April 19, 2021

データセンターと AWS、または Azure クラウドの間に Cloud Connector トンネルを設定できます。

Citrix SD-WAN WANOP アプライアンス CB_DC-1 間で Citrix Cloud Connector トンネルが構成されている例を考えてみます。CB_DC-1 は WCCP/PBR データセンターのワンアームモード、および AWS クラウドで展開されています。CB_DC-1 ルータ R1 に接続されています。データセンターとインターネット間の接続のために、NAT デバイスも R1 に接続されています。

注：この例の設定は、あらゆるタイプの Citrix SD-WAN WANOP 展開でも機能します。この例のこの設定には、目的のサブネットのトラフィックが Citrix Cloud Connector トンネルを通過できるようにするために、netbridge ではなくポリシーベースのルートが含まれています。

次の図に示すように、Citrix Cloud Connector トンネルは Citrix SD-WAN WANOP アプライアンス CB_DC-1 で実行されている Citrix 仮想アプライアンス NS_VPX_CB-DC、および AWS クラウドで実行されている Citrix 仮想アプライアンス NS_VPX-AWS 間に確立されます Citrix Cloud Connector トンネルを介したトラフィックフローを WAN で最適化するには、NS_VPX_CB-DC で実行されている Citrix SD-WAN WANOP インスタンスとペアになっています CB_DC-1, AWS 側では、Citrix SD-WAN WANOP 仮想アプライアンス CB_VPX-AWS AWS で実行されているものは NS_VPX-AWS.



次の表に、この例のデータセンターの設定を示します。

エンティティ	名前	詳細
クライアント CL1 の IP アドレス		10.10.6.90
NAT デバイスの設定 **NAT-Dev-1**		
パブリック側の NAT IP アドレス		66.165.176.15 *
プライベート側の NAT IP アドレス		10.10.7.70
CB_DC-1 での設定		
CB_DC-1 の管理サービス IP アドレス		10.10.1.10
CB_DC-1 で実行中 **NS_VPX_CB-DC** の設定		
NSIP アドレス		10.10.1.20
SNIP アドレス		10.10.5.30
IPSec プロファイル	CBC_DC_AWS_IPSec_Profile	IKE バージョン = v2、暗号化アルゴリズム = AES、ハッシュアルゴリズム = HMAC SHA1

エンティティ	名前	詳細
Cloud Connector トンネル	CBC_DC_AWS	Cloud Connector トンネルのローカルエンドポイント IP アドレス = 10.10.5.30、Cloud Connector のリモートエンドポイント IP アドレス = 上の Cloud Connector エンドポイントアドレス（SNIP）にマップされたパブリック EIP アドレス NS_VPX-AWS AWS で = 203.0.1.150*, トンネルプロトコル = GRE および IPSEC、IPSec プロファイル名 = CBC_DC_AWS_IPSec_Profile
ポリシーベースのルート	CBC_DC_AWS_PBR	ソース IP 範囲 = データセンターのサブネット = 10.10.6.0-10.10.6.255、宛先 IP 範囲 =Subnet AWS で =10.20.6.0-10.20.6.255, ネクストホップタイプ = IP トンネル、IP トンネル名 = CBC_DC_AWS

* パブリック IP アドレスである必要があります。

次の表に、この例の AWS クラウドの設定を示します。

エンティティ	名前	詳細
—	—-	—-
サーバー S1 の IP アドレス		10.20.6.90
**NS_VPX-AWS での設定 **
NSIP アドレス		10.20.1.20
NSIP アドレスにマッピングされたパブリック EIP アドレス		203.0.1.120 *
SNIP アドレス		10.20.5.30
SNIP アドレスにマッピングされたパブリック EIP アドレス		203.0.1.150 *
IPSec プロファイル	CBC_DC_AWS_IPSec_Profile
IKE バージョン = v2、暗号化アルゴリズム = AES、ハッシュアルゴリズム = HMAC SHA1
Cloud Connector トンネル	CBC_DC_AWS	Cloud Connector トンネルのローカルエンドポイント IP アドレス =10.20.5.30, Cloud Connector トンネルのリモートエンドポイント IP アドレス = データセンター内の NAT デバイス NAT-Dev-1 のパブリック NAT IP アドレス = 66.165.176.15*, トンネルプロトコル = GRE および IPSEC、IPSec プロファイル名 = CBC_DC_AWS_IPSec_Profile
ポリシーベースのルート	CBC_DC_AWS_PBR	ソース IP 範囲 = AWS のサブネット = 10.20.6.0-10.20.6.255、

宛先 IP 範囲 = データセンターのサブネット = 10.10.6.0-10.10.6.255、ネクストホップタイプ = IP トンネル、IP トンネル名 = CBC_DC_AWS |

* パブリック IP アドレスである必要があります。

CB_DC-1 の NS_VPX_CB-DC、L3 モード NS_VPX-AWS 機能の両方。データセンター内のプライベートネットワークと AWS クラウド間の通信を可能にします。NS_VPX_CB-DC そして NS_VPX-AWS Cloud Connector トンネルを介したデータセンターのクライアント CL1 と AWS クラウドのサーバー S1 間の通信を有効にします。クライアント CL1 とサーバー S1 は、異なるプライベートネットワーク上にあります。

注：AWS は L2 モードをサポートしていません。したがって、両方のエンドポイントで L3 モードのみを有効にする必要があります。

CL1 と S1 の間の適切な通信のために、L3 モードが有効になっています NS_VPX_CB-DC そして NS_VPX-AWS, ルートは次のように構成されます。

- R1 には NS_VPX_CB-DC 経由で S1 に到達するためのルートがあります。
- NS_VPX_CB-DC には R1 を介して NS_VPX-AWS に到達するためのルートがあります。
- S1 には、NS_VPX-AWS 経由で CL1 に到達するルートが必要です。
- NS_VPX-AWS にはアップストリームルーターを介して NS_VPX_CB-DC に到達するためのルートがあります。

次に、Cloud Connector トンネルが正しく機能するようにデータセンター内のさまざまなネットワークデバイスで構成されたルートを示します。

ルート	ネットワーク	Gateway
ルータ **R1** のルート		
サーバー S1 に到達するためのルート	10.20.6.X/24	のトンネルエンドポイント SNIP アドレス NS_VPX_CB-DC = 10.10.5.30
Cloud Connector トンネルのリモートエンドポイントに到達するためのルート	NS_VPX-AWS = 203.0.1.50 の Cloud connector SNIP アドレスにマップされた EIP アドレス	NAT デバイスのプライベート IP アドレス = 10.10.7.70
NS_VPX_CB-DC 上のルート		
NS_VPX-AWS に到達するためのルート	NS_VPX-AWS = 203.0.1.50 の Cloud connector SNIP アドレスにマップされた EIP アドレス	R1 の IP アドレス = 10.10.5.1

次に、Cloud Connector トンネルが正しく機能するように AWS 内のさまざまなネットワークデバイスで構成されたルートを示します。

ルート	ネットワーク	Gateway
サーバー **S1** 上のルート		
クライアント CL1 に到達するためのルート **Citrix** 仮想アプライアンス **NS_VPX-AWS** 上のルート	10.10.6.X/24	NS_VPX-AWS のトンネルエンドポイント SNIP アドレス = 10.10.6.1
NS_VPX_CB-DC に到達するためのルート	データセンターの NAT_Dev-1 のパブリック IP アドレス = 66.165.176.15*	AWS のアップストリームルーターの IP アドレス

以下は、Cloud Connector トンネル内のクライアント CL1 からの要求パケットのトラフィックフローです。

1. クライアント CL1 はサーバー S1 に要求を送信します。
2. リクエストは Citrix SD-WAN WANOP アプライアンス CB_DC-1 で実行 されている Citrix 仮想アプライアンス NS_VPX_CB-DC に到達します。
3. NS_VPX_CB-DC は、Citrix SD-WAN WANOP アプライアンス CB_DC-1 WAN 最適化用で実行されている Citrix SD-WAN WANOP インスタンスの 1 つにパケットを転送します。パケットを処理した後、Citrix SD-WAN WANOP インスタンスはパケットを NS_VPX_CB-DC に返します。
4. 要求パケットは、PBR エンティティで指定された条件に一致します CBC_DC_AWS_PBR （で構成 NS_VPX_CB-DC), 要求パケットの送信元 IP アドレスと宛先 IP アドレスは、それぞれ、CBC_DC_AWS_PBR で設定された送信元 IP 範囲と宛先 IP 範囲に属しているためです。
5. Cloud connector トンネルのため CBC_DC_AWS にバインドされています CBC_DC_AWS_PBR, アプライアンスは、CBC_DC_AWS トンネルを介して送信されるパケットを準備します。
6. NS_VPX_CB-DC GRE プロトコルを使用して、GRE ヘッダーと GRE IP ヘッダーをパケットに追加することにより、各要求パケットをカプセル化します。GRE IP ヘッダーでは、宛先 IP アドレスが Cloud Connector トンネル AWS 側のエンドポイント (CBC_DC-AWS) の IP アドレスに設定されています。
7. Cloud Connector トンネルの場合 NS_VPX_CB-DC そして NS_VPX-AWS. の間で合意されたように、CBC_DC-AWS, NS_VPX_CB-DC はアウトバウンドパケットを処理するために保存された IPSec セキュリティアソシエーション（SA）パラメータをチェックします。NS_VPX_CB-DC の IPSec カプセル化セキュリティペイロード（ESP）プロトコルはアウトバウンドパケットにこれらの SA パラメータを使用して、GRE カプセル化パケットのペイロードを暗号化します。
8. ESP プロトコルは、HMAC ハッシュ関数と Cloud Connector トンネル CBC_DC-AWS に指定された暗号化アルゴリズムを使用して、パケットの整合性と機密性を保証します。ESP プロトコルは、GRE ペイロードを暗号化して HMAC を計算した後、ESP ヘッダーと ESP トレーラーを生成し、暗号化された GRE ペイロードの前と最後にそれぞれ挿入します。

9. NS_VPX_CB-DC 結果のパケットを NS_VPX-AWS に送信します。
10. Cloud Connector CBC_DC-AWS 用 CB_DC-1 および NS_VPX-AWS で合意されたとおり、NS_VPX-AWS は受信パケットを処理するために、保存されている IPSec セキュリティアソシエーション（SA）パラメータをチェックします。NS_VPX-AWS 上の IPSecESP プロトコルはインバウンドパケットにこれらの SA パラメータを使用し、要求パケットの ESP ヘッダーを使用して、パケットを復号化します。
11. NS_VPX-AWS は 次に、GRE ヘッダーを削除してパケットのカプセル化を解除します。
12. NS_VPX-AWS は 結果のパケットを CB_VPX-AWS に転送します。これは、WAN 最適化関連の処理をパケットに適用します。CB_VPX-AWS は次に、結果のパケットを NS_VPX-AWS に返します
13. 結果のパケットは、CB_DC-1 ステップ 2 で受信されたものと同じパケットです。このパケットの宛先 IP アドレスは、サーバー S1 の IP アドレスに設定されています。NS_VPX-AWS はこのパケットをサーバー S1 に転送します。
14. S1 は要求パケットを処理し、応答パケットを送信します。応答パケットの宛先 IP アドレスはクライアント CL1 の IP アドレスであり、送信元 IP アドレスはサーバー S1 の IP アドレスです。

Office365 アクセラレーション

April 19, 2021

Citrix SD-WAN WANOP は、WAN を最適化して、ブランチオフィスやリモートサイト全体のビジネスアプリケーションに一貫したユーザーエクスペリエンスを提供します。

Microsoft Office 365 は、サービスとしてのソフトウェア（SaaS）アプリケーションであり、Microsoft の Office スイートのエンタープライズグレードの生産性アプリケーションを提供します。このアプリケーションはクラウドでホストされ、オンデマンドでユーザーに配信されます。

Office 365 アクセラレーション機能を使用すると、ブランチオフィスは Citrix SD-WAN WANOP が Microsoft Office 365 アプリケーションに提供する最適化のメリットを享受できます。

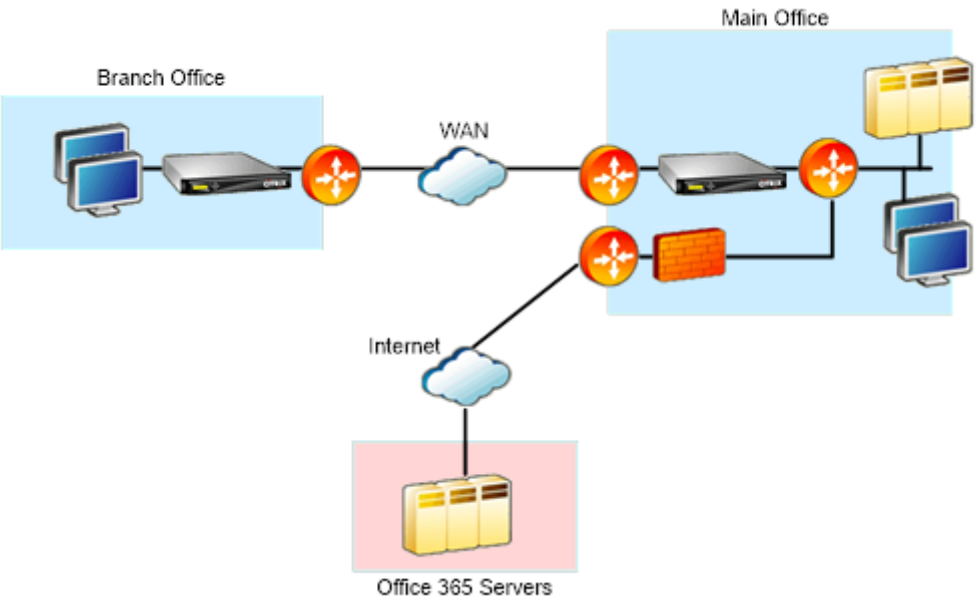
使用例

WAN セグメントがインターネットセグメントよりもかなり遅く、Microsoft の Office365 サーバーがブランチオフィスよりも大きなオフィスに近い場合。

トポロジ

ブランチオフィスの Office365 トラフィックは、WAN を介してメインオフィスに送信され、インターネットを介して Office365 サーバーに転送されます。支社と本社の間のセグメントが加速されます。

> 注
>
> 本社と MicrosoftOffice365 サーバー間のセグメントは高速化されていません。メインオフィスは最も近い Office365 サーバーに接続することをお勧めします。



使い方

Citrix SD-WAN WANOP SSL アクセラレーションは、Office 365 トラフィックを復号化して高速化し、圧縮を提供します。つまり、Office 365 ブランチオフィスアクセラレーションは、RPC-over-HTTPS アクセラレーションの特殊なケースと考えることができます。

手順

1. ブランチとメインオフィスの Citrix SD-WAN WANOP アプライアンス間に安全なピアリングを作成します。
2. プロキシ証明書を生成する / ドメイン証明機関（CA）の秘密鍵。
3. Citrix SD-WAN WANOP に必要なすべての CA を追加します。
   a) CA、中間 CA、Microsoft 証明書のルート CA。
   b) プロキシ certificates/Private Office 365 URL 用に生成されたキー。

   > 注
   >
   > ブラウザでのセキュリティアラートを回避するには、プロキシ証明書を Windows ドメインの CA サーバーで署名する必要があります。これにより、すべてのドメインユーザーがプロキシ証明書を

> 使用できるようになります。

4. SSL 分割プロキシプロファイルを作成し、分割プロキシをサービスクラス（Web（インターネットセキュリティ））にバインドします。
5. Office 365 接続を開始し、Accelerated 接続を確認します。

> 警告
>
> ドメインの一部ではないブランチオフィスデバイスは、証明書を手動でインストールしない限り、セキュリティ警告を表示します。Firefox はデバイスの証明書ストアを尊重しないため、Firefox ユーザーも手動で証明書をインストールする必要があります。

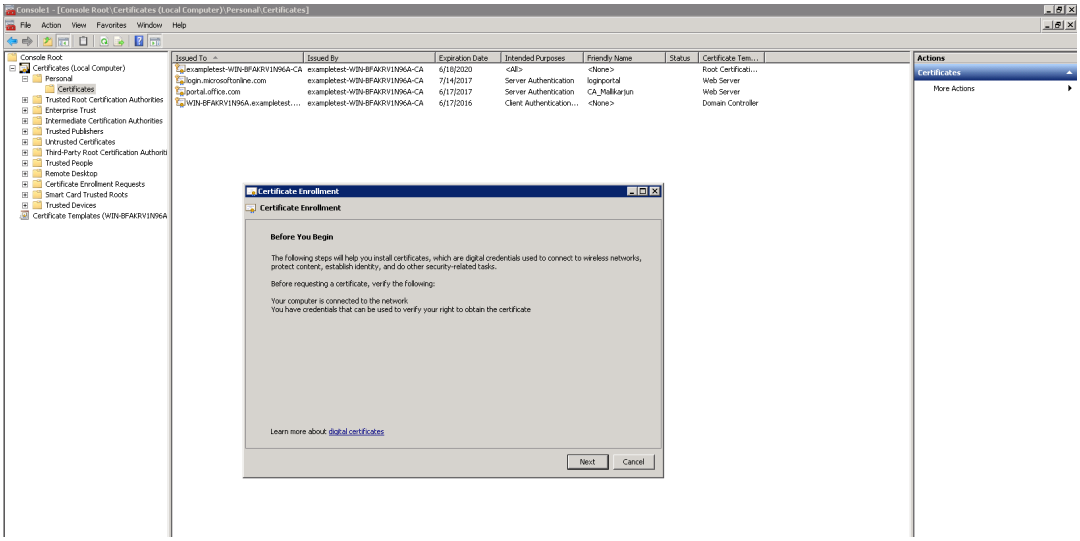
Office365 アクセラレーションを構成する

Office 365 アクセラレーションを構成するには:

1. 「セキュアピアリング *(/en-us/citrix-sd-wan-wanop/11-1/secure-traffic-acceleration/secure-peering.html)*」の説明に従って、*2 つの Citrix SD-WAN[WANOP アプライアンス間のセキュアピアリング関係を設定します]*。
2. 新しい証明書を作成します。

> 注
>
> サーバー側の Citrix SD-WAN WANOP アプライアンスは Office365 とクライアント間の仲介役として機能するため、これらの証明書はサーバー側のドメインコントローラーによって署名されますが、Office356 ドメインを参照します。

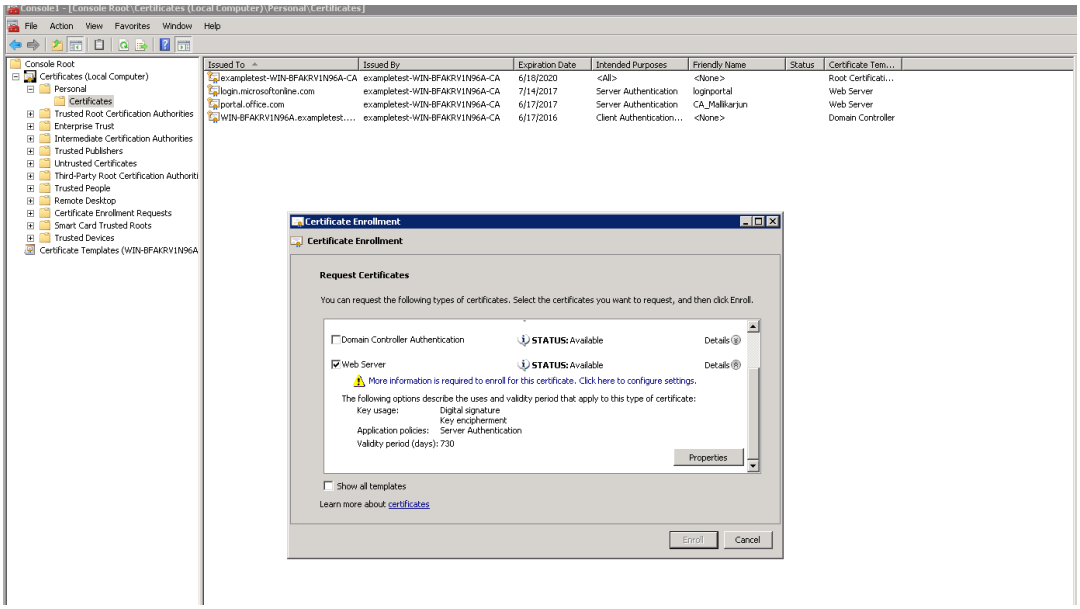
   a) Windows ドメインの 認証局サーバーに ログオンします。
   b) 必要に応じて、証明機関、証明書テンプレート、および 証明書のスナップインを追加します。
   c) 証明書テンプレート > **Web** サーバーのプロパティ > セキュリティに移動しすべてのオプションを選択します。
   d) 証明書 > 個人 > 証明書（コンピューター）> すべてのタスク > 新しい証明書をリクエストに移動します。



e) [証明書の登録] ウィンドウで、[次へ] をクリックします。

f) **[**証明書の登録ポリシー**]** ウィンドウで 、**Active Directory** の登録ポリシーを選択します。

g) [**Active Directory** 登録ポリシー**]** ウィンドウで、[**Web** サーバー**]**> 詳細 > プロパティを 選択します。



3. Office365 証明書から新しい証明書に情報をコピーします。最終的に、3 つの Office365 証明書から 1 つの証明書が作成されます。次の手順に従います。

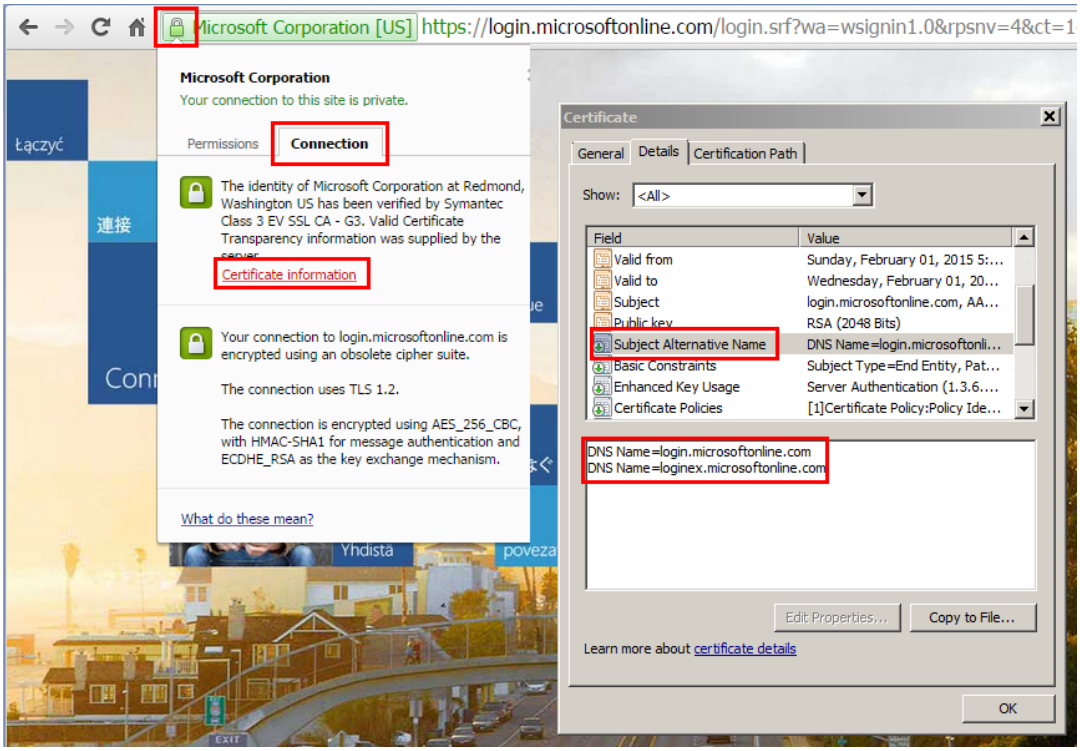
   a) Chrome などのブラウザで、URL を入力します- https://login.microsoftonline.com 。

   > 注
   >
   > ログインしないでください。

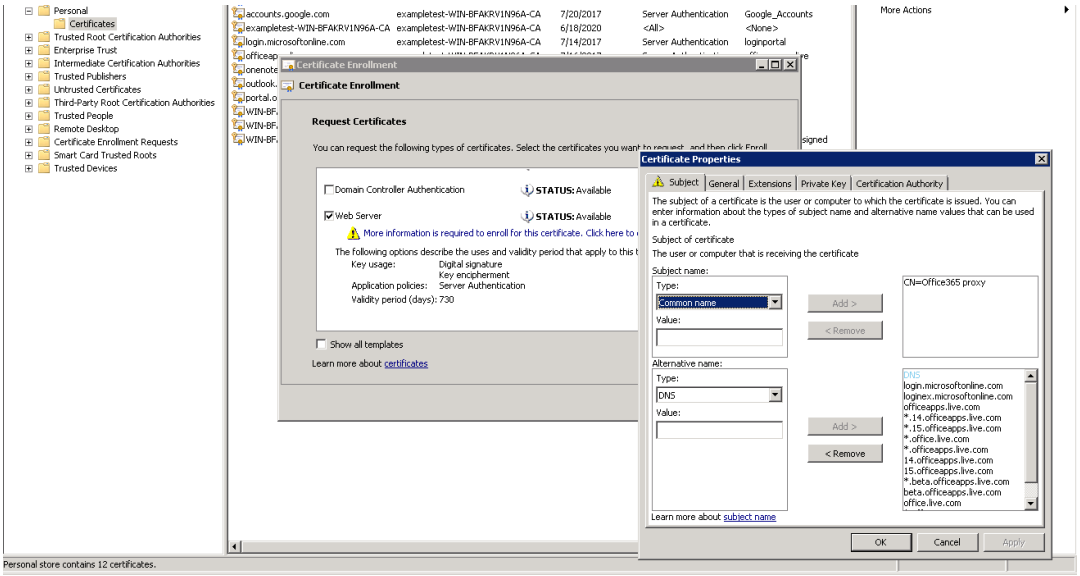
   b) URL バーの南京錠アイコンをクリックして [接続**]**> 証明書情報 > 詳細 を選択します。

> 注
>
> これらの手順は Chrome ブラウザ向けです。手順は他のブラウザでも同じです。

c) [サブジェクト代替名] をクリックすると、「login.microsoftonline.com」などの DNS 名のリストが表示されます。その下のテキストボックスに情報をコピーします。

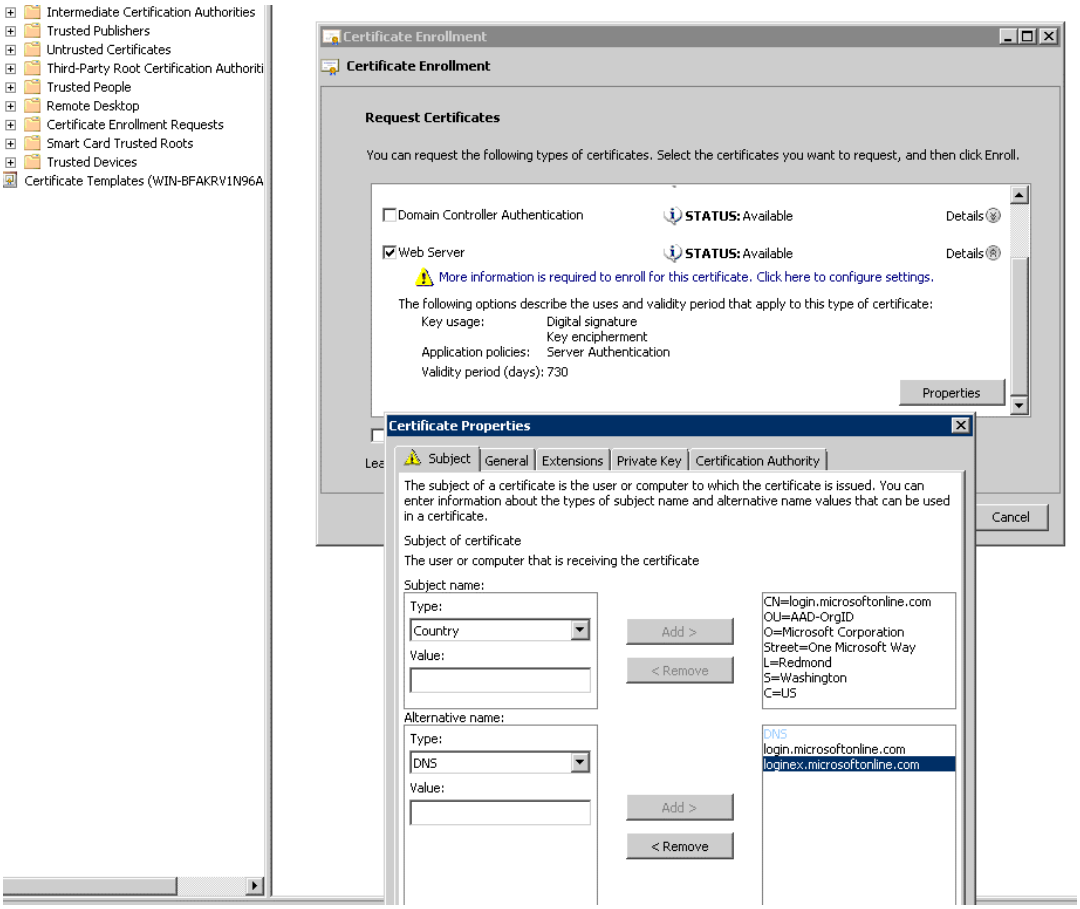


d) 新しい証明書の [証明書のプロパティ] ウィンドウに戻ります。Microsoft 証明書の各代替名と一致するように、**DNS** としてタイプを使用して [値] フィールドに代替名を追加します。



e) サブジェクト代替名を検出し、それらを https://outlook.office365.com、https://portal.office.com、https://office.live.com、および https://sharepoint.com 証明書に追加するプロセスを繰り返します（SharePoint URL は顧客固有です）。

f) 新しい証明書の共通名を作成します。上記の例は、「Office365 プロキシ」という一般名を示しています。

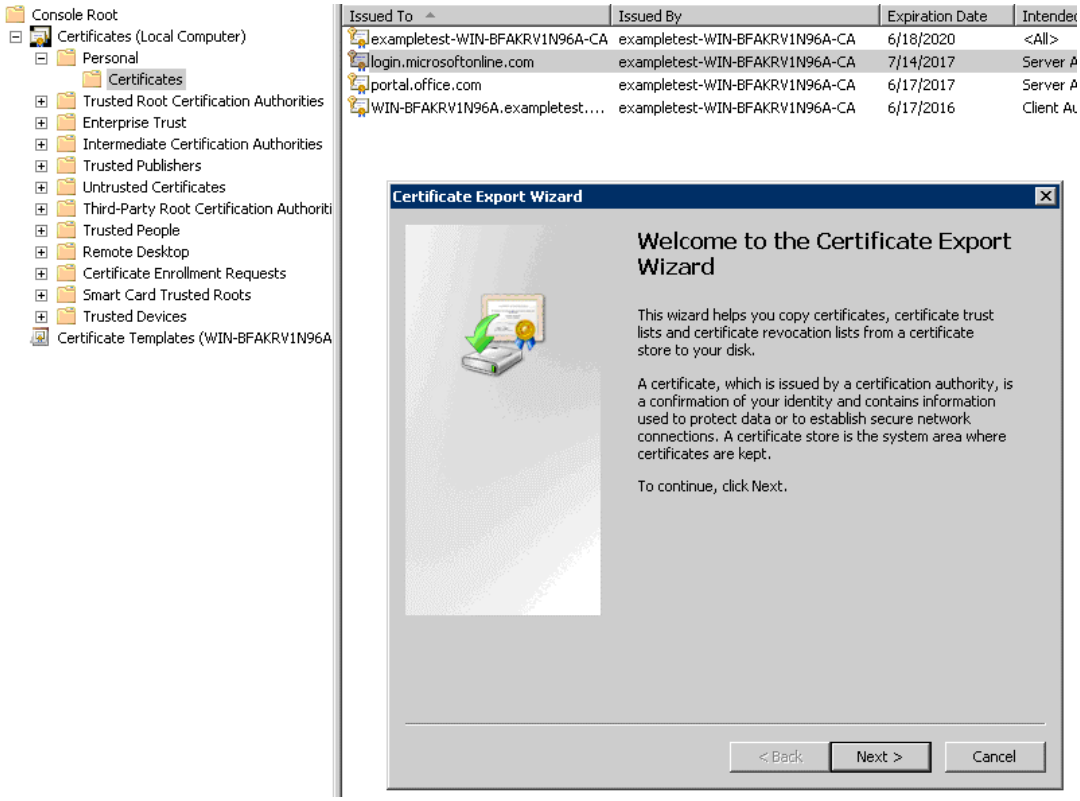


g) [秘密鍵] タブで、[秘密鍵をエクスポート可能にする] を選択します。

h) [**OK**]、[登録]、[完了] の順にクリックします。

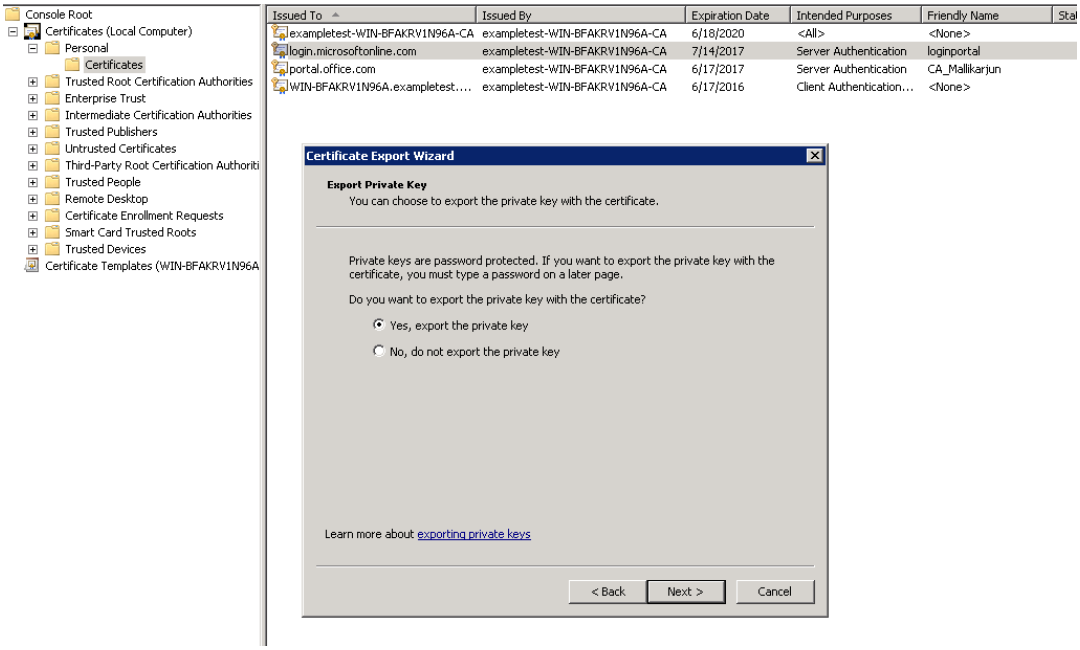
4. 証明書をエクスポートします。

a) 証明書の 下 > 個人 > 証明書、上記で作成したプロキシ証明書を選択し、[すべてのタスク] を選択します > エクスポート。



b) 証明書のエクスポートウィザード が表示されます。[次へ] をクリックします。

c) **[**秘密キーのエクスポートでは 、**[**はい] オプションを選択し、秘密鍵をエクスポートし、[次へ] をクリックします。

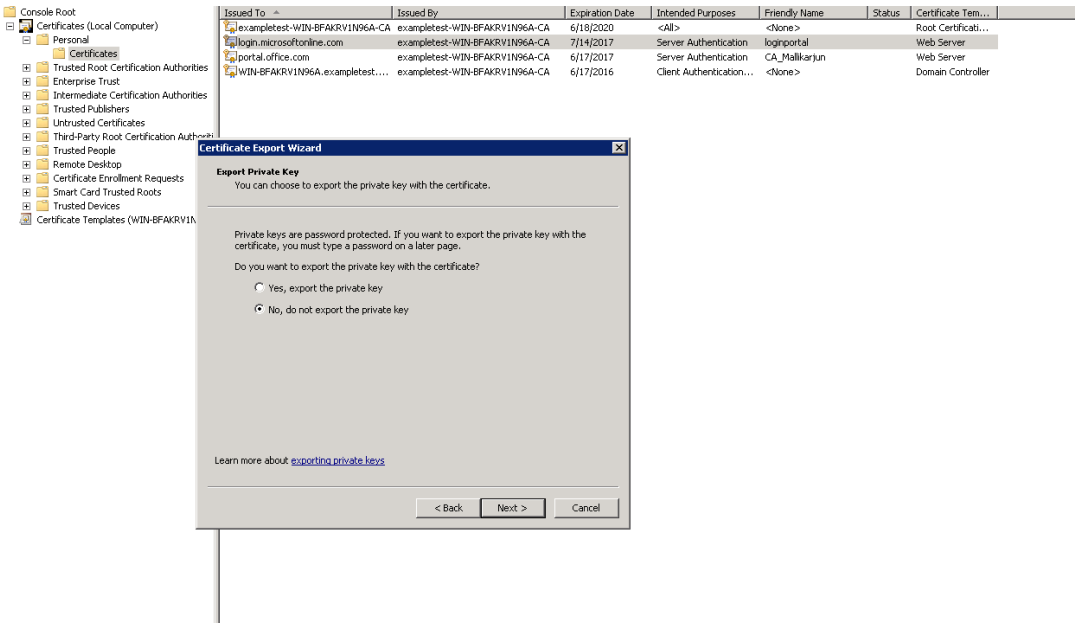


d) エクスポートファイル形式のデフォルト値を保持します。

e) パスワードを入力して確認し、秘密鍵をエクスポートして、証明書を *loginportal.pfx* として保存します。

5. 証明書をエクスポートします。

a) 証明書のエクスポートウィザードで、[次へ] をクリックします。[秘密鍵のエクスポート] で、[いいえ、秘密鍵をエクスポートしない] オプションを選択します。[次へ] をクリックします。



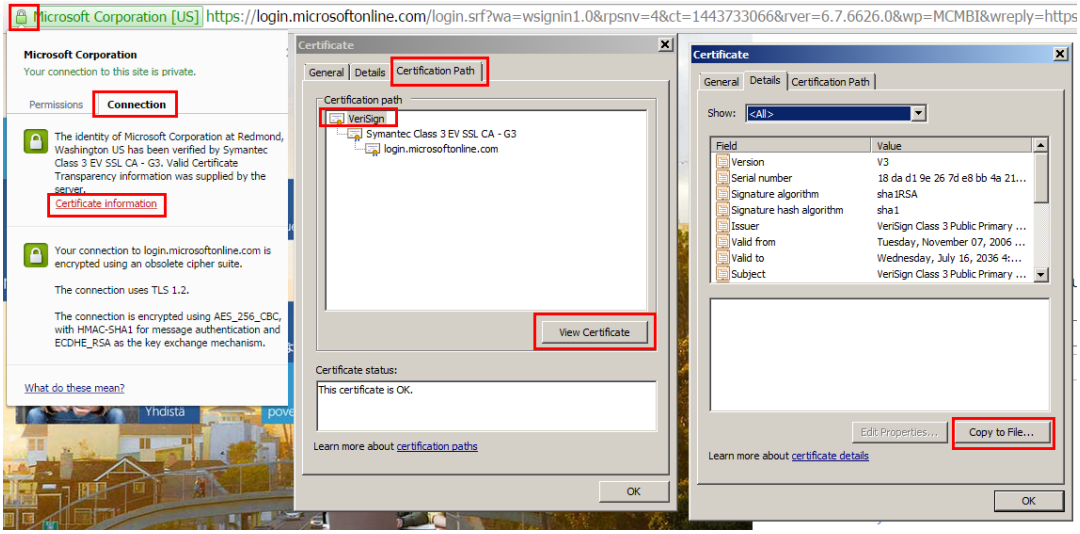
b) エクスポートファイル形式のデフォルト値を保持します。

c) パスワードを入力して確認し、秘密鍵と証明書をエクスポートして、ファイルを次のようなファイル名のファイルに保存します。office365_keys.pfx。

6. Microsoft 証明書のルート CA と中間 CA の公開鍵をダウンロードします。

a) ブラウザーで、https://login.microsoftonline.comに移動します。ブラウザの南京錠アイコンをクリックします。接続 > 証明書情報 > 認定パスに移動します。

b) ルート証明書（リストの一番上にあるもの）を選択し、[証明書の表示] > 詳細 > ファイルにコピーしますをクリックします。証明書のエクスポートウィザード が表示されます。[次へ] をクリックします。



c) ファイル名を入力してファイルを保存します。

> 注
>
> または、Wireshark または OpenSSL を使用して、ルートおよび中間 CA 名を取得し、「AUTHENTIC」ソース（Windows SSL ストアなど）から証明書を取得することもできます。

d) 手順 6 を繰り返して、次のドメインのルート CA と中間 CA を保存します。

   i. login.microsoftonline.com

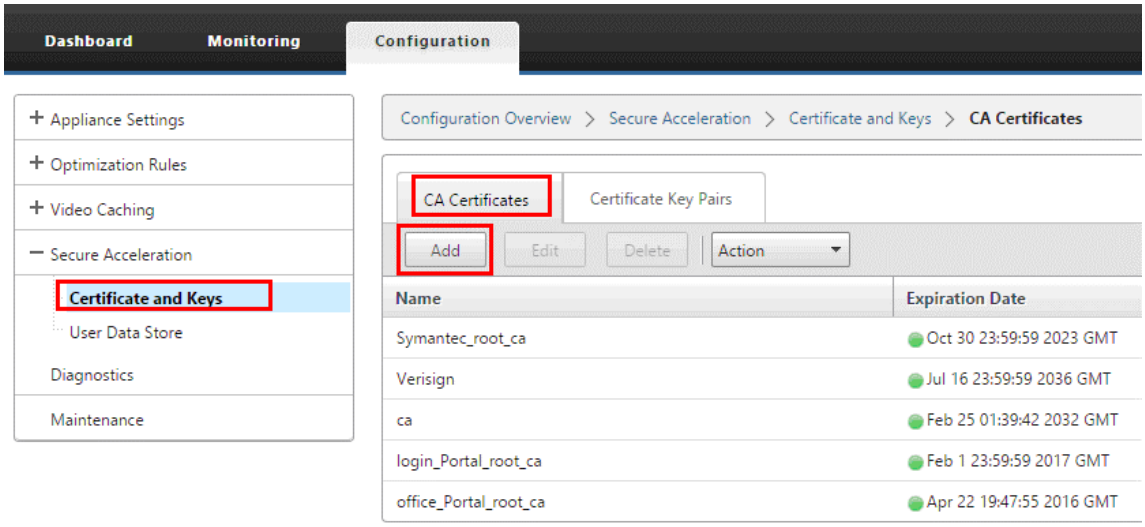
   ii. portal.office.com

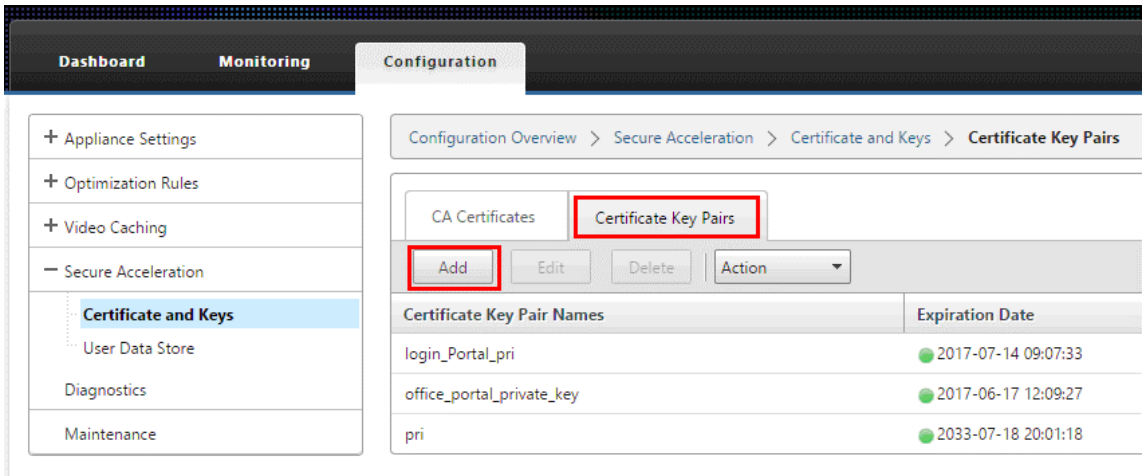
   iii. outlook.office356.com

   iv. *.sharepoint.com

   v. office.live.com

7. すべての Office365 サーバー CA、プロキシ証明書/キーペア、およびサーバー側の Citrix SD-WAN WANOP アプライアンスへの秘密鍵を追加します。CA は、[証明書とキー**]** ページの [**CA** 証明書] タブを使用して追加されます。証明書と certificate/key ペアが追加されます Certificate/Key [ペア] タブ。





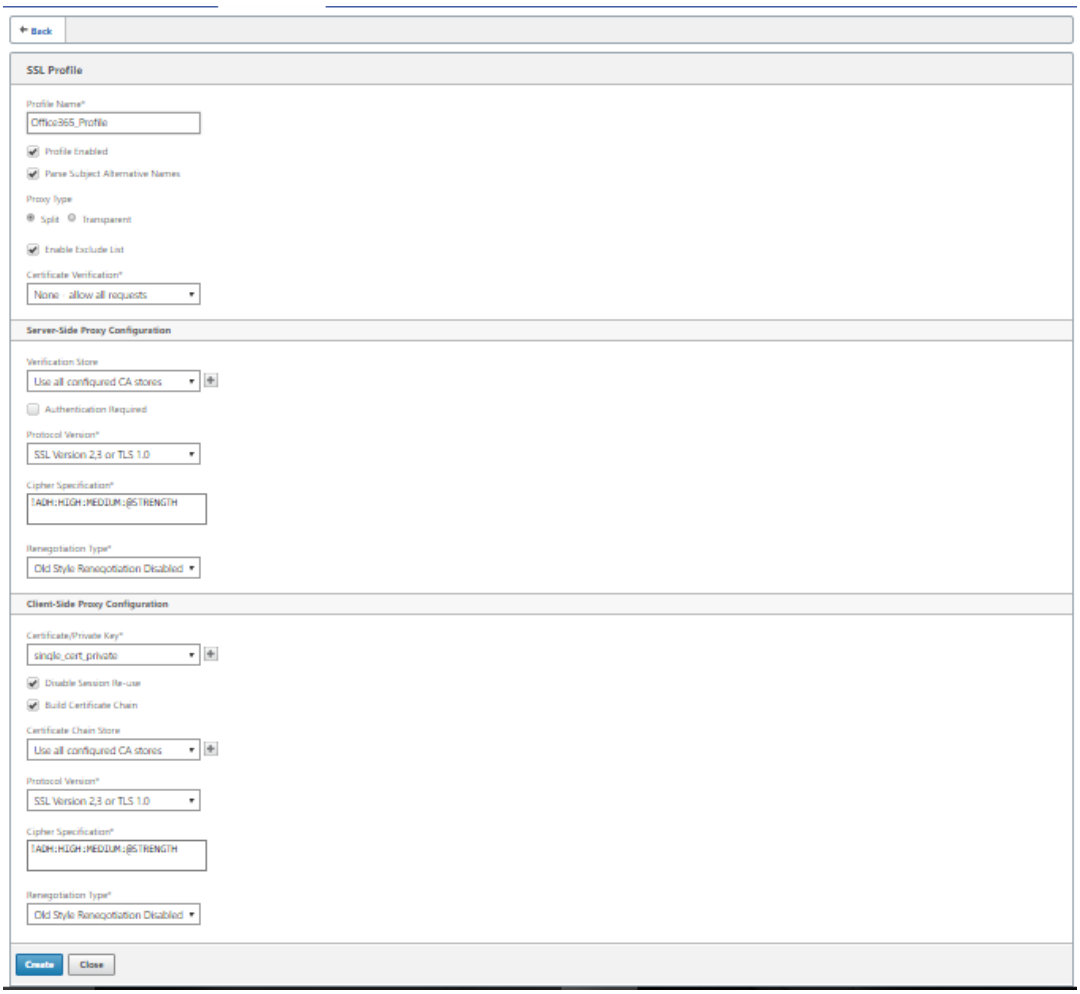
8. SSL スプリットプロキシプロファイルを作成し、スプリットプロキシを Web（Internet-Secure）サービスクラスにバインドします。

   a) 構成 > 安全な加速 > **SSL** プロファイル > プロファイルを追加に移動します。

   b) 選択したプロファイル名を入力します。プロファイル有効、解析サブジェクト 代替名、および スプリットプロキシを選択 します。

   c) サーバー側のプロキシ構成の 下 > 検証ストアで、[構成済みのすべての **CA** ストアを使用する] を選択します。

   d) クライアント側のプロキシ構成の 下 > Certificate/Private キー、以前に作成およびエクスポートした cert/private キーペア（例では loginportal.pfx として示されているもの）を選択します。[証明書チェーンの構築] を選択します。certificate/key 証明書チェーンストアの下のペアに関連付けられている CA を選択します。

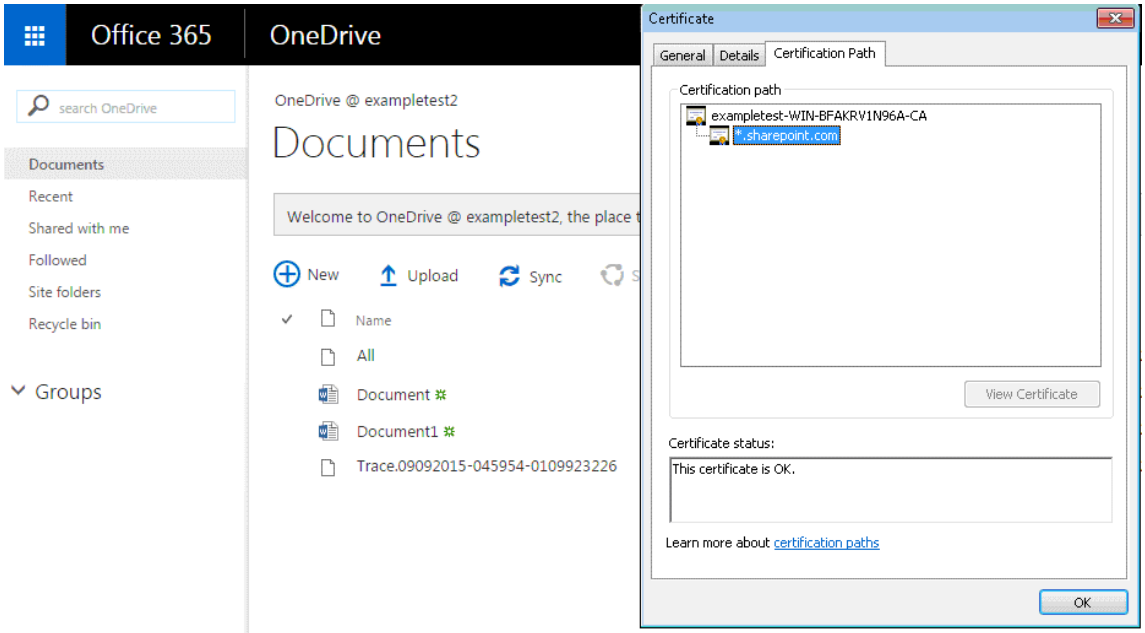


9. 作成した SSL プロファイルをインターネット（Web-Secure）サービスクラスにバインドします。構成 するためのナビゲート > 最適化ルール > サービスクラス を作成し、SSL プロファイルを SSL プロファイルリストに追加します。

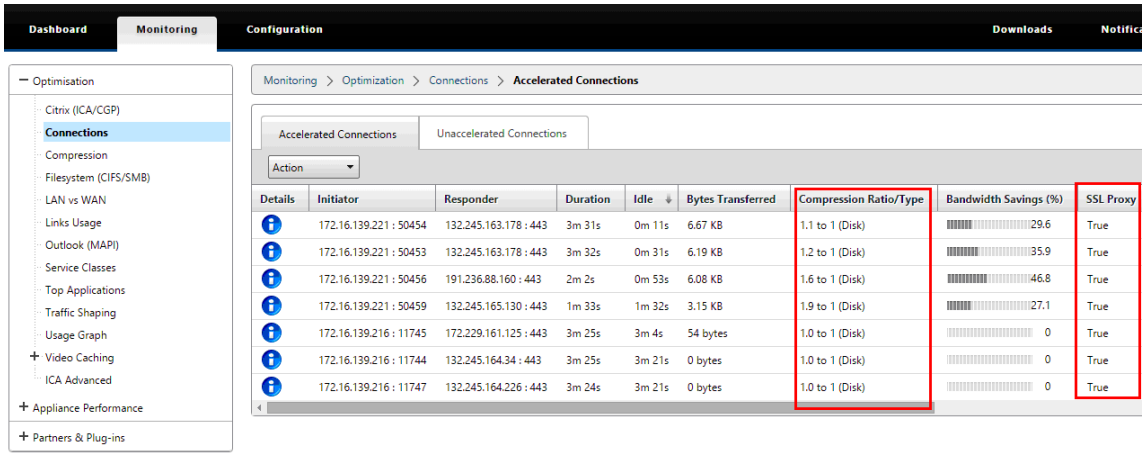
10. インターネット（**Web-Secure**）サービスクラスのアクセラレーションとディスクベースの圧縮を有効にします。

11. ブラウザから Office365 セッションを開始します。

    接続が高速化されます。ブラウザーでは、証明書に、実際の Office 365 証明書ではなく、ルート CA がサーバー側アプライアンスの CA 証明書として表示されます。



12. アプライアンスの 監視について > **[接続]** ページで、Office 365 接続が圧縮され、SSL アクセラレーションを受信していることを確認します。



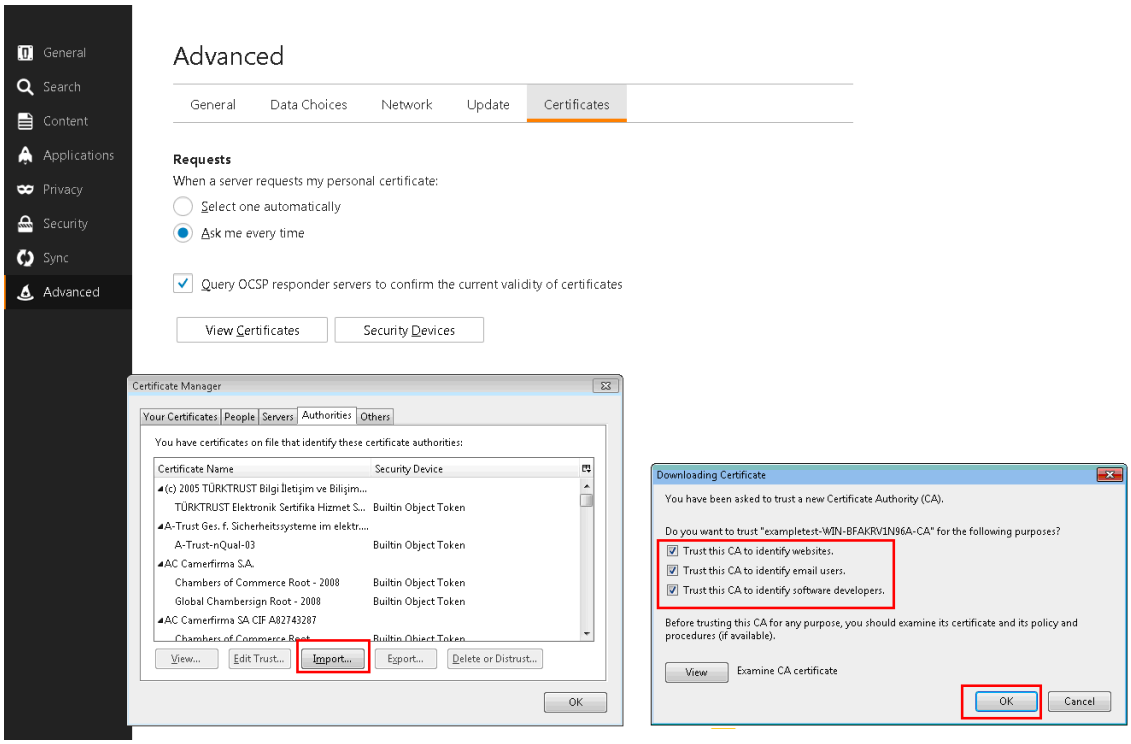
> 注
>
> Firefox はデフォルトでデバイスの証明書を受け入れませんが、独自の証明書ストアを持っています。したがって、他のブラウザやデバイス全体で通常の Windows ドメインの動作で受け入れられる資格情報は、Firefox に手動でインストールする必要があります。Firefox に証明書をインストールするには、「Firefox への証明書のインストール」セクションの手順に従います。

Firefox に証明書をインストールします

サーバー側アプライアンスのプロキシ証明書を Firefox 証明書ストアにインストールするには:

1. Firefox ブラウザで [オプション]> 高度な > 証明書 > 証明書を表示する > 当局 > インポートに移動します。

2. ローカル CA プロキシ証明書をアップロードし、証明書の ダウンロード ウィザードですべてのオプションを選択して、[**OK**] をクリックします。



SCPS サポート

April 19, 2021

Citrix SD-WAN WANOP は、SCPS（Space Communications Protocol Standard）TCP バリアントをサポートします。SCPS は衛星通信に広く使用されています。

一般的な SCPS 情報については、http://www.scps.org を参照してください。

SCPS は、衛星通信および同様のアプリケーションで使用される TCP バリアントです。[構成：チューニング] ページで [**SCPS**] オプションが選択されている場合、アプライアンスは SCPS 接続を高速化できます。

SCPS とデフォルトのアプライアンスの動作の主な実際的な違いは、標準の選択的確認応答（SACK）の代わりに SCPS スタイルの「選択的否定確認応答」（SNACK）が使用されることです。データ再送信を強化するこれらの 2 つの方法は相互に排他的であるため、接続の一方の端にあるアプライアンスで SCPS が有効になっていて、もう一方が有効になっていない場合、再送信のパフォーマンスが低下します。この状態は、「SCPS モードの不一致」アラートも引き起こします。

SCPS 対応アプライアンスと非 SCPS 対応アプライアンスを混在させる必要がある場合は、不一致が発生しないように展開してください。IP ベースのサービスクラスルールを使用するか、各パスに一致するアプライアンスが含まれるように展開を調整できます。

安全な交通加速

April 19, 2021

安全なトラフィックの加速は、安全なピアリングによって実現されます。いくつかの高度な機能では、リンクの両端にある Citrix SD-WAN WANOP アプライアンスが相互に 安全なピア関係 を確立し、SSL シグナリングトンネル（シグナリング接続とも呼ばれます）を設定する必要があります。これらの 関数は、SSL 圧縮、署名付き CIFS サポート、および暗号化された MAPI サポートです。

セキュアピアリングを有効にすると、ローカルアプライアンスとのセキュアピア関係を確立していないすべてのパートナーアプライアンス（および Citrix SD-WAN WANOP プラグインを実行しているコンピューター）の圧縮が自動的に無効になります。

安全なピア関係を確立するには、セキュリティキーと証明書を生成し、アプライアンス間に安全なシグナリングトンネルを設定する必要があります。トンネルを構成する前に、Citrix に暗号ライセンスを注文してください。

安全なピアリング

April 19, 2021

アプライアンスでセキュアピアリングが有効になっている場合、セキュアピア関係がないパートナーとの接続は暗号化または圧縮されませんが、TCP フロー制御アクセラレーションは引き続き使用できます。保護されたパートナーからの圧縮履歴に保存されたデータを保護されていないパートナーと共有できないようにするために、圧縮は無効になっています。

接続の一方の端にあるアプライアンスは、もう一方のアプライアンスでセキュアピアリングが有効になっていることを検出すると、SSL シグナリングトンネルを開こうとします。2 つのアプライアンスがこのトンネルを介して相互に正常に認証された場合、それらは安全なピアリング関係にあります。2 つのアプライアンス間のすべての高速接続は暗号化され、圧縮が有効になります。

> 注
>
> セキュアピアリングが有効になっているアプライアンスは、セキュアでないパートナーへの接続を圧縮しません。同じアプライアンスをセキュアなパートナーとセキュアでないパートナーが混在して正常に使用することは困難です。加速ネットワークを設計するときは、この点に注意してください。

セキュリティパラメータにアクセスするには、キーストアのパスワードが必要です。このキーストアのパスワードは、セキュリティ管理を他のタスクから分離できるように、管理者のパスワードとは異なります。キーストアのパスワードがリセットされると、既存の暗号化されたデータと秘密鍵はすべて失われます。

アプライアンスが盗まれた場合でもデータを保護するには、アプライアンスを再起動するたびにキーストアのパスワードを再入力する必要があります。これが行われるまで、セキュアピアリングと圧縮は無効になります。

セキュリティキーと証明書を生成する

Citrix SD-WAN WANOP 製品は、SSL シグナリングトンネルに必要なキーと証明書なしで出荷されます。自分で生成する必要があります。資格情報を生成するための通常のプロセスを介して、または http://www.openssl.orgの「openssl」パッケージを使用して、キーと証明書を生成できます。

テストの目的で、秘密鍵（これも生成します）に基づいて自己署名 X509 証明書を生成して使用できます。本番環境では、信頼できる認証局を参照する証明書を使用します。次の例では、PC のコマンドラインから openssl を呼び出して、秘密鍵（
my.key）と自己署名証明書（
my.crt）を生成します。

```
pre codeblock
# Generate a 2048-bit private key
openssl genrsa -out my.key 2048
# Now create a Certificate Signing Request
openssl req -new -key my.key -out my.csr
# Finally, create a self-signed certificate with a 365-day expiration
openssl x509 -req -days 365 -in my.csr -signkey my.key -out my.crt
```

本番環境で使用する場合は、組織のセキュリティポリシーを参照してください。

安全なピアリングを構成する

安全なピアリングを確立するには、次の 2 つの方法があります。

1. アプライアンスによって生成された資格情報を使用します。
2. 自分で提供した資格情報を使用します。

   セキュアピアリングが有効になっているアプライアンスは、セキュアピアリング関係にあるパートナーアプライアンスとの接続のみを圧縮するため、この手順はすべてのアプライアンスに同時に適用する必要があります。

安全なピアリングのためにアプライアンスを準備するには:

