Citrix SD-WAN 11

Machine translated content

Disclaimer

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

Contents

新機能

August 30, 2022

アプリケーション中心の拡張機能

動的プロキシ自動構成 (PAC) ファイルのカスタマイズ:

ミッションクリティカルな SaaS アプリケーションと分散型ワークフォースの企業採用が増加するにつれて、データセンターを介したトラフィックのバックホールという従来の方法に内在するレイテンシーと輻輳を低減することが非常に重要になります。

Citrix SD-WAN では、Office 365 などの SaaS アプリケーションを直接インターネットから抜け出すことができます。

ただし、企業展開で明示的な Web プロキシが設定されている場合、SaaS アプリケーショントラフィックを含むすべてのトラフィックが Web プロキシに誘導されるため、分類や直接インターネットブレイクアウトが難しくなります。

この問題を解決するには、エンタープライズ PAC (プロキシ自動構成) ファイルをカスタマイズして、SaaS アプリケーショントラフィックをプロキシから除外します。

Citrix SD-WAN 11.0 では、カスタム PAC ファイルを動的に生成して提供することにより、Office 365 アプリケーショントラフィックのプロキシバイパスとローカルインターネットブレークアウトが可能になります。

リンク集約グループ

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

Citrix SD-WAN リリース 11.0 では、単純な LAG（ACTIVE-BACKUP）がサポートされています。802.3ad LACP プロトコルベースのネゴシエーションは、現在のリリースではサポートされていません。

スタンバイおよび従量制課金リンク

11.0 リリースで「データ上限に達しました」オプションが導入された場合は無効にします。

- [データ上限に達した場合に無効にする] チェックボックスがオンの場合、データ使用量がデータ上限に達すると、次回の請求サイクルまで、従量制課金リンクとその関連パスがすべて無効になります。
- 既定では、[データ上限に達したら無効にする] チェックボックスはオフの状態になります。このチェックボックスは、データ上限に達した後、次の請求サイクルまで継続される従量制課金リンクに設定されている現在のモードまたは状態を保持します。

210-SE LTE 認証

APN 設定フォームに新しい認証入力フィールドが導入されました。この新しいフィールドには、[なし]、[PAP]、[CHAP]、[PAPCHAP] の 4 つの値を使用できます。

の APN 設定に認証フィールドが追加されました。

- SD-WAN センター UI
- SD-WAN アプライアンス UI
- REST API

Packet capture

[**Packet Capture**] オプションを使用して、選択したサイトに存在する選択したアクティブなインターフェイスを通過しているデータパケットを代行受信します。

アクティブなインターフェイスは、選択したサイトでパケットキャプチャに使用できます。ドロップダウンリストからインターフェイスを選択するか、インターフェイスを追加します。パケットキャプチャをトリガーするには、少なくとも 1 つのインターフェイスを選択する必要があります。

> 注:
> すべてのインターフェイスでパケットキャプチャを一度に実行する機能は、トラブルシューティングタスクの高速化に役立ちます。

帯域内管理

Citrix SD-WAN では、帯域外管理と帯域内管理の 2 つの方法で SD-WAN アプライアンスを管理できます。アウトバンド管理では、管理トラフィックだけを伝送する管理用に予約されたポートを使用して管理 IP を作成できます。

インバンド管理では、SD-WAN データポートを管理に使用できます。SD-WAN データポートは、データトラフィックと管理トラフィックの両方を伝送します。追加の管理パスを設定する必要はありません。

ICA トラフィックに対して RED を有効にする

11.0 リリース以降、ICA トラフィックでは、ランダム早期検出（RED）がデフォルトでオンに設定されます。

クラウドサービス

Cloud Direct サービス

Cloud Direct サービスは、ホスト環境 (データセンター、クラウド、インターネット) に関係なく、インターネットへのすべてのトラフィックに対して、信頼性と安全な配信を通じて SD-WAN 機能をクラウドサービスとして提供します。

クラウドダイレクトサービスは、ネットワークの可視性と管理性を向上させます。パートナーは、ビジネスクリティカルな SaaS アプリケーション向けのマネージド SD-WAN サービスをエンドカスタマーに提供できます。

Palo Alto Networks と SD-WAN との統合

Palo Alto Networks は、リモートネットワークを保護するためのクラウドベースのセキュリティインフラストラクチャを提供します。組織が SD-WAN ファブリックを保護する地域的なクラウドベースのファイアウォールをセットアップできるようにすることで、セキュリティを提供します。

リモートネットワーク用の Prisma Access サービスを使用すると、リモートネットワークロケーションをオンボードし、ユーザーにセキュリティを提供できます。

リモートネットワークの場所を Prisma Access サービスに接続するには、Palo Alto Networks の次世代ファイアウォールを使用します。また、サービスへの IPsec トンネルを確立できる SD-WAN など、サードパーティの IPsec 準拠デバイスを使用することもできます。

Citrix SD-WAN アプライアンスは、IPsec トンネルを介して Palo Alto クラウドサービス（Prisma アクセスサービス）ネットワークに接続できます。アプライアンスは、最小限の構成で SD-WAN アプライアンスの場所から接続できます。

レポート

HDX ユーザー名に基づくレポート

HDX レポートページでは、次のレポートタイプを表示できます。

- HDX サイト統計
- HDX サマリー（利用可能なセッションと利用できない HDX 情報チャネルの両方に適用可能）
- HDX ユーザーセッション（HDX 情報チャネルで利用可能なセッションのみに適用）
- HDX アプリ（HDX 情報チャネルで利用可能なセッションのみに適用）

SD-WAN 構成エディターで、**HDX** ユーザーレポートを有効にするオプションが新たに追加されました。このオプションを有効にすると、新しく追加されたユーザーベースのレポート（HDX サマリー、HDX ユーザーセッション、HDX アプリ）が生成され、これらのレポートは SD-WAN Center で利用できます。これは、**HDX** サイト統計レポートには適用されません。

HDX ユーザーレポートを有効にするオプションは、**DPI** オプションを有効にするのと同様グローバルレベルとサイトレベルで利用可能です。

ルーティングの強化

OSPF 再配布タグ

OSPF タグを使用すると、OSPF と他のプロトコル間の相互再配布中のルーティングループを防ぐことができます。

SD-WAN ルートと BGP 学習ルートに異なるタグを指定すると、これらのルートを OSPF ルーティングテーブルにインストールできます。

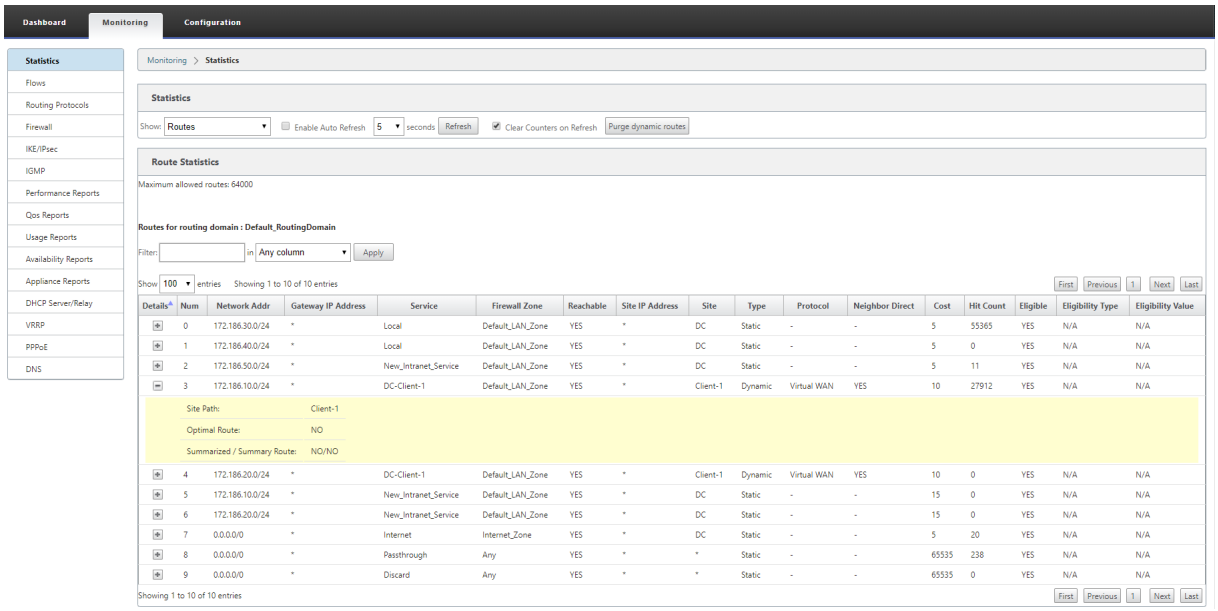
プロトコルプリファレンス

Citrix SD-WAN が仮想パス、OSPF プロトコル、または BGP プロトコルを介してルートプレフィックスを学習すると、次のデフォルトの優先順位が同時に導入されます。

- OSPF-150
- BGP —100
- SD-WAN —250

ルート統計情報

サイトパス、最適ルート、集約ルート、サマリールートなどのその他の詳細は、ルート統計情報レポートに含まれます。



AS パスの長さ

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

Citrix SD-WAN Center

SD-WAN センターアプライアンス証明書

以前は、SD-WAN センターにすでにインストールされている定義済みのアプライアンス証明書が使用されていました。

Citrix SD-WAN 11.0 リリースでは、事前定義された証明書を置き換える MCN でアプライアンス証明書を再生成し、SD-WAN Center にインストールできます。

SD-WAN センターのセキュリティ管理者の役割

セキュリティ管理者の役割が SD-WAN センターに追加されます。セキュリティ管理者は、**Config Editor** のファイアウォールとセキュリティ関連の設定に対する読み取り/書き込みアクセス権のみを持ち、他のセクションには読み取り専用アクセス権があります。

SD-WAN センターから Azure に SD-WAN を展開する

Citrix SD-WAN センターから Azure に Citrix SD-WAN を展開できます。

Citrix SD-WAN for Azure を使用すると、組織は各ブランチから Azure でホストされているアプリケーションに直接安全に接続でき、クラウドにバインドされたトラフィックをデータセンター経由でバックホールする必要がなくなります。

プラットフォーム、拡張性、デプロイメント

ネットワーク向け 6K ノードスケール

Citrix SD-WAN 11.0 は、階層型ネットワークアーキテクチャで最大 128 のリージョンを持つ最大 6000 サイトのネットワークをサポートします。

Google Cloud Platform 上の Citrix SD-WAN SE

Google Cloud Platform（GCP）に Citrix SD-WAN SE VPX を展開すると、組織は各ブランチから GCP でホストされているアプリケーションへの直接的で高度なセキュリティ接続を確立できます。これにより、データセンターを介してクラウドにバインドされたトラフィックをバックホールする必要がなくなります。

GCP で Citrix SD-WAN を使用する主な利点は次のとおりです。

- すべてのブランチサイトから GCP への直接接続を作成します。
- GCP に常時接続していることを確認します。
- セキュアな境界をクラウドに拡張します。
- シンプルで管理しやすい支店ネットワークへと進化します。

Citrix SD-WAN 1100-Y ケーブルによる高可用性のサポートのための小型フォーム・ファクタ・プラグ（SFP）の拡張

1100 アプライアンスで使用可能な SFP（小型フォーム・ファクタ・プラグ）ポートを光ファイバ Y ケーブルとともに使用することで、エッジ・モード導入で高可用性を実現できます。

1100 SE および PE アプライアンスでは、スプリッタケーブルスプリットエンドが 2 台の 1100 アプライアンスのファイバポートに接続します。ファイバポートは、高可用性ペアで設定されます。

REST API

次の API が導入されました。

- アプライアンス HA ステータスの監視 API。

- SIM ピンのサマリーおよび SIM ピンの操作のためのモバイルブロードバンド API です。
- プロキシ自動構成ファイル設定およびサイトプロキシ自動構成ファイル設定用の構成エディタ API。
- SD-WAN センターでは、HDX アプリと HDX セッションの API がレポートされます。
- SD-WAN センターでは、HDX サマリー用の API が報告されます。

リリースノート

September 26, 2023

このリリースノートでは、SD-WANStandard Edition、WANOP、Premium Edition アプライアンス用の Citrix NetScaler SD-WAN ソフトウェアリリース 11.0 に適用される既知の問題と、修正された問題について説明します。

Citrix SD-WAN リリース 11.0.0 では、SD-WAN ソフトウェアの基盤となる OS/カーネルが新しいバージョンにアップグレードされるため、アップグレードプロセス中に自動再起動を実行する必要があります。その結果、各アプライアンスのアップグレードに予想される時間が約 100 秒増加します。さらに、新しい OS を含めることで、各ブランチアプライアンスに転送されるアップグレードパッケージのサイズが約 90 MB 増加します。

以前のリリースバージョンの詳細については、Citrix SD-WANのマニュアルを参照してください。

解決された問題

SDWANHELP-590: Citrix SD-WAN Center のセキュリティ強化。

SDWANHELP-594: 破損した制御パケットが処理されると、仮想パスはすべてのサイトで **DEAD** としてマークされます。制御パケットの形式が不正な場合、そのパケットはドロップされ、パスは非アクティブになります。

SDWANHELP-600: リリース 9.3.2 から 9.3.5 へのソフトウェアのアップグレード後、アップグレード後の SNMP システム名がデフォルトの仮想 WAN として表示され、デバイスのホスト名は使用されません。

SDWANHELP-617: 動的仮想パスを形成する WAN リンクのいずれかで適応帯域幅検出機能が有効の場合、ダイナミック仮想パスに必要な帯域幅が割り当てられません。

SDWANHELP-626: メモリ停止のため、Citrix SD-WAN Center にアクセスできません。

SDWANHELP-649: 過剰な仮想パスパケットの再送信は、低帯域幅の使用率、高い損失または輻輳、および 20 ミリ秒未満の RTT 時間が発生する可能性があります。

SDWANHELP-650: サイトの追加、編集、クローン作成、監査などの設定プロセスにより、MCN GUI が応答しなくなります。

SDWANHELP-654: ICA 接続の解析中に SD-WAN WANOP 4000 アプライアンスが中断されることがあります。

SDWANHELP-666: すべてのルーティングドメインに対するインターネットアクセス機能が有効の場合、インターネットサービス経由の PPTP または GRE トンネルが確立されない。

SD-WAN アプライアンスは、エンドポイントではなくパススルーとして機能しています。

SDWANHELP-671: ライセンスログファイルは、リモートライセンスサーバーを使用しているときに大量のディスク領域を消費します。

SDWANHELP-674: SD-WAN EE および PE アプライアンスで、WANOP 通信のホスト名を変更する必要があります。

SDWANHELP-676: ドメインサービスが時折失敗しても、ドメインサービスが自動的に再起動します。

SDWANHELP-680: 同じ名前のイントラネットサービスが別のサイトに存在する場合、サイト内のイントラネットサービスを削除すると、監査構成が失敗します。

SDWANHELP-682: 基本構成エディタを使用してサイトを作成する際に、[サイトの場所] フィールドは保存されません。

SDWANHELP-698: 次の場合、LAN ポートがダウンした場合、高可用性フェールオーバーは発生しません。

- Citrix SD-WAN アプライアンスは、シリアル高可用性（FTW）モードで展開されます。
- LAN ポート（FTB）は、トラッキング用の高可用性インターフェイスで定義されます。

SDWANHELP-703: メモリ使用量のピークが確認されると、Zscaler への IPSec トラフィックが影響を受けます。

SDWANHELP-712: ブランチオフィスの SD-WAN アプライアンス上でモデムが動作している場合でも、LTE 接続仮想パスが DOWN として報告されます。

SDWANHELP-725: SD-WAN アプライアンスは、高可用性仮想パス情報を SD-WAN Center に送信します。それはそれを認識することができないので、結果では、それは統計エラーをスローします。

SDWANHELP-734: デフォルトのクラス名は、変更後に更新されません。

SDWANHELP-735: 10.2.0 および 10.2.1 リリースで PE として設定された 1100 プラットフォームエディションでは、アクティブ **OS** パーティションが完全にフルであることを示す警告が表示されます。

10.2.2 リリースにアップグレードした後、1100 アプライアンスを手動で再起動する必要があります。

SDWANHELP-736: 2 ボックス展開モードでの設定変更時に、SD-WAN サービスが中断されることがあります。

SDWANHELP-742: アプリケーション **QoS** 規則の数が **IP** ベースの **QoS** 規則を超えると、STS バンドル収集中に SD-WAN サービスが中断されることがあります。

SDWANHELP-746: 2 つの異なるファイアウォールルールを作成する際に、プロトコルが異なる場合でも、IP アドレスとポート番号が同じ場合、監査エラーが発生することがあります。

SDWANHELP-748: ライセンスは複数のサイトに適用されません。

SDWANHELP-754: DHCP 設定を削除しても、DHCP リレーや DHCP オプションセットなどのサブオブジェクトは、古いエントリとして残ります。

親 DHCP 要素を削除するときに、すべての子オブジェクトを削除する必要があります。

SDWANHELP-768: 5100 プレミアムエディション (PE) 仮想 WAN サービスは、シグナリングチャネルの確立時に再起動します。これは、複数の WANOP パケットエンジン間の一時的なポートの競合が原因で発生します。

SDWANHELP-795: 次の場合、パス帯域幅テストが中断されます。

- パス帯域幅テストは、仮想パスがダウンまたは無効になっているために MCN から分離されたブランチで実行されます。
- MCN は、ブランチが起動すると、ブランチ WAN リンクプロパティの変更を実行します。

SDWANHELP-799: ネイバールータからのコスト「AS」の OSPF プレフィクスを SD-WAN ラーニングし、ピアの SD-WAN デバイスへのエクスポートを許可します。再配布コストがネイバールータで外部から変更された場合（BGP および RIP を OSPF メトリックコスト変更に再配布するなど）、新しく変更されたコストは、すぐに接続された SD-WAN デバイスでのみ更新されますが、ピア SD-WAN デバイスには更新されません。

SDWANHELP-801: 仮想 IP への ICMP パケットを高レートで処理し、設定更新が同時にトリガーされると、SD-WAN サービスが中断されることがあります。

SDWANHELP-808: 従来の理由により、SD-WAN はサイト設定に少数のパターンを許可しません。この特定のサイトには、その名前に APN が含まれています。SD-WAN GUI でのみ誤解を招き、サイトレベルでの操作には影響しません。

SDWANHELP-812: DBC ディスクを作成しなかったため、1100 プレミアムエディション (PE) プラットフォームで 10.2.x のプロビジョニングが失敗します。

SDWANHELP-818: ダイナミックルートが学習して収束した後、コスト変更が実行された構成更新が発生した場合、アクティブ化後にダイナミックに学習されたルートのルート ID は、列挙されたままでなく「0」にリセットされ、最適なルートも隣人。

SDWANHELP-819: SD-WAN WANOP プレミアムエディション (PE) でセキュアピアリングを正しく確立できません。

SDWANHELP-830: SD-WAN WANOP で自動セキュアピアリングに使用される CA 証明書は、アップグレード時に削除されます。これは、展開に追加された新しいデバイスに対するセキュアピアリングの形成に影響を与えます。この場合、10.2.3 へのアップグレード後に、CA 証明書を再生成し、証明書とキーのペアをすべてのサイトから削除し、自動セキュアピアリングを再確立する必要があります。

SDWANHELP-831: 210 アプライアンスの電源再投入時に、FTW リレーコントローラが初期化に失敗し、シリアル高可用性（FTW）モードに設定した場合、リレーがクローズ状態のままになる可能性があります。

SDWANHELP-846: マルチルーティングドメイン展開で仮想 IP 宛の ICMP パケットを受信すると、SD-WAN サービスが中断されることがあります。

SDWANHELP-854: まれに、無効なパケットを受信すると、システムが再起動することがあります。この問題は、パス暗号化がデフォルトの有効状態から無効になっている場合に発生することがあります。

SDWANHELP-866: LR0/TSO が有効になっているため、SD-WAN は大きなパケットをドロップします。

SDWANHELP-914: 帯域幅テストをスケジュールするパスを追加するときに、設定を適用できない。

NSSDW-16165: リージョン定義の一部として追加されたサブネットは、ルートテーブルに格納されません。

NSSDW-16825: DHCP エージェントは、サテライトモデムのように余分なパディングを使用して DHCP オファーパケットを解析できませんでした。

NSSDW-17108: WAN リンクテンプレートの設定時に最初の自動パスグループを選択すると、「グループが選択されていません」と表示されます。

NSSDW-18012: PPPoE デバイスの構成更新後に、仮想パスがダウンすることもあります。

NSSDW-19233: Windows Azure エージェントは、Azure ure のポータルによってインストールされているいくつかの拡張機能のルートパーティションでいっぱいです。

既知の問題

NSSDW-17238: XenServer で作成すると、VPXL には 4 つのインターフェイスが表示されません。

- 回避策：以下のように XenServer のカーネルパラメータを設定し、XenServer を再起動します。
  /opt/xensource/libexec/xen-cmdline —set-xen gnttab_max_frames=256

NSSDW-19132: HDX MSI セッションでは、[HDX] タブの [**HDX** ユーザーセッションレポート] の [アイドルストリーム] の一部の接続状態が無効として表示されます。

NSSDW-20154: 同じセッションに再接続すると、XenApplication および XenDesktop top サーバーによってアプリケーション関連の詳細が再送信されません。したがって、**HDX Apps** レポートのデータは、その特定のセッションでは表示されない場合があります。

NSSDW-20371: 集中ライセンスが有効な場合、古いリリースへのダウングレードでエラーがスローされます- エラー**:** ライセンスモデルの解析に失敗しました。

- 回避策：集中ライセンスを無効にして、ダウングレードを続行します。アプライアンスは猶予ライセンスを取得します。ダウングレードが完了したら、一元化されたライセンスを再度有効にし、変更管理を使用して設定を適用できます。

NSSDW-20500: 5100 PE では、ドメイン参加操作が初めて開始されると、WANOP が初期化中であることを示す警告メッセージが表示されることがあります。

- 回避策：2 分後にドメインに再参加します。

NSSDW-20527: UI により、LTE インターフェイスの PPPoE を設定できます。これは予期しない、または許可されません。

NSSDW-27727: IXGBEVF ドライバーを使用する VPX および VPXL インスタンスを持つネットワークは、SR-IOV が有効なときに特定のインテル 10 GB NIC で使用され、11.0 にアップグレードすることはできません。これにより、接続が失われる可能性があります。この問題は、SR-IOV が有効な AWS インスタンスに影響することが知られています。

制限事項

- **HDX** ユーザーベースのレポートは、XenApp および XenDesktop サーバーのバージョン 7.17 以降でのみ表示されます。
- HDX セッションで公開されたアプリケーションは閉じられたと報告されます。つまり、SD-WAN が Xen **Application/Xen** デスクトップサーバーからアプリケーション終了時刻を受信した場合のみ、アプリケーションの終了時刻が **HDX Apps** レポートに表示されます。

  一部のアプリは、アプリ終了時間が受信されない場合に閉じられた場合でもアクティブであると報告されます。
- アプライアンス上で HDX セッション情報が使用できないために意図しないエラーが発生した場合は、構成エディタで HDX ユーザーレポートが有効になっていても、**HDX** ユーザーベースのレポートは表示されません。

  場合によっては、レポート内のユーザー名、サーバー名、サーバーバージョン、ICA RTT などのいくつかのフィールドが **NA** として表示されます。

Citrix SD-WAN 11.0.1 リリースノート

May 10, 2021

はじめに

このリリースノートでは、SD-WANStandard Edition、WANOP、Premium Edition アプライアンス、および SD-WAN センター用の Citrix SD-WAN ソフトウェアリリース 11.0 バージョン 1 に適用される修正された問題と既知の問題について説明します。

以前のリリースバージョンについては、docs.citrix.com のCitrix SD-WANドキュメントを参照してください。

解決された問題

SDWANHELP-981: **SD-WAN Center** 経由の **Azure** 仮想 **WAN** の自動展開で、VPN 構成と関連ルートをダウンロードまたは適用できませんでした。

NSSDW-17552: 11.0 リリースでは、ユーザーまたはソフトウェアのアップグレードによってアプライアンスが再起動された場合、変更管理がパッケージの準備時にフリーズすることがあり、ユーザーがその後の構成更新を実行できないことがあります。

NSSDW-20755: 11.0 リリースにアップグレードした後、SD-WAN アプライアンスがグレースライセンスモードに移行しました。

NSSDW-20901: SD-WAN スタンダードおよびプレミアムエディションの CLI への TACACS および RADIUS ユーザ認証が失敗しました。

NSSDW-20905: 構成エディタを使用した制限チェックが正しくないため、仮想パスへの静的パスの追加が失敗しました。

既知の問題

NSSDW-17238: XenServer で作成すると、VPXL には 4 つのインターフェイスが表示されません。

- 回避策: 次のように XenServer のカーネルパラメータを設定し、XenServer を再起動します。 */opt/xensource/libexec/xen-cmdline –set-xen gnttab_max_frames=256*

NSSDW-19132: HDX MSI セッションでは、[HDX] タブの [**HDX** ユーザーセッションレポート] の [アイドルストリーム] の一部の接続状態が無効として表示されます。

NSSDW-20154: 同じセッションに再接続すると、XenApplication および XenDesktop top サーバーによってアプリケーション関連の詳細が再送信されません。したがって、**HDX Apps** レポートのデータは、その特定のセッションでは表示されない場合があります。

NSSDW-20371: 集中ライセンスが有効な場合、古いリリースへのダウングレードでエラーがスローされます- エラー**:** ライセンスモデルの解析に失敗しました。

- 回避策: 集中ライセンスを無効にして、ダウングレードを続行します。アプライアンスは猶予ライセンスを取得します。ダウングレードが完了したら、一元化されたライセンスを再度有効にし、変更管理を使用して設定を適用できます。

NSSDW-20500: 5100 PE では、ドメイン参加操作が初めて開始されると、WANOP が初期化中であることを示す警告メッセージが表示されることがあります。

- 回避策: 2 分後にドメインに再参加します。

NSSDW-20527: UI により、LTE インターフェイスの PPPoE を設定できます。これは予期しない、または許可されません。

NSSDW-27727: IXGBEVF ドライバーを使用する VPX および VPXL インスタンスを持つネットワークは、SR-IOV が有効なときに特定のインテル 10 GB NIC で使用され、11.0.1 にアップグレードすることはできません。これにより、接続が失われる可能性があります。この問題は、SR-IOV が有効な AWS インスタンスに影響することが知られています。

Citrix SD-WAN 11.0.2 リリースノート

May 10, 2021

はじめに

このリリースノートでは、SD-WANStandard Edition、WANOP、Premium Edition アプライアンス、および SD-WAN センター用の Citrix SD-WAN ソフトウェアリリース 11.0 バージョン 2 に適用される新機能、修正された問題、および既知の問題について説明します。

以前のリリースバージョンの詳細については、Citrix SD-WANのマニュアルを参照してください。

新機能

1100 プラットフォームでの Palo Alto 統合

Palo Alto Networks の次世代ファイアウォール VM シリーズ（VM 50 および VM 100）は、SD-WAN 1100 プラットフォーム上でホストされています。

ユーザーアカウント—ネットワーク管理者

新しいユーザアカウント権限レベル **Network Admin** が導入されました。ネットワーク管理者は、ネットワーク設定への読み取り/書き込み権限のみを持っています。

ルーティングドメイン

次のルーティングドメインのユースケースがサポートされています。

- ルーティングドメインはサイトを通過できますが、サイトには終了ポイントがありません。
- ルーティング可能な IP がないルーティングドメインが存在することを許可します。

ドメイン名ベースのアプリケーションの分類

DPI 分類エンジンが拡張され、ドメイン名とパターンに基づいてアプリケーションを分類できるようになりました。分類されたドメイン名ベースのアプリケーションは、次の設定に使用されます。

- DNS プロキシ
- DNS トランスペアレントフォワーダ
- アプリケーションオブジェクト
- アプリケーションルート
- ファイアウォールポリシー
- アプリケーション QoS ルール
- アプリケーション QoE

証明書の認証

証明書ベースの認証は、Citrix SD-WAN 11.0.2 で導入されました。これにより、組織はプライベート認証局によって発行された証明書を使用して、サイト間の仮想パスを確立する前にアプライアンスを認証できます。

解決された問題

SDWANHELP-779: SD-WAN パッケージアップグレードトラフィックが遅く、ネットワーク内の順序外パケットを最適に処理しません。

SDWANHELP-896: SA が頻繁に作成および破棄される動的仮想パスまたはセキュリティアソシエーション **(SA)** ライフタイムが短い展開では、サービス中断エラーが発生することがあります。

SDWANHELP-899: ルール設定の更新で競合状態が発生する可能性があり、データパスが中断されることがあります。

SDWANHELP-901: システムに高可用性があり、多くの仮想パスがある場合、他のピアから多くのルート更新イベントが使用できるたびに、ピアへのルートの同期を見逃す可能性があります。

SDWANHELP-919: 負荷がかかり、TTL の有効期限パケットの到着率が高い場合、[モニタリング**] > [**フロー] でフィルタを適用すると、サービスがクラッシュする可能性があります。これにより、HA 展開で高可用性 (HA) スイッチオーバーが発生します。

SDWANHELP-934: 次の場合、アドレス解決プロトコル（ARP）要求を送信します（これは送信しないでください)。

- 仮想ルータ冗長プロトコル（VRRP）インスタンスは無効状態です。
- ピアルータから受信した Gratuitous ARP（GARP; アドレス解決プロトコル）要求。

この問題は、VRRP が設定され、インスタンスが無効になっている場合に発生します。

SDWANHELP-945: コンフィギュレーションエディタで [**BGP**] セクションで [**Audit**] をクリックすると、**OSPF** が設定されていない場合でも OSPF セクションに移動します。

SDWANHELP-947: 従量課金リンクで報告された使用量が異常に高い。

SDWANHELP-950: MIB で公開されているスカラー OID が有効な応答を返していません。

SDWANHELP-978: SD-WAN 210 アプライアンスを再起動すると、LTE モデムが失われます。これは、電源を入れ直してモデムをオンラインに戻す必要がある断続的な問題です。

SDWANHELP-981: **SD-WAN Center** を介した **Azure** 仮想 WAN の自動展開で、VPN 構成と関連ルートをダウンロードして適用できませんでした。

SDWANHELP-999: ファイル名に複数の‘.’を含むライセンスファイルを削除できません。

SDWANHELP-1004: 静的 VP、DVP、イントラネット/インターネットサービスが WAN リンクで有効になっている場合、WAN から LAN 方向に割り当てられた帯域幅共有を取得できません。

SDWANHELP-1009: まれに、イントラネットまたは LAN IPSec パケットの一部が無効な宛先 MAC アドレスで送信され、ネットワーク内でパケットが失われたりドロップされたりすることがあります。

NSSDW-17552: ユーザーまたはソフトウェアのアップグレードによってアプライアンスが再起動された場合、パッケージを準備するときに変更管理がフリーズし、ユーザーがその後の構成更新を実行できないことがあります。

NSSDW-17238: XenServer で作成すると、ビルドルート VPXL には 4 つのインターフェイスが表示されません。

既知の問題

NSSDW-21802: **2** ボックス配置で、WANOP で 2 ボックスモードが無効になり、変更管理が仮想 WAN で実行された場合、WANOP で 2 ボックスモードを再度有効にすると、WCCP キャッシュ IP は断続的に入力されません。

回避策: WANOP GUI から 2 ボックスモードを無効にしてから再度有効にします。

NSSDW-21808: SD-WAN Center でプロビジョニングされたアプライアンス情報は、SD-WAN アプライアンスでの実際のプロビジョニング解除操作が完了する前にクリアされます。

回避策: SD-WAN Center GUI で、[構成] > [ホストされたファイアウォール] > [ホストされたファイアウォールサイト] > [プロビジョニング] に移動し、プロビジョニング解除された失敗したサイトを選択し、プロビジョニングを開始してサイト情報を復元します。

NSSDW-21806: PPPoE インターフェイスグループの場合、AC 名、サービス名、ユーザ名を大文字に設定すると、エントリは小文字に変わります。これにより、アクセスコンセントレータ（ISP）からの IP 学習で問題が発生する可能性があります。

回避策: [AC 名] と [サービス名] に値を設定しないか、小文字を使用します。

NSSDW-21873: カスタムアプリケーションは SD-WAN Center で報告されません。

回避策: カスタムアプリケーションをアプリケーションオブジェクトに追加し、アプリケーションオブジェクトのレポートを有効にします。

NSSDW-20371: Citrix SD-WAN 10.2.3 またはそれ以前のバージョンにダウングレードすると、「ライセンスモデルの解析に失敗しました」というエラーメッセージが表示され、集中ライセンスが有効になり、ライセンスレートが自動に設定されます。

回避策: Citrix SD-WAN 10.2.4 にダウングレードします。

NSSDW-27727: IXGBEVF ドライバーを使用する VPX および VPXL インスタンスを持つネットワークは、SR-IOV が有効なときに特定のインテル 10 GB NIC で使用され、11.0.2 にアップグレードすることはできません。これにより、接続が失われる可能性があります。この問題は、SR-IOV が有効な AWS インスタンスに影響することが知られています。

Citrix SD-WAN 11.0.3 リリースノート

May 10, 2021

はじめに

このリリースノートでは、SD-WANStandard Edition、WANOP、Premium Edition アプライアンス、および SD-WAN センター用の Citrix SD-WAN ソフトウェアリリース 11.0 バージョン 3 に適用される新機能、修正された問題、および既知の問題について説明します。

以前のリリースバージョンの詳細については、Citrix SD-WANのマニュアルを参照してください。

> 注
>
> - CVE-2019-19781-Citrix SD-WAN WANOP アプライアンスの脆弱性（4000-WO、4100-WO、5000-WO、5100-WO プラットフォームモデルのみに適用）がリリース 10.2.6b で修正されました。詳しくは、「CVE KB」を参照してください。
> - 11.0.3.1018 リリースにはセキュリティ修正が含まれています。このパッチは、Amazon Web Services すべてのお客様に適用することをお勧めします。

新機能

Microsoft 仮想 WAN に対する複数のハブのサポート

11.0.3 リリースでは、1 つのブランチを Azure Virtual WAN リソース内の複数のハブに接続できます。1 つの Azure 仮想 WAN リソースを、複数のオンプレミスのブランチサイトに接続できます。IPsec トンネルを確立するには、ブランチサイトを Azure WAN リソースに関連付ける必要があります。

SD-WAN Standard Edition (SE) VPX パスワードの変更

11.0.3 以降のリリースでは、SD-WAN アプライアンスの Provisioning 時または新しい SD-WAN SE VPX のデプロイ時に、デフォルトの admin ユーザーアカウントパスワードの変更が必須です。この変更は、CLI と UI の両方を使用して適用されます。

システムメンテナンスアカウント（CBVWSSH）は、開発およびデバッグ用に存在し、外部ログイン権限はありません。このアカウントには、通常の管理ユーザーの CLI セッションからのみアクセスできます。

SD-WAN 210-LTE ファームウェアのアップグレード

11.0.3 リリースでは、シングルステップアップグレードパッケージの一部として LTE アクティブファームウェアが更新されます。アップグレードするには、[**Change Management Setting**] ページを使用してスケジュールウィンドウを更新するか、LTE ファームウェアをアップグレードするためのデフォルトのスケジュールされた時刻（毎日 21:20:00）を待機する必要があります。

解決された問題

SDWANHELP-941: 設定の更新中、仮想パス変更イベントのリセットを見逃し、対応する仮想パスがダウンしてもルートをダウンさせない、このバグが発生する可能性があります。

SDWANHELP-961: この問題は、SD-WAN 4000 および 5000 WANOP アプライアンスに影響を与える可能性があります。アプライアンスが 10.1.0 ～10.2.5 を 1 年以上実行すると、ログに保存されるデータが多すぎるという障害が発生する可能性があります。

SDWANHELP-988: RADIUS および **TACACS+** ユーザは、SD-WAN Center UI から診断パッケージを生成できません。ターミナル経由の診断パッケージの作成が、すべてのユーザーに対して失敗しています。[構成**] > [**ライセンス] オプションは、SD-WAN Center UI では使用できません。

SDWANHELP-1000: 高可用性（HA）セットアップで NetFlow を有効にすると、リソース不足により HA フラップが発生します。

SDWANHELP-1023: NAT 変換後にパケットが誤ってルーティングされると、SD-WAN サービスの再起動が発生することがあります。

SDWANHELP-1035: MCN および RCN 経由でリモートサイトにルートが正しく伝播されません。

SDWANHELP-1042: 既存の HDX セッションで切断された公開アプリケーションをユーザーが再起動して閉じると、SD-WAN がクラッシュする。

SDWANHELP-1049: XenServer ベースのプラットフォーム上の仮想 WAN 仮想マシン（VM）は、時間の経過とともに大きな時間オフセットを持つことがあります。この場合、再起動後に仮想 WAN VM の時刻が不正確になります。

SDWANHELP-1051: ライセンスサーバのバージョンが v11.16.3 未満の場合、11.16.3 未満のすべてのレガシーライセンスサーバに何らかのサービス拒否 (DOS) 攻撃が発生する可能性があります。

SDWANHELP-1070: 時刻が変更された後、ハードウェアクロックに同期されません。たとえば、手動による時刻更新や NTP 時刻更新などです。

SDWANHELP-1088: PAC ファイル機能が有効になった後にアプライアンスを再起動すると、SD-WAN アプライアンスの GUI ページの一部が応答しなくなることがあります。

SDWANHELP-1095: EPSV モードまたは EPRT モードを使用して FTP セッションが失敗した場合、FTP アプリケーション層ゲートウェイ (ALG) は FTP セッションを正しく解析しない可能性があります。

SDWANHELP-1112: BGP 自律システム（AS）番号は 32 ビット番号をサポートします。

SDWANHELP-1113: 11.0.2 にアップグレードした後、WANOP のみのプラットフォーム上で管理 GUI に断続的にアクセスできない。

SDWANHELP-1116: 設定の更新中に、高可用性（HA）フラップが原因で同期イベント処理が失われて、アプライアンスが問題状態になり、他のブランチとのルート同期が行われず、ネットワーク停止につながる可能性があります。

SDWANHELP-1123: DHCP インターフェイスだけでルーティングドメインを設定すると、監査エラーが表示されます。

SDWANHELP-1160: Citrix SD-WAN Center では、構成エディタのサイトの WAN リンクの下に重複する IP アドレスが表示されます。この問題は、任意の 2 つの WAN リンク IP アドレスの 4 番目の数字が同じ数字で始まり、4、45、486 などの桁数によって異なる場合に発生します。

SDWANHELP-1164: SD-WAN Center からアプライアンス設定を転送する際に、アプライアンス設定のパスワードにドル記号の後に文字が含まれていると、転送は失敗します。たとえば、パスワード test$1、test$1$d は失敗します。しかし、test1 $ は動作します。

SDWANHELP-1169: 削除保留中の DVP に対するパケットの転送がスケジュールされている場合、サービスは中止されます。ソフトウェアは、誤って空のパケットリストから削除しようとします。ソフトウェアが更新されました。

SDWANHELP-117: 構成データベース内のいくつかの孤立エントリのために、config_editor/virtual_paths の GET API が応答とともにいくつかの例外をスローします。カスケード削除 が修正され、孤立したデータベースエントリが回避されました。

SDWANHELP-1189: ソフトウェアアプライアンスのアップグレード中に、SD-WAN 210 Standard Edition（SE）アプライアンスでインストールプロセスが失敗することがあります。障害検出時に、アプライアンスは自動的に再起動して問題を回避し、アップグレードを続行します。

SDWANHELP-1201: LTE モデムは、単独で散発的に再起動できます。データセッションの開始時に、モデムはエラーを報告し続けます。サービスはサポートされていません。この問題を解決するには、モデムを自動的に無効にして再度有効にして障害を回復します。

SDWANHELP-1385: SD-WAN 210 プラットフォーム上の BIOS ファームウェア v1.0b の問題により、SD-WAN デバイスのシリアル番号情報が失われ、デフォルト文字列にリセットされることがあります。

SDWANHELP-1365：ワンツー **WAN** 転送を有効にした高可用性 GEO MCN セットアップでは、インターネットサービスダウンイベントによって、セカンダリ GEO MCN から学習されたルートがプライマリ GEO MCN よりも優先される誤ったシナリオがトリガーされることがあります。

NSSDW-22847：BGP が有効の場合、デフォルトでは、SD-WAN UI で BGP の [マルチホップ] チェックボックスがオンになっていました。しかし、ユーザーが再び無効にして有効にならない限り、設定は有効になっていませんでした。

NSSDW-25032：BGP ポリシーが MED メトリックで設定され、ネイバーにバインドされている場合、Multiple Exit Discinator（MED）がネイバーにアドバタイズされませんでした。この問題は、コンパイラによって誤ったネットワーク接頭辞（32）が設定されていました。

NSSDW-25067: LTE モデムが無効になり、動作モードが **Lower Power** に切り替わる前に LTE モデムを再度有効にすると、警告メッセージまたはビジーメッセージが表示されます。修正は、有効/無効操作を実行する前に、ユーザーに警告し、現在の動作モードを表示することです。

NSSDW-25135: Zscaler の展開中に、マッピングの作成に誤った構成が使用される場合がありました。この問題は、データベース内の誤った重複エントリが原因で発生します。この修正により、データベースに重複するエントリがないことが保証されます。

NSSDW-25147: SD-WAN アプライアンスで PPPoE 機能を設定すると、ポイントツーポイントプロトコルデーモン (PPPD) が実行され、PPPoE セッションが確立されます。この設定は、バッファオーバーフローの脆弱性である CVE-2020-8597 に対して脆弱です。この問題は 11.1.0 リリース以降で修正されています。

NSSDW-25440: ネットワークアクセラレーションが有効になっているインスタンスでは、Azure で大量のパケット損失またはネットワーク遅延が発生することがあります。

NSSDW-28971: SD-WAN アプライアンスおよび仮想マシンにログインすると、ハードコードされたパスワードを使用して 11.x ベースのイメージを使用して root シェルにアクセスすることができます。影響を受ける SD-WAN プラットフォームは 110 および 11.x イメージでプロビジョニングされた VPX です。これは CLI 関連の問題であり、GUI には適用されません。

既知の問題

NSSDW-23264: SD-WAN Center のビルドが 11.x で、アプライアンスビルドが 10.x 上にある場合、リモートライセンスの取得に失敗します。

回避策： SD-WAN Center は、SD-WAN アプライアンスが構成されている 10.x と同じにビルドされます。

NSSDW-23132: 11.x へのアップグレード後、実際のトラフィック中断時間は秒単位で非常に大きな値になることがあります。

回避策**:** 後続の変更管理では正しい値が表示されます。これは表示上の問題に過ぎません。

NSSDW-23134：ネットワークを 11.x にアップグレードしたばかりのときに、ネットワークにサイトを追加しようとすると、一貫したソフトウェアプッシュが発生することがあります。

回避策：変更管理をもう一度実行します。

NSSDW-23485: MCN のアクティブな構成の名前にドット文字が含まれている場合、クラウドダイレクトは操作を許可しません。

回避策： DOT を含まない設定ファイル名を更新します。

SDWANHELP-1110: まれに、短命の動的仮想パスを継続的に作成すると、ローエンドアプライアンス（210/410）のデータパスサービスで中断が発生することがあります。

回避策：ダイナミック仮想パス（DVP）を無効にするか、短命な DVP を避けるように構成を調整します。

SDWANHELP-1159: Citrix SD-WAN は、OSPF ネイバーにルートをアドバタイズしません。これは、SD-WAN でルートが変更された場合、または仮想パスフラップが発生し、仮想 WAN ルートがサイト間で再同期される場合に発生します。この場合、OSPF ピアへのリンクが不可逆である場合、SD-WAN は SD-WAN ルートを OSPF ネイバーに対してアドバタイズしない状態になることがあります。

回避策：仮想 WAN サービスを停止して再起動します。

NSSDW-27727: IXGBEVF ドライバーを使用する VPX および VPXL インスタンスを持つネットワークは、SR-IOV が有効なときに特定のインテル 10 GB NIC で使用され、11.0.3 にアップグレードすることはできません。これにより、接続が失われる可能性があります。この問題は、SR-IOV が有効な AWS インスタンスに影響することが知られています。

システム要件

May 10, 2021

ハードウェア要件

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

ファームウェアの要件

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

> 注
>
> 以前のソフトウェアバージョンを実行しているアプライアンスでは、SD-WAN リリース 11.0 を実行しているアプライアンスへの Virtual Path 接続を確立できません。詳細については、Citrix サポートチームにお問い合わせください。

ソフトウェア要件

ライセンス要件の詳細については、ライセンスを参照してください。

ブラウザの要件

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

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

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

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

Hypervisor

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

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

クラウドプラットフォーム

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

- Microsoft Azure
- Amazon Web Services
- Google Cloud Platform

SD-WAN プラットフォームモデルとソフトウェアパッケージ

September 26, 2023

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

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

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

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

ソフトウェアパッケージをダウンロードする

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

Citrix SD-WAN ソフトウェアパッケージをダウンロードするには、URL; に移動します 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で提供されています。

Citrix SD-WAN ソフトウェアパッケージ

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

サポートされる **SD-WAN** アプライアンスモデル

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

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

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

SD-WAN アプライアンスの詳細については、製品ダウンロードサイトの SD-WAN 製品プラットフォームエディション データシート を参照してください。

SD-WAN 標準エディションのハードウェアアプライアンス

Citrix SD-WAN リリース 11.0 では、次の SD-WAN 標準エディションのハードウェアアプライアンスモデルがサポートされています。

SD-WAN SE プラットフォームモデル	役割
210-SE/210-SE LTE	小規模ブランチアプライアンス
410-SE	小規模ブランチアプライアンス
1000-SE	小規模ブランチアプライアンス
1100-SE	大規模なブランチアプライアンス
2100-SE	大規模なブランチアプライアンス

SD-WAN SE プラットフォームモデル	役割
4100-SE	データセンター-マスターコントロールノード（MCN）アプライアンス
5100-SE	データセンター-マスターコントロールノード（MCN）アプライアンス
6100-SE	データセンター-マスターコントロールノード（MCN）アプライアンス

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

Citrix SD-WAN 11.0 は、以下の SD-WAN WAN 最適化（WANOP）アプライアンスモデルをサポートしています。

SD-WAN WANOP プラットフォームモデル	役割
WANOP 800	小規模ブランチアプライアンス
WANOP 1000	大規模なブランチアプライアンス
WANOP 2000	大規模なブランチアプライアンス
WANOP 3000	大規模なブランチアプライアンス
WANOP 4100	データ・センター・アプライアンス
wANOP 5100	データ・センター・アプライアンス

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

Citrix SD-WAN 11.0 では、次の SD-WAN VPX 仮想アプライアンス（VPX-SE）モデルがサポートされています。

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

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

詳細については、Citrix SD-WAN 仮想 VPX スタンダードエディションの前提条件を参照してください。

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

Citrix SD-WAN 11.0 では、次の SD-WAN WANOP 仮想アプライアンス（VPX-WANOP）モデルがサポートされています。

SD-WAN VPX WANOP プラットフォームモデル	役割
WANOP VPX-2	小規模ブランチアプライアンス
WANOP VPX-6	小規模ブランチアプライアンス
WANOP VPX-10	小規模ブランチアプライアンス
WANOP VPX-20	小規模ブランチアプライアンス
WANOP VPX-50	大規模なブランチアプライアンス
WANOP VPX-100	大規模なブランチアプライアンス
WANOP VPX-200	大規模なブランチアプライアンス

> 重要
>
> リリースバージョン 10.1 では、エンタープライズプラットフォームエディションは「Premium Edition」にリブランドされています。

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

Citrix SD-WAN 11.0 は、次の SD-WANPremium（エンタープライズ）エディションアプライアンス（SD-WAN PE）モデルをサポートしています。

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

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

アップグレード・パス

November 8, 2021

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

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

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

> 注
>
> - Citrix SD-WAN リリース 9.3.x からアップグレードする場合は、メジャーリリースにアップグレードする前に 10.2.8 にアップグレードすることをお勧めします。
> - ソフトウェアアップグレードの実行中は、アクティブ化する前に、接続されているすべてのサイトへのステージングが完了していることを確認してください。不完全な無視（Ignore Complete）を有効にしてステージングが完了する前にアクティベーションが行われた場合、ステージングがまだ進行中のサイトの MCN で仮想パスが表示されないことがあります。ネットワークをリカバリするには、それらのサイトの

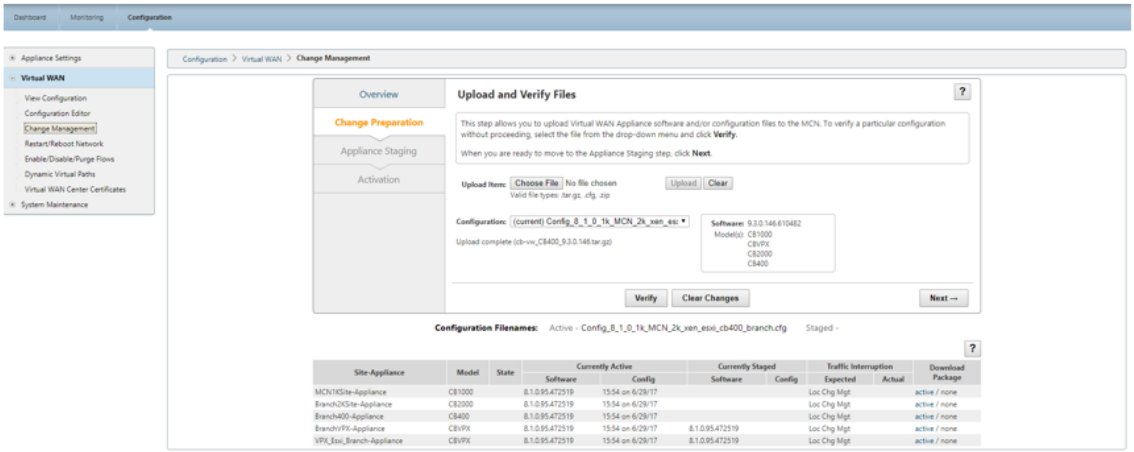
> ローカル変更管理を手動で実行する必要があります。
> - Citrix SD-WAN リリース 11.0.0 以降、SD-WAN ソフトウェアの基盤となる OS/カーネルが新しいバージョンにアップグレードされます。アップグレードプロセス中に自動再起動を実行する必要があります。その結果、各アプライアンスのアップグレードに予想される時間が約 100 秒増加します。さらに、新しい OS を含めることで、各ブランチアプライアンスに転送されるアップグレードパッケージのサイズが約 90 MB 増加します。

仮想 **WAN** ソフトウェアを **9.3.5** にアップグレードし、仮想 **WAN** 展開を正常に

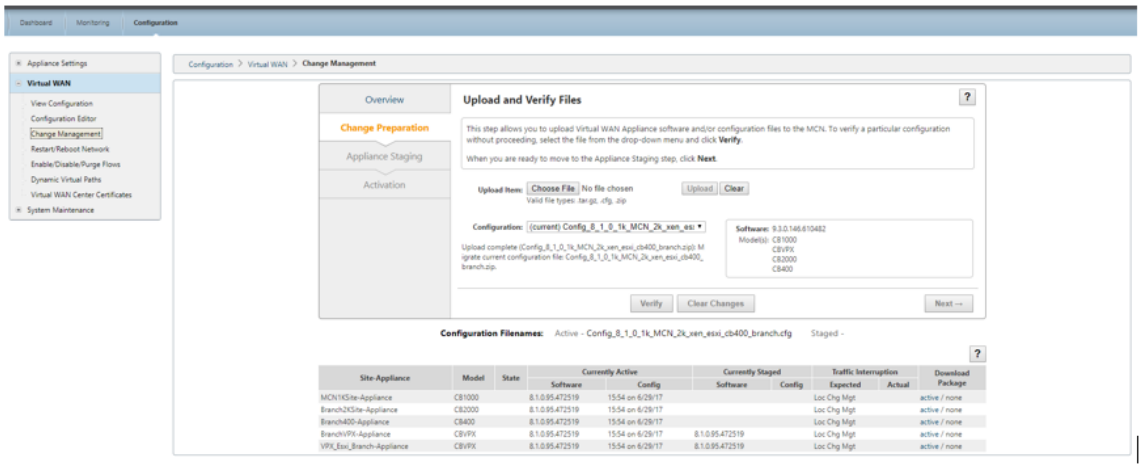
May 10, 2021

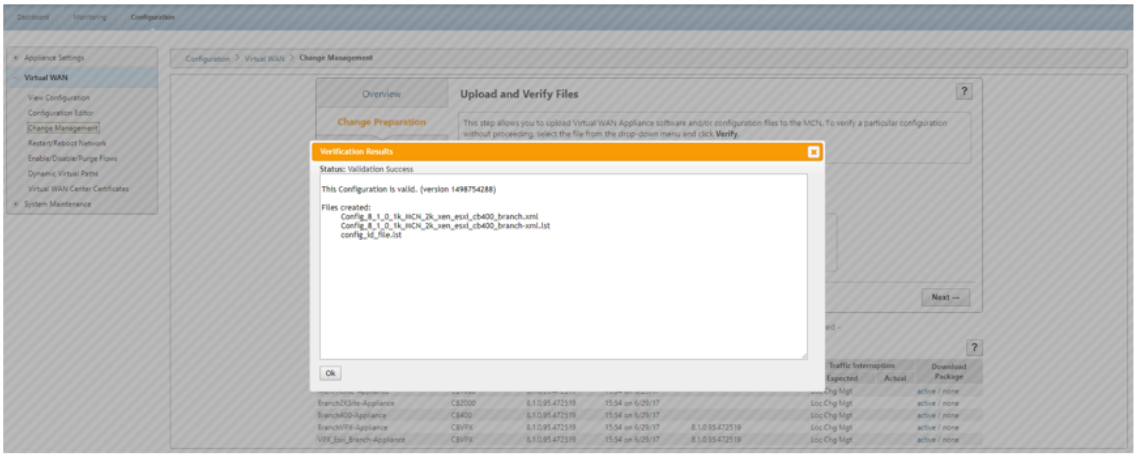
> 注:
>
> MCN からブランチサイトへの仮想パスを確立して、9.3.4 以降のビルドを実行中の仮想 WAN 構成を作成します。

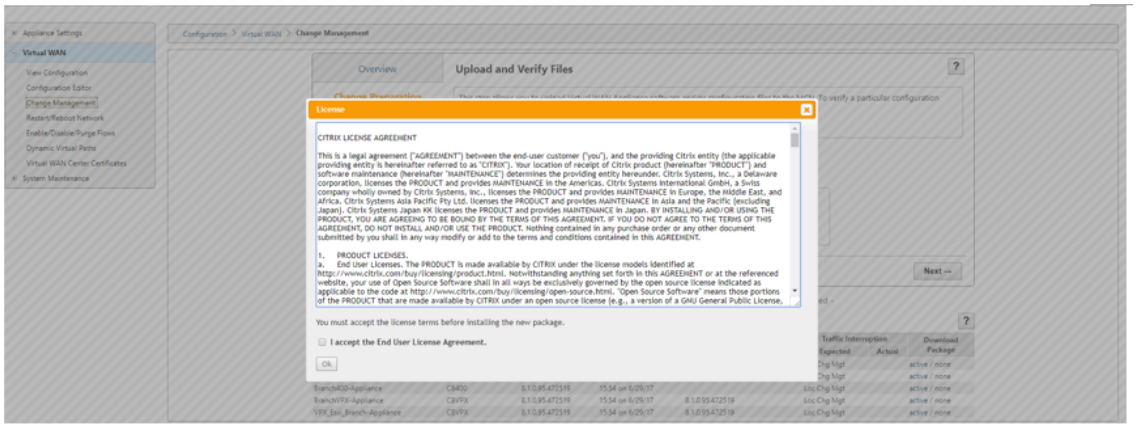
1. MCN アプライアンスで、[構成] > [仮想 **WAN**] > [変更管理] に移動します。
2. シトリックスのダウンロードページから Virtual WAN ネットワークのすべてのサイトの *cb-vw-<ApplianceModel>-9.3.5.23.tar.gz* ファイルを取得します。
3. <ApplianceModel> アップグレードを実行する必要がある構成ファイルで定義されたブランチの *cb-vw–9.3.5.23.tar.gz* ファイルをアップロードします。MCN アプライアンスの SD-WAN Web インターフェイスで変更管理を実行し、変更管理プロセス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



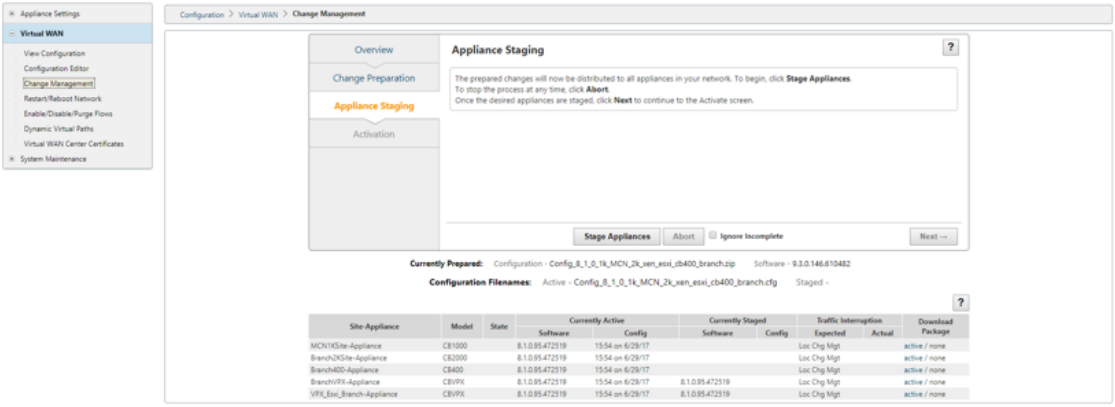
4. [次へ] をクリックして、さらに進みます。



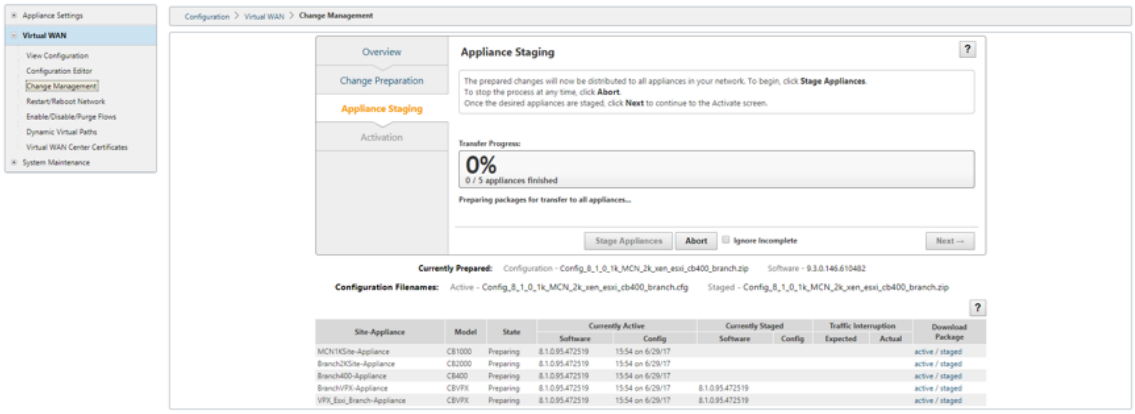


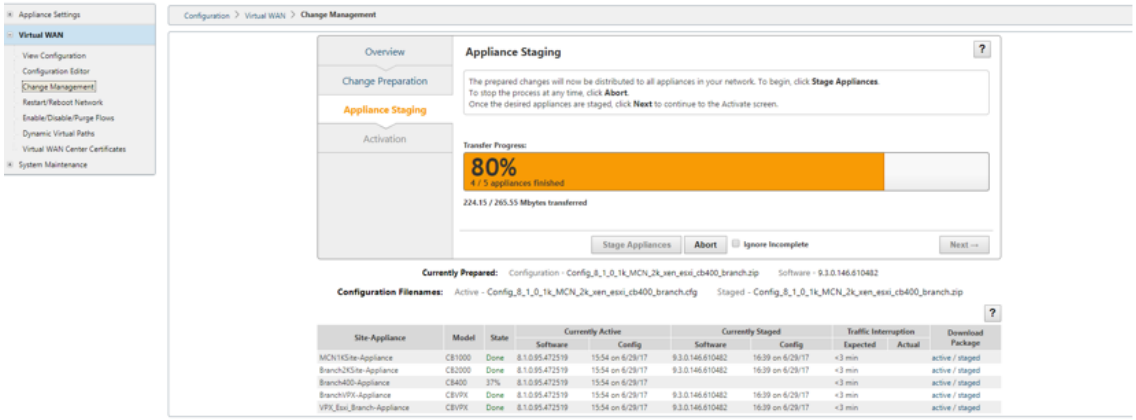


5. ライセンス契約に同意すると、アプライアンスのステージングに移動します。アプライアンスをステージングするには、アプライアンスのステージングをクリックします。

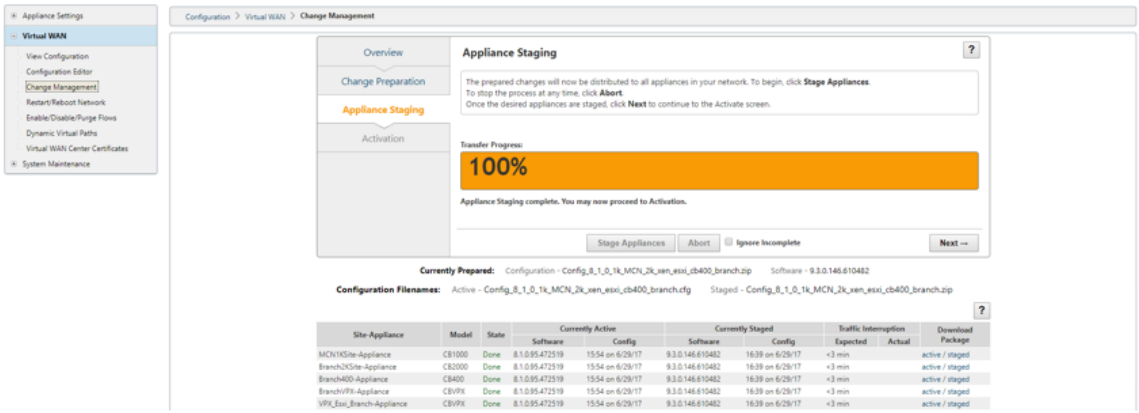


6.「転送の進行状況」ステータスは、アプライアンスにソフトウェア・パッケージを準備およびステージングの一部として表示されます。

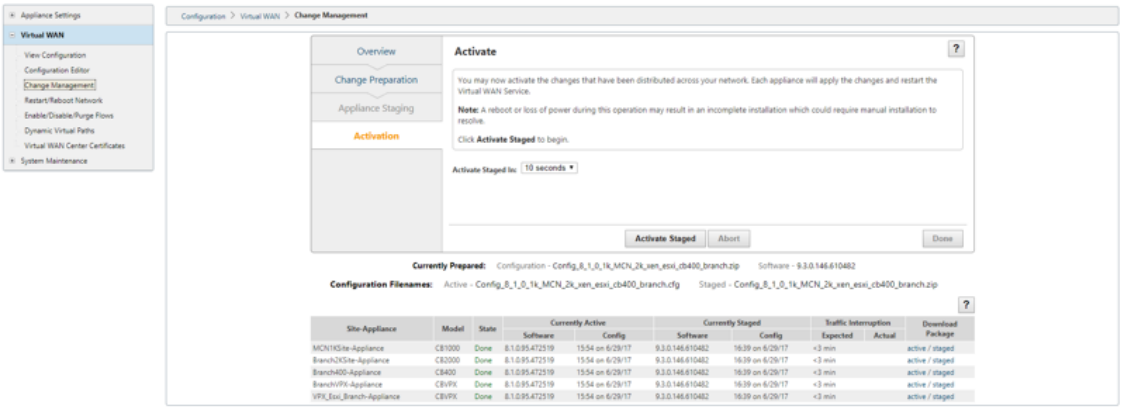


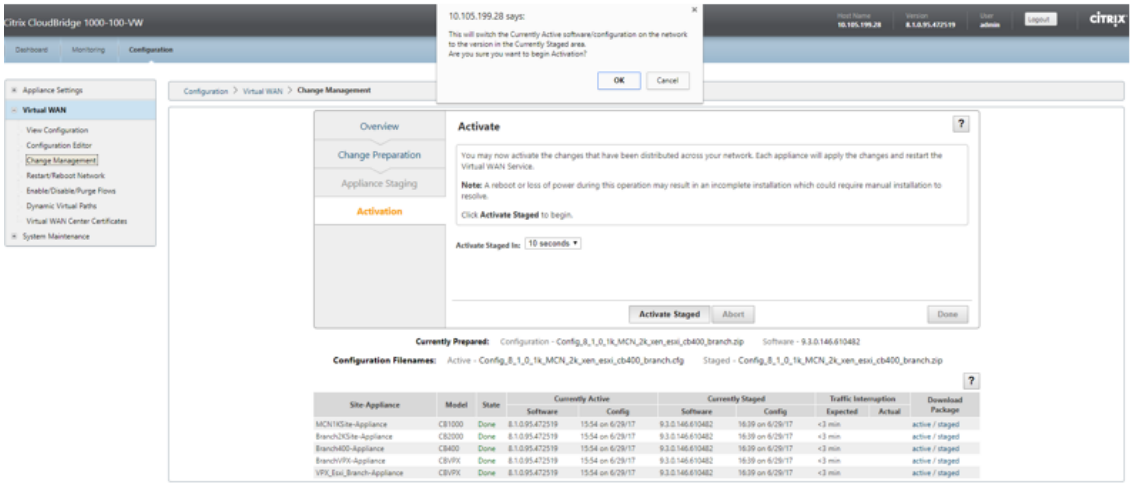


7. 転送の進行状況が 100% と表示されたら、[次へ] をクリックして続行します。

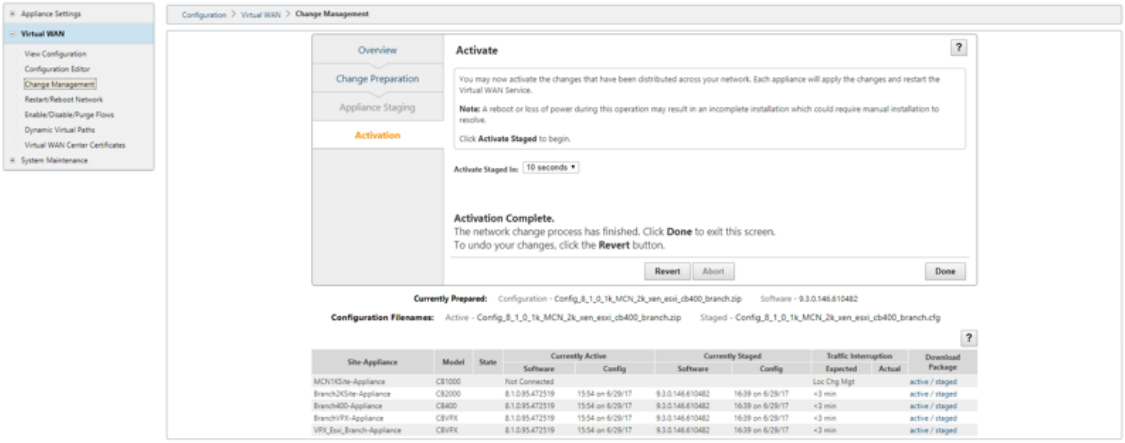


8. [アクティブ化] ページで、[ステージングのアクティブ化] をクリックしてアクティブ化を開始します。





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

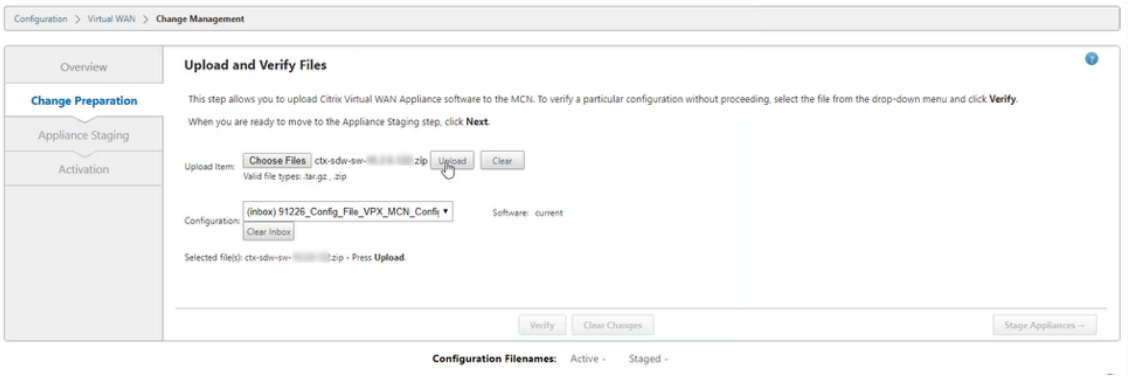


仮想 **WAN** 展開機能で **11.0** にアップグレードする

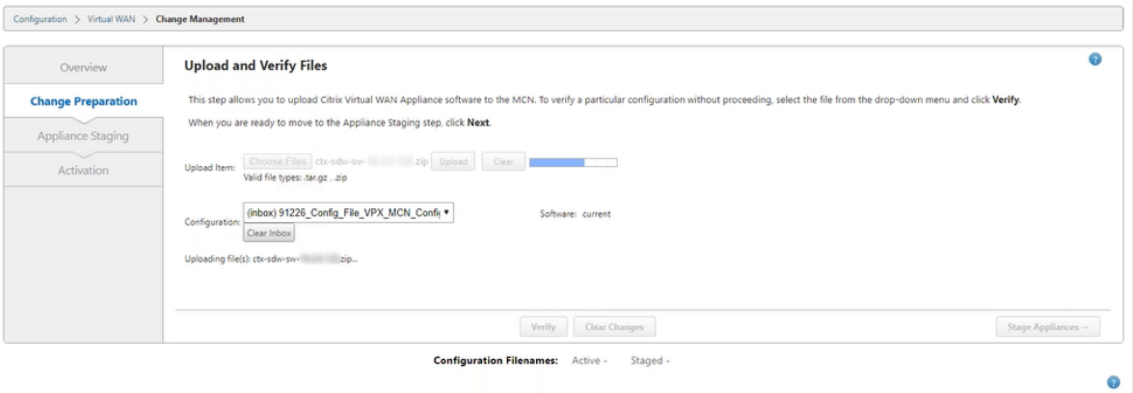
May 10, 2021

1. [変更管理**] > [**変更の準備] ページで、[ファイルの選択] をクリックし、*ctx-sdw-sw-11.0.0.x.zip* ソフトウェアパッケージファイルを選択します。［アップロード］をクリックします。

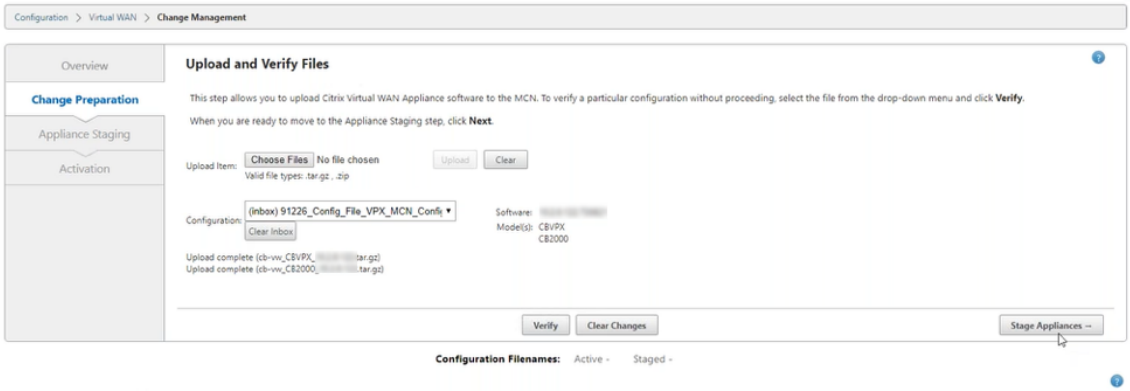
   > 注:
   >
   > ダウンロードページから Citrix SD-WAN リリース 11 ソフトウェアパッケージをダウンロードできます。



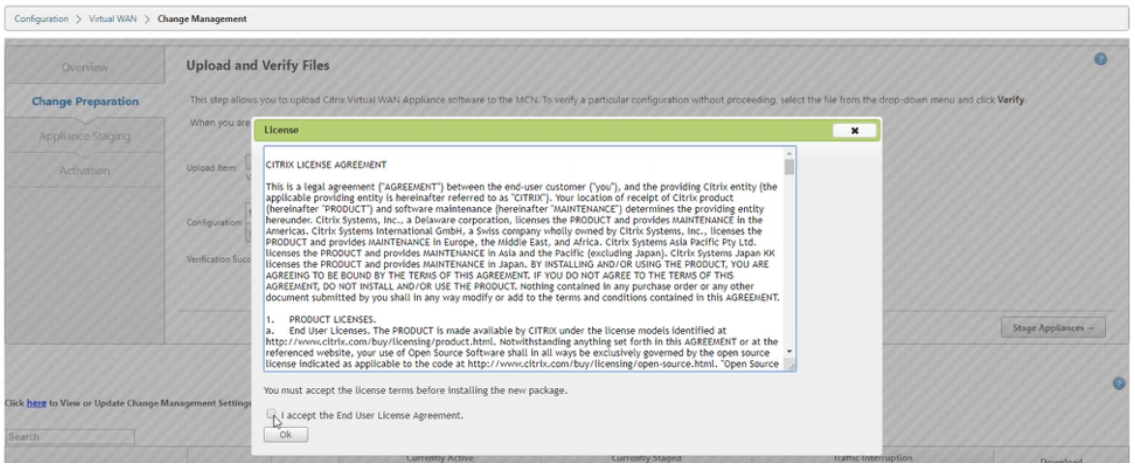
   進行状況バーが表示され、現在のアップロードの進行状況が表示されます。



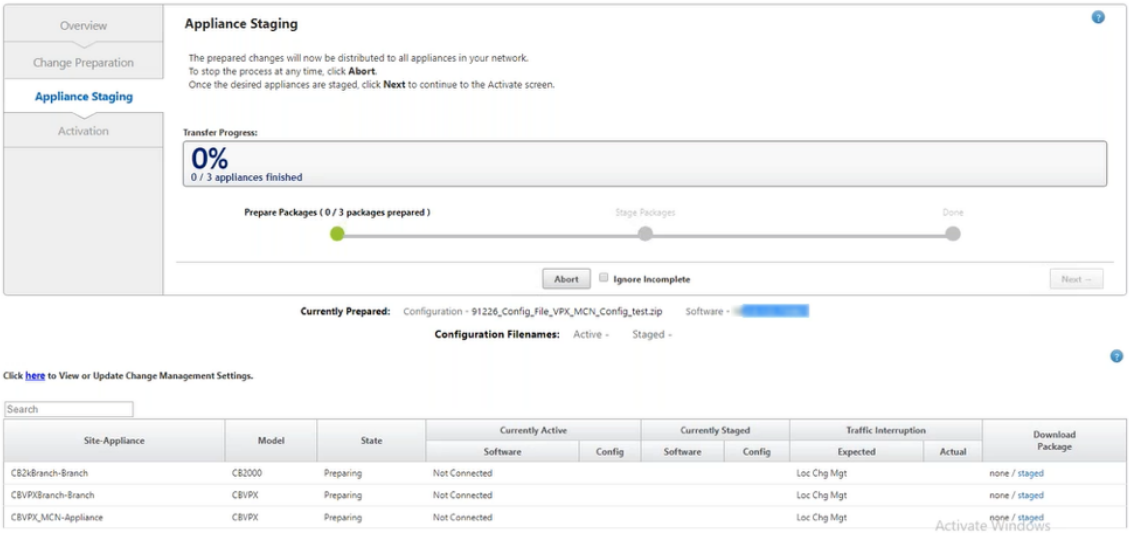
2. アップロードプロセスが成功すると、関連するアプライアンスモデルが表示されます。アプライアンスは、構成ファイルに基づいてアップグレードされます。



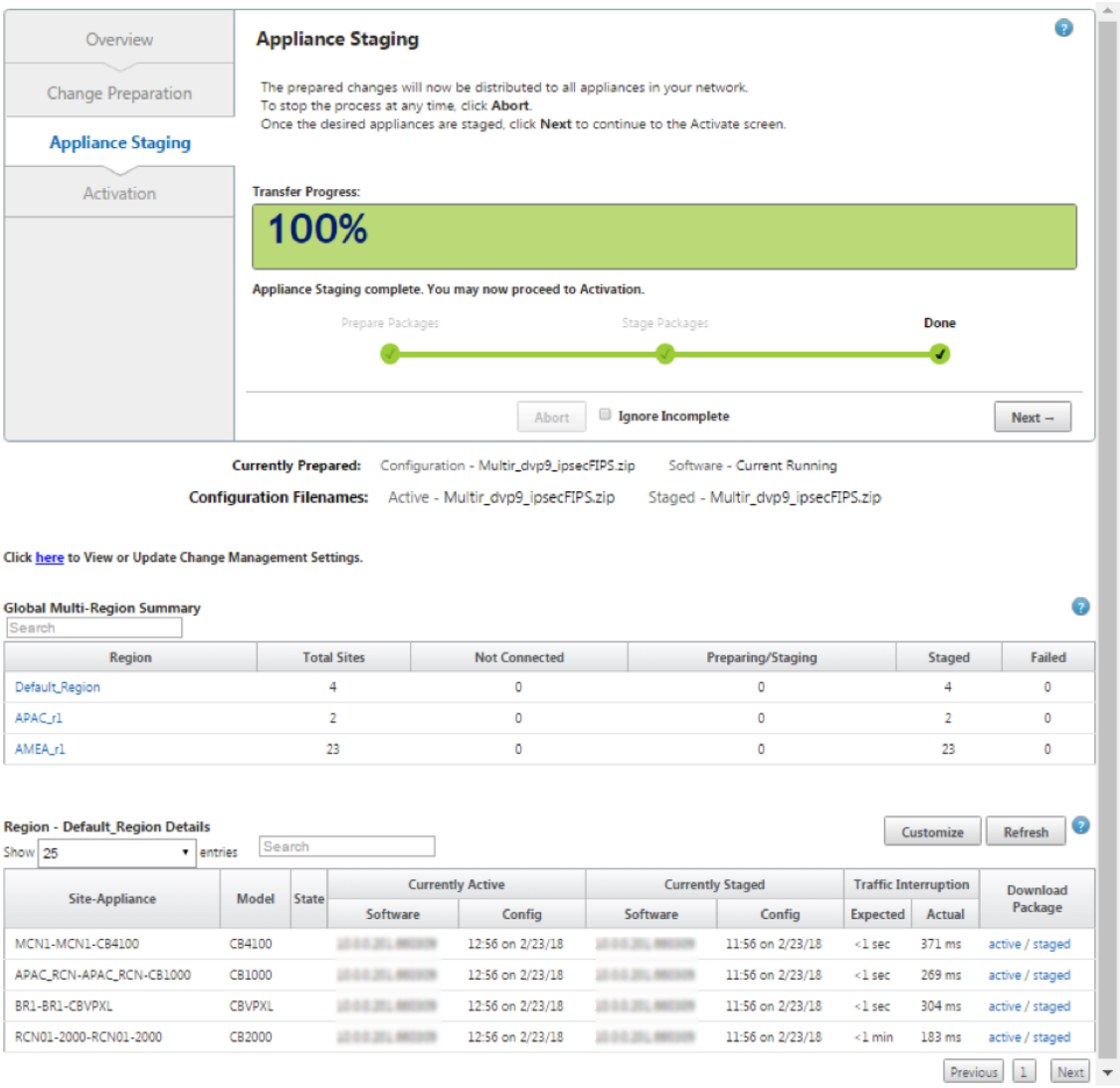
3. [**Stage Appliance**] をクリックして、構成ファイルの検証を続行します。ユーザー同意の [使用許諾契約] ページが表示されます。[使用 許諾契約書に同意 します] をクリックし、[**OK**] をクリックします。



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



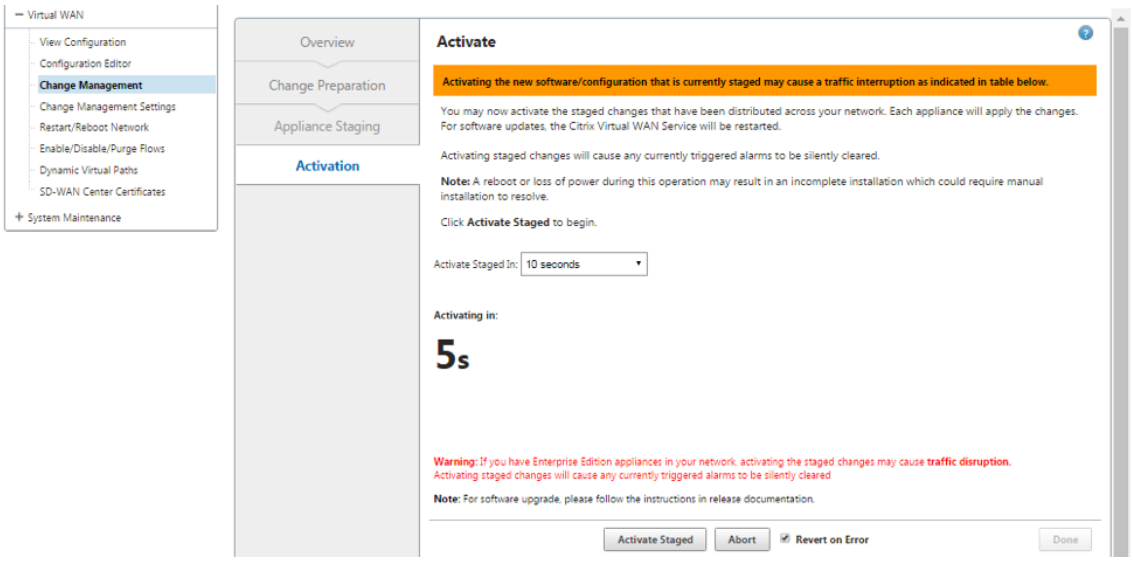
5. 転送の進行状況が 100% 完了したら、[次へ] をクリックしてアクティベーションに進みます。



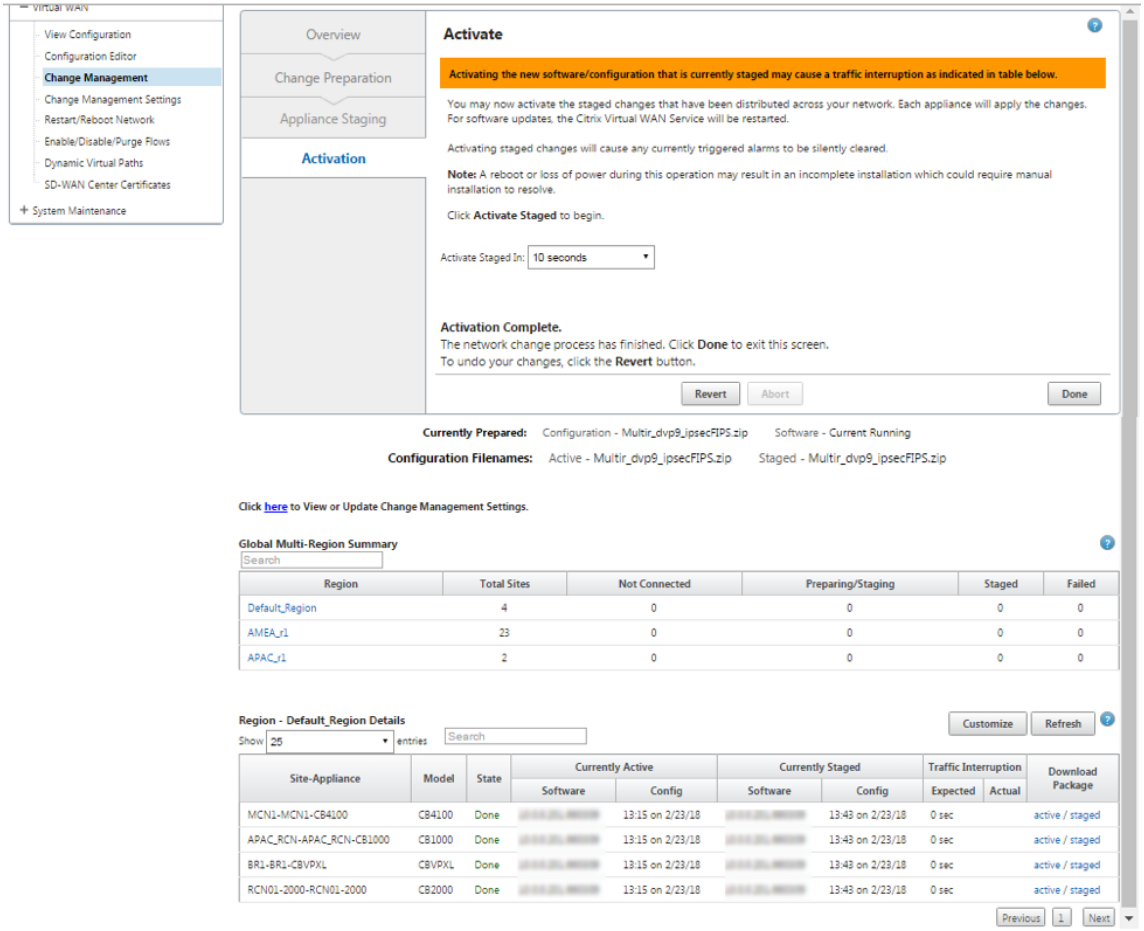
サマリーテーブルに表示されるソフトウェアパッケージ設定のさまざまな状態は、次のことを示しています。

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

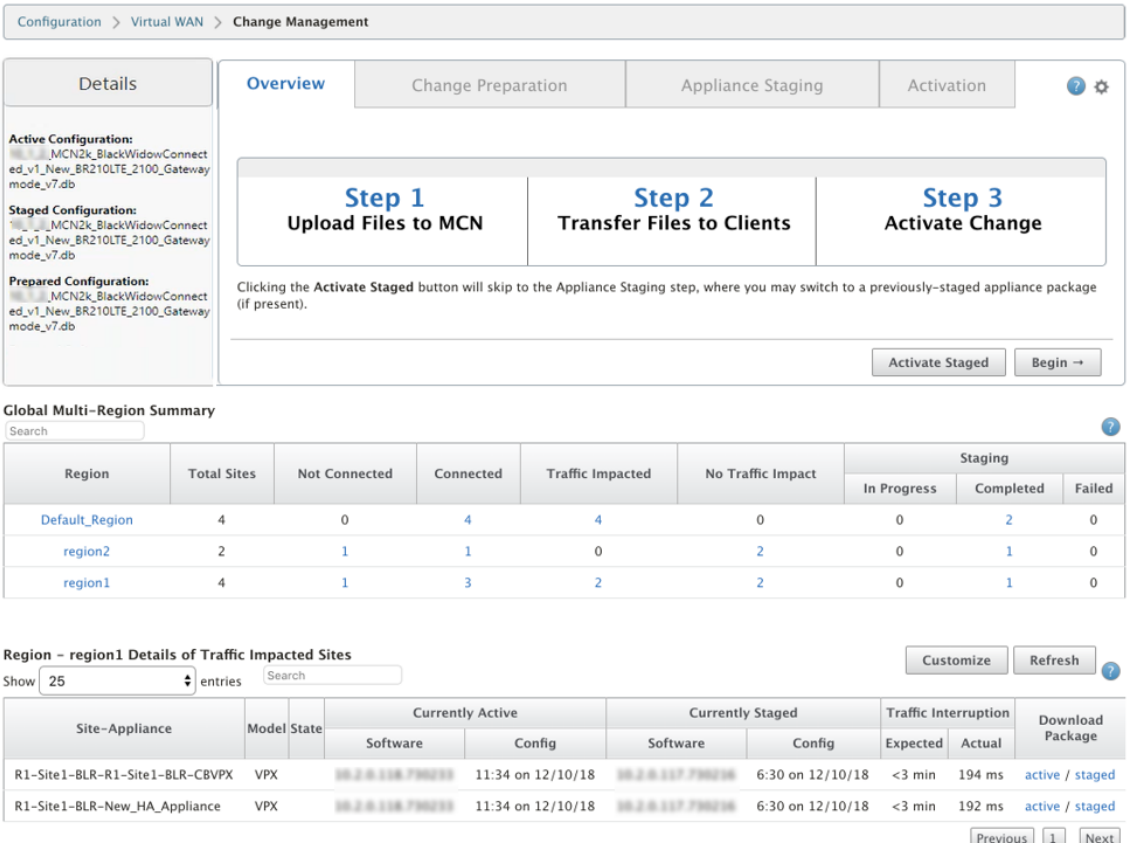
6. ステージ ングされたソフトウェアをアクティブ化するには、**[**ステージ ングされたアクティブ化] をクリックします。



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

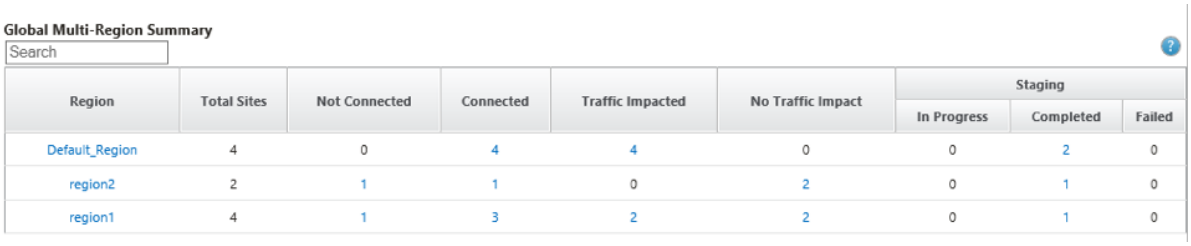


8.「変更管理」ページにナビゲートして、転送ステータスを表示します。

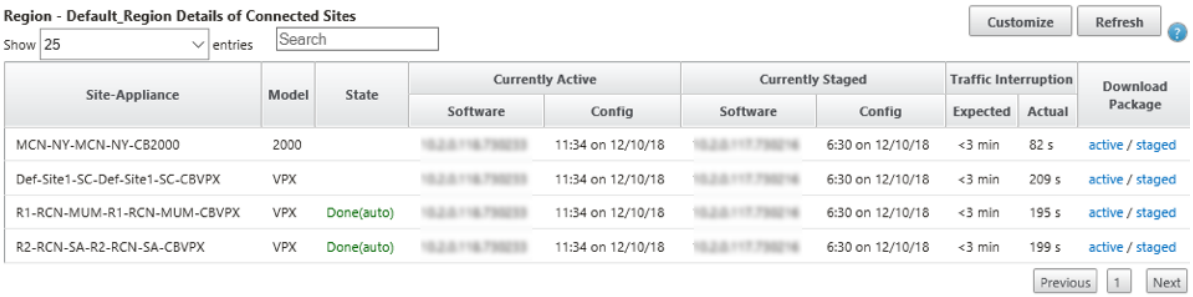


複数リージョンのサマリーテーブルには、次の詳細が表示されます。

- リージョン：リージョンの名前
- サイト合計 -地域内のサイトの合計数。
- 未接続 -リージョンに接続されていないサイトの合計数。
- **Connected**： リージョン内で接続されているサイトの合計数。
- [**Traffic Impacted**]：リージョン内のトラフィックが影響を受けるサイトの合計数。
- **No Traffic Impact**： リージョン内のトラフィックが影響を受けないサイトの合計数。
- ステージング処理中 -ローカル処理がリージョンで転送する更新パッケージを準備しようとしているサイトの合計数。
- ステージング完了-リージョンでステージングが完了したサイトの合計数。
- ステージング失敗 -リージョンで不完全な転送が削除されたサイトの合計数。



[**Global Multi-Region Summary**] テーブルエントリリンクをクリックして、リージョン固有の設定レポートをフィルタリングします。



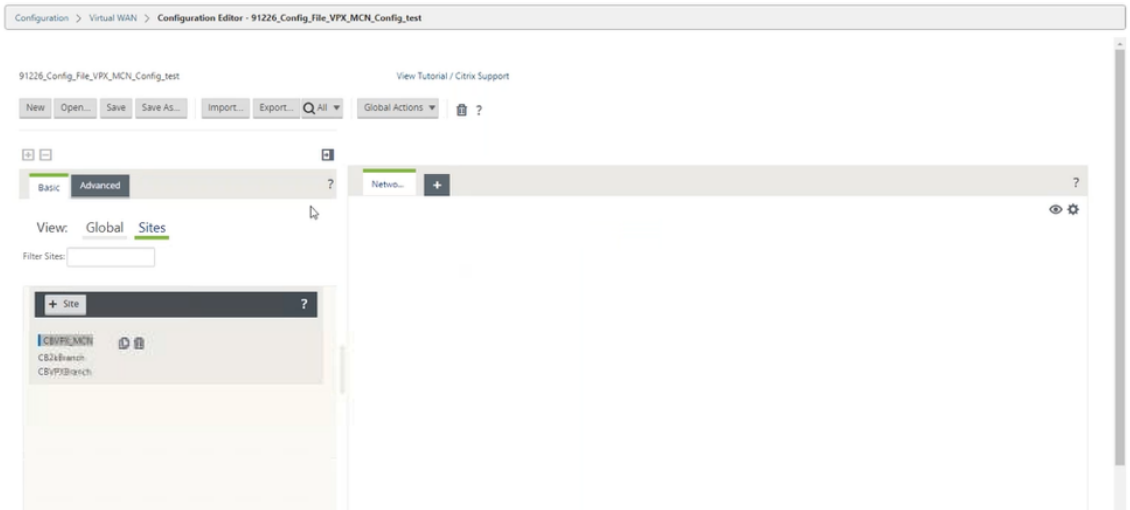
マルチリージョン展開の場合は、各 RCN で [変更管理設定] ページに移動し、依存コンポーネントのインストールをスケジュールします。デフォルトでは、MCN/RCN は、ブランチでのソフトウェアの可用性に基づいて、毎日 21:20:00 にインストールを試行するスケジュールを割り当てます。詳細については、「管理設定の変更」を参照してください。

仮想 **WAN** 展開を行わずに **11.0** へのアップグレード

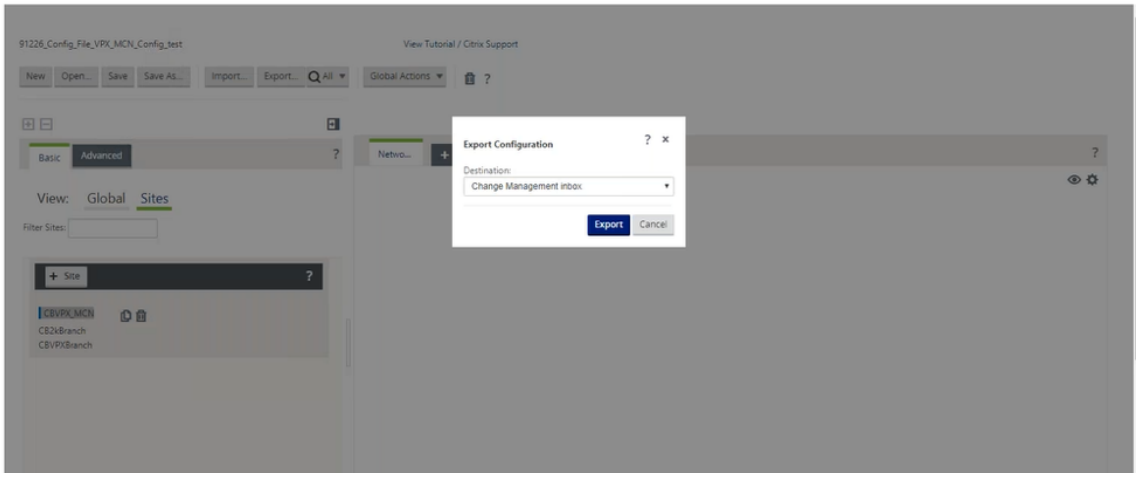
May 10, 2021

> 注: 最新の 11.0 機能を設定するには、MCN アプライアンスを 11.0 ソフトウェアにリマイアします。詳しくは、「Citrix SD-WAN アプライアンスソフトウェアの再イメージ化」を参照してください。

1. 構成 エディタを使用して構成 を準備し、有効な名前で構成を保存します。詳細については、構成を参照してください。

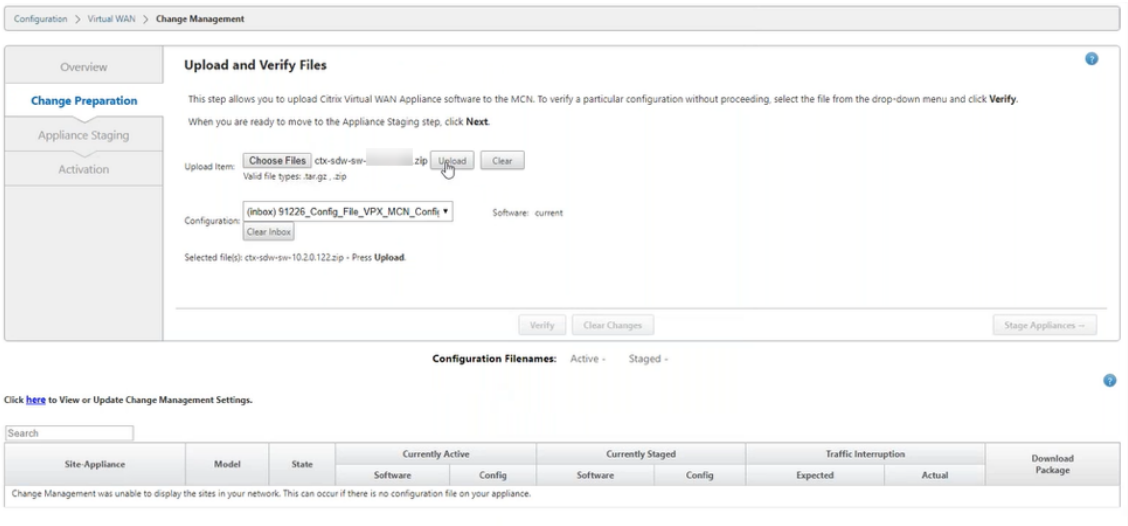


2. 保存した構成を変更管理にエクスポートします。[エクスポート] をクリックし、宛先として [変更管理の受信トレイ] を選択します。[エクスポート] をクリックします。

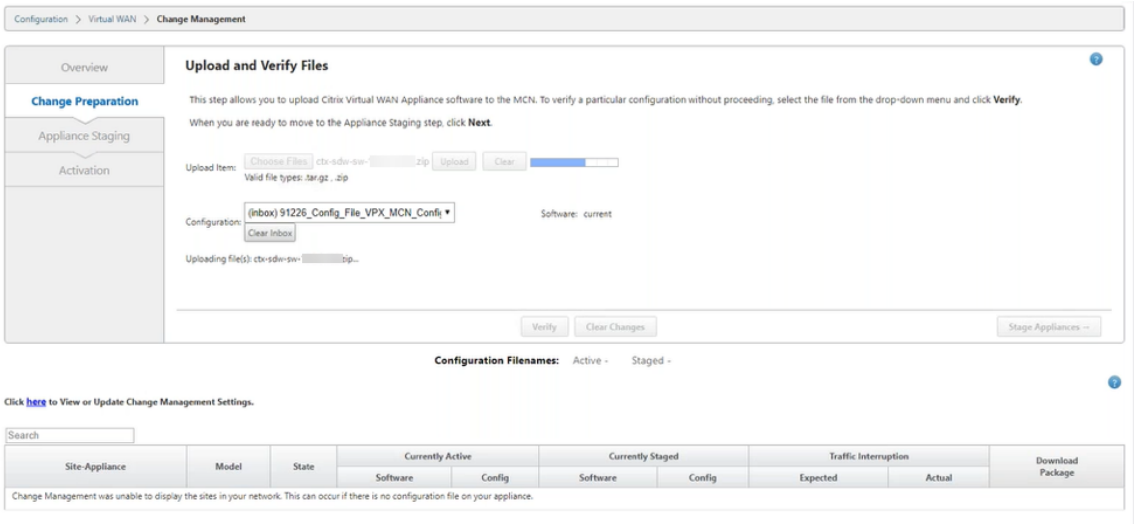


3. [変更管理**] > [**変更の準備] ページで、[ファイルの選択] をクリックし、*ctx-sdw-sw-11.0.0.x.zip* ソフトウェアパッケージファイルを選択します。［アップロード］をクリックします。

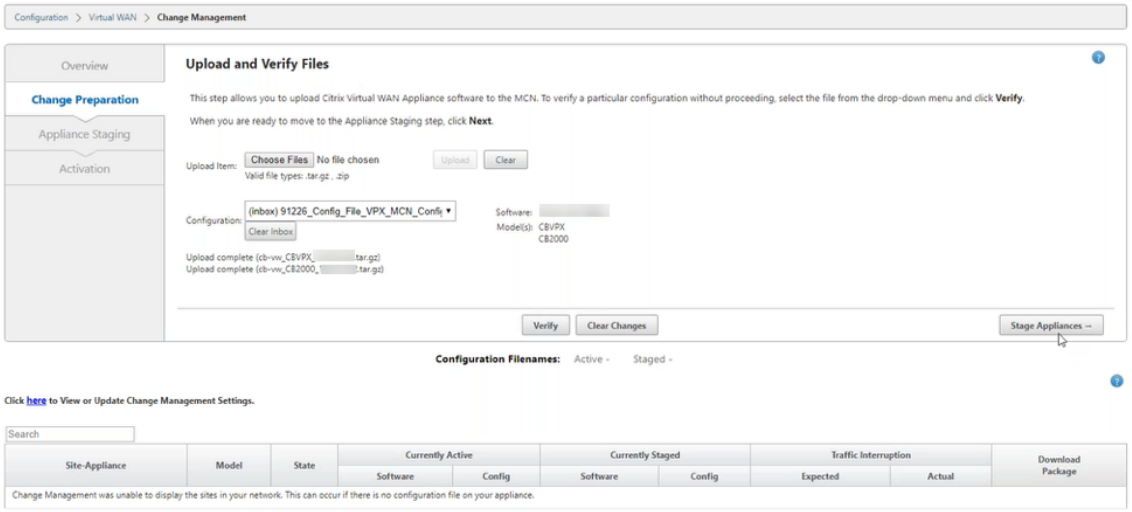
> 注:
>
> ダウンロード ページから Citrix SD-WAN リリース 11 ソフトウェアパッケージをダウンロードできます。



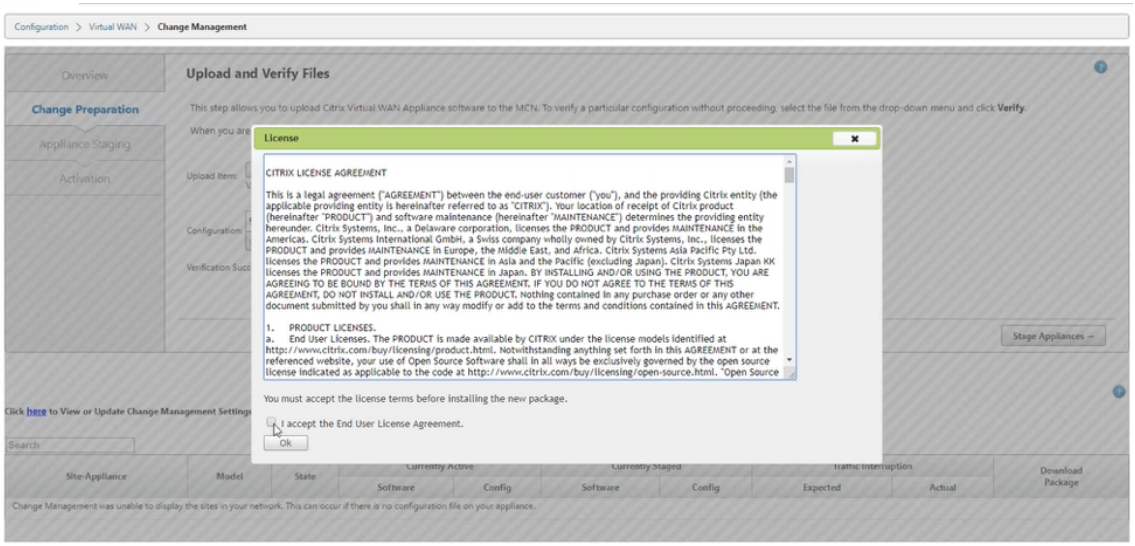
進行状況バーが表示され、現在のアップロードの進行状況が表示されます。



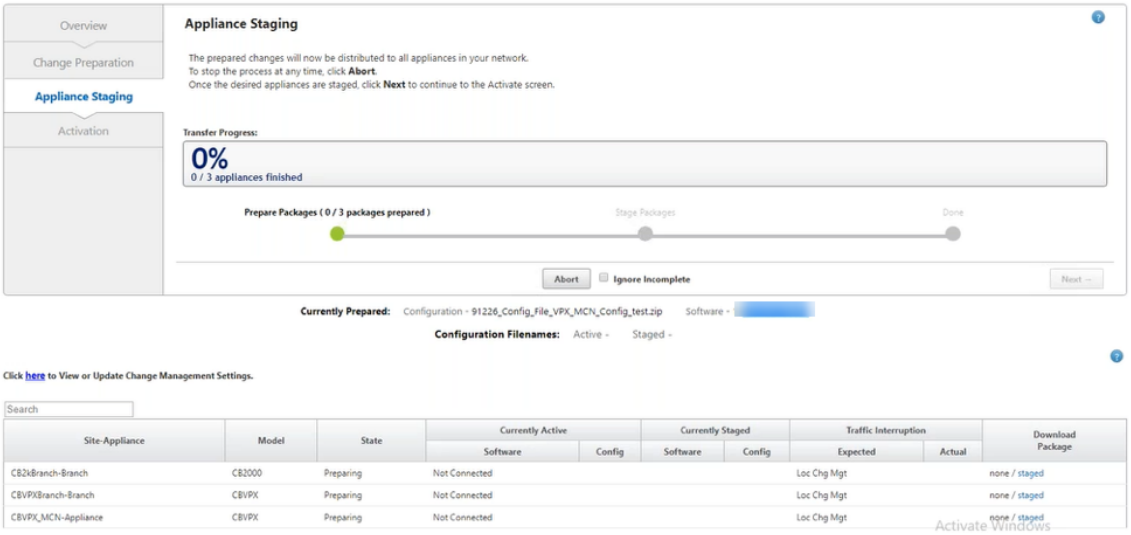
4. アップロードプロセスが成功すると、各ブランチプラットフォームモデルに関する情報を含む構成ファイルに基づいてアップグレードされる関連モデルが表示されます。



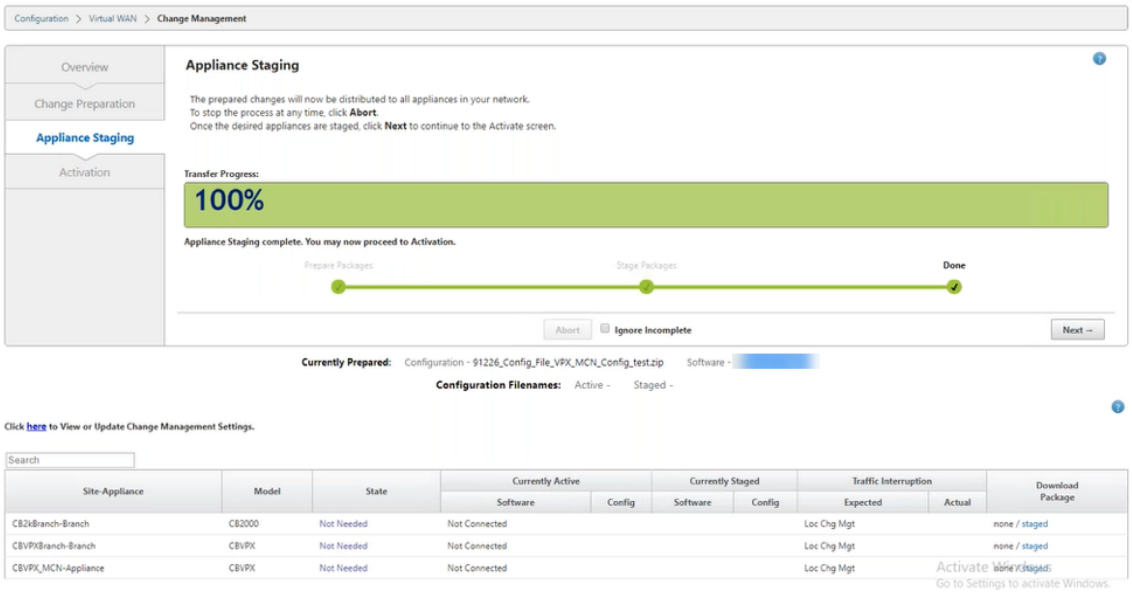
5. [**Stage Appliance**] をクリックして、構成ファイルの検証を続行します。ユーザー同意の [使用許諾契約] ページが表示されます。[使用 許諾契約書に同意 します] をクリックし、[**OK**] をクリックします。



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

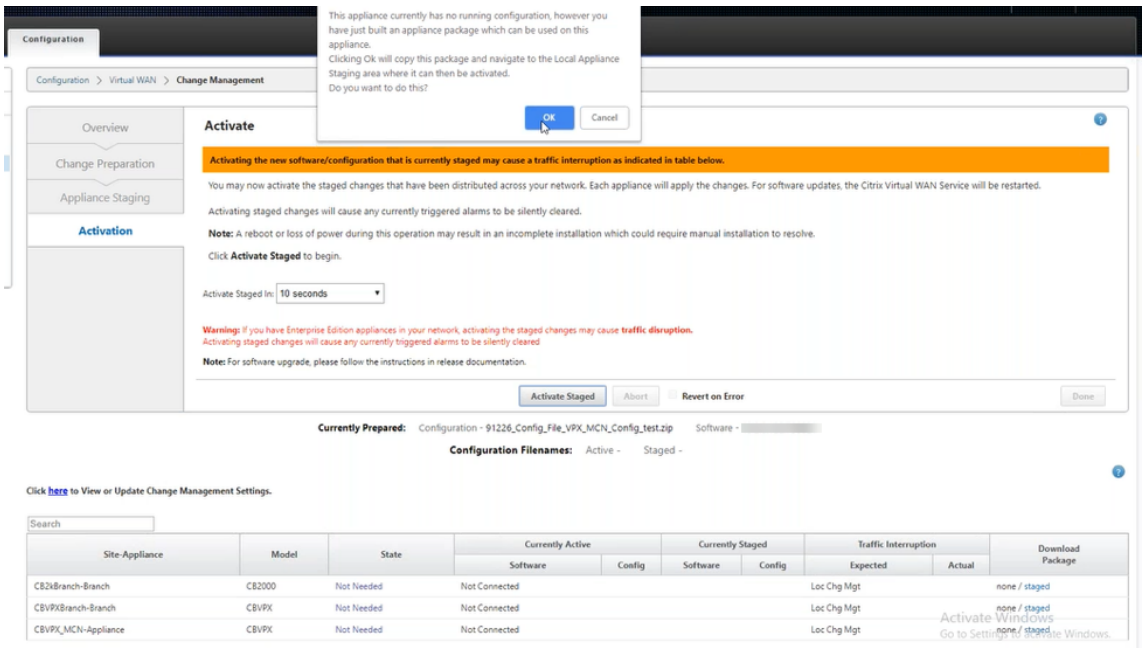


7. 転送の進行状況が 100% 完了したら、[次へ] をクリックしてアクティベーションに進みます。

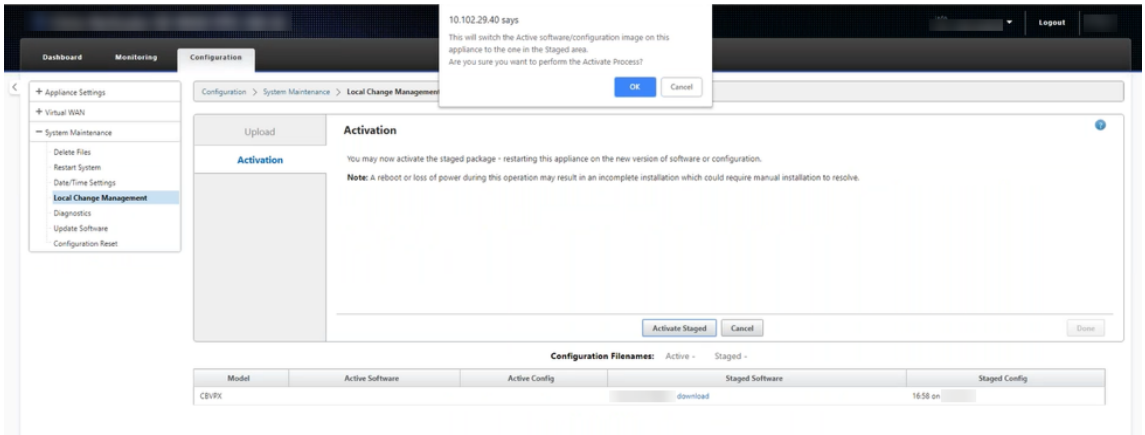


8. [ステージングを有効化] をクリックします。アプライアンスが初めてステージングされるときに、ユーザー承認のポップアップメッセージが表示されます。

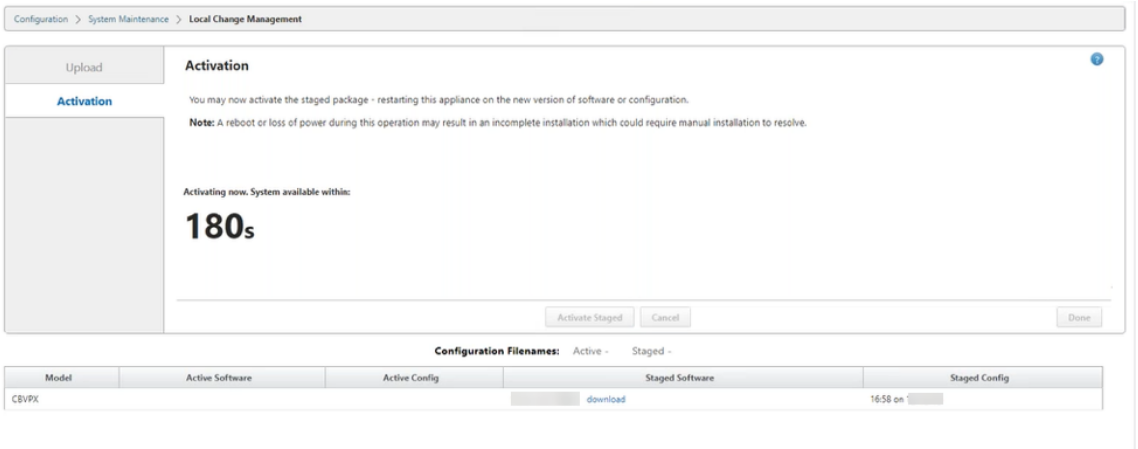
   ローカルアプライアンスをアクティブ化するための [ローカル変更管理] ページにリダイレクトされます。[**OK]** をクリックして続行します。



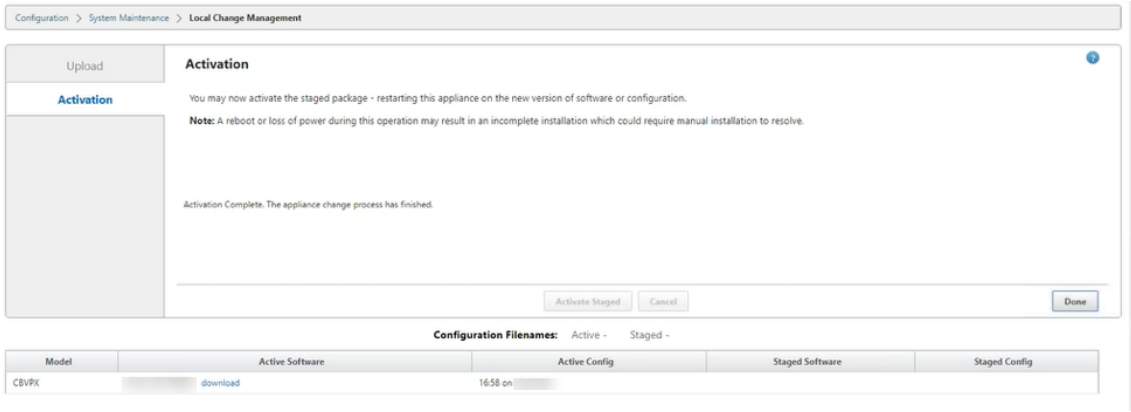
9. [ローカル変更管理で ステージングされたアクティブ化] をクリックします。アクティベーション確認メッセージが表示されます。[**OK**] をクリックします。



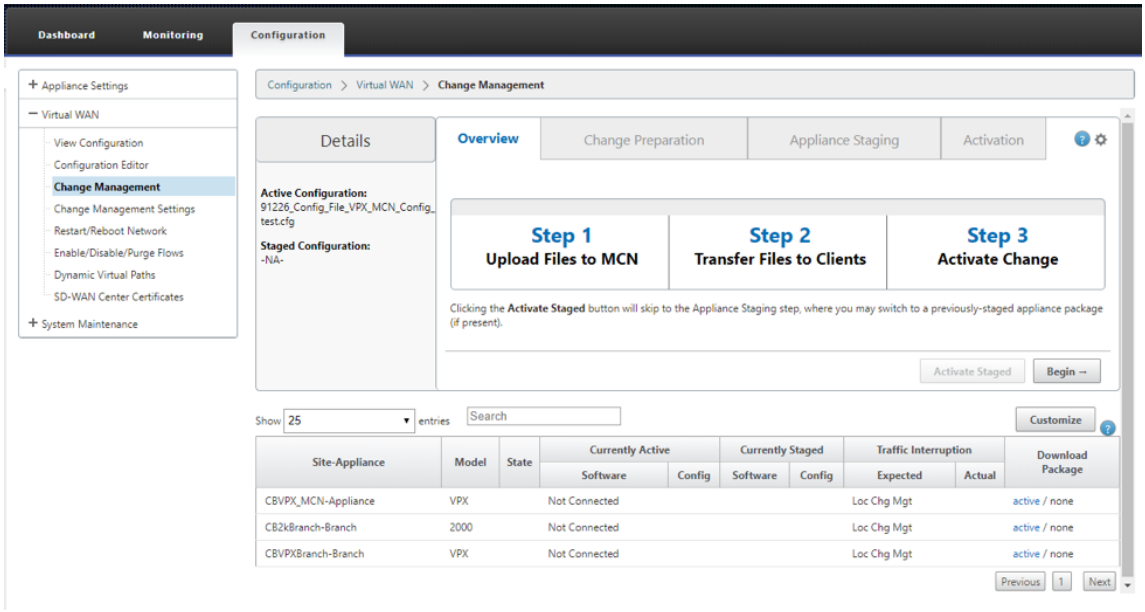
アクティベーションは 180 秒のカウントダウンタイマーから始まります。



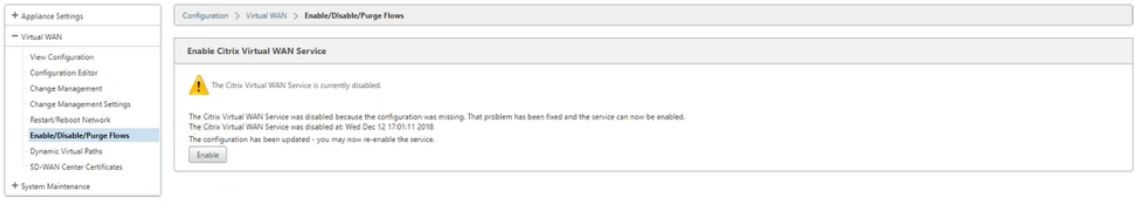
10. カウントダウン後、アクティブ化が完了したことを示すメッセージが表示されます。「完了」をクリックすると、アプライアンスが再起動します。



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



12. アプライアンスで SD-WAN サービスを有効にします。[仮想 **WAN] > [**フローの有効化**/**無効化**/**パージ] に移動し、[有効] をクリックします。



さらに構成し、新しいサイトをネットワークに追加するには、「ブランチノードの構成」の手順を実行します。

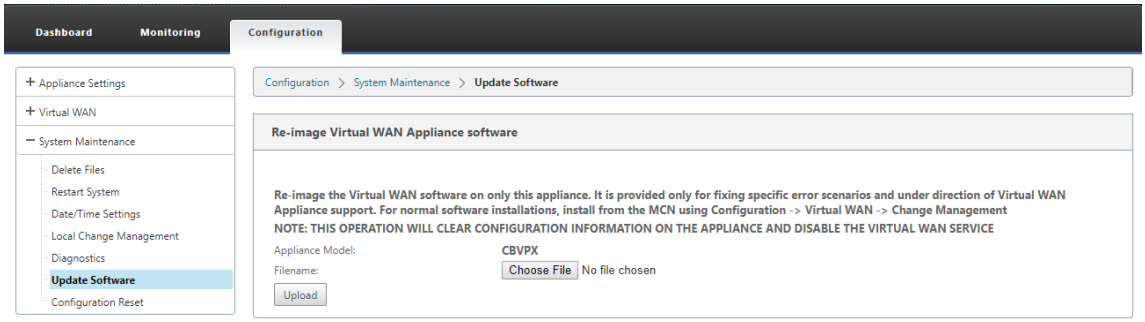
Citrix SD-WAN アプライアンスソフトウェアのイメージを再作成する

May 10, 2021

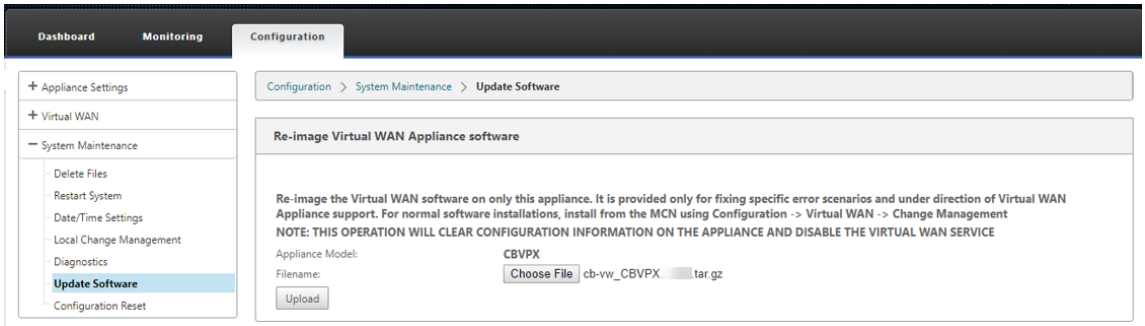
必要な Citrix SD-WAN ソフトウェアバージョンとプラットフォームの *.tar.gz* ファイルを シトリックスのダウンロード ポータルからダウンロードします。

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

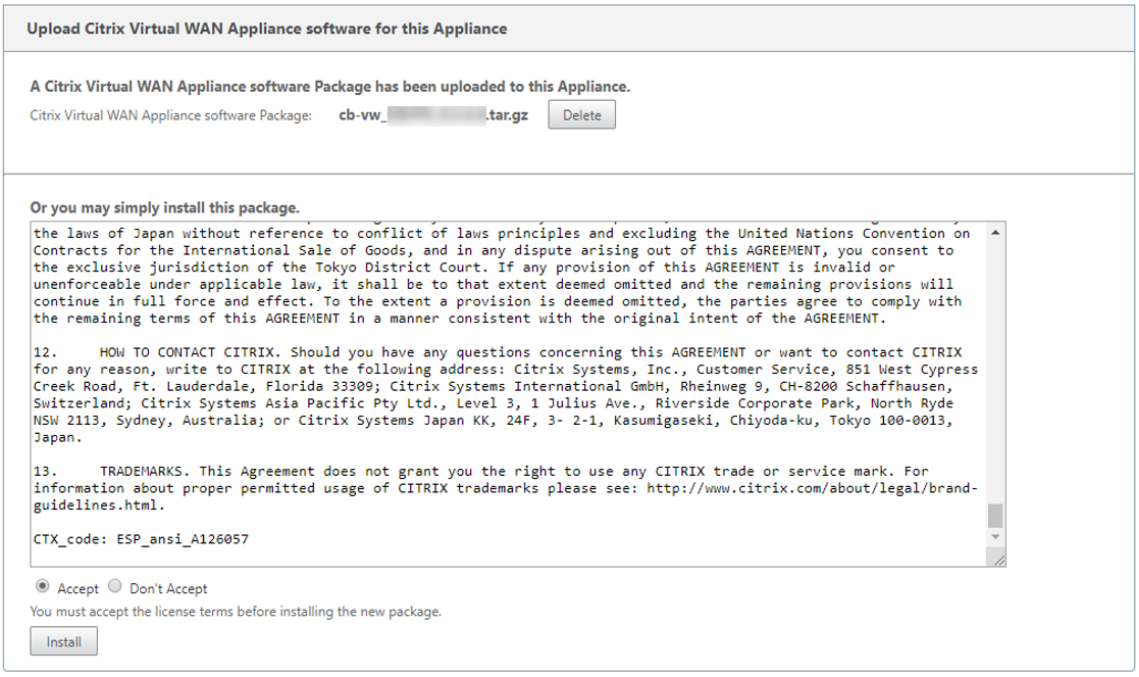
1. SD-WAN アプライアンスの GUI で、[構成] > [システムメンテナンス] > [ソフトウェアの更新] に移動します。



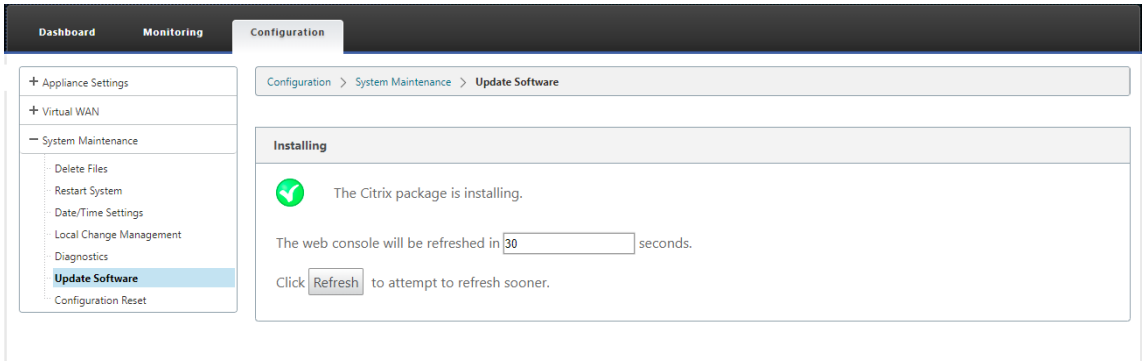
2. ［ファイルの選択］をクリックし、ダウンロードした Citrix SD-WAN アプライアンスソフトウェアを選択します。［アップロード］をクリックします。



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



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



ローカル変更管理を使用した部分的なソフトウェアのアップグレード

May 10, 2021

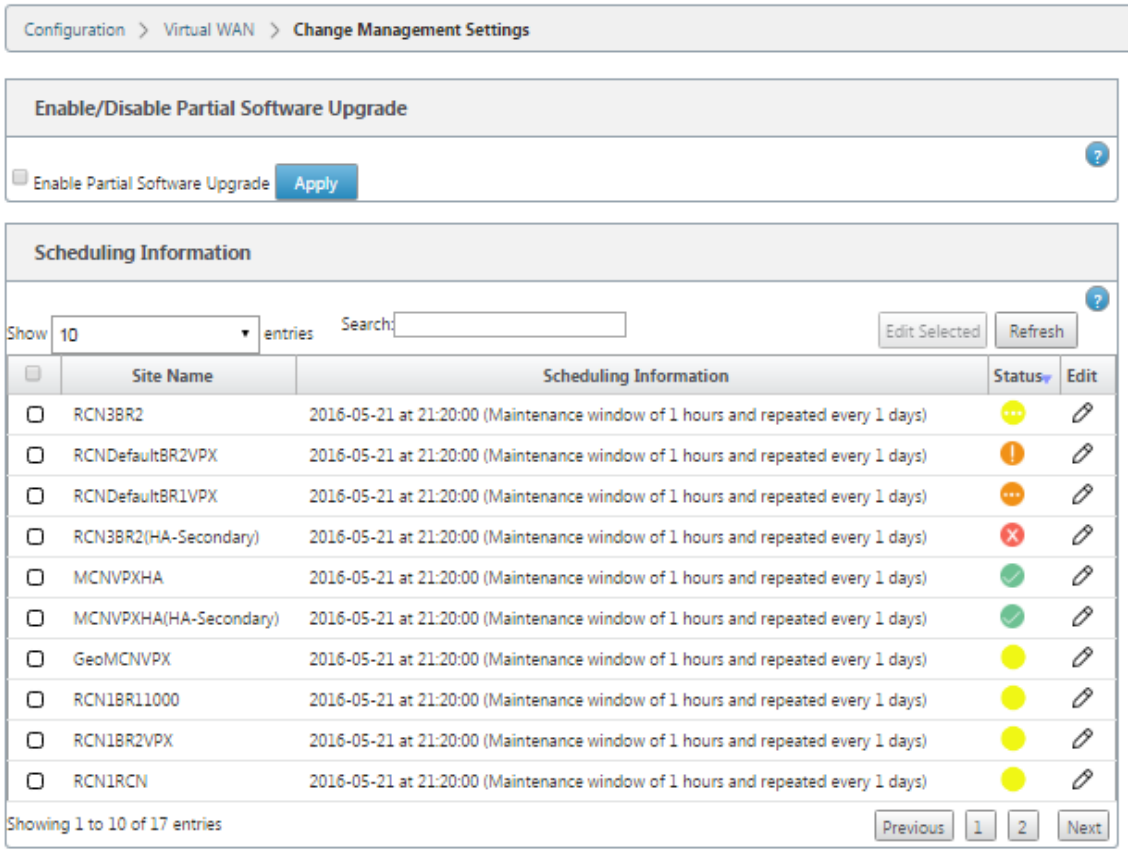
> 重要
>
> デフォルトでは、［部分的なソフトウェアアップグレード］オプションは無効になっています。

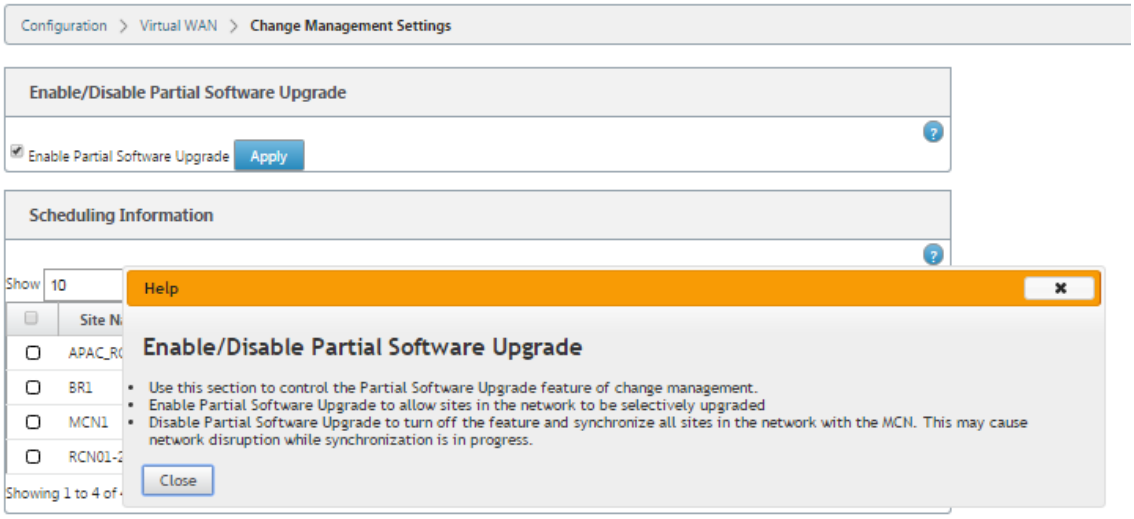
[ローカル変更管理] オプションを使用すると、クライアントサイトのサブセットに新しい SD-WAN ソフトウェアリリースバージョンをインストールできます。これは、部分的なソフトウェアアップグレード機能によって実現されます。この機能により、ネットワーク管理者は、すべてのサイトを同時にアップグレードすることなく、ネットワーク上のサイト上のソフトウェアを選択的にアップグレードできます。この機能の特定のユースケースは、管理者が新しいソフトウェアを少数のブランチサイトでテストしてから、ネットワーク内のすべてのサイトにインストールすることです。

前提条件と要件

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

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





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

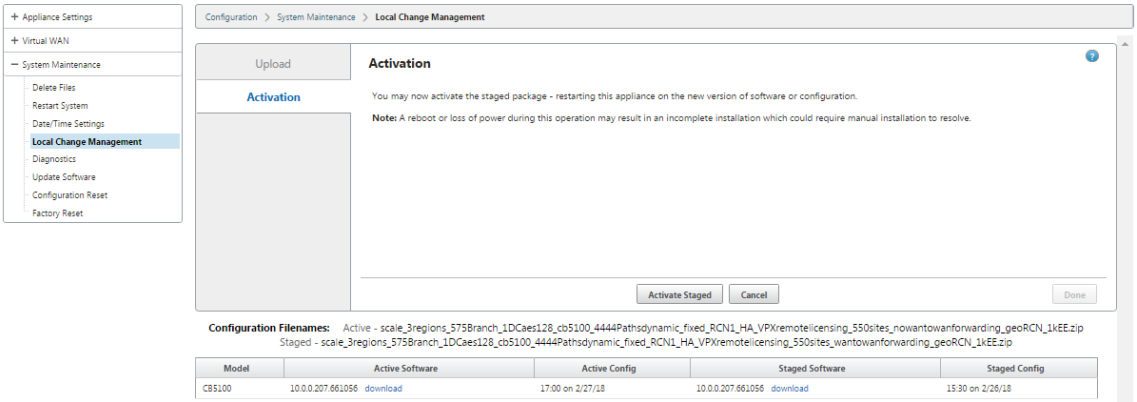
アクティブサイトと部分サイトの構成では、MCN サイトとブランチサイトでソフトウェアが同一である必要があります。部分的にアップグレードされたサイトでは、別の機能セットを有効にすることはできません。個々のサイトに進み、ローカル変更管理を実行します。高可用性の展開については、以下の手順を参照してください。