ネットワーク内の各アプライアンスで次の手順を実行します。

1. アプライアンスに暗号ライセンスをインストールします。暗号ライセンスがないと、安全なアクセラレーションは利用できません。

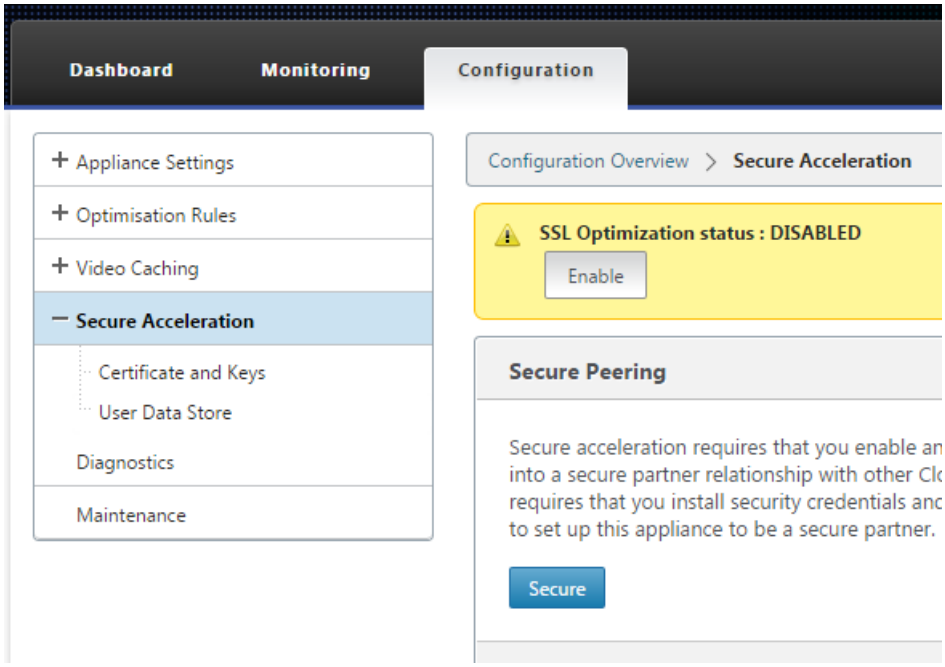
   a) まだ行っていない場合は、Citrix から暗号ライセンスを取得してください。

   b) ネットワークライセンスサーバーを使用している場合は、構成 > アプライアンスの設定 > ライセンスに移動します。[ライセンス の追加] セクションで [編集] をクリックし、[リモートライセンスサーバー] を選択して [暗号ライセンスをオン] に設定します。

   c) ローカルライセンスを使用している場合は、[構成]> アプライアンスの設定 > ライセンス に移動します。[ライセンス の追加] ページで、[ローカルライセンスサーバー] オプションをクリックし、[追加] をクリックしてローカル暗号ライセンスをアップロードします。

d) 構成 > アプライアンスの設定 > ライセンスページでのライセンスのインストールが成功したことを確認します。[ライセンス情報] で、暗号化ライセンスがアクティブであり、将来の有効期限が設定されていることを示す必要があります。

2. 構成 > **SecureAcceleration** ページに移動します。ページに「セキュア」というラベルの付いたボタンがある場合は、それをクリックします。



3. キーストア設定画面が自動的に表示される場合は、次の手順を実行します。

   a) キーストアのパスワードを 2 回入力し、[保存] をクリックします。

   b) 画面が更新されて [SecurePeering Certificates and Keys] セクションが表示されたら、[Enable Secure Peering and CA Certificate] をクリックし、[Save] をクリックします。

   c) 手順 6 にスキップします。

4. [キーストア設定] 画面が自動的に表示されない場合は、[セキュアピアリング] の下の鉛筆アイコンをクリックしてから、[キーストア設定] の下の鉛筆アイコンをクリックします。「キーストアステータス」プルダウンメニューで開き、キーストアパスワードを 2 回入力します。[保存] をクリックします。

5. 構成 > **Secure Acceleration** ページに移動して、安全なピアリングを有効にし、**Enable** ボタンをクリックします。この段階では警告を無視してください。この設定により、必要な追加構成が完了したときに安全なピアリングが有効になります。

6. 構成 > **Secure Acceleration User DataStore** に移動して、圧縮履歴の暗号化を有効にし、鉛筆アイコンをクリックします。[ディスク暗号化を有効にする] をクリックし、[保存] をクリックします。ユーザーデータストアの暗号化により、アプライアンスが盗まれたり工場に返送されたりした場合に、ディスクベースの圧縮履歴が不正に読み取られるのを防ぎます。ディスクデータ暗号化のセキュリティは、キーストアのパスワード

に依存しています。この機能は AES-256 暗号化を使用します。（ディスクデータの暗号化は、ディスク全体を暗号化するのではなく、圧縮履歴のみを暗号化します。）

7. アプライアンスで生成された資格情報を使用している場合は、次の手順にスキップしてください。独自の資格情報を使用している場合は、次の手順を実行します。

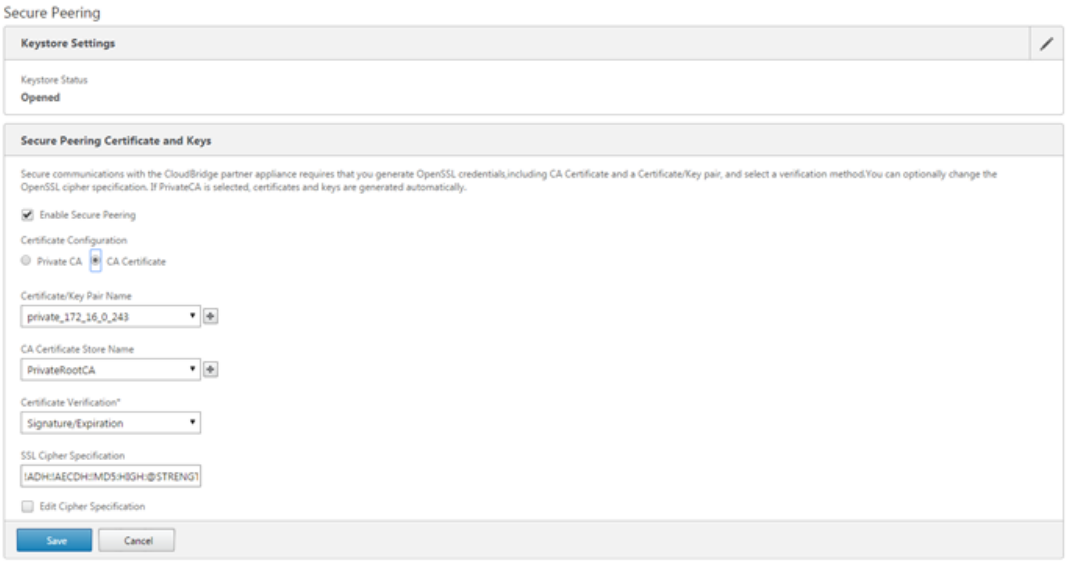
   a) 構成 > **Secure Acceleration** をクリックし、Secure Peering の下の鉛筆アイコンをクリックしてから、**Secure Peering Certificates andKeys** の下の鉛筆アイコンをクリックします。[安全なピアリングと証明書の構成を有効にする**]>CA** 証明書をクリックします。資格情報の指定フィールドが表示されます。

   b) **Certificate/Key** ペア名で、**+** アイコンをクリックしてこのアプライアンスの cert/key ペアをアップロードまたは貼り付けます。資格情報で必要な場合は、キーパスワードまたはファイルパスワードも入力します。［作成］をクリックします。

   c) **CA Certificate Store Name** で、**+** アイコンをクリックしてこのアプライアンスの CA Certificate をアップロードまたは貼り付けます。

   d) 組織で特に要求されない限り、[証明書の検証] フィールドと [SSL 暗号化仕様] フィールドのデフォルト値を保持します。

   e) ［保存］をクリックします。



8. 残りのアプライアンスについても繰り返します。
9. 自分で指定した資格情報を使用している場合は、安全なピアリングの構成が完了しています。
10. アプライアンスで生成された資格情報を使用している場合は、次の手順を実行します。

アプライアンスで生成された資格情報で安全なピアリングを使用するには:

1. 上記の「ピアリングを保護するためのアプライアンスの準備」手順を使用して、この手順のためにアプライアンスを準備します。

2. 1 つのデータセンターアプライアンスで、[構成]>**Secure Acceleration** を選択し、[**Enable**] ボタンがある場合はそれをクリックして、安全なピアリングを有効にします。
3. セキュアピアリングの下の鉛筆アイコンをクリックします。キーストアが開いている必要があります。そうでない場合は、今すぐ開きます。
4. **Secure Peering Certificate andKeys** の下にある鉛筆アイコンをクリックします。[セキュアピアリングとプライベート **CA** を有効にする] オプションをクリックし、[保存] をクリックします。これにより、ローカルの自己署名 CA 証明書とローカルの証明書とキーのペアが生成されます。
5. 接続されたピアの下 **+** をクリックします。リモートアプライアンスの 1 つの IP アドレス、管理者のユーザー名、および管理者のパスワードを入力し、[接続] をクリックします。これにより、リモートアプライアンスの CA 証明書と証明書とキーのペアが発行され、リモートアプライアンスにコピーされます。

   > 注
   >
   > SD-WAN WANOP アプライアンスの場合、IP アドレスは、Web アクセスが有効になっている任意のインターフェイスの IP アドレスにすることができます。SD-WAN PE アプライアンスの場合、IP アドレスは管理 IP アドレスです。

6. 他のリモートアプライアンスに対してこのプロセスを繰り返します。
7. データセンターアプライアンスで、**[** 監視**]**> パートナーとプラグイン > 安全なパートナーに移動して 接続を確認します。リモートアプライアンスごとに、[セキュア] フィールドの内容が True であり、[接続ステータス] が [接続可能] である必要があります。

CIFS、SMB2、および MAPI

April 19, 2021

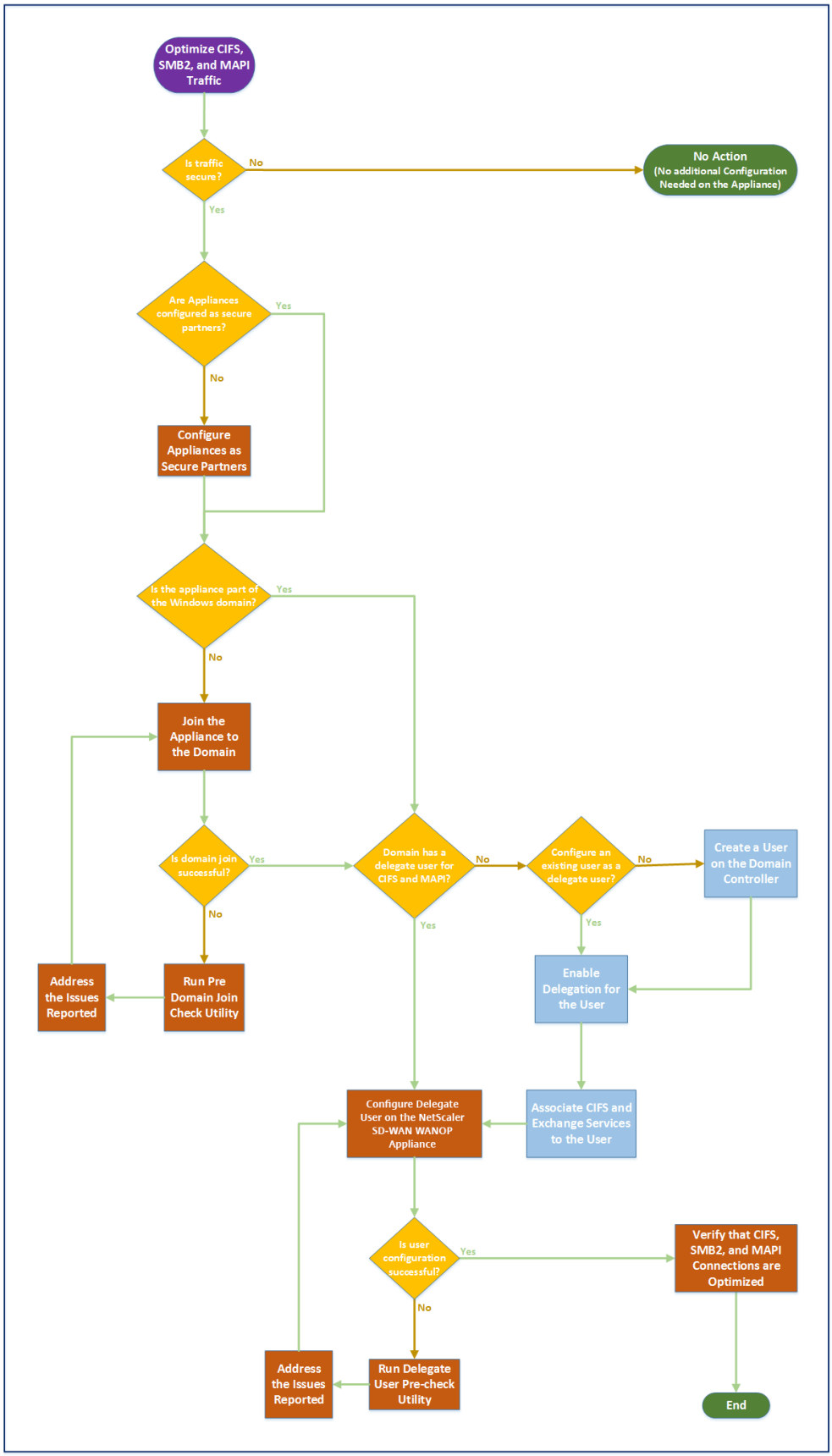
Windows は、ネットワークに展開される一般的なオペレーティングシステムの 1 つです。Windows オペレーティングシステムは、場所間で共有される分散リソースをサポートします。たとえば、データセンター内のリソースにさまざまなブランチオフィスからアクセスできるようにすることができます。ネットワーク経由でアクセスする場合、Windows は共有ファイルにアクセスするために Common Internet File System（CIFS）プロトコルを使用し、MicrosoftOutlook を介して電子メールにアクセスするために MessagingApplication Programming Interface（MAPI）プロトコルを使用します。つまり、Windows は CIFS ベース（Windows および Samba）のファイル転送とディレクトリブラウジングに CIFS プロトコルを使用し、Microsoft Outlook は MAPI プロトコルを使用して Outlook データにアクセスします。

Citrix SD-WAN WANOP アプライアンスを使用して、ネットワークを介した CIFS、サーバーメッセージブロックバージョン 2（SMB2）、および MAPI 接続を最適化できます。

Citrix SD-WAN WANOP アプライアンスは、Windows オペレーティングシステムのサポートに加えて、NetApp および Hitachi ストレージシステム上の CIFS および SMB2 をサポートします。

以下のフローチャートは、CIFS、SMB2、および MAPI トラフィックを最適化するために Citrix SD-WAN WANOP アプライアンスを構成するための完全な手順を示しています。

CIFS、SMB2、および MAPI トラフィックを最適化するための Citrix SD-WAN WANOP アプライアンスの構成



安全な **Windows** トラフィックを最適化するように **Citrix SD-WAN WANOP** アプライアンスを構成する

April 19, 2021

署名された Windows ファイルシステムと暗号化された MAPI を最適化する前に、Citrix SD-WAN WANOP アプライアンスを Windows セキュリティインフラストラクチャに追加する必要があります。Outlook/Exchange トラフィック。

最近の Windows リリースで Windows セキュリティシステムが強化された結果、クライアントとサーバーはデータを認証および暗号化することでトラフィックを保護します。これには、署名された Windows ファイルシステムと暗号化された MAPI Outlook/Exchange トラフィックを最適化する前に、Citrix SD-WAN WANOP アプライアンスが Windows セキュリティインフラストラクチャの信頼できるメンバーである必要があります。

アプライアンスを Windows セキュリティインフラストラクチャに追加すると、アプライアンスには次の機能があります。

- 署名付き SMB および署名付き SMB2 プロトコルを使用した、Microsoft Windows サーバー、NetApp サーバー、および HitachiHNAS のファイルサーバートラフィックの高速化。
- 暗号化された MAPI または RPC over HTTPS を使用して Outlook クライアントからアクセスされた場合の Microsoft Exchange サーバートラフィックの高速化。

Citrix SD-WAN WANOP アプライアンスが **Windows** セキュリティシステムでどのように機能するか

アプライアンスを Windows ドメインに参加させるには、管理者の資格情報が必要です。Windows ドメインに参加すると、アプライアンスはドメインの信頼できるメンバーになります。これにより、アプライアンスをドメインのセキュリティインフラストラクチャのメンバーとして宣言できます。

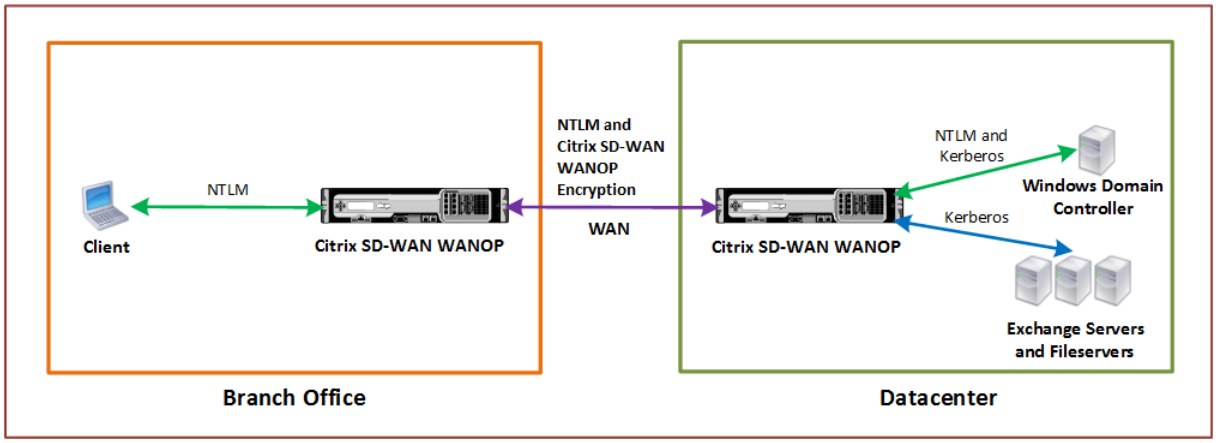
アプライアンスが Windows セキュリティインフラストラクチャの一部になった後、ユーザーがリソースにアクセスする前に認証を受ける必要があります。ドメイン内に多数のユーザーを構成することの難しさを回避するために、認証の責任を委任ユーザーに委任できます。

ActiveDirectory にデリゲートユーザーを作成します。このユーザーは通常のユーザーに似ていますが、特別な権限があります。デリゲートユーザーを作成した後、Citrix SD-WAN WANOP アプライアンスでこのユーザーを構成する必要があります。アプライアンスは、ユーザーが CIFS や MAPI などの Windows プロトコルを使用して認証および暗号化されたデータストリームにアクセスするときに、デリゲートユーザーを使用してユーザーに代わって認証します。

CIFS および MAPI トラフィックを高速化するために、標準の Windows 委任メカニズムを使用すると、セキュリティ委任を関連するサービスに制限できます。この制約付きの委任は、Windows Server 2003 のリリース以降利用可能です。

ドメインの一部になった後、アプライアンスは安全な Windows トラフィックを加速します。Windows ドメインに参加するデータセンターアプライアンスは、リモートアプライアンスまたは Citrix SD-WAN WANOP プラグインとの安全なピア関係を持っている必要がありますが、Windows ドメインに参加するのはデータセンターアプライアンスのみです。CIFS または MAPI アクセラレーションの目的で、リモートアプライアンスはデータセンターアプライアンスのスレーブとして機能し、2 つの間の安全な SSL トンネルを介して制御されます。したがって、デリゲートユーザーの資格情報はデータセンターを離れません。

次の図は、このセットアップのトポロジ図の例を示しています。



上の図では、ブランチオフィスのクライアントがデータセンターのリソースにアクセスしています。別のドメインにあるブランチオフィスクライアントは、Windows セキュリティシステムの一部として NTLM 認証を使用します。安全なピア関係にある 2 つの Citrix SD-WAN WANOP アプライアンス間のすべての高速接続と同様に、WAN を介した CIFS または MAPI 接続と NTLM 認証は暗号化されます。Windows ドメインコントローラーのバージョンに応じて、データセンター Citrix SD-WAN WANOP アプライアンスからのユーザー要求は、NTLM または Kerberos 認証プロトコルを使用して認証されます。ドメインがユーザーを認証した後、Exchange サーバーおよびファイルサーバーへの後続のアクセス要求は Kerberos 認証プロトコルを使用します。次に、Citrix SD-WAN WANOP アプライアンスは、クライアントとサーバー間で確立された接続を最適化します。

アプライアンスに安全なピア関係がない場合、またはデータセンターアプライアンスがドメインに正常に参加していない場合、接続は TCP フロー制御アクセラレーションを使用します。これにより、セキュリティ操作、圧縮、またはデータ変換は実行されません。クライアントとサーバー間の接続は、Citrix SD-WAN WANOP アプライアンスが存在しないかのように確立されます。

Windows オペレーティングシステムでさまざまなクライアント認証モードを構成できます。Citrix SD-WAN WANOP アプライアンスが最適化する接続の種類は、構成するクライアント認証モードによって異なります。

次の表に、Windows の Windows クライアント認証モードと、対応する Citrix SD-WAN WANOP の最適化を示します。

Windows オペレーティングシステムでサポートされる認証と最適化

クライアントオペレーティングシステム	クライアント認証モード	最適化	コメント
Windows XP/Windows Vista/Windows7/Windows 8	認証のネゴシエーション（SPNEGO）	TCP フロー制御アクセラレーション、圧縮、CIFS プロトコルアクセラレーション	すべての Windows リリースで使用されるデフォルト設定。
Windows XP/Windows Vista/Windows 7/Windows 8	NTLM のみまたは Kerberos のみ	TCP フロー制御アクセラレーションのみ	デフォルト以外の認証モード

注：NTLM のみまたは Kerberos のみのクライアント認証モードを使用する場合、暗号化されていればトラフィックは高速化されません。

Citrix SD-WAN WANOP アプライアンスを **Windows** セキュリティシステムに追加するための要件

保護された Windows 署名付き SMB および暗号化された MAPI トラフィックのトラフィックを最適化するには、アプライアンスを Windows セキュリティインフラストラクチャに追加する前に、Citrix SD-WAN WANOP 展開が次の要件を満たしている必要があります。

- クライアント側とサーバー側の両方のアクセラレーションアプライアンスは、安全なピア関係を確立している必要があります。
- アプライアンスは、Windows ドメインサーバーの時刻と厳密に同期された NTP サーバーを使用する必要があります。理想的には、アプライアンスと Windows ドメインサーバーはすべて同じ NTP サーバーのクライアントです。
- Outlook は、（デフォルト以外の）**Kerberos** のみ または **NTLM** のみの オプション用に構成しないでください。アクセラレーションには、デフォルトの（ネゴシエートされた）オプションが必要です。
- クライアントとサーバーは、サーバー側アプライアンスのドメインと双方向の信頼関係を持つ任意のドメインのメンバーにすることができます。一方向の信頼はサポートされていません。
- ドメインのセキュリティインフラストラクチャに参加しているアプライアンスで使用するには、Kerberos デリゲートユーザーをドメインコントローラーに設定する必要があります。
- ドメインの DNS サーバーの IP アドレスを構成し、サーバー側のアプライアンスで到達可能にする必要があります。
- ドメインサーバーは完全に到達可能である必要があり、DNS サーバーで構成されたドメインコントローラーのすべての IP アドレスの順方向と逆方向の両方のルックアップが必要です。
- サーバー側の Citrix SD-WAN WANOP アプライアンスのホスト名は一意である必要があります。デフォルトのホスト名「hostname」を使用すると、問題が発生する可能性があります。

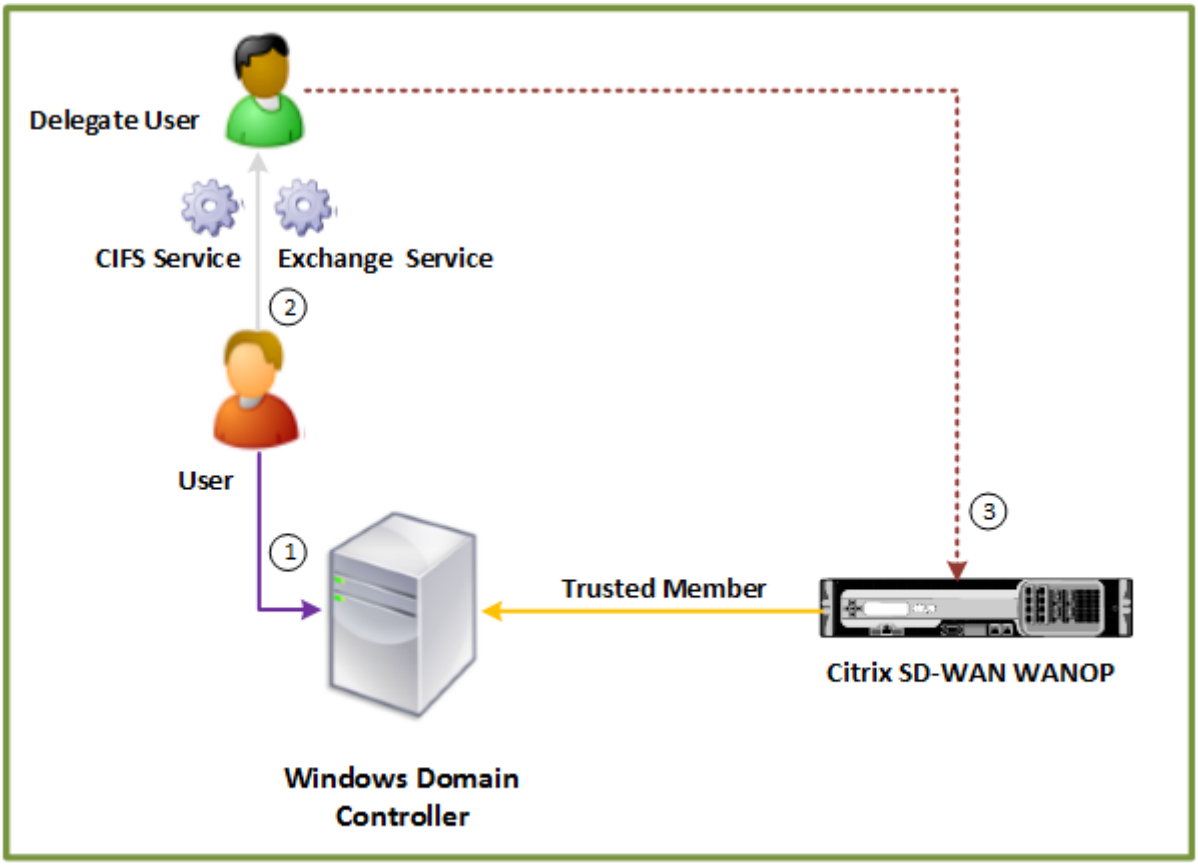
> 注
>
> Macintosh Outlook クライアントは MAPI を使用しません (Outlook/Exchange) 標準であり、この機能によって加速されません。

Citrix SD-WAN WANOP アプライアンスを **Windows** セキュリティインフラストラクチャに追加します

安全な Windows トラフィックを最適化するには、Citrix SD-WAN WANOP アプライアンスが Windows セキュリティシステムの一部であり、セキュリティシステムまたはドメインで自身を認証する必要があります。次の図に示すように、アプライアンスを Windows セキュリティシステムの一部にするには、アプライアンスをドメインに参加させる必要があります（管理者の資格情報を使用）。さらに、CIFS および Exchange サービスをそのユーザーに関連付けることにより、新規または既存のユーザーを委任ユーザーとして構成する必要があります。次に、Citrix SD-WAN WANOP アプライアンスでこのデリゲートユーザーを構成する必要があります。

プレドメインチェック ユーティリティを使用して、アプライアンスのドメインへの参加に問題があるかどうかを確認できます。

> 注
>
> Windows セキュリティシステムは、Exchange サービスを使用して MAPI 接続を管理します。安全な Windows トラフィックを最適化するためのセットアップの構成



Citrix SD-WAN WANOP アプライアンスを **Windows** ドメインに参加させます。

アプライアンスがドメインに参加すると、共有シークレットがドメインコントローラーと交換され、アプライアンスがドメインの一部であり続けることができます。アプライアンスをドメインに参加させるときは、ドメインコントローラーの管理者資格情報があることを確認してください。

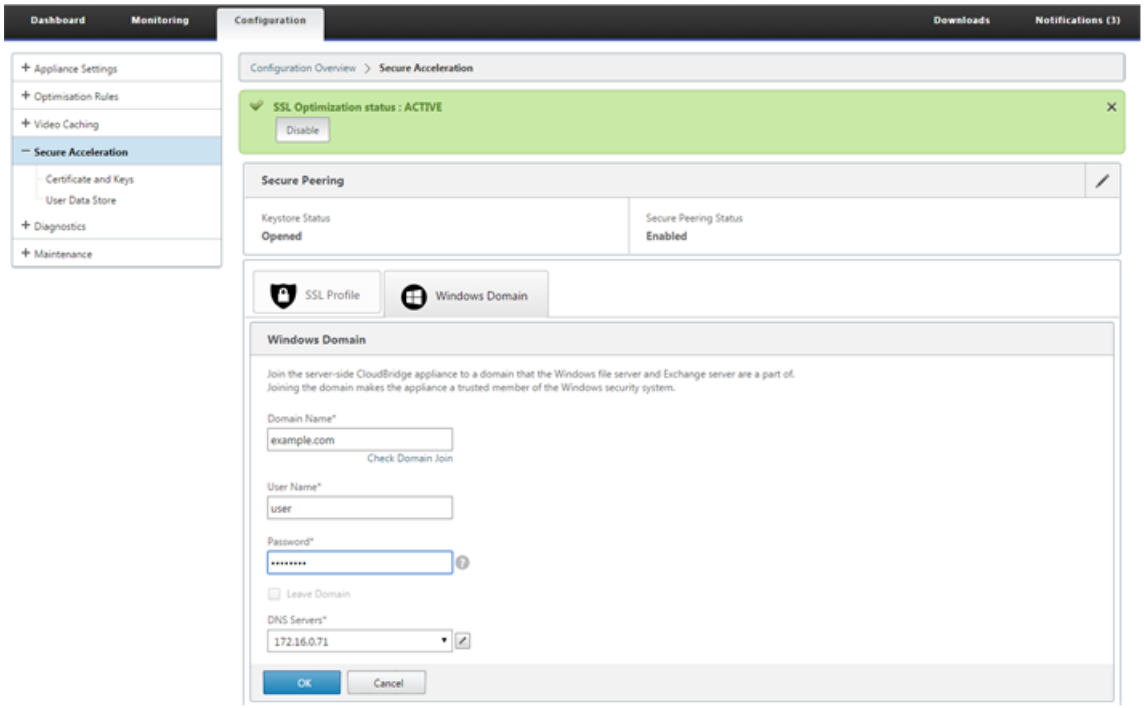
Citrix SD-WAN WANOP アプライアンスが CIFS および MAPI トラフィック（RPC over HTTPS としてカプセル化されたトラフィックを含む）を確実に最適化するには、アプライアンスを Windows ファイルサーバーおよび Exchange サーバーが含まれるドメインの一部にする必要があります。サーバー側アプライアンスをドメインに参加させる必要があります。

注：ドメイン管理資格情報はアプライアンスに保存されません。

Citrix SD-WAN WANOP アプライアンスを **Windows** ドメインに参加させるには:

1. 構成 > 安全な加速 > **Windows** ドメイン タブに移動します。
2. [**Windows** ドメインに参加] をクリックします。
3. [ドメイン名] フィールドに Windows ドメイン名を入力します。
4. [ユーザー名] フィールドに、ドメインコントローラー管理者のユーザー名を入力します。

5. [パスワード] フィールドで、ドメインコントローラーの管理者パスワードを指定します。
6. 必要に応じて、Windows ドメインとの整合性を保つために DNS サーバーを編集します。
7. [**OK**] をクリックします。
8. 以下の手順の説明に従って、[代理ユーザー] セクションで代理ユーザーを追加します。



デリゲートユーザーを構成する:

アプライアンスを Windows ドメインに参加させた後、アプライアンスがドメインでユーザーを認証するために使用できるユーザーを作成する必要があります。このユーザーは、デリゲートユーザーと呼ばれます。

注: デリゲートユーザーアカウントを作成するには、Windows ドメインコントローラーとアプライアンスへの管理者アクセスが必要です。Windows ドメインコントローラーへの管理者アクセス権がない場合は、権限のある管理者がドメインコントローラーで必要なタスクを実行していることを確認してください。

Kerberos 委任を使用してユーザー認証を設定するには、ドメインコントローラーで委任ユーザーを構成してから、このユーザーを Citrix SD-WAN WANOP アプライアンスに追加するという 2 つのタスクが必要です。

ドメインコントローラーでデリゲートユーザーを構成する:

Citrix SD-WAN WANOP アプライアンスでデリゲートユーザーを構成する前に、ドメインコントローラーで必要なプロパティを使用してデリゲートユーザーを構成する必要があります。デリゲートユーザーアカウントを作成するか、既存のユーザーアカウントをデリゲートユーザーアカウントとして使用できます。

アカウントを作成するか、既存のアカウントを選択した後、このユーザーの委任を有効にします。次に、デリゲートユーザーを CIFS および Exchange サービスに関連付けて、これらのサービスのトラフィックを高速化できるようにします。このユーザーを Citrix SD-WAN WANOP アプライアンスに追加すると、アプライアンスは、このアカウントに関連付けられているサービスの委任された資格情報を提示します。

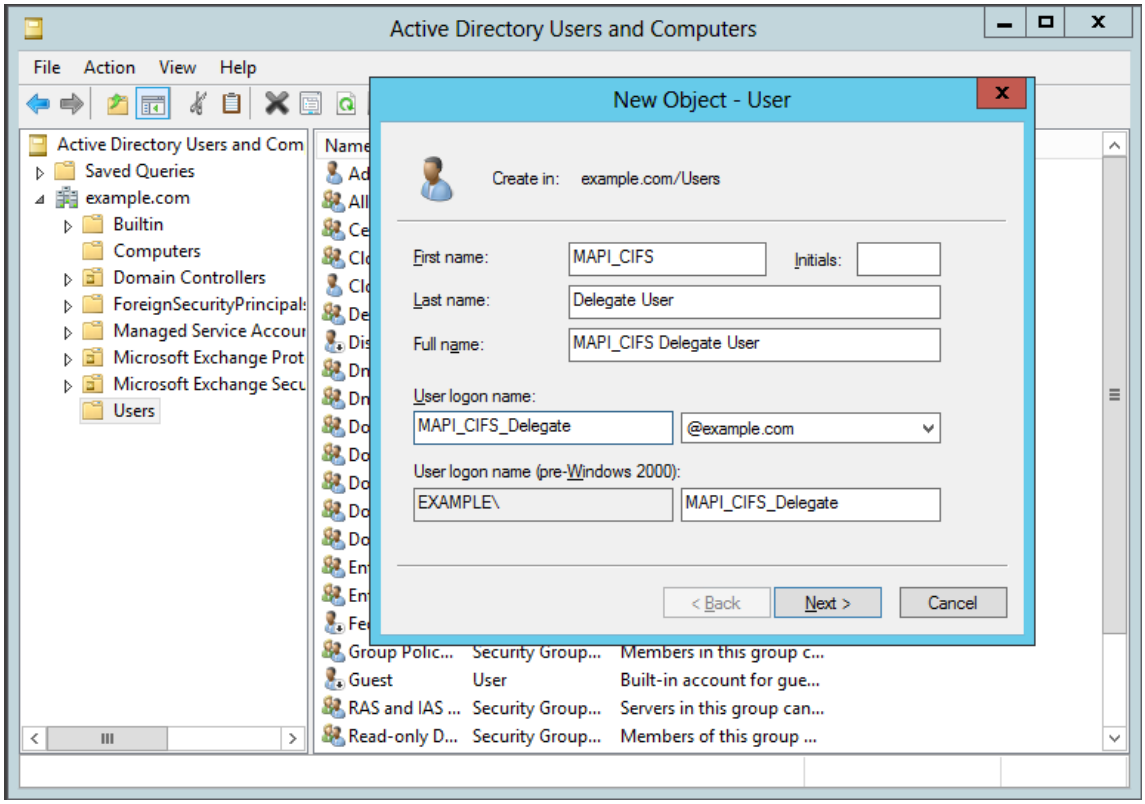
代理ユーザーアカウントを作成する:

Windows ドメインコントローラーで代理ユーザーアカウントを作成して、Citrix SD-WAN WANOP アプライアンスがユーザーに代わってこのアカウントを使用してドメインコントローラーでユーザーを認証できるようにします。

注：既存のユーザーを委任ユーザーとして構成する場合は、この手順をスキップしてください。

代理ユーザーアカウントを作成するには:

1. 管理者として Windows ドメインコントローラーにログオンします。ファイルサーバーまたは Exchange サーバーがこのドメインのメンバーであることを確認してください。
2. **[**スタート] メニューから、[Active Directory ユーザーとコンピューター**]** ウィンドウを開きます。
3. 次のスクリーンショットに示すように、デリゲートユーザーを作成します。



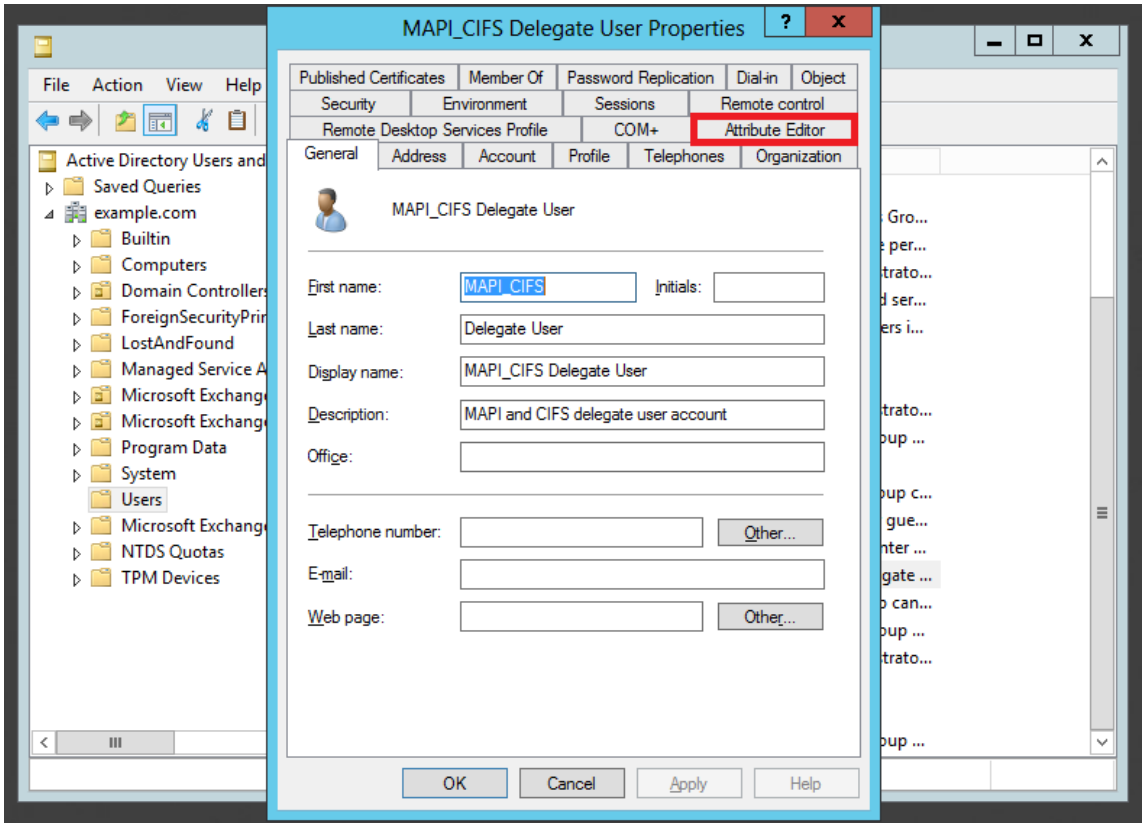
ユーザーの委任を有効にする:

これまでのところ、作成したユーザーは、ActiveDirectory サーバーで作成した他のユーザーと似ています。ユーザーの委任を有効にするには、ユーザーのサービスプリンシパル名属性を設定して 委任 し、委任ユーザーを必要なサービスに関連付ける必要があります。これにより、ユーザーは特別な特権を付与され、委任ユーザーになります。

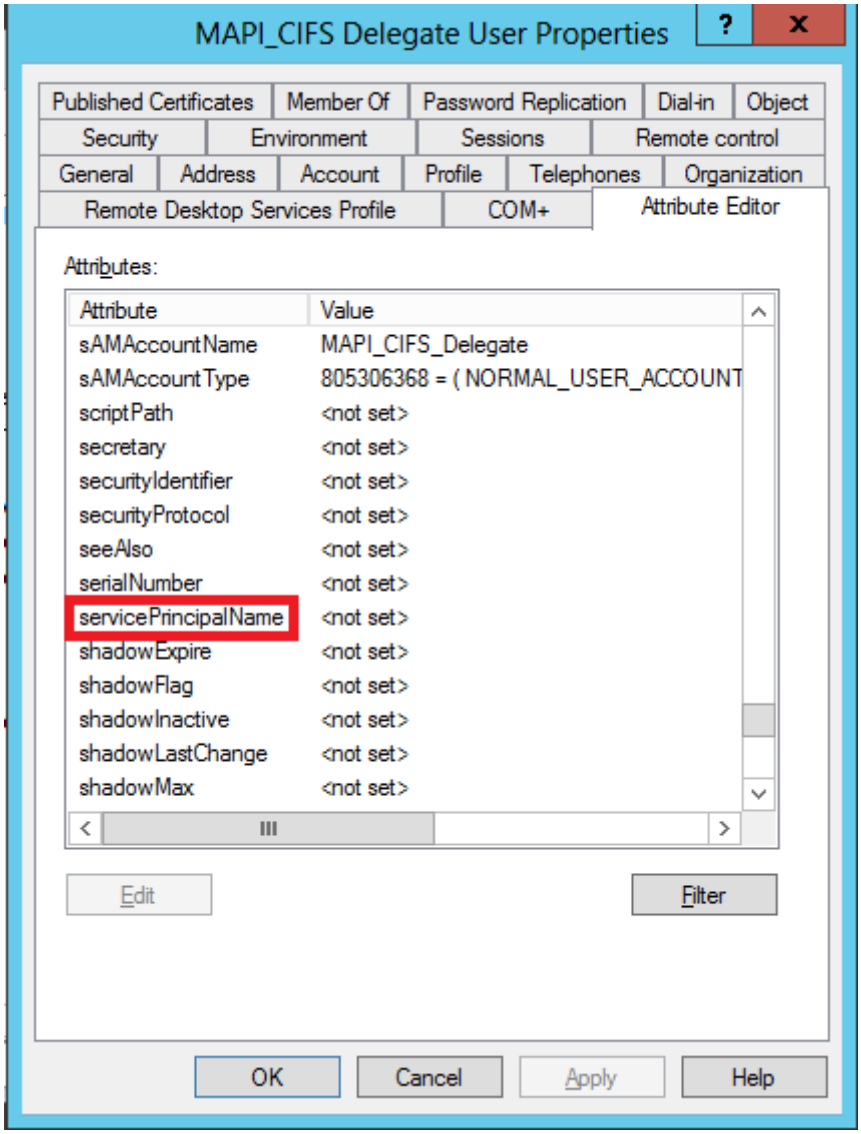
ユーザーの委任を有効にするには:

1. **[**スタート] メニューから、[Active Directory ユーザーとコンピューター**]** ウィンドウを開きます。
2. [表示] メニューから、[高度な機能] を選択します。

3. ユーザー ノードを選択します。
4. デリゲートユーザーにするユーザーを右クリックします。
5. 次のスクリーンショットに示すように、ショートカットメニューから [プロパティ] を選択し、[属性エディター] タブに移動します。

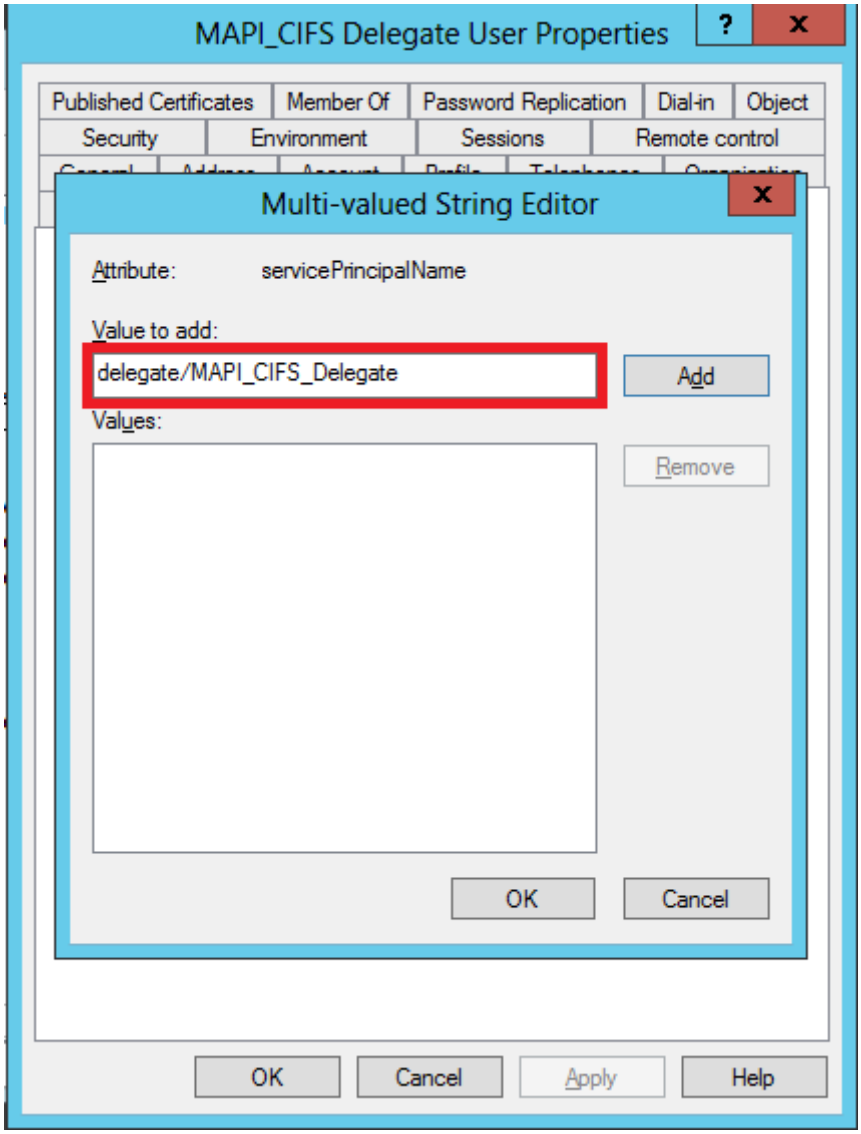


6. 次のスクリーンショットに示すように、[属性] リストから [**servicePrincipalName**] を選択します。

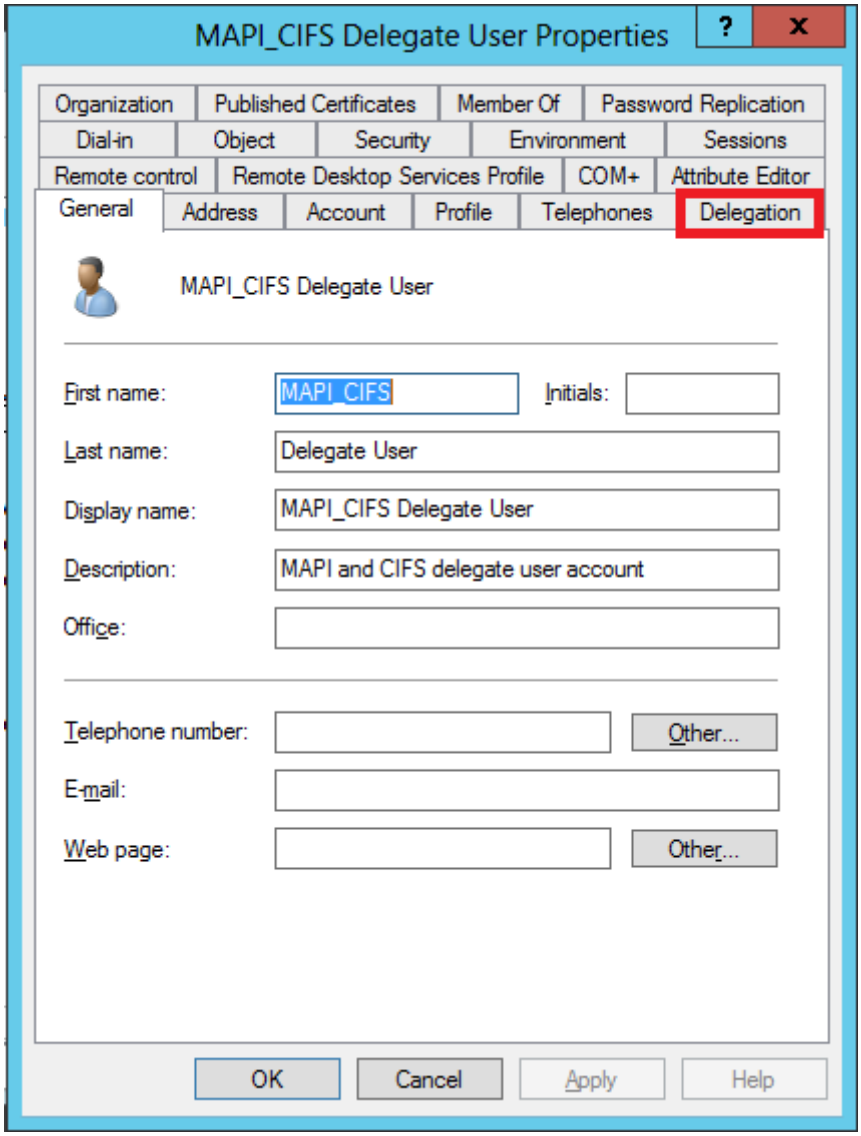


7. ［編集］をクリックします。

8. [複数値の文字列エディター] ダイアログボックスの [追加する値] フィールドで、**delegate /**を指定します。< User_Name > 、次のスクリーンショットに示すように：**



9. ［追加］をクリックします。
10. ［**OK**］をクリックします。
11. ［**Apply**］をクリックします。
12. ［**OK**］をクリックします。
13. 次のスクリーンショットに示すように、ユーザーの **MAPI-CIFS Delegate User Properties** ダイアログボックスを開き、［ **Delegation** ］タブがダイアログボックスに追加されていることを確認します。

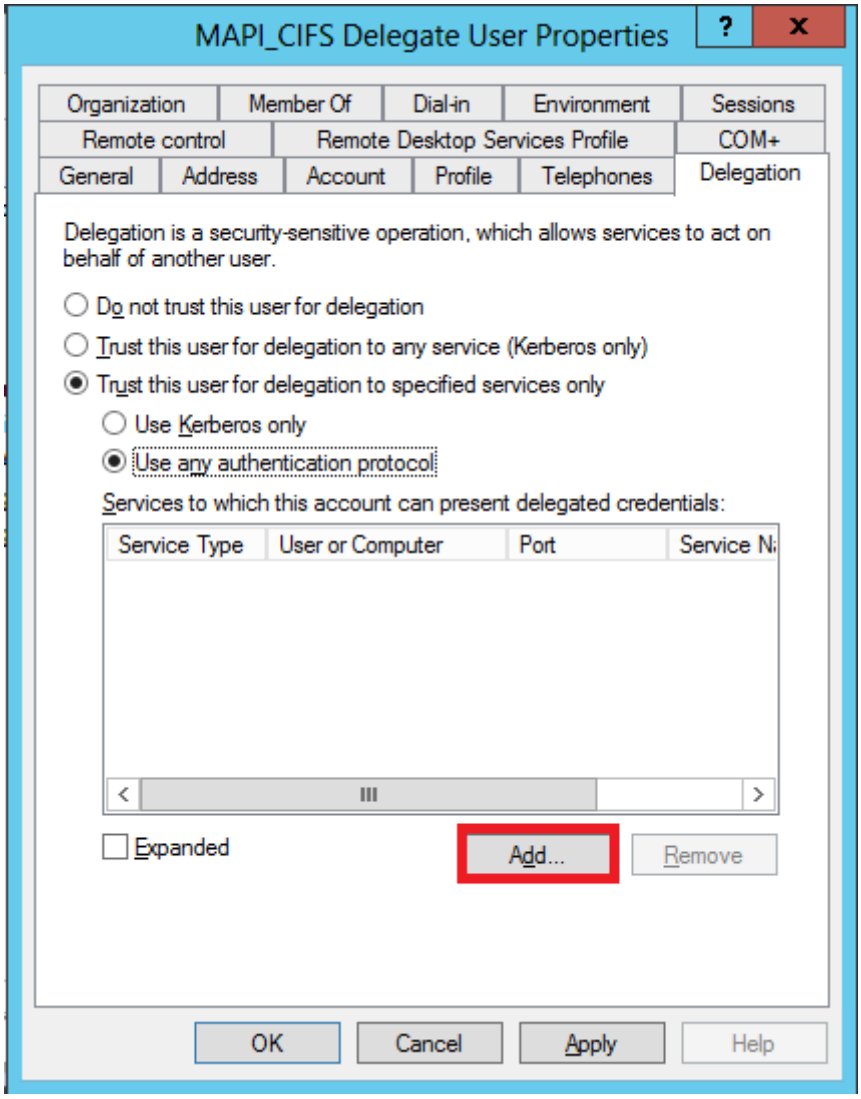


代理ユーザーを **CIFS** および **Exchange** サービスに関連付けます:

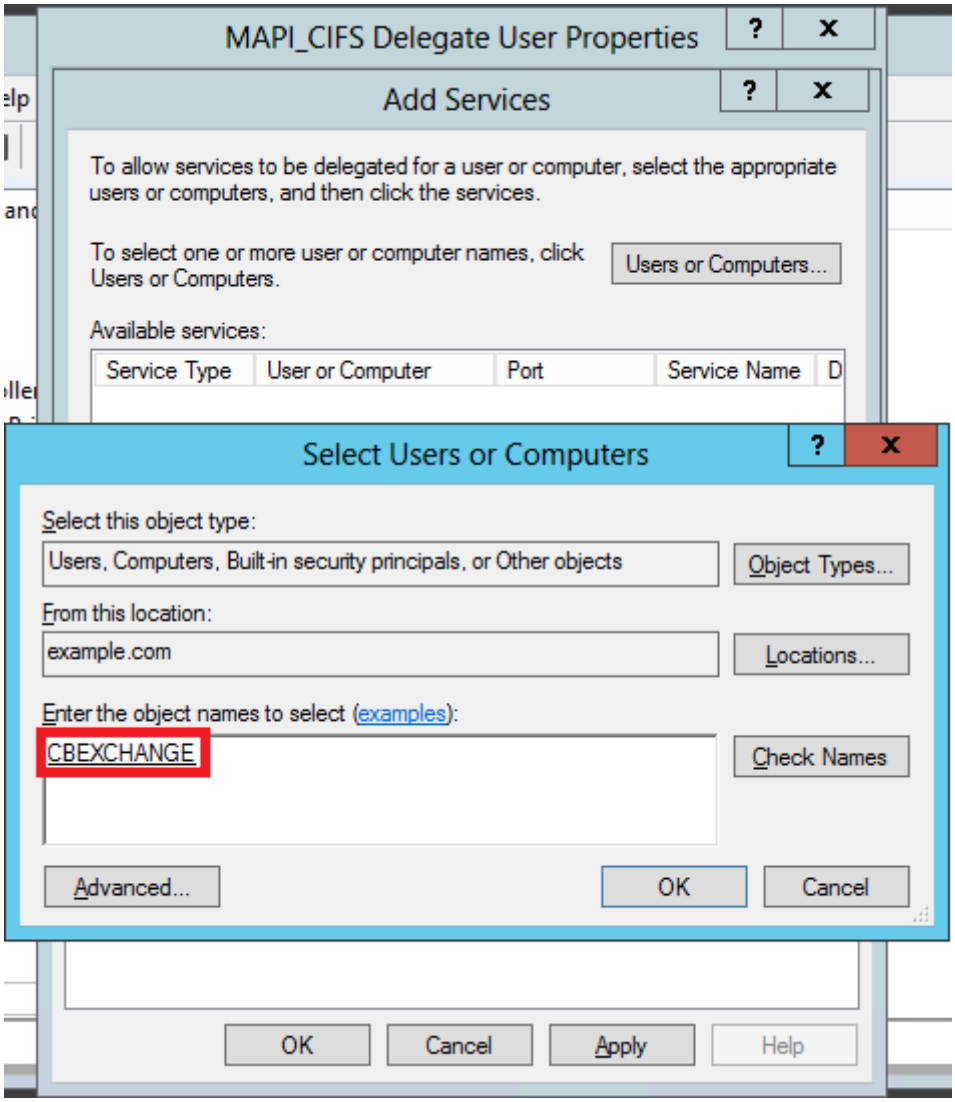
ユーザーの [委任] タブを有効にした後、ユーザーを委任された資格情報を提示できるサービスに関連付けることができます。このユーザーを Citrix SD-WAN WANOP アプライアンスに追加すると、アプライアンスはこのアカウントに関連付けられたサービスの委任された資格情報を提示します。
注: Windows セキュリティインフラストラクチャは、Exchange サービスを使用して MAPI トラフィックを管理します。

デリゲートユーザーを **CIFS** および **Exchange** サービスに関連付けるには:

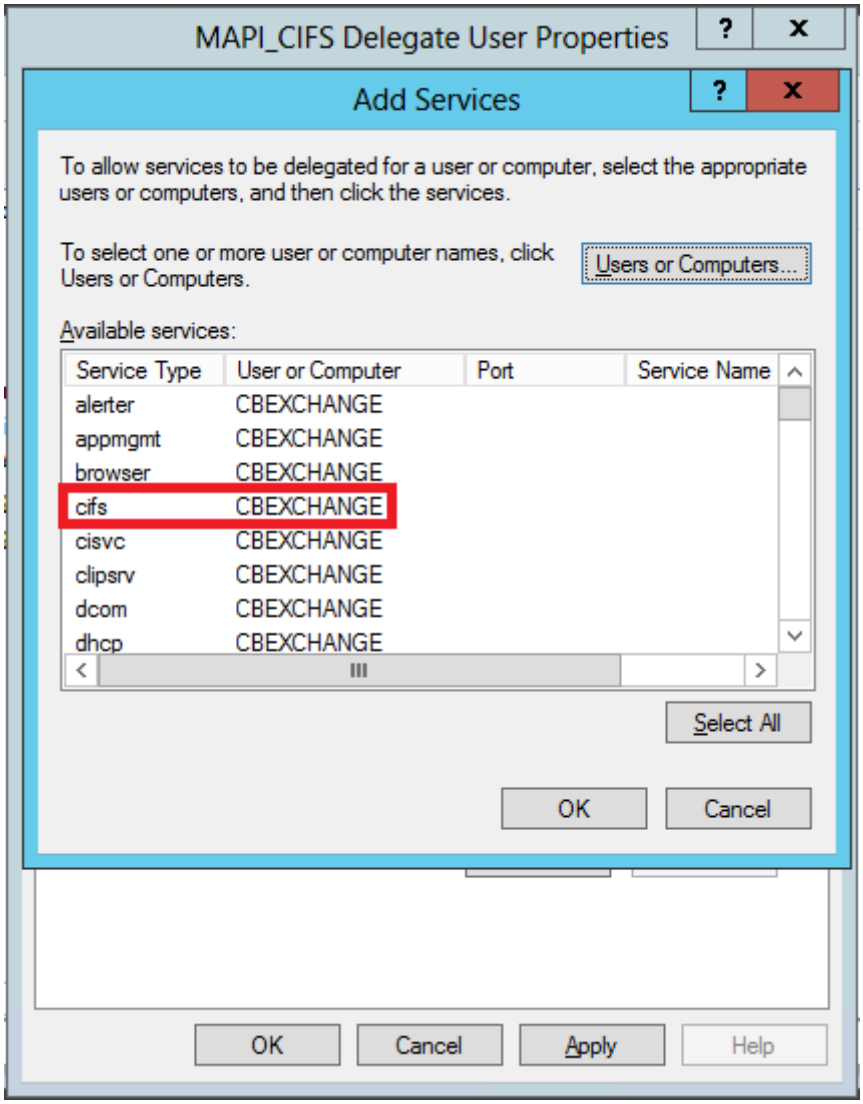
1. [委任] タブで、[特定のサービスのみへの委任についてこのユーザーを信頼 する] オプションを選択します。
2. [任意の認証プロトコルを使用する] オプションを選択します。
3. 次のスクリーンショットに示すように、[追加] をクリックします。



4. [サービス の追加] ダイアログボックスで、[ユーザーとコンピューター] をクリックします。
5. 次のスクリーンショットに示すように、**[**ユーザーまたはコンピューター の選択] ダイアログボックスで、選択するローカルコンピューターを追加します。

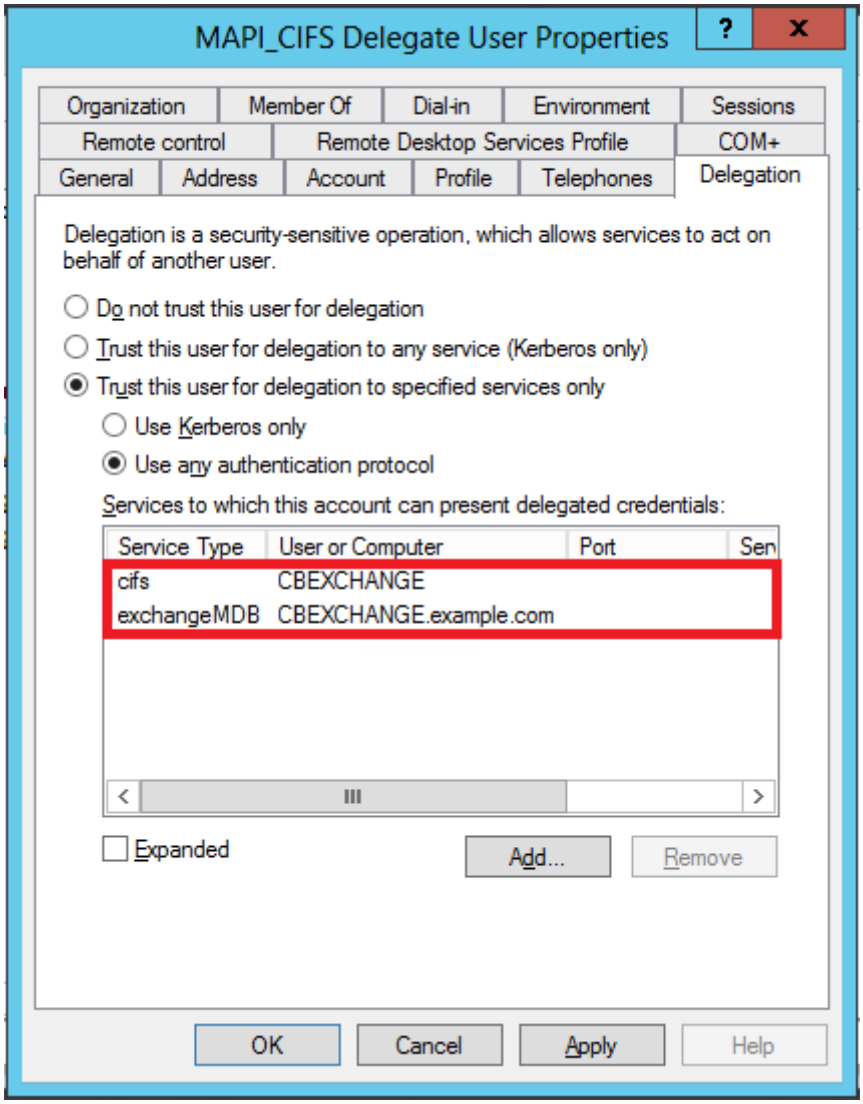


6. [**OK**] をクリックします。
7. 次のスクリーンショットに示すように、[サービス の追加] ダイアログボックスの [利用可能なサービス] リストから、**cifs** を選択します。



8. Citrix SD-WAN WANOP アプライアンスで MAPI アクセラレーションを設定する必要がある場合は、**Ctrl** キーを押したまま、**exchangeMDB** サービスを選択します。

9. ［**OK**］をクリックします。次のスクリーンショットに示すように、選択した サービスが、このアカウントが委任された資格情報 リストを提示できるサービスに追加されます。



10. [**OK**] をクリックします。
11. ActiveDirectory ユーザーとコンピューター ウィンドウを閉じます。

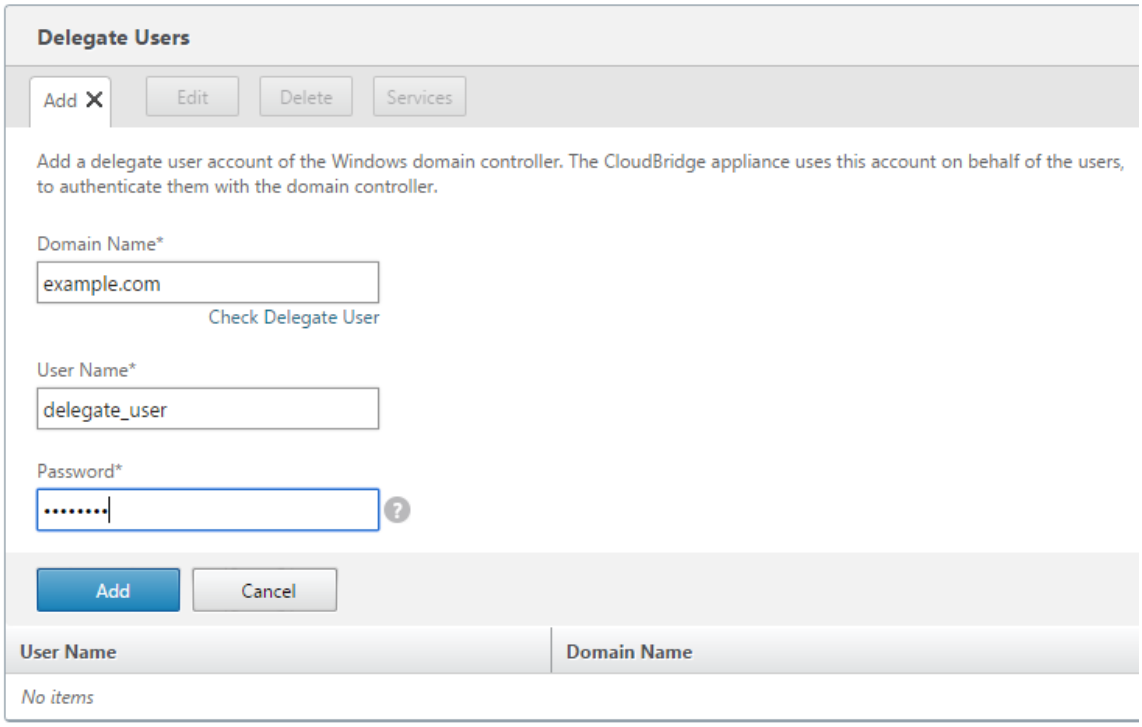
Citrix SD-WAN WANOP アプライアンスでデリゲートユーザーを構成する:

Active Directory サーバーで委任ユーザーを構成した後、Citrix SD-WAN WANOP アプライアンスでこのユーザーを構成して、アプライアンスがこのユーザーの委任資格情報をドメインに提示できるようにする必要があります。これにより、アプライアンスは高度な CIFS および MAPI アクセラレーション機能のためにネットワークトラフィックをアクティブに最適化できます。

デリゲートユーザーをサーバー側アプライアンスに追加するには:

1. 構成 > 安全な加速 > **Windows** ドメイン タブに移動します。
2. 存在する場合は、**[Windows** ドメインに参加] ボタンをクリックします。
3. [ユーザーの委任] で、[追加] をクリックします。

4. 「ドメイン名」フィールドで、ドメイン名を指定します。これは通常、**[Windows** ドメイン**]** セクションで指定したドメインです。
5. 「ユーザー名」フィールドに、代理ユーザーのユーザー名を入力します。
6. [パスワード**]** フィールドで、代理ユーザーのパスワードを指定します。
7. [追加] をクリックします。



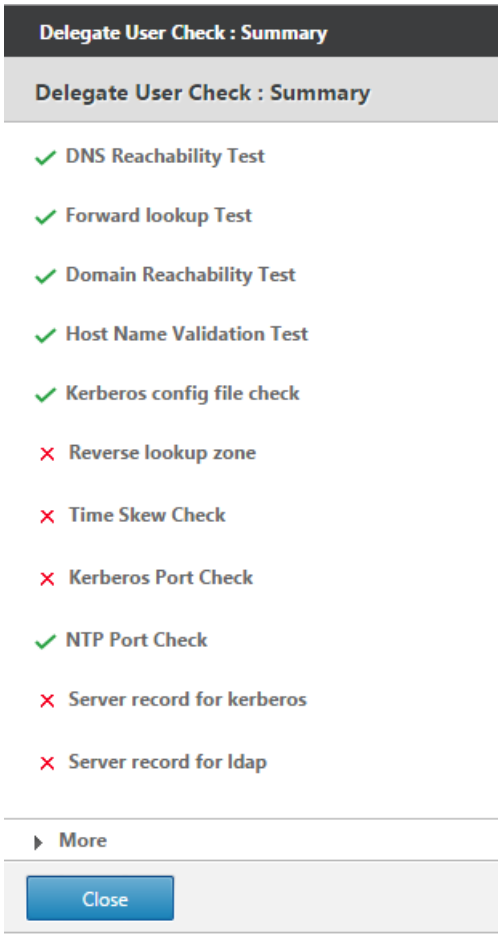
アプライアンスがドメインに参加していることを確認します

アプライアンスをドメインに追加した後、アプライアンスが安全な Windows トラフィックを最適化していないことに気付いた場合は、何らかのエラーが原因でアプライアンスがドメインに参加できなかった可能性があります。**Pre Domain Check** ユーティリティを使用して、ドメインへのアプライアンスの参加に問題があるかどうかを確認できます。アプライアンスをドメインに参加させる前に、このユーティリティを実行して考えられる問題を特定することもできます。

デリゲートユーザーを確認するには:

1. サーバー側の Citrix SD-WAN WANOP アプライアンスにログオンします。
2. 構成 > 安全な加速 > **Windows** タブに移動します。
3. 存在する場合は、**[Windows** ドメインに参加] ボタンをクリックします。
4. 委任ユーザーを選択し、[編集] をクリックします。
5. [デリゲートユーザーの確認**]** をクリックします。

6. デリゲートユーザードメインチェックが完了するのを待ち、結果を調べます。



CIFS を構成し、SMB2/SMB3 アクセラレーション

April 19, 2021

CIFS アクセラレーション機能は、CIFS トランスポートや DCERPC などの関連プロトコルの拡張を含む、CIFS ベース（Windows および Samba）のファイル転送およびディレクトリブラウジングに対する一連のプロトコル固有のパフォーマンス拡張を提供します。

CIFS アクセラレーションには 3 つの部分があります。

- TCP フロー制御アクセラレーション：これは、プロトコルバージョン（SMB1、SMB2、または SMB3）または認証と暗号化の程度に関係なく、すべてのアクセラレーションされた CIFS 接続で実行されます。
- CIFS プロトコルアクセラレーション-これらの最適化は、CIFS コマンドの実行に必要なラウンドトリップの数を減らすことにより、CIFS のパフォーマンスを向上させます。これらの最適化は、CIFS パケット認証（「署

名」）を使用しない SMB1 および SMB2 CIFS 接続、または署名が使用され、アプライアンスが「セキュリティデリゲート」の役割で Windows ドメインに参加している場合に自動的に実行されます。

- CIFS 圧縮：CIFS 接続は、CIFS プロトコルアクセラレーションの要件を満たすたびに自動的に圧縮されます。さらに、SMB3 接続は、署名および封印されていない場合に圧縮されます。

CIFS 署名が有効になっているネットワークでは、CIFS プロトコルの高速化と圧縮を行うには、CIFS パケット認証（署名）を無効にするか、データセンターアプライアンスを Windows ドメインに参加させ、データセンターアプライアンスとリモートアプライアンスと Citrix SD-WAN WANOP プラグインの間に安全なピア関係を作成する必要があります。

表 **1. SMB** プロトコルバージョン別およびアプライアンスが **Windows** ドメインに参加しているかどうかによる **CIFS** アクセラレーション機能。

SMB バージョン	**TCP** フロー制御	圧縮	プロトコルアクセラレーション
		署名が無効	
SMB 1.0	○	○	○
SMB 2.0	○	○	○
SMB 2.1	○	○	×
SMB 3.0	○	○	×
		署名が有効になり、*Citrix SD-WAN WANOP* がドメインに参加しました **	
SMB 1.0	○	○	○
SMB 2.0	○	○	○
SMB 2.1	○	○	○
SMB 3.0	○	○	Y *
		署名が有効で、*Citrix SD-WAN WANOP* がドメインに参加していません	
SMB 1.0	○	×	×
SMB 2.0	○	×	×
SMB 2.1	○	×	×
SMB 3.0	○	×	×

* SMB3.0 サポートはリリース 7.4.2 で追加されました。

** Citrix SD-WAN WANOP は、SMB での 1/ SMB 2/ SMB3 および NetApp サーバーを使用した NTLMv2 認証（Windows 7 のデフォルト）をサポートしていません Kerberos 認証を有効にすると、アクセラレーションが可能になります。

表 **2**。クライアントおよびサーバーのオペレーティングシステムによって使用される **SMB** プロトコルのバージョン。

Client/Server**OS**	**Windows 8**、**Windows 10**、または **Windows Server 2012**	**Windows 7** または **Windows Server 2008 R2**	**Windows Vista** または **Windows Server 2008**	以前のバージョンの **Windows**
Windows 8、**Windows 10**、または **Windows Server 2012**	SMB 3.0	SMB 2.1	SMB 2.0	SMB 1.0
Windows 7 または **Windows Server 2008 R2**	SMB 2.1	SMB 2.1	SMB 2.0	SMB 1.0
Windows Vista または **Windows Server 2008**	SMB 2.0	SMB 2.0	SMB 2.0	SMB 1.0
以前のバージョンの **Windows**	SMB 1.0	SMB 1.0	SMB 1.0	SMB 1.0

CIFS のサポートされているバージョン:

すべての CIFS 実装が、アプライアンスによって認識される要求パターンを使用するわけではありません。次の表に示すように、これらのサポートされていないバージョンは、すべてのケースでアクセラレーションを実現しません。

表 **3. CIFS** サーバーおよびクライアントに対する **Citrix SD-WAN WANOP** のサポート。

製品	サーバー	クライアント
Windows Server 2003-2012	はい *	はい *
Windows XP、Vista、7、8、2000	はい *	はい *
NetApp	はい **	-
Hitachi	はい **	N/A
Windows NT	はい	いいえ

製品	サーバー	クライアント
Windows ME 以前	いいえ	いいえ
そのほか	「注」を参照してください	「注」を参照してください

* SMB 3.0 のサポートはリリース 7.4.2 で導入されました。

** リリース 7.4.2 では、SMB 3.0 での動作はテストされていません。

> 注意: ほとんどのサードパーティ CIFS 実装は、上記のサーバーまたはクライアントの 1 つをエミュレートします。上記の表に示すように、エミュレーションが成功する範囲で、トラフィックは加速されるかどうかが決まります。エミュレーションの動作が CIFS アクセラレータの期待と異なる場合、CIFS アクセラレーションはその接続で終了します。

特定の CIFS 実装での CIFS アクセラレーションの動作は、テストされるまで確実に知ることはできません。

CIFS アクセラレーションのモードは次のとおりです。

- 大きなファイルの読み取りと書き込み
- 小さなファイルの読み取りと書き込み
- ディレクトリブラウジング。

大きなファイルの読み取りと書き込み-これらの SMB1 最適化は、少なくとも 640KB のファイル転送用です。安全な先読みおよび後書きの手法を使用して、転送ごとに一時停止せずにデータをストリーミングします（転送は 64 KB 以下です）。

これらの最適化は、転送に BATCH または EXCLUSIVE ロックがあり、「単純」である場合にのみ有効になります。ファイルのコピーは常に単純です。アプリケーションを介して開かれたファイルは、アプリケーション内での処理方法に応じて、そうである場合とそうでない場合があります。

リンクとディスクが現在の転送速度の 10 倍に対応するのに十分な速度である場合、CIFS アクセラレーションを使用すると 10 倍のスピードアップ率を簡単に得ることができます。必要に応じて 50 倍の高速化を実現できますが、メモリを消費するため、通常は有効になりません。10 倍では不十分な場合は、Citrix の担当者にお問い合わせください。

小さなファイルの読み取りと書き込み-小さなファイルの機能強化は、データストリーミングよりもメタデータ（ディレクトリ）の最適化に重点を置いています。ネイティブ CIFS は、メタデータ要求を効率的な方法で結合しません。CIFS アクセラレーションはそうです。大容量ファイルアクセラレーションと同様に、これらの最適化は安全でない限り実行されません（たとえば、CIFS クライアントにディレクトリの排他ロックが付与されていない場合は実行されません）。SMB2 プロトコルを使用すると、さらに大きな改善のためにローカルでファイルメタデータがキャッシュされます。

ディレクトリブラウジング-標準の CIFS クライアントは、非常に非効率的な方法でディレクトリブラウジングを実行するため、リモートフォルダを開くために膨大な数のラウンドトリップが必要になります。CIFS アクセラレーション

により、ラウンドトリップの数が 2 または 3 に減少します。SMB2 プロトコルを使用すると、ディレクトリデータがローカルにキャッシュされ、さらに改善されます。

CIFS プロトコルアクセラレーション

CIFS アクセラレーションはすべてのモデルでサポートされています。CIFS は TCP ベースのプロトコルであり、フロー制御の恩恵を受けます。ただし、CIFS は、長距離ネットワークでは非常に非効率的な方法で実装されているため、操作を完了するために過剰なラウンドトリップが必要になります。プロトコルはリンク遅延に非常に敏感であるため、完全なアクセラレーションはプロトコルを認識する必要があります。

CIFS アクセラレーションは、さまざまな手法によってラウンドトリップの数を減らします。クライアントからの要求のパターンが分析され、その次のアクションが予測されます。多くの場合、予測が間違っていても安全に行動できます。これらの安全な操作は、多くの最適化の基礎です。

たとえば、SMB1 クライアントは、重複しない方法で順次ファイル読み取りを発行し、64KB の読み取りが完了するのを待ってから次の読み取りを発行します。先読みを実装することにより、アプライアンスは、予想されるデータを事前にフェッチすることにより、最大 10 倍の加速を安全に提供できます。

追加の手法により、ディレクトリの参照と小さなファイルの操作が高速化されます。アクセラレーションは、CIFS 操作だけでなく、関連する RPC 操作にも適用されます。

前提条件

CIFS アクセラレーションはすべてのモデルでサポートされています。CIFS は TCP ベースのプロトコルであり、フロー制御の恩恵を受けます。ただし、CIFS は、長距離ネットワークでは非常に非効率的な方法で実装されているため、操作を完了するために過剰なラウンドトリップが必要になります。プロトコルはリンク遅延に非常に敏感であるため、完全なアクセラレーションはプロトコルを認識する必要があります。

CIFS アクセラレーションは、さまざまな手法によってラウンドトリップの数を減らします。クライアントからの要求のパターンが分析され、その次のアクションが予測されます。多くの場合、予測が間違っていても安全に行動できます。これらの安全な操作は、多くの最適化の基礎です。

たとえば、SMB1 クライアントは、重複しない方法で順次ファイル読み取りを発行し、64KB の読み取りが完了するのを待ってから次の読み取りを発行します。先読みを実装することにより、アプライアンスは、予想されるデータを事前にフェッチすることにより、最大 10 倍の加速を安全に提供できます。

追加の手法により、ディレクトリの参照と小さなファイルの操作が高速化されます。アクセラレーションは、CIFS 操作だけでなく、関連する RPC 操作にも適用されます。

ネットワークで CIFS 署名を使用する場合、アプライアンスはドメインの信頼できるメンバーである必要があります。アプライアンスをドメインの信頼できるメンバーにするには、「Citrix SD-WAN WANOP アプライアンスを Windows セキュリティインフラストラクチャに追加する」を参照してください。

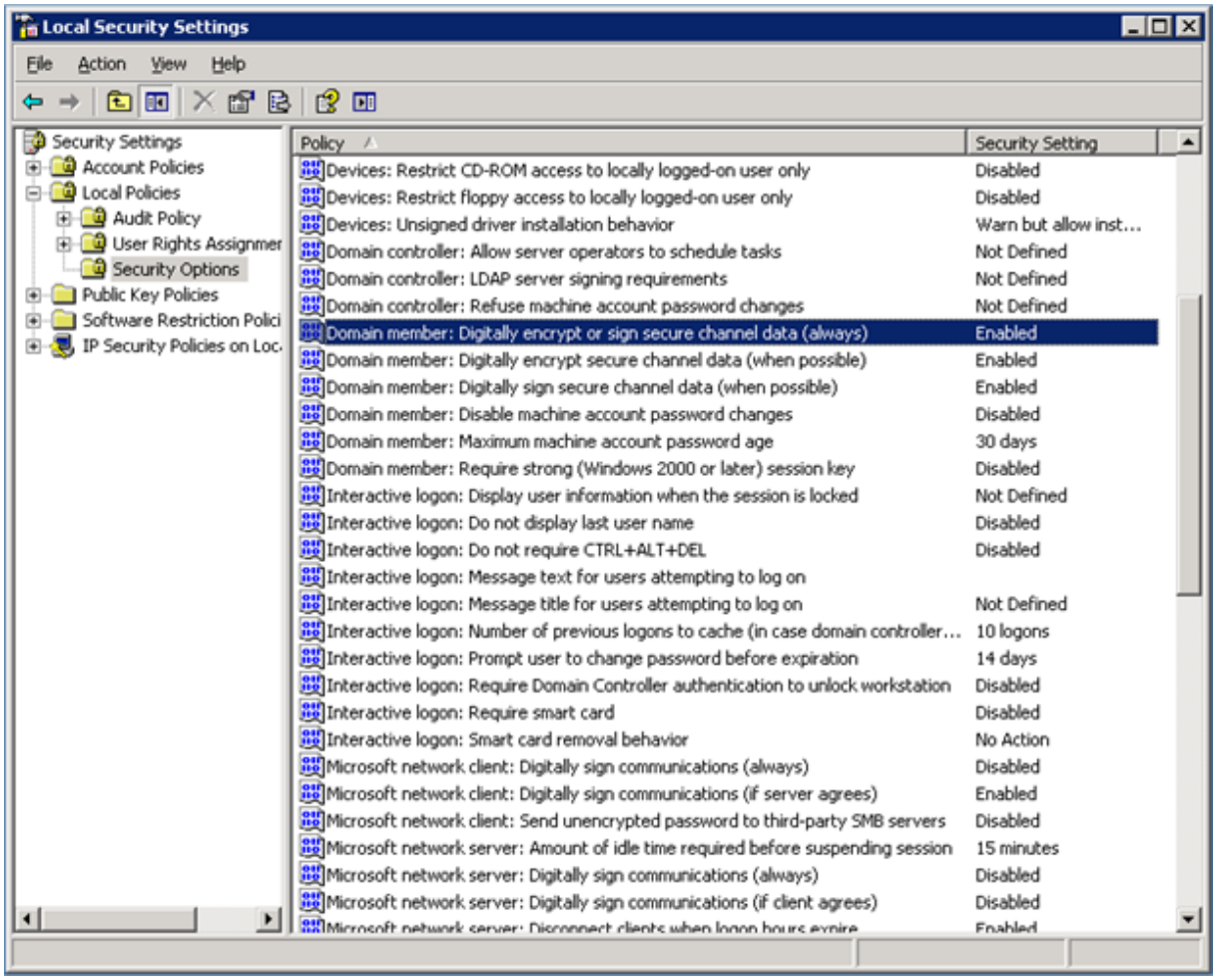
CIFS プロトコルアクセラレーションを構成する

CIFS アクセラレーションは、CIFS 署名を使用しない接続に対してデフォルトで有効になっています。ネットワークで署名を使用している場合は、無効にするか、サーバー側のアプライアンスでWindows ドメインに参加するすることができます。

CIFS 署名を無効にする

セキュリティ設定によっては、Windows サーバーまたはドメインサーバーでセキュリティ設定を調整する必要がある場合があります。

図 1: Windows Server セキュリティオプション、Windows Server 2003 および Windows Server 2008。



Windows ファイルサーバーには、「シーリング」と「署名」の 2 つのセキュリティモードがあります。

シーリングはデータストリームを暗号化し、CIFS プロトコルの高速化を完全に防ぎます。

署名は、データストリームを暗号化せずに、すべてのデータパケットに認証データを追加します。これにより、Citrix SD-WAN WANOP アプライアンスを Windows セキュリティインフラストラクチャに追加するで説明されている手

順を実装していない限り、加速が防止されます。この要件が満たされると、署名が自動的に加速されます。それ以外の場合、プロトコルアクセラレーションを実行するには、署名を無効にする必要があります（まだ無効になっていない場合）。

デフォルトでは、Windows ファイルサーバーは署名を提供しますが、デフォルトで署名を必要とするドメインサーバーを除いて、署名は必要ありません。

現在署名が必要なシステムで CIFS アクセラレーションを実現するには、システムセキュリティ設定を変更してこの要件を無効にする必要があります。これは、ファイルサーバーのローカルセキュリティ設定またはグループポリシーで行うことができます。次の例は、Windows Server 2003 および Windows Server 2008 の場合、ローカル設定を示しています。もちろん、グループポリシーの変更はほとんど同じです。

Citrix SD-WAN WANOP

サーバーの設定を変更して **CIFS** アクセラレーションを許可するには

1. システムの [ローカルセキュリティ設定] ページに移動します。
2. ドメインメンバーの設定：セキュリティで保護されたチャネルデータを（常に）デジタル暗号化または署名して無効にします。
3. Microsoft ネットワーククライアントを設定します：通信に（常に）デジタル署名して無効にします。
4. Microsoft ネットワークサーバーを設定します：通信に（常に）デジタル署名して無効にします。

CIFS 統計を解釈する

監視：ファイルシステム (CIFS/SMB) ページには、高速化された CIFS 接続のリストが表示されます。これらの接続は、「最適化された」接続と「最適化されていない」接続に分けられます。これらの接続はすべて（フロー制御と圧縮を使用して）高速化されるため、「最適化」接続にはフロー制御と圧縮に加えて CIFS 最適化があり、「非最適化」接続にはフロー制御と圧縮のみがあります。

CIFS 管理の概要

- CIFS アクセラレーションは、リンク距離が比較的短い場合でも大幅に改善されます。
- CIFS アクセラレーションは、クライアントがファイルシステムに最初にアクセスしたときに開始されます。ファイルサーバーとクライアントが既に稼働している状態でアクセラレーションが有効になっている場合、既存の CIFS 接続が完全に閉じられるまで、何分間もアクセラレーションは発生しません。CIFS 接続は非常に永続的であり、アイドル状態の場合でも、接続を閉じるまでに長時間続きます。この動作はテスト中は煩わしいものですが、通常の展開ではほとんど重要ではありません。
- Windows でファイルシステムをマウント解除および再マウントしても、CIFS 接続は閉じられません。これは、Windows がファイルシステムを完全にマウント解除しないためです。クライアントまたはサーバーの再

起動は機能します。侵襲性の低い対策として、NET USE デバイス名を使用します /DELETE Windows コマンドラインからコマンドを実行して、ボリュームを完全にマウント解除します。Linux では、smbmount と umount はボリュームを完全にマウント解除します。

- アプライアンスで CIFS の読み取りと書き込みの最適化を無効にしてから再度有効にすると、同様の問題が発生します。CIFS が有効になっている場合、既存の接続は高速化されず、監視：ファイルシステムで検出された「プロトコルエラー」の数 (CIFS/SMB) ページが一時的に増加します。
- ファイルサーバーから最も遠いアプライアンスのみが完全な統計で CIFS アクセラレーションを報告するため、CIFS 統計は混乱を招く可能性があります。他のアプライアンスは、それを通常の加速と見なします。
- CIFS アクセラレーションは、プロキシモードではサポートされていません。
- Windows サーバーで CIFS アクセラレーションが実行されない場合は、サーバーのセキュリティ設定を確認してください。

MAPI アクセラレーションを設定する

April 19, 2021

Microsoft Outlook アクセラレーションは、Microsoft Outlook クライアントと Microsoft Exchange Server 間のトラフィックのパフォーマンスを向上させ、データのプリフェッチや圧縮などのさまざまな最適化によってスループットを向上させます。

この機能は、Outlook と Exchange Server の間で使用される MAPI プロトコルにちなんで、「MAPI アクセラレーション」とも呼ばれます。

Outlook データストリームが暗号化されていないネットワーク（Outlook 2007 より前のデフォルト）では、この機能を構成する必要はありません。

Outlook データが暗号化されているネットワーク（Outlook 2007 以降のデフォルト）では、Outlook クライアントで暗号化を無効にするか、アプライアンスを使用する 2 つの方法のいずれかでアクセラレーションを取得できますWindows ドメインに参加する 。

サポートされている **Outlook Exchange** のバージョンとモード

Citrix SD-WAN WANOP アプライアンスは、次の状況で Microsoft Outlook 2003-2016 および Exchange Server 2003-2010 に MAPI アクセラレーションを提供します。

- サポートされているクライアントとサーバーの任意の組み合わせ（MAPI プロトコルを使用）がサポートされています。
- サーバー側アプライアンスが Windows ドメインに参加している場合、MAPI 暗号化を使用した接続が高速化されます。それ以外の場合はそうではなく、Outlook クライアントで暗号化を無効にする必要があります。

> 注
>
> Exchange Server 2013 では、MAPI プロトコルが RPC over HTTP プロトコルに変更され、このプロトコルがサポートされています。Exchange Server SP1 では、RPC over HTTP プロトコルが MAPI over HTTP プロトコルに変更されたため、このプロトコルは現在サポートされていません。

前提条件

ネットワークで暗号化された Outlook データ（Outlook 2007 以降のデフォルト設定）を使用している場合は、MAPI 接続が高速化されるように、次のいずれかの前提条件を実装する必要があります。

- Outlook クライアントで暗号化を無効にします。
- Citrix SD-WAN WANOP アプライアンスを Windows セキュリティインフラストラクチャに追加するで説明されているタスクを実行します。

構成

Outlook アクセラレーションは、デフォルトで有効になっている構成なしの機能です。（不要な場合は、構成：サービスクラスポリシー ページで MAPI サービスクラスのアクセラレーションを無効にすることで無効にできます。）次の条件が満たされた場合、Outlook アクセラレーションが自動的に実行されます。

- WAN の Exchange Server 側にアプライアンスがあります。
- WAN の Outlook 側にアプライアンスがあるか、Outlook を実行しているシステムが Citrix SD-WAN WANOP プラグインも実行しています。
- すべて Outlook/Exchange トラフィックはアプライアンス（またはアプライアンスとプラグイン）を通過します。
- Exchange Server または Outlook のいずれかが再起動されます（既存の MAPI 接続が閉じられるまでアクセラレーションは開始されません）。
- Outlook で暗号化が無効になっているか、サーバー側アプライアンスが Windows ドメインに属し、クライアント側アプライアンス（または Citrix SD-WAN WANOP プラグイン）と安全なピア関係にあります。アプライアンスが Windows ドメインに参加している場合、アクセラレーションを機能させるには、ドメインでの認証をデフォルト設定（ネゴシエート）に維持する必要があります。

Outlook2007 または **Outlook2010** で暗号化を無効にする

サーバー側アプライアンスが Windows ドメインに参加していて、クライアント側アプライアンス（または Citrix SD-WAN WANOP プラグイン）と安全なピア関係にある場合を除き、高速化を実行するには、Outlook と Exchange Server 間の暗号化を無効にする必要があります。

Outlook 2007 より前は、暗号化はデフォルトで無効にされていました。Outlook 2007 以降、暗号化はデフォルトで有効になっています。

パフォーマンスノート

MAPI は、他のプロトコルとは異なるデータ形式を使用します。この違いにより、効果的なクロスプロトコル圧縮が妨げられます。つまり、最初に FTP を介して転送され、次に電子メールの添付ファイルとして転送されたファイルは、2 回目の転送で圧縮の利点を享受しません。同じデータが MAPI 形式で 2 回送信された場合、2 回目の転送は完全に圧縮されます。

SSL 圧縮

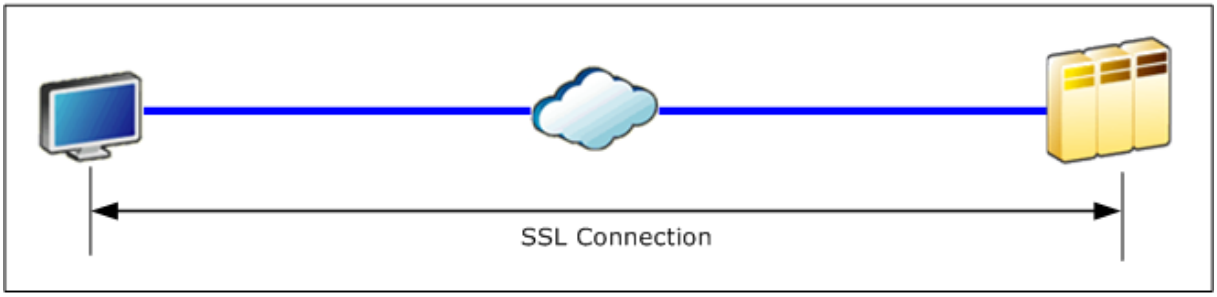
April 19, 2021

Citrix SD-WAN WANOP SSL 圧縮は、SSL 接続（HTTPS トラフィックなど）にマルチセッション圧縮を適用し、最大 10,000:1 の圧縮率を提供します。

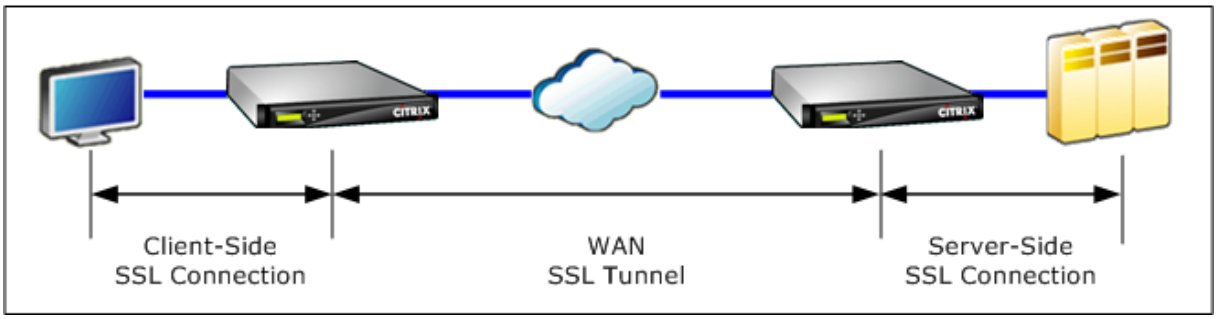
> 注
>
> SSL 圧縮には、高速リンクの両端にある 2 つのアプライアンス間の安全なピアリング（シグナリング）接続が必要です。

暗号化は、接続を 3 つの暗号化されたセグメント（クライアントからクライアント側のアプライアンス、クライアント側のアプライアンスからサーバー側のアプライアンス、およびサーバー側のアプライアンスからサーバー）に分割することにより、エンドツーエンドで維持されます。

Ordinary SSL Connection



Accelerated SSL Connection



注意：SSL 圧縮は、暗号化されたデータストリームを復号化します。ユーザーデータ暗号化オプションを使用しない限り、両方のアクセラレーションユニットの圧縮履歴は、復号化されたデータのクリアテキストレコードを保持します。展開と設定が組織のセキュリティポリシーと一致していることを確認します。SSL アクセラレーションに必要なセキュアピアリングシグナリング接続を構成するときは、各ユニットで圧縮履歴の暗号化を有効にすることをお勧めします。

> 注
>
> - SSL 圧縮を有効にすると、アプライアンスは、安全なピア関係を持たない他のアプライアンス（Citrix SD-WAN WANOP または Citrix SD-WAN WANOP プラグイン）との圧縮の試行を停止します。したがって、この機能は、すべてのアプライアンスが SSL 圧縮用に構成されているネットワークに最適です。
> - SSL 圧縮を有効にすると、アプライアンスを再起動するたびに、キーストアのパスワードを手動で入力する必要があります。

SSL 圧縮のしくみ

April 19, 2021

サーバー側アプライアンスはエンドポイントサーバーの セキュリティデリゲート として機能するため、SSL 圧縮は接続のクリアテキストデータにアクセスできます。この動作が可能なのは、サーバー側アプライアンスがサーバーのセキュリティ資格情報（秘密鍵と証明書）のコピーで構成されており、サーバーに代わって動作できるようにしているためです。クライアントにとって、この動作はエンドポイントサーバーと直接通信することと同じです。

アプライアンスはサーバーのセキュリティデリゲートとして機能しているため、ほとんどの構成はサーバー側アプライアンスで行われます。クライアント側アプライアンス（またはプラグイン）はサーバー側アプライアンスのサテライトとして機能し、サーバーごとの構成を必要としません。

サーバー側とクライアント側のアプライアンスは、*SSL* シグナリング接続を介してセッションステータスを共有します。元の接続が暗号化されているかどうかに関係なく、2 つのアプライアンス間のすべての高速接続は *SSL* データ接続を 介して送信されます。

注：SSL 圧縮は、必ずしもすべてのリンクトラフィックを暗号化するわけではありません。元々暗号化されていたトラフィックは暗号化されたままですが、暗号化されていないトラフィックは常に暗号化されるとは限りません。アプライアンスは、加速されていないトラフィックを暗号化しようとはしません。特定の接続が高速化されるという絶対的な保証はないため（さまざまなイベントが高速化を妨げる）、アプライアンスが特定の暗号化されていない接続を暗号化するという保証はありません。

SSL 圧縮は、透過プロキシまたは分割プロキシの 2 つのモードのいずれかで動作します。これらの 2 つのモードは、わずかに異なる SSL 機能をサポートします。特定のアプリケーションに必要な機能を提供するモードを選択します。

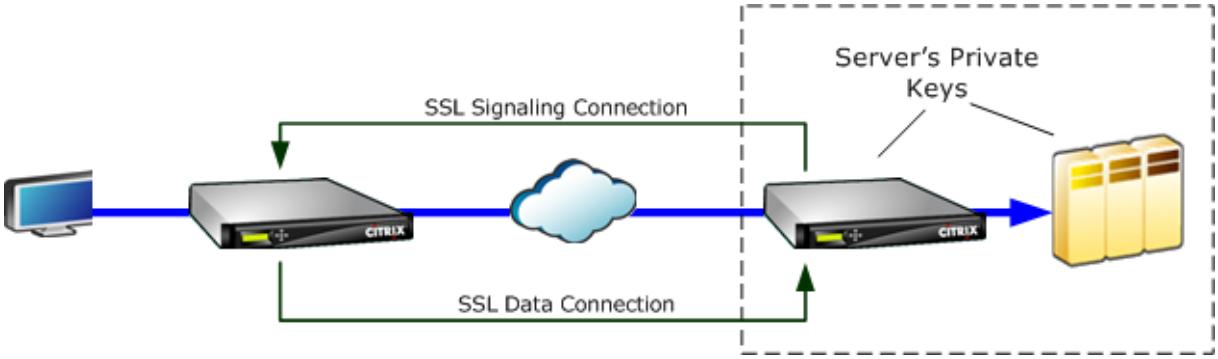
使用する **SSL** プロキシモード**-**真のクライアント認証（つまり、個々のエンドポイントクライアントを正しく識別する認証）が必要で、Diffie-Hellman、Temp RSA、TLS セッションチケット、SSL バージョン 2、またはセッションの再ネゴシエーションが必要 ない 場合にのみ SSL 透過プロキシモードを使用 し ます。他のすべての展開には SSL 分割プロキシを使用します。

SSL 透過プロキシ

SSL 透過プロキシモード（Citrix SD-WAN WANOP プラグインの透過モードと混同しないでください）では、サーバー側のアプライアンスがサーバーになりすます。サーバーの資格情報（証明書とキーのペア）は、サーバーに代わって動作できるようにサーバー側のアプライアンスにインストールされます。次に、サーバー側アプライアンスは、接続のクライアント側を処理するようにクライアント側アプライアンスを構成します。サーバーの資格情報は、クライアント側のアプライアンスにインストールされていません。

このモードでは真のクライアント認証がサポートされていますが、TempRSA と Diffie-Hellman はサポートされていません。SSL 透過プロキシモードは、クライアント認証を必要とするアプリケーションに適していますが、次の機能のいずれも必要とされない場合に限ります：Diffie-Hellman、Temp RSA、TLS セッションチケット、SSL バージョン 2。また、セッションの再ネゴシエーションを試行しないでください。そうしないと、接続が終了します。

クライアント側アプライアンスでの構成は不要であり（サーバー側アプライアンスとの安全なピアリング関係の構成を除く）、サーバーと直接通信しているかのように接続を処理するクライアントでの構成も必要ありません。



SSL 分割プロキシ

SSL 分割プロキシモード は、多くのアプリケーションで必要とされる Temp RSA と Diffie-Hellman をサポートしているため、ほとんどの場合に推奨されます。SSL 分割プロキシモードでは、サーバー側アプライアンスはサーバーからクライアントへ、およびクライアントからサーバーへのマスカレードを行います。サーバー側のアプライアンスにサーバーの資格情報（証明書とキーのペア）をインストールして、サーバーに代わって動作できるようにします。

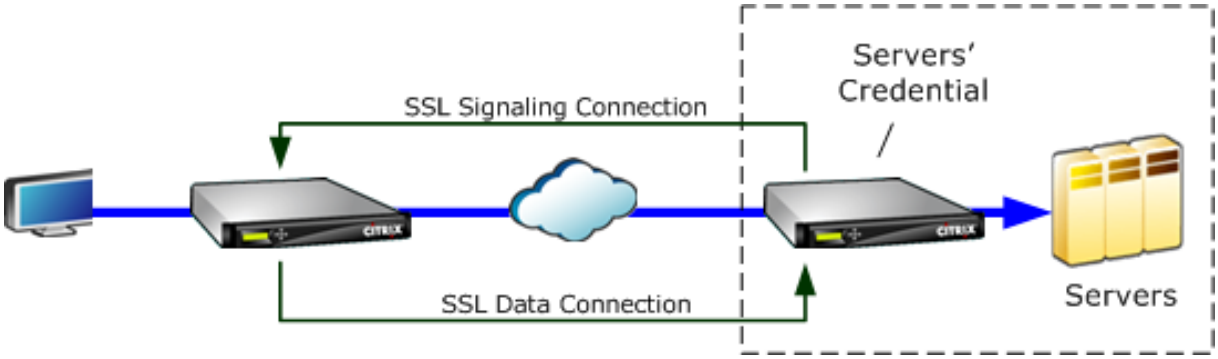
分割プロキシモードは、オプションのクライアント資格情報をインストールした場合にもプロキシクライアント認証をサポートします。オプションのクライアント資格情報は、クライアント認証を要求した場合にエンドポイントサーバーアプリケーションに提示されます。これらのクライアント資格情報は、実際のエンドポイントクライアントの資格情報の代わりに表示されます。（エンドポイントクライアントの資格情報がアプリケーションで必要な場合は、透過プロキシを使用します。）

このモードでは真のクライアント認証がサポートされていないため、サーバーは実際のエンドポイントクライアントを認証できません。サーバー側アプライアンスがクライアント資格情報で構成されていない場合、サーバー側アプリケーションによるクライアント認証の試行はすべて失敗します。サーバー側アプライアンスがクライアント資格情報で構成されている場合、実際のクライアントの ID に関係なく、クライアント認証のすべての要求はこれらの資格情報で応答されます。

クライアント側アプライアンスでの構成は必要ありません（サーバー側アプライアンスとの安全なピアリング関係の構成を除く）。また、接続をサーバーと直接通信しているかのように扱うクライアントでの構成も必要ありません。サーバー側アプライアンスのサーバー資格情報は、クライアント側アプライアンスにインストールされていません。

複数のサーバーをサポートするために、SSL プロファイルごとに 1 つずつ、複数のプライベート証明書とキーのペアをアプライアンスにインストールできます。サービスクラス定義の特別な SSL ルールは、サーバーを SSL プロファイルに一致させ、SSL プロファイルを資格情報に一致させます。

SSL 分割プロキシモードでは、CA 証明書と証明書とキーのペア、および CA 証明書は、実際にはサーバーのものと一致する必要はありませんが、一致する必要があります。分割プロキシの性質上、サーバー側アプライアンスは、クライアントアプリケーションに受け入れられる資格情報（信頼できる機関によって発行された有効な資格情報）を使用できます。HTTPS 接続の場合、共通名が URL のドメイン名と一致しないと、Web ブラウザーは警告を発行することに注意してください。一般に、サーバーの資格情報のコピーを使用する方が問題のないオプションです。



SSL 圧縮を構成する

April 19, 2021

Citrix SD-WAN WO SSL 圧縮機能により、SSL 接続（HTTPS トラフィックなど）のマルチセッション圧縮が可能になり、最大で 10,000:1 の圧縮率が提供されます。詳しくは、「SSL 圧縮」を参照してください。

SSL 圧縮を機能させるには、Citrix SD-WAN WANOP アプライアンスにサーバーまたはクライアントからの証明書が必要です。複数のサーバーをサポートするために、SSL プロファイルごとに 1 つずつ、複数の秘密鍵をアプライアンスにインストールできます。サービスクラス定義の特別な SSL ルールは、サーバーを SSL プロファイルに一致させ、SSL プロファイルを秘密鍵に一致させます。

SSL 圧縮は、スプリットプロキシモードまたはトランスペアレントプロキシモードで機能します。要件に応じてモードを選択できます。詳しくは、「SSL 圧縮のしくみ」を参照してください。

> 注
>
> 透過プロキシモードは現在サポートされていません。

SSL トンネルによる安全なアクセスを可能にするために、最新の SSL プロトコル TLS1.2 が SSL プロキシで使用されます。TLS1.2 プロトコルのみを使用するか、TLS1.0、TLS1.1、および TLS1.2 プロトコルを使用するかを選択できます。

> 注
>
> SSL プロトコル SSLv3 および SSLv2 はサポートされなくなりました。

SSL 圧縮を構成するには:

1. サーバーの CA 証明書と秘密証明書とキーのペアのコピーを取得し、サーバー側のアプライアンスにインストールします。これらの資格情報は、アプリケーション固有である可能性があります。つまり、サーバーは、ApacheWeb サーバーと RPC over HTTPS を実行している Exchange Server の資格情報が異なる場合があります。

2. 分割プロキシ SSL プロファイルまたは透過プロキシ SSL プロファイルの作成を選択できます。

   分割プロキシ SSL プロファイルの構成については、以下の「分割プロキシ SSL プロファイルの 構成」セクションを参照してください。

   透過プロキシ SSL プロファイルの構成については、以下の「透過プロキシ **SSL** プロファイルの構成」セクションを参照してください。

   > 注
   >
   > 透過プロキシ SSL プロファイルは現在サポートされていません。

3. SSL プロファイルをサーバー側アプライアンスのサービスクラスにアタッチします。これは、サーバー IP に基づいて新しいサービスクラスを作成するか、既存のサービスクラスを変更することによって実行できます。

   詳細については、以下の 「サービスクラスの作成または変更」セクションを参照してください。

4. クライアント側アプライアンスでサービスクラスを設定します。SSL トラフィックは、アクセラレーションと圧縮を可能にするクライアント側アプライアンスのサービスクラスに分類されない限り、圧縮されません。これは、SSL ルールではなく通常のサービスクラスルールにすることができます（サーバー側アプライアンスのみが SSL ルールを必要とします）が、アクセラレーションと圧縮を有効にする必要があります。トラフィックは、「HTTPS」や「その他の TCP トラフィック」などの既存のサービスクラスに分類されます。このクラスのポリシーでアクセラレーションと圧縮が有効になっている場合、追加の構成は必要ありません。

5. ルールの動作を確認します。アプライアンスを介して SSL アクセラレーションを受信する必要があるトラフィックを送信します。サーバー側アプライアンスの [監視]: [最適化]: [接続]: [アクセラレーション接続] タブで、[サービスクラス] 列は安全なアクセラレーション用に設定したサービスクラスと一致し、[SSL プロキシ] 列には適切な接続の場合は True が表示されます。

分割プロキシ **SSL** プロファイルを構成する

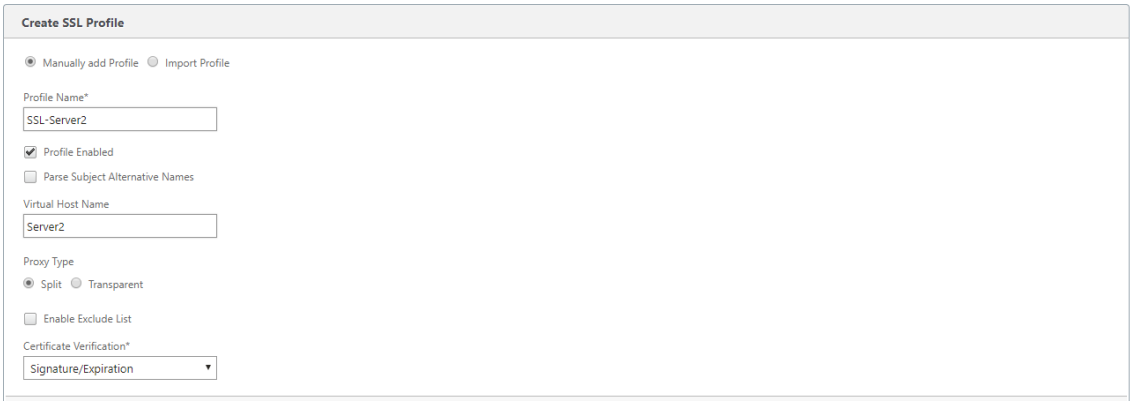
分割プロキシ **SSL** プロファイルを構成するには:

1. サーバー側の Citrix SD-WAN WO アプライアンスで、[構成**]>** 安全な加速 **>SSL** プロファイル に移動し、[プロファイルの追加] をクリックします。

   > 注
   >
   > SSL プロファイルを手動で追加するか、ローカルコンピューターに保存されているプロファイルをインポートすることができます。

2. [プロファイル名**]** フィールドに SSL プロファイルの名前を入力し、[プロファイルを有効にする] を選択します。

3. SSL サーバーが複数の仮想ホスト名を使用している場合は、[仮想ホスト名**]** フィールドにターゲットの仮想ホスト名を入力します。これは、サーバーの資格情報にリストされているホスト名です。



> 注
>
> 複数の仮想ホストをサポートするには、ホスト名ごとに個別の SSL プロファイルを作成します。

4. 分割 プロキシタイプを選択します。
5. [証明書の検証] フィールドで、デフォルト値を保持します (Signature/Expiration) ポリシーで別段の指示がない限り。
6. サーバー側のプロキシ構成を実行します。

   [検証ストア**]** フィールドで、既存のサーバー認証局（CA）を選択するか、**+** をクリックしてサーバー CA をアップロードします。

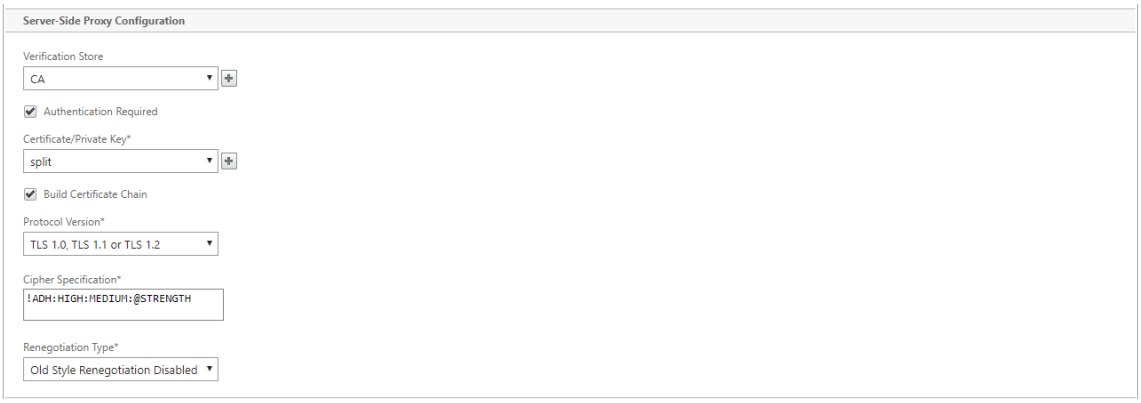
   [認証が必要] を選択し、**Certificate/Private** キーフィールドで証明書キーペアを選択するか、**+** をクリックして証明書キーペアをアップロードします。

   [プロトコルバージョン] フィールドで、サーバーが受け入れるプロトコルを選択します。

   > 注
   >
   > Citrix SD-WAN WO は、**TLS1.0**、**TLS1.1**、**TLS1.2** の組み合わせ、または **TLS1.2** のみをサポートします **。** SSL プロトコル SSLv3 および SSLv2 はサポートされていません。

   必要に応じて、OpenSSL 構文を使用して 暗号仕様 文字列を編集します。

   必要に応じて、[再ネゴシエーション タイプ] ドロップダウンリストから再ネゴシエーションのタイプを選択して、クライアント側の SSL セッションの再ネゴシエーションを許可します。



7. クライアント側のプロキシ構成を実行します。

   Certificate/Private キー フィールドの中にデフォルト値を保持します。

   サーバー側アプライアンスが SSL 証明書チェーンを構築できるようにするには、[証明書チェーンの構築] を選択します。

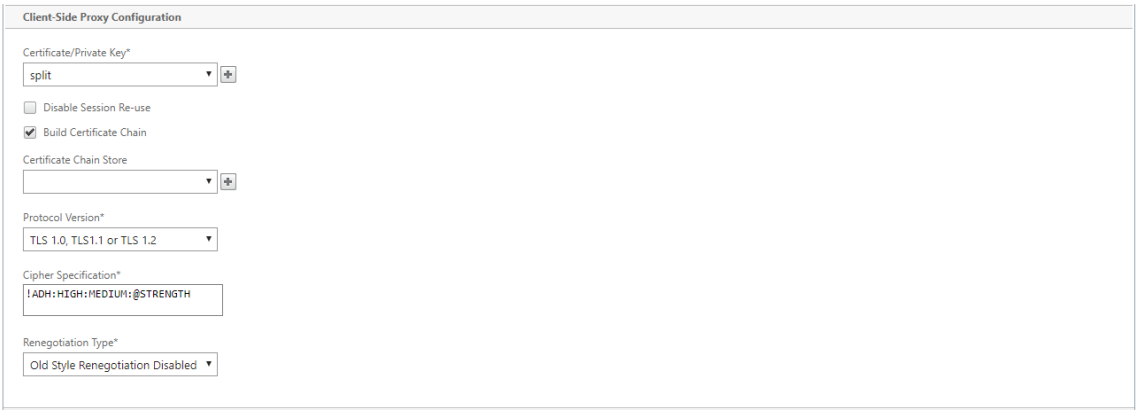
   必要に応じて、証明書チェーンストアとして使用する CA ストアを選択またはアップロードします。

   [プロトコルバージョン] フィールドで、クライアント側でサポートするプロトコルバージョンを選択します。

   > 注
   >
   > Citrix SD-WAN WO は、**TLS1.0**、**TLS1.1**、**TLS1.2** の組み合わせ、または **TLS1.2** のみをサポートします **。** SSL プロトコル SSLv3 および SSLv2 はサポートされていません。

   必要に応じて、クライアント側の暗号仕様を編集します。

   必要に応じて、[再ネゴシエーション タイプ] ドロップダウンリストから再ネゴシエーションのタイプを選択して、クライアント側の SSL セッションの再ネゴシエーションを許可します。



8. ［作成］をクリックします。

透過プロキシ **SSL** プロファイルを構成する

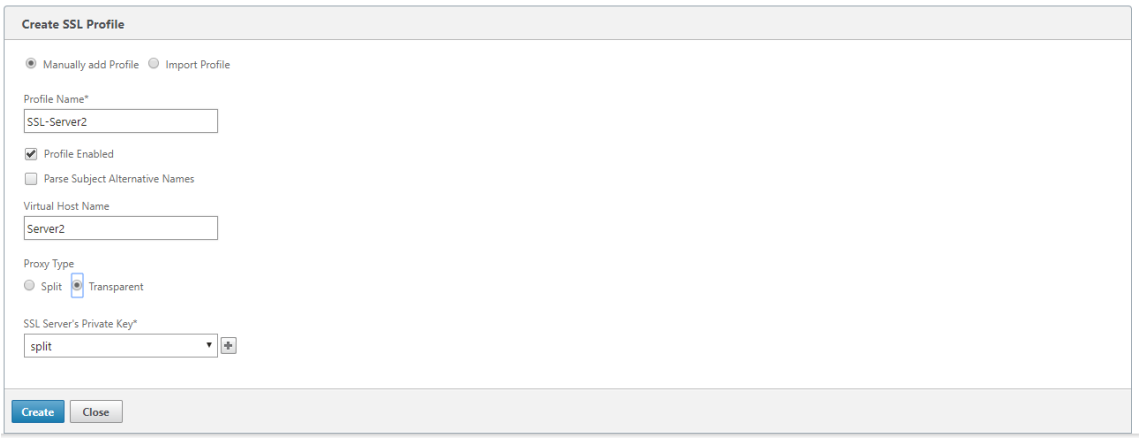
透過プロキシ **SSL** プロファイルを構成するには:

1. サーバー側の Citrix SD-WAN WO アプライアンスで、[構成]> 安全な加速 >**SSL** プロファイル に移動し、[プロファイルの追加] をクリックします。

   > 注
   >
   > SSL プロファイルを手動で追加するか、ローカルコンピューターに保存されているプロファイルをインポートすることができます。

2. [プロファイル名] フィールドに SSL プロファイルの名前を入力し、[プロファイルを有効にする] を選択します。
3. SSL サーバーが複数の仮想ホスト名を使用している場合は、[仮想ホスト名] フィールドにターゲットの仮想ホスト名を入力します。これは、サーバーの資格情報にリストされているホスト名です。

   > 注
   >
   > 複数の仮想ホストをサポートするには、ホスト名ごとに個別の SSL プロファイルを作成します。



4. 透過 プロキシタイプを選択します。
5. [**SSL** サーバーの秘密鍵] フィールドで、ドロップダウンメニューからサーバーの秘密鍵を選択するか、**+** をクリックして新しい秘密鍵をアップロードします。
6. ［作成］をクリックします。

サービスクラスを作成または変更する

サービスクラスを作成または変更して **SSL** プロファイルを添付するには:

1. Citrix SD-WAN WO アプライアンスの Web インターフェイスで、構成 **>** 最適化ルール **>** サービスクラスをクリックし、[追加] をクリックします。既存のサービスクラスを編集するには、適切なサービスクラスを選択し、[編集] をクリックします。
2. [名前] フィールドに、新しいサービスクラスの名前を入力します（たとえば、「AcceleratedHTTPS」）。

3. Acceleration Policy を **Disk**、**Memory**、または **Flow Control** に設定して、圧縮を有効にします。
4. [フィルタールール] セクションで、[追加] をクリックします。
5. [宛先 **IP** アドレス] フィールドに、サーバーの IP アドレスを入力します（たとえば、172.16.0.1、または同等に、172.16.0.1/32。
6. [方向] フィールドで、ルールを [単方向] に設定します。双方向が指定されている場合、SSL プロファイルは無効になります。
7. [**SSL** プロファイル] セクションで、作成した SSL プロファイルを選択し、[構成済み] セクションに移動します。
8. [作成] をクリックしてルールを作成します。
9. [作成] をクリックして、サービスクラスを作成します。

更新された **CLI** コマンド

Citrix SD-WAN WO 9.3 は、最新の TLS1.2 SSL プロトコルをサポートしています。TLS1.2 プロトコルのみを使用するか、TLS プロトコルの任意のバージョンを使用するかを選択できます。SSL プロトコル SSLv3 と SSLv2、および透過プロキシ SSL プロファイルはサポートされていません。**addssl-profile** および **setssl-profile** CLI コマンドが更新され、これらの変更が反映されます。

ssl プロファイルを追加します:

```
*-name  “profile-name” *

*\[-state {
 enable, disable }
 \]*

*-proxy-type split*

*\[-virtual-hostname  “hostname” \]*

*-cert-key  “cert-key-pair-name” *

*\[-build-cert-chain {
 enable, disable }
 \]*

*\[-cert-chain-store {
 use-all-configured-CA-stores,  “store-name”  }
 \]*

*\[-cert-verification {
 none, Signature/Expiration, Signature/Expiration/*

*Common-Name-White-List, Signature/Expiration/Common-Name-Black-List }
 \]*
```



```
*\[-verification-store {
 use-all-configured-CA-stores,  “store-name”  }
 \]*

*\[-server-side-protocol {
  TLS-1.2, TLS-version-any }
 \]*

*\[-server-side-ciphers  “ciphers” \]*

*\[-server-side-authentication {
 enable, disable }
 \]*

*\[-server-side-cert-key  “cert-key-pair-name” \]*

*\[-server-side-build-cert-chain {
 enable, disable }
 \]*

*\[-server-side-renegotiation {
 disable-old-style, enable-old-style, new-style,*

*compatible }
 \]*

*\[-client-side-protocol-version {
  TLS-1.2, TLS-version-any }
 \]*

*\[-client-side-ciphers  “ciphers” \]*

*\[-client-side-renegotiation {
 disable-old-style, enable-old-style, new-style,*

*compatible }
 \]*
```

set ssl-profile:

```
*-name  “profile-name”  \[-state {
 enable, disable }
 \]*

*\[-proxy-type split\]*

*\[-virtual-hostname  “hostname” \]*

*\[-cert-key  “cert-key-pair-name” \]*

*\[-build-cert-chain {
 enable, disable }
```



```
13  \]*
14
15 *\[-cert-chain-store {
16  use-all-configured-CA-stores,  “store-name”  }
17  \]*
18
19 *\[-cert-verification {
20  none, Signature/Expiration, Signature/Expiration/*
21
22 *Common-Name-White-List, Signature/Expiration/Common-Name-Black-List }
23  \]*
24
25 *\[-verification-store {
26  use-all-configured-CA-stores,  “store-name”  }
27  \]*
28
29 *\[-server-side-protocol {
30   TLS-1.2、 TLS-version-any }
31  \]*
32
33 *\[-server-side-ciphers  “ciphers” \]*
34
35 *\[-server-side-authentication {
36  enable, disable }
37  \]*
38
39 *\[-server-side-cert-key  “cert-key-pair-name” \]*
40
41 *\[-server-side-build-cert-chain {
42  enable, disable }
43  \]*
44
45 *\[-server-side-renegotiation {
46  disable-old-style, enable-old-style, new-style,*
47
48 *compatible }
49  \]*
50
51 *\[-client-side-protocol-version {
52  TLS-1.2, TLS-version-any }
53  \]*
54
55 *\[-client-side-ciphers  “ciphers” \]*
56
57 *\[-client-side-renegotiation {
58  disable-old-style, enable-old-style, new-style,*
59
60 *compatible }
61  \]*
```


Citrix SD-WAN WANOP プラグインを使用した SSL 圧縮

April 19, 2021

Citrix SD-WAN WANOP プラグインは常にクライアント側ユニットとして使用されるため、SSL シグナリング（セキュアピアリング）接続の資格情報をインストールする以外に、追加の SSL 構成は必要ありません。プラグインとアプライアンスの SSL 圧縮の主な違いは、プラグインがディスクベースの圧縮履歴内のユーザーデータを暗号化できないことです。

注意：プラグインのディスクベースの圧縮履歴は暗号化されていないため、機密性が高く一時的な暗号化通信のクリアテキストレコードが保持されます。この暗号化の欠如は、物理的なアクセスが制御されていないコンピューターでは潜在的に危険です。したがって、Citrix は次のベストプラクティスを推奨します。

- 証明書の検証を 使用しないでください：アプライアンスではなし。（この場合、アプライアンスは適切な証明書を持たないプラグインでの圧縮を許可しないことに注意してください。）
- 物理セキュリティまたはデータセキュリティに関する組織の要件を満たすことを確認できるシステム（たとえば、フルディスク暗号化を使用するラップトップ）にのみ証明書をインストールします。

Citrix SD-WAN WANOP プラグインは、SSL 分割プロキシと SSL 透過プロキシの両方をサポートします。プラグインは、SSL シグナリング接続用の証明書とキーのペアなしで出荷されます。必要に応じて、すべてのプラグインで同じ資格情報を使用することも、各プラグインに独自の資格情報を持たせることもできます。

資格情報がインストールされていない限り、プラグインは SSL 圧縮を試行しません。

プラグインは、アプライアンスから暗号ライセンスを継承します。

RPC over HTTP

April 19, 2021

Microsoft Exchange Server は、組織全体で使用される一般的な電子メールサーバーの 1 つです。Microsoft Exchange Server の最近の機能強化の結果として、インターネット経由で安全に接続できます。使用可能な帯域幅によっては、Outlook クライアントに配信される電子メールに遅延が発生する場合があります。MAPI プロトコルに加えて、Citrix SD-WAN WANOP アプライアンスは、Microsoft Exchange トラフィックを最適化するために HTTPS 経由のリモートプロシージャコール（RPC over HTTPS）をサポートしています。この機能は、Outlook Anywhere とも呼ばれます。

RPC over HTTPS は新しいプロトコルではありませんが、Microsoft Exchange 2013 以降、デフォルトのプロトコルとして MAPI に取って代わります。RPC over HTTPS の主な利点は、クライアントがインターネット経由でメールサーバーに安全に接続できることです。

RPC over HTTPS を使用する場合、Microsoft Exchange サーバーは、デジタル証明書と秘密鍵を使用して、Outlook クライアントに対して自身を認証する必要があります。クライアントとサーバー間の通信では、トランスポートプロトコルとして HTTPS を使用します。

Citrix SD-WAN WANOP アプライアンスでは、RPC over HTTPS が次の Microsoft Outlook および Exchange Server バージョンでサポートされています。

- Microsoft Outlook
  - Microsoft Outlook バージョン 2007
  - Microsoft Outlook バージョン 2010
  - Microsoft Outlook バージョン 2013
- Microsoft Exchange Server
  - Microsoft Exchange Server バージョン 2007
  - Microsoft Exchange Server バージョン 2010
  - Microsoft Exchange Server バージョン 2013

これらのうち、Microsoft Exchanges Server 2013 を除くすべてのバージョンは、MAPI（TCP 経由）および RPC over HTTPS をサポートしています。ただし、Microsoft Exchange Server 2013 は、使用している Microsoft Outlook のバージョンに関係なく、Exchange サーバーへの接続に RPC over HTTPS を使用するように接続を強制します。