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

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

高可用性モードを使用せずにブランチノードをアップグレードする

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



高可用性モードでのブランチノードのアップグレード

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

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

ネットワークのアップグレード

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

USB で Premium 版変換に WANOP

May 10, 2021

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

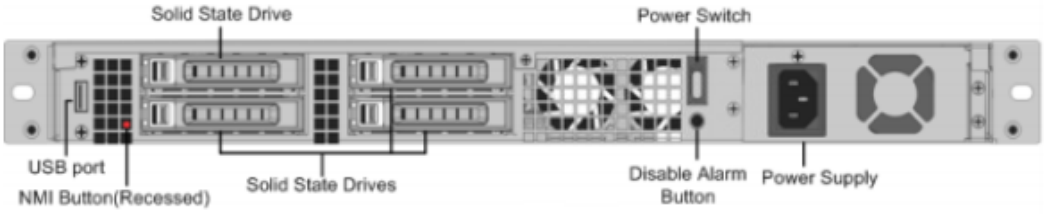
はじめに

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

アップグレード手順

変換手順は、次の手順を含む 2 段階のプロセスです。

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

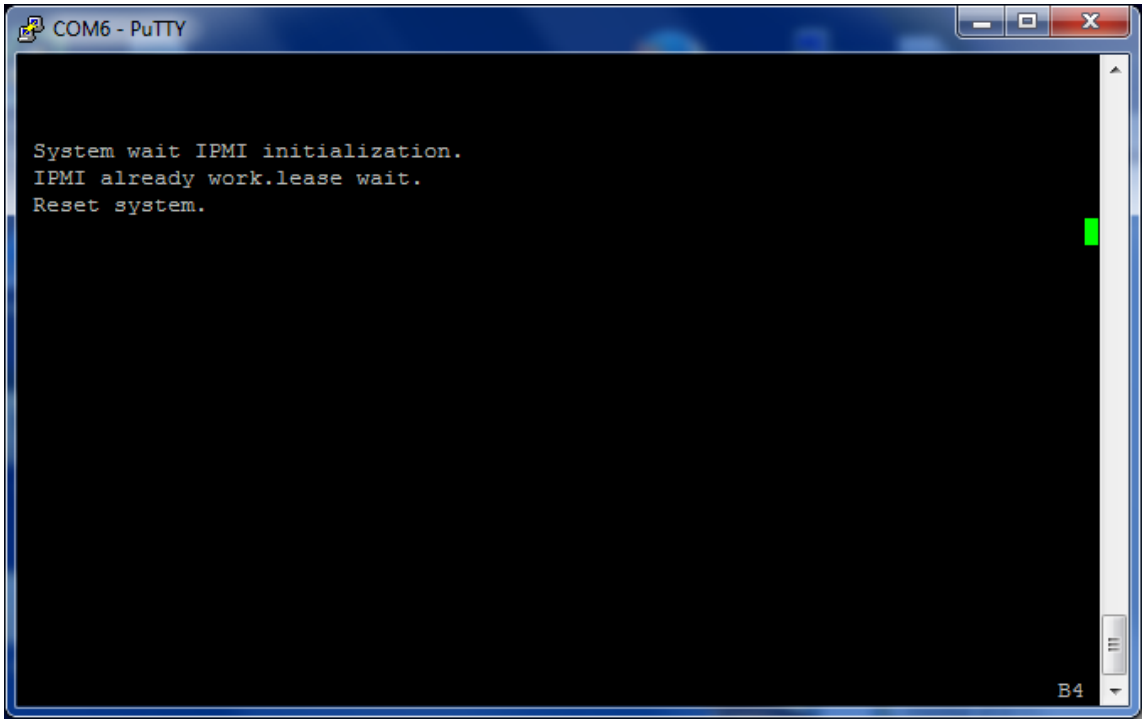


USB スティックで変換する方法

USB スティックを使用してアプライアンスをアップグレードするには:

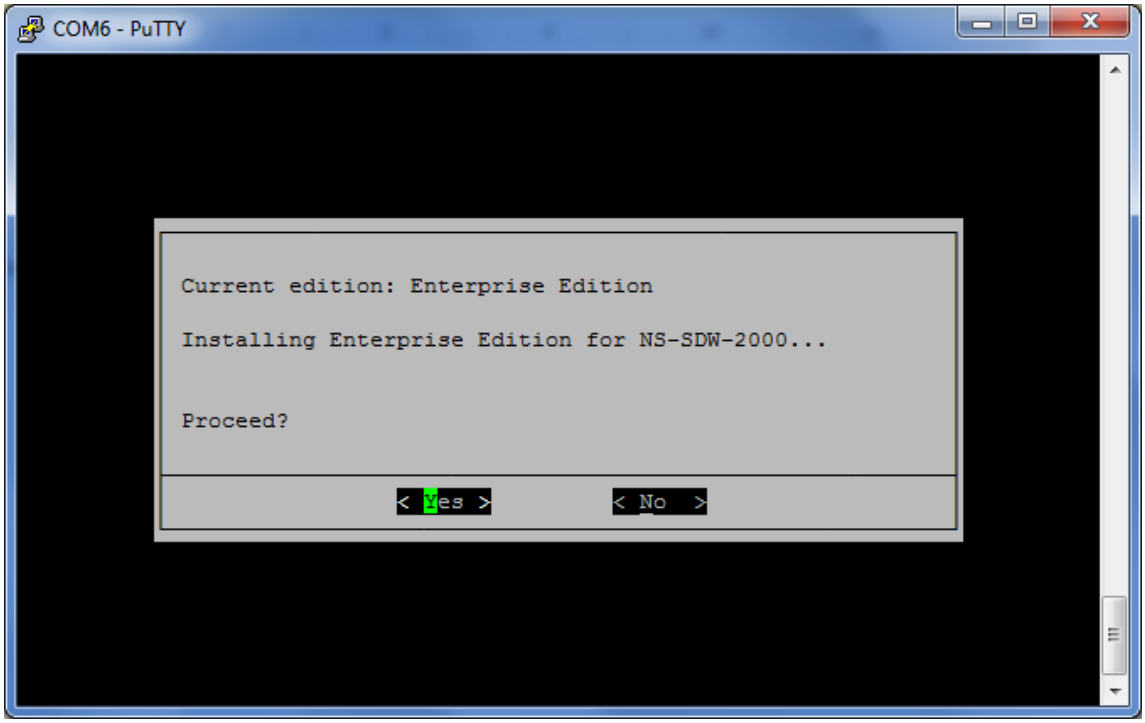
1. 付属の USB スティックを Citrix SD-WAN アプライアンスに挿入します。
2. アプライアンスのシリアルコンソールに接続します。
3. アプライアンスを再起動します。
4. 起動プロセス中に、カーソルが画面上を移動しているのを確認したら、次の操作を行います。
   a) [**Esc**] キーを押したままにします。
   b) **Shift** キーを押したままにします。
   c) 数字 **1** キーを押します（SHIFT+1=!）キーを押し、すべてのキーを放します。
   d) カーソルの移動を停止するまで、手順 a、b、c を繰り返します。

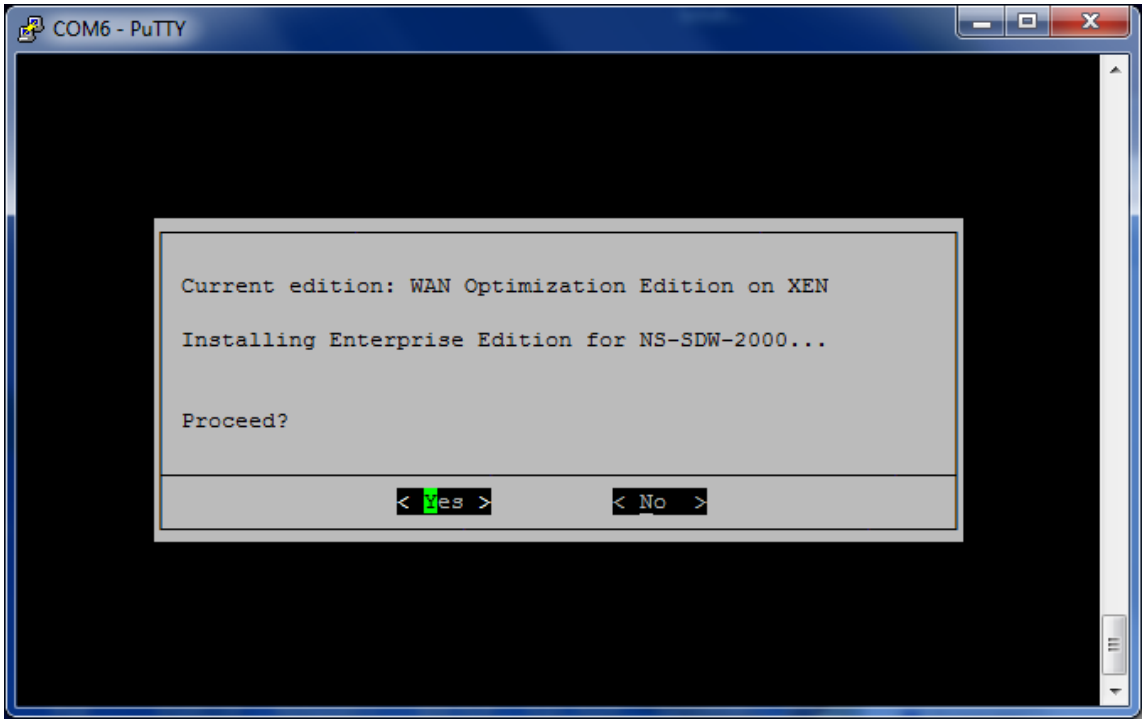
> 注
>
> 上記の手順は、アプライアンスの再起動プロセス中に実行する必要があります。キーストロークは、手順 4 で説明したように、BIOS のポストステージ中に発生します。



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

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





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

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

8. 手順が完了したら、USB メモリを取り外します。

参照ドキュメント

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

Standard Edition から Premium Edition への変換

May 10, 2021

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

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

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

WAN 最適化プロビジョニングの条件を次に示します。

1. サイトロールが MCN の場合、WAN 最適化プロビジョニングは以下だけ実行されます。

- ソフトウェアのアップグレードは、.zip パッケージ (SSUP) を使用して行われます
- ライセンスは PE
- 仮想 WAN サービスが有効になっている

2. サイトロールが [クライアント] の場合、WAN 最適化プロビジョニングは次の場合にのみ実行されます。

   - ソフトウェアのアップグレードは、.zip パッケージ (SSUP) を使用して行われます
   - 仮想 WAN サービスが有効になっている
   - ライセンスは PE
   - 仮想パスは MCN で形成される

3. WAN 最適化を即座にプロビジョニングするには、対応するサイトの [管理設定の変更] ページで [メンテナンスウィンドウ] の値を 0 に設定します。

USB イメージ再作成ユーティリティ

May 10, 2021

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

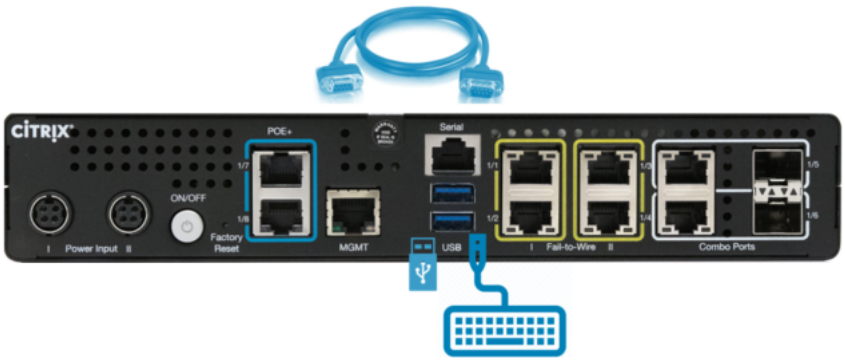
次の表に、使用可能な USB FRU イメージの詳細と、SD-WAN アプライアンスでサポートされているエディションを示します。

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

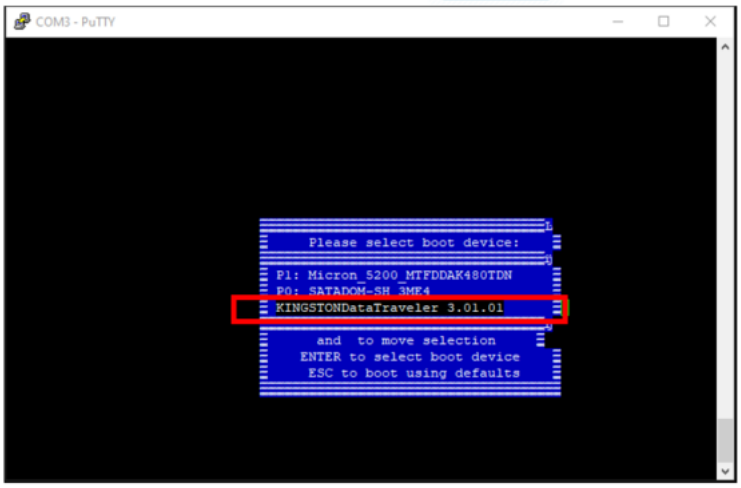
USB イメージの再作成を実行するには、次の手順に従います。

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

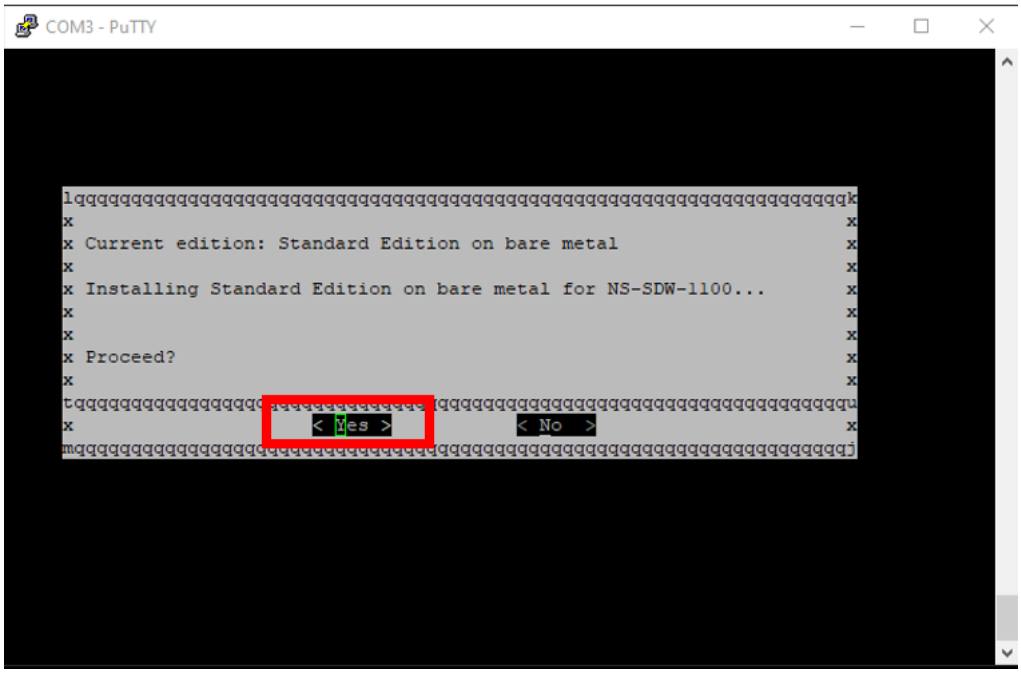
> ヒント
>
> アプライアンスに 1 つの USB ポートがある場合は、USB スプリッタを使用して USB スティックと USB キーボードの両方を接続します。



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



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



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

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

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

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

   コマンド‘*management_ip*’を発行します。

   コマンドを発行する‘インターフェイス *192.168.100.1 255.255.255.0 192.168.100.254*’

   コマンド「適用」を発行します。

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

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

Citrix SD-WAN ライセンスオプション

May 10, 2021

3 つの Citrix SD-WAN エディションには、それぞれ異なる SD-WAN 機能のセットまたはサブセットがあります。インストールするライセンスの種類によって、プラットフォームエディション（Standard Edition、WANOP、Premium Edition アプライアンス）が決まります。

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

Citrix SD-WAN プラットフォームソフトウェアのサポート

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

> 注
>
> リリースバージョン 10.2 では、エンタープライズプラットフォームエディションは「Premium」エディションにリブランドされます。

バージョン	WAN Optimization Edition	Standard Edition	Premium Edition
リリース 7.x	はい	いいえ	いいえ
リリース 8.x	いいえ	はい	いいえ
リリース 9.0、9.1、9.2、9.3	はい	はい	はい
リリース 10.0、10.1、10.2	はい	はい	はい
リリース 11.0	はい	はい	はい

Citrix SD-WAN リリース 11.0 でサポートされているすべてのアプライアンスモデルを表示するには、Citrix SD-WAN のデータシートを参照してください。

VPX-WANOP モデルでは、2、6、10、20、50、100、200 Mbps の帯域幅ライセンスを許可します。VPX インスタンスをサポートするには、2.1 GHz CPU が少なくとも 2 つ必要です。

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

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

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

> 注
>
> 2020 年 11 月 4 日より、「Citrix ライセンスの返却と変更」プロセスに変更が加えられています。この新しいプロセスでは、Citrix.com の [ライセンスの管理] ポータルおよび Partner Central の [マイライセンスツール] を使用して、ライセンスを返却または変更することはできません。
> 詳細およびユースケースのリストについては、「KB 記事 CTX285157」を参照してください。

ローカルライセンス

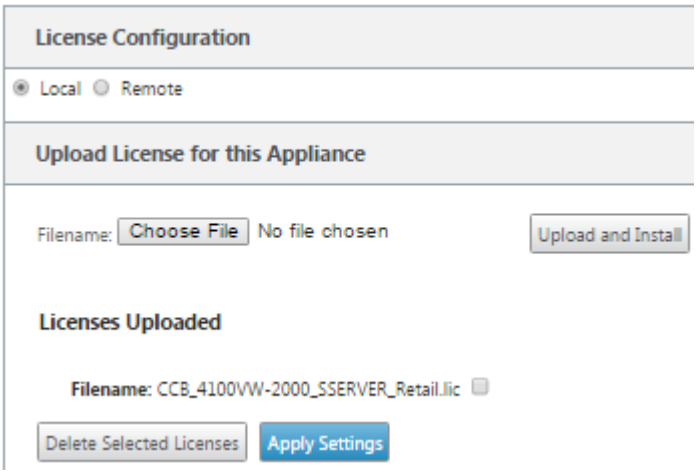
May 10, 2021

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

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

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

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



リモートライセンス

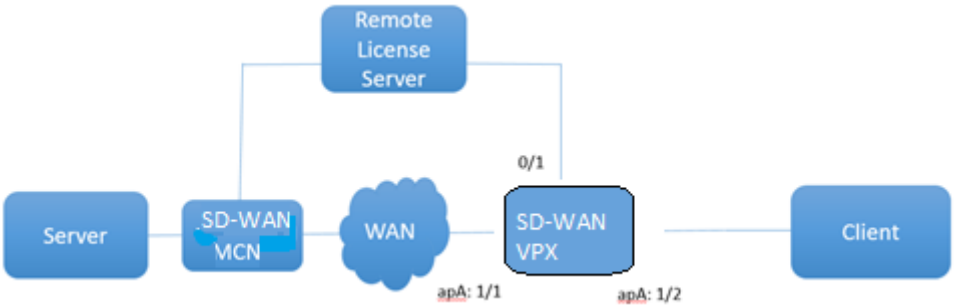
May 10, 2021

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

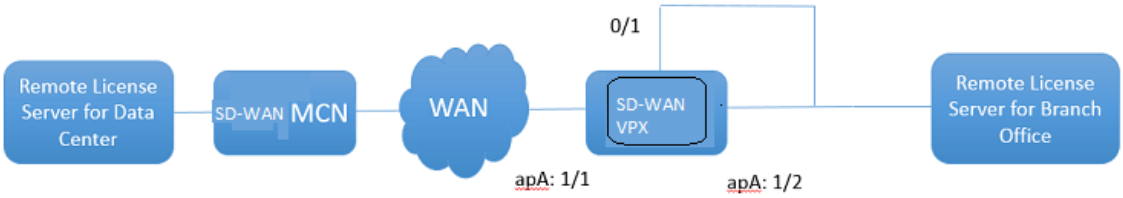
- NTP は、ライセンスサーバと SD-WAN の両方に対して構成する必要があります（日付と時刻は同期している必要があります）。
- 最新のライセンスサーバーバージョンを使用することをお勧めします。
  - リリース 9.1、9.2：11.13.1 L.S
  - Release 10.0, 10.1, 10.2, 11.0, 11.0.1, 11.0.2:11.14.1 L.S
  - リリース 11.0.3：11.16.3 L.S

ユースケース:

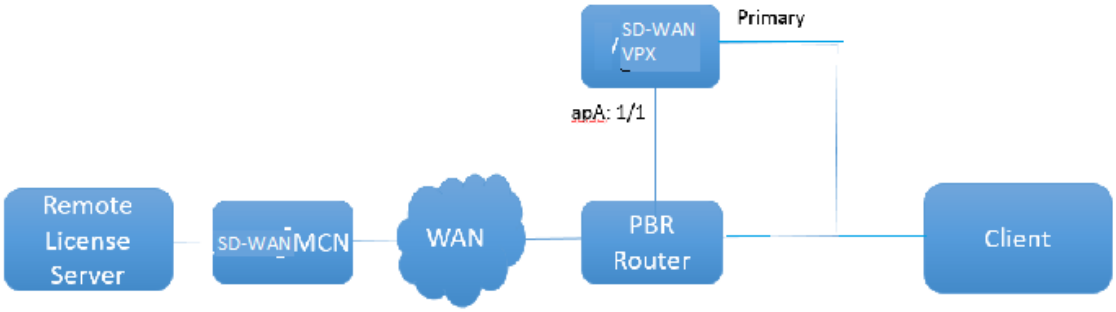
1. Data/APA ポートを使用せずに管理ネットワーク経由で到達可能なリモートライセンスサーバ。



2. ブランチネットワーク内のリモートライセンスサーバ。

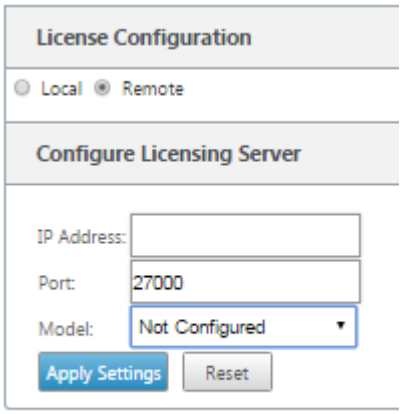


3. SD-WAN VPX-SE-支社における PBR の導入。



リモートライセンス:

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



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

> 重要
>
> SD-WAN センターを使用して SD-WAN アプライアンスのリモートライセンスをインストールする場合は、SD-WAN Web 管理インターフェイスの構成エディターのグローバル設定で、SD-WAN MCN アプライアンスの集中ライセンスを有効にします。

一元化されたライセンス

May 10, 2021

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

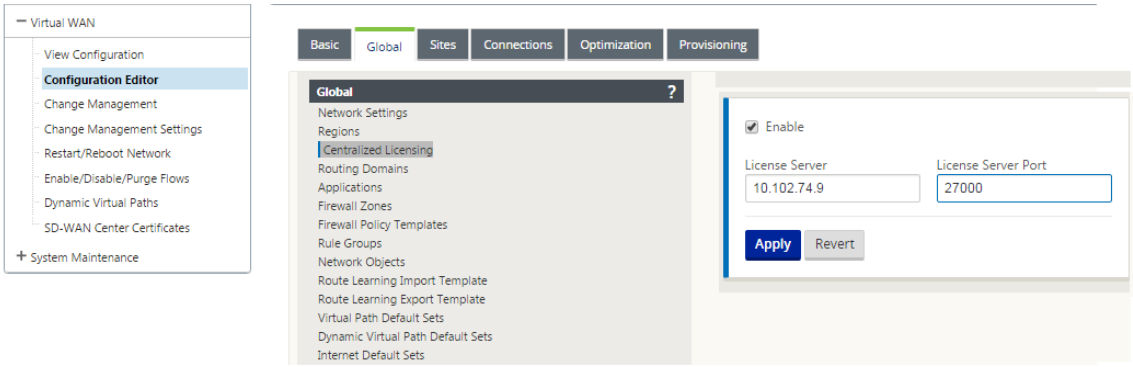
新しい集中型ライセンスモデルでは、SD-WAN Center Web 管理インターフェイス（SD-WAN アプライアンス管理およびレポートポータル）によって、アプライアンスにログインしなくても、ネットワーク上の個々の SD-WAN アプライアンスにライセンスサービスが提供されます。

SD-WAN Center IP アドレスは、SD-WAN アプライアンス GUI の [グローバル**] > [**集中型ライセンス] の下で提供されます。この IP アドレスは、構成パッケージまたは更新によって個々のアプライアンスに伝播されます。IP アドレスが変更されたら、変更管理プロセスを実行して、アプライアンスをプッシュする必要があります。グローバル設定は、ローカルサイト設定によって上書きできます。

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

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

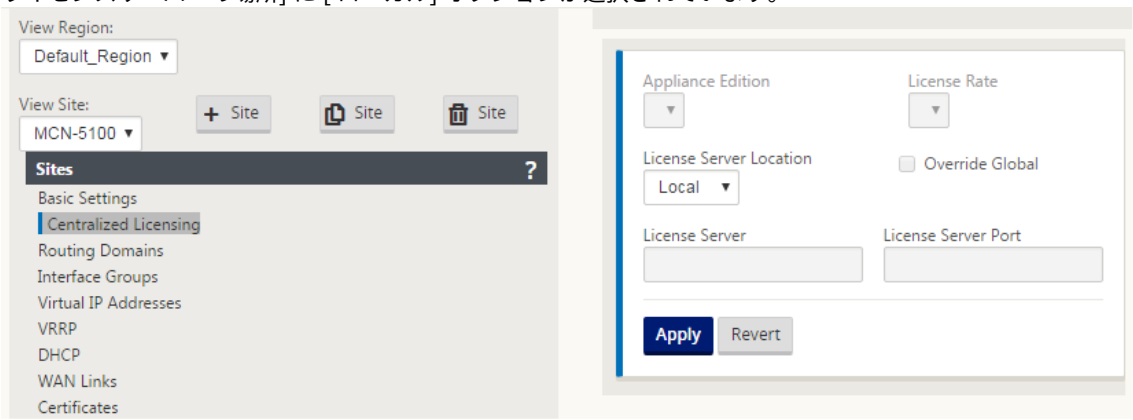
1. [構成] > [仮想 **WAN**] > [構成エディタ**]** に移動します。既存の仮想 WAN 構成パッケージを開くか、構成パッケージを作成します。構成パッケージが開きます。
2. 「グローバル」タブに移動します。[集中型ライセンス] を選択します。[有効] をクリックします。
3. SD-WAN ライセンスをダウンロードして管理できるライセンスサーバーの IP アドレスを入力します。SD-WAN MCN またはブランチアプライアンスの構成パッケージが SD-WAN Center からライセンスをダウンロードできるように、SD-WAN Center 管理 IP アドレスを指定しま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



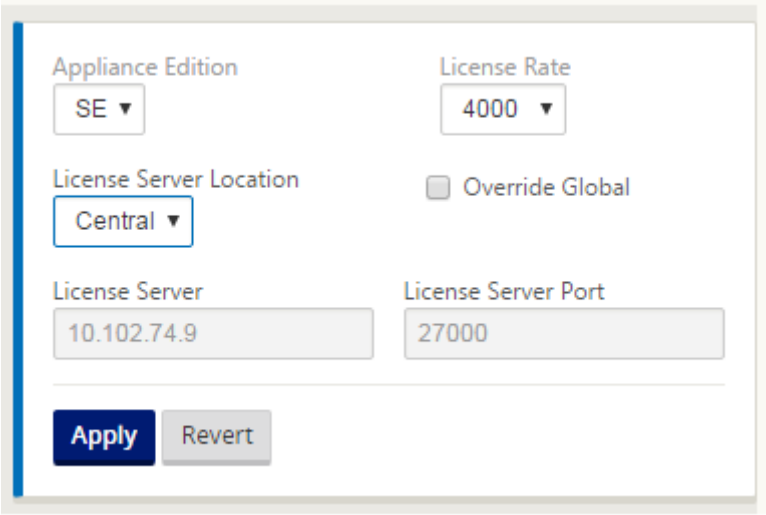
5. ［適用］をクリックします。

6.「サイト」タブにナビゲートします。中央ライセンスを管理する地域とサイトに応じて、[サイトの表示] で [MCN] または [ブランチサイト] を選択します。

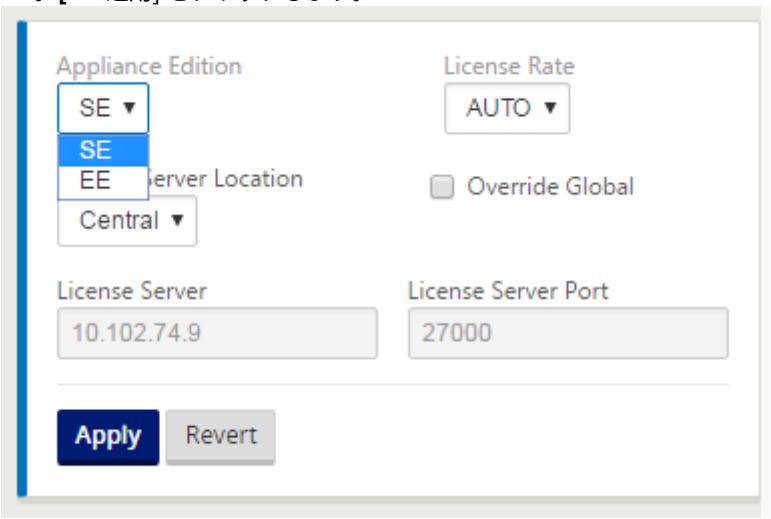
7. [集中型ライセンス] を選択します。中央のライセンスオプションビューが表示されます。デフォルトでは、[ライセンスサーバーの場所] に [ローカル] オプションが選択されています。



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

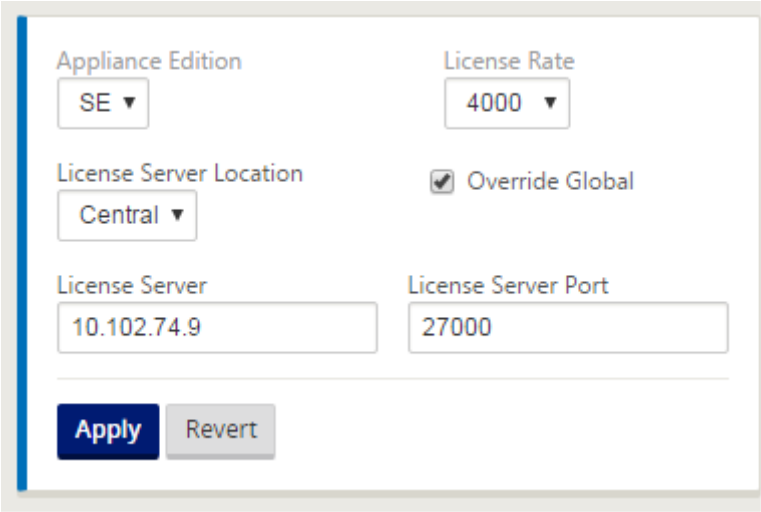


9. インストールするアプライアンスに応じて、アプライアンスのエディションとライセンスレートを選択します **。[** 適用] をクリックします。



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

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



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

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

帯域幅割り当てに基づくライセンス:

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

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

ライセンスの猶予期間:

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

> 注
>
> 選択したライセンスレートが設定された WAN リンクレートと一致しない場合、ライセンスイベントに関する次のメッセージがアプライアンス GUI に表示されます。
>
> メッセージ: 設定されている許可レート (LAN から WAN へ) NNN (Kbps) の合計は、ライセンスレート (NNN (Kbps) の 2 倍を超えてはなりません。

> 重大度: 警告
>
> イベント:Syslog、電子メール

ライセンスの管理

May 10, 2021

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

SD-WAN アプライアンスのライセンス管理プロセス

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

MCN アプライアンスのアウトオブボックスライセンス (OOB):

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

クライアントアプライアンスのアウトオブボックスライセンス (OOB):

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

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

ライセンスの有効期限

May 10, 2021

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

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

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

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

猶予期間:

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

構成

May 10, 2021

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

SD-WAN アプライアンスの設定には、次のものが含まれます。

MCN の設定: MCN は、初期システム構成およびその後の構成変更の配布ポイントとして機能します。ほとんどのアップグレード手順は、MCN の管理 Web インターフェイスを使用して実行します。仮想 WAN に存在できるアクティ

ブな MCN は 1 つだけです。
デフォルトでは、アプライアンスには client という役割が事前に割り当てられています。アプライアンスを MCN として確立するには、まず MCN サイトを追加して構成し、指定した MCN アプライアンス上で構成と適切なソフトウェアパッケージをステージングしてアクティブ化する必要があります。

ブランチの構成: ブランチサイトを追加する手順は、MCN サイトの作成と構成と非常によく似ています。ただし、構成手順と設定の一部は、ブランチサイトでは若干異なります。さらに、最初のブランチサイトを追加したら、同じアプライアンスモデルを持つサイトについては、クローン（複製）機能を使用して、これらのサイトを追加および構成するプロセスを合理化できます。MCN サイトを作成する場合と同様に、ブランチサイトを設定するには、MCN アプライアンスの管理 Web インターフェイスで **Configuration Editor** を使用する必要があります。構成エディタ は、インターフェイスが **MCN** コンソール モードに設定されている場合にのみ使用できます。

MCN とブランチサイト間の仮想パスの構成: MCN と各クライアント (ブランチ) サイト間の仮想パスサービスを構成します。これを行うには、構成 エディタ の「接続」セクション構成ツリーにある構成フォームと設定を使用します。

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

初期設定

September 26, 2023

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

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

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

> 警告
>
> コンソールセッションがタイムアウトになったり、構成を保存する前に管理 Web Interface からログアウトした場合、保存されていない構成の変更はすべて失われます。その後、システムに再度ログインし、設定手順を最初から繰り返す必要があります。そのため、構成パッケージを作成または変更したり、そ

> の他の複雑なタスクを実行したりするときは、コンソールセッションの タイムアウト 間隔を高い値に設定することを強くお勧めします。

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

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

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

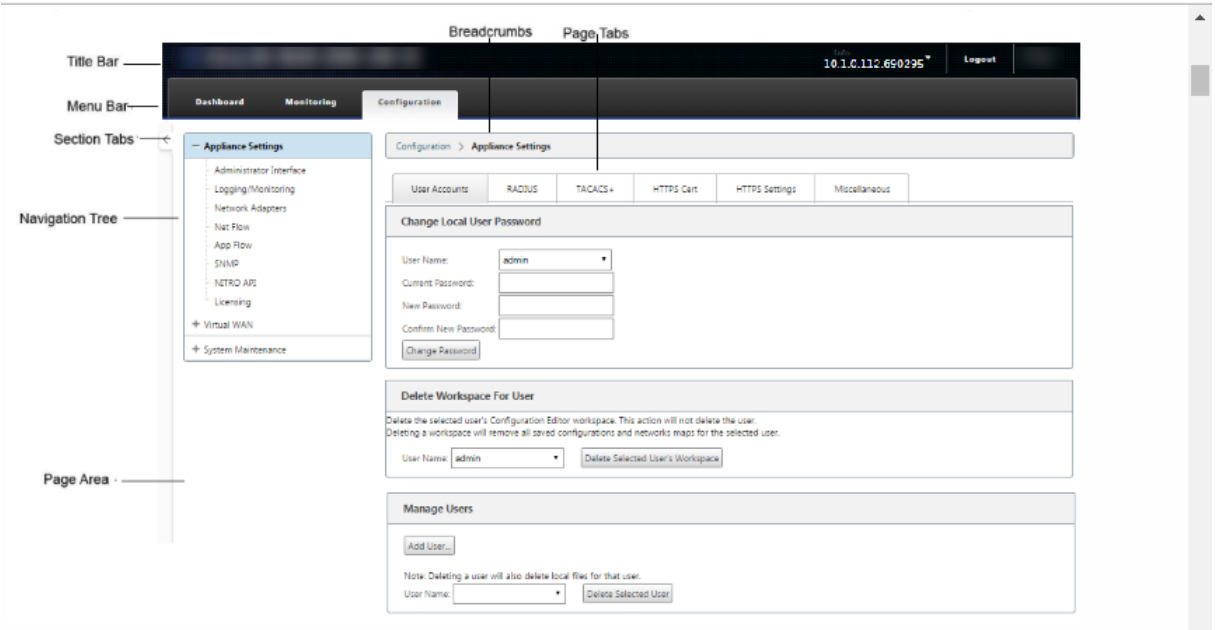
Web インターフェイス (UI) レイアウトの概要

May 10, 2021

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

基本的なナビゲーション

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



基本的なナビゲーション要素は次のとおりです。

- タイトル・バー: アプライアンスのモデル番号、アプライアンスのホスト IP アドレス、アプライアンス上で現在実行されているソフトウェア・パッケージのバージョン、および現在のログイン・セッションのユーザー名が表示されます。タイトルバーには、セッションを終了するための [ログアウト] ボタンもあります。
- メイン・メニュー・バー—すべての管理 Web Interface 画面のタイトル・バーの下に表示されるバーです。これには、選択したセクションのナビゲーション・ツリーおよびページを表示するためのセクション・タブが含まれます。
- セクションタブ—セクションタブは、ページ上部のメインメニューバーにあります。これらは、Web 管理インタフェースのページおよびフォームの最上位カテゴリです。各セクションには、そのセクションのページ階層を移動するための独自のナビゲーションツリーがあります。セクションタブをクリックして、そのセクションのナビゲーション・ツリーを表示します。
- ナビゲーション・ツリー—ナビゲーション・ツリーは、メイン・メニュー・バーの下の左ペインにあります。これにより、セクションのナビゲーションツリーが表示されます。セクションタブをクリックして、そのセクションのナビゲーションツリーを表示します。ナビゲーションツリーには、次の表示オプションとナビゲーションオプションが用意されています。
  - セクション・タブをクリックすると、そのセクションのナビゲーション・ツリーおよびページ階層が表示されます。
  - ツリー内の分岐の横にある [+] (プラス記号) をクリックすると、その分岐トピックで使用可能なページが表示されます。
  - ページ名をクリックすると、そのページがページ領域に表示されます。
  - ブランチ項目の横にある「-」(マイナス記号) をクリックして、ブランチを閉じます。
- ブレッドクラム -これは、現在のページへのナビゲーションパスを表示します。ブレッドクラムは、ページ領域の上部、メインメニューバーのすぐ下にあります。アクティブなナビゲーションリンクは青いフォントで表示されます。現在のページの名前は、黒の太字フォントで表示されます。
- ページ領域 -これは、選択したページのページ表示と作業領域です。ナビゲーションツリーでアイテムを選択すると、そのアイテムのデフォルトページが表示されます。
- ページタブ—一部のページには、そのトピックまたは設定フォームの子ページを表示するためのタブが含まれています。これらは、ページ領域の上部、ブレッドクラム表示のすぐ下にあります。「変更管理」ウィザードと同様に、タブはページ領域の左ペイン、ナビゲーション・ツリーとページの作業領域の間にあります。
- ページ領域のサイズ変更—一部のページでは、ページ領域 (またはそのセクション) の幅を拡大または縮小して、テーブルまたはフォーム内のフィールドの数を増やすことができます。この場合、ページ領域ペイン、フォーム、またはテーブルの右枠にグレーの縦のサイズ変更バーが表示されます。カーソルが双方向矢印に変わるまで、サイズ変更バーの上にカーソルを移動します。次に、バーをクリックして右または左にドラッグし、領域の幅を拡大または縮小します。

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

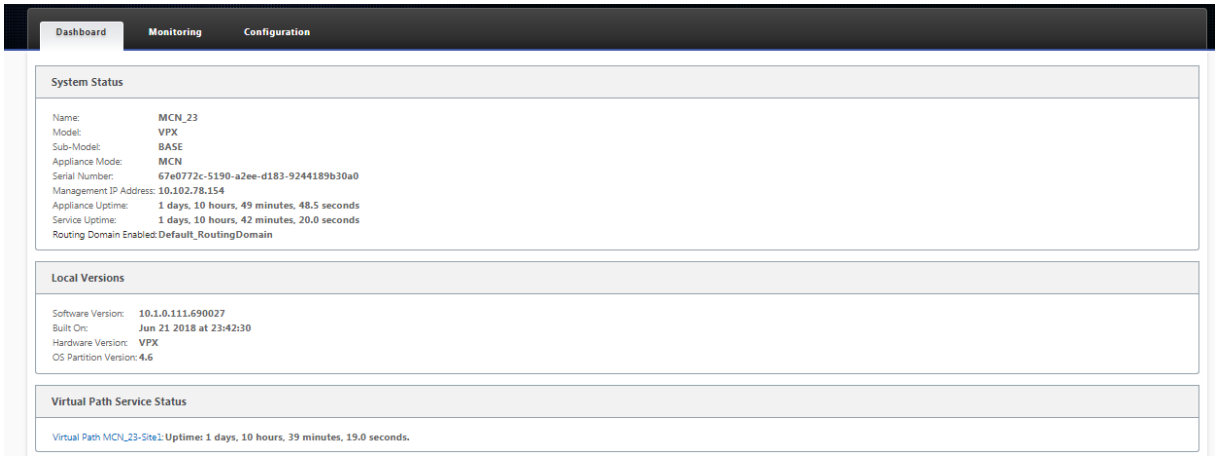
Web 管理インターフェイスのダッシュボード

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

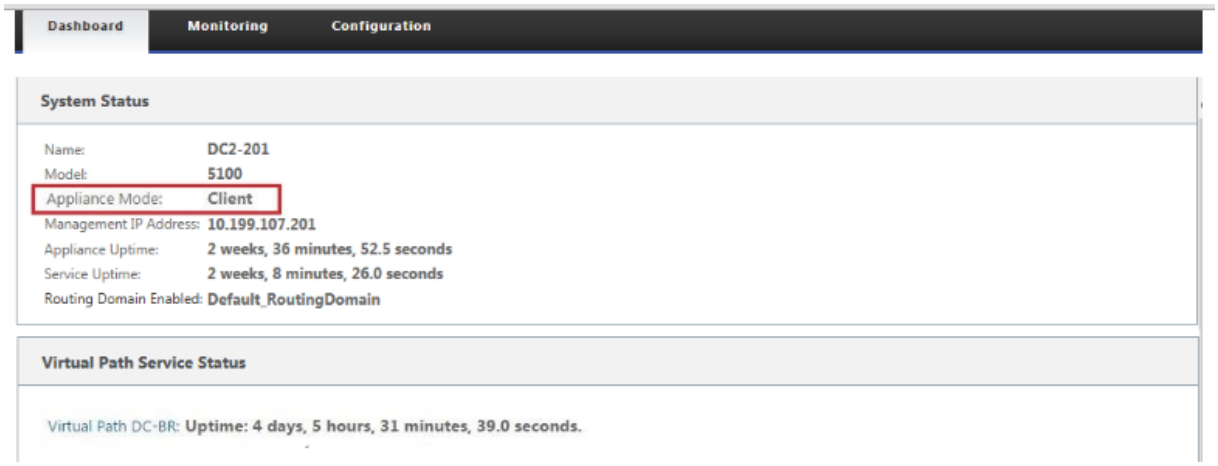
[ダッシュボード］ページには、アプライアンスの次の基本情報が表示されます。

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

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



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



構成エディタ

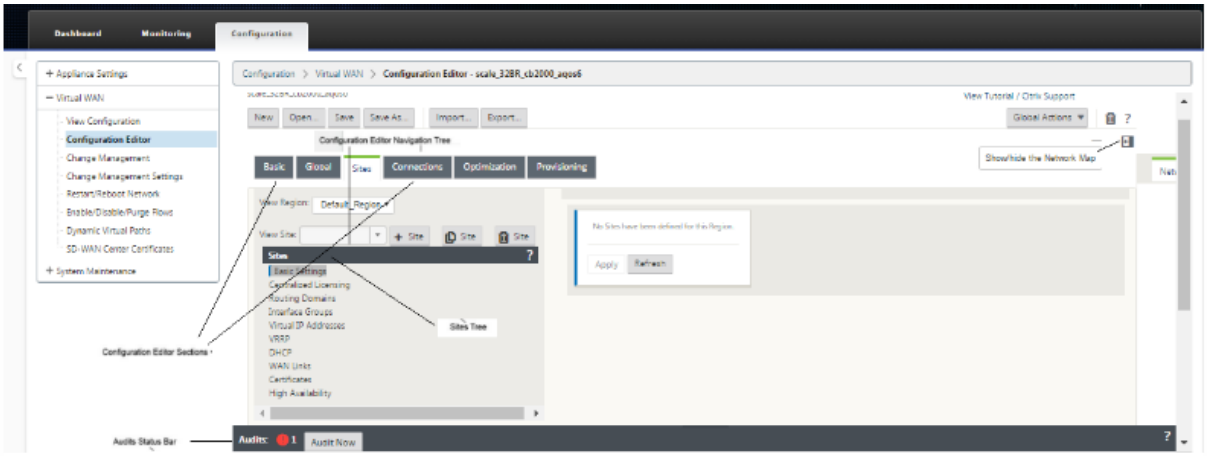
構成エディタを使用すると、仮想 WAN アプライアンスサイト、接続、最適化、Provisioning の追加と構成、仮想 WAN 構成の作成と定義を行うことができます。

構成エディタは、Web 管理インターフェイスが MCN コンソールモードの場合にだけ使用できます。デフォルトでは、新しいアプライアンスの Web Interface がクライアントモードに設定されています。構成エディタにアクセスする前に、モード設定を MCN コンソールに変更する必要があります。手順については、「[管理 Web インターフェイスを MCN コンソールモードに切り替える。]」を参照してください。(/en-us/citrix-sd-wan/11/configuration/set-up-master-control-node/switch-to-mcn-console.html)

構成エディタに移動するには、次の操作を行います。

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

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



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

- 構成エディターのメニュー・バー—ページ領域の上部、ブレッドクラム・リンクのすぐ下にあります。メニューバーには、構成エディターの 操作のための主要なアクティビティボタンがあります。さらに、メニューバーの右端には、構成エディタの チュートリアルを開始するための「チュートリアルの表示」リンクボタンがあります。このチュートリアルでは、構成エディタの 表示の各要素について、一連のバブルの説明を順を追って説明します。
- 構成エディターのセクションツリー—これは、構成エディターの ページ領域の左ペインにある濃い灰色のバーのスタックです。各グレーのバーは、トップレベルのセクションを表します。セクション名をクリックすると、そのセクションのサブブランチが表示されます。
- 「セクション」**(Sections Tree br** anch)-セクションツリーでセクション名をクリックすると、セクションブランチが開きます。各セクションブランチには、構成カテゴリとフォームのサブブランチが 1 つ以上含まれ、さらに子ブランチとフォームを含めることができます。
- サイトツリー—構成 エディタで現在開いている構成に追加されているサイトノードが表示されます。セクションツリーで。サイト名をクリックすると、そのサイトのブランチが開きます。ブランチを閉じるには、サイト

をクリックします。サイト・ツリーおよび構成フォームのナビゲートおよび使用方法の詳細については、次のセクションを参照してください。

  - マスター・コントロール・ノード（MCN）サイトの設定
  - ブランチサイトの追加と構成

- 監査ステータスバー—これは、「構成エディタ」ページの下部にある濃いグレーのバーで、「管理 Web Interface」画面の幅全体にわたって表示されます。監査 ステータスバーは、構成エディタ が開いている場合にのみ使用できます。ステータスバーの左端にある監査アラートアイコン（赤い点またはゴールデンロッドデルタ）は、現在開いている構成に 1 つ以上のエラーが存在することを示します。ステータスバーをクリックすると、その構成のすべての未解決の監査アラートの完全なリストが表示されます。

変更管理ウィザード

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

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

MCN グローバル変更管理ウィザードの使用

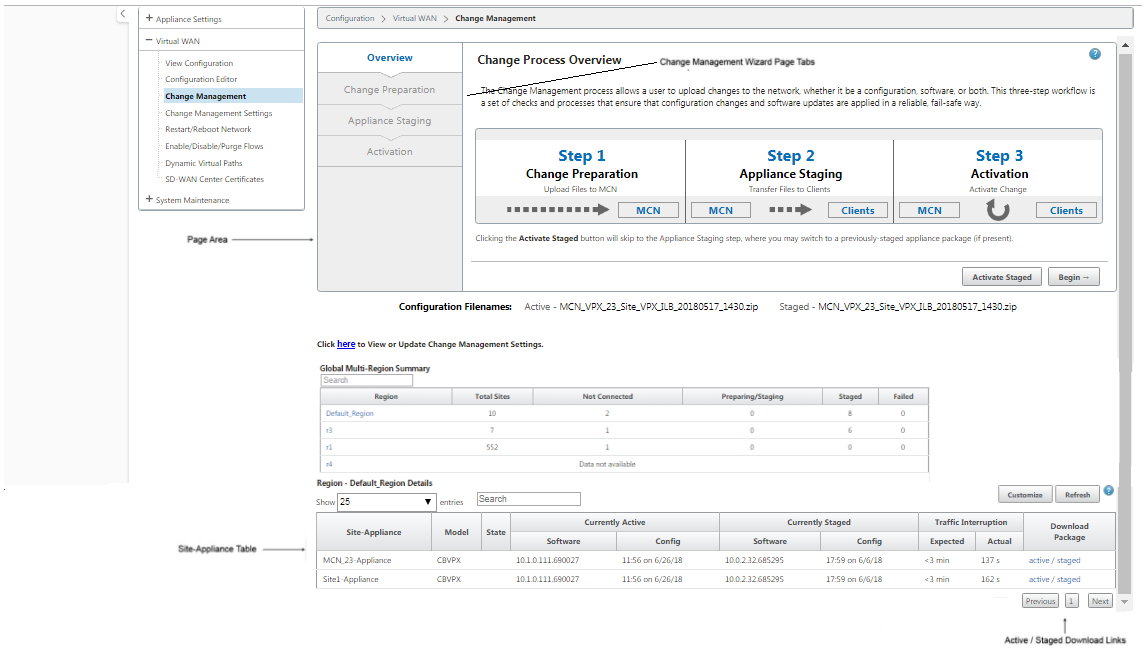
MCN グローバル 変更管理 ウィザードを開くには、次の操作を行います。

1. MCN アプライアンスの Web 管理インターフェイスにログインします。

2. ［構成］タブを選択します。ナビゲーションツリーで、ツリーの [**Virtual WAN**] ブランチの横にある [**+**] をクリックします。

3. 仮想 **WAN** ブランチ。「変更管理」を選択します。

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



4. ウィザードを開始するには、[開始] をクリックします。

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

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

変更管理 ウィザードには、次のナビゲーション要素があります。

- ページ領域 - 変更管理 ウィザードの各ページのフォーム、テーブル、アクティビティボタンが表示されます。
- 変更管理ウィザードのページ・タブ—ページ・タブは、ウィザードの各ページのページ領域の左ペインにあります。タブは、ウィザードプロセスで対応する手順が実行された順に一覧表示されます。タブがアクティブになっている場合、タブをクリックしてウィザードの前のページに戻ることができます。タブがアクティブな場合、名前は青いフォントで表示されます。グレーのフォントは、非アクティブなタブを示します。すべての依存関係（前の手順）がエラーなしで実行されるまで、タブは非アクティブです。
- **Appliance-Site** テーブル：ほとんどのウィザードページでは、ウィザードページ領域の下部にあります。この表には、構成済みの各アプライアンス・サイトに関する情報と、そのアプライアンス・モデルおよびサイトのアクティブまたはステージングされたアプライアンス・パッケージをダウンロードするためのリンクが

含まれています。このコンテキストのパッケージは、そのアプライアンスモデルに対応する適切な SD-WAN ソフトウェアパッケージと、指定された構成パッケージを含む Zip ファイルバンドルです。表の上にある **Configuration Filenames** セクションには、ローカルアプライアンス上で現在アクティブでステージングされているパッケージのパッケージ名が表示されます。

- アクティブ/ステージングされたダウンロードリンク：これらは、**Appliance-Site** テーブルの各エントリの [**Download Package**] フィールド（右端の列）にあります。エントリ内のリンクをクリックして、そのアプライアンスサイトのアクティブなパッケージまたはステージングされたパッケージをダウンロードします。
- 開始—「開始」をクリックして、変更管理 ウィザードプロセスを開始し、「変更の準備」タブページに進みます。
- **[Activate Staged]** —これが初期展開ではなく、現在ステージングされている構成をアクティブ化する場合は、**Activation** ステップに直接進むことができます。[**Activate Staged**] をクリックして、[Activation] ページに直接進み、現在ステージングされている構成のアクティブ化を開始します。

アプライアンスハードウェアの設定

May 10, 2021

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

1. シャーシをセットアップします。

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

2. 電源を接続します。

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

3. アプライアンスの管理ポートをパーソナル・コンピュータに接続します。

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

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

SD-WAN VPX-SE 管理ポート

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

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

管理 IP アドレスの設定

September 26, 2023

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

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

- **SD-WAN VPX** 仮想アプライアンス—「SD-WAN VPX-SE の管理 IP アドレスの設定、および [SD-WAN VPX-SE と SD-WAN WANOP VPX インストールの違い」の項を参照してください。

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

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

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

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

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

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

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

3. PC の IP アドレスを変更します。

   PC で、ネットワークインターフェイスの設定を開き、PC の IP アドレスを次のように変更します。

   - 192.168.100.50

4. PC の [サブネットマスク] 設定を次のように変更します。

   - 255.255.0.0

5. PC でブラウザを開き、アプライアンスのデフォルトの IP アドレスを入力します。ブラウザのアドレス行に次の IP アドレスを入力します。

   - 192.168.100.1

   > 注
   >
   > SD-WAN アプライアンスに接続する場合は、Google Chrome ブラウザを使用することをお勧めします。
   >
   > 管理 Web インターフェイスのブラウザ証明書の警告を無視します。

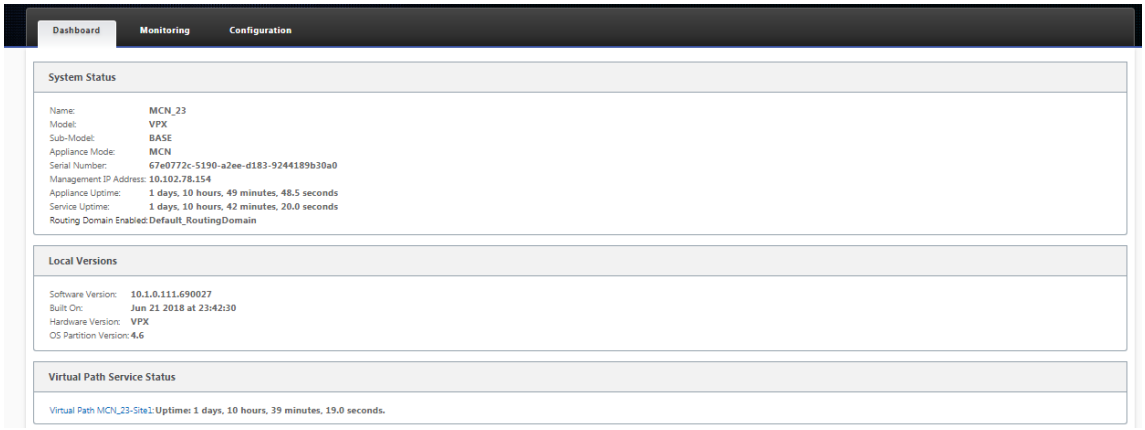
   これにより、接続されたアプライアンスで SD-WAN 管理 Web インターフェイスのログイン画面が開きます。

6. 管理者のユーザー名とパスワードを入力し、[**Login**] をクリックします。

   - デフォルトの管理者ユーザー名: *admin*
   - デフォルトの管理者パスワード: パスワード

   > 注
   >
   > デフォルトのパスワードを変更することをお勧めします。パスワード回復には設定のリセットが必要になる場合があるため、必ず安全な場所にパスワードを記録してください。

   管理 Web インターフェイスにログインすると、次に示すように [ダッシュボード] ページが表示されます。



   アプライアンスの管理 Web インターフェイスに初めてログインすると、ダッシュボード に Alert アイコン（goldenrod dtela）と SD-WAN サービスが無効になっていてライセンスがインストールされていないこと

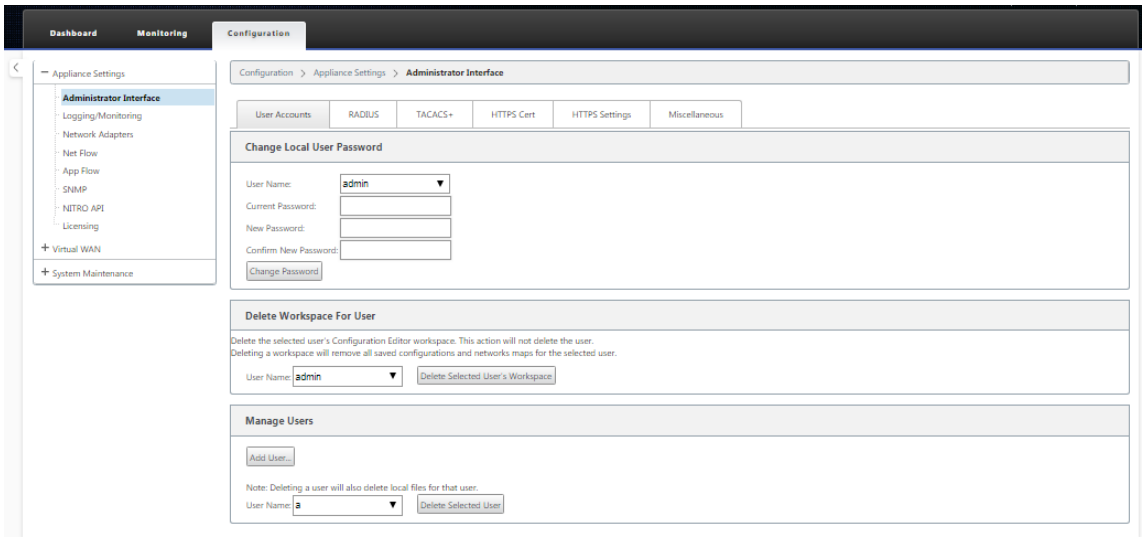
を示すアラートメッセージが表示されます。現時点では、このアラートは無視できます。このアラートは、ライセンスをインストールし、アプライアンスの構成および展開プロセスを完了した後に解決されます。

7. メインメニューバーで、[構成] セクションタブを選択します。

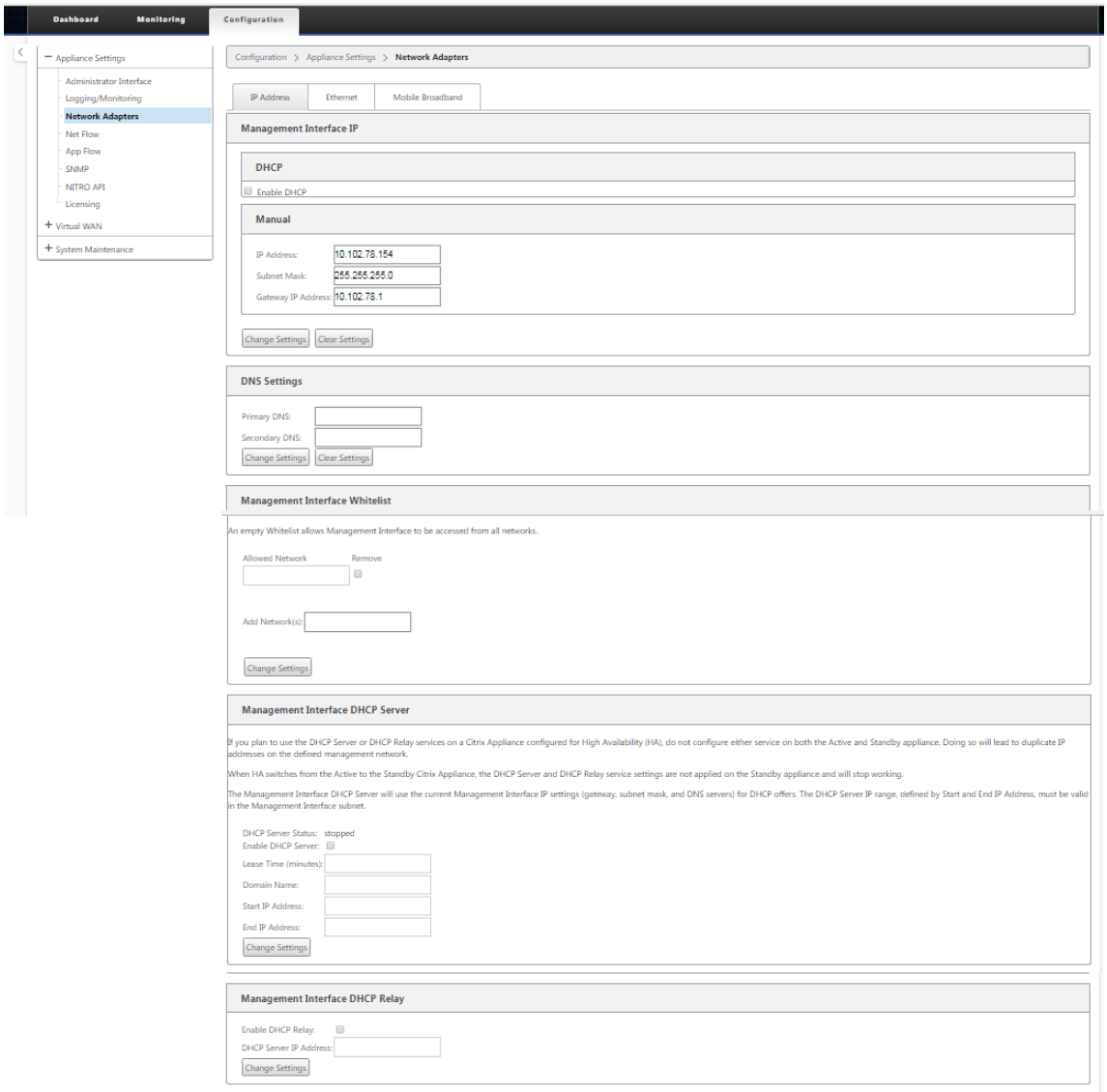
   これにより、画面の左ペインに [構成] ナビゲーションツリーが表示されます。[構成] ナビゲーションツリーには、次の 3 つの主要なブランチがあります。

   - アプライアンスの設定
   - 仮想 WAN
   - システムメンテナンス

   ［構成］タブを選択すると、［アプライアンスの設定］ブランチが自動的に開きます。デフォルトでは、［管理者インタフェース］ページが選択されています（次の図を参照）。



8. ナビゲーション・ツリーの「アプライアンス設定」ブランチで、「ネットワーク・アダプタ」を選択します。これにより、[ネットワークアダプタ] 設定ページが表示され、次の図に示すように、[**IP** アドレス] タブが既定で事前に選択されています。



9. [**IP Address**] タブページで、設定する SD-WAN アプライアンスの次の情報を入力します。

   - IP アドレス
   - サブネット マスク
   - Gateway IP アドレス

   > 注
   >
   > 管理 IP アドレスは、アプライアンスごとに一意である必要があります。

10. ［設定の変更］をクリックします。確認ダイアログボックスが表示され、これらの設定を変更することを確認するメッセージが表示されます。

11. ［**OK**］をクリックします。

12. PC のネットワークインターフェイスの設定を元の設定に戻します。

> 注
>
> PC の IP アドレスを変更すると、アプライアンスへの接続が自動的に切断され、管理 Web インターフェイス上のログインセッションが終了します。

13. アプライアンスを PC から切断し、アプライアンスをネットワークルーターまたはスイッチに接続します。イーサネットケーブルを PC から取り外しますが、アプライアンスからは取り外さないでください。ケーブルの自由な端をネットワークルーターまたはスイッチに接続します。

    これで、SD-WAN アプライアンスがネットワークに接続され、ネットワーク上で利用可能になりました。

14. 接続をテストします。ネットワークに接続されている PC で、ブラウザを開き、アプライアンスに構成した管理 IP アドレスを入力します。

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

    > ヒント
    >
    > 接続を確認したら、管理 Web インターフェイスからログアウトしないでください。これを使用して、以降のセクションで概説されている残りのタスクを完了します。

    これで、SD-WAN アプライアンスの管理 IP アドレスが設定され、ネットワーク上の任意の場所からアプライアンスに接続できるようになります。

日付と時刻の設定

May 10, 2021

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

> 注
>
> ネットワークに追加するアプライアンスごとに、このプロセスを繰り返す必要があります。

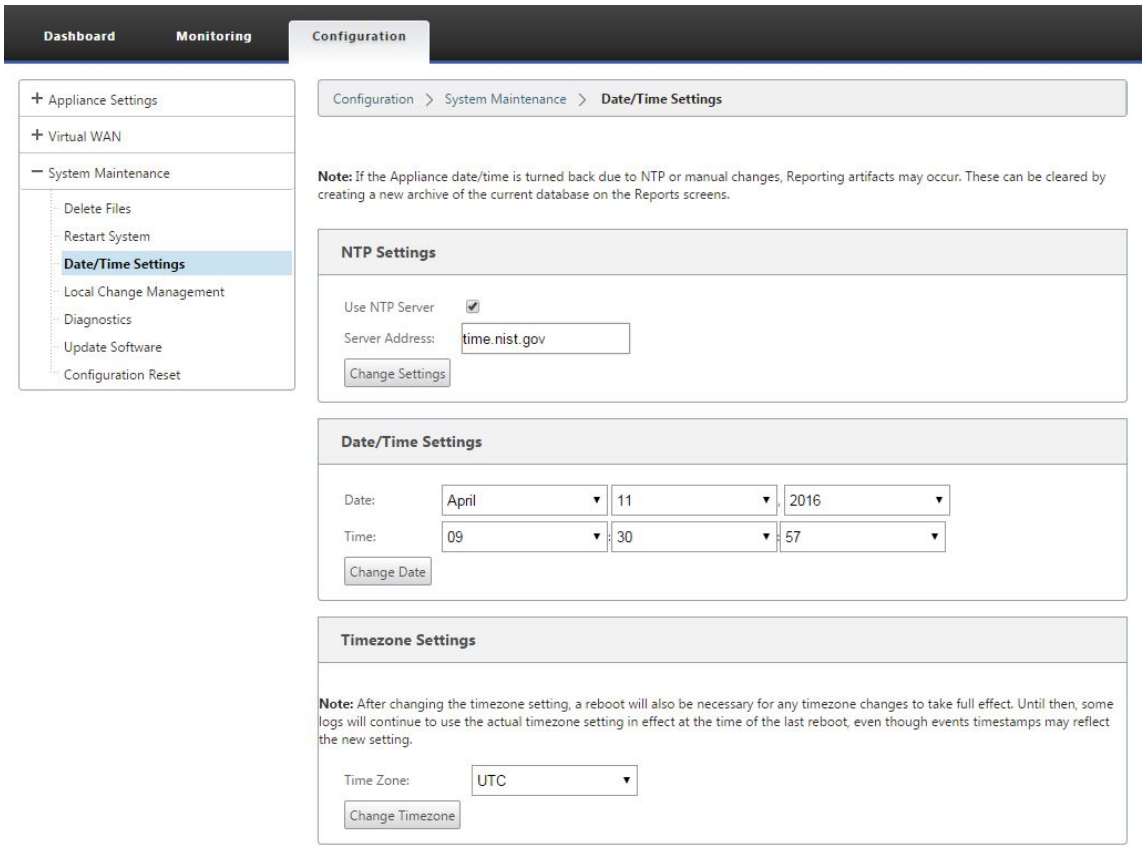
日付と時刻を設定するには、次の操作を行います。

1. 構成しているアプライアンスの管理 Web Interface にログインします。
2. メインメニューバーで、[構成] タブを選択します。

   これにより、画面の左ペインに [構成] ナビゲーションツリーが表示されます。

3. ナビゲーションツリーで [システムメンテナンス] ブランチ を開きます。

4. [システムメンテナンス] ブランチで、**[日付/時刻の設定]** を選択します。これにより、次のように [日付/時刻の設定] ページが表示されます。



5. ページの下部にある [**Time Zone]** フィールドのドロップダウンメニューからタイムゾーン を選択します。

> 注
>
> タイムゾーンの設定を変更する必要がある場合は、日付と時刻を設定する前に変更する必要があります。変更しないと、入力したとおりに設定が維持されません。

6. [タイムゾーンの変更] をクリックします。これにより、タイムゾーンが更新され、それに応じて現在の日付と時刻の設定が再計算されます。この手順の前に正しい日付と時刻を設定すると、設定が正しくなくなります。タイムゾーンの更新が完了すると、成功の警告アイコン（緑色のチェックマーク）とステータスメッセージがページの上部セクションに表示されます。

7. （任意）NTP サーバサービスを有効にします。

   a) [**NTP** サーバを使用] を選択します。
   b) [Server Address] フィールドに サーバアドレスを入力します。
   c) ［設定の変更］をクリックします。
      更新が完了すると、成功の警告アイコン (緑のチェックマーク) とステータスメッセージが表示されます。

8. 「日付」フィールドのドロップダウンメニューから月、日、年を選択します。

9. [**Time**] フィールドのドロップダウンメニューから時、分、および秒を選択します。
10. [日付を変更] をクリックします。

> 注:
>
> これにより、日付と時刻の設定が更新されますが、成功の警告アイコンやステータスメッセージは表示されません。

次の手順では、コンソールセッションの タイムアウト しきい値を最大値に設定します。この手順はオプションですが、推奨されます。これにより、設定作業中にセッションが途中で終了することを防ぎ、作業が失われる可能性があります。コンソールセッションの タイムアウト 値を設定する手順は、次のセクションで説明します。タイムアウトしきい値をリセットしない場合は、「SD-WAN ソフトウェアライセンスファイルのアップロードとインストール」セクションに直接進んでください。

> 警告
>
> コンソールセッションがタイムアウトになったり、構成を保存する前に管理 Web Interface からログアウトした場合、保存されていない構成の変更はすべて失われます。システムに再度ログインし、最初から設定手順を繰り返します。

セッションのタイムアウト

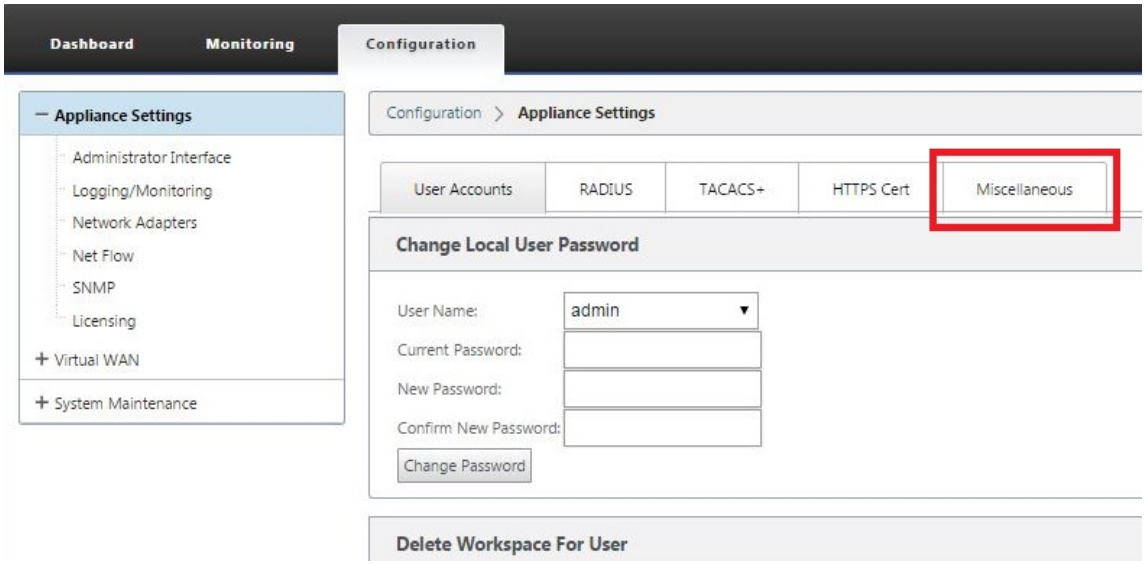
May 10, 2021

コンソールセッションがタイムアウトになったり、構成を保存する前に管理 Web Interface からログアウトした場合、保存されていない構成の変更はすべて失われます。その後、システムに再度ログインし、設定手順を最初から繰り返す必要があります。そのため、構成パッケージを作成または変更する場合や、その他の複雑なタスクを実行する場合は、コンソールセッションのタイムアウト間隔を高い値に設定することをお勧めします。デフォルトは 60 分です。最大値は 9,999 分です。セキュリティ上の理由から、これらのタスクを完了した後、しきい値を下限値にリセットする必要があります。

コンソールセッションの タイムアウト 間隔をリセットするには、次の手順を実行します。

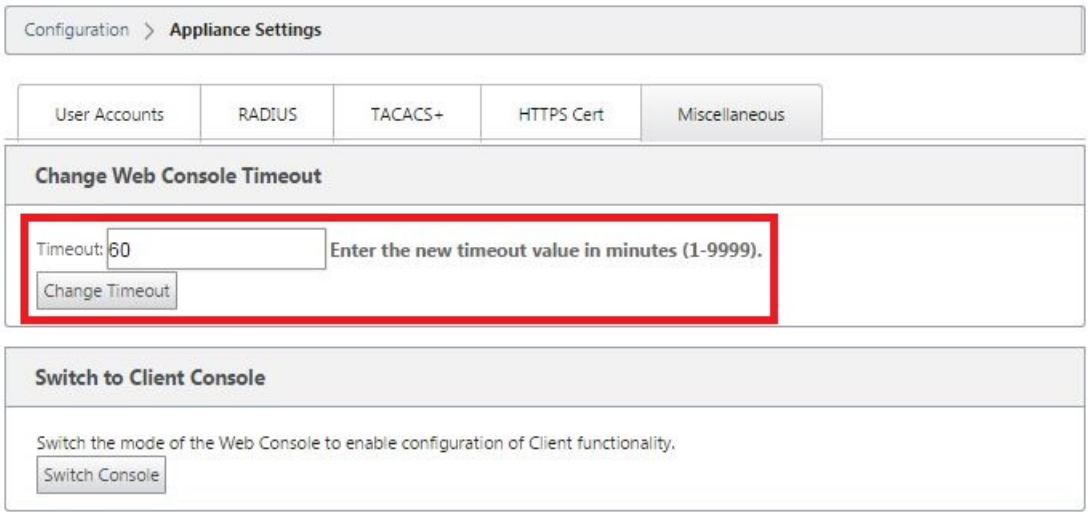
1. ［構成］タブを選択し、ナビゲーション・ツリーで［アプライアンスの設定］ブランチを選択します。

   これにより、「アプライアンスの設定」ページが表示され、デフォルトで「ユーザー・アカウント」タブが事前に選択されています。



2. [その他] タブ (右端隅) を選択します。

「その他」タブ・ページが表示されます。



3. コンソールの [タイムアウト] 値を入力します。

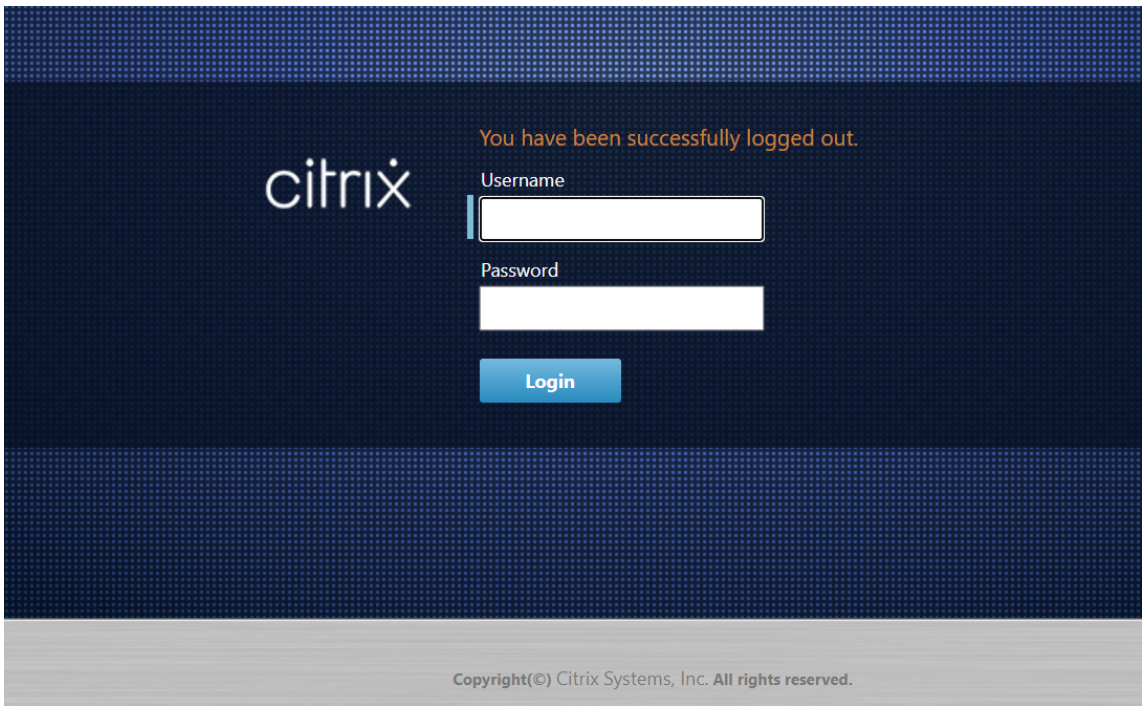
[**Web** コンソールの ****** タイムアウト の変更 **] セクションの [タイムアウト] フィールドに、最大値 9999 まで大きい値（分単位）を入力します。デフォルトは 60 で、初期設定セッションでは非常に短すぎます。

> 注
>
> セキュリティ上の理由から、設定と展開の完了後に、この値をより低い間隔にリセットしてください。

4. [タイムアウトの変更] をクリックします。

これにより、セッションの タイムアウト 間隔がリセットされ、操作が完了すると成功メッセージが表示されます。

短い間隔（数秒）後、セッションは終了し、管理 Web Interface から自動的にログアウトされます。[ログイン] ページが表示されます。



5. 管理者のユーザー名（*admin*）とパスワード（パスワード）を入力し、「ログイン」をクリックします。

   次のステップでは、SD-WAN ソフトウェアライセンスファイルをアプライアンスにアップロードしてインストールします。

アラームの設定

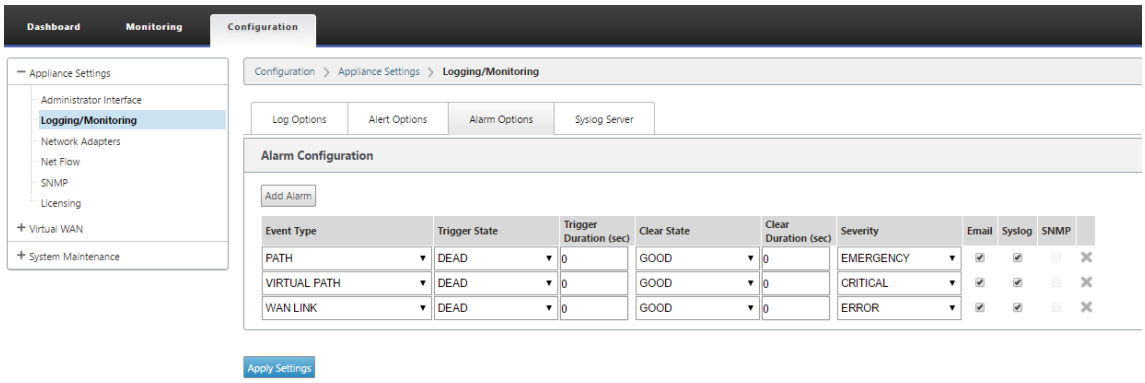
May 10, 2021

SD-WAN アプライアンスを設定して、ネットワークと優先順位に基づいてアラーム状態を特定し、アラートを生成し、電子メール、syslog、または SNMP トラップ経由で通知を受信できるようになりました。

アラームは、イベントタイプ、トリガー状態、クリア状態、重大度で構成されたアラートです。

アラーム設定を構成するには:

1. SD-WAN Web 管理インターフェイスで、［構成］>［アプライアンスの設定］>［ログ/モニタリング］の順に選択し、［アラームオプション］をクリックします。
2. [**Add Alarm**] をクリックして、新しいアラームを追加します。



3. 次のフィールドの値を選択または入力します。

   - イベントタイプ: SD-WAN アプライアンスは、ネットワーク内の特定のサブシステムまたはオブジェクトに対してアラームをトリガーできます。これらはイベントタイプと呼ばれます。使用可能なイベントタイプは、SERVICE、VIRTUAL_PATH、WANLINK、PATH、DYNAMIC_VIRTUAL_PATH、WAN_LINK_CONGESTION、USAGE_CONGESTION、FAN、POWER_SUPPLY、PROXY_ARP、ETHERNET、DISCOVERED_MTU、GRE_TUNNEL、IPSEC_TUNNEL です。
   - トリガー状態: イベントタイプのアラームをトリガーするイベント状態。使用可能なトリガー状態オプションは、選択したイベントタイプによって異なります。
   - トリガー期間: 秒単位の期間。アプライアンスがアラームをトリガーする速度を決定します。即時アラートを受信するには「0」を入力するか、15～7200 秒の値を入力します。Trigger Duration 期間内に同じオブジェクトでさらにイベントが発生すると、アラームはトリガーされません。イベントが Trigger Duration 期間よりも長く持続する場合のみ、より多くのアラームがトリガーされます。
   - **Clear State**: アラームがトリガーされた後に、イベントタイプのアラームをクリアするイベント状態。使用可能な Clear State オプションは、選択したトリガー状態によって異なります。
   - **[Clear Duration]:** アラームをクリアするまでの待機時間を秒単位で指定します。「0」と入力してアラームをただちにクリアするか、15-7200 秒の値を入力します。指定された時間内に同じオブジェクトで別のクリア状態イベントが発生した場合、アラームはクリアされません。
   - 重大度: アラームの緊急度を決定するユーザー定義フィールド。重大度は、アラームがトリガーまたはクリアされたときに送信されるアラートと、トリガーされたアラームの概要に表示されます。
   - **Email**: イベントタイプのアラームトリガーとクリアアラートが電子メールで送信されます。
   - **Syslog**: イベントタイプのアラームトリガーおよびクリアアラートが Syslog 経由で送信されます。
   - **SNMP**: イベントタイプのアラームトリガーおよびクリアアラートは、SNMP トラップを介して送信されます。

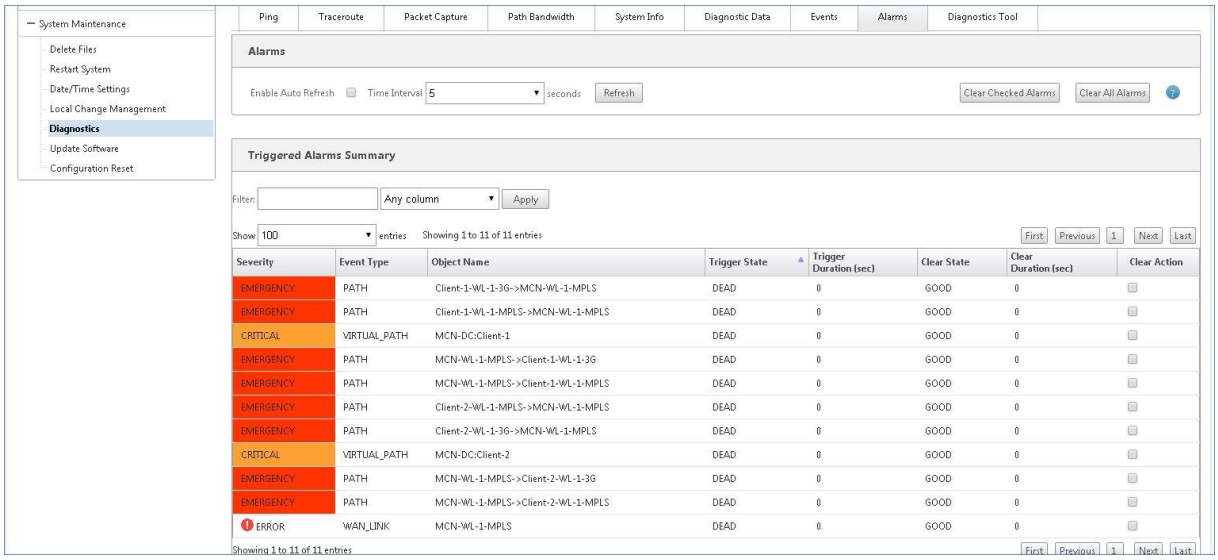
4. 必要に応じて、引き続きアラームを追加します。
5. [設定の適用] をクリックします。

トリガーされたアラームの表示

トリガーされたすべてのアラームの概要を表示するには、次の手順を実行します。

SD-WAN Web 管理インターフェイスで、[構成] > [システムメンテナンス**] > [**診断**] > [**アラーム] に移動します。

トリガーされたすべてのアラームのリストが表示されます。



トリガーされたアラームのクリア

トリガーされたアラームを手動でクリアするには、次の手順を実行します。

1. SD-WAN Web 管理インターフェイスで、[構成] > [システムメンテナンス**] > [**診断**] > [**アラーム] に移動します。
2. [**Clear Action**] カラムで、クリアするアラームを選択します。
3. [チェック済みアラームをクリア] をクリックします。または、[**Clear All Alarms**] をクリックして、すべてのアラームをクリアします。

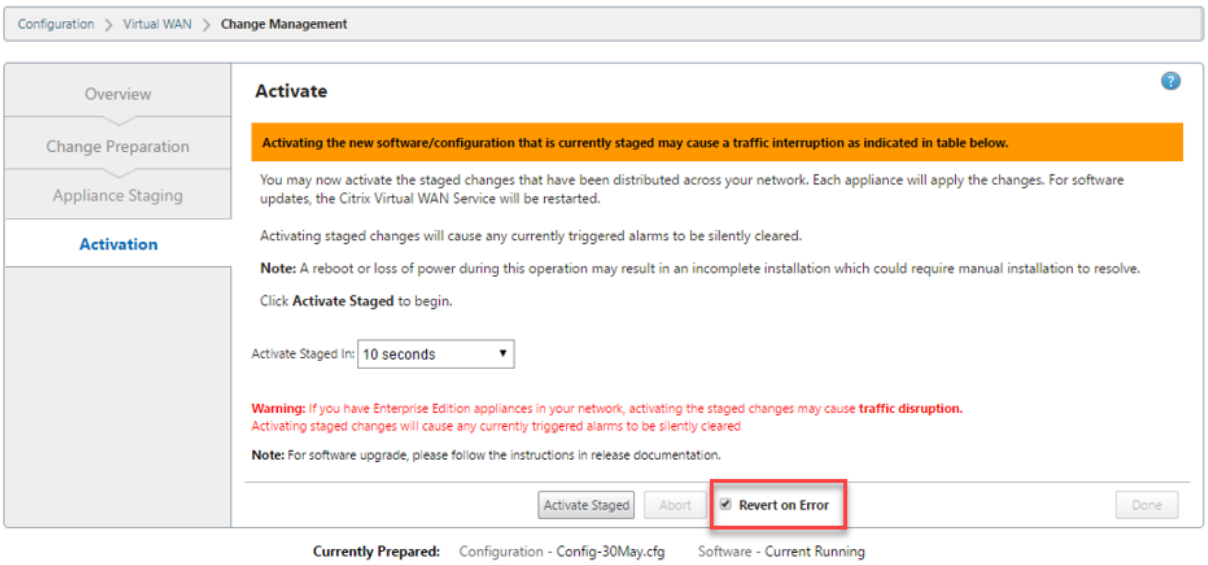
ロールバックの構成

May 10, 2021

構成ロールバック機能を使用すると、変更管理システムは、以前にアクティブだったソフトウェア/構成に戻すことにより、次のソフトウェア/構成エラーを検出してリカバリできます。

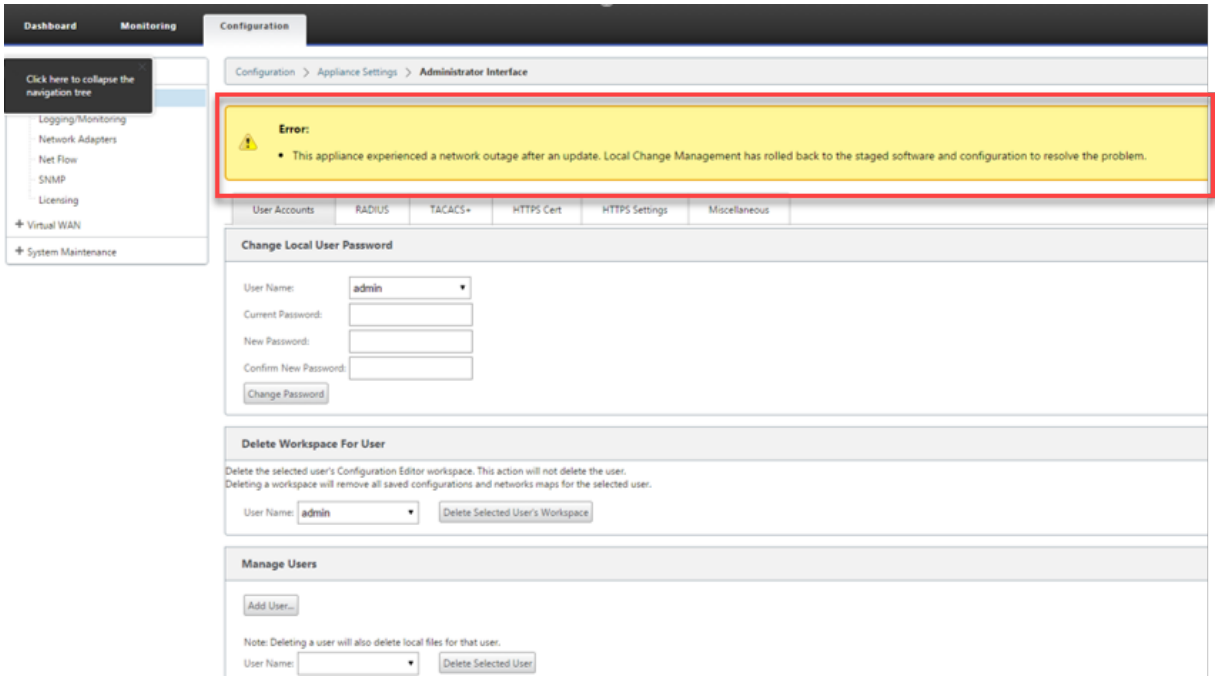
- ソフトウェアのアップグレード後、Virtual Path は停止し、ソフトウェアのクラッシュが発生するとサービスが無効になります。
- 構成を変更した後、Virtual Path はソフトウェアクラッシュなしで停止します。
- MCN アプライアンス自体の構成によって MCN サイトでネットワークの問題が発生した場合、システム停止は検出されず、それ自体をロールバックしません。ただし、ネットワーク内の他のすべてのクライアントは、MCN に接続できなかったため、自身をロールバックします。

構成ロールバック機能はデフォルトで有効になっています。この機能を無効にするには、変更管理ウィザードの **[** アクティブ化] タブの [エラー時に元に戻す **] オプションをオフにします。



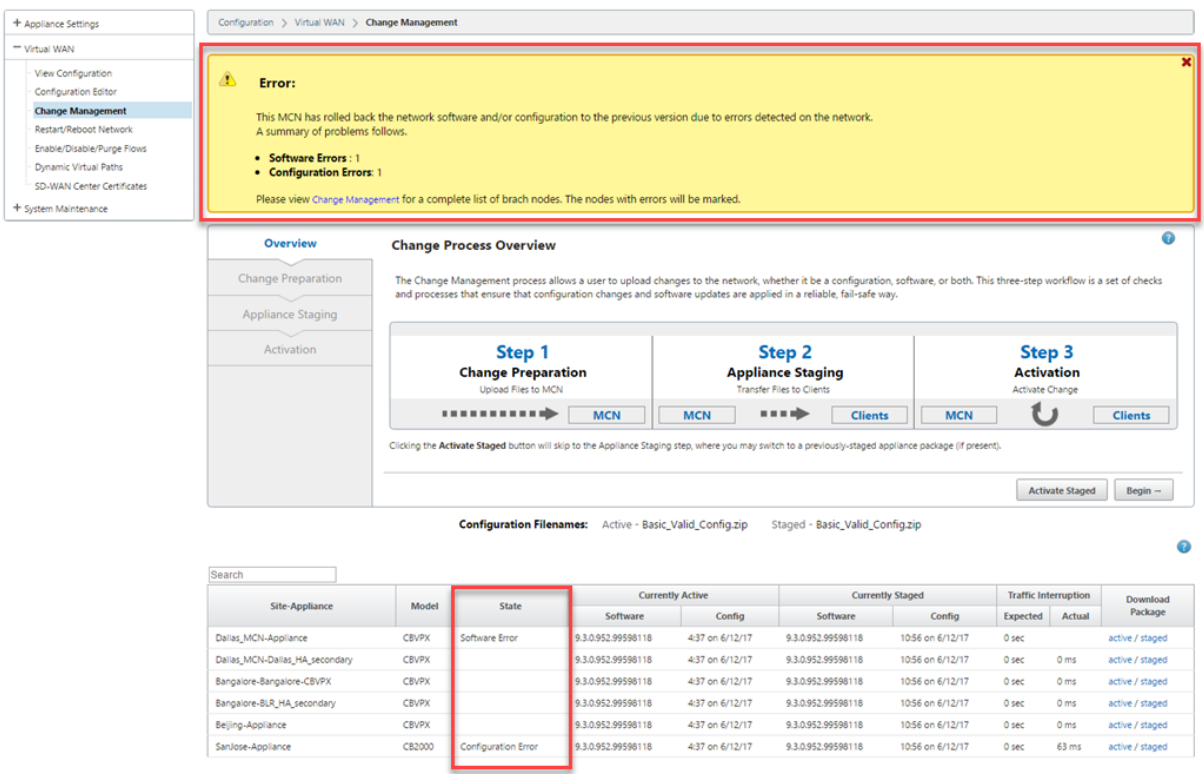
MCN からステージングされたパッケージをアクティブ化中にクライアント上でシステム構成エラーが発生した場合は、クライアントは以前のソフトウェア構成に戻り、次のスクリーンショットに示すように、エラーメッセージが表示されます。

アプライアンスのクラッシュが検出された場合、クライアントは SOFTWARE_UPDATE オブジェクトのクリティカル重大度イベントを生成し、ネットワーク障害が検出された場合は CONFIG_UPDATE オブジェクトのクリティカル重大度イベントを生成します。



「エラー時に元に戻す」が有効な場合、クライアントアプライアンスは自身を約 30 分間監視します。ソフトウェアが 30 分以内にクラッシュした場合、またはネットワークが 30 分間ダウンしている場合（MCN への仮想パスを確立できない場合）、ロールバックがトリガーされます。

次のスクリーンショットに示すように、MCN では、エラーメッセージが表示されます。クライアントがネットワークに再参加すると、検出されたエラーの種類が報告されます。エラー数の要約カウントがエラーメッセージに表示されます。



MCN の [**Change Management**] ウィンドウには、サイト・アプライアンスの状態が表示され、そのサイトでソフトウェアエラーまたは構成エラーが発生したかどうかが示されます。

マスター制御ノードの設定

May 10, 2021

SD-WAN マスターコントロールノード（**MCN**）は、仮想 WAN のヘッドエンドアプライアンスです。通常、これはエンタープライズデータセンターに導入された 4000 または 5100 の仮想 WAN アプライアンスです。MCN は、初期システム設定とその後の設定変更の配布ポイントとして機能します。また、ほとんどのアップグレード手順は、MCN の管理 Web インターフェイスを通じて行います。仮想 WAN に存在できるアクティブな MCN は 1 つだけです。

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

MCN サイト展開の補足情報

次のサポート技術情報サポート資料をお勧めします。

- 仮想 WAN PBR モードの展開手順（CTX201577）

http://support.citrix.com/article/CTX201577

- 仮想 WAN ゲートウェイモードの展開手順（CTX201576）

  http://support.citrix.com/article/CTX201576

MCN サイト構成手順の概要

MCN サイトを追加および設定する手順は、次のとおりです。

1. 管理 Web インターフェイスを **MCN** コンソール モードに切り替えます。
2. MCN サイトを追加します。
3. MCN サイトの仮想インターフェイスグループを設定します。
4. MCN サイトの仮想 IP アドレスを設定します。
5. （任意）サイトの LAN GRE トンネルを設定します。
6. MCN サイトの WAN リンクを設定します。
7. MCN サイトのアクセスインターフェイスを設定します。
8. MCN サイトのルートを設定します。
9. （任意）MCN サイトの高可用性を設定します。
10. （任意）仮想 WAN のセキュリティと暗号化を設定します。
11. MCN サイト構成に名前を付けて保存します。

これらの各タスクの手順については、次のセクションで説明します。

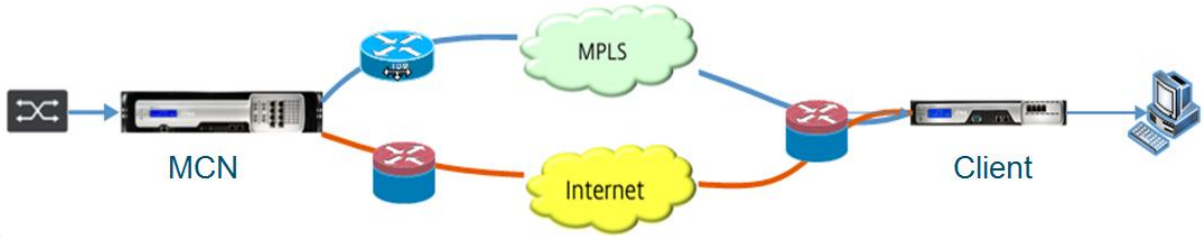
MCN の概要

May 10, 2021

マスターコントロールノード **(MCN)** は、仮想 WAN のマスター Controller として機能する中央の仮想 WAN アプライアンスであり、クライアントノードの中央管理ポイントです。すべての構成アクティビティ、およびアプライアンスパッケージの準備、およびクライアントへの配布は MCN で実行されます。また、特定の仮想 WAN モニタリング情報は MCN 上でのみ使用できます。MCN は
Virtual WAN 全体を監視できますが、クライアントノードはローカルイントラネットのみを監視でき、接続先のクライアントに関する情報も監視できます。

MCN の主な目的は、企業のサイト間通信のために、仮想 WAN 上に配置された 1 つ以上のクライアントノードで仮想パスを確立して利用することです。MCN は、複数のクライアントノードを管理し、仮想パスを持つことができます。複数の MCN を設定できますが、一度にアクティブにできるのは 1 つだけです。

以下の図は、Virtual WAN Edition 展開における MCN（データセンター）アプライアンスとクライアント（ブランチノード）アプライアンスの基本的な役割とコンテキストを示しています。



MCN コンソールに切り替える

May 10, 2021

MCN サイトを追加および構成するには、まず MCN ロールに昇格するアプライアンスの管理 Web インターフェイスにログインし、管理 Web インターフェイスを **MCN** コンソール モードに切り替える必要があります。**MCN** コンソール モードでは、現在接続している管理 Web インターフェイスの構成エディタにアクセスできます。その後、構成エディタ を使用して MCN サイトを追加および構成できます。

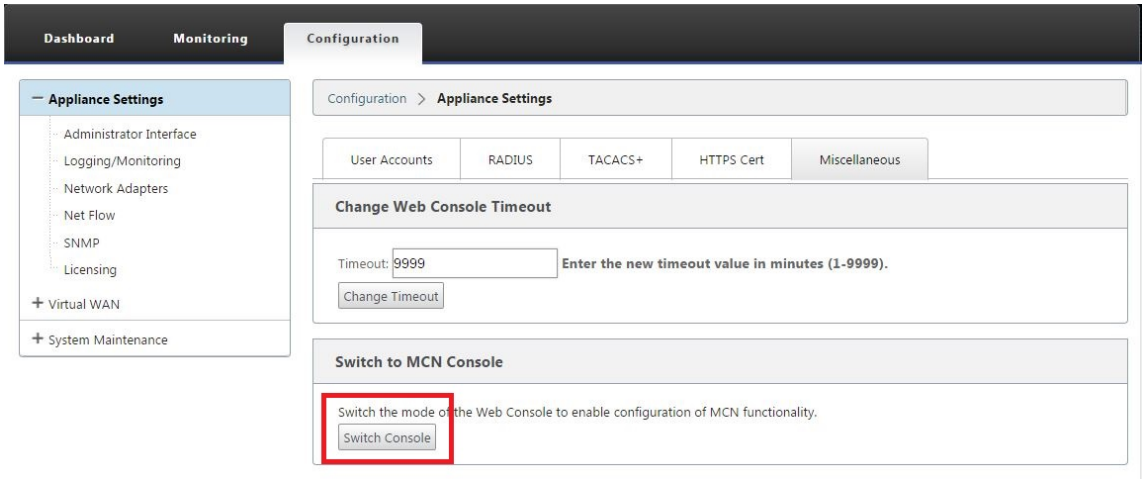
> 注
>
> **MCN** コンソール モードに切り替えると、管理 Web インターフェイスモードの動作モードだけが変更され、アプライアンス自体のアクティブロールは変更されません。アプライアンスを MCN のロールに昇格するには、最初に MCN サイトを追加して設定し、指定した MCN アプライアンス上で構成とソフトウェアパッケージをアクティブ化する必要があります。

管理 Web インターフェイスを **MCN** コンソール モードに切り替えるには、次の手順を実行します。

1. MCN として設定するアプライアンスの管理 Web インターフェイスにログインします。
2. 管理 Web Interface のメイン画面のメインメニューバーにある「構成」をクリックします (ページ上部にある青いバー)。
3. ナビゲーション・ツリー（左ペイン）で、アプライアンスの設定 ブランチを開き、管理者インタフェースをクリックします。

   これにより、中央のペインに [管理者インタフェース] ページが表示されます。
4. 「その他」タブを選択します。

   [その他の管理 設定] ページが表示されます。



[その他] タブページの下部には、[クライアントへの切り替え] **> [MCN** コンソール] セクションがあります。このセクションには、アプライアンスのコンソールモードを切り替えるための [Switch Console] ボタンが含まれます。

セクション見出しは、次のように現在のコンソールモードを示します。

- クライアントコンソール モード（デフォルト）の場合、セクションの見出しは **MCN** コンソールに切り替えるです。
- **MCN** コンソール モードの場合、セクションの見出しは [クライアントコンソールに切り替え] です。

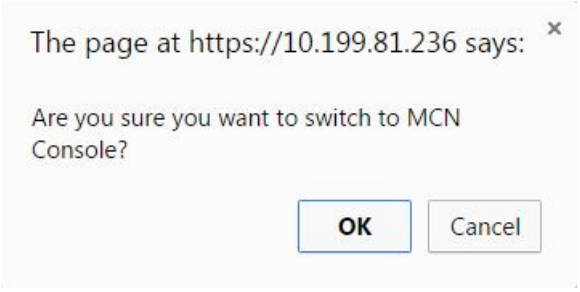
デフォルトでは、新しいアプライアンスは クライアント・コンソール・モードに設定されています。

MCN コンソール モードでは、ナビゲーションツリーの **[**構成エディタ**]** ブランチが有効になります。構成エディタ は MCN アプライアンスでのみ使用できます。

> 注
>
> 次の手順に進む前に、アプライアンスがデフォルト（**Client Console** モード）に設定されていることを確認します。セクションの見出しは、**MCN** コンソールに切り替えます。

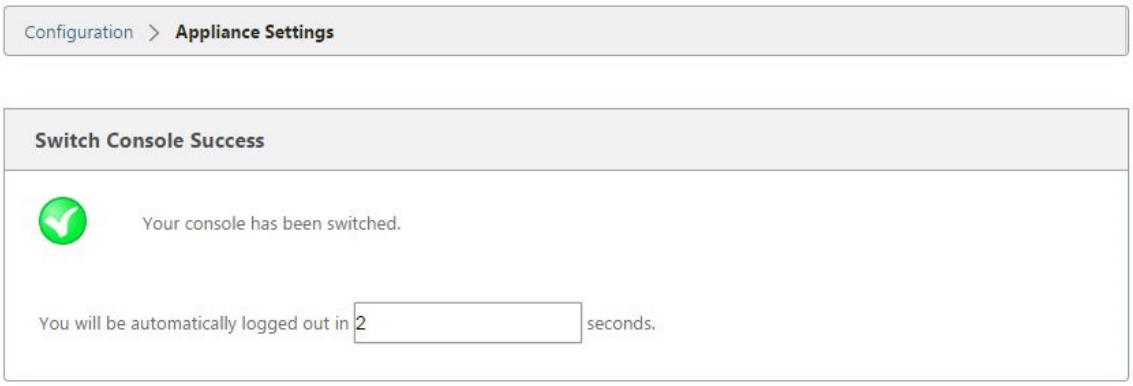
5. スイッチ・モード をクリックして、アプライアンス・モードを **MCN** コンソール・モードに設定します。

   MCN モードに切り替えるかどうかを確認するダイアログボックスが表示されます。

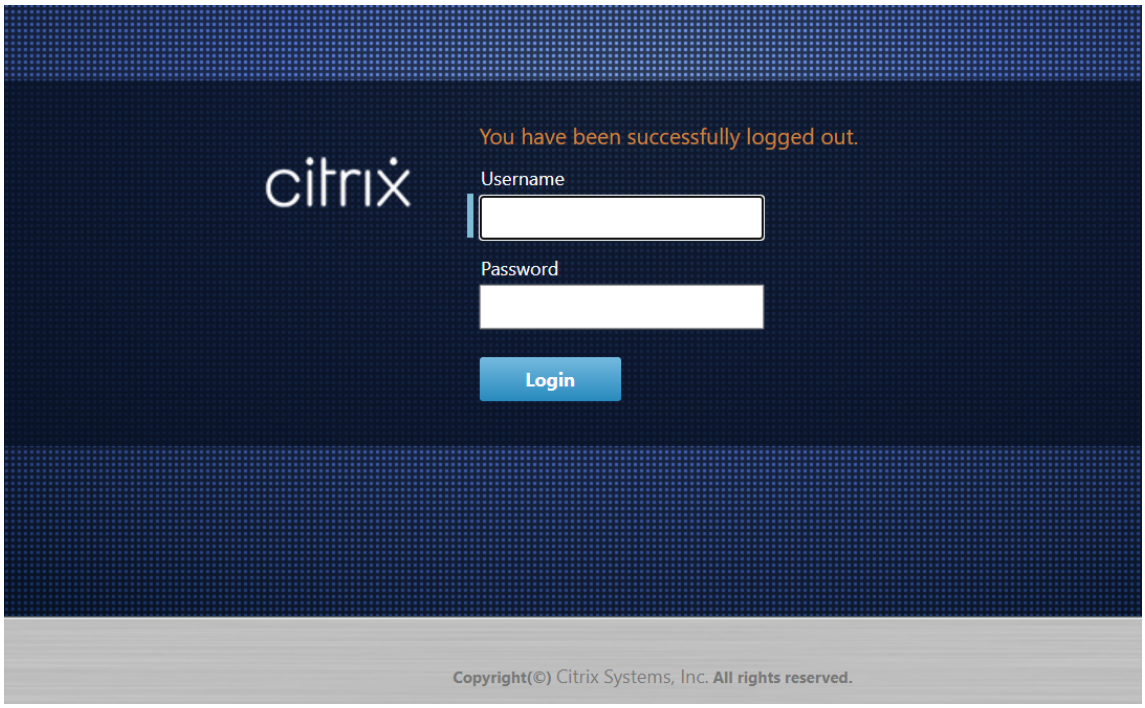


6. [**OK**] をクリックします。

これにより、コンソールモードが **MCN** コンソール モードに切り替わり、現在のセッションが終了します。成功メッセージと、セッションが終了するまでの残り秒数を示すカウントダウンステータスが表示されます。



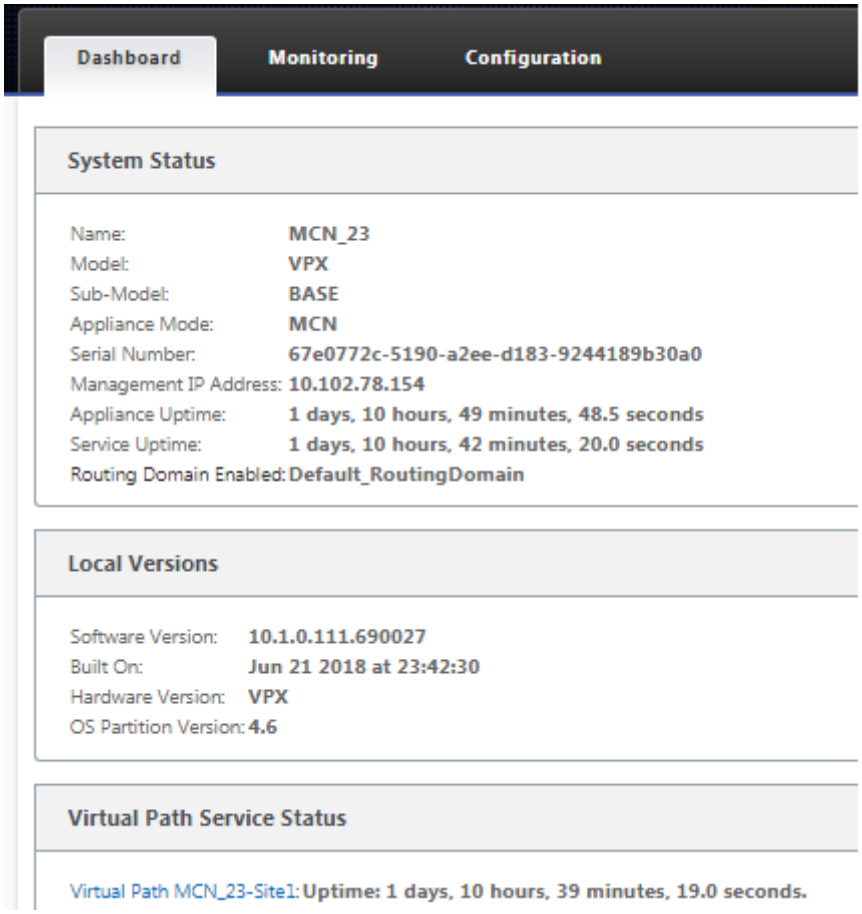
カウントダウンが完了すると、セッションが終了し、ログインページが表示されます。



7. 管理者のユーザー名とパスワードを入力し、[ログイン] をクリックします。

   - デフォルトの管理者ユーザー名: *admin*
   - デフォルトの管理者パスワード: パスワード

   ログイン後、ダッシュボード が表示され、アプライアンスが MCN モードであることを示します。



次の手順では、新しい構成を開き、MCN サイトを [サイト] テーブルに追加し、新しい MCN サイトの構成を開始します。

MCN を構成する

May 10, 2021

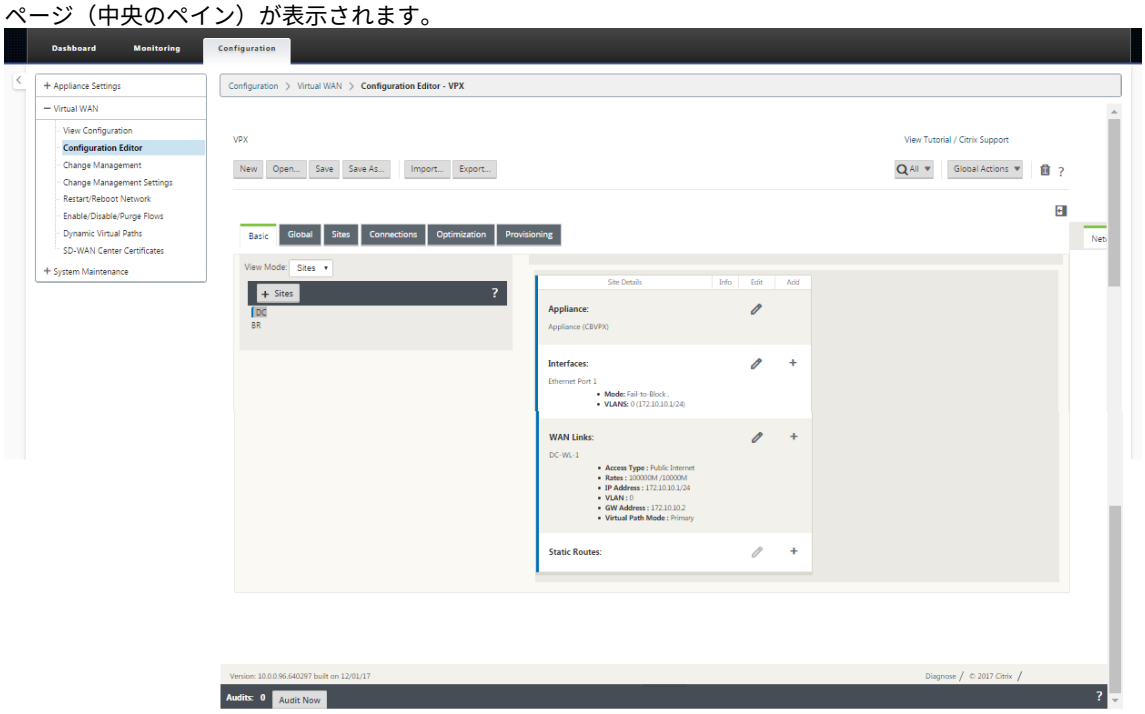
最初のステップは、新しい構成パッケージを開き、MCN サイトを新しい構成に追加します。

> 注
>
> 構成エディタ は、**MCN** コンソール モードでのみ使用できます。ナビゲーションツリーの [Virtual WAN] ブランチで [**Configuration Editor**] オプションが使用できない場合は、管理 Web インターフェイスの MCN コンソールモードへの切り替えのセクションを参照してください。コンソールモードの変更手順については、を参照してください。
>
> 構成パッケージは頻繁に保存するか、構成内の重要なポイントに保存することをお勧めします。手順については、「MCN サイト設定の命名、保存、およびバックアップ」セクションに記載 されています。

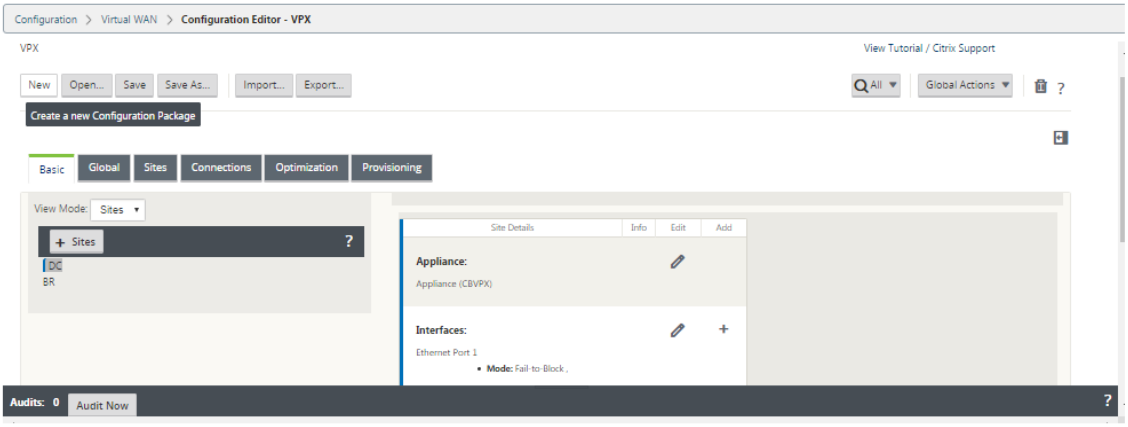
> 警告
>
> コンソールセッションがタイムアウトになったり、構成を保存する前に管理 Web Interface からログアウトした場合、保存されていない構成の変更はすべて失われます。その後、システムに再度ログインし、設定手順を最初から繰り返す必要があります。そのため、構成パッケージを作成または変更したり、その他の複雑なタスクを実行したりするときは、コンソールセッションのタイムアウト間隔を高い値に設定することをお勧めします。デフォルトは 60 分です。最大値は 9,999 分です。セキュリティ上の理由から、これらのタスクを完了した後、しきい値を下限値にリセットする必要があります。手順については、「コンソール・セッションのタイムアウト間隔の設定（オプション）」を参照してください。

MCN アプライアンスサイトを追加して構成を開始するには、次の手順を実行します。

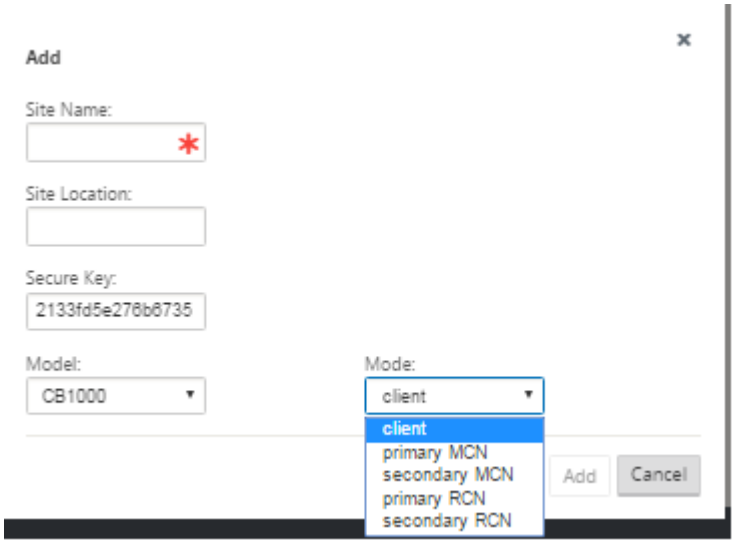
1. ナビゲーションツリーで、[仮想 **WAN**] > [構成エディタ] に移動します。これにより、構成エディタのメインページ（中央のペイン）が表示されます。



2. 「新規」**(New**) をクリックして、新しい構成の定義を開始します。[新しい 構成設定] ページが表示されます。



3. **** サイト バーの [+ S** ites] をクリックして、MCN サイトの追加と構成を開始します。[サイトの追加] ダイアログボックスが表示されます。



4. サイト情報を入力します。

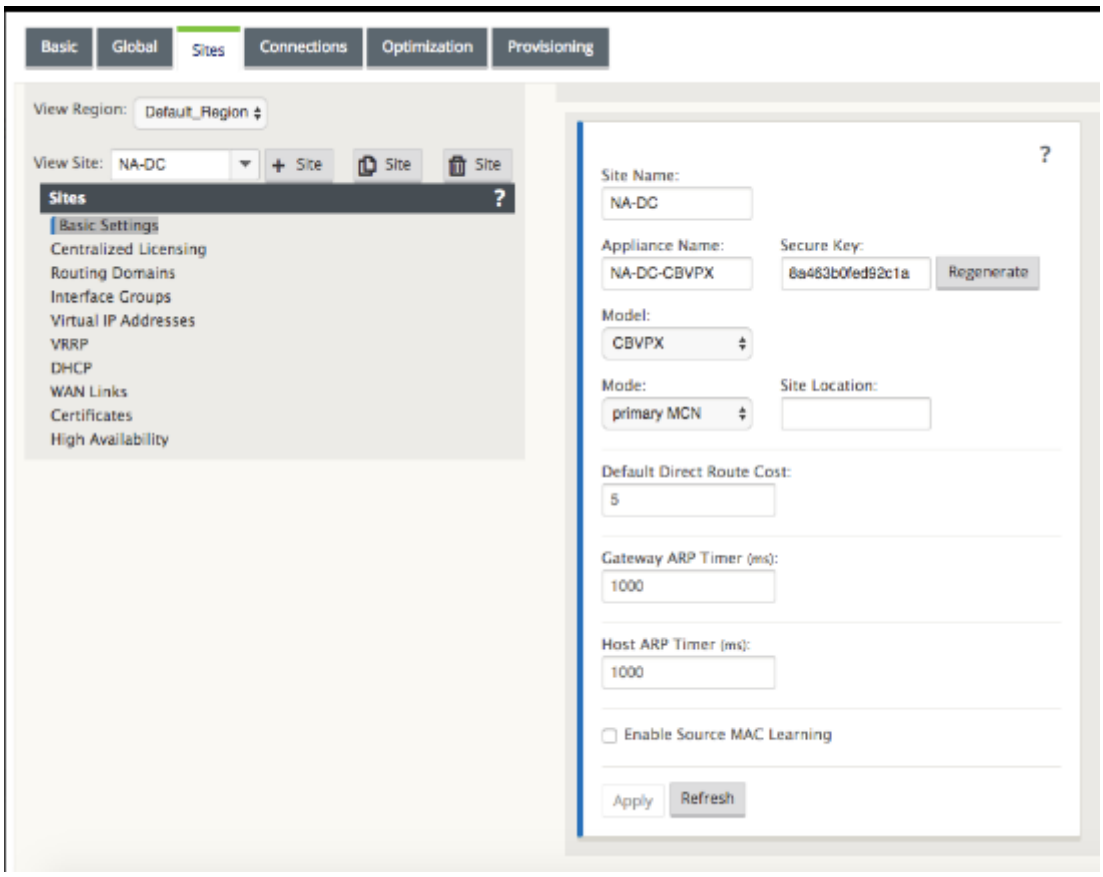
以下を実行します:

1. サイト名とセキュアキーを入力します。
2. アプライアンスの モデルを選択します。
3. モードを選択します。
4. モードとして プライマリ **MCN** を選択します。

> 注
>
> モデル・オプション・メニューには、サポートされているアプライアンス・モデルの汎用モデル名がリストされます。一般名には、Standard Edition モデルのサフィックスは含まれませんが、対応する SD-WAN アプライアンスモデルに対応しています。この SD-WAN アプライアンスモデルに対応するモデル番号を選択します。(たとえば、これが SD-WAN 4000-SE アプライアンスの場合は 4000 を選択します)。
>
> エントリにはスペースを含めることはできません。また、Linux 形式である必要があります。

サイトを追加するには、次の手順に従います。

1. [追加] をクリックしてサイトを追加します。これにより、新しいサイトが **[サイト]** ツリーに追加され、新しいサイトの [基本設定] 構成フォームが表示されます。



[適用] をクリックすると、追加のアクションが必要であることを示す監査警告が表示されます。赤い点または金色のデルタアイコンは、表示されるセクションにエラーを示します。これらの警告を使用して、エラーや不足している構成情報を識別できます。監査警告アイコンの上にカーソルを置くと、そのセクションのエラーの簡単な説明が表示されます。暗いグレーの 監査 ステータスバー (ページ下部) をクリックして、未解決の監査警告をすべて一覧表示することもできます。設定時にサイトレベルで設定可能なホスト ARP タイマー（ms）が追加されます。現在のデフォルト値は 1,000 ミリ秒です。設定可能な範囲は 1,000 ミリ秒から 18,000 ミリ秒です。ホスト ARP タイマーの設定は、管理ポートには適用されません。

2. 新しいサイトの基本設定を入力するか、デフォルトをそのまま使用します。ゲートウェイや One-ARM などの Citrix SD-WAN 展開では、ARP 要求を頻繁に受信すると、トラフィックフローに影響するアクセスポイントが過負荷になります。ARP タイマーを設定して、特定のインターバル時間で ARP 要求を送信できるようになりました。時間間隔は秒単位で設定されます。ARP の間隔は、Citrix SD-WAN アプライアンス GUI の［基本設定］タブでデータセンターサイトを構成するときに設定できます。

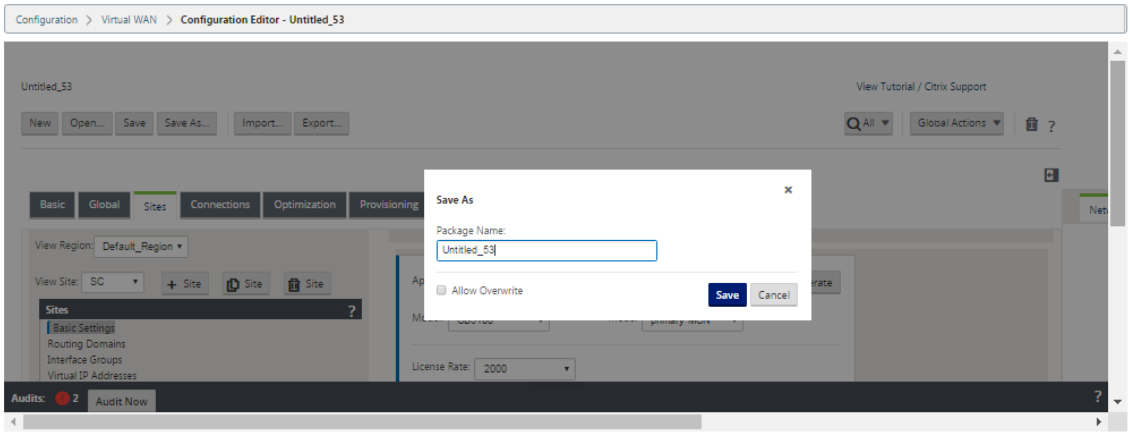
3. （オプション、推奨）進行中の構成を保存します。

1 つのセッションで設定を完了できない場合は、いつでも保存できるため、後で再び設定を完了できます。構成は、ローカルアプライアンスの Workspace に保存されます。保存した構成での作業を再開するには、構成エディタの メニューバー（ページ上部）の「開く」をクリックします。これにより、変更する構成を選択するためのダイアログボックスが表示されます。

> 注
>
> 余分な予防策として、間違った構成パッケージを上書きしないように、[保存] ではなく [名前を付けて保存] を使用することをお勧めします。

現在の構成パッケージを保存するには、次の手順を実行します。

1. ［名前を付けて保存］をクリックします（[構成エディタ］の中央ペインの上部にある)。[名前を付けて保存] ダイアログボックスが表示されます。



2. 構成パッケージ名を入力します。構成を既存のパッケージに保存する場合は、保存する前に [上書きを許可] を選択してください。
3. ［保存］をクリックします。

MCN のインターフェイスグループの設定方法

新しい MCN サイトを追加した後、次の手順では、サイトの仮想インターフェイスグループを作成して設定します。

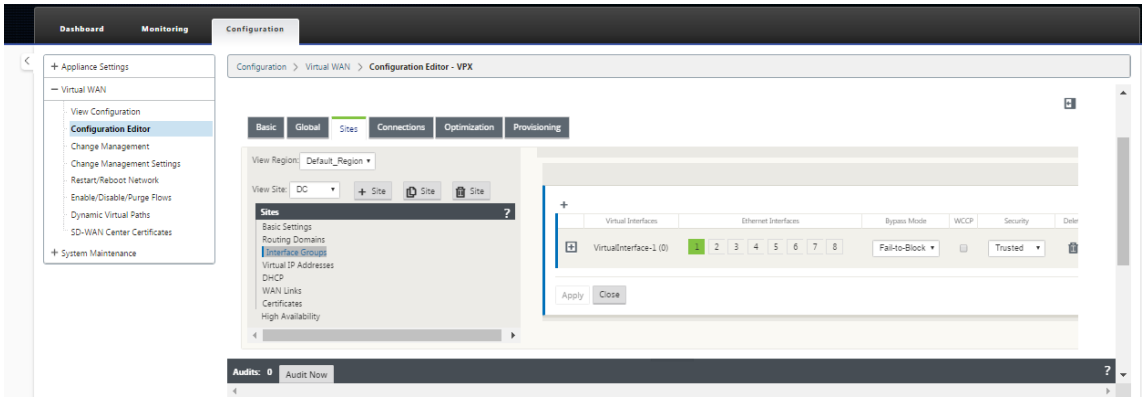
次に、仮想インターフェイスグループの設定に関する注意事項をいくつか示します。

- グループに最も適した論理名を使用します。
- 信頼できるネットワークは、ファイアウォールの背後に保護されるネットワークです。
- 仮想インターフェイスは、インターフェイスを Fail to Wire (FTW) ペアに関連付けます。
- 単一の WAN インターフェイスを FTW ペアにすることはできません。

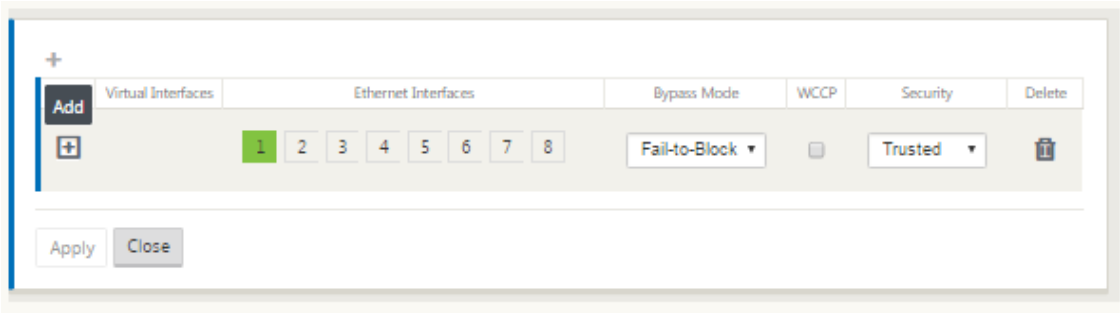
> 注
>
> 仮想インターフェイスグループの設定に関する注意事項および詳細については、「仮想ルーティングおよび転送」の項を参照してください。

新しい MCN サイトに仮想インターフェイスグループを追加するには、次の手順を実行します。

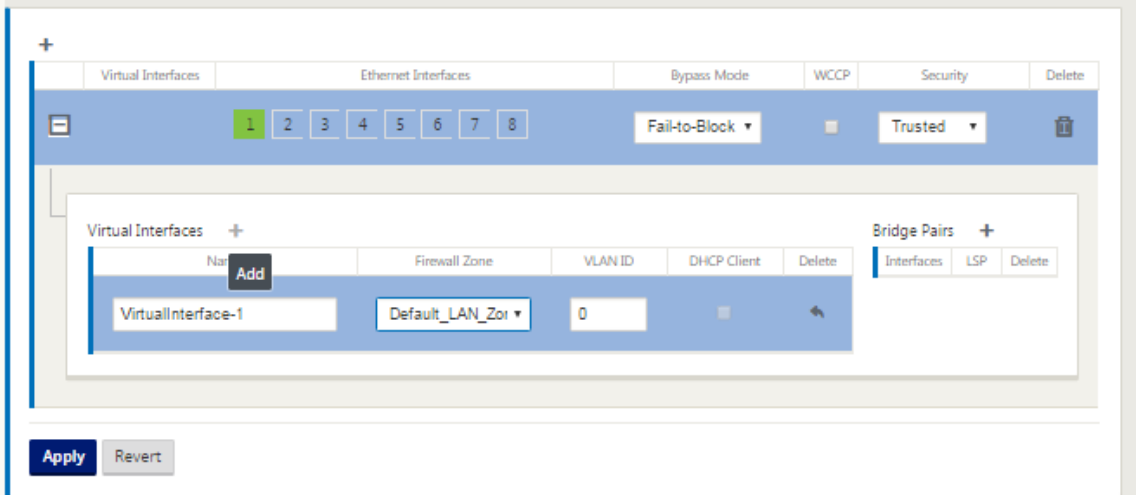
1. 構成エディタの［サイト］ビューで、［サイトの 表示］ドロップダウンメニューからサイト を選択します。これにより、選択したサイトの構成ビューが開きます。



2. [**+**] をクリックして、仮想インターフェイスグループを追加します。これにより、新しい空の Virtual インターフェイスグループエントリがテーブルに追加され、編集用に開きます。



3. [仮想インターフェイス] の右側にある [**+**] をクリックします。これにより、新しい空のグループエントリがテーブルに追加され、編集用に開きます。

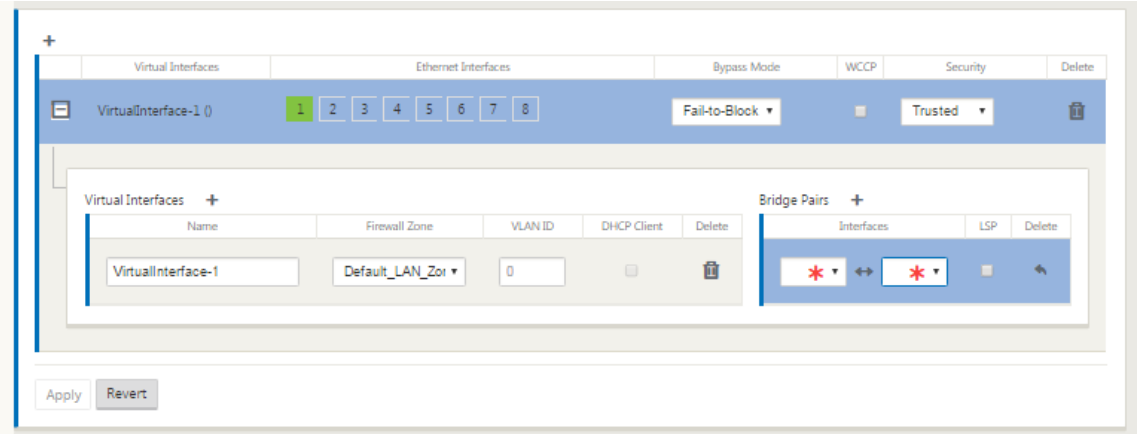


4. グループに含める イーサネットインターフェイスを 選択します。[**Ethernet Interf**aces] で、そのインターフェイスを含める/除外するインターフェイスをクリックします。グループに含めるインターフェイスはいくつでも選択できます。