HTTPS 経由で **RPC** を構成する

デフォルトでは、RPC over HTTPS 機能はアプライアンスで有効になっています。ただし、RPC over HTTPS を高速化するようにアプライアンスを構成するには、次の追加タスクを実行する必要があります。

- 暗号化された MAPI を構成します。
- サーバー証明書を使用して SSL プロファイルを構成します。
- RPC over HTTPS サービスクラスを作成し、SSL プロファイルをそれにバインドします。

暗号化された **MAPI** を構成する

> 注
>
> アプライアンスで暗号化された MAPI アクセラレーションをすでに構成している場合は、このセクションをスキップしてください。

Microsoft Outlook は、Outlook クライアントと Microsoft Exchange サーバー間でメッセージングアプリケーションプログラミングインターフェイス（MAPI）接続を使用します。MAPI 接続は、HTTP 接続によってカプセル化された RPC を使用します。したがって、Citrix SD-WAN WANOP アプライアンスで RPC over HTTPS を構成する前に、アプライアンスで暗号化された MAPI を構成する必要があります。

前提条件:

暗号化された MAPI を構成する前に、次の前提条件が満たされていることを確認してください。

- Secure Peer オプションは、サーバー側アプライアンスだけでなくクライアントでも True に設定する必要があります。安全なパートナーを構成するには、安全なピアリングを参照してください。
- サーバー側アプライアンスで構成された DNS IP アドレスは到達可能である必要があります。
- データセンター側のアプライアンスは、ドメインに正常に参加する必要があります。
- デリゲートユーザーをデータセンター側のアプライアンスに追加し、そのステータスを「成功」としてマークする必要があります。

詳しくは、「安全な Windows トラフィックを最適化するように Citrix SD-WAN WANOP アプライアンスを構成する」を参照してください。

サーバー証明書を使用して **SSL** プロファイルを構成する

MAPI 接続をカプセル化する HTTPS 接続は、SSL によって保護されています。その結果、RPC over HTTPS には、TCP ポート 443 を介した接続が必要です。このポートは HTTPS に割り当てられ、Web サーバー管理者は通常ファイアウォールアプリケーションで開いたままにします。SSL で保護された通信を使用すると、RPC over HTTPS がすべての通信のセキュリティを維持するのに役立ちます。

RPC over HTTPS アクセラレーションを有効にするには、アプライアンスにサーバー証明書をインストールする必要があります。このサーバー証明書を使用して、RPC over HTTPS が安全な通信に使用する SSL プロファイルを構成できます。Exchange サーバー証明書を使用して SSL プロファイルを構成するには、サーバー証明書とクライアント証明書のインストールを参照してください。

> 注
>
> SSL プロファイルは、データセンター側のアプライアンスでのみ構成する必要があります。

RPC over HTTPS サービスクラスを作成し、**SSL** プロファイルをそれにバインドします

RPC over HTTP 接続を最適化するには、HTTPS とすべての MAPI アプリケーションを一覧表示するサービスクラスを作成する必要があります。このサービスクラスの宛先 IP アドレスとして Microsoft Exchange サーバーの IP アドレスを指定してから、作成した SSL プロファイルをこのサービスクラスにバインドする必要があります。プロファイルをサービスクラスにバインドすると、このプロファイルを使用して Outlook クライアントと Microsoft Exchange サーバー間の通信が保護されます。

> 注
>
> データセンター側のアプライアンスでのみ SSL プロファイルを構成してサービスクラスにバインドする必要があります。

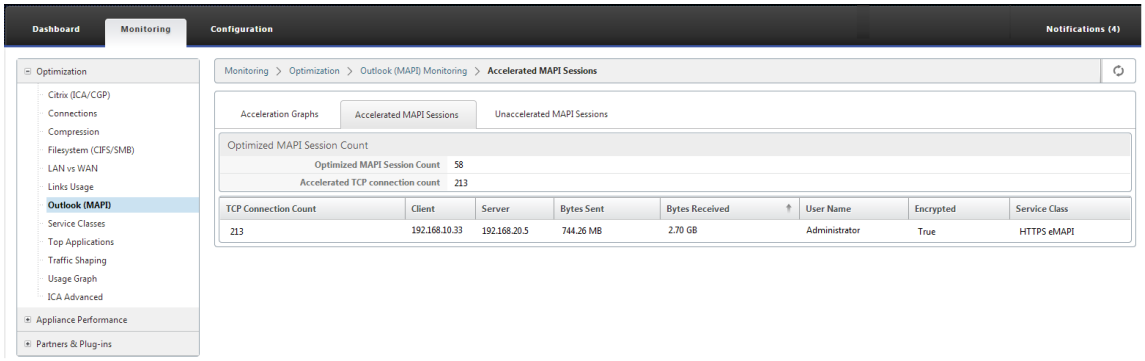
HTTPS 接続を介した高速 **RPC** の確認

アプライアンスで RPC over HTTPS を構成した後、MAPI の [監視] ページで、アプライアンスが RPC over HTTPS 接続を高速化していることを確認できます。HTTPS 接続を介した高速 RPC は、[高速 MAPI セッション] タブに一覧表示されます。

> 注
>
> RPC over HTTPS 接続を高速化するには、クライアント側アプライアンスとサーバー側 Citrix SD-WAN WANOP アプライアンスで RPC over HTTPS を構成する必要があります。

RPC over HTTPS 接続が高速化されていることを確認するには

1. モニタリング > 最適化 > **Outlook**（**MAPI**）に移動します。
2. [**Accelerated MAPI Sessions**] タブで、RPC over HTTPS 接続が高速化されていることを確認します。



> 注
>
> アプリケーションには、HTTPS eMAPI、HTTP eMAPI、HTTPS MAPI、および HTTP MAPI の可能な値があります。

TCP フロー制御アクセラレーション

April 19, 2021

通常の WAN は、リンクの使用率が高く、長距離での応答性が非常に低くなります。通常の高速化されていない WAN リンクで広く使用されている経験則は、「リンクの使用率が到達すると、40%, リンクがほとんど使用できなくなるま

でパフォーマンスと信頼性が低下したため、帯域幅を追加するときが来ました。」インタラクティブなパフォーマンスが低下し、人々が仕事をするのが難しくなり、接続が頻繁にタイムアウトします。加速リンクにはこの問題はありません。使用率が 95%のリンクは、引き続き完全に使用できます。

Citrix SD-WAN WANOP アプライアンスは、WAN リンク上の TCP トラフィックを制御する仮想ゲートウェイになります。通常の TCP は、エンドポイントデバイスによって接続ごとに制御されます。エンドポイントデバイスも個々の接続もリンク速度や競合するトラフィックの量を認識していないため、リンクトラフィックの最適な制御は困難です。一方、ゲートウェイは、リンクトラフィックを監視および制御するのに理想的な位置にあります。通常のゲートウェイは、TCP に欠けているフロー制御を提供できないため、この機会を浪費します。Citrix SD-WAN WANOP テクノロジーは、ネットワーク機器と TCP 接続に欠けているインテリジェンスを同様に追加します。その結果、高損失や極端な距離などの過酷な条件下でも、WAN のパフォーマンスが大幅に向上します。

Citrix SD-WAN WANOP フロー制御はロスレスで透過的であり、幅広い速度最適化を実装します。自動検出と自動構成のため、構成は必要ありません。ただし、ファイアウォールがアクセラレーションアルゴリズムで使用される TCP オプションをブロックしている場合は、ファイアウォールを微調整する必要がある場合があります。

ロスレスで透過的なフロー制御

April 19, 2021

アクセラレーションは、2 つのアプライアンス（1 つは送信サイトともう 1 つは受信サイト）、または Citrix SD-WAN WANOP アプライアンスと Citrix SD-WAN WANOP プラグインを通過する TCP 接続で動作します。上の図は 2 つのアプライアンスのネットワークを示していますが、どのアプライアンスでも、他のアプライアンスを備えたサイト間の接続を同時に加速できます。これにより、リンクごとに 2 つではなく、サイトごとに 1 つのアプライアンスを使用できます。

他のゲートウェイと同様に、Citrix SD-WAN WANOP アプライアンスはパケットをリンクに計測します。ただし、通常のゲートウェイとは異なり、次のような各リンクセグメントに透過的でロスレスのフロー制御を課します。

- 送信側と送信側アプライアンス間の LAN セグメント
- 送信アプライアンスと受信アプライアンス間の WAN セグメント
- 受信アプライアンスと受信機の間の LAN セグメント

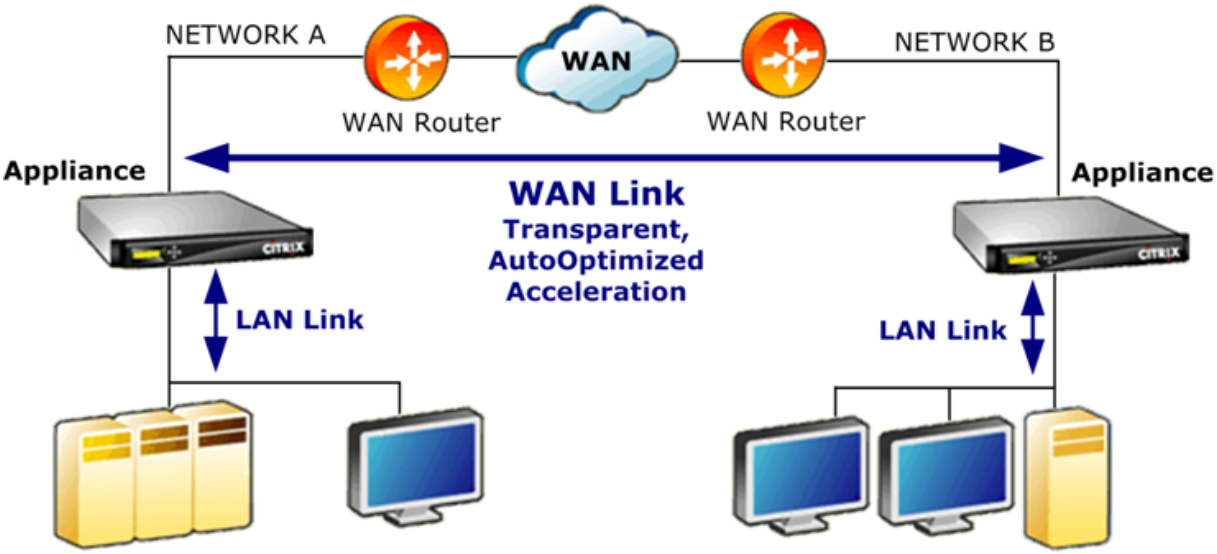
フロー制御は、これら 3 つのセグメントごとに個別に管理できます。セグメントは部分的に分離されているため、各セグメントの速度を個別に制御できます。これは、接続の速度をその公平な帯域幅シェアまですばやく増減する必要がある場合に重要であり、拡張 WAN アルゴリズムと圧縮をサポートする手段としても重要です。

TCP プロトコルは、すべての TCP 接続が帯域幅の使用量を継続的に増加させようとするように設計されています。ただし、リンク帯域幅には制限があります。その結果、リンクがオーバーランします。Citrix SD-WAN WANOP フロー制御は、TCP 接続を適切な速度でフローし続けます。リンクはいっぱいになりますが、オーバーランすることはないため、キューイングの遅延とパケット損失が最小限に抑えられ、スループットが最大化されます。

通常の TCP では、実行時間の長い接続（すべての帯域幅を占有する時間があった）は、実行時間の短い接続を絞り出す傾向があります。インタラクティブな応答性を損なうこの問題は、フロー制御では発生しません。

フロー制御は、Citrix SD-WAN WANOP ファミリのすべてのアプライアンスの標準機能です。

図 1：アクセラレーションはパフォーマンスを透過的に向上させます



速度の最適化

April 19, 2021

ほとんどの TCP 実装は、WAN リンク上ではうまく機能しません。2 つの問題を挙げれば、標準の TCP 再送信アルゴリズム（SelectiveAcknowledgements と TCPFast Recovery）は、損失率の高いリンクには不十分であり、短期間のトランザクション接続の必要性を考慮していません。

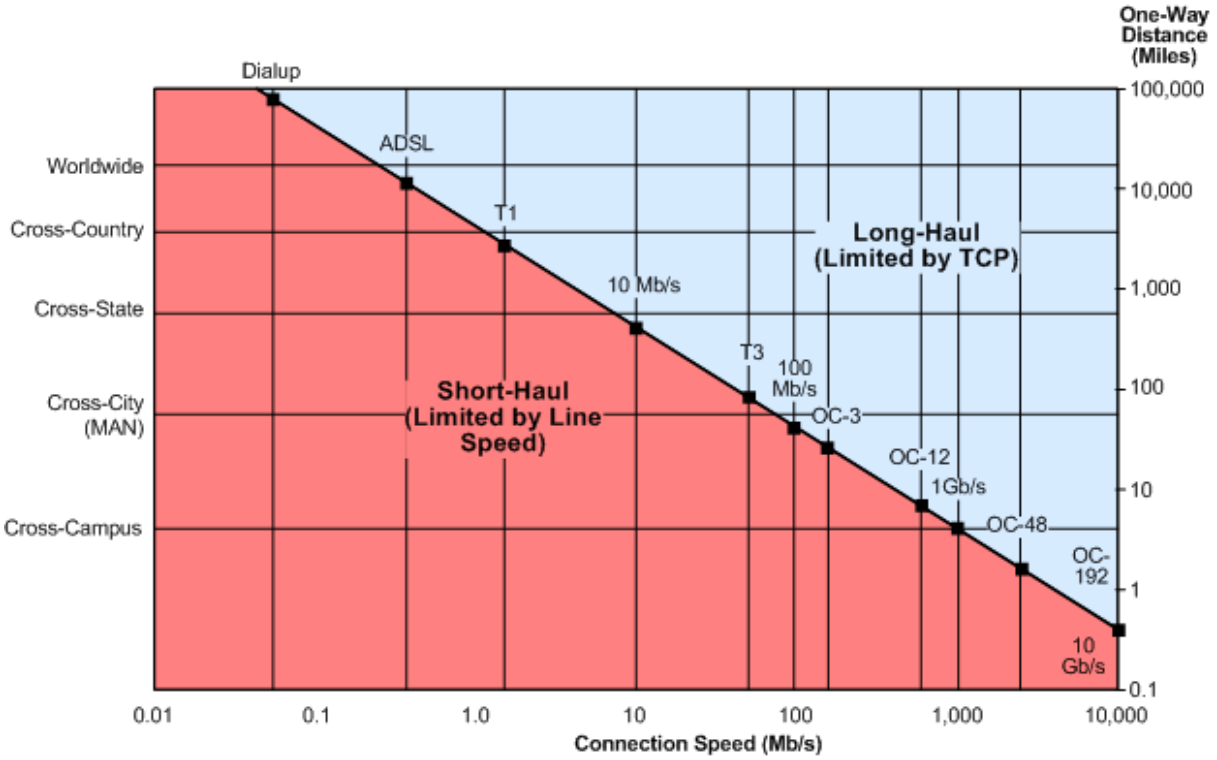
Citrix SD-WAN WANOP は、あらゆる種類の悪条件の下でデータの流れを維持するために、幅広い WAN 最適化を実装しています。これらの最適化は透過的に機能し、データができるだけ早く宛先に到着するようにします。

WAN 最適化は透過的に動作し、構成は必要ありません。

WAN 最適化は、すべての Citrix SD-WAN WANOP アプライアンスの標準機能です。

次の図は、エンドポイントが標準 TCP（TCP Reno）を使用している場合に、加速なしでさまざまな距離で可能な転送速度を示しています。たとえば、ギガビットスループットは、半径数マイル以内の加速なしで可能であり、100 Mbps は 100 マイル未満に到達可能であり、世界中の接続でのスループットは、リンクの実際の速度に関係なく、1Mbps 未満に制限されます。ただし、加速すると、対角線より上の速度がアプリケーションで使用できるようになります。距離はもはや制限要因ではありません。

図 1：距離のある加速されていない TCP パフォーマンスの急落



> 注
>
> Citrix アクセラレーションがないと、TCP スループットは距離に反比例し、長距離の高速リンクの全帯域幅を抽出できなくなります。加速すると、距離係数がなくなり、リンクの全速力を任意の距離で使用できます。（Mathis、*et al*、 Pittsburgh Supercomputer Center によるモデルに基づくチャート。）

加速された転送パフォーマンスは、リンク帯域幅とほぼ同じです。転送速度は、高速化されていない TCP の場合よりも高速であるだけでなく、ネットワークの状態が変化してもはるかに一定です。その効果は、離れた接続をローカルであるかのように動作させることです。リンクの使用率に関係なく、ユーザーが知覚する応答性は一定のままです。90%の使用率で動作する WAN が対話型タスクに役に立たない通常の TCP とは異なり、高速リンクは、90%のリンク使用率での応答性で 10% と同じ応答性を持ちます。

短距離接続（上の図の対角線より下にある接続）では、良好なネットワーク条件下では加速はほとんどまたはまったく発生しませんが、ネットワークが劣化すると、パフォーマンスの低下は通常の TCP よりもはるかに遅くなります。

UDP などの非 TCP トラフィックは加速されません。ただし、それでもトラフィックシェーパーによって管理されます。

例

高度な TCP 最適化の一例は、トランザクションモードと呼ばれる再送信の最適化です。TCP の特徴は、トランザクションの最後のパケットがドロップされた場合、受信者のタイムアウト（RTO）期間が経過するまで、送信者はその損失に気付かないことです。この遅延は、常に少なくとも 1 秒長く、多くの場合それより長くなりますが、損失のあるリンクで見られる数秒の遅延の原因です。これは、対話型セッションを不快または不可能にする遅延です。

トランザクションモードは、少し遅れてトランザクションの最後のパケットを自動的に再送信することにより、この問題を解決します。したがって、両方のコピーが削除されない限り、RTO は発生しません。これはほとんどありません。

バルク転送は基本的に単一の巨大なトランザクションであるため、トランザクションモードでバルク転送に使用される追加の帯域幅は、ファイルごとに 1 パケット程度です。ただし、キーの押下やマウスの動きなどのインタラクティブなトラフィックには、小さなトランザクションがあります。トランザクションは、単一の小さめのパケットで構成される場合があります。このようなパケットを 2 回送信するには、適度な帯域幅要件があります。事実上、トランザクションモードは、インタラクティブトラフィックに前方誤り訂正（FEC）を提供し、他のトラフィックにトランザクション終了の RTO 保護を提供します。

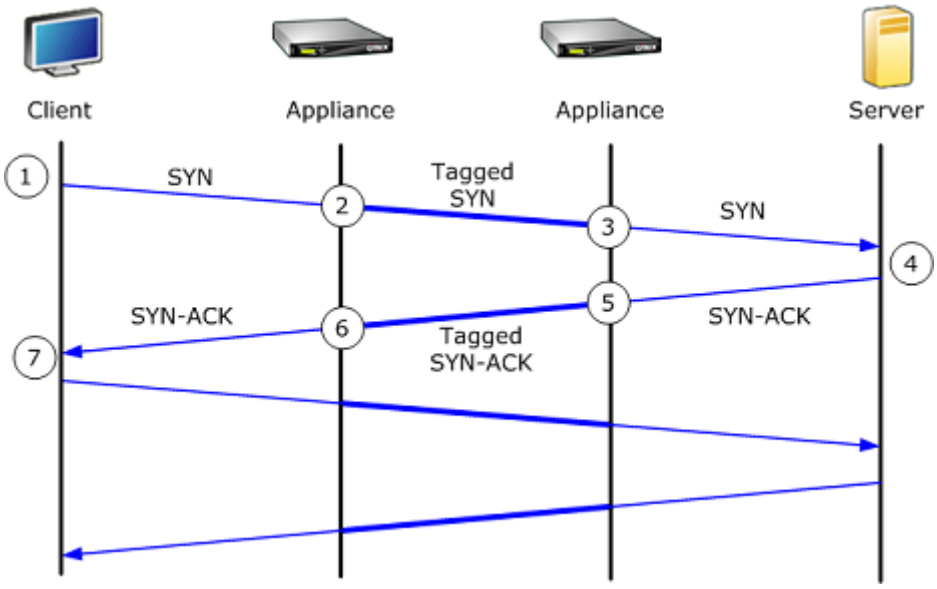
自動検出と自動構成

April 19, 2021

自動検出と呼ばれるプロセスで、Citrix SD-WAN WANOP ユニットは互いの存在を自動的に検出します。アプライアンスは、各接続の最初のパケットに TCP ヘッダーオプションを添付します。SYN パケット（接続を開くためにクライアントからサーバーに送信されます）、および SYN-ACK パケット（接続を示すためにサーバーからクライアントに送信されます）受け入れられました）。SYN パケットにタグを付け、タグ付きの SYN パケットと SYN-ACK パケットをリッスンすることにより、アプライアンスは接続ごとにリアルタイムで互いの存在を検出できます。

自動検出の主な利点は、ネットワークに新しいアプライアンスを追加するたびにすべてのアプライアンスを再構成する必要がないことです。彼らは自動的にお互いを見つけます。さらに、同じプロセスで自動構成が可能です。2 つのアプライアンスは、TCP ヘッダーオプションを使用して、帯域幅制限（送信方向と受信方向の両方）、基本アクセラレーションモード（ハードブーストまたはソフトブースト）、および許容可能な圧縮モード（ディスク、メモリ、またはなし）などの動作パラメーターを交換します。。各アプライアンスがそのパートナーに関して必要とするすべての情報は、各接続と交換され、接続ごとのバリエーション（たとえば、許容される圧縮タイプのサービスクラスごとのバリエーション）が可能になります。

図 1：自動検出の仕組み



自動検出プロセスは次のように機能します。

1. クライアントは、通常どおり、TCP SYN パケットを送信することにより、サーバーへの TCP 接続を開きます。
2. 最初のアプライアンスは、アプライアンス固有の TCP ヘッダーオプションのセットをアタッチし、ウィンドウサイズを調整した後、SYN パケットを通過させます。
3. 2 番目のアプライアンスは TCP オプションを読み取り、パケットから削除して、サーバーに転送します。
4. サーバーは、通常どおり TCP SYN-ACK パケットで応答することによって接続を受け入れます。
5. 2 番目のアプライアンスは、この接続がアクセラレーションの候補であることを記憶し、独自のアクセラレーションオプションを SYN-ACK ヘッダーに付加します。
6. 最初のアプライアンスは、2 番目のアプライアンスによって追加されたオプションを読み取り、パケットヘッダーからそれらを取り除き、パケットをクライアントに転送します。これで接続が高速化されました。2 つのアプライアンスは、オプション値を介して必要なパラメーターを交換し、接続の間、それらをメモリーに保管します。

接続は高速化され、高速化はクライアント、サーバー、ルーター、およびファイアウォールに対して透過的です。

TCP フロー制御モード

April 19, 2021

TCP フロー制御には、softboost と hardboost の 2 つのモードがあります。

Softboost は、リンクの帯域幅制限までの速度で高速トラフィックを送信するレートベースの送信者を使用します。帯域幅制限がリンク速度よりわずかに低く設定されている場合、パケット損失と遅延は最小化され、リンク使用率は

最大化されます。対話型アプリケーションでは応答時間が速く、一括転送アプリケーションでは帯域幅が広くなります。Softboost は、任意のトポロジの他のアプリケーションとネットワークを共有し、サードパーティの QoS システムと相互運用します。

Hardboost は softboost よりも攻撃的です。パケット損失やその他のいわゆる「輻輳信号」を無視することにより、衛星リンクなど、輻輳に関連しない重い損失に悩まされているリンクで非常に優れたパフォーマンスを発揮します。また、多くの海外リンクなど、バックグラウンドパケット損失が高い低品質の長距離リンクにも優れています。Hardboost は、softboost で十分なパフォーマンスが得られないポイントツーポイントリンクにのみ推奨されます。

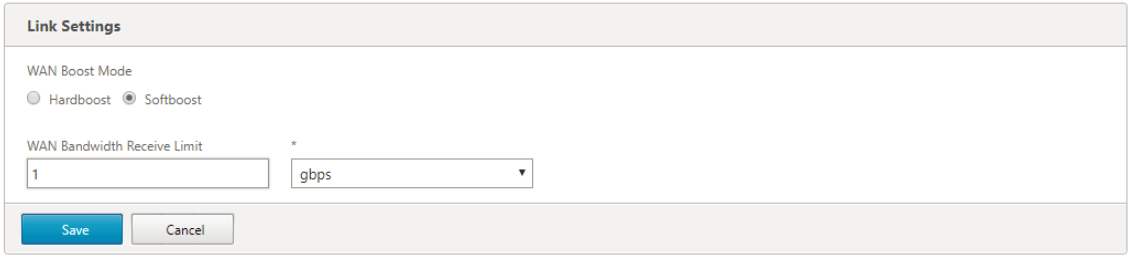
Softboost はデフォルトのモードであり、ほとんどの場合推奨されます。

> 注
>
> - ハードブーストは、ハブ帯域幅が少なくとも加速されたスポーク帯域幅の合計に等しい、固定速度のポイントツーポイントリンクまたはハブアンドスポーク展開でのみ使用する必要があります。
> - Softboost と hardboost は相互に排他的です。つまり、相互に通信する必要のあるすべてのアプライアンスを同じに設定する必要があります。一方のユニットがハードブーストに設定され、もう一方のユニットがソフトブーストに設定されている場合、加速は行われません。

ソフトブーストモードを選択するには:

Softboost はデフォルトのモードであり、ほとんどの場合推奨されます。

1. 構成 > リンク > ハードブースト /ソフトブースト をクリックして編集をクリックします。
2. **WAN** ブーストモード として **Softboost** を選択します。



3. [保存] をクリックします

ハードブーストモードを選択するには:

ハードブーストモードは、ハブ帯域幅がアクセラレーションスポークリンクの帯域幅以上である固定速度のポイントツーポイントリンクまたはハブアンドスポークリンクでのみ選択します。

1. 構成 > リンク > ハードブースト /ソフトブースト をクリックして編集をクリックします。
2. **WAN** ブーストモード として ハードブーストを選択します。
3. **WAN** 帯域幅の受信制限 をリンク速度の 95%に設定します。
4. ［保存］をクリックします。

ファイアウォールについての考慮事項

April 19, 2021

Citrix SD-WAN WANOP アプライアンスで TCP オプションを使用すると、あまり一般的ではない TCP オプションを使用した接続へのサービスの拒否に関する積極的なルールを持つファイアウォールからの高速トラフィックが危険にさらされます。

一部のファイアウォールは、「不明な」オプションを取り除き、パケットを転送します。このアクションは加速を防ぎますが、接続を損なうことはありません。

他のファイアウォールは、不明なオプションの接続へのサービスを拒否します。つまり、Citrix SD-WAN WANOP オプションを使用した SYN パケットはファイアウォールによってドロップされます。アプライアンスが繰り返し接続試行の失敗を検出すると、オプションなしで再試行します。これにより、通常 20〜60 秒の範囲で、加速なしで可変長の遅延後に接続が復元されます。

Citrix SD-WAN WANOP オプションを変更せずに通過させないファイアウォールは、24〜31（10 進数）の範囲の TCP オプションを受け入れるように再構成する必要があります。

ほとんどのファイアウォールはこれらのオプションをブロックしません。ただし、リリース 7.x ファームウェアを搭載した Cisco ASA および PIX ファイアウォール（およびおそらく他のファイアウォール）は、デフォルトでこれを行う場合があります。

リンクの両端にあるファイアウォールを調べる必要があります。どちらかが発信接続ではオプションを許可しているが、着信接続ではそれらをブロックしている可能性があるためです。

次の例は、7.x ファームウェアを使用する Cisco ASA55x0 ファイアウォールで機能するはずです。24〜31 の範囲のオプションをグローバルに許可するため、カスタマイズされたインターフェイスごとまたはユニットごとの構成はありません。

```
==================================================================
CONFIGURATION FOR CISCO ASA 55X0 WITH 7.X CODE TO ALLOW TCP OPTIONS
==================================================================
hostname(config)# tcp-map WSOptions
hostname(config-tcp-map)# tcp-options range 24 31 allow
hostname(config-tcp-map)# class-map WSOptions-class
hostname(config-cmap)# match any
hostname(config-cmap)# policy-map WSOptions
hostname(config-pmap)# class WSOptions-Class
hostname(config-pmap-c)# set connection advanced-options WSOptions
hostname(config-pmap-c)# service-policy WSOptions global
```

PIX ファイアウォールの構成は次のとおりです。

```
=====================================================
POLICY MAP TO ALLOW APPLIANCE TCP OPTIONS TO PASS (PIX 7.x)
=====================================================
pixfirewall(config)#access-list tcpmap extended permit tcp any any
```

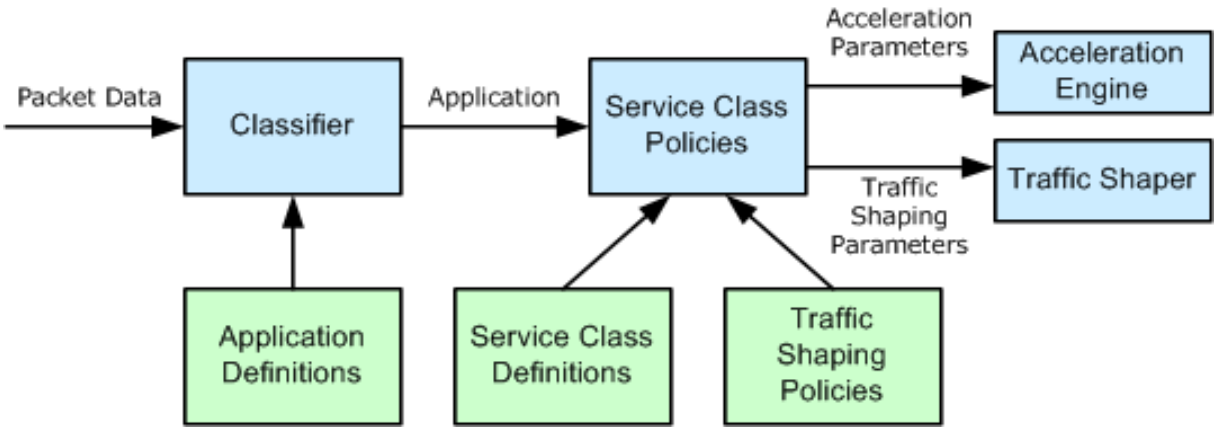


```
pixfirewall(config)# tcp-map tcpmap
pixfirewall(config-tcp-map)# tcp-opt range 24 31 allow
pixfirewall(config-tcp-map)# exit
pixfirewall(config)# class-map tcpmap
pixfirewall(config-cmap)# match access-list tcpmap
pixfirewall(config-cmap)# exit
pixfirewall(config)# policy-map global_policy
pixfirewall(config-pmap)# class tcpmap
pixfirewall(config-pmap-c)# set connection advanced-options tcpmap
```

トラフィックの分類

April 19, 2021

Citrix SD-WAN WANOP アプライアンスの 2 つの主な機能は、すべてのタイプのトラフィックのリンク使用量を最大化するトラフィックシェーピングと、圧縮とさまざまな最適化を適用して TCP トラフィックを高速化するアクセラレーションです。トラフィックシェーピングとアクセラレーションの両方の 2 つの基本コンポーネントは、アプリケーション分類メカニズムとサービスクラスメカニズムです。前者はトラフィックのタイプを識別し、後者がトラフィックをサービスクラスに割り当てることができるようにします。各サービスクラスには、トラフィックシェーピングポリシーとアクセラレーションポリシーがあります。



アプリケーション分類子

April 19, 2021

アプリケーション分類子は、アプリケーション定義を使用して、プロトコルとアプリケーションによってトラフィックを分類します。この情報は、レポートの作成とサービスクラスメカニズムによって使用されます。多くのアプリケーションはすでに定義されており、必要に応じてさらに定義できます。

アプリケーション定義のプロトコルとポートの仕様

アプリケーション分類子は、Internet Assigned Numbers Authority（IANA）の公式プロトコルとポート仕様を使用します。http://www.iana.org。公式以外のアプリケーションがポートを使用する場合があります。分類器は通常、そのような使用を検出できません。ネットワークでこのようなアプリケーションを使用している場合は、通常、アプリケーション分類子でアプリケーションの名前を変更して、ネットワークでこのポートを使用している実際のアプリケーションを示すことで、この問題を解決できます。たとえば、ポート 3128 を Squid Web キャッシュの標準的な使用ではなく、SOCKS プロキシに使用する場合、わかりやすくするために、Squid（TCP）アプリケーションの名前を S OCKS（ポート 3128）に変更できます。

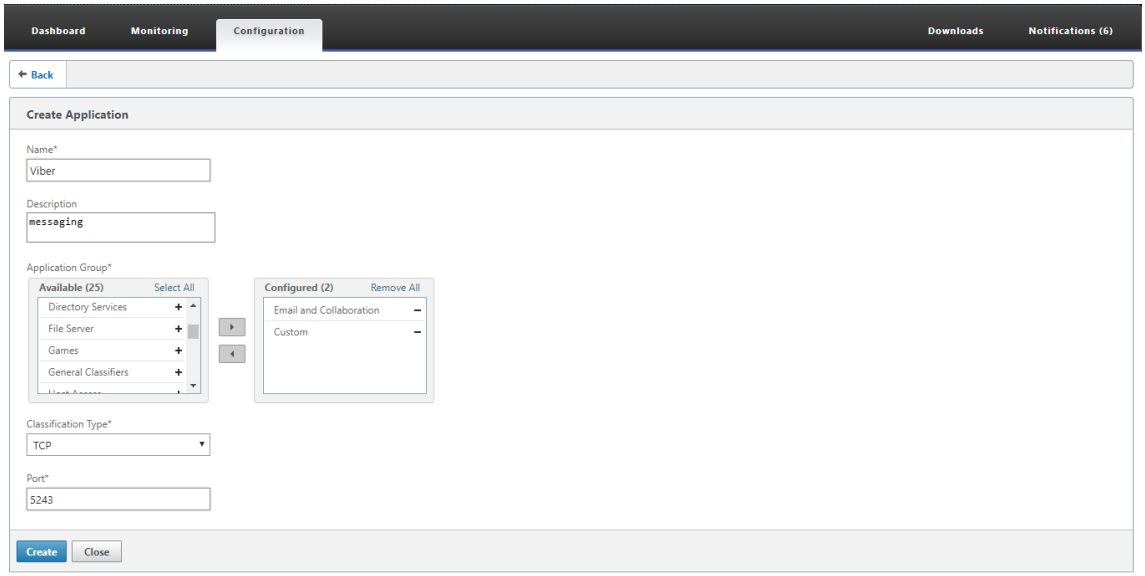
アプリケーションの定義が重複していてはなりません。たとえば、ネットワーク上の 1 つのアプリケーションが TCP ポート 3120 および 3128 を使用し、別のアプリケーションがポート 3120 を使用する場合、1 つの Citrix SD-WAN WANOP アプリケーション定義にのみポート 3120 を含めることができます。

アプリケーション定義を構成する

- 動的 TCP、動的ポート割り当てを使用するアプリケーション用
- イーサネットパケットタイプの場合、Ether タイプ
- ICA 公開アプリ、Virtual Apps/Virtual Desktops アプリケーション用
- IP、ICMP や GRE などの IP プロトコル用
- TCP、TCP アプリケーション用
- UDP、UDP アプリケーション用
- 特定の Web サイトまたはドメインの Web アドレス。

アプリケーション防御を構成するには:

1. 構成 > 最適化ルール > アプリケーション分類子 をクリックし、[追加] をクリックします。



2. 【アプリケーションの作成】ページで、次のパラメーターを設定します。

   - 名前 -アプリケーション分類子の名前。ASCII 英数字またはアンダースコア (_) で始める必要があり、ASCII 英数字、アンダースコア、ハッシュ (#)、ピリオド（。）、コロン (:)、アットマーク (@)、等しい (=)、ハイフン（-）文字のみを含める必要があります。最大長：31 文字。
   - 説明 -アプリケーション分類子の説明。
   - アプリケーショングループ -アプリケーション分類子は、このアプリケーショングループに属しています。アプリケーショングループは、機能に基づいて分類された、事前定義されたアプリケーションのグループのセットです。
   - 分類タイプ -このアプリケーション分類子に使用する高レベルの分類。高レベルの分類は、ほとんどの場合、アプリケーションが使用するポートに基づいて行われます。
   - ポート–使用するポート番号。0～65535 の範囲、リスト、または数値を入力できます。

3. ［作成］をクリックします。

   [アプリケーション分類子] ページには、SD-WAN WANOP 分類子によって認識されるすべてのアプリケーションが一覧表示されます。

[アプリケーション分類子] ページには、SD-WAN WANOP 分類子によって認識されるすべてのアプリケーションが一覧表示されます。

> ヒント
>
> [自動検出] をクリックして、データストリームに表示される Citrix 公開アプリケーションをアプリケーションリストに自動的に追加できるようにします。検出されると、レポートに表示され、トラフィックシェーピングポリシーに使用できます。

サービスクラス

April 19, 2021

サービスクラスには、サービスクラス定義に一致するすべての接続に使用されるトラフィックシェーピングポリシーとアクセラレーションポリシーが割り当てられます。サービスクラスは、次のパラメータに基づくことができます。

- アプリケーション
- IP または VLAN アドレス
- DSCP ビット
- SSL プロファイル

開始点として、デフォルトのサービスクラス定義をお勧めします。リンクに対して不十分であることが判明した場合は、それらを変更してください。

サービスクラスは、順序付きリストで定義されます。処理中のトラフィックに一致する最初の定義が、トラフィックのサービスクラスになります。

加速の決定とトラフィックシェーピングポリシーの違い

アクセラレーションを決定するために、Citrix SD-WAN WANOP アプライアンスは各 TCP 接続の最初の SYN パケットを調べて、接続がアクセラレーションの候補であるかどうかを判断します。SYN パケットにはペイロードが含まれず、ヘッダーのみが含まれるため、アクセラレーションの決定は、接続の宛先ポートや宛先 IP アドレスなど、SYN パケットのヘッダーの内容に基づいて行う必要があります。加速は、一度適用されると、接続の間持続します。

アクセラレーションの決定とは異なり、トラフィックシェーピングポリシーは、接続のデータストリームのコンテンツに基づくことができます。アプリケーション分類子が最終的な分類に十分なデータを受信するのにかかる時間によっては、接続がその存続期間中に再分類される場合があります。

たとえば、`http://www.example.com` への HTTP 接続の最初のパケットは、ヘッダーを含むがペイロードを含まない SYN パケットです。ヘッダーの IP 宛先ポートは 80 で、これは HTTP：インターネットサービスクラスの定義と一致するため、アクセラレーションエンジンはアクセラレーションの決定に基づいて決定します。この場合、そのサービスクラスに基づいてなし（アクセラレーションなし）になります。

トラフィックシェーパーは、HTTP：Internet service-class のトラフィックシェーピングポリシーを使用しますが、この決定は一時的なものです。最初のペイロードパケットには、文字列 GET `http://www.example.com`が含まれています。これは、アプリケーション分類子のサンプルアプリケーション定義と一致します。サンプルアプリケーションを含むサービスクラスは、HTTP：Internet を含むサービスクラスではなく、トラフィックシェーパーによって選択され、トラフィックシェーパーは、そのサービスクラス定義で指定されたサービスクラスポリシーを使用します。

> 注
>
> サービスクラスポリシーに関係なく、レポート機能はサンプルアプリケーションの使用状況を追跡します。
>
> 重要
>
> すべてのトラフィックはアプリケーションとサービスクラスに関連付けられており、すべてのサービスクラスにはトラフィックシェーピングポリシーがありますが、TCP 接続のみにアクセラレーションポリシーがあります。

サービスクラス定義を構成する

サービスクラス定義は順序付きリストであるため、一般的なケースの例外である定義は、サービスクラスページのより一般的な定義の前に置く必要があります。ルールがトラフィックに一致する最初の定義は、適用される定義です。例：

- URL ベースのルールも HTTP サービスクラスと一致するため、URL に基づくサービスクラスは、サービスクラスリスト内の HTTP サービスクラスの前に置く必要があります。したがって、HTTP サービスクラスを最初に配置すると、URL ベースのルールまたは公開されたアプリケーションベースのルールが使用されなくなります。
- 同様に、ICA（Virtual Apps/Virtual Desktops）公開アプリケーションに基づくサービスクラスは、Citrix サービスクラスの前にする必要があります。

すべての URL ベースのルールは HTTP サービスクラスと一致するため、HTTP サービスクラスをそれらの上に置くと、URL ベースのルールまたは公開されたアプリケーションベースのルールが使用されなくなります。

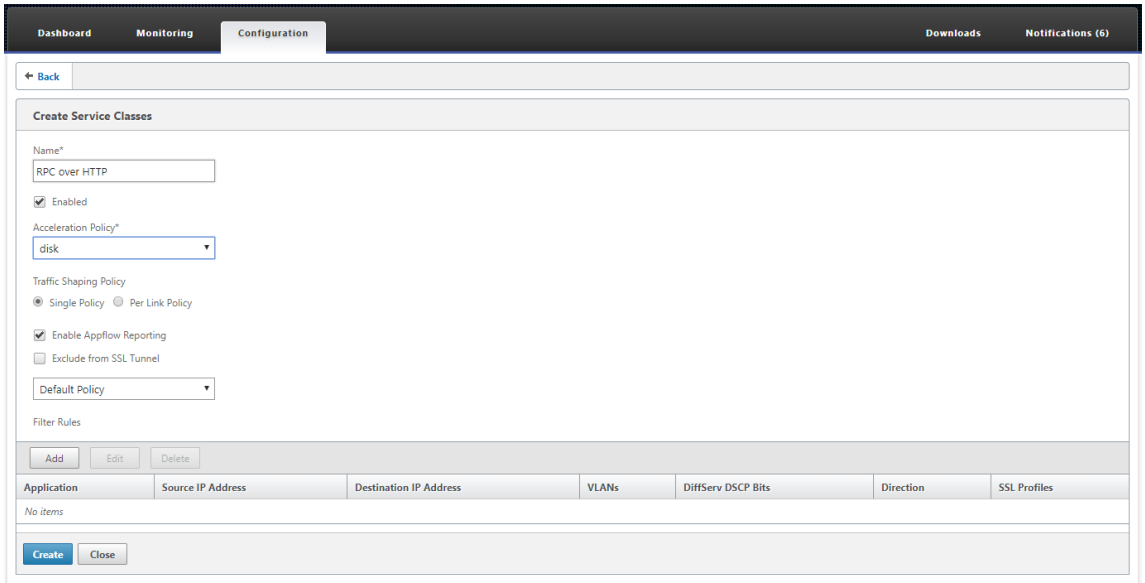
Configuration Overview > Optimization Rules > **Service Classes**

Add | Edit | Delete | Update Order | Filter Rules | Show User Modified Service Classes Only

Order	Name	Status	Acceleration Policy	Traffic Shaping Policy	Appflow Reporting Status
1	ICA	Enabled	disk	ICA Priorities	Enabled
2	Web (Private)	Enabled	disk	Default Policy	Enabled
3	Web (Private-Secure)	Enabled	Flow Control Only	Default Policy	Enabled
4	Web (Internet)	Enabled	disk	Default Policy	Enabled
5	Web (Internet-Secure)	Enabled	Flow Control Only	Default Policy	Enabled
6	CIFS	Enabled	disk	Default Policy	Enabled
7	NFS	Enabled	disk	Default Policy	Enabled
8	Microsoft Exchange (MAPI)	Enabled	disk	Default Policy	Enabled
9	Mail (Other)	Enabled	disk	Default Policy	Enabled
10	VOIP and Multimedia	Enabled	None	VOIP Traffic	Enabled
11	VOIP Webcam	Enabled	None	High Priority Traffic	Enabled
12	FTP Data	Enabled	disk	Low Priority Traffic	Enabled
13	FTP Control	Enabled	Flow Control Only	Default Policy	Enabled
14	Instant Messaging	Enabled	disk	Default Policy	Enabled
15	Session Applications	Enabled	Flow Control Only	Default Policy	Enabled
16	Directory and Security	Enabled	Flow Control Only	Default Policy	Enabled
17	Database Applications	Enabled	Flow Control Only	Default Policy	Enabled
18	Secure Applications	Enabled	Flow Control Only	Default Policy	Enabled
19	Iperf	Enabled	Flow Control Only	Low Priority Traffic	Enabled
20	NetApp SnapMirror	Enabled	memory	Default Policy	Enabled
21	Other TCP Traffic	Enabled	None	Default Policy	Enabled
22	Unclassified Traffic	Enabled	None	Default Policy	Enabled

RPC over HTTP サービスクラスを作成し、SSL プロファイルをそれにバインドするには:

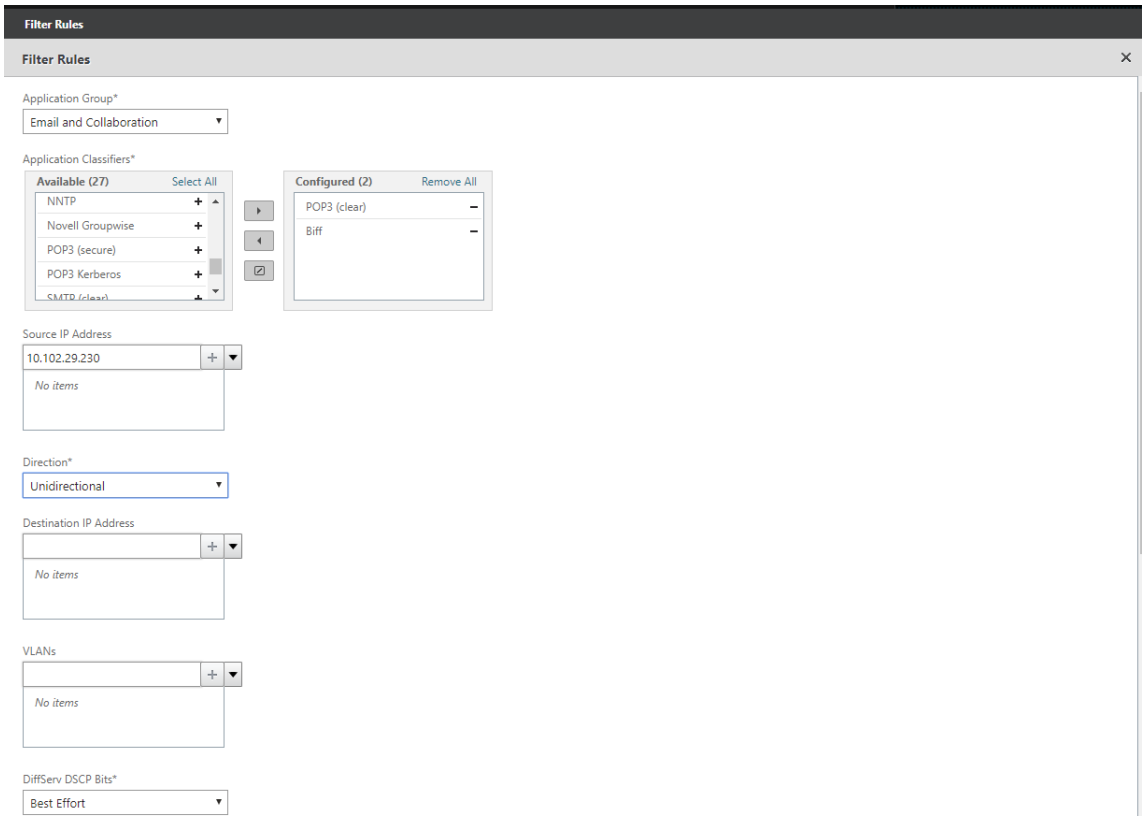
1. [構成] > [最適化ルール] > [サービスクラス] に移動し、[追加] をクリックします。



2. 「名前」フィールドに、サービスクラスの名前を入力します。
3. [有効] オプションが選択されていることを確認してください。
4. [アクセラレーションポリシー] リストから、アクセラレーションポリシーを選択します。メモリとディスクは、圧縮に使用されるトラフィック履歴を保存する場所を指定します。アプライアンスはトラフィックに適しているかどうかに応じてディスクまたはメモリを自動的に選択するため、通常はディスクが最適です。メモリはメモリのみを指定します。**Flow Control Only** を選択して、圧縮を無効にし、フロー制御の加速を有効にします。常に暗号化されるサービス、および FTP 制御チャネルの場合はこれを選択します。**None** は、非圧縮の暗号化されたトラフィックとリアルタイムビデオにのみ使用されます。
5. このサービスクラスの **AppFlow** レポート を有効にするには、[AppFlow レポートを有効にする] を選択します。このサービスクラスからの情報は、AppFlow レポートに含まれています。AppFlow は、ネットワークインフラストラクチャによって処理されるアプリケーショントランザクションデータのロックを解除するための業界標準です。WAN Optimization AppFlow インターフェイスは、任意の AppFlow コレクタと連携してレポートを生成します。コレクターは、AppFlow オープンスタンダードを使用して、アプライアンスから詳細情報を受け取ります。
6. サービスクラスに関連付けられたトラフィックを SSL トンネリングから 除外するには、**SSL** トンネルから除外 を選択します。
7. トラフィックシェーピングポリシーリストで、[デフォルトポリシー] オプションが選択されていることを確認します。トラフィックシェーピングポリシーには、他のトラフィックと比較して、一致するトラフィックがどのように処理されるかを決定する加重優先度およびその他の属性があります。ほとんどのサービスクラスはデフォルトポリシーに設定されていますが、優先度の高いトラフィックには優先度の高いトラフィックシェーピングポリシーを割り当て、優先度の低いトラフィックには優先度の低いポリシーを割り当てることができます。
8. [フィルタールール] セクションで、[追加] をクリックして、すべてのパラメーターのデフォルト値として [任意] を持つフィルタールールを作成します。特定の接続に対してルールが TRUE と評価された場合、その接続はそのサービスクラスに割り当てられます。ほとんどのサービスクラスのフィルタルールは、アプリケーショ

ンのリストのみで構成されていますが、ルールには、IP アドレス、VLAN タグ、DSCP 値、SSL プロファイル名を含めることもできます。ルールのすべてのフィールドのデフォルトは Any（ワイルドカード）です。ルール内のフィールドは AND で結合されます。

9. [追加] をクリックして、フィルタールールを追加します。



10. [アプリケーショングループ] リストから、[電子メールとコラボレーション] を選択します。
11. [利用可能] リストから、必要なアプリケーションを選択します。
12. 選択したアプリケーションを [構成済み] リストに移動します。
13. [送信 元 **IP** アドレス] フィールドに、クライアント IP アドレスを追加します。
14. [方向] リストから、トラフィックの方向を選択します。
15. [**SSL** プロファイル] リストから、作成した SSL プロファイルを選択します。
16. ［作成］をクリックします。

> 注
>
> - データセンター側のアプライアンスでのみ SSL プロファイルを構成してサービスクラスにバインドする必要があります。
> - SSL プロファイルに関連付けることができるのは、フィルタールールの方向が単方向に設定されているサービスクラスのみです。

トラフィックシェーピング

April 19, 2021

2018 年 4 月 18 日

トラフィックシェーピングを使用すると、ネットワークトラフィックフローを調整して、特定のレベルのサービス品質（QoS）を保証できます。ネットワークへのパケットの流れ（帯域幅調整）またはネットワークからのパケットの流れ（レート制限）を調整できます。

トラフィックシェーピングポリシーを使用すると、さまざまなリンクトラフィックの優先度を設定し、リンク速度に近いがそれ以下の速度でトラフィックをリンクに送信できます。にのみ適用される加速とは異なり TCP/IP トラフィック、トラフィックシェーパーは、リンク上のすべてのトラフィックを処理します。

残りのトラフィックフローよりも重要と見なされるトラフィックフローに高帯域幅を設定して、不足しているリンクリソースを最適に使用できるようにします。

トラフィックシェーピングは、重み付き公平キューイングに基づいており、各サービスクラスにリンク帯域幅の公平なシェアを提供します。リンクがアイドル状態の場合、（任意のサービスクラスの）すべての接続でリンク全体を使用できます。複数の接続がリンク帯域幅をめぐって競合している場合、トラフィックシェーパーはトラフィックシェーピングポリシーを適用して、トラフィックの適切な組み合わせを決定します。

重み付き公平キューイングの詳細については、重み付き公平キューイングを参照してください。

トラフィックシェーピングを設定するには：

1. リンク定義を構成します。

   リンク定義は、トラフィックシェーパーによって、送受信リンク速度およびその他のリンク関連情報を決定するために使用されます。トラフィックシェーパーがリンク定義を使用する方法とリンク定義を構成する方法の詳細については、リンクの定義を参照してください。

2. アプリケーション定義を構成します。

   リンクを流れるトラフィックは、アプリケーション分類子によって調べられて、どのアプリケーションに属しているかが判別されます。次に、アプリケーションがサービスクラスリストで検索され、どのサービスクラスに属しているかが判別されます。アプリケーション分類とアプリケーション定義の構成方法の詳細については、トラフィックの分類を参照してください。

3. トラフィックシェーピングポリシーを作成します。

   デフォルトのトラフィックシェーピングポリシーを使用するか、新しいポリシーを作成して、ネットワーク要件に従って加重優先度およびその他のパラメータを設定できます。トラフィックシェーピングポリシーの作成については、トラフィックシェーピングポリシーを参照してください。

4. サービスクラス定義を設定し、トラフィックシェーピングポリシーをサービスクラスに関連付けます。

   IPSec サービスの設定については、「サービスクラス」を参照してください。

トラフィックシェーパーのいくつかのハイライト：

- すべての WAN トラフィックは、トラフィックシェーピングの対象になります。つまり、高速接続、非高速接続、および UDP フローや GRE ストリームなどの非 TCP トラフィックです。
- アルゴリズムは重み付き公平キューイングであり、管理者は各サービスクラスに優先順位を割り当てます。各サービスクラスは、(my_priority/sum_of_all_priorities) と同等のリンク速度の最小部分が与えられた帯域幅プールを表します。加重優先度が 100 のサービスクラスは、加重優先度が 50 のサービスクラスの 2 倍の帯域幅を取得します。1 から 256 までの重みを割り当てることができます。
- サービスクラス内の各接続は、そのサービスクラスに割り当てられた帯域幅の等しいシェアを取得します。
- 圧縮後に転送される実際の WAN データに優先順位が適用されるため、各接続はリンク帯域幅の公平なシェアを取得します。たとえば、同じ優先度の 2 つのデータストリームがある場合、1 つは 10:1 圧縮およびその他の達成 2:1 圧縮、ユーザーには 5:1 2 つの接続の WAN リンクの使用法は同じですが、スループットの違いがあります。実際には、アプリケーションの帯域幅ではなく WAN 帯域幅が管理する必要のあるリソースが不足しているため、この不一致は望ましいものです。
- トラフィックシェーピングポリシーは、加速トラフィックと非加速トラフィックの両方に等しく適用されます。たとえば、高速 Virtual Apps 接続と高速化されていない Virtual Apps 接続は、どちらもトラフィックシェーピングを受信するため、バルクトラフィックと比較して両方の優先順位が高くなります。別の例として、VoIP（UDP プロトコルを使用）などの時間に敏感な非 TCP トラフィックを促進できます。
- トラフィックシェーピングは、加速トラフィックと非加速トラフィックの両方に対して、送信方向と受信方向の両方で WAN リンクに適用されます。この機能は、リンクの反対側に Citrix SD-WAN WANOP アプライアンスが装備されていない場合でも、輻輳と遅延の増加を防ぎます。たとえば、インターネットのダウンロードに優先順位を付けて管理することができます。
- サービスクラスのトラフィックシェーピングポリシーは、必要に応じてリンクごとに指定できます。
- トラフィックシェーパーは、トラフィックを直接シェーピングするだけでなく、Differentiated Services Code Point（DSCP）フィールドを設定して、各パケットが必要とするトラフィックシェーピングのタイプについてダウンストリームルーターに通知することにより、トラフィックに間接的に影響を与えることができます。

重み付き公平キューイング

April 19, 2021

どのリンクでも、ボトルネック以外のゲートウェイのデータはバックアップされないため、ボトルネックのゲートウェイがキューイングの規律を決定します。キューに保留中のデータがない場合、キューイングプロトコルは関係ありません。

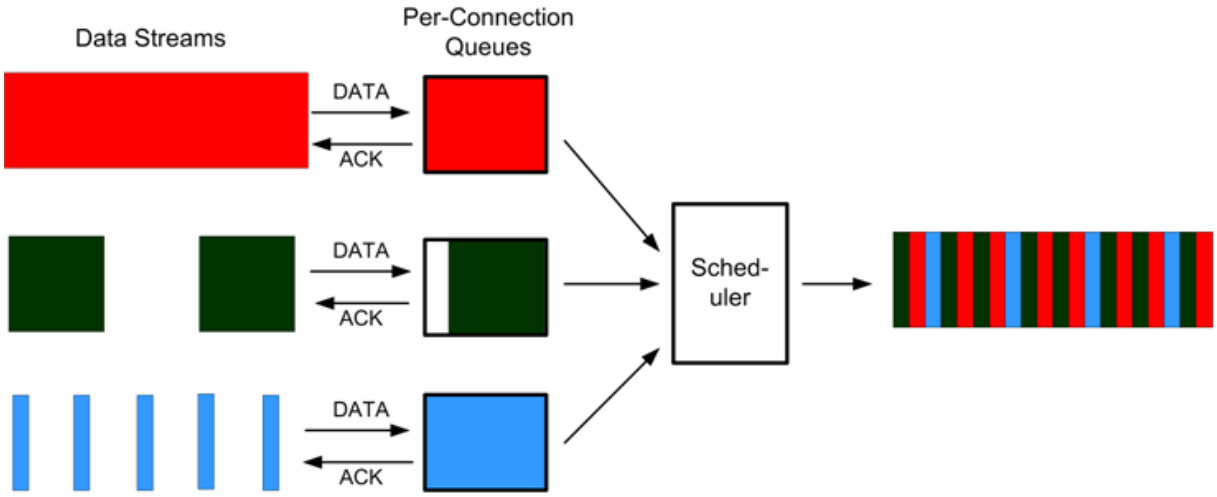
ほとんどの IP ネットワークはディープ FIFO キューを使用します。トラフィックがボトルネック速度よりも速く到着すると、キューがいっぱいになり、すべてのパケットのキューイング時間が長くなります。トラフィックが別々の FIFO を持ついくつかの異なるクラスに分割されることがありますが、問題は残ります。単一の接続が送信するデータが多すぎると、そのクラスの他のすべての接続で大きな遅延、パケット損失、またはその両方が発生する可能性があります。

Citrix SD-WAN WANOP アプライアンスは、重み付き公平キューイングを 使用します。これにより、接続ごとに個別のキューが提供されます。均等化キューイングでは、接続が速すぎると、それ自体のキューのみがオーバーフローする可能性があります。他の接続には影響しません。ただし、ロスレスフロー制御により、接続が速すぎるなどの問題はなく、キューはオーバーフローしません。

その結果、各接続のトラフィックが公平にリンクに計測され、リンク全体で最適な帯域幅と遅延プロファイルが得られます。

次の図は、均等化キューイングの効果を示しています。必要な帯域幅の公平なシェアよりも少ない接続（下部の接続）は、使用しようとするのと同じ量の帯域幅を取得します。さらに、キューイングの待ち時間はほとんどありません。フェアシェアを超えて使用しようとする接続は、フェアシェアに加えて、フェアシェア未満を使用する接続から残った帯域幅を取得します。

図 1：均等化キューイングの実施



最適な遅延プロファイルは、インタラクティブなトランザクションアプリケーションのユーザーに、複数の一括転送でリンクを共有している場合でも、理想的なパフォーマンスを提供します。ロスレスで透過的なフロー制御と均等化キューイングの組み合わせにより、同じリンク上のすべての種類のトラフィックを安全かつ透過的に組み合わせることができます。

重み付き公平キューイングと非重み付き公平キューイングの違いは、重み付き公平キューイングには、一部のトラフィックに他のトラフィックよりも高い優先度（重み）を与えるオプションが含まれていることです。重みが 2 のトラフィックは、重みが 1 のトラフィックの 2 倍の帯域幅を受信します。Citrix SD-WAN WANOP 構成では、重みはトラフィックシェーピングポリシーで割り当てられます。

トラフィックシェーピングポリシー

April 19, 2021

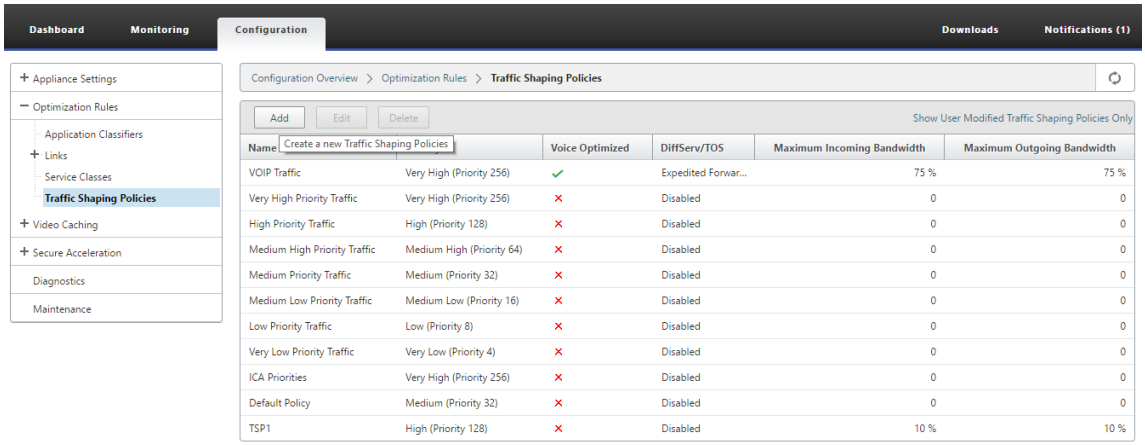
すべてのサービスクラス定義は、関連付けられたサービスクラスのトラフィックのパラメータを設定するトラフィックシェーピングポリシーに関連付けられています。特別なニーズのあるサイトのトラフィックシェーピングポリシーを作成および構成できますが、デフォルトのポリシー設定はほとんどのインストールで正常に機能し、次の利点があります。

- Citrix Virtual Apps and Desktops などの対話型トラフィックの応答性が向上。
- 遅延およびジッターに敏感な VoIP トラフィックの保護。
- ピーク時に「壁にぶつかる」ことはありません。極端な負荷でも使用可能なパフォーマンスが得られます。
- バルク転送でインタラクティブタスクから残った帯域幅でリンクを埋めることができるため、帯域幅の使用率が向上します。
- 均等化キューイングのメリットをすべてのトラフィックに拡張

Citrix SD-WAN WANOP アプライアンスには、さまざまな優先順位にまたがる工場出荷時のデフォルトのトラフィックシェーピングポリシーが付属しています。これらのポリシーは、[トラフィックシェーピングポリシー] ページに一覧表示されています。デフォルトポリシーとは別に、他の工場出荷時のデフォルトポリシーは編集または削除できません。その理由は、それらがすべてのアプライアンスで同じ意味を持つようにするためです。変更を加えるには、新しいパラメータを使用して新しいトラフィックシェーピングポリシーを作成し、適切なサービスクラス定義を変更して、新しいトラフィックシェーピングポリシーを参照します。