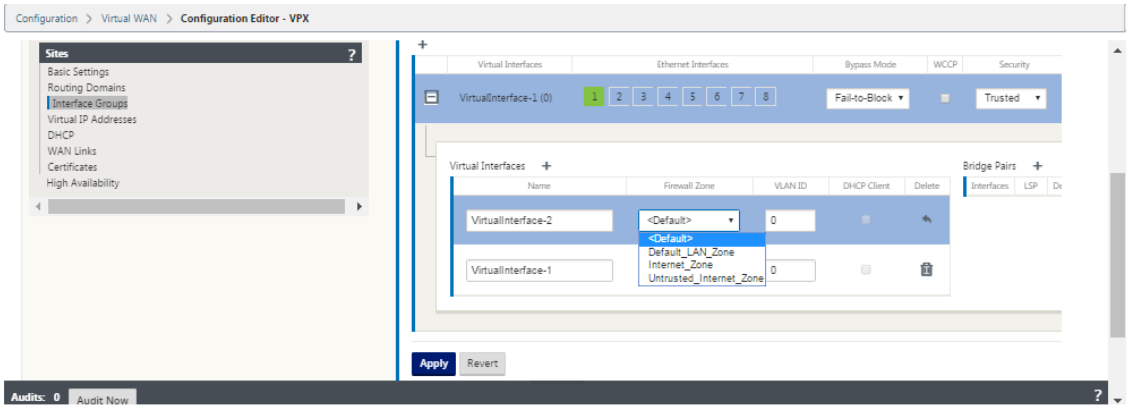
5. ドロップダウンメニューから [バイパスモード] を選択します（デフォルトなし）。バイパスモード は、アプライアンスまたはサービスの障害または再起動が発生した場合に、仮想インターフェイスグループ内のブリッジペアインターフェイスの動作を指定します。オプションは、[配線失敗] または [ブロック失敗] です。

6. ドロップダウンメニューから [セキュリティレベル] を選択します。仮想インターフェイスグループのネットワークセグメントのセキュリティレベルを指定します。オプションは、[信頼済み] または [信頼できない] です。信頼できるセグメントはファイアウォールで保護されます（デフォルトは Trusted です）。

7. 追加した仮想インターフェイスの左端にある [**+**] をクリックします。[仮想インターフェイス] テーブルが表示されます。



8. [仮想インターフェイス] の右側にある [**+**] をクリックします。これにより、名前、ファイアウォールゾーン、**VLAN ID ID** が表示されます。



9. この仮想インターフェイスグループ の名前 と **VLAN ID** を入力します。

- **Name** —この仮想インターフェイスが参照される名前です。
- ファイアウォールゾーン -ドロップダウンメニューからファイアウォールゾーンを選択します。
- **VLAN ID**： これは、仮想インターフェイスとの間で送受信されるトラフィックを識別およびマーキングするための ID です。ネイティブ/タグなしトラフィックには、0（ゼロ）の ID を使用します。

10. [ブリッジペア] の右側にある [**+**] をクリックします。これにより、新しい **Bridge Pairs** エントリが追加され、編集用に開きます。
11. ペアリングするイーサネットインターフェイスをドロップダウンメニューから選択します。さらにペアを追加するには、[ブリッジペア] の横にある [**+**] をもう一度クリックします。
12. ［適用］をクリックします。これにより、設定が適用され、新しい仮想インターフェイスグループがテーブルに追加されます。この段階では、新しい仮想インターフェイスグループエントリの右側に、黄色の Delta Audit Alert アイコンが表示されます。これは、サイトの仮想 IP アドレス (VIP) をまだ構成していないためです。現時点では、このアラートは、サイトの仮想 IP を正しく構成すると自動的に解決されるため、無視できます。
13. さらに仮想インターフェイスグループを追加するには、[Interface Group **s**] ブランチの右側にある [**+**] をクリックし、上記の手順に進みます。

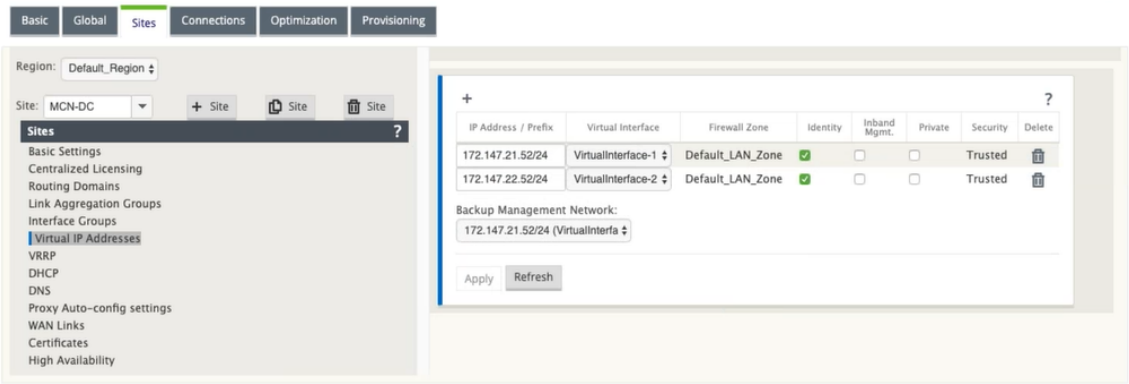
MCN の仮想 **IP** アドレスを設定する方法

次の手順では、サイトの仮想 IP アドレスを構成し、適切なグループに割り当てます。

1. 新しい MCN サイト の [サイト] ビューで、[仮想 **IP** アドレス] の左にある [**+**] をクリックします。これにより、新しいサイトの 仮想 **IP** アドレス テーブルが表示されます。
2. [仮想 **IP** アドレス] の右側にある [**+**] をクリックして、アドレスを追加します。これにより、新しい仮想 IP アドレスを追加および構成するためのフォームが開きます。
3. **IP** アドレス / プレフィクス 情報を入力し、アドレスが関連付けられている 仮想インターフェイスを 選択します。仮想 IP アドレスには、完全なホストアドレスとネットマスクを含める必要があります。
4. [ファイアウォールゾーン]、[ID]、[プライベート]、[セキュリティ] など、仮想 IP アドレスの設定を選択します。
5. [**Inband Mgmt**] を選択すると、仮想 IP アドレスが Web UI や SSH などの管理サービスに接続できるようになります。

   > 注:
   >
   > インターフェイスは、セキュリティタイプ「信頼済み」および「**ID** 」が有効である必要があります。

6. バックアップ管理ネットワークとして仮想 IP を選択します。これにより、管理ポートにデフォルト Gateway が設定されていない場合に、管理に仮想 IP アドレスを使用できます。

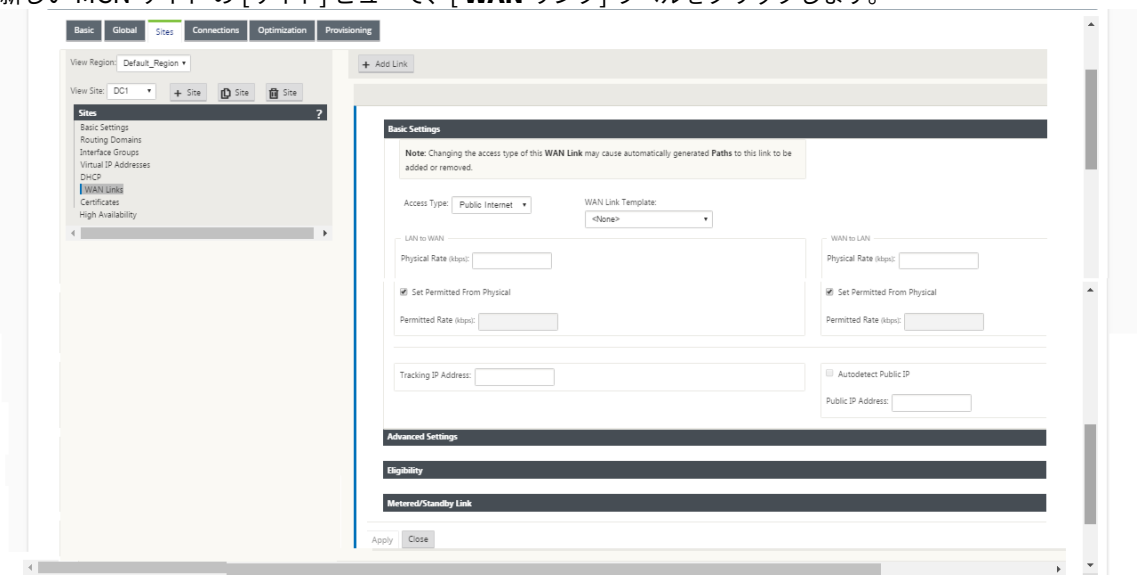


7. [適用] をクリックします。これにより、アドレス情報がサイトに追加され、サイトの 仮想 **IP** アドレス テーブルに含められます。
8. さらに仮想 IP アドレスを追加するには、[仮想 **IP** アドレス] の右側にある [**+**] をクリックし、上記の手順を実行します。

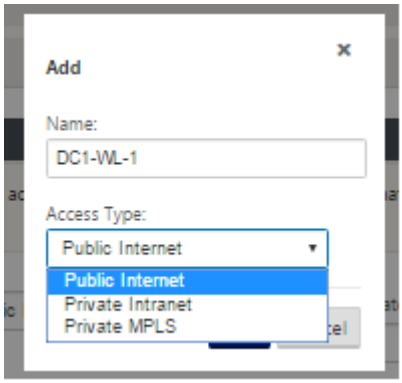
MCN の **WAN** リンクの設定方法

次のステップでは、サイトの WAN リンクを構成します。

1. 新しい MCN サイト の [サイト] ビューで、[**WAN** リンク] ラベルをクリックします。



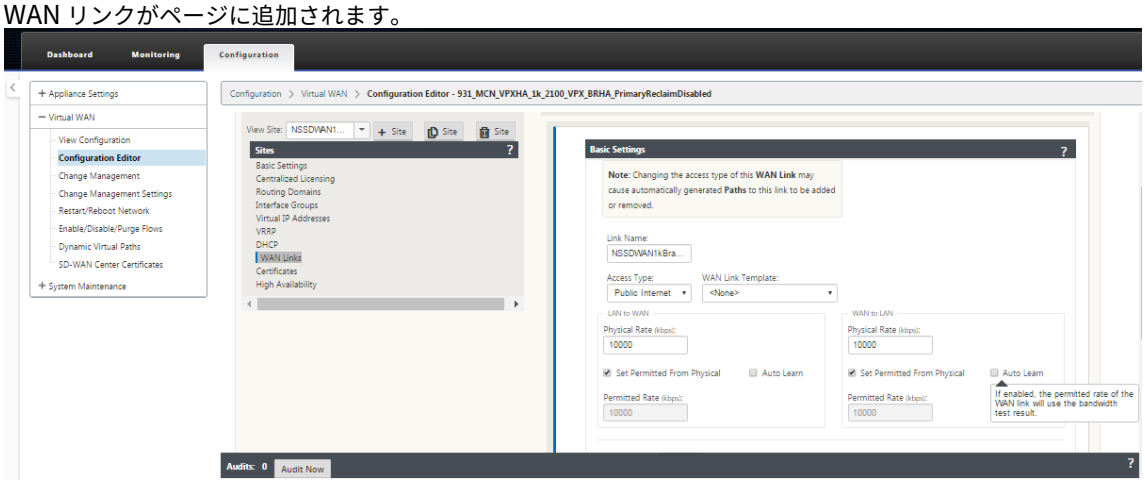
2. [**W** AN リンク] の右側にある [Add Link] をクリックして、新しい WAN リンクを追加します。[追加] ダイアログボックスが表示されます。



3. （オプション）デフォルトを使用しない場合は、WAN リンクの名前を入力します。デフォルトはサイト名で、次のサフィックス「WL-」が付加されます。<number> ここで、<number> はこのサイトの WAN リンクの数を 1 ずつ増やします。

4. ドロップダウンメニューから「アクセスタイプ」を選択します。オプションは、[パブリックインターネット**]**、**[**プライベートイントラネット**]**、または [プライベート **MPLS]** です。

5. ［追加］をクリックします。これにより、[**WAN** リンク の基本設定] 設定ページが表示され、新しい未設定の WAN リンクがページに追加されます。

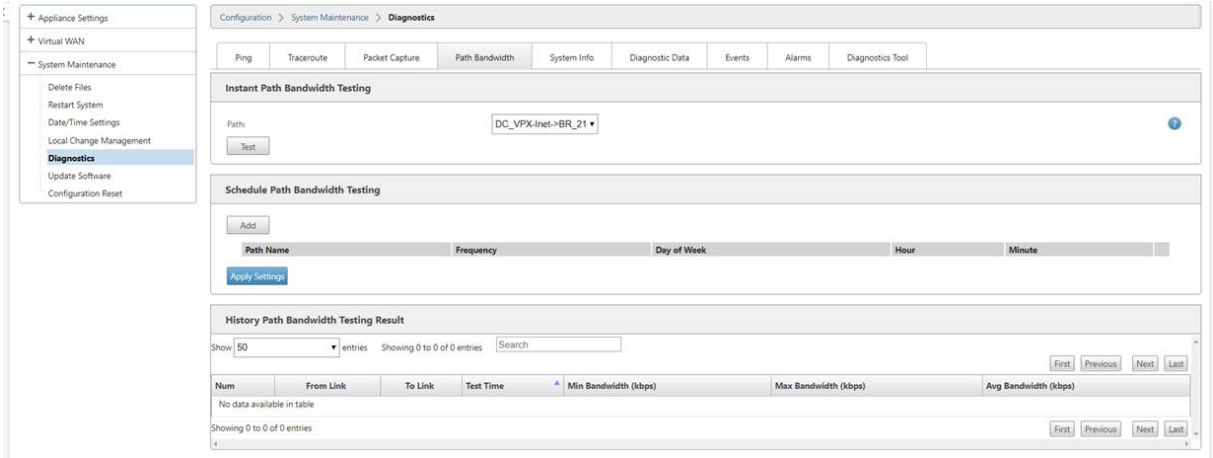


帯域幅消費の自動学習

自動学習は、システムの起動時に実行され、正常な結果が観察されるまで 5 分ごとに繰り返されます。自動学習は、設定エディタから WAN リンク設定の変更が行われた後にも実行されます。

テストは手動で実行することも、SD-WAN GUI でスケジュールすることもできます。テストが成功し、自動学習が有効になっている場合、これらのテストの結果は、許可されたレートにも適用されます。

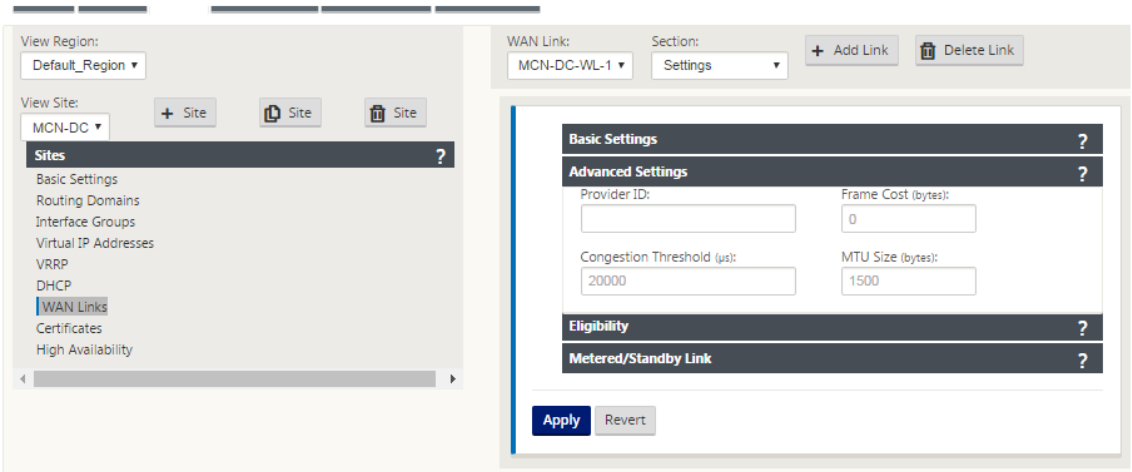
大規模なネットワークで自動学習を使用する場合、config change が再起動すると、すべてのサイトが MCN で同時にテストを実行し、帯域幅の使用率が高くなり、結果が不正確になります。帯域幅テストは、1 日 1 ～2 回（通常はトラフィック量が少ない場合）にスケジュールすることをお勧めします。



1. 新しい WAN リンクのリンクの詳細を入力します。LAN から WAN、WAN から **LAN** への設定を構成します。いくつかのガイドラインは次のとおりです。

   - 一部のインターネットリンクは非対称である場合があります。
   - 許可された速度を誤って設定すると、そのリンクのパフォーマンスに悪影響を及ぼす可能性があります。
   - 認定レートを超えるバースト速度は使用しないでください。
   - インターネット WAN リンクの場合は、必ずパブリック IP アドレスを追加してください。

2. グレーの [詳細設定] セクションバーをクリックします。リンクの [詳細設定] フォームが開きます。

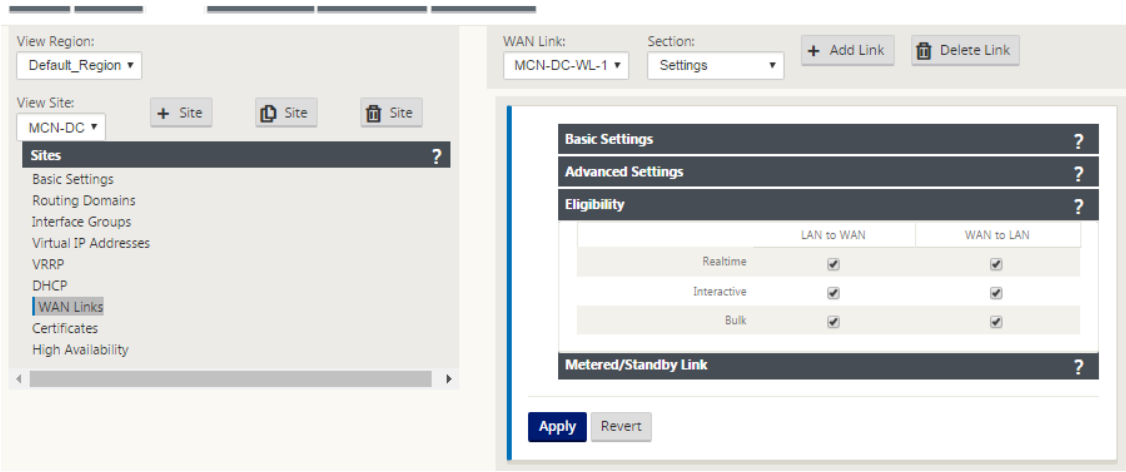


3. リンクの **[**詳細設定**]** を入力します。

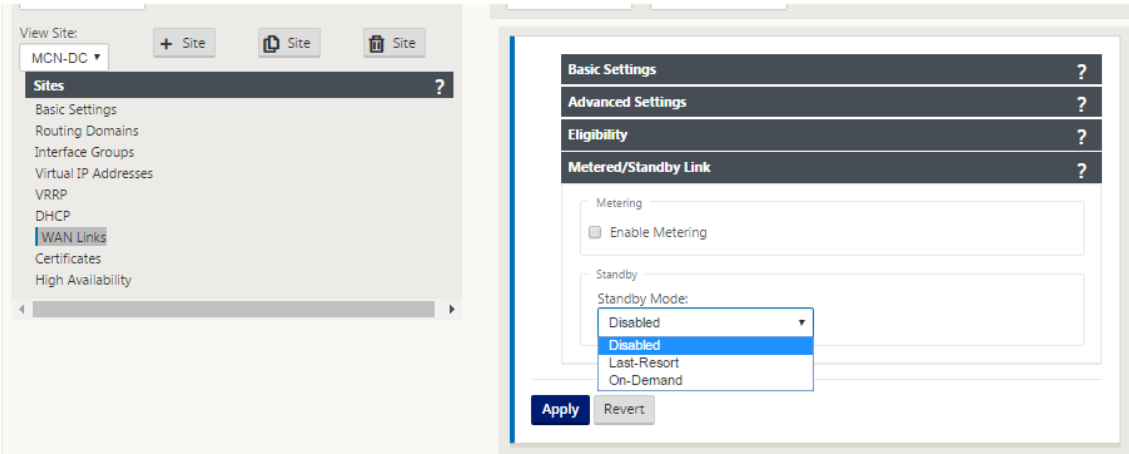
   - [Prov **ider ID**]:（オプション）同じサービスプロバイダーに接続されている WAN リンクを指定するための一意の ID 番号 1 ～100 を入力します。仮想 WAN は、重複パケットを送信するときにプロバイダー ID を使用してパスを区別します。
   - [Frame C **ost (bytes)**]: 各パケットに追加するヘッダー/トレーラのサイズ（バイト単位）を入力します。たとえば、追加されたイーサネット IPG または AAL5 トレーラーのバイト単位のサイズ。
   - 輻輳 しきい値: 輻輳しきい値（マイクロ秒単位）を入力します。このしきい値は、WAN リンクがパケット転送を抑制し、それ以上の輻輳を回避します。

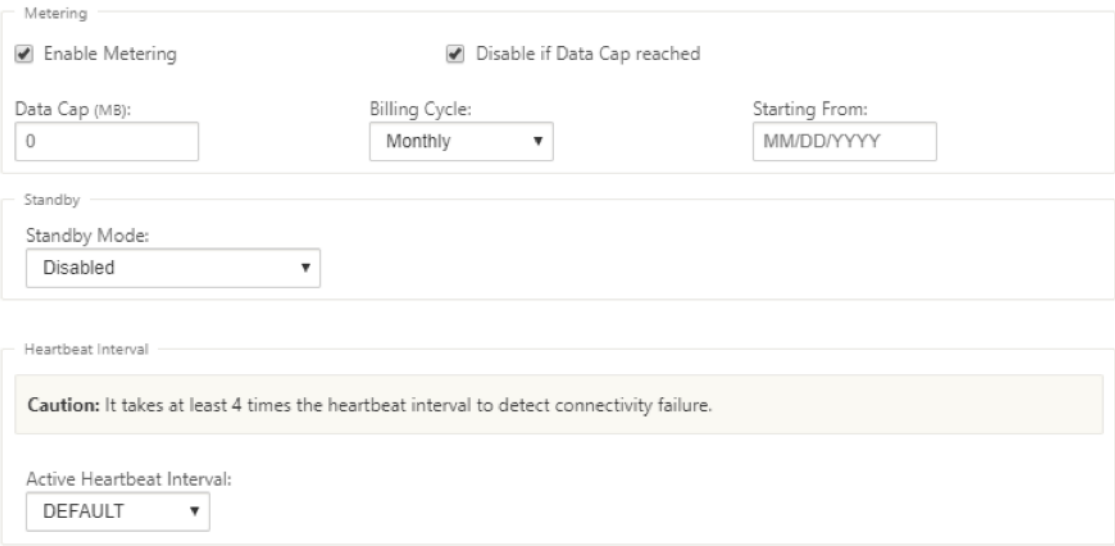
- [MTU **Size (bytes)**]: フレームコストを含まない、最大の raw パケットサイズ（バイト単位）を入力します。

4. グレーの「適格」セクション・バーをクリックします。リンクの [適格 設定] フォームが開きます。
5. リンクの「適格」設定を選択します。



6. グレーの [従量制課金リンク] セクションバーをクリックします。リンクの [従量制課金リンク 設定] フォームが開きます。
7. （オプション）このリンクの メータリング を有効にするには、[メータリングを有効にする] を選択します。これにより、[メータリング設定を有効にする] フィールドが表示されます。





8. リンクのメータリング設定を構成します。以下のコマンドを実行します。

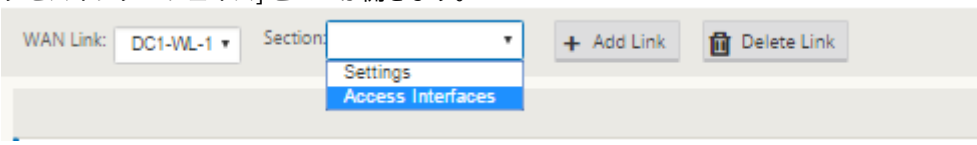
- 「データ上 限 **(MB)** 」—リンクに対するデータ上限割り当てをメガバイト単位で入力します。
- 「請求 サイクル」—ドロップダウンメニューから「月次」または「週次」を選択します。
- 開始日—請求サイクルの開始日を入力します。
- 「Set **Last Resort** 」—他のすべての使用可能なリンクに障害が発生した場合に、このリンクを最後の手段のリンクとして有効にする場合に選択します。通常の WAN 条件下では、仮想 WAN は、リンクステータスを確認するために、従量制課金リンクを介して最小限のトラフィックだけを送信します。ただし、障害が発生した場合、SD-WAN は本番トラフィックを転送するための最後の手段として、アクティブな従量制課金リンクを使用できます。

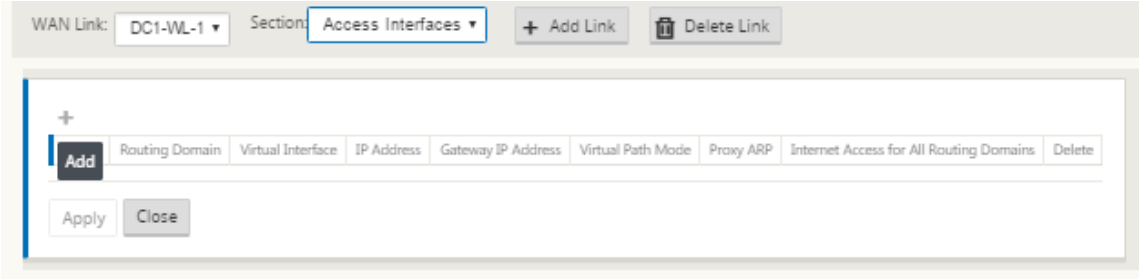
［適用］をクリックします。これにより、指定した設定が新しい WAN リンクに適用されます。

次のステップでは、新しい WAN リンクのアクセスインターフェイスを設定します。アクセスインターフェイスは、特定の WAN リンクのインターフェイスとしてまとめて定義された、仮想インターフェイス、WAN エンドポイント IP アドレス、ゲートウェイ IP アドレス、および仮想パスモードで構成されます。各 WAN リンクには、少なくとも 1 つのアクセスインターフェイスが必要です。

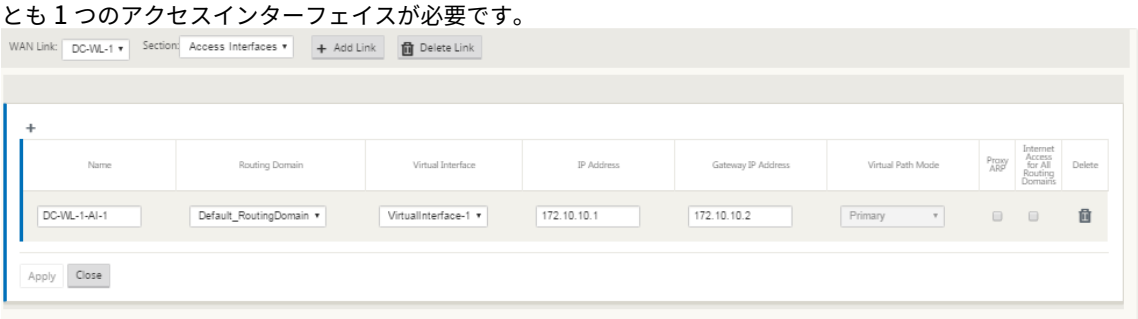
アクセスインターフェイスの設定方法

1. リンクの [WAN リンク] 設定ページで [アクセスインターフェイス] を選択します。これにより、サイトの [アクセスインターフェイス] ビューが開きます。





2. [**+**] をクリックして、インターフェイスを追加します。これにより、テーブルに空白のエントリが追加され、編集用に開かれます。リンクの [アクセスインターフェイス] 設定を入力します。各 WAN リンクには、少なくとも 1 つのアクセスインターフェイスが必要です。



3. 以下のコマンドを実行します。

- [Name]: このアクセスインターフェイスが参照される名前です。新しいアクセスインターフェイスの名前を入力するか、デフォルトをそのまま使用します。デフォルトでは、WAN_Link_name-AI-number: という命名規則が使用されます。W *AN_link_* name はこのインターフェイスに関連付ける WAN リンクの名前で、number はこのリンクに現在設定されているアクセスインターフェイスの数を 1 ずつ増やしたものです。

> 注
>
> 名前が切り捨てられた場合は、フィールドにカーソルを置き、クリックしたままマウスを右または左に回転すると、切り捨てられた部分が表示されます。

- 仮想インターフェイス: このアクセスインターフェイスが使用する仮想インターフェイスです。このブランチサイト用に構成された Virtual Interfaces のドロップダウンメニューからエントリを選択します。
- ルーティングドメイン -アクセスインターフェイス用に選択するルーティングドメイン。
- **IP** アドレス—アプライアンスから WAN へのアクセスインターフェイスエンドポイントの IP アドレスです。
- **Gateway IP** アドレス—ゲートウェイルータの IP アドレスです。
- **Virtual Path Mode**： この WAN リンク上の仮想パストラフィックのプライオリティを指定します。オプションは、[プライマリ]、[セカンダリ]、または [除外] です。[除外] に設定すると、このアクセスインターフェイスはインターネットおよびイントラネットトラフィックにのみ使用されます。
- 「プロキシ **ARP** 」—有効にするチェックボックスを選択します。有効にすると、Gateway に到達できない場合に、仮想 WAN アプライアンスはゲートウェイ IP アドレスの ARP 要求に応答します。

1. ［適用］をクリックします。

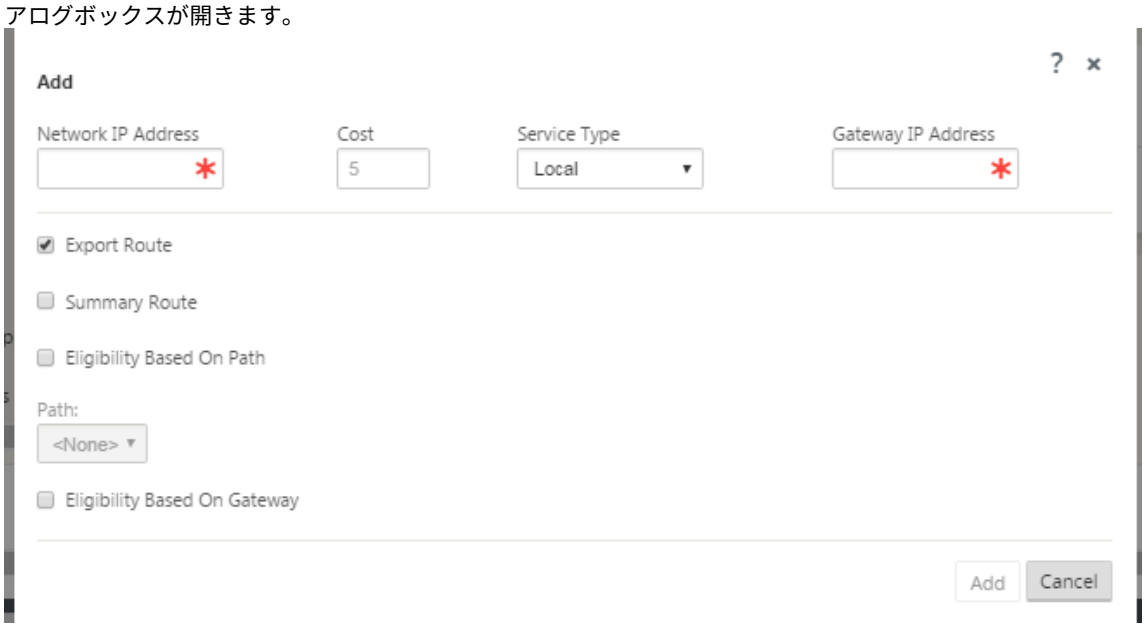
これで、新しい WAN リンクの設定が完了しました。これらの手順を繰り返して、サイトの WAN リンクを追加および構成します。

次のステップでは、サイトのルートを追加および構成します。

MCN のルートを設定する方法

サイトのルートを追加および構成するには、次の手順を実行します。

1. 新しい MCN サイトの [接続] ビューをクリックし、[ルート] を選択します。これにより、サイトの [ルート] ビューが表示されます。
2. ルート を追加するには、[ルート] の右側にある [**+**] をクリックします。これにより、編集用の [ルート] ダイアログボックスが開きます。



3. 新しいルートのルート設定情報を入力します。以下のコマンドを実行します。

- 「ネットワーク **IP** アドレス」—ネットワーク **IP** アドレスを入力します。
- **Cost** —このルートのルートプライオリティを決定するために、1 ～15 の重みを入力します。低コストのルートは、高コストのルートよりも優先されます。デフォルト値は 5 です。
- [**Service Type**] —このフィールドのドロップダウンメニューからルートのサービスタイプを選択します。

使用できるオプションは、次のとおりです。

- 仮想パス—このサービスは、仮想パスを通過するトラフィックを管理します。仮想パスは、2 つの WAN リンク間の論理リンクです。これは、2 つの SD-WAN ノード間で高いサービス・レベル通信を提供するために結合された WAN パスの集合で構成されます。これは、変化するアプリケーションの需要と WAN の状態に常に測定し、適応することによって達成されます。SD-WAN アプライアンスは、パス単位でネットワークを測定

します。仮想パスは、スタティック（常に存在）またはダイナミック（2 つの SD-WAN アプライアンス間のトラフィックが設定されたしきい値に達した場合のみ存在）のいずれかになります。

- インターネット—このサービスは、エンタープライズサイトとパブリックインターネット上のサイト間のトラフィックを管理します。このタイプのトラフィックはカプセル化されません。輻輳時には、SD-WAN は、仮想パスに対するレート制限によるインターネットトラフィックと、管理者が確立した SD-WAN 構成に従ってイントラネットトラフィックによって、帯域幅を積極的に管理します。
- イントラネット—このサービスは、仮想パス経由の送信用に定義されていないエンタープライズイントラネットトラフィックを管理します。インターネットトラフィックと同様に、カプセル化されていないままであり、SD-WAN は、輻輳時にこのトラフィックを他のサービスタイプと比較してレート制限することで、帯域幅を管理します。特定の条件下では、仮想パスでイントラネットフォールバック用に構成されている場合、通常は仮想パスで移動するトラフィックは、ネットワークの信頼性を維持するために、代わりにイントラネットトラフィックとして扱われることがあります。
- パススルー—このサービスは、仮想 WAN を通過するトラフィックを管理します。パススルーサービスに送信されるトラフィックには、ブロードキャスト、ARP、その他の非 IPv4 トラフィック、および Virtual WAN アプライアンスのローカルサブネット、構成済みサブネット、またはネットワーク管理者が適用したルール上のトラフィックが含まれます。このトラフィックは、SD-WAN によって遅延、シェーピング、または変更されません。したがって、SD-WAN アプライアンスが他のサービスで使用するように構成されている WAN リンク上で、パススルートラフィックが実質的なリソースを消費しないようにする必要があります。
- ローカル：このサービスは、他のサービスと一致しないサイトへのローカルな IP トラフィックを管理します。SD-WAN は、ローカルルートを送信元および宛先とするトラフィックを無視します。
- **GRE** トンネル：このサービスは、GRE トンネル宛ての IP トラフィックを管理し、サイトで設定された LAN GRE トンネルと一致します。GRE トンネル機能を使用すると、LAN 上の GRE トンネルを終了するように SD-WAN アプライアンスを設定できます。サービスタイプ GRE Tunnel のルートの場合、Gateway はローカル GRE トンネルのトンネルサブネットの 1 つに存在する必要があります。
- **LAN IPsec** トンネル—このサービスは、IPsec トンネル宛の IP トラフィックを管理します。
- 「ゲートウェイ **IP** アドレス」—このルートの ゲートウェイ **IP** アドレスを 入力します。
- 適格性 -パスに基づく（チェックボックス）：（オプション）有効の場合、選択したパスがダウンしているときにルートはトラフィックを受信しません。
- 「パス」(Path) —ルートの適格性を判断するために使用するパスを指定します。

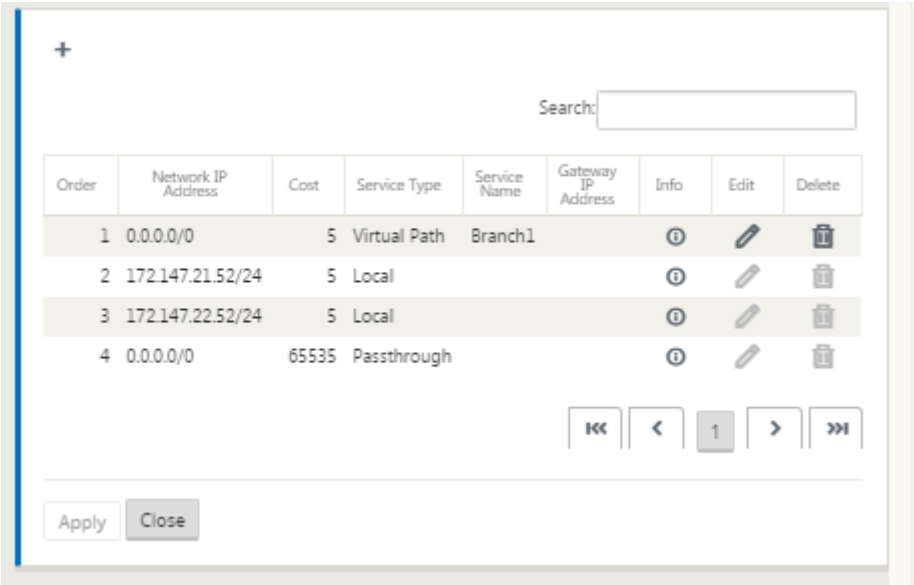
「サービスタイプ」に応じて、次の設定が表示されます。

サービスの種類	サービスタイプ設定
仮想パス	[Next Hop Site]：仮想パスパケットの送信先となるリモートサイトを示します。
インターネット	ルートのエクスポート: ルートを他の接続されたサイトにエクスポートするには、有効/無効にします。パスに基づく適格性
イントラネット	エクスポートルート、イントラネットサービス、パスに基づく適格性、トンネルに基づく適格性

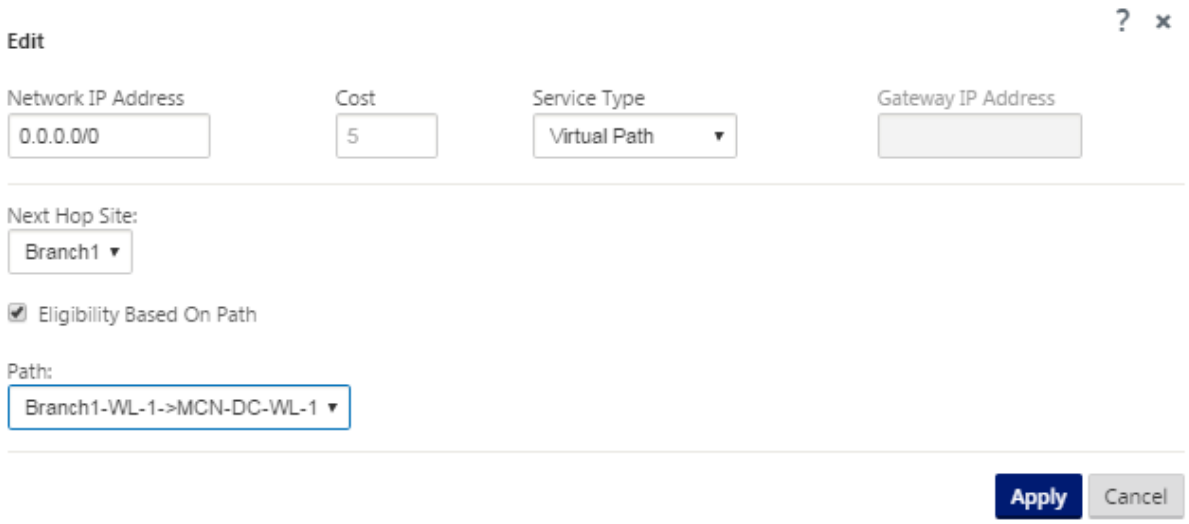
サービスの種類	サービスタイプ設定
パススルー	パスに基づく適格性
ローカル	エクスポートルート、サマリールート、パスに基づく適格性
GRE トンネル	エクスポートルート、パスに基づく適格性、ゲートウェイに基づく適格性
IPSec トンネル	エクスポートルート、パスに基づく適格性、IPSec トンネル、トンネルに基づく適格性
破棄	エクスポートルート、サマリールート

1. ［適用］をクリックします。

> 注
>
> [適用] をクリックすると、追加のアクションが必要であることを示す監査警告が表示されることがあります。赤い点または金色のデルタアイコンは、表示されるセクションにエラーを示します。これらの警告を使用して、エラーや不足している構成情報を識別できます。監査警告アイコンの上にカーソルを置くと、そのセクションのエラーの簡単な説明が表示されます。暗いグレーの 監査 ステータスバー (ページ下部) をクリックして、すべての監査警告の一覧を表示することもできます。



設定済みのルートを次のように編集することもできます。



サイトのルートを追加するには、**[ルート]** ブランチの右側にある **[**+**]** をクリックし、上記の手順を実行します。**

これで、新しい MCN サイトのプライマリ設定情報の入力が完了しました。次の 2 つのセクションでは、オプションの手順について説明します。

- MCN サイトの高可用性（HA）の設定（オプション）。
- 仮想 WAN セキュリティおよび暗号化の有効化と設定（オプション）。

これらの機能を今すぐ設定したくない場合は、[MCN サイト設定の命名、保存、およびバックアップ] に進みます。(/en-us/citrix-sd-wan/11/configuration/set-up-master-control-node/manage-mcn-configuration.html)

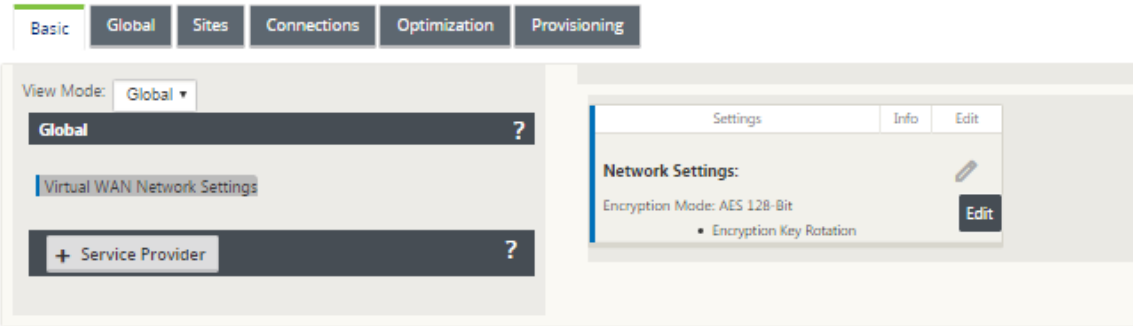
仮想 **WAN** セキュリティと暗号化の有効化と構成 **(**オプション**)**

May 10, 2021

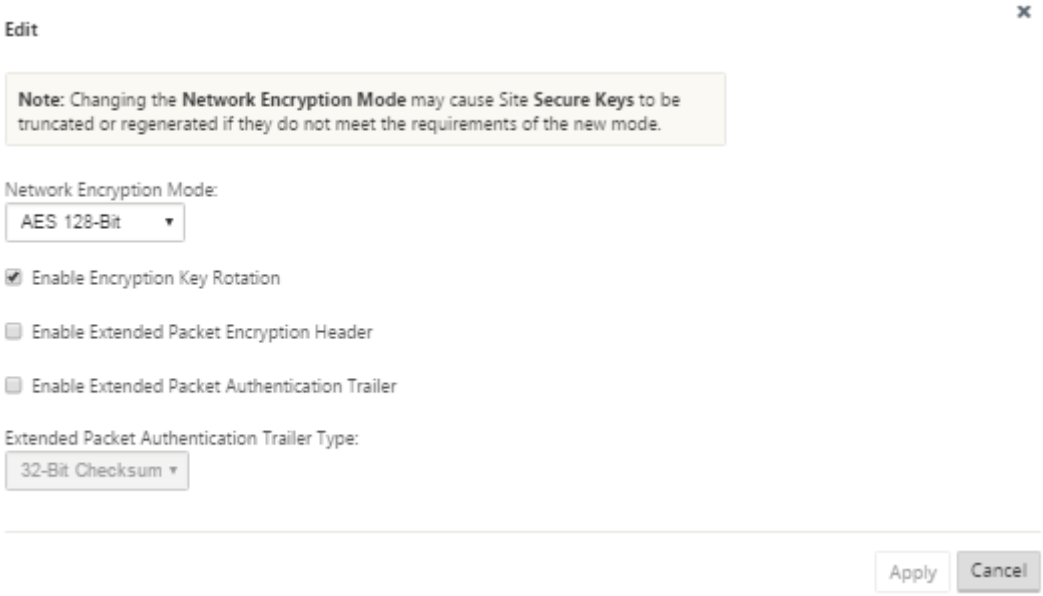
仮想 WAN のセキュリティと暗号化を有効にして構成するには、次の手順を実行します。

> 注
>
> 仮想 WAN セキュリティと暗号化の有効化はオプションです。

1. 構成エディタ の「基本」タブに移動し、「表示 モードから グローバル」を選択します。[仮想ネットワーク設定] 構成フォームが表示されます。



2. [編集] (鉛筆アイコン) をクリックして、フォームの編集を有効にします。



3. グローバルセキュリティ設定を入力します。使用できるオプションは、次のとおりです。

   - ネットワーク暗号化モード—暗号化パスに使用される暗号化アルゴリズムです。ドロップダウンメニューから [AE **S 128** ビット**]** または **[AES **256** ビット **] のいずれかを選択します。
   - 暗号化キーのローテーションを有効にする：有効にすると、暗号化キーは 10 ～15 分間隔でローテーションされます。
   - **Enable Extended Packet Encryption Header**：有効にすると、暗号化トラフィックの先頭に 16 バイトの暗号化カウンタが付加され、初期化ベクトルとして機能し、パケット暗号化をランダム化します。
   - 拡張パケット認証トレーラーを有効にする：有効にすると、暗号化されたトラフィックの内容に認証コードが追加され、メッセージが変更されずに配信されることを確認します。
   - 拡張パケット認証トレーラタイプ: これは、パケットの内容を検証するために使用されるトレーラのタイプです。ドロップダウンメニューから [**32** ビットチェックサム] または [**SHA-256**] のいずれかを選択します。

4. [**Apply**] をクリックして、設定を構成に適用します。

これで、MCN サイトの構成は完了です。次のステップでは、次のセクションで説明するように、新しい MCN サイト設定に名前を付けて保存します（オプションですが、推奨）。

> 警告
>
> コンソールセッションがタイムアウトになったり、構成を保存する前に管理 Web Interface からログアウトした場合、保存されていない構成の変更はすべて失われます。その後、システムに再度ログインし、設定手順を最初から繰り返す必要があります。そのため、構成パッケージを頻繁に保存するか、構成内の重要なポイントに保存することをお勧めします。

セカンダリ **MCN** の設定

November 8, 2021

MCN 冗長性をサポートするために、サイトをセカンダリ MCN として設定できます。セカンダリ MCN は、プライマリ MCN の健全性を継続的に監視します。プライマリ MCN に障害が発生すると、セカンダリ MCN が MCN の役割を引き継ぎます。セカンダリ MCN を作成するには、[モード] オプションで新しいサイトを追加するときに、セカンダリ MCN を選択します。仮想インターフェイス、仮想 IP、WAN リンク、およびその他の設定を手動で設定できます。同様に、セカンダリ RCN を設定することもできます。

> 注
>
> セカンダリ MCN 設定と高可用性設定を混同しないでください。セカンダリ MCN 構成では、異なる地理的な場所にあるブランチ/クライアントサイトがセカンダリ MCN として構成され、ディザスタリカバリが可能になります。HA 構成では、フォールトトレランスを確保するために、2 つのアプライアンスを同じサブネットまたは地理的な場所で構成します。高可用性構成の構成については、「高可用性展開」を参照してください。

セカンダリ MCN のアプライアンスモデルは、使用状況、帯域幅要件、およびサポートされるサイト数に基づいて選択できます。

プライマリ MCN からセカンダリ MCN への切り替えは、プライマリ MCN が非アクティブ状態の 15 秒後に発生します。セカンダリ MCN のプライマリ再要求は設定できません。プライマリ再要求は、プライマリアプライアンスが再びオンになり、ホールドタイマーが期限切れになると、自動的に実行されます。

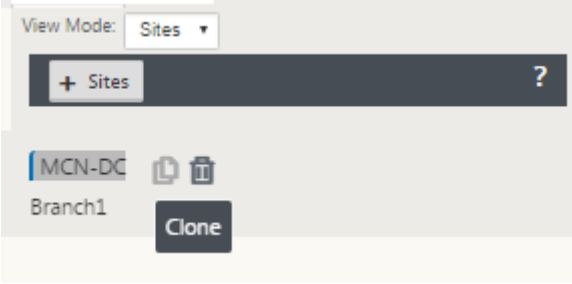
セカンダリ MCN を設定する最善の方法は、MCN 設定のほとんどを保持するため、既存の MCN のクローンを作成することです。サイトのクローンが作成されると、サイトの構成設定セット全体がコピーされ、単一のフォーム画面に表示されます。その後、要件に従って設定をすばやく簡単に変更できます。

> 注

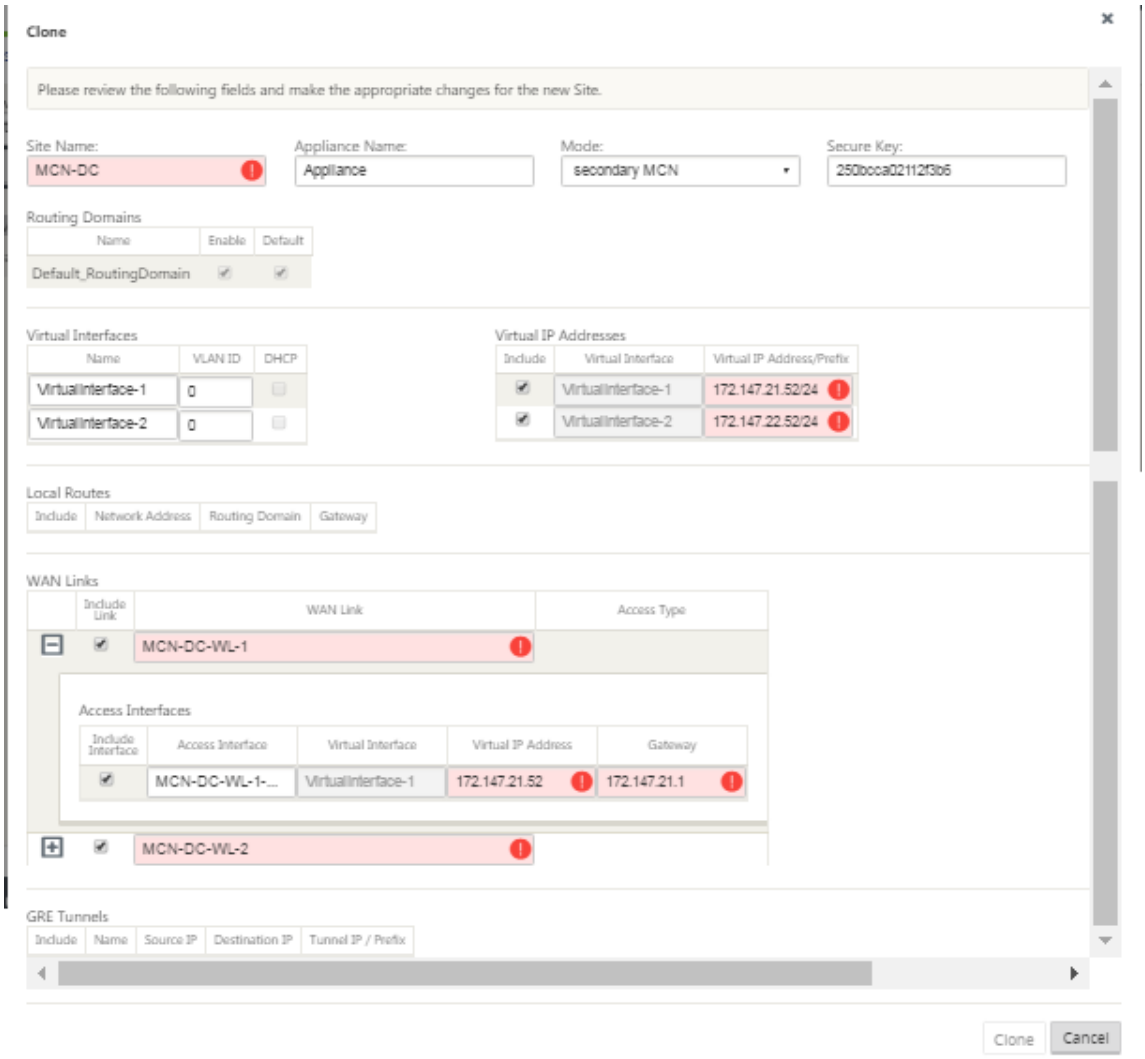
> MCN をクローンして、セカンダリ MCN またはブランチサイトを作成できます。設定できるセカンダリ MCN は 1 つだけです。

MCN サイトのクローンを作成し、セカンダリ **MCN** を作成するには

1. 構成エディタで、[基本] > [サイト] に移動し、 MCN サイトのクローンアイコンをクリックします。



2. 新しいサイトの構成パラメータ設定を入力します。



> 注:
>
> Audit Alert アイコン（赤いドット）が付いた強調表示されたフィールドは、現在の設定とは異なる値を持つ必要がある必須パラメータ設定を示します。

3. [モード] フィールドで、セカンダリ **MCN** を選択します。すべての監査アラートを解決します。
4. [クローン] をクリックして、セカンダリ MCN サイトを作成します。

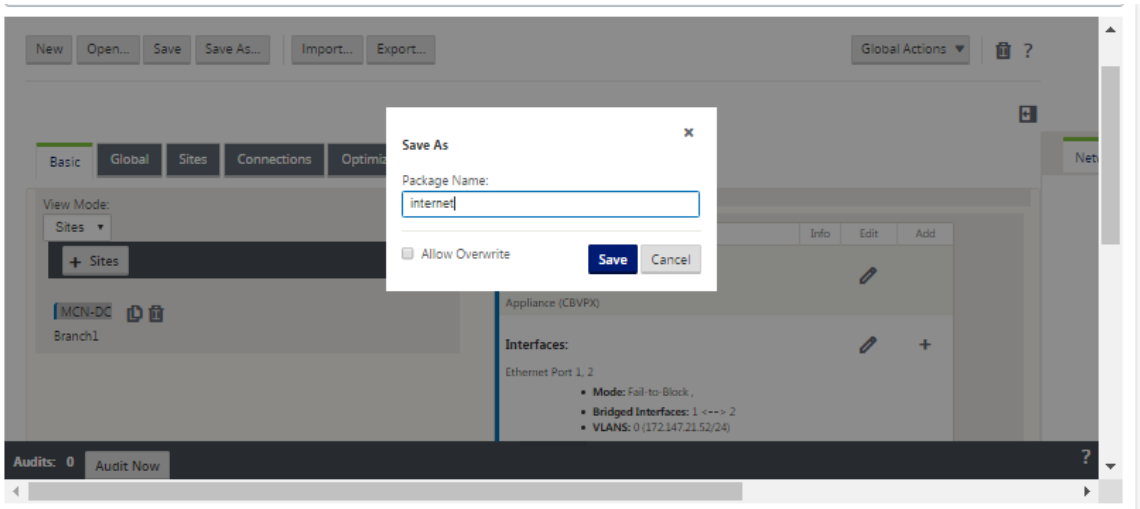
MCN 設定の管理

May 10, 2021

次のステップは、新しい設定に名前を付けて保存することです。これは、設定パッケージとしても見られます。このステップは、設定のこの時点ではオプションですが、推奨されています。構成パッケージは、ローカルアプライアンスの Workspace に保存されます。その後、管理 Web インターフェイスからログアウトし、後で構成プロセスを続行します。ただし、ログアウトした場合は、再開時に保存した設定を再度開く必要があります。保存した設定を開く手順を以下に示します。

> 警告
>
> Console セッションがタイムアウトになったり、構成を保存する前に Management Web Interface からログアウトした場合、保存されていない構成の変更はすべて失われます。システムに再度ログインし、最初から設定手順を繰り返す必要があります。そのため、構成パッケージを頻繁に保存するか、構成内の重要なポイントに保存することをお勧めします。
> ヒント:
>
> 追加の予防策として、誤った構成パッケージを上書きしないように、[保存] ではなく [名前を付けて保存] を使用することをお勧めします。

1. ［名前を付けて保存］をクリックします（［構成エディタ］の中央ペインの上部にある）。[名前を付けて保存] ダイアログボックスが表示されます。



2. 構成パッケージ名を入力します。

> 注
>
> 構成を既存の構成パッケージに保存する場合は、保存する前に [上書きを許可] を選択してください。

3. ［保存］をクリックします。

> 注
>
> 構成ファイルを保存したら、管理 Web Interface からログアウトして、後で構成プロセスを続行できます。ただし、ログアウトした場合は、再開時に保存した設定を再度開く必要があります。手順については、「保存した構成パッケージの構成エディタへのロード」の項を参照してください。

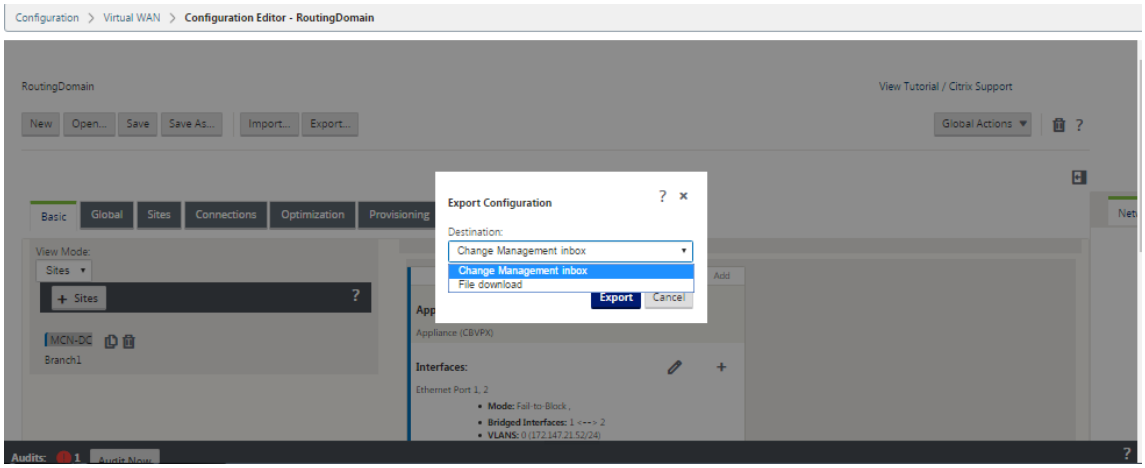
これで、MCN サイトの構成が完了し、新しい SD-WAN 構成パッケージが作成されました。これで、ブランチサイトを追加および構成する準備が整いました。手順については、セットアップブランチサイト] (/en-us/citrix-sd-wan/11/configuration/setup-branch-nodes.html) に記載されています。

構成パッケージのバックアップコピーのエクスポート

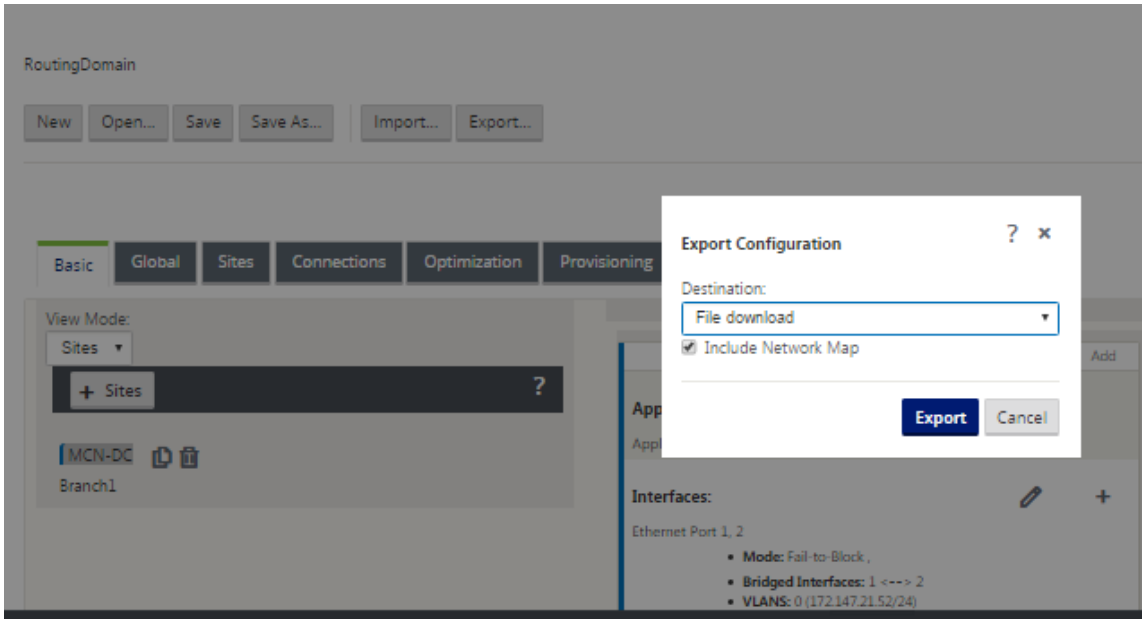
進行中の構成をアプライアンス Workspace に保存するだけでなく、定期的にローカル PC に構成をバックアップすることをお勧めします。

現在の構成パッケージを PC にエクスポートするには、次の手順を実行します。

1. ［エクスポート］をクリックします。[設定のエクスポート] ダイアログボックスが表示されます。



2. [宛先**:**] ドロップダウンメニューから [ファイル**] [**ダウンロード] を選択します。これにより、既定で選択されている [ネットワークマップを含める] オプションが表示されます。



3. デフォルトを受け入れ、[エクスポート] をクリックします。これには、構成パッケージに ネットワークマップ情報が含まれ、構成を保存する名前と場所を指定するためのファイルブラウザが開きます。

4. PC の保存場所に移動し、[保存] をクリックします。これにより、構成パッケージが PC に保存されます。

> 注
>
> バックアップされた構成パッケージを復元するには、**Import** 操作を使用して、PC からパッケージをインポートし、構成エディターにロードします。その後、インポートしたパッケージを管理 Web インターフェイス Workspace に保存して、将来使用できるようにすることができます。

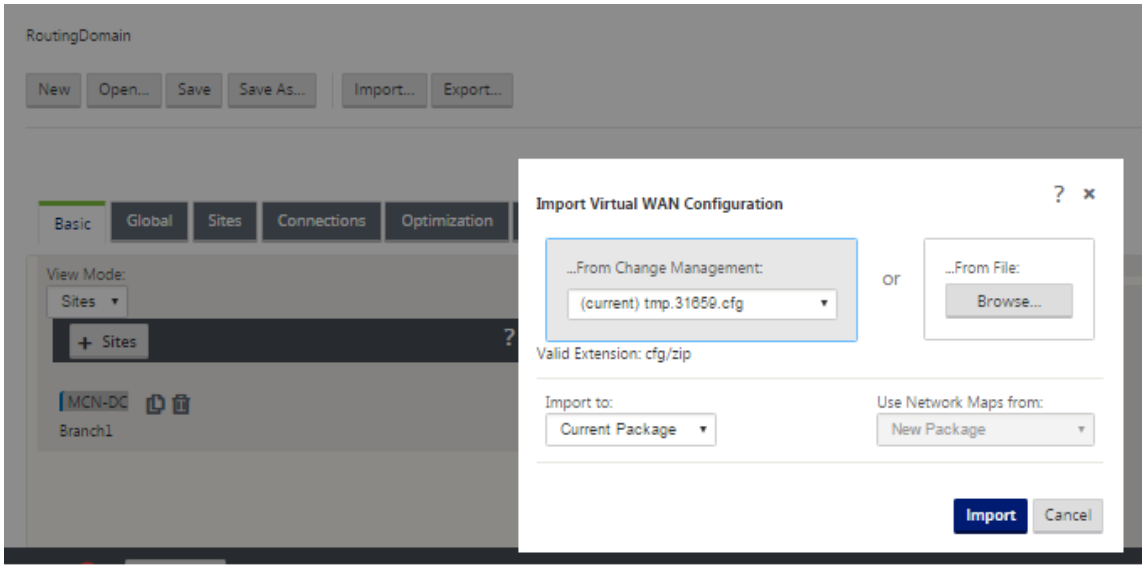
バックアップされた構成パッケージのインポート

場合によっては、以前のバージョンの構成パッケージに戻したいことがあります。以前のバージョンのコピーをローカル PC に保存した場合は、そのコピーを Configuration Editor にインポートし、編集用に開くことができます。これが初期展開でない場合は、現在の MCN のグローバル変更管理受信ボックスから既存の構成パッケージをインポートすることもできます。これらの両方の手順の手順を以下に示します。

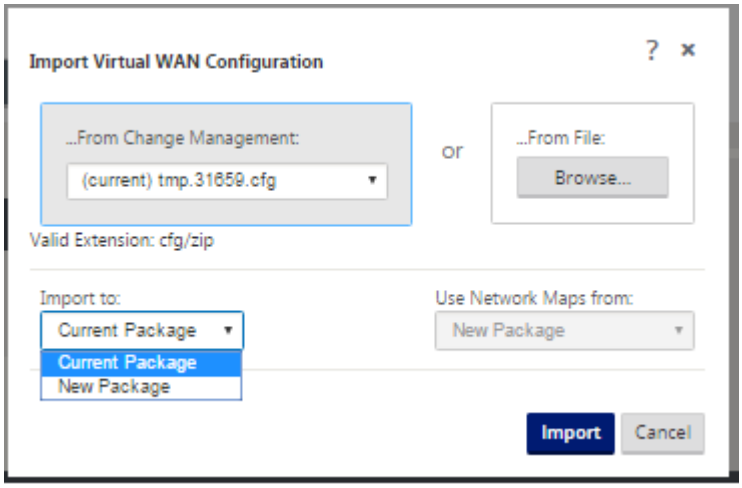
構成パッケージをインポートするには、次の手順を実行します。

1. 構成エディタを開きます。
2. 構成エディターの メニューバーで、「インポート」をクリックします。

   [仮想 **WAN** 構成のインポート] ダイアログボックスが表示されます。



3. パッケージのインポート元となる場所を選択します。
   - 変更管理から構成パッケージをインポートするには、「変更管理から」ドロップダウンメニュー（左上）から パッケージを選択します。
   - ローカル PC から構成パッケージをインポートするには、[参照] をクリックして、ローカル PC でファイルブラウザを開きます。ファイルを選択し、[**OK**] をクリックします。
4. インポート先を選択します (該当する場合)。構成パッケージがすでに 構成エディタで開いている場合は、「インポート先**:** 」ドロップダウンメニューが表示されます。



次のいずれかのオプションを選択します:

「現在のパッケージ」—現在開かれている構成パッケージの内容を、インポートされたパッケージの内容に置き換え、開かれているパッケージの名前を保持するには、これを選択します。ただし、変更されたパッケージを明示的に保存するまで、現在のパッケージの保存バージョンの内容は上書きされません。[名前を付けて保存] を使用してパッケージを保存する場合は、[上書きを許可] を選択して、前のバージョンの上書きを有効にします。

- 「新規パッケージ」(New Package) —新しい空白の構成パッケージを開き、インポートされたパッケージの内容をこのパッケージに移入するには、これを選択します。新しいパッケージには、インポートされたパッケージと同じ名前が自動的に付けられます。

5. 含めるネットワークマップを指定します（該当する場合)。構成パッケージが 構成エディタで既に開かれている場合は、[使用元ネットワークマップ**:**] ドロップダウンメニューを使用できます。

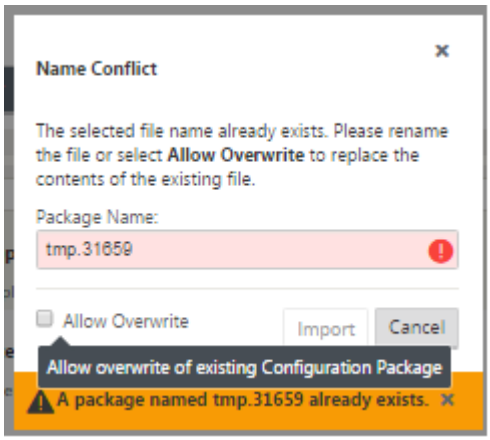
次のいずれかのオプションを選択します:

- [Current Package] —これで、パッケージに現在設定されているネットワークマップが Configuration Editor で利用可能になったままになり、インポートされたパッケージからネットワークマップはすべて破棄されます。
- [New Package] —現在開いているパッケージに現在設定されているネットワークマップが、インポートされたパッケージのネットワークマップ (存在する場合) に置き換えられます。

- Both **Packages** —現在のパッケージ とインポートされたパッケージの両方からすべてのネットワークマップが含まれます。

6. [インポート] をクリックします。インポートされたファイルは、仕様に従って 構成エディタにロードされます。

> 注
>
> Workspace に同じ名前のパッケージが存在する場合は、「名前の競合」(**Name Conflict**) ダイアログボックスが表示されます。



インポートしたパッケージに使用する名前を指定するには、次のいずれかの操作を行います。

- 「パッケージ名」**(Package Name)** フィールドに別の名前 を入力して、新しいパッケージの名前を変更し、「インポート」**(Import**) ボタンを有効にします。インポートされたパッケージは、指定された名前で 構成エディタ にロードされます。パッケージ名は Workspace に保存されますが、パッケージを明示的に保存するまで、パッケージの内容はワークスペースに保存されます。
- [**Allow Overwrite**] を選択して、既存の名前を保持し、保存したパッケージの内容の上書きを有効にすることを確認します。ただし、変更されたパッケージを明示的に保存するまで、現在のパッケージの保存バージョンの内容は上書きされません。

これにより、[名前の競合] ダイアログボックスの [インポート] ボタンも有効になります。[インポート] をクリックして、インポート操作を完了します。

保存された構成パッケージをロードする

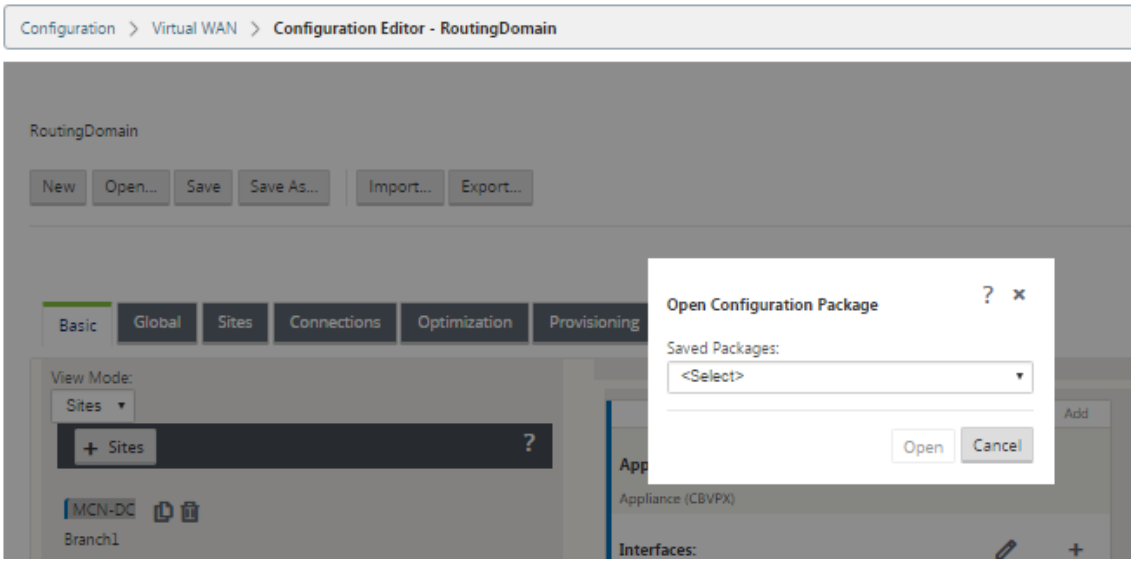
保存した構成パッケージの作業を再開するには、まずパッケージを開き、構成エディタにロードする必要があります。

保存した構成パッケージをロードするには、次の手順を実行します。

1. 管理 Web インターフェイスにログインし直して、構成エディタに移動します。これにより、新しいセッションの [構成エディター] のメインページが開きます。

管理 Web インターフェイスにログインし直した場合、構成エディタ は最初に新しいセッション用に開かれ、構成パッケージはロードされません。新しい構成を開始（新規）、保存された既存の構成を開く（開く）、またはインポート（インポート）してから、以前にローカル PC にバックアップした構成 を開く（開く）ことができます。

2. [開く] をクリックします。[構成パッケージを開く] ダイアログボックスが表示されます。



3.「保存されたパッケージ」ドロップダウンメニューから開くパッケージ を選択します。

> 注
>
> 構成エディタを開いた場合、Workspace に保存した構成の数によっては、「保存済みパッケージ」**(Saved Packages**) メニューが表示されるまでに数秒または 1、2 分かかる場合があります。その場合は、暫定的に [保存済みパッケージ] メニューフィールドに [保存済みパッケージなし] というメッセージが表示されることがあります。このような場合は、[キャンセル] をクリックしてダイアログボックスを閉じ、しばらく待ってから、もう一度 [開く] をクリックしてダイアログボックスを再度開きます。

4. [開く] をクリックします。

> 注
>
> これにより、指定した構成パッケージが開き、編集のために 構成エディタ にロードされます。これは、選択した構成をローカルアプライアンスにステージングしたりアクティブ化したりしません。

サイト名の変更

構成エディタで MCN サイトの名前を変更する場合は、サイトの名前を変更した設定を MCN および SD-WAN ネットワークに適用する必要があります。MCN の役割と、高可用性が有効か無効かによって、サイト名を変更するときの SD-WAN ネットワーク設定には次のシナリオが適用されます。

- MCN
- 高可用性の MCN
- GEO
- 高可用性の GEO
- RCN
- 高可用性を備えた RCN

MCN サイトの名前変更

MCN の名前を変更した後、名前を変更したサイトで新しい設定をロードする必要があります。

名前を変更したサイトの新しい構成をアップロードするには、次の手順に従います。

1. MCN から、新しい構成でネットワークをステージングします。
2. 名前を変更した MCN のステージング構成パッケージをダウンロードします。
3. MCN の「ローカル変更管理」ページにナビゲートします。
   a) 先にダウンロードしたパッケージをアップロードします。
   b) 処理が完了したら、[次へ] をクリックします。
   c) ［アクティブ化］をクリックします。

> 注
>
> ステップ 3 (c) が完了すると、変更管理プロセスによって、ネットワーク内のアプライアンス (ノード) 用のステージングされたソフトウェアが自動的にアクティブ化されます。

高可用性による **MCN** サイト名の変更

高可用性が有効になっている MCN の名前を変更したら、新しい設定をロードする必要があります。

1. MCN から、新しい構成でネットワークをステージします。
2. アクティブ MCN アプライアンスと高可用性 MCN アプライアンスのステージング構成パッケージを新しい名前でダウンロードします。
3. スタンバイ MCN アプライアンスでサービスを無効にします。
4. アクティブな MCN の [ローカル変更管理] ページにナビゲートします。
   a) 先にダウンロードしたパッケージをアップロードします。
   b) 処理が完了したら、[次へ] をクリックします。
   c) ［アクティブ化］をクリックします。
   d) 高可用性が無効になっているスタンバイ MCN アプライアンスについて、ステップ i、ii、iii、iv を繰り返します。
   e) スタンバイ MCN アプライアンス上でサービスを有効にします。

> 注
>
> ステップ 4 (c) が完了すると、変更管理プロセスによって、ネットワーク内のアプライアンスのステージングされたソフトウェアが自動的にアクティブ化されます。

GEO サイトの名前を変更する

名前を変更した GEO サイトの新しい構成をアップロードするには:

1. MCN から、名前が変更された GEO サイトを含む新しい構成を持つステージネットワーク。
2. MCN から、名前を変更した GEO サイトのステージング構成パッケージをダウンロードします。
3. **MCN** で、[ネットワーク用に ステージングされたアクティブ化] を選択します。これにより、名前を変更したサイトが無効になり、サイトが使用できなくなります。
4. GEO サイトの「ローカル変更管理」ページにナビゲートします。
   a) 先にダウンロードしたパッケージをアップロードします。
   b) パッケージの処理が完了したら、[次へ] をクリックします。
   c) ［アクティブ化］をクリックします。

高可用性で **GEO** サイトの名前を変更する

名前を変更した GEO サイトを高可用性で有効にした新しい設定をアップロードするには、次の手順を実行します。

1. MCN から、名前が変更された GEO サイトを含む新しい構成を持つステージネットワーク。
2. MCN から、名前が変更された GEO サイトを持つアクティブアプライアンスと高可用性アプライアンスの両方のステージング構成パッケージをダウンロードします。
3. **MCN** で、ネットワークの [ステージングの有効化] を選択します。これにより、名前を変更したサイトが無効になり、サイトが使用できなくなります。
4. アクティブな GEO アプライアンスに移動します。
   a)「ローカル変更管理」ページに移動します。
   b) 先にダウンロードしたパッケージをアップロードします。
   c) パッケージの処理が完了したら、[次へ] をクリックします。
   d) ［アクティブ化］をクリックします。
   e) スタンバイアプライアンスに対して、手順 a、b、c、d を繰り返します。

RCN サイトの名前変更

RCN サイトの名前を変更して新しい設定をアップロードするには、次の手順に従います。

1. MCN から、名前が変更された RCN サイトを含む新しい構成を持つステージネットワーク。
2. MCN から、名前を変更した RCN サイトのステージングパッケージをダウンロードします。
3. **MCN** で、[ネットワーク用に ステージングされたアクティブ化] を選択します。これにより、名前が変更された RCN サイトが無効になり、MCN でリージョンサイトが使用できなくなります。リージョンの RCN サイトとブランチは相互に通信しますが、ステップ 4 が完了するまで、リージョンは MCN と通信できません (名前が変更されていない GEO RCN がない限り)。
4. RCN の「ローカル変更管理」ページにナビゲートします。
   a) 先にダウンロードしたパッケージをアップロードします。
   b) パッケージ処理が完了したら、[次へ] をクリックします。
   c) ［アクティブ化］をクリックします。

> 注
>
> リージョンのステージングは、ステップ 4 (c) が完了するまで行われないため、リージョンのブランチが使用可能になるまでに時間がかかります。RCN の変更管理プロセスは、リージョンのステージングを管理します。

高可用性による **RCN** サイト名の変更

名前を変更した RCN サイトを高可用性で有効にした新しい設定をアップロードします。

1. MCN から、名前が変更された RCN サイトを含む新しい構成を持つステージネットワーク。
2. MCN から、RCN サイトの名前を変更したアクティブアプライアンスと高可用性アプライアンスの両方のステージングパッケージをダウンロードします。これにより、名前が変更された RCN サイトが無効になり、MCN でリージョンサイトが使用できなくなります。リージョンの RCN サイトとブランチは相互に通信しますが、ステップ 4 が完了するまで、リージョンは MCN と通信できません (名前が変更されていない GEO RCN がない限り)。
3. **MCN** で、ネットワークの **[**ステージをアクティブ化] を選択します。
4. スタンバイ RCN アプライアンスでサービスを無効にします。
5. アクティブな RCN の「ローカル変更管理」ページにナビゲートします。
   a) 先にダウンロードしたパッケージをアップロードします。
   b) パッケージの処理が完了したら、[次へ] をクリックします。
   c) ［アクティブ化］をクリックします。
   d) 無効になっているスタンバイ RCN アプライアンスに対して、手順 a、b、c を繰り返します。

6. スタンバイ RCN アプライアンスでサービスを有効にします。

GEO RCN サイトの名前を変更する

名前が変更された GEO RCN サイトを使用して新しい設定をアップロードするには:

1. MCN から, 名前を変更した GEO RCN サイトを持つ新しい構成を持つステージネットワーク.
2. MCN から、名前を変更した GEO RCN サイトのステージングパッケージをダウンロードします。
3. **MCN** で、[ネットワーク用に ステージングされたアクティブ化] を選択します。これにより、名前を変更したサイトが無効になり、サイトが使用できなくなります。プライマリ RCN がオンラインの場合、GEO RCN サイトの名前を変更しても、リージョンはネットワークに接続されたままになります。
4. GEO RCN の「ローカル変更管理」ページにナビゲートします。
   a) 先にダウンロードしたパッケージをアップロードします。
   b) パッケージの処理が完了したら、[次へ] をクリックします。
   c) ［アクティブ化］をクリックします。

GEO RCN サイトを高可用性で名前変更する

1. MCN から, 名前を変更した GEO RCN サイトを持つ新しい構成を持つステージネットワーク.
2. MCN から、名前が変更された GEO RCN サイトのアクティブアプライアンスと高可用性アプライアンスの両方のステージングパッケージをダウンロードします。
3. **MCN** で、[ネットワーク用に ステージングされたアクティブ化] を選択します。これにより、名前を変更したサイトが無効になり、サイトが使用できなくなります。プライマリ RCN がオンラインの場合、GEO RCN サイトの名前を変更しても、リージョンはネットワークに接続されたままになります。
4. アクティブな GEO RCN の「ローカル変更管理」ページにナビゲートします。
   a) 先にダウンロードしたパッケージをアップロードします。
   b) パッケージの処理が完了したら、[次へ] をクリックします。
   c) ［アクティブ化］をクリックします。
   d) スタンバイアプライアンスに対して手順 a、band c を繰り返します。

ブランチノードのセットアップ

May 10, 2021

この章では、ブランチサイトを追加および構成する手順について説明します。ブランチサイトを追加する手順は、MCN サイトを作成および設定する場合とよく似ています。ただし、構成手順と設定の一部は、ブランチサイトでは若干異なります。さらに、最初のブランチサイトを追加したら、同じアプライアンスモデルを持つサイトについては、クローン（複製）機能を使用して、これらのサイトを追加および構成するプロセスを合理化できます。

ブランチサイトをセットアップするために MCN サイトを作成する場合と同様に、MCN アプライアンスの管理 Web インターフェイスで **Configuration Editor** を使用する必要があります。構成エディタ は、インターフェイスが **MCN** コンソール モードに設定されている場合にのみ使用できます。

補足的なブランチサイトの展開情報

このガイドに加えて、以下の Knowledge Base サポート記事も推奨されます。

- 仮想 WAN PBR モードの展開手順（CTX201577）

  http://support.citrix.com/article/CTX201577
- 仮想 WAN ゲートウェイモードの展開手順（CTX201576）

  http://support.citrix.com/article/CTX201576

ブランチサイト構成手順の概要

このプロセスを完了するための手順は次のとおりです。

1. ブランチサイトを追加します。
2. ブランチサイトの仮想インターフェイスグループを設定します。
3. ブランチサイトの仮想 IP アドレスを構成します。
4. （任意）ブランチサイトの LAN GRE トンネルを設定します。
5. ブランチサイトの WAN リンクを構成します。
6. ブランチサイトのルートを設定します。
7. （オプション）ブランチサイトの高可用性を設定します。
8. （オプション）新しいブランチサイトのクローンを作成し、追加のサイトを作成および構成します。

   > 注
   >
   > サイトのクローン作成は任意です。仮想 WAN アプライアンスモデルは、オリジナルサイトとクローンサイトの両方で同じである必要があります。クローンの指定されたアプライアンスモデルを変更することはできません。アプライアンスモデルがサイトで異なる場合は、サイトを手動で追加する必要があります。

9. 構成監査アラートを解決します。

10. 完了した設定を保存します。

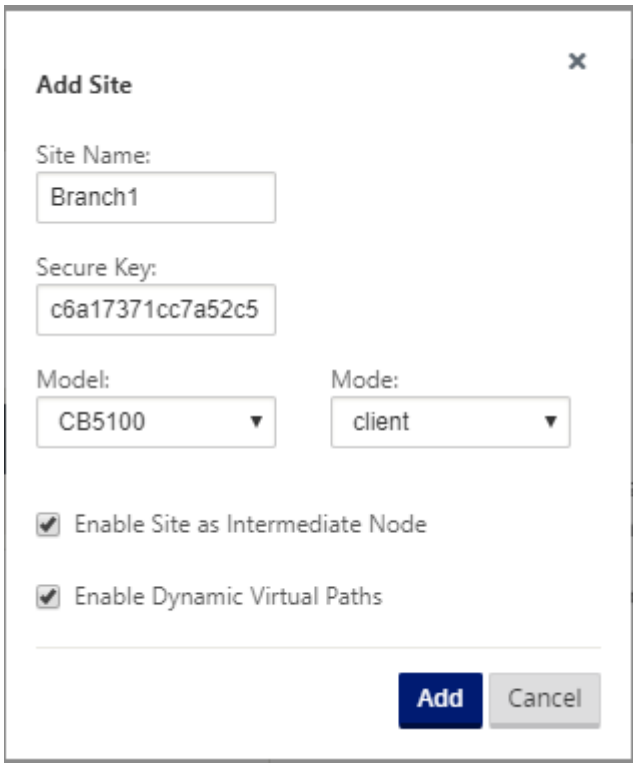
ブランチノードの構成

May 10, 2021

新しいブランチサイトを [S **it** es] テーブルに追加し、サイトの構成を開始するには、次の手順を実行します。

> 注
>
> 新しい構成パッケージを作成して保存した後で MCN からログアウトした場合、続行する前に、再度ログインして設定を再度開く必要があります。これを行うには、構成エディターの メニューバー (ページ上部) の「開く」をクリックします。これにより、変更する構成を選択するためのダイアログボックスが表示されます。

1. 構成エディタで続行し、サイト バーの [追加] をクリックして、新しいブランチサイトの追加と構成を開始します。[サイトの追加] ダイアログボックスが表示されます。



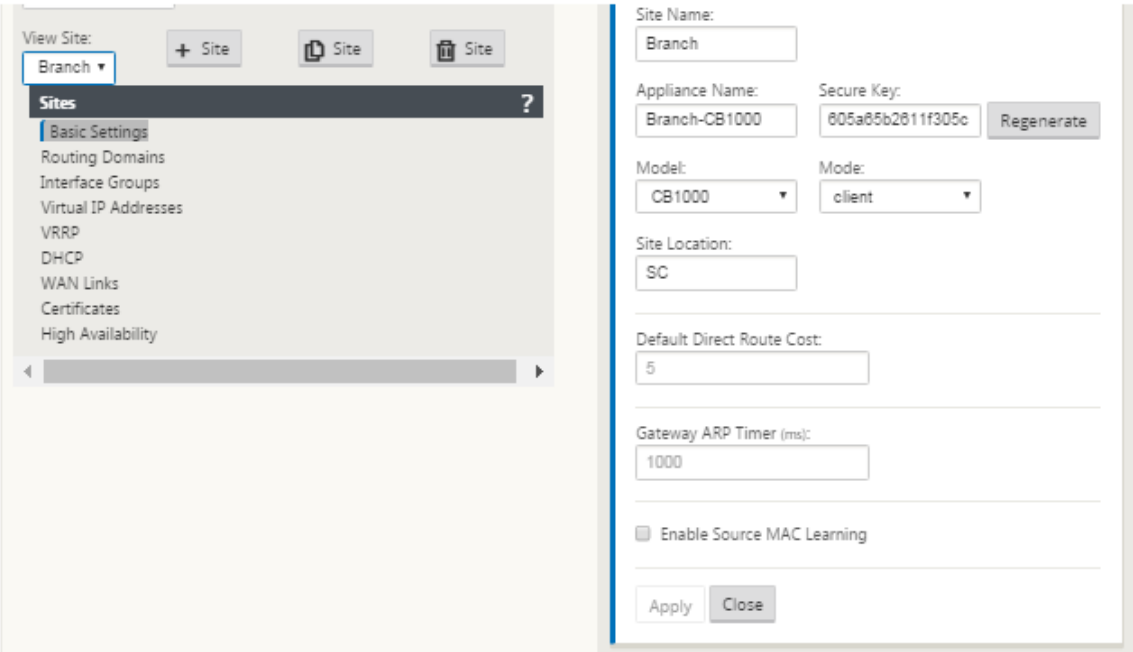
2. 次のサイト情報を入力します。

> 注
>
> エントリにはスペースを含めることはできません。また、Linux 形式である必要があります。

- 「サイト名」—サイトの名前を入力します。
- アプライアンス名—アプライアンスに割り当てる名前を入力します。

- セキュアキー—これは、SD-WAN アプライアンスの暗号化とメンバーシップの検証に使用される 8 ～ 32 桁の 16 進キーです。デフォルトでは、このフィールドには自動的に生成されたセキュリティキーがあらかじめ入力されています。デフォルトをそのまま使用するか、カスタムキーイン 16 進形式を入力します。
- モデル：ドロップダウンメニューからアプライアンス・モデルを選択します。
- モード：モード としてクライアントを選択します。

3. [追加] をクリックしてサイトを追加します。新しいサイトが [サイト] ツリーに追加され、サイト の [基本設定] 構成フォームが開きます。



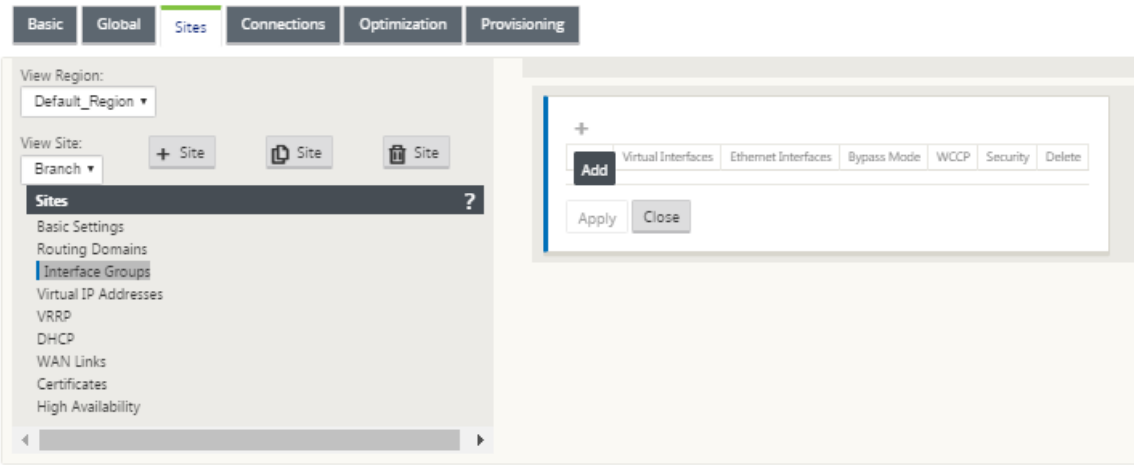
4. サイトの基本設定を入力し、[適用] をクリックします。

   次のステップでは、新しいブランチサイトのインターフェイスグループを追加および設定します。

ブランチのインターフェイスグループの設定方法

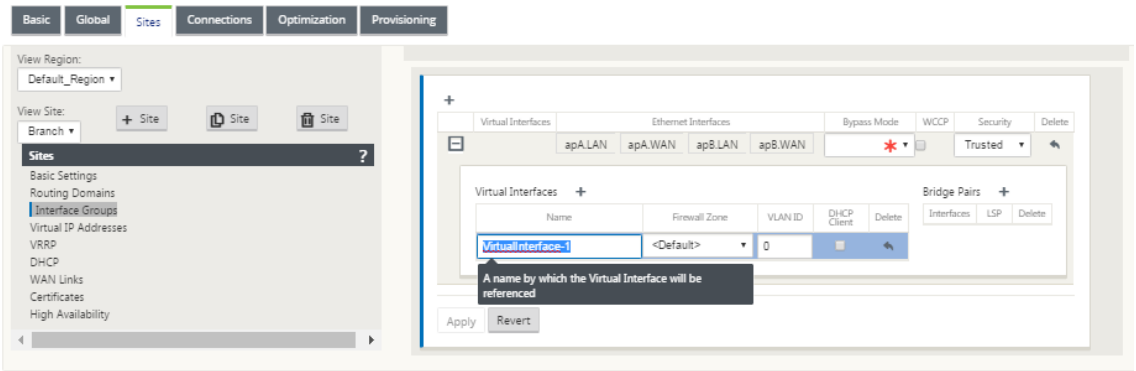
インターフェイスグループを新しいブランチサイトに追加するには、次の手順を実行します。

1. 構成エディタの「サイト」ビューで、「サイトの 表示」ドロップダウンメニューからブランチサイト を選択します。選択したサイトの構成ビューが開きます。



2. [**+**] をクリックして、仮想インターフェイスグループを追加します。新しい空の Virtual インターフェイスグループエントリがテーブルに追加され、編集用に開きます。

3. [仮想インターフェイス] の右側にある [**+**] をクリックします。新しい空のグループエントリがテーブルに追加され、編集のために開きます。



4. グループに含める イーサネットインターフェイスを 選択します。

   [**Ethernet Interf**aces] で、そのインターフェイスを含める/除外するインターフェイスをクリックします。グループに含めるインターフェイスはいくつでも選択できます。

5. ドロップダウンメニューから [バイパスモード] を選択します（デフォルトなし）。

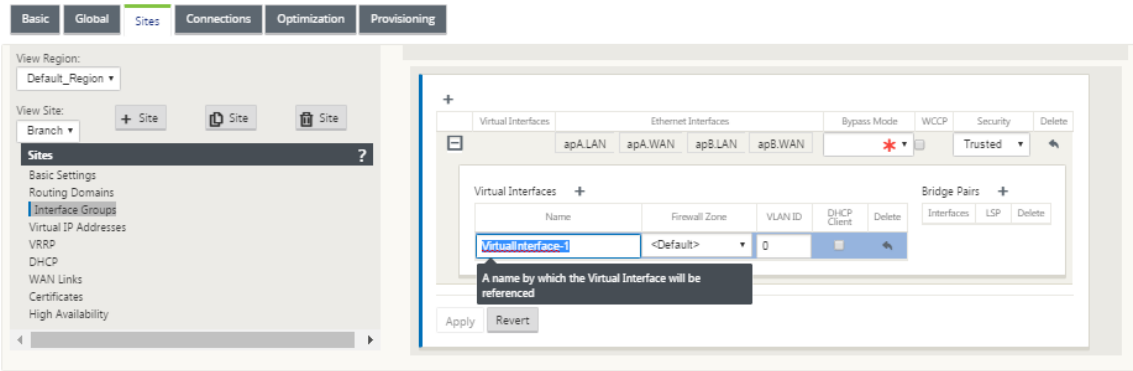
   バイパスモード は、アプライアンスまたはサービスの障害または再起動が発生した場合に、仮想インターフェイスグループ内のブリッジペアインターフェイスの動作を指定します。オプションは、[配線失敗] または [ブ

ロック失敗] です。

6. ドロップダウンメニューから [セキュリティレベル] を選択します。

   仮想インターフェイスグループのネットワークセグメントのセキュリティレベルを指定します。オプションは、[信頼済み] または [信頼できない] です。信頼できるセグメントはファイアウォールで保護されます（デフォルトは Trusted です）。

7. 追加した仮想インターフェイスの左端にある [**+**] をクリックします。[仮想インターフェイス] テーブルが表示されます。



8. [仮想インターフェイス] の右側にある [**+**] をクリックします。名前、ファイアウォールゾーン、**VLAN ID ID** が表示されます。

9. この仮想インターフェイスグループ の名前 と **VLAN ID** を入力します。

   - **[Name**]：この仮想インターフェイスが参照される名前。
   - ファイアウォールゾーン -ドロップダウンメニューからファイアウォールゾーンを選択します。
   - **VLAN ID**：仮想インターフェイスとの間で送受信されるトラフィックを識別およびマーキングするための ID。ネイティブ/タグなしトラフィックには、0（ゼロ）の ID を使用します。

10. [ブリッジペア] の右側にある [**+**] をクリックします。新しい **Bridge Pairs** エントリが追加され、編集用に開きます。

11. ペアリングするイーサネットインターフェイスをドロップダウンメニューから選択します。さらにペアを追加するには、[ブリッジペア] の横にある [**+**] をもう一度クリックします。

12. [適用] をクリックします。設定が適用され、テーブルの新しい仮想インターフェイスグループに追加されます。

    > 注
    >
    > この段階では、新しい仮想インターフェイスグループエントリの右側に、黄色の Delta Audit Alert アイコンが表示されます。これは、サイトの仮想 IP アドレス (VIP) をまだ構成していないためです。現時点では、このアラートは、サイトの仮想 IP を正しく構成すると自動的に解決されるため、無視できます。

13. さらに仮想インターフェイスグループを追加するには、[インターフェイスグループ] ブランチの右側にある [**+**] をクリックし、上記の手順を実行します。

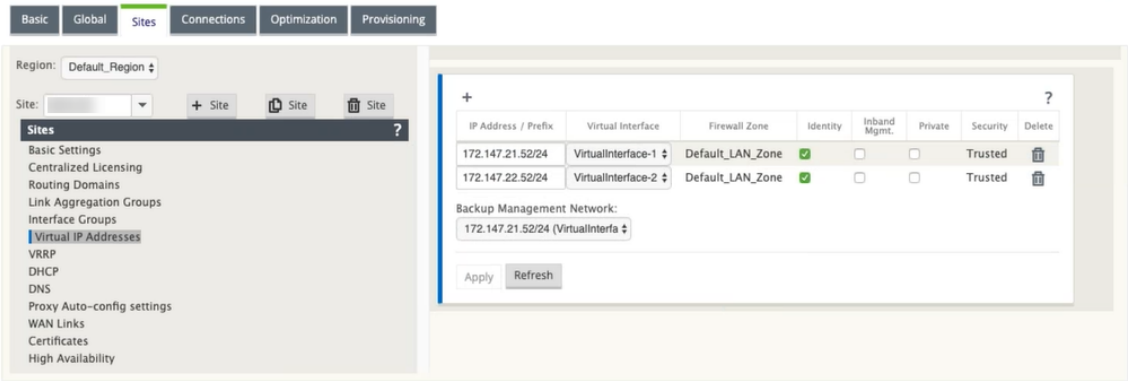
ブランチサイトの仮想 **IP** アドレスを構成する方法

次の手順では、サイトの仮想 IP アドレスを構成し、適切なグループに割り当てます。

1. 新しいブランチ サイト の [サイト] ビューで、[仮想 **IP** アドレス] の左にある [**+**] をクリックします。これにより、新しいサイトの 仮想 **IP** アドレス テーブルが表示されます。
2. [仮想 **IP** アドレス] の右側にある [**+**] をクリックして、アドレスを追加します。新しい仮想 IP アドレスを追加および設定するためのフォームが表示されます。
3. **IP** アドレス / プレフィックス 情報を入力し、アドレスが関連付けられている 仮想インターフェイスを 選択します。仮想 IP アドレスには、完全なホストアドレスとネットマスクを含める必要があります。
4. [ファイアウォールゾーン]、[ID]、[プライベート]、[セキュリティ] など、仮想 IP アドレスの設定を選択します。
5. [**Inband Mgmt**] を選択すると、仮想 IP アドレスが Web UI や SSH などの管理サービスに接続できるようになります。

   > 注:
   >
   > インターフェイスは、セキュリティタイプ「信頼済み」および「**ID** 」が有効である必要があります。

6. バックアップ管理ネットワークとして仮想 IP を選択します。これにより、管理ポートにデフォルト Gateway が設定されていない場合に、管理に仮想 IP アドレスを使用できます。

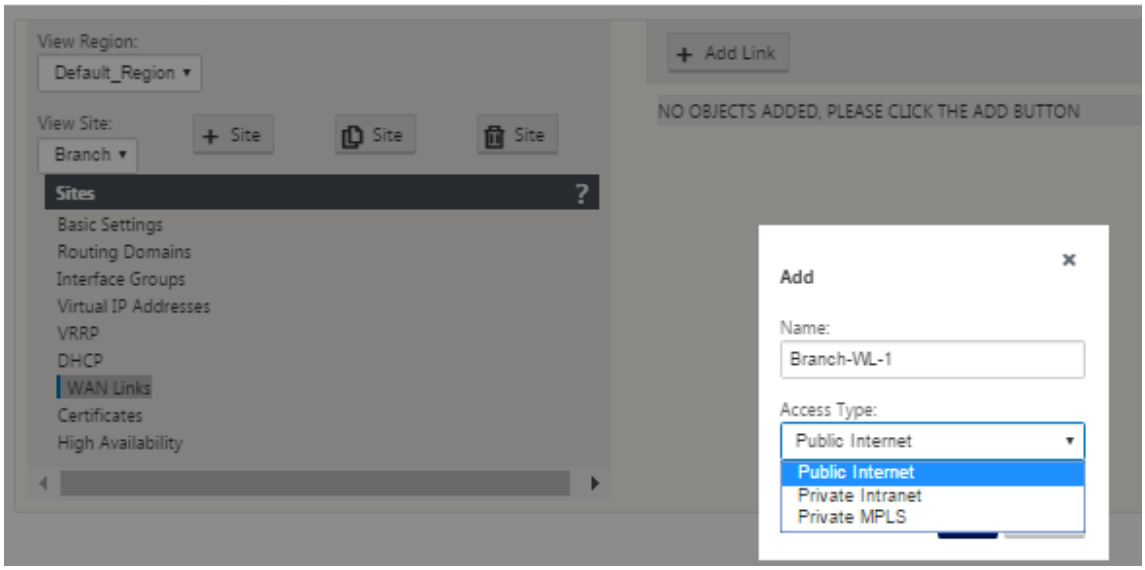


7. [適用] をクリックします。サイトへのアドレス情報が追加され、サイトの 仮想 **IP** アドレス テーブルに含められます。
8. さらに仮想 IP アドレスを追加するには、[仮想 **IP** アドレス] の右側にある [**+**] をクリックし、上記の手順を実行します。

ブランチの **WAN** リンクを構成する方法

次のステップでは、サイトの WAN リンクを構成します。

1. 新しいブランチ サイト の [サイト] ビューで、[**WAN** リンク] ラベルをクリックします。
2. [**W** AN リンク] の右側にある [Add Link] をクリックして、新しい WAN リンクを追加します。[追加] ダイアログボックスが表示されます。



3. （オプション）デフォルトを使用しない場合は、WAN リンクの名前を入力します。

   デフォルトはサイト名で、次のサフィックスを付加します。

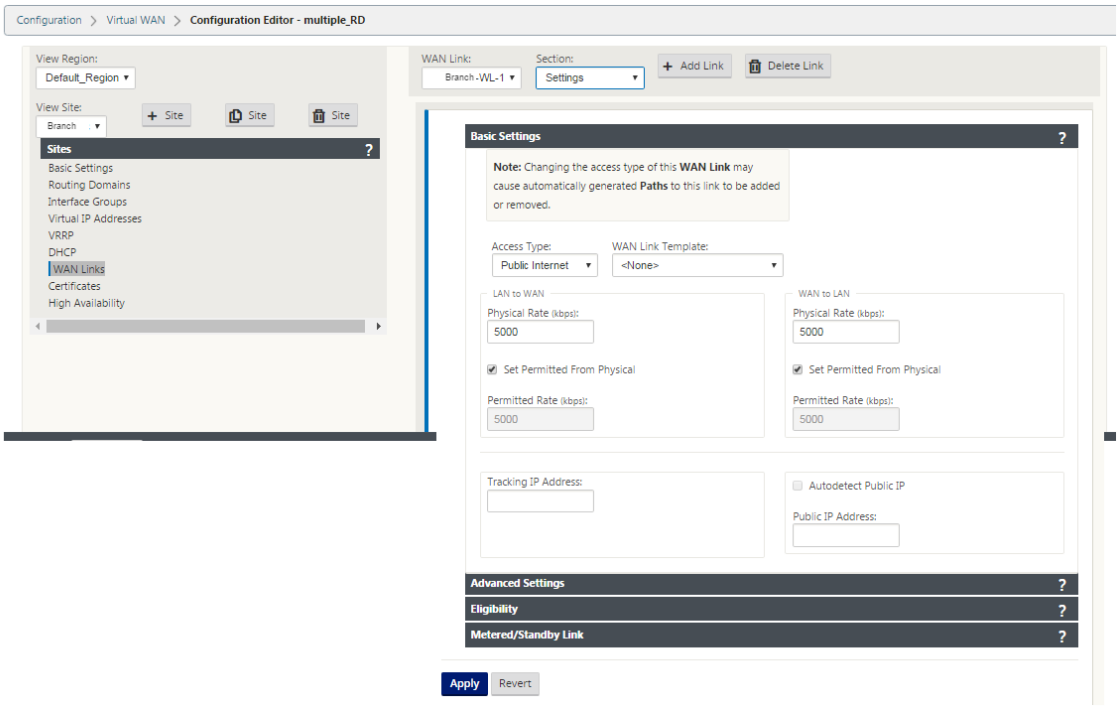
   -WL-<number>

   ここで <number>、はこのサイトの WAN リンクの数を 1 ずつ増やします。

4. ドロップダウンメニューから「アクセスタイプ」を選択します。

   オプションは、[パブリックインターネット**]**、**[**プライベートイントラネット**]**、または [プライベート マルチプロトコルラベルスイッチング**]** です。

5. [追加] をクリックします。[**WAN** リンク の基本設定] 設定ページが表示され、新しい未設定の WAN リンクがページに追加されます。

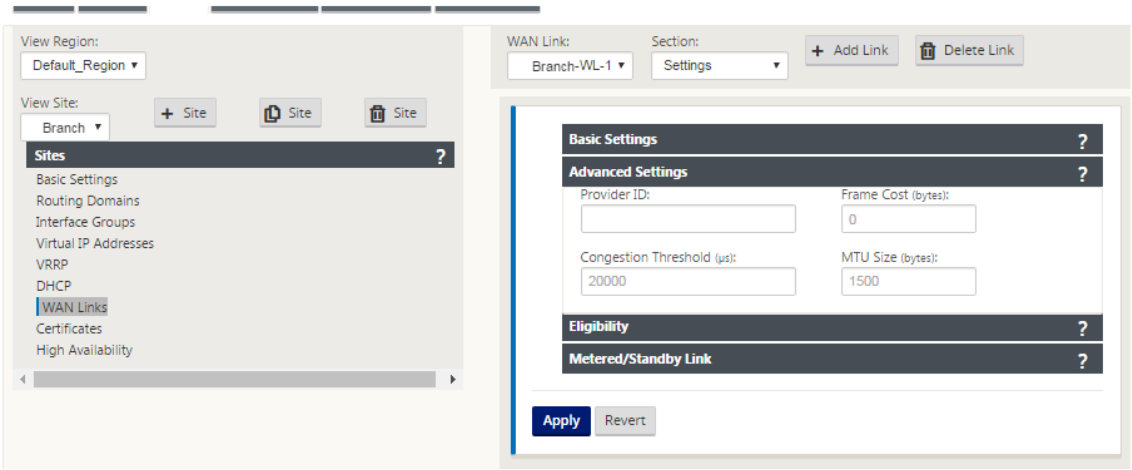


6. 新しい WAN リンクのリンクの詳細を入力します。LAN から WAN、WAN から **LAN** への設定を構成します。

   いくつかのガイドラインは次のとおりです。

   - 一部のインターネットリンクは非対称である場合があります。許可された速度を誤って設定すると、そのリンクのパフォーマンスに悪影響を及ぼす可能性があります。
   - 認定レートを超えるバースト速度は使用しないでください。
   - インターネット WAN リンクの場合は、必ずパブリック IP アドレスを追加してください。

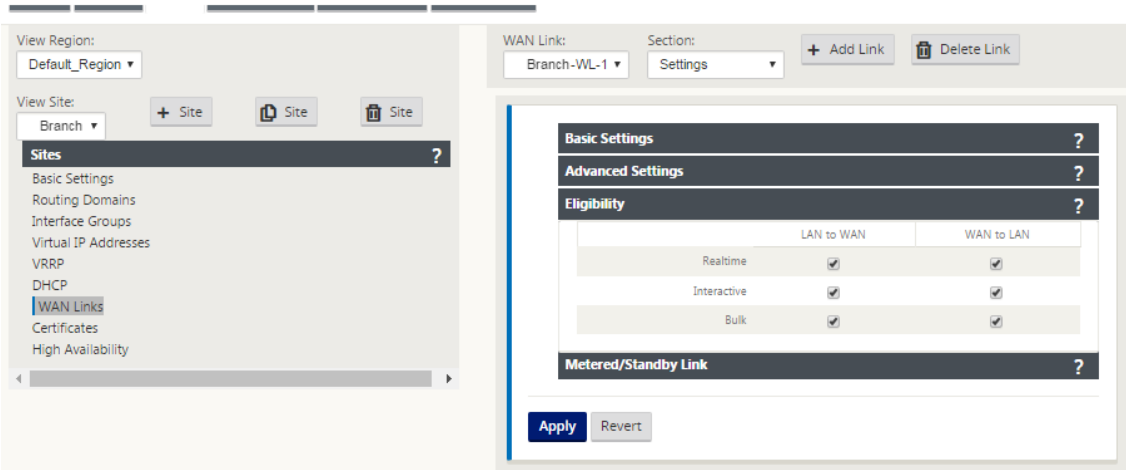
7. グレーの [詳細設定] セクションバーをクリックします。リンクの [詳細設定] フォームが開きます。



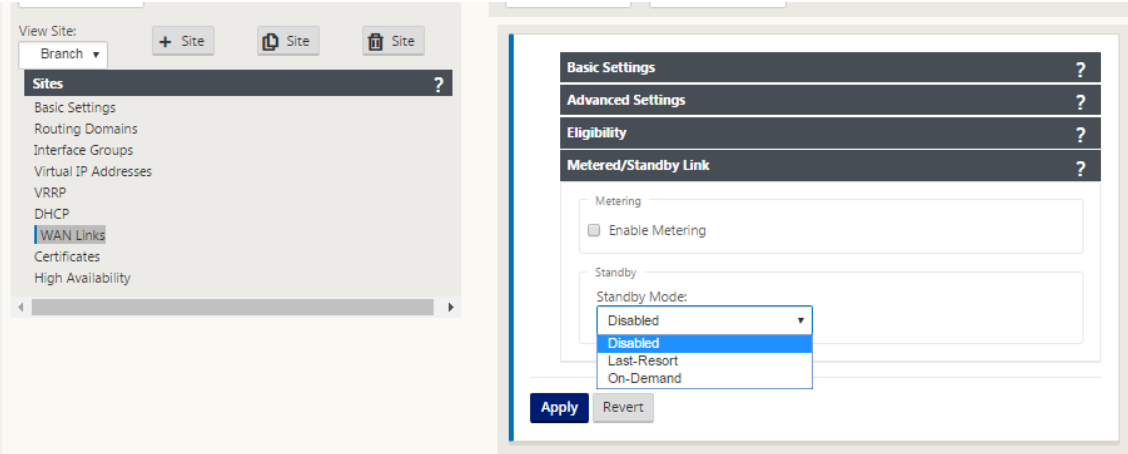
8. リンクの **[詳細設定]** を入力します。

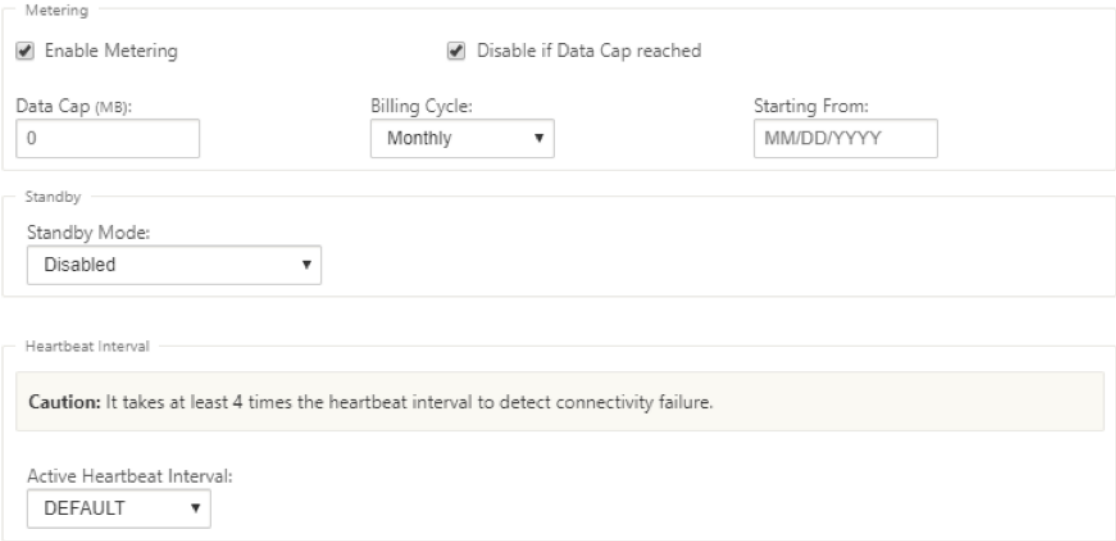
- [**Provider ID**]:（オプション）一意の ID 番号 1 ～100 を入力し、同じサービスプロバイダーに接続されている WAN リンクを指定します。仮想 WAN は、重複パケットを送信するときにプロバイダー ID を使用してパスを区別します。
- フレームコスト（バイト）: 各パケットに追加するヘッダー/トレーラのサイズ（バイト単位）を入力します。たとえば、追加されたイーサネット IPG または AAL5 トレーラーのバイト単位のサイズ。
- 輻輳しきい値: 輻輳しきい値（マイクロ秒）を入力します。このしきい値は、WAN リンクがパケット転送を抑制し、それ以上の輻輳を回避します。
- [**MTU Size**（**bytes**）]: フレームコストを含まない、最大の raw パケットサイズ（バイト単位）を入力します。

9. グレーの「適格」セクション・バーをクリックします。リンクの [適格 設定] フォームが開きます。
10. リンクの「適格」設定を選択します。



11. グレーの [従量制課金リンク] セクションバーをクリックします。リンクの [従量制課金リンク 設定] フォームが開きます。
12. （オプション）このリンクの メータリング を有効にするには、[メータリングを有効にする] を選択します。これにより、[メータリング設定を有効にする] フィールドが表示されます。





13. リンクのメータリング設定を構成します。次のように入力します：

    - 「データ上限 **(MB)** 」—リンクに対するデータ上限割り当てを MB 単位で入力します。
    - [請求サイクル] —ドロップダウンメニューから [毎月] または [毎週] を選択します。
    - [開始 日] —請求サイクルの開始日を入力します。
    - [最後のリゾートを設定]：他のすべての利用可能なリンクに障害が発生した場合に、このリンクをラストリゾートリンクとして有効にするには、このオプションを選択します。通常の WAN 条件下では、仮想 WAN は、リンクステータスを確認するために、従量制課金リンクを介して最小限のトラフィックだけを送信します。ただし、障害が発生した場合、SD-WAN は本番トラフィックを転送するための最後の手段として、アクティブな従量制課金リンクを使用できます。

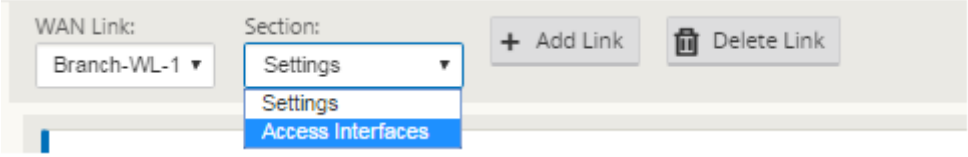
14. ［適用］をクリックします。これにより、指定した設定が新しい WAN リンクに適用されます。

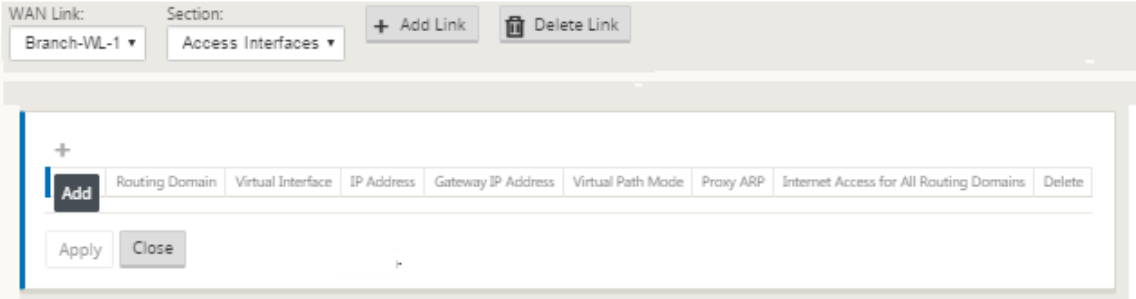
    次のステップでは、新しい WAN リンクのアクセスインターフェイスを設定します。アクセスインターフェイスは、特定の WAN リンクのインターフェイスとしてまとめて定義された、仮想インターフェイス、WAN エンドポイント IP アドレス、ゲートウェイ IP アドレス、および仮想パスモードで構成されます。各 WAN リン

クには、少なくとも 1 つのアクセスインターフェイスが必要です。

> 注
>
> リモート帯域幅を考慮して共有を自動プロビジョニングするオプションが追加され、WAN リンクが設定されます。[リモート帯域幅を使用して Provisioning を設定] オプションを使用すると、大規模なネットワークと多様な帯域幅構成を持つユーザーは、データセンターサイトの帯域幅プロビジョニングを動的に管理できます。

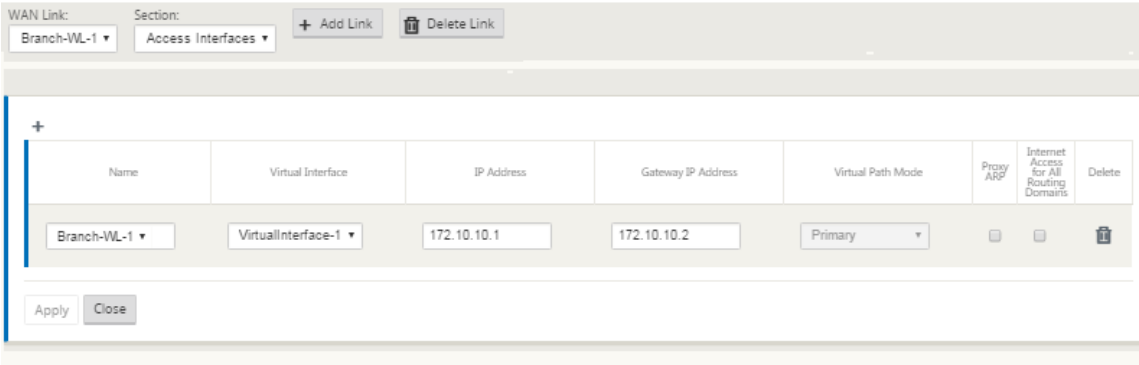
15. リンクの [WAN リンク] 設定ページで [アクセスインターフェイス] を選択します。これにより、サイトの [アクセスインターフェイス] ビューが開きます。





16. [**+**] をクリックして、インターフェイスを追加します。テーブルに空白のエントリが追加され、編集のために開きます。リンクの [アクセスインターフェイス] 設定を入力します。

> 注
>
> 各 WAN リンクには、少なくとも 1 つのアクセスインターフェイスが必要です。



17. 次のように入力します:

    - 名前: これは、このアクセスインタフェースが参照される名前です。新しいアクセスインターフェイスの名前を入力するか、デフォルトをそのまま使用します。デフォルトでは、次の命名規則が使用されます。

WAN_link_name-AI-number

ここで、W *AN_Link_name* はこのインターフェイスに関連付ける WAN リンクの名前です。number は、このリンクに現在設定されているアクセスインターフェイスの数で、1 ずつ増加します。

> 注
>
> 名前が切り捨てられた場合は、フィールドにカーソルを置き、クリックしたままマウスを右または左に回転すると、切り捨てられた部分が表示されます。

- 仮想インターフェイス—このアクセスインターフェイスが使用する仮想インターフェイス。このブランチサイト用に構成された Virtual Interfaces のドロップダウンメニューからエントリを選択します。
- **IP** アドレス—アプライアンスから WAN へのアクセスインターフェイスエンドポイントの IP アドレス。
- **Gateway IP** アドレス -ゲートウェイルータの IP アドレスです。
- 仮想パスモード：この WAN リンク上の仮想パストラフィックのプライオリティ。オプションは、[プライマリ]、[セカンダリ]、または [除外] です。[除外] に設定すると、このアクセスインターフェイスはインターネットおよびイントラネットトラフィックにのみ使用されます。
- 「プロキシ **ARP** 」—有効にするチェックボックスを選択します。有効にすると、Gateway に到達できない場合に、仮想 WAN アプライアンスはゲートウェイ IP アドレスの ARP 要求に応答します。

18. ［適用］をクリックします。

    これで、新しい WAN リンクの設定が完了しました。この手順を繰り返して、サイトに追加の WAN リンクを追加および構成します。

    次のステップでは、サイトのルートを追加および構成します。

ブランチのルートを構成する方法

サイトのルートを追加および構成するには、次の手順を実行します。

1. 新しいブランチサイトの [接続] ビューをクリックし、[ルート] を選択します。これにより、サイトの [ルート] ビューが表示されます。
2. ルート を追加するには、[ルート] の右側にある [**+**] をクリックします。これにより、編集用の [ルート] ダイアログボックスが開きます。

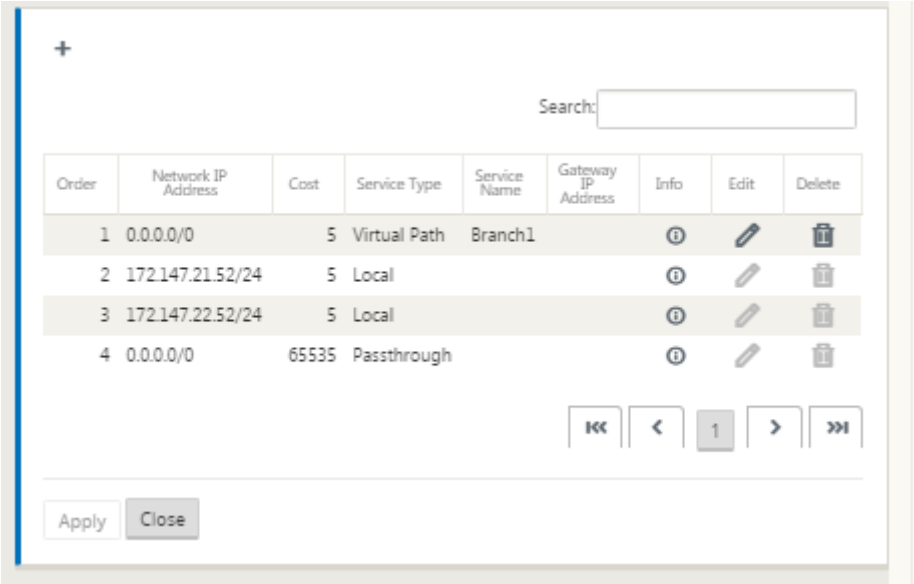
3. 新しいルートのルート設定情報を入力します。

- 「ネットワーク **IP** アドレス」—ネットワーク IP アドレスを入力します。
- **Cost**: このルートのルートプライオリティを決定するために、1 ～15 の重みを入力します。低コストのルートは、高コストのルートよりも優先されます。デフォルト値は 5 です。
- [**Service Type**] —このフィールドのドロップダウンメニューからルートのサービスタイプを選択します。使用できるオプションは、次のとおりです。
- 仮想パス—このサービスは、仮想パスを通過するトラフィックを管理します。仮想パスは、2 つの WAN リンク間の論理リンクです。これは、2 つの SD-WAN ノード間で高いサービス・レベル通信を提供するために結合された WAN パスの集合で構成されます。これは、変化するアプリケーション需要と WAN 条件を常に測定し、適応させることによって行われます。SD-WAN アプライアンスは、パス単位でネットワークを測定します。仮想パスは、スタティック（常に存在）またはダイナミック（2 つの SD-WAN アプライアンス間のトラフィックが設定されたしきい値に達した場合のみ存在）のいずれかになります。
- インターネット—このサービスは、エンタープライズサイトとパブリックインターネット上のサイト間のトラフィックを管理します。このタイプのトラフィックはカプセル化されません。輻輳時には、SD-WAN は、仮想パスに対するレート制限によるインターネットトラフィックと、管理者が確立した SD-WAN 構成に従ってイントラネットトラフィックによって、帯域幅を積極的に管理します。
- イントラネット—このサービスは、仮想パス経由の送信用に定義されていないエンタープライズイントラネットトラフィックを管理します。インターネットトラフィックと同様に、カプセル化されていないままであり、SD-WAN は、輻輳時にこのトラフィックを他のサービスタイプと比較してレート制限することで、帯域幅を管理します。特定の条件下では、仮想パス上のイントラネットフォールバック用に構成されている場合、通常は仮想パスとともに移動するトラフィックは、代わりにイントラネットトラフィックとして扱われ、ネットワークの信頼性を維持できます。

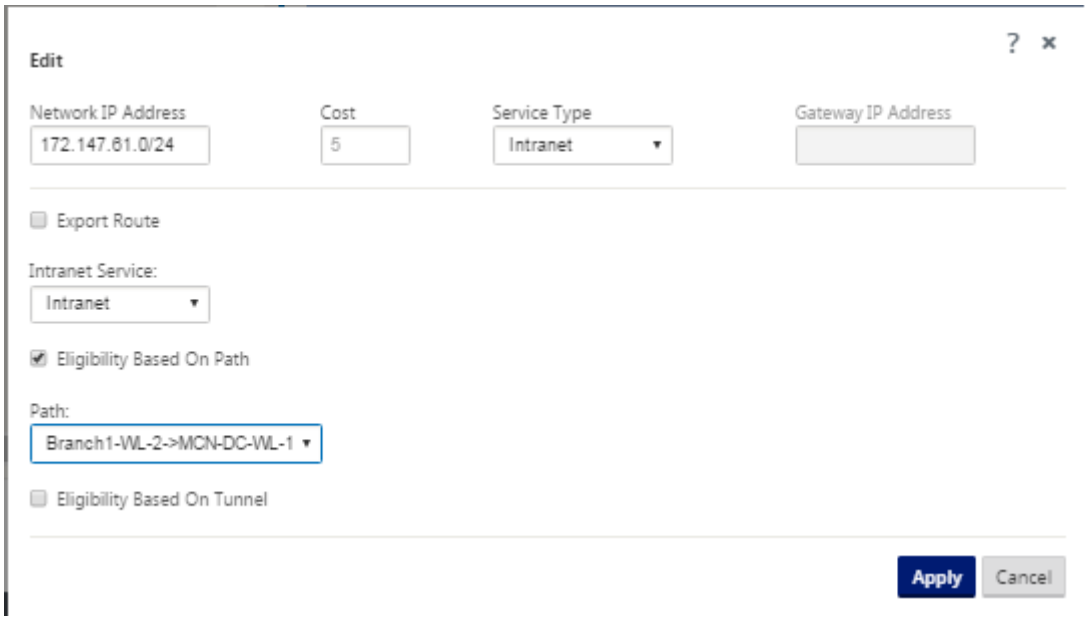
- パススルー—このサービスは、仮想 WAN を通過するトラフィックを管理します。パススルーサービスに送信されるトラフィックには、ブロードキャスト、ARP、その他の非 IPv4 トラフィック、および Virtual WAN アプライアンスのローカルサブネット、構成済みサブネット、またはネットワーク管理者が適用したルール上のトラフィックが含まれます。このトラフィックは、SD-WAN によって遅延、シェーピング、または変更されません。したがって、SD-WAN アプライアンスが他のサービスで使用するように構成されている WAN リンク上で、パススルートラフィックが実質的なリソースを消費しないようにする必要があります。
- ローカル：このサービスは、他のサービスと一致しないサイトへのローカルな IP トラフィックを管理します。SD-WAN は、ローカルルートを送信元および宛先とするトラフィックを無視します。
- **GRE** トンネル：このサービスは、GRE トンネル宛ての IP トラフィックを管理し、サイトで設定された LAN GRE トンネルと一致します。GRE トンネル機能を使用すると、LAN 上の GRE トンネルを終了するように SD-WAN アプライアンスを設定できます。サービスタイプ GRE Tunnel のルートの場合、Gateway はローカル GRE トンネルのトンネルサブネットの 1 つに存在する必要があります。
- **LAN IPsec** トンネル—このサービスは、IPsec トンネル宛の IP トラフィックを管理します。
- 「ゲートウェイ **IP** アドレス」—このルートのゲートウェイ IP アドレスを入力します。
- [パスに基づく適格性]（チェックボックス）：（オプション）有効にすると、選択したパスがダウンしても、ルートはトラフィックを受信しません。
- 「パス」(Path) —ルートの適格性を判断するために使用するパスを指定します。

4. ［適用］をクリックします。

> 注
>
> [適用] をクリックすると、追加のアクションが必要であることを示す監査警告が表示されることがあります。赤い点または金色のデルタアイコンは、表示されるセクションにエラーを示します。これらの警告を使用して、エラーや不足している構成情報を識別できます。監査警告アイコンの上にカーソルを置くと、そのセクションのエラーの簡単な説明が表示されます。暗いグレーの 監査 ステータスバー (ページ下部) をクリックして、すべての監査警告の一覧を表示することもできます。



以下に示すように、設定済みのルートを編集することもできます。



これで、クライアントサイトの構成に必要な手順が完了しました。また、展開の次のフェーズに進む前に、完了するように選択できる、追加のオプションの手順もいくつかあります。これらの手順のリストと手順へのリンクを以下に示します。これらの機能を今すぐ設定したくない場合は、直接 [MCN での SD-WAN アプライアンスパッケージの準備] に進みます。(/en-us/citrix-sd-wan/11/configuration/installing-virtual-wan-appliance-packages-clients.html)

オプションの手順は次のとおりです。

- 高可用性の構成—高可用性は、1 つのサイトの 2 つの Virtual WAN アプライアンスが冗長性のためにアクティブ/スタンバイパートナーシップ容量でサービスを提供する構成です。このサイトに高可用性を実装していない場合は、この手順を省略できます。手順については、[ブランチサイトの高可用性（高可用性）の設定（オ

プション)。] を参照してください。(/en-us/citrix-sd-wan/11/configuration/setup-branch-nodes/ha-for-a-branch-node.html)

- 新しいブランチサイトのクローン—構成したブランチサイトのクローンを作成し、別のサイトを追加するためのテンプレートとして使用することもできます。元のサイトとクローンのアプライアンスモデルは、同じである必要があります。手順については、「ブランチ・サイトのクローン作成（オプション）」を参照してください。
- **WAN Optimization** の構成—**Citrix SD-WAN** 仮想 **WAN** ライセンスに **WAN Optimization** 機能が含まれている場合は、これらの機能を有効にして構成に追加できます。これを行うには、構成エディタ の「最適化」セクションを完了し、変更した構成を保存する必要があります。

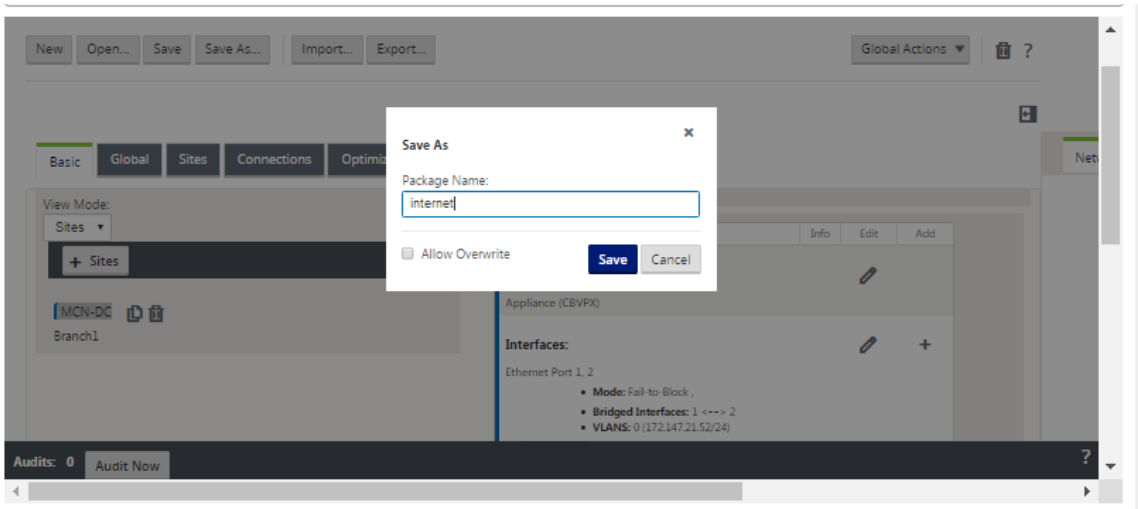
構成の保存

次のステップでは、完了した サイト 構成を保存します。構成は、ローカルアプライアンスの Workspace に保存されます。

> 警告
>
> コンソールセッションがタイムアウトになったり、構成を保存する前に管理 Web Interface からログアウトした場合、保存されていない構成の変更はすべて失われます。その後、システムに再度ログインし、設定手順を最初から繰り返す必要があります。そのため、構成パッケージを頻繁に保存するか、構成内の重要なポイントに保存することをお勧めします。
> 注
>
> 余分な予防策として、間違った構成パッケージを上書きしないように、[保存] ではなく [名前を付けて保存] を使用することをお勧めします。
>
> 構成ファイルを保存した後、管理 Web Interface からログアウトし、後で構成プロセスを続行するオプションがあります。ただし、ログアウトした場合は、再開時に保存した設定を再度開く必要があります。手順については、「**MCN** の設定」のセクションを参照してください。保存した構成パッケージの構成エディタへのロード。