トラフィックシェーピングポリシーを作成するには:

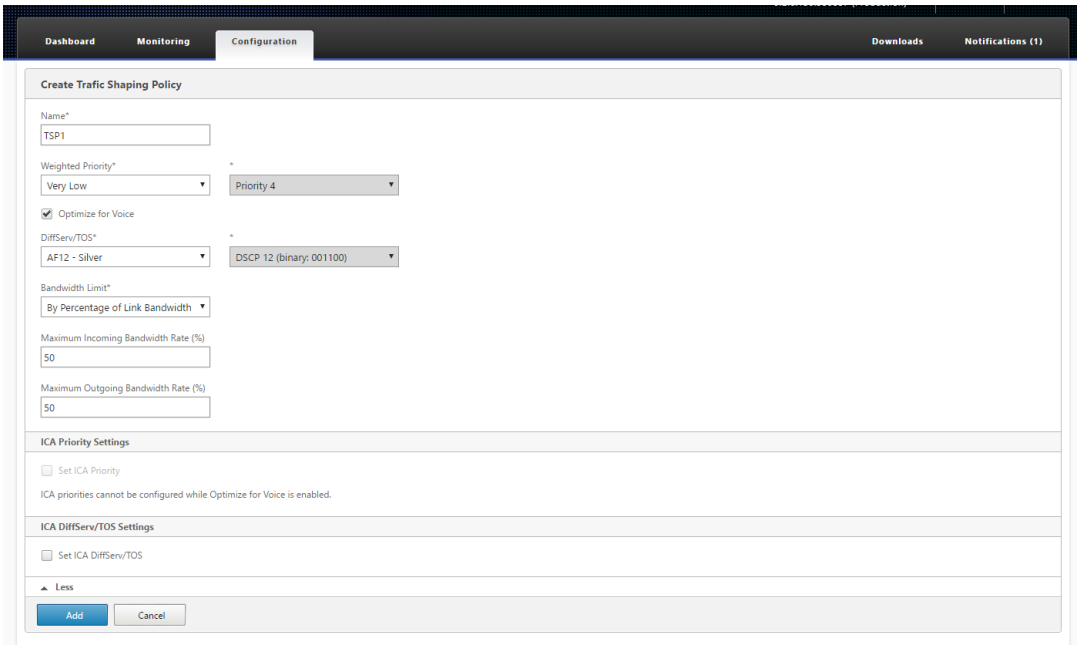
1. SD-WAN WANOP 管理 UI で、[構成]> 最適化ルール > トラフィックシェーピングポリシー をクリックし、[追加] をクリックします。



2. [トラフィックシェーピングポリシー の作成] ページで、次のパラメータの値を入力します。

- 名前—新しいポリシーの名前。一意である必要があります。
- 加重優先度—既存の優先度値を選択することも、1～256 のカスタム値を選択することもできます。優先度 256 の接続は、優先度 1 の接続の 256 倍の帯域幅シェアを取得します。
- 音声用に最適化—選択した場合、このポリシーの優先度は事実上無限になります。これは、意味のあるトラフィックシェーピングを妨げ、リンクを満たすのに十分な「音声用に最適化された」トラフィックがある場合に他のトラフィックのデータ不足を引き起こすため、ほとんどのトラフィックにとって非常に望ましくありません。VoIP にのみ使用し、常にポリシーの帯域幅制限（たとえば、リンク速度の 50%）と組み合わせて使用します。

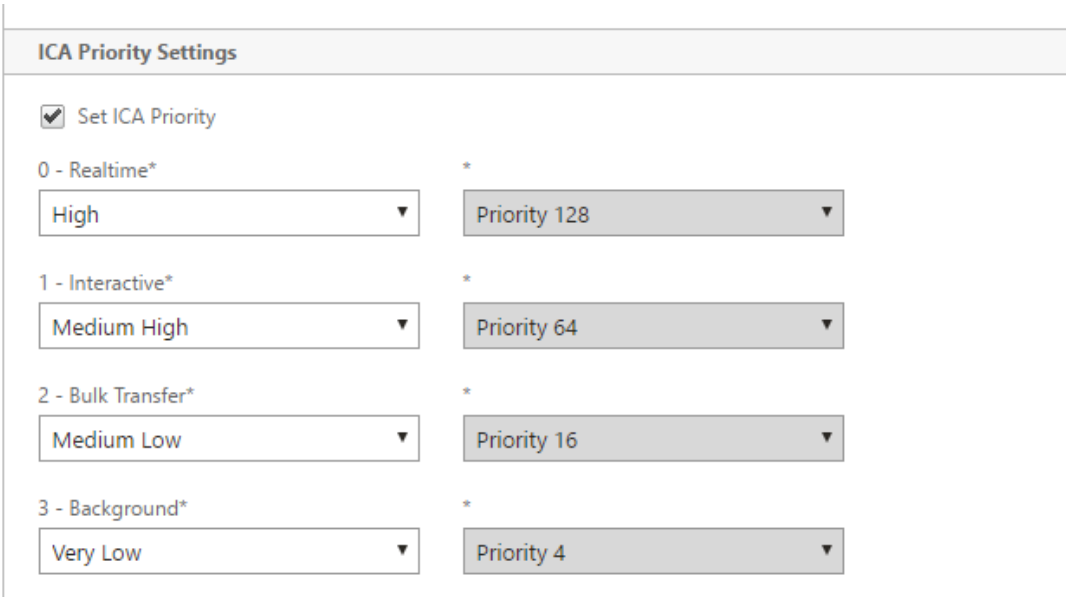
> 注
>
> ICA 優先順位が設定されている間は、音声最適化を設定できません。



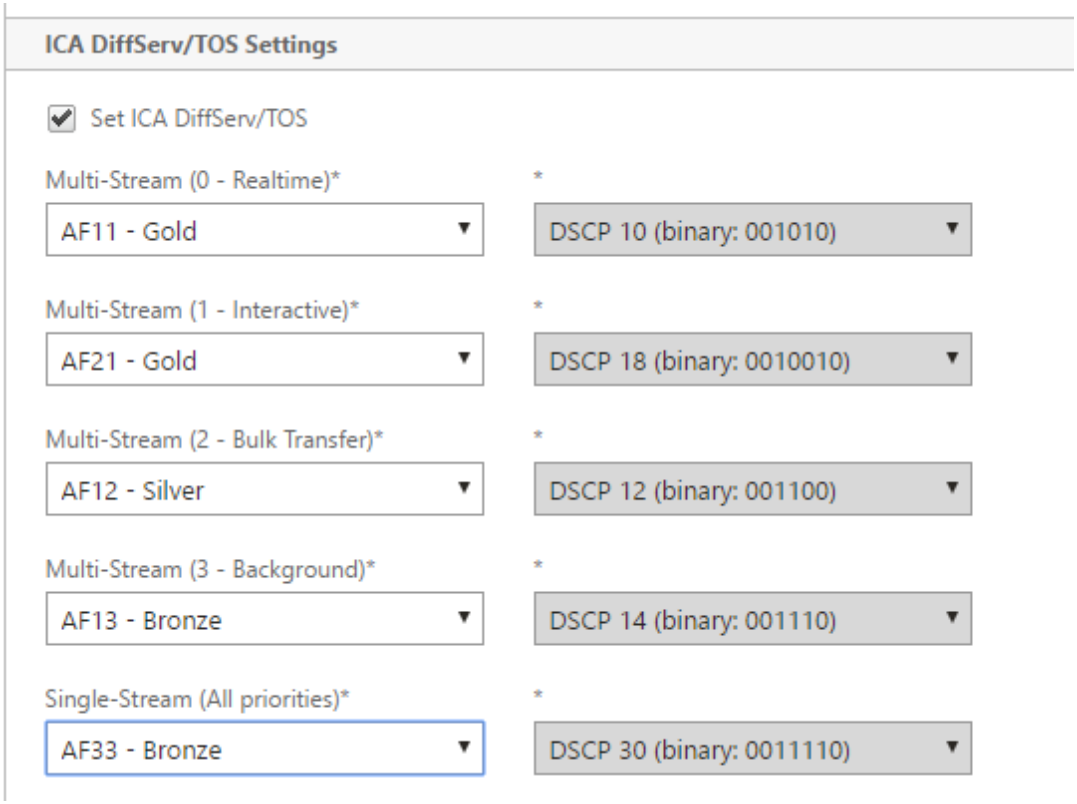
- **Diffserv/TOS** -出力パケットの DSCP ビットを選択した値に設定します。ダウンストリームルーターの制御に使用されます。
- 帯域幅制限：このポリシーを使用するトラフィックが、リンク速度のパーセンテージまたは絶対値として指定された帯域幅を超えないようにします。同じ定義を異なる速度のリンクに適用できるように、パーセンテージを指定することをお勧めします。この機能により、帯域幅が未使用のままになる可能性があります。たとえば、リンク速度の 50%に設定されたポリシーでは、リンクがアイドル状態であっても、影響を受けるトラフィックがリンクの 50%を超えて使用することは許可されません。この方法でトラフィックをスロットリングすると最大パフォーマンスと矛盾するため、[音声用に最適化] 設定の VoIP トラフィックを除いて、この機能が使用されることはめったにありません。

> 注
>
> 帯域幅制限の 構成は、Citrix SD-WAN WANOP エディションにのみ適用されます。Citrix SD-WAN PE エディションの場合、帯域幅制限 パラメーターはデフォルトで無効になっています。

- **ICA** 優先度の設定—このポリシーを Citrix Virtual Apps/Virtual Desktops のトラフィックに使用すると、リアルタイム、インタラクティブ、一括転送、バックグラウンドトラフィックに対するトラフィックの内部優先度は、ここで設定した優先度によって上書きされます。



- **ICA diffServ/TOS** の設定：ICA（Virtual Apps/Virtual Desktops）トラフィックの場合、4 つの ICA プライオリティ値のそれぞれに異なる DSCP 値でタグを付けることができます。この機能は、Virtual Apps または Virtual Desktops クライアントが異なる優先度レベルで異なる接続を使用する新しいマルチストリーム ICA 機能で特に便利です。



3. ［追加］をクリックします。新しく作成されたトラフィックシェーピングポリシーが［トラフィックシェーピングポリシー］リストに表示されます。

   トラフィックシェーピングポリシーをサービスクラスに関連付けることができるようになりました。詳細については、サービスクラスを参照してください。

ビデオキャッシング

April 19, 2021

多くの組織は、時間に敏感ではないコミュニケーションにビデオを使用しています（たとえば、トレーニングセッションや従業員への事前に録音されたメッセージ）。ビデオを介したメッセージの伝達は、費用効果が高いだけでなく、視聴者がタイムゾーンに分散している場合にも便利です。ただし、ビデオをインターネット経由で再生すると、多くの帯域幅が消費されます。帯域幅が不十分な場合、遅延が発生し、ユーザーエクスペリエンスに影響を与え、ビデオ通信の影響を低下させます。

ビデオキャッシングは、特に低速リンクでの HTTP ビデオストリームの表示エクスペリエンスを向上させます。ビデオキャッシュは、ローカルの Citrix SD-WAN WANOP アプライアンスで維持されます。ローカルユーザーがすでにキャッシュされているビデオを表示すると、アプライアンスはキャッシュされたコピーをフル LAN 速度で配信できます。

ビデオをキャッシュするようにアプライアンスを構成すると、ユーザーが表示したビデオがキャッシュされます。事前入力オプションを使用して、後で使用することを見越して、ローカルビデオサーバーから選択したビデオをフェッチすることもできます。

ビデオキャッシング機能は、インターセプトプロキシキャッシュを使用してすべての HTTP リクエストを調べます。以下の要件を満たすリクエストはキャッシュされます。ビデオは、キャッシュエンジンによって新鮮であると評価されない限り、キャッシュから提供されません。それ以外の場合は、ビューア用に再度フェッチされ、以前にキャッシュされたバージョンが上書きされます。

最新のコンテンツを保証します。ビデオが表示されるたびに、キャッシュはオリジンサーバーをチェックし、ビデオが変更された場合、キャッシュされたコンテンツは破棄され、新しいコンテンツがダウンロードされます。

> 注
>
> キャッシングが透過的になりました。つまり、クライアントとサーバーの両方の IP アドレスがエンドツーエンドで維持されます。以前のリリースでは、Citrix SD-WAN WANOP アプライアンスの IP アドレスが送信元アドレスとして表示されていました。

次のすべての基準が満たされると、ビデオがキャッシュされます。

- ビデオのストリーミングに使用されるプロトコルは HTTP です。デフォルトでは、ポート 80 はビデオキャッシング用に構成されています。ただし、Web サーバー用に 8080 などの別のポートを構成している場合は、ビデオをキャッシュするためにこのポートを指定する必要があります。
- ビデオをキャッシュするビデオソースを追加しました。デフォルトでは、YouTube、Vimeo、Youku、Dailymotion、Metacafe のビデオソースがアプライアンスに追加されますが、有効になっているのは YouTube と Vimeo のみです。他のデフォルトソースのいずれかからビデオをキャッシュする場合は、それらを有効にする必要があります。新しいビデオソースを追加するときは、追加するときにそれらを有効にすることができます。
- YouTube、Vimeo、Metacafe、Dailymotion、Youku の他に、追加の Web サイト、IP アドレス、またはサブネットをビデオソースとして指定できます。これらの Web サイトには、URL にランダムな文字を追加するなどの回避メカニズムを含めるべきではないことに注意してください。
- ビデオは、認識されているビデオ形式のいずれかであり、次のファイル拡張子のいずれかである必要があります：.3gp、.avi、.dat、.divx、.dvx、.dv-avi、.flv、.fmv、.h264、.hdmov、.m15、.m1v、.m21、.m2a、.m2v、.m4e .m4v、.m75、.moov、.mov、.movie、.mp21、mp2v、.mp4、.mp4v、.mpe、。mpeg、mpeg4、mpg、mpg2、.mpv、.mts、.ogg、.ogv、.qt、.qtm、.ra、.rm、.ram、.rmd、.rms、rmvb、.rp、rv、.swf 、.ts、.vfw、.vob、.webm、.wm、.wma、.wmv、および.wtv。

サポートされているプラットフォーム

ビデオキャッシュ機能は、次のアプライアンスでサポートされています。

- 1Mbps および 2Mbps 帯域幅ライセンスモデルを備えた SD-WAN WANOP600 アプライアンス。

- すべての帯域幅ライセンスモデルを備えた SD-WAN WANOP 800 アプライアンス。
- すべての帯域幅ライセンスモデルを備えた、Windows Server を備えた SD-WAN WANOP1000 アプライアンス。
- すべての帯域幅ライセンスモデルを備えた SD-WAN WANOP 2000 アプライアンス。
- すべての帯域幅ライセンスモデルを備えた、Windows Server を備えた SD-WAN WANOP 2000 アプライアンス。
- すべての帯域幅ライセンスモデルを備えた SD-WAN WANOP 3000 アプライアンス。
- Amazon 向け SD-WAN WANOP VPX および SD-WAN WANOP VPX

サポートされているビデオサーバー

ビデオキャッシュ機能は、Adobe Flash Media Server 4.5 以降でサポートされています。さらに、静的リンクとして HTTP 経由でビデオを提供するビデオサーバーは、ビデオキャッシュでサポートされています。

サポートされている展開モード

ビデオキャッシングは、インライン、VLAN トランクポート内のインライン、仮想インライン、および WCCP 展開モードでサポートされます。

ビデオキャッシュ機能の使用に関する考慮事項

以下は、ビデオキャッシュ機能を使用する際に注意すべきいくつかのポイントです。

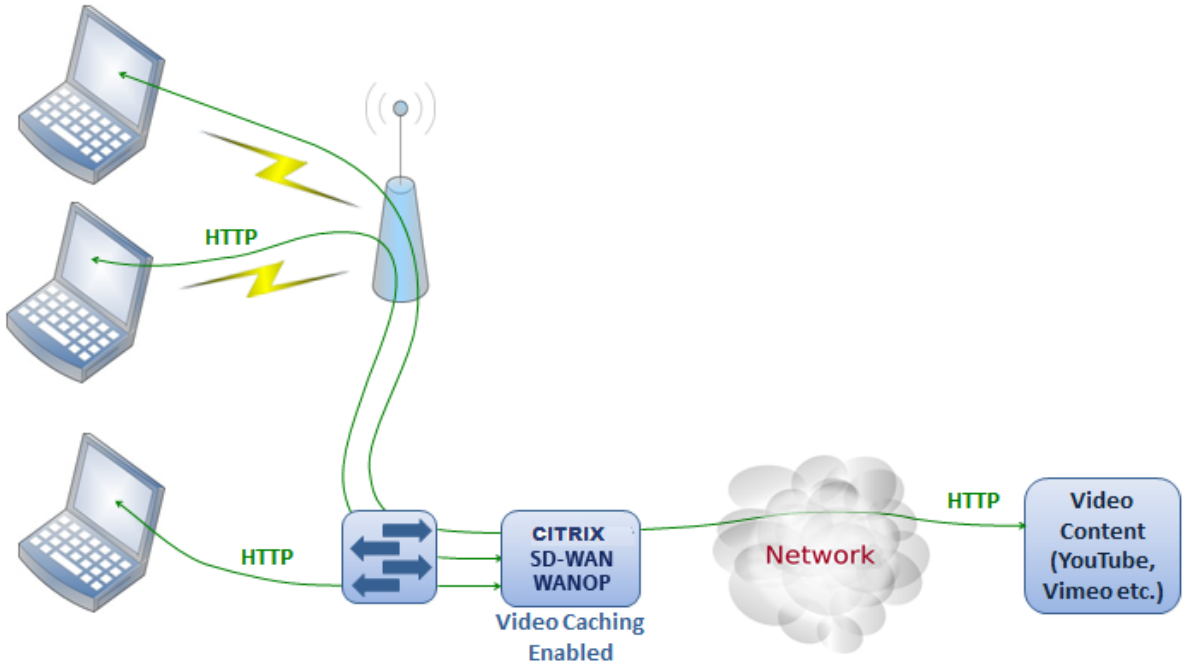
- サポートされている Web サイトのいずれかがコンテンツの表示方法を変更した場合、それらのサイトのビデオキャッシュの利点は、ビデオキャッシュポリシーファイルが更新されるまで達成されない可能性があります。このような不定期の変更に対して、Citrix は更新されたビデオキャッシュポリシーファイルを提供します。これを使用するには、ビデオキャッシュポリシーファイルのアップグレードを参照してください。
- 一部のビデオ Web サイトは、ビデオへのアクセスに使用されるオペレーティングシステムまたはブラウザに応じて、同じビデオに対して異なるファイル形式を使用する場合があります。これにより、キャッシュミスが発生する可能性があります。
- YouTube などの一部のビデオ Web サイトは、ネットワークの状態に適応します。したがって、ビデオの品質は、キャッシュされたときのネットワークの状態に依存する可能性があります。

ビデオキャッシングシナリオ

April 19, 2021

次のシナリオでは、Citrix SD-WAN WANOP アプライアンスにビデオキャッシュを展開できます。

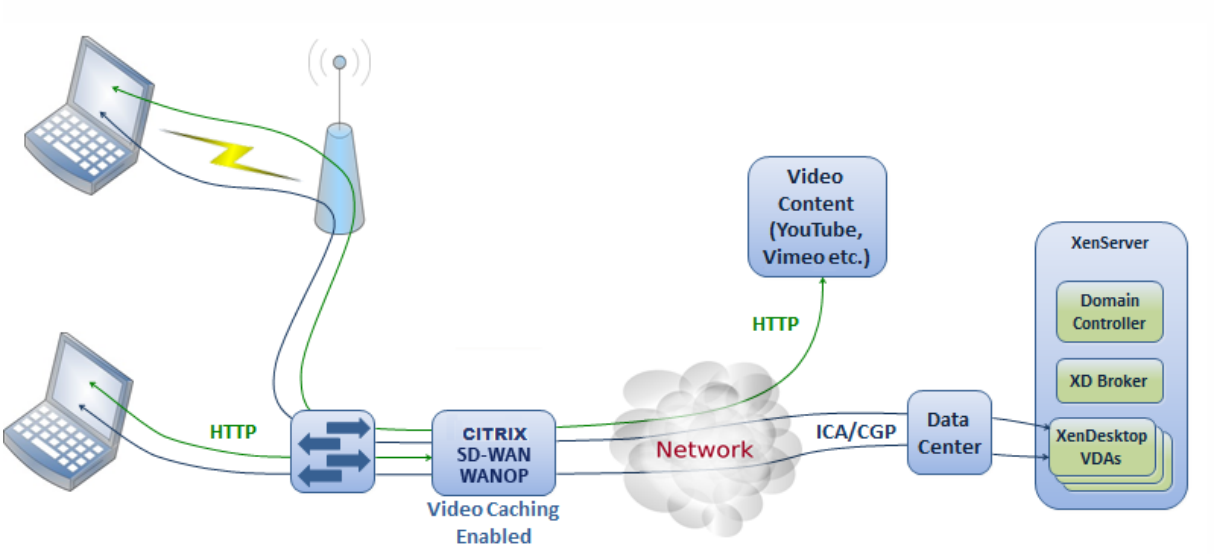
ブランチオフィスへのアクセス



この使用例では、ユーザーは自分のコンピューターの Web ブラウザーを介してインターネットにアクセスします。Vimeo などの有効なサイトからのビデオコンテンツを含むこれらのリクエストは、ローカルの Citrix SD-WAN WANOP アプライアンスにキャッシュされます。その後、同じビデオにアクセスすると、ローカルアプライアンスでキャッシュヒットが発生し、リモートサーバーを待たずに LAN 速度でビデオを配信できるようになります。

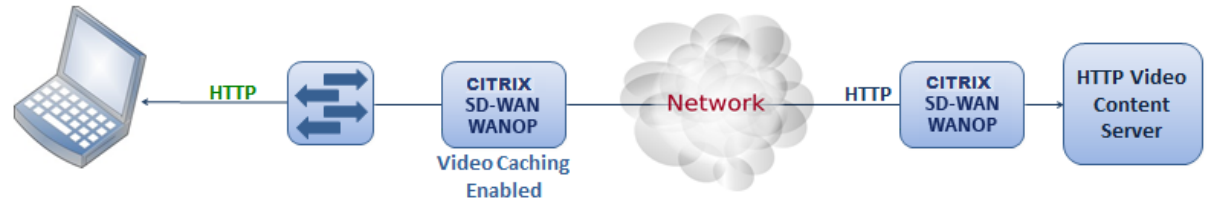
ペアリングされたデバイス間のトラフィックを高速化する他の Citrix SD-WAN WANOP 機能とは異なり、この機能は、ビデオ Web サイトにアクセスできるローカルアプライアンスのみを必要とするシングルエンド操作です。

HDX MediaStream フラッシュリダイレクトを使用した **Citrix Virtual Apps and Desktops** ユーザーのブランチオフィス



HDX フラッシュリダイレクトは、Citrix Virtual Apps and Desktops の機能です。サーバー側またはデータセンターのインターネットを使用して、リモート Virtual Desktops ディスプレイにビデオをレンダリングする代わりに、この機能を使用してローカルシステムにフラッシュビデオがトンネリングされます。ビデオは実際のクライアントマシンにストリーミングされ、ブランチオフィスのインターネットを使用して実際のクライアントでレンダリングされます。ブランチサイドの Citrix SD-WAN WANOP アプライアンスでビデオキャッシュ機能を有効にすると、ユーザーの視聴体験が大幅に向上します。さらに、この機能を有効にすると、ストリーミングビデオの帯域幅要件が軽減されます。

エンタープライズ **HTTP** ビデオ **Web** サーバー



このユースケースでは、ユーザーはデータセンターからビデオ Web サーバーにアクセスします。ブランチ側の Citrix SD-WAN WANOP アプライアンスでビデオキャッシュ機能を有効にすると、ユーザー要求はブランチ側の Citrix SD-WAN WANOP アプライアンスのキャッシュから処理されます。これにより、データセンターの Citrix SD-WAN WANOP アプライアンスへのネットワークトラフィックを削減できます。その結果、データセンターの Citrix SD-WAN WANOP アプライアンスの帯域幅を使用して、他のブランチのトラフィックを処理できます。

ビデオキャッシュを構成する

April 19, 2021

ビデオキャッシュ機能は、Citrix SD-WAN WANOP グラフィカルユーザーインターフェイスまたはコマンドラインインターフェイスのいずれかを介して構成できます。デフォルトでは、アプライアンスは YouTube と Vimeo からのビデオをキャッシュするように構成されています。Youku、Metacafe、Dailymotion もデフォルトでアプライアンスに設定されています。あなたがしなければならないのはそれらを有効にすることです。ビデオチュートリアルやその他の情報を提供する内部 Web サイトなどのビデオ Web サイトを追加できます。

> 注
>
> デフォルトで有効になっていないオプション機能のビデオキャッシュ。大量の HTTP ビデオトラフィックがない限り、有効にする必要はありません。

前提条件

アプライアンスでビデオキャッシングを構成するには、次の前提条件が満たされていることを確認してください。

- ビデオキャッシングに使用する予定のアクセラレーションブリッジポートに適切な IP アドレスを設定しました。
- あなたは ping することができます apA/apB アプライアンスからのゲートウェイ。
- DNS サーバーの詳細は正確です。
- アプライアンスは DNS 名 www.Citrix.com を解決できます。
- Citrix SD-WAN WANOP apX IP アドレスは、企業ネットワークで HTTP アクセスが可能です。
- アプライアンスが 2 つのネットワークデバイスのトランクポート間に展開されている場合は、[ネットワーク構成] ページでアプライアンスが HTTP 要求を送信するために使用する IP アドレスとともに VLAN ID を指定する必要があります。
- **Web**（インターネット）および **Web**（プライベート）サービスクラスの場合、**AccelerationPolicy** 設定を **None** に設定しないでください。

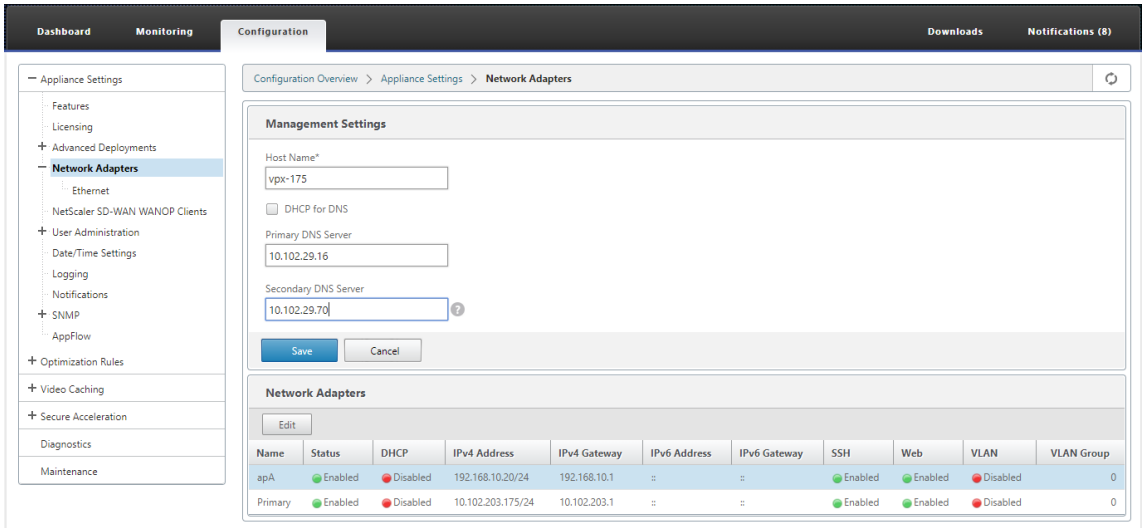
ビデオキャッシュ機能を有効にする

ビデオキャッシュ機能の使用を開始する前に、それを有効にする必要があります。

ビデオキャッシュを有効にするには:

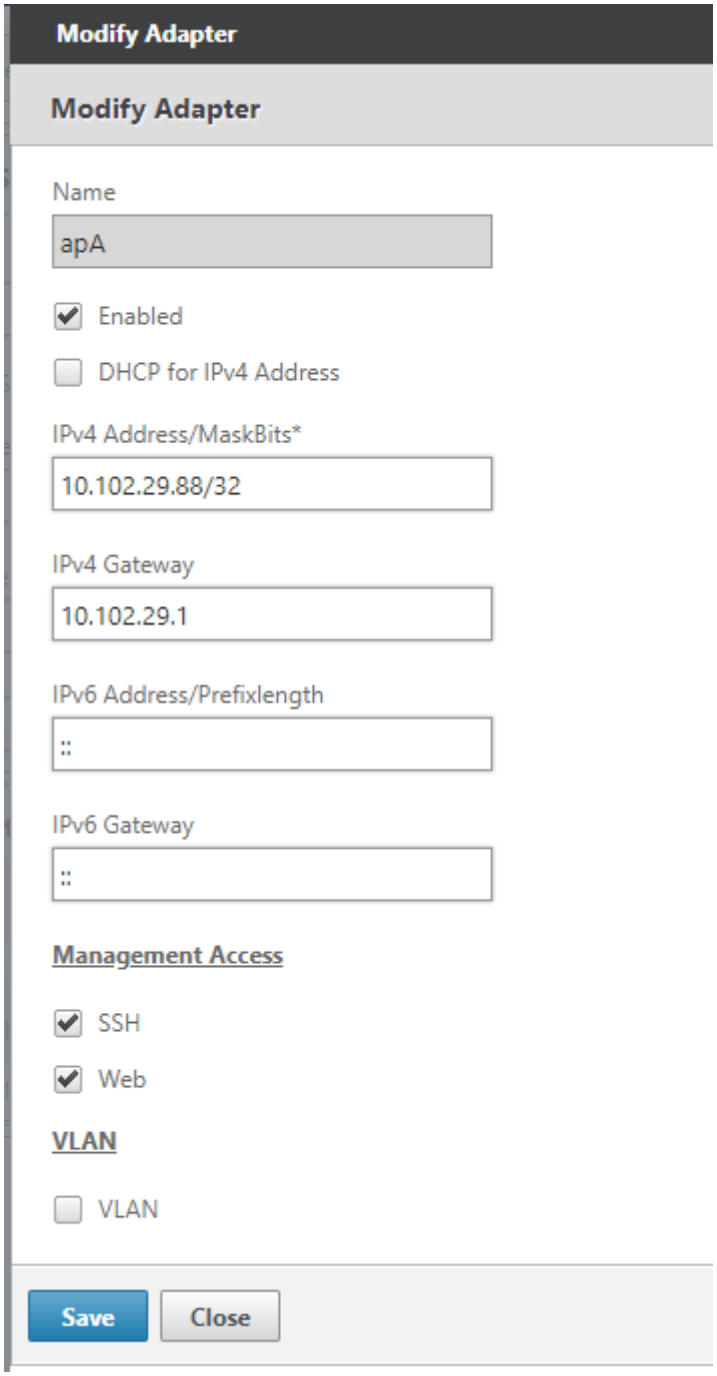
1. 構成 >
   アプライアンスの設定 > ネットワークアダプタの **[管理設定]** セクションで、プライマリ DNS サーバーの詳細

が正確であり、アプライアンスが DNS 名 www.Citrix.com を解決できることを確認および確認します。設定を変更するには、編集アイコンをクリックします。



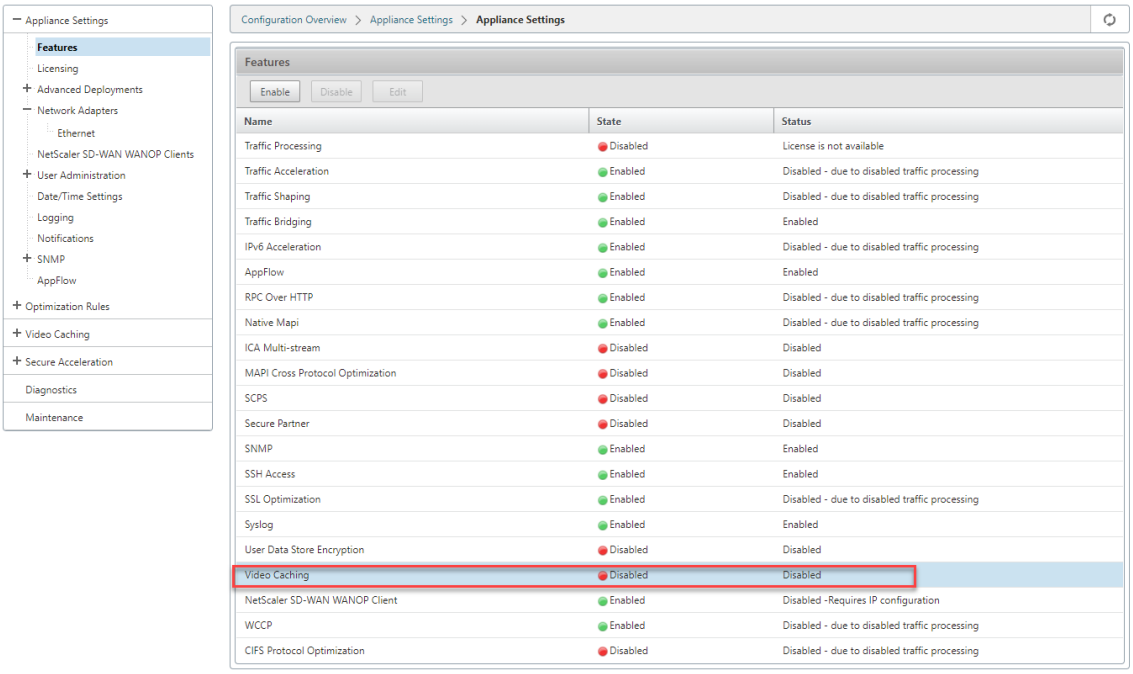
2. 構成 > アプライアンスの設定 > ネットワークアダプタに移動します。[ネットワークアダプター] セクションで、アクセラレーションペア（apA など）を選択し、[編集] をクリックします。

   アクセラレーションペアに指定された IP アドレス、ネットワークマスク、およびデフォルトゲートウェイの IP アドレスが正確であることを確認してください。



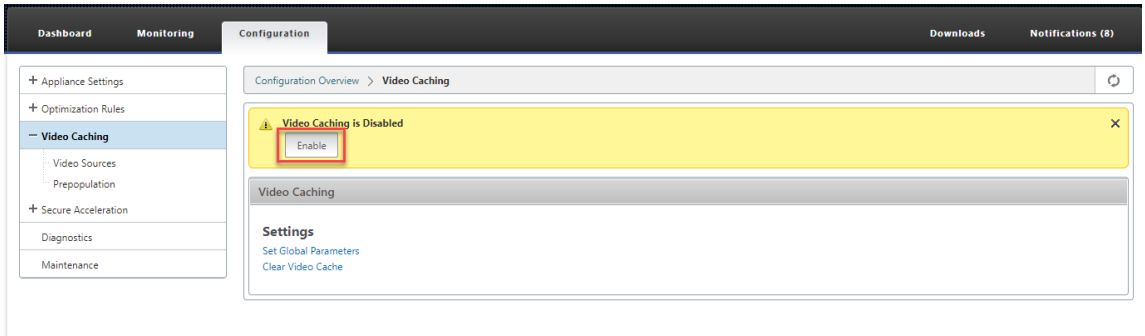
3. 構成に移動します > アプライアンスの設定 > 機能 ページを開き、ビデオキャッシュ 機能を有効にします。

   確認ダイアログボックスが表示されたら、[はい] をクリックします。



> 注
>
> サービスが再起動し、新しいキャッシュパーティションが作成されます。アプライアンスでこの機能を初めて有効にする場合は、他のディスクベースの圧縮に割り当てられるディスク領域を減らすことにより、新しいパーティションが作成されます。ディスクベースの圧縮履歴がリセットされ、既存の接続が終了します。

4. または、[構成]> 最適化ルール > ビデオキャッシング をクリックし、[有効にする] をクリックします。



ビデオウェブサイトを追加する

アプライアンスは、YouTube と Vimeo からのビデオをキャッシュするように構成されており、Youku、Metacafe、Dailymotion からのビデオをキャッシュするように部分的に構成されています。後者の 3 つのサイトのいずれかからビデオをキャッシュするには、サイトを有効にする必要があります。有効になっている Web サイトのビデオは、ユーザーがアクセスするとすぐにキャッシュされます。アプライアンスのビデオソースリストにホスト名または IP ア

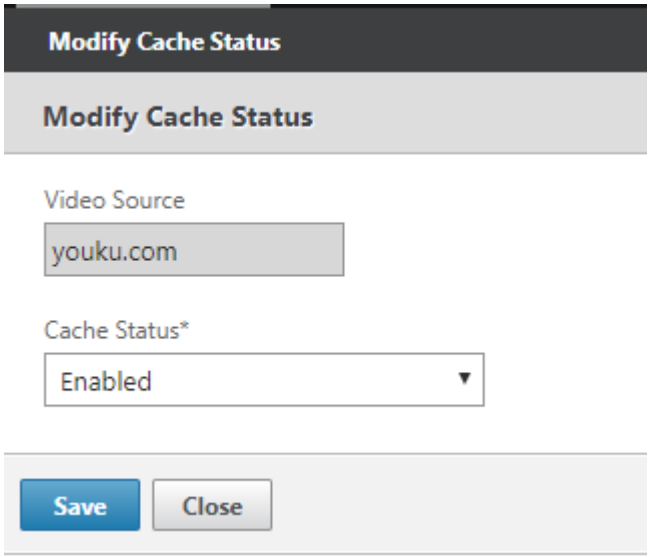
ドレスを追加することにより、URL の書き換えを必要としない追加のビデオ Web サイトを構成できます。キャッシュ回避メカニズムを持たないカスタムサイトを含めることもできます。

アプライアンスがこれらのビデオソースからビデオをキャッシュする前に、これらのビデオソースを有効にする必要があります。

ビデオキャッシュ機能は、構成ワークフローにビデオソースを使用します。ビデオソースのいずれかをホスト名または website/hostname, アプライアンスは、アプライアンスを通過するすべての HTTP トラフィックをプロキシします。ただし、すべてのビデオソースを IP アドレスのみで構成すると、アプライアンスはこれらの IP アドレスのみをプロキシしてキャッシュします。ホスト名または IP アドレスのどちらを使用するかに関係なく、組織が YouTube、Vimeo、Dailymotion、Metacafe、および Youku の Web サイトへのアクセスを許可していない場合は、これらのビデオソースを必ず無効にしてください。

ビデオソースを有効にするには:

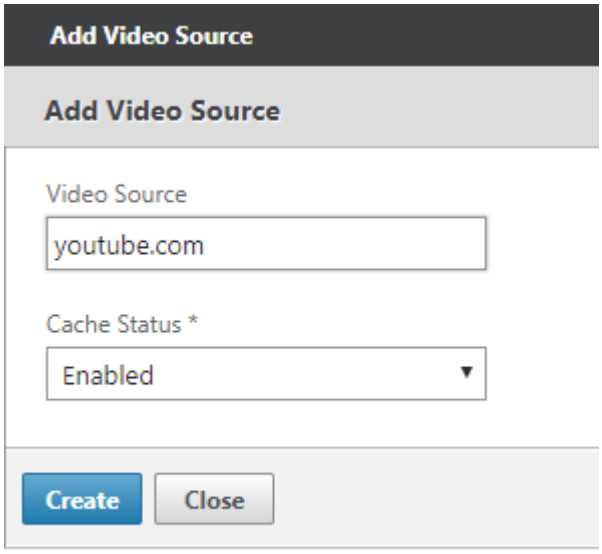
1. 構成 > 最適化ルール > ビデオキャッシング > ビデオソースに移動。
2. リストからビデオソースを選択し、[変更] をクリックします。



3. [キャッシュステータス] ドロップダウンボックスで、[有効 にする] を選択し、[保存] をクリックします。

ビデオソースを追加するには:

1. 構成 > 最適化ルール > ビデオキャッシング > ビデオソースをクリックし、[追加] をクリックします。
2. [ビデオソース] フィールドに、ビデオソースリストに追加する Web サーバーの Web サイト名または IP アドレスを入力します。
3. [キャッシュステータス] リストで、[有効] が選択されていることを確認します。後でこのサイトのビデオキャッシュを有効にする場合は、このリストから [無効] を選択できます。



4. ［作成］をクリックします。

   ビデオソースを削除するには、[ビデオソース] リストからビデオソースを選択し、[削除] をクリックします。

ビデオの事前入力

April 19, 2021

Citrix SD-WAN WANOP アプライアンスは、誰もが見る前に、内部ビデオサーバーからビデオをダウンロードしてキャッシュできます。この機能は、すべてのユーザーが同じメリットを確実に得られるようにする場合（たとえば、特定の時間にスケジュールされたセルフトレーニングビデオを再生する場合）に役立ちます。ビデオをフェッチする静的 URL をスケジュールできます。

フェッチされたビデオはビデオキャッシュに保存されます。ユーザーが URL のリクエストを送信するとすぐに、ビデオへの最初のアクセスであっても、ビデオはキャッシュから提供されます。

事前に動画を取得するには、次のタスクを実行できます:

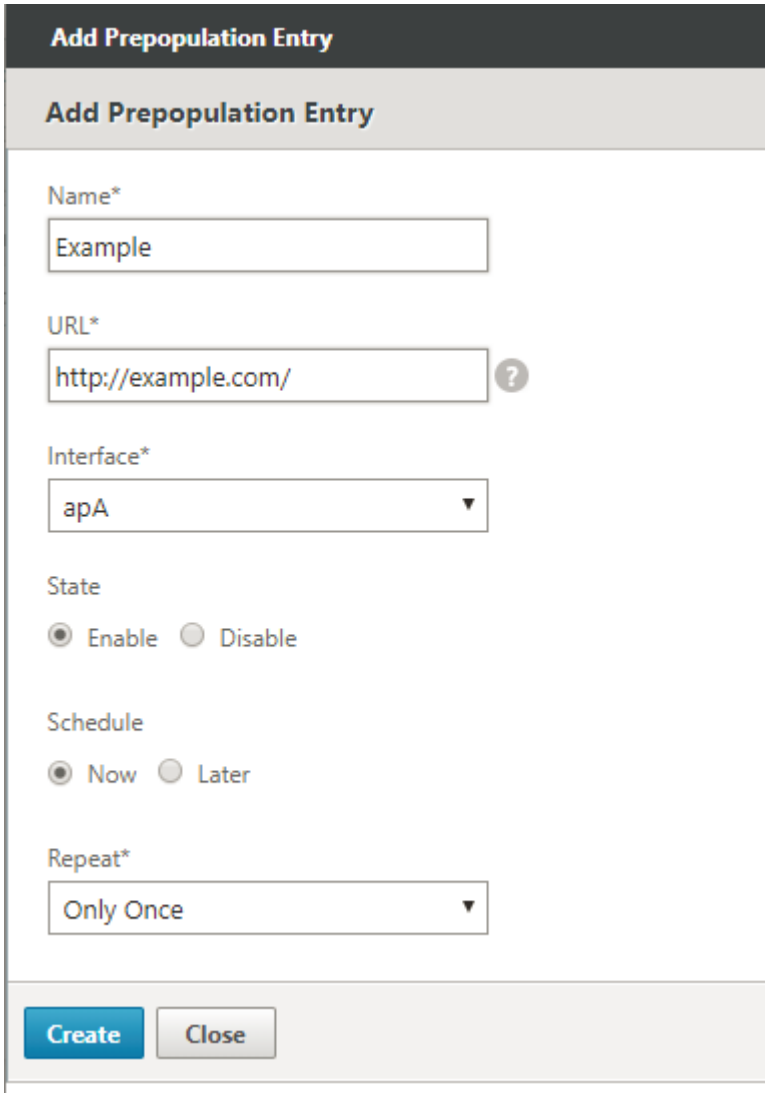
- 動画をキャッシュする URL を事前に指定してください。
- ビデオをキャッシュする日時をスケジュールします。
- ビデオをキャッシュする間隔をスケジュールします。
- リストに追加したエントリを管理します。

ビデオを事前にダウンロードしてキャッシュするには、特定のビデオの URL の絶対パス、またはディレクトリインデックスが有効になっているビデオフォルダを指定する必要があります。

> 注
>
> ビデオの事前入力タスクにエントリを追加するだけで、関連するビデオがダウンロードされてキャッシュされます。ただし、クライアントがビデオにアクセスすると、ビデオサーバーから提供され、キャッシュのメリットは得られません。クライアントがキャッシュのメリットを確実に得られるようにするには、事前入力タスクで使用されるビデオサーバーまたは IP アドレスをビデオソースリストに追加する必要があります。

事前に動画をキャッシュする **URL** を追加するには:

1. 構成 > ビデオキャッシング > 事前入力、[追加] をクリックします。



2. [名前] フィールドで、事前入力エントリを識別するために使用できる名前を指定します。
3. [**URL**] フィールドで、1 つ以上のビデオをキャッシュする URL を指定します。URL は、特定のビデオまたはビデオサーバー用にすることができます。完全な URL またはビデオフォルダを指定してください。
4. [インターフェース] フィールドで、加速ブリッジポートを選択して、URL からビデオをダウンロードします。

5. 設定された 状態 の状態情報を受信するために 有効 にします。さまざまな状態とその説明は、以下の表に示されています。
6. URL からアプライアンスへのビデオのダウンロードとキャッシュをすぐに開始するか、スケジュールされた時間にダウンロードすることができます。
7. ［作成］をクリックします。

   次の表で、ステータスメッセージについて説明します。

ステータス	説明
構成済み	最初のビューが URL に設定され、新しいタスクが追加される前に、キャッシュのためにビデオをフェッチします。
接続タイムアウトエラー	サーバーへの接続がタイムアウトし、サーバーからの応答がありません。
エラー 301-恒久的に移動しました	ダウンロードしてキャッシュするビデオは、恒久的に別の場所に移動されました。
エラー 403-禁止	ダウンロードしてキャッシュするビデオへのアクセスは拒否されます。
エラー 404-見つかりません	ダウンロードしてキャッシュするビデオは、提供されているリンクから入手できません。
エラー 504：サーバーに到達できません	指定した URL にアクセスできません。
「x」ファイルを正常にダウンロードしました	URL のダウンロードが成功し、「x」個のメディアファイルがキャッシュにダウンロードされます。
「y」ファイルから「x」をダウンロードできませんでした	一部のメディアファイルの URL からのダウンロードに失敗しました。
x ファイルのダウンロードに失敗しました	URL からメディアファイルをダウンロードできませんでした。
ダウンロードが完了しました	このエントリのすべての URL の処理が完了しました。
ダウンロードを実行しています	ダウンロードが進行中です。
起動しています	アプライアンスは、URL からメディアファイルのダウンロードを開始しました。
このエントリを削除する	エントリは URL のリストから削除されています。
ディレクトリリストの取得に失敗しました	指定したリモートディレクトリからリストを取得できませんでした。
キャッシュのクリア操作によりエントリが削除されました	エントリは、キャッシュのクリア操作によってパージされました。
ステータスの更新	アプライアンスはエントリのステータスを更新しています。

ステータス	説明
スケジュール経過時間	リモートオブジェクトをダウンロードする予定時刻が過ぎています。
キャッシュ内“x”/”y”ファイル	エントリのステータスを更新すると、アプライアンスは、「y」個のファイルのうち「x」個のファイルがキャッシュに存在することを検出しました。
ビデオキャッシングでインターフェイス ap “X”が無効になっています	ブリッジインターフェイス ap “X”は、ビデオキャッシングに対して有効になっていません。
更新ステータス	エントリのステータスが更新されています。
エラー 0	ビデオのダウンロード中に不明なエラーが発生しました。問題を解決するには、Citrix テクニカルサポートチームに連絡してください。

ビデオキャッシングの事前入力を管理する

ビデオキャッシュの事前入力を管理して、URL からビデオをダウンロードしてキャッシュする方法を制御できます。次のタスクを実行して、ビデオキャッシュの事前入力を管理できます。

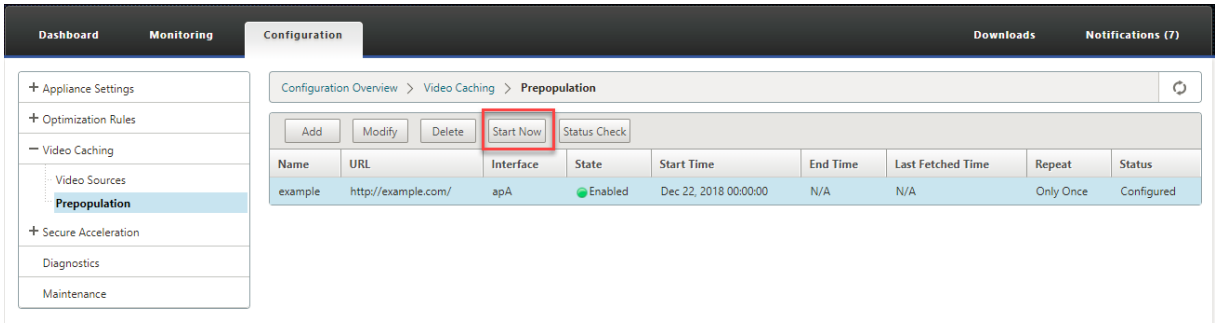
- 予定日時の前後に動画のダウンロードを開始します。
- エントリの URL を更新します。
- URL エントリからのビデオのキャッシュを無効にします。
- URL エントリからのビデオのキャッシュをスケジュールします。
- URL エントリのインターフェイスを更新します。
- URL エントリのステータスを更新します。
- URL エントリを削除します。

次のフローチャートは、ビデオ事前入力機能のさまざまなアクティビティを管理するときに実行されるプロセスのフロー制御を示しています。

動画をダウンロードする

追加した Web サイトまたは URL の技術的な問題により、スケジュールされたダウンロードとキャッシュが妨げられる場合は、必要に応じていつでもビデオのダウンロードとキャッシュを開始できます。

ビデオをすぐにダウンロードしてキャッシュするには、[構成]> ビデオキャッシング > 事前入力、キャッシュするビデオのエントリを選択し、[今すぐ開始] をクリックします。ビデオのステータスの更新には約 1 分かかります。



[今すぐ開始] をクリックすると、[ステータス] 列に URL からのビデオダウンロードのステータスが表示されます。

事前入力エントリの **URL** を更新します

ビデオをダウンロードしてキャッシュする URL を事前に追加した後、ビデオの場所が変更されたときやソース内のメディアファイルの名前が変更されたときに URL を再構成するなど、最適な結果が得られるように URL を微調整できます。

URL を更新するには:

1. 構成 > ビデオキャッシング > 事前入力 ページに移動します。
2. 更新するエントリを選択し、[変更] をクリックします。
3. [URL] フィールドで、新しい URL を指定します。
4. [**OK**] をクリックします。

事前入力エントリの **URL** からのビデオのキャッシュを無効にする

特定の URL からのビデオを定期的にキャッシュに事前入力する場合は、エントリを削除する必要はありません。無効にして、必要に応じて有効にすることができます。

エントリを無効にするには:

1. 構成 > ビデオキャッシング > 事前入力 ページに移動します。
2. 更新するエントリを選択し、[変更] をクリックします。
3. [状態] から、[無効] オプションを選択します。
4. [**OK**] をクリックします。

事前入力エントリの **URL** からのビデオのキャッシュをスケジュールします

URL からアプライアンスへのビデオのダウンロードとキャッシュを開始する日時をスケジュールできます。たとえば、ユーザーが動画にアクセスし始める直前に動画を取得したい場合があります。これにより、ディスクスペースが節約されるだけでなく、最新バージョンのビデオがキャッシュに保存されます。

URL からのキャッシュをスケジュールするには:

1. 構成 > ビデオキャッシング > 事前入力 ページに移動します。
2. 更新するエントリを選択し、[変更] をクリックします。
3. [スケジュール] から、[後で] オプションを選択します。
4. **[**開始**]** フィールドで、URL からビデオをダウンロードする日時を指定します。日付と時刻の形式は YYYY-MM-DD です。HH:MM:SS.
5. [繰り返し**]** リストから、ビデオをダウンロードしてキャッシュする頻度を選択します。以下の種類から選択できます。
   - **1** 回だけ: スケジュールされた日時に、URL からビデオを 1 回だけダウンロードします。
   - 毎日: スケジュールされた日時から始めて、毎日 URL からビデオをダウンロードします。ダウンロードは、指定した開始時刻に毎日開始されます。
   - 毎週: スケジュールされた日時から、週に 1 回 URL からビデオをダウンロードします。ダウンロードは毎週、指定した日時に開始されます。
   - 毎月: スケジュールされた日時から、月に 1 回 URL から動画をダウンロードします。ダウンロードは毎月、指定した日時に開始されます。
6. [**OK**] をクリックします。

URL エントリのインターフェイスを更新します

ネットワーク上に複数のリンクを構成している場合は、ネットワーク接続が向上するため、特定のリンクを使用してビデオをダウンロードすることをお勧めします。複数のリンクを構成するには、apA および apB ブリッジポートなどの使用可能なブリッジポートを使用します。これらのポートを使用して、URL エントリのビデオをダウンロードできます。

URL エントリのインターフェイスを更新するには:

1. 構成 > ビデオキャッシング > 事前入力に移動します。
2. 更新するエントリを選択します。変更をクリックします。
3. 「インターフェース」リストから、URL エントリーに使用するインターフェースを選択します。リストには、アプライアンスで使用可能で構成されているインターフェースが表示されます。
4. [**OK**] をクリックします。

URL エントリのステータスを更新します

時間の経過とともに、キャッシュされたビデオのステータスが変わる可能性があります。エントリのステータスを定期的にチェックすることで、ユーザーがビデオにアクセスしたときに予期しない結果が発生しないようにします。

URL からキャッシュされた動画の最新ステータスを確認するには:

1. 構成 > ビデオキャッシング > 事前入力に移動します。
2. キャッシュされたビデオのステータスを更新するエントリを選択します。
3. [ステータスチェック] をクリックします。

URL エントリを削除します

URL エントリが必要ない場合は、リストから削除できます。URL エントリを削除するには、エントリを選択して [削除] をクリックします。

> 注
>
> リストからビデオ事前入力タスクを削除すると、関連するビデオオブジェクトもキャッシュから削除されます。

ビデオキャッシュを確認する

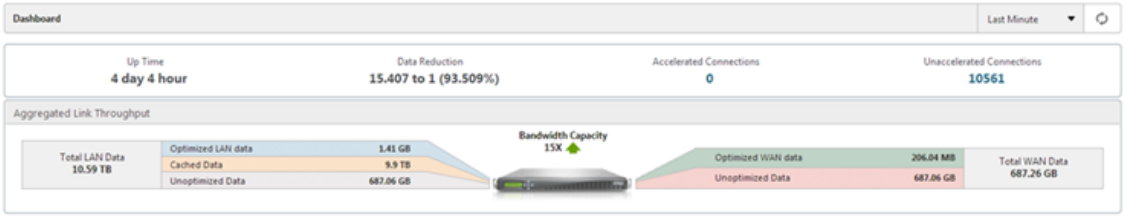
April 19, 2021

[監視] ページ、[ダッシュボード] ページ、および [使用状況] ページのグラフとデータは、ビデオキャッシュ構成によって提供される利点を評価するのに役立ちます。ビデオキャッシングによるデータ削減率（全体的な圧縮率と同様）は、ダッシュボード、ビデオキャッシング監視ページ、および使用状況グラフページに表示されます。また、[ダッシュボード] ページの [データ削減率] にカーソルを合わせると、サポートされているプラットフォームでのキャッシュのメリットの割合と圧縮のメリットの割合が表示されます。

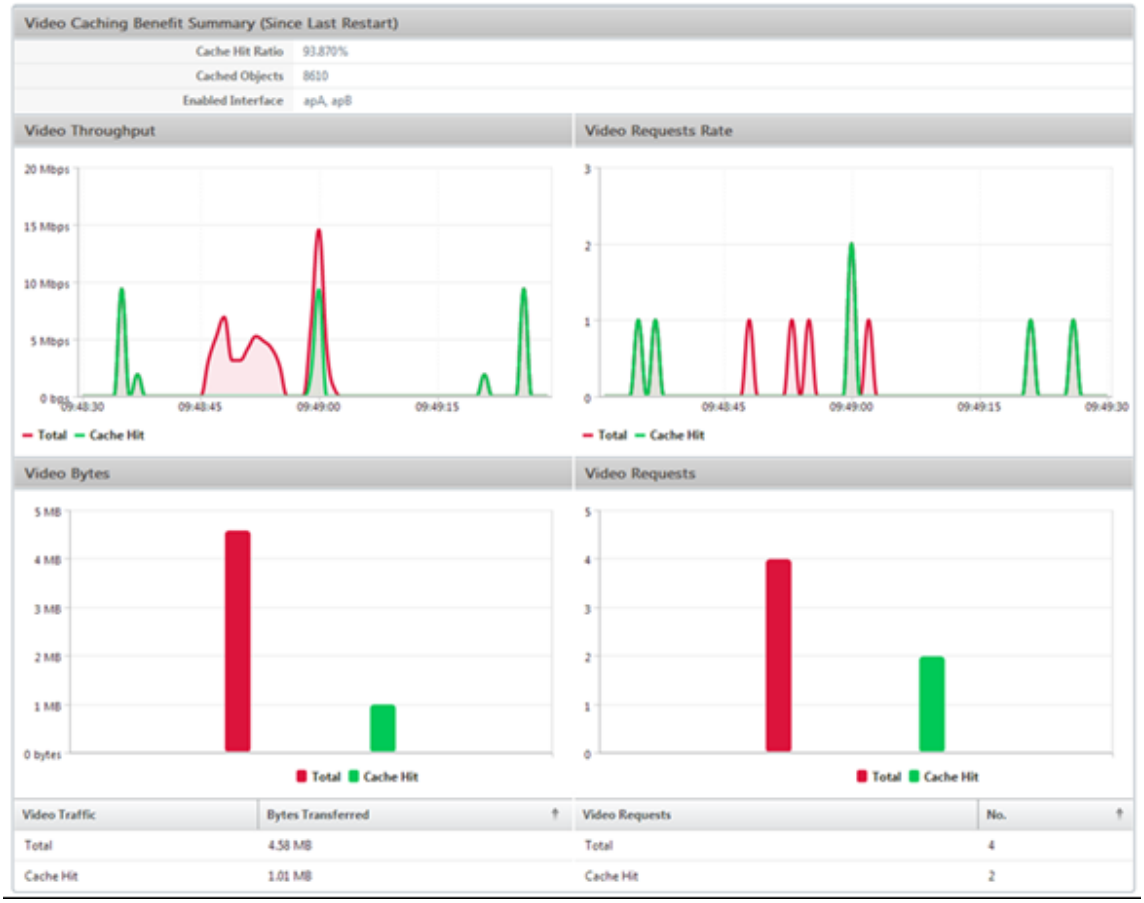
キャッシュの目的は、帯域幅を節約するだけでなく、パフォーマンスを向上させ、ビデオサーバーの負荷を軽減し、ネットワークの輻輳の影響を軽減することです。

ビデオキャッシングによる WAN 帯域幅の節約の見積もりは、次のように表示されます。

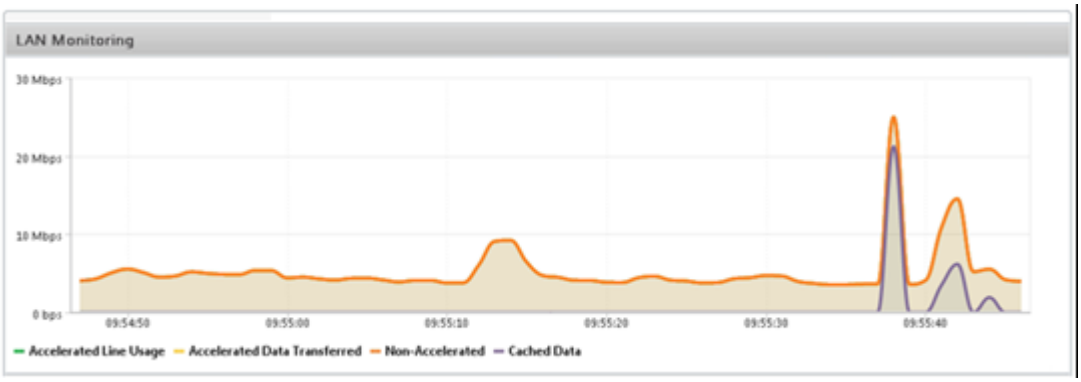
- [ダッシュボード] ページで、ダッシュボードの [データ削減] フィールドにカーソルを合わせると、キャッシュのメリットをパーセンテージで表示できます。集約リンクスループットの下で、キャッシュ（キャッシュデータ）から提供されたバイトを表示することもできます。



- モニタリングについて > ビデオキャッシュ ページでは、キャッシュされたオブジェクトの数とキャッシュヒット率（パーセンテージ）を表示できます。バーと時間のグラフには、1 分、1 時間、1 日、1 週間、1 か月にわたってキャッシュから提供されたリクエストとバイトの数が表示されます。このデータもグラフの下に表形式で表示されます。

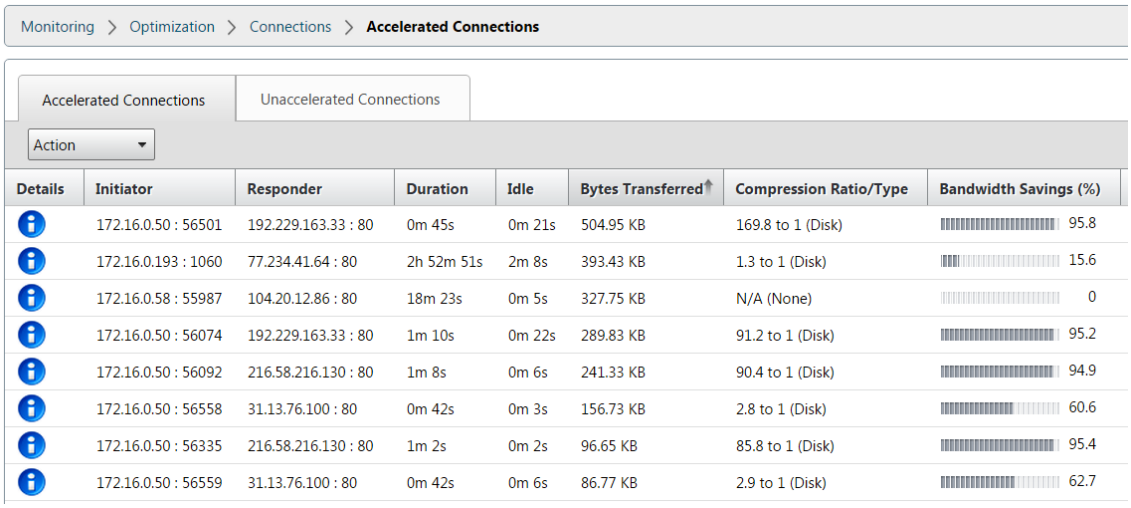


- モニタリング > 最適化 > 使用状況グラフ ページでは、LAN 監視グラフにキャッシュされたデータを表示できます。



- モニタリング > ビデオキャッシング > **HTTP** 状態 リスト ページでは、改善されたキャッシュ動作を監視できます。このページでは、ビデオキャッシュに関する HTTP 接続の状態を報告します。