現在の構成パッケージを保存するには、次の手順を実行します。

1. ［名前を付けて保存］をクリックします（[構成エディタ］の中央ペインの上部にある)。[名前を付けて保存] ダイアログボックスが表示されます。



2. 構成パッケージ名を入力します。[保存] をクリックします。

> 注
>
> 構成を既存の構成パッケージに保存する場合は、保存する前に [上書きを許可] を選択してください。

次の手順では、MCN とクライアントサイト間の仮想パスと仮想パスサービスを構成します。手順については、MCN サイトとクライアントサイト間の仮想パスサービスの設定を参照してください。

ブランチサイトの名前変更

ブランチサイトの名前を変更した後、新しい構成パッケージをネットワークにアップロードする必要があります。

1. MCN から、名前が変更されたブランチサイトを含む新しい構成を持つステージネットワーク。
2. 名前を変更したブランチサイトのステージングパッケージをダウンロードします。
3. **MCN** で、[ステージングされたネットワークのアクティブ化] を選択します。これにより、名前を変更したサイトが無効になり、サイトが使用できなくなります。
4. ブランチの「ローカル変更管理」ページにナビゲートします。
5. 先にダウンロードしたパッケージをアップロードします。[次へ] をクリックし、[アクティブ化] をクリックします。

高可用性を使用したブランチサイトの名前の変更

高可用性を有効にしたブランチサイトの名前を変更した後に新しい設定をアップロードするには、次の手順を実行します。

1. MCN から、名前が変更されたブランチサイトを含む新しい構成でネットワークをステージングします。

2. ブランチサイトの名前を変更したアクティブアプライアンスと高可用性アプライアンスの両方のステージングパッケージをダウンロードします。
3. **MCN** で、[ネットワーク用に ステージングされたアクティブ化] を選択します。これにより、名前を変更したサイトが無効になり、サイトが使用できなくなります。
4. ブランチでアクティブなアプライアンスにナビゲートします。[ローカル変更管理] ページに移動します。
5. 先にダウンロードしたパッケージをアップロードします。[次へ] をクリックし、[アクティブ化] をクリックします。
6. スタンバイアプライアンスに対して、手順 4 (a) と 4 (b) を繰り返します。

ブランチサイトのクローン（オプション）

May 10, 2021

このセクションでは、新しいブランチサイトをクローンして、ブランチサイトを追加するための部分的なテンプレートとして使用する方法について説明します。

> 注
>
> サイトのクローン作成は任意です。仮想 WAN アプライアンスモデルは、オリジナルサイトとクローンサイトの両方で同じである必要があります。クローンの指定されたアプライアンスモデルを変更することはできません。アプライアンスモデルがサイトで異なる場合は、前のセクションで説明したように、手動でサイトを追加する必要があります。

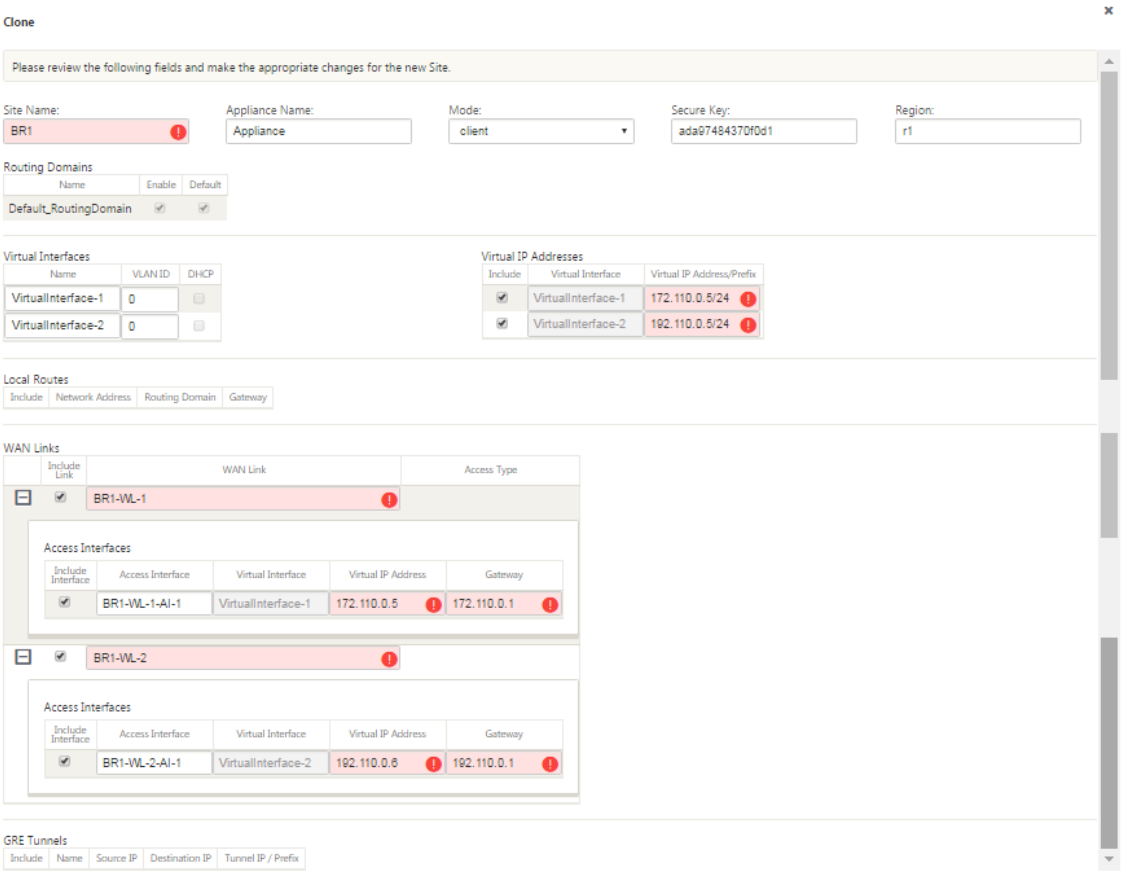
サイトのクローンを作成すると、ブランチノードの追加および構成プロセスが合理化されます。サイトのクローンが作成されると、サイトの構成設定セット全体がコピーされ、単一のフォームページに表示されます。その後、新しいサイトの要件に従って設定を変更できます。元の設定の一部は、必要に応じて保持できます。ただし、ほとんどの設定はサイトごとに一意である必要があります。

サイトのクローンを作成するには、次の操作を行います。

1. 構成エディタ の［サイト］ツリー（中央のペイン）で、複製するブランチサイトをクリックします。

   これにより、サイトツリーでその サイト ブランチが開き、「クローン」ボタン（ダブルページアイコン）と「削除」ボタン（ゴミ箱アイコン）が表示されます。
2. ツリー内のブランチサイト名の右側にある [クローン] アイコンをクリックします。

   これにより、クローンサイトの 構成ページが開きます。



3. 新しいサイトの構成パラメータ設定を入力します。

   Audit Alert アイコン（赤いドット）が付いたピンク色のフィールドは、必要なパラメータ設定を示し、元のクローンサイトの設定とは異なる値を指定する必要があります。通常、この値は一意である必要があります。

   > ヒント
   >
   > クローン作成プロセスをさらに合理化するには、クローンに名前を付ける際に、一貫した事前定義された命名規則を使用します。

4. すべての監査アラートを解決します。

   エラーを診断するには、[**Audit Alert**] アイコン（赤い点またはゴールデンロッドのデルタ）にカーソルを合わせて、特定のアラートのバブルヘルプを表示します。

5. 「クローン」(右端隅) をクリックしてサイトを作成し、「サイト」(S **it** es) テーブルに追加します。

   > 注
   >
   > [クローン] ボタンは、必要な値をすべて入力するまで使用できず、新しいサイト構成にエラーがない状態になります。

6. （オプション）設定への変更を保存します。

> 注
>
> 余分な予防策として、間違った構成パッケージを上書きしないように、[保存] ではなく [名前を付けて保存] を使用することをお勧めします。既存の構成に保存する前に、[上書きを許可] を選択してください。そうしないと、変更は保存されません。

追加する各ブランチサイトについて、この時点までの手順を繰り返します。

すべてのサイトの追加が完了したら、次の手順では、監査アラートの構成を確認し、必要に応じて修正または追加を行います。

ブランチ構成の監査

May 10, 2021

項目の横にある Audit Alert アイコン (赤い点または金色のデルタ) は、その項目の構成エラーまたはパラメータ情報が不足していることを示します。アイコンの横にある数字は、そのアラートに関連するエラーの数を示します。特定のアラートのバブル・ヘルプを表示するには、アラート・アイコンにカーソルを合わせます。これにより、そのアラートによってフラグ付けされた特定のエラーの簡単な説明が表示されます。構成内のすべての監査アラートを解決する必要があります。そうしないと、展開プロセスの後半で、構成パッケージの検証、ステージングおよびアクティブ化ができなくなります。

すべての監査アラート（存在する場合）を解決すると、構成の「サイト」フェーズが完了します。次のステップでは、完成した サイト 構成を保存します。

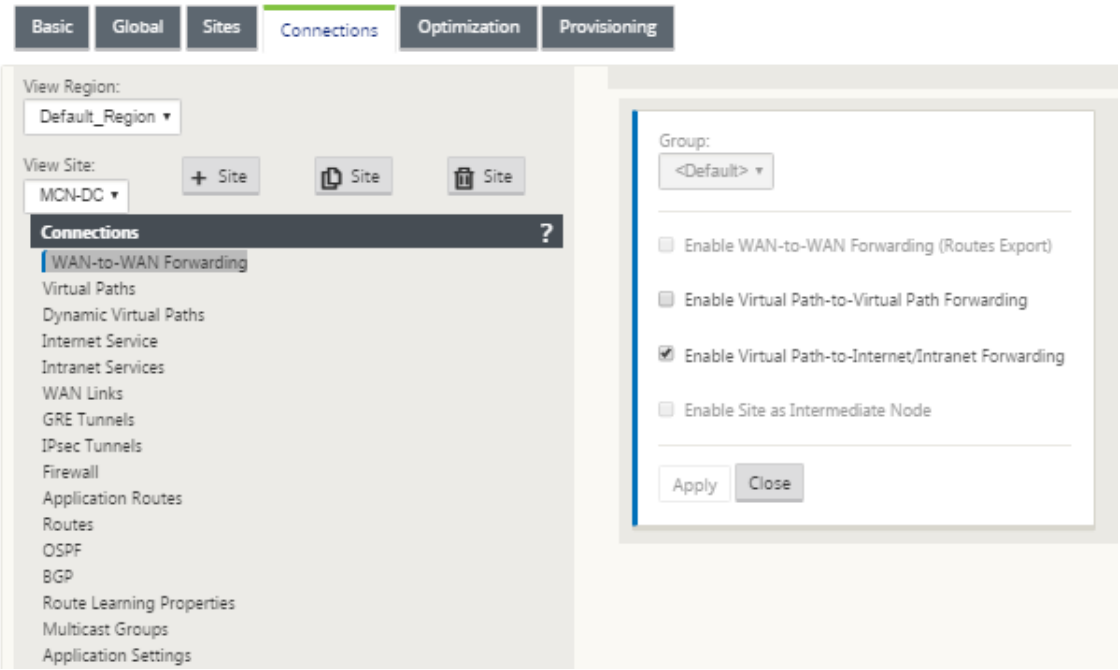
MCN サイトとクライアントサイト間の仮想パスサービスの構成

May 10, 2021

次の手順では、MCN と各クライアント (ブランチ) サイト間の仮想パスサービスを構成します。これを行うには、構成 エディタ の「接続」セクション構成ツリーにある構成フォームと設定を使用します。

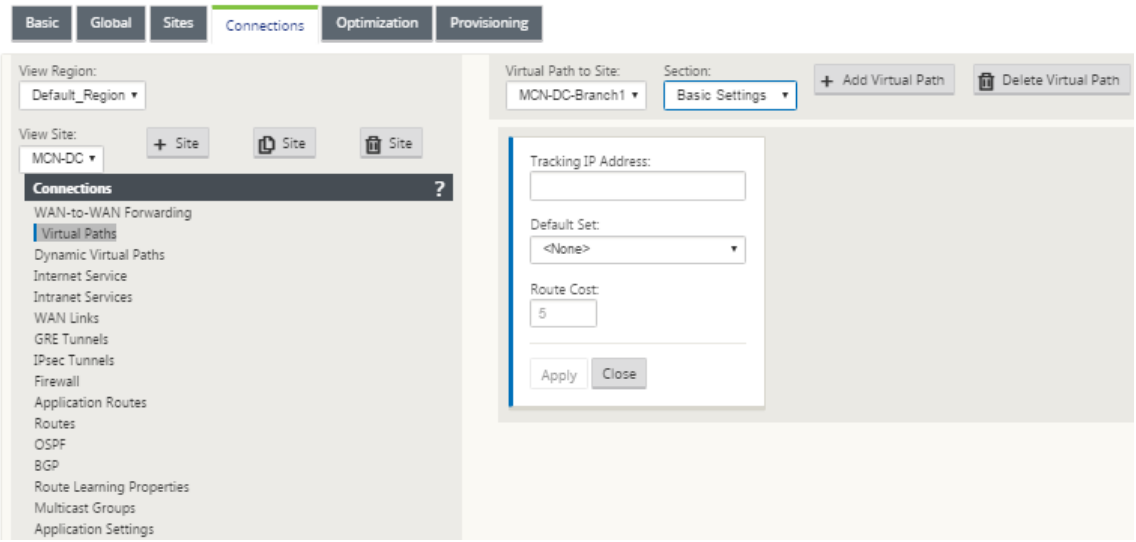
MCN とクライアントサイト間の仮想パスサービスを構成するには、次の手順を実行します。

1. 構成エディタで続行し、[接続] タブをクリックします。[接続] セクションの設定ツリーが表示されます。
2. [接続] セクションページの [サイトの表示] ドロップダウンメニューを選択します。これにより、接続 構成で MCN サイトが開きます。

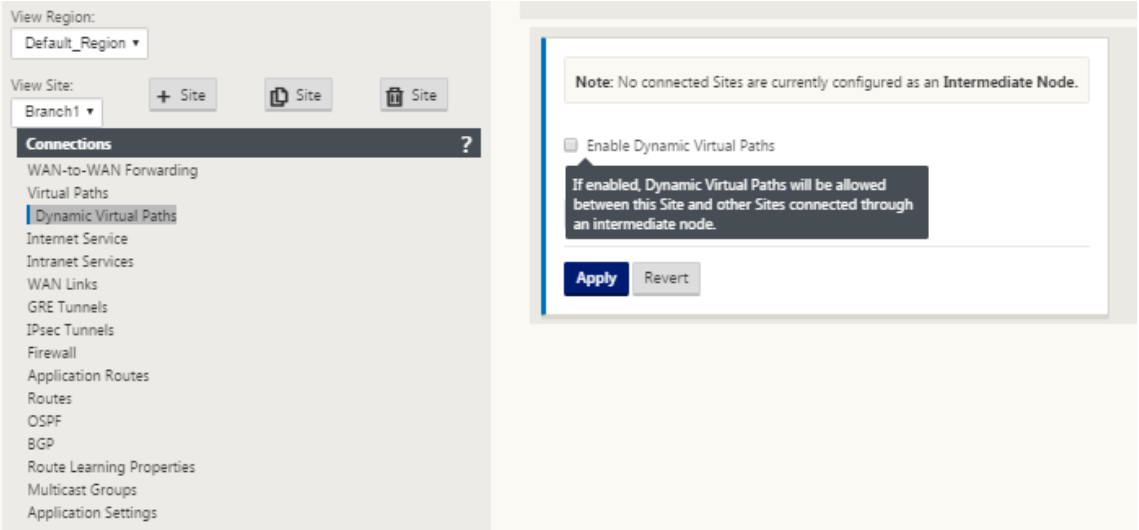


> 注
>
> WAN から WAN への転送グループは、リージョン内でのみサポートされ、リージョン間ではサポートされません。リージョンを使用すると、WAN から WAN への転送グループに依存する代わりに、ネットワークを分離できます。

3. [仮想パス] をクリックします。これにより、MCN サイトの [仮想パス構成] セクション (子ブランチ) が開きます。このセクションでは、MCN と各仮想 WAN クライアントサイト間の仮想パスサービスを構成するための設定とフォームについて説明します。次の図は、MCN サイトの [仮想パス] セクションの例を示しています。



次の図は、ブランチサイトの 動的仮想パス セクションの例を示しています。



[動的仮想パス] セクションでは、次の項目を設定できます。

- 動的 仮想パス:（オプション）このセクションの設定では、動的仮想パスの有効化と無効化、およびサイトの動的仮想パスの最大許容値を設定できます。動的仮想パスは、構成されたしきい値に基づいて、サイト間で直接確立される仮想パスです。しきい値は、通常、これらのサイト間で発生するトラフィックの量に基づきます。動的仮想パスは、指定されたしきい値に達した後にのみ動作します。動的仮想パスは通常の動作では必要ないため、このセクションの設定は任意です。
- < MCN_Site_Name>**_< Branch_Site_Name >**: この仮想パスが必要なため、システムは最初に **MCN** とクライアントサイト間に静的な仮想パスを自動的に追加します。パスの名前は次の形式を使用します。

  <MCN_Site_Name>_<Branch_Site_Name>

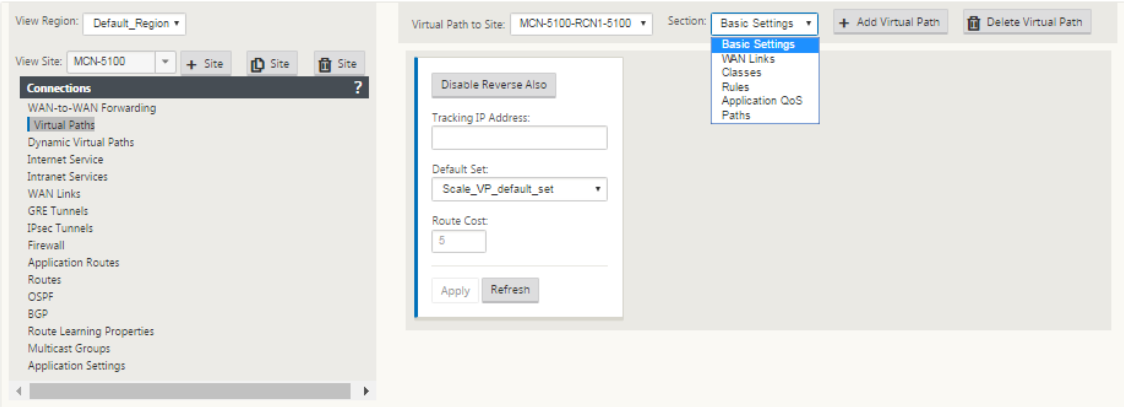
  各項目の意味は次の通りです:

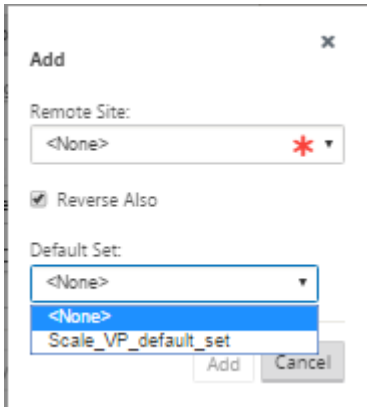
  MCN_Site_name は、この仮想 WAN の MCN の名前です。

  Branch_Site_Name は、現在の構成パッケージで識別されるクライアントサイトの名前です。

ユーザーが構成可能なデフォルト設定は、[接続] 構成ツリーの [仮想パス**] > [**デフォルトセット] セクションで定義されているように、最初は静的な仮想パスに適用されます。ただし、定義済みの デフォルトセットをカスタマイズしたり、追加したり、特定のサイトと仮想パスの構成をカスタマイズしたりできます。

> 注
>
> サイトの静的仮想パスを追加するには、手動で追加する必要があります。静的仮想パスを手動で追加する手順は、次の手順に記載されています。



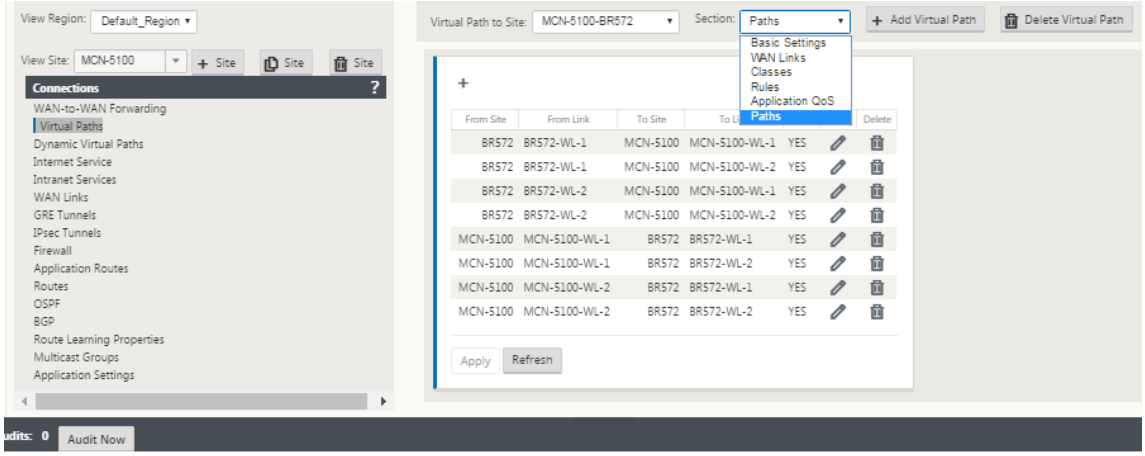


4. [仮想パス] セクションの静的仮想パスの名前の横にある **[+ ** 仮想パスの 追加 **]** をクリックします。これにより、スタティック仮想パスの設定が増えることが明らかになります。

   a) リモート・サイト：このセクションでは、リモート・サイトの観点から 仮想パスの 設定を表示および構成できます。この特定の仮想パスの必要に応じて、クラス または 規則 を表示、カスタマイズ、および追加できます。必要に応じて、仮想パスをリモートサイトに追加することもできます。
   b) **Reverse Aso-** 有効にすると、クラスとルールは両方のサイトで仮想パスでミラーリングされます。
   c) **Default Set**： サイト上の仮想パスのルールとクラスを設定するために使用される仮想パスのデフォルト・セットの名前。

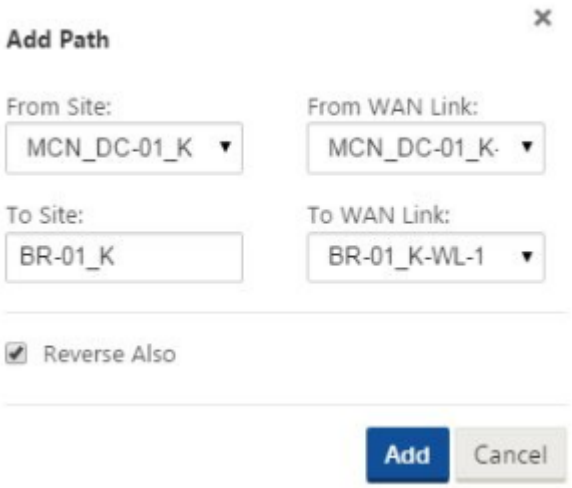
   次の図は、MCN 静的仮想パスブランチと子ブランチの例を示しています。

5. [断面] ドロップダウンメニューから [パス] を選択します。



6. [パス] テーブルの上の [**+**] (追加) をクリックします。

   [**Add Path**] ダイアログボックス (設定フォーム) が表示されます。



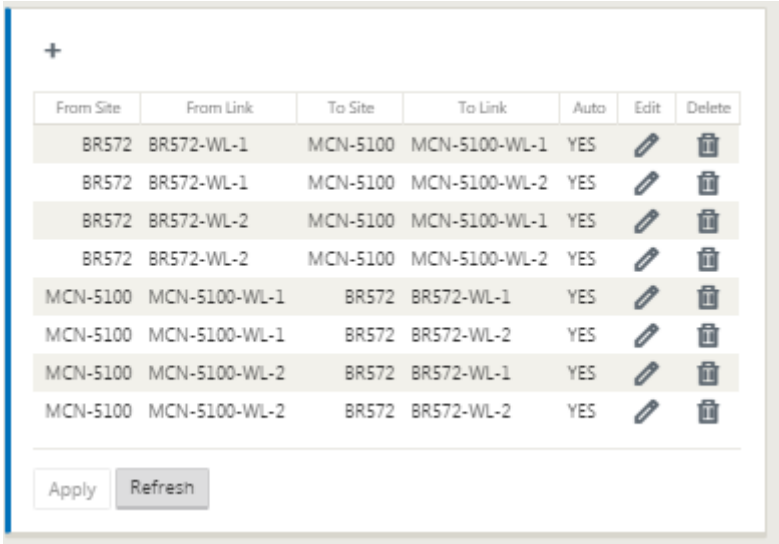
7. 新しい仮想パスのソース・サイトとデスティネーション・サイト情報を指定します。
8. 使用可能なドロップダウンメニューから次の項目を指定します。

   > 注
   >
   > サイトの WAN リンクの構成方法に応じて、一部のフィールドは読み取り専用です。設定可能なフィールドには、使用可能な選択項目のドロップダウンメニューが表示されます。

   - [**From Site**]: 仮想パスのソース・サイトです。必須の静的仮想パスの場合、これはデフォルトで MCN サイトとして設定されます。
   - **From WAN Link**： 仮想パスの発信元の WAN リンクです。
   - **[** 宛先]: 仮想パスのデスティネーション・サイトです。
   - 宛先 **WAN** リンク—仮想パスの宛先 WAN リンクです。

9. ［追加］をクリックします。

   これにより、構成済みの仮想パスが、**[接続] > [**仮想パス] ツリーの MCN および関連付けられたクライアントサイトの両方に追加されます。これにより、仮想パス (この場合は MCN) の [F **rom Site**] の [パス設定] 構成フォームも自動的に開きます。



From Site	From Link	To Site	To Link	Auto	Edit	Delete
BR572	BR572-WL-1	MCN-5100	MCN-5100-WL-1	YES		
BR572	BR572-WL-1	MCN-5100	MCN-5100-WL-2	YES		
BR572	BR572-WL-2	MCN-5100	MCN-5100-WL-1	YES		
BR572	BR572-WL-2	MCN-5100	MCN-5100-WL-2	YES		
MCN-5100	MCN-5100-WL-1	BR572	BR572-WL-1	YES		
MCN-5100	MCN-5100-WL-1	BR572	BR572-WL-2	YES		
MCN-5100	MCN-5100-WL-2	BR572	BR572-WL-1	YES		
MCN-5100	MCN-5100-WL-2	BR572	BR572-WL-2	YES		

Apply Refresh

10. ［MCN からクライアントへの仮想パス］ラベルの右側にある［編集］（鉛筆のアイコン）をクリックします。これにより、編集用の仮想パスサービス構成フォームが開きます。

11. 仮想パスの設定を構成するか、デフォルトをそのまま使用します。

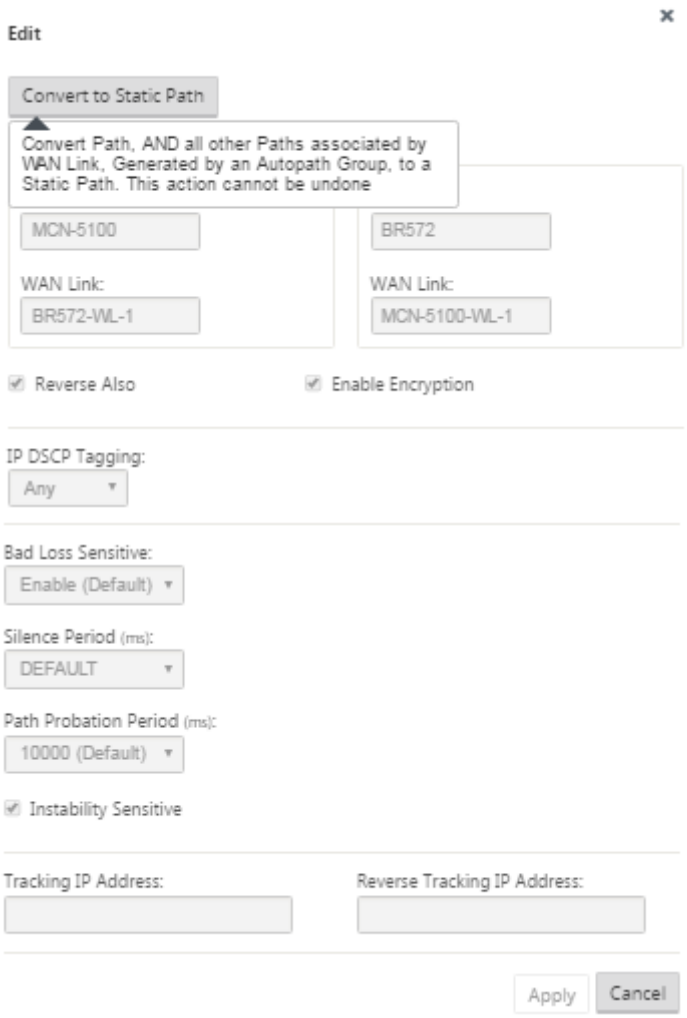
    パス 構成フォームには、次の設定が含まれています。

    - [サイト] セクションから:
      - サイト：仮想パスのソース・サイトです。必須の静的仮想パスの場合、これはデフォルトで MCN サイトとして設定されます。
      - **WAN** リンク：仮想パスの発信元の WAN リンクです。
    - 「サイト」セクション:
      - サイト：仮想パスのデスティネーション・サイトです。
      - **WAN** リンク：仮想パスの宛先 WAN リンクです。
    - リバース：この仮想パスに対して「リバース」を使用可能にするには、このチェックボックスを選択します。有効にすると、システムは元のパスに対して設定されたものと同じ WAN リンクを使用して、構成されたパスの反対方向に仮想パスを自動的に構築します。
    - [**IP DSCP** タグ付け] —ドロップダウンメニューからタグを選択します。これは、この仮想パスを通過するトラフィックの IP ヘッダーに設定する DSCP タグを指定します。
    - **Enable Encrypt** ion —この仮想パスに沿って送信されるパケットの暗号化を有効にするには、このチェックボックスを選択します。

- 不良損失に敏感 です—ドロップダウンメニューから設定を選択します。使用できるオプションは、次のとおりです:
  - **[Enable**]:（デフォルト）有効にすると、パスが失われたために **BAD** とマークされ、パススコアリングのペナルティが発生します。
  - **Disable** :
    Bad Loss Sens itive を無効にすると、帯域幅の損失が許容できない場合に便利です。
  - [**Cust** om]: パスを BAD としてマークするのに必要な経過時間の経過に伴う損失の割合を指定するには、[Custom] を選択します。このオプションを選択すると、さらに次の設定が表示されます。
    * **Percent Loss (%)** : パスが BAD とマークされるまでの損失しきい値の割合を指定します。指定した時間内に測定されます。デフォルトでは、パーセンテージは最後に受信した 200 個のパケットに基づきます。
    * [**Over Time (ms)**]: パケット損失を測定する期間 (ミリ秒単位) を指定します。このフィールドのドロップダウンメニューから、100 ～2000 のオプションを選択します。
  - 無音期間（**ms**）: パスの状態が **GO** OD から **BA**D に移行するまでの期間（ミリ秒単位）を指定します。

  デフォルトは 150 ミリ秒です。このフィールドのドロップダウンメニューから 150 ～1000 のオプションを選択します。
  - パス保護期間（ミリ秒）: パスが BAD から GOOD に移行するまでの待機時間（ミリ秒）を指定します。このフィールドのドロップダウンメニューから 500 ～6000 のオプションを選択します。デフォルトは 10,000 ミリ秒です。
  - 「不安定性の感受性」—有効にするには、このチェックボックスを選択します。有効の場合、パススコアリングアルゴリズムでは、パス状態が
    BA D とその他の遅延スパイクによる遅延ペナルティが考慮されます。
  - [**Tracking IP Add** ress]: 仮想パスに仮想 IP アドレスを入力します。この仮想 IP アドレスを入力すると、パスの状態を確認できます。
  - 逆トラッキング **IP** アドレス: 仮想パスに対して
    逆方向も 有効になっている場合は、ping 可能なパスに仮想 IP アドレスを入力します。このアドレスを入力すると、逆方向パスの状態を確認できます。

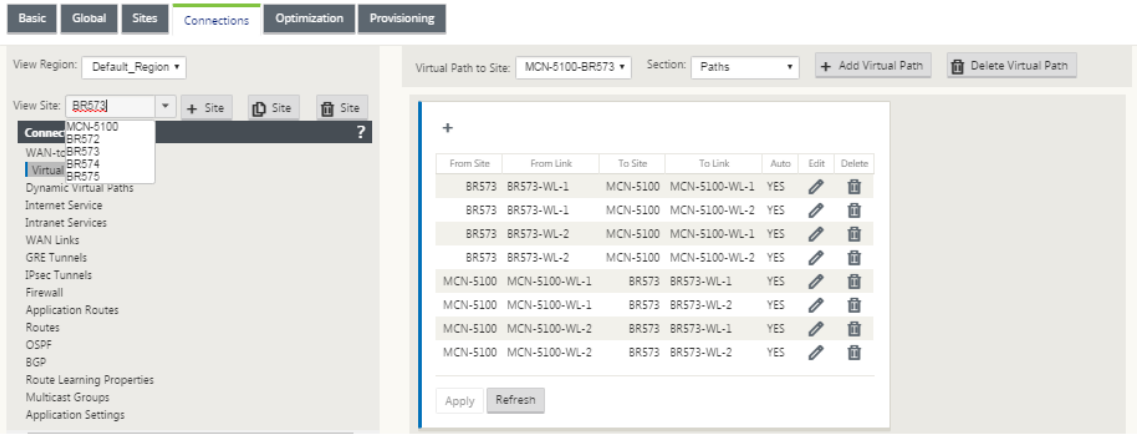
12. ［適用］をクリックします。これにより、MCN とクライアント サイト間の **2** つの新しい **FromS** ite および To Site の仮想パスが [Paths] テーブルに追加されたことがわかります。



13. MCN に接続するブランチごとに、上記の手順を繰り返します。

    次に、クライアントサイトの仮想パス構成をカスタマイズしたり、クライアント間のパスを追加および構成したりできます。手順については、以下の残りの手順で説明します。

14. [サイトの 表示] ドロップダウンメニューからクライアントサイトブランチを選択します。接続 ツリーでクライアントサイトブランチの構成が開きます。

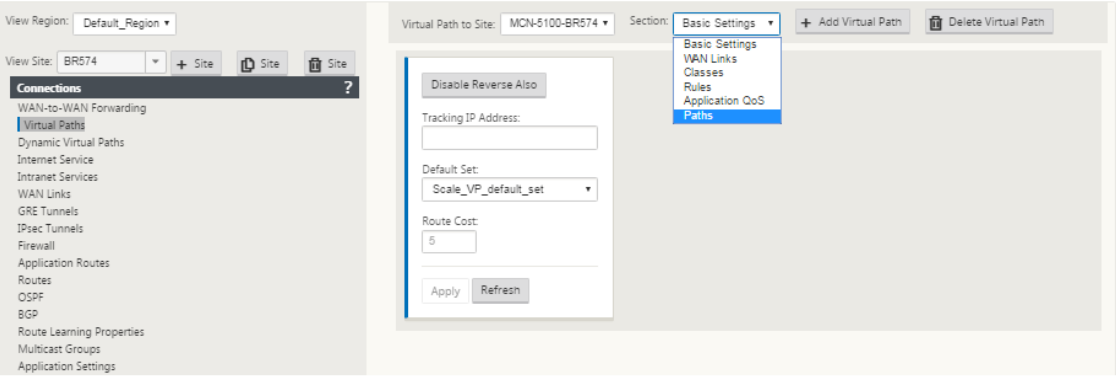


15. 構成するクライアントサイトの仮想 パス の [パス設定] 構成フォームに移動します。

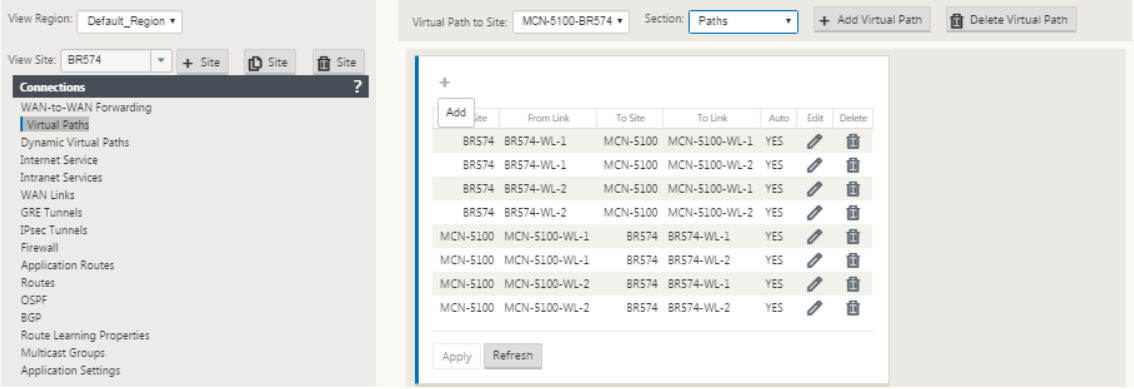
    クライアントサイトの [パス 設定] フォームに移動するには、次の操作を行います。

16. クライアントサイトのブランチページの [セクション] タブから [パス] を選択します。

    次の図は、前の手順で追加された新しいサイトからのパスのパス設定フォームの例を示しています。



17. カスタマイズする各パスの設定を構成します。MCN サイトの仮想パスを構成するのと同じ手順に従います。



これで、クライアントサイトと MCN 間の仮想パスの基本構成は完了です。

> 注
>
> 構成エディタの「接続」セクションまたは「プロビジョニング」セクションでその他の設定を構成する方法については、管理 Web インタフェースのオンライン・ヘルプを参照してください。これらの設定を現在設定したくない場合は、以下に示す適切な手順に進むことができます。

次の手順は、展開用にアクティブ化した SD-WAN エディションライセンスによって異なります。

- **SD-WAN** プレミアム（エンタープライズ）エディション—プレミアム（エンタープライズ）エディションには、WAN 最適化機能のフルセットが含まれています。サイトに WAN Optimization を設定する場合は、WAN Optimization の有効化と設定 トピックに進んでください。それ以外の場合は、直接 [クライアントへの SD-WAN アプライアンスパッケージのインストール] に進むことができます (/en-us/citrix-sd-wan/11/configuration/installing-virtual-wan-appliance-packages-clients.html)
- **SD-WAN** エディション—このエディションには、WAN Optimization 機能は含まれません。これで、直接 [クライアントへの SD-WAN アプライアンスパッケージのインストール] に進むことができます (/en-us/citrix-sd-wan/11/configuration/installing-virtual-wan-appliance-packages-clients.html)

MCN 設定のデプロイ

May 10, 2021

次の手順では、SD-WAN アプライアンスパッケージをクライアントノードに配布できるように準備します。これには、次の 2 つの手順が含まれます。

1. 構成パッケージを変更管理にエクスポートします。

   アプライアンス・パッケージを生成する前に、構成 エディタから **MCN** 上のグローバル変更管理ステージング受信トレイに完成した構成 パッケージをエクスポートする必要があります。手順については、「変更管理の実行」セクションに記載 されています。

2. アプライアンス・パッケージを生成およびステージングします。

   新しい構成パッケージ を変更管理 受信トレイに追加したら、アプライアンスパッケージを生成してステージングできます。これを行うには、MCN 上の 管理 **Web** インターフェイスで **[**変更 管理] ウィザードを使用します。手順については、セクションを参照してください。構成をブランチに配備します。

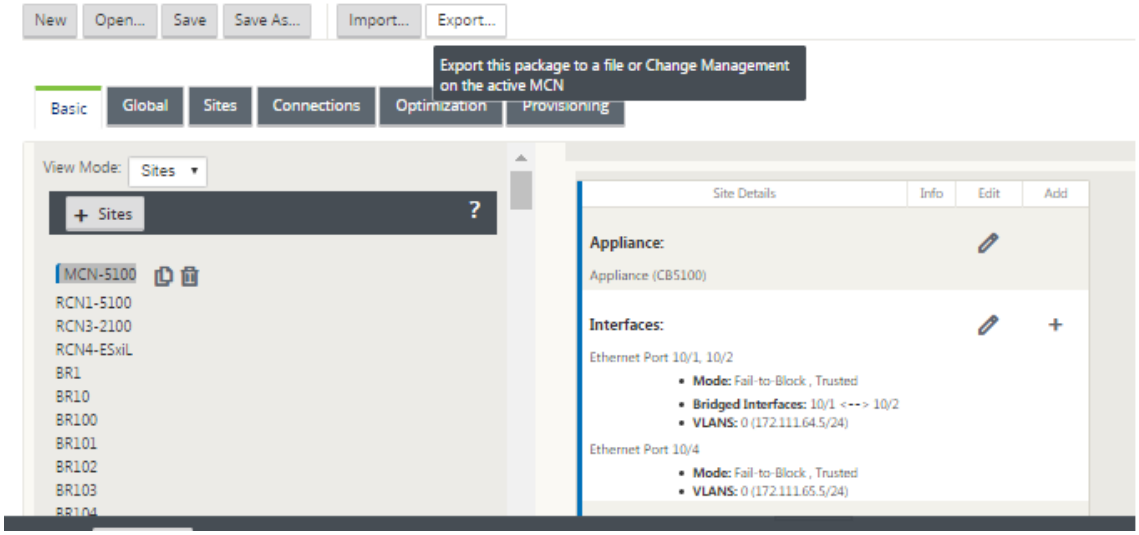
MCN 変更管理の実行

May 10, 2021

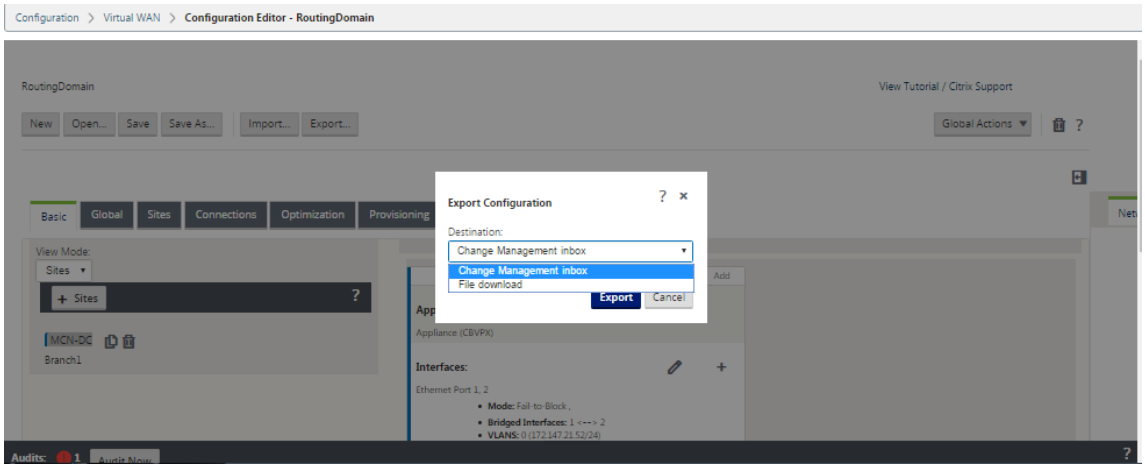
アプライアンス・パッケージを生成する前に、完成した構成パッケージを管理 Web Interface 変更管理 システムにエクスポートする必要があります。

構成パッケージ を変更管理にエクスポートするには、次の手順を実行します。

1. [構成エディタ] ページで、[エクスポート] (ページ上部にある) をクリックします。



これにより、[設定のエクスポート] ダイアログボックスが開きます。



2. エクスポート先として「変更管理の 受信トレイ」を選択します。[D **estination**] フィールドのドロップダウンメニューを使用して、選択を行います。

3. [エクスポート] をクリックします。

エクスポート操作が完了すると、ページの上部に緑色の成功ステータスメッセージが表示されます。

> ヒント
>
> 成功メッセージにある青い「変更管理」リンクをクリックすると、変更 管理 ウィザードの「変更準備 - ファイルのアップロードと確認」ページ（2 ページ）に直接移動できます。構成プロセスの次のステップを実行するに

> は、このページに移動する必要があります。ただし、成功メッセージは数秒間しか表示されません。その後、ナビゲーションツリーを使用してウィザードを開き、このページに進んでください。手順は次のセクションで説明します。

これで、SD-WAN ソフトウェアパッケージを MCN アプライアンスにアップロードし、クライアントノードに配布するアプライアンスパッケージを準備する準備が整いました。

ブランチへの構成のデプロイ

May 10, 2021

構成エディタを使用して構成を準備し、構成パッケージを変更管理の受信ボックスにエクスポートしたら、次の手順で SD-WAN アプライアンスパッケージをクライアントノードに配布できるように準備します。MCN 上の 管理 **Web** インターフェイスで、変更 管理ウィザードを使用します。

SD-WAN アプライアンスモデルごとに異なる SD-WAN ソフトウェアパッケージがあります。アプライアンス・パッケージは、展開する構成パッケージにバンドルされた、特定のモデルのソフトウェア・パッケージで構成されます。したがって、ネットワーク内のアプライアンス・モデルごとに異なるアプライアンス・パッケージを用意し、生成する必要があります。

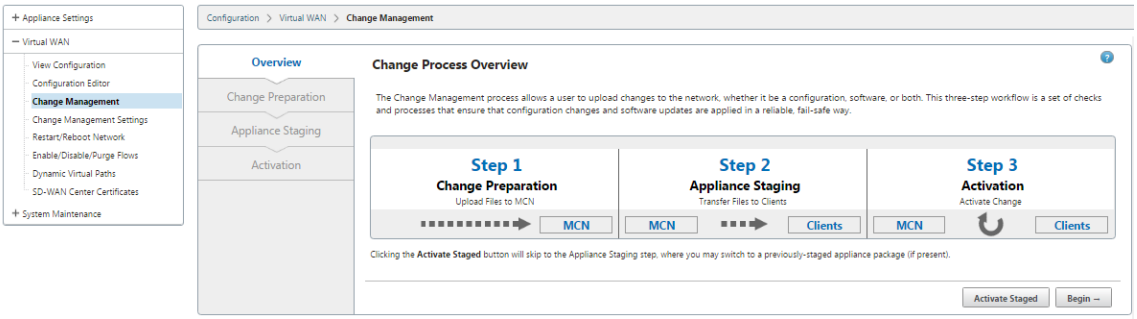
> 注
>
> 必要な SD-WAN ソフトウェアパッケージをネットワークに接続されている PC にまだダウンロードしていない場合は、ここでダウンロードできます。ソフトウェアの取得とダウンロードについては、「SD-WAN ソフトウェアパッケージの取得」を参照してください。

パッケージと設定を MCN にアップロードしてインストールするには、次の手順を実行します。

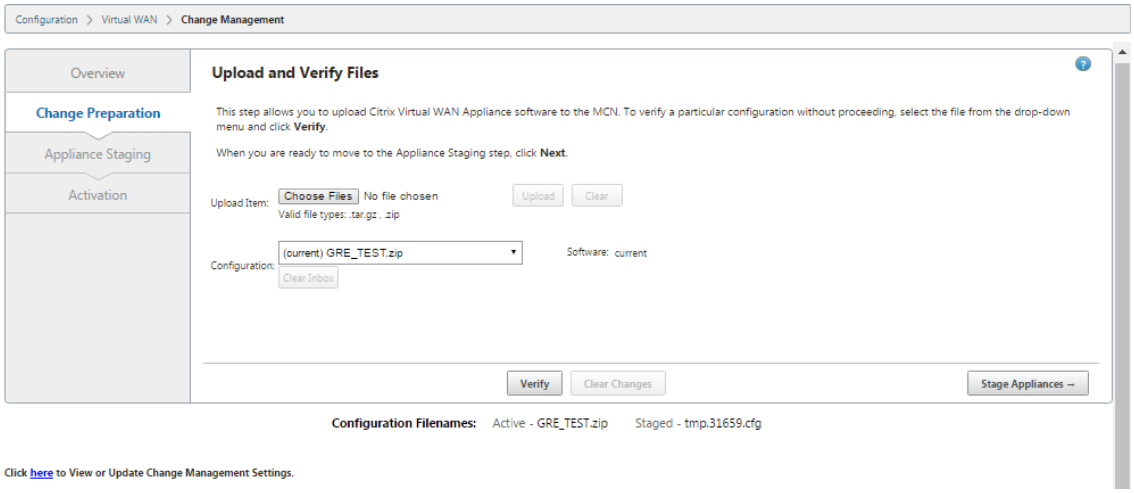
1. MCN アプライアンスの管理 Web インターフェイスにログインします。

   > 注
   >
   > 接続された PC に以前にダウンロードしたソフトウェアパッケージをアップロードしています。便宜上、この同じ PC を使用して MCN に再度接続することもできます。

2. ［構成］タブを選択します。
3. 左側のペインで、[仮想 **WAN**] セクションを開き、[変更管理] を選択します。変更管理 ウィザードの最初のページである「変更プロセスの概要」ページが表示されます。



4. [開始] をクリックします。指定した構成およびソフトウェアパッケージが表示されることをアップロードおよび確認するための [**Change Prepar** ation] ページです。



5. ネットワークに必要な各 SD-WAN ソフトウェアパッケージをアップロードします。
   展開する SD-WAN ソフトウェアパッケージごとに、次の手順を実行します。

   a)「アイテムの アップロード」フィールドの 横にある「ファイルを選択」をクリックします。アップロードする SD-WAN ソフトウェアパッケージを選択するためのファイルブラウザが開きます。

   b) SD-WAN ソフトウェアパッケージを選択し、[**OK]** をクリックします。

   c) 以前にローカル PC にダウンロードした SD-WAN ソフトウェアパッケージに移動し、アップロードするパッケージを選択します。

   d) [アップロード**]** をクリックします。

   e) ネットワークに必要な各 SD-WAN ソフトウェアパッケージについて、手順 (i) ～(iii) を繰り返します。

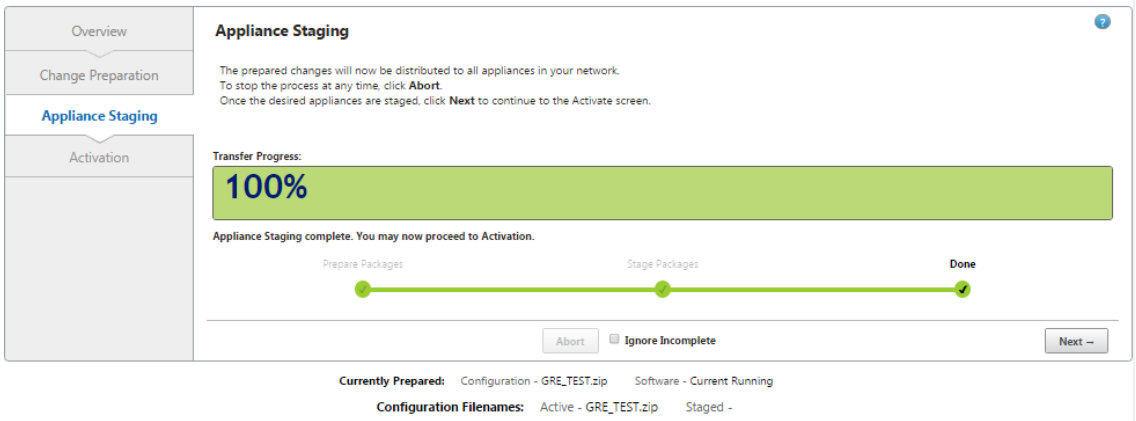
6.「構成」フィールドのドロップダウンメニューで、変更管理にエクスポートした新しい構成パッケージを選択します。

7. アプライアンスのステージをクリックします。アプライアンスのステージングでは、次のアクションが開始されます。

   - 選択したソフトウェアパッケージと設定を MCN に転送します。

- 選択した構成で識別される各アプライアンス・モデルに対して、アプライアンス・パッケージを生成します。
- 新しいアプライアンス・パッケージを、サイト・アプライアンス・テーブルで使用可能なパッケージのリストに追加します。
- 新しい設定と適切なソフトウェアパッケージを MCN にステージングします。

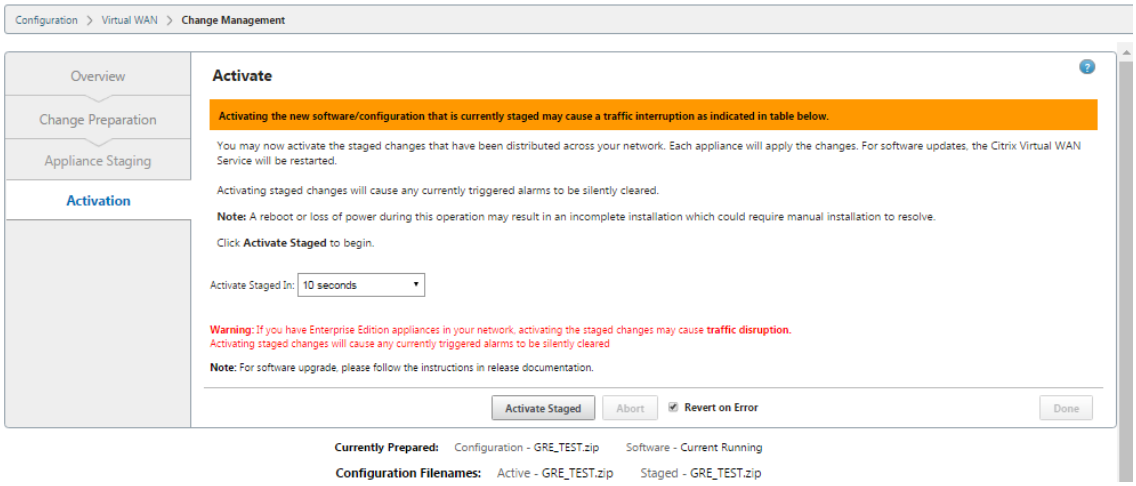
8. ［次へ］をクリックします。「アプライアンスのステージング」ページに進みます。



ステージング操作が完了すると、Site-Appliance** テーブルに、新しくステージングされたアプライアンス・パッケージ情報が入力されます。

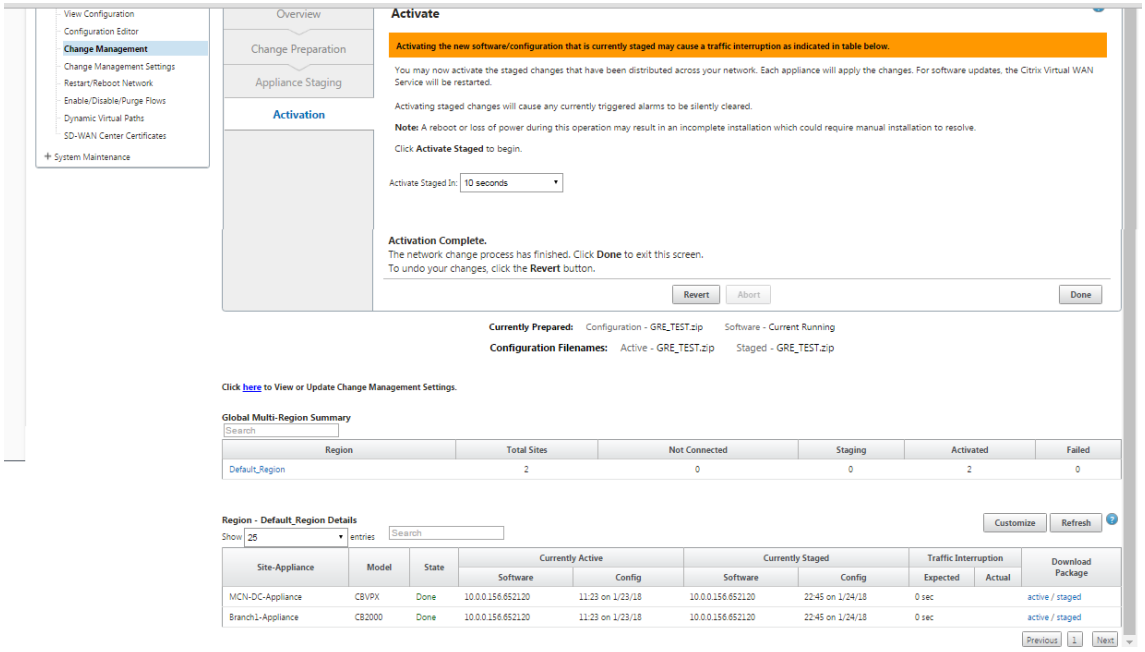
> 注
>
> これが初期展開の場合、MCN のみが更新され、ステージングされます。既存の展開を更新していて、展開されたサイト間で仮想パスがすでに機能している場合は、展開されたクライアントノードに適切なアプライアンスパッケージが配布され、それらのノードでステージングが開始されます。ただし、既存の Virtual WAN 展開に新しいクライアント・ノードを追加する場合は、この手順の残りの手順で説明するように、新しいクライアントごとに適切な Appliance パッケージを手動でアップロード、ステージングおよびアクティブ化する必要があります。
>
> ネットワークにサイトを追加する場合、またはサイトが接続されていない状態の場合は、[不完全無視] を選択します。これは、接続されているサイトと MCN だけが更新され、ステージングされることを示します。接続されていない状態にあったサイトがオンラインに戻ると、自動修正の一環として MCN によって自動的にステージングおよび更新されます。

9. エラーが発生したときに以前のアプリケーションパッケージに戻すには、**[** エラー時に元に戻す] を選択します。詳細については、「構成のロールバック」を参照してください。
10. [ステージングを有効化] をクリックします。



この時点の結果と次のステップは、これが初期構成であるか、既存の構成を更新または置き換えるかによって、次のように異なります。

- 既存の配置の設定を更新または変更する場合。
  - これが初期構成でない場合は、MCN アプライアンスの新しい構成と適切なアプライアンスパッケージがアクティブになります。その後、適切なアプライアンスパッケージが SD-WAN 内の各クライアントに配布され、自動的にアクティブ化されます。この処理が完了するまで数秒かかることがあります。



アクティベーションが完了すると、[アクティベーション完了] ステータスメッセージが表示され、[完了] ボタンが有効になります。さらに、表の上にある [**Configuration Filenames]** ステータス行 **(Configuration Filenames**) の [**Active]** フィールドに、新しくアクティブ化されたパッケージの名前が表示されるようになりました。

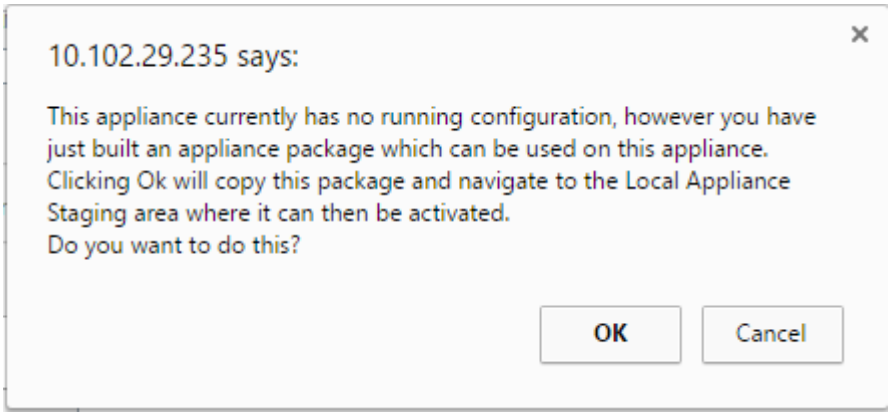
11. [完了] をクリックし、次のいずれかの操作に進みます。

    - SD-WAN に新しいノードを追加しない場合は、SD-WAN 内の新しいアプライアンス・パッケージの準備、配布、アクティベーションが完了します。仮想 WAN サービスの有効化に直接進むことができます。
    - SD-WAN に新しいクライアントノードを追加する場合は、「クライアントアプライアンスのネットワークへの接続」を参照してください。

    -初期構成をアクティブ化 する場合、新しい構成パッケージはこの時点ではアクティブ化されず、さらに実行する必要がある手順があります。次の手順では、構成パッケージをローカルアプライアンスのステージング領域にコピーし、MCN 上で構成パッケージをステージングおよびアクティブ化するための準備を行います。

    以下を実行します:

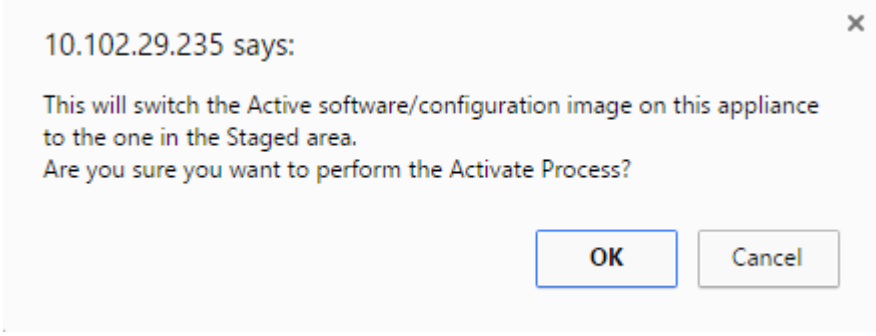
12. [ステージのアクティブ化] をクリックすると、次のメッセージが表示されます。

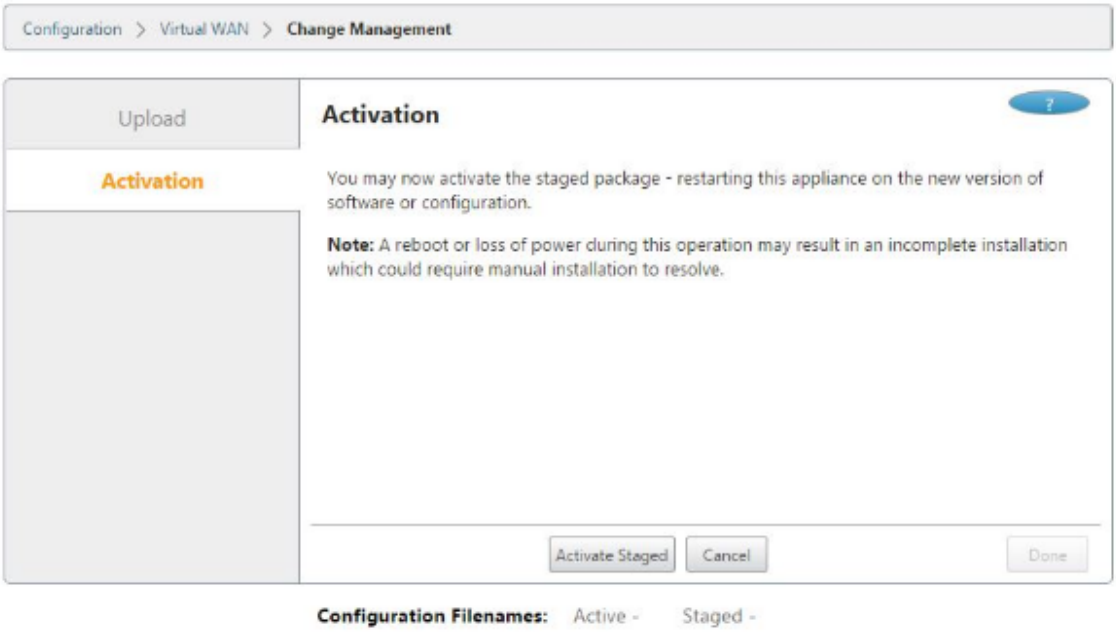


13. [**OK**] をクリックします。

14. [ステージングされたアクティブ化] をクリックします。

    これにより、アクティベーション操作の確認を求めるダイアログボックスが表示されます。





15. ［**OK**］をクリックします。

    これにより、ステージングされた構成パッケージのアクティブ化が開始されます。この処理には数秒かかります。この間、進捗状況メッセージが表示されます。

    アクティベーションが完了すると、アクティベーションが完了したことを示すステータスメッセージが表示され、[完了] ボタンが有効になります。

16. ［完了］をクリックします。これにより、[管理 Web Interface **Dashboard**] ページに進み、アクティブ化の結果を表示できます。

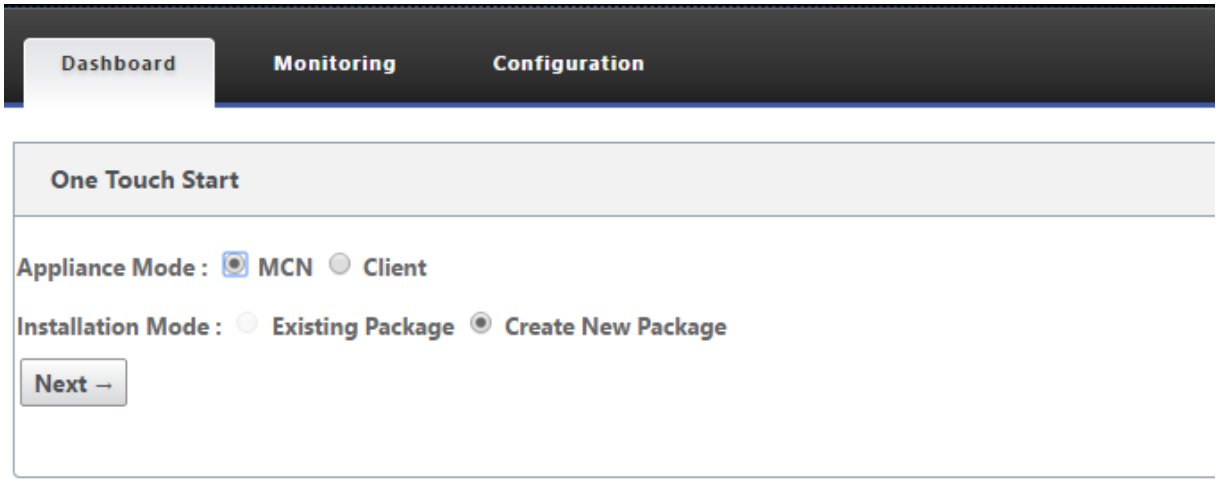
これで、MCN での SD-WAN アプライアンスパッケージの準備が完了しました。クライアントアプライアンスのネットワークへの接続に進みます。

> ヒント
>
> 変更管理 ウィザードでは、サイト・アプライアンスのテーブルを検索できます。これにより、複数のサイトがある大規模なネットワーク上のサイトを検索し、必要な段階的な構成をダウンロードできます。エラー状態を検索することもできます。たとえば、「失敗」や「未接続」などです。これにより、その状態にあるすべてのサイトのリストが表示されます。

ワンタッチスタート

May 10, 2021

タッチスタートにより、初回起動時に SD-WAN アプライアンスをクライアントとして簡単かつ迅速に構成できます。アプライアンスを初めて起動すると、ワンタッチ起動オプションが表示されます。



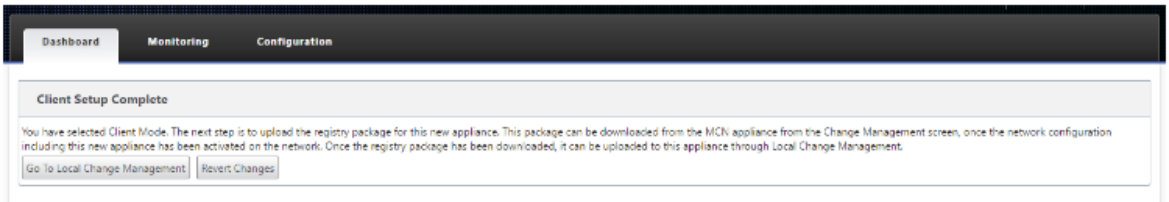
> 注
>
> SD-WAN アプライアンスを MCN として設定するには、構成 エディタを使用して構成を作成するか、既存の構成をインポートします。詳細については、「MCN での SD-WAN アプライアンスパッケージの準備」を参照してください。

既存の構成ファイルを使用して SD-WAN アプライアンスをクライアントとして設定するには、次の手順を実行します。

1. アプライアンスモードとして [クライアント] を選択します。
2. [既存のパッケージ インストールモード] を選択します。管理者は、MCN の既存のパッケージを利用するために MCN の設定を定期的に保存する必要があります。
3. [ファイルの選択] をクリックして、ローカルコンピュータから構成パッケージを選択します。
4. [アップロードとインストール] をクリックします。

ローカル変更管理を使用して SD-WAN アプライアンスをクライアントとして設定するには、以下の手順に従ってください。

1. アプライアンスモードとして [クライアント] を選択します。
2. [**Create New Package**] を選択して、ローカル変更管理を使用してこのアプライアンスの構成パッケージをアップロードします。パッケージは、変更管理画面から MCN アプライアンスからダウンロードできます。
3. [次へ] をクリックします。
4. [ローカル変更管理に移動] をクリックします。



トピッククライアントへの SD-WAN アプライアンスパッケージのインストールの手順に従います。

クライアントアプライアンスのネットワークへの接続

May 10, 2021

初期展開の場合、または既存の SD-WAN にクライアントノードを追加する場合、次の手順は、ブランチサイト管理者がクライアントアプライアンスをそれぞれのブランチサイトのネットワークに接続することです。これは、適切な SD-WAN アプライアンスパッケージをクライアントにアップロードおよびアクティブ化する準備です。各ブランチサイト管理者に接続して、これらの手順を開始および調整してください。

サイトアプライアンスを SD-WAN に接続するには、サイト管理者は次の操作を行う必要があります。

1. まだクライアントアプライアンスをセットアップしていない場合は、クライアントアプライアンスをセットアップします。

   SD-WAN に追加するアプライアンスごとに、次の操作を行います。

   a) SD-WAN アプライアンスハードウェアと、展開する SD-WAN VPX 仮想アプライアンス（SD-WAN VPX-SE）をセットアップします。
   b) アプライアンスの管理 IP アドレスを設定し、接続を確認します。
   c) アプライアンスの日付と時刻を設定します。コンソールセッションタイムアウトしきい値を高い値または最大値に設定します。
   d) アプライアンスにソフトウェアライセンスファイルをアップロードしてインストールします。

2. アプライアンスをブランチサイトの LAN に接続します。イーサネットケーブルの一端を SD-WAN アプライアンスの LAN 用に設定されたポートに接続します。次に、ケーブルのもう一方の端を LAN スイッチに接続します。

3. アプライアンスを WAN に接続します。イーサネットケーブルの一端を SD-WAN アプライアンスの WAN 用に設定されたポートに接続します。次に、ケーブルのもう一方の端を WAN ルータに接続します。

次のステップは、ブランチサイト管理者がそれぞれのクライアントに適切な SD-WAN アプライアンスパッケージをインストールしてアクティブ化することです。

クライアントへの **SD-WAN** アプライアンスパッケージのインストール

May 10, 2021

アプライアンスパッケージを準備し、MCN を接続し、ブランチサイト管理者がそれぞれのクライアントアプライアンスを LAN および WAN に接続したら、次のステップは、各クライアントで適切な SD-WAN アプライアンスパッケージをアップロードしてアクティブ化することです。変更管理ウィザードの指示に従って、このプロセスを実行します。

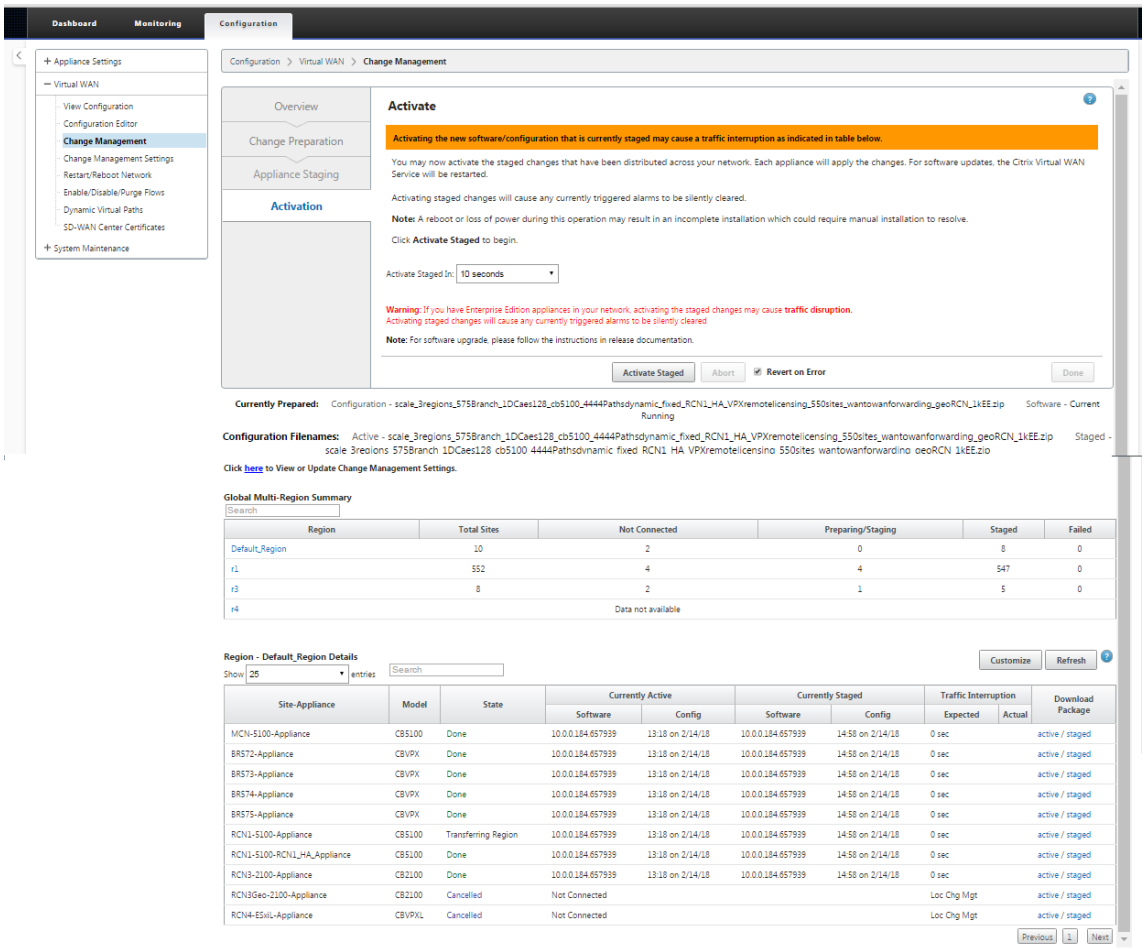
クライアントアプライアンスにソフトウェアと構成をインストールしてアクティブ化するには、次の手順に従います。

1. 接続されている PC でブラウザを開き、MCN アプライアンスの管理 Web インターフェイスにログオンします。

   ブラウザアドレスフィールドに MCN の管理 IP アドレスを入力します。これにより、MCN アプライアンスの管理 Web インターフェイス ダッシュボード ページが表示されます。

2. [構成] タブを選択します。左側のナビゲーションペインで、[**Virtual WAN**] を選択し、[変更管理] を選択します。

   これにより、「変更プロセスの概要」ページ (「変更管理」ウィザードの最初のページ) が表示されます。



このページの下部には、個々のサイトとアプライアンスを一覧表示する表が表示されます。「パッケージのダウンロード」列の表の右端には、アクティブ（使用可能な場合）および ステージングされたパッケージへのリンクがあります。

Traffic Interruption		Download Package
Expected	Actual	
0 sec		active / staged
Loc Chg Mgt		active / staged

> 注
>
> これが初期インストールの場合、アクティブ リンクはまだ利用できず、プレーンテキストマーカー **none** に置き換えられます。

3. ダウンロードするパッケージの [**Staged**] リンクをクリックします。

   [**Site-Appliance**] テーブルで、サイト・アプライアンスのエントリを探し、そのエントリの [**Download Package**] 列にある [**Staged**] リンクをクリックします。(ローカル PC 上の) ダウンロード場所を選択するためのファイルブラウザが表示されます。

4. ダウンロード場所を選択し、[**OK]** をクリックします。

5. （オプション）ダウンロードが完了したら、MCN 管理 Web インターフェイスからログアウトします。

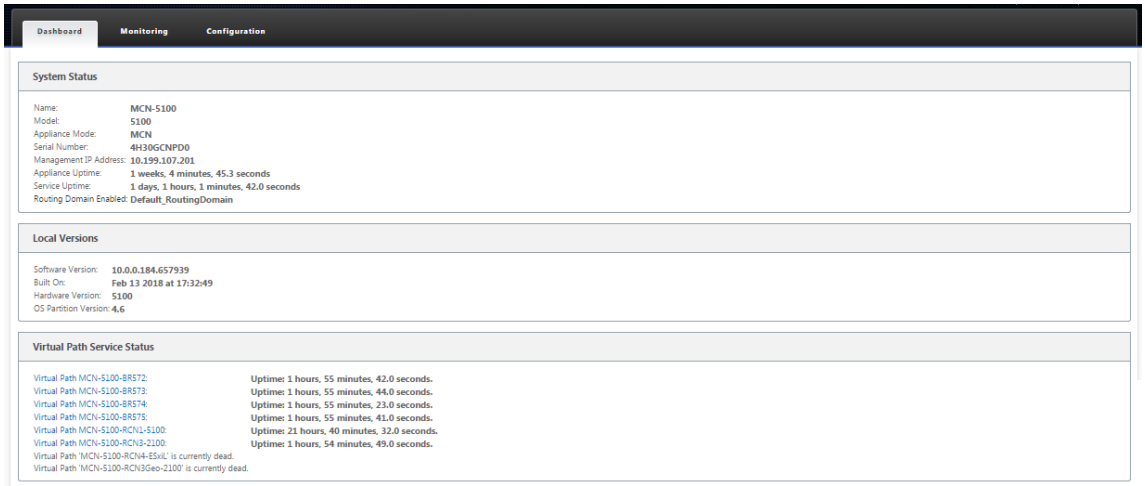
6. ブラウザを開き、アプライアンス・パッケージの.zip ファイルをアップロードするクライアントの IP アドレスを入力します。

   > 注
   >
   > 管理 Web インターフェイスのブラウザ証明書の警告は無視してください。

   これにより、クライアントアプライアンスの［Citrix SD-WAN 管理 Web インターフェイスのログイン］画面が開きます。

7. 管理者のユーザー名とパスワードを入力し、[ログイン] をクリックします。デフォルトの管理者ユーザー名は *admin* です。デフォルトの パスワードは *password* です。

   これにより、クライアントアプライアンスの [管理 Web インターフェイス ダッシュボード] ページが表示されます。

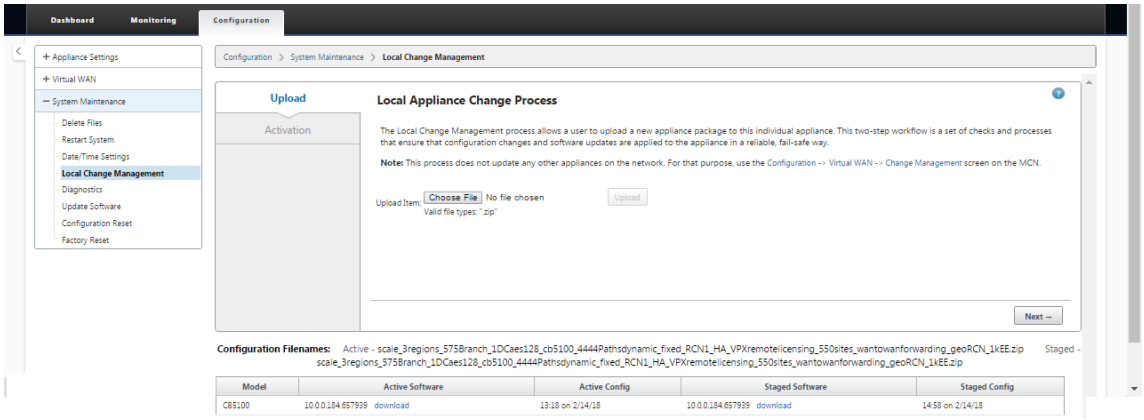


> 注
>
> これが初期インストールの場合、またはこのアプライアンスで仮想 WAN サービスを一時的に無効にした場合は、仮想 WAN サービスが非アクティブまたは無効であることを示すステータスメッセージと共

> に、金色の監査アラートアイコンが表示されます。現時点では、このアラートは無視できます。アラートは、インストールが完了した後、手動でサービスを開始するまで [ダッシュボード] ページに残ります。

8. ［構成］タブを選択します。
9. ナビゲーション・ツリー（左ペイン）で「システムメンテナンス」ブランチを開き、「ローカル変更管理」を選択します。

   アプライアンスパッケージをアップロードするための「ローカルアプライアンスの変更プロセスのアップロード」ページが表示されます。

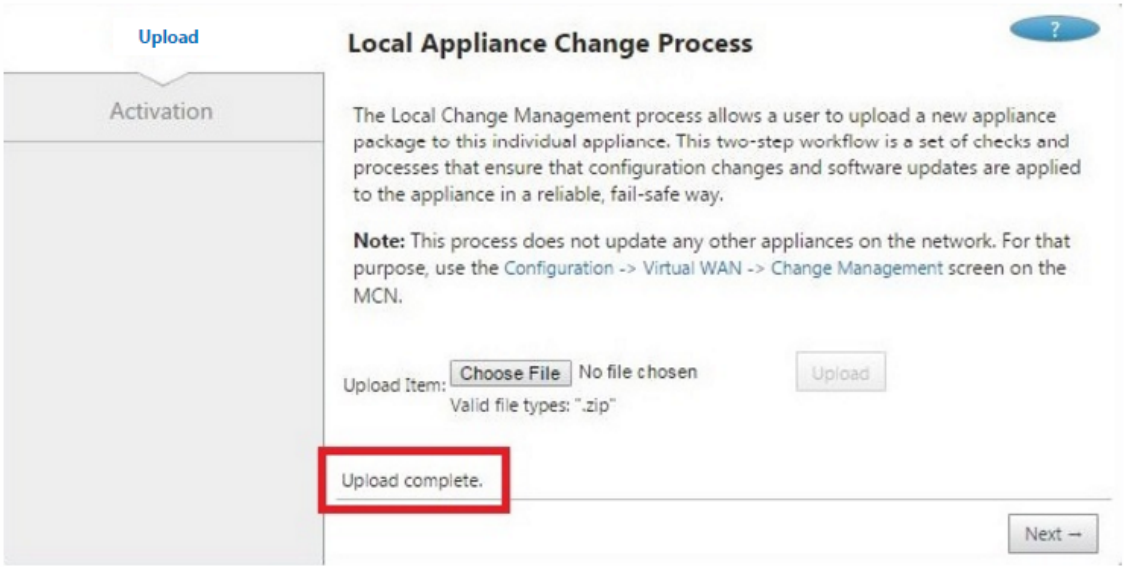


10. 「商品をアップロード」ラベルの横にある 「ファイルを選択」をクリックします。

    これにより、クライアントにアップロードするアプライアンス・パッケージを選択するためのファイル・ブラウザが開きます。

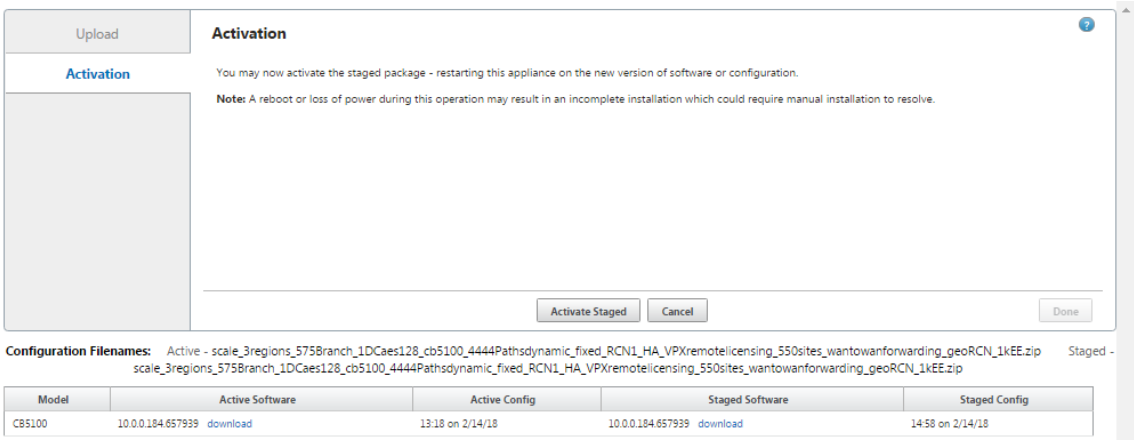
11. MCN からダウンロードした SD-WAN アプライアンスパッケージの zip ファイルに移動して選択し、[**OK**] をクリックします。
12. ［アップロード］をクリックします。

    アップロード処理が完了するまで数秒かかります。完了すると、アップロードが完了したことを示すステータスメッセージ **(**ページの左中央**)** が表示されます。



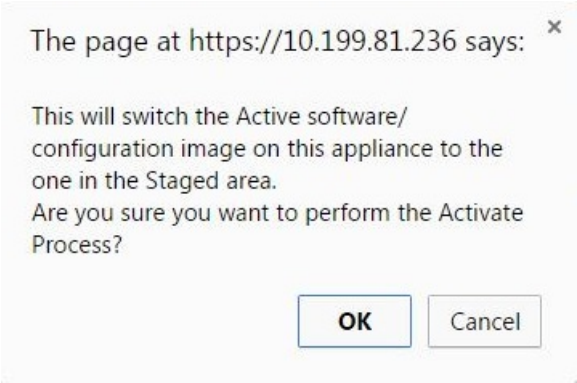
13. ［次へ］をクリックします。

指定したソフトウェアパッケージがアップロードされ、[ローカル変更管理の アクティブ化] ページが表示されます。



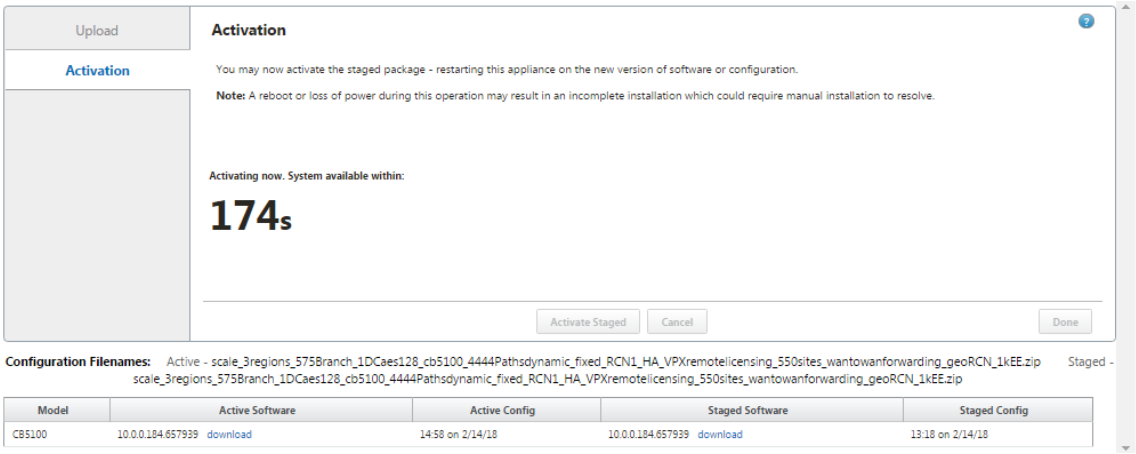
14. [ステージングを有効化] をクリックします。

これにより、アクティブ化操作の確認を求めるダイアログボックスが表示されます。

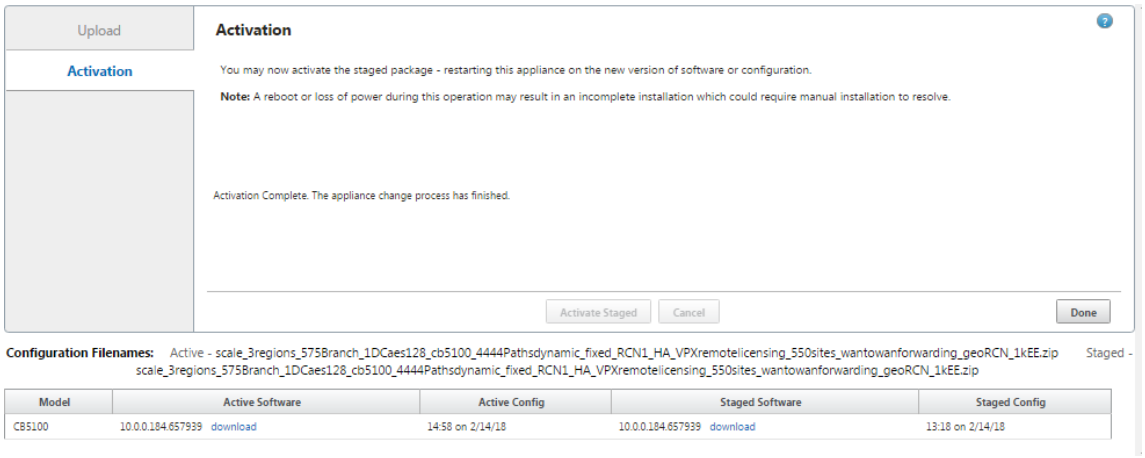


15. [**OK**] をクリックします。

これにより、新しくインストールされたパッケージがアクティブになり、初期展開でない場合は、クライアントアプライアンスで仮想 WAN サービスが起動します。この処理には数秒かかります。この間、進捗状況メッセージが表示されます。



アクティベーションが完了すると、アクティベーションが完了したことを示すステータスメッセージが表示され、[完了] ボタンが使用可能になります。

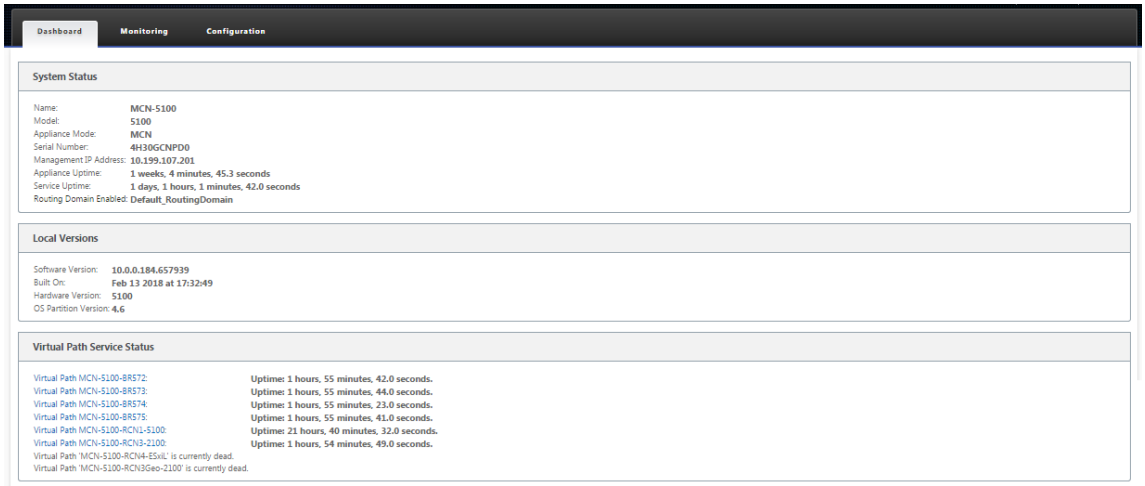


16. [完了] をクリックしてウィザードを終了し、アクティベーション結果を表示します。

アクティベーションが完了したら、**[**アクティベーション**]** ページの **[**** 完了] をクリックして、[管理 Web Interface ダッシュボード] ページに戻ります。**

これが初期展開でない場合、このページには、現在アクティブなバージョンのソフトウェアパッケージ、OS パーティション、および仮想パスのステータスに関する更新された情報が表示されます。これが初期インストールの場合、「監査アラート」アイコンと、Virtual WAN サービスが非アクティブまたは無効であることを示すステータスメッセージが表示されます。この場合、仮想 WAN サービスの有効化の説明に従って、サービスを手動で有効にする必要があります。

次の図は、アラート・アイコンとステータス・メッセージを表示するクライアントの ダッシュボード・ページのサンプルを示しています。



SD-WAN の初期展開を完了するための最後の手順は、仮想 WAN サービスを有効にすることです。手順については、「仮想 WAN サービスの有効化」セクションに記載 されています。

デプロイメント

May 10, 2021

Citrix SD-WAN アプライアンスを使用して実装されるユースケースシナリオを次に示します。

- ゲートウェイモードでの SD-WAN の導入
- インラインモード
- PBR モードでの SD-WAN の導入（仮想インラインモード）
- ブランチ間通信の動的パス
- WAN から WAN への転送
- SD-WAN ネットワークの構築
- LAN セグメンテーションのルーティング
- Premium（エンタープライズ）エディションのアプライアンスを利用して、WAN 最適化サービスのみを提供する
- 2 ボックスモード
- ゼロタッチ展開
- 単一リージョン展開
- 複数リージョン展開
- 高可用性

チェックリストと展開方法

May 10, 2021

仮想 WAN の概念と配置を計画するためのガイドラインについては、Citrix 仮想 WAN 展開計画ガイドを参照してください。

展開の準備

SD-WAN Standard Edition と Premium （Enterprise）Edition を展開する手順と手順を次に示します。

デプロイメントのユースケースの一部を表示するには、「デプロイ」を参照してください。

1. Citrix SD-WAN 展開情報を収集します。
2. Citrix SD-WAN アプライアンスをセットアップします。
   - SD-WAN 展開に追加するハードウェアアプライアンスごとに、次のタスクを完了する必要があります。
     - アプライアンスのハードウェアを設定します。
     - アプライアンスの管理 IP アドレスを設定し、接続を確認します。
     - アプライアンスの日付と時刻を設定します。
     - （任意）コンソールセッションの タイムアウト 間隔を高い値または最大値に設定します。
3. アプライアンスにソフトウェアライセンスファイルをアップロードしてインストールします。

インストールと構成のチェックリスト

展開する各 SD-WAN サイトについて、次の情報を収集します。

- ご使用の製品のライセンス情報
- デプロイする各アプライアンスの必要なネットワーク IP アドレス:
  - 管理 IP アドレス
  - 仮想 IP アドレス
  - サイト名
  - アプライアンス名（サイトごとに 1 つ）
  - SD-WAN アプライアンスモデル（デプロイする各アプライアンス用）
  - 展開モード（MCN またはクライアント）

- トポロジ
- Gateway MPLS
- GRE トンネル情報
- ルート
- VLAN
- 各回線の各サイトの帯域幅

ベストプラクティス

May 10, 2021

この記事では、Citrix SD-WAN ソリューションの導入のベストプラクティスについて説明します。以下の Citrix SD-WAN 展開モードの一般的なガイダンス、利点、ユースケースについて説明します。

Edge/Gateway モード

推奨事項

ゲートウェイモードの展開に関する推奨事項を次に示します。

1. ゲートウェイモードは、ルータの統合が実行され、お客様が SD-WAN をエッジデバイス終端接続にできる状態にある SD-WAN 支店に最適です。
2. プロジェクトをゼロから構築すると、優れたネットワークアーキテクチャを綿密な設計でレンダリングすることができます。

> 注:
>
> ゲートウェイモードは、インフラストラクチャが一部の中断を伴う既存のプロジェクトに対して、データセンター側で使用できます。

アドバンテージ/ユースケース

ゲートウェイモード展開の利点と使用例を次に示します。

1. 顧客支社でのルータ/ファイアウォール/ネットワーク要素の統合に最適な使用例
2. DHCP によるシンプルで簡単な LAN ホスト管理。

    - SD-WAN をネクストホップにして、データポート用のすべての LAN ホストに DHCP ベースの IP アドレッシングを提供できるようにします。

3. すべての接続は SD-WAN エッジ/ゲートウェイで終了し、管理が容易になります。
4. SD-WAN はエッジルーティングの焦点であり、すべてのトラフィックを操舵します。帯域幅/容量のアカウンティングを含め、ブレークアウト、バックホール、またはオーバーレイにエッジ上で決定が行われます。
5. LAN ホストとしてのすべての LAN サブネットホストは、SD-WAN LAN VIP をネクストホップとして使用できます。SD-WAN LAN がコアスイッチに接続されている場合は、ダイナミックルーティングを実行して、すべての LAN サブネットを可視化できます。
6. 高可用性（HA）のための優れた柔軟性-サイトがアクティブ/スタンバイモードで動作するように、Gateway モードに対する厳格な推奨事項。また、SD-WAN デバイスがダウンした場合のトラフィックのブラックホールを防ぐのに役立ちます。

    - ブランチで使用可能なスイッチ-パラレル高可用性は、Gateway モードで動作します。
    - ブランチでは使用できないスイッチ-SD-WAN は、SD-WAN エッジ高可用性モード（フェールツーワイヤ高可用性モード）でも動作できます。このモードでは、2 つの SD-WAN ボックスがデイジーチェーン接続され、フェールツーワイヤポートを使用してコンバージド高可用性ペアとして機能します。

7. インターネットを **UNTRUSTED** インターフェイスとして定義できます。これにより、ブレークアウト用のダイナミック NAT が自動的に作成され、接続元 NAT によって応答が SD-WAN に戻されます。
8. 4980 上の ICMP/ARP/UDP 制御パケットだけが許可されるという点では、信頼できないインターフェイスに対するセキュリティ上の考慮事項は当然暗黙的に示されています。

注意事項

ゲートウェイモードで注意する必要がある情報は、次のとおりです。

- 慎重な設計とネットワークアーキテクチャ -ゲートウェイモードでは、ブランチ/エッジネットワーク全体が SD-WAN にあるため、慎重な設計とネットワークに関する考慮事項が必要になる場合があります。ブロックするもの、ルーティングするもの、ネットワーク LAN の方法、WAN の終端方法など。
- デバイスの障害 -エッジモードでは、Failto Wire 機能を使用できません。デバイスがダウンすると、ブランチ全体がダウンします。
- セキュリティポスチャー -ルーティングはエッジで管理されるため、ファイアウォール、ブレークアウト/バックホールの考慮事項などのセキュリティ姿勢は極めて重要であり、お客様との認識が必要です。
- 高可用性：Fail-to-Wire の高可用性には、ポートアベイラビリティに関する考慮事項がいくつか必要であり、配置によっては設計が難しい場合があります。

    - SD-WAN 110 は、フェイル・トゥ・ワイヤ・ポートを持たないため、オプションではありません。

たとえば、2 つの WAN リンクを動作させる必要がある場合は、LAN インターフェイスを含む高可用性インターフェイス用の専用ポートを含む 5 つのポートが必要です。

インライン・モード：フェイル・トゥ・ワイヤ/フェイル・トゥ・ブロック

推奨事項

インラインモード展開の推奨事項を次に示します。

1. インラインモードは、既存のインフラストラクチャを変更せず、SD-WAN が LAN セグメントに対して透過的にインラインに配置されているブランチに最適です。
2. また、データセンターのワークロードがデバイスのダウン/クラッシュによってブラックホールにならないようにすることが非常に重要であるため、データセンターでは、インライン・フェイル・トゥ・ワイヤまたはインライン・パラレル高可用性を採用することもできます。

利点とユースケース

インラインモード展開の利点と使用例を次に示します。

1. したがって、MPLS ルータを維持することは素晴らしい機能です。Fail-to-Wire 対応デバイスにより、ボックスがダウンした場合にインフラストラクチャをアンダーレイにシームレスにフェイルオーバーできます。
    - デバイスが Fail-to-WAN（SD-WAN 210 以上）をサポートしている場合、これにより、SD-WAN がクラッシュまたはダウンしたときに、1 つの SD-WAN をハードウェアにインラインで配置して、カスタマーエッジルータへの LAN トラフィックをバイパスできます。
    - お客様の LAN/イントラネットに自然な拡張をもたらす MPLS リンクが存在する場合、Fail-to-Wire ブリッジ-pair ポートが最良の選択肢（Fail-to-Wire 対応ペア）であり、デバイスがクラッシュまたはダウンしたときに LAN トラフィックがカスタマーエッジルータにハードウェアがバイパスされます（次のホップ）。
2. ネットワークはシンプルです。
3. SD-WAN は、インラインモードを介してすべてのトラフィックを認識するため、適切な帯域幅/キャパシティアカウンティングの最適なシナリオです。
4. L2 セグメントの IP のみを必要とするため、統合要件はほとんどありません。LAN セグメントは、LAN インターフェイスに腕があるためよく知られています。コアスイッチに接続する場合は、ダイナミックルーティングを実行して、すべての LAN サブネットを可視化することもできます。
5. お客様の期待は、SD-WAN が新しいネットワークノードとして既存のインフラストラクチャに溶け込む必要があることです（他に何も変わりません）。

6. プロキシ **ARP**：インラインモードでは、ゲートウェイがダウンした場合、またはネクストホップへの SD-WAN インターフェイスがダウンした場合、SD-WAN が ARP 要求を LAN ネクストホップにプロキシすることが祝福されます。
    - 一般に、複数の WAN 接続（MPLS/インターネット）を持つブリッジペア（Fail-to-Block または Fail-to-Wire）を使用するインラインモードでは、LAN ホストをネクストホップ Gateway に接続するブリッジペアインターフェイスに対してプロキシ ARP を有効にすることを推奨します。
    - 何らかの理由で、ネクストホップがダウンしているか、ネクストホップへの SD-WAN インターフェイスがダウンして Gateway に到達不能になっている場合、SD-WAN は ARP 要求のプロキシとして機能し、LAN ホストはパケットをシームレスに送信し、仮想パスを維持する残りの WAN 接続を使用できます。
7. 高可用性：Failto-Wire がオプションでない場合、デバイスを並列高可用性（アクティブ/スタンバイ用の共通の LAN および WAN インターフェイス）デバイスに配置して、冗長性を実現できます。
    - SD-WAN 110 のように、アプライアンスが Fail-to-Wire をサポートしていない場合は、プライマリがダウンした場合に、スタンバイデバイスを起動できるインライン並列高可用性を実現する必要があります。

注意事項

インラインモードで注意する必要がある情報は次のとおりです。

- SD-WAN (LAN と WAN 側) に 2 つのアームを持つ配管ネットワーク, ネットワークは 2 つのアームで配管する必要があるため、いくつかのダウンタイムを必要とします.
- Failto Wire が使用されている場合、セキュリティが侵害されないように、信頼ゾーン内のカスタマーエッジルータ/ファイアウォールの背後にあることを確認する必要があります。
- MPLS QoS は、以前の QoS ポリシーが送信元 IP アドレスまたは DSCP ベースに依存していた可能性があるため、この点では少し変化します。これは、オーバーレイのためにマスクされるためです。
- SD-WAN の QoS がトラフィックの優先順位付けを処理し、優先順位の高いアプリケーションをすぐに他のクラスを送信するように、適切に設計された SD-WAN 固有の予約帯域幅を使用して MPLS ルータを再利用するように注意する必要があります（ただし、MPLS ルータ上の SD-WAN 用に予約された帯域幅）。MPLS キューは、自動パスグループに 1 つの DSCP が設定された代替または MPLS で、これを処理できます。
- カスタマーエッジルータでリンクが終端しているためにインターネットインターフェイスが信頼されている場合は、インターネットサービスを使用するには、アプライアンスからのインターネットブレークアウトを有効にする排他的なダイナミック NAT ルールを作成する必要があります。
- インターネットリンクが WAN 接続だけであり、カスタマーエッジルータで終端している場合でも、カスタマーエッジルータが既存のアンダーレイインフラストラクチャを介してパケットを操縦するための予防措置を講じている場合は、接続をバイパスしても問題ありません。

  - インターネット接続のあるブリッジペア経由で LAN トラフィックをバイパスする流れや、アプライアンスがダウンしているときの流れを考慮する必要があります。これは機密性の高い企業イントラネットトラフィックであるため、障害発生前夜には、その処理方法を知っている必要があります。

仮想インライン/ワンアームモード

推奨事項

仮想インラインモードの展開に関する推奨事項を次に示します。

1. 仮想インラインモードは、SD-WAN ネットワーク配管を並列処理しながら、データセンターが既存のインフラストラクチャを使用して既存のワークロードを処理できるため、データセンターのネットワークに最適です。
2. SD-WAN はワンアームインターフェイスにあり、VIP の SLA トラッキングで管理されます。トラッキングが停止すると、トラフィックは既存のアンダーレイインフラストラクチャを介してルーティングを再開します。
3. ブランチは仮想インラインモードでデプロイすることもできますが、インライン/ゲートウェイのデプロイの方が優勢です。

利点とユースケース

仮想インラインモード展開の利点/使用例を次に示します。

1. データセンターで SD-WAN をネットワーク化するための最も簡単で推奨される方法
   - 仮想インラインモードでは、ヘッドエンドコアルータと SD-WAN の並列ネットワークプラミングが可能になります。
   - 仮想インラインモードを使用すると、LAN トラフィックを迂回するために PBR を簡単に定義でき、SD-WAN を通過し、オーバーレイのメリットを得ることができます。
2. SD-WAN に障害が発生した場合、基盤となるインフラストラクチャへのシームレスなフェイルオーバー、および通常の条件下では SD-WAN へのシームレスな転送により、オーバーレイのメリットが得られます。
3. **** ネットワークと統合のシンプルな要件 ** 。ヘッドエンドルータから仮想インラインの SD-WAN へのシングルワンアームインターフェイス。
4. インポート専用モード（何もエクスポートしない）でダイナミックルーティングを簡単に展開でき、LAN サブネットをリモートの SD-WAN ピアアプライアンスに送信できます。
5. 物理的なを選択する方法を示すために、ルータ上で PBR を簡単に定義できます（WAN VIP ごとに 1 つ）。

注意事項

仮想インラインモードで注意する必要がある情報は次のとおりです。

- 定義された WAN リンクの SD-WAN 論理 VIP を適切な物理インターフェイスに明確にマッピングするには、適切な注意が必要です（そうしないと、WAN メトリック評価および WAN パスの選択で望ましくない問題が発生する可能性があります）。
- すべてのトラフィックが SD-WAN を介して転送されるか、特定のトラフィックだけ転送されるかを知るために、設計上の適切な考慮事項が必要です。
- つまり、SD-WAN は、SD-WAN の容量が他の非 SD-WAN トラフィックによって使用されないように、インターフェイス上で設定する必要がある帯域幅の一部分だけ専用にする必要があります。
  - SD-WAN WAN リンク容量が正しく定義されていないと、帯域幅アカウンティングの問題や輻輳の問題が発生することがあります。
- ダイナミックルーティングは、SD-WAN がデータセンターおよびブランチオフィスの VIP をヘッドエンドにエクスポートし、ルーティングが SD-WAN に対して影響される場合、オーバーレイパケットがループを開始し、望ましくない結果を引き起こすような設計が不適切に行われている場合、いくつかの問題を引き起こす可能性があります。
- ダイナミックルーティングは、学習対象とアドバタイズ対象のすべての潜在的な要因を考慮して適切に管理する必要があります。
- ワンアームの物理インターフェイスがボトルネックになることがあります。これらの回線では、アップロード/ダウンロードの両方に対応し、SD-WAN からの LAN と LAN から WAN/WAN から LAN へのトラフィックとしても機能するため、設計上の考慮事項が必要です。
- 過剰な LAN から LAN へのトラフィックは、設計時に注意すべき点である可能性があります。
- ダイナミックルーティングを使用しない場合、すべての LAN サブネットを管理する場合は、適切な注意が必要です。そうしないと、望ましくないルーティングの問題が発生する可能性があります。
- 仮想インラインの SD-WAN にデフォルトルート（0.0.0.0/0）を定義して、ヘッドエンドルータを指すようにすると、ルーティングループの問題が発生する可能性があります。このような状況では、仮想パスがダウンした場合、データセンター LAN からのトラフィック（トラフィックのモニタリングなど）がヘッドエンドにループバックされ、SD-WAN に戻され、望ましくないルーティングの問題が発生します（仮想パスがダウンしている場合、リモートブランチサブネットは到達可能になりません。デフォルトルートは HIT になり、ループの問題が発生します）。

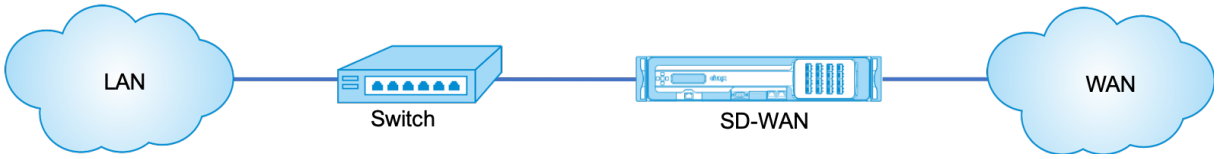
ゲートウェイモード

May 10, 2021

Gateway モードでは、SD-WAN アプライアンスが物理的にパスに配置されます（ツーアーム配置）。SD-WAN アプライアンスをそのサイトの LAN ネットワーク全体のデフォルトゲートウェイにするには、既存のネットワークイン

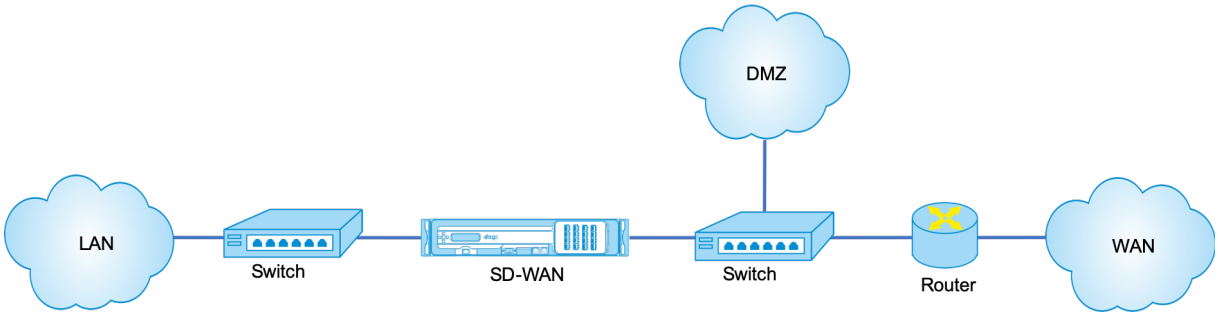
フラストラクチャを変更する必要があります。新しいネットワークとルータの交換に使用されるゲートウェイモード。ゲートウェイモードでは、SD-WAN アプライアンスが次のようになります。

- WAN との間で送受信されるすべてのトラフィックを表示するには
- ローカルルーティングを実行するには



> 注
>
> ゲートウェイモードで展開された SD-WAN は、レイヤ 3 デバイスとして機能し、フェールツーワイヤを実行できません。関連するすべてのインターフェイスが **Fail-to-Block** 用に設定されます。アプライアンスに障害が発生すると、サイトのデフォルト Gateway も失敗し、アプライアンスとデフォルト Gateway が復元されるまで停止します。

インラインモードでは、SD-WAN アプライアンスはイーサネットブリッジのように見えます。SD-WAN アプライアンスモデルのほとんどは、インラインモード用の フェールツーワイヤ（イーサネットバイパス）機能を備えています。電源が故障すると、リレーが閉じ、入力ポートと出力ポートが電気的に接続され、イーサネット信号がポート間で通過できるようになります。Fail-to-Wire モードでは、SD-WAN アプライアンスは 2 つのポートを接続するクロスオーバーケーブルのように見えます。すでに定義されたネットワークに統合するために使用されるインラインモード。

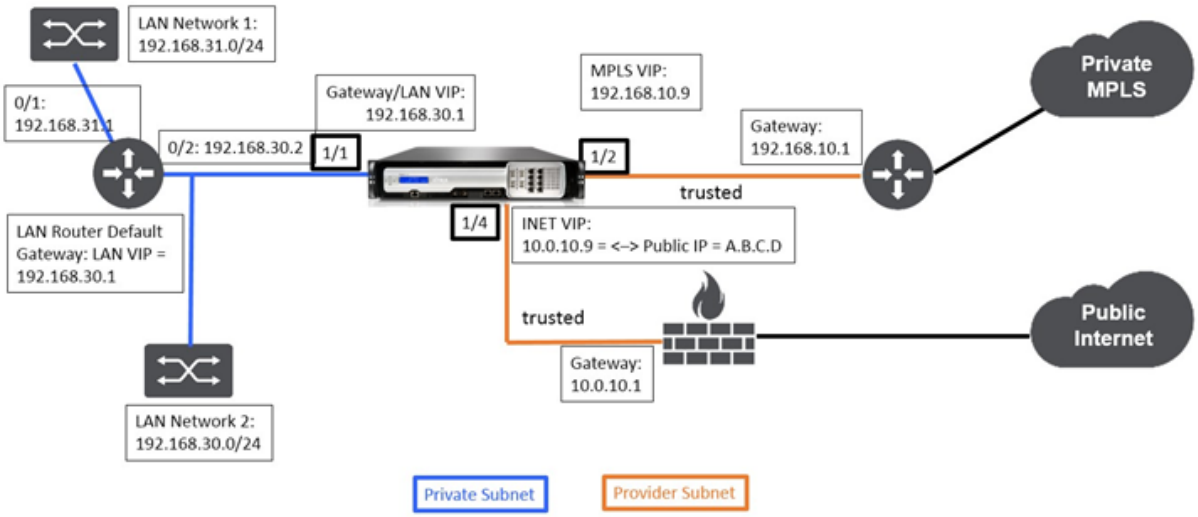


この記事では、ネットワーク設定のサンプルで SD-WAN アプライアンスをゲートウェイモードで構成する手順を順を追って説明します。インライン展開は、ブランチ側で設定を完了するためにも説明されています。Inline デバイスが削除されても、ネットワークは引き続き機能しますが、Gateway デバイスが削除されるとすべてのアクセスが失われます。

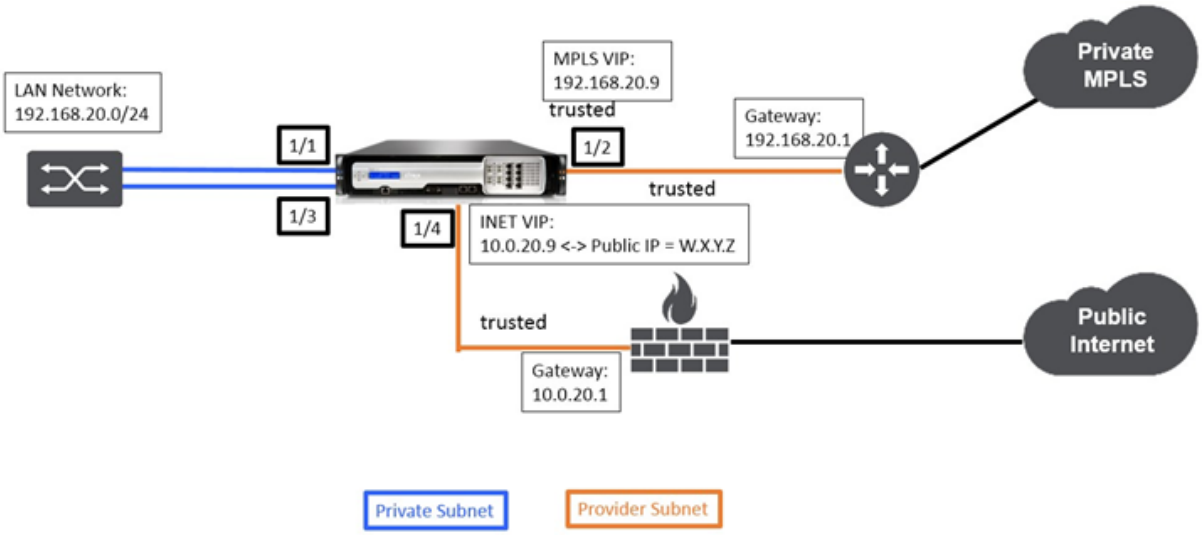
トポロジ

次の図は、SD-WAN ネットワークでサポートされるトポロジを示しています。

Gateway 導入におけるデータセンター



インライン展開でのブランチ



導入の要件

構成を構築する際に役立つように、展開の要件と関連情報を以下に説明します。

サイト名	データセンターサイト	ブランチサイト
アプライアンス名	A_DC1	A_BR1
管理 IP	172.30.2.10/24	172.30.2.20/24

サイト名	データセンターサイト	ブランチサイト
セキュリティキー	もしあれば	もしあれば
モデル/エディション	4000	2000
モード	Gateway	インライン
トポロジ	2 x WAN パス	2 x WAN パス
VIP アドレス	192.168.10.9/24 —MPLS, 10.0.10.9/24 —インターネット (Public IP —A.B.C.D), 192.168.30.1/24-LAN	192.168.20.9/24-MPLS, 10.0.20.9/24 —インターネット (パブリック IP —W.X.Y.Z)
Gateway MPLS	192.168.10.1	192.168.20.1
ゲートウェイ・インターネット	10.0.10.1	10.0.20.1
リンク速度	MPLS —100 Mbps, インターネット —20 Mbps	MPLS —10 Mbps, インターネット —2 Mbps
Route	ネットワーク IP アドレス-192.168.31.0/24、サービスタイプ-ローカル、ゲートウェイ IP アドレス-192.168.30.2	もしあれば
VLAN	もしあれば	もしあれば

構成の前提条件

- SD-WAN アプライアンスをマスターコントロールノードとして有効にします。
- 構成は SD-WAN アプライアンスのマスターコントロールノード (MCN) でのみ行われます。

アプライアンスをマスター・コントロール・ノードとして有効にするには:

1. SD-WAN Web 管理インターフェイスで、［構成］>［アプライアンスの設定］>［管理者インターフェイス］>［その他］タブ **>**［スイッチコンソール］に移動します。

   > 注
   >
   > 「クライアントコンソールに切り替える」と表示されている場合、アプライアンスはすでに MCN モードになっています。SD-WAN ネットワークには、アクティブな MCN が 1 つだけ存在する必要があります。

2. [構成] > [仮想 **WAN**] > [構成エディター**]** の順に選択して、構成を開始します。[新規] をクリックして設定を開始します。

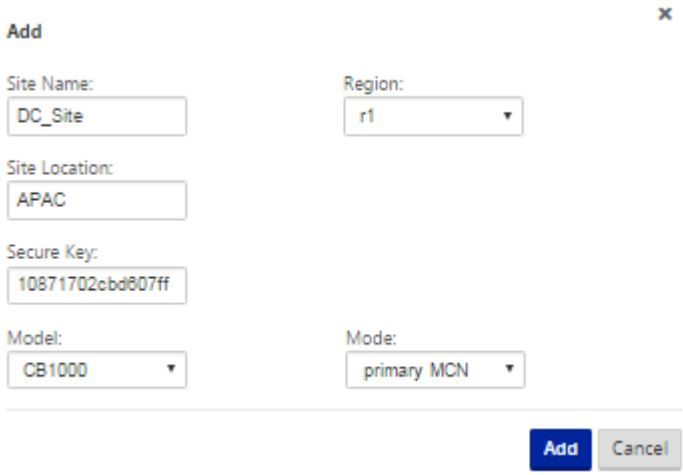
データセンターサイト **Gateway** モードの設定

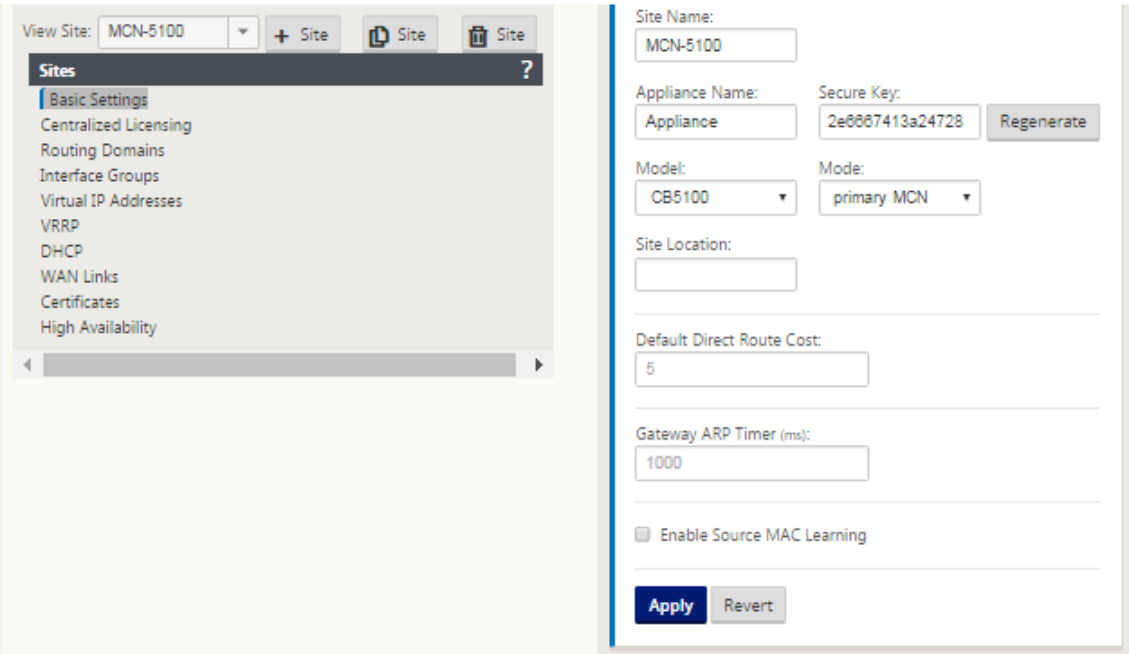
データセンターサイトゲートウェイの展開を構成するための高レベルの構成手順を次に示します。

1. DC サイトを作成します。
2. 接続されたイーサネットインターフェイスに基づいてインターフェイスグループを設定します。
3. 各仮想インターフェイスの仮想 IP アドレスを作成します。
4. インターネットおよび MPLS リンクを使用して、バースト速度ではなく、物理レートに基づいて WAN リンクを設定します。
5. LAN インフラストラクチャにさらにサブネットがある場合は、Routes を設定します。

DC サイトを作成するには

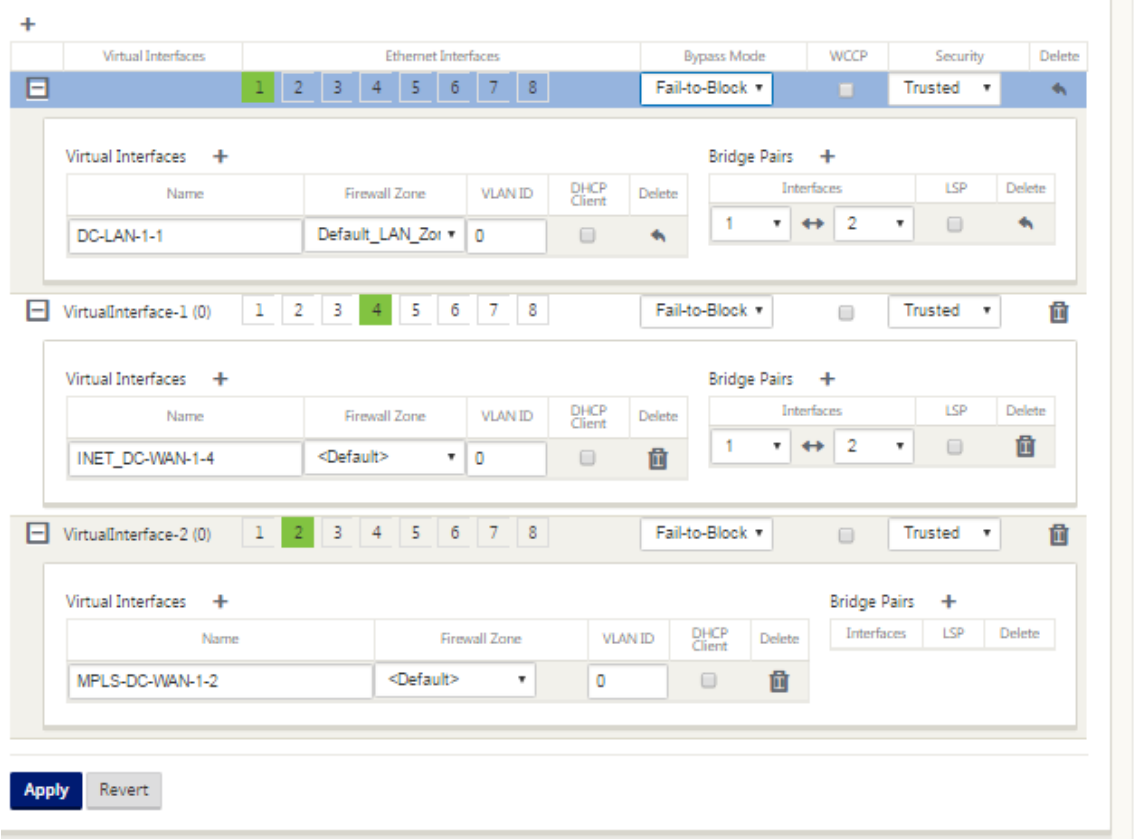
1. [構成エディタ]-[サイト] に移動し、[**+** 追加] ボタンをクリックします。
2. 以下に示すようにフィールドに入力します。
3. 変更するように指示されない限り、デフォルト設定を保持します。





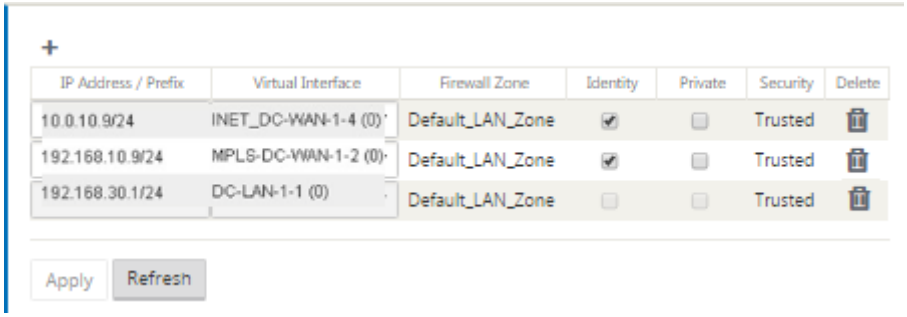
接続されたイーサネットインターフェイスに基づいてインターフェイスグループを設定するには

1. 構成エディタで、[サイト**] > [**サイトの表示**] > [**[**サイト名**]****] > [インタフェースグループ] に移動します。**[+]** をクリックして、使用するインターフェイスを追加します。ゲートウェイモードでは、各インターフェイスグループに 1 つのイーサネットインターフェイスが割り当てられます。
2. 仮想インターフェイスごとに 1 つのイーサネット/物理インターフェイスだけが使用されるため、バイパスモードは **Failto Block** に設定されます。ブリッジペアもありません。
3. この例では、3 つのインターフェイスグループが作成されます。1 つが LAN に面し、もう 2 つは各 WAN リンクに面しています。上記の「DC ゲートウェイモード」トポロジのサンプルを参照し、次に示すように [Interface Groups] フィールドに入力します。



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

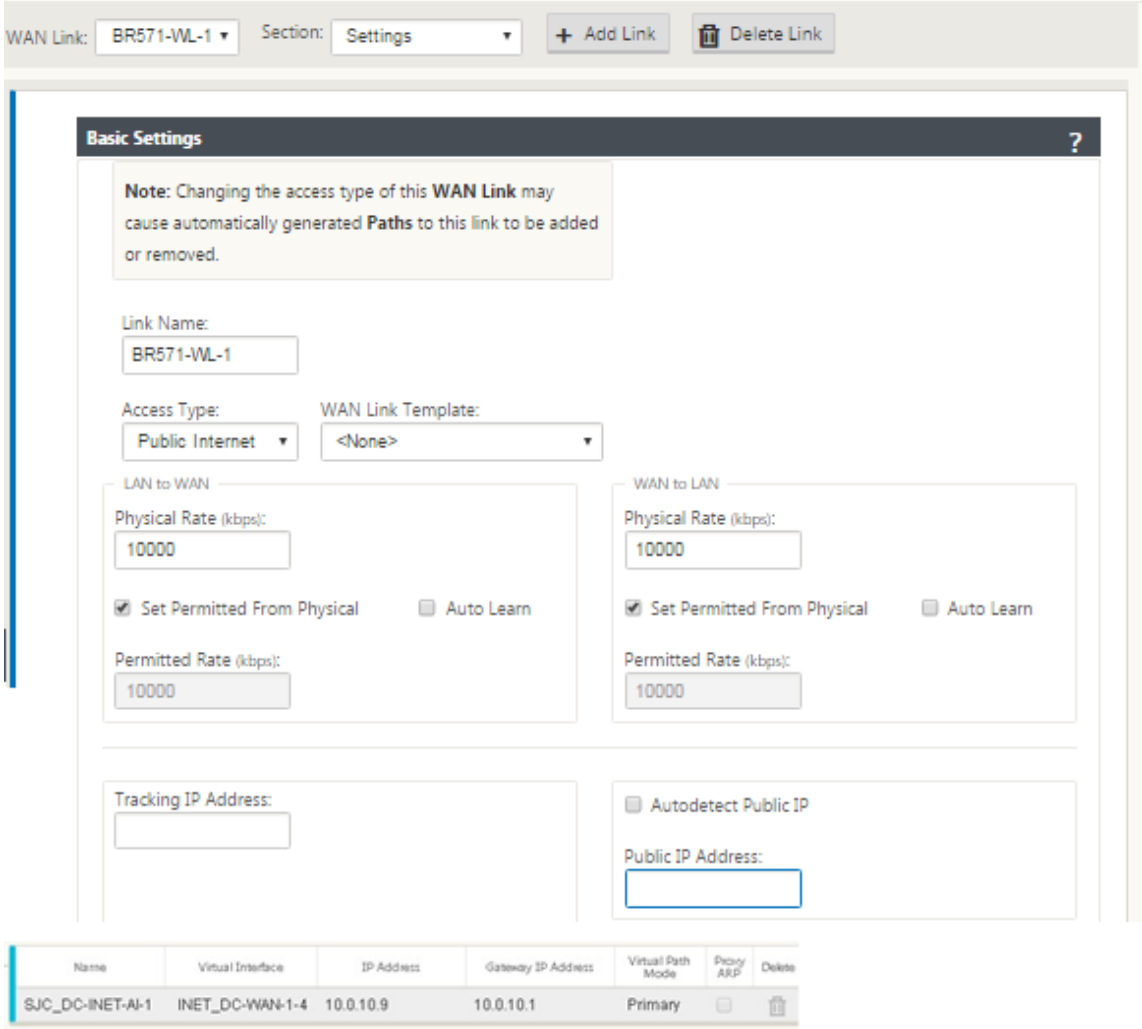
1. WAN リンクごとに適切なサブネットに VIP を作成します。VIP は、仮想 WAN 環境内の 2 つの SD-WAN アプライアンス間の通信に使用されます。
2. LAN ネットワークのゲートウェイアドレスとして使用する仮想 IP アドレスを作成します。



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

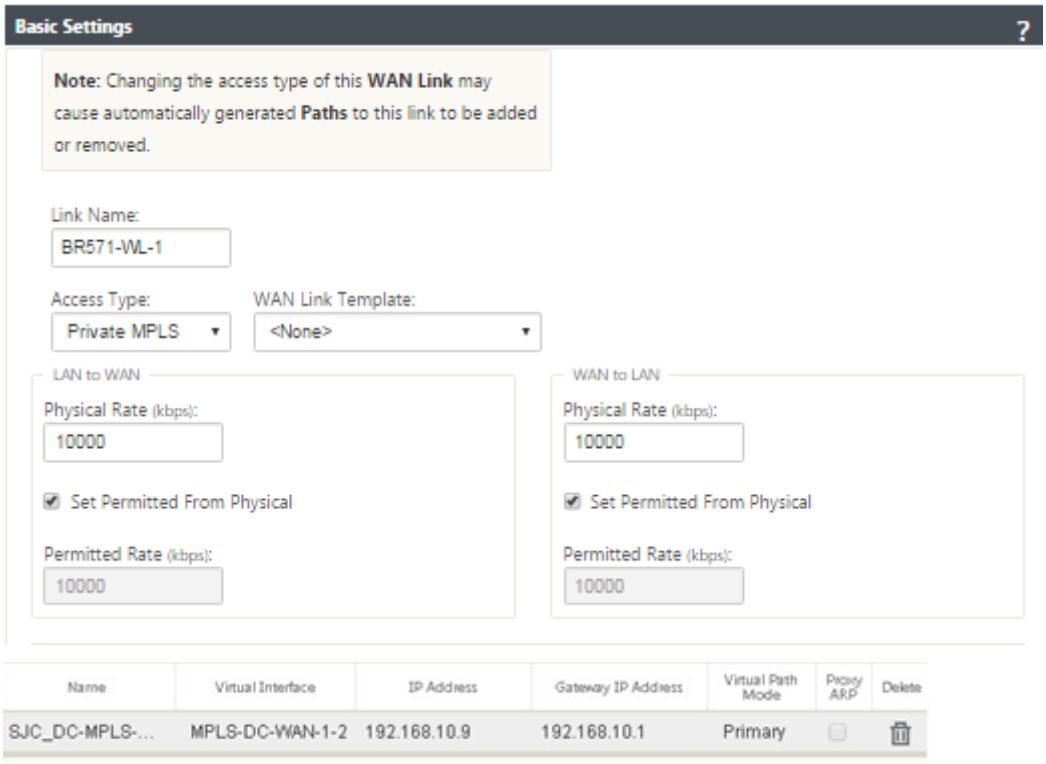
1. [**WAN** リンク] に移動し、[**+** リンクの追加] ボタンをクリックして、インターネットリンクの WAN リンクを追加します。