- モニタリング > 最適化 > **[接続]** ページでは、[高速接続] タブでキャッシュされた接続を表示できます。キャッシュヒットとキャッシュミスの両方がここに表示されます。キャッシュ接続は、加速されていなくてもここに表示されます。つまり、パートナーの Citrix SD-WAN WANOP アプライアンスが接続に関与していない場合でも、キャッシュされた接続がここに表示されます。帯域幅の節約 (%) 列には、キャッシュまたは圧縮のいずれを介しても、トランザクションによって節約された WAN 帯域幅の量の棒グラフが表示されます。キャッシュと圧縮の目的は、帯域幅の使用量を減らすことではなく、速度と使いやすさを向上させることですが、速度と使いやすさの向上は、多くの場合、帯域幅の削減に関連しています。つまり、帯域幅を 90%節約すると、速度が 10 倍になります。



Details	Initiator	Responder	Duration	Idle	Bytes Transferred	Compression Ratio/Type	Bandwidth Savings (%)
	172.16.0.50 : 56501	192.229.163.33 : 80	0m 45s	0m 21s	504.95 KB	169.8 to 1 (Disk)	95.8
	172.16.0.193 : 1060	77.234.41.64 : 80	2h 52m 51s	2m 8s	393.43 KB	1.3 to 1 (Disk)	15.6
	172.16.0.58 : 55987	104.20.12.86 : 80	18m 23s	0m 5s	327.75 KB	N/A (None)	0
	172.16.0.50 : 56074	192.229.163.33 : 80	1m 10s	0m 22s	289.83 KB	91.2 to 1 (Disk)	95.2
	172.16.0.50 : 56092	216.58.216.130 : 80	1m 8s	0m 6s	241.33 KB	90.4 to 1 (Disk)	94.9
	172.16.0.50 : 56558	31.13.76.100 : 80	0m 42s	0m 3s	156.73 KB	2.8 to 1 (Disk)	60.6
	172.16.0.50 : 56335	216.58.216.130 : 80	1m 2s	0m 2s	96.65 KB	85.8 to 1 (Disk)	95.4
	172.16.0.50 : 56559	31.13.76.100 : 80	0m 42s	0m 6s	86.77 KB	2.9 to 1 (Disk)	62.7

ビデオキャッシュソースを管理する

April 19, 2021

ビデオソースは、グローバル設定を構成することによってグローバルに管理することも、ビデオソースのステータスを変更することによって個別に管理することもできます。

グローバル設定を構成する

グローバル設定を使用すると、アプライアンスレベルで機能を構成できます。追加したビデオソースに関係なく、これらの設定はアプライアンスのビデオキャッシュ機能全体に適用できます。次の操作を実行できます:

- キャッシュされたオブジェクトの最大サイズを構成します
- DNS サフィックスを構成する
- キャッシュポートの構成
- ビデオキャッシュポリシーファイルを更新します

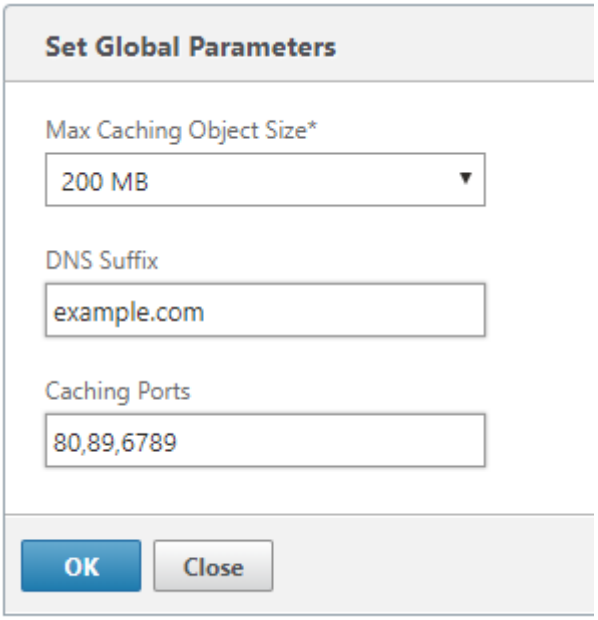
キャッシュされたオブジェクトの最大サイズを構成できます。この制限より大きなオブジェクトはキャッシュされません。デフォルトでは、キャッシュされるオブジェクトサイズは最大 100MB です。

完全なドメイン名を含まず、ドメイン名のサフィックスをビデオサーバーのホスト名に追加する必要がある URL の場合、サーバーからの応答を引き出すためにデフォルトのドメイン名を追加する必要があります。たとえば、`http://training/CitrixSD-WANWANOP\\_VideoCaching.mp4` ビデオにアクセスすると、アプライアンスは URL を `http://training.example.com/CitrixSD-WANWANOP\\_VideoCaching.mp4`に変換することが期待される場合があります。この場合、ドメイン名のサフィックスとして example.com を指定する必要があります。

ビデオキャッシュ機能には、HTTP ビデオサーバーのポート番号が必要です。デフォルトはポート 80 です。HTTP ビデオサーバーがこの既知の HTTP ポート以外のポートを使用している場合は、キャッシュポートのリストにポート番号を追加する必要があります。

ビデオキャッシュのグローバル設定を構成するには:

1. 構成 > ビデオキャッシング > グローバルパラメータを設定します。



2. [**MaxCaching** オブジェクトサイズ] フィールドで、キャッシュされたオブジェクトの最大サイズを設定します。

   使用可能な制限から値を選択します。この制限より大きなオブジェクトはキャッシュされません。

3. [**DNS** サフィックス] フィールドに、完全なドメイン名を含まず、ビデオサーバーのホスト名にドメイン名サフィックスを追加する必要がある URL に追加するドメイン名を入力します。

4. [キャッシュポート] フィールドに、HTTP ビデオサーバーのポートを入力して、キャッシュポートのリストに追加します。必要に応じて、コンマで区切って複数のポート番号を追加します。

5. [**OK**] をクリックします。

アプライアンスは、割り当てられたディスク領域の 10%を管理目的で使用します。ディスク使用量が割り当てられたディスク容量の 90%に達すると、ディスクがいっぱいになったことを示します。より多くのビデオオブジェクトをキャッシュするために、アプライアンスは最も使用されていないオブジェクトをビデオキャッシュから削除します。キャッシュが古いビデオオブジェクトを提供しない限り、キャッシュをクリアする必要はありません。

ビデオキャッシュをクリアするには、[構成]> ビデオキャッシュ をクリックし、[ビデオキャッシュのクリア] をクリックします。

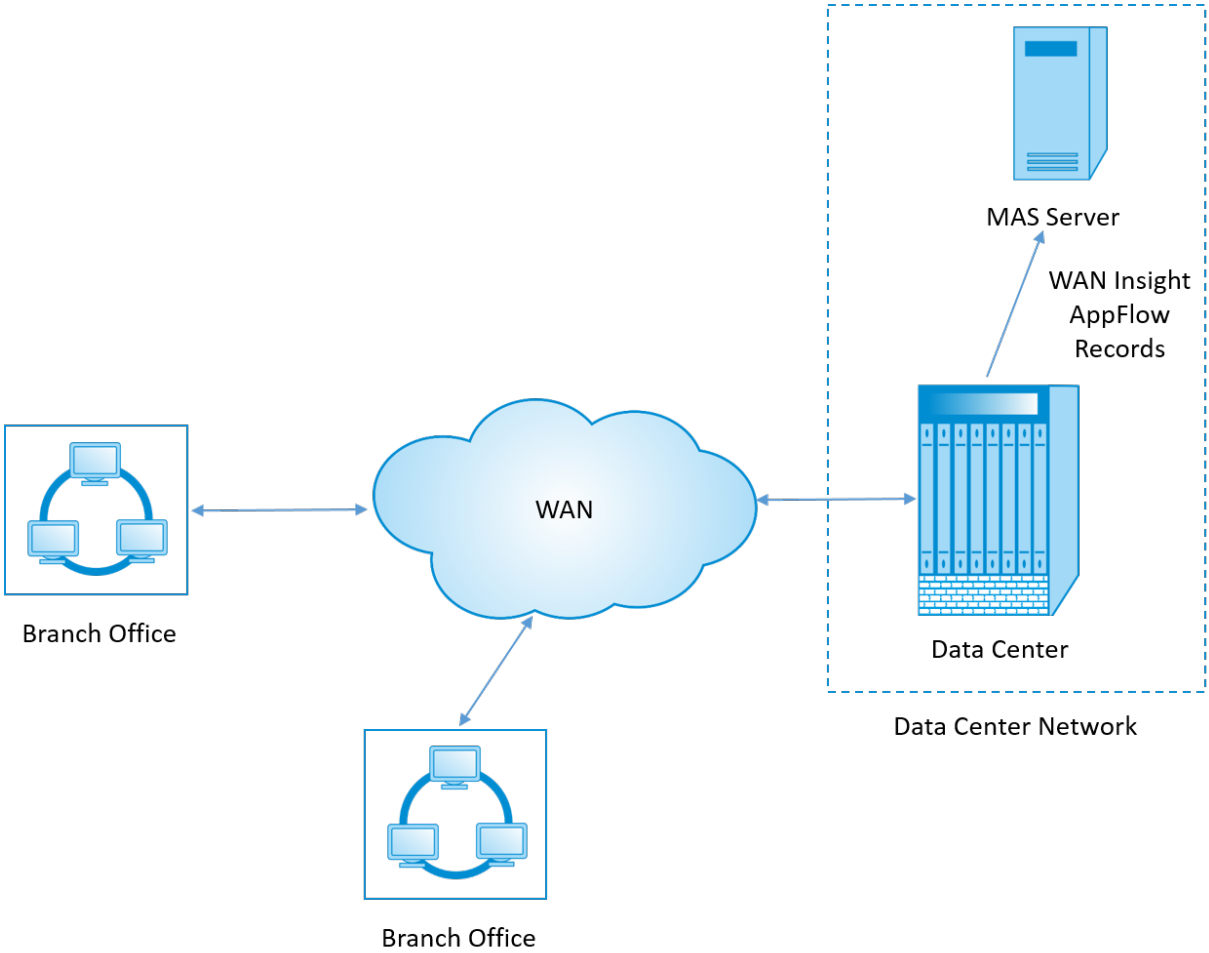
WAN インサイト

December 16, 2022

Citrix SD-WAN WANOP アプライアンスは、データセンターとブランチサイト間のネットワーク全体のデータフローの効率を向上させることにより、WAN を介した多数のアプリケーションの配信を最適化します。WAN Insight の分析機能を使用すると、管理者はデータセンターと Branch WAN 最適化アプライアンス間を流れる高速および非高速の WAN トラフィックを容易に監視できます。WAN Insight では、ネットワーク上のクライアント、アプリケーション、ブランチの状態を把握し、ネットワーク問題を効果的にトラブルシューティングできます。ライブレポートと履歴レポートを使用すると、問題がある場合はプロアクティブに対処できます。

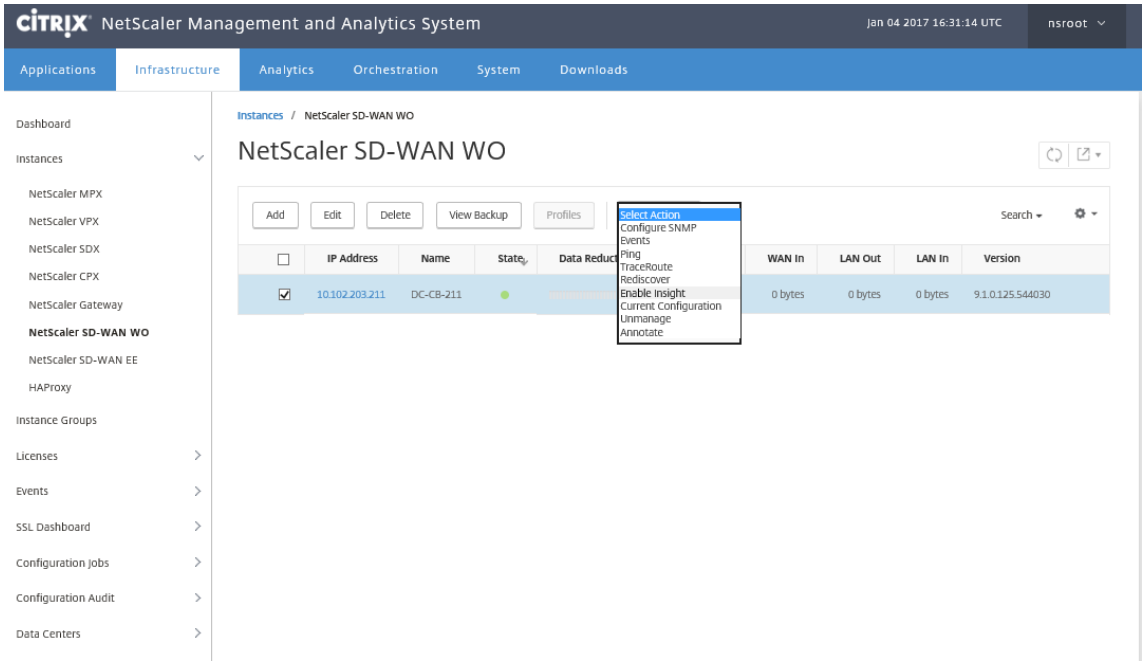
データセンター WAN 最適化アプライアンスで分析を有効にすると、Citrix Application Delivery Management（ADM）はデータを収集し、データセンターおよびブランチ WAN 最適化アプライアンスのレポートと統計を提供できるようになります。

> 注
>
> ARP エントリの追加の詳細については、Citrix ADM へのインスタンスの追加を参照してください。

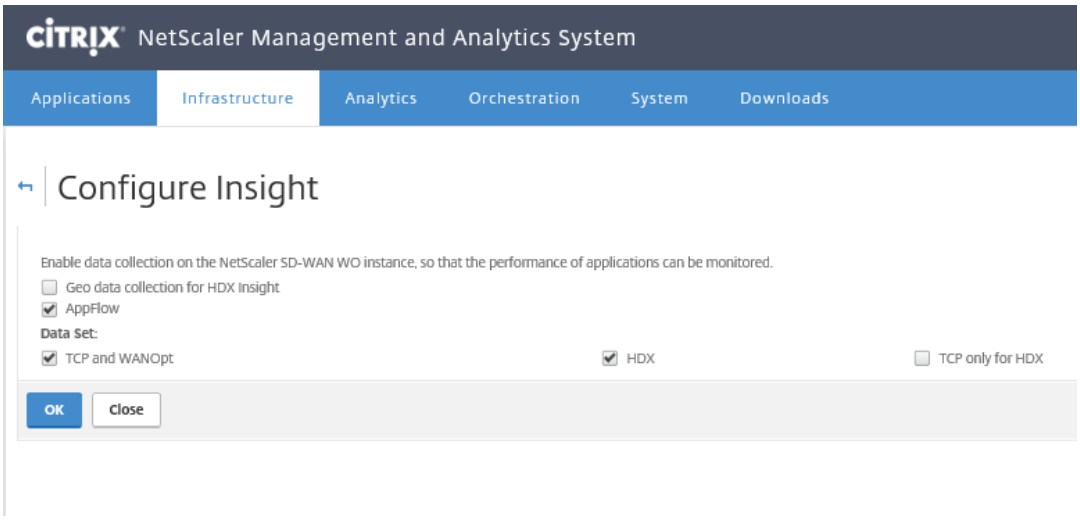


WAN 最適化アプライアンスで分析を有効にするには:

1. Web ブラウザで、Citrix ADM IP アドレス（例: http://192.168.100.1）を入力します。
2. ［**User Name**］と ［**Password**］の各フィールドに管理者の資格情報を入力します。
3. ［インフラストラクチャ］> ［インスタンス］**>** ［**Citrix SD-WAN WO**］の順に選択し、データセンターの WAN 最適化アプライアンスを選択します。



4. [アクション] ドロップダウンから、[インサイトを有効にする] を選択します。
5. 必要に応じて以下のパラメーターを選択します。
   - **HDX Insight** の地情報データ収集: クライアントの IP アドレスを Google Geo API と共有します。
   - **AppFlow**: WAN 最適化インスタンスからのデータの収集を開始します。
   - **TCP** および **WanOt**: TCP および WAonPt インサイトレポートを提供します。
   - **HDX**: HDX Insight レポートを提供します。
   - **HDX** のみの **TCP**: **HDX**Insight レポートにのみ TCP を提供します。



6. [**OK**] をクリックします。

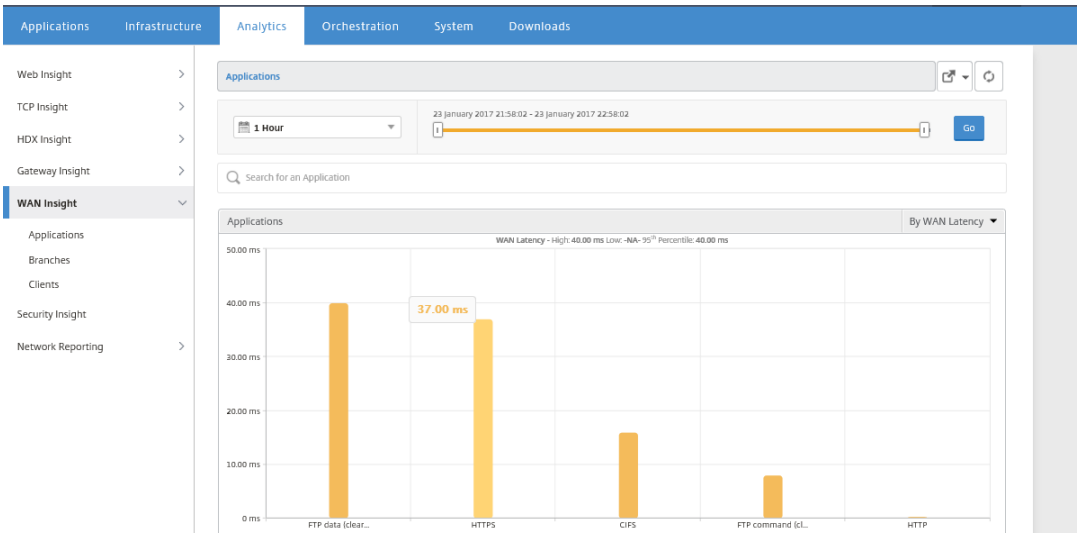
WAN インサイトレポートを表示するには、次の手順を実行します。

1. Web ブラウザで、Citrix ADM IP アドレス（例：http://192.168.100.1）を入力します。
2. ［**User Name**］と ［**Password**］の各フィールドに管理者の資格情報を入力します。
3. [**Analytics**] > [**WAN Insight**] に移動します。

> 注
>
> WAN Insight オプションは、SD-WAN WO インスタンスを Citrix ADM に追加した後にのみ表示されます。

次のレポートを表示できます。

- アプリケーション -選択した期間におけるすべてのアプリケーションの使用状況とパフォーマンスの統計を表示します。
- **Branches-** すべての WAN 最適化ブランチアプライアンスの使用状況とパフォーマンス統計を表示します。
- **Clients-** 各ブランチで WAN 最適化アプライアンスにアクセスするすべてのクライアントの使用状況とパフォーマンス統計を表示します。



次のメトリックが表示されます。
** 測定基準 **	** 説明 **
——-	————
Active Accelerated Connections	アクセラレーションが有効なアクティブ WAN 接続の数です。
Active Unaccelerated Connections	アクセラレーションが無効なアクティブ WAN 接続の数です。
WAN 遅延	アプリケーションとの対話中にユーザーに生じる遅延（ミリ秒単位）です。
圧縮率	選択した期間における支社アプライアンスとデータセンターアプライアンス間のデータ圧縮率です。

送信済みパケット	選択した期間に WAN 最適化アプライアンスからネットワーク経由で送信されたパケットの数です。
受信済みパケット	選択した期間に WAN 最適化アプライアンスがネットワークから受信したパケットの数です。
WAN で送信されたバイト数	選択した期間に Citrix WAN 最適化アプライアンスが WAN 経由で送信したバイト数。
WAN で受信したバイト数	選択した期間に WAN 最適化アプライアンスが WAN から受信したバイトの数です。
LAN RTO	選択した期間に WAN 最適化アプライアンスから LAN への再送信がタイムアウトになった回数です。
WAN RTO	選択した期間に WAN 最適化アプライアンスから WAN への再送信がタイムアウトになった回数です。
再転送パケット (LAN)	選択した期間に WAN 最適化アプライアンスから LAN ネットワークに再送信されたパケットの数です。
再転送パケット (WAN)	選択した期間に WAN 最適化アプライアンスから WAN ネットワークに再送信されたパケットの数です。

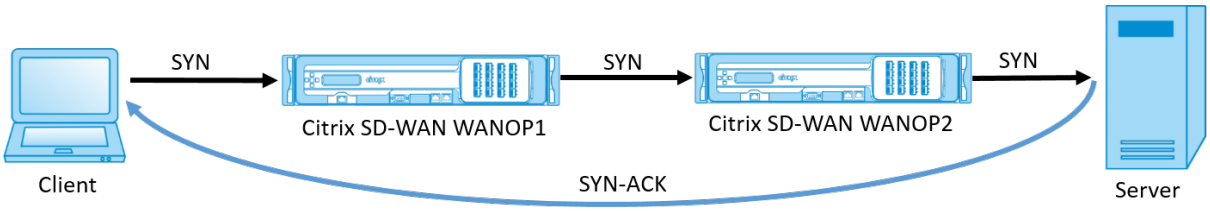
非対称ルーティング

April 19, 2021

Citrix SD-WAN WANOP ネットワークでは、同じ TCP 接続でクライアントからサーバーまたはサーバーからクライアントに流れるパケットがクライアント側とサーバー側の WANOP アプライアンスの一方または両方を通過しない場合に非対称ルーティングが発生します。以下の非対称性のケースが観察されます。

完全な非対称性:

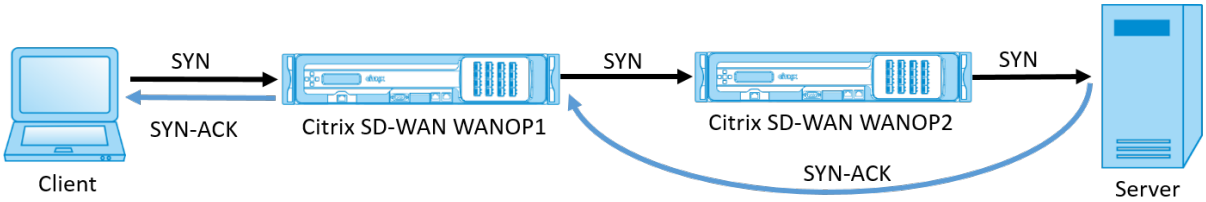
完全な非対称性は、パケットがクライアント側とサーバー側の両方の Citrix SD-WAN WANOP アプライアンスを介してクライアントからサーバーに流れるときに発生します。ただし、サーバーからクライアントへのリターンパスでは、パケットは両方の Citrix SD-WAN WANOP アプライアンスをバイパスする別のルートを取ります。



サーバー側の非対称性:

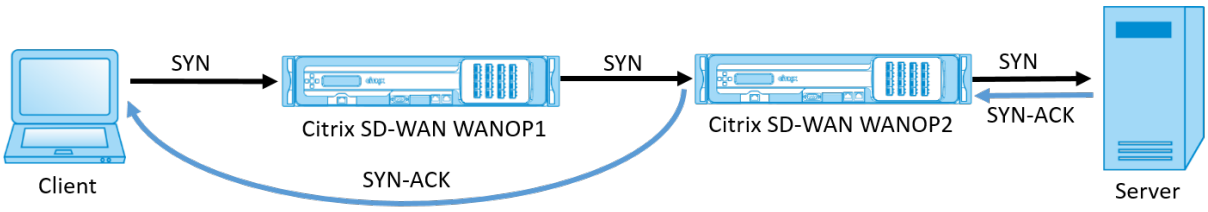
サーバー側の非対称性は、パケットがクライアント側とサーバー側の両方の Citrix SD-WAN WANOP アプライアンスを介してクライアントからサーバーに流れるときに発生します。ただし、リターンパスでは、パケットはサーバー

側の Citrix SD-WAN WANOP アプライアンスをバイパスしますが、クライアント側の Citrix SD-WAN WANOP アプライアンスを通過します。



クライアント側の非対称性:

クライアント側の非対称性は、パケットがクライアント側とサーバー側の両方の Citrix SD-WAN WANOP アプライアンスを介してクライアントからサーバーに流れるときに発生します。ただし、リターンパスでは、パケットはサーバー側の Citrix SD-WAN WANOP アプライアンスを通過しますが、クライアント側の Citrix SD-WAN WANOP アプライアンスをバイパスします。



Citrix SD-WAN WANOP ネットワークで非対称性を処理する

Citrix SD-WAN WANOP ネットワークでは、完全な非対称性が発生すると、TCP 接続がリセットされます。TCP 接続の切断を回避し、高速化されていないトラフィックの送信を継続するために、非対称接続リストが SD-WAN WANOP10.1 に導入されました。この機能はデフォルトで無効になっています。この機能は、クライアント側とサーバー側の両方の SD-WAN WANOP アプライアンスで有効にできます。

非対称接続を初めて検出すると、クライアントとサーバー間の TCP 接続がリセットされ、非対称接続リストにタプルのエントリが作成されます。タプルは、クライアント IP アドレスとサーバー IP アドレスで構成されます。タプルからの後続の接続は、加速されずに通過します。接続タプルは、デフォルトのタイムアウト期間である 4 時間、または対称性が検出されるまで、非対称接続リストに残ります。加速されていないパススルーは、タイムアウトが発生するまで、またはアプライアンスが非対称性が存在しなくなったことを動的に検出するまで有効です。

クライアント側の非対称性またはサーバー側の非対称性が検出されると、TCP 接続は保持され、パケットはデフォルトで加速されずに Citrix SD-WAN WANOP アプライアンスを通過します。

Citrix SD-WAN WANOP アプライアンスで非対称接続リストを有効にするには:

1. WANOP CLI コマンドプロンプトにアクセスします（WANOP Accelerator/Broker IP）。
2. 次の資格情報を使用してログインします。

```
**ログイン: ** *cli*****

```



```
**ログイン**: **** *admin*****

**パスワード**: **** *nsroot*****
```

> 注
>
> admin のデフォルトのパスワードは *nsroot* です。パスワードを変更した場合は、正しいパスワードを使用してください。

3. 次のコマンドを入力して、Enter キーを押します。

```
*Set parameter AssymetricConnectionList.Enable on*
```

> 注
>
> *AssymetricConnectionList.AutoFlushDuration* コマンドを使用して、ネットワーク要件に従ってタイムアウト期間を構成できます。

ネットワーク環境に基づいて、オンデマンドで微調整できる非対称リストで使用可能な複数のパラメーターがあります。詳細については、Citrix カスタマーサポートにお問い合わせください。

Citrix SD-WAN WANOP クライアントプラグイン

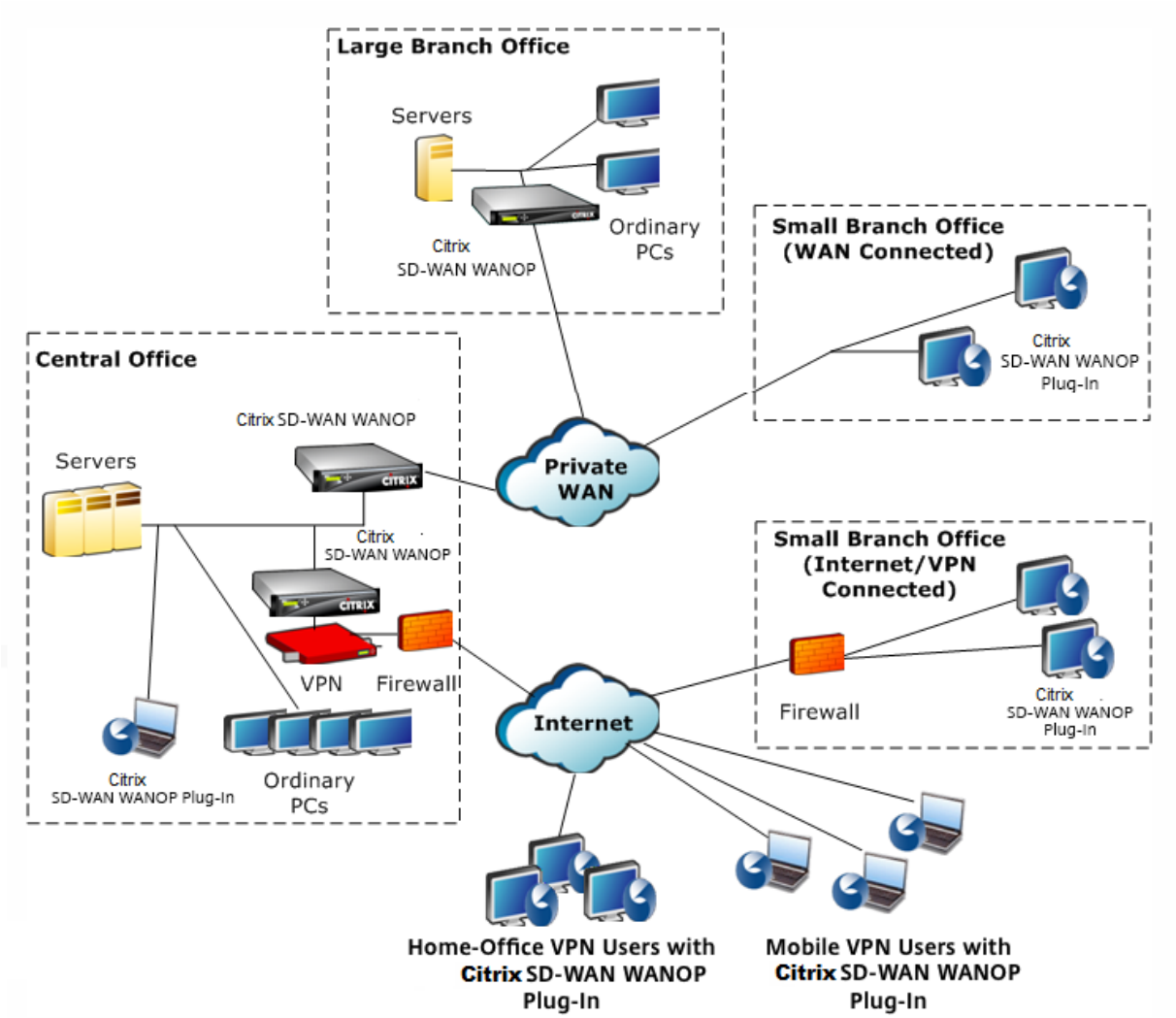
April 19, 2021

Citrix WANOP クライアントプラグインは、Windows ラップトップおよびワークステーションで実行されるソフトウェアベースのネットワークアクセラレータであり、WANOP クライアントプラグインアプライアンスを備えたオフィスだけでなく、どこでも高速化を提供します。リンクのもう一方の端で Citrix WANOP アプライアンスに接続します。

WANOP クライアントプラグインの動作原理は、通常、WANOP クライアントプラグインアプライアンスの原理と同じです。プラグインのドキュメントに含まれていないトピックについては、より大きなドキュメントセットを参照してください。

プラグインは、標準の Microsoft インストールファイル（MSI）として配布されます。プラグインの展開には、リンクのもう一方の端にある WANOP アプライアンスのプラグイン固有の構成が必要です。WANOP アプライアンスの DNS アドレスまたは IP アドレス、およびその他のいくつかのパラメーターを使用して MSI ファイルをカスタマイズする場合、ユーザーは、Windows コンピューターにプラグインをインストールするときに構成情報を入力する必要はありません。

図 1: WANOP クライアントプラグインを示す典型的な WANOP クライアントプラグインネットワーク



> 注
>
> プラグインは Citrix Receiver 1.2 以降でサポートされており、Citrix Receiver で配布および管理できます。

ハードウェアとソフトウェアの要件

April 19, 2021

アクセラレーションリンクのクライアント側では、
WANOP クライアントプラグインは Windows デスクトップおよびラップトップシステムでサポートされていますが、ネットブックやシンクライアントではサポートされていません。
WANOP クライアントプラグインを実行しているコンピューターには、次の最小ハードウェア仕様をお勧めします。

- Pentium4 クラス CPU
- 2GB の RAM
- 2GB の空きディスク容量

WANOP クライアントプラグインは Windows10 プラットフォームでサポートされており、次のシステム要件が必要です。

- 4GB RAM
- 10GB の空きディスク容量

WANOP クライアントプラグインは、次のオペレーティングシステムでサポートされています。

- Windows XP Home
- Windows XP Professional
- Windows Vista（Home Basic、Home Premium、Business、Enterprise、Ultimate のすべての 32 ビットバージョン）
- Windows 7（Home Basic、Home Premium、Professional、Enterprise、および Ultimate のすべての 32 ビットおよび 64 ビットバージョン）
- Windows 8（Enterprise Edition の 32 ビットおよび 64 ビットバージョン）
- Windows 10（Enterprise Edition の 32 ビットおよび 64 ビットバージョン）

サーバー側では、現在、次のアプライアンスが
WANOP クライアントプラグインの展開をサポートしています。

- WANOP クライアントプラグイン VPX
- WANOP クライアントプラグイン 2000
- WANOP クライアントプラグイン 3000
- WANOP クライアントプラグイン 4000
- WANOP クライアントプラグイン 5000

WANOP プラグインのしくみ

April 19, 2021

WANOP クライアントプラグイン製品は既存のものを使用します WAN/VPN インフラ。プラグインがインストールされているコンピューターは、プラグインのインストール前と同じように、LAN、WAN、およびインターネットに引

き続きアクセスします。ルーティングテーブル、ネットワーク設定、クライアントアプリケーション、またはサーバーアプリケーションを変更する必要はありません。

Citrix Access Gateway VPN には、少量の WANOP クライアントプラグイン固有の構成が必要です。

プラグインとアプライアンスによる接続の処理方法には、透過モード と リダイレクタモードの 2 つのバリエーションがあります。リダイレクタはレガシーモードであり、新しい展開には推奨されません。

- プラグインからアプライアンスへのアクセラレーションの透過モード は、アプライアンスからアプライアンスへのアクセラレーションと非常によく似ています。WANOP クライアントプラグインアプライアンスは、プラグインとサーバー間を移動するときにパケットがたどるパス内にある必要があります。アプライアンス間のアクセラレーションと同様に、透過モードは透過プロキシとして動作し、接続の一方の端からもう一方の端までの送信元と宛先の IP アドレスとポート番号を保持します。
- リダイレクタモード（非推奨）は、明示的なプロキシを使用します。プラグインは、発信パケットをアプライアンスのリダイレクタ IP アドレスに再アドレス指定します。次に、アプライアンスはパケットをサーバーに再アドレス指定し、リターンアドレスをプラグインではなく自身を指すように変更します。このモードでは、アプライアンスは WAN インターフェースとサーバー間のパスと物理的にインラインである必要はありません（これは理想的な展開ですが）。

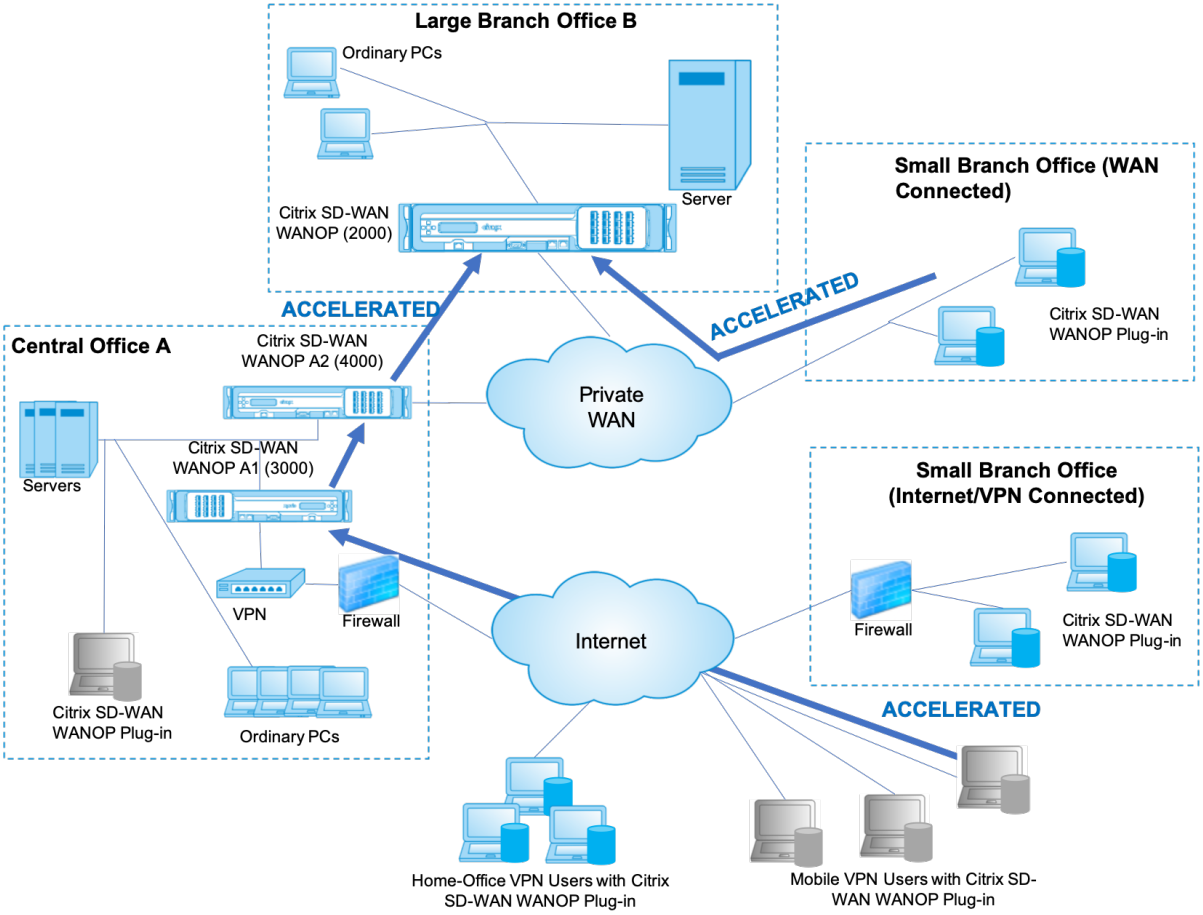
  ベストプラクティス：可能な場合は透過モードを使用し、必要な場合はリダイレクタモードを使用します。

透過モード

透過モードでは、高速化された接続のパケットは、アプライアンス間の高速化の場合と同様に、ターゲットアプライアンスを通過する必要があります。

プラグインは、アクセラレーションに使用できるアプライアンスのリストで構成されます。各アプライアンスへの接続を試み、シグナリング接続を開きます。シグナリング接続が成功すると、プラグインはアプライアンスからアクセラレーションルールをダウンロードし、アプライアンスがアクセラレーションできる接続の宛先アドレスを送信します。

図 1：透過モード、3 つの加速パスを強調表示



注

- トラフィックフロー-透過モードは、CitrixWANOP クライアントプラグインとプラグイン対応アプライアンス間の接続を高速化します。
- ライセンス-アプライアンスには、必要な数のプラグインをサポートするためのライセンスが必要です。この図では、Citrix SD-WAN WANOP はプラグインアクセラレーションのためにライセンスを取得する必要はありません。これは、Citrix SD-WAN WANOP A1 は、サイト A のプラグインアクセラレーションを提供します。
- デイジーチェーン-接続がターゲットアプライアンスに向かう途中で複数のアプライアンスを通過する場合、中央のアプライアンスで「デイジーチェーン」を有効にする必要があります。そうしないと、アクセラレーションがブロックされます。この図では、大規模なブランチオフィス B 宛てのホームオフィスおよびモバイル VPN ユーザーからのトラフィックは、Citrix SD-WAN WANOP B によって加速されます。これを機能させるには、Citrix SD-WAN WANOP A1 および A2 でデイジーチェーンを有効にする必要があります。

プラグインが新しい接続を開くたびに、加速ルールを参照します。宛先アドレスがいずれかのルールに一致する場合、プラグインは、接続の最初のパケット（SYN パケット）にアクセラレーションオプションを付加することにより、接続をアクセラレーションしようとします。プラグインに認識されているアプライアンスが SYN-ACK 応答パケットにアクセラレーションオプションを接続すると、そのアプライアンスとのアクセラレーション接続が確立されます。

アプリケーションとサーバーは、高速接続が確立されたことを認識していません。プラグインソフトウェアとアプライアンスだけが、加速が行われていることを認識しています。

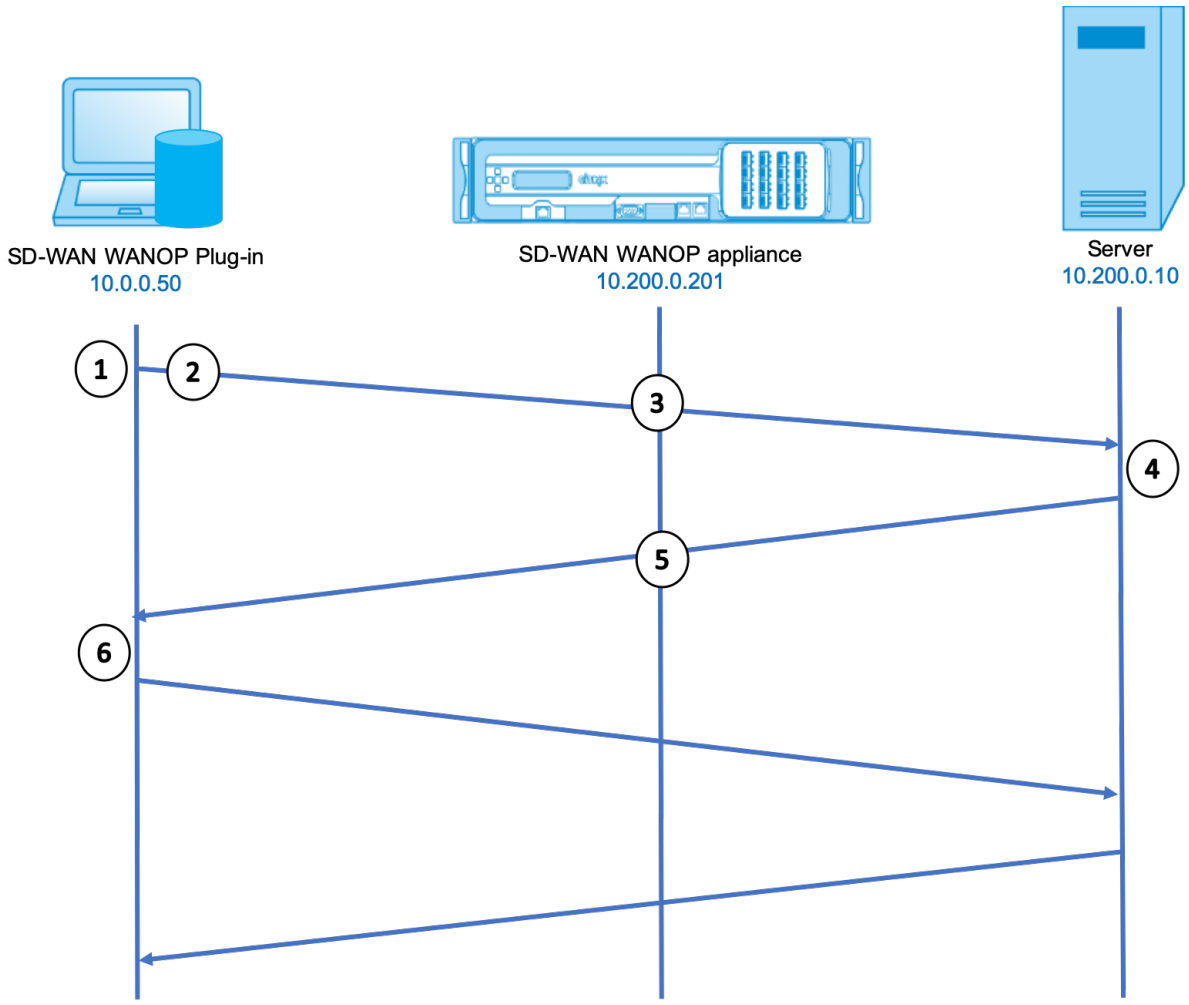
透過モードは、アプライアンス間のアクセラレーションに似ていますが、同じではありません。違いは次のとおりです。

- クライアントが開始する接続のみ-透過モードは、プラグインを備えたシステムによって開始される接続のみを受け入れます。プラグインを搭載したシステムをサーバーとして使用する場合、サーバー接続は高速化されません。一方、アプライアンス間のアクセラレーションは、どちらの側がクライアントでどちらがサーバーであるかに関係なく機能します。（アクティブモード FTP は、プラグインによって要求されたデータ転送を開始する接続がサーバーによって開かれるため、特殊なケースとして扱われます。）
- シグナリング接続-透過モードは、ステータス情報の送信にプラグインとアプライアンス間のシグナリング接続を使用します。アプライアンス間のアクセラレーションは、デフォルトで無効になっているセキュアなピア関係を除いて、シグナリング接続を必要としません。プラグインがシグナリング接続を開くことができない場合、アプライアンスを介した接続を高速化しようとはしません。
- デイジーチェーン-プラグインとその選択されたターゲットアプライアンスの間のパスにあるアプライアンスの場合、[構成：チューニング] メニューでデイジーチェーンを有効にする必要があります。

透過モードは、VPN でよく使用されます。WANOP クライアントプラグインプラグインは、ほとんどの IPSec および PPTP VPN、および Citrix Access GatewayVPN と互換性があります。

次の図は、透過モードでのパケットフローを示しています。このパケットフローは、接続の高速化を試みるかどうかの決定がシグナリング接続を介してダウンロードされた高速化ルールに基づくことを除いて、アプライアンス間の高速化とほぼ同じです。

図 2：透過モードでのパケットフロー



1. ユーザーのアプリケーションはサーバーへの TCP 接続を開き、TCPSYN パケットを送信します。

   Src: **10.0.0.50**、**Dst**: **10.200.0.10**

2. WANOP プラグインは宛先アドレスを検索し、アプライアンスによって高速化されたサブネットと一致することを確認します。これは、SYN パケットの TCP ヘッダーに WANOP オプションを付加します。アドレスは変更されません。

   Src: **10.0.0.50**、**Dst**: **10.200.0.10**

3. アプライアンスは SYN オプションを記録し、これが加速可能な接続であることを認識します。パケットからオプションを取り除き、サーバーにパススルーできるようにします。アドレスは変更されません。

   Src: **10.0.0.50**、**Dst**: **10.200.0.10**

4. サーバーは接続を受け入れ、TCP SYN-ACK パケットで応答します。

   Src: **10.200.0.10**、**Dst**: **10.0.0.50**

5. アプライアンスは、加速が行われることを示す TCP ヘッダーオプションで SYN-ACK パケットにタグを付けます。

Src：**10.200.0.10**、**Dst**：**10.0.0.50**

6. WANOP プラグインは SYN-ACK パケットを受信します。パケットヘッダーのオプションは、接続が高速化されていることを示します。プラグインはオプションを取り除き、SYN-ACK パケットをアプリケーションに渡します。これで接続が完全に開き、加速されます。

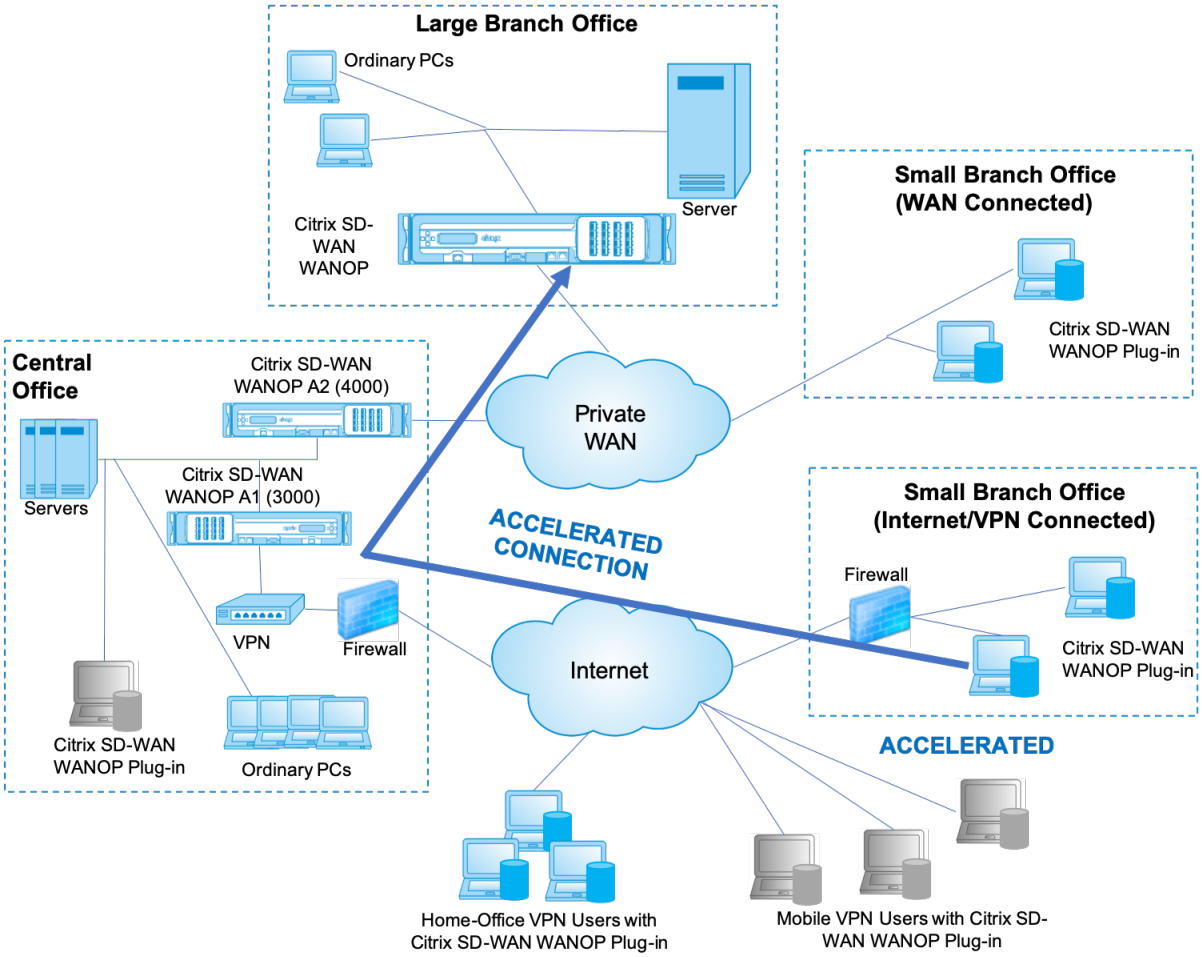
リダイレクタモード

リダイレクタモードは、次の点で透過モードとは動作が異なります。

- WANOP クライアントプラグインプラグインソフトウェアは、パケットをアプライアンスに明示的にアドレス指定することにより、パケットをリダイレクトします。
- したがって、リダイレクタモードアプライアンスは、すべての WAN リンクトラフィックを傍受する必要はありません。アクセラレーションされた接続は直接アドレス指定されるため、プラグインとサーバーの両方から到達できる限り、どこにでも配置できます。
- アプライアンスは最適化を実行してから、出力パケットをサーバーにリダイレクトし、パケット内の送信元 IP アドレスを独自のアドレスに置き換えます。サーバーの観点からは、接続はアプライアンスで開始されます。
- サーバーからのリターントラフィックはアプライアンスにアドレス指定されます。アプライアンスはリターン方向で最適化を実行し、出力パケットをプラグインに転送します。
- 宛先ポート番号は変更されないため、ネットワーク監視アプリケーションは引き続きトラフィックを分類できます。

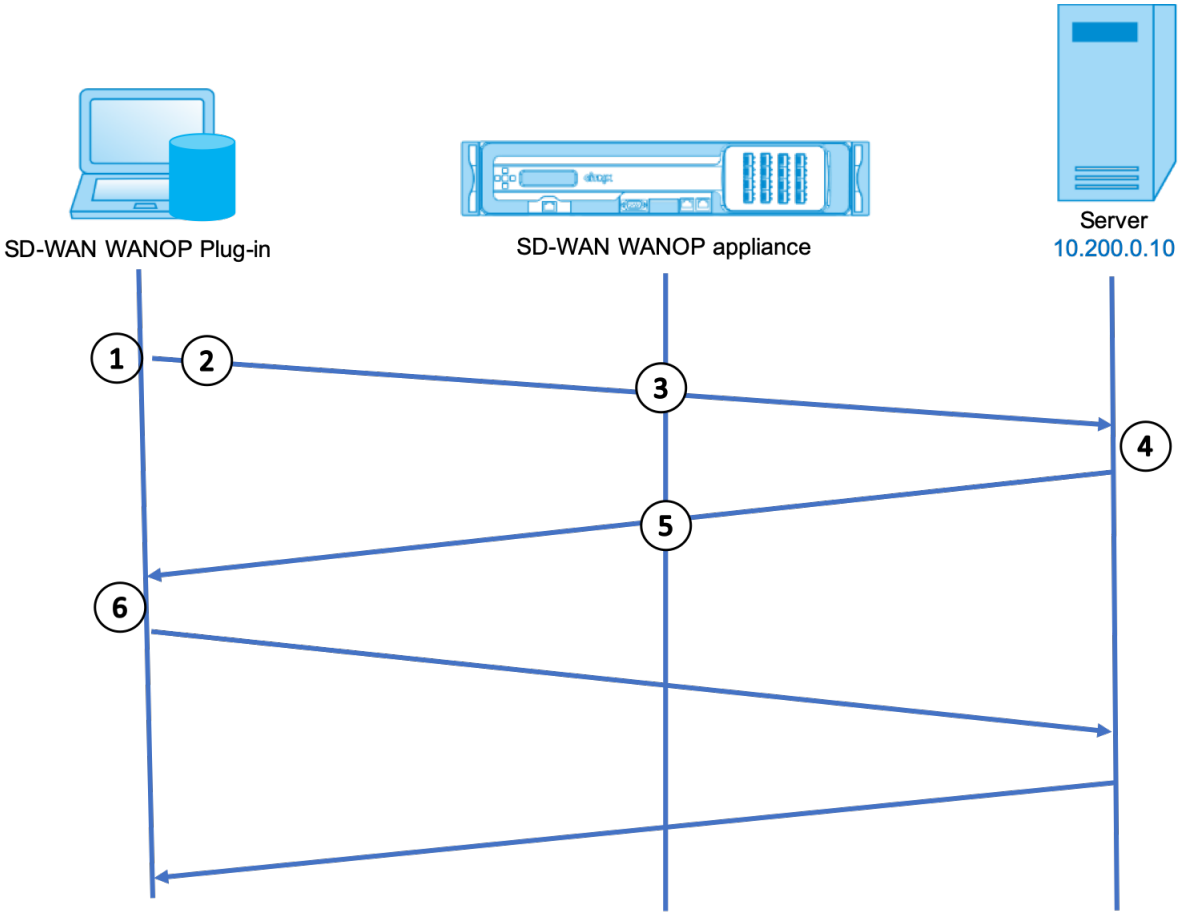
次の図は、リダイレクタモードがどのように機能するかを示しています。

図 1：リダイレクタモード



次の図は、リダイレクタモードでのパケットフローとアドレスマッピングを示しています。

図 2：リダイレクタモードでのパケットフロー



1. ユーザーのアプリケーションはサーバーへの TCP 接続を開き、TCPSYN パケットを送信します。

   Src：**10.0.0.50**、**Dst**：**10.200.0.10**

2. Citrix SD-WAN WANOP プラグインは、宛先アドレスを検索し、接続を 10.200.0.201 のアプライアンスにリダイレクトすることを決定します。

   Src：**10.0.0.50**、**Dst**：**10.200.0.201**

   (10.200.0.10 は TCP オプションフィールドに保持されます。オプション 24～31 は、さまざまなパラメーターに使用されます。)

3. アプライアンスは接続を受け入れ、パケットをサーバーに転送し（TCP オプションフィールドの宛先アドレスを使用)、それ自体を送信元として提供します。

   Src：**10.200.0.201**、**Dst**：**10.200.0.10**

4. サーバーは接続を受け入れ、TCP SYN-ACK パケットで応答します。

   Src：**10.200.0.10**、**Dst**：**10.200.0.201**

5. アプライアンスはアドレスを書き換え、パケットをプラグインに転送します（サーバーアドレスをオプションフィールドに配置します)。

   Src：**10.200.0.201**、**Dst**：**10.0.0.50**

6. これで接続が完全に開きます。クライアントとサーバーは、アプライアンスを介してパケットを送受信します。

   アドレスがリダイレクタモードで分析されている間、宛先ポート番号はニットです（ただし、エフェメラルポート番号はニットである可能性があります）。データはカプセル化されていません。リダイレクタモードはプロキシであり、トンネルではありません。

   ありません 1:1 パケット間の関係（最終的には、受信したデータは常に送信したデータと同じです）。圧縮により、多くの入力パケットが 1 つのパケットに削減される場合があります。CIFS アクセラレーションは、投機的な先読みおよびホワイトビハインド操作を実行します。また、appliace と Reperter プラグインの間でパケットがドロップされた場合、再送信は、高度な回復アルゴリズムを使用して、サーバーではなくアプライアンスによって処理されます。

プラグインがアプライアンスを選択する方法

各プラグインは、高速接続を要求するために接続できるアプライアンスのリストで構成されています。

アプライアンスにはそれぞれ、アクセラレーションルールのリストがあります。これは、アプライアンスがアクセラレーション接続を確立できるターゲットアドレスまたはポートのリストです。プラグインはこれらのルールをアプライアンスからダウンロードし、各接続の宛先アドレスとポートを各アプライアンスのルールセットと照合します。特定の接続を高速化するアプライアンスが 1 つしかない場合、選択は簡単です。複数のアプライアンスが接続を高速化することを提案している場合、プラグインはアプライアンスの 1 つを選択する必要があります。

アプライアンスの選択のルールは次のとおりです。

- 接続を高速化するために提供しているすべてのアプライアンスがリダイレクタモードアプライアンスである場合、プラグインのアプライアンスリストの左端のアプライアンスが選択されます。（アプライアンスが DNS アドレスとして指定されていて、DNS レコードに複数の IP アドレスがある場合、これらも左から右にスキャンされます。）
- 接続を高速化するために提供しているアプライアンスの一部がリダイレクタモードを使用し、一部が透過モードを使用している場合、透過モードアプライアンスは無視され、リダイレクタモードアプライアンスから選択が行われます。
- 接続を高速化するために提供しているすべてのアプライアンスが透過モードを使用している場合、プラグインは特定のモードを選択しません appliance. WANOP クライアントプラグイン SYN オプションを使用して接続を開始し、返される SYN-ACK パケットに適切なオプションをアタッチする候補アプライアンスが使用されます。これにより、実際にトラフィックと一致しているアプライアンスがプラグインに対して自身を識別できるようになります。ただし、プラグインは応答するアプライアンスとのオープンなシグナリング接続を備えている必要があります。そうでない場合、アクセラレーションは行われません。
- 一部の構成情報はグローバルと見なされます。この構成情報は、シグナリング接続を開くことができるリストの左端のアプライアンスから取得されます。

プラグインで使用するアプライアンスをデプロイする

April 19, 2021

クライアントアクセラレーションには、WANOP クライアントプラグインアプライアンスでの特別な構成が必要です。その他の考慮事項には、アプライアンスの配置が含まれます。プラグインは通常、VPN 接続用に展開されます。

可能な場合は専用のアプライアンスを使用してください

プラグインアクセラレーションとリンクアクセラレーションの両方に同じアプライアンスを使用しようとすると、多くの場合困難になります。これは、2 つの用途でアプライアンスをデータセンターの異なるポイントに配置する必要があり、2 つの用途で異なるサービスクラスルールが必要になる場合があるためです。

さらに、単一のアプライアンスがプラグインアクセラレーションのエンドポイントまたはサイト間アクセラレーションのエンドポイントとして機能できますが、同じ接続に対して同時に両方の目的を果たすことはできません。したがって、VPN のプラグインアクセラレーションとリモートデータセンターへのサイト間アクセラレーションの両方にアプライアンスを使用する場合、プラグインユーザーはサイト間アクセラレーションを受信しません。この問題の深刻さは、プラグインユーザーが使用するデータのどれだけがリモートサイトからのものであるかによって異なります。

最後に、専用アプライアンスのリソースはプラグインとサイト間の要求に分割されないため、より多くのリソースを提供し、各プラグインユーザーにより高いパフォーマンスを提供します。

可能な場合はインラインモードを使用してください

アプライアンスは、サポートする VPN ユニットと同じサイトに展開する必要があります。通常、2 つのユニットは互いに一致しています。インライン展開は、最も単純な構成、ほとんどの機能、および最高のパフォーマンスを提供します。最良の結果を得るには、アプライアンスが VPN ユニットと直接一致している必要があります。

ただし、アプライアンスは、グループモードまたは高可用性モードを除き、任意のデプロイモードを使用できます。これらのモードは、アプライアンスからアプライアンスへのアクセラレーションとクライアントからアプライアンスへのアクセラレーションの両方に適しています。これらは、単独で（透過モード）、またはリダイレクタモードと組み合わせて使用できます。

アプライアンスをネットワークの安全な部分に配置します

アプライアンスは、サーバーと同じように既存のセキュリティインフラストラクチャに依存します。ファイアウォール（および使用する場合は VPN ユニット）のサーバーと同じ側に配置する必要があります。

NAT の問題を回避する

プラグイン側のネットワークアドレス変換（NAT）は透過的に処理され、問題にはなりません。アプライアンス側では、NAT が面倒になる可能性があります。スムーズな展開を確実にするために、次のガイドラインを適用してください。

- アプライアンスをサーバーと同じアドレス空間に配置して、サーバーに到達するために使用されるアドレス変更もアプライアンスに適用されるようにします。
- アプライアンスがそれ自体に関連付けられていないアドレスを使用してアプライアンスにアクセスしないでください。
- アプライアンスは、プラグインユーザーが同じサーバーにアクセスするのと同じ IP アドレスを使用してサーバーにアクセスできる必要があります。
- つまり、サーバーやアプライアンスのアドレスに NAT を適用しないでください。

ソフトブーストモードを選択します

[設定の構成：帯域幅管理] ページで、[ソフトブーストモード] を選択します。Softboost は、WANOP クライアントプラグインプラグインでサポートされている唯一のタイプのアクセラレーションです。

プラグインアクセラレーションルールを定義する

アプライアンスは、どのトラフィックを加速するかをクライアントに指示する加速ルールのリストを維持します。各ルールは、アプライアンスが高速化できるアドレスまたはサブネットとポート範囲を指定します。

何を加速するか-どのトラフィックを加速するかの選択は、アプライアンスが使用されている用途によって異なります。

- VPN アクセラレータ-アプライアンスが VPN アクセラレータとして使用されており、すべての VPN トラフィックがアプライアンスを通過している場合、宛先に関係なく、すべての TCP トラフィックを高速化する必要があります。
- リダイレクタモード-トランスペアレントモードとは異なり、リダイレクタモードのアプライアンスは明示的なプロキシであるため、プラグインは、望ましくない場合でもトラフィックをリダイレクタモードアプライアンスに転送します。クライアントがサーバーから離れたアプライアンスにトラフィックを転送する場合、特にこの「三角形のルート」によって低速または信頼性の低いリンクが導入される場合、アクセラレーションは逆効果になる可能性があります。したがって、特定のアプライアンスが自身のサイトのみを高速化できるようにアクセラレーションルールを構成することをお勧めします。
- その他の用途-プラグインを VPN アクセラレータとしてもリダイレクタモードでも使用しない場合、アクセラレーションルールには、ユーザーからリモートでデータセンターからローカルのアドレスを含める必要があります。

Rules-を定義する設定 の上、アプライアンスの加速ルールを定義します。WANOP クライアントプラグイン：加速度は、タブをルール。

ルールは順番に評価され、アクション（加速または除外）は最初に一致したルールから実行されます。接続を高速化するには、接続が高速化ルールに一致する必要があります。

デフォルトのアクションは加速しないことです。

1. 構成：WANOP プラグイン：アクセラレーションルールタブ：
   - アプライアンスが到達できるローカル LAN サブネットごとに Accelerated ルールを追加します。つまり、[追加] をクリックし、[加速] を選択して、サブネット IP アドレスとマスクを入力します。
   - アプライアンスに対してローカルなサブネットごとに繰り返します。
2. 含まれる範囲の一部を除外する必要がある場合は、除外ルールを追加して、より一般的なルールの上に移動します。たとえば、10.217.1.99 はローカルアドレスのように見えます。それが実際に VPN ユニットのローカルエンドポイントである場合は、次の Accelerate ルールの上の行に Exclude ルールを作成します。10.217.1.0/24.
3. HTTP のポート 80 など、単一のポートのみにアクセラレーションを使用する場合（非推奨）、[ポート] フィールドのワイルドカード文字を特定のポート番号に置き換えます。ポートごとに 1 つずつルールを追加することで、追加のポートをサポートできます。
4. 一般に、一般的なルールの前に狭いルール（通常は例外）をリストします。
5. ［**Apply**］をクリックします。適用する前にこのページから移動した場合、変更は保存されません。

IP ポートの使用法

IP ポートの使用については、次のガイドラインを使用してください。

- **WANOP** クライアントプラグインプラグインとの通信に使用されるポート-プラグインは、シグナリング接続を介してアプライアンスとのダイアログを維持します。この接続は、デフォルトでポート 443（HTTPS）にあり、ほとんどのファイアウォールを通過できます。
- サーバーとの通信に使用されるポート-WANOP クライアントプラグインプラグインとアプライアンス間の通信では、プラグインとアプライアンスが存在しない場合にクライアントがサーバーとの通信に使用するのと同じポートが使用されます。つまり、クライアントがポート 80 で HTTP 接続を開くと、ポート 80 でアプライアンスに接続します。次に、アプライアンスはポート 80 でサーバーに接続します。

  リダイレクタモードでは、既知のポート（つまり、TCP SYN パケットの宛先ポート）のみが保持されます。エフェメラルポートは保持されません。透過モードでは、両方のポートが保持されます。

  アプライアンスは、クライアントが要求した任意のポートでサーバーと通信できると想定し、クライアントは、任意のポートでアプライアンスと通信できると想定します。これは、アプライアンスがサーバーと同じファイアウォールルールの対象である場合にうまく機能します。このような場合、直接接続で成功する接続はすべて、高速接続で成功します。

TCP オプションの使用法とファイアウォール

WANOP クライアントプラグインパラメータは、TCP オプションで送信されます。TCP オプションは任意のパケットで発生する可能性があり、接続を確立する SYN および SYN-ACK パケットに存在することが保証されています。

ファイアウォールが 24〜31（10 進数）の範囲の TCP オプションをブロックしてはなりません。ブロックしないと、アクセラレーションを実行できません。ほとんどのファイアウォールはこれらのオプションをブロックしません。ただし、リリース 7.x ファームウェアを搭載した Cisco PIX または ASA ファイアウォールはデフォルトでそうする可能性があるため、設定を調整する必要がある場合があります。

プラグインの **MSI** ファイルをカスタマイズする

April 19, 2021

WANOP クライアントプラグイン配布ファイルのパラメーターを変更できます。これは、標準の Microsoft インストーラー（MSI）形式です。カスタマイズには、MSI エディターを使用する必要があります。

> 注
>
> 編集したパラメータの変更。MSI ファイルは、新規インストールにのみ適用されます。既存のプラグインユーザーが新しいリリースに更新しても、既存の設定は保持されます。したがって、パラメータを変更した後は、新しいバージョンをインストールする前に、古いバージョンをアンインストールするようにユーザーにアドバイスする必要があります。

ベストプラクティス:

最も近いプラグイン対応アプライアンスに解決される DNS エントリを作成します。たとえば、アプライアンスが 1 つしかない場合は、「Repeater.mycompany.com」を定義して、アプライアンスに解決させます。または、たとえば 5 つのアプライアンスがある場合は、Repeater.mycompany.com を 5 つのアプライアンスの 1 つに解決し、クライアントまたは VPN ユニットへの近さに基づいてアプライアンスを選択します。たとえば、特定の VPN に関連付けられたアドレスを使用しているクライアントは、Repeater.mycompany.com がその VPN に接続されている WANOP クライアントプラグインアプライアンスの IP アドレスに解決されることを確認する必要があります。Orca などの MSI エディターを使用して、このアドレスをプラグインバイナリに組み込みます。アプライアンスを追加、移動、または削除するときに、DNS サーバーでこの単一の DNS 定義を変更すると、プラグインのアプライアンスリストが自動的に更新されます。

DNS エントリを複数のアプライアンスに解決することもできますが、プラグインはリストの左端のアプライアンスからその特性の一部を取得し、それらをグローバルに適用するため（SSL 圧縮特性を含む）、すべてのアプライアンスが同じように構成されていない限り、これは望ましくありません。。これは、特に DNS サーバーが各要求の IP アドレスの順序をローテーションする場合に、望ましくない混乱を招く結果につながる可能性があります。

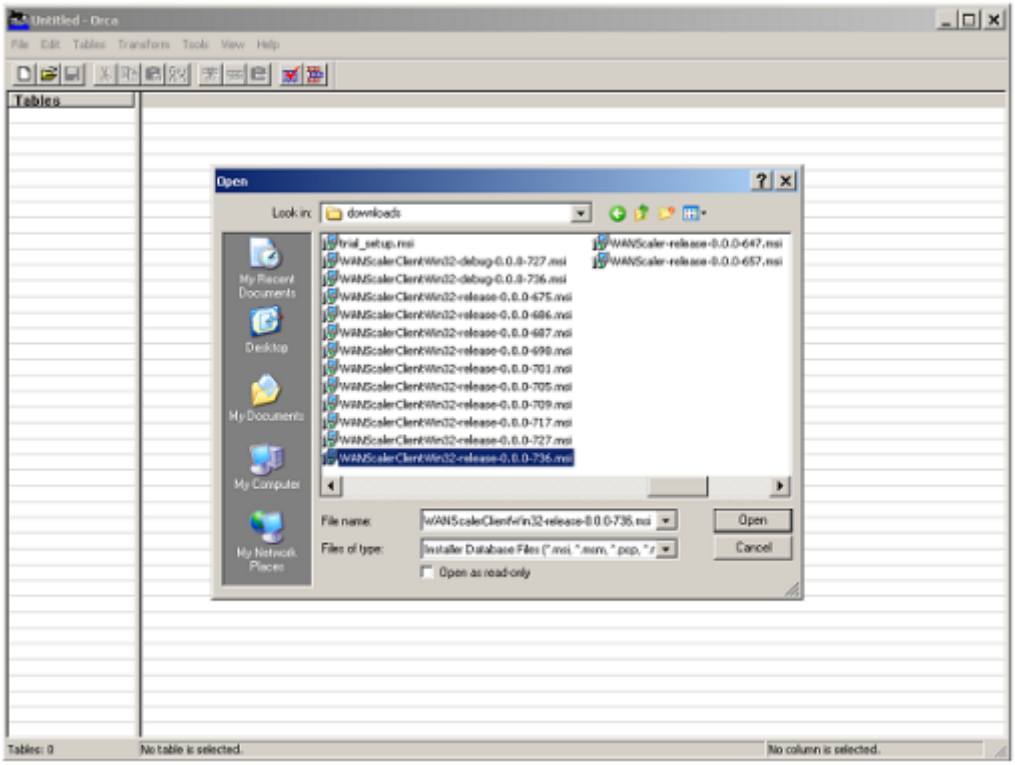
OrcaMSI エディターをインストールします:

Microsoft の無料の PlatformSDK の一部であり、Microsoft からダウンロードできる Orca を含む、多くの MSI エディターがあります。

OrcaMSI エディターをインストールするには:

1. SDK の PSDK-x86.exe バージョンをダウンロードして実行します。インストール手順に従います。
2. SDK をインストールしたら、Orca エディターをインストールする必要があります。これは、Microsoft プラットフォーム SDK\ Bin\ Orca.Msi の下になります。Orca.msi を起動して、実際の Orca エディター（orca.exe）をインストールします。
3. **Orca** の実行：Microsoft は Orca のドキュメントをオンラインで提供しています。以下の情報は、最も重要な WANOP クライアントプラグインプラグインパラメータを編集する方法を説明しています。
4. スタート **>** 全てのプログラム **> Orca** で Orca を起動します。空白の Orca ウィンドウが表示されたら、ファイル **>** 開くで WANOP クライアントプラグインプラグイン MSI ファイルを開きます。

   図 **1**：**Orca** の使用



5. [テーブル] メニューの [プロパティ] をクリックします。.MSI ファイルの編集可能なすべてのプロパティのリストが表示されます。次の表に示すパラメーターを編集します。パラメータを編集するには、その値をダブルクリックし、新しい値を 入力して、**Enter** キーを押します。

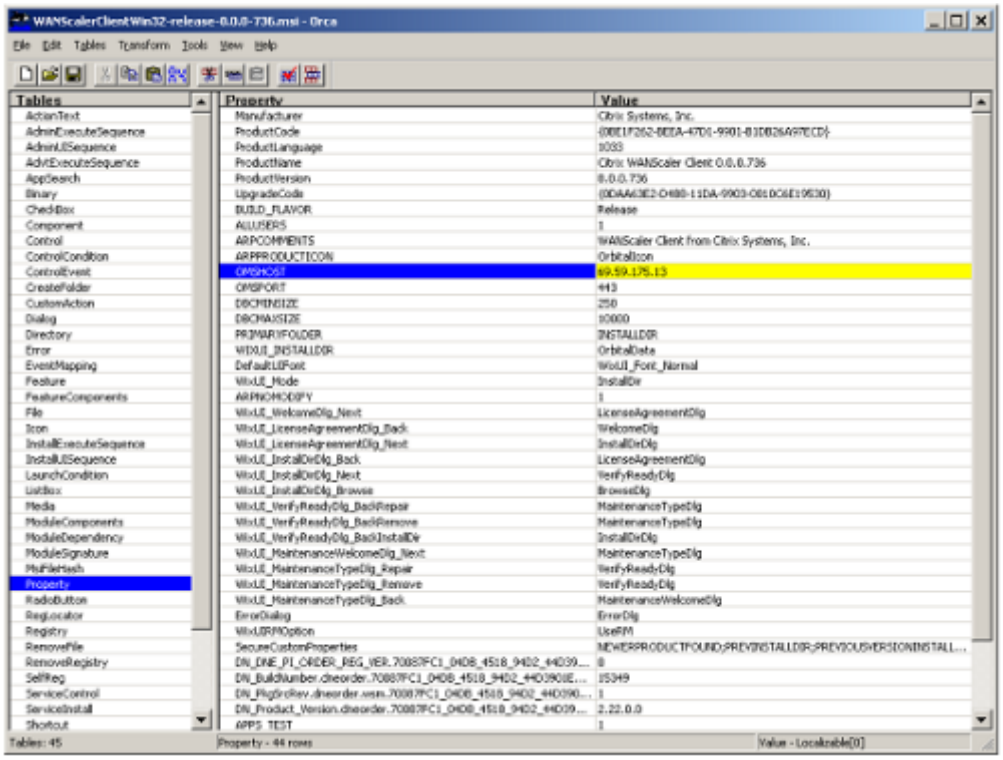
   詳しくは、tableを参照してください。

   a) [テーブル] メニューの [プロパティ] をクリックします。.MSI ファイルの編集可能なすべてのプロパティのリストが表示されます。次の表に示すパラメーターを編集します。パラメータを編集するには、そ

の値をダブルクリックし、新しい値を 入力して、**Enter** キーを押します。

詳しくは、tableを参照してください。

図 2: Orca でのパラメータの編集:



6. 完了したら、**[**ファイル：名前を付けて保存**]** コマンドを使用して、編集したファイルを新しいファイル名で保存します。たとえば、test.msi です。

これで、プラグインソフトウェアがカスタマイズされました。

> 注
>
> 一部のユーザーは、ファイルを 1MB に切り捨てる orca のバグを確認しています。保存したファイルのサイズを確認してください。切り捨てられている場合は、元のファイルのコピーを作成し、[保存] コマンドを使用して元のファイルを上書きします。

Orca を使用してアプライアンスリストをカスタマイズし、カスタマイズした MSI ファイルをユーザーに配布すると、ユーザーはソフトウェアのインストール時に構成情報を入力する必要がなくなります。

Windows にプラグインをデプロイする

April 19, 2021

WANOP クライアントプラグインは、他の Web 配布プログラムと同様にダウンロードしてインストールする実行可能な Microsoft インストーラー（MSI）ファイルです。このファイルは、Citrix.comWeb サイトの MyCitrix セクションから入手します。

> 注
>
> WANOP クライアントプラグインのユーザーインターフェイスは、それ自体を「CitrixAcceleration プラグインマネージャー」と呼びます。

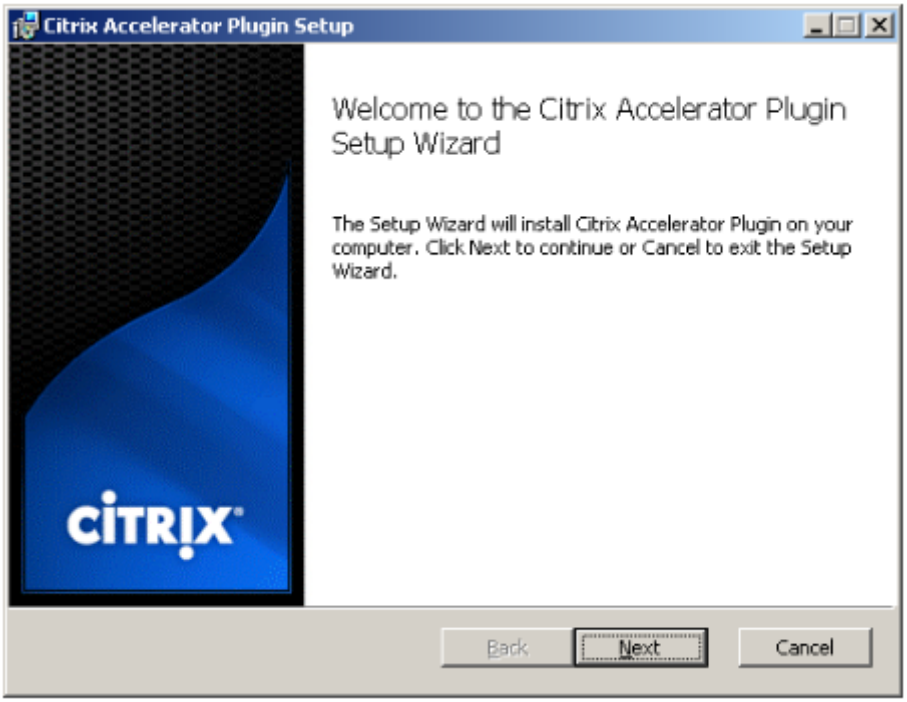
プラグインに必要な唯一のユーザー構成は、アプライアンスアドレスのリストです。このリストは、IP アドレスまたは DNS アドレスのコンマ区切りのリストで構成できます。2 つの形式を混在させることができます。リストがデフォルトでアプライアンスを指すように、配布ファイルをカスタマイズできます。インストールすると、操作は透過的になります。アクセラレーションされたサブネットへのトラフィックは適切なアプライアンスを介して送信され、他のすべてのトラフィックはサーバーに直接送信されます。ユーザーアプリケーションは、これが発生していることに気づいていません。

インストール

WANOP クライアントプラグインプラグインアクセラレータを Windows システムにインストールするには:

1. ザ・Repeater*.msi file はインストールファイルです。すべてのアプリケーションと開いている可能性のあるウィンドウをすべて閉じてから、通常の方法でインストーラーを起動します（ファイルウィンドウをダブルクリックするか、実行コマンドを使用します）。

   図 **1**: 初期インストール画面:



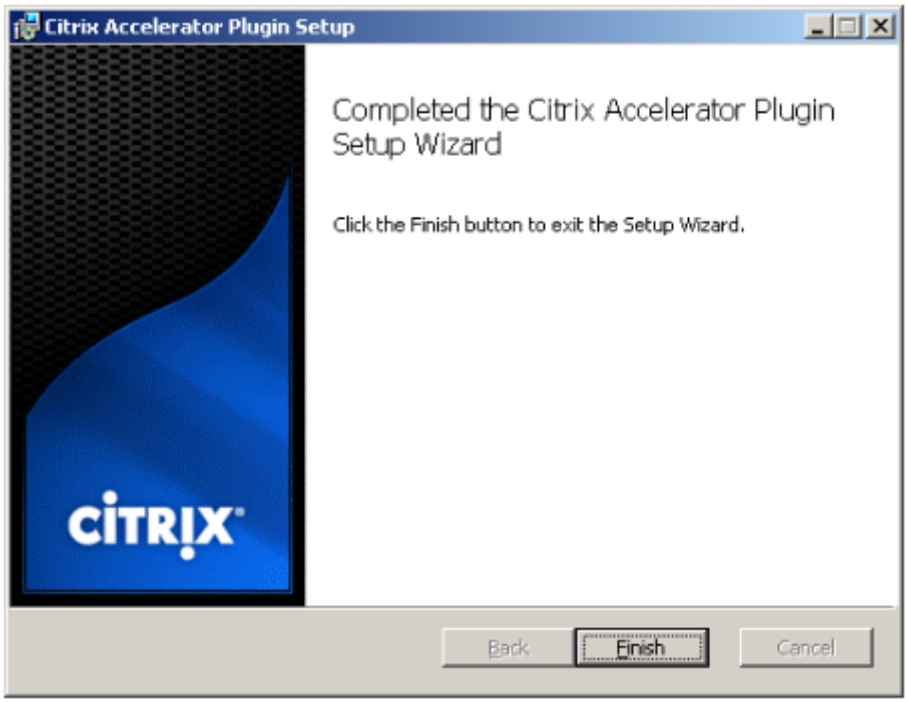
以下の手順は、インタラクティブインストール用です。サイレントインストールは、次のコマンドで実行できます。

msiexec/i client_msi_file /qn

2. インストールプログラムは、ソフトウェアをインストールする場所の入力を求めます。指定したディレクトリは、クライアントソフトウェアとディスクベースの圧縮履歴の両方に使用されます。これらを合わせると、最低 500MB のディスク容量が必要です。

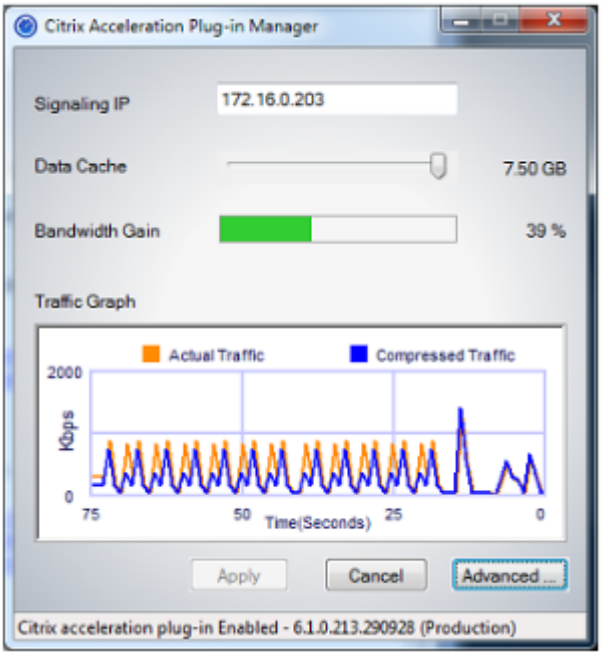
3. インストーラーが終了すると、システムを再起動するように求められる場合があります。再起動後、WANOP クライアントプラグインプラグインが自動的に起動します。

図 **2**: 最終インストール画面:



4. タスクバーの Accelerator アイコンを右クリックし、[**Manage Acceleration]** を選択して、Citrix Plug-in AcceleratorManager を起動します。

図 **3**: **Citrix Accelerator** プラグインマネージャー、初期（基本）ディスプレイ:



5. .MSI ファイルがユーザー向けにカスタマイズされていない場合は、シグナリングアドレスと圧縮に使用するディスク容量を指定します。

   - [アプライアンス：シグナリングアドレス] フィールドに、アプライアンスのシグナリング IP アドレスを入力します。プラグイン対応アプライアンスが複数ある場合は、それらすべてをコンマで区切ってリストします。IP アドレスまたは DNS アドレスのいずれかを使用できます。
   - [データキャッシュ] スライダーを使用して、圧縮に使用するディスク容量を選択します。多いほど良いです。利用可能なディスク容量が多ければ、7.5GB はそれほど多くありません。
   - [適用] を押します。

   これで、WANOP クライアントプラグインアクセラレータが実行されます。加速されたサブネットへの今後のすべての接続は加速されます

   プラグインの [AdvancedRules] タブで、[Acceleration Rules] リストに、各アプライアンスが Connected として表示され、各アプライアンスの Accelerated サブネットが Accelerated として表示されます。そうでない場合は、Signaling Addresses IP フィールドと一般的なネットワーク接続を確認してください。

プラグインのトラブルシューティング

プラグインのインストールは一般的にスムーズに進みます。そうでない場合は、次の問題を確認してください。

一般的な問題:

- システムを再起動しないと、WANOP クライアントプラグインが正しく実行されません。
- 高度に断片化されたディスクは、圧縮パフォーマンスを低下させる可能性があります。

- アクセラレーションの失敗（[診断] タブに加速された接続がリストされていない）は、通常、何かがアプライアンスとの通信を妨げていることを示します。プラグインの [構成：アクセラレーションルール] リストをチェックして、アプライアンスが正常に接続されていること、およびターゲットアドレスがアクセラレーションルールの 1 つに含まれていることを確認します。接続障害の一般的な原因は次のとおりです。
  - アプライアンスが実行されていないか、アクセラレーションが無効になっています。
  - ファイアウォールは、プラグインとアプライアンスの間のある時点で WANOP クライアントプラグイン TCP オプションを削除しています。
  - プラグインはサポートされていない VPN を使用しています。

確定的ネットワークエンハンサーロックエラー

まれに、プラグインをインストールしてコンピューターを再起動した後、次のエラーメッセージが 2 回表示されます。

確定的ネットワークエンハンサーのインストールでは、ロックされたリソースを解放するために、最初に再起動する必要があります。コンピュータを再起動した後、このインストールを再度実行してください。

これが発生した場合は、次のようにします。

1. に移動 Add/Remove WANOP クライアントプラグインが存在する場合は、プログラム して削除します。
2. コントロールパネル > ネットワークアダプタ > ローカルエリアでの接続 > プロパティで、Deterministic Network Enhancer のエントリを見つけ、チェックボックスをオフにして、[**OK**] をクリックします。(ネットワークアダプタが「ローカルエリア接続」以外の名前で呼び出されることがあります。)
3. コマンドウィンドウを開き、に移動します c:\windows\inf（または、Windows を非標準の場所にインストールした場合は同等のディレクトリ)。
4. 次のコマンドを入力します。

   find “dne2000.cat” oem*.inf
5. 最も大きい番号を見つける oem*.inf 一致する行を返したファイル（一致する行は CatalogFile = dne2000.cat）を編集します。例：

   notepad oem13.inf
6. セミコロンで始まる上部の 3 行を除くすべてを削除してから、ファイルを保存します。これにより、不適切または廃止された設定がすべてクリアされ、次のインストールではデフォルト値が使用されます。
7. インストールを再試行してください。

その他のインストールの問題

WANOP クライアントプラグインのインストールに関する問題は、通常、既存のネットワーク、ファイアウォール、またはウイルス対策ソフトウェアがインストールを妨害した結果です。通常、インストールが完了すると、それ以上の問題は発生しません。

インストールが失敗した場合は、次の手順を試してください。

1. プラグインインストールファイルがローカルシステムにコピーされていることを確認してください。
2. アクティブなものをすべて切断します VPN/remote ネットワーククライアント。
3. ファイアウォールとウイルス対策ソフトウェアを一時的に無効にします。
4. これのいくつかが難しい場合は、できることをしてください。
5. WANOP クライアントプラグインを再インストールします。
6. これが機能しない場合は、システムを再起動して再試行してください。

Citrix SD-WAN WANOP プラグイン GUI

April 19, 2021

WANOP クライアントプラグイン GUI は、**Citrix Accelerator** プラグイン アイコンを右クリックして **[**アクセラレーションの管理] を選択すると表示されます。GUI の基本画面が最初に表示されます。必要に応じて使用できる高度なディスプレイもあります。

基本表示

[基本] ページでは、次の 2 つのパラメーターを設定できます。

- Signaling Addresses フィールドは、プラグインが接続できる各アプライアンスの IP アドレスを指定します。アプライアンスを 1 つだけリストすることをお勧めしますが、コンマ区切りのリストを作成することもできます。これは順序付きリストであり、左端のアプライアンスが他のアプライアンスよりも優先されます。信号接続を確立できる左端のアプライアンスで加速が試行されます。DNS アドレスと IP アドレスの両方を使用できます。

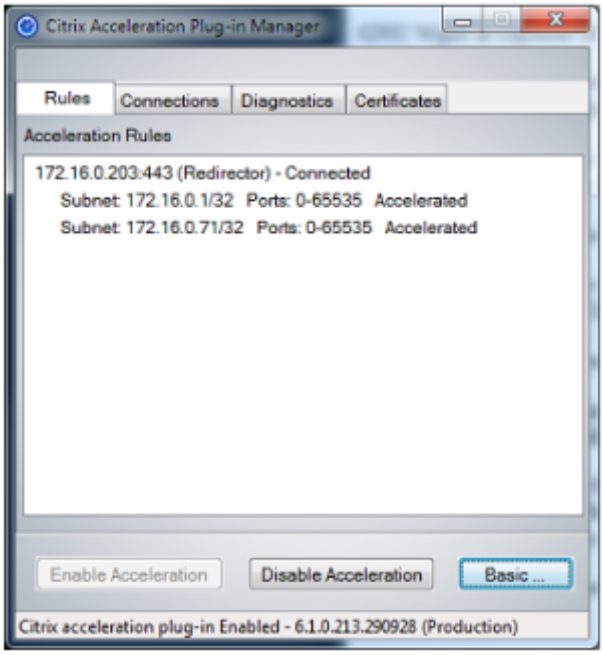
  例：10.200.33.200、ws.mycompany.com、ws2.mycompany.com

- データキャッシュスライダーは、プラグインのディスクベースの圧縮履歴に割り当てられるディスクスペースの量を調整します。多いほど良いです。

さらに、詳細表示に移動するためのボタンがあります。

高度な表示

[詳細設定] ページには、[ルール]、[接続]、[診断]、および [証明書] の 4 つのタブがあります。



ディスプレイの下部には、アクセラレーションを有効にしたり、アクセラレーションを無効にしたり、基本ページに戻ったりするためのボタンがあります。

[ルール] タブ

[ルール] タブには、アプライアンスからダウンロードされたアクセラレーションルールの簡略リストが表示されます。各リスト項目には、アプライアンスのシグナリングアドレスとポート、アクセラレーションモード（リダイレクタまたはトランスペアレント）、接続状態が表示され、その後にアプライアンスのルールの概要が表示されます。

[接続] タブ

[接続] タブには、さまざまなタイプの開いている接続の数が一覧表示されます。

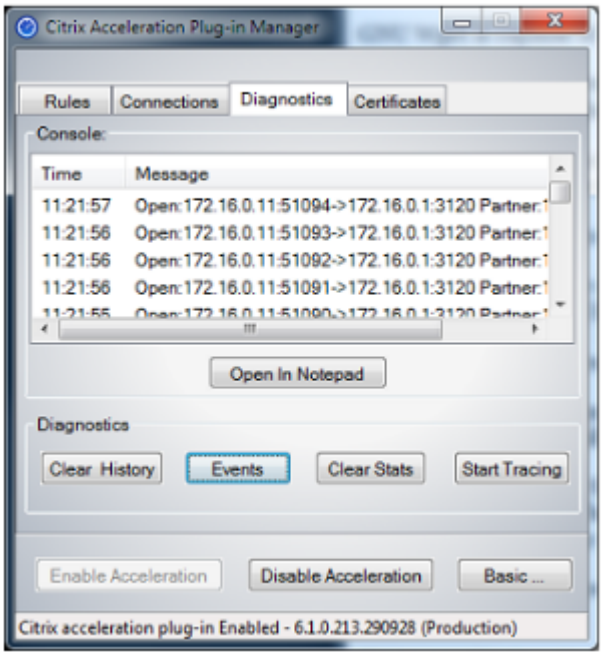
- 加速接続-WANOP クライアントプラグインプラグインとアプライアンスの間で開いている接続の数。この数には、アプライアンスごとに 1 つのシグナリング接続が含まれますが、高速化された CIFS 接続は含まれません。[詳細] をクリックすると、各接続の簡単な概要を示すウィンドウが開きます。([その他] ボタンはすべて、サポートと共有する場合に、ウィンドウ内の情報をクリップボードにコピーできます。)
- **Accelerated CIFS Connections**-CIFS（Windows ファイルシステム）サーバーとのオープンで高速化された接続の数。これは通常、マウントされたネットワークファイルシステムの数と同じです。[詳細] をクリックすると、高速接続の場合と同じ情報に加えて、CIFS 接続が WANOP クライアントプラグインの特別な CIFS 最適化で実行されている場合にアクティブを報告するステータスフィールドが表示されます。

- **Accelerated MAPI Connections-**開いている、加速された数 Outlook/Exchange 接続。
- 高速 **ICA** 接続：ICA または CGP プロトコルを使用したオープンで高速化された Citrix Virtual Apps and Desktops 接続の数。
- 加速されていない接続-加速されていない接続を開きます。[詳細] をクリックすると、接続が高速化されなかった理由の簡単な説明が表示されます。通常、その理由は、サービスポリシールールとして報告される宛先アドレスを高速化するアプライアンスがないためです。
- Opening/Closing 接続-完全に開いていないが、開いているか閉じている途中の接続（TCP「ハーフオープン」または「ハーフクローズ」接続）。[詳細] ボタンには、これらの接続に関する追加情報が表示されます。

[診断] タブ

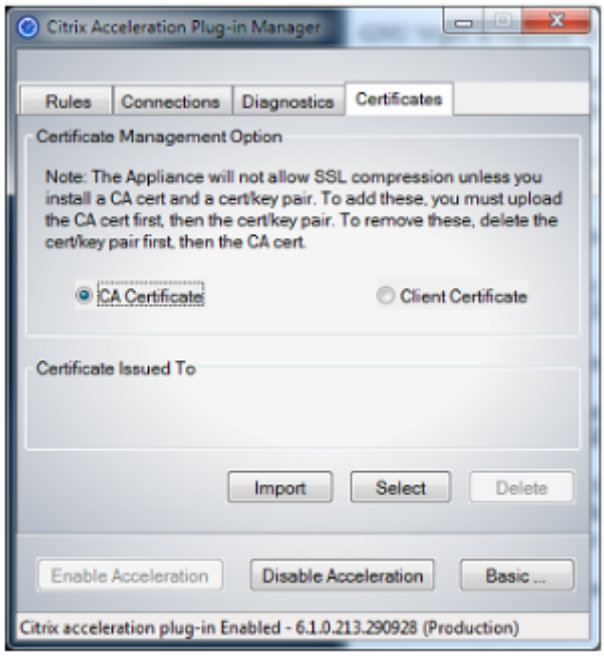
[診断] ページには、さまざまなカテゴリの接続数やその他の役立つ情報が報告されます。

- 開始 Tracing/Stop トレース-問題を報告した場合、Citrix の担当者は、問題を特定するために接続トレースを実行するように依頼する場合があります。このボタンは、トレースを開始および停止します。トレースを停止すると、ポップアップウィンドウにトレースファイルが表示されます。Citrix の担当者が推奨する方法でそれらを送信します。
- 履歴のクリア-この機能は使用しないでください。
- **Clear Statistics**-このボタンを押すと、[Performance] タブの統計情報がクリアされます。
- コンソール**-**最近のステータスメッセージ（主に接続を開くメッセージと接続を閉じるメッセージ）だけでなく、エラーやその他のステータスメッセージも表示されるスクロール可能なウィンドウ。



[証明書] タブ

[証明書] タブで、オプションのセキュアピアリング機能のセキュリティ資格情報をインストールできます。これらのセキュリティ資格情報の目的は、プラグインが信頼できるクライアントであるかどうかをアプライアンスが確認できるようにすることです。



CA 証明書と証明書とキーのペアをアップロードするには:

1. CA **CertificateManagement** を選択します。
2. ［インポート］をクリックします。
3. CA 証明書をアップロードします。証明書ファイルは、サポートされているファイルタイプ（.pem、.crt、.cer、または.spc）のいずれかを使用する必要があります。使用する証明書ストアを選択するように求めるダイアログボックスが表示され、キーワードのリストが表示される場合があります。リストの最初のキーワードを選択します。
4. [クライアント証明書の管理] を選択します。
5. ［インポート］をクリックします。
6. 証明書とキーのペアの形式を選択します（PKCS12 または PEM/DER).
7. 「送信」をクリックします。

> 注
>
> の場合 PEM/DER, 証明書とキー用に別々のアップロードボックスがあります。証明書とキーのペアが 1 つのファイルに結合されている場合は、ファイルを 2 回、各ボックスに 1 回指定します。

Citrix SD-WAN WANOP プラグインを更新します

April 19, 2021

新しいバージョンの WANOP クライアントプラグインをインストールするには、プラグインを初めてインストールするときに使用したのと同じ手順に従います。

WANOP クライアントプラグインをアンインストールします

WANOP クライアントプラグインをアンインストールするには、Windows の [プログラムの追加と削除] ユーティリティを使用します。WANOP クライアントプラグインは、現在インストールされているプログラムのリストに **Citrix AccelerationPlug-in** としてリストされています。それを選択し、[削除] をクリックします。

システムを再起動して、クライアントのアンインストールを完了します。

Citrix Virtual Apps and Desktops の高速化

April 19, 2021

> 注
>
> この説明では、*Virtual Apps* とは、ICA プロトコルストリームと CGP プロトコルストリームを指します。したがって、Virtual Apps について言われていることは、Virtual Desktops にも適用されます。

Virtual Apps/Virtual Desktops (ICA/CGP) アクセラレーションには、次の 3 つのコンポーネントがあります。

- 圧縮：アプライアンスは Virtual Apps クライアントおよびサーバーと連携して、対話型データ（キーボード/マウス/ディスプレイ/オーディオ）およびバッチデータ（印刷およびファイル転送）用に Virtual Apps のデータ・ストリームを圧縮します。この相互作用は透過的に行われ、アプライアンスの構成は必要ありません。古い Virtual Apps サーバー (リリース 4.x) では、以下に説明する少量の構成が必要です。
- マルチストリーム ICA-圧縮に加えて、Citrix SD-WAN WANOP アプライアンスは新しいマルチストリーム ICA プロトコルをサポートします。このプロトコルでは、同じ接続ですべての優先順位を多重化する代わりに、最大 4 つの接続が異なる ICA 優先順位に使用されます。このアプローチにより、特にアプライアンスのトラフィックシェーピングと組み合わせると、インタラクティブタスクの応答性が向上します。
- トラフィックシェーピング：Citrix SD-WAN WANOP トラフィックシェーパーは、Virtual Apps データプロトコルのプライオリティビットを使用して、接続の優先度をリアルタイムで調整し、各接続の帯域幅共有と現時点で接続を送信しているものと一致させます。

> 注
>
> マルチストリーム ICA はデフォルトで無効になっています。機能ページで有効にできます。マルチストリーム ICA および AutoQoS では、セッションの信頼性を有効にする必要があります。

Citrix Virtual Apps and Desktops リリース 7.0 以降の ICA 接続を最適化するために、Citrix SD-WAN WANOP アプライアンスは、Citrix Receiver for Chrome リリース 1.4 以降、および Citrix Receiver for HTML5 リリース 1.4 以降をサポートしています。

からの **HDX** トランスポートプロトコル UDP/EDT TCP へ-特定のネットワーク条件では、UDP/EDT HDX トラフィックを配信するための最適化されたプロトコルとして使用することはできません。プロトコルを TCP に変更して、WANOP が 提供できるようにすることができます。

- Compression/DDup 利点
- 可視性（ローカルレポートと HDX Insight）

WANOP は、EDT トラフィックをブロックし、セッションを TCP に強制することができます。セッションの開始時に、Citrix Receiver は TCP と EDT の両方でセッションを開始します。EDT セッションが確立されていない場合は、TCP セッションが使用されます。WANOP GUI は、機能ページで TCP プロトコルでセッションを強制するオプションを提供します。

Virtual Apps アクセラレーションの構成

April 19, 2021

Virtual Apps のアクセラレーションは、Virtual Apps 内の ICA プロトコルと CGP プロトコルの両方に適用されます。Citrix SD-WAN WANOP アプライアンス、Virtual Apps サーバー、および Virtual Apps クライアントは、Virtual Apps 接続の連携高速化を実現し、Virtual Apps のみと比較して大幅に高速化します。この協力には、3 つのコンポーネントすべての最新バージョンが必要です。

Virtual Apps 圧縮は、対話型チャネル (マウス、キーボード、画面データなど) のメモリベースの圧縮と、バルクタスク用のディスクベースの圧縮 (ファイル転送や印刷ジョブなど) を動的に切り替えます。圧縮履歴がいっぱいになると圧縮率が高くなり、新しいデータと照合できるデータの量が増えます。Virtual Apps の圧縮は、サポートされていない Virtual Apps の数倍のデータ削減を実現します。同じドキュメントの連続したバージョンの印刷や保存など、繰り返しの一括転送では 50:1 を超えることがよくあります。

Virtual Apps の圧縮は、ユーザーが互いに干渉するのを防ぐことで、輻輳なしで高いリンク使用率を実現します。

Virtual Apps のアクセラレーションを有効にするには

1. ICA サービスクラスポリシーを確認してください。[Configuration：Service Classes] ページで、ICA サービスクラスの [Acceleration] 列にディスクが表示され、[TrafficShaping] 列に ICAPriorities が表示されま

す。そうでない場合は、サービスクラス定義を編集します。

2. Virtual Apps 4.x サーバーとクライアントを更新します。(Virtual Apps 5.0 以降では不要)。Hotfix Rollup Pack PSE450W2K3R03（ベータ版）以降で Presentation Server4.5 を使用します。このリリースには、次のサーバーおよびクライアントソフトウェアが含まれています。Virtual Apps 圧縮では、どちらもインストールする必要があります。

   a) サーバーパッケージ PSE450R03W2K3WS.msp 以降。

   b) クライアントバージョン 11.0.0.5357 以降。

3. Virtual Desktops サーバーおよびクライアントをリリース 4.0 以降に更新します。

4. Virtual Apps サーバーのレジストリ設定を確認します。(Virtual Apps 5.0 以降では不要)Virtual Apps サーバーで、次の設定を確認し、必要に応じて修正または作成します。

   ```
   pre codeblock HKLM\System\CurrentControlSet\Control\Citrix\
   WanScaler\EnableForSecureIca = 1 HKLM\System\CurrentControlSet
   \Control\Citrix\WanScaler\EnableWanScalerOptimization = 1 HKLM\
   System\CurrentControlSet\Control\Citrix\WanScaler\UchBehavior = 2
   ```

   これらはすべて DWORD 値です。

5. 更新された Citrix SD-WAN WANOP を通過する、更新された Virtual Apps クライアントとサーバー間の Virtual Apps 接続を開いて使用します。デフォルトでは、これらのセッションは CGP を使用します。ICA の場合、クライアントの Citrix ProgramNeighborhood で [カスタム ICA 接続] チェックボックスをオフにします。次に、接続アイコンを右クリックして、[プロパティ] に移動します > [オプション] をクリックし、[セッションの信頼性を有効にする] チェックボックスをクリックします。マルチストリーム ICA および AutoQoS では、セッションの信頼性を有効にする必要があります。

6. 加速を確認します。

   アクセラレーションリンクを介して Virtual Apps セッションを開始すると、アクセラレーションされた ICA 接続がアプライアンスの［監視：接続］ページに表示されます。より大きい圧縮比 1:1 圧縮が行われていることを示します。

HTML5 用に Citrix Receiver を最適化する

December 16, 2022

動的コンテンツを提供する必要のあるアプリケーションは、HTML5WebSocket で動作します。Citrix Receiver for Chrome および Citrix Receiver for HTML5 は、HTML5 WebSocket をサポートするアプリケーションです。これらのアプリケーションは、HTML5 WebSockets をサポートする最新の Web ブラウザと統合できるため、Virtual Desktops へのアクセスが簡素化されています。

> 注
>
> この機能を使用するために、アプライアンスの構成を変更する必要はありません。

Citrix SD-WAN WANOP アプライアンスが Citrix Receiver for HTML5 を最適化する方法

一般的なブランチオフィスおよびデータセンターの設定では、仮想デスクトップエージェント（VDA）などの共有リソースがデータセンター内の Citrix Hypervisor サーバーにインストールされます。ブランチオフィスのクライアントは、Citrix Receiver を使用してネットワーク経由でこれらの共有リソースにアクセスします。

一般的なブランチオフィスおよびデータセンターの設定では、仮想デスクトップエージェント（VDA）などの共有リソースがデータセンター内の Citrix Hypervisor サーバーにインストールされます。ブランチオフィスのクライアントは、Citrix Receiver を使用してネットワーク経由でこれらの共有リソースにアクセスします。

HTML に準拠しているため、VDA はポート 8008 で実行される WebSocket リスナーを使用します。アプリケーションにアクセスすると、クライアントはポート 8008 で TCP 接続を開始し、それを使用してサーバーに HTTP 要求を送信し、接続をアップグレードして WebSocket プロトコルを使用します。クライアントが WebSocket 接続を VDA とネゴシエートした後、Independent Computing Architecture（ICA）ネゴシエーションが開始され、クライアントとサーバーは ICA over HTML5 を使用してデータを交換します。クライアントとサーバー間で交換されるメッセージのシーケンスの詳細については、「クライアントとサーバー間で交換されるメッセージ」を参照してください。

クライアントとサーバー間の接続が確立された後、Citrix SD-WAN WANOP アプライアンスは、ネットワーク上のトラフィックを高速化し、Citrix Receiver for HTML5 を使用して Web ページやその他のアプリケーションを高速化することで接続の最適化を開始します。HTML5 接続用に Citrix Receiver を最適化する機能は、HTTP アクセラレーションに似ています。

> 注
>
> - INC の詳細については、HTML5 のしくみを参照してください。
> - Citrix Receiver for Windows 5 について詳しくは、Receiver for HTML5を参照してください。
> - Receiver for HTML のシステム要件について詳しくは、「システム要件」を参照してください。

Citrix SD-WAN WANOP アプライアンスを構成して Citrix Receiver for HTML5 を最適化する

HTML5 接続用の Citrix Receiver の最適化は、構成ゼロの機能です。アプライアンスの構成を変更する必要はありません。Citrix SD-WAN WANOP ソフトウェアをリリース CB 7.3.1 以降にアップグレードすると、アプライアンスに alt-http アプリケーション分類子が作成され、このアプリケーション分類子はポート 8008（Virtual Desktops のデフォルト値）にマップされます。アプライアンスのソフトウェアをアップグレードするとすぐに、Citrix Receiver for HTML5 を使用するネイティブ Chrome 接続を最適化する準備が整います。

Citrix Receiver for HTML5 を介した接続に SSL 暗号化を使用している場合、接続は ICA over SSL を使用します。Citrix Receiver for HTML5 で ICA over SSL アクセラレーションを有効にするには、標準の SSL アクセラレーシ

ョンを構成する必要があります。これには、サービスクラスの適切な宛先 IP アドレスと SSL プロファイルマッピングが含まれます。アプライアンスを ICA プロキシモードで展開することを計画している場合は、StoreFrontVIP アドレスを StoreFront 証明書にマップする必要があります。同様に、アプライアンスをエンドツーエンドの SSL 暗号化展開モードで展開する場合は、VDAIP アドレスを VDA 証明書にマップする必要があります。

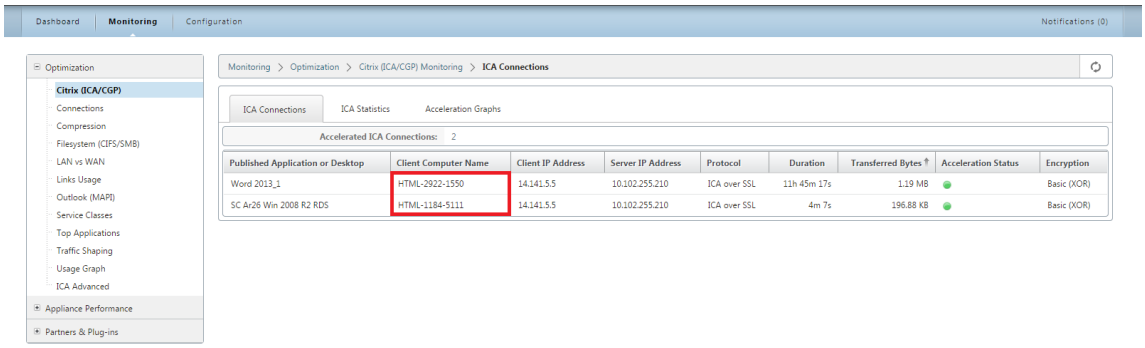
> 警告
>
> alt-http アプリケーションのポート番号を他のポート番号に変更しないでください。このアプリケーション分類子を削除するか、変更する必要がある場合は、ポート 8008 を HTTP アプリケーション分類子に追加する必要があります。

HTML5 接続用の **Citrix Receiver** を確認する

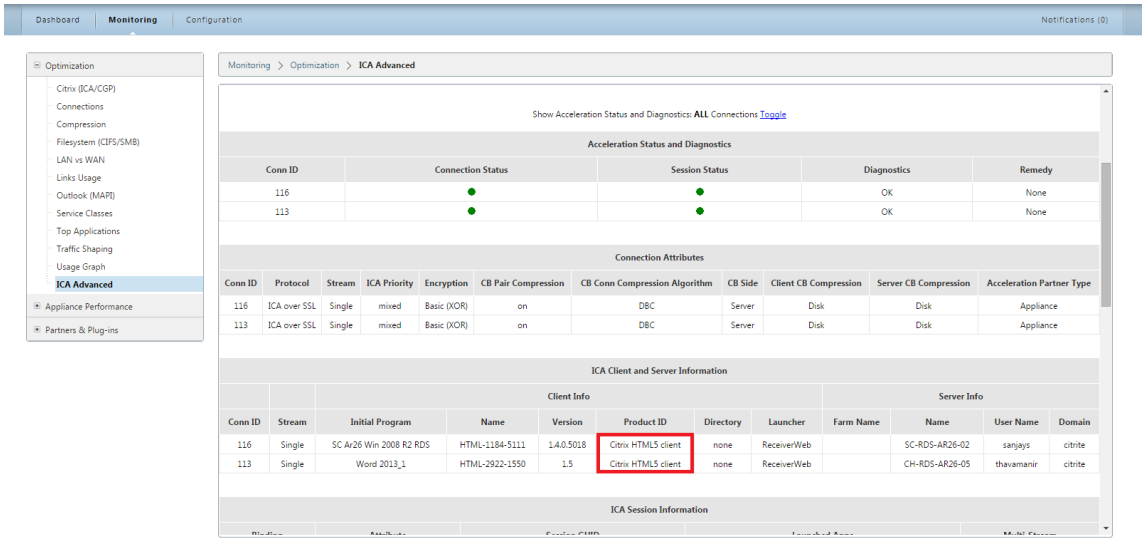
アプライアンスが HTML5 接続用に Citrix Receiver を最適化していることを確認するために、接続が Citrix にリストされているかどうかを確認できます (ICA/CGP) および ICAAdvanced モニタリングページ。監視ページに HTML5 接続が存在することは、アプライアンスが Citrix Receiver を HTML5 接続用に最適化していることを示しています。

Citrix SD-WAN WANOP アプライアンスで **Citrix Receiver for HTML5** 接続を確認するには:

1. モニタリング > 最適化 > **Citrix** (ICA/CGP) ページに移動します。
2. [**ICA** 接続] タブで、HTML5 接続が一覧表示されていることを確認します。次のスクリーンショットに示すように、HTML5 接続は、[クライアントコンピューター名] 列のプレフィックスとして HTML を使用して表示されます。



3. モニタリング **>** 最適化 **> ICA** 詳細ページに移動します。
4. [接続 情報] タブで、[ICA クライアントおよびサーバー情報] セクションまで下にスクロールします。次のスクリーンショットに示すように、HTML5 接続のエントリでは、[製品 ID] 列に CitrixHTML5 クライアントがあります。

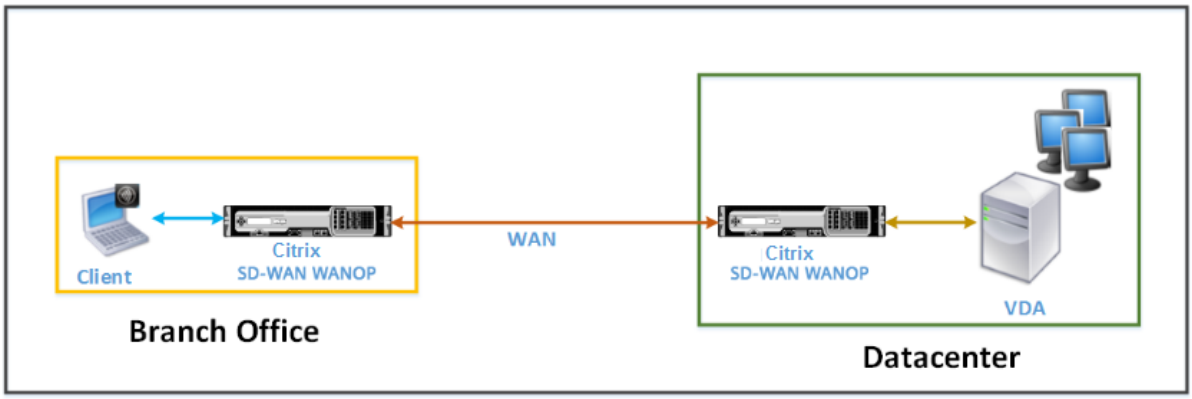


展開モード

April 19, 2021

典型的な Citrix SD-WAN WANOP 展開では、Citrix SD-WAN WANOP アプライアンスはブランチオフィスとデータセンター間でペアになっています。VDA などの共有リソースをデータセンターにインストールします。次の図に示すように、さまざまなブランチオフィスのクライアントは、Citrix Receiver を使用してデータセンターリソースにアクセスします。

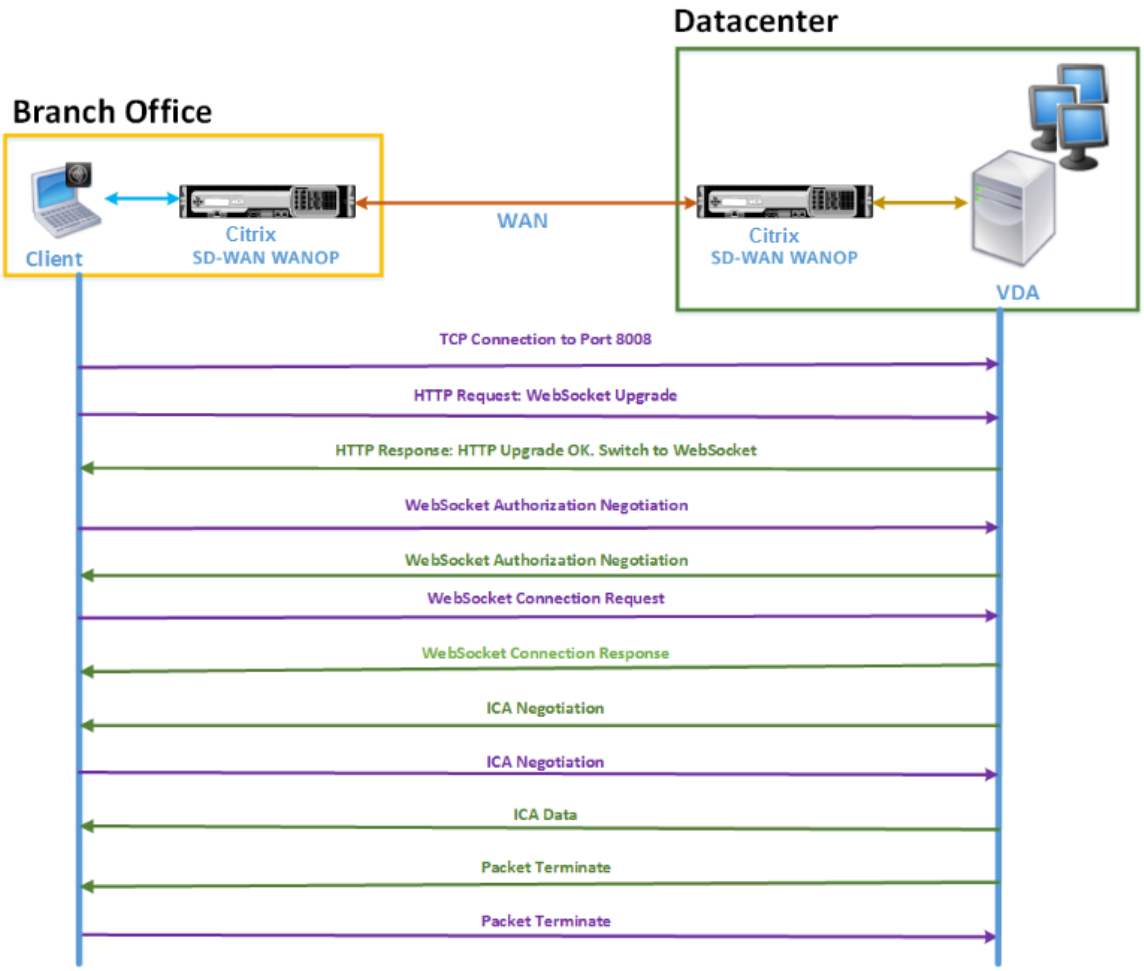
典型的な Citrix SD-WAN WANOP 展開トポロジ



クライアントは、Citrix Receiver for HTML5 などの Citrix Receiver ソフトウェア製品をローカルコンピューターにインストールし、それを使用してデータセンターのリソースにアクセスします。Citrix SD-WAN WANOP アプライアンスのペアを介した接続が最適化されます。

クライアントとサーバー間で交換されるメッセージを理解する

他のタイプのネットワーク接続と同様に、Citrix Receiver for HTML5 を使用するクライアントはサーバーとさまざまなメッセージを交換します。次の図は、クライアントとサーバー間で接続が確立されたときの、クライアントとサーバー間のメッセージの一般的なフローを示しています。



上の図に示すように、ブランチオフィスのクライアントがデータセンターサーバーリソースにアクセスする場合、次の一連のメッセージがクライアントとサーバー間で交換されます。

1. クライアントは Citrix Receiver for HTML5 を使用して、TCP 接続要求をポート 8008 で VDA に送信します。
2. TCP 接続を確立した後、クライアントは WebSocket アップグレード要求を VDA に送信します。
3. VDA はアップグレード要求に応答し、WebSocket プロトコルに切り替えます。
4. クライアントと VDA は WebSocket 認証をネゴシエートします。
5. クライアントは WebSocket 接続要求を VDA に送信します。
6. VDA は WebSocket 接続要求に応答します。

7. VDA は、クライアントとの ICA ネゴシエーションを開始します。
8. ICA ネゴシエーション後、VDA は ICA データの送信を開始します。
9. VDA はパケット終了メッセージを送信します。
10. クライアントはパケット終了メッセージで応答します。

> 注
>
> 上記の例は、WebSocket を介して ICA と交換されるサンプルメッセージを示しています。Common Gateway Protocol (CGP) を介して ICA を使用している場合、クライアントとサーバーは WebSocket ではなく CGP をネゴシエートします。ただし、ICA over TCP の場合、クライアントとサーバーは ICA をネゴシエートします。

ネットワークに展開したコンポーネントに応じて、接続はさまざまなポイントで終了します。前の図は、ネットワーク上に追加のコンポーネントが展開されていないトポロジを表しています。その結果、クライアントはポート 8008 で VDA と直接通信します。ただし、Citrix Gateway などのゲートウェイをデータセンターにインストールしている場合は、ゲートウェイとの接続が確立され、VDA がプロキシされます。ゲートウェイが WebSocket 承認をネゴシエートするまで、VDA との通信はありません。ゲートウェイは WebSocket 承認をネゴシエートした後、VDA との接続を開きます。その後、ゲートウェイは仲介者として機能し、クライアントから VDA にメッセージを渡します。

同様に、クライアントにインストールされた Citrix ゲートウェイプラグインとデータセンターにインストールされた Citrix Gateway の間に VPN トンネルが作成された場合、ゲートウェイは TCP 接続を確立するとすぐにすべてのクライアントメッセージを VDA に透過的に転送します。

> 注
>
> エンドツーエンドの SSL 暗号化を必要とする接続を最適化するために、VDA のポート 443 で TCP 接続が確立されます。

サポートされている展開モード

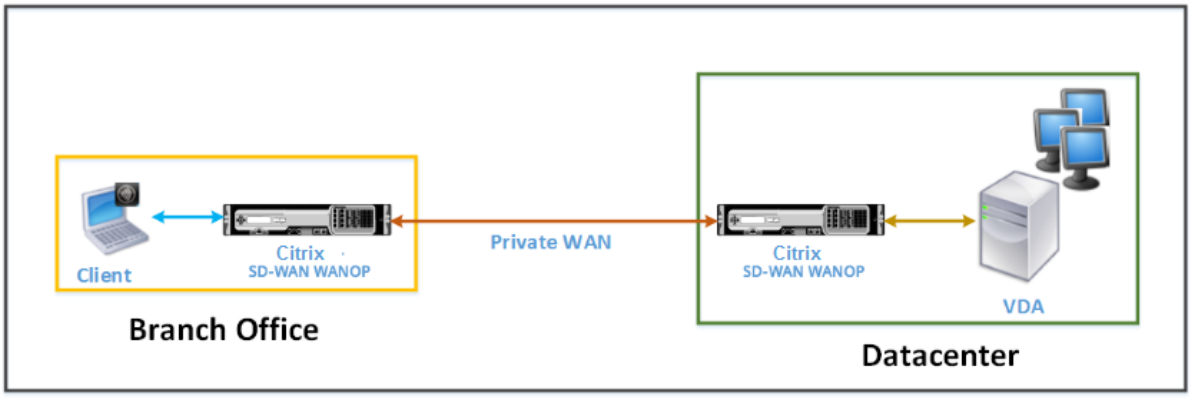
Citrix Receiver for HTML5 を最適化するために Citrix SD-WAN WANOP アプライアンスを構成する場合、ネットワーク要件に応じて、次の展開モードのいずれかを検討できます。HTML5 接続用に Citrix Receiver を最適化するために、Citrix SD-WAN WANOP アプライアンスは次の展開モードをサポートしています。

- 直接アクセス
- エンドツーエンド SSL 暗号化による直接アクセス
- ICA プロキシモード
- エンドツーエンド SSL 暗号化を使用した ICA プロキシモード
- フル仮想プライベートネットワーク（VPN）モード
- エンドツーエンド SSL 暗号化を備えた完全仮想プライベートネットワーク（VPN）モード

直接アクセス:

次の図は、直接アクセスモードでクライアントにインストールされた Citrix Receiver for HTML5 の展開トポロジを示しています。

直接アクセスモードで展開された Citrix SD-WAN WANOP アプライアンス



ダイレクトアクセスモードでは、Citrix SD-WAN WANOP アプライアンスのペアがブランチオフィスとデータセンターにインラインモードでインストールされます。クライアントは、プライベート WAN を介して Citrix Receiver for HTML5 を介して VDA リソースにアクセスします。クライアントから VDA リソースへの接続は、ICA レベルの暗号化を使用して保護されます。クライアントと VDA の間で交換されるメッセージについては、「クライアントとサーバーの間で交換されるメッセージについて」で説明されています。

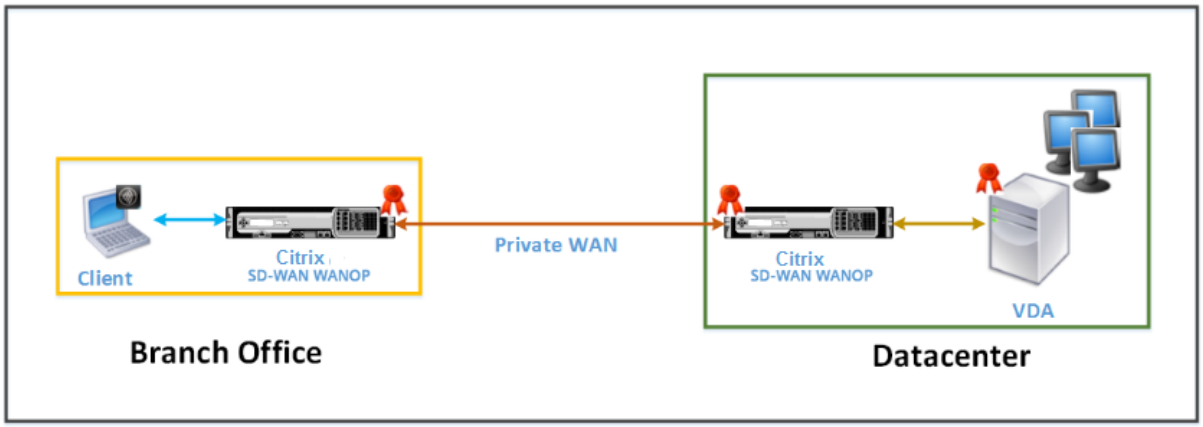
クライアントと VDA データセンターの間にインストールされた Citrix SD-WAN WANOP アプライアンスは、それらの間に確立された HTML5 接続用に Citrix Receiver を最適化します。

直接アクセス展開は、クライアントが Citrix Gateway やその他のファイアウォールを使用せずに接続する企業イントラネットに適しています。Citrix SD-WAN WANOP アプライアンスがインラインモードで展開され、プライベート WAN からのクライアントが VDA リソースに接続する場合は、直接アクセスを使用してセットアップを展開します。

エンドツーエンド **SSL** 暗号化による直接アクセス:

次の図は、エンドツーエンドの SSL 暗号化で保護されたダイレクトアクセスモードでクライアントにインストールされた Citrix Receiver for HTML5 の展開トポロジを示しています。