2. 以下に示すように、提供されたパブリック IP アドレスなど、インターネットリンクの詳細を入力します。自動検出 パブリック **IP** は、MCN として設定された SD-WAN アプライアンスでは選択できません。
3. セクションのドロップダウンメニューから [**Access Interfaces**] に移動し、[**+ Add**] ボタンをクリックして、インターネットリンクに固有のインターフェイスの詳細を追加します。
4. 以下に示すように、IP アドレスと Gateway アドレスのアクセスインターフェイスを設定します。



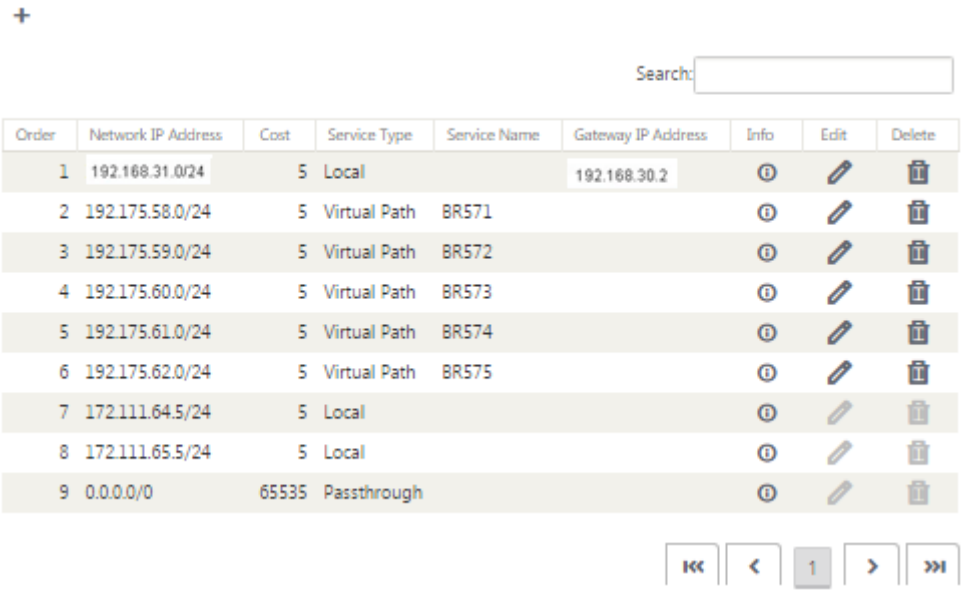
MPLS リンクを作成するには

1. [**WAN** リンク] に移動し、[**+**] ボタンをクリックして、MPLS リンクの WAN リンクを追加します。
2. 次に示すように、MPLS リンクの詳細を入力します。
3. [アクセスインターフェイス] に移動し、[**+**] ボタンをクリックして、MPLS リンクに固有のインターフェイスの詳細を追加します。
4. 以下に示すように、IP アドレスと Gateway アドレスのアクセスインターフェイスを設定します。



ルートを設定するには

ルートは、上記の設定に基づいて自動作成されます。上記の DC LAN サンプルトポロジには、**192.168.31.0/24** という追加の LAN サブネットがあります。このサブネットのルートを作成する必要があります。ゲートウェイ IP アドレスは、次に示すように DC LAN VIP と同じサブネット内に存在する必要があります。



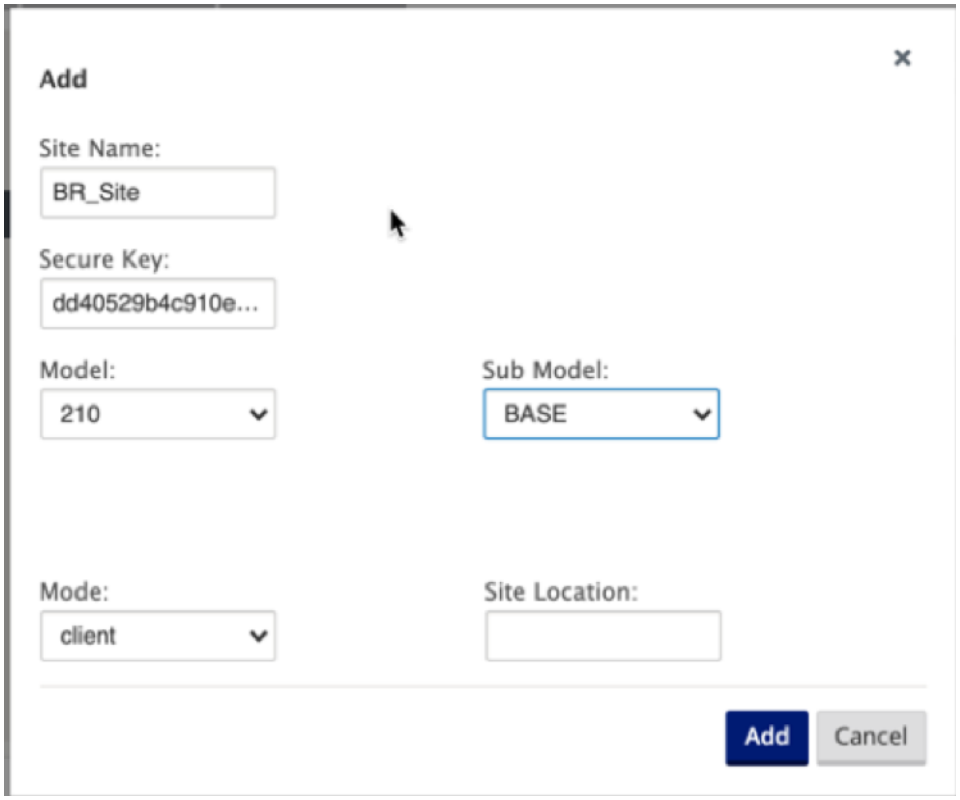
ブランチサイトのインライン展開設定

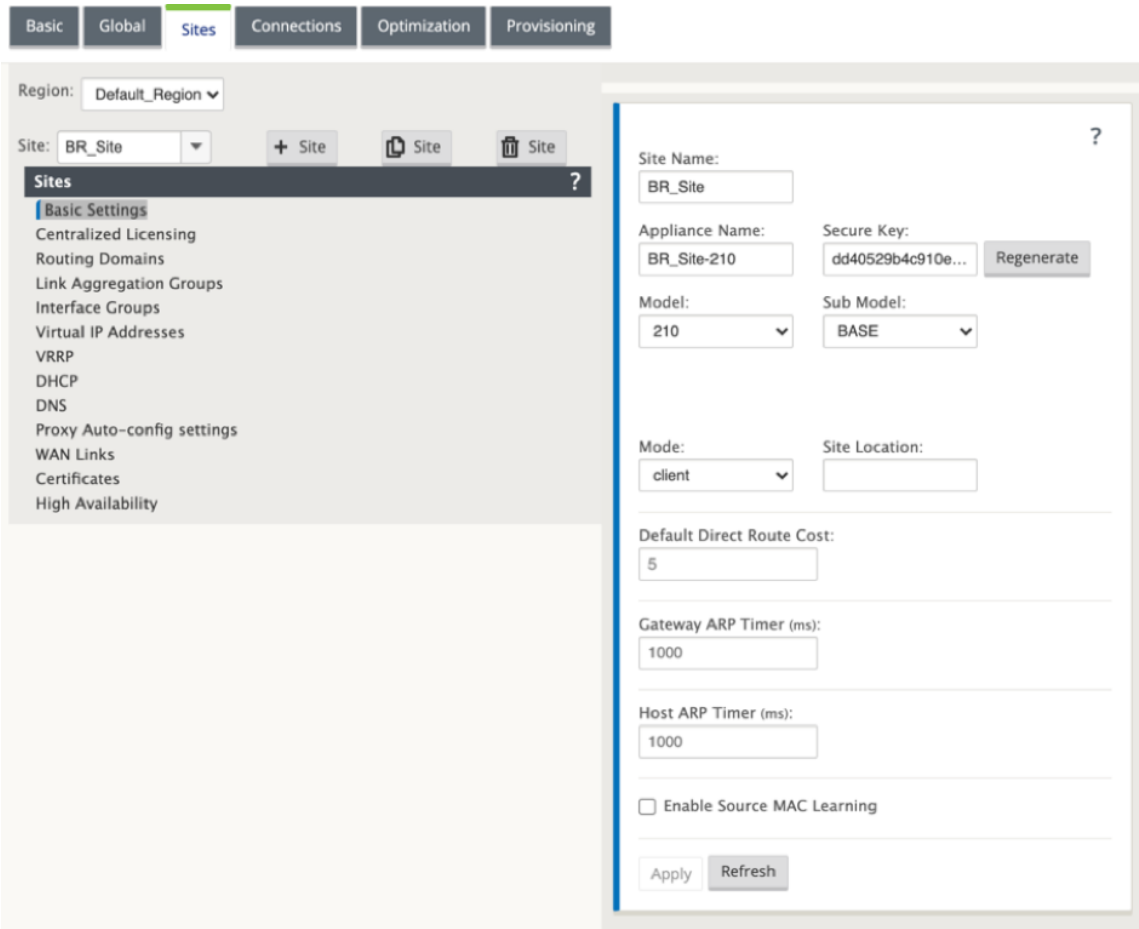
次に、インライン展開用にブランチサイトを構成するための高レベルの構成手順を示します。

1. ブランチサイトを作成します。
2. 接続されたイーサネットインターフェイスに基づいてインターフェイスグループを設定します。
3. 各仮想インターフェイスの仮想 IP アドレスを作成します。
4. インターネットおよび MPLS リンクを使用して、バースト速度ではなく、物理レートに基づいて WAN リンクを設定します。
5. LAN インフラストラクチャにさらにサブネットがある場合は、Routes を設定します。

ブランチサイトを作成するには

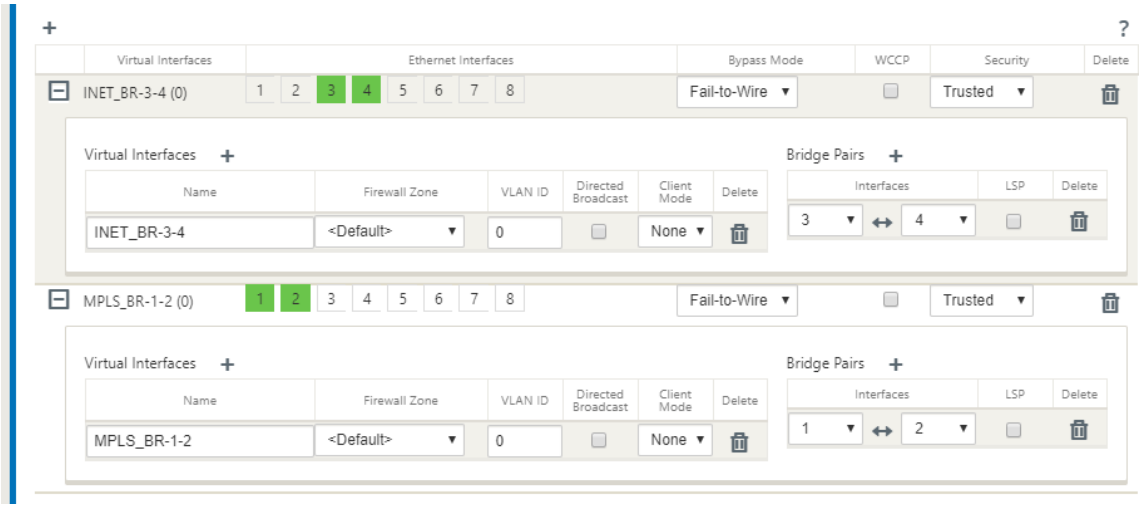
1. [構成エディタ] > [サイト] に移動し、[**+** 追加] ボタンをクリックします。
2. 以下に示すようにフィールドに入力します。
3. 変更するように指示されない限り、デフォルト設定を保持します。





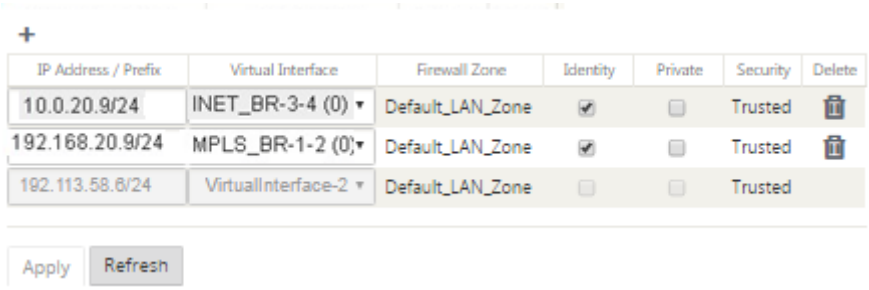
接続されたイーサネットインターフェイスに基づいてインターフェイスグループを設定するには

1. 構成エディタで、[サイト**] > [**サイトの表示**] > [**[**クライアントサイト名**]****] > [インターフェイスグループ] に移動します。[**+**] をクリックして、使用するインターフェイスを追加します。インラインモードの場合、各インターフェイスグループには 2 つのイーサネットインターフェイスが割り当てられます。
2. バイパスモードは **fail-to-wire** に設定され、ブリッジペアは 2 つのイーサネットインターフェイスを使用して作成されます。
3. 上記の「リモートサイトインラインモード」トポロジのサンプルを参照し、次に示すように [Interface Groups] フィールドに入力します。



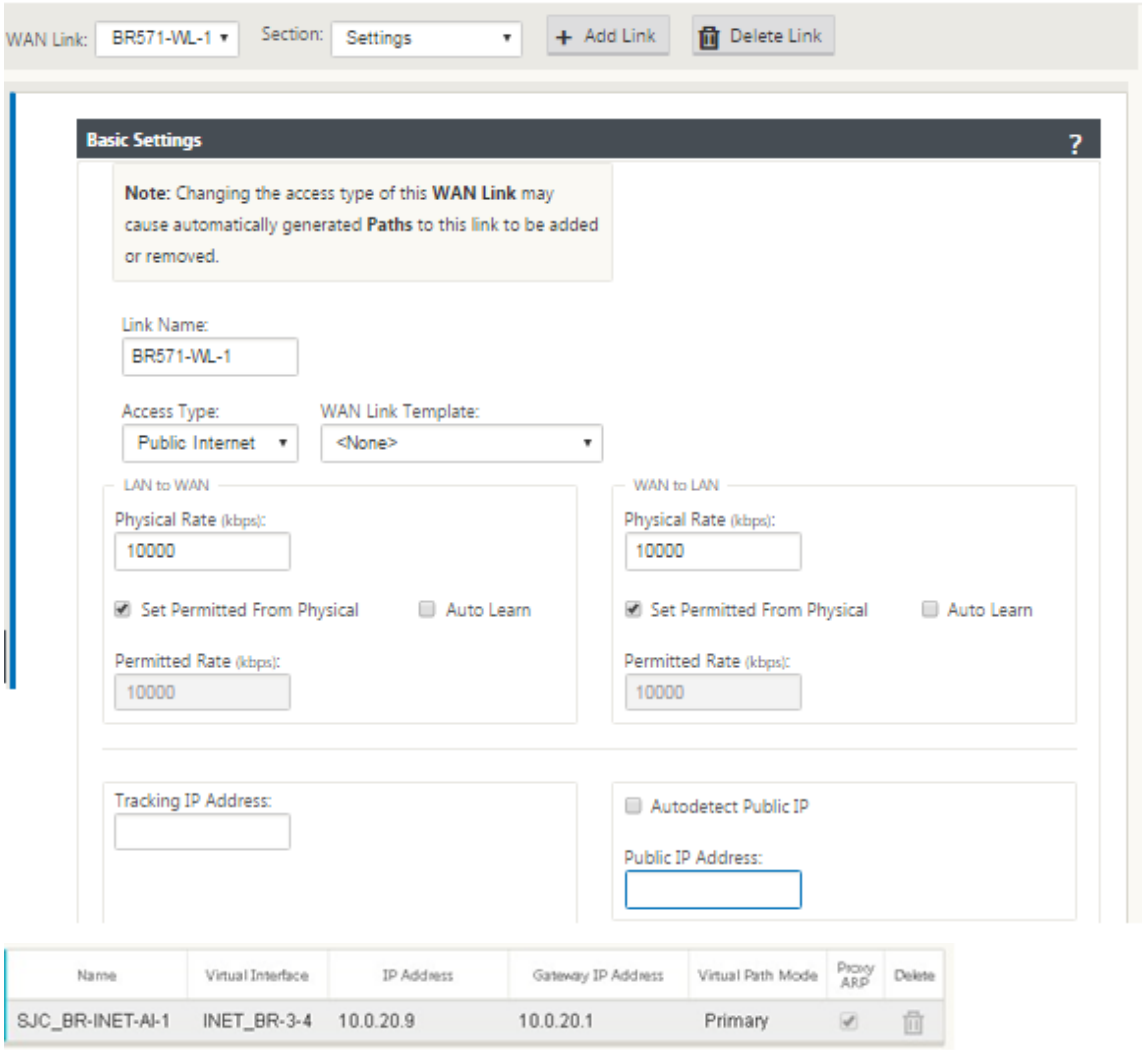
仮想インターフェイスごとに仮想 **IP**（**VIP**）アドレスを作成するには

1. 各 WAN リンクの適切なサブネット上に仮想 IP アドレスを作成します。VIP は、仮想 WAN 環境内の 2 つの SD-WAN アプライアンス間の通信に使用されます。



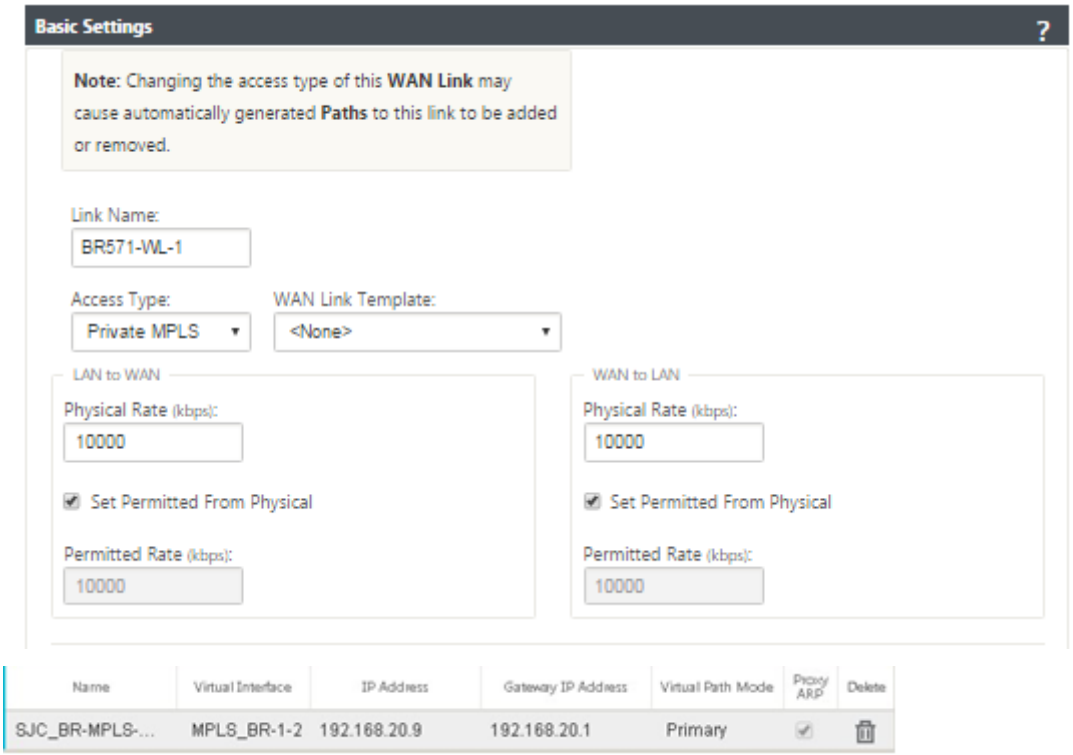
インターネットリンクを使用して、バースト速度ではなく、物理レートに基づいて WAN リンクを設定するには、次の手順を実行します。

1. [**WAN** リンク] に移動し、[**+**] ボタンをクリックして、インターネットリンクの WAN リンクを追加します。
2. 以下に示すように、自動検出パブリック IP アドレスなど、インターネットリンクの詳細を入力します。
3. [**Access Interfaces**] に移動し、[**+**] ボタンをクリックして、インターネットリンクに固有のインターフェイスの詳細を追加します。
4. 以下に示すように、IP アドレスと Gateway のアクセスインタフェースを設定します。



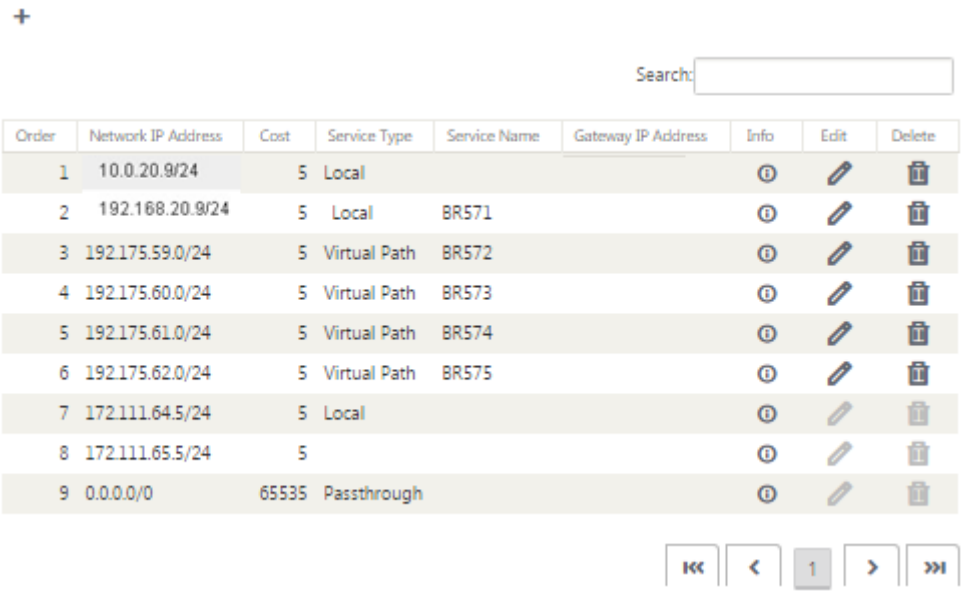
MPLS リンクを作成するには

1. [WAN リンク] に移動し、[**+**] ボタンをクリックして、MPLS リンクの WAN リンクを追加します。
2. 次に示すように、MPLS リンクの詳細を入力します。
3. [アクセスインターフェイス] に移動し、[**+**] ボタンをクリックして、MPLS リンクに固有のインターフェイスの詳細を追加します。
4. 以下に示すように、IP アドレスと Gateway のアクセスインタフェースを設定します。



ルートを設定するには

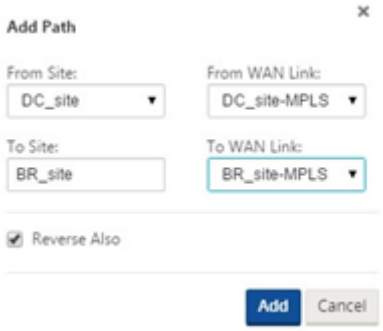
ルートは、上記の設定に基づいて自動作成されます。このリモートブランチオフィスに固有のサブネットがさらに存在する場合は、それらのバックエンドサブネットに到達するためにトラフィックを誘導する Gateway を特定する特定のルートを追加する必要があります。



監査エラーを解決する

DC サイトとブランチサイトの構成が完了すると、DC サイトと BR サイトの両方で監査エラーを解決するように警告が表示されます。

デフォルトでは、アクセスタイプ [パブリックインターネット] として定義された WAN リンクのパスが生成されます。アクセスタイプが [プライベートインターネット] の WAN リンクでは、自動パスグループ機能を使用するか、手動でパスを有効にする必要があります。MPLS リンクのパスは、緑の四角形にある [Add operator] をクリックして有効にすることができます。



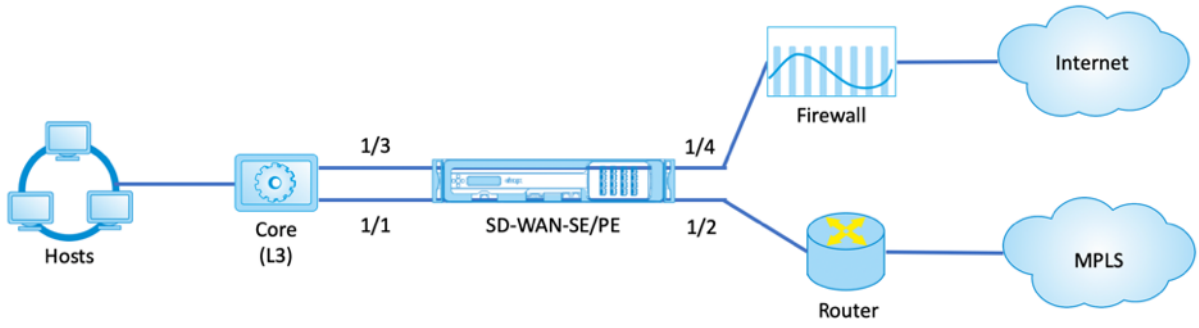
上記の手順をすべて完了したら、SD-WAN アプライアンスパッケージの準備に進みます。

インラインモード

May 10, 2021

この記事では、インライン展開モードでブランチを構成する方法について詳しく説明します。このモードでは、SD-WAN アプライアンスはイーサネットブリッジのように見えます。SD-WAN アプライアンスモデルのほとんどは、インラインモード用の配線接続（イーサネットバイパス）機能を備えています。電源が故障すると、リレーが閉じ、入力ポートと出力ポートが電気的に接続され、イーサネット信号がポート間で通過できるようになります。Fail-to-Wire モードでは、SD-WAN アプライアンスは 2 つのポートを接続するクロスオーバーケーブルのように見えます。

次の図では、インターフェイス 1/1 および 1/2 はハードウェアバイパスペアであり、コアとエッジ MPLS ルータを接続するフェールツーワイヤです。インターフェイス 1/3 および 1/4 はハードウェアバイパスペアでもあり、コアをエッジファイアウォールに接続するフェールツーワイヤリングを行います。



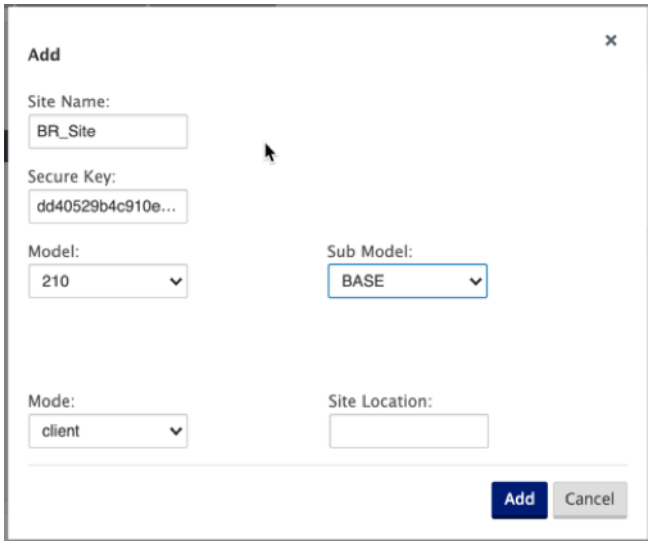
ブランチサイトのインライン展開設定

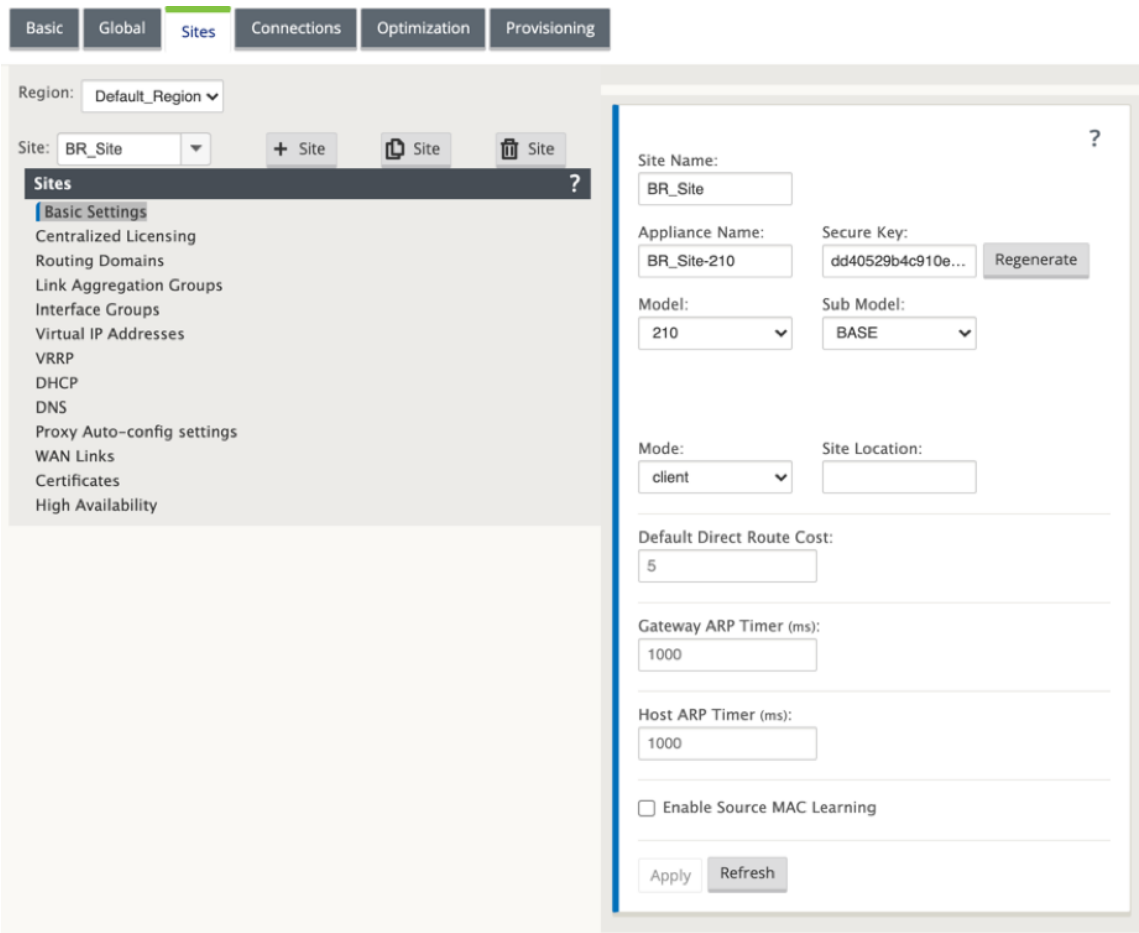
次に、インライン展開用にブランチサイトを構成するための高レベルの構成手順を示します。

1. ブランチサイトを作成します。
2. 接続されたイーサネットインターフェイスに基づいてインターフェイスグループを設定します。
3. 各仮想インターフェイスの仮想 IP アドレスを作成します。
4. インターネットおよび MPLS リンクを使用して、バースト速度ではなく、物理レートに基づいて WAN リンクを設定します。
5. LAN インフラストラクチャにさらにサブネットがある場合は、Routes を設定します。

ブランチサイトを作成するには

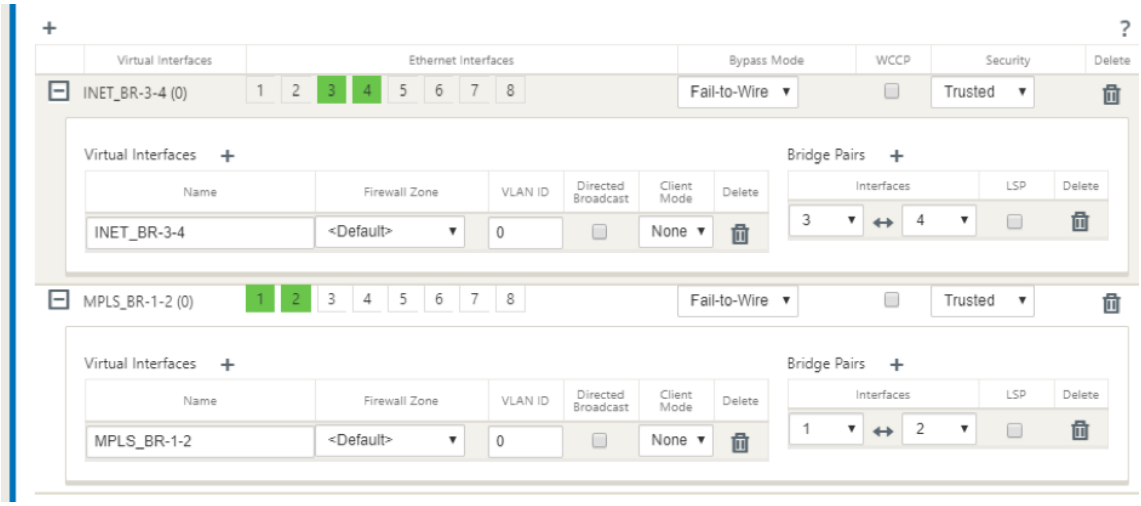
1. [構成エディタ**] > [**サイト] に移動し、[**+** 追加] ボタンをクリックします。
2. 変更するように指示されない限り、デフォルト設定を保持します。





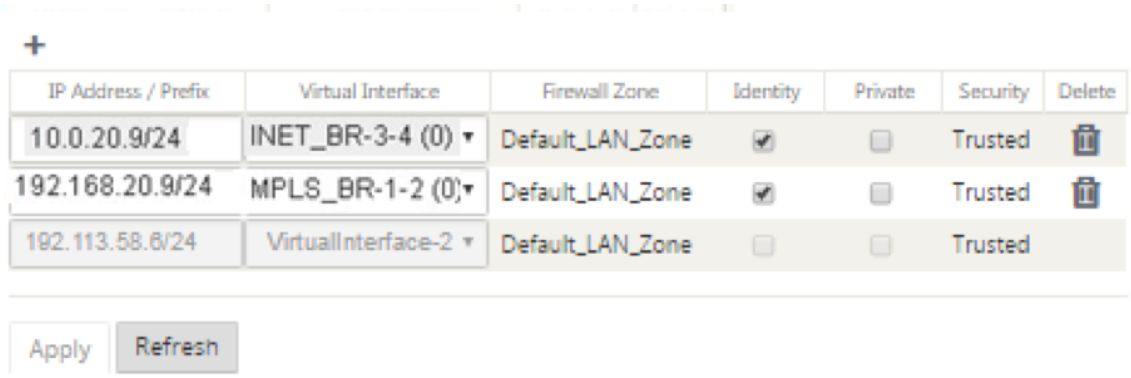
接続されたイーサネットインターフェイスに基づいてインターフェイスグループを設定するには

1. 構成エディタで、[サイト**] > [**サイトの表示**] > [[**クライアントサイト名**]] > [**インターフェイスグループ] に移動します。[**+**] をクリックして、使用するインターフェイスを追加します。インラインモードの場合、各インターフェイスグループには 2 つのイーサネットインターフェイスが割り当てられます。
2. バイパスモードは **fail-to-wire** に設定され、ブリッジペアは 2 つのイーサネットインターフェイスを使用して作成されます。
3. 上記のサンプルトポロジを参照し、次に示すように [Interface Groups] フィールドに入力します。



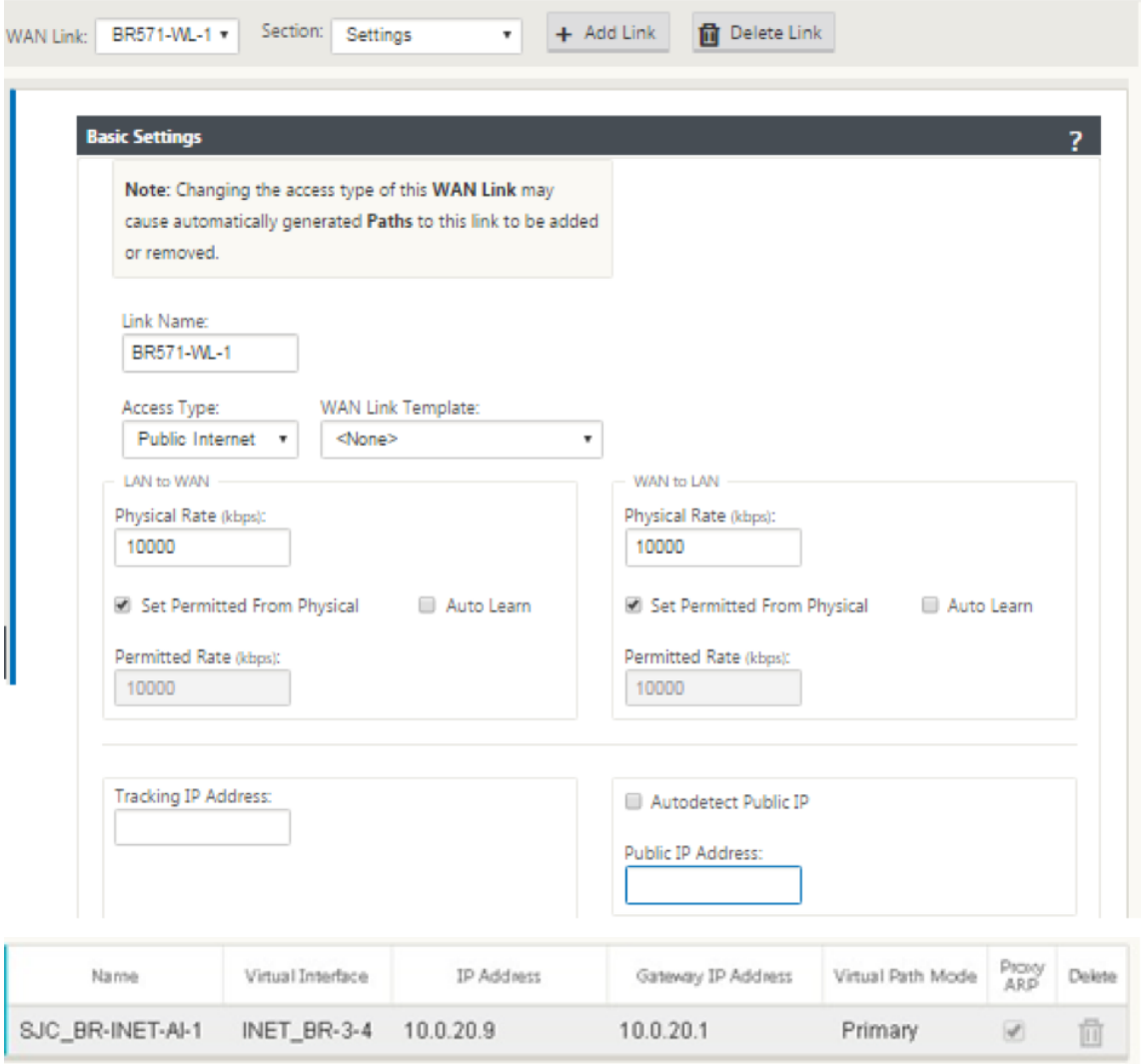
仮想インターフェイスごとに仮想 **IP**（**VIP**）アドレスを作成するには

1. 各 WAN リンクの適切なサブネット上に仮想 IP アドレスを作成します。VIP は、仮想 WAN 環境内の 2 つの SD-WAN アプライアンス間の通信に使用されます。



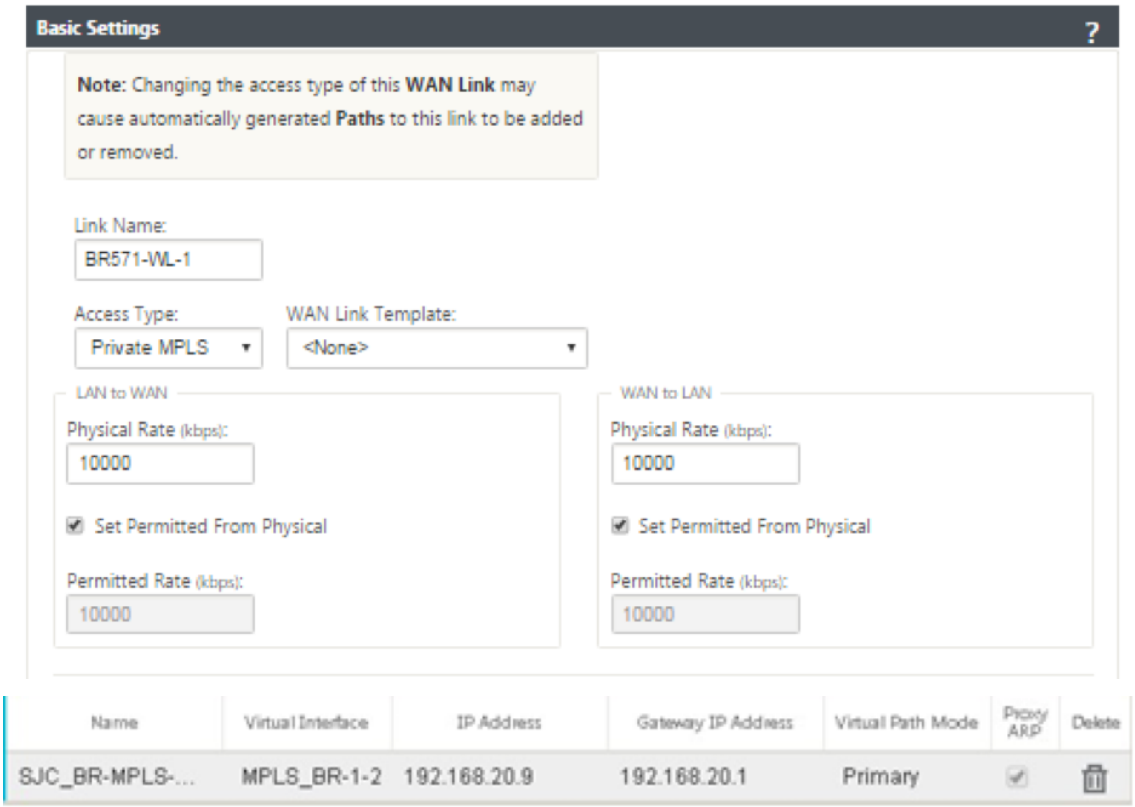
インターネットリンクを使用してバースト速度ではなく、物理レートに基づいて **WAN** リンクを設定するには

1. [**WAN** リンク] に移動し、[**+**] ボタンをクリックして、インターネットリンクの WAN リンクを追加します。
2. 以下に示すように、自動検出パブリック IP アドレスなど、インターネットリンクの詳細を入力します。
3. [**Access Interfaces**] に移動し、[**+**] ボタンをクリックして、インターネットリンクに固有のインターフェイスの詳細を追加します。
4. 以下に示すように、IP アドレスと Gateway のアクセスインタフェースを設定します。



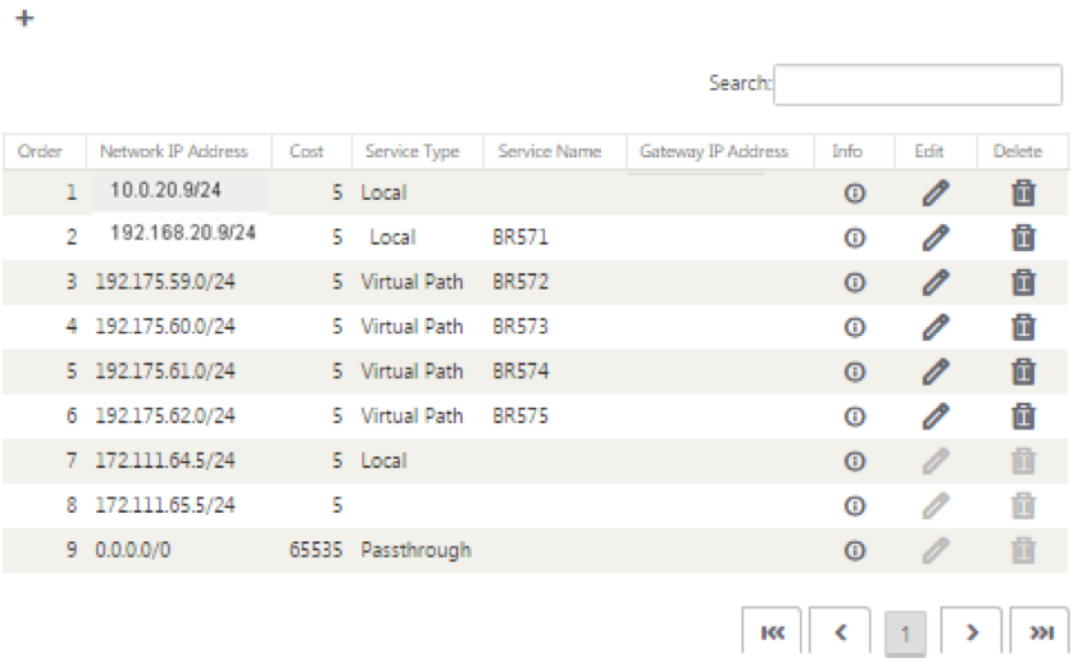
MPLS リンクを作成するには

1. [**WAN** リンク] に移動し、[**+**] ボタンをクリックして、MPLS リンクの WAN リンクを追加します。
2. 次に示すように、MPLS リンクの詳細を入力します。
3. [アクセスインターフェイス] に移動し、[**+**] ボタンをクリックして、MPLS リンクに固有のインターフェイスの詳細を追加します。
4. 以下に示すように、IP アドレスと Gateway のアクセスインタフェースを設定します。



ルートを設定するには

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



仮想インラインモード

November 8, 2021

仮想インラインモードでは、ルータは PBR、OSPF、BGP などのルーティングプロトコルを使用して、着信および発信 WAN トラフィックをアプライアンスにリダイレクトし、アプライアンスは処理されたパケットをルータに転送します。

次の資料では、2 つの SD-WAN（SD-WAN SE）アプライアンスを構成する手順について説明します。

- 仮想インラインモードのデータセンターアプライアンス
- インラインモードのブランチアプライアンス
- ルーティングプロトコルは、コアスイッチで設定するか、ルータでさらにアップストリームで設定する必要があります。ルータは SD-WAN アプライアンスの健全性を監視し、障害が発生した場合にアプライアンスをバイパスできるようにする必要があります。
- 仮想インラインモードでは、SD-WAN アプライアンスは物理的にパス外（ワンアーム展開）になります。つまり、バイパスモードが Fail-to-Block（FTB）に設定された単一のイーサネットインターフェイス（例：インターフェイス 1/5）のみが使用されます。
  Citrix SD-WAN アプライアンスは、トラフィックを適切な Gateway に渡すように構成する必要があります。仮想パス用のトラフィックは SD-WAN アプライアンスに向けられ、カプセル化され、適切な WAN リンクに送信されます。

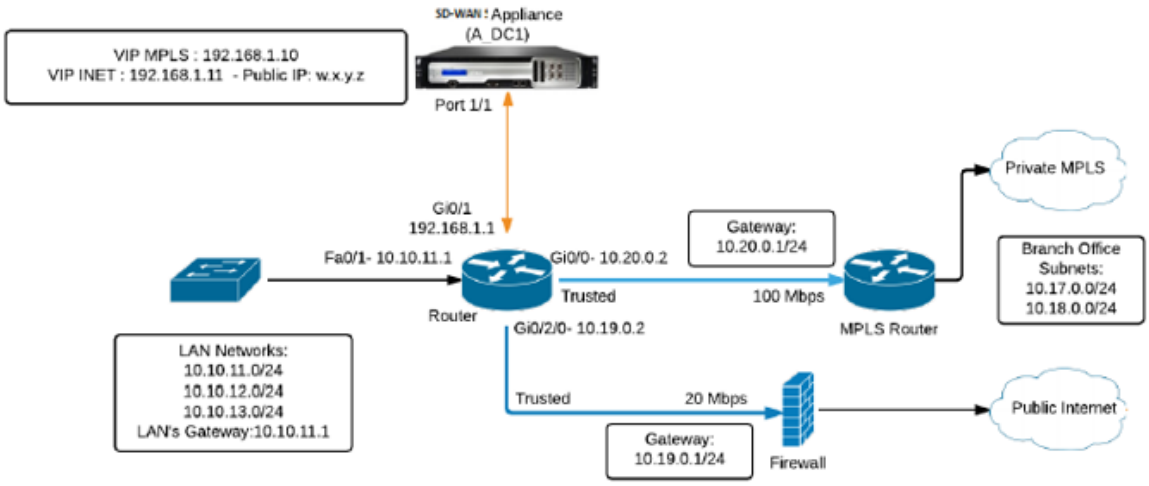
情報を収集する

仮想インラインモードの設定に必要な次の情報を収集します。

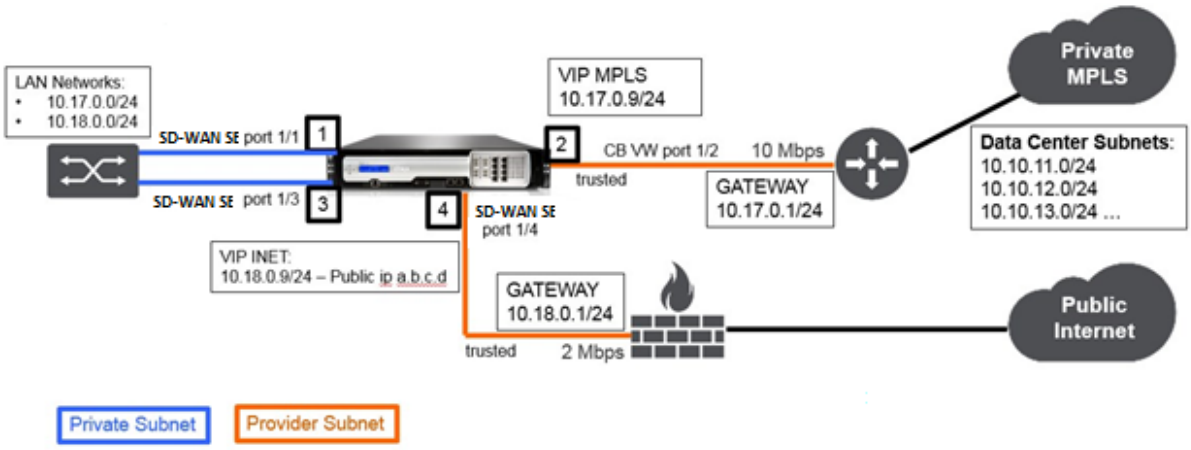
- 以下を含む、ローカルサイトとリモートサイトの正確なネットワーク図
  - ローカルおよびリモートの WAN リンクおよび両方向の帯域幅、サブネット、各リンク、ルート、VLAN からの仮想 IP アドレスおよびゲートウェイ。
- デプロイメントテーブル

次に、ネットワークダイアグラムと配置テーブルの例を示します。

データセンターのトポロジ—仮想インラインモード



ブランチトポロジ—インラインモード



サイト名	データ・センター・サイト	ブランチサイト
アプライアンス名	SJC-DC	SJC-BR
管理 IP	172.30.2.10/24	172.30.2.20/24
セキュリティキー	もしあれば	もしあれば
モデル/ Edition	4000	2000
Mode	仮想インラインモード	インライン
トポロジ	2 x WAN パス	2 x WAN パス
VIP アドレス	192.168.1.10/24 —MPLS, 192.168.2.10/24 —インターネット, パブリック IP w.x.y.z	10.17.0.9/24-MPLS, 10.18.0.9/24 —インターネット, パブリック IP a.b.c.d
Gateway MPLS	10.20.0.1	10.17.0.1
Gateway・インターネット	10.19.0.1	10.18.0.1
リンク速度	MPLS —100 Mbps, インターネット —20 Mbps	MPLS —10 Mbps, インターネット —2 Mbps

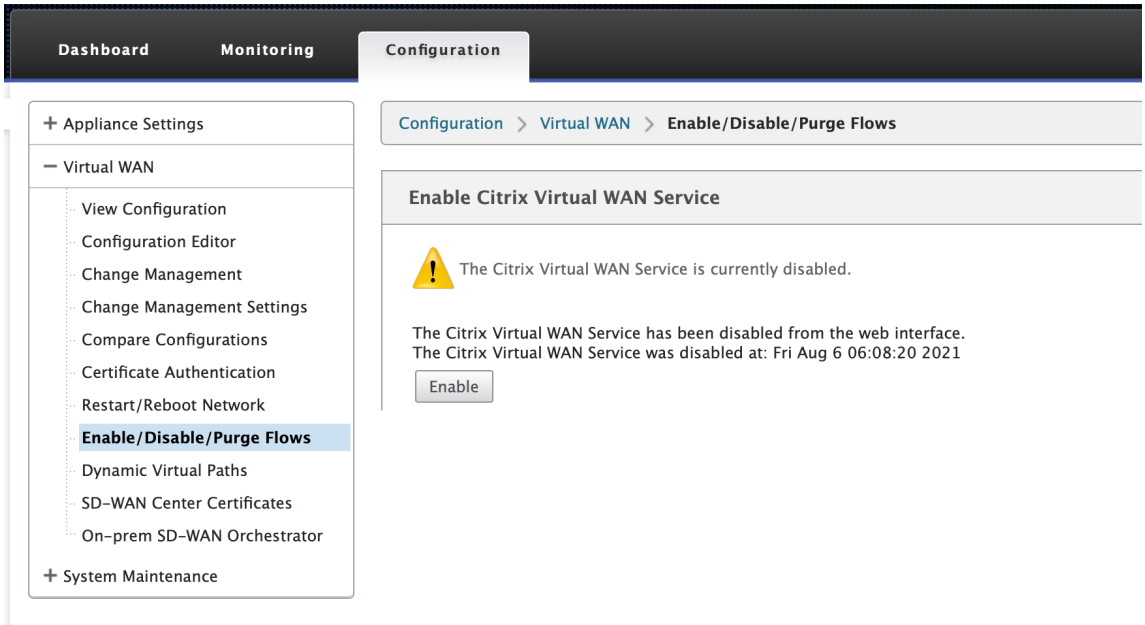
サイト名	データ・センター・サイト	ブランチサイト
Route	物理インターフェイスのいずれかを介して LAN サブネット（10.10.11.0/24、10.10.12.0/24、10.10.13.0/24、など）に到達する方法について、SD-WAN SE アプライアンスのルートを追加する必要があります。Gi0/1-192.168.1.1、構成 **>** 仮想 **WAN >** 設定エディタ **> SJC_DC\ >** ルート。この例では、インターフェイス 192.168.1.1 が使用されています。- なしアドレス:10.10.13.0/24、10.10.12.0/24、10.10.11.0/24、-サービスタイプ: ローカル、-Gateway IP アドレス:192.168.1.1	追加のルートは追加されませんでした
VLAN	MPLS-VLAN 10、インターネット-VLAN 20	なし (デフォルト 0)

前提条件

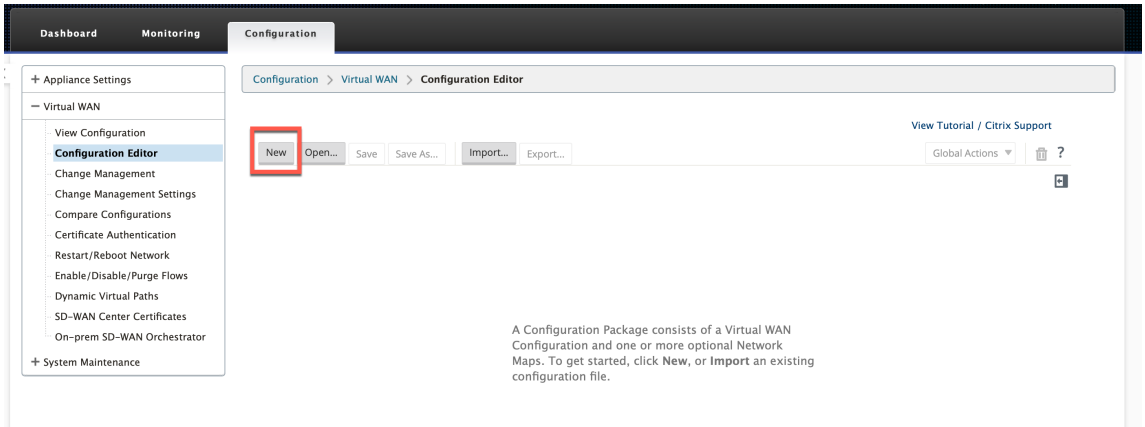
1. SD-WAN アプライアンス Web 管理インターフェイスで、構成 **>** アプライアンスの設定 **>** 管理者インターフェイス **>** その他タブに移動し、スイッチコンソールをクリックします。

   > （注
   >
   > ）[クライアントコンソールに切り替え] が表示されている場合、アプライアンスはすでに MCN モードになっています。SD-WAN ネットワークには、アクティブな MCN が 1 つだけ必要です。

2. **[**** 構成**] > [**仮想 **WAN] > [**フローの有効化**/**無効化**/**消去] に移動し、[**Citrix** 仮想 **WAN** サービスの有効化] セクションで [有効] をクリックします。**



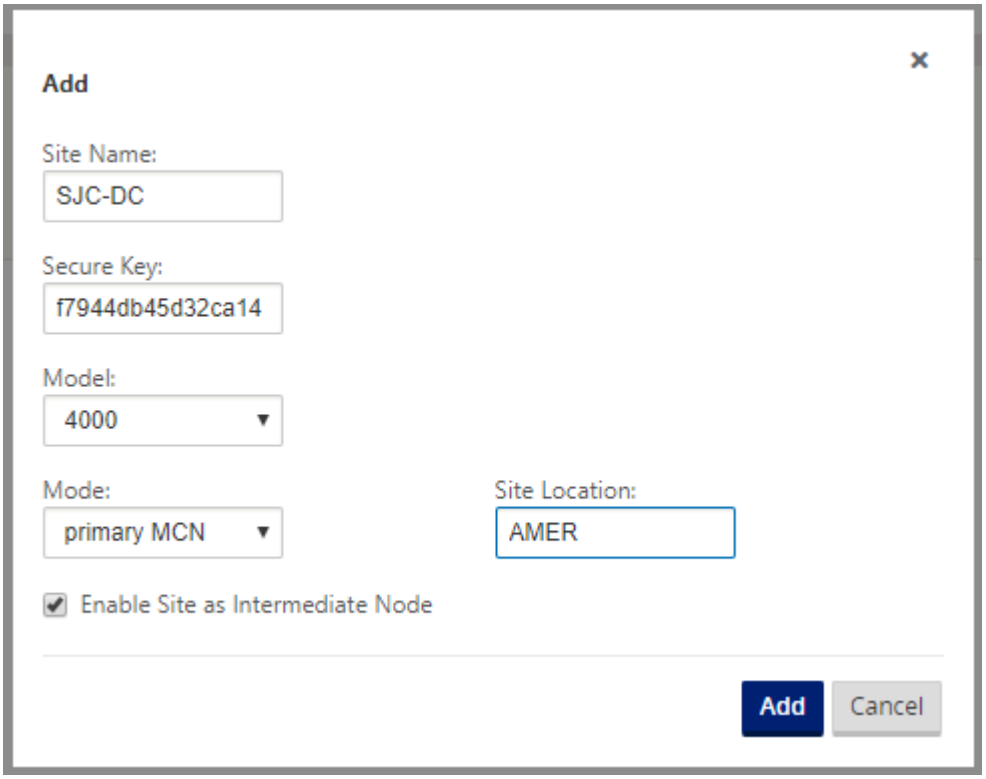
3. 設定 **>** 仮想 **WAN >** 設定エディタに移動して、設定を開始します。[**New**] をクリックして、設定を開始します。[新規] をクリックすると、ファイル名に **Untitled_1** を持つ初期設定ファイルが作成されます。[オプションファイルの名前は] 、後で [名前を付けて保存] ボタンを使用して変更できます。



データセンターサイト-仮想インラインモードの設定

データセンターサイトを作成する

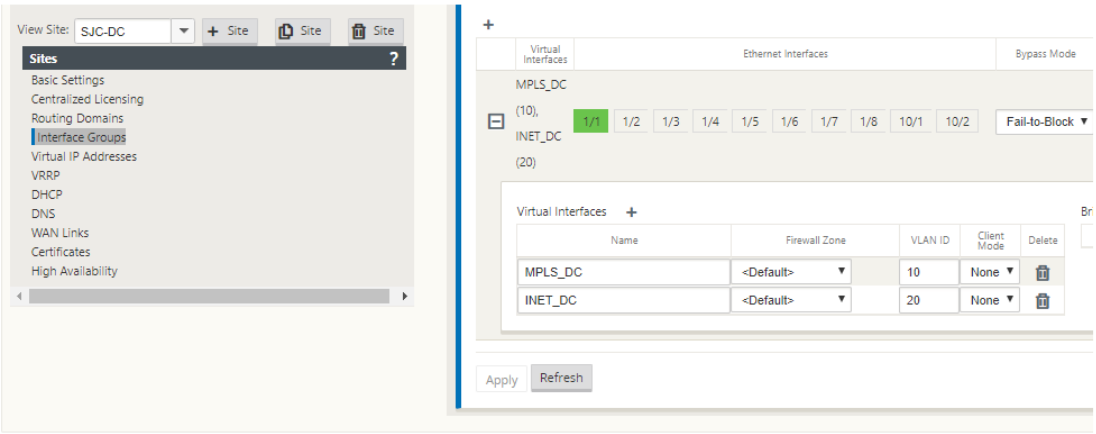
1. 設定 **>** 仮想 **WAN >** 設定エディタ **>** サイトに移動し、**+** サイトをクリックします。
2. サイトの名前と場所を入力します。[モデル（Model）] ドロップダウンリストからアプライアンスモデルを選択し、[モード（Mode）] ドロップダウンリストからプライマリ **MCN** を選択します。
3. [追加] をクリックします。



接続されたイーサネットインターフェイスに基づくインターフェイスグループの設定

仮想インラインモードの設定では、1 つのイーサネットインターフェイス、つまりルーティングポリシーの影響を提供するアップストリームルータを接続するインターフェイスだけが使用されます（例：インターフェイス 1/5）。仮想インターフェイスごとに 1 つのイーサネット/物理インターフェイスだけが使用されるため、バイパスモードは Fail-to-Block（FTB）に設定されます。また、ブリッジペアはありません。

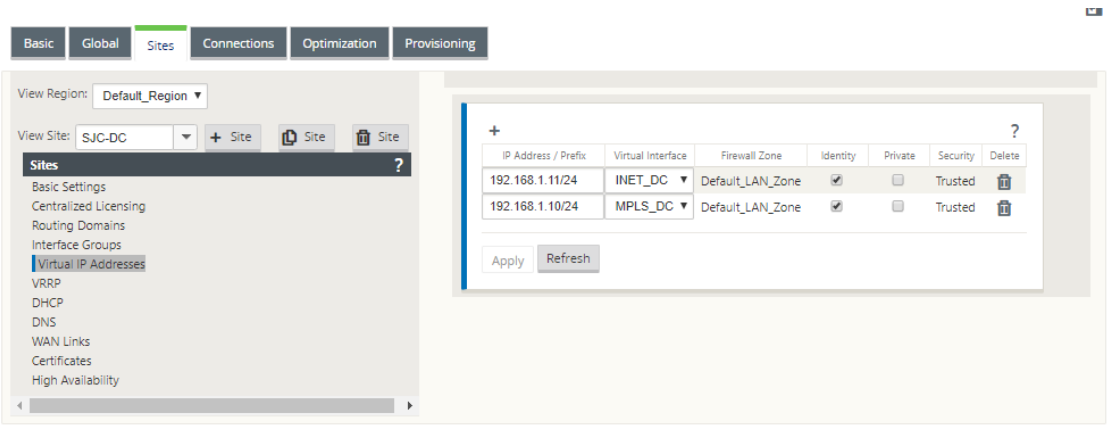
1. 構成エディタで、[サイト] > [**[**サイト名**]] > [**インターフェイスグループ] に移動します。[**+**] をクリックして、使用するインターフェイスを追加します。
2. アップストリームルータに接続するイーサネットインターフェイスを選択し、[仮想インターフェイス（Virtual Interfaces）] の横にある [**+**] をクリックします。MPLS リンクとインターネットリンクの両方の仮想インターフェイスを追加します。サンプルトポロジに従って、以下を追加します。
   - **VLAN 10** に設定された仮想インターフェイス **MPLS**
   - **VLAN 20** に設定された仮想インターフェイスインターネット
3. [バイパスモード] ドロップダウンリストから [**Fail-to-Block**] を選択します。[**Apply**] をクリックします。



仮想インターフェイスごとに仮想 **IP** アドレスを作成する

各 WAN リンクの適切なサブネット上に仮想 IP（VIP）アドレスを作成します。VIP は、仮想 WAN 環境内の 2 つの SD-WAN アプライアンス間の通信に使用されます。

1. 構成エディタで、[サイト**]> [**サイト名**] > [**仮想 **IP** アドレス] に移動します。[**+**] をクリックして VIP を作成します。
2. IP アドレス/プレフィクスを入力し、MPLS とインターネットに対応する仮想インターフェイスを選択します。
3. ［**Apply**］をクリックします。

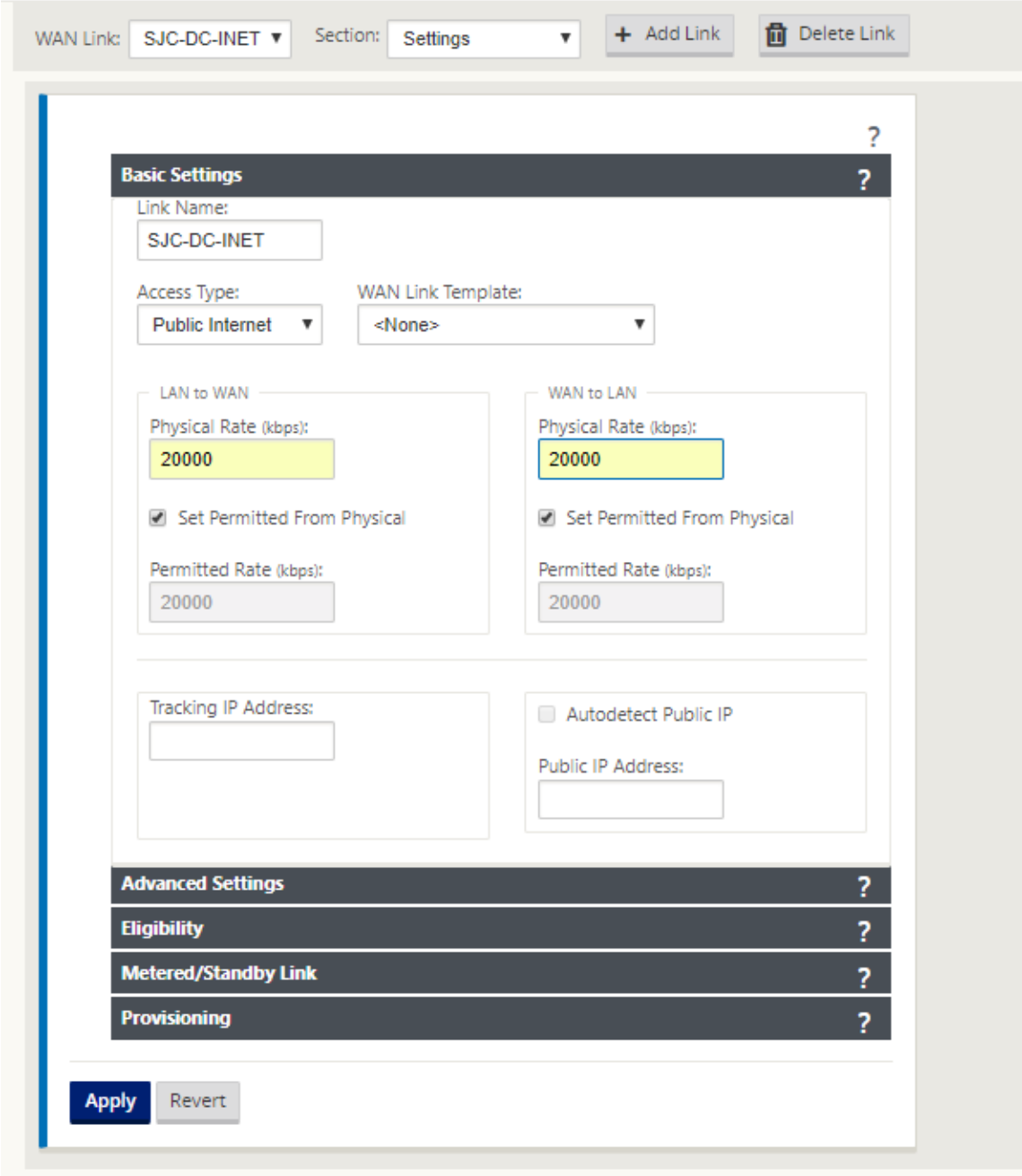


インターネット **WAN** リンクの作成

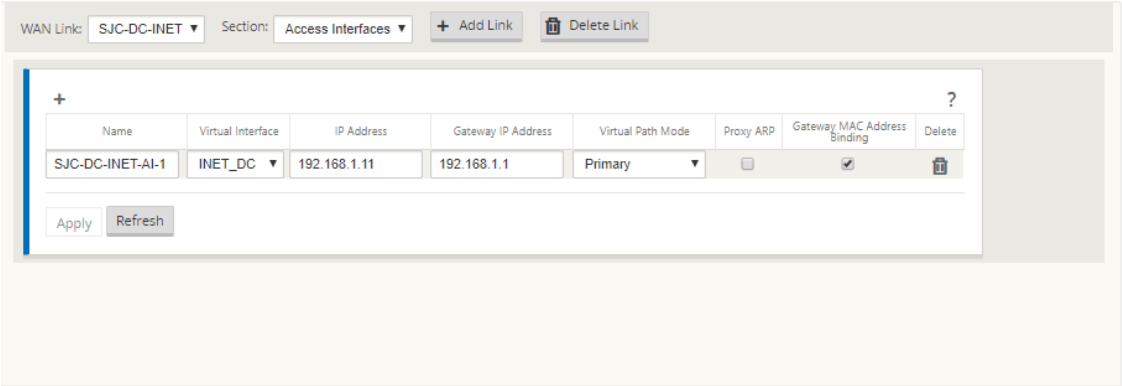
バースト速度ではなく物理レートに基づいてインターネット WAN リンクを作成します。

1. 構成エディタで、[サイト**] >[**サイト名**] > [WAN** リンク] に移動し、[**+** リンク] をクリックします。名前を入力し、[アクセスタイプ] として [パブリックインターネット] を選択します。［追加］をクリックします。

2. 現物レートを入力します。[パブリック **IP** を自動検出する] チェックボックスは選択しないでください。MCN として構成されている SD-WAN アプライアンスの場合、[パブリック **IP** を自動検出] チェックボックスは選択できません。

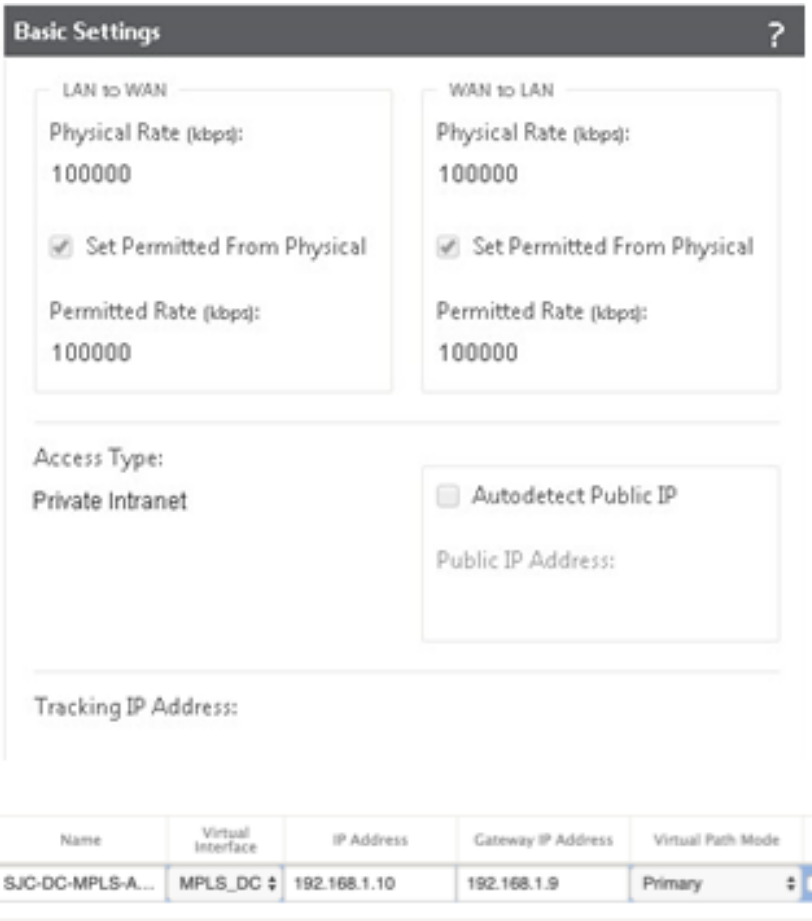


3. [セクション（**Section**）] ドロップダウンリストから [アクセスインターフェイス（Access Interfaces）] を選択し、[**+**] ボタンをクリックして、インターネットリンクに固有のインターフェイスの詳細を追加します。
4. インターネット WAN 仮想 IP アドレスとゲートウェイアドレスを入力します。プロキシ ARP では、イーサネットインターフェイスが 2 つ未満の場合はチェックされません。
5. [**Apply**] をクリックします。

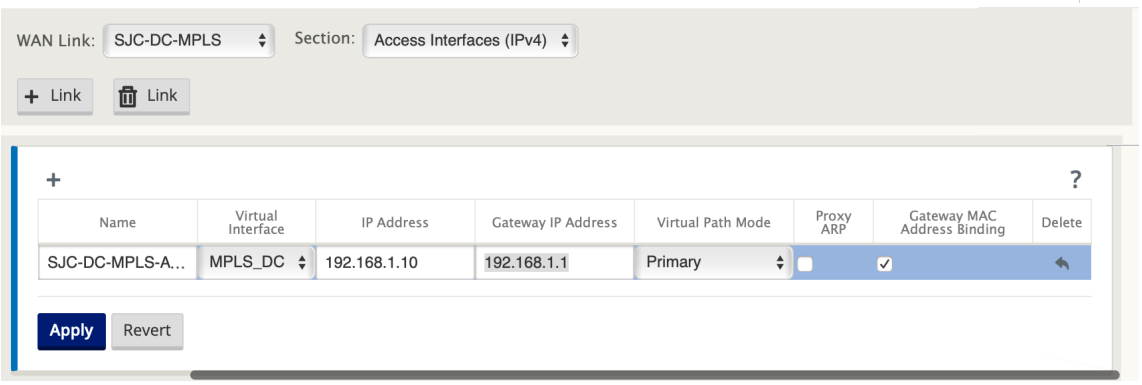


MPLS リンクの作成

1. [サイト**] > [**サイト名**] > [WAN** リンク] ページで、[セクション] ドロップダウンリストから [設定] を選択します。[**+** リンク（**+ Link** ）] ボタンをクリックして、MPLS 用の WAN リンクを追加します。
2. MPLS WAN リンク名を入力し、[アクセスタイプ] を [プライベートイントラネット] として選択します。[追加] をクリックします。
3. 現物レートおよびその他の詳細を入力します。[**Apply**] をクリックします。



4. [セクション（**Section** ）] ドロップダウンリストから [アクセスインターフェイス（Access Interfaces）] を選択し、[**+**] ボタンをクリックして、MPLS リンクに固有のインターフェイスの詳細を追加します。
5. MPLS 仮想 IP アドレスと Gateway アドレスを入力します。プロキシ ARP では、イーサネットインターフェイスが 2 つ未満の場合はチェックされません。
6. [**Apply**] をクリックします。



ルートを設定する

データセンター側で、任意の物理インターフェイスを経由して LAN サブネット（10.10.11.0/24、10.10.12.0/24、10.10.13.0/24 など）に到達する方法について、SD-WAN アプライアンスにルートを追加します。

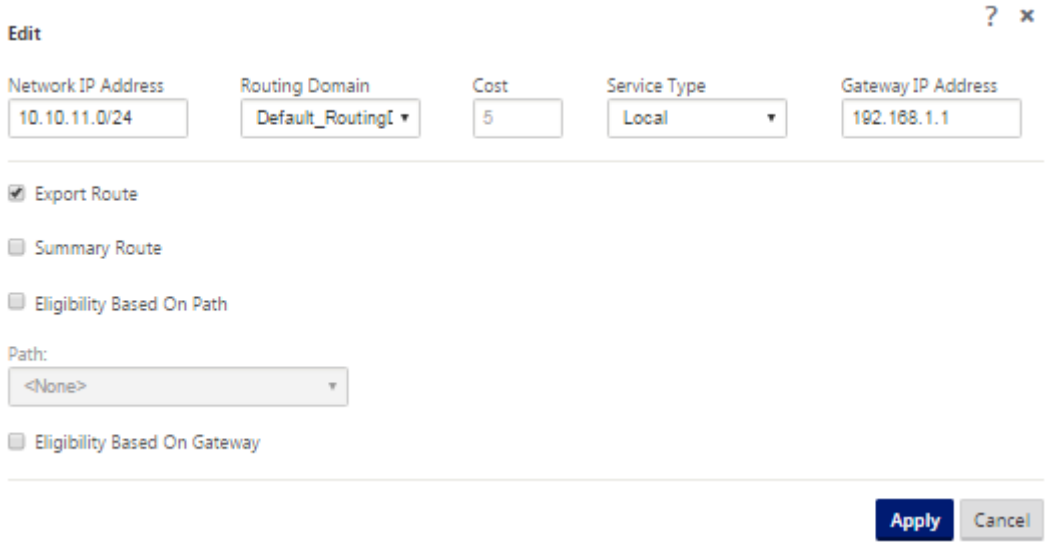
VLAN 10 上の 0/1/0.1 —192.168.1.1

VLAN 20 上の 0/1/0.2 —192.168.2.1

この例では、インターフェイス 192.168.1.1 が使用されています。

設定エディタで、[接続**] > [**ルート] に移動し、[**+**] をクリックしてルートを追加します。

ネットワーク **IP** アドレス、コスト、および **Gateway** アドレスを入力します。［追加］をクリックします。

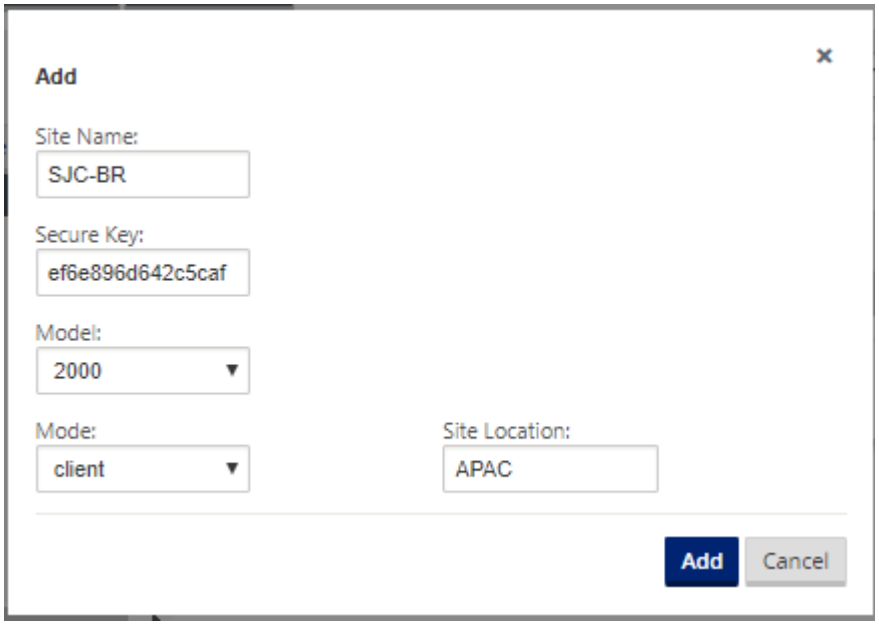


Order	Network IP Address	Cost	Service Type	Service Name	Gateway IP Address	Info	Edit	Delete
1	10.10.13.0/24	5	Local		192.168.1.1			
2	10.10.12.0/24	5	Local	BR571	192.168.1.1			
3	10.10.11.0/24	5	Local	BR572	192.168.1.1			
4	192.175.60.0/24	5	Virtual Path	BR573				
5	192.175.61.0/24	5	Virtual Path	BR574				
6	192.175.62.0/24	5	Virtual Path	BR575				
7	172.111.64.5/24	5	Local					

ブランチサイトのインライン展開設定

ブランチサイトの作成

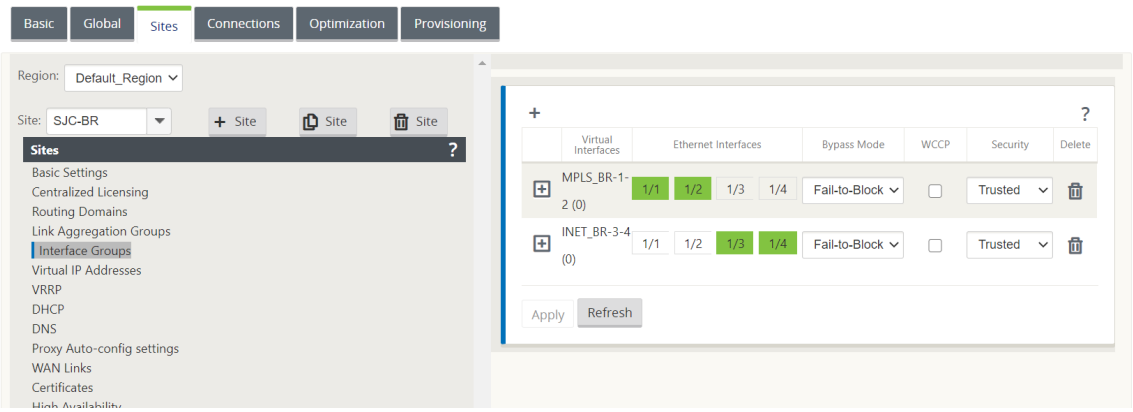
1. [構成エディタ**] > [**サイト] に移動し、[**+** サイト] をクリックします。
2. サイトの名前と場所を入力します。[Model] ドロップダウンリストからアプライアンスモデルを選択し、[**Mode**] ドロップダウンリストから [**Client**] を選択します。
3. [追加] をクリックします。



接続されたイーサネットインターフェイスに基づくインターフェイスグループの設定

1. 構成エディタで、[サイト] **> [[**クライアントサイト名**]] > [**インターフェイスグループ] に移動します。[**+**] をクリックして、使用するインターフェイスを追加します。インラインモード設定では、インターフェイスペア 1/3、1/4、インターフェイスペア 1/1 および 1/2 の 4 つのイーサネットインターフェイスが使用されます。
2. 仮想インターフェイスごとに 2 つのイーサネット/物理インターフェイスが使用されるため、バイパスモードを fail-to-Wire に設定します。ブリッジペアは 2 つあります。
3. [仮想インターフェイス] の横にある [**+**] をクリックし、インターネットおよび MPLS リンクを使用して、バースト速度ではなく物理レートに基づいて WAN リンクを設定します。
   - ブリッジペア 1/3 および 1/4 に設定された仮想インターフェイスインターネット
   - ブリッジペア 1/1 および 1/2 に設定された仮想インターフェイス **MPLS** 。
4. [**Bridge Pairs**] の横にある [**+**] をクリックし、適切なインターフェイスを選択してブリッジペアを作成します。

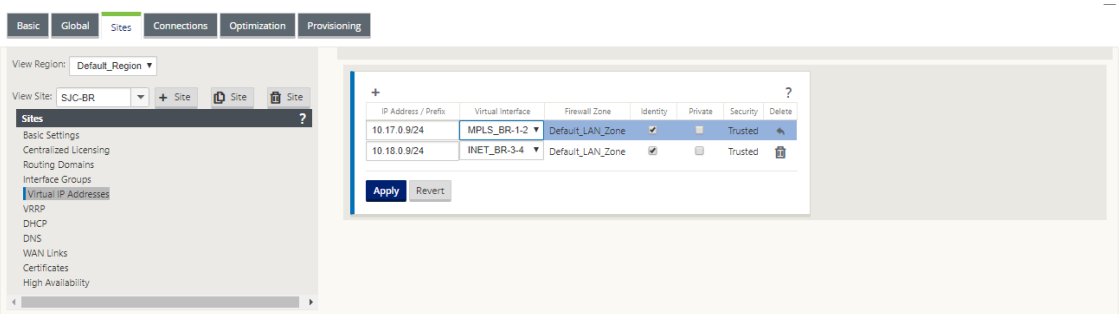
「前提条件 」セクションの「ブランチトポロジ-インラインモードトポロジ図」を参照し、インターフェイスグループを入力します。



各仮想インターフェイスの仮想 **IP**（**VIP**）アドレスを作成

各 WAN リンクの適切なサブネット上に仮想 IP アドレスを作成します。VIP は、仮想 WAN 環境内の 2 つの SD-WAN アプライアンス間の通信に使用されます。

1. 構成エディタで、[サイト**]> [**サイト名**] > [**仮想 **IP** アドレス] に移動します。[**+**] をクリックして VIP を作成します。
2. IP アドレス/プレフィクスを入力し、MPLS とインターネットに対応する仮想インターフェイスを選択します。
3. [**Apply**] をクリックします。

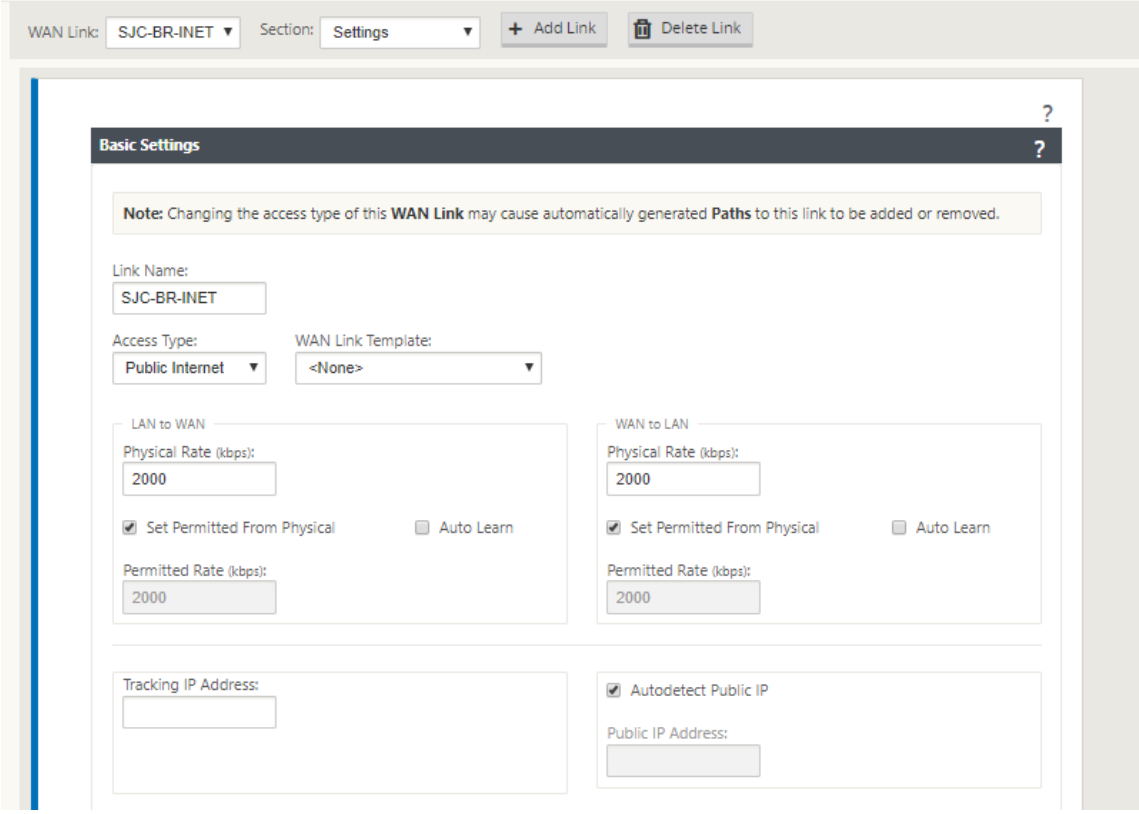


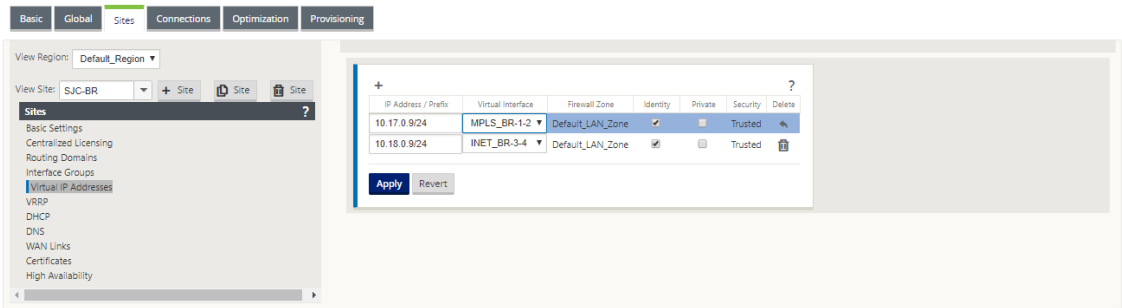
インターネット **WAN** リンクの作成

インターネットリンクを使用してバースト速度ではなく、物理レートに基づいて WAN リンクを設定するには

1. [**WAN** リンク] に移動し、[**+** リンク] ボタンをクリックして、インターネットリンクの WAN リンクを追加します。名前を入力し、[アクセスタイプ] として [パブリックインターネット] を選択します。[追加] をクリックします。

2. インターネットリンクの詳細を入力し、[パブリック **IP** アドレスを自動検出する] チェックボックスをオンにします。
3. [セクション（**Section** ）] ドロップダウンリストから [アクセスインターフェイス（Access Interfaces）] を選択し、[**+**] をクリックして、インターネットリンクに固有のインターフェイスの詳細を追加します。
4. インターネット WAN 仮想 IP アドレスとゲートウェイアドレスを入力します。プロキシ ARP では、イーサネットインターフェイスが 2 つ未満の場合はチェックされません。

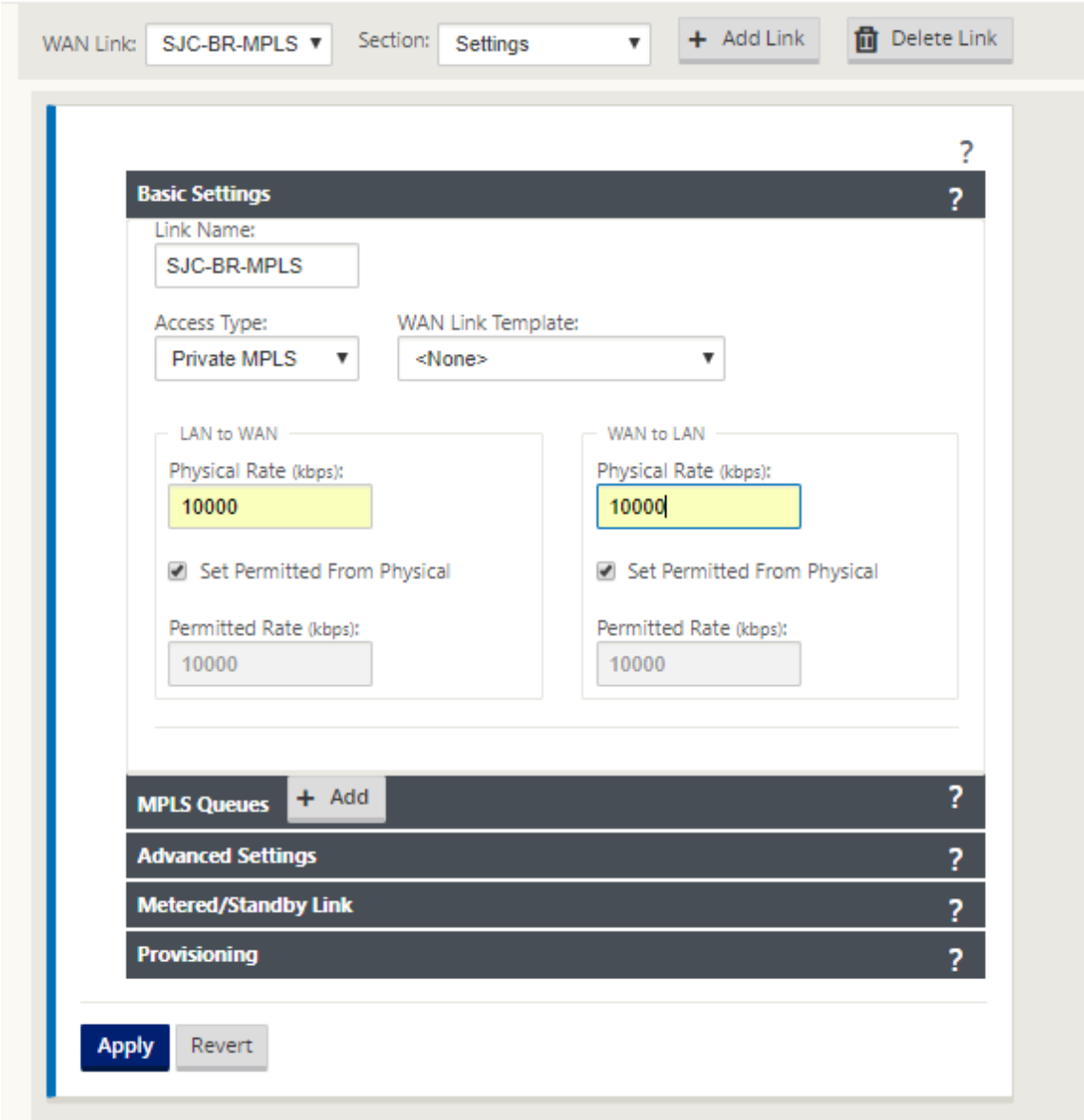




MPLS WAN リンクの作成

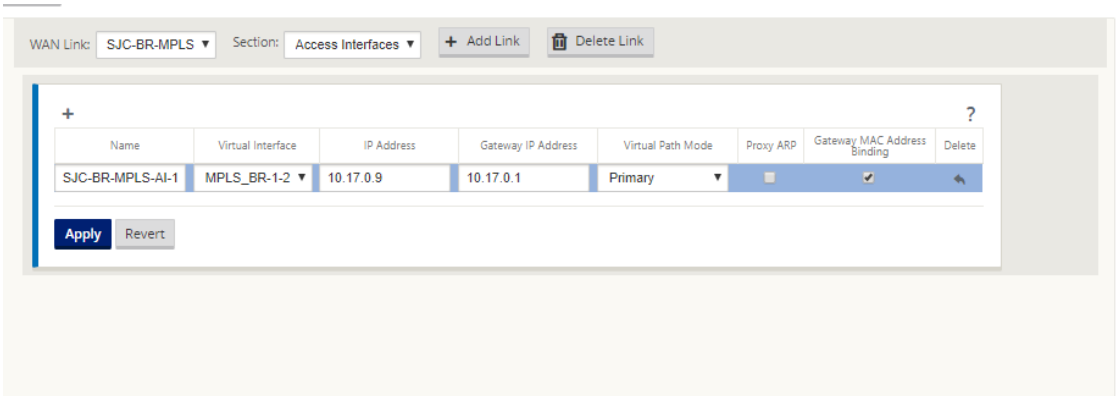
1. [**WAN** リンク] に移動し、[セクション] ドロップダウンリストから [設定] を選択します。[**+** リンク（**+ Link** ）] ボタンをクリックして、MPLS リンクの WAN リンクを追加します。

2. MPLS WAN リンク名およびその他の詳細を入力します。[アクセスタイプ] を [プライベートイントラネット] として選択します。



3. [セクション（**Section**）] ドロップダウンリストから [アクセスインターフェイス（Access Interfaces）] を選択し、[**+**] ボタンをクリックして、MPLS リンクに固有のインターフェイスの詳細を追加します。

4. MPLS 仮想 IP アドレスと Gateway アドレスを入力します。プロキシ ARP では、イーサネットインターフェイスが 2 つ未満の場合はチェックされません。

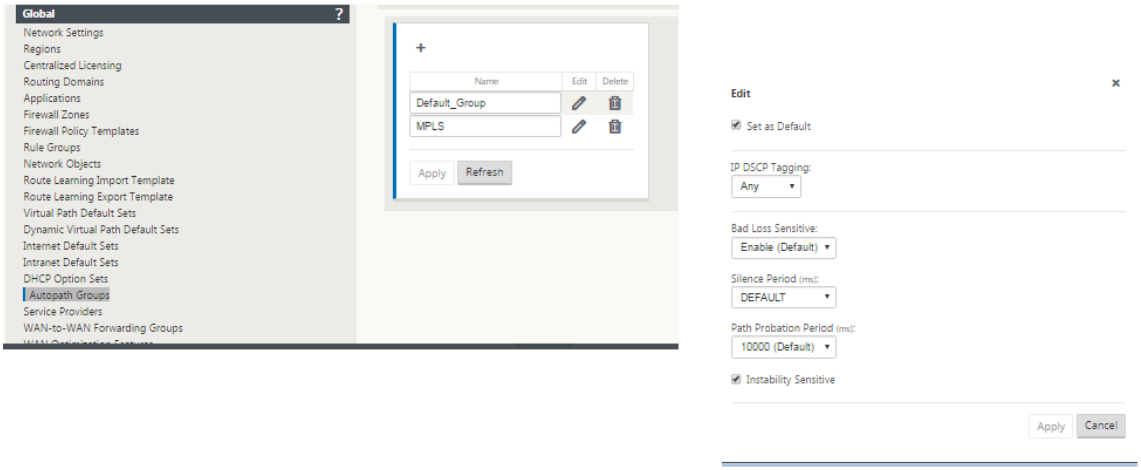


ルートを設定する

ルートは、前の設定に基づいて自動作成されます。このリモートブランチオフィスに固有のサブネットがさらに存在する場合は、それらのバックエンドサブネットに到達するためにトラフィックを転送するゲートウェイを識別する特定のルートを追加する必要があります。

オートパスグループの作成

1. 構成エディタで、[グローバル**] > [Autopath Groups**] に移動します。[**+**] をクリックします。
2. 名前を入力し、[適用] をクリックします。
3. 要件に従って Autopath グループを設定し、[**Apply**] をクリックします。



4. [接続**] > [WAN** リンク] に移動します。[WAN リンク（WAN **Links**）**]** ドロップダウンリストからインターネット **WAN** リンクを選択し、[セクション（**Section** ）] ドロップダウンリストから仮想パスを選択します。
5. [使用] チェックボックスをオンにし、各サイト（データセンターとブランチの両方）のイントラネット WAN リンクの [**Autopath Group]** チェックボックスから、新しく作成したオートパスグループを選択します。

2 つの Autopath Group をデフォルトとしてマークすることはできません。マークされている場合、監査エラーが発生します。

アクセスタイプが [プライベートイントラネット] の WAN リンクの仮想パスを手動で追加すると、[パス] の下に仮想パスが設定されます。

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

監査エラーの解決

データセンターサイトとブランチサイトの構成が完了すると、DC サイトと BR サイトの両方で監査エラーを解決するように警告されます。監査エラーを解決します (存在する場合)。

SD-WAN ネットワークの構築

May 10, 2021

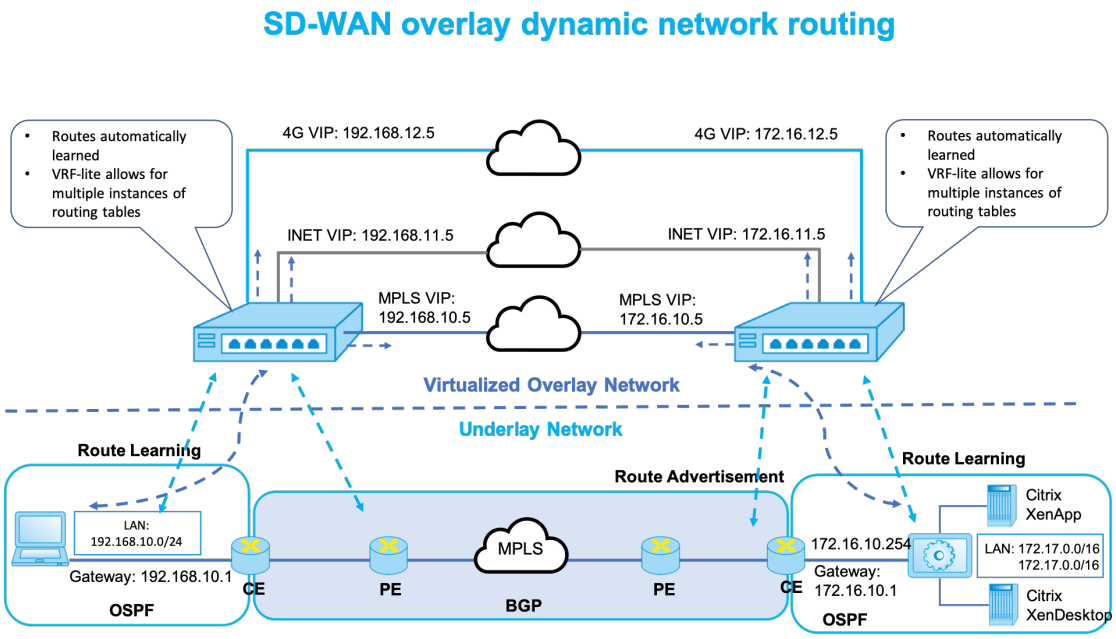
SD-WAN オーバーレイルートテーブルを構築せずに SD-WAN オーバーレイネットワークを構築するには、次の手順を実行します。

1. 2 つの SD-WAN アプライアンス間の各 WAN リンクにわたって WAN パストンネルを作成します。
2. 各 WAN リンクのエンドポイントを表すように仮想 IP を設定します。現在の L3 ネットワークを介して暗号化された WAN パスを確立できます。
3. 2、3、および 4 つの WAN パス（物理リンク）を 1 つの仮想パスに集約すると、最もインテリジェントでコスト効率が悪い既存のアンダーレイではなく、SD-WAN オーバーレイネットワークを利用してパケットを WAN を通過できるようになります。

SD-WAN ルーティングコンポーネントとネットワークトポロジ

- Local：サブネットがこのサイトに存在する（SD-WAN 環境にアドバタイズされる）
- 仮想パス—仮想パスを通じて、選択したサイト・アプライアンスに送信されます。
- イントラネット—SD-WAN アプライアンスがないサイト

- インターネット—インターネットにバインドされたトラフィック
- パススルー：手つかずのトラフィック、一方のブリッジインターフェイスで他方のブリッジインターフェイスへ
- デフォルトルート（0.0.0.0/0）定義-SD-WAN オーバーレイルートテーブルによってキャプチャされないパススルートラフィックに使用されます。または MCN で使用され、インターネットトラフィックのバックホールのためにすべてのトラフィックを MCN ノードに転送するようにクライアントサイトに指示します。



Premium（エンタープライズ）エディションでのみ WAN 最適化

May 10, 2021

SD-WAN Premium（エンタープライズ）エディション・アプライアンスには、WAN 仮想化に加えて、フル機能の WAN Optimization 機能が搭載されています。一部のお客様は、SD-WAN サービスに移行する前に WAN Optimization 機能を実装することを好む場合があります。この導入ユースケースでは、Premium (Enterprise) Edition アプライアンスを利用して WAN 最適化サービスを利用するための手順について説明します。

Citrix SD-WAN 製品プラットフォームエディションには、次のアプライアンスが含まれます。

- SD-WAN: SD-WAN Standard Edition アプライアンス
- Premium (エンタープライズ): SD-WAN Premium (エンタープライズ) エディションアプライアンス
- WANOP: SD-WAN WANOP Edition アプライアンス

Premium (Enterprise) Edition アプライアンスを既存の分散 WANOP ネットワークに統合するには、DC サイトで SD-WAN (物理または仮想) アプライアンスを MCN として構成します。SD-WAN アプライアンスは、ネットワークのすべての構成を管理します。ブランチサイトと DC サイトの MCN の間に仮想パスが確立されます。この仮想パスは、アプライアンス間の制御トラフィックの送信にのみ使用されます。ブランチアプライアンスでは、データトラフィックはイントラネットサービスとして処理されます。イントラネットトラフィックはカプセル化されず、既存の WAN リンクを経由して DC サイトに到達します。DC サイトの WANOP アプライアンスは、エンドツーエンドのトラフィック最適化を提供するために、トラフィックパス内に配置する必要があります。

ヘッドエンドに SD-WAN ハードウェアアプライアンスを持たないお客様のサイトでは、HA ペアの VPX アプライアンス（2 つの仮想 WAN VPX）をワンアームモードで MCN として使用できます。ワンアームモードの場合、トラフィックを SD-WAN アプライアンスにリダイレクトするには、サードパーティルータの PBR 規則が必要です。

このドキュメントでは、DC サイトアプライアンスが冗長性のために HA モードで展開されていることを前提としています。この展開では、HA モードは必須ではありません。

前提条件

- DC サイトに HA モードで展開された WANOP アプライアンスのペアと SD-WAN アプライアンスのペア。
- ブランチサイトの Premium (エンタープライズ) エディションアプライアンス。

ネットワークトポロジ

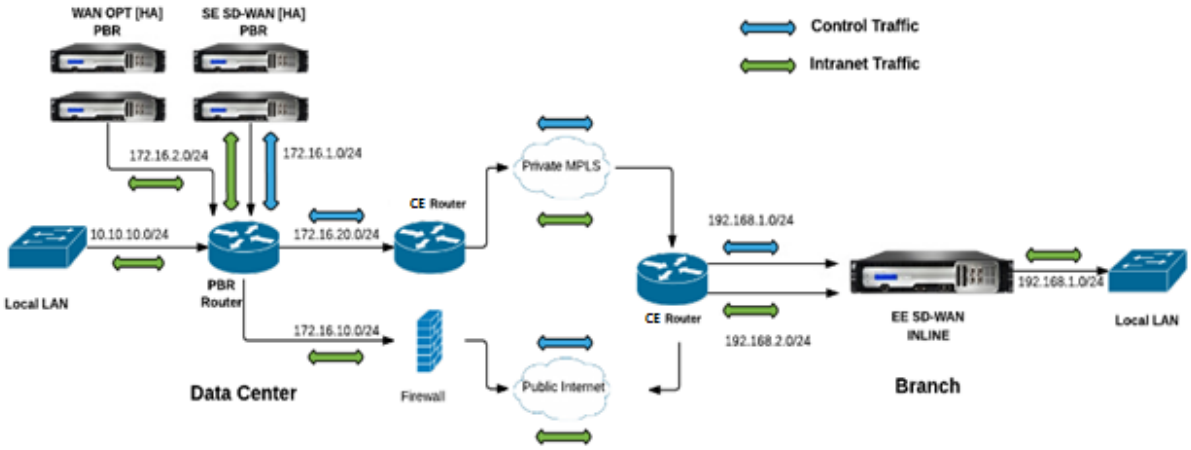
PBR 導入における **SD-WAN** スタンダードエディションおよび **WANOP** アプライアンス：

次の図では、DC サイトの SD-WAN SE アプライアンスと WAN OP アプライアンスの両方がワンアームモードで展開されています。SD-WAN アプライアンスは PBR 展開をサポートし、WANOP アプライアンスは PBR と WCCP の両方をサポートします。DC サイトの WAN から受信した制御トラフィック（仮想パストラフィック）は、PBR ルータによって SD-WAN アプライアンスにリダイレクトされます。データトラフィックは、PBR ルータによって WAN Optimization アプライアンスにリダイレクトされます。

WAN から DC LAN へのトラフィックフロー：

- CE（カスタマーエッジ）ルータ-> PBR ルータ-> SD-WAN-> PBR ルータ-> LAN
- CE（カスタマーエッジ）ルータ-> PBR ルータ-> WAN OPT-> PBR ルータ-> LAN

同じトラフィックフローが逆方向に続きます。



PBR モードの **SD-WAN** スタンダードエディション、インライン展開での **WANOP**:

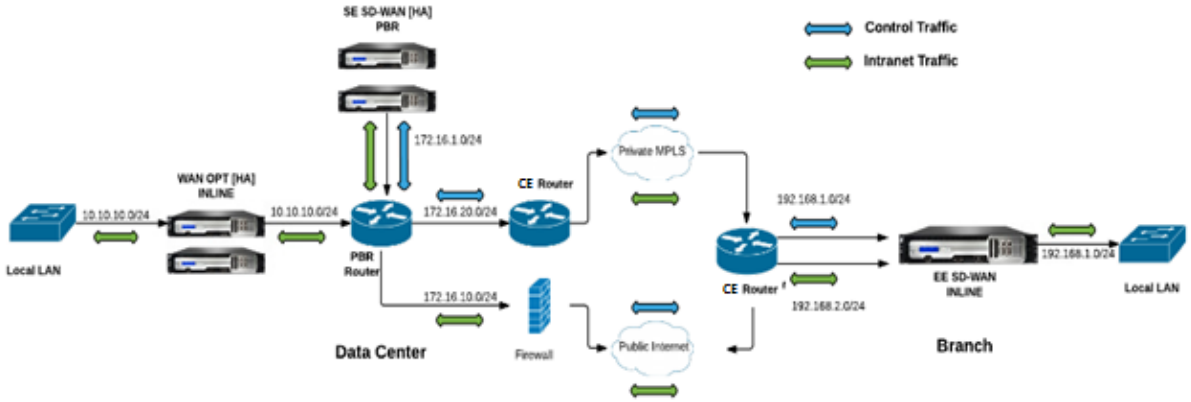
次の図では、DC サイトの SD-WAN アプライアンスはワンアームモードでデプロイされ、WANOP アプライアンスはインラインモードでデプロイされます。

DC サイトの WAN から受信した制御トラフィック（仮想パストラフィック）は、PBR ルータによって SD-WAN アプライアンスにリダイレクトされます。データトラフィックは、PBR ルータによって WAN Optimization アプライアンス（インライン）に転送されます。

WAN から DC LAN へのトラフィックフロー:

- CE（カスタマーエッジ）ルータ-> PBR ルータ-> SD-WAN-> PBR ルータ-> LAN
- CE（カスタマーエッジ）ルータ-> PBR ルータ-> WAN OPT-> LAN

同じトラフィックフローが逆方向に続きます。



構成の手順

1. DC [MCN] で SD-WAN アプライアンスを構成して、DC サイトとブランチサイト間の仮想パスを確立します。

   構成, MCN とクライアント間の仮想パスサービスを参照してください。

2. DC サイトでイントラネットサービスを構成します。

   a) MCN (DC サイト) で、**[**構成**] > [**仮想 **WAN] > [**構成エディタ**] > [**接続**] > [**サイト **(DC)] > [**イントラネットサービス] の順に選択します。**[+]** 記号をクリックして、イントラネットサービスを追加します。

   b) [イントラネットサービス] の 1 つ以上の WAN リンクを選択し、[適用] をクリックします。

   c) 同じ サイト **(DC)** の下の [ルート] に移動し、[**[+]** 記号] をクリックしてコストが 5 未満のリモートネットワークを追加し、[追加] をクリックします。

      たとえば、[ネットワーク **IP** アドレス] フィールドに **192.168.1.0/24** と入力し、[イントラネット] として [サービスタイプ] を選択します。

      > 注
      >
      > イントラネットルートが優先されるためには、各サイトのコストを 5 未満にする必要があります。

3. ブランチサイトでイントラネットサービスを構成します。

   a) ブランチサイトで、上記の 手順 **2** のサブステップ a から c を繰り返します。

      たとえば、[ネットワーク IP アドレス] フィールドに **172.16.1.0/24** と入力し、[イントラネット] として [サービスタイプ] を選択します。

4. 変更管理 を実行して、構成をブランチサイトにアップロードおよび配布します。

「構成パッケージと変更管理のエクスポート」を参照してください。

デフォルトでは、トラフィックは仮想パスを経由して、ブランチから DC に送信されます。

> 注
>
> PBR ルータは、提供された展開手順に従って、トラフィックをリダイレクトするように設定する必要があります。

WAN Optimization の設定の詳細については、有効化-設定-WAN 最適化を参照してください。

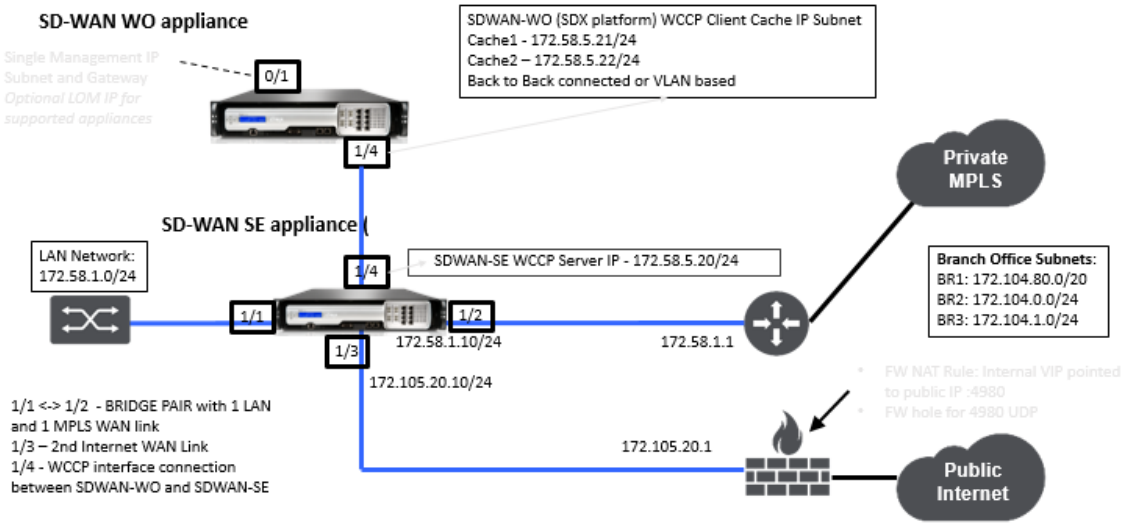
2 ボックスモード

May 10, 2021

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

2 ボックスモードは、次のアプライアンスモデルでのみサポートされます。

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



注

Two Box モードが有効の場合、高可用性および WCCP 配置モードにアクセスできません。ただし、これらの展開モードは、ユーザーが管理するために使用できます。

重要

- Two Box Mode が有効の場合、レガシー WCCP 配置は無効になりますが、サービスグループのコンバージェンスは WCCP モニタリングページからしか確認できません。Two BoxMode の監視セクションの下に個別の GUI ページはありません。
- Standard Edition アプライアンスで実行されている WCCP プロセスが、短い時間間隔内に複数回、たとえば 1 分間に 3 回再起動すると、サービスグループは自動的にシャットダウンします。このようなシナリオでは、WANOP アプライアンスで WCCP コンバージェンスを取得するには、WANOP アプライアンスの Web GUI で WCCP 機能を再度有効にします。
- Standard Edition アプライアンスの構成に関連する WCCP 構成または WAN 最適化に変更があると、外部 WANOP アプライアンスがリブートします。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 つのボックスモードを実装する際には、次の点に注意してください。

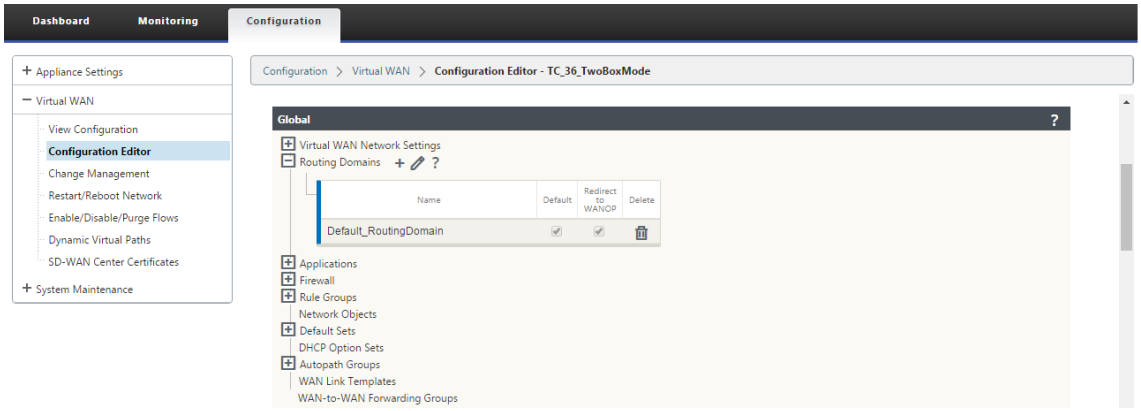
- 構成エディタから WANOP アプライアンスにリダイレクトするようにルーティングドメインを選択した場合は、WCCP が有効になっているインターフェイスグループに追加する必要があります。
- パートナーサイトでも、同じルーティングドメインのトラフィックを選択する必要があります。たとえば、**MCN** > **Branch01** では、WAN 最適化のメリットを観察できます。

> - WCCP が有効になっているインターフェイスグループでルーティングドメインが選択されている場合、ブリッジドインターフェイスを含む別のインターフェイスグループには、同じルーティングドメインが設定されている必要があります。WCCP 対応のインターフェイスグループにルーティングドメインが設定されている場合にのみ、WAN 最適化の利点を備えたエンドツーエンドのトラフィックフローを送信するだけでは不十分です。

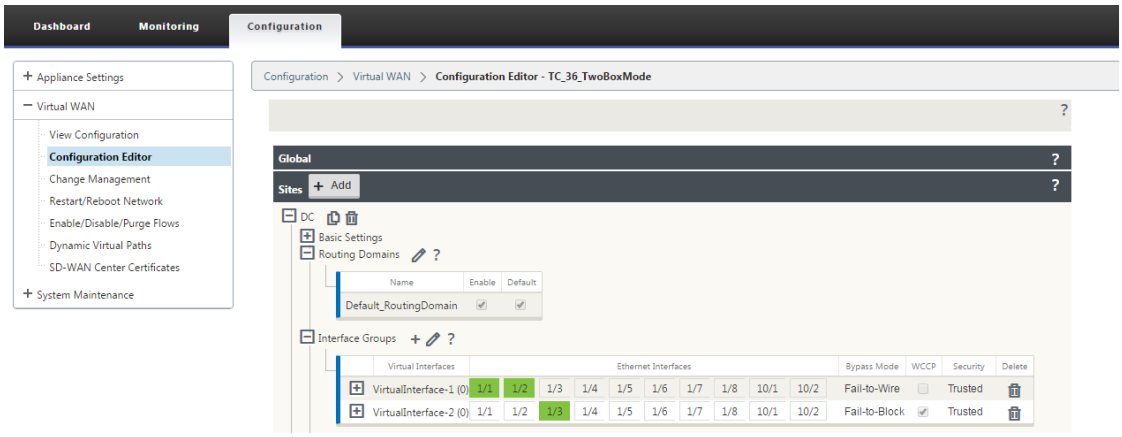
Citrix SD-WAN 標準版

DC サイトまたはブランチサイトの Standard Edition アプライアンスで 2 ボックスモードソリューションを構成するには、次の手順を実行します。

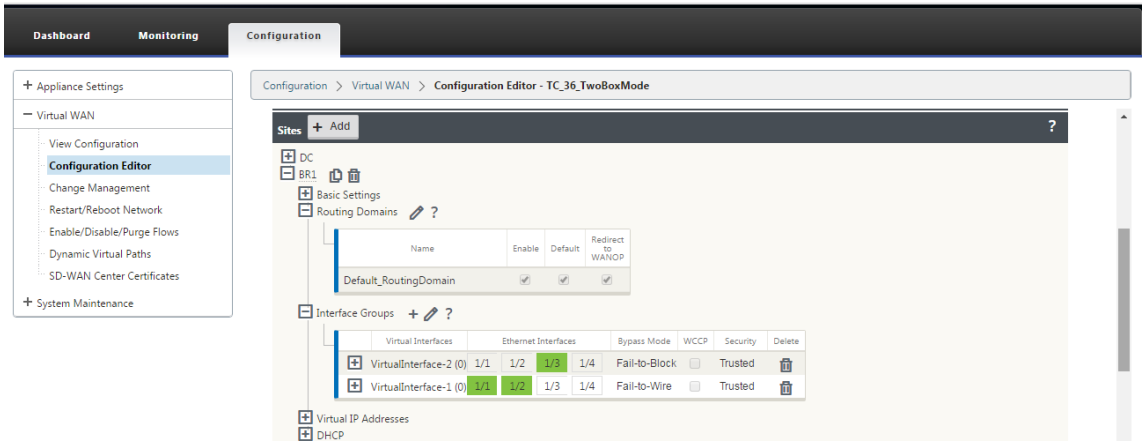
1. SD-WAN SE Web 管理インターフェイスで、[構成] > [仮想 **WAN**] > [構成エディタ] に移動します。既存の構成パッケージを開くか、パッケージを作成します。
2. 選択した構成パッケージで、[**Advanced**] タブに移動して構成の詳細を表示します。
3. [グローバル 設定] を開き、[ルーティングドメイン] を展開し、[**WANOP** にリダイレクト] チェックボックスが有効になっていることを確認します。



4. DC を展開して、アプライアンスが有効になっている 仮想 ネットワーク インターフェイスを示すインターフェイスグループ 設定で、仮想インターフェイスの **WCCP** を有効にします。



5. [サイト **+** 追加] を展開し、ブランチルーティングドメインとインターフェイスグループの設定を表示します。ブランチサイトの [**WANOP** へのリダイレクト] チェックボックスは、ルーティングドメインに対して有効になっています。

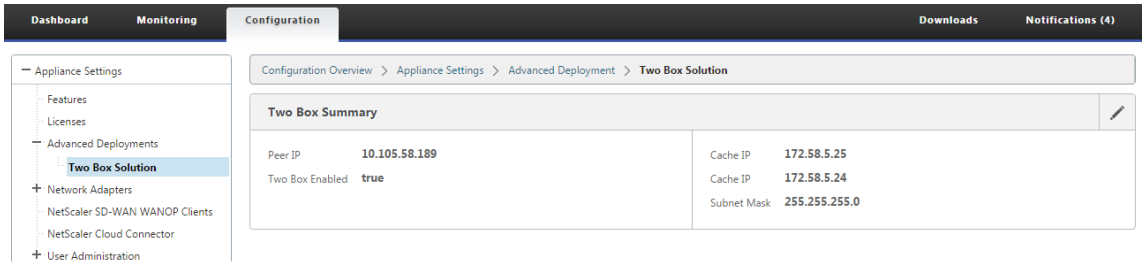


> 注
>
> WCCP リスナーは、イーサネットインターフェイスが 1 つだけ設定されている仮想ネットワークインターフェイスに対してだけ有効にする必要があります。ブリッジドペアで WCCP リスナーを有効にしないでください。SD-WAN SE アプライアンスと SD-WAN WANOP アプライアンス間の ONE-ARM インターフェイスで有効にすることを意図しています。

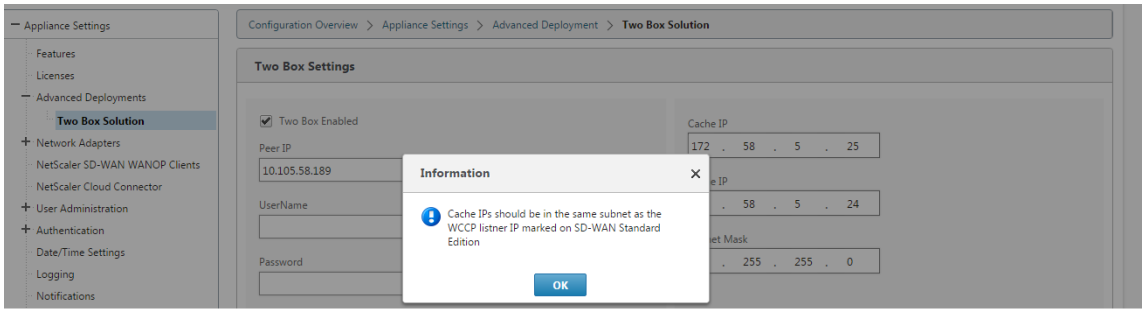
Citrix SD-WAN WANOP 構成

SD-WAN WANOP アプライアンス Web GUI で 2 ボックス配置モードを設定するには、次の手順を実行します。

1. SD-WAN WANOP ウェブ管理インターフェイスで、「構成」>「アプライアンスの設定」>「高度な展開」>「T**wo Box** ソリューション」の順に選択します。



2. **2** ボックスモードの設定を編集するには、**[**編集**]** アイコンをクリックします。キャッシュ **IP** の情報ダイアログが表示されます。[**OK**] をクリックします。



3.「**2** ボックス有効」チェックボックスを有効 にします。

4. ピア **IP** を入力します。ピア IP は、SD-WAN StandardEdition アプライアンスの IP アドレスです。

5. ユーザー資格情報を入力し、[**Apply**] をクリックします。

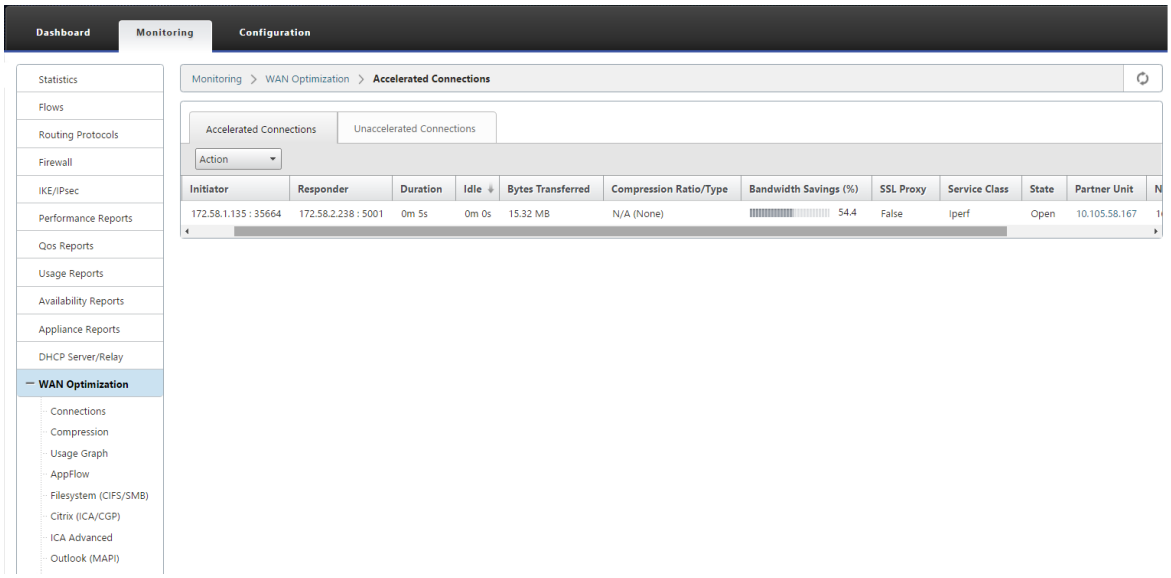
2 ボックスモードの構成と管理性

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

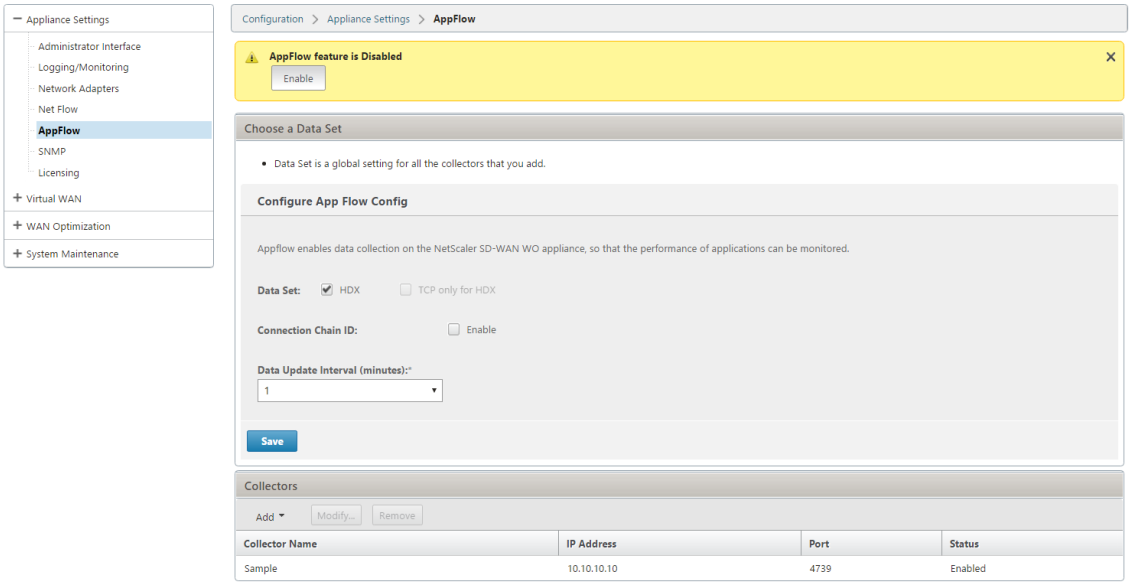
監視

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。



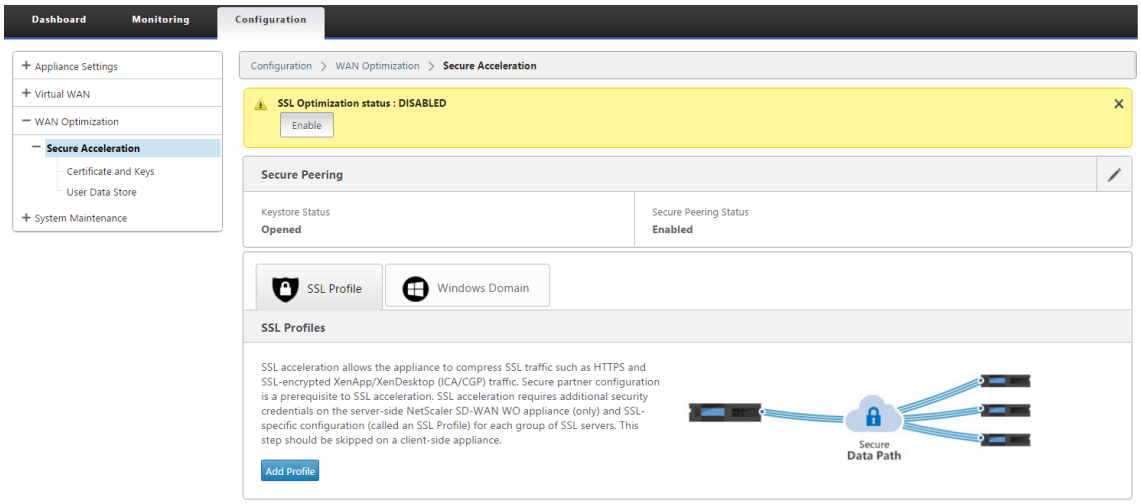
構成

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



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

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



- ライセンスは、SD-WAN SE および SD-WAN WANOP アプライアンスごとに個別に管理する必要があります。
- ソフトウェアアップグレードは、SD-WAN SE および SD-WAN WANOP アプライアンスごとに、それぞれのソフトウェアパッケージで個別に管理する必要があります。たとえば、SD-WAN SE の場合は tar.gz、

SD-WAN WANOP の場合は upg をアップグレードします。

- データパス統合は、WCCP 展開モードを介して SD-WAN SE と外部 WANOP アプライアンス間で構成する必要があります。
  - データパスレベルでは、WCCP と仮想 WAN の両方の機能が、WANOP と SE の間のデータパス統合を通じてワンアームモードで外部的に提供され、最適化のメリットが得られます。

統一された構成と監視

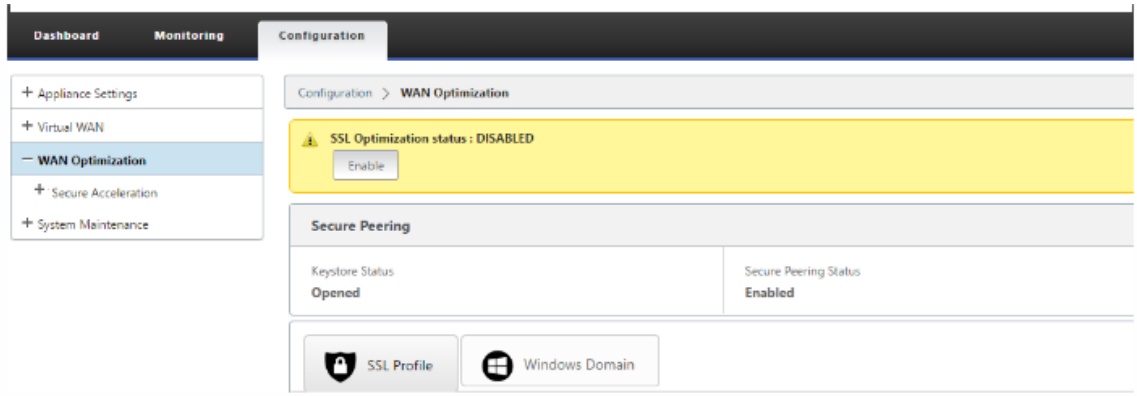
SD-WAN SE および SDWAN-WANOP アプライアンスでツーボックスモードを有効にすると、SD-WAN-EE アプライアンスでのツーボックス構成の表示と同様に、SD-WAN SE アプライアンスで設定を表示できます。

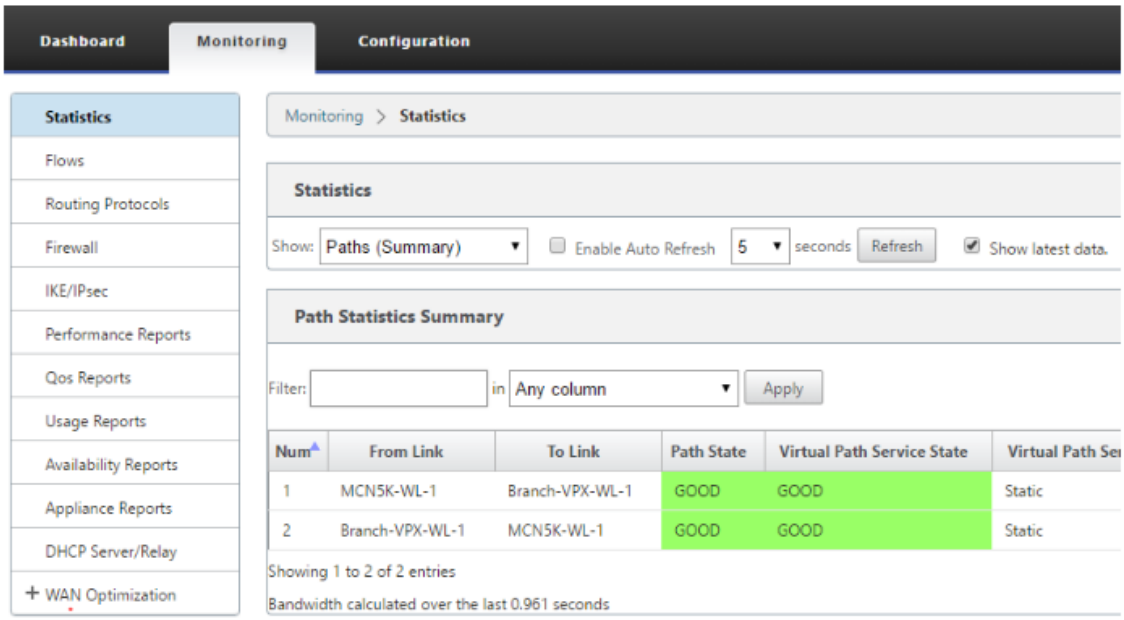
1. 構成 > 仮想 **WAN** > **WAN Optimization**
2. 「構成」>「アプライアンスの設定」の「Appflow」ノード
3. [構成] の [WAN Optimization] ノード。

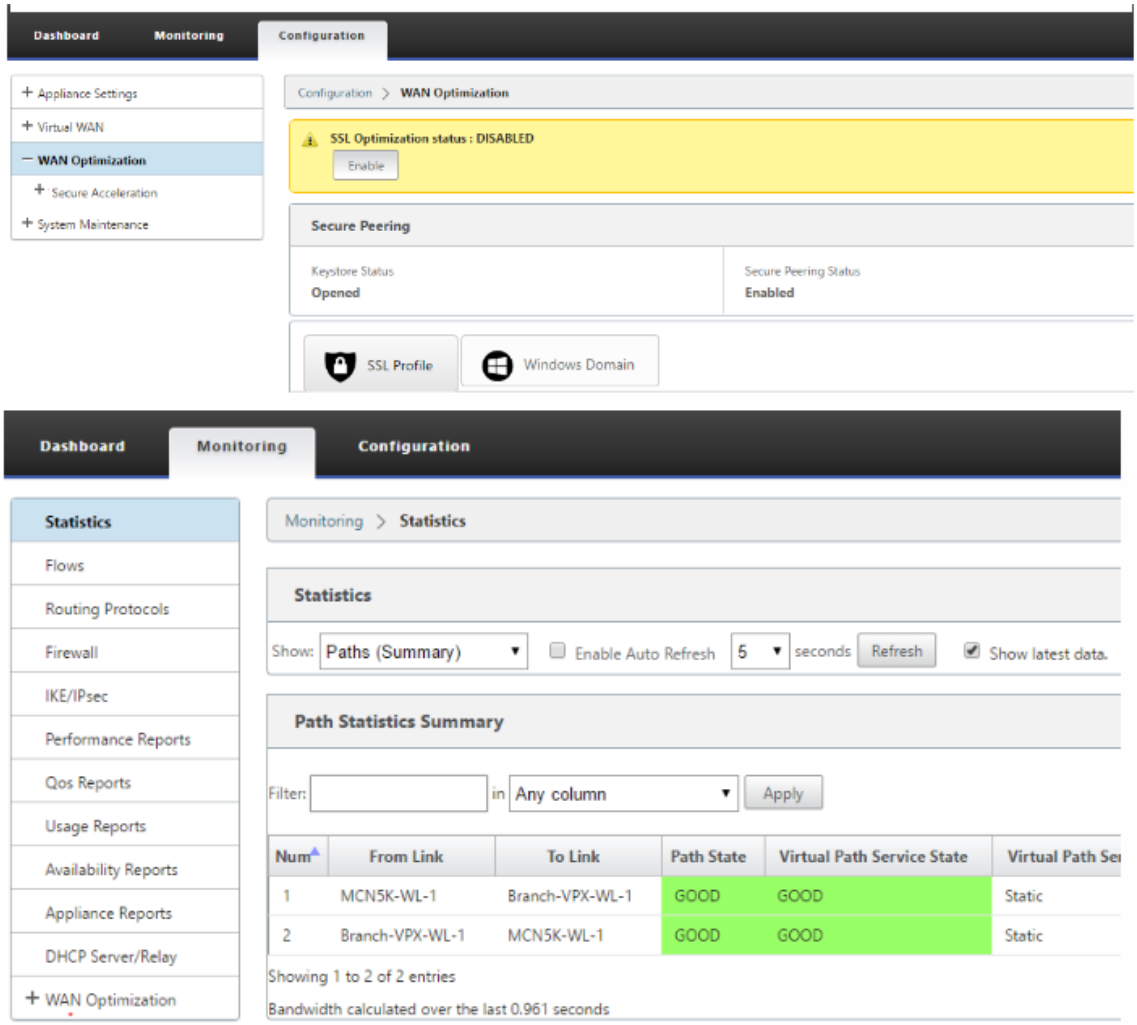
   この情報は、SD-WAN SE アプライアンスで 2 ボックスモードになっている SD-WAN WANOP アプライアンスからリダイレクトされます。

   SSL アクセラレーションや AppFlow など、WANOP に関連する設定を、SD-WAN SE Web GUI から行うことができるようになった。

   接続、圧縮、などのトラフィック関連の統計 CIFS/SMB, ICA Advanced、MAPI、およびパートナーは、SD-WAN プレミアム（エンタープライズ）エディションアプライアンスと同様の [監視**]>WAN** 最適化 の SD-WAN SE WebGUI から監視できるようになりました。







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

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

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

管理 IP アドレスは、ピア IP アドレスの構成に使用されます。

SD-WAN WANOP アプライアンスで 2 ボックスモードを無効にする

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

1. SD-WAN WANOP アプライアンスから TwoBox モードを無効にします。
2. SD-WAN SE Web GUI では、SD-WAN WANOP アプライアンスの 2 つのボックスモードページが表示されることが予想されます。これらのページを消去するには、c *lear_wo_sync* コマンドを実行します。

高可用性

November 8, 2021

このトピックでは、SD-WAN アプライアンス (Standard Edition および Premium (Enterprise) Edition) でサポートされる高可用性 (高可用性) の展開と構成について説明します。

Citrix SD-WAN アプライアンスは、アクティブ/スタンバイの役割のアプライアンスのペアとして、高可用性構成で展開できます。高可用性配置には、次の 3 つのモードがあります。

- パラレルインライン高可用性
- フェール・ツー・ワイヤー高可用性
- ワンアーム高可用性

これらの高可用性展開モードは、仮想ルータ冗長プロトコル（VRRP）に似ており、独自の SD-WAN プロトコルを使用します。SD-WAN ネットワーク内のクライアントノード（クライアント）とマスターコントロールノード（MCN）の両方を高可用性構成で展開できます。プライマリアプライアンスとセカンダリアプライアンスは、同じプラットフォームモデルである必要があります。

高可用性構成では、サイトの 1 つの SD-WAN アプライアンスがアクティブアプライアンスとして指定されます。スタンバイアプライアンスはアクティブアプライアンスを監視します。構成は両方のアプライアンスにミラーリングされます。スタンバイ・アプライアンスがアクティブ・アプライアンスとの接続性を一定期間失った場合、スタンバイ・アプライアンスはアクティブ・アプライアンスの ID を引き受け、トラフィックの負荷を引き継ぎます。デプロイモードによっては、高速フェールオーバーは、ネットワークを通過するアプリケーショントラフィックへの影響を最小限に抑えます。

高可用性展開モード

ワンアームモード**:**

ワンアームモードでは、高可用性アプライアンスペアがデータパスの外にあります。アプリケーショントラフィックは、ポリシーベースルーティング（PBR）を使用してアプライアンスペアにリダイレクトされます。ワンアーム・モードは、ネットワーク内の単一の挿入ポイントが不可能な場合、または配線へのフェイル・トゥ・ワイヤの課題に対処するために実装されます。スタンバイアプライアンスは、アクティブアプライアンスおよびルータと同じ VLAN またはサブネットに追加できます。

One-Arm モードでは、SD-WAN アプライアンスはデータネットワークサブネットに存在しないことをお勧めします。仮想パストラフィックは PBR を通過する必要はなく、ルートループを回避します。SD-WAN アプライアンスとルータは、イーサネットポートを介して、または同じ VLAN 内に直接接続する必要があります。

- フォールバックのための **IP SLA** モニタリング:

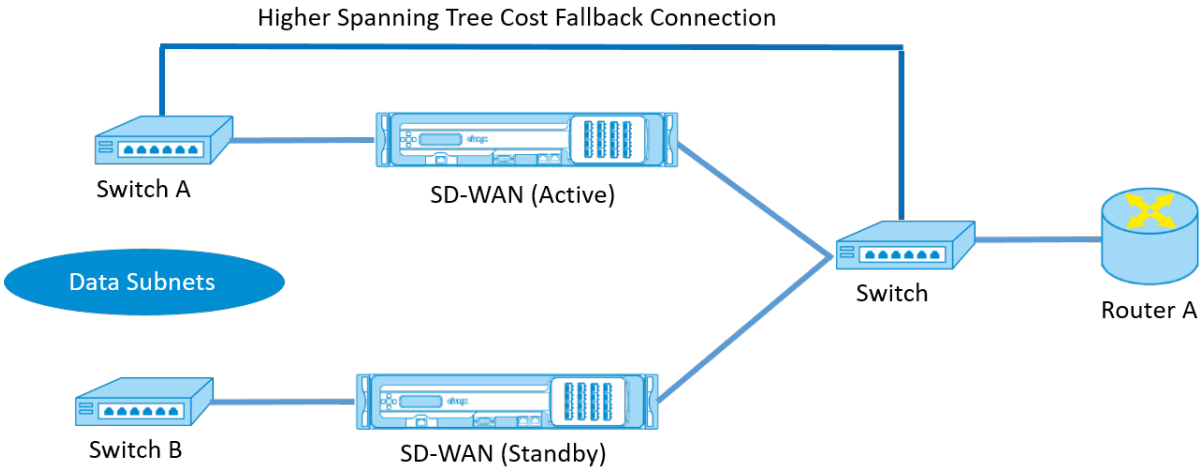
  SD-WAN アプライアンスの 1 つがアクティブである限り、仮想パスがダウンしていても、アクティブトラフィックはフローします。SD-WAN アプライアンスは、トラフィックをイントラネットトラフィックとしてルータにリダイレクトします。ただし、アクティブ/スタンバイ SD-WAN アプライアンスの両方が非アクティブになると、ルータはトラフィックをアプライアンスにリダイレクトしようとします。次のアプライアンスに到達できない場合、ルータで IP SLA モニタリングを設定して PBR を無効にすることができます。これにより、ルータがフォールバックしてルート検索を実行し、パケットを適切に転送できます。

並列インライン高可用性モード:

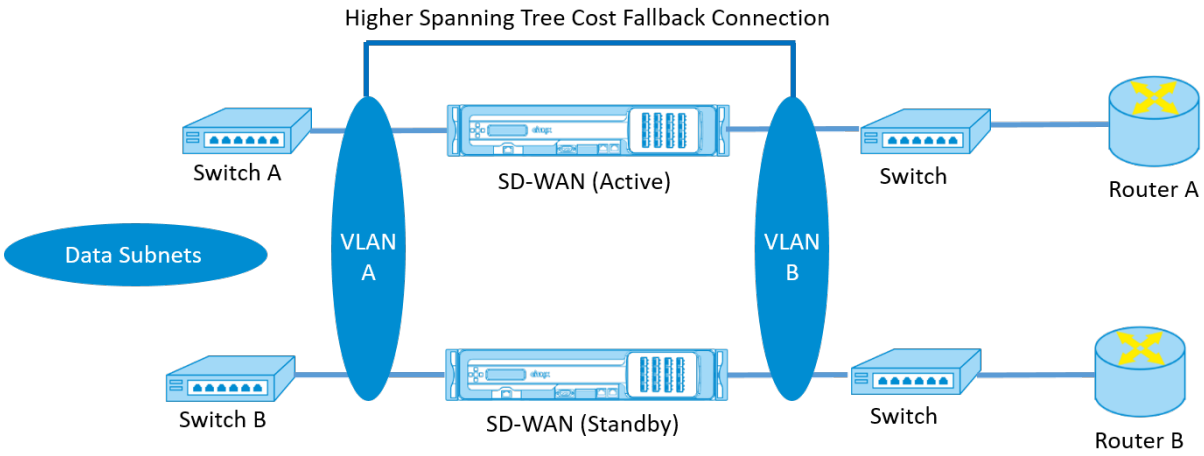
パラレルインライン高可用性モードでは、SD-WAN アプライアンスはデータパスにインラインで配置されます。アクティブアプライアンスを経由するパスは 1 つだけ使用されます。バイパスインターフェイスグループは、フェールオーバー中のブリッジングループを回避するために fail-to-block に設定されることに注意してください。

高可用性ステートは、インラインインターフェイスグループを介して、またはアプライアンス間の直接接続を介して監視できます。External Tracking を使用して、アップストリームまたはダウンストリームのネットワークインフラストラクチャの到達可能性を監視できます。たとえば、必要に応じて、高可用性状態の変更を指示するスイッチポートの障害。

アクティブ SD-WAN アプライアンスとスタンバイ SD-WAN アプライアンスの両方が無効または障害が発生した場合、スイッチとルータ間でターシャリパスを直接使用できます。このパスは、通常の条件で使用されないように、SD-WAN パスよりもスパニングツリーコストが高い必要があります。パラレルインライン高可用性モードでのフェールオーバーは、設定されているフェールオーバー時間によって異なります。デフォルトのフェールオーバー時間は 1000 ミリ秒です。ただし、フェールオーバーのトラフィックへの影響は 3 ～5 秒です。ターシャリパスへのフォールバックは、スパニングツリーの再コンバージェンスの間、トラフィックに影響を与えます。他の WAN リンクへのパス外接続がある場合は、両方のアプライアンスを接続する必要があります。



複数のルータが VRRP を使用している可能性があるより複雑なシナリオでは、LAN 側のスイッチとルータがレイヤ 2 で到達可能であることを確認するために、ルーティング不能 VLAN が推奨されます。



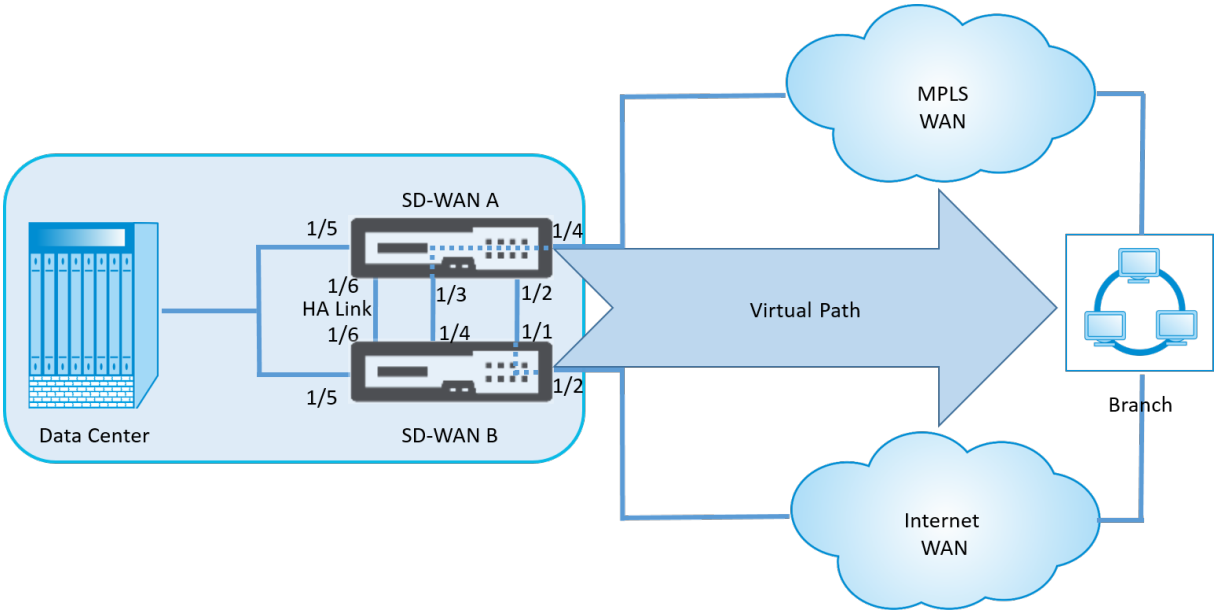
フェール・ツー・ワイヤ・モード：

Fail-to-Wire モードでは、SD-WAN アプライアンスは同じデータパスでインラインになります。バイパスインターフェイスグループは、スタンバイアプライアンスがパススルーまたはバイパスステートである状態で、Fail-to-Wire モードである必要があります。別のポート上の 2 つのアプライアンス間の直接接続を構成し、高可用性インターフェイスグループに使用する必要があります。

> 注
>
> - フェールツーワイヤモードでの高可用性スイッチオーバーには、Fail-to-Wire モードからの回復にポートが遅延するため、約 10 ～12 秒かかります。
> - アプライアンス間の高可用性接続に障害が発生すると、両方のアプライアンスがアクティブ状態になり、サービスが中断されます。サービスの中断を軽減するには、単一障害点がないように、複数の高可用性接続を割り当てます。
> - 高可用性 Fail-to-Wire モードでは、ステートのコンバージェンスを支援するために、高可用性制御交換メカニズム用のハードウェアアプライアンスのペアで別個のポートを使用することが不可欠です。

SD-WAN アプライアンスがアクティブからスタンバイに切り替わるときに物理的な状態が変化するため、オートネゴシエーションがイーサネットポートでかかる時間に応じて、フェールオーバーによって接続が部分的に切断されることがあります。

次の図に、Fail-to-Wire 展開の例を示します。



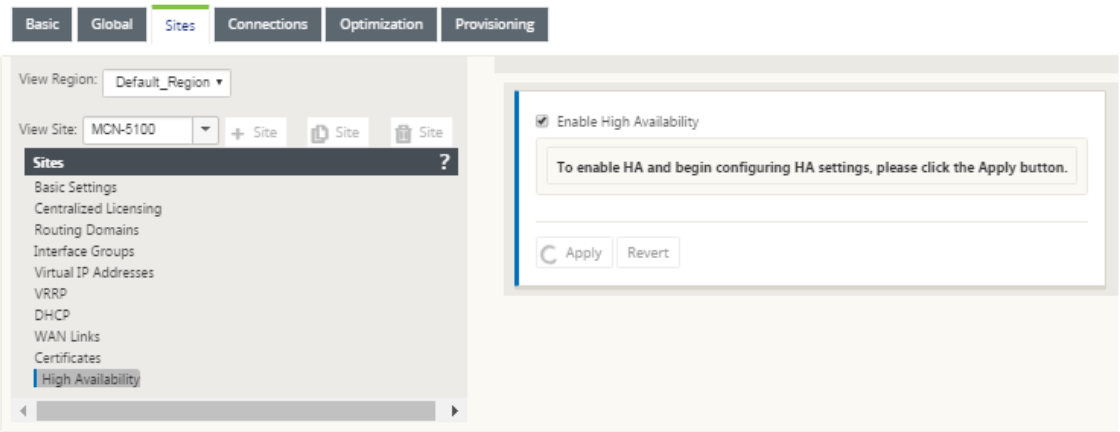
One-Arm 高可用性構成または Parallel Inline 高可用性構成は、フェールオーバー中の中断を最小限に抑えるために大量のトラフィックを転送するデータセンターまたはサイトにお勧めします。

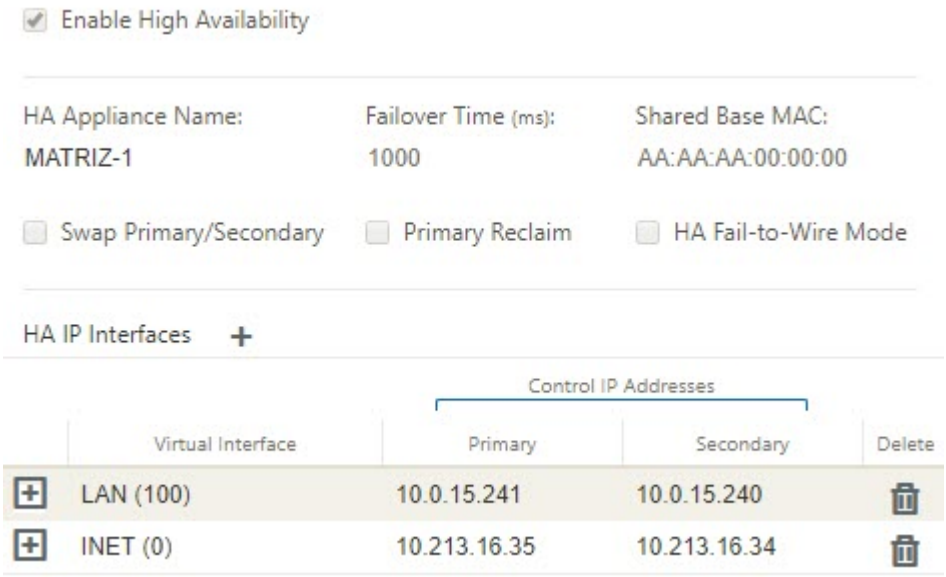
フェールオーバー中に最小限のサービス損失が許容できる場合は、Fail-to-Wire 高可用性モードが適しています。Fail-to-Wire 高可用性モードは、アプライアンスの障害から保護し、パラレルインライン高可用性はすべての障害から保護します。すべてのシナリオにおいて、高可用性は、システム障害時に SD-WAN ネットワークの継続性を維持するために有用です。

高可用性の構成

高可用性を構成するには、次の手順を実行します。

1. 構成エディタで、[サイト] > [** サイト名 **] > [高可用性] に移動します。[高可用性の有効化] を選択し、[適用] をクリックします。





2. 次のパラメータに値を入力します。

   - 高可用性アプライアンス名**:** 高可用性（セカンダリ）アプライアンスの名前。
   - フェイルオーバー時間：プライマリアプライアンスとの接続後、スタンバイアプライアンスがアクティブになるまでの待機時間（ミリ秒単位）。
   - 共有ベース **MAC**：高可用性ペアアプライアンスの共有 MAC アドレス。フェールオーバーが発生すると、セカンダリアプライアンスの仮想 MAC アドレスは、障害が発生したプライマリアプライアンスと同じになります。
   - プライマリ**/**セカンダリのスワップ：選択すると、高可用性ペアの両方のアプライアンスが同時に起動すると、セカンダリアプライアンスがプライマリアプライアンスになり、優先されます。

- **Primary Reclaim**：選択すると、フェイルオーバーイベント後の再起動時に、指定されたプライマリアプライアンスが制御を再利用します。
- 高可用性フェイル**-**ワイヤモード**:** Fail-to-Wire 高可用性展開モードを有効にする場合に選択します。

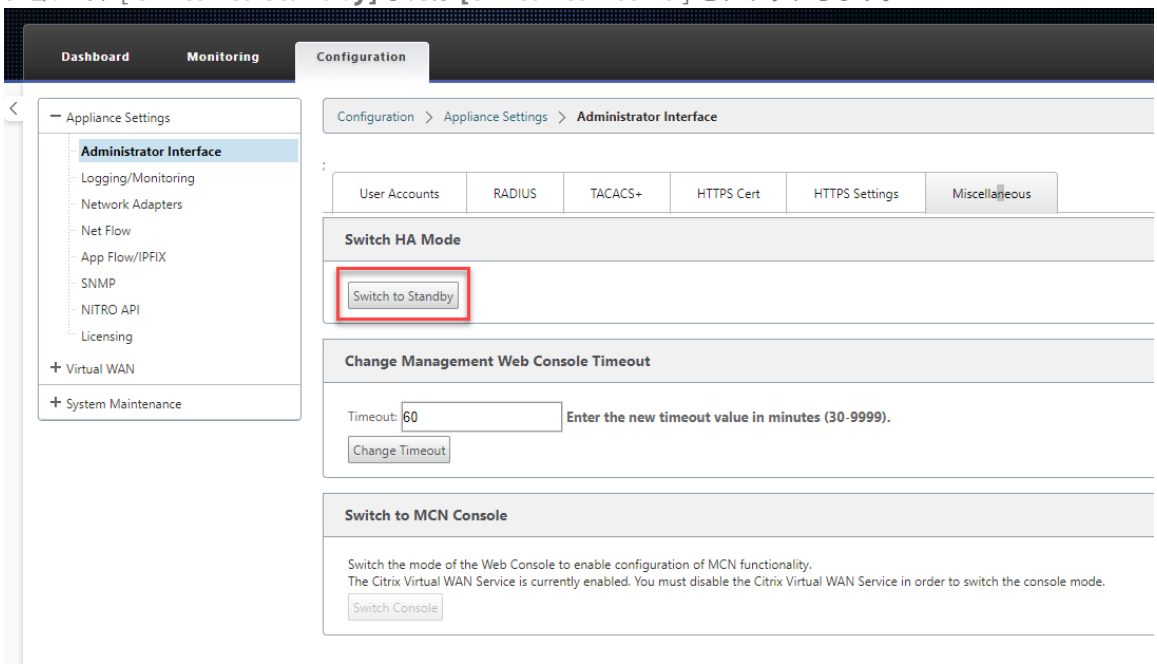
> 注
>
> ハイパーバイザーおよびクラウドベースのプラットフォームの場合は、共有ベース **MAC** を無効にするオプションを選択して、共有仮想 MAC アドレスを無効にします。
>
> Hypervisor ベースのプラットフォームでは、ハイパーバイザーで無差別モードが有効になっていることを確認して、高可用性の共有 MAC アドレスからのパケットソースを許可します。無差別モードが有効になっていない場合は、共有ベース **MAC** を無効にするオプションを有効にできます。

インターフェイスグループを設定するには、**[**高可用性 **IP Interfaces**] の横にある [**+**] をクリックします。次のパラメータに「値」を入力します。

- 仮想インターフェイス—高可用性ペア内のアプライアンス間の通信に使用される仮想インターフェイス。アクティブアプライアンスの到達可能性を監視します。ワンアーム高可用性モードの場合、必要なインターフェイスグループは 1 つだけです。
- プライマリ—プライマリアプライアンスの一意の仮想 IP アドレス。セカンダリアプライアンスは、プライマリ仮想 IP アドレスを使用して、プライマリアプライアンスと通信します。
- セカンダリ—セカンダリアプライアンスの一意の仮想 IP アドレス。プライマリアプライアンスは、セカンダリ仮想 IP アドレスを使用してセカンダリアプライアンスと通信します。

新しい 高可用性 **IP** インターフェイス エントリの左側にある [**+**] をクリックします。[External **Tracking IP Address**] フィールドに、ARP 要求に応答する外部デバイスの IP アドレスを入力して、プライマリアプライアンスの状態を特定し、[**Apply**] をクリックします。

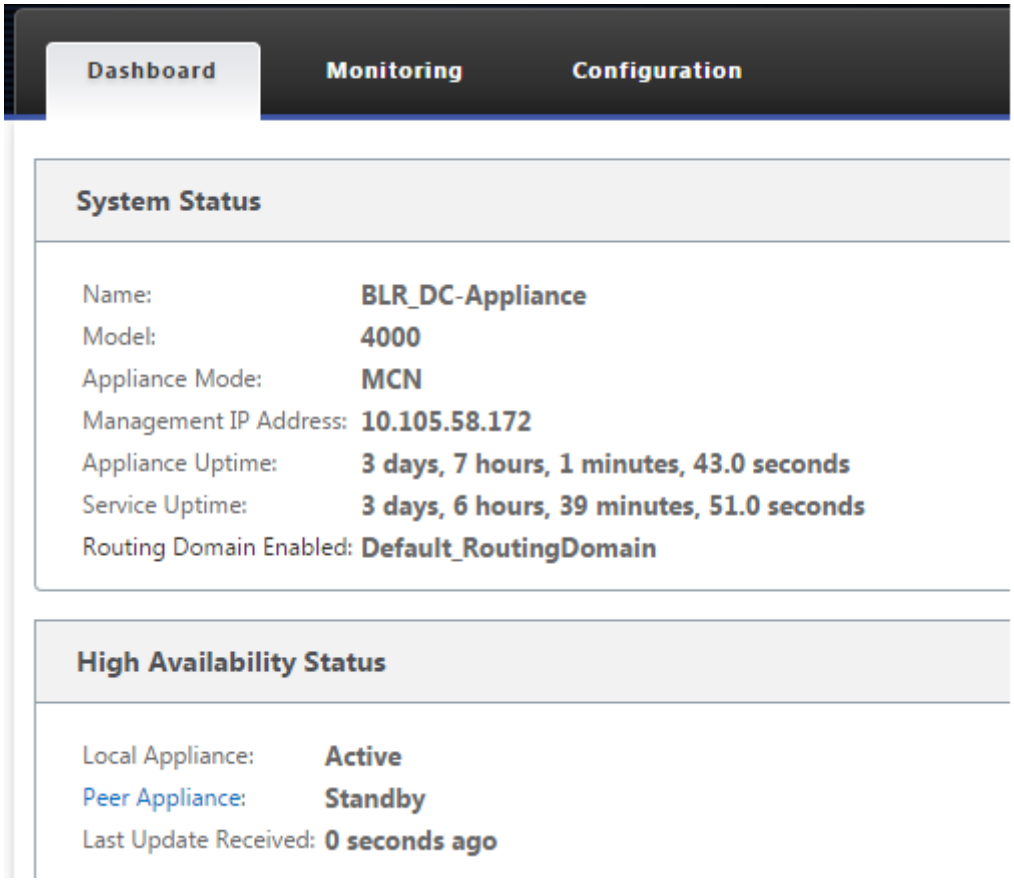
> 注:
>
> アプライアンスから HA スイッチオーバーを手動でトリガーすることもできます。構成 > アプライアンスの設定 > 管理者インターフェイス > その他に移動します。HA アプライアンスに応じて、[Switch HA Mode] セクションで、[**Switch to Standby]** または **[Switch to Active**] をクリックします。

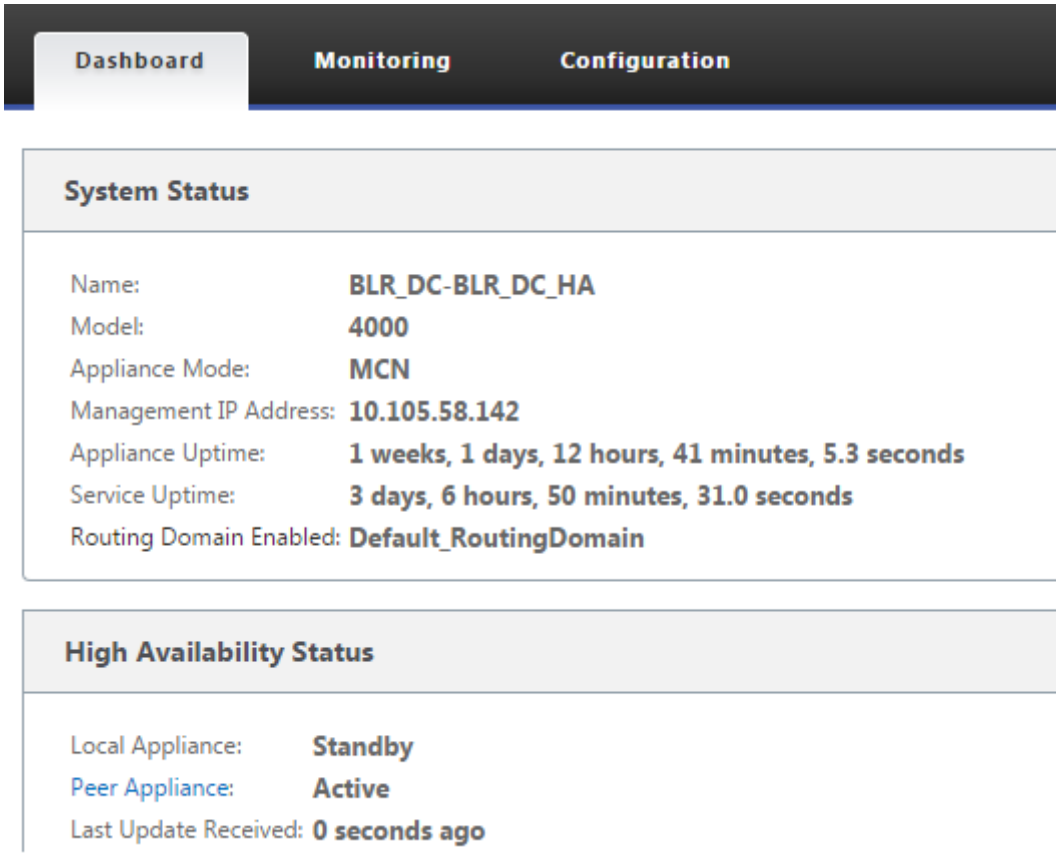


監視

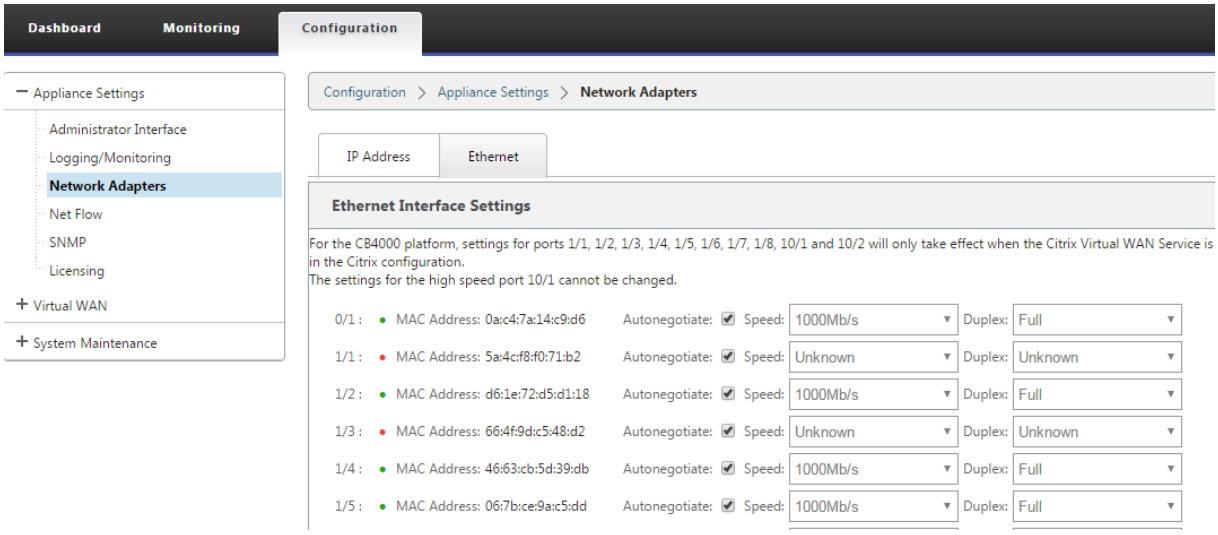
高可用性構成を監視するには、次の手順を実行します。

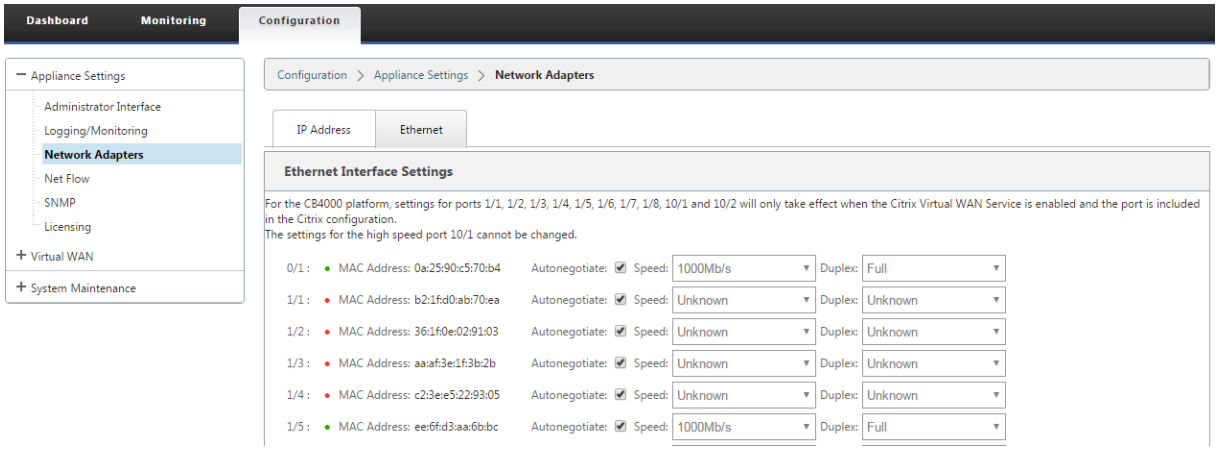
高可用性が実装されているアクティブおよびスタンバイアプライアンスの SD-WAN Web 管理インターフェイスにログインします。[ダッシュボード] タブに高可用性ステータスを表示します。





アクティブおよびスタンバイの高可用性アプライアンスのネットワークアダプタの詳細については、「構成」>「アプライアンスの設定」>「ネットワークアダプタ」>「イーサネット」タブに移動します。





トラブルシューティング

SD-WAN アプライアンスを高可用性（HA）モードに設定するときに、次のトラブルシューティング手順を実行します。

1. スプリットブレインの問題の主な理由は、HA アプライアンス間の通信の問題が原因です。
   - SD-WAN アプライアンス間の接続に問題があるかどうかを確認します（両方の SD-WAN アプライアンスのポートがアップまたはダウンしているなど）。
   - 1 つの SD-WAN アプライアンスのみをアクティブにするには、いずれかの SD-WAN アプライアンスで SD-WAN サービスを無効にする必要があります。
2. **SDWAN_common.log** ファイルにログインした HA 関連ログを確認できます。

   > 注：
   > すべての高可用性関連ログは、キーワード **racp** で記録されます。

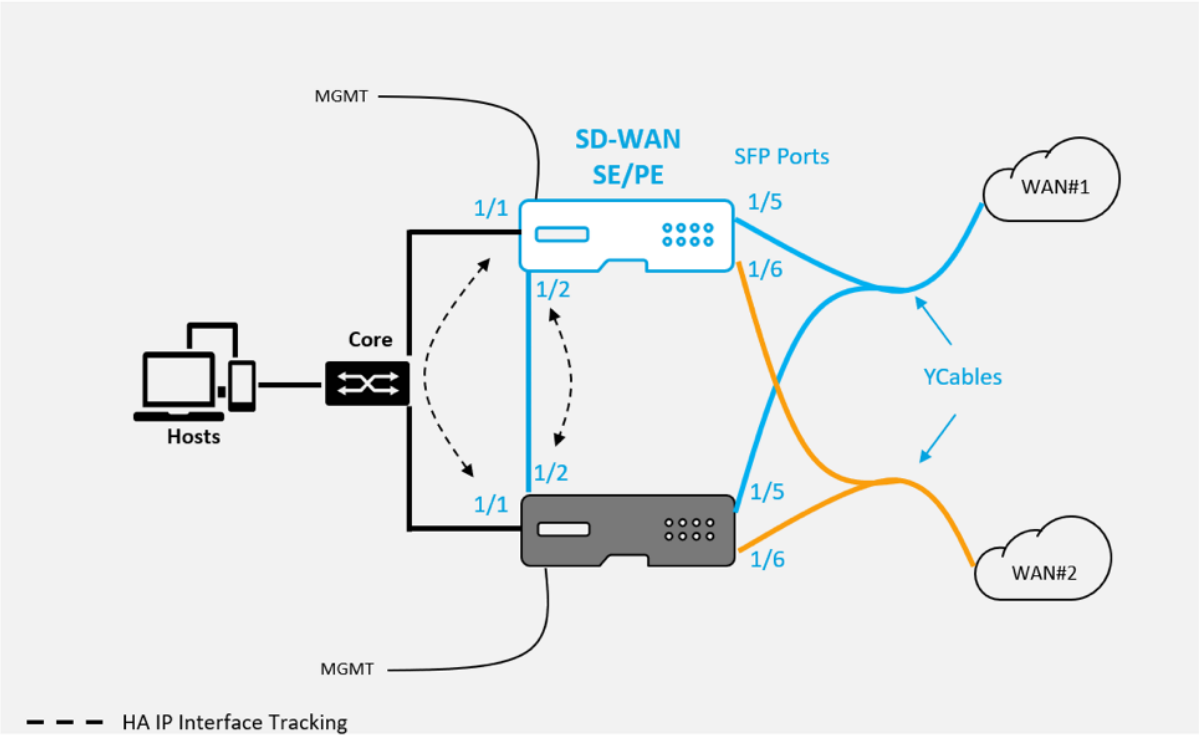
3. **SDWAN_common.log** ファイル内のポート関連のイベント（HA が有効なポートがダウンまたはアップになったなど）を確認できます。
4. HA 状態の変更ごとに、1 つの SD-WAN イベントが記録されます。したがって、ログがロールオーバーされた場合、イベントログを確認してイベントの詳細を取得できます。

光ファイバ **Y** ケーブルを使用したエッジモードの高可用性の有効化

September 26, 2023

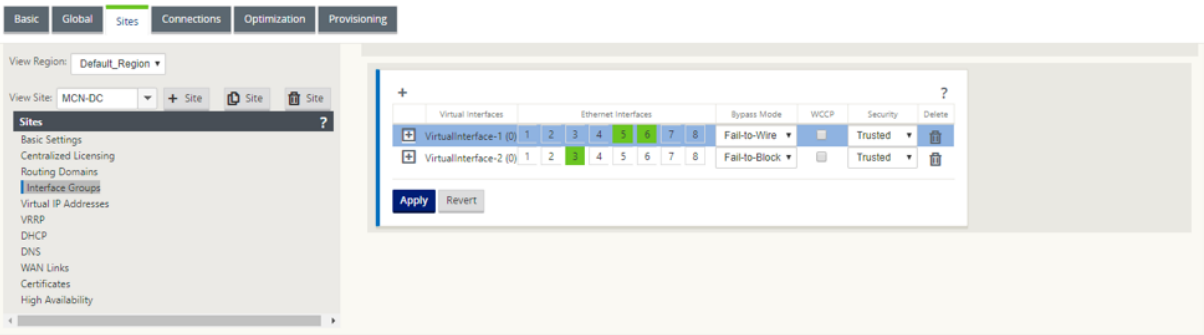
> 注：リリース 10.2 バージョン 2 では、この機能は 1100 SE/PE アプライアンスにだけ適用できます。

次の手順では、WAN リンクサービスプロバイダーからのハンドオフが光ファイバであるエッジモードで配置された 1100 SE/PE アプライアンスで High Availability（HA; 高可用性）を有効にする手順について説明します。
1100 アプライアンスで使用可能な SFP（小型フォーム・ファクタ・プラグ）ポートを光ファイバ Y ケーブルとともに使用すると、エッジ・モード導入で高可用性機能を実現できます。
1100 SE/PE アプライアンスでは、スプリッタケーブルのスプリットエンドは、HA ペアで設定された 2 つの 1100 アプライアンスのファイバポートに接続します。
光ファイバ Y ケーブルには 3 つの端があります。一方の端はプロバイダのファイバハンドオフに接続し、もう一方の端は HA ペアに展開された 2 つの 1100 SE/PE アプライアンス上の WAN リンク用に設定された SFP ポートに接続します。スプリッタケーブルは、1 つの入力信号を複数の信号に分割するために使用されます。



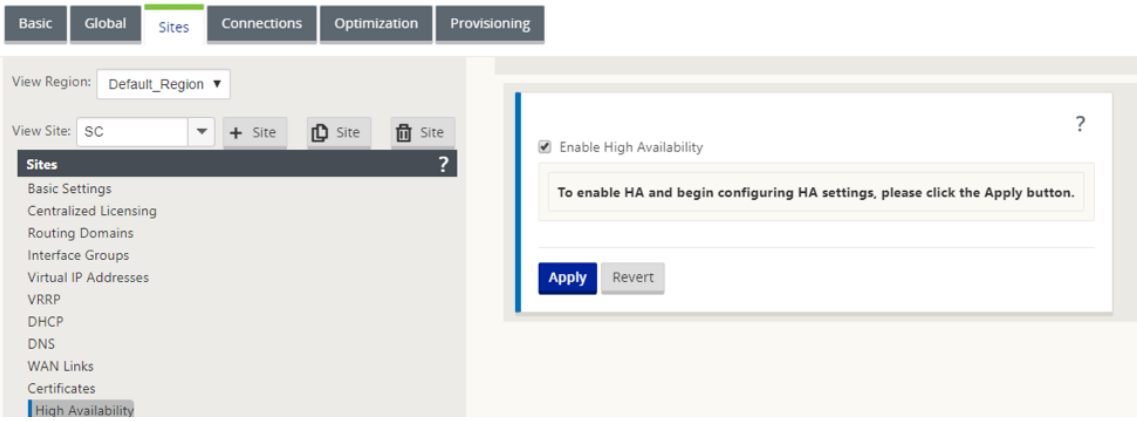
前提条件:

1. 1100 SE/PE アプライアンスでは、ポート 1/5 および 1/6 は SFP ポートです。Y ケーブルのスプリッタの端を、HA ペアの両方のアプライアンスのいずれかのポートに接続します。詳細については、1100 SEを参照してください。
2. SFP ポートを SD-WAN アプライアンス構成に追加します。SFP ポートの設定は、ネットワークインターフェイスポートの設定と同じです。詳しくは、「インターフェイスグループの設定方法」を参照してください。設定に 1/5 または 1/6 ポートを追加すると、Y ケーブルサポート機能を有効にできます。



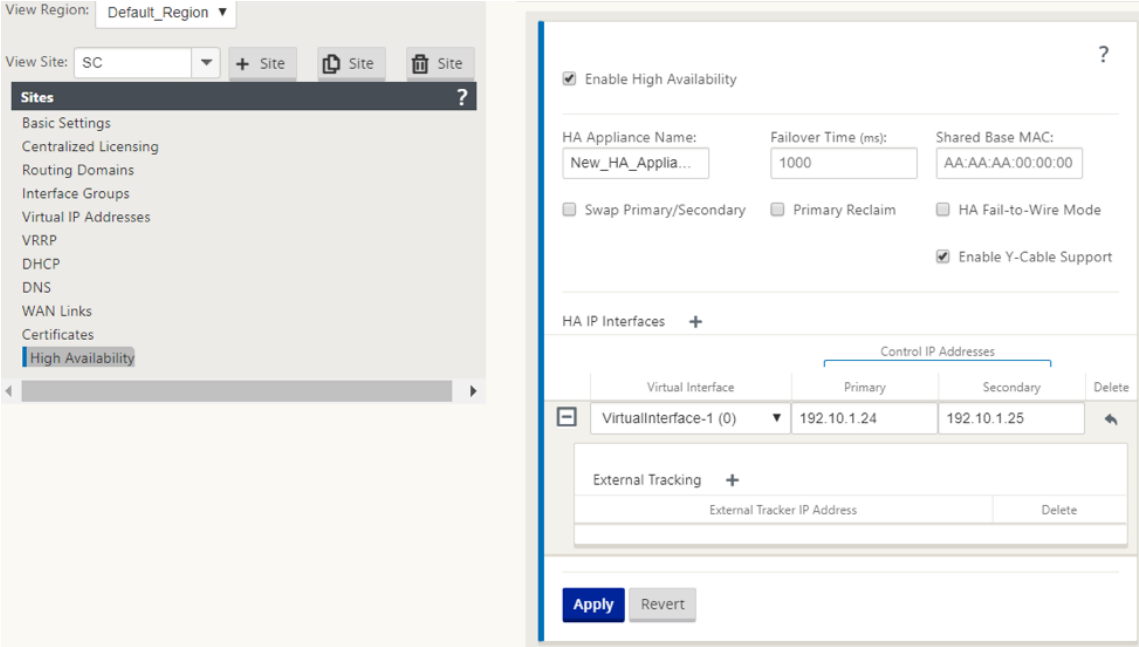
Y ケーブルを使用して高可用性を有効にするには、次の手順を実行します。

1. 1100 SE/PE アプライアンスの GUI で、[構成] **> [**仮想 **WAN] > [**構成エディタ**] > [**サイト**]** に移動します。[高可用性の有効化] をクリックします。



2. [**Y** ケーブルサポートを有効にする] をクリックします。

3. Y ケーブルに接続されたインターフェイス以外のインターフェイスを使用して HA IP インターフェイスを追加します（例：1/1 LAN 方向インターフェイス、または 1/2 直接接続されたインターフェイス）。Y ケーブル機能が有効の場合、SFP ポートを HA IP インターフェイスに使用できません。



4. 設定を適用、ステージングおよびアクティブ化します。

制限事項:

- Y ケーブルを使用した HA フェールツーワイヤモードの設定はサポートされていません。
- Y ケーブルに接続された SFP は、HA IP インターフェイストラッキングとして使用できません。
- この展開をサポートするには、リリース 10.2.2 以降、11.0 以降が必要です。

ゼロタッチ

November 8, 2021

> 注
>
> ゼロタッチ展開サービスは、一部の Citrix SD-WAN アプライアンスでのみサポートされます。
>
> - SD-WAN 210 Standard Edition
> - SD-WAN 410 Standard Edition
> - SD-WAN 2100 Standard Edition
> - SD-WAN 1100 Standard Edition
> - SD-WAN 1100 Premium Edition
> - SD-WAN 1000 Standard Edition（再イメージ化が必要）
> - SD-WAN 1000 Enterprise Edition (Premium Edition)
> - SD-WAN 2000 Standard Edition

> - SD-WAN 2000 Enterprise Edition (Premium Edition)
> - SD-WAN 2100 Enterprise Edition (Premium Edition)
> - SD-WAN AWS VPX インスタンス

ゼロタッチ展開クラウドサービスは、Citrix が運用および管理するクラウドベースのサービスで、Citrix SD-WAN ネットワーク内の新しいアプライアンスを検出できます。主に支店またはクラウドサービスオフィスでの Citrix SD-WAN の展開プロセスの合理化に焦点を当てています。ゼロタッチデプロイメントクラウドサービスは、パブリックインターネットアクセスを介して、ネットワーク内のどこからでもパブリックにアクセスできます。ゼロタッチデプロイメントクラウドサービスは、セキュアソケットレイヤー (SSL) プロトコルを介してアクセスします。

ゼロタッチ展開クラウドサービスは、ゼロタッチ対応デバイス（SD-WAN 410-SE、2100-SE など）を購入した Citrix 顧客の保存された ID をホストするバックエンドの Citrix サービスと安全に通信します。バックエンドサービスは、Zero Touch Deployment 要求を認証し、Citrix SD-WAN アプライアンスのカスタマーアカウントとシリアル番号の間の関連付けを適切に検証します。

ZTD ハイレベルアーキテクチャとワークフロー：

データ・センター・サイト：

Citrix SD-WAN 管理者**-SD-WAN** 環境の管理者権限を持つユーザーで、次の主な役割を担います。

- Citrix SD-WAN Center ネットワーク構成ツールを使用した構成の作成、またはマスターコントロールノード（MCN）SD-WAN アプライアンスからの構成のインポート
- 新しいサイトノードの展開のためにゼロタッチ展開サービスを開始する Citrix Cloud ログイン。

> 注
>
> SD-WAN Center がプロキシサーバ経由でインターネットに接続されている場合は、SD-WAN Center でプロキシサーバの設定を構成する必要があります。詳細については、「ゼロタッチ展開のプロキシサーバー設定」を参照してください。

ネットワーク管理者—エンタープライズネットワーク管理 (DHCP、DNS、インターネット、ファイアウォールなど) を担当するユーザー。

- 必要に応じて、***SD-WAN Center*** から ***FQDN sdwanzt.citrixnetworkapi.net*** へのアウトバウンド通信用のファイアウォールを構成します。

リモート・サイト：

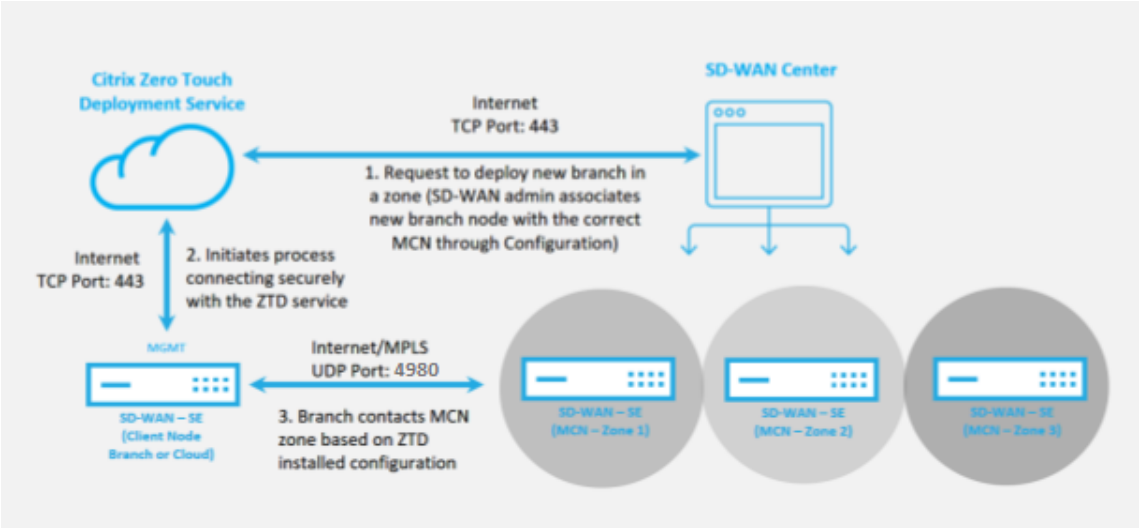
オンサイト・インストーラ—オンサイト・アクティビティの担当者、または雇用されたインストーラ。主に次の責任があります。

- Citrix SD-WAN アプライアンスを物理的に解凍します。
- ZTD 対応でないアプライアンスのイメージを再作成します。
  - 必須：SD-WAN 1000-SE、2000-SE、1000-EE、2000-EE

  - 不要:SD-WAN 410-SE、2100-SE

- アプライアンスの電源ケーブル。
- 管理インターフェイス（MGMT、0/1 など）でインターネットに接続するためにアプライアンスをケーブル接続します。
- データインターフェイス（Apa.WAN、Apb.WAN、apc.WAN、0/2、0/3、0/5 など）で WAN リンク接続用にアプライアンスをケーブル接続します。

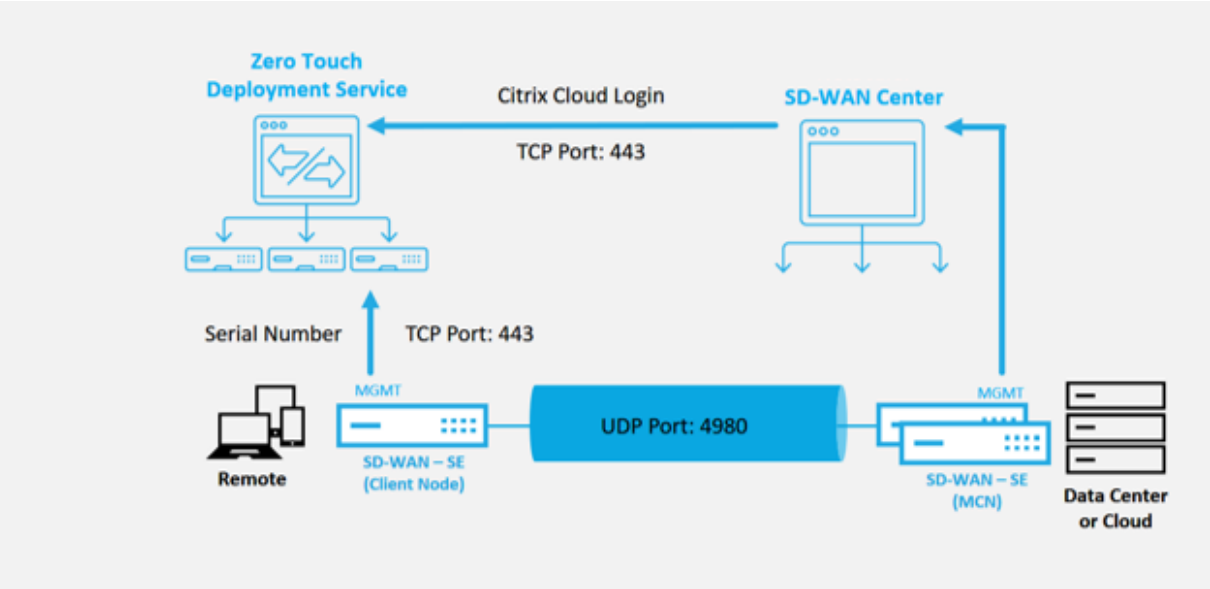
> 注
>
> インターフェイスのレイアウトはモデルごとに異なるため、データポートと管理ポートの識別についてはドキュメントを参照してください。



ゼロタッチ展開サービスを開始する前に、次の前提条件が必要です。

- マスターコントロールノード（MCN）に昇格したアクティブに実行されている SD-WAN。
- 仮想パス経由の MCN に接続して、SD-WAN Center をアクティブに実行しています。
- https://onboarding.cloud.com で作成された Citrix Cloud ログイン資格情報（アカウント作成に関する以下の説明を参照）。
- 管理ネットワーク接続（SD-WAN Center および SD-WAN アプライアンス）をポート 443 でインターネットに直接接続するか、プロキシサーバー経由で接続します。
- （オプション）MCN への有効な仮想パス接続を使用してクライアントモードでブランチオフィスで動作するアクティブに実行されている少なくとも 1 つの SD-WAN アプライアンス。

最後の前提条件は必須ではありませんが、新しく追加されたサイトで Zero Touch Deployment が完了したときに、アンダーレイネットワークで仮想パスを確立できるかどうかを SD-WAN 管理者が検証できます。これは主に、適切なファイアウォールポリシーとルートポリシーが NAT トラフィックに適宜配置されているか、または UDP ポート 4980 がネットワークに正常に侵入して MCN に到達できることを確認します。



ゼロタッチ展開サービスの概要:

Zero Touch Deployment Service は、SD-WAN Center と連携して機能し、ブランチオフィスの SD-WAN アプライアンスを簡単に導入できます。SD-WAN Center は、SD-WAN 標準および Enterprise （Premium）Edition アプライアンスの中央管理ツールとして構成および使用されます。ゼロタッチ展開サービス（またはゼロタッチ展開クラウドサービス）を使用するには、管理者は最初に環境に最初の SD-WAN デバイスを展開してから、SD-WAN Center を管理の中心点として構成および展開する必要があります。SD-WAN センター（リリース 9.1 以降）をポート 443 にパブリックインターネットに接続してインストールすると、SD-WAN Center は自動的にクラウドサービスを開始し、ゼロタッチ展開機能のロックを解除し、ゼロタッチ展開オプションを SD-WAN Center GUI。ゼロタッチ展開は、SD-WAN Center ソフトウェアでは既定では使用できません。これは、管理者がゼロタッチ配置に関連するオンサイトアクティビティを開始する前に、アンダーレイネットワーク上に適切な予備コンポーネントが存在することを確認するために意図的に設計されています。

SD-WAN 環境が稼働し始めたら、Citrix Cloud アカウントのログインを作成することにより、ゼロタッチ展開サービスへの登録が完了します。SD-WAN Center がゼロタッチ展開サービスと通信できる場合、GUI は [設定] タブの下にゼロタッチ展開オプションを公開します。ゼロタッチサービスにログインすると、特定の SD-WAN 環境に関連付けられたカスタマー ID が認証され、SD-WAN Center が登録されます。さらに、ゼロタッチデプロイアプライアンスの展開をさらに認証するためのアカウントのロックが解除されます。

SD-WAN 管理者は、SD-WAN Center ネットワーク構成ツールを使用して、テンプレートまたはサイトのクローン作成機能を使用して SD-WAN 構成を構築し、新しいサイトを追加する必要があります。新しい設定は SD-WAN Center で使用され、新しく追加されたサイトのゼロタッチ展開の展開を開始します。SD-WAN 管理者がゼロタッチ展開プロセスを使用して展開するサイトを開始する場合、シリアル番号を事前に入力し、オンサイトインストーラへの電子メール通信を開始してオンサイトを開始することで、ゼロタッチ展開に使用するアプライアンスを事前認証するオプションがあります。アクティビティ。

オンサイトインストーラーは、サイトがゼロタッチ展開の準備ができているという電子メール通信を受信し、DHCP IP アドレスの割り当てと MGMT ポートでのインターネットアクセスのためにアプライアンスの電源を入れてケーブ

ル接続するインストール手順を開始できます。また、LAN ポートおよび WAN ポートでのケーブル配線。それ以外はすべてゼロタッチ展開サービスによって開始され、アクティベーション URL を使用して進行状況が監視されます。インストールするリモートノードがクラウドインスタンスである場合、アクティベーション URL を開くと、ワークフローが開始され、指定されたクラウド環境にインスタンスが自動的にインストールされます。ローカルインストーラーによるアクションは必要ありません。

ゼロタッチデプロイメントクラウドサービスは、次のアクションを自動化します。

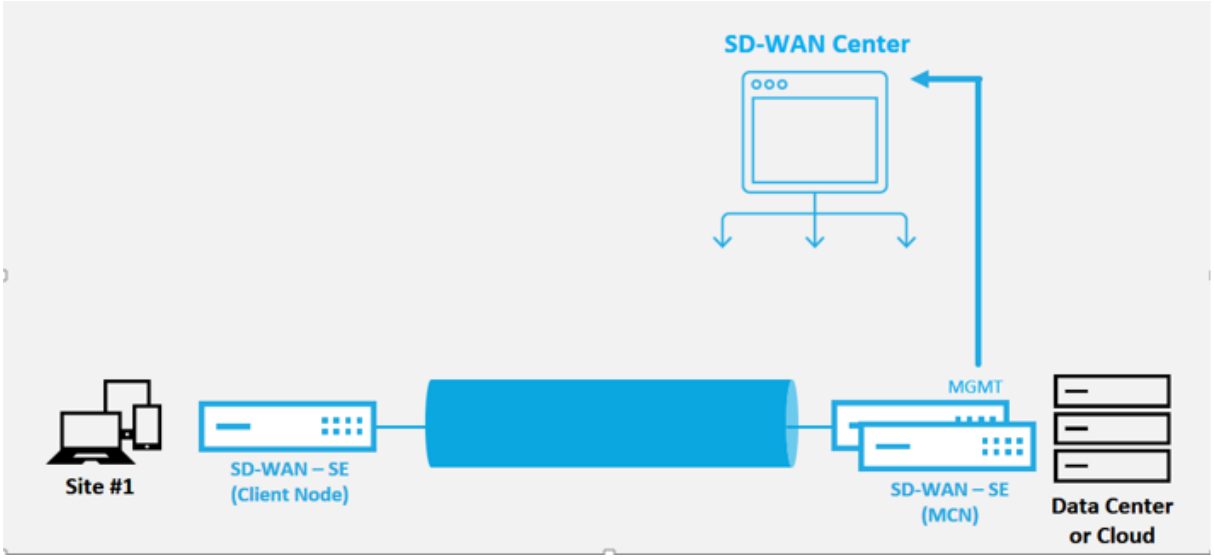
ブランチアプライアンスで新機能が利用できる場合は、ゼロタッチデプロイメントエージェントをダウンロードして更新します。

- シリアル番号を検証して、ブランチアプライアンスを認証します。
- SD-WAN 管理者がサイトを SD-WAN Center を使用してゼロタッチ展開を受け入れたことを認証します。
- SD-WAN Center から、ターゲットアプライアンスに固有の設定ファイルをプルします。
- 対象のアプライアンスに固有の構成ファイルをブランチアプライアンスにプッシュします。
- ブランチアプライアンスに構成ファイルをインストールします。
- 不足している SD-WAN ソフトウェアコンポーネントまたは必要な更新をブランチアプライアンスにプッシュします。
- 仮想パスの確立を確認するための一時的な 10 Mbps ライセンスファイルをブランチアプライアンスにプッシュします。
- ブランチアプライアンスで SD-WAN サービスを有効にします。

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

ゼロタッチ展開デバイス手順

以下の手順では、ゼロタッチ展開サービスを使用して新しいサイトを展開するために必要な手順を詳しく説明します。実行中の MCN と 1 つのクライアントノードがすでに SD-WAN Center との適切な通信で動作しており、アンダーレイネットワーク全体の接続を確認する仮想パスを確立します。SD-WAN 管理者がゼロタッチの展開を開始するには、次の手順が必要です。



ゼロタッチ展開サービスを構成する方法

SD-WAN Center には、新しく接続されたアプライアンスから SD-WAN エンタープライズネットワークに参加するための要求を受け付ける機能があります。要求は、ゼロタッチ展開サービスを介して Web インターフェイスに転送されます。アプライアンスがサービスに接続すると、構成とソフトウェアのアップグレードパッケージがダウンロードされます。

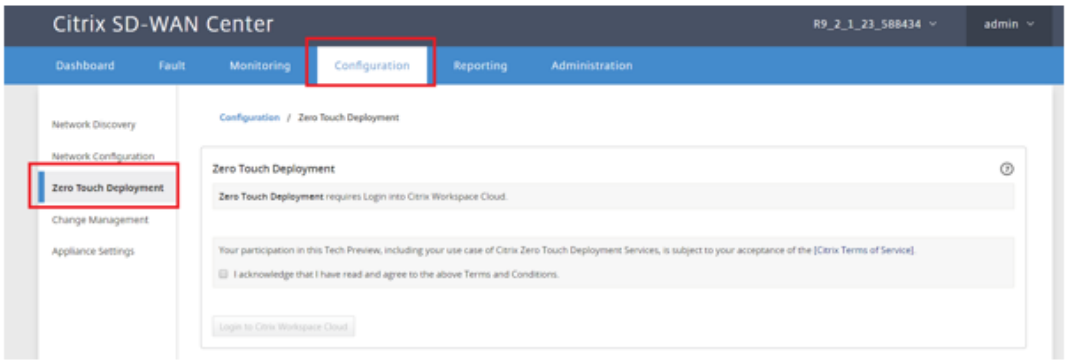
設定ワークフロー:

- [**SD-WAN Center] > [**新しいサイト構成の作成] にアクセスするか、既存の構成をインポートして保存します。
- Citrix Workspace にログインして、ゼロタッチ展開サービスを有効にします。SD-WAN Center Web 管理インターフェイスに「ゼロタッチ配置」メニューオプションが表示されるようになりました。
- SD-WAN Center で、設定 > **** ゼロタッチ展開 **>** 展開新しいサイトへのナビゲート **。
- アプライアンスを選択して [有効化] をクリックし、[デプロイ] をクリックします。
- インストーラがアクティベーションメールを受信し、シリアル番号を入力 > アクティベーション > アプライアンスが正常にデプロイされました。

ゼロタッチ展開サービスを構成するには:

1. ゼロタッチ展開機能を有効にした SD-WAN Center をインストールします。
   a) DHCP が割り当てられた IP アドレスを持つ SD-WAN Center をインストールします。
   b) SD-WAN Center に適切な管理 IP アドレスとネットワーク DNS アドレスが割り当てられ、管理ネットワークを介してパブリックインターネットに接続できることを確認します。
   c) SD-WAN Center を最新の SD-WAN ソフトウェアリリースバージョンにアップグレードします。

d) 適切なインターネット接続により、SD-WAN Center はゼロタッチ展開クラウドサービスを開始し、ゼロタッチ展開に固有のファームウェアアップデートを自動的にダウンロードしてインストールします。この Call Home プロシージャが失敗すると、次のゼロタッチ展開オプションが GUI で使用できなくなります。



e) 利用規約を読み、上記の利用規約を読み、同意したことを認めますを選択します。

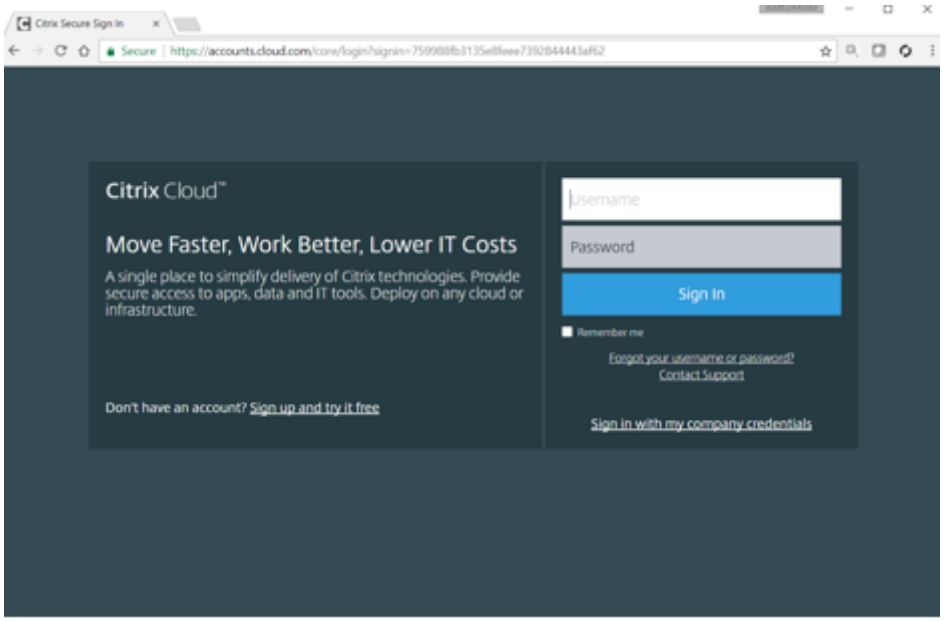
f) **Citrix Cloud** アカウントがすでに作成されている場合は、［**Citrix Workspace Cloud** にログイン］ボタンをクリックします。

g) Citrix Cloud アカウントにログインし、ログイン成功の次のメッセージを受け取っ たら、このウィンドウを閉じないでください。プロセスには別のウィンドウが必要です ~20 SD-WAN Center GUI を更新するための秒数。ウィンドウが完了したら、ウィンドウを単独で閉じる必要があります。

2. クラウドログインアカウントを作成するには、以下の手順に従います。ウェブブラウザを開いて https://onboarding.cloud.com

3.「待って、**Citrix.com** アカウントを持っています」のリンクをクリックします。

4. 既存の Citrix アカウントでサインインします。



5. SD-WAN Center Zero Touch Deployment ページにログインすると、次の理由により、ゼロタッチ展開に使用できるサイトがないことがあります。

   - アクティブな構成が [構成] ドロップダウンメニューから選択されていません
   - 現在アクティブな構成のすべてのサイトが既に展開されています
   - 構成は SD-WAN Center を使用して構築されたものではなく、MCN で利用可能な構成エディタを使用

して構築されたものでした。

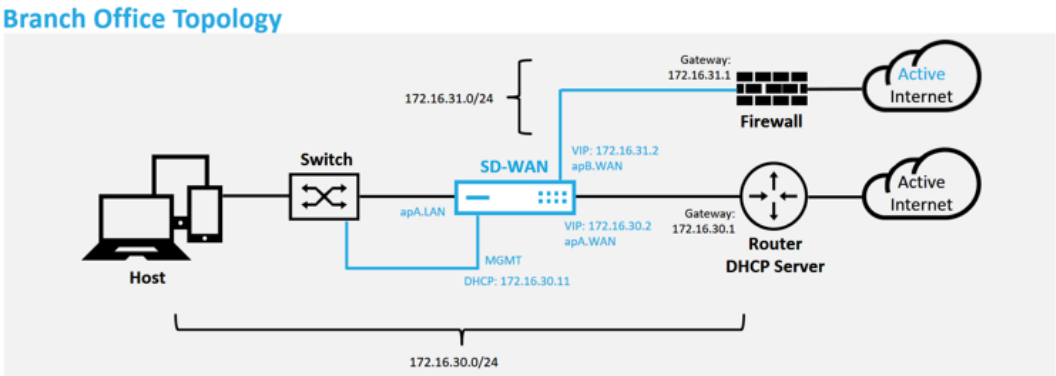
- ゼロタッチ対応アプライアンス（410-SE、2100-SE、Cloud VPX など）を参照する構成でサイトが構築されていない

6. SD-WAN SD-WAN Center ネットワーク構成を使用して、**ZTD** 対応 **SD-WAN** アプライアンスを備えた新しいリモートサイトを追加するように設定を更新します **。

   SD-WAN 設定が SD-WAN Center ネットワーク設定を使用して構築されていない場合は、MCN からアクティブな設定をインポートし、SD-WAN Center を使用して設定の変更を開始します。Zero Touch Deployment 機能を使用するには、SD-WAN 管理者は SD-WAN Center を使用して設定を構築する必要があります。ゼロタッチ展開の対象となる新しいサイトを追加するには、以下の手順を使用する必要があります。

   a) 新しいサイトの詳細（つまり、アプライアンスモデル、インターフェイスグループの使用、仮想 IP アドレス、帯域幅を備えた WAN リンク、およびそれぞれの Gateway）を最初に概説することにより、SD-WAN アプライアンス展開用の新しいサイトを設計します。

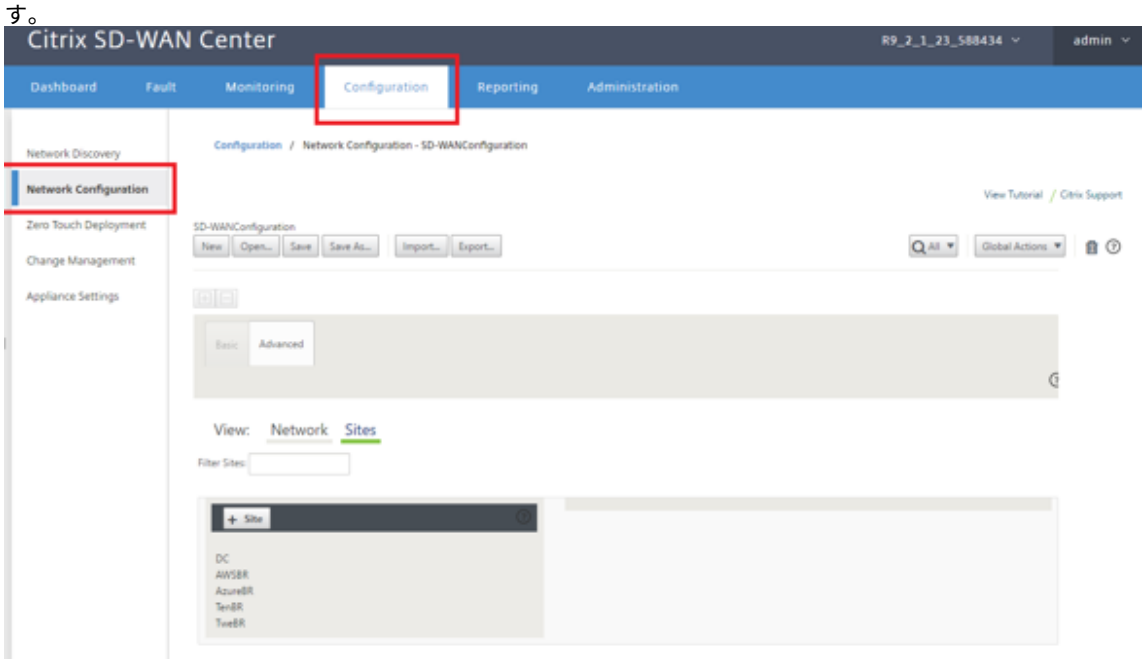
   > 重要
   >
   > モデルとして VPX が選択されているサイトノードも一覧表示されますが、現在、ゼロタッチデプロイメントサポートは AWS VPX インスタンスでのみ利用可能です。
   >
   > 注
   >
   > - Citrix SD-WAN Center のサポート Web ブラウザを使用していることを確認します
   > - Citrix Workspace ログイン中に、Web ブラウザーがポップアップウィンドウをブロックしていないことを確認します。



   これは、ブランチオフィスサイトの展開例です。SD-WAN アプライアンスは、172.16.30.0/24 ネットワーク上の既存の MPLS WAN リンクのパスに物理的に展開され、既存のバックアップリンクを使用して、アクティブ状態に有効にし、その 2 番目の WAN リンクを SD-WAN に直接終端します。アプライアンスを別のサブネット 172.16.31.0/24 に配置します。

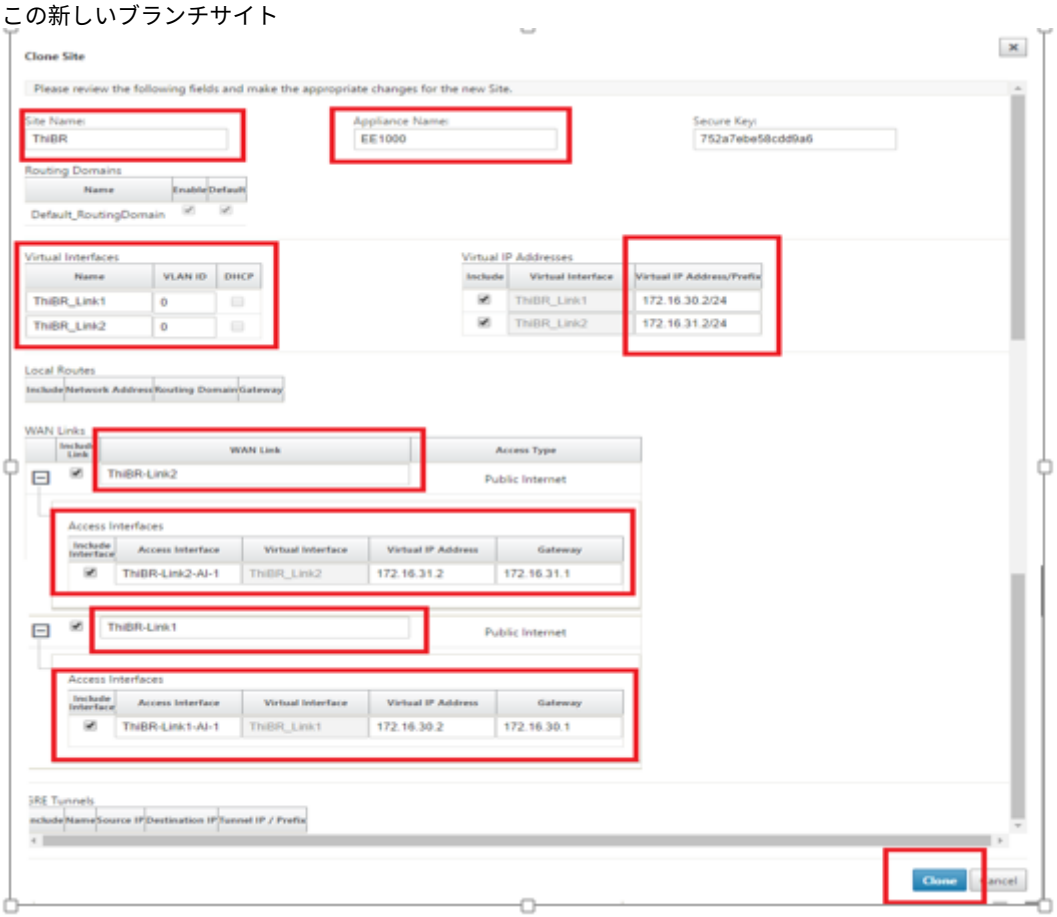
> 注
>
> SD-WAN アプライアンスは、デフォルトの IP アドレス 192.168.100.1/16 を自動的に割り当てます。DHCP がデフォルトで有効になっている場合、ネットワーク内の DHCP サーバは、デフォルトと重複するサブネット内の 2 番目の IP アドレスをアプライアンスに提供することがあります。これにより、アプライアンスがゼロタッチデプロイメント Cloud Service に接続できない可能性があるアプライアンスでルーティングの問題が発生する可能性があります。DHCP サーバーを構成して、192.168.0.0/16 の範囲外の IP アドレスを割り当てます。
>
> ネットワーク内の SD-WAN 製品の配置には、さまざまな展開モードを使用できます。上記の例では、SD-WAN が既存のネットワークインフラストラクチャの上にオーバーレイとして展開されています。新しいサイトの場合、SD-WAN 管理者は、SD-WAN をエッジモードまたは Gateway モードで展開し、WAN エッジルータとファイアウォールが不要になり、エッジルーティングとファイアウォールのネットワークニーズを SD-WAN ソリューションに統合できます。

7. SD-WAN Center Web 管理インターフェイスを開き、[設定] **> [**** ネットワーク設定 **] ページに移動します。



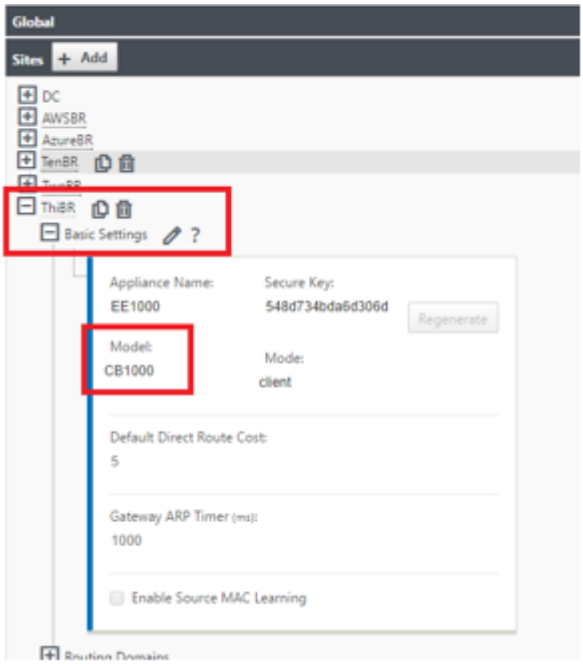
8. 作業設定が既に設定されていることを確認するか、MCN から設定をインポートします。
9. [詳細] タブに移動して、サイトを作成します。
10. [サイト] タイルを開いて、現在構成されているサイトを表示します。
11. 既存のサイトのクローン機能を使用して、新しいサイトの構成をすばやく構築しました。

12. この新しいブランチサイト



。

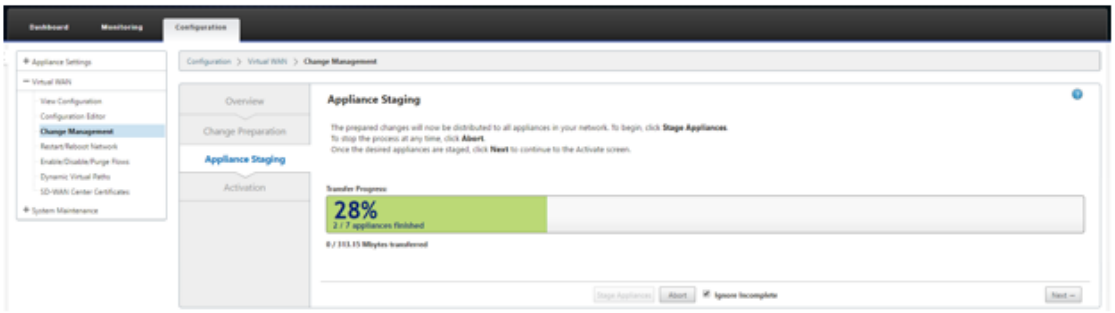
13. 新しいサイトのクローンを作成した後、サイトの [基本設定] に移動し、ゼロタッチサービスをサポートする SD-WAN のモデルが正しく選択されていることを確認します。



サイトの SD-WAN モデルは更新できますが、更新されたアプライアンスはクローン作成に使用されたインターフェイスレイアウトよりも新しいインターフェイスレイアウトを持つ場合があるため、インターフェイスグループの再定義が必要になる場合があることに注意してください。

14. 新しい構成を SD-WAN Center に保存し、変更管理受信トレイへのエクスポートオプションを使用して、変更管理 を使用して構成をプッシュします。

15. 変更管理の手順に従って、新しい構成を適切にステージングします。これにより、既存の SD-WAN デバイスは、ゼロタッチで展開される新しいサイトを認識します。「Ignore Concomplete」オプションを使用して、まだ実行する必要がある新しいサイトに構成をプッシュすることをスキップする必要があります。ゼロタッチ導入ワークフロー。

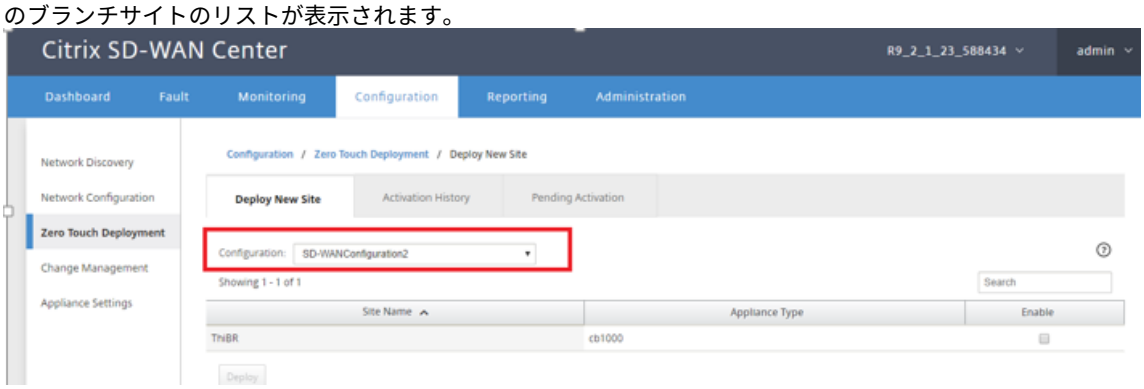


16. SD-WAN Center のゼロタッチ展開ページに戻り、新しいアクティブな構成が実行されている状態で、新しいサイトを展開できます。

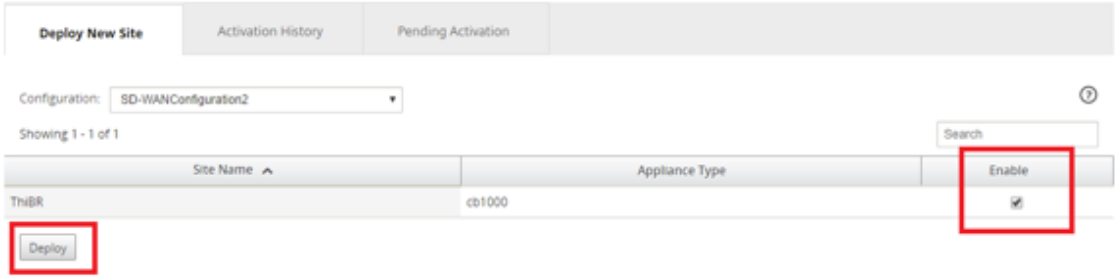
17. [ゼロタッチ展開] ページの [新しいサイトの展開] タブで、実行中のネットワーク設定ファイルを選択します。

18. 実行構成ファイルを選択すると、ゼロタッチでサポートされている未展開の SD-WAN デバイスを持つすべて

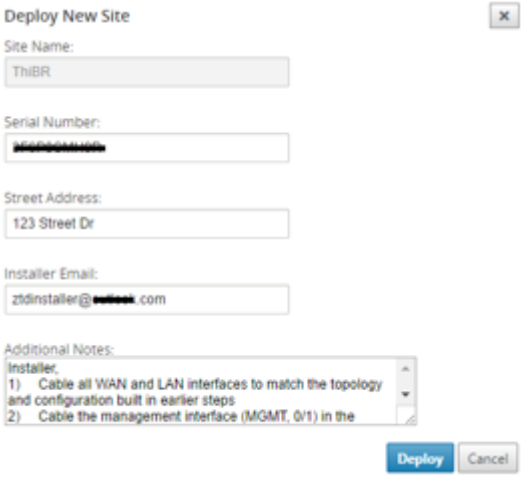
のブランチサイトのリストが表示されます。



19. ゼロタッチサービス用に構成するブランチサイトを選択し、[有効化]、[展開] の順にクリックします。



20. Deploy New Site ポップアップウィンドウが表示されます。管理者は、必要に応じて、シリアル番号、ブランチサイトのストリートアドレス、インストーラの電子メールアドレス、その他のメモを提供できます。



> 注
>
> シリアル番号入力フィールドはオプションであり、入力されているかどうかに応じて、インストーラーが担当するオンサイトのアクティビティが変更されます。

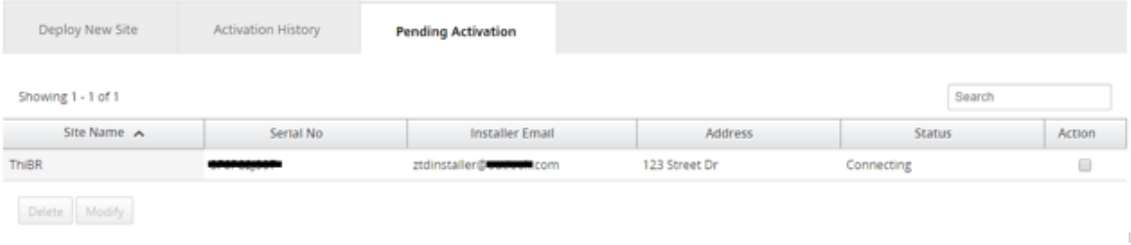
```
>- シリアル番号フィールドが入力されている場合 — インストーラは、deploy site コマンドで生成されたアクティベーション URL にシリアル番号を入力する必要がありません
>
```



```
3     >- シリアル番号フィールドが黒のままの場合 — インストーラは、deploy site コマンドで生成されたアクティベーション URL に、アプライアンスの正しいシリアル番号を入力します。
```

21. [展開] ボタンをクリックすると、「サイト構成が展開されました。」というメッセージが表示されます。この操作により、以前にゼロタッチデプロイ Cloud Service に登録された SD-WAN Center がトリガーされ、この特定のサイトの構成がゼロタッチデプロイ Cloud Service に格納される一時的なものになります。

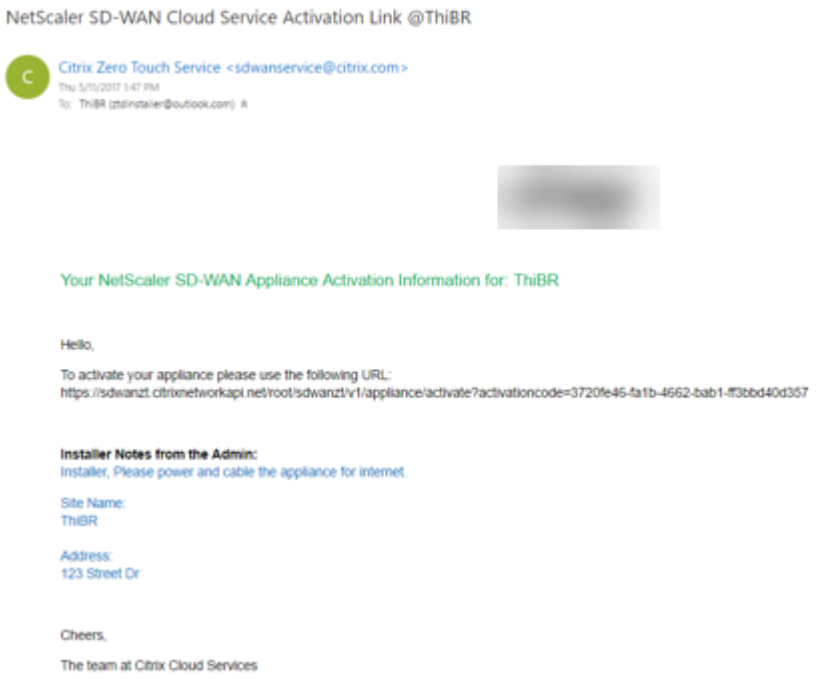
22. [保留中のアクティブ化] タブに移動して、ブランチサイト情報が正常に入力され、インストーラーアクティビティが保留中の状態になったことを確認します。



> 注
>
> 情報が正しくない場合は、[Pending Activation] 状態のゼロタッチ展開を [Delete] または [Modify] にオプションとして選択できます。保留中のアクティブ化ページからサイトが削除されると、そのサイトは [新しいサイトのデプロイ] タブページでデプロイできるようになります。アクティベーションの保留からブランチサイトを削除することを選択すると、インストーラーに送信されたアクティベーションリンクは無効になります。
>
> SD-WAN 管理者が [シリアル番号] フィールドに入力しなかった場合、ステータスフィールドには「接続中」ではなく「インストーラを待機中」と表示されます。

23. 次の一連の作業は、オンサイトインストーラによって実行されます。

    a) インストーラーは、SD-WAN 管理者がサイトの展開時に使用した電子メールアドレスのメールボックスを確認します。



b) インターネットブラウザーウィンドウでゼロタッチ展開アクティベーション URL を開きます。

c) SD-WAN 管理者がサイトの展開手順でシリアル番号を事前に入力しなかった場合は、インストーラが物理アプライアンスのシリアル番号を特定し、アクティベーション URL にシリアル番号を手動で入力し、[**Activate**] ボタンをクリックします。

d) 管理者がシリアル番号情報を事前に入力している場合、アクティベーション URL は次のステップに進んでいます。

e) 次のアクションを実行するには、設置者が現場にいる必要があります。

- 前の手順で構築したトポロジと構成に一致するように、すべての WAN および LAN インターフェ

イスをケーブルで接続します。

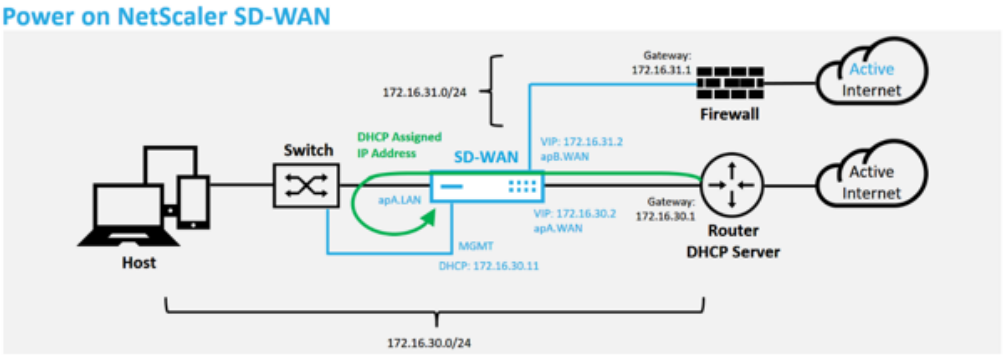
- 管理インターフェース（MGMT、0/1) DHCP IP アドレスと、DNS および FQDN から IP アドレスへの解決によりインターネットへの接続を提供するネットワークのセグメント内。
- SD-WAN アプライアンスの電源ケーブル。
- アプライアンスの電源スイッチをオンにします。

> 注
>
> ほとんどのアプライアンスは、電源ケーブルを接続すると自動的に電源が入ります。アプライアンスによっては、アプライアンスの前面にある電源スイッチを使用して電源をオンにする必要がある場合や、アプライアンスの背面にある電源スイッチを使用する場合があります。一部の電源スイッチでは、ユニットの電源が入るまで電源ボタンを押し続ける必要があります。

24. 次の一連のステップは、ゼロタッチ展開サービスの助けを借りて自動化されますが、次の前提条件が利用可能であることが必要です。

    - ブランチアプライアンスの電源がオンになっている必要があります
    - 管理と DNS IP アドレスを割り当てるには、既存のネットワークで DHCP を使用できる必要があります
    - DHCP が割り当てた IP アドレスには、FQDN を解決する機能を備えたインターネットへの接続が必要です
    - 他の前提条件が満たされている限り、IP 割り当てを手動で構成できます。

    a) アプライアンスは、ネットワークの DHCP サーバから IP アドレスを取得します。このトポロジ例では、これは工場出荷時のデフォルトステートアプライアンスのバイパスされたデータインターフェイスを介して実現されます。

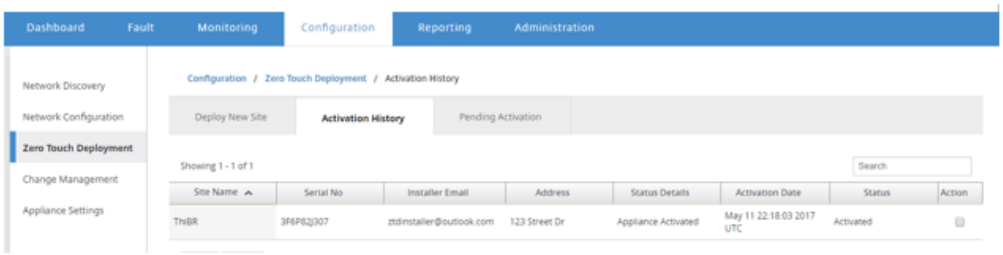
    

    b) アプライアンスがアンダーレイネットワーク DHCP サーバーから Web 管理および DNS IP アドレスを取得すると、アプライアンスはゼロタッチ展開サービスを開始し、ゼロタッチ展開に関連するソフトウェアアップデートをダウンロードします。

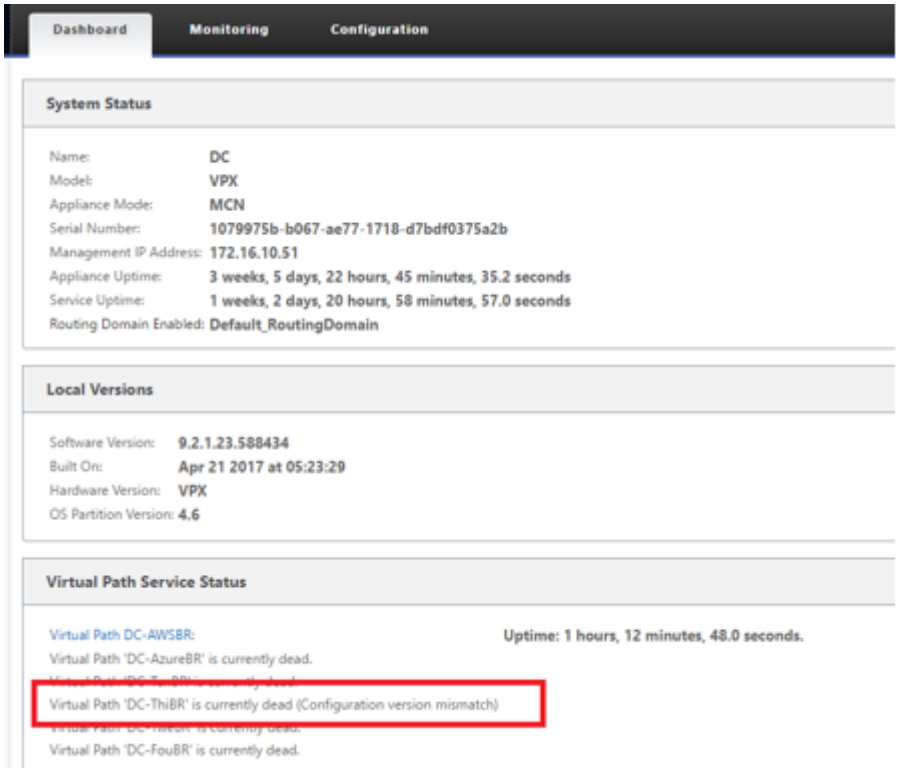
    c) ゼロタッチデプロイメントクラウドサービスへの接続に成功すると、デプロイメントプロセスは自動的に次の処理を実行します。

- SD-WAN Center によって以前に保存された構成ファイルをダウンロードします。
- ローカルアプライアンスへの構成の適用
- 10 MB の一時ライセンスファイルをダウンロードしてインストールする
- 必要に応じて、ソフトウェアの更新をダウンロードしてインストールします
- SD-WAN サービスをアクティブ化する

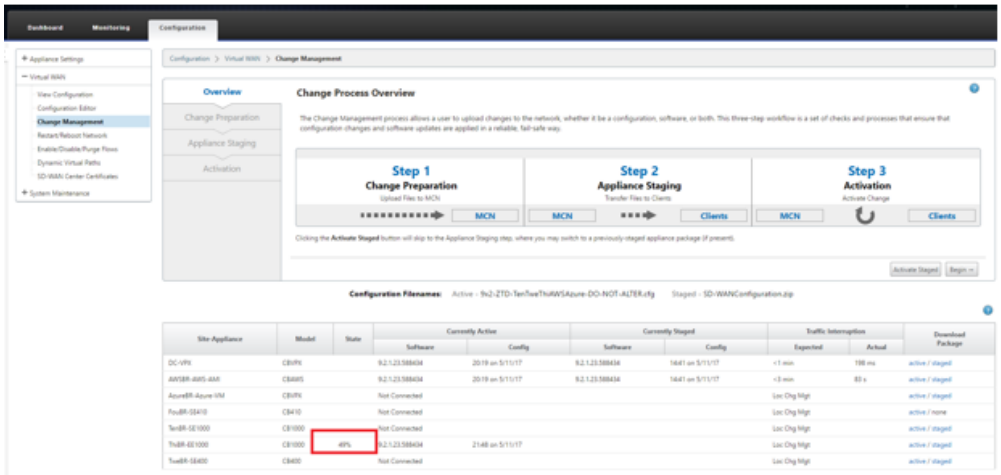
d) SD-WAN Center Web 管理インターフェイスでさらに確認することができます。Zero Touch Deployment メニューには、アクティベーション履歴タブに正常にアクティベーションされたアプライアンスが表示されます。



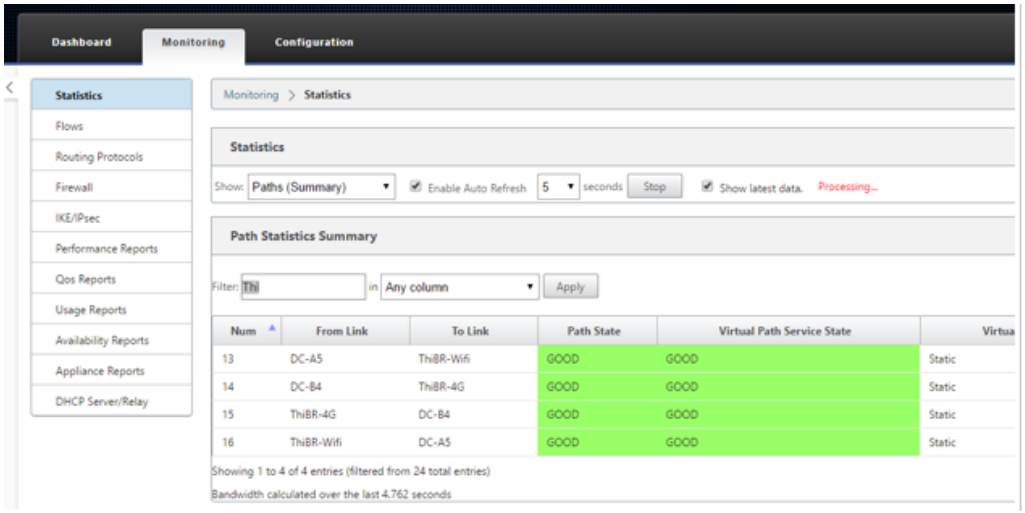
e) MCN がゼロタッチ展開クラウドサービスから継承された設定を信頼しない場合があり、MCN ダッシュボードで「構成バージョンの不一致」を報告するため、仮想パスが接続状態ですぐには表示されないことがあります。



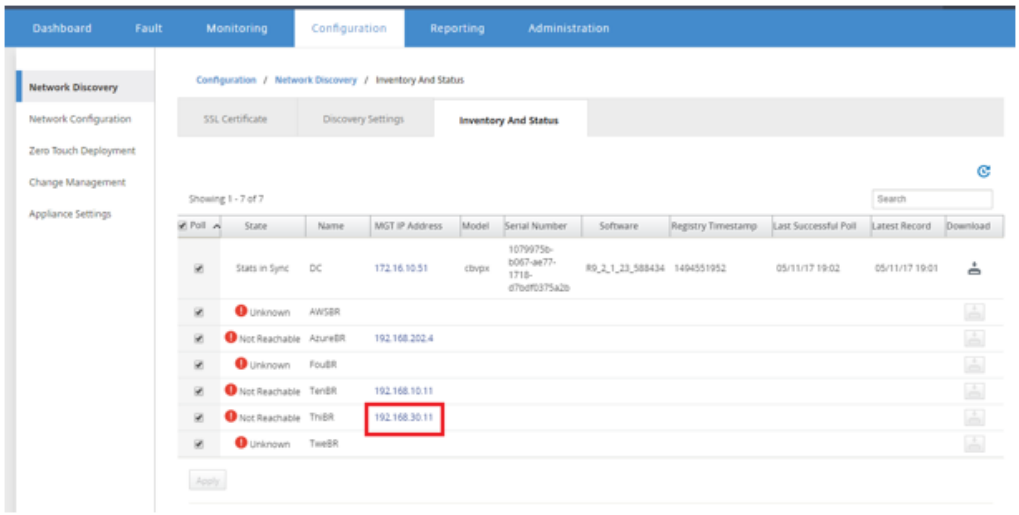
f) 構成は新しくインストールされたブランチオフィスアプライアンスに再配信され、ステータスは [**MCN**] > [構成] > [仮想 **WAN**] > [変更管理] ページで監視されます（このプロセスが完了するまで数分かかる場合があります）。



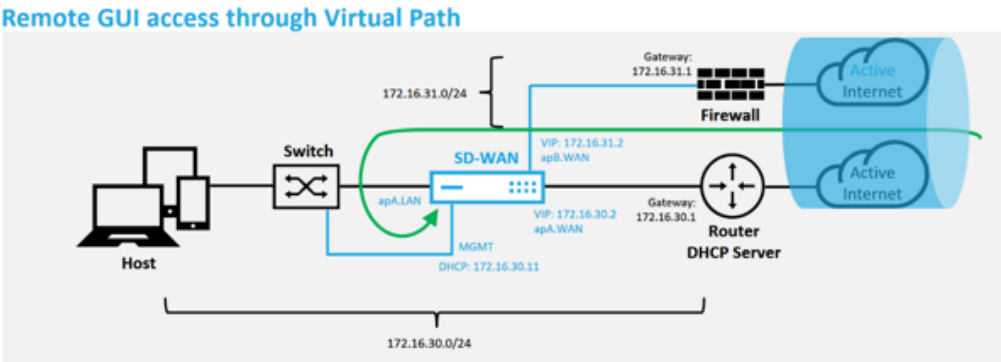
g) SD-WAN 管理者は、リモートサイトの確立された仮想パスのヘッドエンド MCN Web 管理ページを監視できます。



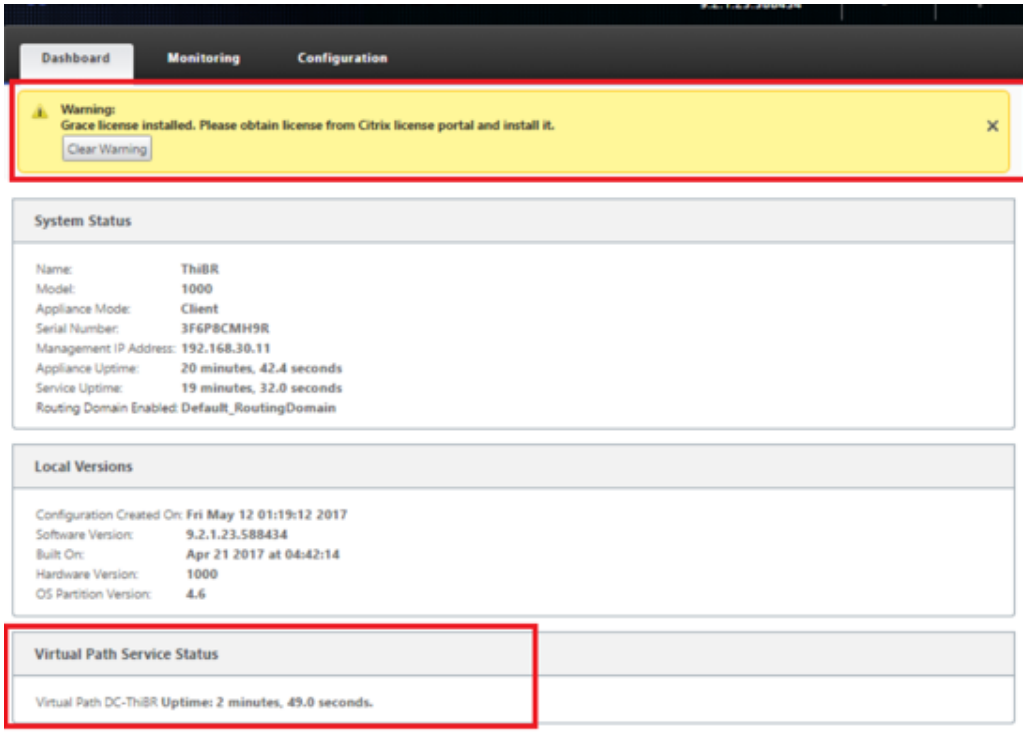
h) SD-WAN Center は、[設定] > [ネットワーク探索] > [インベントリとステータス] ページから、オンサイトアプライアンスの DHCP 割り当てられた IP アドレスを識別するためにも使用できます。



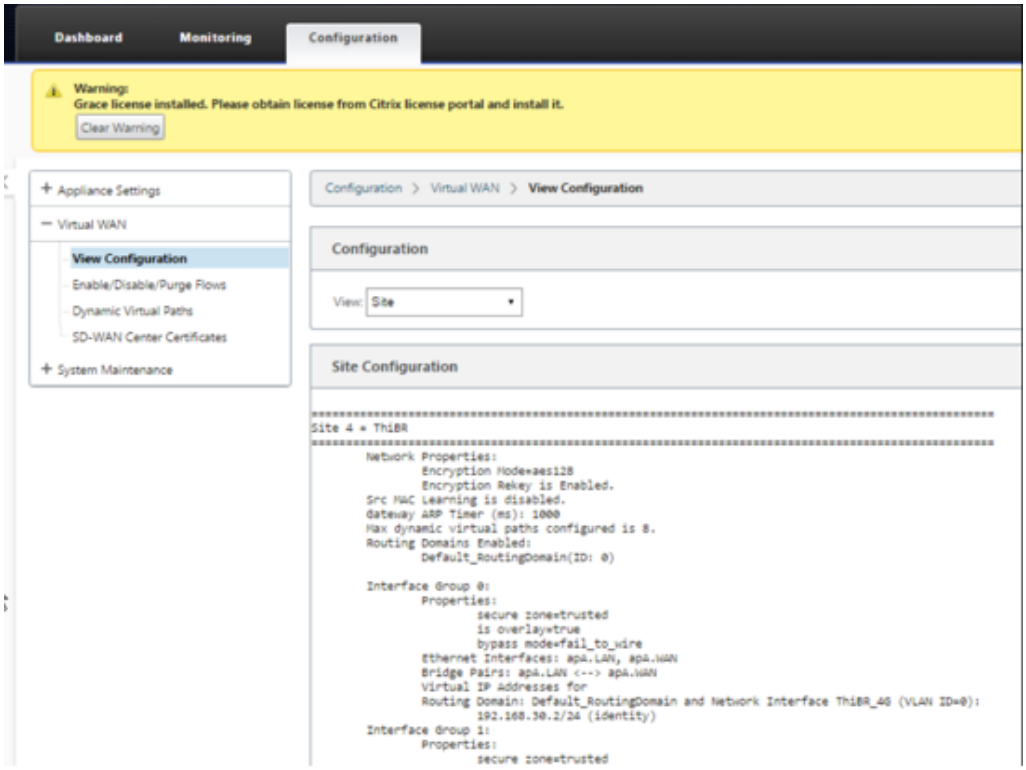
i) この時点で、SD-WAN ネットワーク管理者は、SD-WAN オーバーレイネットワークを使用して、オンサイトアプライアンスへの Web 管理アクセスを取得できます。



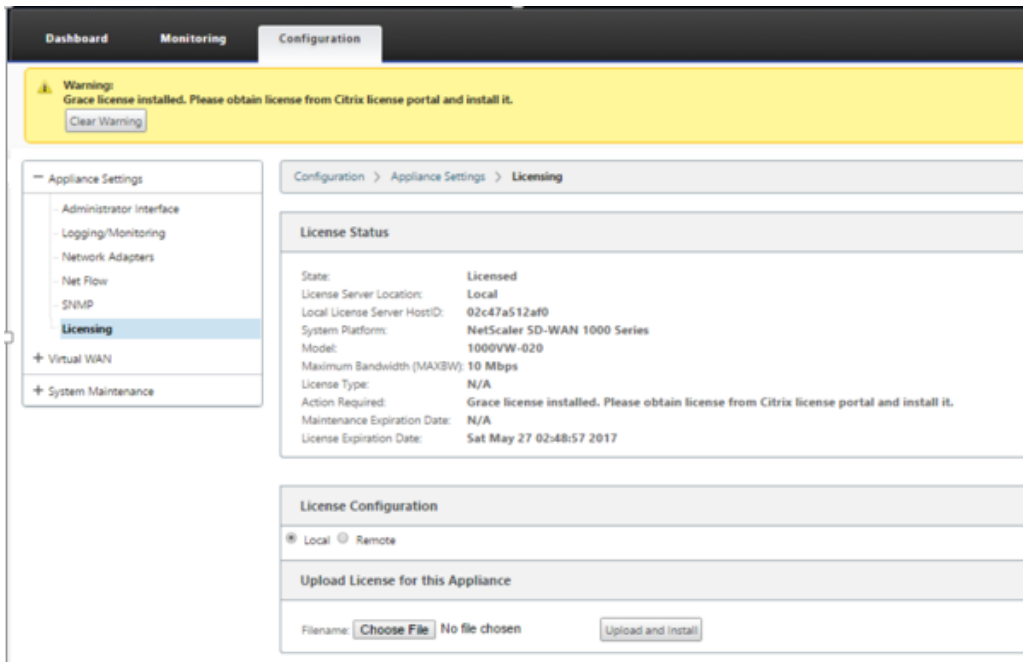
j) リモートサイトアプライアンスへの Web 管理アクセスは、アプライアンスに 10 Mbps の一時的な猶予ライセンスがインストールされていることを示しています。これにより、仮想パスサービスステータスをアクティブとして報告することができます。



k) アプライアンスの構成は、構成 > 仮想 **WAN** > 「構成の 表示」ページを使用して検証できます。



l) アプライアンスライセンスファイルは、構成 > アプライアンスの設定 > ライセンス ページを使用して永久ライセンスに更新できます。



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

オンプレミスのゼロタッチ

May 10, 2021

ゼロタッチサービスを使用して SD-WAN アプライアンスをデプロイする方法については、トピック「ゼロタッチ展開サービスを構成する方法」を参照してください。

AWS

May 10, 2021

以下のセクションでは、AWS 環境に ZTD をデプロイする方法について説明します。

AWS でのデプロイ:

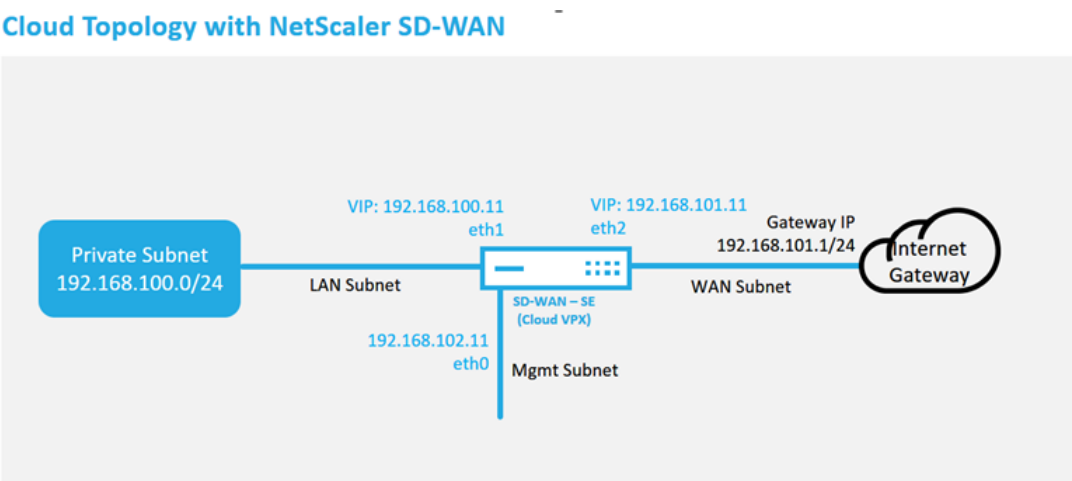
SD-WAN リリース 9.3 では、ゼロタッチ展開機能がクラウドインスタンスに拡張されました。ゼロタッチデプロイメントプロセス 4 つのクラウドインスタンスをデプロイする手順は、ゼロタッチサービスのアプライアンスデプロイとは少し異なります。

1. SD-WAN Center ネットワーク構成を使用して、ZTD 対応の SD-WAN クラウドデバイスを持つ新しいリモートサイトを追加するように構成を更新します。

   SD-WAN 設定が SD-WAN Center ネットワーク設定を使用して構築されていない場合は、MCN からアクティブな設定をインポートし、SD-WAN Center を使用して設定の変更を開始します。Zero Touch Deployment 機能を使用するには、SD-WAN 管理者は SD-WAN Center を使用して設定を構築する必要があります。ゼロタッチ展開を対象とする新しいクラウドノードを追加するには、次の手順を使用する必要があります。

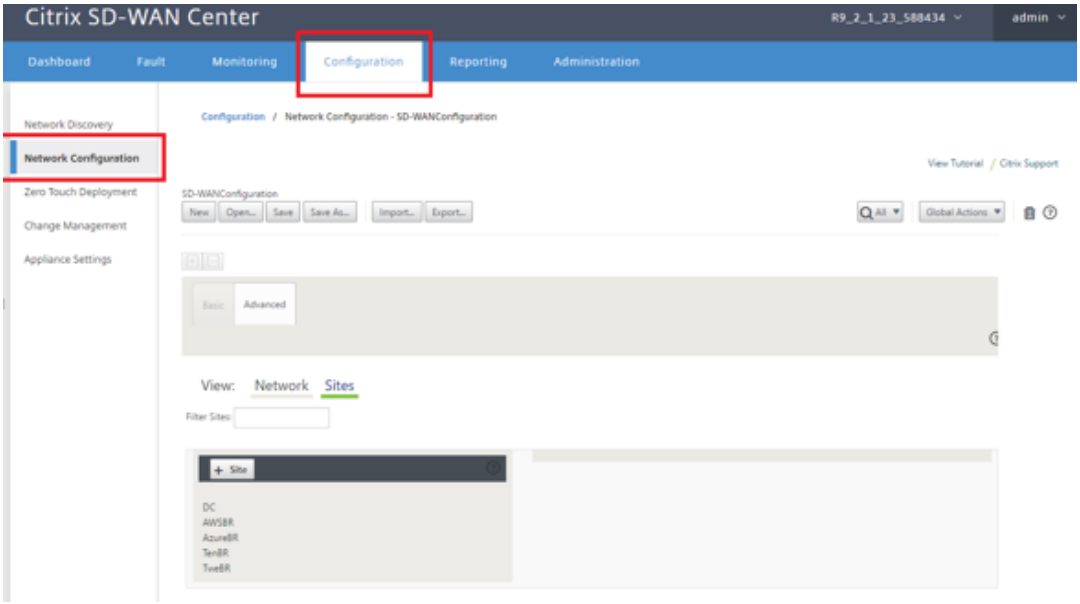
   a) 最初に新しいサイトの詳細（つまり、VPX サイズ、インターフェイスグループの使用状況、仮想 IP アドレス、帯域幅を備えた WAN リンク、およびそれぞれの Gateway）を概説することにより、SD-WAN クラウド展開用の新しいサイトを設計します。

      > 注
      >
      > - クラウドにデプロイされた SD-WAN インスタンスは、Edge/Gateway モード。
      > - クラウドインスタンスのテンプレートは、管理、LAN、WAN（順序）の 3 つのインターフェイスに制限されています。
      > - SD-WAN VPX で使用可能なクラウドテンプレートは、現在、VPC で使用可能なサブネットの #.#..11 IP アドレスを取得するためにハードセットされています。



これは、SD-WAN クラウド展開サイトの展開例です。Citrix SD-WAN デバイスは、このクラウドネットワーク内の単一のインターネット WAN リンクサービスを提供するエッジデバイスとして展開されます。リモートサイトは、クラウド用のこの同じ Internet Gateway に接続する複数の異なるインターネット WAN リンクを活用して、任意の SD-WAN 展開サイトからクラウドインフラストラクチャへの耐障害性と集約帯域幅接続を提供します。これにより、コスト効率に優れ、信頼性の高いクラウド接続が可能になります。

b) SD-WAN Center Web 管理インターフェイスを開き、[設定**] > [**** ネットワーク設定 **] ページに移動します。



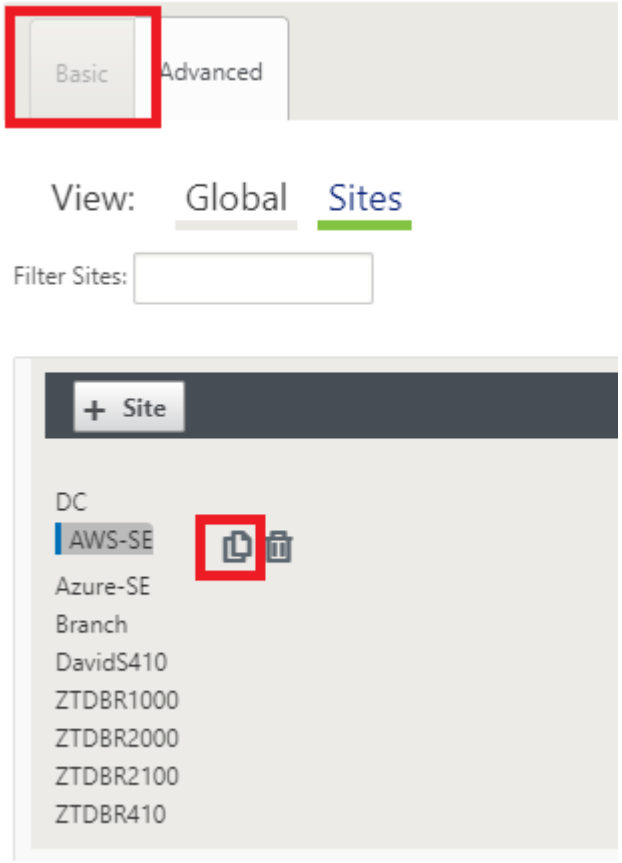
c) 動作中の構成がすでに配置されていることを確認するか、MCN から構成をインポートします。

d) [基本] タブに移動して、新しいサイトを作成します。

e) [サイト] タイルを開いて、現在構成されているサイトを表示します。

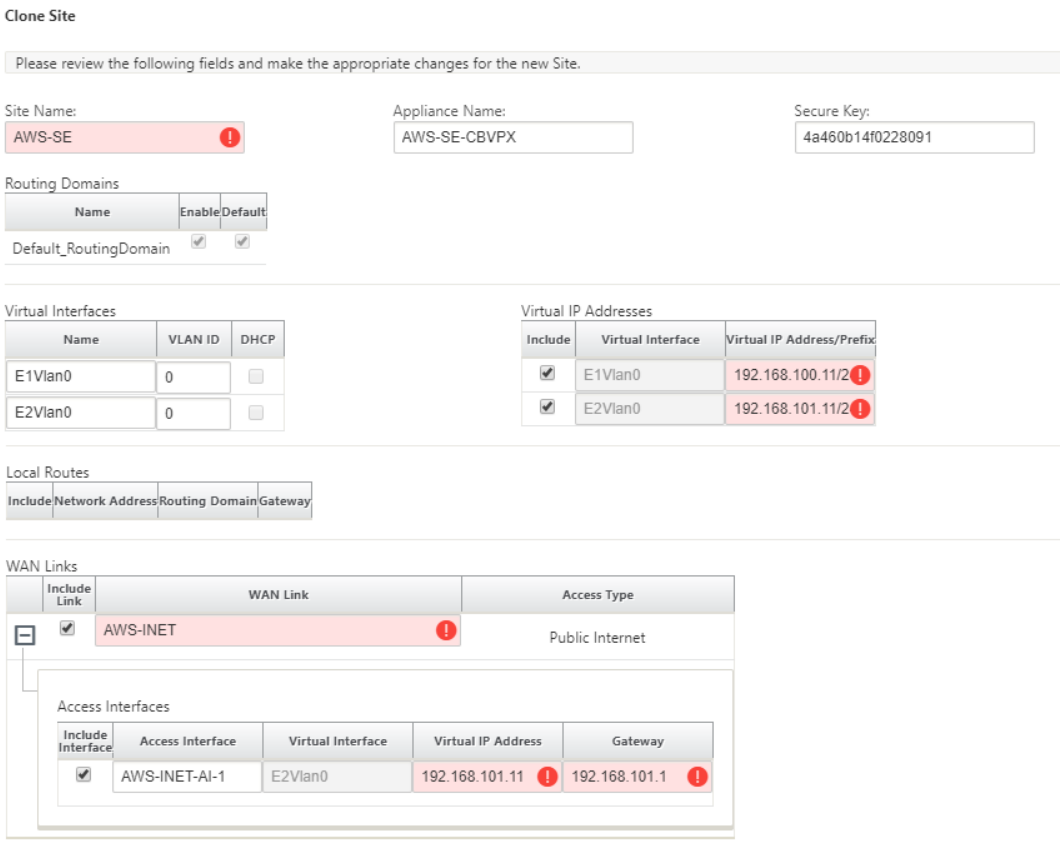
f) 既存のサイトのクローン機能を利用して新しいクラウドサイトの構成をすばやく構築するか、新しいサ

イトを手動で構築します。

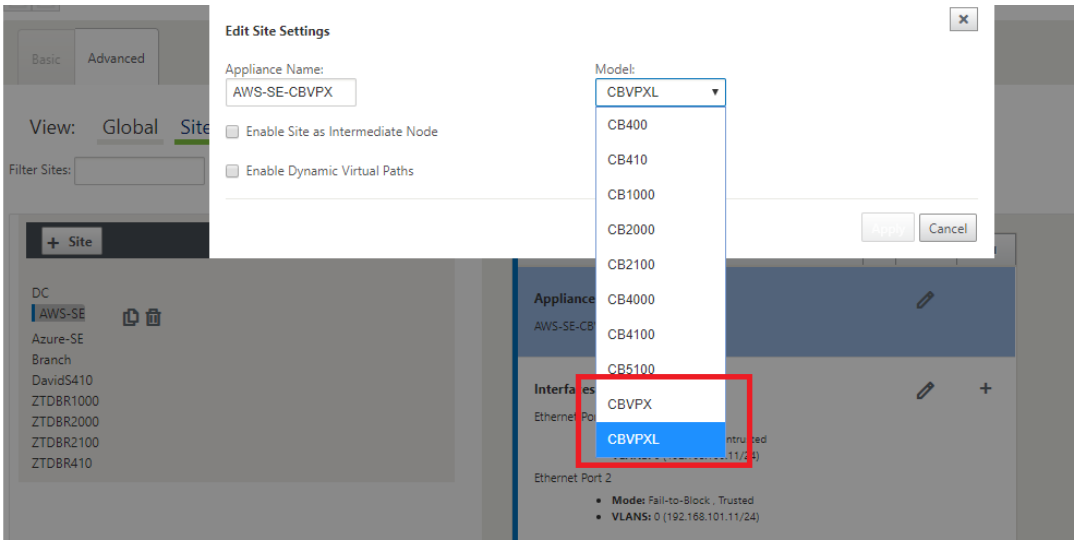


g) この新しいクラウドサイト用に設計したトポロジから、必要なフィールドをすべて入力します。

クラウド ZTD 展開で使用できるテンプレートは、管理サブネット、LAN サブネット、および WAN サブネットの #..11 IP アドレスを使用するのが難しいことに注意してください。各インターフェイスで予想される.11 IP ホストアドレスと一致するように設定されていない場合、デバイスはクラウド環境ゲートウェイへの ARP と MCN の仮想パスへの IP 接続を適切に確立できません。



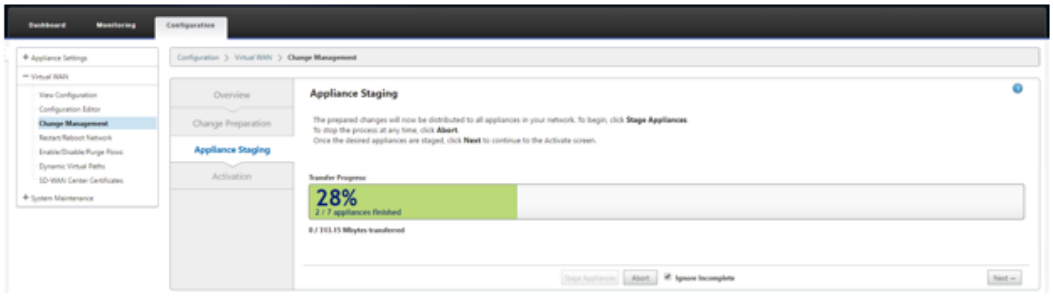
h) 新しいサイトのクローンを作成したら、サイトの [基本設定] に移動し、ゼロタッチサービスをサポートする SD-WAN のモデルが正しく選択されていることを確認します。



i) 新しい構成を SD-WAN Center に保存し、変更管理受信トレイへのエクスポートオプションを使用して、変更管理 を使用して構成をプッシュします。

j) 変更管理手順に従って新しい構成を適切にステージングします。これにより、既存の SD-WAN デバイ

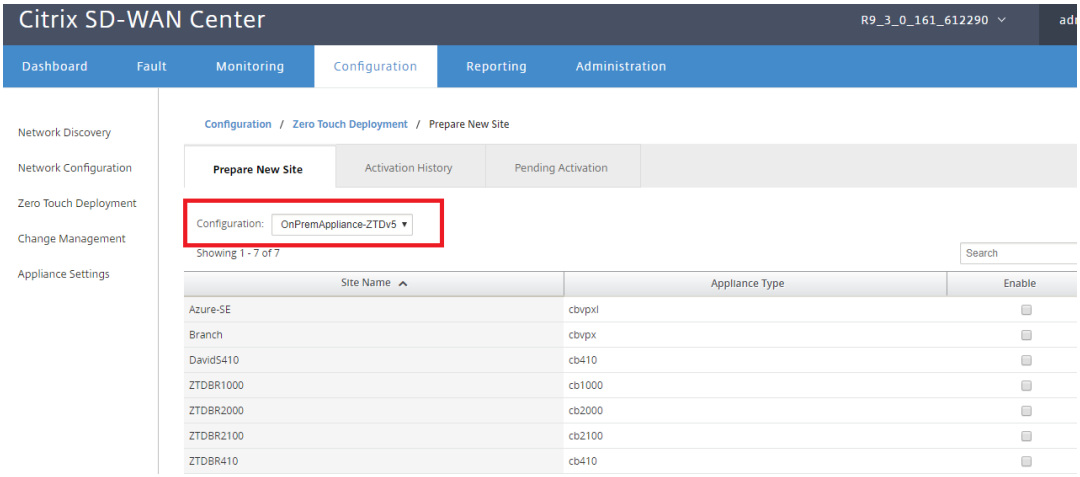
スが、ゼロタッチで展開される新しいサイトを認識します。[*Ignore In* freted] オプションを使用して、新しいサイトに構成をプッシュしないようにする必要があります。は引き続き ZTD ワークフローを通過する必要があります。