エンドツーエンドの SSL 暗号化で保護されたダイレクトアクセスモードで展開された Citrix SD-WAN WANOP アプライアンス



エンドツーエンド SSL 暗号化モードでの直接アクセスは直接アクセスモードに似ていますが、クライアントと VDA リソース間の接続が SSL 暗号化によって保護され、接続にポート 8008 ではなくポート 443 を使用する点が異なります。

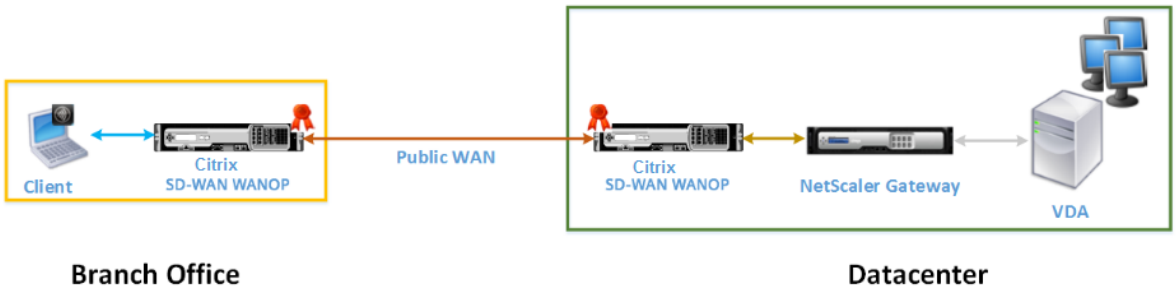
この展開では、Citrix SD-WAN WANOP アプライアンスのペア間の通信は、2 つのアプライアンスを保護されたパートナーにすることで保護されます。この展開は、クライアントと VDA リソース間の接続が SSL 暗号化によって保護されている企業ネットワークに適しています。

> 注
>
> 安全なパートナーを作成するには、アプライアンスで適切な証明書を構成する必要があります。安全なパートナー関係の詳細については、安全なピアリングを参照してください。

ICA プロキシモード:

次の図は、ICA プロキシモードでクライアントにインストールされた Citrix Receiver for HTML5 の展開トポロジを示しています。

ICA プロキシモードで展開された Citrix SD-WAN WANOP アプライアンス



ICA プロキシモードでは、Citrix SD-WAN WANOP アプライアンスのペアがブランチオフィスとデータセンターにインラインモードでインストールされます。さらに、VDA をプロキシする Citrix Gateway をデータセンターにインストールします。クライアントは、パブリック WAN を介して Citrix Receiver for HTML5 を介して VDA リソースにアクセスします。ゲートウェイは VDA をプロキシするため、2 つの接続が確立されます。クライアントと Citrix

Gateway 間の SSL 接続と、Citrix Gateway と VDA 間の ICA で保護された接続です。Citrix Gateway は、クライアントに代わって VDA リソースとの接続を確立します。ゲートウェイから VDA リソースへの接続は、ICA レベルでの暗号化によって保護されます。

クライアントと VDA の間で交換されるメッセージについては、「クライアントとサーバーの間で交換されるメッセージについて」で説明されています。ただし、この場合、接続は Citrix Gateway で終了します。ゲートウェイは VDA をプロキシし、ゲートウェイが WebSocket 承認をネゴシエートした後にのみ VDA への接続を開きます。次に、ゲートウェイはクライアントから VDA に、またはその逆にメッセージを透過的に渡します。

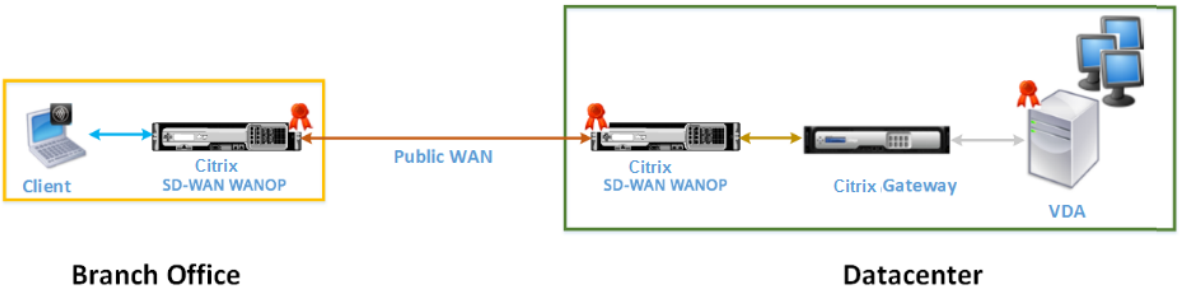
ユーザーがパブリック WAN から VDA リソースにアクセスすることを期待している場合は、ICA プロキシモードの設定を展開することを検討できます。

> 注
>
> 安全なパートナーを作成するには、アプライアンスで適切な証明書を構成する必要があります。安全なパートナー関係の詳細については、安全なピアリングを参照してください。

エンドツーエンド **SSL** 暗号化を使用した **ICA** プロキシモード:

次の図は、エンドツーエンドの SSL 暗号化で保護された ICA プロキシモードでクライアントにインストールされた Citrix Receiver for HTML5 の展開トポロジを示しています。

エンドツーエンドの SSL 暗号化で保護された ICA プロキシモードで展開された Citrix SD-WAN WANOP アプライアンス



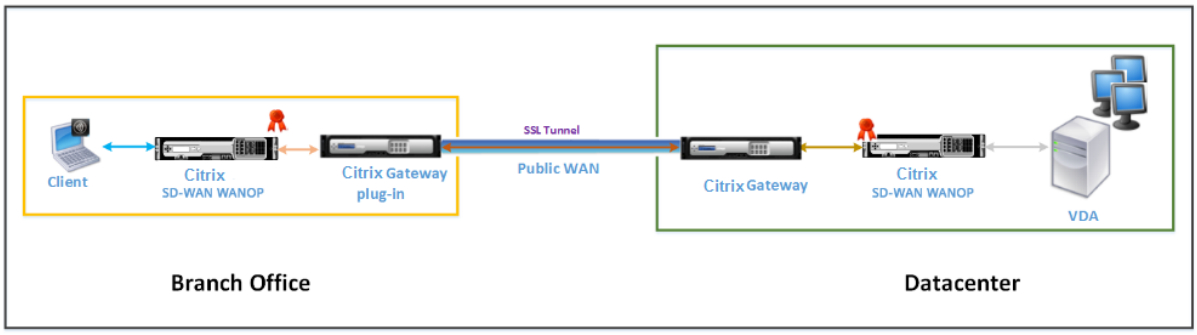
エンドツーエンド SSL 暗号化モードの ICA プロキシモードは、通常の ICA プロキシモードと似ていますが、Citrix Gateway と VDA 間の接続が、ICA で保護された接続を使用する代わりに SSL 暗号化によって保護される点が異なります。このシナリオでは、Citrix SD-WAN WANOP アプライアンスと VDA に適切な証明書をインストールする必要があります。Citrix Gateway と VDA 間の接続では、通常の ICA プロキシモードの場合と同様に、ポート 8008 ではなくポート 443 が使用されます。

この展開は、Citrix Gateway と VDA 間の接続を含め、クライアントと VDA 間のエンドツーエンド通信を保護する必要があるネットワークに適しています。

フル仮想プライベートネットワーク（**VPN**）モード:

次の図は、完全な仮想プライベートネットワーク（VPN）モードでクライアントにインストールされた Citrix Receiver for HTML5 の展開トポロジを示しています。

VPN モードで展開された Citrix SD-WAN WANOP アプライアンス



フル VPN モードでは、Citrix SD-WAN WANOP アプライアンスのペアがブランチオフィスとデータセンターにインラインモードでインストールされます。HTML5 用の Citrix Receiver に加えて、クライアントに Citrix Gateway プラグインをインストールし、データセンターの外部ネットワークにインターフェイスする Citrix Gateway をインストールします。クライアントの Citrix Gateway プラグインとデータセンターの Citrix Gateway は、接続を確立するときにネットワーク上に SSL トンネルまたは VPN を作成します。その結果、クライアントは VDA リソースに直接安全にアクセスでき、Citrix SD-WAN WANOP アプライアンスを介した透過的な接続が可能になります。クライアント接続が Citrix Gateway で終了すると、ゲートウェイは VDA のポート 8008 への透過的な接続を開きます。

クライアントと VDA の間で交換されるメッセージについては、「クライアントとサーバーの間で交換されるメッセージについて」セクションで説明されています。ただし、この場合、接続は Citrix Gateway で終了します。ゲートウェイは VDA をプロキシし、ポート 8008 で VDA への透過的な接続を開き、クライアントから VDA へ、またはその逆にすべてのメッセージを透過的に渡します。

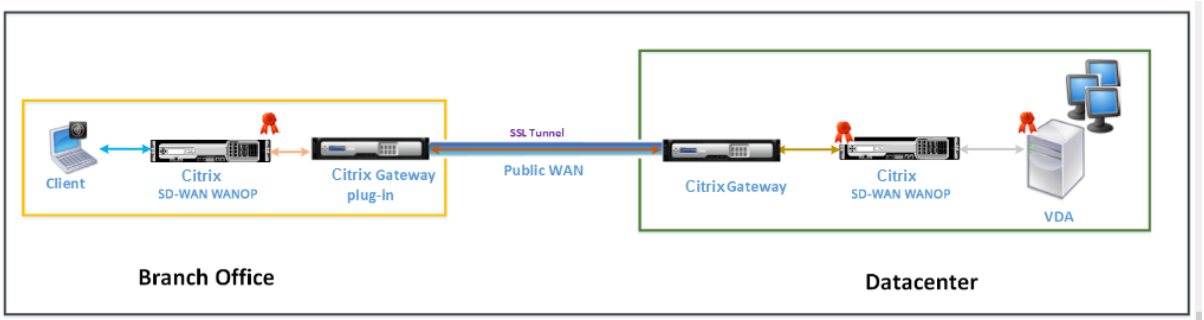
Citrix SD-WAN WANOP プラグインを使用すると、クライアントの場所に関係なく、クライアントはリソースにアクセスできます。クライアントがデスクトップ以外の場所から VDA リソースにアクセスする必要があると予想される場合は、セットアップを完全仮想プライベートネットワーク（VPN）モードで展開できます。

この展開は、従業員が出張中にリソースにアクセスすることを期待している組織に適しています。

エンドツーエンド **SSL** 暗号化を備えた完全仮想プライベートネットワーク（**VPN**）モード:

次の図は、エンドツーエンドの SSL 暗号化で保護されたフル VPN モードでクライアントにインストールされた Citrix Receiver for HTML5 の展開トポロジを示しています。

エンドツーエンドの SSL 暗号化で保護された VPN モードで展開された Citrix SD-WAN WANOP アプライアンス



エンドツーエンドの SSL 暗号化展開を備えたフルバーチャルプライベートネットワーク（VPN）モードは、通常のフル VPN モードと似ていますが、Citrix Gateway と VDA 間の通信が SSL 暗号化によって保護され、ポート 8008 ではなくポート 443 を使用する点が異なります。

この展開は、出張中の従業員がアクセスするリソースに対してエンドツーエンドの SSL 暗号化を必要とする組織に適しています。

適応型トランスポートの相互運用性

April 19, 2021

アダプティブトランスポートは、Citrix Virtual Apps and Desktops のデータ転送メカニズムです。高速で拡張性が高く、アプリケーションの対話機能が向上し、厳しい長距離の WAN とインターネット接続でのインタラクティブ性を高めます。アダプティブトランスポートでは、サーバーの高スケーラビリティと帯域幅の使用効率が維持されます。アダプティブトランスポートを使用すると、ICA 仮想チャネルはネットワーク状況の変化に自動的に対応します。Enlightened Data Transport（EDT）と呼ばれる Citrix プロトコルと TCP との間で、基になるプロトコルをインテリジェントに切り替えて、最適なパフォーマンスを実現します。デフォルトでは、アダプティブトランスポートが有効になっており、可能な場合は EDT が使用され、TCP にフォールバックされます。

Citrix SD-WAN WANOP は、URL ベースのビデオキャッシングを含む、セッション間のトークン化された圧縮（データ重複排除）を提供します。オフィスの場所にいる 2 人以上の人が同じクライアントフェッチビデオを視聴したり、同じファイルやドキュメントのかなりの部分を転送または印刷したりすると、帯域幅が大幅に削減されます。さらに、支社にあるアプライアンス上で ICA データ削減および印刷ジョブ圧縮プロセスを実行することにより、WANOP により VDA サーバーの CPU 負荷を軽減し、Citrix Virtual Apps and Desktops サーバーでより高いスケーラビリティを実現します。

TCP がデータトランスポートプロトコルとして使用される場合、Citrix SD-WAN WANOP は上記の最適化をサポートします。ネットワーク接続で Citrix SD-WAN WANOP を使用する場合は、TCP を選択し、EDT を無効にします。TCP フロー制御と輻輳制御を使用することにより、Citrix SD-WAN WANOP は、高遅延と中程度のパケット損失で EDT と同等の双方向性を保証します。

Citrix Virtual Apps and Desktops でのアダプティブトランスポートの構成については、アダプティブトランスポートを参照してください。

Citrix Hypervisor 6.5 のアップグレード

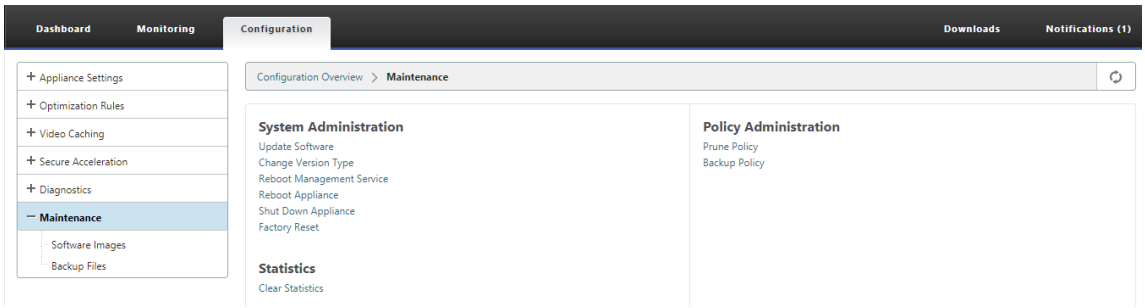
April 19, 2021

> 重要
>
> **Citrix Hypervisor** バージョン **6.5** にアップグレードするには、アプライアンスで **Citrix SD-WAN WANOP** ソフトウェアリリース **9.0.x** 以降が実行されている必要があります。
>
> 注
>
> アップグレードの問題を防ぐために、アプライアンスがリリース 9.0.x より前のソフトウェアバージョンで実行されている場合は、アップグレードを試みないでください。

Citrix Hypervisor 6.5 にアップグレードする方法

SD-WAN WANOP アプライアンスで Citrix Hypervisor 6.5 にアップグレードするには、アプライアンスでソフトウェアリリースバージョン 9.0.x 以降が実行されていることを確認します。アプライアンスが古いソフトウェアリリースバージョンを実行している場合は、最初に最新のソフトウェアリリースバージョンにアップグレードしてください。

1. Citrix SD-WAN WANOP GUI で、[構成]> メンテナンス > ソフトウェアを更新に移動します。*ns-sdw-wo-*をダウンロード < Build_No>.upg アプライアンスをアップグレードするためのファイル。

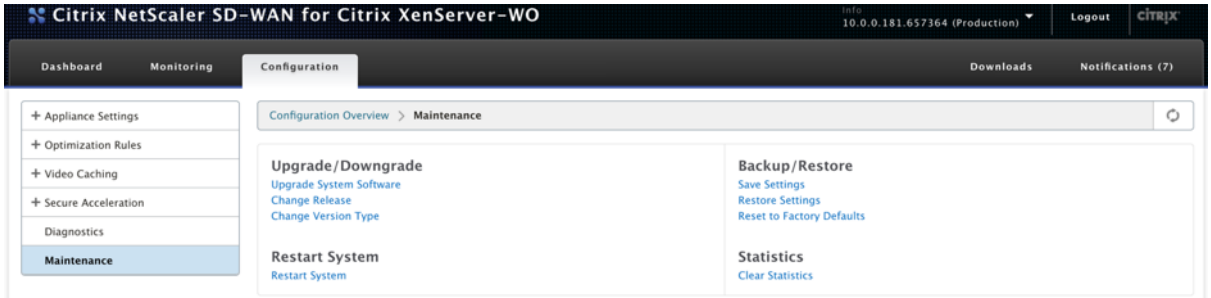


2. WANOP ソフトウェアの最新のソフトウェアバージョンにアップグレードした後、GUI で [構成] **>** メンテナンス **>** ソフトウェアを更新に移動します。*ns-sdw-xen65-pkg_v1.5.upg* ファイルをアップロードします。
3. アップグレードが完了するまで約 20 分待ちます。アップグレードが正常に完了すると、アプライアンスが再起動します。

保守

April 19, 2021

[メンテナンス] ページを使用して、ダウングレードシステムソフトウェアのアップグレード、構成のバックアップと復元、統計のクリアなどのメンテナンスアクティビティを実行します。



Upgrade/Downgrade

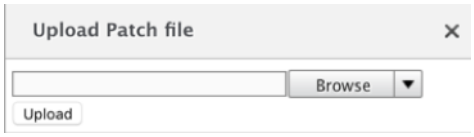
システムソフトウェアをアップグレードする

アプライアンスモデルごとに異なる Citrix SD-WAN ソフトウェアパッケージがあります。ネットワークに含めたいアプライアンスに適切な SD-WAN WANOP ソフトウェアパッケージをダウンロードして、ローカルドライブに保存する必要があります。

アプライアンスソフトウェアは、Citrix から入手したパッチファイルを使用してアップグレードされます。

> 注:
>
> アプライアンスが古いソフトウェアリリースバージョンを実行している場合は、最初に最新のソフトウェアリリースバージョンにアップグレードする必要があります。

システムソフトウェアをアップグレードするには、**[構成]>** メンテナンスに移動します。Upgrade/Downgrade の [システムソフトウェアのアップグレード] を選択します。パッチファイルを選択し、アプライアンスにアップロードします。**



パッチファイルはアプライアンスによって検査されます。有効なパッチファイルのみが、現在使用されているものとは異なるリリースにシステムをアップグレードできます。

アップグレードにより、ライセンスファイルとシステム設定が保持されます。アップグレードされたユニットは、新しいリリースで追加された新機能を除いて、再構成する必要はありません。

リリースの変更

リリース変更ページには、現在インストールされているリリースが表示されます。リリースバージョンを変更する場合は、[リリースの変更] オプションをクリックし、ドロップダウンリストからリリースを選択して、[変更] をクリックします。

バージョンタイプの変更

[バージョンタイプ の変更] オプションを使用すると、リリースのデバッグバージョンを選択できます。[タイプ] ドロップダウンリストからバージョンタイプを選択し、[変更] をクリックできます。可能なデバッグバージョンは次のとおりです。

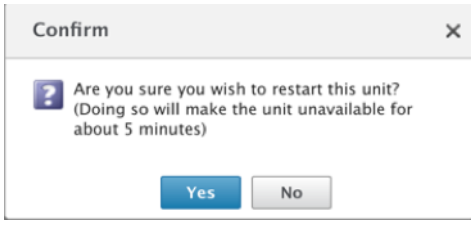
- デフォルト
- レベル 1
- レベル 2
- デフォルトの MC
- レベル 1MC
- レベル 2MC

サポートチームの指示に従って、このアクションを実行する必要があります。

システムを再起動します

パッチがインストールされると、アプライアンスを再起動できるかどうかを尋ねるポップアップメッセージが表示されます。アプライアンスが再起動されるまで、パッチは適用されません。システムをすぐに再起動しないことを選択した場合、各ページの上部にリマインダーが表示されます。

[システムの再起動] を クリックして、SD-WAN WANOP アプライアンスを再起動します。このプロセスには数分かかります。



バックアップ設定

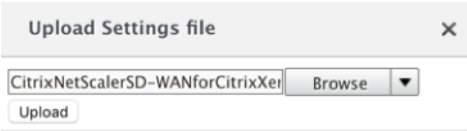
アプライアンスの構成をテキストファイルとして保存することでバックアップできます。

[設定を保存] をクリックすると、テキストファイルがローカルドライブにダウンロードされます。[管理 IP] ページのライセンスファイル、SSH パラメーター、および IP アドレスは保存できません。このファイルは通常のテキストファイルですが、手動で編集しないでください。

設定を復元する

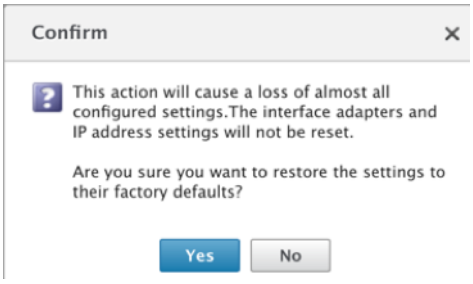
ファイルを保存すると、同じ SD-WAN WANOP アプライアンスに復元できます。

アプライアンスは、古いリリースのコピーを保持します。[設定の復元] オプションは、構成済みの設定を復元するのに役立ちます。[管理 IP] ページのライセンスファイル、SSH パラメーター、および IP アドレスは、新しいリリースから古いリリースにコピーされません。代わりに、アプライアンスは、古いリリースがアップグレードされたときに有効だった設定に戻ります。



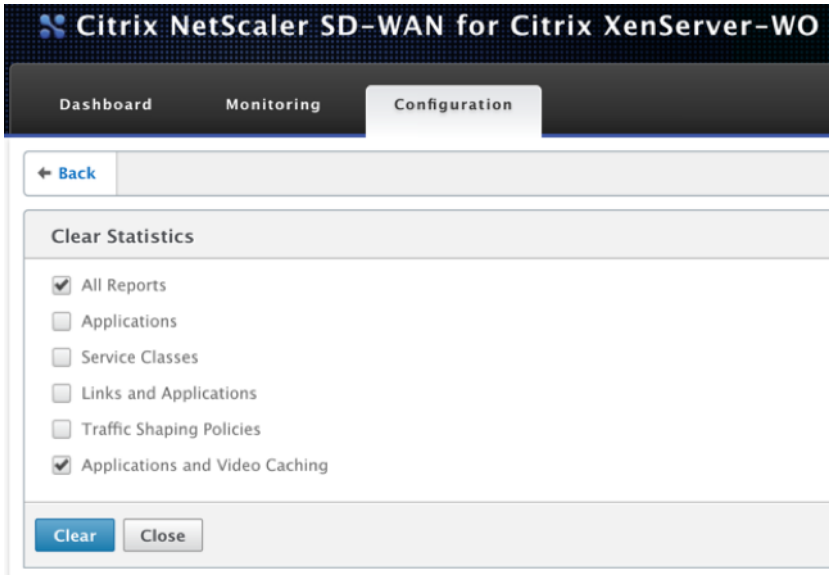
工場出荷時のデフォルトにリセット

工場 出荷時のデフォルトにリセットオプションを使用すると、設定をリセットできます。IP アドレス、帯域幅設定、およびライセンスを除くすべてのパラメーターを工場出荷時のデフォルトに設定します。[工場出荷時のデフォルトにリセット] をクリックすると、確認メッセージが表示されます。設定を工場出荷時のデフォルトに戻す場合は、[はい] を クリックします。



明確な統計

[統計のクリア] ページでは、SD-WAN WANOP アプライアンスの統計をリセットできます。また、目的のサンプリングウィンドウの最初から始まるレポートを作成することもできます。アプライアンスからクリアする統計オプションを選択し、[クリア] をクリックします。



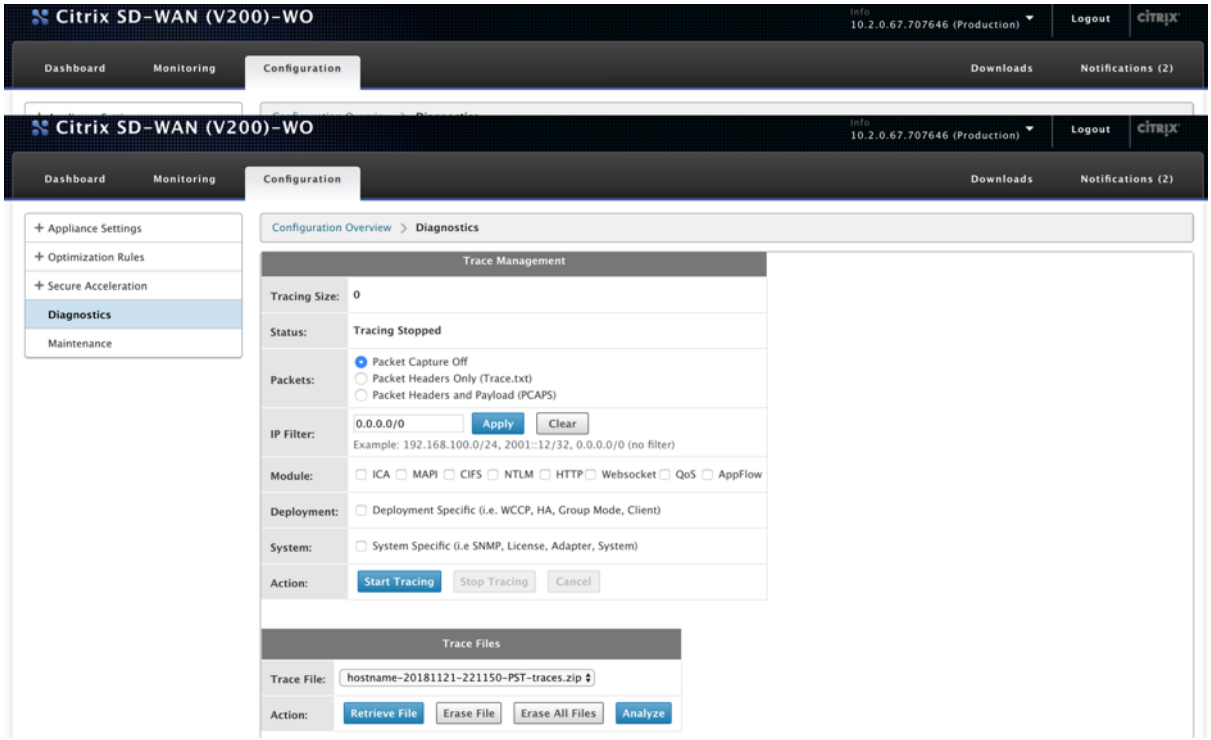
診断

April 19, 2021

このセクションでは、SD-WAN WANOP ネットワークのネットワークの問題を特定してトラブルシューティングするための診断ツールを提供します。Citrix SD-WAN サポートチームがネットワークの問題を診断および解決するのに役立つシステムログファイル、システム情報、およびその他の必要な詳細を取得することもできます。

SD-WAN WANOP で使用できる診断ツールは次のとおりです。

- トレース
- パケットアナライザ
- カードテストをバイパスする
- コースを取得
- ラインテスター
- Ping
- Traceroute
- システム情報
- 診断データ



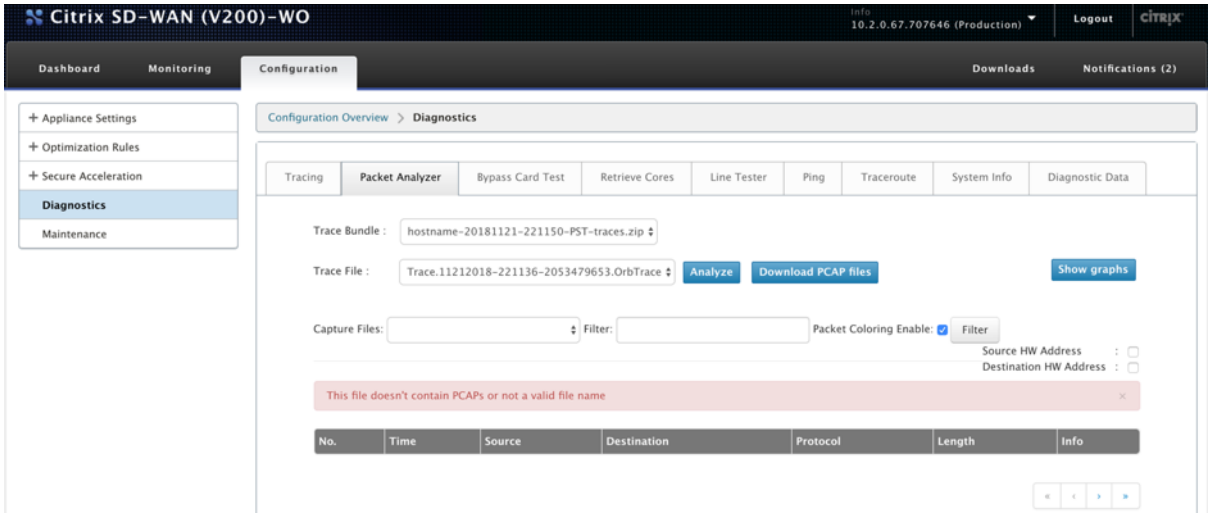
トレース

トレース ツールは、SD-WAN WANOP ネットワーク上を流れるパケットを監視するために使用されます。各パケットを開き、使用されているプロトコル、送信元と宛先の IP アドレス、およびその他のペイロード情報を識別できます。この情報は、ネットワークの問題の根本原因を見つけるために Citrix サポートチームによって使用されます。

パケットヘッダーのみ をトレースするか、パケットヘッダーとペイロードをトレースするかを選択できます。トレースするモジュールを選択し、トレースをデプロイメント固有にするかシステム固有にするかを指定できます。

[トレースの開始] をクリックすると、アプライアンスはパケットのトレースを開始します。[トレースの停止] をクリックすると、結果が ZIP アーカイブにパッケージ化されます。
** このアーカイブは、[ファイルの取得] オプションを使用してコンピューターにダウンロードできます。
** その後、これらのファイルをサポートチームに転送できます。トレースファイルは、クラッシュ分析データも提供します。

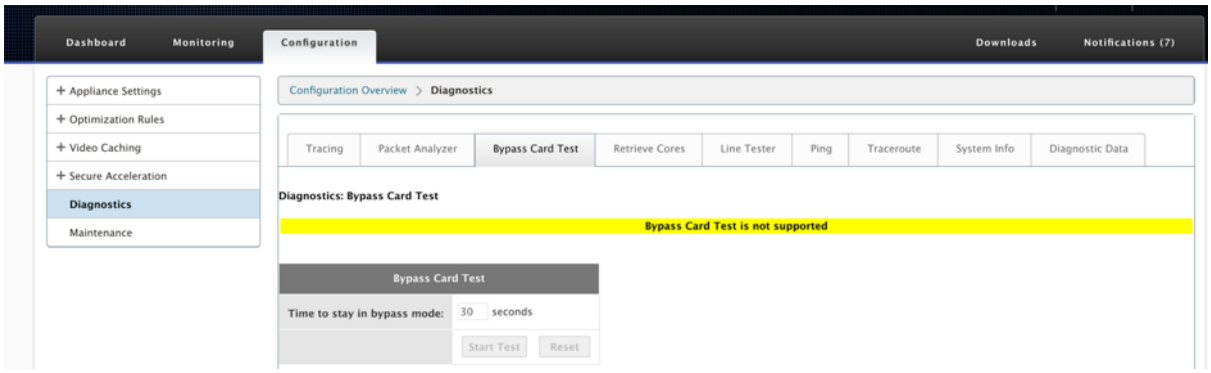
[分析] をクリックして、[パケットアナライザ] タブにパケットの詳細を表示します。



時間、送信元アドレス、宛先アドレス、プロトコル、長さ、およびペイロード情報を表示できます。

カードテストをバイパスする

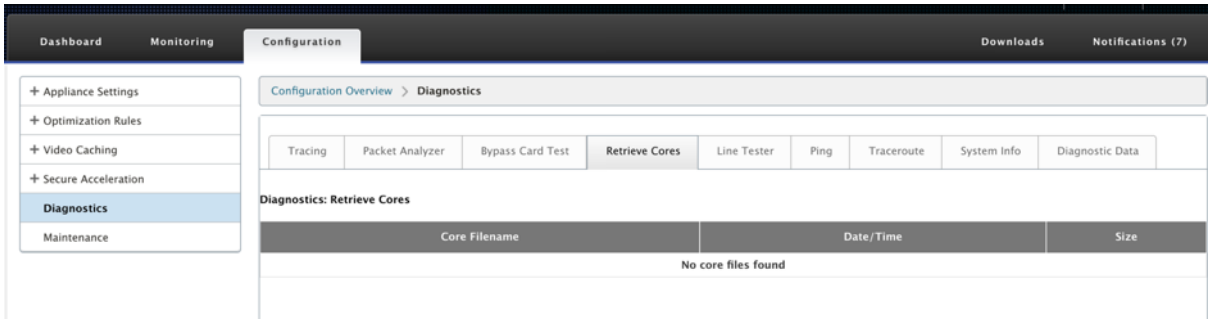
インライン (Fail-to-wire) モードでのアプライアンス展開について、イーサネットインターフェイスの Fail-to-Wire 機能をテストできます。アプライアンスがバイパスモードを維持する秒数を入力し、[テストの開始] をクリックします。この期間中、アプライアンスはバイパスされます。その後、通常の動作に戻ります。



コアを取得する

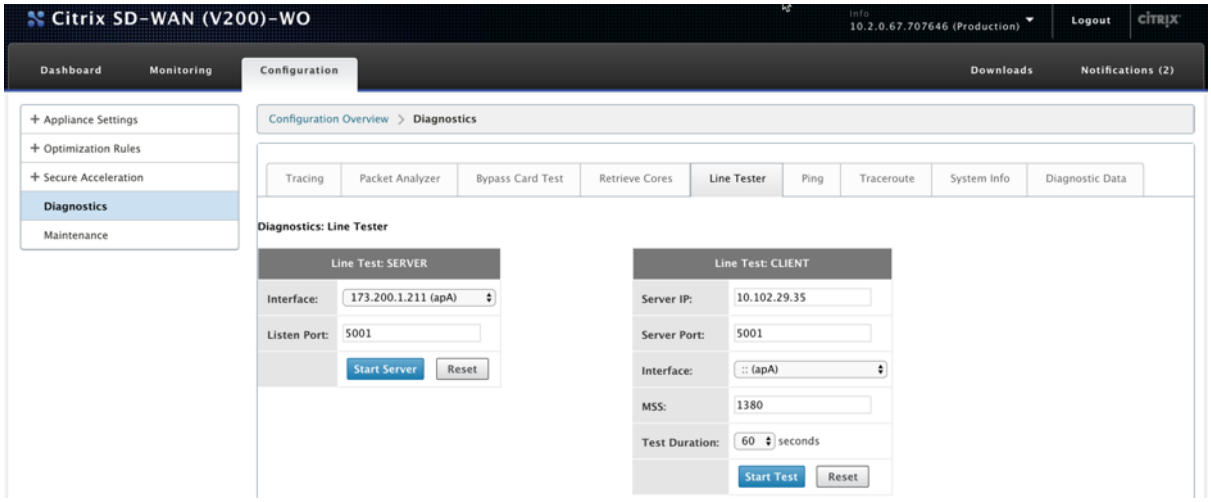
コア ファイルは、SD-WAN WANOP アプライアンスが異常終了またはクラッシュしたときに作成されます。アプライアンスは、クラッシュ後に自動的に再起動します。クラッシュが続く場合、アクセラレーションは無効になりますが、管理インターフェイスはアクティブなままです。

アプライアンスのクラッシュ時またはアプライアンスの異常動作時に作成された必要なコアファイルを選択して取得できます。取得したファイルは ZIP アーカイブに保存されます。これをサポートチームと共有して、さらに分析することができます。



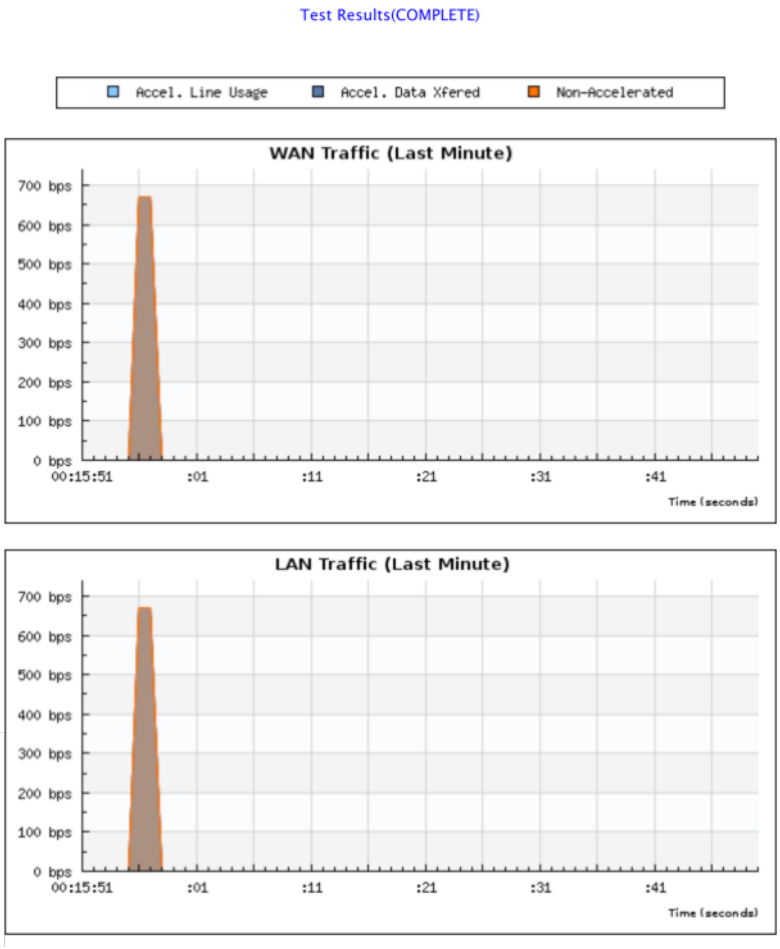
ラインテスター

Line Test: **SERVER** 関数は、TCP モードで実行されているアプライアンス上の iperf サーバーを起動します。このオプションは、WANOP アプライアンス間の接続を確認し、ネットワークトラフィックをトラブルシューティングするために使用できます。iperf テストを実行するには、1 つのシステム（アプライアンスまたは別のホスト）がサーバーとして iperf を実行し、別のシステムがクライアントとして接続する必要があります。



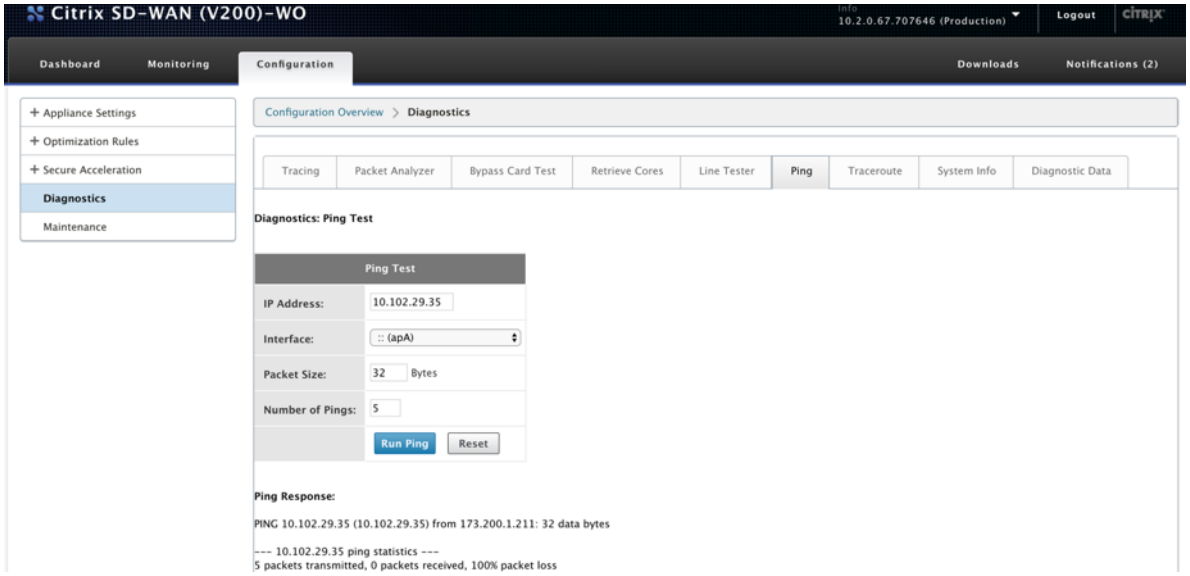
デフォルトの **LineTesterServer** インターフェイスとポート番号を使用できます。[サーバーの開始] をクリックして、アプライアンスで iperf サーバーを開始します。

ラインテスト: **CLIENT** 機能は、TCP モードで実行されているユニットで iperf クライアントを起動します。iperf サーバーのポート番号とテストの長さを指定することもできます。テストが完了すると、接続速度が報告されます。[テストの開始] を クリックして、WAN および LAN トラフィックの結果を確認します。



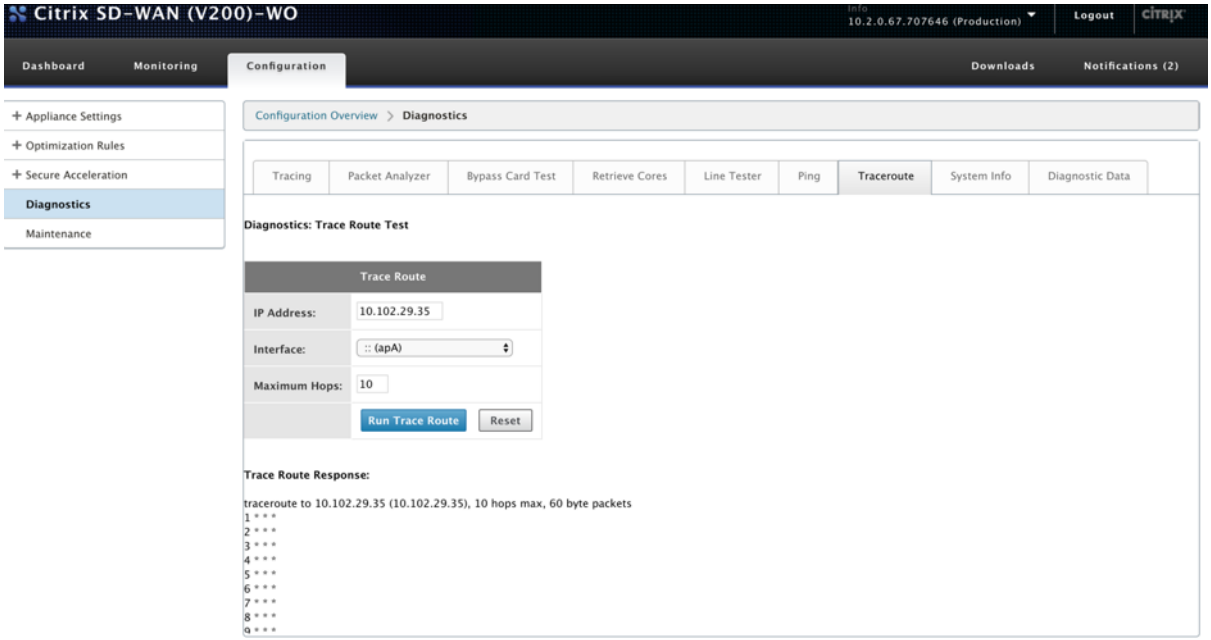
Ping

Ping を 使用すると、SD-WAN ネットワーク内のネットワーク要素の接続を確認できます。ネットワーク要素の IP アドレスを入力し、[**Ping** の実行] をクリックして結果を確認します。



Traceroute

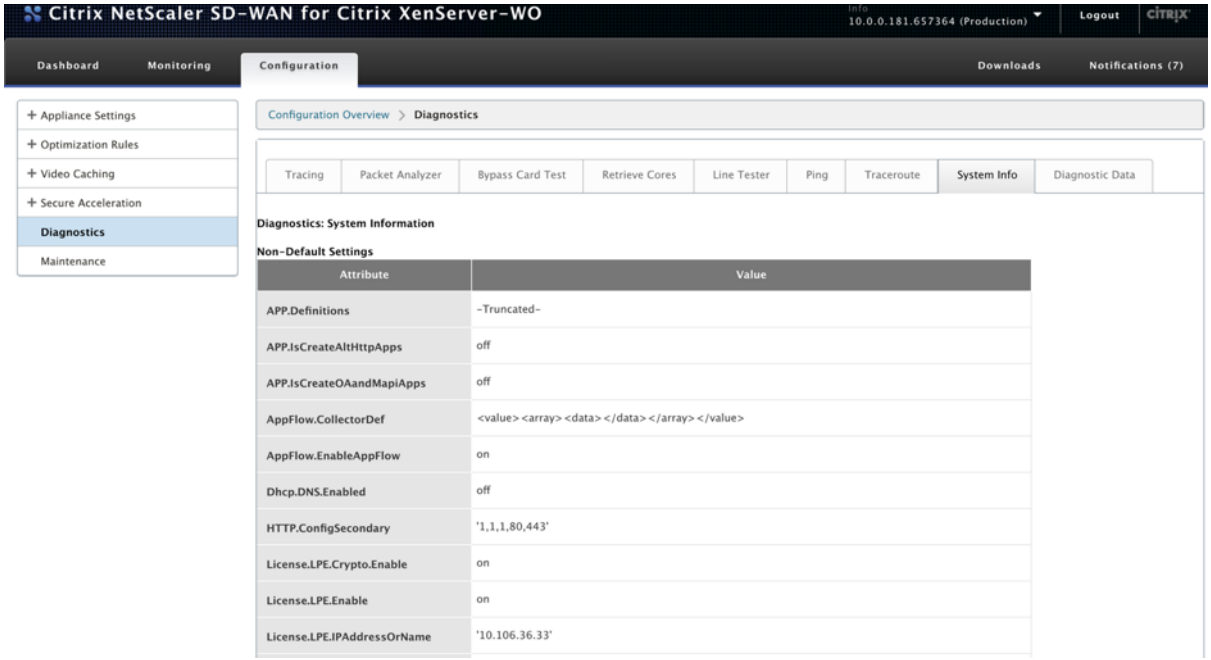
Traceroute を 使用すると、SD-WAN アプライアンスと SD-WAN ネットワークまたはインターネット上の他のネットワーク要素との間のルートを記録できます。各ホップにかかった時間を計算して表示します。



システム情報

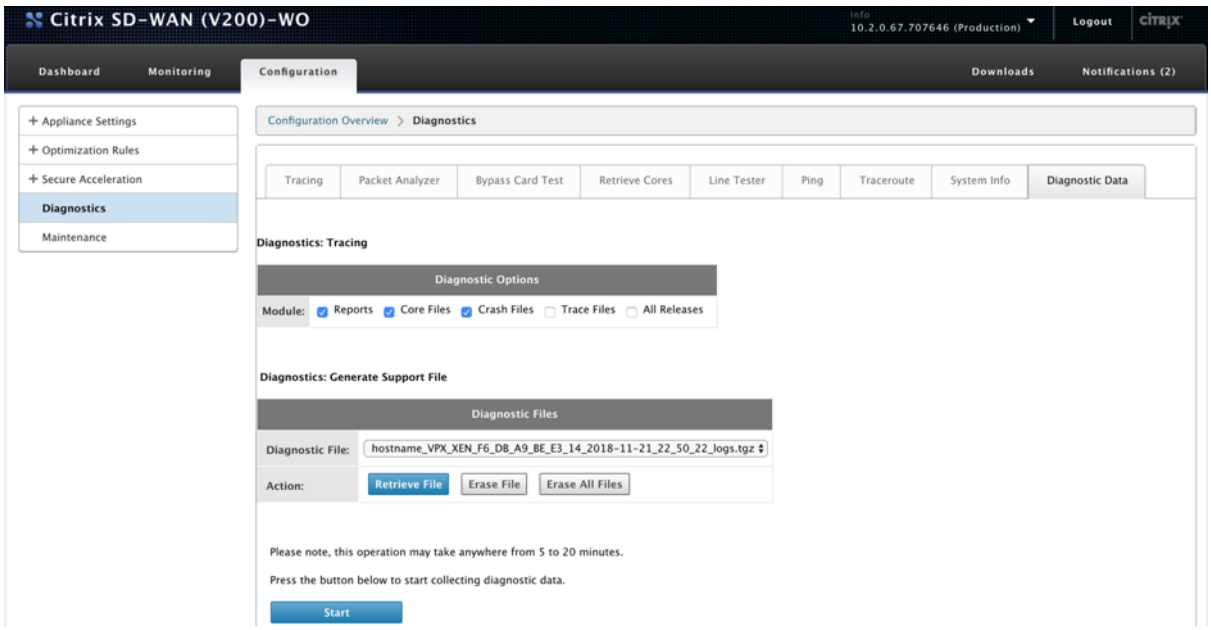
システム情報に は、デフォルトに設定されていないすべてのパラメーターがリストされます。この情報は読み取り専用です。なんらかの設定ミスが疑われる場合にサポートが使用します。問題を報告すると、このページで 1 つ以上の値を確認するように求められる場合があります。

デフォルト以外の設定、アダプタプライマリの詳細情報、アダプタ **apA.2** の詳細情報、およびアダプタ apA.1 の詳細情報を提供します。



診断データ

診断データを 使用すると、Citrix サポートチームによる分析のために診断データをパッケージ化できます。必要な診断ファイルを選択し、[開始] をクリックします。次に、[ファイルの取得] をクリックして zip アーカイブをダウンロードし、Citrix サポートと共有できます。



トラブルシューティング

April 19, 2021

次のトピックでは、問題のリスト、問題の原因、および一部の Citrix SD-WAN WANOP 機能の解決手順について説明します。

CIFS と MAPI

April 19, 2021

- 問題: ドメインコントローラーがネットワークから削除されます。ただし、Citrix SD-WAN WANOP アプライアンスはドメインを離れることができません。

  原因: これは、アプライアンスの既知の問題です。

  回避策: [Windows ドメイン] ページで、DNS を目的のドメインを解決できる DNS に変更します。次に、Rejoin**Domain** オプションを使用して、Citrix SD-WAN WANOP アプライアンスをそのドメインに参加させます。ドメインから離れてみてください。

- 問題: MAPI 接続が最適化されておらず、次のエラーメッセージが表示されます。

  Outlook のデフォルト以外の設定はサポートされていません

  原因: これは、リリース 6.2.3 以前のリリースの既知の問題です。

  解決: アプライアンスを最新リリースにアップグレードします。

- 問題: アプライアンスは MAPI 接続を最適化しました。ただし、監視ページには、送信バイト数と受信バイト数がゼロとして表示されます。

  原因: これは、アプライアンスの既知の問題です。

  解決: これは良性の問題であり、アプライアンスの機能には影響しません。あなたはそれを無視することができます。

- 問題: Citrix SD-WAN WANOP アプライアンス間で安全なピアリングを確立できません。

  原因: パートナーアプライアンスとの安全なピアリングが適切に構成されていません。

  解決: 以下をせよ:

  1. CA 証明書とサーバー証明書の適切な組み合わせをアプライアンスにアップロードしたことを確認します。
  2. **Citrix SD-WAN WANOP** > 構成 > **SSL** 設定 > セキュアパートナー ページに移動します。
  3. [パートナーセキュリティ] セクションの [証明書の確認] で、[なし-すべての要求を許可する] オプションを選択して、証明書の有効期限が切れないようにします。
  4. アプライアンスがパートナーアプライアンスとの安全なピアリングを確立できることを確認します。
  5. [リッスンオン] セクションに、目的の Citrix SD-WAN WANOP アプライアンスの IP アドレスのエントリがあることを確認します。

- 問題: Exchange クラスターに接続するときに、接続が最適化されている Outlook ユーザーがバイパスされるか、ログオン資格情報の入力を求められることがあります。

  原因: MAPI 最適化では、Exchange クラスター内の各ノードが exchangeMDB サービスプリンシパル名（SPN）に関連付けられている必要があります。時間の経過とともに、より多くの容量が必要になると、クラスターにノードを追加します。ただし、構成タスクが完了せず、一部のノードが SPN 設定なしでクラスター内に残る場合があります。この問題は、Exchange Server2003 または Exchange Server2007 を使用する Exchange クラスターで最もよく見られます。

  解決: セットアップ内の各 Exchange サーバーで次の手順を実行します。

  1. ドメインコントローラーにアクセスします。
  2. コマンドプロンプトを開きます。
  3. 次のコマンドを実行します:

     ```
     pre codeblock setspn -A exchangeMDB/Exchange1 Exchange1
     setspn -A exchangeMDB/Exchange1.example.com Exchange1
     ```

- 問題: Outlook に接続しようとすると、「接続しようとしています」というメッセージが表示され、接続が終了します。

  原因: クライアント側の Citrix SD-WAN WANOP アプライアンスには、サーバー側のアプライアンスには存在しないブラックリストエントリがあります。

  解決: 両方のアプライアンスからブラックリストエントリを削除するか、（推奨）アプライアンスのソフトウェアをリリース 6.2.5 以降にアップグレードします。

- 問題: ドメイン前のチェックに合格した後でも、アプライアンスはドメインへの参加に失敗します。

  原因: これは既知の問題です。

  解決: 以下をせよ:

1. SSH ユーティリティを使用してアプライアンスにアクセスします。
2. ルート資格情報を使用してアプライアンスにログオンします。
3. 次のコマンドを実行します。

   ```
   /opt/likewise/bin/domainjoin-cli join \<Domain\\_Name\>
   administrator
   ```

- 問題: デリゲートユーザーを Citrix SD-WAN WANOP アプライアンスに追加すると、LdapError エラーメッセージが表示されます。

  解決: 次のいずれかを実行します。

  - Citrix SD-WAN WANOP アプライアンスの DNS サーバーで、すべてのドメインコントローラー IP アドレスに逆引き参照ゾーンが構成されていることを確認します。
  - クライアントマシンのシステムクロックが ActiveDirectory サーバーのシステムクロックと同期していることを確認します。Kerberos を使用する場合、これらのクロックを同期する必要があります。
  - 代理ユーザーのパスワードをもう一度入力して、Windows ドメインページで代理ユーザーを更新します。

- 問題: 代理ユーザーを Citrix SD-WAN WANOP アプライアンスに追加すると、タイムスキューエラーメッセージが表示されます。

  解決: アプライアンスがドメインに参加していることを確認します。そうでない場合は、アプライアンスをドメインに参加させます。これにより、アプライアンスの時刻がドメインサーバーの時刻と同期され、問題が解決されます。

- 問題: クライアントは加速のために一時的に除外されます。Citrix SD-WAN WANOP アプライアンスにデリゲートユーザーを追加すると、最後のエラー（Kerberos エラー）エラーメッセージが表示されます。

  原因: デリゲートユーザーは、**Kerberos** のみを使用する 認証用に構成されています。

  解決: ドメインコントローラーで、デリゲートユーザーの認証設定が [任意の認証プロトコルを使用する] になっていることを確認します。

- 問題: デリゲートユーザーを Citrix SD-WAN WANOP アプライアンスに追加すると、デリゲートユーザーの準備ができていませんというエラーメッセージが表示されます。

  解決: メッセージがクライアント側アプライアンスにのみ表示される場合は、無視してください。ただし、メッセージがサーバー側アプライアンスに表示される場合は、**Windows** ドメイン ページで利用可能な代理ユーザー事前チェックツールを実行してから、サーバー側アプライアンスで代理ユーザーを構成します。

- 問題: 最後のエラー（サーバーは Kerberos 認証用に委任されていません。委任ユーザー、委任が許可されているサービスとサーバーのチェックリストを追加してください。）UR:4 デリゲートユーザーを Citrix SD-WAN WANOP アプライアンスに追加すると、エラーメッセージが表示されます。

  解決: デリゲートユーザーがドメインコントローラーで正しく構成されていること、およびドメインコントローラーに適切なサービスが追加されていることを確認します。

- 問題: アプライアンスはドメインに参加できません。

  解決: Windows ドメインページで利用可能なドメイン事前チェックツールを実行し、問題がある場合は解決します。ドメイン事前チェックツールで問題が報告されない場合は、Citrix テクニカルサポートに連絡して、問題の解決についてさらにサポートを受けてください。

Citrix SD-WAN WANOP プラグイン

April 19, 2021

- 問題: シグナリングチャネルの接続の問題に直面しています。これらの問題を解決するにはどうすればよいですか?

  解決策: シグナリングチャネルの接続の問題を解決するには、次のトラブルシューティング手順を実行します。

  - シグナリング IP アドレスが正しく構成されていることを確認します。これを行うには、シグナリング IP アドレスに ping を実行し、応答を確認します。
  - WANOP アプライアンスでシグナリングステータスが有効になっていることを確認します。
  - ネットワークにインストールされているファイアウォールが WANOP TCP オプションを削除しないことを確認します。
  - 有効な WANOP プラグインライセンスが WANOP アプライアンスにインストールされていることを確認します。
  - シグナリングチャネルソースフィルタリング構成がクライアントソース IP アドレスをブロックしないことを確認します。
  - LAN 検出を有効にしている場合は、WANOP プラグインと WANOP アプライアンス間のラウンドトリップ時間が許容値であることを確認してください。

- 問題: WANOP 4000 アプライアンスで、WANOP プラグインを無効にできません。

  原因: これは既知の問題です。

  解決: 無し。WANOP4000 アプライアンスで WANOP プラグインを無効にすることはできません。

- 問題: WANOP プラグインを使用して WANOP アプライアンスに接続すると、次のエラーメッセージエントリが [アラート] タブに記録されます。

  現在の制限よりも多くの WANOP プラグイン < 番号 > はこのアプライアンスへの接続を試みました。

  原因: WANOP アプライアンスへの接続数がライセンスユーザー制限を超えました。

  解決: ユーザーが切断するのを待つか、接続を終了します。

- 問題: 誤ったシグナリング IP アドレスが WANOP4000 または 5000 アプライアンスで構成されています。

  解決: WANOP 4000 または 5000 アプライアンスのシグナリング IP アドレスを更新するには、次の手順を実行します。

  1. WANOP アプライアンスの Citrix インスタンスにログオンします。
  2. トラフィック管理 > 負荷分散 > 仮想サーバー > BR_LB_VIP_SIG ページに移動します。
  3. シグナリング IP アドレスを更新します。
  4. 構成を保存します。

- 問題: CIFS および ICA トラフィックは加速されていません。

  解決: この問題を解決するには、次のトラブルシューティング手順を実行します。

  – IP アドレスとポート番号のアクセラレーションルールが WANOP プラグインに対して正しく定義されていることを確認します。
  – シグナリング接続が成功した後、CIFS または ICA 接続が確立されていることを確認します。
  – 使用されているサービスクラスのアクセラレーションポリシーを確認します。

HTTPS 経由の RPC

April 19, 2021

- 問題: アプライアンスのソフトウェアをリリース 7.3 にアップグレードした後、監視レポートには、HTTPS 接続を介した RPC の特別なカテゴリはありません。

  原因: アプライアンスをリリース 7.3 にアップグレードすると、RPC over HTTPS アプリケーションは独自のサービスクラスに属しません。その結果、すべての RPC over HTTPS 接続は、レポートに TCP その他の接続としてリストされます。

  解決: これらの接続を RPC over HTTPS 接続として分類するには、それらのアプリケーションのサービスクラスを作成します。

- 問題: RPC over HTTPS のサービスクラスを作成した後、すべての HTTP および HTTPS トラフィックは RPC over HTTP として分類されます。

  原因: RPC over HTTPS アプリケーション用に作成したサービスクラスに宛先 IP アドレスを追加していません。

  解決: サーバーの宛先 IP アドレスを追加して、RPC over HTTPS アプリケーション用に作成したサービスクラスを変更します。

ビデオキャッシング

April 19, 2021

- 問題: 事前入力タスクのリストにエントリを追加した後も、エントリはまだ構成済み状態です。

  原因: 事前入力タスクは、ダウンロード状態に約 1 分かかります。

  解決: 1 分後にエントリのステータスを確認するか、ページを更新して、ステータスが [ダウンロード中] に変わることを確認します。

- 問題: 事前入力タスクのリストにエントリを追加すると、エントリのステータスに ERROR403 が表示されます。ただし、Web ブラウザでは Web サイトは正常に機能します。

  原因: Citrix SD-WAN WANOPapA の IP アドレスはビデオサーバーにアクセスできません。

  解決: この問題を解決するには、以下を確認して更新します。

  - ファイアウォールを越えたアクセスルール
  - ビデオサーバーの httpd.conf ファイルのソース IP アドレスベースの制限

  原因: ビデオサーバーは HEAD メソッドをサポートしていません。

  解決: ビデオサーバーは、この方法で Citrix SD-WAN WANOP IP アドレスを許可する必要があります。

  原因: ビデオサーバーでフォルダーのディレクトリリストが有効になっていません。

  解決: ビデオサーバーは、フォルダのディレクトリリストを有効にする必要があります。

- 問題: 事前入力タスクのエントリを作成した後は、エントリを変更または削除することはできません。

  原因: エントリの **[今すぐ開始]** をクリックした可能性があります。

  解決: これは仕様によるものです。エントリの **[今すぐ開始]** をクリックし、エントリがキュー、開始、またはダウンロードの状態になった後は、エントリを変更または削除することはできません。ダウンロードが完了した後でのみ、エントリを削除できます。

- 問題: 人口増加タスクのエントリを作成した後、ビデオがダウンロードおよびキャッシュされません。エントリのステータスに「ダウンロードに失敗しました」と表示されます。

  原因: 事前入力エントリには、ビデオの絶対 URL がありません。

  解決: この問題を解決するには、次の手順を実行します。

  1. 事前入力エントリに、HTML ファイルではなく、`http://10.102.29.16/Citrix SD-WAN WANOP\\_demo.mp4`などのビデオの実際の URL が含まれていることを確認します。Citrix SD-WAN WANOP アプライアンスは、HTML ファイルのコンテンツを検索してビデオリンクを見つけることができません。

2. HTTP プロトコルがビデオの提供に使用されていることを確認します。これは、Web ブラウザの [ソースの表示] オプションを使用して確認できます。
3. Web ブラウザの開発ツールオプションを使用して、ビデオの絶対 URL を取得できます。

Citrix Virtual Apps and Desktops の高速化

April 19, 2021

- 問題: アプライアンスをリリース 7.3.1 にアップグレードした後、ICA 接続は ICA 監視ページで HTML5 接続用の Citrix Receiver として分類されません。

  原因: アプライアンスで定義されているサービスクラスは、Web（プライベート）ではなく **HTTP**（プライベート）です。アプライアンスをリリース 7.3.1 にアップグレードすると、**ALTHTTP** アプリケーションはこのサービスクラスに追加されません。その結果、Citrix Receiver for HTML5 を介した ICA 接続が最適化されていても、ICA 監視ページでは Citrix Receiver for HTML5 接続として分類されません。

  解決: Citrix Receiver for HTML5 を介した ICA 接続を分類するには、次の手順を実行します。

  1. 構成 > 最適化ルール > サービスクラス ページに移動します。
  2. **HTTP**（プライベート）サービスクラスを編集します。
  3. **[**ルールの追加**]** をクリックします。
  4. [フィルタールール] の [アプリケーション] で、[任意] をクリックします。
  5. [アプリケーション] リストから、[**ALTHTTP]** を選択します。
  6. ［追加］をクリックします。
  7. ［保存］をクリックします。
  8. 必要に応じて、フィルタールールに他の変更を加えます。
  9. ［保存］をクリックします。