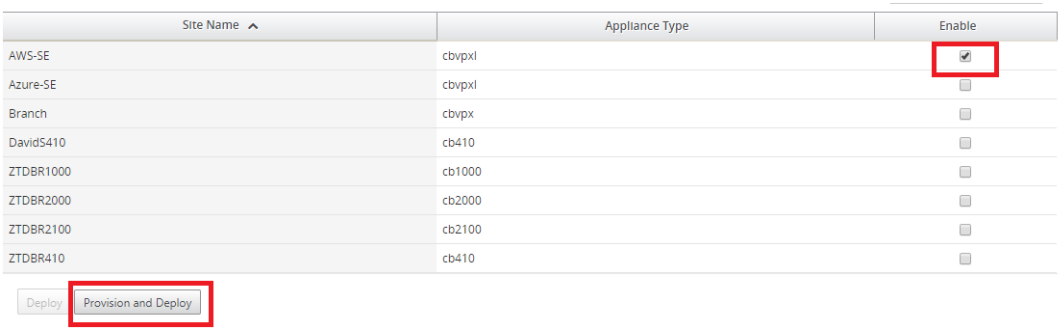
2. SD-WAN Center のゼロタッチ展開ページに戻り、新しいアクティブな構成を実行すると、新しいサイトを展開できるようになります。

   a) [ゼロタッチ展開] ページの [新しいサイトの展開] タブで、実行中のネットワーク構成ファイルを選択します。

   b) 実行構成ファイルを選択すると、ゼロタッチでサポートされている展開されていない Citrix SD-WAN デバイスを持つすべてのブランチサイトのリストが表示されます。

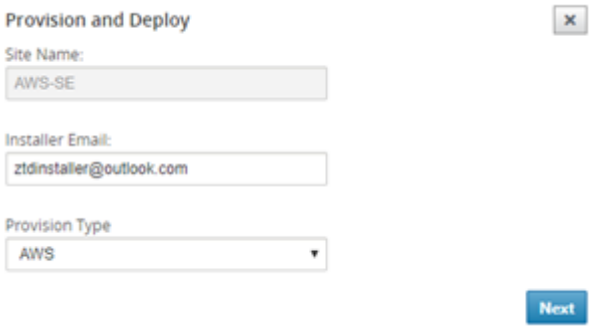


   c) Zero Touch サービスを使用してデプロイするターゲットクラウドサイトを選択し、[有効にする]、[プロビジョニングとデプロイ] の順にクリックします。

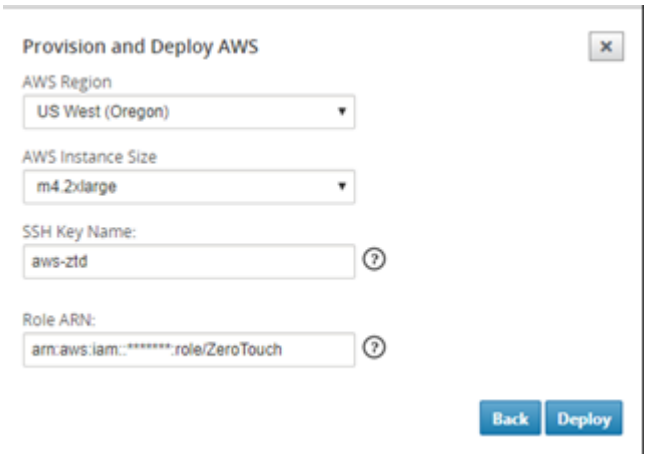


d) ポップアップウィンドウが表示され、Citrix SD-WAN 管理者がゼロタッチの展開を開始できます。

アクティベーション URL を配信できる電子メールアドレスを入力し、目的のクラウドの プロビジョニングタイプ を選択します。



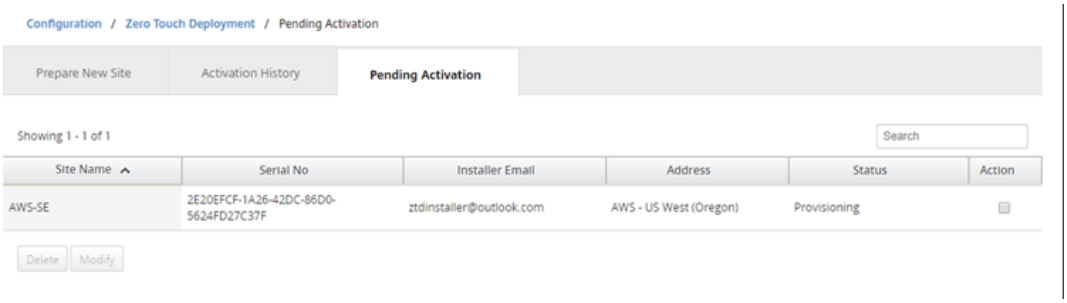
e) [次へ] をクリックし、適切なリージョン、インスタンスのサイズを選択し、SSH キー名とロール ARN フィールドに適切に設定します。



> 注
>
> クラウドアカウントで SSH キーとロール ARN を設定する方法のガイダンスについては、ヘルプリンクを利用してください。また、選択したリージョンがアカウントで利用可能なリージョンと一致し、選択したインスタンスサイズが、SD-WAN 構成で選択したモデルとして VPX または VPXL と一致していることを確認します。

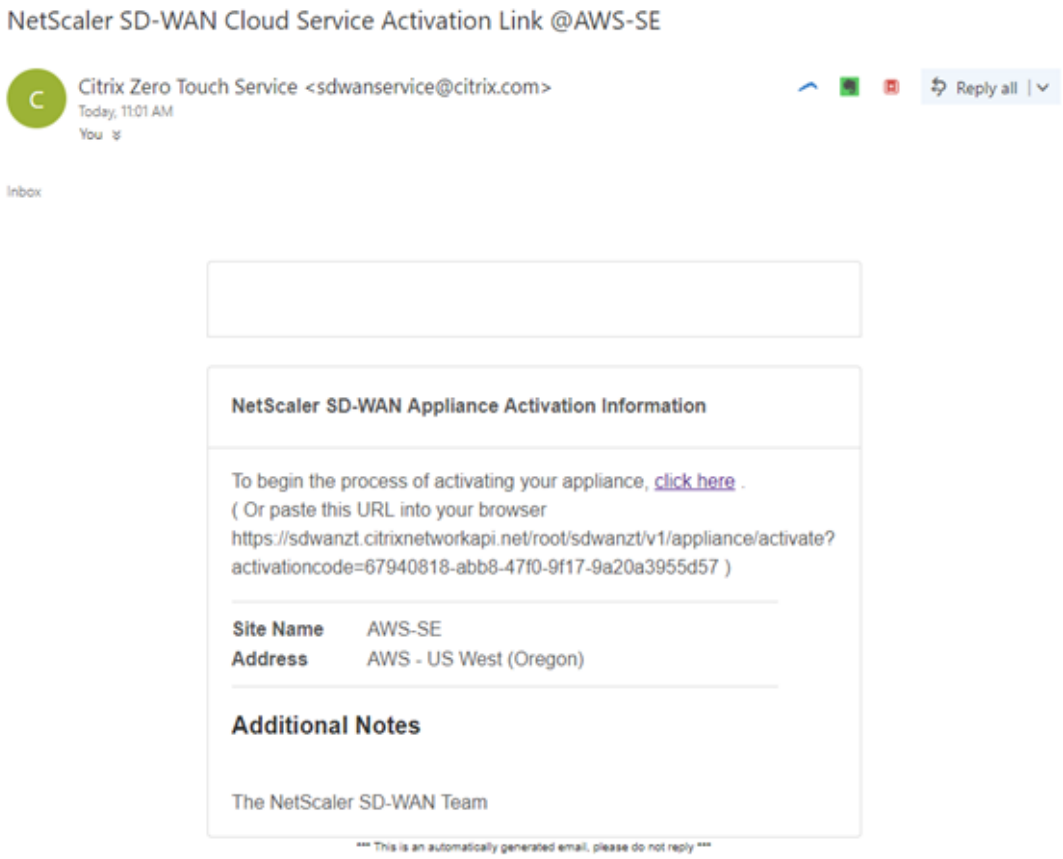
f) 以前に ZTD クラウドサービスに登録されていた SD-WAN Center を起動して、ZTD クラウドサービスに保存されているサイトの設定を共有します。

g) [**Pending Activation**] タブに移動して、サイト情報が正常に入力され、Provisioning 状態になったことを確認します。



3. クラウド管理者としてゼロタッチ導入プロセスを開始します。

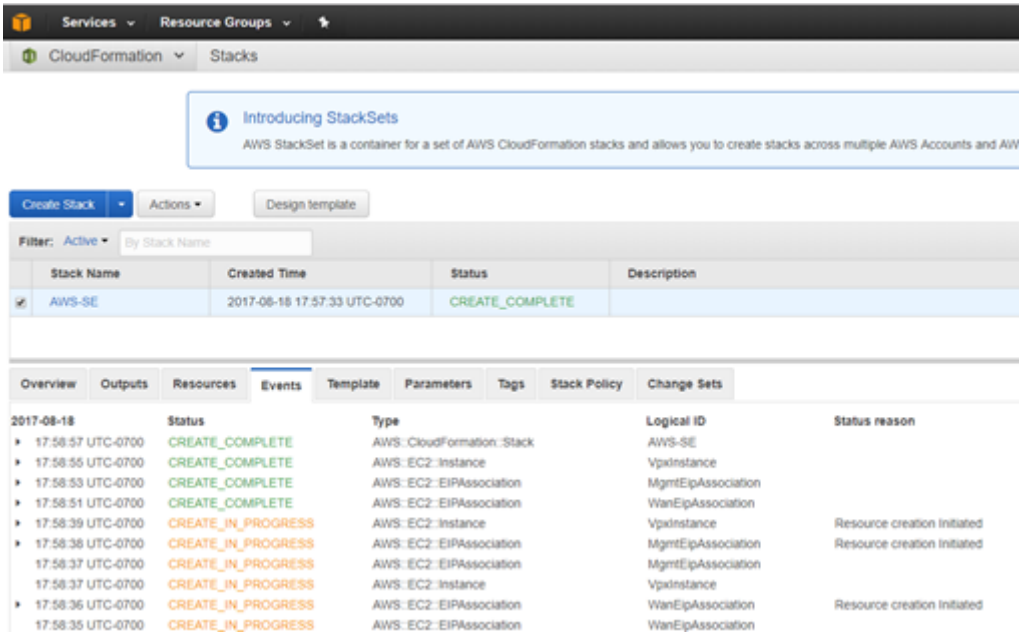
   a) インストーラーは、サイトの展開時に SD-WAN 管理者が使用した電子メールアドレスのメールボックスを確認する必要があります。



   b) 電子メールにあるアクティベーション URL をインターネットブラウザウィンドウで開きます（例; `https://sdwanzt.citrixnetworkapi.net`）。

   c) SSH キーとロール ARN が正しく入力されている場合、ゼロタッチ展開サービスはすぐに SD-WAN インスタンスのプロビジョニングを開始します。それ以外の場合は、接続エラーがすぐに表示されます。

d) AWS コンソールでの追加のトラブルシューティングでは、クラウド形成サービスを利用して、プロビジョニングプロセス中に発生するイベントをキャッチできます。

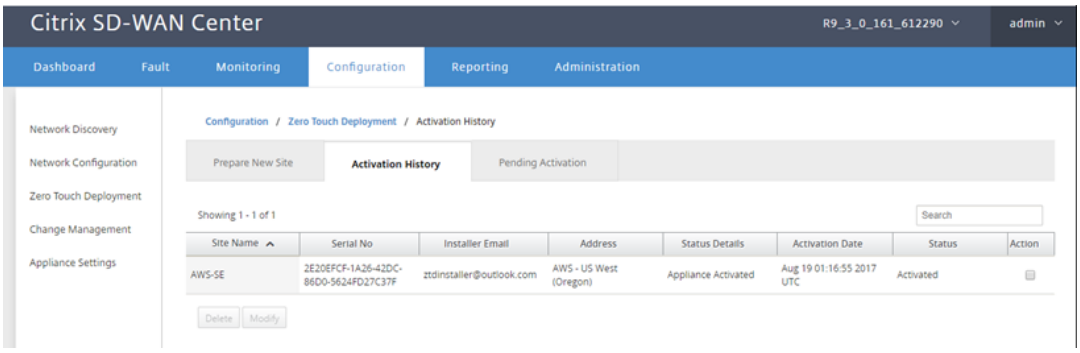


e) プロビジョニングプロセスを許可する ~8-10 分とアクティベーション別 ~3-5 完全に完了するまで数分。

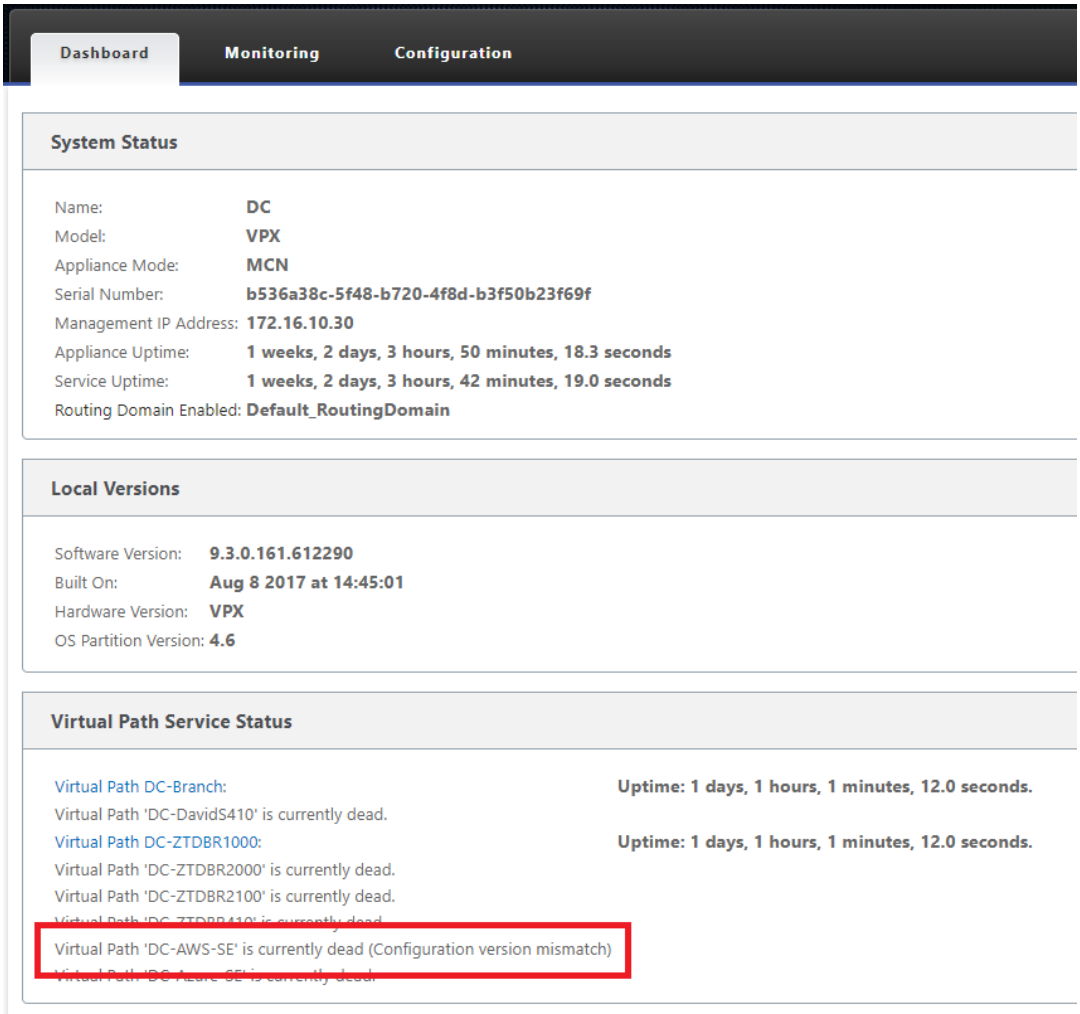
f) SD-WAN クラウドインスタンスの ZTD クラウドサービスへの接続が成功すると、サービスは自動的に以下を実行します。

- SD-WAN Center によって以前に保存されたサイト固有の設定ファイルをダウンロードします。
- ローカルインスタンスへの構成の適用
- 10 MB の一時ライセンスファイルをダウンロードしてインストールする
- 必要に応じて、ソフトウェアの更新をダウンロードしてインストールします
- SD-WAN サービスをアクティブ化する

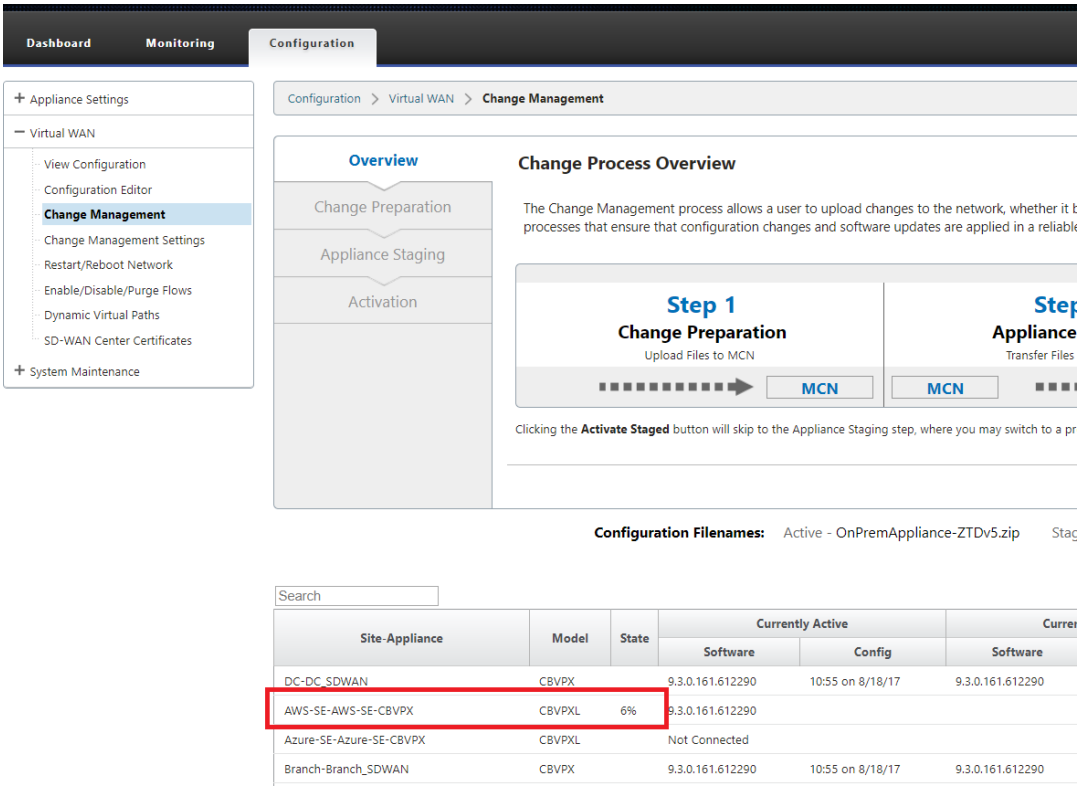
g) SD-WAN Center Web 管理インターフェイスでさらに確認を行うことができます。ゼロタッチ展開メニューには、アクティベーション履歴タブに正常にアクティ ベートされたアプライアンスが表示されます。



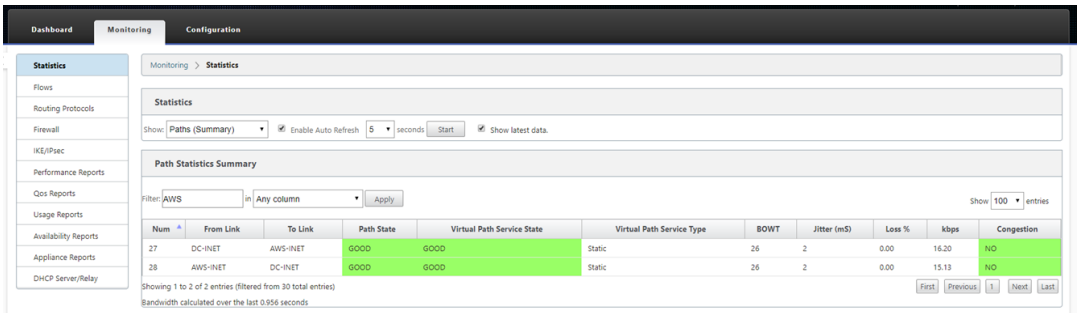
h) 仮想パスは接続状態ですぐに表示されないことがあります。これは、MCN が ZTD Cloud Service から受け継がれた設定を信頼していない可能性があり、MCN ダッシュボード で設定バージョンの不一致を報告するためです。



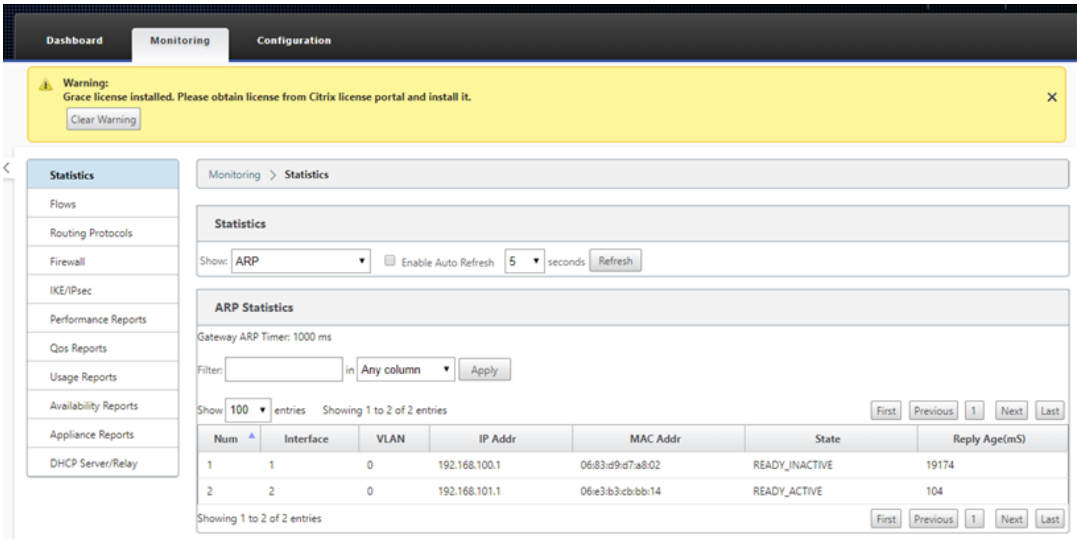
i) 構成は、新しくインストールされたブランチオフィスアプライアンスに自動的に再配信されます。このステータスは、[**MCN**] > [構成] > [仮想 **WAN**] > [変更管理] ページで監視できます (接続によっては、このプロセスが完了するまで数分かかる場合があります)。



j) SD-WAN 管理者は、新しく追加されたクラウドサイトの確立された仮想パスについて、ヘッドエンドの MCN Web 管理ページを監視できます。



k) トラブルシューティングが必要な場合は、Provisioning 中にクラウド環境によって割り当てられたパブリック IP を使用して SD-WAN インスタンスのユーザーインターフェイスを開き、[**Monitor** ing] > [**Statistics**] ページの [ARP] テーブルを使用して、予想されるゲートウェイへの接続に関する問題を特定します。は、診断でトレースルートとパケットキャプチャオプションを使用します。



Azure

May 10, 2021

クラウドインスタンスのゼロタッチ展開プロセスを展開する手順は、ゼロタッチサービスのアプライアンス展開とは少し異なります。

SD-WAN Center のネットワーク構成を使用して、ZTD 対応の SD-WAN クラウドデバイスを持つ新しいリモートサイトを追加するように構成を更新します。

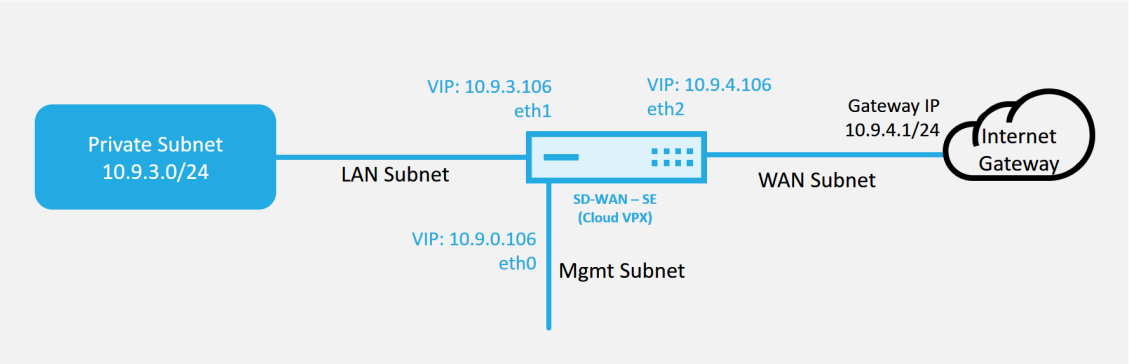
SD-WAN 設定が SD-WAN Center ネットワーク設定を使用して構築されていない場合は、MCN からアクティブな設定をインポートし、SD-WAN Center を使用して設定の変更を開始します。Zero Touch Deployment 機能を使用するには、SD-WAN 管理者は SD-WAN Center を使用して設定を構築する必要があります。ゼロタッチ展開を対象とする新しいクラウドノードを追加するには、次の手順を使用する必要があります。

1. 最初に新しいサイトの詳細（つまり、VPX サイズ、インターフェイスグループの使用状況、仮想 IP アドレス、帯域幅を備えた WAN リンク、およびそれぞれの Gateway）を概説することにより、SD-WAN クラウド展開用の新しいサイトを設計します。

   > 注
   >
   > - クラウドにデプロイされた SD-WAN インスタンスは、Edge/Gateway モード。
   > - クラウドインスタンスのテンプレートは 3 つのインターフェースに制限されています。管理、LAN、WAN（この順序で）。
   > - SD-WAN VPX で使用できる Azure クラウドテンプレートは、現在、WAN に 10.9.4.106 IP、LAN に 10.9.3.106 IP、管理アドレスに 10.9.0.16 IP を取得するようにハードセットされています。ゼ

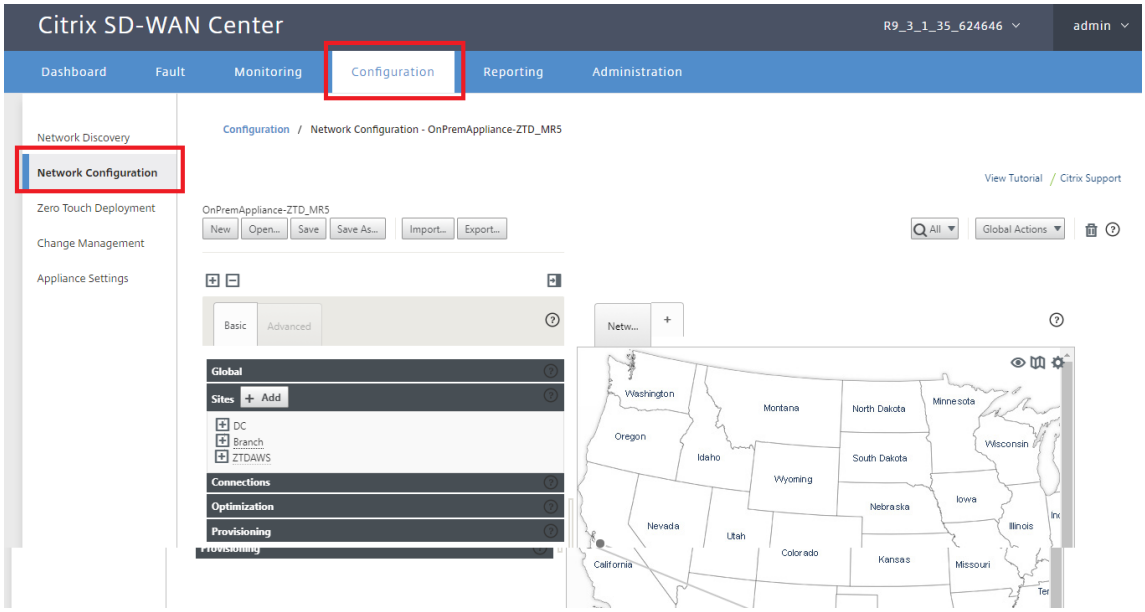
> ロタッチの対象となる Azure ノードの SD-WAN 構成は、このレイアウトと一致する必要があります。
>
> - 構成内の Azure サイト名は、特殊文字を含まないすべて小文字にする必要があります（ztdazure など）。

Azure Cloud Topology with NetScaler SD-WAN



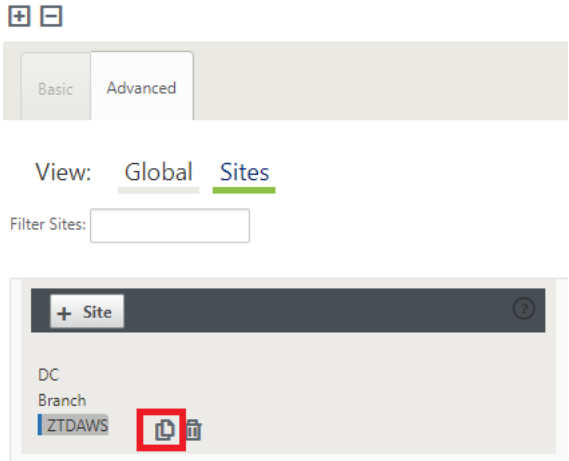
これは、SD-WAN クラウド展開サイトの展開例です。Citrix SD-WAN デバイスは、このクラウドネットワーク内の単一のインターネット WAN リンクサービスを提供するエッジデバイスとして展開されます。リモートサイトは、クラウド用のこの同じ Internet Gateway に接続する複数の異なるインターネット WAN リンクを活用して、任意の SD-WAN 展開サイトからクラウドインフラストラクチャへの耐障害性と集約帯域幅接続を提供します。これにより、費用対効果が高く、信頼性の高いクラウドへの接続が可能になります。

2. SD-WAN Center Web 管理インターフェイスを開き、[設定] **> [**** ネットワーク設定 **] ページに移動します。



3. 動作中の構成がすでに配置されていることを確認するか、MCN から構成をインポートします。
4. [基本] タブに移動して、新しいサイトを作成します。

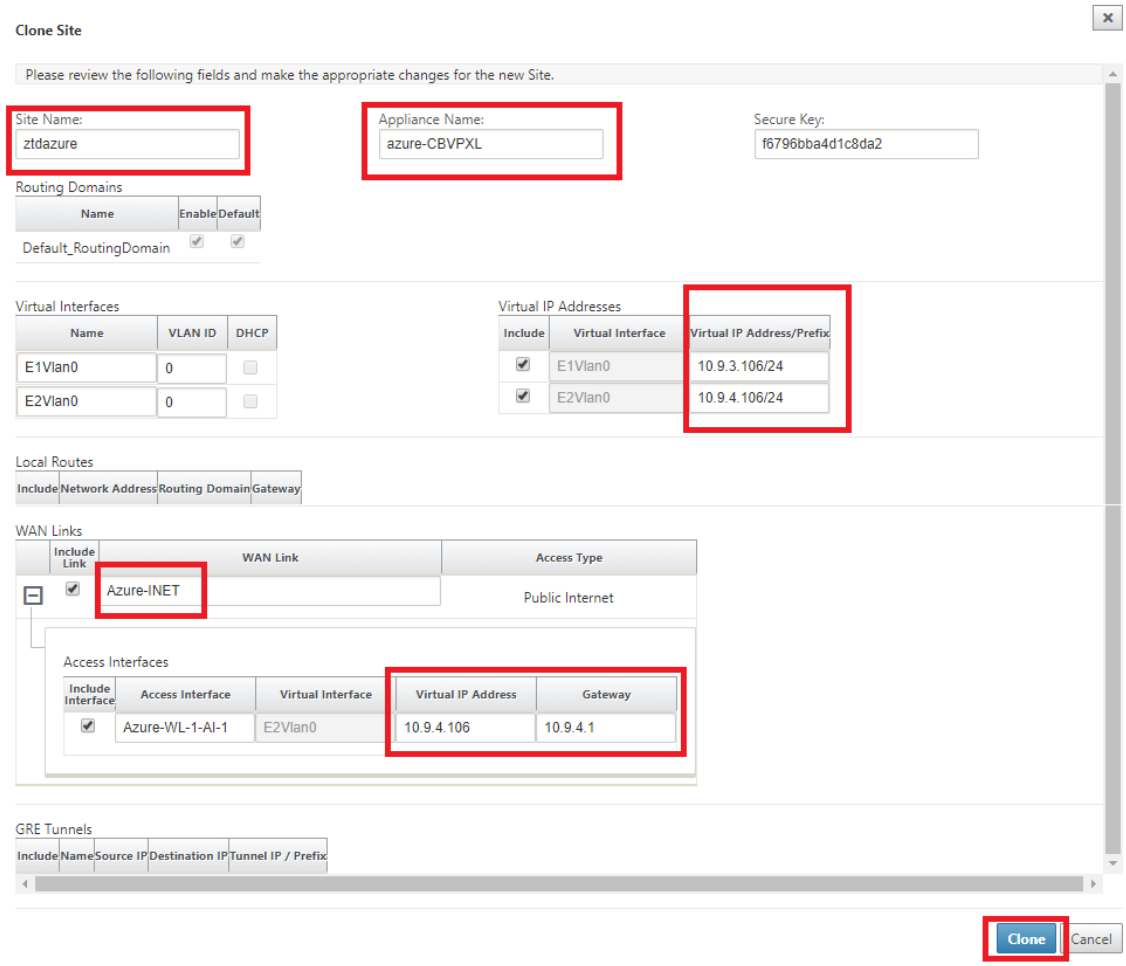
5. [サイト] タイルを開いて、現在構成されているサイトを表示します。
6. 既存のサイトのクローン機能を利用して新しいクラウドサイトの構成をすばやく構築するか、新しいサイトを手動で構築します。



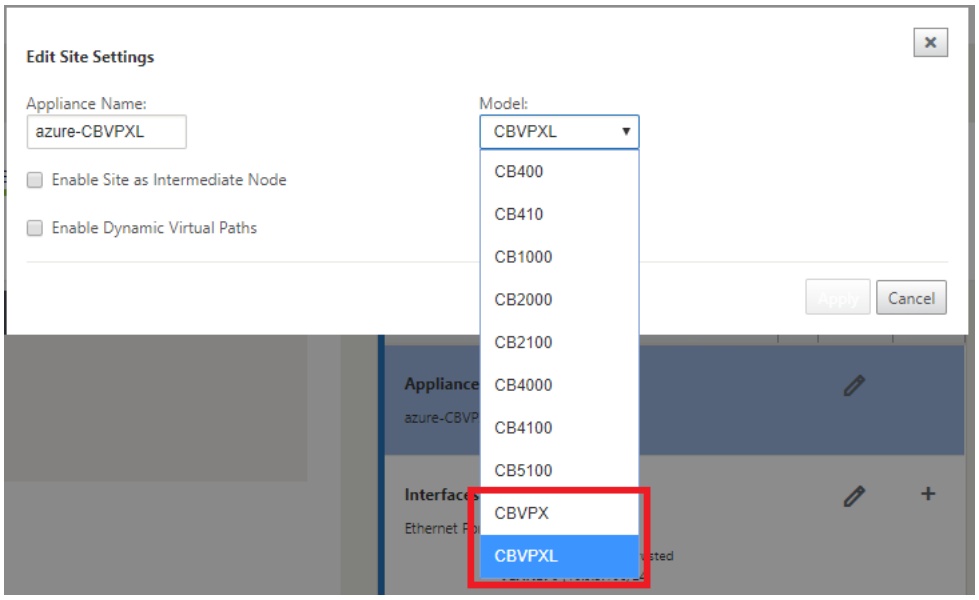
7. この新しいクラウドサイト用に以前に設計されたトポロジのすべての必須フィールドに入力します。

   Azure クラウド ZTD デプロイメントに使用できるテンプレートは現在、WAN に 10.9.4.106 IP、LAN に 10.9.3.106 IP、管理アドレスに 10.9.0.16 IP を取得するようにハードセットされていることに注意してください。各インターフェイスの予想される VIP アドレスと一致するように設定されていない場合、デバイスはクラウド環境ゲートウェイへの ARP と MCN の仮想パスへの IP 接続を適切に確立できません。

   サイト名が Azure が期待するものに準拠していることが重要です。サイト名は、特殊文字を使用せず、すべての小文字、少なくとも 6 文字でなければなりません。次の正規表現 **^ [a-z] [a-z0-9-] {1,61} [a-z0-9] $** を確認する必要があります。

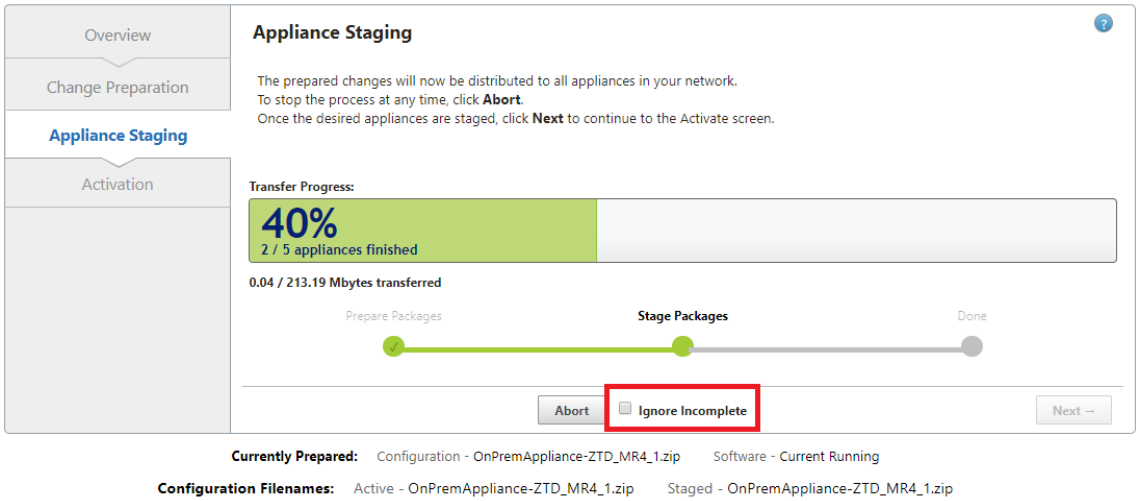


8. 新しいサイトのクローンを作成したら、サイトの [基本設定] に移動し、ゼロタッチサービスをサポートする SD-WAN のモデルが正しく選択されていることを確認します。



9. 新しい構成を SD-WAN Center に保存し、変更管理受信トレイへのエクスポートオプションを使用して、変更管理 を使用して構成をプッシュします。

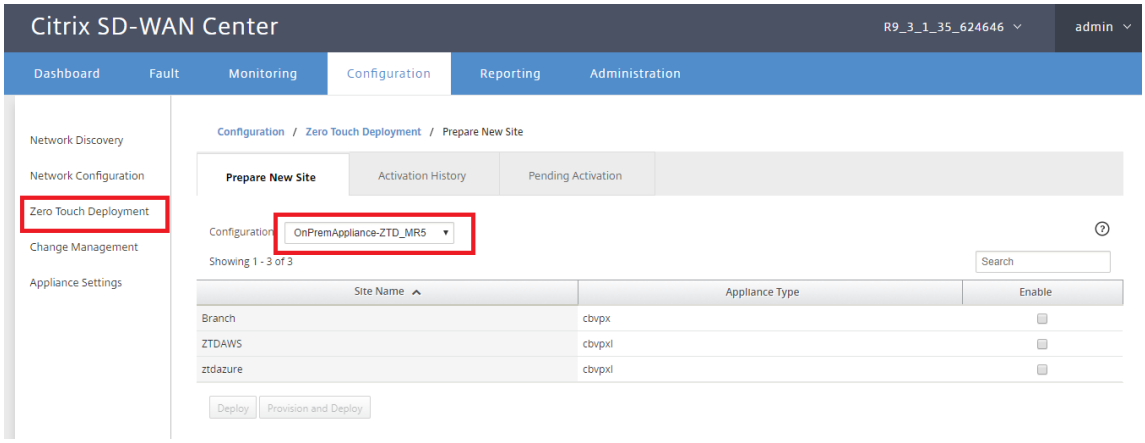
10. 変更管理手順に従って新しい構成を適切にステージングします。これにより、既存の SD-WAN デバイスが、ゼロタッチで展開される新しいサイトを認識します。[*Ignore In* freted] オプションを使用して、新しいサイトに構成をプッシュしないようにする必要があります。は引き続き ZTD ワークフローを通過する必要があります。



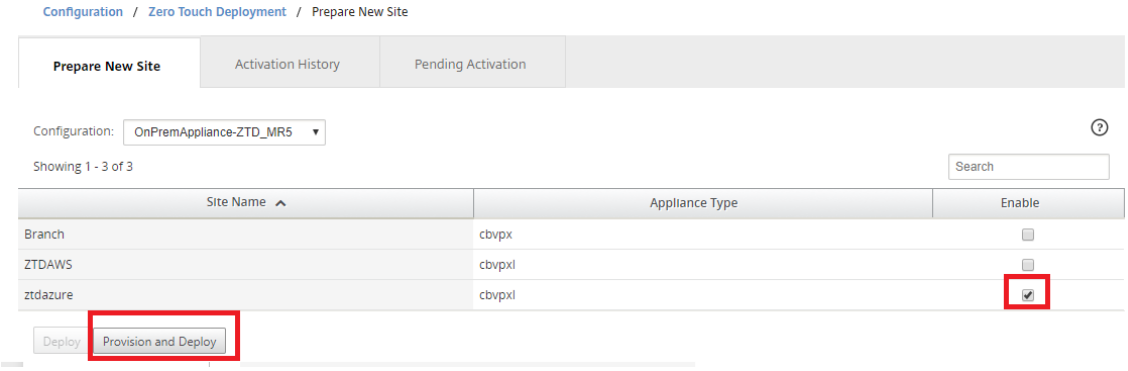
SD-WAN Center の **[**ゼロタッチデプロイ**]** ページに移動し、新しいアクティブな構成が実行されている状態で、新しいサイトを **SD-WAN Center** のプロビジョニングとデプロイ **Azure** で使用できるようになります **(**ステップ **1/2)**

1. Zero Touch Deployment ページで、Citrix アカウントの認証情報を使用してログインします。[新しいサイトの展開] タブで、実行中のネットワーク構成ファイルを選択します。

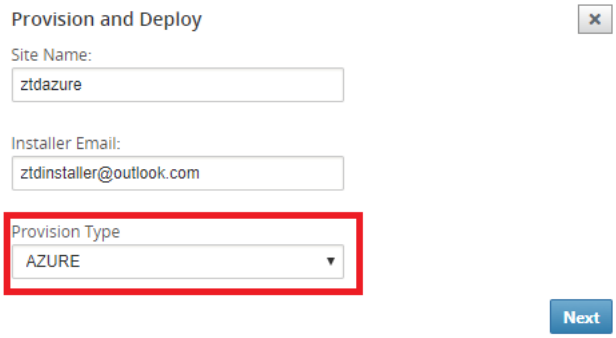
2. 実行構成ファイルを選択すると、ZTD 対応の Citrix SD-WAN デバイスを持つすべてのブランチサイトのリストが表示されます。



3. Zero Touch サービスを使用してデプロイするターゲットクラウドサイトを選択し、[有効にする]、[プロビジョニングとデプロイ] の順にクリックします。

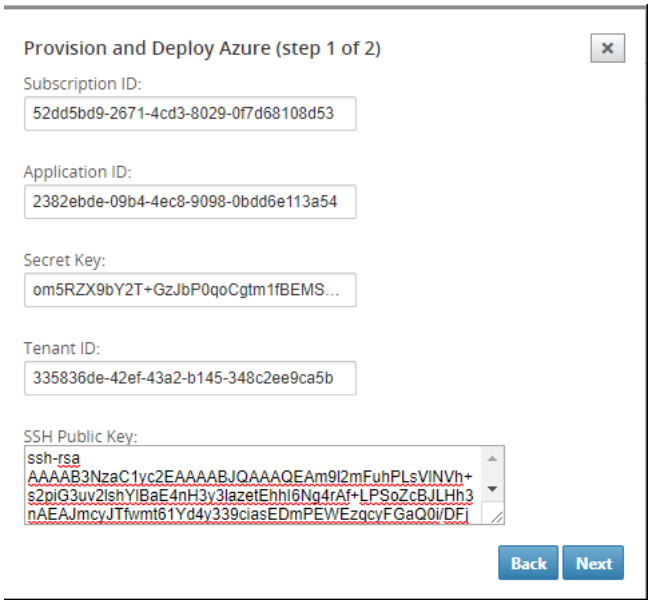


4. ポップアップウィンドウが表示され、Citrix SD-WAN 管理者がゼロタッチの展開を開始できます。サイト名が Azure の要件 (特殊文字のない小文字) に準拠していることを確認します。ライセンス認証 URL を配信できる電子メールアドレスを入力し、目的のクラウドの [プロビジョニングの種類] として [Azure] を選択し、[次へ] をクリックします。

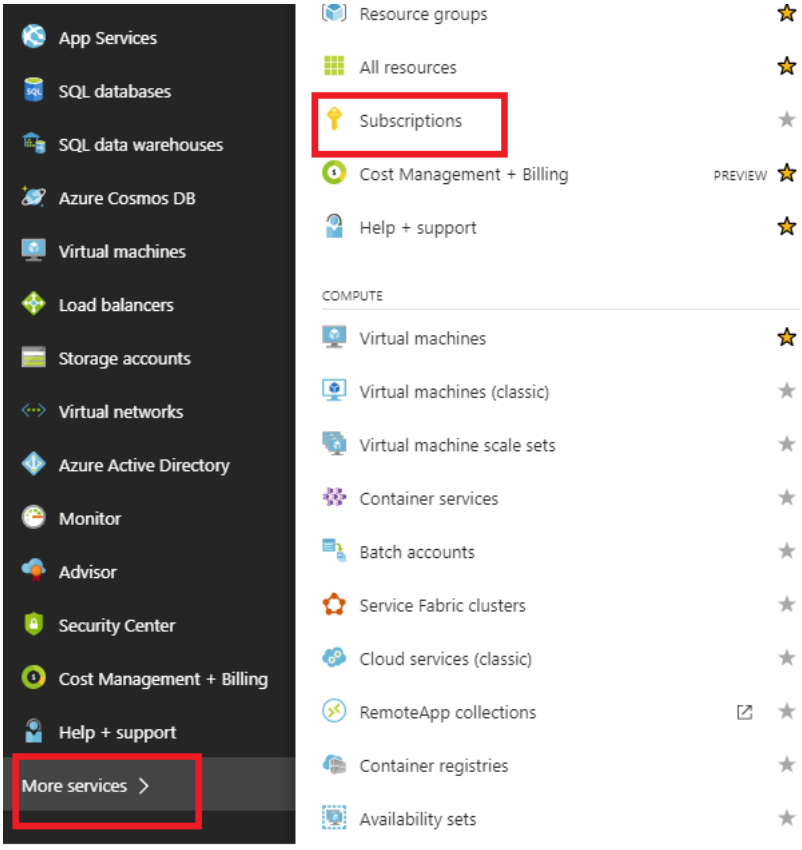


5. [次へ] をクリックすると、Azure のプロビジョニングとデプロイ (ステップ 1/2) ウィンドウには、Azure アカウントから取得したの入力が必要になります。

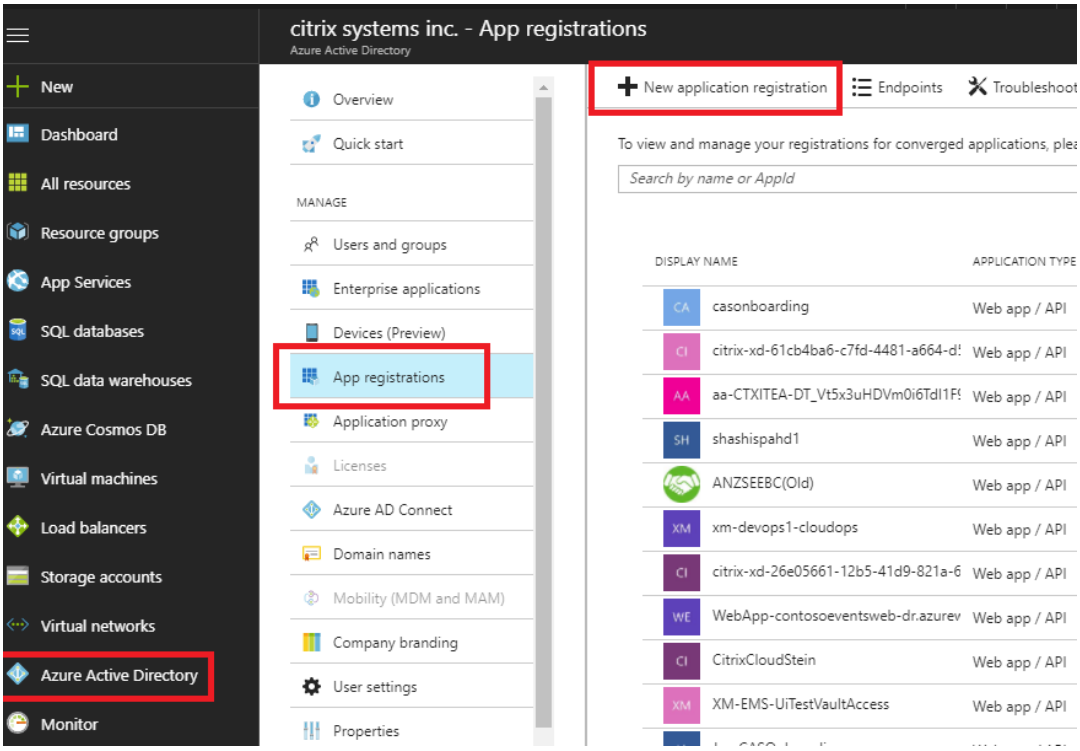
   Azure アカウントから情報を取得したら、各必須フィールドをコピーして貼り付けます。以下の手順では、Azure アカウントから必要なサブスクリプション ID、アプリケーション ID、秘密キー、およびテナント ID を取得し、[次へ] をクリックして続行する方法の概要を説明します。



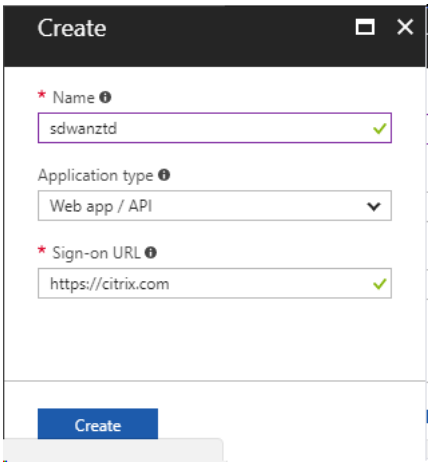
a) Azure アカウントで、[その他のサービス] に移動し、[サブスクリプション] を選択することで、必要なサブスクリプション **ID** を特定できます。



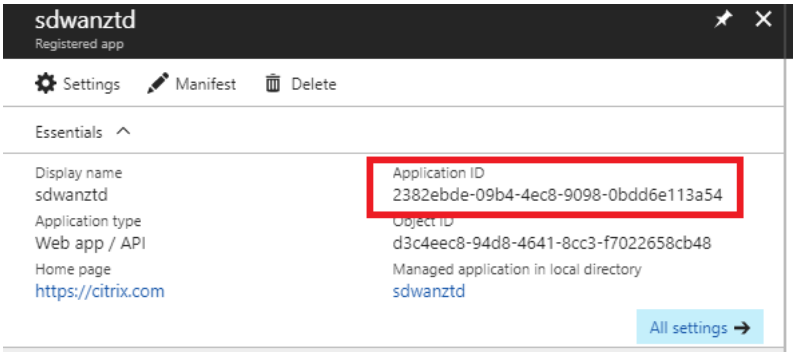
b) 必要な * アプリケーション **ID** を特定するには、Azure Active Directory、アプリケーションの登録に移動し、[新しいアプリケーション登録] をクリックします。



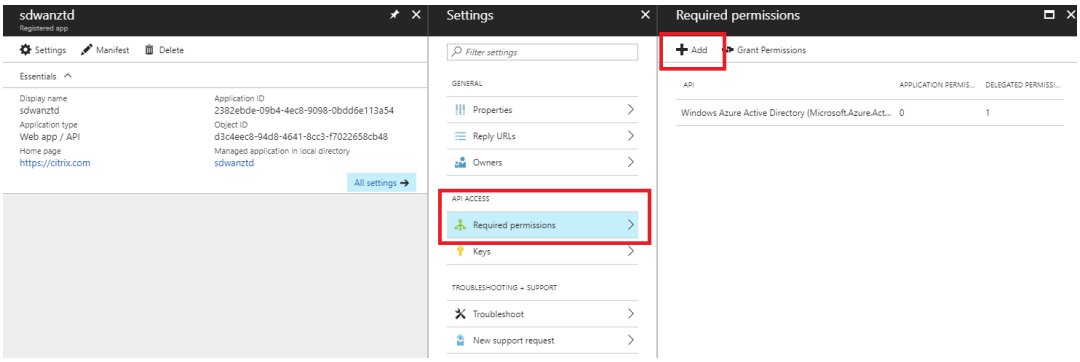
c) アプリ登録の作成メニューで、[名前] と [サインオン URL] (任意の URL でもかまいません。唯一の要件は、有効であることが必要です) を入力し、[作成] をクリックします。



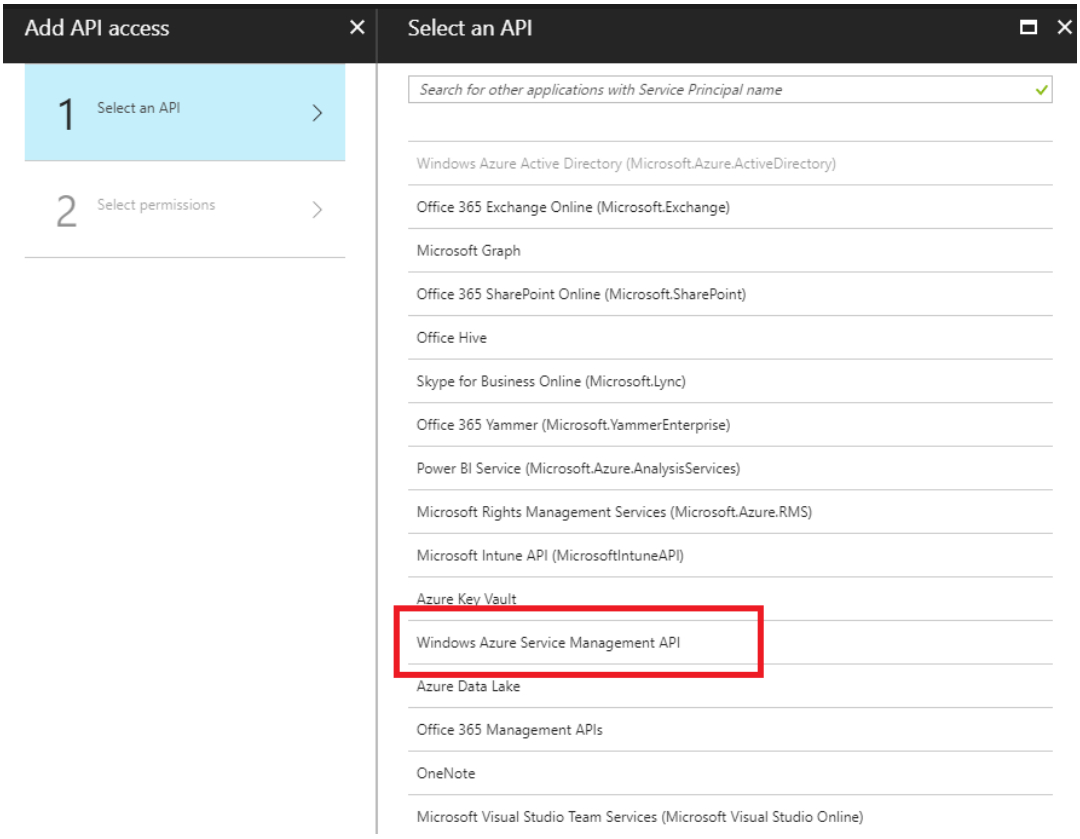
d) 新しく作成された登録済みアプリを検索して開き、アプリケーション ID をメモします。



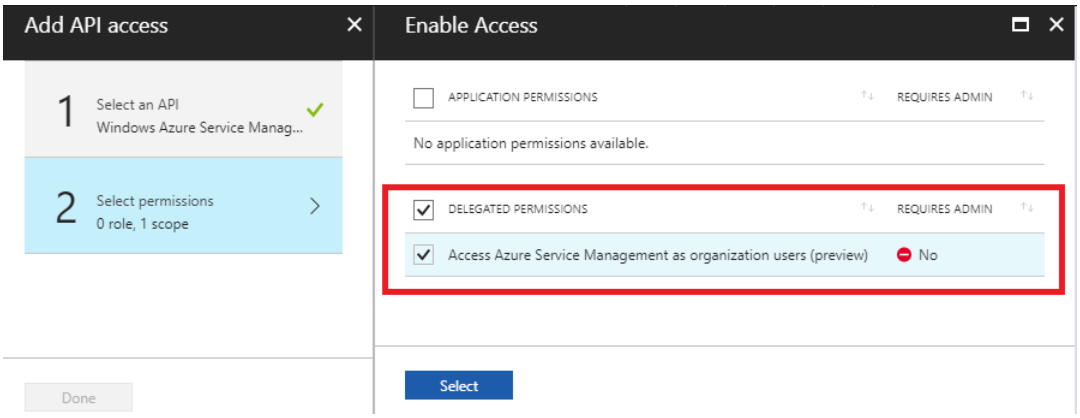
e) 新しく作成した登録アプリを再度開き、必要な セキュリティキーを特定するには、[API アクセス] で [必要なアクセス許可] を選択し、サードパーティがプロビジョニングとインスタンスを許可します。次に、[追加] を選択します。



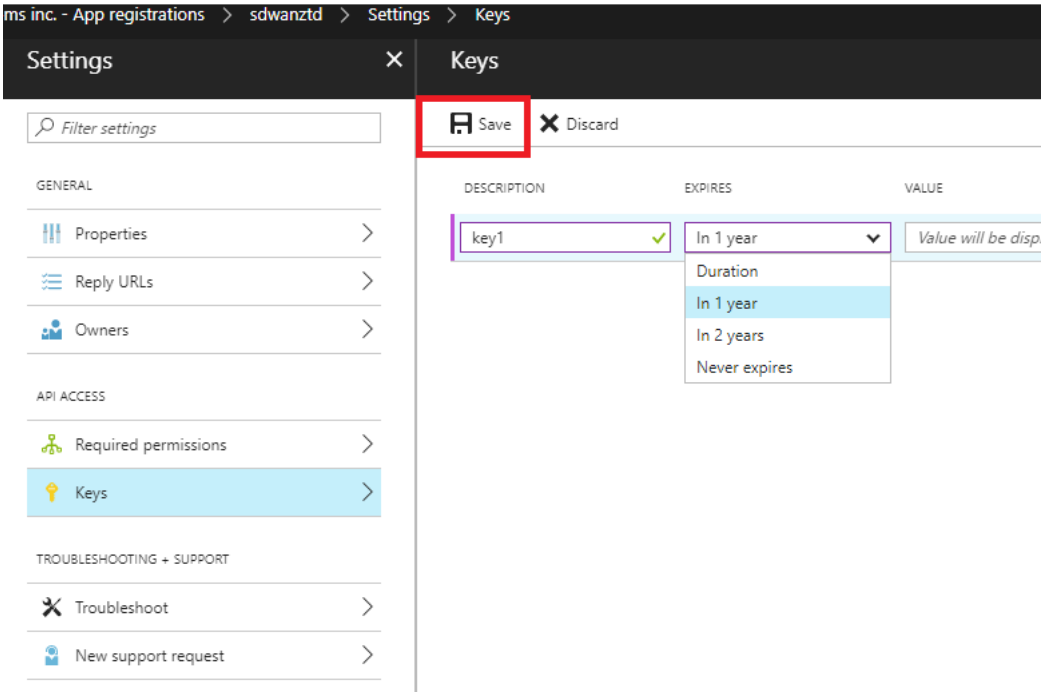
f) 必要なアクセス許可を追加する場合は、**[API** を選択**]** を選択し、 [**Windows Azure** サービス管理 **API]** を強調表示します。



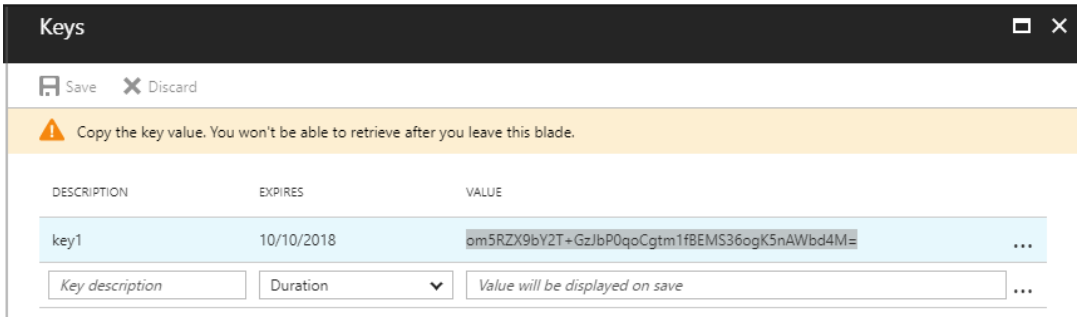
g) 代理アクセス権限 を有効にしてインスタンスをプロビジョニングし、[**Select** and **Done**] をクリックします。



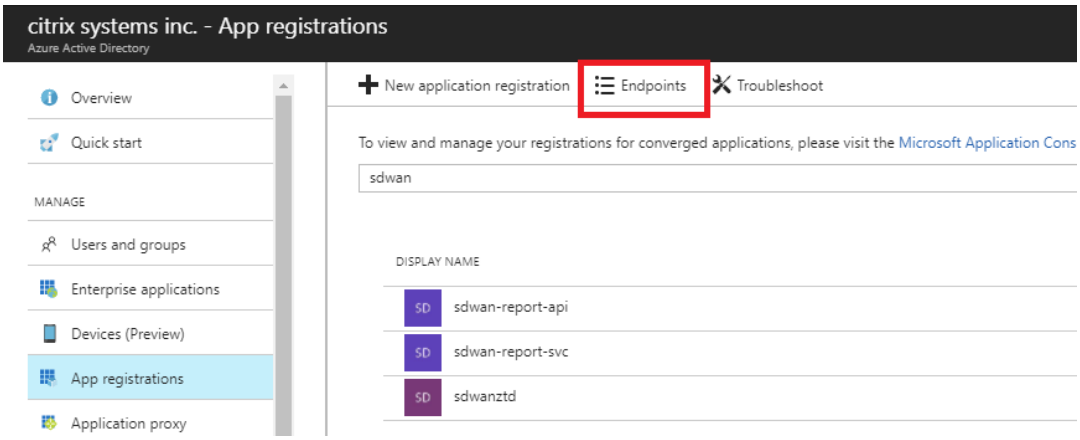
h) この登録済みアプリの場合、[API アクセス] で [キー**]** を選択し、秘密キーの説明とキーが有効になるまでの所要時間を作成します。次に、[**Save**] をクリックすると、シークレットキー が生成されます（キーは Provisioning プロセスでのみ必要であり、インスタンスが利用可能になった後に削除できます）。



i) 秘密鍵をコピーして保存します（後でこれを取得することはできません）。

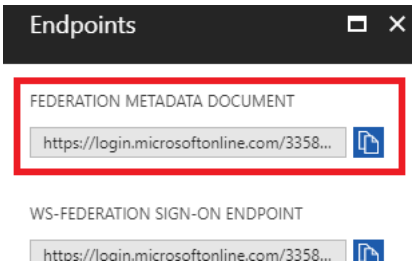


j) 必要な テナント ***ID*** を特定するには、[アプリ登録] ペインに戻り、[エンドポイント] を選択します。

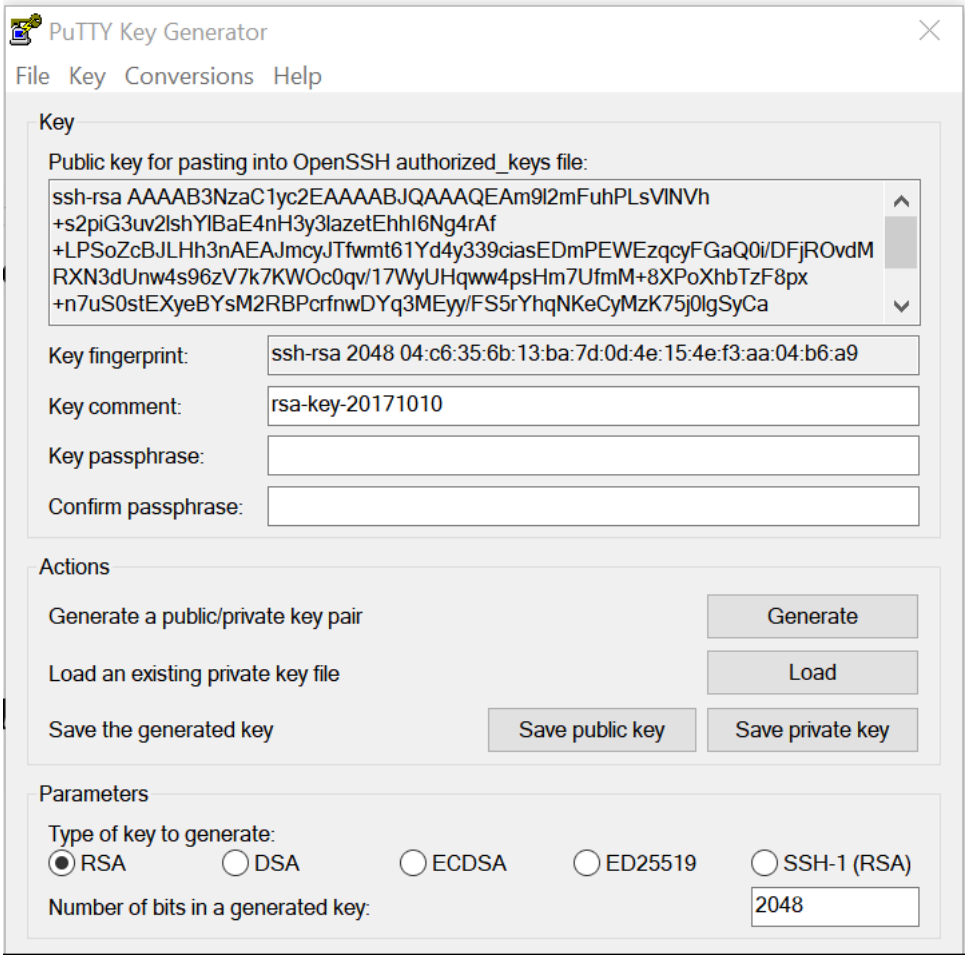


k) テナント ID を識別するために、フェデレーションメタデータドキュメントをコピーします (テナント ID は URL 内の`online.com/`と`/federation`の間にある 36 文字の文字列であることに注意して

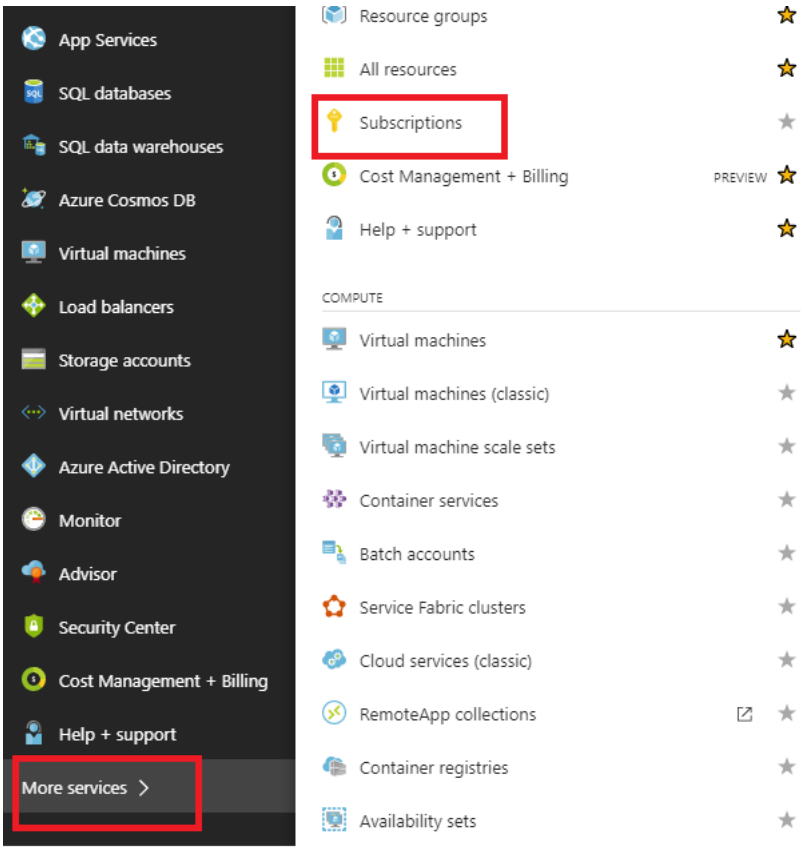
ください)。



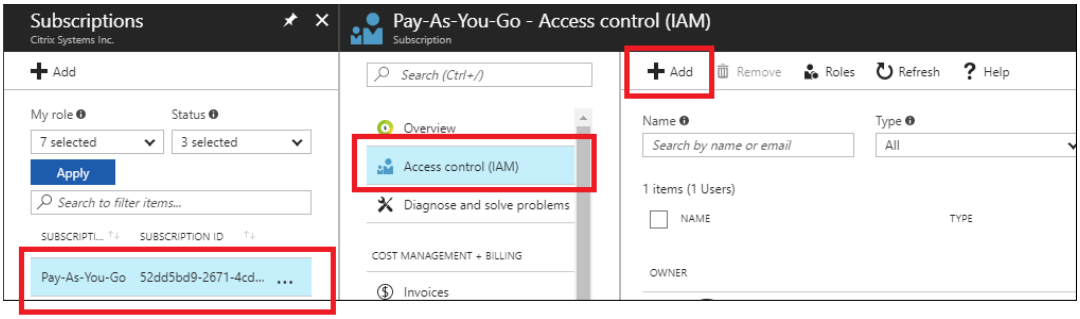
l) 最後に必要な項目は ***SSH*** 公開鍵です。これは、パテキージェネレータまたは ssh-keygen を使用して作成することができ、認証に利用されるため、パスワードがログインする必要はありません。SSH 公開鍵はコピーできます（見出しの ssh-rsa と末尾の rsa-key 文字列を含む）。この公開鍵は、Citrix ゼロタッチ展開サービスへの SD-WAN Center 入力を通じて共有されます。



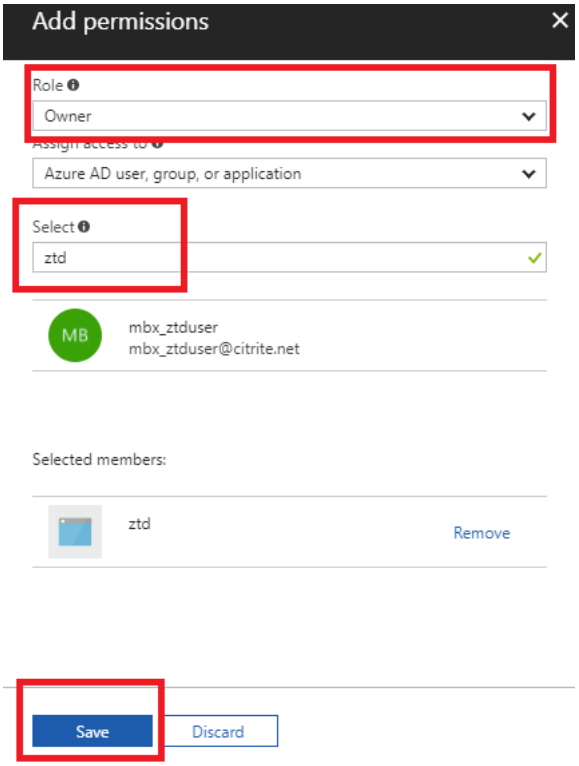
m) アプリケーションにロールを割り当てるには、追加の手順が必要です。「その他のサービス」、「サブスクリプション」に戻ります。



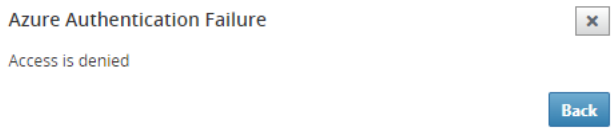
n) アクティブなサブスクリプションを選択し、アクセス制御 **(AIM)** を選択し、次に [追加] をクリックします。



o) [アクセス許可の追加] ペインで、[所有者の ロール] を選択し、**Azure AD** ユーザー、グループ、またはアプリケーションへのアクセス権を割り当て、**[選択]** フィールド で登録済みアプリを検索して、Zero Touch Deployment Cloud Service が Azure でインスタンスを作成および構成できるようにします。サブスクリプション。アプリを特定したら、[保存] をクリックする前に、アプリを選択し、[選択済み] メンバーとして入力されていることを確認します。

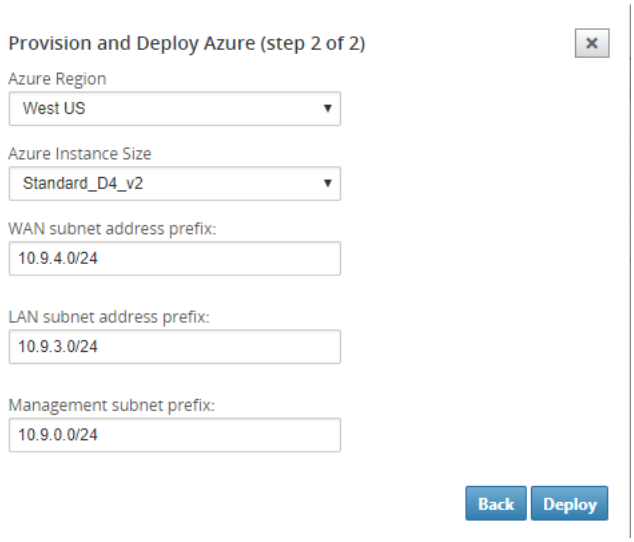


p) 必要な入力を収集し、SD-WAN Center に入力したら、[**Next**] をクリックします。入力が正しくない場合は、認証に失敗します。

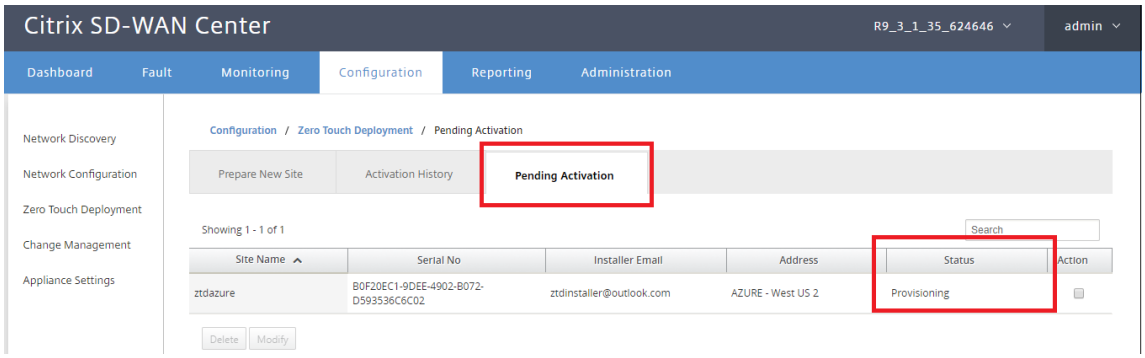


SD-WAN Center の **Azure** のプロビジョニングとデプロイ **(**ステップ **2/2)**

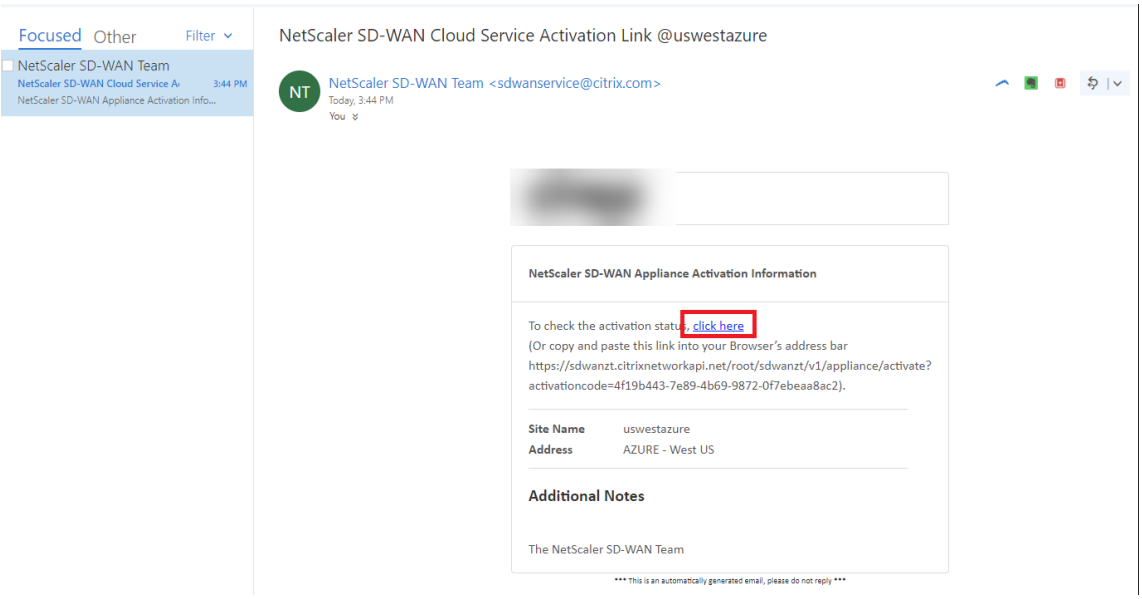
1. Azure 認証が成功したら、適切なフィールドに入力して目的の Azure リージョンと適切なインスタンスサイズを選択し、[デプロイ] をクリックします。



2. SD-WAN Center の [アクティブ化を保留中] タブに移動すると、展開の現在のステータスを追跡できます。

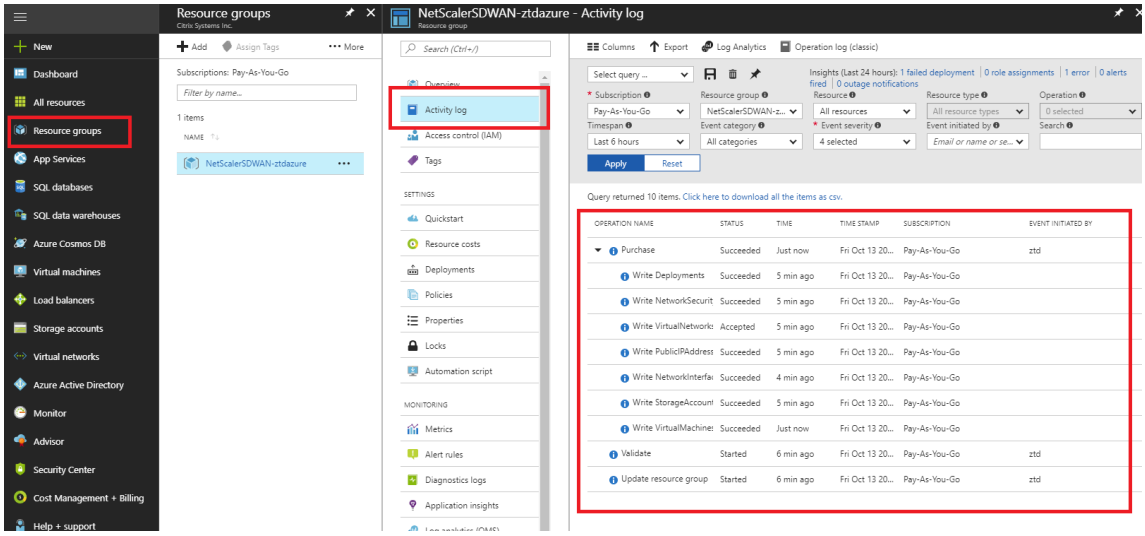


3. 手順 1 で入力したメールアドレスにアクティベーションコードが記載された電子メールが配信され、電子メールを入手して アクティベーション **URL** を開いてプロセスをトリガーし、アクティベーションステータスを確認します。

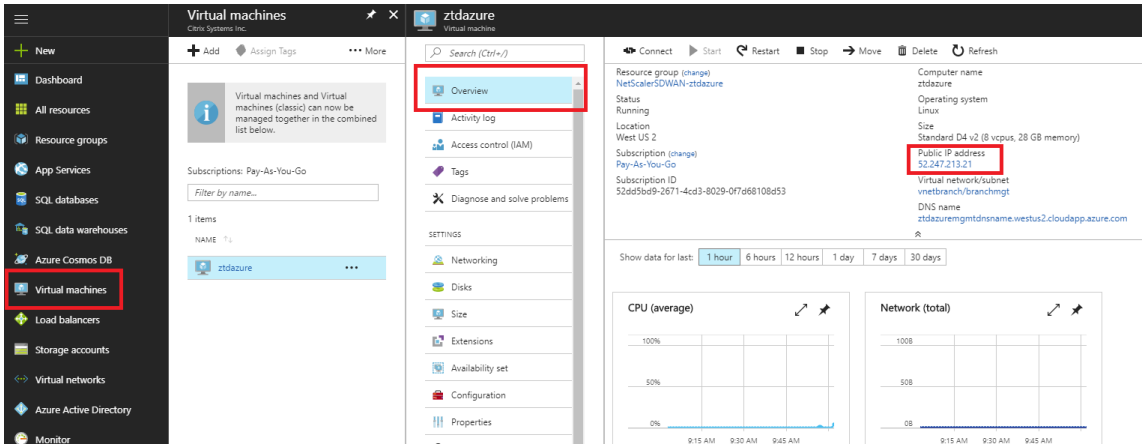


4. 手順 1 で入力したメールアドレスにアクティベーション URL が記載されたメールが届きます。電子メールを入手し、アクティベーション **URL** を開いてプロセスをトリガーし、アクティベーションステータスを確認します。

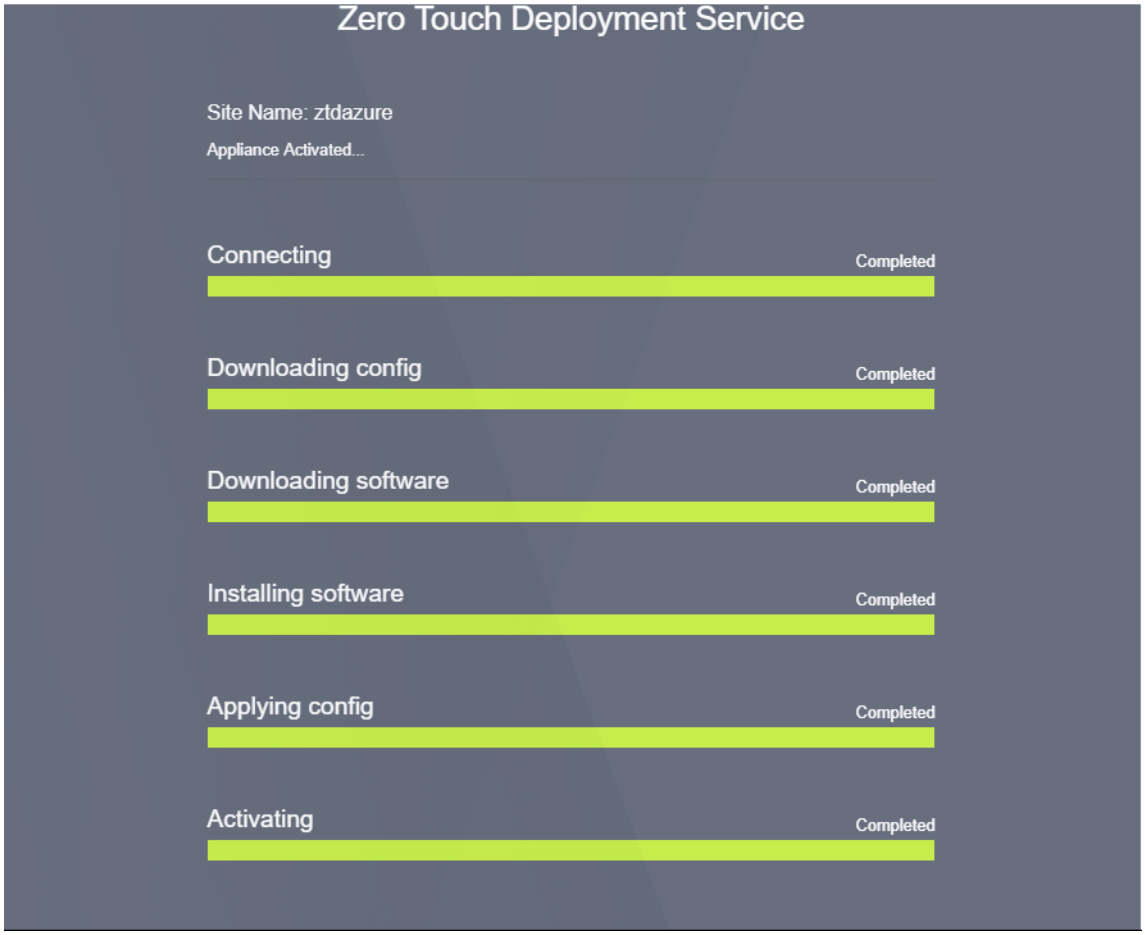
5. SD-WAN クラウドサービスによってインスタンスがプロビジョニングされるまで数分かかります。自動的に作成される リソースグループのアクティビティログ の下で、Azure Portal でアクティビティを監視できます。Provisioning に関する問題やエラーはすべてここに入力され、アクティブ化ステータスで SD-WAN センターにレプリケートされます。



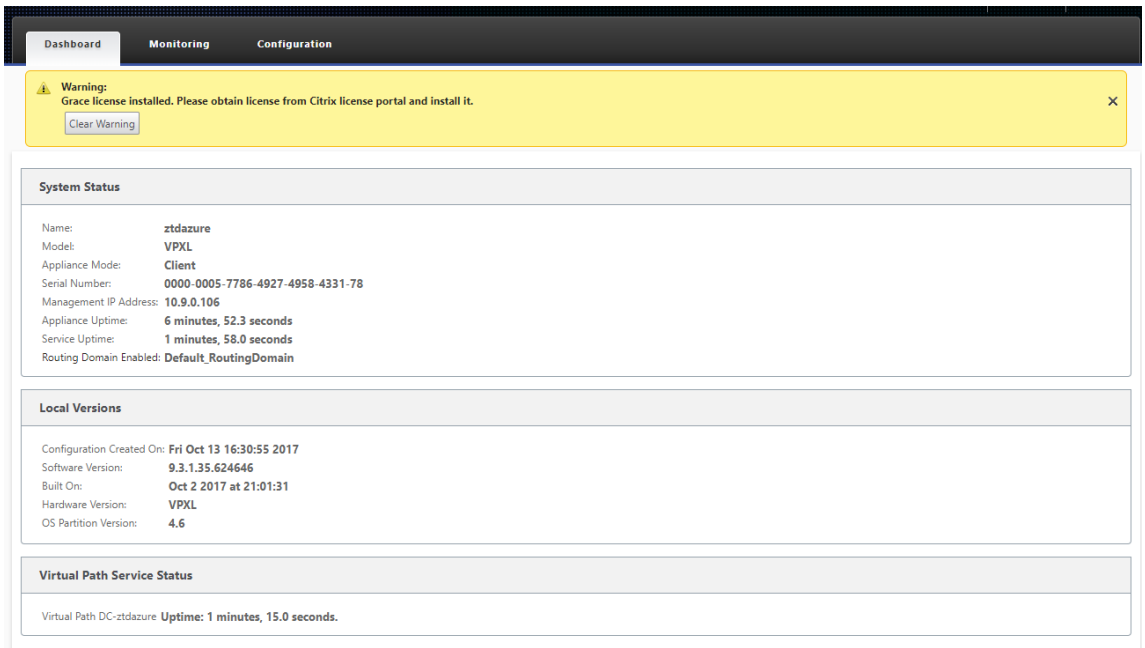
6. Azure Portal では、正常に起動されたインスタンスは [仮想マシン] の下で使用できます。割り当てられたパブリック IP を取得するには、インスタンスの [概要] に移動します。



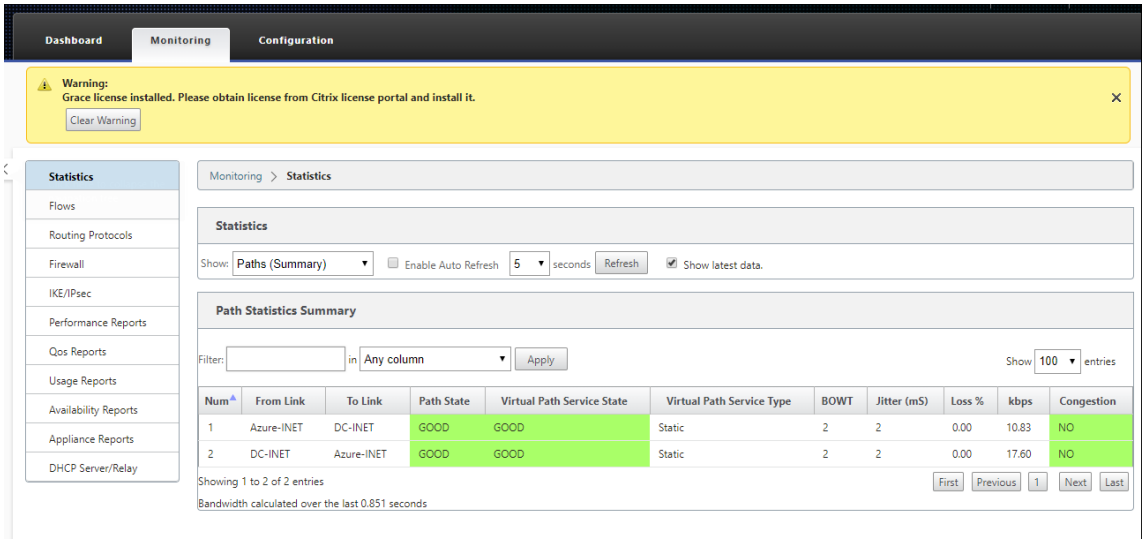
7. VM が実行状態になった後、サービスが到達し、構成、ソフトウェア、およびライセンスのダウンロードプロセスを開始するまでに 1 分かかります。



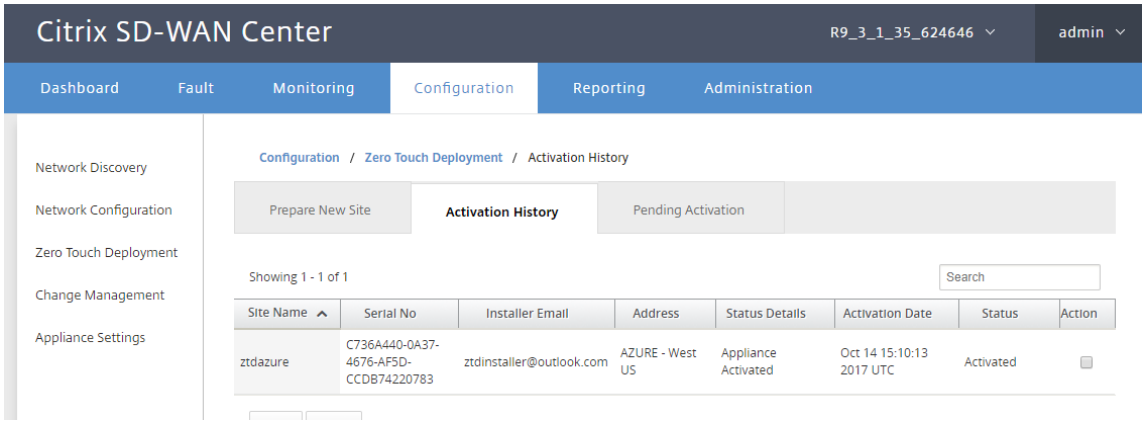
8. SD-WAN クラウドサービスの各手順が自動的に複雑になった後、Azure ポータルから取得したパブリック IP を使用して SD-WAN インスタンスの Web インターフェイスにログインします。



9. [Citrix SD-WAN 監視統計情報] ページでは、MCN から Azure の SD-WAN インスタンスへの正常な接続が識別されます。



10. さらに、Provisioning の成功（または失敗）は、SD-WAN Center の [アクティベーション履歴] ページに記録されます。



単一リージョンの展開

May 10, 2021

リージョンを使用すると、分散管理を使用してネットワーク階層を定義できます。リージョンは、そのリージョンのネットワーク制御ノード（MCN）によって実行される機能を引き継ぐリージョナル制御ノード（RCN）を定義する必要があります。MCN は、デフォルトリージョンの Controller です。

静的仮想パスと動的仮想パスは、リージョン間で許可されません。RCN は、リージョン間のトラフィックを管理します。

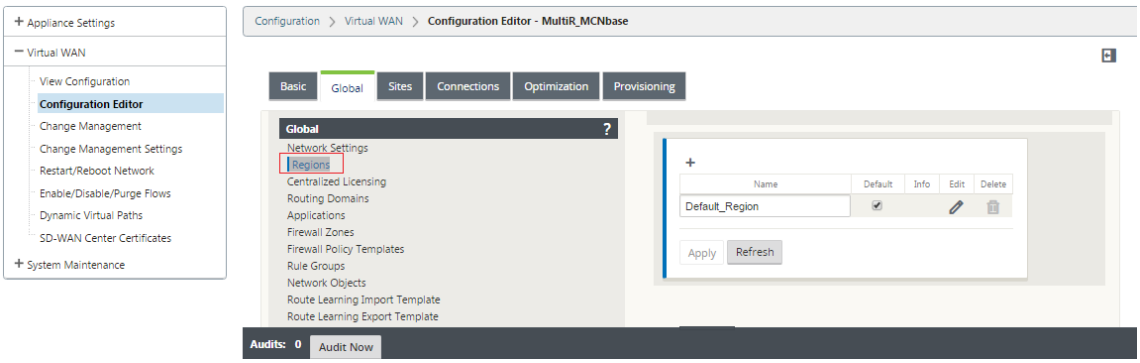
SD-WAN ネットワークでの単一リージョン展開では、550 未満のネットワークサイトをサポートできます。

SD-WAN アプライアンスの GUI の構成エディタでデフォルトの領域を構成できます。基本エディタは、MCN ノードとクライアント SD-WAN ノードを持つ小規模なネットワークだけを作成するのに便利です。MCN、RCN、クライアント、または高度な機能を使用してマルチリージョンネットワークを構成するには、構成エディタで他の構成オプションを使用します。

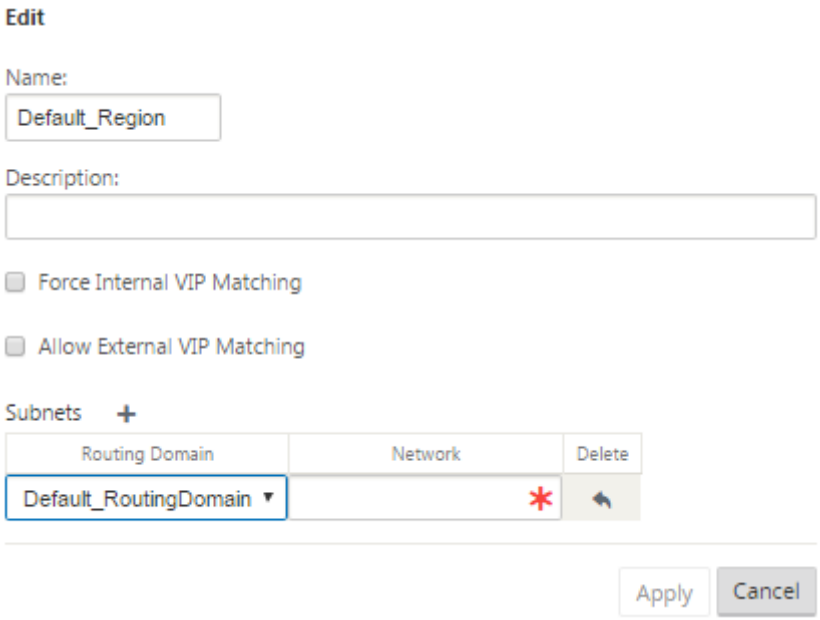
単一リージョン展開を構成するには、次の手順に従います。

1. 構成エディタの「グローバル」タブに移動します。[リージョン] を選択します。デフォルトのリージョン設定オプションが表示されます。

   デフォルトのリージョンの名前と説明は、編集することで変更できます。



2. **Default_Region** を編集して、名前を変更し、サブネットを設定します。
3. [強制内部 **VIP** マッチング] または **[**外部 **VIP** マッチングを許可**]** のどちらを使用するかに基づいて、インターバル **VIP** マッチングを有効にします。
   - 強制内部 VIP：有効にすると、リージョン内のすべての非プライベート仮想 IP アドレスが、設定されたサブネットと一致するように強制されます。
   - 許可された外部 VIP-有効にすると、他のリージョンからの非プライベート仮想 IP アドレスが、設定されたサブネットと一致することを許可されます。
4. サブネットを追加するには、[+] をクリックします。



5. ルーティングドメインを選択し、ネットワーク アドレスを入力します。［適用］をクリックします。ネットワークアドレスは、サブネットの IP アドレスとマスクです。

マルチリージョンの展開

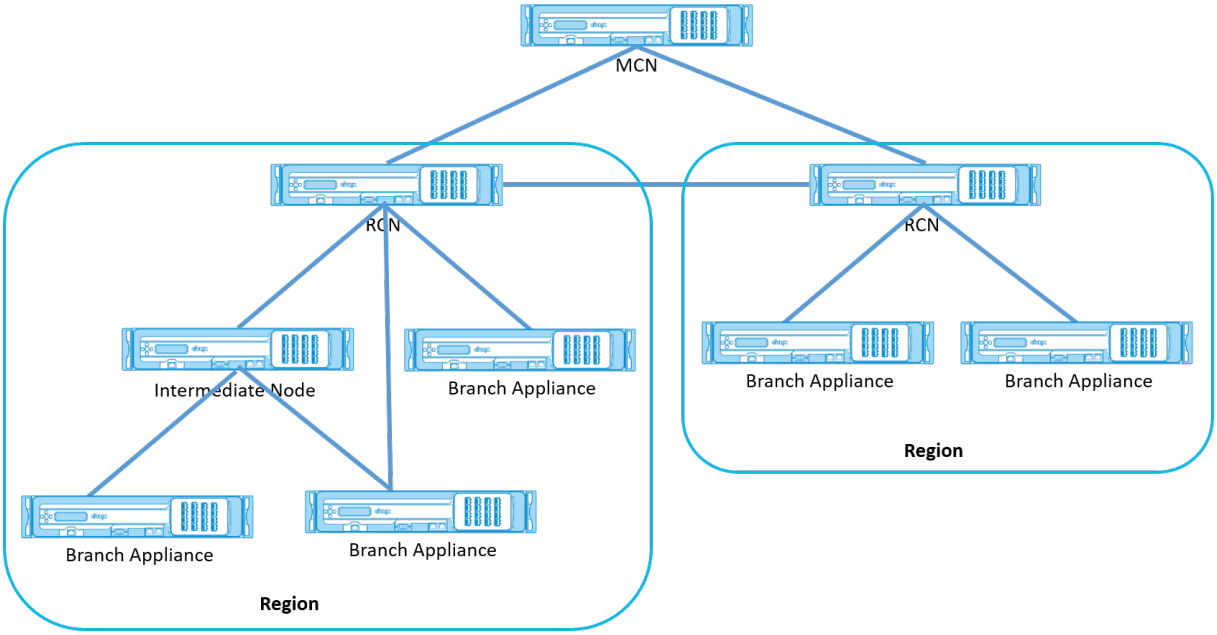
May 10, 2021

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

MCN をネットワークの制御ノードとし、RCN をリージョンの制御ノードとして使用すると、SD-WAN は最大 6000 のサイトを管理できます。

マルチリージョン展開では、ネットワークをリージョンにフラグメント化し、ブランチ (クライアント) > RCN > MCN などの階層型ネットワークを設定できます。

1 つのリージョンを持つ MCN は、最大 550 のサイトで構成できます。既存のサイトを既定のリージョンに保持し、RCN とそのサイトを持つ新しいリージョンを複数リージョン展開に追加できます。



次の表に、プライマリおよびセカンダリ MCN/RCN の設定でサポートされているプラットフォームの一覧を示します。

> メモ
>
> - Premium Edition (PE) アプライアンスは、以前はエンタープライズエディション (EE) と呼ばれていました。
> - Citrix SD-WAN 210 SE アプライアンスは、SD-WAN Orchestrator が管理するネットワークでのみ MCN として使用します。

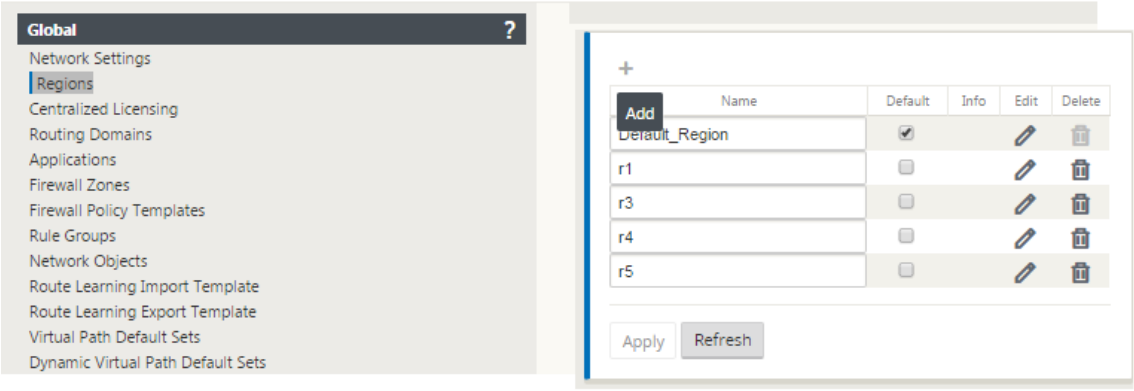
プラットフォーム・エディション	プライマリ/セカンダリ MCN	プライマリ/セカンダリ RCN
210-SE	はい	はい
400-SE	はい	いいえ
410-SE	はい	いいえ
1000-SE, 1000-PE	はい	いいえ
1100-SE, 1100-PE	はい	はい
VPX-SE、VPXL-SE	はい	はい
2000-SE, 2100-SE, 2000-PE, 2100-PE, 4000-SE, 4100-SE, 5100-SE, 5100-PE, 6100-SE	はい	はい

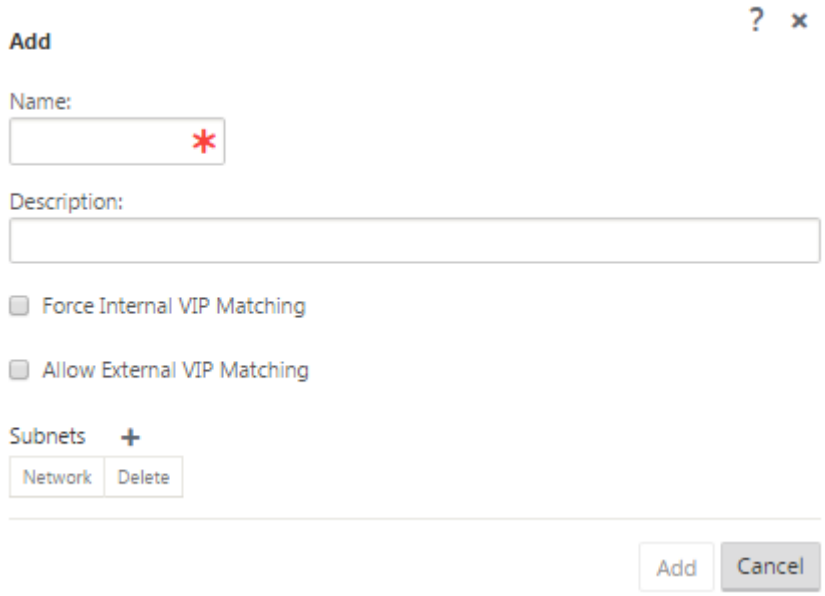
SD-WAN ネットワークのマルチリージョン配置を設定するには、次の手順を実行します。

1. 構成エディタの「グローバル」タブに移動します。[リージョン] を選択します。デフォルトのリージョン設定オプションが表示されます。

   デフォルトのリージョンの名前と説明は、編集することで変更できます。

2. [**+** 追加] をクリックして、新しいリージョンを追加します。



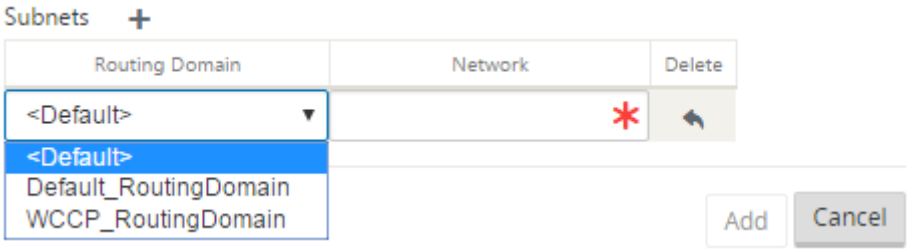


3. リージョンの「名称」および「摘要」を入力します。

4. [強制内部 **VIP** マッチング] または **[**外部 **VIP** マッチングを許可**]** のどちらを使用するかに基づいて、内部 **VIP** マッチングを有効にします。

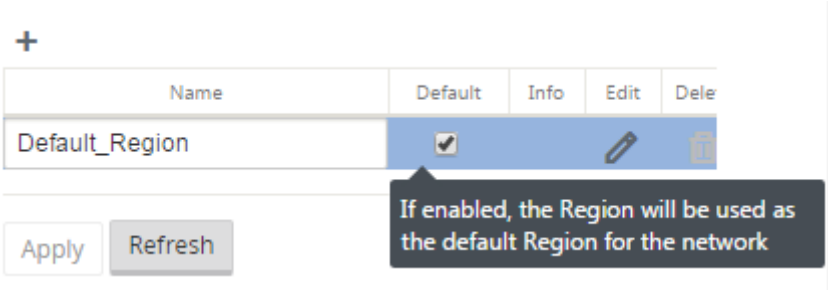
   - 強制内部 VIP：有効にすると、リージョン内のすべての非プライベート仮想 IP アドレスが、設定されたサブネットと一致するように強制されます。
   - 許可された外部 VIP-有効にすると、他のリージョンからの非プライベート仮想 IP アドレスが、設定されたサブネットと一致することを許可されます。

5. サブネットを追加するには、[+] をクリックします。ルーティングドメインを選択します。



6. ネットワーク アドレスを入力します。[追加] をクリックします。ネットワークアドレスは、サブネットの IP アドレスとマスクです。新しく作成されたリージョンが、既存のリージョンのリストに追加されます。

「デフォルト」(**Default**) チェックボックスを選択すると、目的の領域をデフォルトとして使用できます。



> 注
>
> MCN を GEO サイトまたはクライアントサイトにクローンすることができます。

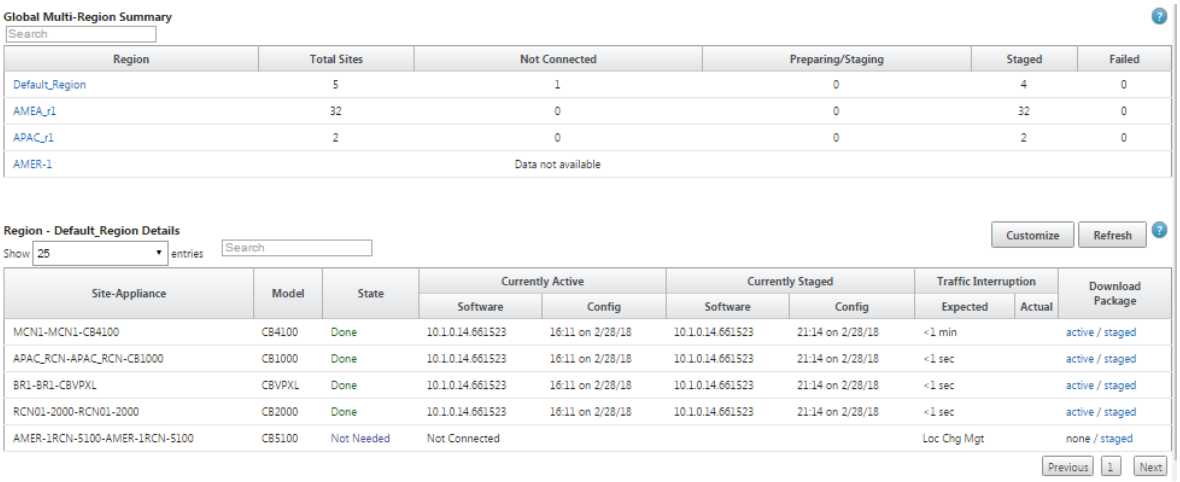
SD-WAN Center では、マルチリージョンの展開がサポートされています。詳しくは、「SD-WAN Center マルチリージョンの導入とレポート作成」を参照してください。

変更管理の概要ビュー

マルチリージョン展開で構成されたアプライアンスの変更管理プロセスを実行すると、SD-WAN アプライアンスの GUI に変更管理の概要テーブルが表示されます。

[リージョン] 列には、ネットワークで現在設定されているリージョンのリストが表示されます。特定のリージョンの変更管理サマリーは、サマリーテーブルで選択することで表示できます。

デフォルトのリージョンの概要:



Global Multi-Region Summary

Search

Region	Total Sites	Not Connected	Preparing/Staging	Staged	Failed
Default_Region	5	1	0	4	0
AMEA_r1	32	0	0	32	0
APAC_r1	2	0	0	2	0
AMER-1	Data not available				

Region - Default_Region Details

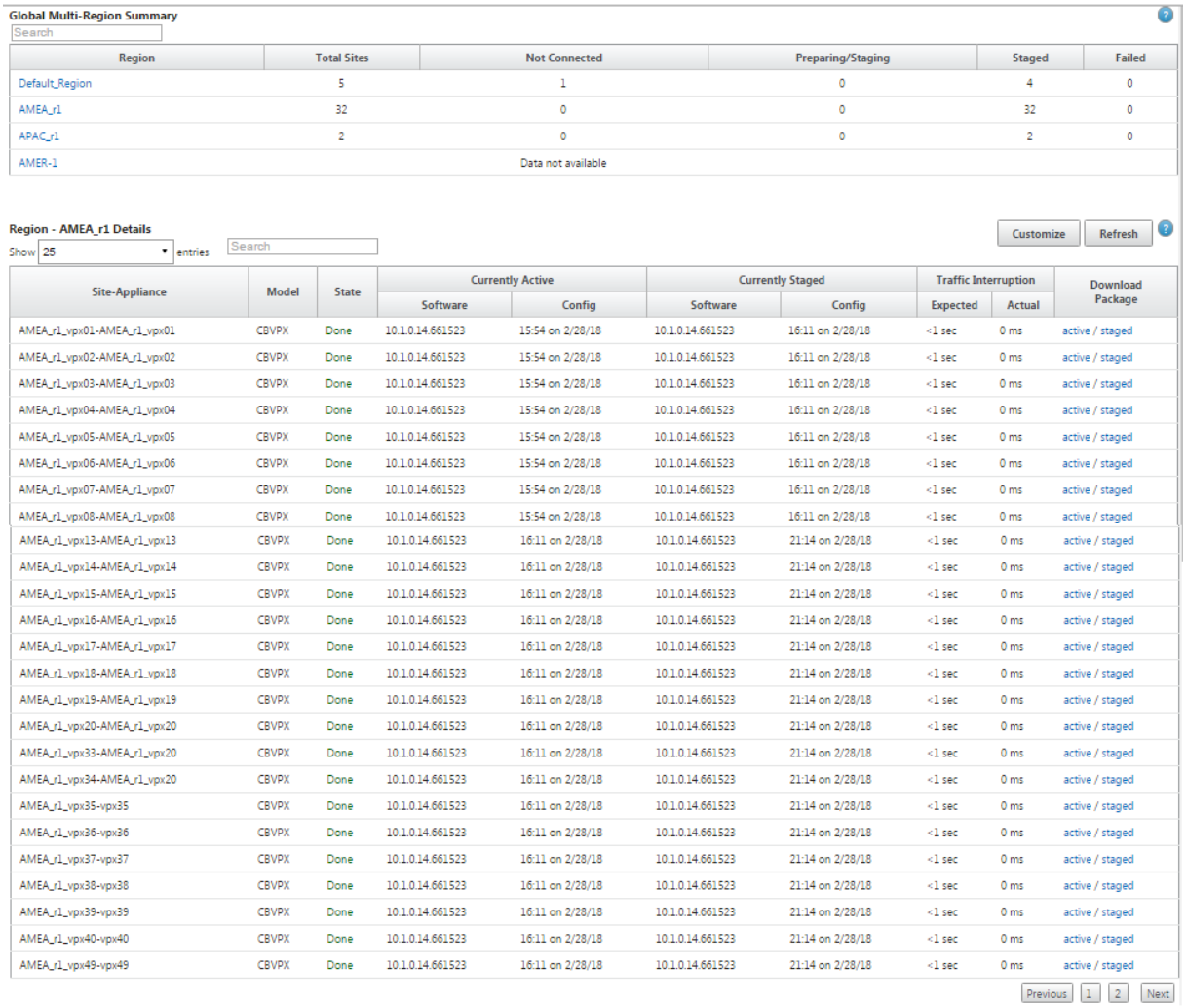
Show 25 entries Search

Customize Refresh

Site-Appliance	Model	State	Currently Active		Currently Staged		Traffic Interruption		Download Package
			Software	Config	Software	Config	Expected	Actual	
MCN1-MCN1-CB4100	CB4100	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 min		active / staged
APAC_RCN-APAC_RCN-CB1000	CB1000	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec		active / staged
BR1-BR1-CBVPXL	CBVPXL	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec		active / staged
RCN01-2000-RCN01-2000	CB2000	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec		active / staged
AMER-1RCN-5100-AMER-1RCN-5100	CB5100	Not Needed	Not Connected				Loc Chg Mgt		none / staged

Previous 1 Next

リージョンの要約:



Global Multi-Region Summary

Search

Region	Total Sites	Not Connected	Preparing/Staging	Staged	Failed
Default_Region	5	1	0	4	0
AMEA_r1	32	0	0	32	0
APAC_r1	2	0	0	2	0
AMER-1	Data not available				

Region - AMEA_r1 Details

Show 25 entries Search

Customize Refresh

Site-Appliance	Model	State	Currently Active		Currently Staged		Traffic Interruption		Download Package
			Software	Config	Software	Config	Expected	Actual	
AMEA_r1_vpx01-AMEA_r1_vpx01	CBVPX	Done	10.1.0.14.661523	15:54 on 2/28/18	10.1.0.14.661523	16:11 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx02-AMEA_r1_vpx02	CBVPX	Done	10.1.0.14.661523	15:54 on 2/28/18	10.1.0.14.661523	16:11 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx03-AMEA_r1_vpx03	CBVPX	Done	10.1.0.14.661523	15:54 on 2/28/18	10.1.0.14.661523	16:11 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx04-AMEA_r1_vpx04	CBVPX	Done	10.1.0.14.661523	15:54 on 2/28/18	10.1.0.14.661523	16:11 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx05-AMEA_r1_vpx05	CBVPX	Done	10.1.0.14.661523	15:54 on 2/28/18	10.1.0.14.661523	16:11 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx06-AMEA_r1_vpx06	CBVPX	Done	10.1.0.14.661523	15:54 on 2/28/18	10.1.0.14.661523	16:11 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx07-AMEA_r1_vpx07	CBVPX	Done	10.1.0.14.661523	15:54 on 2/28/18	10.1.0.14.661523	16:11 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx08-AMEA_r1_vpx08	CBVPX	Done	10.1.0.14.661523	15:54 on 2/28/18	10.1.0.14.661523	16:11 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx13-AMEA_r1_vpx13	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx14-AMEA_r1_vpx14	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx15-AMEA_r1_vpx15	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx16-AMEA_r1_vpx16	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx17-AMEA_r1_vpx17	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx18-AMEA_r1_vpx18	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx19-AMEA_r1_vpx19	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx20-AMEA_r1_vpx20	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx33-AMEA_r1_vpx20	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx34-AMEA_r1_vpx20	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx35-vpx35	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx36-vpx36	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx37-vpx37	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx38-vpx38	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx39-vpx39	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx40-vpx40	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx49-vpx49	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged

Previous 1 2 Next

> 注
>
> 場合によっては、「グローバルマルチリージョンサマリ」テーブルに表示される「サイト合計」の値が、残りの列の合計よりも小さくなることがあります。
>
> たとえば、分岐ノードが接続されていない場合、分岐が 2 回カウントされます。1 回は「未接続」として、1 回は「準備/ステージング」としてカウントされます。

210 SE LTE アプライアンスでの LTE 機能の構成

September 26, 2023

LTE 接続を使用して、Citrix SD-WAN 210-SE LTE アプライアンスをネットワークに接続できます。このトピックでは、モバイルブロードバンド設定の構成、LTE 用のデータセンターおよびブランチアプライアンスの構成などについて詳しく説明します。Citrix SD-WAN 210-SE LTE ハードウェアプラットフォームの詳細については、「Citrix SD-WAN 210 スタンダードエディションアプライアンス」を参照してください。

Citrix SD-WAN 210-SE LTE の使用を開始する

1. Citrix SD-WAN 210-SE LTE の SIM カードスロットに SIM カードを挿入します。

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

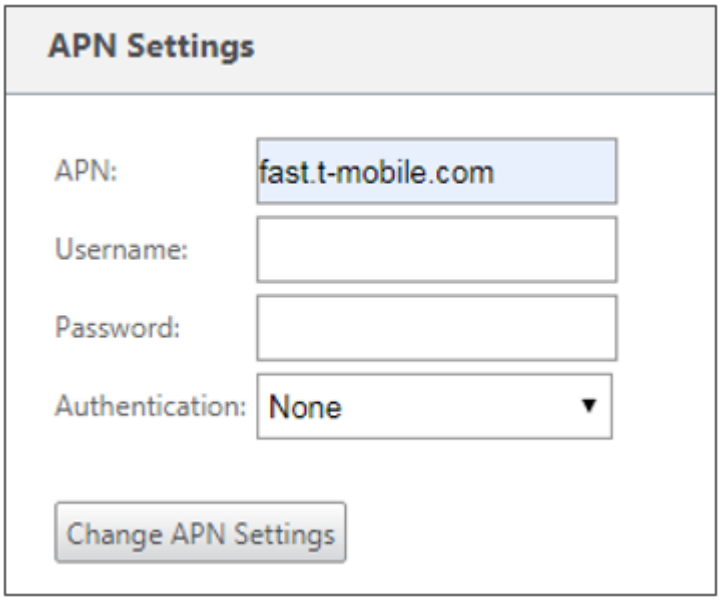
2. アンテナを Citrix SD-WAN 210-SE LTE アプライアンスに固定します。詳しくは、「LTE アンテナの取り付け」を参照してください。
3. アプライアンスの電源を入れます。

   > 注
   >
   > すでに電源が入っていて、起動しているアプライアンスに SIM を挿入した場合は、構成 **>** アプライアンスの設定 **>** ネットワークアダプタ **>** モバイルブロードバンド **> SIM** カードの更新をクリックします。

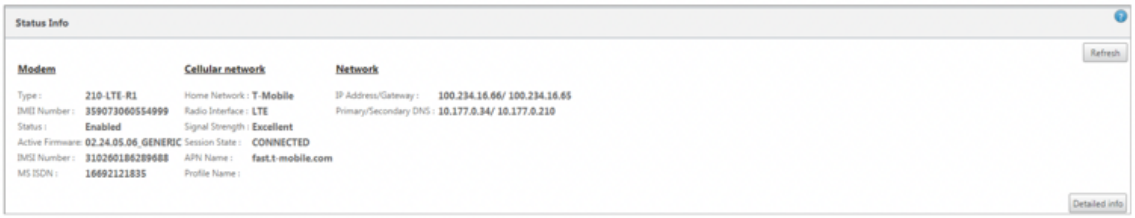
4. APN 設定を構成します。SD-WAN GUI で、[構成] **>** [アプライアンスの設定] **>** [ネットワークアダプタ] **>** [モバイルブロードバンド] **>** [**APN** 設定] に移動します。

> **注:**
> 通信事業者から APN 情報を取得します。



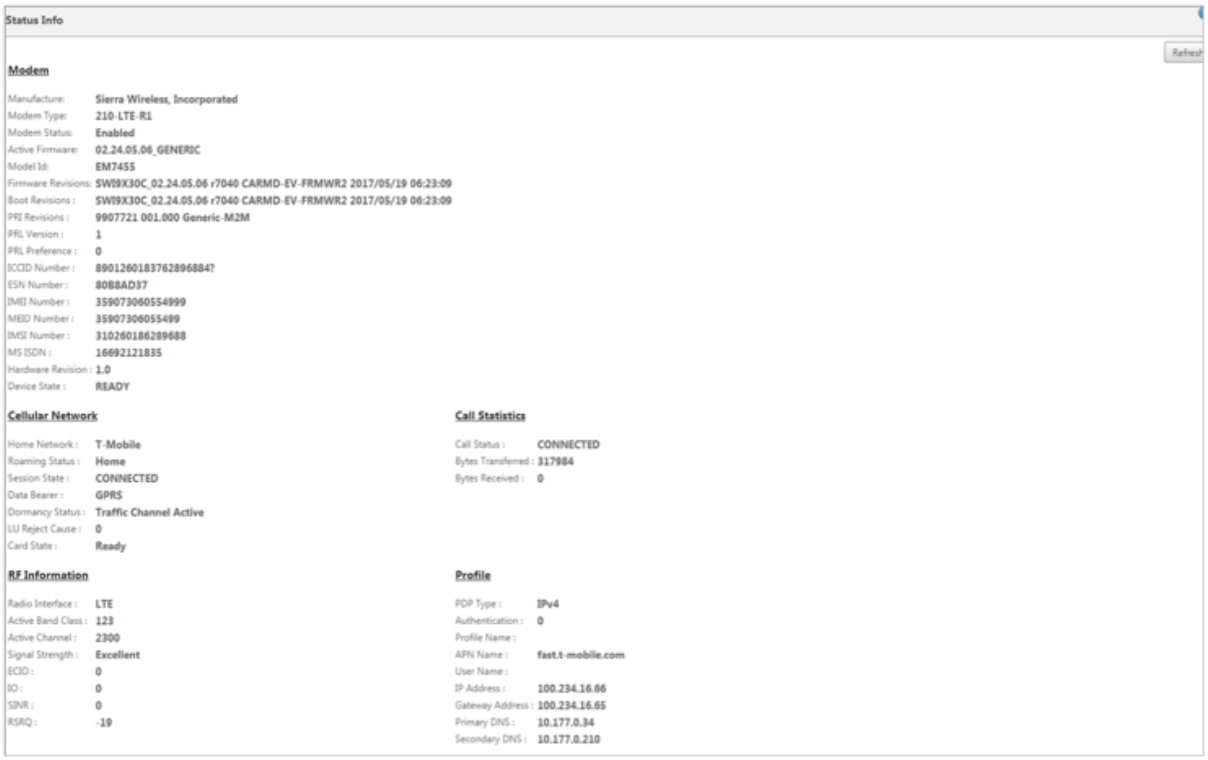
5. キャリアから提供された **APN**、ユーザー名、パスワード、および 認証 を入力します。PAP、CHAP、PAPCHAP 認証プロトコルから選択できます。キャリアが認証タイプを提供していない場合は、**[**なし**]** に設定します。
6. [**APN** 設定の変更] をクリックします。
7. SD-WAN アプライアンスの GUI で、[構成**] > [**アプライアンスの設定**] > [**ネットワークアダプタ**] > [**モバイルブロードバンド] に移動します。

   モバイルブロードバンド設定のステータス情報を表示できます。



以下は、いくつかの有用なステータス情報です。

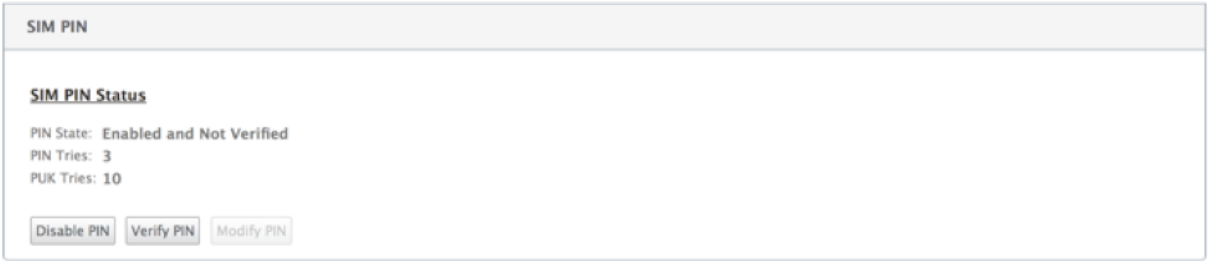
- **Status**: Enabled は、モデムがデータセッションを確立しようとすることを示します。
- カードの状態: Present は、SIM が正しく挿入されていることを示します。
- 信号強度: 信号強度の品質-優秀、良好、公正、不良、または信号なし。
- ホームネットワーク: 挿入された SIM のキャリア。
- **APN** 名: LTE モデムで使用されるアクセスポイント名。
- セッション状態: [接続] は、デバイスがネットワークに参加したことを示します。セッション状態が切断されている場合は、データプランが有効になっているかどうかでアカウントがアクティベートされているかどうかを通信事業者に確認してください。



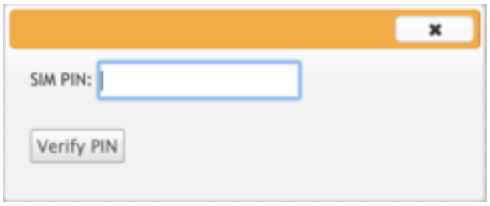
SIM ピン

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

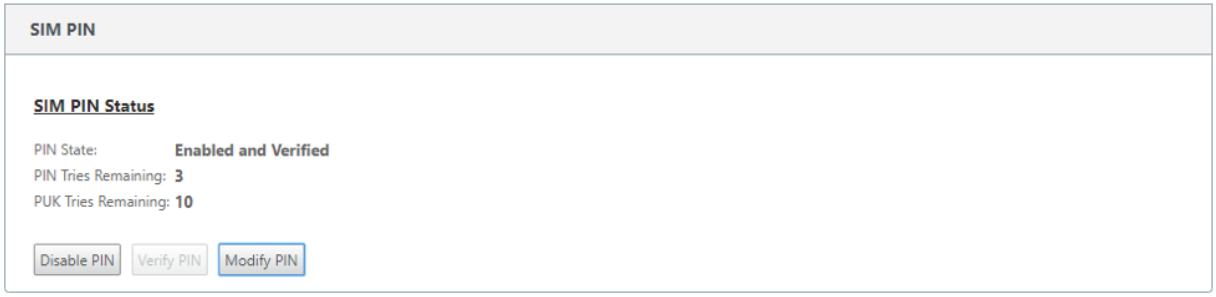
SIM PIN 操作を実行するには、[構成**] > [**アプライアンスの設定**] > [**ネットワークアダプタ**] > [**モバイルブロードバンド**] > [SIM PIN**] に移動します。



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

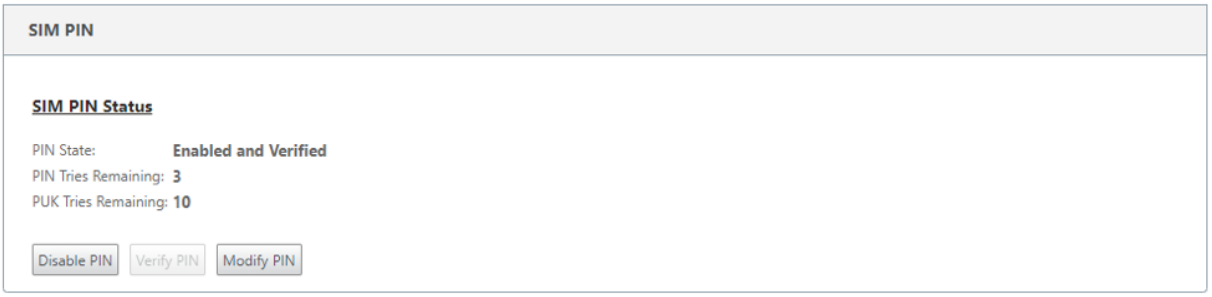


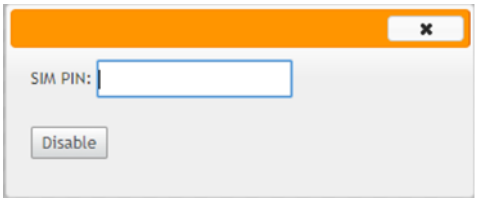
ステータスが [有効] および **[**確認済み] に変わります。



SIM PIN を無効にする

SIM PIN が有効で確認されている SIM の SIM PIN 機能を無効にすることができます。

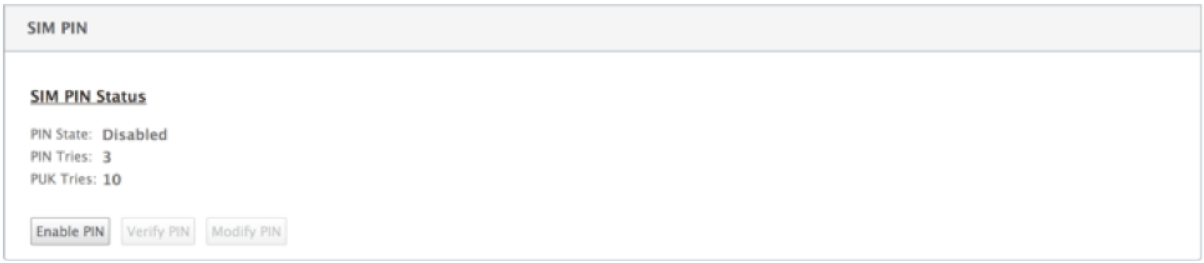




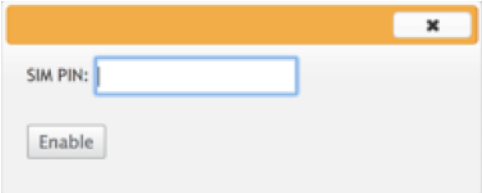
[**PIN** を無効にする] をクリックします。**SIM PIN** を入力し、[無効] をクリックします。

SIM PIN を有効にする

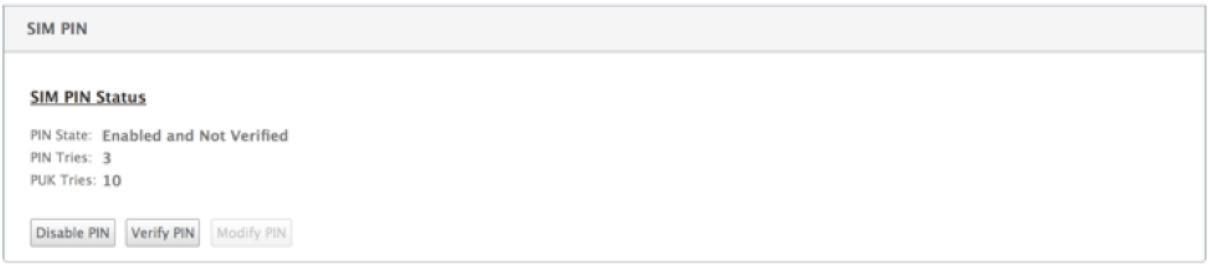
SIM PIN は、無効になっている SIM に対して有効にすることができます。



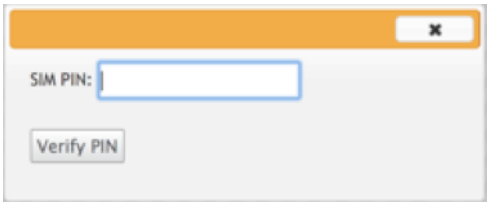
[**PIN** を有効にする] をクリックします。通信事業者から提供された SIM PIN を入力し、[有効] をクリックします。



SIM PIN の状態が **[**有効**]** および **[**未確認] に変わると、PIN が検証されず、PIN が検証されるまで LTE 関連の操作を実行できなくなります。



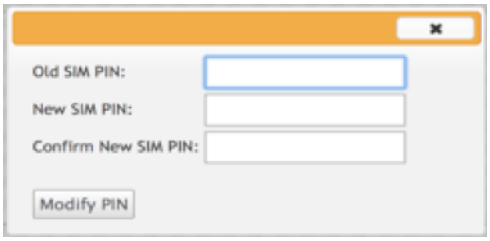
[**PIN** の確認] をクリックします。通信事業者から提供された SIM PIN を入力し、[**PIN** の確認] をクリックします。



SIM PIN の変更

PIN が [有効**]** および **[**確認済み] の状態になったら、PIN を変更できます。

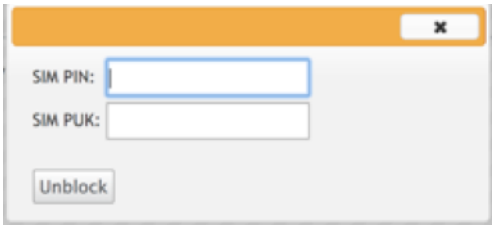
[**PIN** の変更] をクリックします。通信事業者から提供された SIM PIN を入力します。新しい SIM PIN を入力し、確認します。[**PIN** の変更] をクリックします。



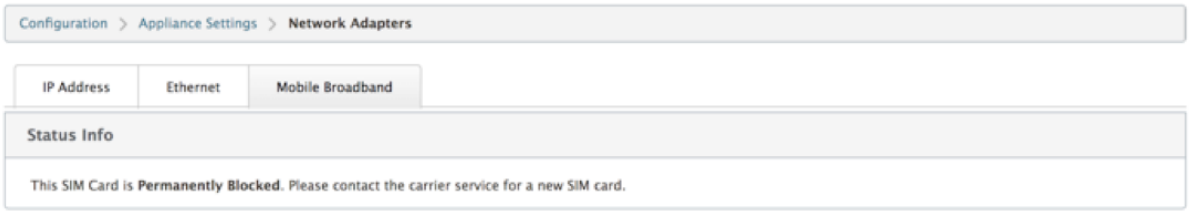
SIM のブロック解除

SIM カードは、SIM PIN 入力の 3 回失敗するとブロックされ、LTE 機能にアクセスできなくなります。キャリアから取得した SIM PUK を使用して、SIM のブロックを解除することができます。

SIM のブロックを解除するには、[ブロック解除] をクリックします。通信事業者から取得した **SIM PIN** と **SIM PUK** を入力し、[ブロック解除] をクリックします。



> 注:
> SIM カードは、SIM のブロックを解除しながら、PUK の 10 回の試行に失敗して永久にブロックされます。新しい SIM カードについては、通信事業者に連絡する必要があります。



ファームウェアの管理

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

使用するファームウェアが不明な場合は、AUTO-SIM オプションを選択して、LTE モデムが挿入された SIM カードに基づいて最も一致するファームウェアを選択できるようにします。

> 注
>
> 11.0.3 リリースでは、LTE アクティブファームウェアはシングルステップアップグレードパッケージの一部として更新されます。アップグレードするには、［管理設定の変更］ページを使用してスケジュール・ウィンドウを更新するか、LTE ファームウェアをアップグレードするためのデフォルトのスケジュール時間（毎日 21:20:00）を待つ必要があります。

モデムの有効化/無効化

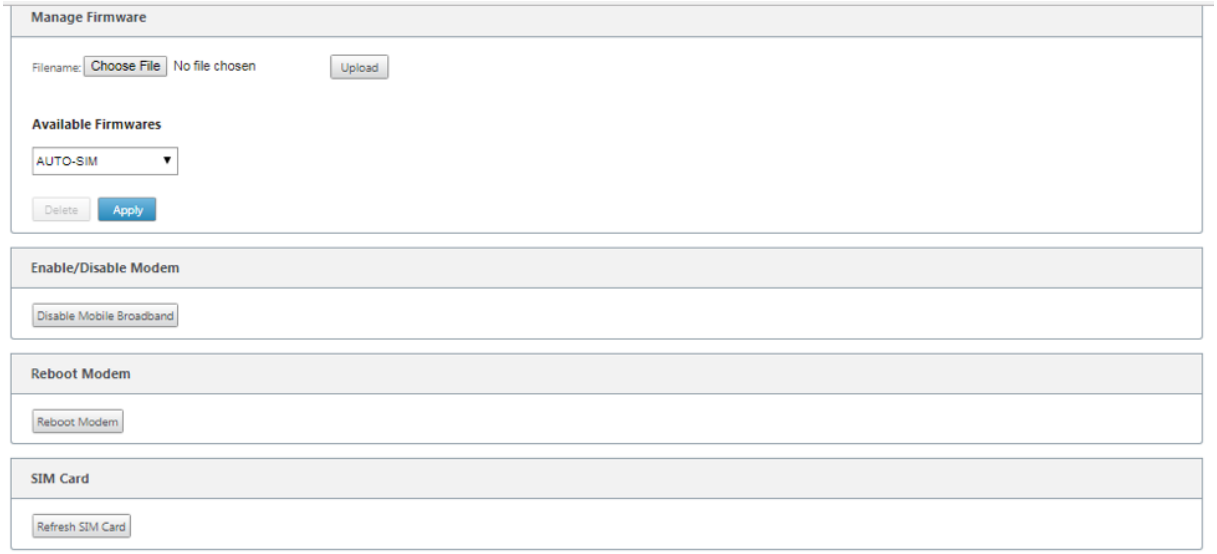
LTE 機能を使用する意図に応じて、モデムを有効/無効にします。デフォルトでは、LTE モデムは有効になっています。

モデムの再起動

モデムをリブートします。再起動操作が完了するまで、最大 3 ～5 分かかる場合があります。

SIM のリフレッシュ

このオプションは、SIM カードをホットスワップして 210-SE LTE モデムで新しい SIM カードを検出する場合に使用します。



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

CLI を使用した LTE 機能の設定

CLI を使用して 210-SE LTE モデムを設定するには

1. Citrix SD-WAN アプライアンスコンソールにログインします。
2. プロンプトで、CLI インターフェイスにアクセスするためのユーザー名とパスワードを入力します。
3. プロンプトで、**lte** コマンドを入力します。「ヘルプ」と入力します。これにより、設定に使用できる LTE コマンドのリストが表示されます。

```
site210>lte
lte>help
status                                  # Show status
show                                    # Show settings
disable                                 # Disable LTE modem
enable                                  # Enable LTE modem
apn <apn> [<user name> [<password> [<PAP|CHAP|PAPCHAP>]]]   # Set APN
sim-power <off|on|reset>                # Off, on, reset SIM card power
sim-pin <show>                          # SIM card pin status
sim-pin <verify|disable|enable> <sim pin> # Verify/Disable/Enable SIM card PIN
sim-pin <modify> <old pin> <new pin>    # Modify SIM card PIN
sim-pin <unblock> <sim puk> <sim pin>   # Unblock SIM card PIN
reboot                                  # Reboot modem
ping                                    # Check if modem manager ready
list-fw                                 # List available firmware
apply-fw <fw>                           # Apply the specified firmware
```

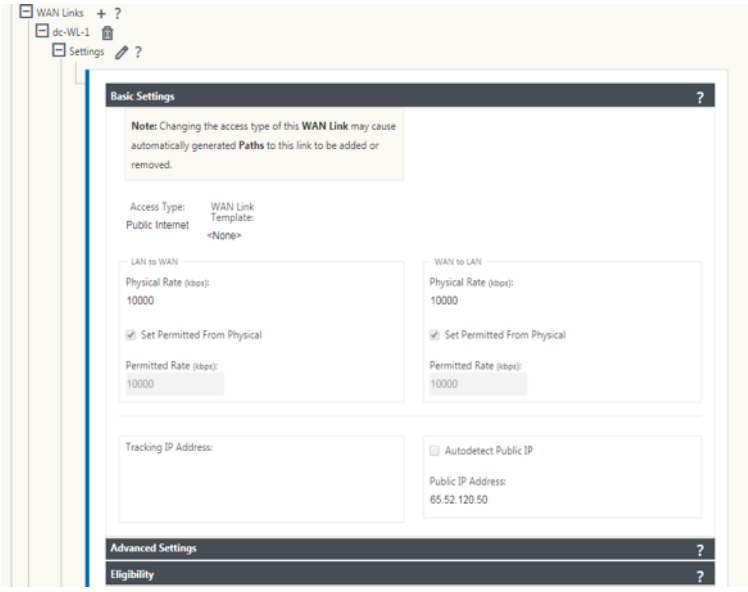
次の表に、**LTE** コマンドの説明を示します。

コマンド	説明
ヘルプ {lte>help}	使用可能な LTE コマンドとパラメータをリストします
ステータス {lte> ステータス}	LTE 接続ステータスを表示します。
{lte>show} を表示	LTE 設定を表示します。
{lte> 無効にする} を無効にする	LTE モデムを無効にします。
有効にする {lte> 有効にする}	LTE モデムを有効にします。
apn {lte>apn}	APN 設定情報を設定します。
SIM 電源オフ、オン、リセット > {lte>SIM 電源オフ、オン、リセット}	SIM カードの電源を切る、SIM カードの電源を入れ、SIM カードをリフレッシュする
SIM PIN {lte>sim-pin}	SIM カードの電源を切る、SIM カードの電源を入れ、SIM カードをリフレッシュする
再起動 {lte> 再起動}	LTE モデムを再起動します
ping {lte>ping}	LTE モデムの PING
リスト-fw {lte>list-fw}	R1 または R2 LTE モデムで使用可能なファームウェアの一覧を表示します。
適用-fw {lte> 適用-fw}	キャリア固有のファームウェアを適用

LTE 用の MCN の設定

MCN を設定するには、次の手順を実行します。

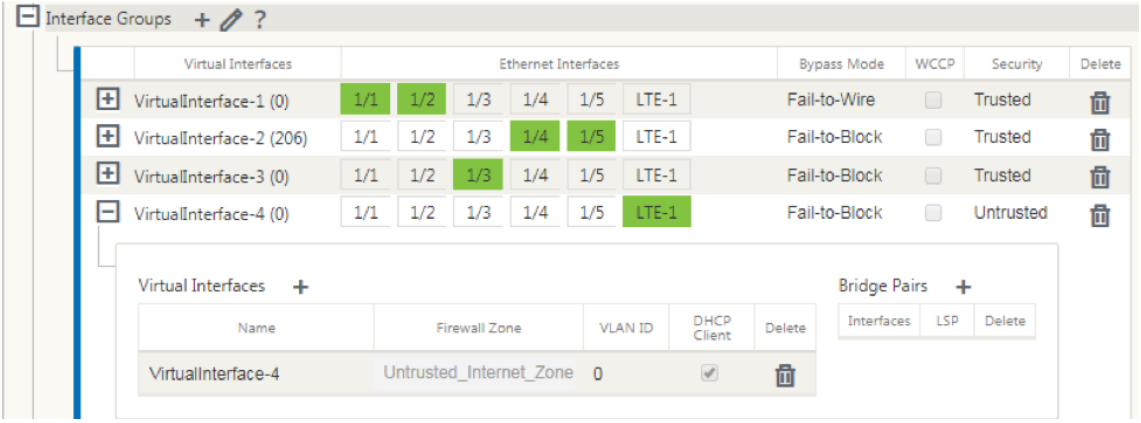
1. SD-WAN アプライアンスの GUI にログインします。[構成エディタ] に移動します。MCN サイトの設定を完了します。MCN の設定を参照してください。
2. WAN リンク設定の一部として、ルーティング可能なパブリック IP アドレスを指定してください。クライアントアプライアンスのパブリック IP アドレスを設定する必要はありません。



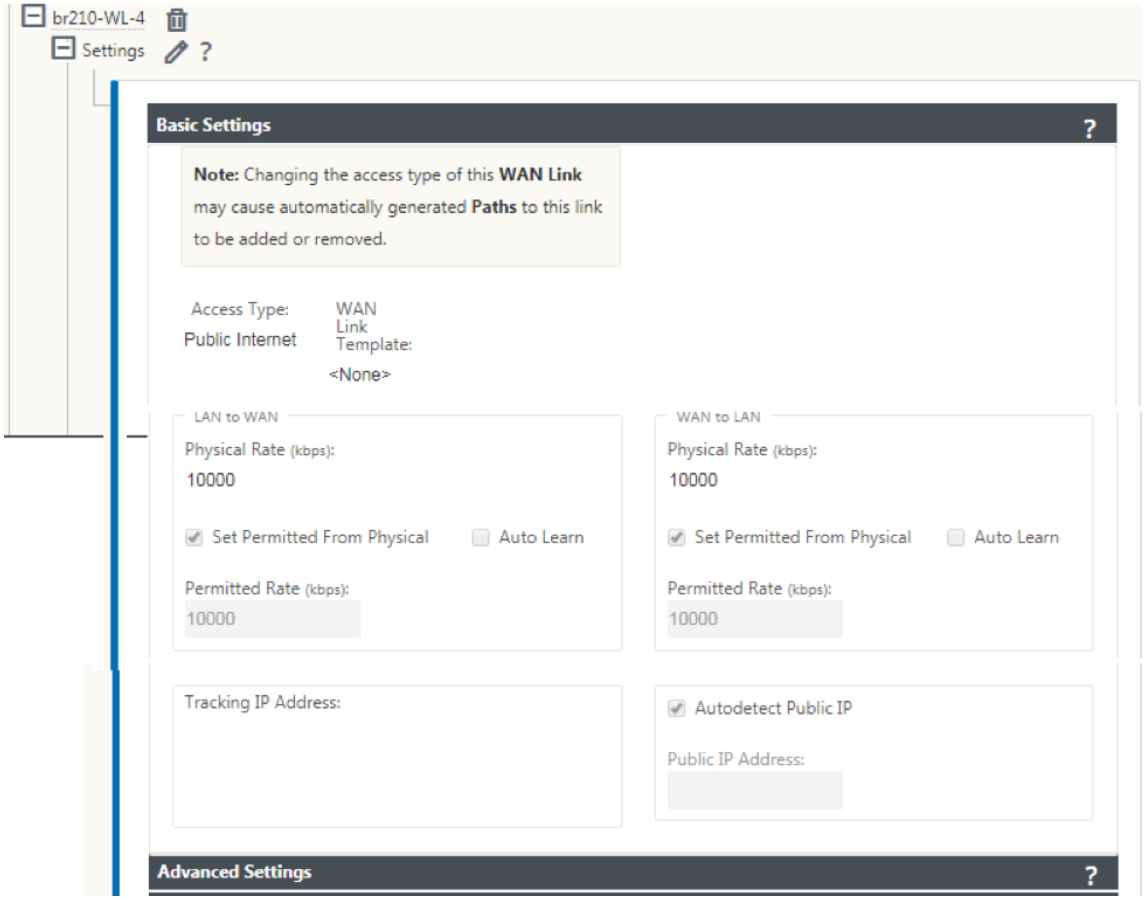
LTE のブランチを構成する

210-SE LTE アプライアンスをブランチサイトとして設定するには、次の手順を実行します。

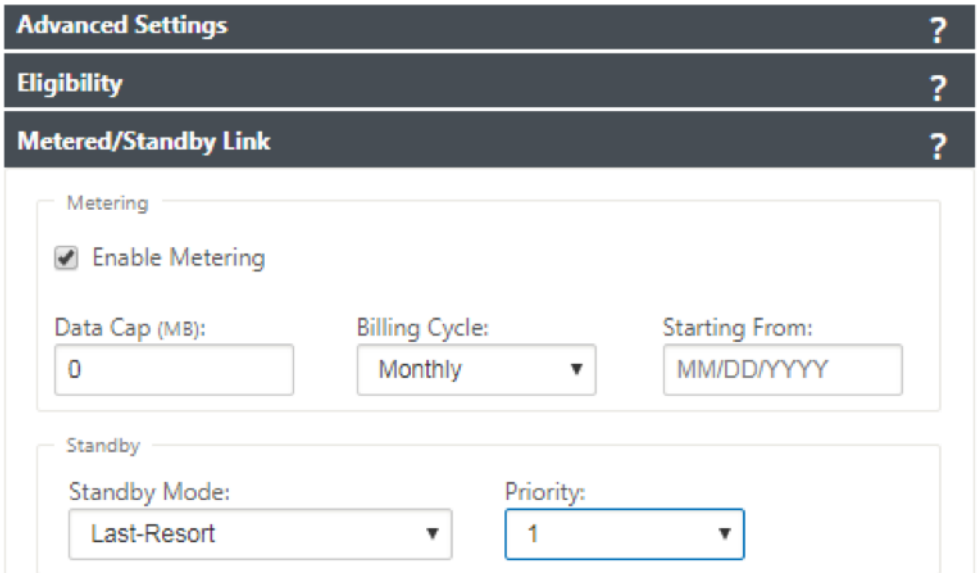
1. SD-WAN アプライアンスの GUI で、構成エディタに移動します。「ブランチの構成」を参照してください。
   - インターフェイスグループを作成します。
   - 次の項目を選択して、LTE アダプタ用に最大 1 つの仮想インターフェイスと 1 つのインターフェイスグループを作成し、WAN リンクを設定します。
     - イーサネットインターフェイス—LTE 1
     - セキュリティ：信頼できない（デフォルト）
     - DHCP クライアント：有効（デフォルト）



2. LTE インターフェイス用に作成された仮想インターフェイスを使用して WAN リンクを設定するときに、WAN リンク構成の **AutoDetect** パブリック **IP** を有効にします。

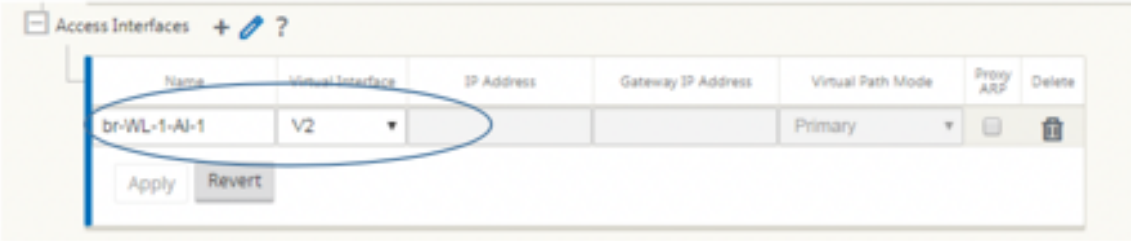


3. デフォルトでは、LTE インターフェイスを使用して WAN リンクを設定しようとすると、WAN リンクは従量制課金リンクおよびラストリゾートスタンバイモードとしてマークされます。必要に応じて、これらのデフォルト設定を変更できます。



WAN リンクのアクセスインターフェイスの IP アドレスおよび Gateway アドレスは、DHCP を介してキャ

リアから情報を受信するため、設定する必要はありません。



4. 210-SE LTE アプライアンスに必要な残りのブランチ構成を完了します。「ブランチを構成」を参照してください。
5. SD-WAN ソフトウェアをアップロードして、変更管理を実行します。「変更管理手順」を参照してください。
6. ローカル変更管理プロセスを通じて構成をアクティブ化します。変更管理を実行すると、構成がアクティブになり、必要な構成が適用されます。

LTE 経由のゼロタッチ展開

LTE 経由のゼロタッチ導入サービスを実現するための前提条件

1. 210-SE LTE アプライアンス用のアンテナと SIM カードを取り付けます。
2. SIM カードに有効なデータプランがあることを確認します。
3. 管理ポートが接続されていないことを確認します。
   - 管理ポートが接続されている場合は、管理ポートを切断し、アプライアンスを再起動します。
   - 管理インターフェイスで固定 IP アドレスが設定されている場合は、DHCP を使用して管理インターフェイスを設定し、設定を適用してから、管理ポートを切断し、アプライアンスを再起動する必要があります。
4. 210-SE アプライアンス構成で、LTE インターフェイス用にインターネットサービスが定義されていることを確認します。

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

SD-WAN Center GUI を使用して、ゼロタッチ展開サービス用の 210-SE LTE アプライアンスを展開および構成できます。

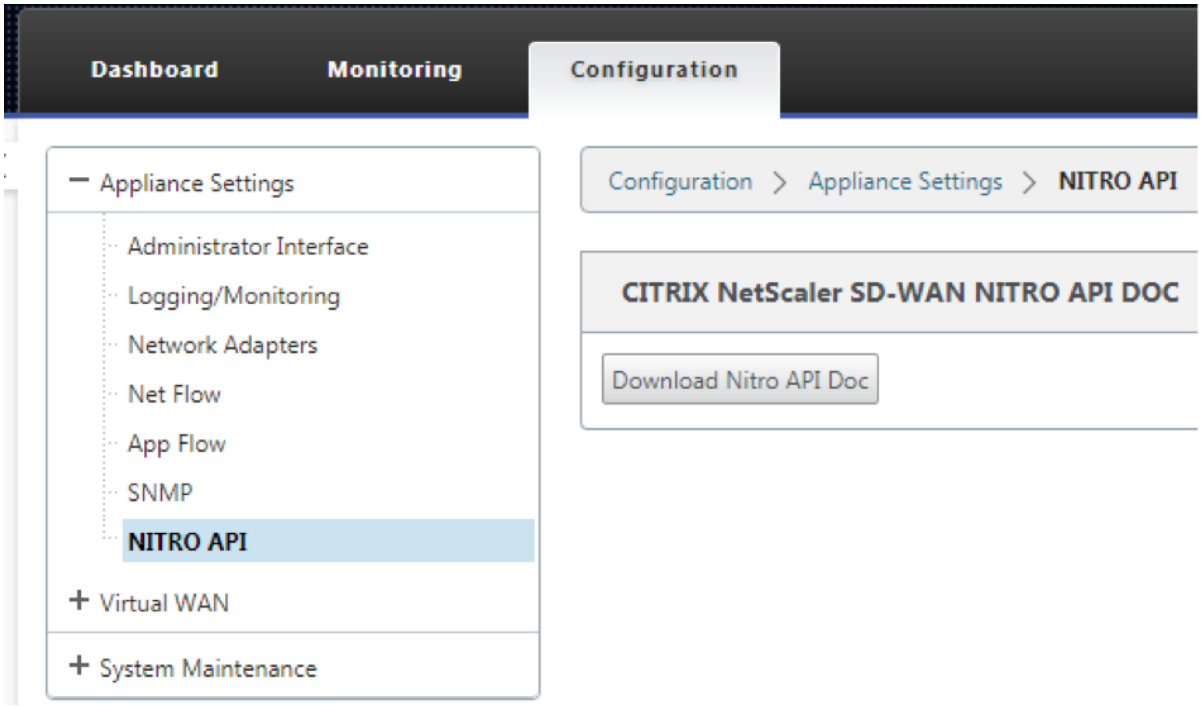
SD-WAN Center を使用した 210-SE LTE アプライアンスの配置および設定の詳細については、ゼロタッチ展開手順を参照してください。

210-SE LTE アプライアンスの管理インターフェースを介したゼロタッチ導入サービス

管理ポートを接続し、他のすべての非 LTE プラットフォームでサポートされている標準ゼロタッチ展開手順を使用します。

LTE 休息 API

LTE REST API の詳細については、SD-WAN GUI に移動し、「構成」**>**「アプライアンスの設定」**>**「**NITRO API**」の順に選択します。[**Nitro API** ドキュメントのダウンロード] をクリックします。SIM PIN 機能用の REST API は、Citrix SD-WAN 11.0 で導入されています。



ドメイン・ネーム・システム

May 10, 2021

ドメインネームシステム（**DNS**）は、人間が読めるドメイン名を機械読める IP アドレスに変換し、その逆も同様です。SD-WAN リリース 10 バージョン 2 では、次の DNS 機能が導入されています。

- DNS プロキシ
- DNS 透過転送

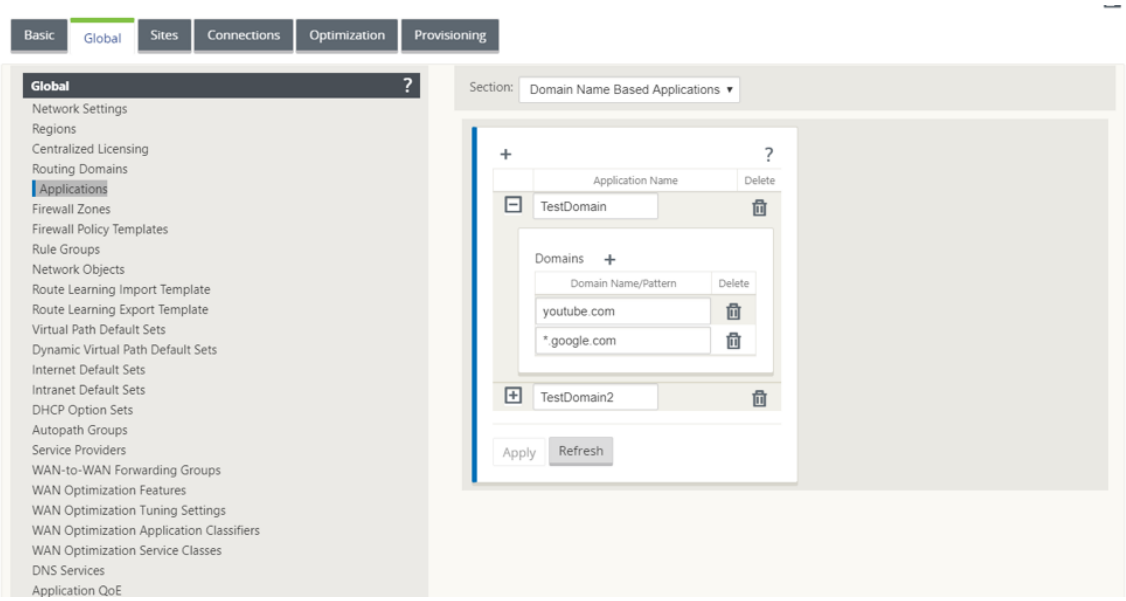
DNS プロキシ

DNS プロキシは、SD-WAN IP アドレス宛の DNS 要求を代行受信し、選択的な DNS サービスに転送します。アプリケーションのドメイン名に基づいて DNS 要求の操作に役立つ複数のフォワーダーを持つプロキシを構成できます。DNS 転送は、UDP 接続を介して受信される要求に対して機能します。

SD-WAN を DNS プロキシとして設定するには、次の手順を実行します。

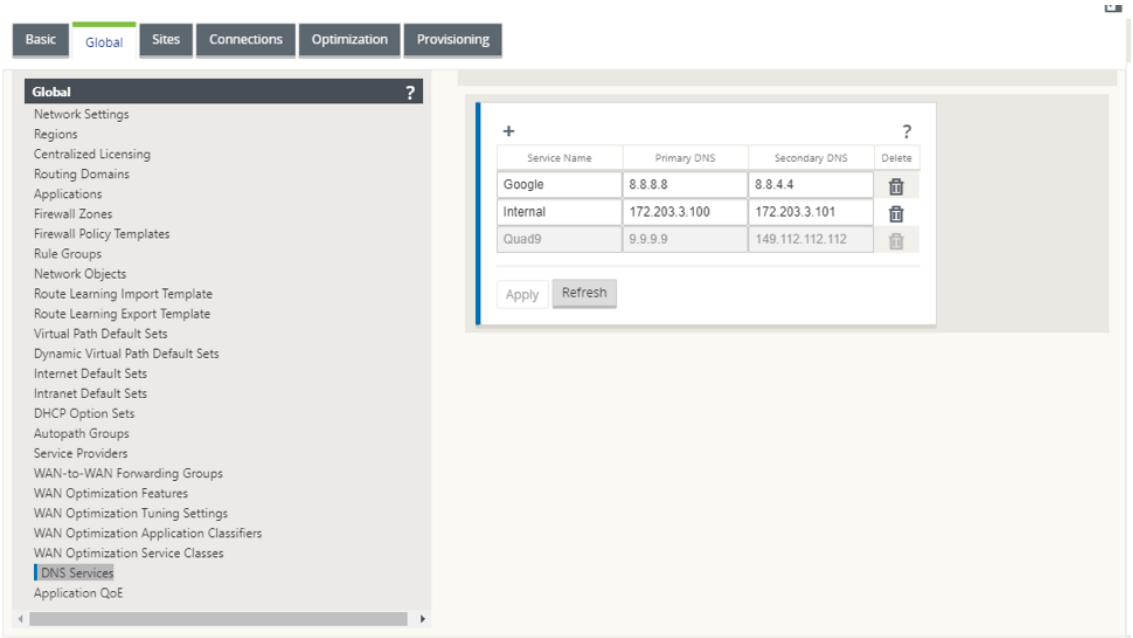
1. ドメイン名ベースのアプリケーションを定義します。構成エディタで、[グローバル] **>** [アプリケーション] **>** [ドメイン名ベースのアプリケーション] に移動します。

   アプリケーション名と必要なドメイン名またはパターンを入力します。複数のドメイン名をアプリケーションとしてグループ化できます。完全なドメイン名を入力することも、先頭にワイルドカードを使用することもできます。たとえば-*.google.com



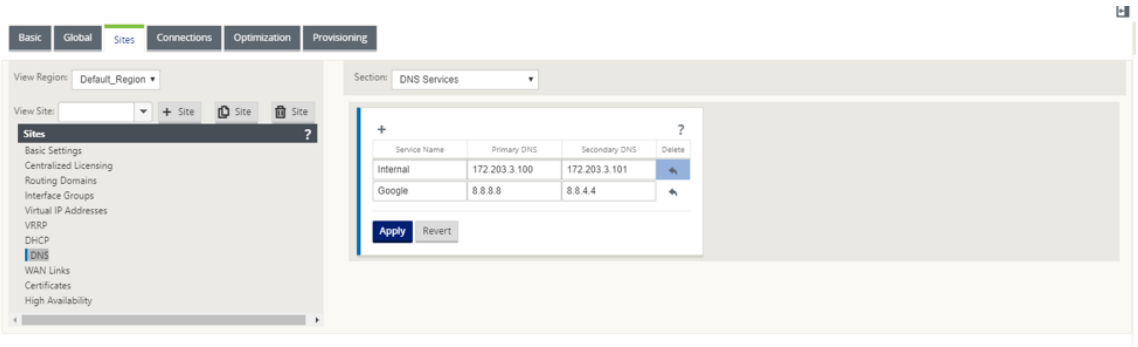
2. 必要な DNS サービスを定義します。[グローバル] **>** [**DNS** サービス] に移動します。サービス名と、プライマリとセカンダリ **DNS** サーバの **IP** アドレスのペアを入力します。

   内部、ISP、グーグル、またはその他のオープンソースの DNS サービスを作成できます。



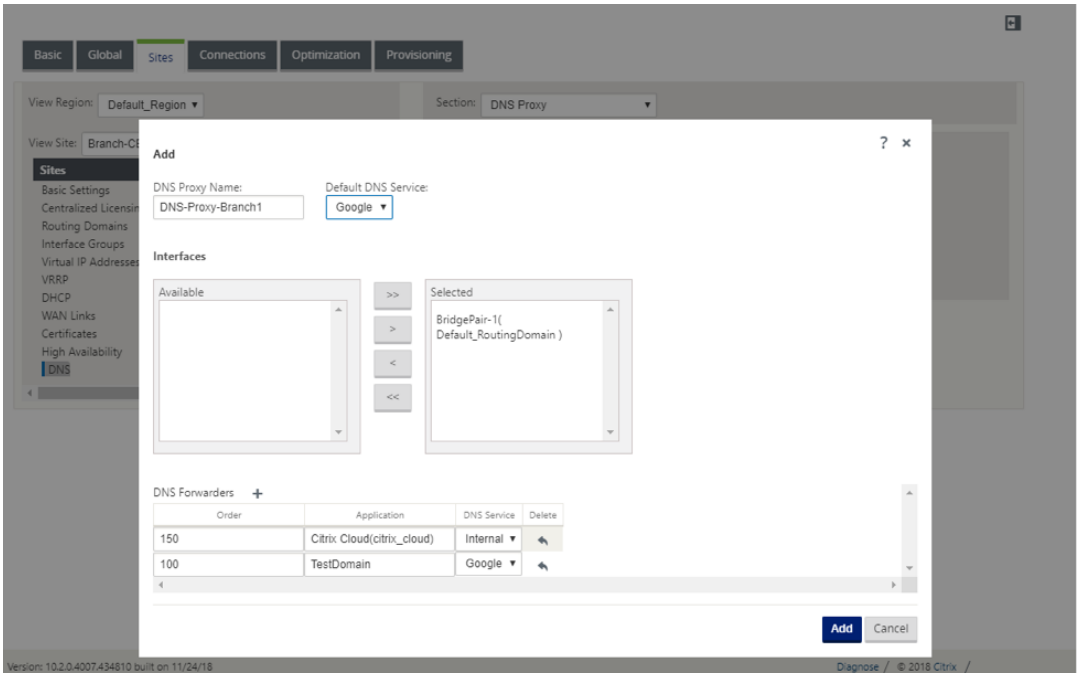
> 注:
>
> Office 365 ブレークアウトポリシーを構成している場合は、Quad9 DNS サービスが自動作成されます。詳しくは、「Office 365 の最適化」を参照してください。

また、個々のサイトレベルで DNS サービスを定義することもできます。サイトレベルの DNS サービス設定は、グローバル設定を上書きします。サイト固有の DNS サービスを構成するには、[サイト] **> [DNS] > [DNS** サービス] に移動します。サービス名と、プライマリとセカンダリ **DNS** サーバの **IP** アドレスのペアを入力します。



3. サイトの DNS プロキシを構成します。[サイト] **> [DNS] > [DNS** プロキシ] に移動します。[**+**] をクリックします。次のパラメーターの値を入力します。

   - **DNS** プロキシ名: DNS プロキシの名前。
   - **[** 既定の **DNS** サービス]: DNS フォワーダルックアップでアプリケーションが一致しない場合、DNS 要求の転送先となる既定の DNS サービス。
   - インターフェイス: DNS 要求が代行受信されるインターフェイス。信頼できるインターフェイスだけが許可されます。
   - **DNS** フォワーダー: DNS フォワーダーのリスト。
     - 順序: フォワーダの優先順位。
     - アプリケーション: 選択した DNS サービスに DNS 要求を転送する必要があるアプリケーション。
     - **DNS** サービス: 指定されたアプリケーションの DNS 要求が転送される DNS サービス。

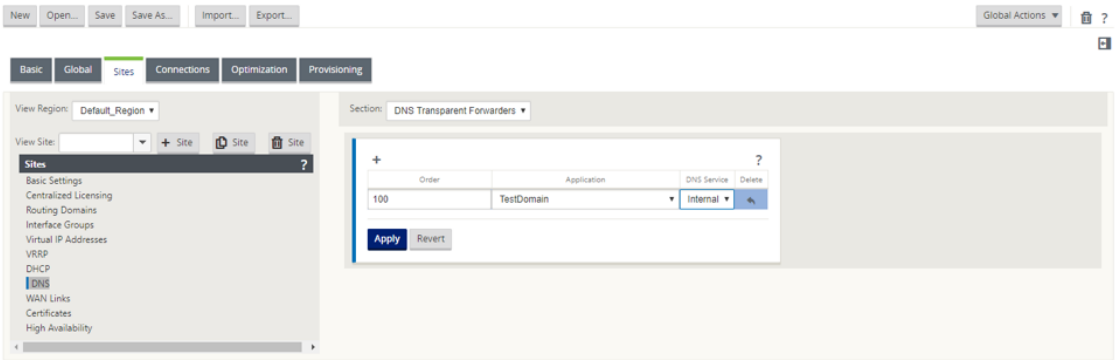


DNS トランスペアレントフォワーダ

SD-WAN は、トランスペアレント DNS フォワーダとして設定できます。このモードでは、SD-WAN は、その IP アドレス宛てではない DNS 要求を傍受し、指定された DNS サービスに転送できます。信頼できるインターフェイス上のローカルサービスからの DNS 要求だけが傍受されます。DNS 要求が DNS フォワーダリスト内のアプリケーションと一致する場合、その要求は設定された DNS サービスに転送されます。DNS 転送は、UDP 接続経由で着信する要求に対してのみサポートされます。

SD-WAN を DNS トランスペアレントフォワーダとして設定するには、次の手順を実行します。

1. [サイト**] > [DNS] > [DNS** 透過フォワーダー] に移動します。[**+**] をクリックします。
2. 次のパラメーターの値を入力します。
   - 順序: フォワーダの優先順位。
   - アプリケーション: 選択した DNS サービスに DNS 要求を転送する必要があるアプリケーション。
   - **DNS** サービス: 指定されたアプリケーションの DNS 要求が転送される DNS サービス。



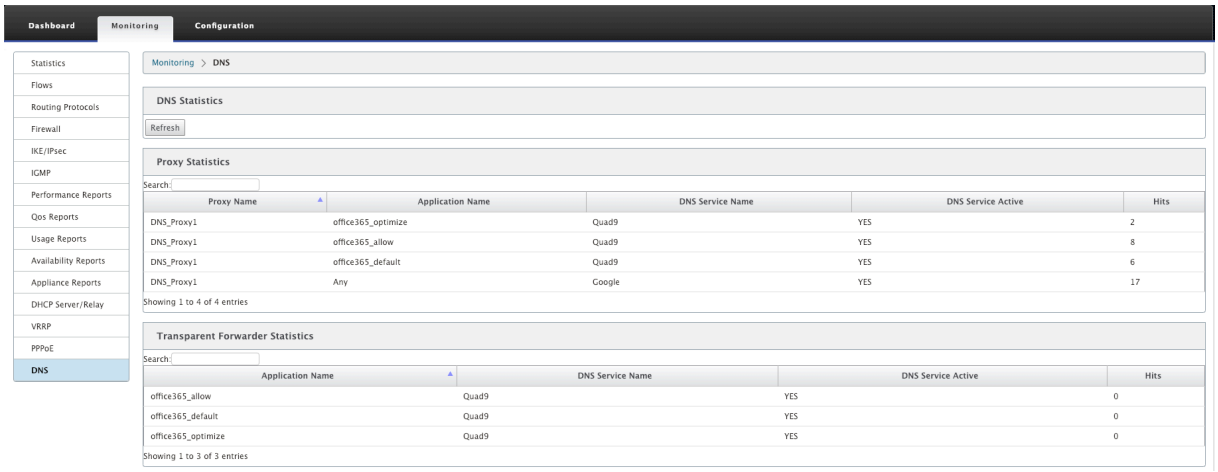
同様に、必要に応じて他の DNS トランスペアレントフォワーダを追加します。

3. ［適用］をクリックします。

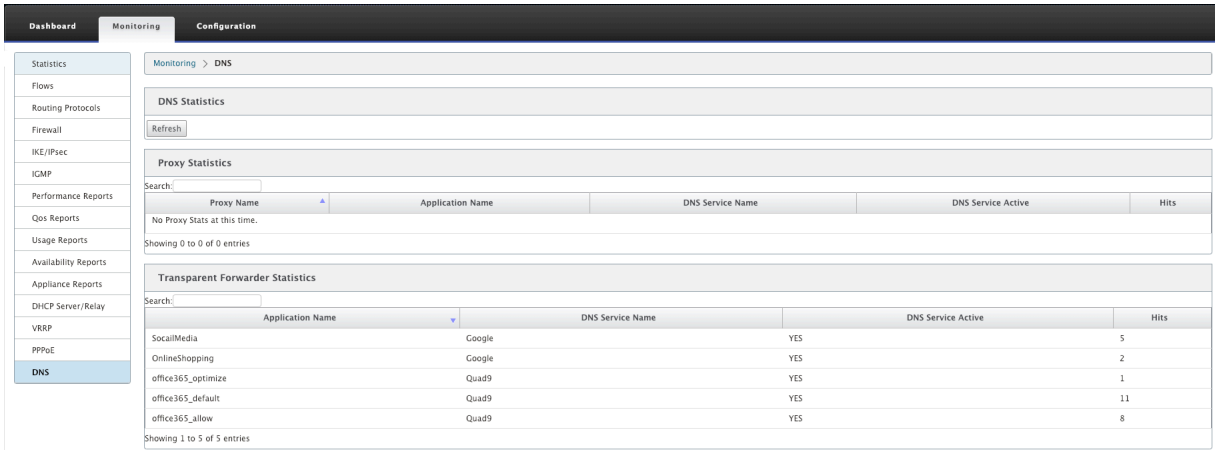
監視

プロキシ統計情報および透過フォワーダの統計情報を表示するには、[モニタリング**] > [DNS]** に移動します。アプリケーション名、DNS サービス名、DNS サービスの状態、および DNS サービスへのヒット数を表示できます。

プロキシ統計情報



トランスペアレントフォワーダの統計



DHCP サーバと DHCP リレー

May 10, 2021

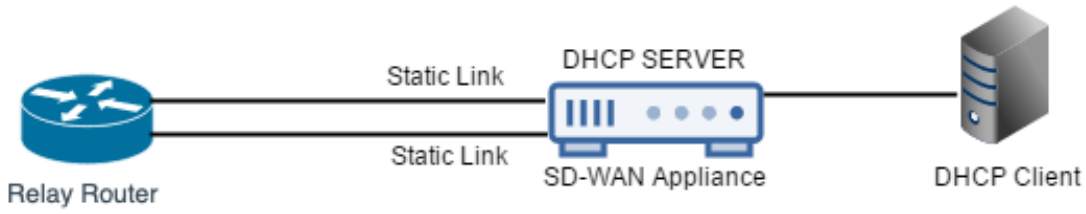
Citrix SD-WAN では、標準版または Premium 版のアプライアンスを DHCP サーバーまたは DHCP リレーエージェントとして使用できます。DHCP サーバー機能を使用すると、SD-WAN アプライアンスの LAN/WAN インターフェイスと同じネットワーク上のデバイスが、SD-WAN アプライアンスから IP 設定を取得できます。DHCP リレー機能を使用すると、SD-WAN アプライアンスは DHCP クライアントとサーバ間で DHCP パケットを転送できます。

DHCP サーバおよび DHCP リレー機能を使用する利点は次のとおりです。

- クライアントサイトの機器の量を減らします。
- クライアントサイトのルーターを置き換える (エッジルーターサービスの容易な展開)。
- クライアントサイトネットワークを簡素化します。
- CLI コマンドを使用しないルータの設定
- 単純なクライアントサイトでの手動構成を減らします。

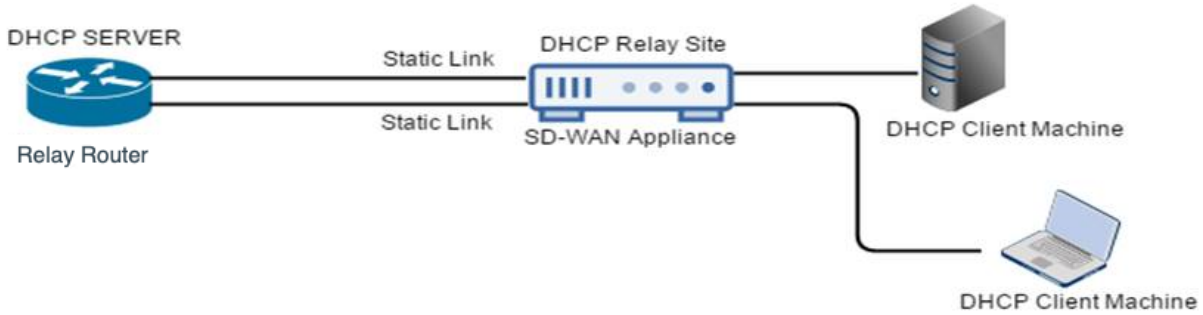
DHCP サーバ

Citrix SD-WAN アプライアンスは、DHCP サーバーとして構成できます。ネットワーク内の指定されたアドレスプールの IP アドレスを DHCP クライアントに割り当てて管理することができます。DHCP サーバは、ドメインネームシステム (DNS) サーバの IP アドレスやデフォルトルータなど、さらに多くのパラメータを割り当てるように設定できます。DHCP サーバは、アドレス割り当て要求と更新を受け入れます。DHCP サーバは、ローカルに接続された LAN セグメントからのブロードキャストや、ネットワーク内の他の DHCP リレーエージェントによって転送された DHCP 要求からのブロードキャストも受け付けます。



DHCP リレー

DHCP リレーエージェントは、クライアントとサーバ間で DHCP パケットを転送するホストまたはルータです。ネットワーク管理者は、SD-WAN アプライアンスの DHCP リレーサービスを使用して、ローカルの DHCP クライアントとリモートの DHCP サーバー間で要求と応答をリレーできます。これにより、ローカルホストはリモート DHCP サーバーからダイナミック IP アドレスを取得できます。リレーエージェントは DHCP メッセージを受信し、新しい DHCP メッセージを生成して別のインターフェイスに送信します。



DHCP サーバと DHCP リレーの設定

May 10, 2021

設定エディタを使用した DHCP サーバと DHCP リレーの設定

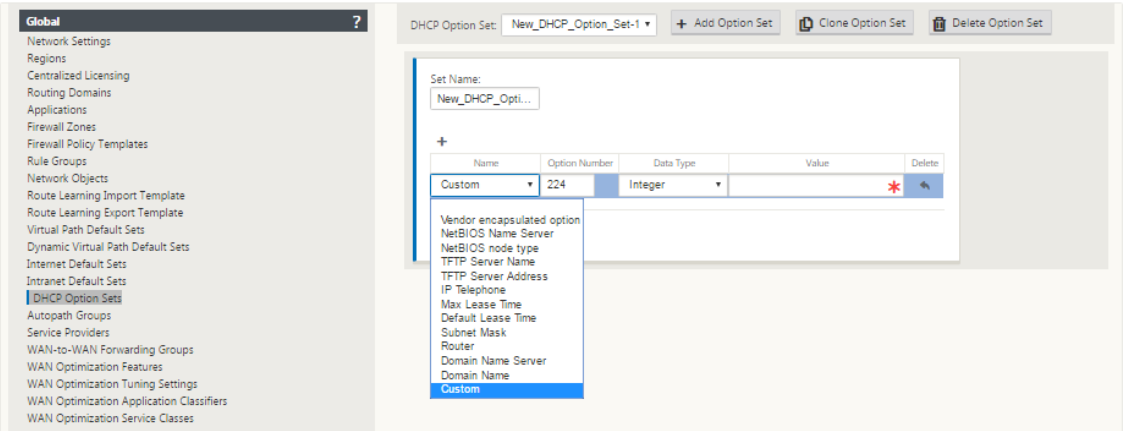
構成エディタを使用して、ネットワーク上のアプライアンスの DHCP サーバーおよび DHCP リレー設定を構成できます。構成は、変更管理プロセスを通じて SD-WAN ネットワーク内のアプライアンスにプッシュされます。

構成エディタを使用してサイトを DHCP サーバーとして構成するには、次の手順を実行します。

1. [構成エディタ] > [サイト] >[サイト名]> [DHCP] > [サーバーサブネット] に移動します。[**+**] をクリックします。

2. 複数のドメインが存在する場合は、構成済みのルーティングドメインを選択します。
3. DHCP 要求の受信に使用する 仮想インターフェイスを 選択します。DHCP サーバがアドレスを提供するために使用する IP サブネットは、自動的に設定されます。
4. [ドメイン名]、[プライマリ **DNS**]、および [セカンダリ **DNS**] を入力します。DHCP サーバはこの情報をクライアントに転送します。
5. [**Enable**] をクリックして、サブネットを有効にします。
6. クライアントに IP アドレスを割り当てるために使用されるダイナミック IP アドレスプールを構成します。開始 IP アドレスと終了 IP アドレスの範囲を指定し、オプションセットを選択します。

   > 注:
   >
   > DHCP オプションセットは、個々の IP アドレス範囲に適用できる DHCP 設定のグループです。DHCP オプションセットを作成するには、[グローバル] > [**DHCP** オプションセット] に移動します。必要な DHCP オプションを選択し、その値を指定します。



7. MAC アドレスに基づいて固定 IP アドレスを必要とする個々のホストを設定します。[固定 **IP** アドレス]、[**MAC** アドレス]、および **[**オプションセット**]** を選択します。

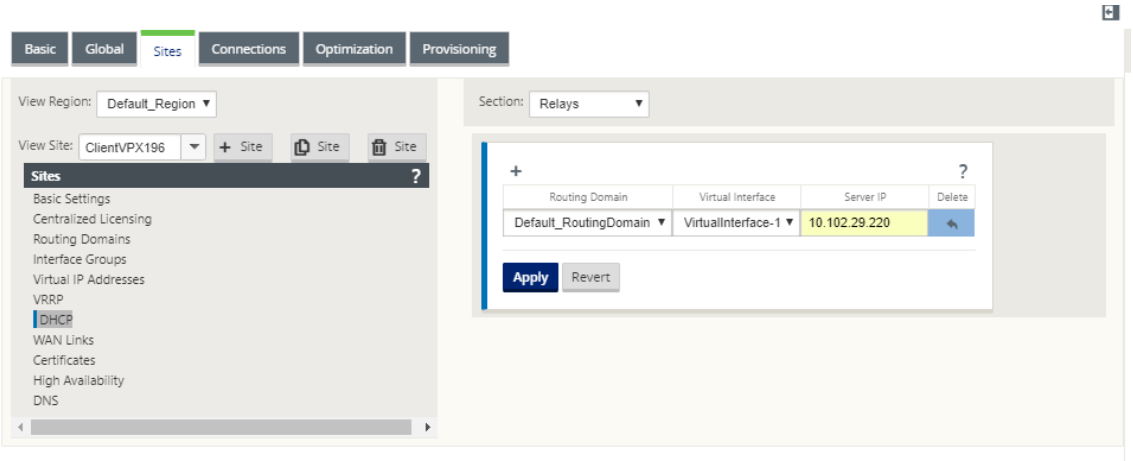
> 注
>
> 固定 IP アドレスの場合、ゲートウェイ **IP** は **DHCP** オプションセットで Router オプションを設定することによって設定されます。

構成エディタを使用して、サイトを DHCP リレーとして設定するには、次の手順を実行します。

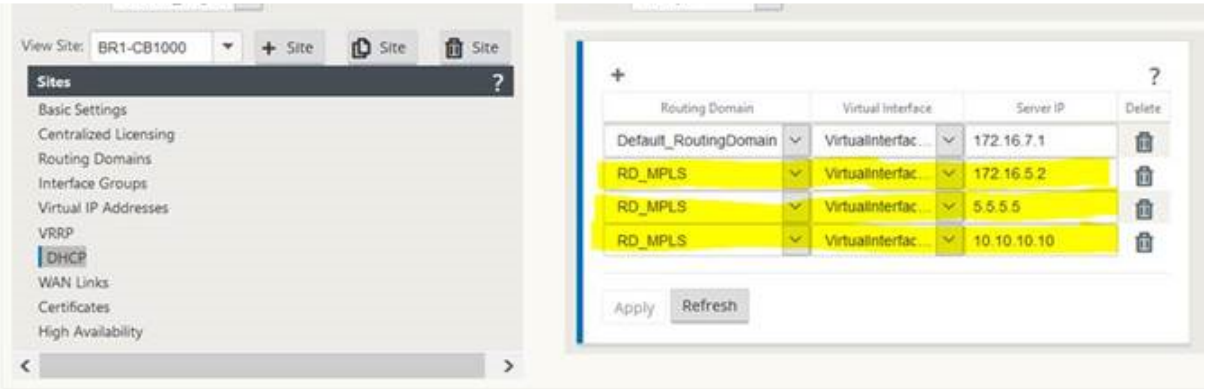
1. [構成 エディタ] > [サイト] > [**DHCP [**サイト名**]**] > [リレー] に移動します。[**+**] をクリックします。

   > 注:
   >
   > DHCP リレーは最大 16 個まで設定できます。

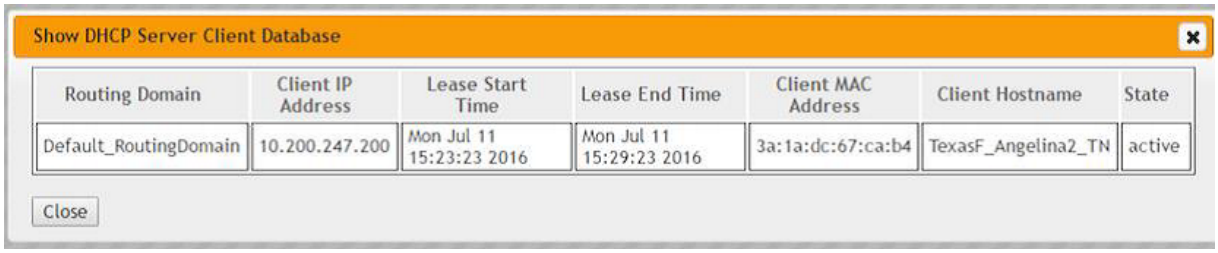
2. 複数のドメインが存在する場合は、構成済みのルーティングドメインを選択します。
3. リモート DHCP サーバーと通信する仮想インターフェイスを選択します。
4. リレーがクライアントからの要求と応答を転送するために使用する DHCP サーバ IP を入力します。



共通の仮想ネットワークインターフェイスを使用して単一の DHCP リレーを構成し、複数の DHCP サーバーを指し示すことができます。



DHCP サーバーデータベースからクライアントのリストを表示するには、Web 管理インターフェイスで、[モニター] > [**DHCP** サーバー**/**リレー] に移動します。



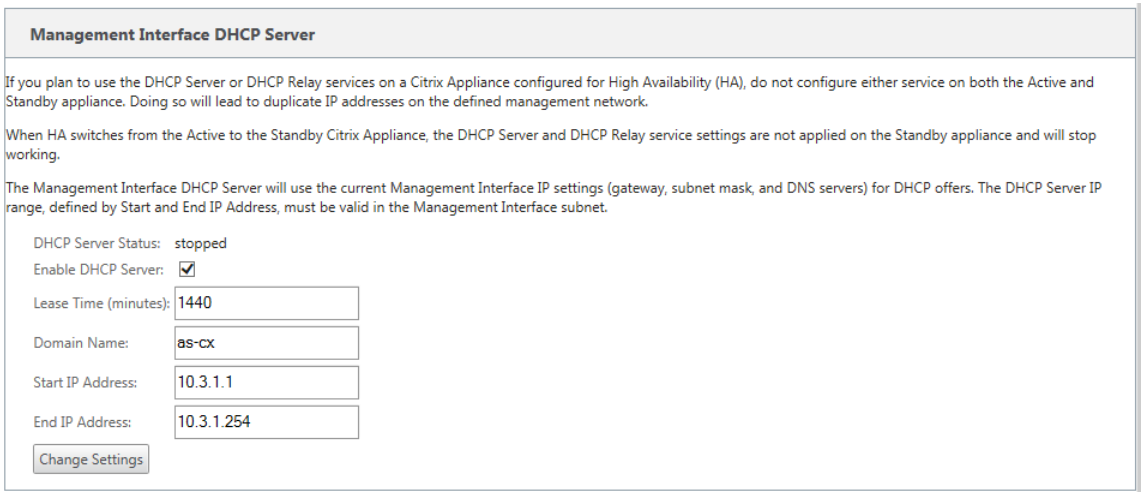
アプライアンスの設定を使用して、**SD-WAN** アプライアンスを **DHCP** サーバーまたは **DHCP** リレーとして構成する

個別の SD-WAN アプライアンスは、アプライアンスの設定ページから手動で DHCP サーバーまたは DHCP リプレイとして構成できます。

SD-WAN アプライアンスで DHCP サーバーを有効にするには、次の手順を実行します。

1. 「構成」>「アプライアンスの設定」>「ネットワークアダプタ」に移動します。[ネットワークアダプタ] ページで、[管理インターフェイス **DHCP** サーバー] ペインを探します。
2. [**DHCP** サーバを有効にする] をクリックしてサーバを起動し、リース時間 (分単位) と [ドメイン名] を入力し、[開始 **IP** アドレス] と **[**終了 **IP** アドレス ****]** を入力して **IP** アドレスの範囲 ** を定義します。

   > 注:
   >
   > サーバーの IP アドレスプールは、管理ネットワーク内にある必要があります。



3. [設定の変更] をクリックして、DHCP サーバーの設定を終了します。

   > 注
   >
   > 高可用性（HA）用に構成された SD-WAN アプライアンスで DHCP サーバを使用する場合は、アクティ

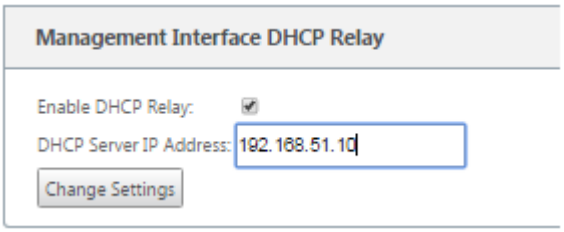
> ブアプライアンスとスタンバイアプライアンスの両方でサービスを構成しないでください。これにより、定義された管理ネットワーク上で IP アドレスが重複します。

4. [クライアントの表示] をクリックして現在の DHCP クライアントを表示し、[クライアントの クリア] をクリックして DHCP クライアントのリースを解放します。

SD-WAN アプライアンスで DHCP リレーサービスを有効にするには:

1. 「構成」>「アプライアンスの設定」>「ネットワークアダプタ」に移動します。[ネットワークアダプタ] ページで、[管理インターフェイス **DHCP** リレー] ペインを探します。
2. [**DHCP** リレーを有効にする] チェックボックスをオンにして、サービスを有効にします。**DHCP** サーバーの **IP** アドレスを 入力し、[設定の変更] をクリックして、アプライアンスを DHCP リレーエージェントとして使用し始めます。

> 注
>
> 高可用性（HA）用に構成されたアプライアンスで DHCP リレーサービスを使用する場合は、アクティブアプライアンスとスタンバイアプライアンスの両方でサービスを構成しないでください。これにより、定義された管理ネットワーク上で IP アドレスが重複します。



DHCP クライアントによる WAN リンク IP アドレスの学習

May 10, 2021

Citrix SD-WAN アプライアンスは、DHCP クライアントによる WAN リンクの IP アドレス学習をサポートします。この機能により、SD-WAN アプライアンスの導入に必要な手動設定の量が削減され、静的 IP アドレスを購入する必要がなくなり、ISP のコストが削減されます。SD-WAN アプライアンスは、信頼できないインターフェイス上の WAN リンクのダイナミック IP アドレスを取得できます。これにより、この機能を実行するために中間 WAN ルータが不要になります。

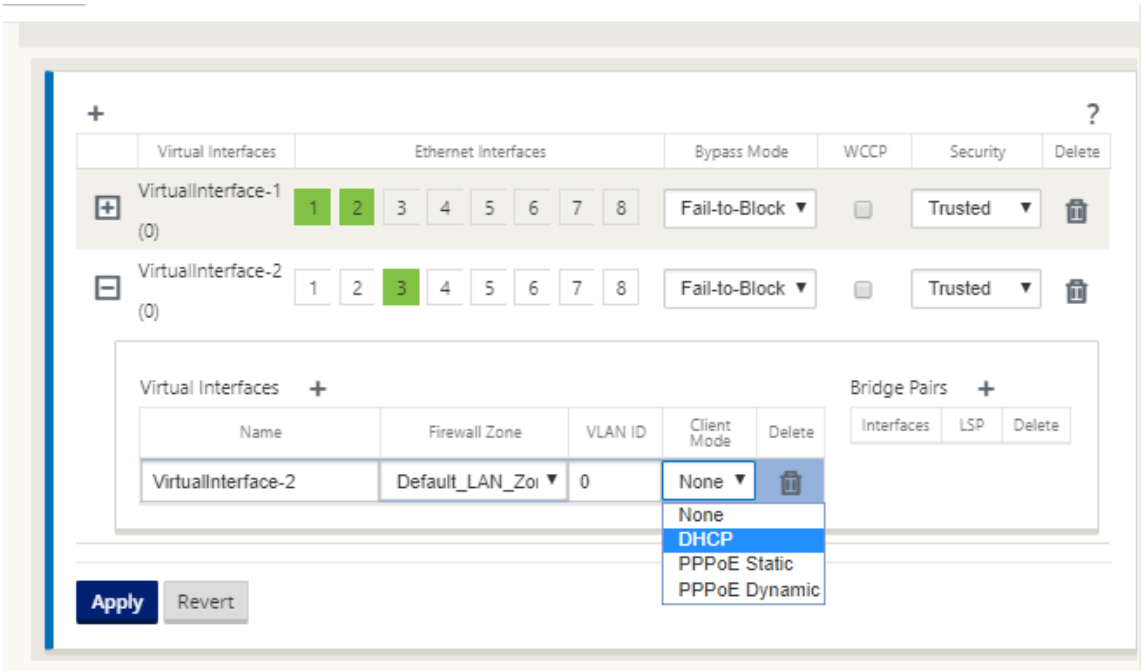
> 注
>
> - DHCP クライアントは、クライアントノードとして構成された信頼できないブリッジドインターフェイスに対してのみ構成できます。
> - データポート用 DHCP クライアントは、非 MCN サイトまたは非 RCN サイトでのみ有効にできます。

> - ワンアームまたはポリシーベースルーティング (PBR) 展開は、DHCP クライアント構成のサイトではサポートされません。
> - DHCP イベントは、クライアントの観点からのみログに記録され、DHCP サーバーログは生成されません。

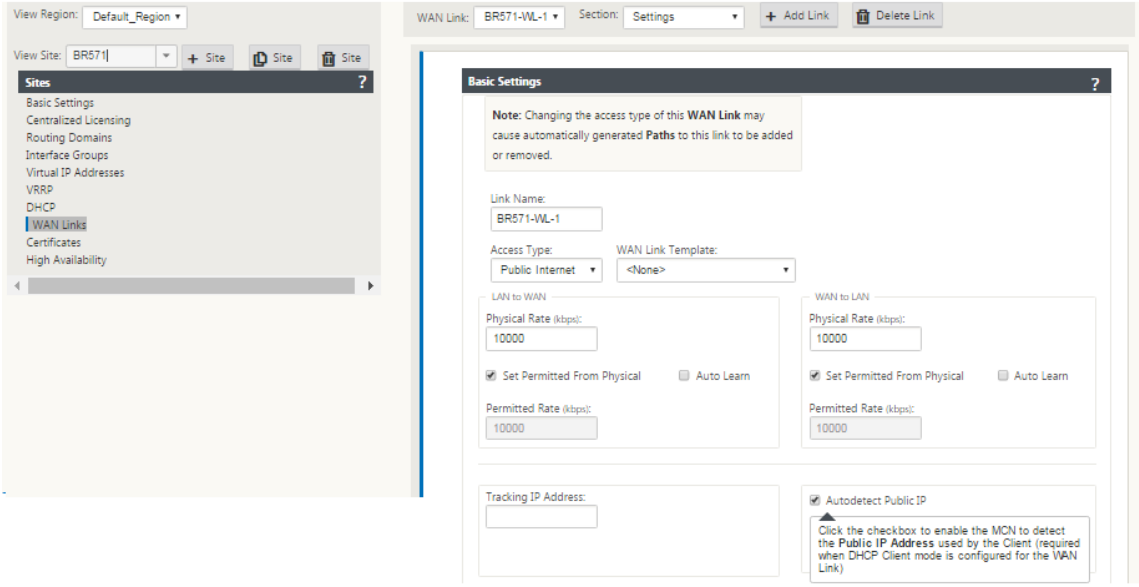
信頼できない仮想インターフェイスに DHCP を設定するには、次の手順を実行します。

1. 構成エディターで、[サイト] >[サイト名]> [インターフェイスグループ] **>** [仮想インターフェイス **] の順に選択します。

   > 注
   >
   > インターフェイスグループ内の物理インターフェイスは、単一のインターフェイス上の非ブリッジドペアである必要があります。



2. クライアントモードとして DHCP を選択します。
3. [**WAN** リンク] > [**[WAN** リンク名**]**] > [設定**]**> [基本設定**]** に移動します。
4. MCN でクライアントが使用する パブリック **IP** アドレスを検出できるようにするには、**[**パブリック **IP** の自動 検出] チェックボックスをオンにします。これは、WAN リンクに DHCP クライアントモードが設定されている場合に必要です。

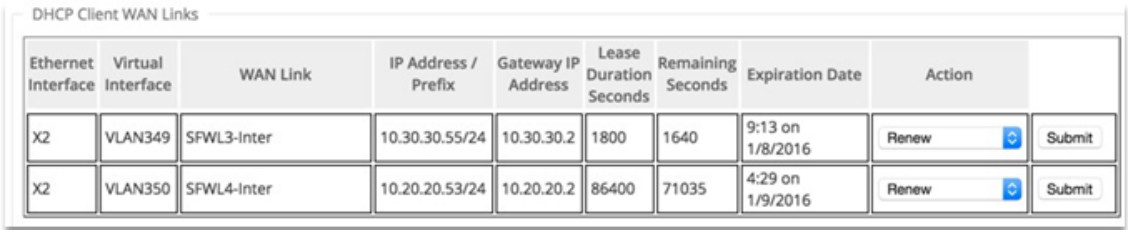


DHCP クライアントの **WAN** リンクの監視

ランタイム仮想 IP アドレス、サブネットマスク、およびゲートウェイの設定は、*SDWANVW_IP_learned.log* というログファイルに記録され、アーカイブされます。イベントは、動的仮想 IP が学習されたとき、解放されたとき、または期限切れになったとき、および学習されたゲートウェイまたは DHCP サーバとの通信に問題があるときに生成されます。または、アーカイブされたログファイルで重複した IP アドレスが検出された場合。サイトで重複した IP が検出された場合、動的仮想 IP アドレスは解放され、サイトのすべての仮想インターフェイスが一意の仮想 IP アドレスを取得するまで更新されます。

DHCP クライアントの WAN リンクを監視するには

1. SD-WAN アプライアンスの [フローの有効化/無効化/パージ] ページで、DHCP クライアント WAN リンクテーブルに、学習した IP のステータスが表示されます。
2. IP の更新を要求できます。これにより、リース時間が更新されます。[**Release Renew**] を選択することもできます。これにより、新しいリースで新しい IP アドレスが発行されます。



DHCP Client WAN Links

Ethernet Interface	Virtual Interface	WAN Link	IP Address / Prefix	Gateway IP Address	Lease Duration Seconds	Remaining Seconds	Expiration Date	Action	
X2	VLAN349	SFWL3-Inter	10.30.30.55/24	10.30.30.2	1800	1640	9:13 on 1/8/2016	Renew	Submit
X2	VLAN350	SFWL4-Inter	10.20.20.53/24	10.20.20.2	86400	71035	4:29 on 1/9/2016	Renew	Submit

ダイナミック **PAC** ファイルのカスタマイズ

May 10, 2021

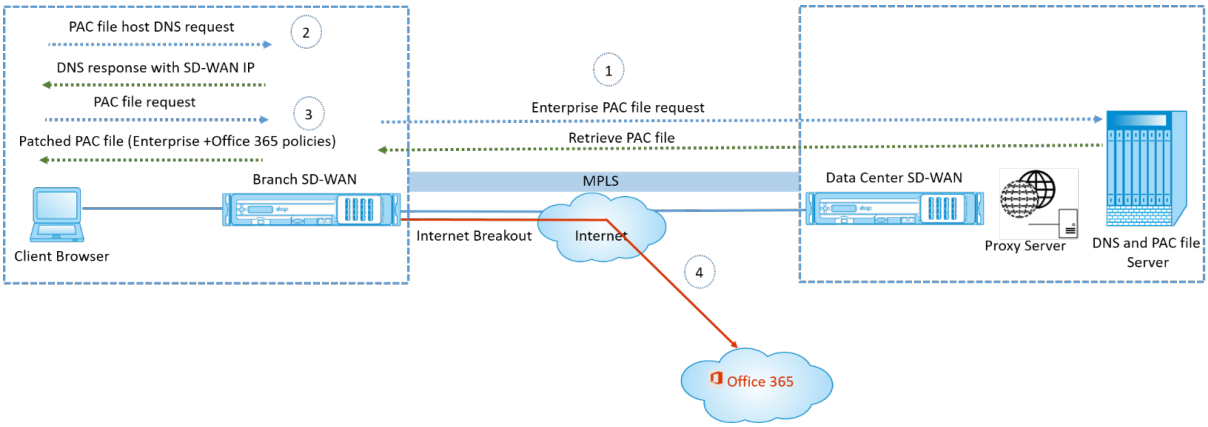
ミッションクリティカルな SaaS アプリケーションと分散型ワークフォースの企業導入の増加に伴い、レイテンシーと輻輳を低減することが非常に重要になります。レイテンシーと輻輳は、データセンターを通過するトラフィックをバックホールする従来の方法に固有のものです。Citrix SD-WAN では、Office 365 などの SaaS アプリケーションを直接インターネットから抜け出すことができます。詳しくは、「Office 365 の最適化」を参照してください。

企業展開で明示的な Web プロキシが設定されている場合、すべてのトラフィックが Web プロキシに誘導されるため、分類や直接インターネットブレイクアウトが難しくなります。解決策は、エンタープライズ PAC (Proxy Auto-Config) ファイルをカスタマイズすることによって、SaaS アプリケーショントラフィックがプロキシされないようにすることです。

Citrix SD-WAN 11.0 では、カスタム PAC ファイルを動的に生成して提供することにより、Office 365 アプリケーショントラフィックのプロキシバイパスとローカルインターネットブレークアウトが可能になります。PAC ファイルは、Web ブラウザーの要求が送信先に直接送信されるか、Web プロキシサーバーに送信されるかを定義する JavaScript 関数です。

PAC ファイルのカスタマイズの仕組み

理想的には、内部 Web サーバー上のエンタープライズネットワークホスト PAC ファイル、これらのプロキシ設定はグループポリシーを介して配布されます。クライアントブラウザは、エンタープライズ Web サーバから PAC ファイルを要求します。Citrix SD-WAN アプライアンスは、Office 365 ブレークアウトが有効なサイト用にカスタマイズされた PAC ファイルを提供します。



1. Citrix SD-WAN は、エンタープライズ Web サーバーからエンタープライズ PAC ファイルの最新のコピーを定期的に要求し、取得します。Citrix SD-WAN アプライアンスは、オフィス 365 の URL をエンタープライズ PAC ファイルにパッチします。エンタープライズ PAC ファイルには、Office 365 の URL にシームレスにパッチが適用されるプレースホルダ (SD-WAN 固有のタグ) が必要です。

2. クライアントブラウザは、エンタープライズ PAC ファイルホストの DNS 要求を生成します。Citrix SD-WAN は、プロキシ構成ファイル FQDN に対する要求を代行受信し、Citrix SD-WAN VIP に応答します。
3. クライアントブラウザが PAC ファイルを要求します。Citrix SD-WAN アプライアンスは、パッチが適用された PAC ファイルをローカルで提供します。PAC ファイルには、エンタープライズプロキシ構成と Office 365 の URL 除外ポリシーが含まれています。
4. Office 365 アプリケーションの要求を受信すると、Citrix SD-WAN アプライアンスは直接インターネットブレイクアウトを実行します。

前提条件

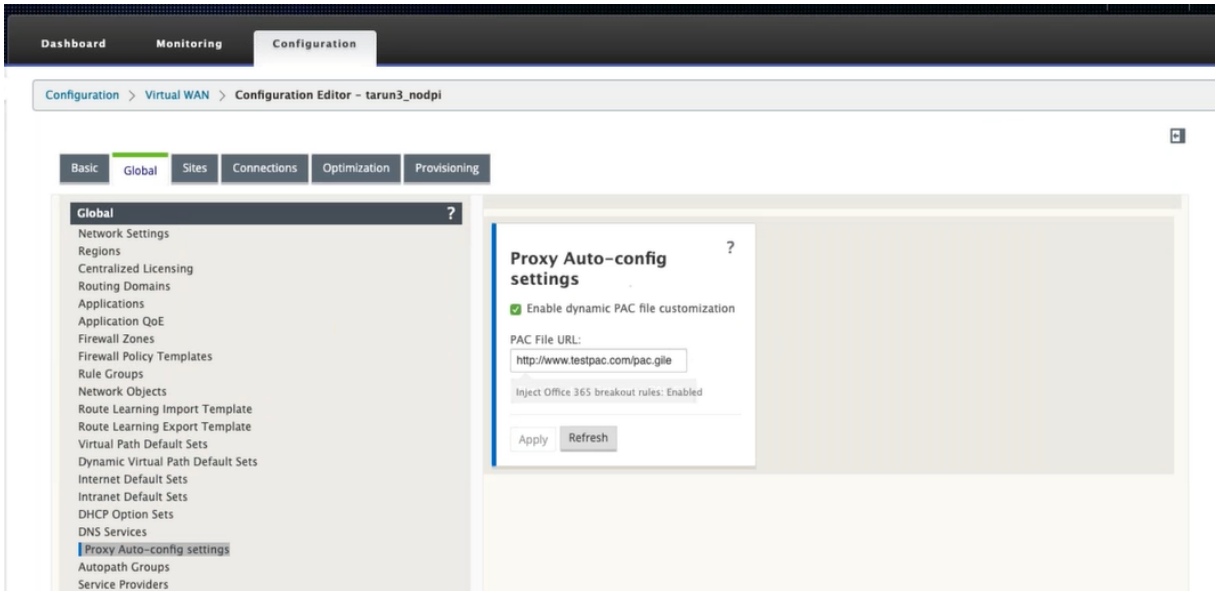
1. 企業は、PAC ファイルをホストする必要があります。
2. PAC ファイルには、プレースホルダ *SDWAN_TAG* または Office 365 の *URL* にパッチを適用するための *findproxyforurl* 関数が 1 つある必要があります。
3. PAC ファイルの URL は、IP ベースではなく、ドメインベースである必要があります。
4. PAC ファイルは、信頼されたアイデンティティ VIP を介してのみ提供されます。
5. Citrix SD-WAN アプライアンスは、管理インターフェイス経由でエンタープライズ PAC ファイルをダウンロードできる必要があ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

PAC ファイルのカスタマイズを設定する

PAC ファイルのカスタマイズは、グローバルに有効にすることも、サイトレベルで有効にすることもできます。

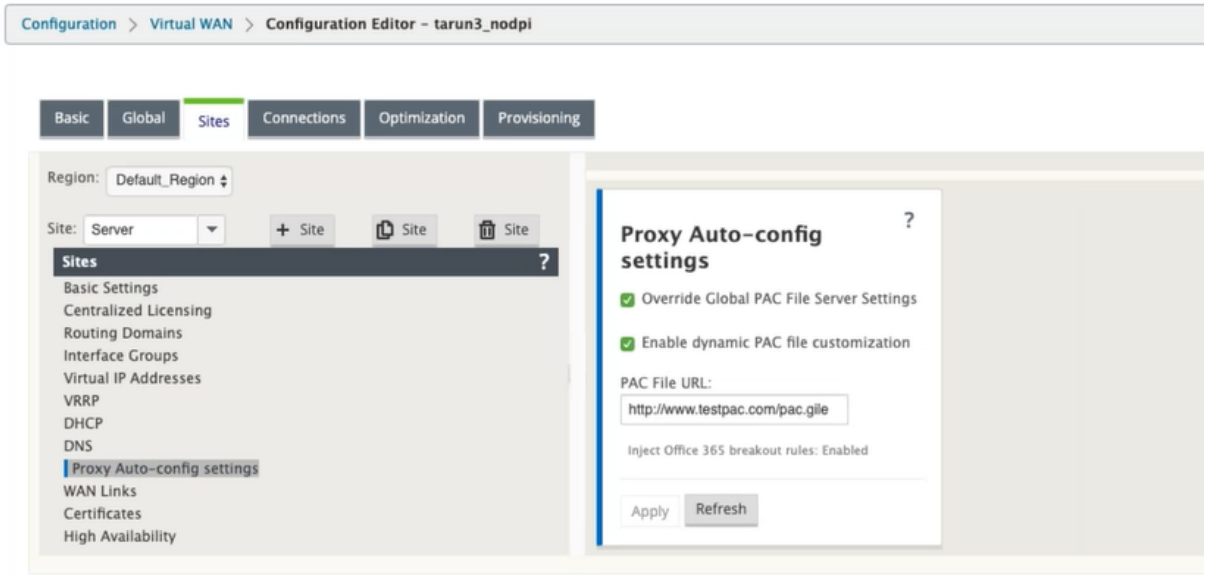
> 注**:**
>
> Office 365 ブレークアウトオプションは、PAC ファイルの動的カスタマイズを有効にする必要があります。Office 365 ブレークアウトを有効にする方法については、「Office 365 の最適化」を参照してください。

ダイナミック PAC ファイルのカスタマイズをすべてのサイトでグローバルに設定するには、設定エディタで [グローバル] > [プロキシ自動設定設定] に移動します。



[ダイナミック **PAC** ファイルのカスタマイズを有効にする] を選択します。[**PAC** ファイル **URL**] フィールドに、エンタープライズ PAC ファイルサーバの URL を入力します。Office 365 ブレークアウトルールは、エンタープライズ PAC ファイルに動的に修正されます。

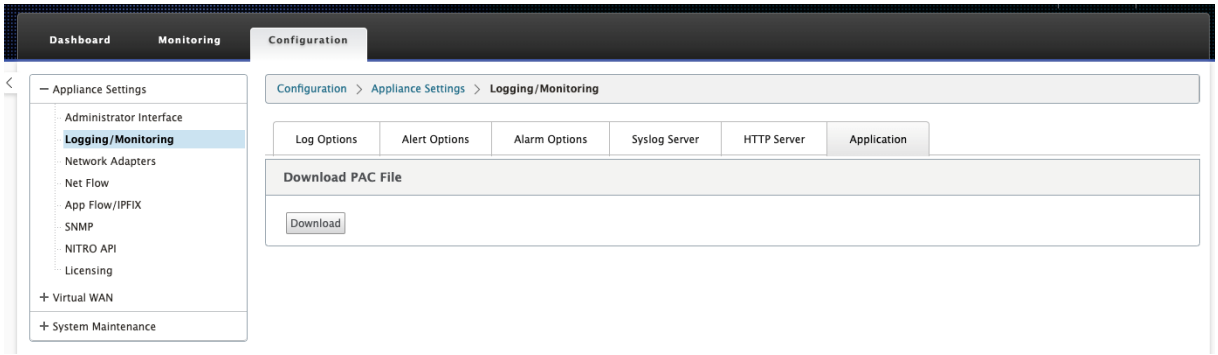
サイトの PAC ファイルの動的カスタマイズを構成するには、[サイト]> [サイト] > [プロキシ自動構成設定**]** に移動します。また、グローバル PAC ファイルサーバの設定を上書きし、別の PAC ファイルサーバの URL を指定することもできます。



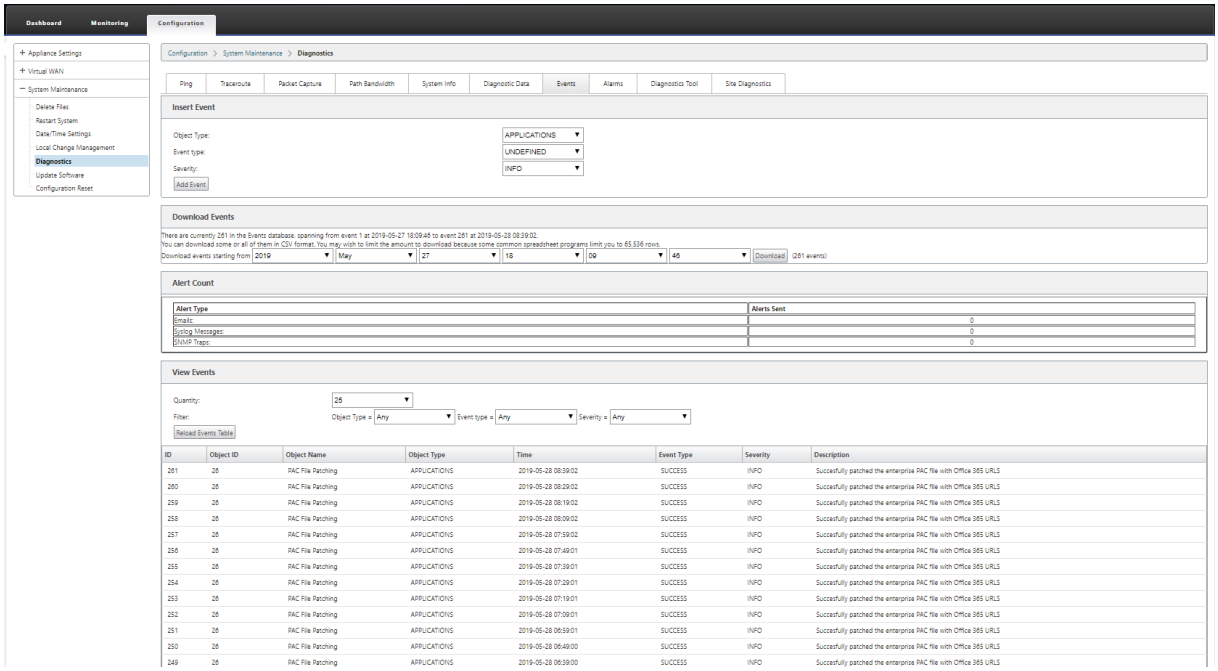
トラブルシューティング

カスタマイズした PAC ファイルは、Citrix SD-WAN アプライアンスからダウンロードしてトラブルシューティングを行うことができます。「構成」>「アプライアンスの設定」>「ログ/監視」>「アプリケーション」の順に選択し、「ダ

ウンロード」をクリックします。



PAC ファイルのパッチ適用のステータスは、［イベント］セクションで表示し、［構成］>［システムメンテナンス］>［診断］の順に選択し、［イベント］タブをクリックします。



制限事項

- HTTPS PAC ファイルサーバー要求はサポートされていません。
- ルーティングドメインまたはセキュリティゾーンの PAC ファイルなど、ネットワーク内の複数の PAC ファイルはサポートされません。
- Citrix SD-WAN 上の PAC ファイルをゼロから生成することはできません。
- DHCP を介した WPAD はサポートされていません。

GRE トンネル

May 10, 2021

SD-WAN GRE トンネル設定を使用すると、LAN 上の GRE トンネルを終了するように SD-WAN アプライアンスを設定できます。サイトを GRE トンネル終端ノードとして設定しない場合は、この手順を省略して、MCN サイトの WAN リンクの設定に進んでください。

GRE トンネルを設定するには、次の手順を実行します。

新しい MCN サイト の [Sites] ビューで続行し、[**GRE Tun** nels] ラベルの左側にある [**+**] をクリックします。新しいサイトの **GRE** トンネル テーブルが開きます。詳細については、GRE のトピックを参照してください。

「MCN サイトへの GRE トンネルの設定」を参照してください。

「ブランチサイトの GRE トンネルの設定」を参照してください。

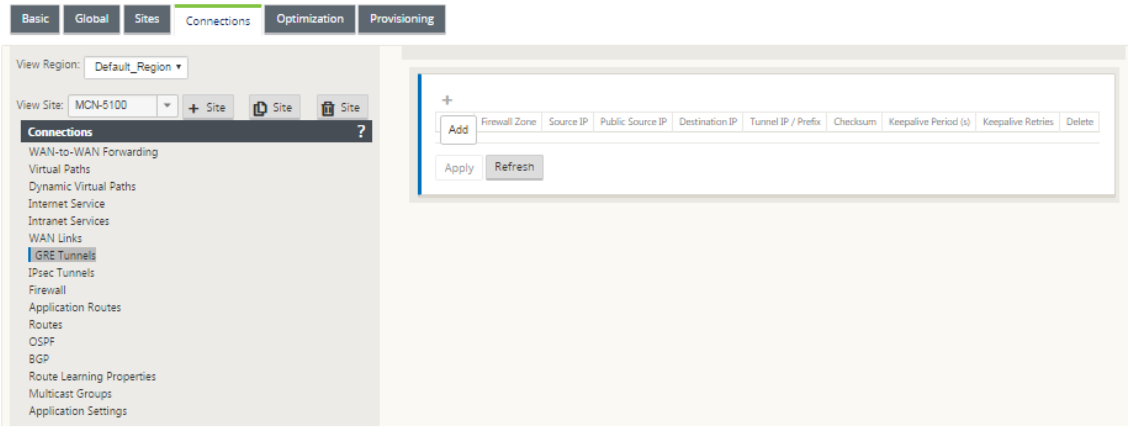
MCN サイトの GRE トンネルの設定（任意）

November 8, 2021

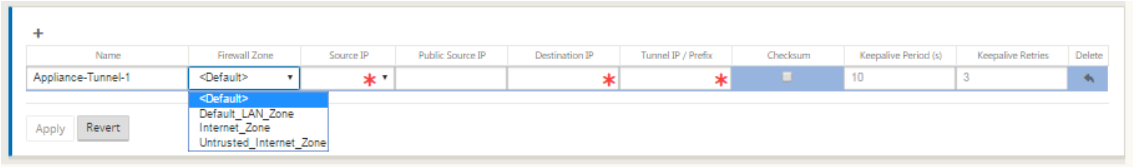
SD-WAN GRE トンネル設定では、LAN 上の GRE トンネルを終了するように SD-WAN アプライアンスを設定できます。このサイトを GRE トンネル終端ノードとして設定しない場合は、この手順をスキップして、MCN サイトの WAN リンクの設定のセクションに進んでください。

GRE トンネルを設定するには、次の手順を実行します。

1. 新しい MCN サイトの [接続] タブで続行し、[**GRE** トンネル] をクリックします。これにより、新しいサイトの **GRE** トンネル テーブルが開きます。



2. **GRE** トンネルの右側にある [**+**] をクリックします。これにより、新しい空の GRE トンネルエントリがテーブルに追加され、編集用に開きます。

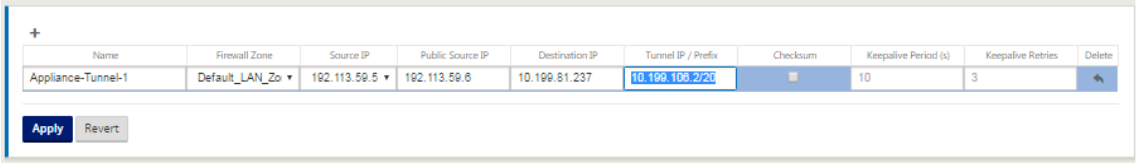


3. GRE トンネルの設定を行います。

   以下のコマンドを実行します。

   - [**Name**]: 新しい GRE トンネルの名前を入力するか、デフォルトを受け入れます。デフォルトでは、次の命名形式が使用されます。
   - **Appliance-Tunnel-** <number>-<*number*> は、このサイトに設定されている GRE トンネルの数で、1 ずつ増加します。
   - ファイアウォールゾーン -GRE トンネルのファイルゾーンを選択します。
   - [**Source IP**]: このフィールドのドロップダウンメニューからトンネルの送信元 IP アドレスを選択します。メニューオプションは、このサイトに対して構成されている仮想インターフェイスのリストです。GRE トンネルを設定する前に、少なくとも 1 つの仮想インターフェイスを設定してください。手順については、「MCN サイトの仮想インターフェイスグループの構成」および「MCN サイトの仮想IP アドレスの設定」を参照してください。
     - **Public Source IP**: GRE トンネル内のパケットの送信元アドレスとして使用する IP アドレスを入力します。送信元 IP アドレスは、GRE トンネルの始点です。
     - 宛先 **IP** —ホストの宛先として使用する IP アドレスを入力します。宛先 IP アドレスは、GRE トンネルのエンドポイントです。
     - [**Tunnel IP/Prefix**]: GRE トンネルインターフェイスに使用する IP アドレスとプレフィクスを入力します。
     - [**Checksum**]: トンネル GRE ヘッダーのチェックサムを有効にするには、これを選択します。
     - [**Keepalive PerioD**]: キープア ライブメッセージ間の待機時間（秒単位）を入力します。0 に設定した場合、キープアライブパケットは送信されませんが、トンネルはアップしたままになります。デフォルトは 10 です。
     - [**Keepalive Retries**] —仮想 WAN アプライアンスがトンネルをダウンさせるまでに試行するキープアライブの再試行回数を入力します。デフォルトは 3 です。

4. [**Apply**] をクリックします。これにより、設定が送信され、新しい GRE トンネルがテーブルに追加されます。



5. さらに多くの GRE トンネルを設定するには、**GRE** トンネルの右側にある [**+**] をクリックし、前の手順に従って進みます。

次のステップは、MCN サイトの WAN リンクを設定することです。

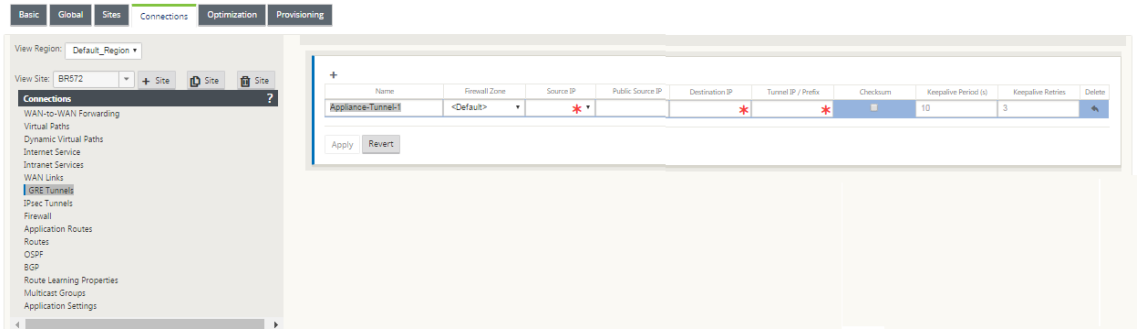
ブランチサイトの **GRE** トンネルの設定

November 8, 2021

仮想 WAN LAN GRE トンネル設定を使用すると、仮想 WAN アプライアンスを構成して、LAN 上の GRE トンネルを終了させることができます。このブランチサイトを LAN GRE トンネル終端ノードとして設定しない場合は、この手順をスキップして、ブランチサイトの WAN リンクの設定の項に進んでください。

ブランチサイトの LAN GRE トンネルを設定するには、次の手順を実行します。

1. 新しいブランチサイトの接続ビューで続行し、[**GRE Tunnels**] をクリックします。新しいサイトの **GRE** トンネルビューが開きます。
2. [**GRE** トンネル] の右にある [**+**] をクリックします。これにより、新しい空の GRE トンネルエントリがテーブルに追加され、編集用に開きます。

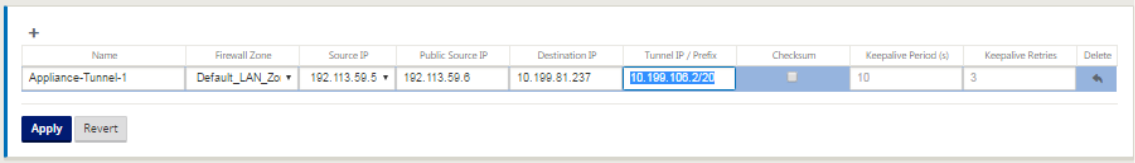


3. GRE トンネルの設定を行います。以下のコマンドを実行します。

- [**Name**]: 新しい GRE トンネルの名前を入力するか、デフォルトを受け入れます。デフォルトでは、次の命名形式が使用されます。
- **Appliance-Tunnel-**: <number><*number*> は、このサイトに設定された GRE トンネルの数を 1 増分した数です。
- ファイアウォールゾーン -GRE トンネルのファイアウォールゾーンを選択します。
- [**Source IP**]: このフィールドのドロップダウンメニューからトンネルの送信元 IP アドレスを選択します。メニューオプションは、このサイト用に構成した仮想 IP アドレスのリストです。LAN GRE トンネルを設定する前に、少なくとも 1 つの仮想インターフェイスと 1 つの仮想 IP アドレスを設定してください。手順については、「ブランチサイトの仮想インターフェイスグループの設定」および「ブランチサイトの仮想IP アドレスの設定」の項を参照してください。

- **Public Source IP**： GRE トンネル内のパケットの送信元アドレスとして使用する IP アドレスを入力します。送信元 IP アドレスは、GRE トンネルの始点です。
- 宛先 **IP** —ホストの宛先として使用する IP アドレスを入力します。宛先 IP アドレスは、GRE トンネルのエンドポイントです。
- [**Tunnel IP/Prefix**]： GRE トンネルインターフェイスに使用する IP アドレスとプレフィクスを入力します。
- [**Checksum**]： トンネル GRE ヘッダーのチェックサムを有効にするには、これを選択します。
- [**Keepalive Per** itods]： キープアライブメッセージ間の待機時間（秒単位）を入力します。0 に設定した場合、キープアライブパケットは送信されませんが、トンネルはアップしたままになります。デフォルトは 10 です。
- [**Keepalive Retries**] —仮想 WAN アプライアンスがトンネルをダウンさせるまでに試行するキープアライブの再試行回数を入力します。デフォルトは 3 です。

1. [**Apply**] をクリックします。これにより、設定が送信され、新しい GRE トンネルエントリがテーブルに追加されます。



2. さらに GRE トンネルを設定するには、[**GRE Tunnels**] ラベルの右側にある [**+**] をクリックし、前の手順に進みます。

次のステップは、ブランチサイトの WAN リンクを設定することです。

帯域内およびバックアップ管理

May 10, 2021

帯域内管理

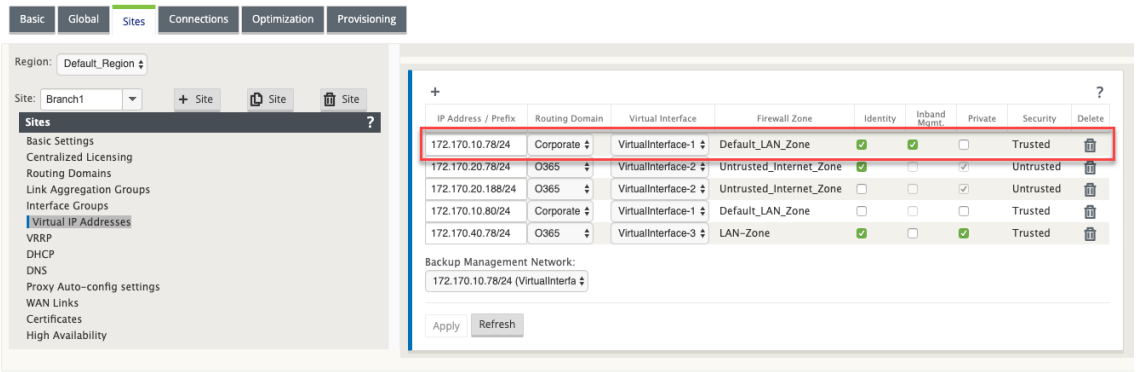
Citrix SD-WAN では、帯域外管理と帯域内管理の 2 つの方法で SD-WAN アプライアンスを管理できます。アウトオブバンド管理では、管理トラフィックだけを伝送する管理用に予約されたポートを使用して管理 IP を作成できます。インバンド管理では、SD-WAN データポートを管理に使用できます。SD-WAN データポートは、データトラフィックと管理トラフィックの両方を伝送します。追加の管理パスを設定する必要はありません。

インバンド管理では、仮想 IP アドレスが Web UI や SSH などの管理サービスに接続できます。IP サービスに使用できるように有効になっている複数の信頼できるインターフェイスで、インバンド管理を有効にできます。管理 IP とインバンド仮想 IP を使用して、Web UI と SSH にアクセスできます。

仮想 IP で帯域内管理を有効にするには、次の手順を実行します。

1. 構成エディタで、[サイト] > [仮想 **IP** アドレス] に移動します。
2. 帯域内管理 を有効にする仮想 IP の [帯域内管理] を選択します。

> 注:
>
> インターフェイスは、セキュリティタイプ「信頼済み」および「**ID** 」が有効である必要があります。



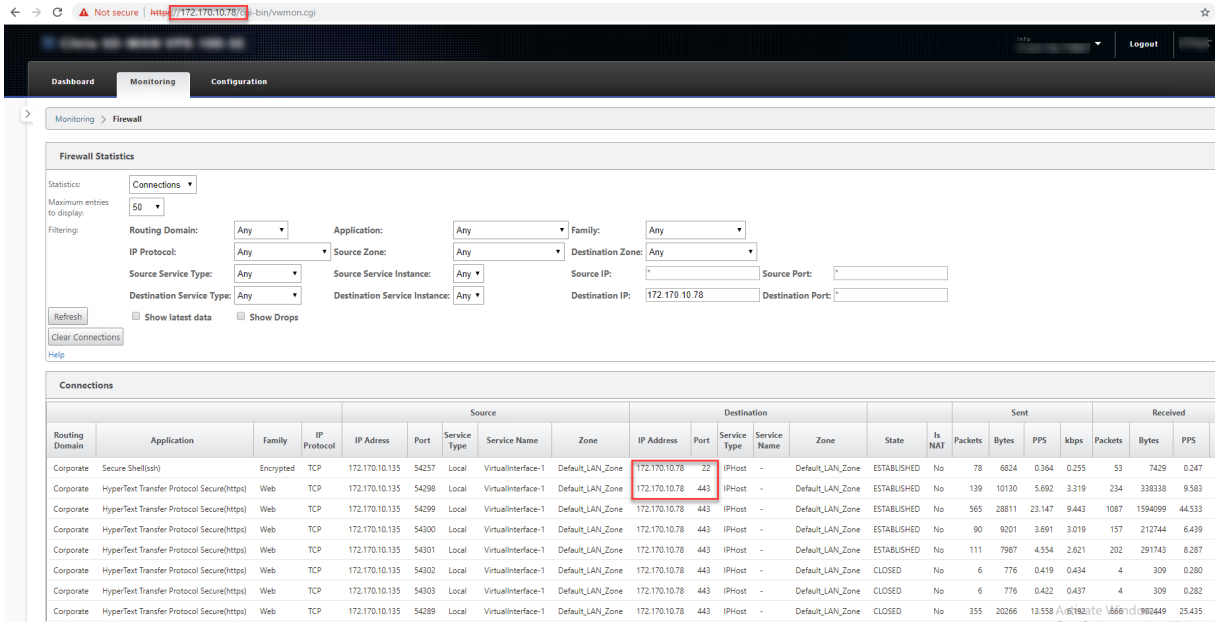
3. [適用] をクリックします。

仮想 IP アドレスの設定手順の詳細については、仮想 IP の設定方法を参照してください。

帯域内管理のモニタリング

前の例では、172.170.10.78 仮想 IP でインバンド管理を有効にしました。この IP を使用して、Web UI と SSH にアクセスできます。

Web UI で、[監視] > [ファイアウォール] に移動します。ポート 22 および 443 の仮想 IP を使用してアクセスする SSH および Web UI が [宛先 **IP** アドレス] 列に表示されます。



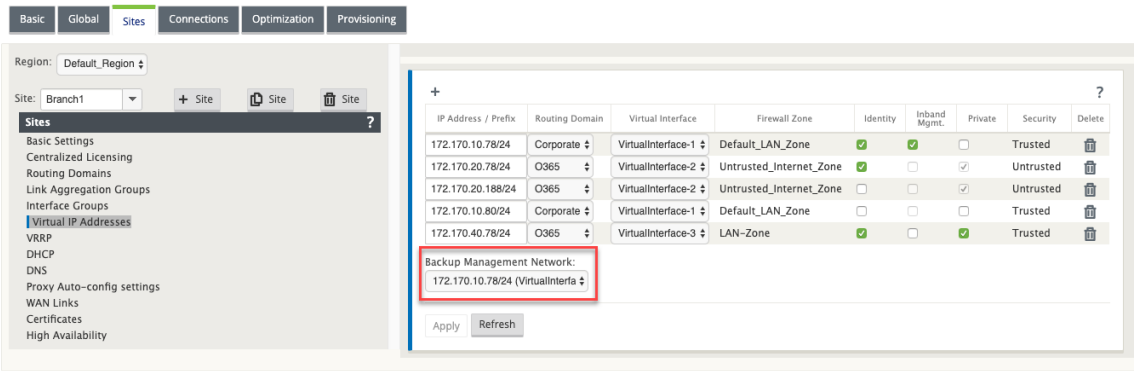
バックアップ管理ネットワーク

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

> 注:
>
> サイトに 1 つのルーティングドメインで構成されたインターネットサービスがある場合、既定では、ID が有効な信頼できるインターフェイスがバックアップ管理ネットワークとして選択されます。

仮想 IP をバックアップ管理ネットワークとして選択するには

1. 構成エディタで、[サイト] > [仮想 **IP** アドレス] に移動します。
2. バックアップ管理ネットワークとして仮想 IP アドレスを選択します。



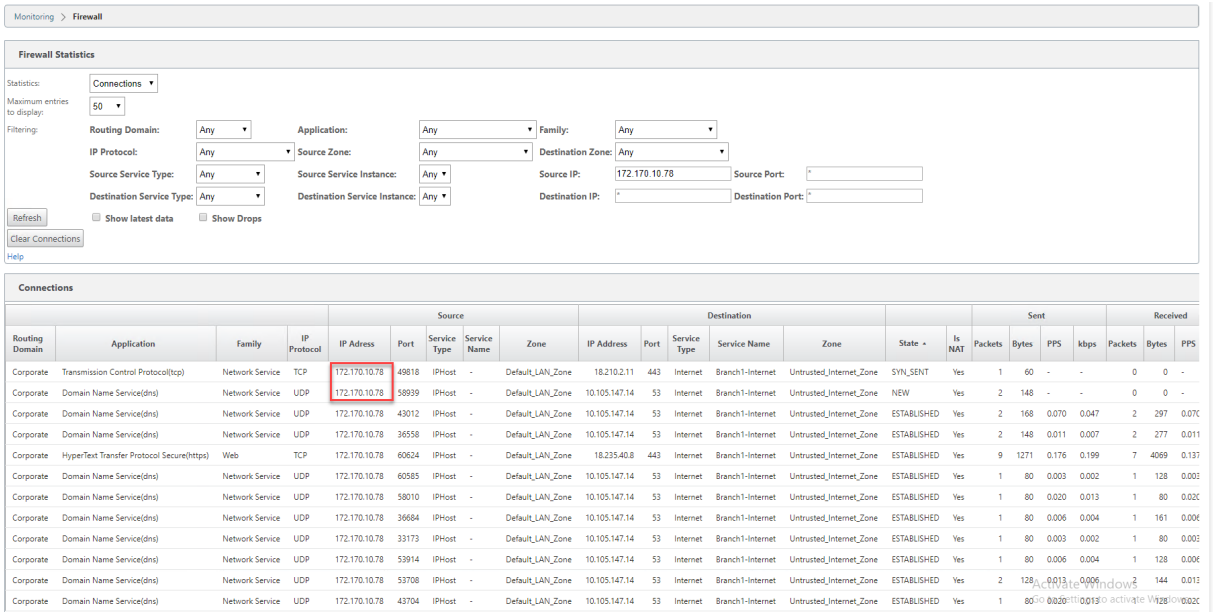
3. ［適用］をクリックします。

仮想 IP アドレスの設定手順の詳細については、「構成」の「仮想 **IP** アドレスの構成方法」セクションを参照してください。

バックアップ管理の監視

前の例では、バックアップ管理ネットワークとして 172.170.10.78 の仮想 IP を選択しています。管理 IP アドレスがデフォルト Gateway で設定されていない場合は、この IP を使用して Web UI と SSH にアクセスできます。

Web UI で、[監視] > [ファイアウォール] に移動します。この仮想 IP アドレスは、SSH および Web UI アクセスの送信元 IP アドレスとして確認できます。



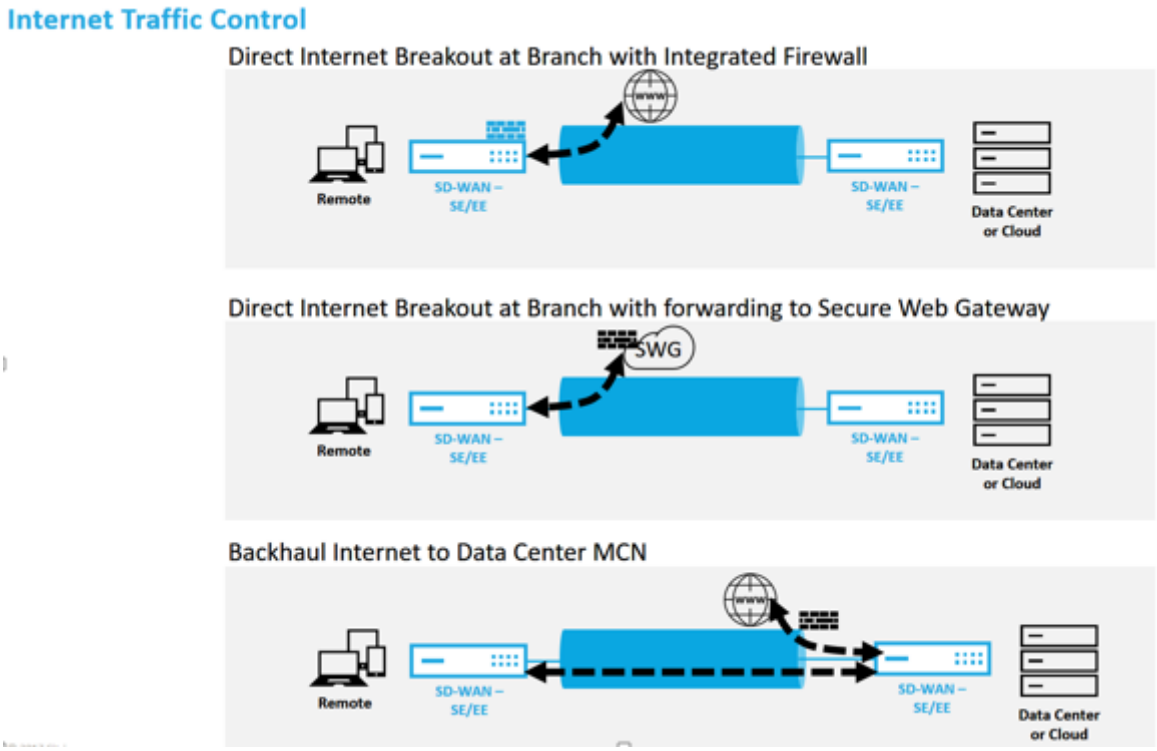
インターネットアクセス

May 10, 2021

インターネットサービスは、エンドユーザーサイトとパブリックインターネット上のサイト間のトラフィックに使用されます。インターネットサービストラフィックは SD-WAN によってカプセル化されず、仮想パスサービスを通して配信されるトラフィックと同じ機能を持ちません。ただし、SD-WAN でこのトラフィックを分類し、考慮することが重要です。インターネットサービスとして識別されるトラフィックにより、管理者が設定した構成に従って、仮想パスおよびイントラネットトラフィックを介して配信されるトラフィックに対するインターネットトラフィックのレート制限によって、SD-WAN のリンク帯域幅をアクティブに管理できるようになります。SD-WAN には、帯域幅の Provisioning 機能に加えて、複数のインターネット WAN リンクを使用してインターネットサービス経由で配信されるトラフィックの負荷分散機能が追加されています。また、プライマリまたはセカンダリ構成でインターネット WAN リンクを使用することもできます。

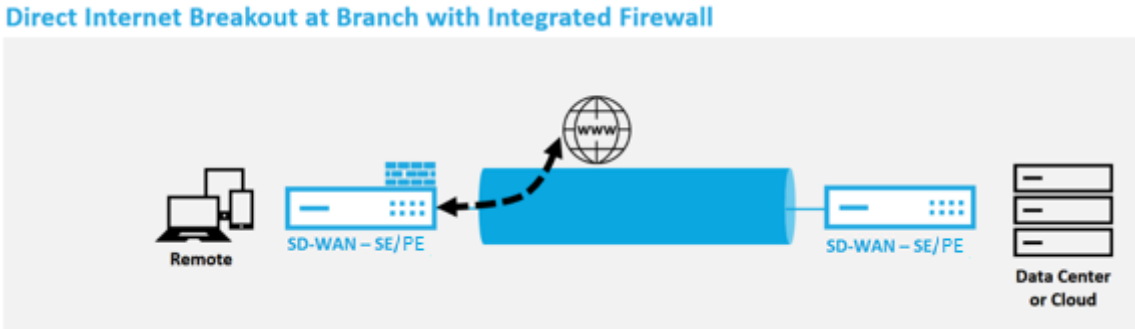
SD-WAN アプライアンスの Internet Service を使用したインターネットトラフィック制御は、次の展開モードで構成できます。

- 統合ファイアウォールを使用したブランチでの直接インターネットブレイクアウト
- Secure Web Gateway への支店転送での直接インターネットブレイクアウト
- インターネットからデータセンター MCN へのバックホール



統合ファイアウォールを使用したブランチでの直接インターネットブレイクアウト

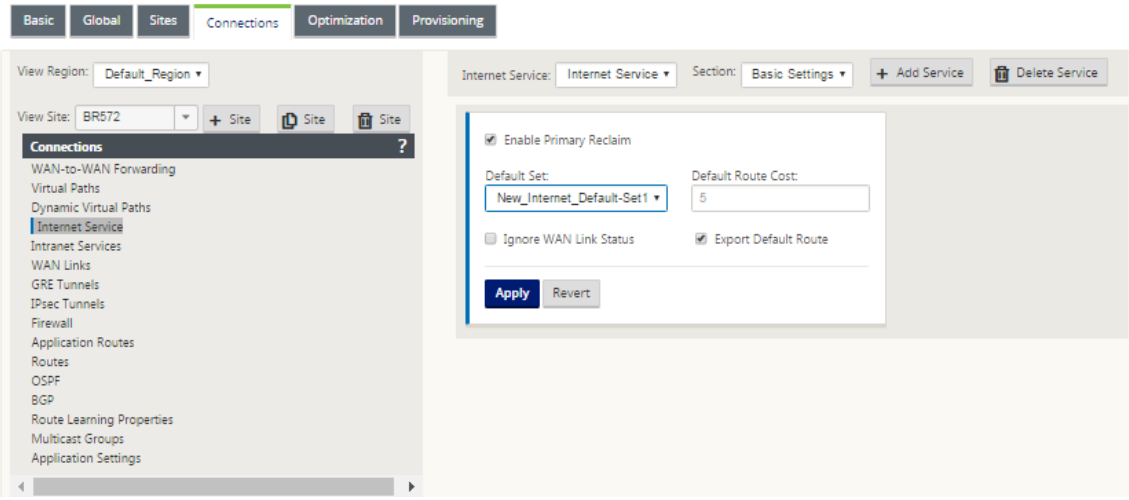
May 10, 2021



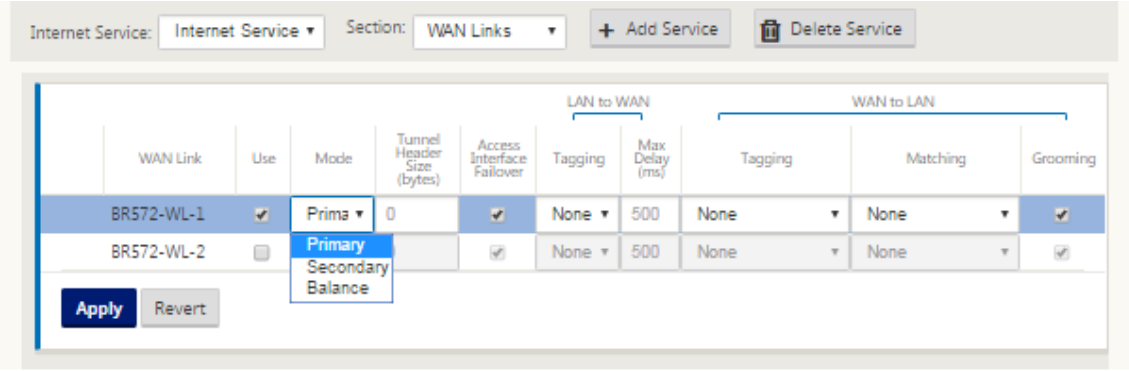
任意のサイト (クライアントノードまたは MCN) でインターネットサービスを有効にするには、次の手順を実行します。

1. 構成エディタで、[接続] タイルに移動します。追加 (+) アイコンをクリックして、そのサイトのインターネットサービスを追加します。サイトごとに作成できるインターネットサービスは 1 つだけです。

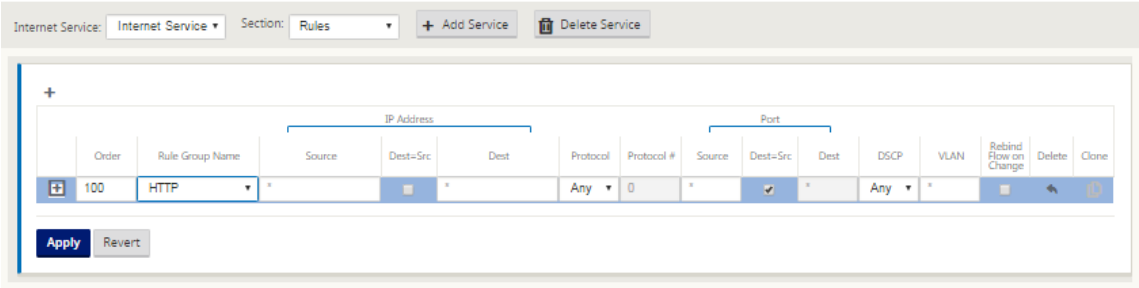
2. [インターネットサービスの 基本設定] には、WAN リンクが使用できないときにインターネットサービスをどのように動作させるかに関するオプションがいくつかあります。インターネットデフォルトセットは、インターネットサービスを有効にした構成内の任意のノードに適用できる規則のセットを使用して、グローバルタイルで定義できます。これにより、各ノードを個別に構成することなく、インターネットサービスの管理を一元的に制御できます。



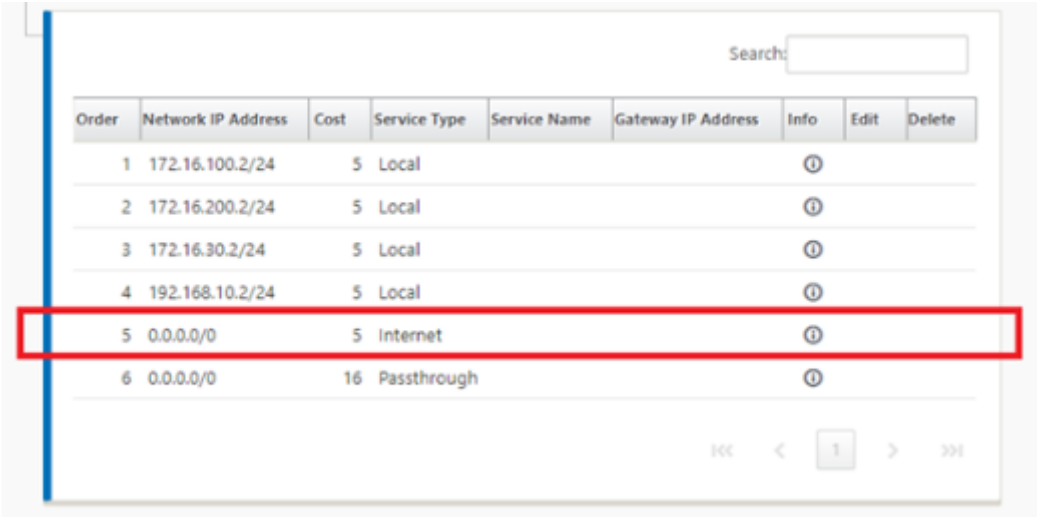
3. [インターネットサービス WAN リンク] ノードでは、[サイト] タイルに構築された WAN リンクを使用して、インターネットトラフィックに使用する WAN リンクを選択できます。他のオプションに加えて、[プライマリ]、[セカンダリ]、[バランス] の各モードも使用できます。これにより、管理者は利用可能な WAN リンクを同時に使用することも、アクティブ/パッシブ役割で使用することもできます。



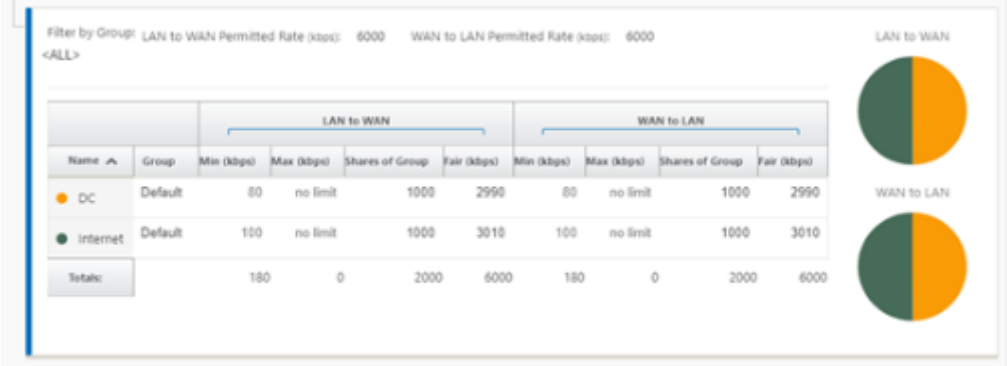
4. サイトノード固有のルールが使用可能で、グローバルデフォルトセットで構成された一般設定を一意に上書きして、各サイトのカスタマイズ機能を有効にします。モードには、特定の WAN リンクを介した目的の配信や、フィルタリングされたトラフィックのパススルーまたは廃棄を可能にするオーバーライドサービスとしての配信が含まれます。



ノードに対してインターネットサービスが作成されると、その特定のノードのルートテーブルが自動的に更新され、サービスタイプに等しいインターネット、ルートコストが 5 のルート 0.0.0.0/0 ルートで更新されます。そうでない場合は、サービスタイプとしてパススルーを使用したコスト 16 のデフォルトルートが制定され、インターネットトラフィックは配線するアンダーレイネットワークに引き渡される。



サイトノードでインターネットサービスを有効にすると、[プロビジョニング] タイルが使用可能になります。これにより、WAN リンクを使用するさまざまなサービス間で、WAN リンクの帯域幅の双方向 (LAN から WAN または WAN から LAN へ) 分散が可能になります。[Services] セクションでは、帯域幅割り当てをさらに微調整できます。さらに、フェアシェアを有効にして、フェア配布が制定される前に、すべてのサービスが最小の予約帯域幅を受け取ることができます。



インターネットサービスは、Citrix SD-WAN でサポートされているさまざまな展開モードで使用できます。

- インライン展開モード（SD-WAN オーバーレイ）

Citrix SD-WAN は、どのネットワークでもオーバーレイソリューションとして導入できます。オーバーレイソリューションとして、SD-WAN は通常、既存のエッジルータやファイアウォールの背後に展開されます。SD-WAN がネットワークファイアウォールの背後に展開されている場合、インターフェイスを信頼できるものとして構成し、インターネットトラフィックをインターネット Gateway としてファイアウォールに配信できます。

- エッジモードまたはゲートウェイモード

Citrix SD-WAN をエッジデバイスとして展開し、既存のエッジルーターやファイアウォールデバイスを置き換えることができます。オンボードファイアウォール機能により、SD-WAN は直接インターネット接続からネットワークを保護できます。このモードでは、パブリックインターネットリンクに接続されているインターフェイスが信頼できないように設定され、暗号化が強制的に有効になり、ファイアウォールとダイナミック NAT 機能が有効になり、ネットワークを保護します。

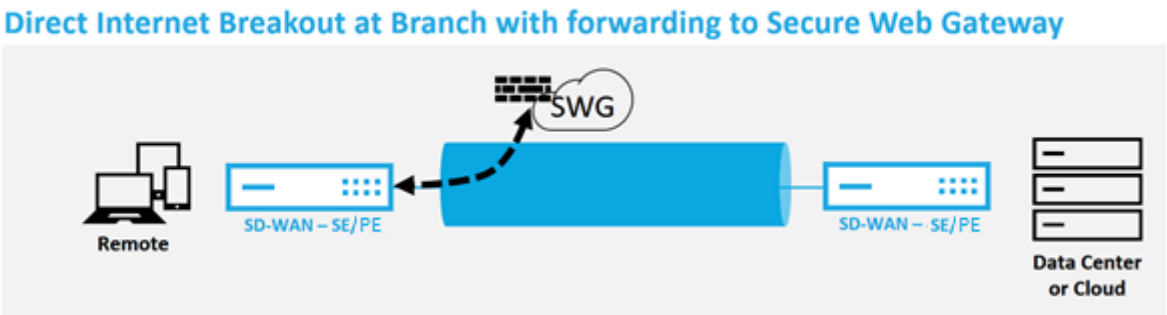
Secure Web Gateway による直接インターネットアクセス

November 8, 2021

トラフィックを保護し、ポリシーを適用するために、企業は多くの場合、MPLS リンクを使用して、ブランチトラフィックを企業のデータセンターにバックホールします。データセンターは、セキュリティポリシーを適用し、セキュリティアプライアンスを介してトラフィックをフィルタリングしてマルウェアを検出し、トラフィックを ISP 経由でルーティングします。プライベート MPLS リンクを介したこのようなバックホールは高価です。また、レイテンシーが大きくなるため、ブランチサイトでのユーザーエクスペリエンスが低下します。また、ユーザーがセキュリティ制御をバイパスするリスクもあります。

バックホールに代わる方法として、支店にセキュリティアプライアンスを追加する方法があります。ただし、複数のアプライアンスをインストールして、サイト全体で一貫したポリシーを維持するにつれて、コストと複雑さが増大します。最も重要なのは、支店の数が多い場合、コスト管理は実用的ではありません。

もう 1 つの方法は、コスト、複雑さ、または遅延を追加せずにセキュリティを強化することです。これは、Citrix SD-WAN を使用してすべての支店のインターネットトラフィックを Secure Web Gateway Service にルーティングすることです。サードパーティの Secure Web Gateway Service を使用すると、接続されているすべてのネットワークで使用できる、きめ細かな一元的なセキュリティポリシー作成が可能になります。ポリシーは、ユーザーがデータセンターにいるかブランチサイトにいるかにかかわらず、一貫して適用されます。Secure Web Gateway ソリューションはクラウドベースであるため、高価なセキュリティアプライアンスをネットワークに追加する必要はありません。



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

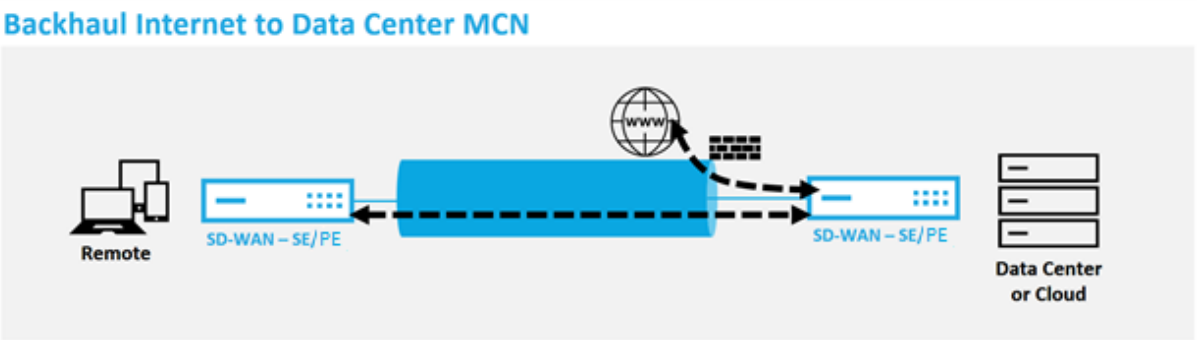
- Zscaler
- フォースポイント
- パロ・アルト
- Citrix Secure Internet Access

バックホールインターネット

May 10, 2021

Citrix SD-WAN ソリューションでは、インターネットトラフィックを MCN サイトまたは他のブランチサイトにバックホールできます。バックホールは、インターネット宛てのトラフィックが、インターネットにアクセスできる別の定義済みサイトを介して送り返されることを示します。セキュリティ上の問題やアンダーレイネットワークトポロジが原因で、インターネットに直接アクセスできないネットワークに便利です。たとえば、内蔵の SD-WAN ファイアウォールがそのサイトのセキュリティ要件を満たしていない外部ファイアウォールがないリモートサイトが挙げられます。環境によっては、データセンターで強化された DMZ を経由するすべてのリモートサイトのインターネットトラフィックをバックホールすることが最善のアプローチである場合があります。ただし、この方法では、次の点に注意しなければならない制限があり、アンダーレイ WAN リンクのサイズが適切になります。

- インターネットトラフィックのバックホールは、インターネット接続にレイテンシーを増大させ、データセンターのブランチサイトの距離に応じて変化します。
- インターネットトラフィックのバックホールは、仮想パスの帯域幅を消費し、WAN リンクのサイジングに考慮されます。
- インターネットトラフィックのバックホールは、データセンターでインターネット WAN リンクを過剰にサブスクライブする可能性があります。



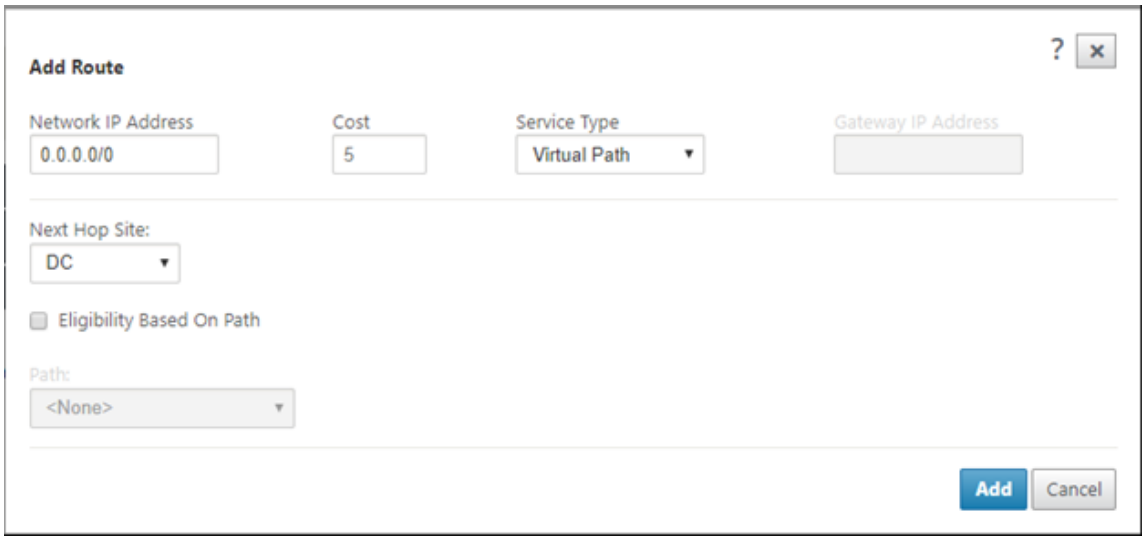
すべての Citrix SD-WAN デバイスは、1 つのデバイスに最大 8 つの異なるインターネット WAN リンクを終了できます。集約された WAN リンクのライセンスされたスループット機能は、Citrix SD-WAN のデータシートに各アプライアンスごとに一覧表示されます。

Citrix SD-WAN ソリューションは、次の構成でインターネットトラフィックのバックホールをサポートします。

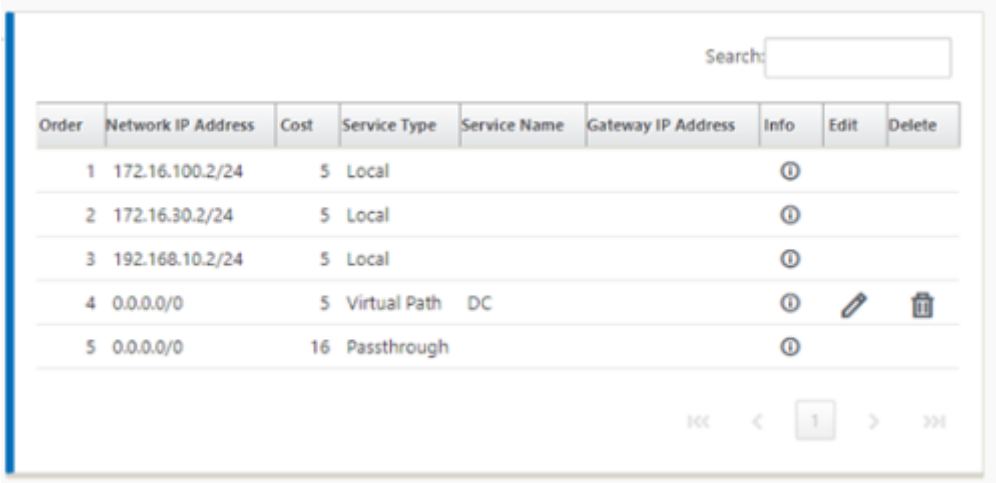
1. MCN サイトノード、またはインターネットサービスが必要なその他のサイトノートでインターネットサービスを有効にします。

   > 注
   >
   > 他のすべてのサイトが WAN から WAN への転送グループにある場合は、インターネットサービスとエクスポートルートを有効にします。

2. インターネットトラフィックがバックホールされるブランチノードで、0.0.0.0/0 ルートを手動で追加して、すべてのデフォルトトラフィックを仮想パスサービスに送信します。ネクストホップは MCN（中間サイト）として表されます。



3. ブランチサイトのルートテーブルに、目的のバックホールルート以外のトラフィックを誘導する他の低コストのルートがないことを確認します。

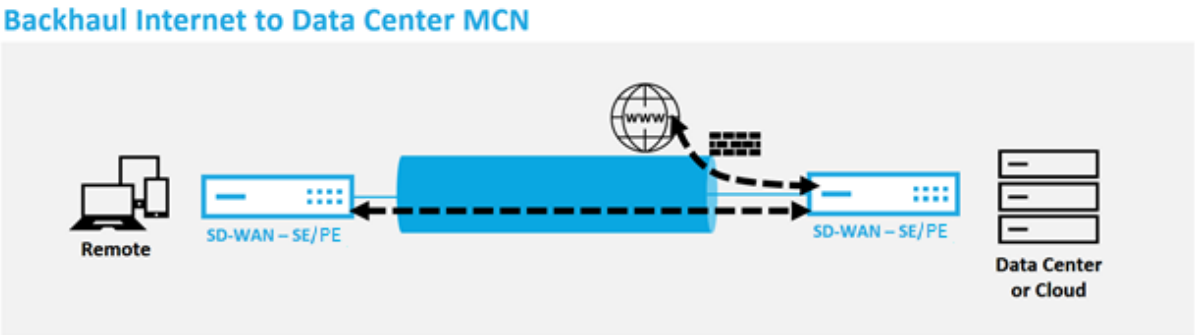


ヘアピンモード

May 10, 2021

ヘアピンの展開では、ローカルインターネットサービスが使用できない場合や、トラフィックが遅い場合に、バックホールまたはヘアピンを介したインターネットアクセスにリモートハブサイトを実装できます。特定のサイトからのバックホールを許可することで、クライアントサイト間に高帯域幅ルーティングを適用できます。

非 WAN から WAN 転送サイトへのヘアピン展開の目的は、より効率的な展開プロセスを提供し、技術的な実装を合理化することです。必要に応じて、リモートハブサイトを使用してインターネットアクセスでき、フローを仮想パス経由で SD-WAN ネットワークにルーティングできます。



たとえば、複数の SD-WAN サイト A と B を持つ管理者が、サイト A のインターネットサービスが不十分な場合を考えます。サイト B には使用可能なインターネットサービスがあり、サイト A からサイト B へのトラフィックだけをバックホールします。戦略的に重み付けされたルートコストや、トラフィックを受信すべきでないサイトへの伝播を複雑にすることなく、これを実現できます。

また、ルートテーブルは、Hairpin デプロイメントのすべてのサイトで共有されるわけではありません。たとえば、サイト A とサイト B の間でサイト C を介してトラフィックがヘアピンされている場合、サイト C だけがサイト A と

B のルートを認識します。WAN から WAN への転送とは異なり、サイト A とサイト B は互いのルートテーブルを共有しません。

サイト A とサイト B の間でサイト C を介してトラフィックがヘアピンされる場合は、両方のサイトのネクストホップが中間サイト C であることを示す静的ルートをサイト A とサイト B に追加する必要があります。

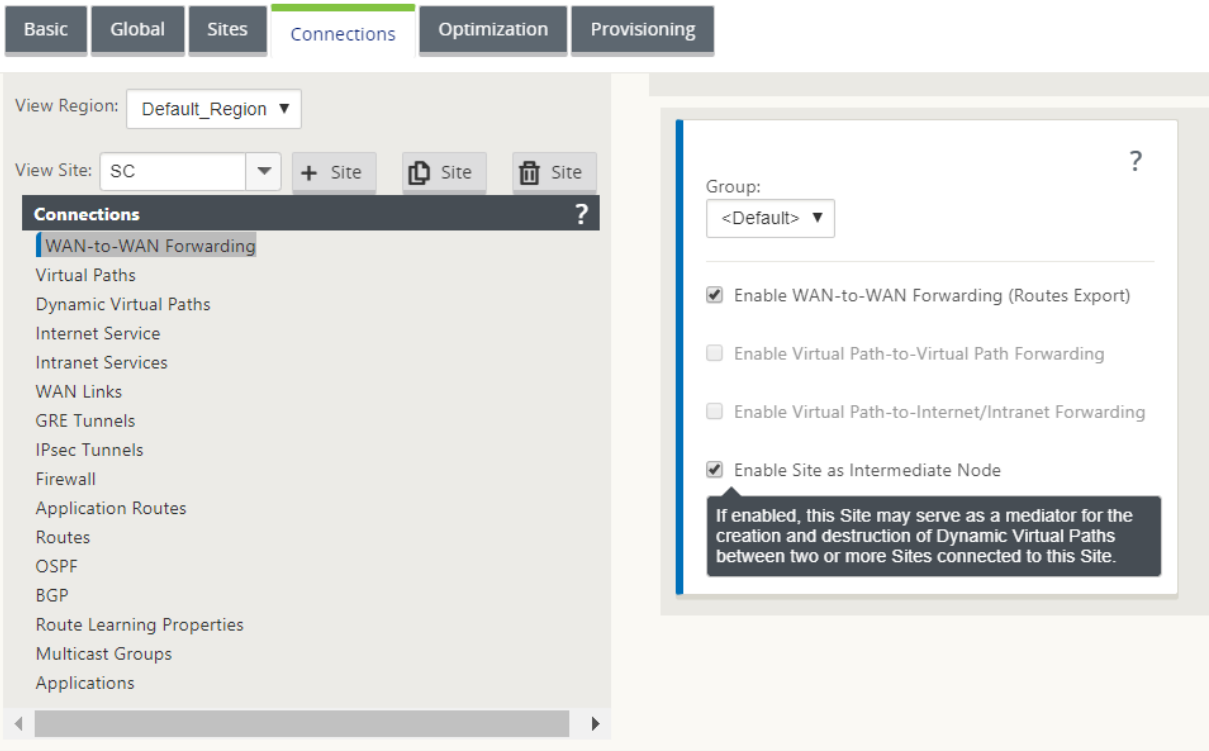
WAN から WAN への転送と Hairpin の配置には、次のような違いがあります。

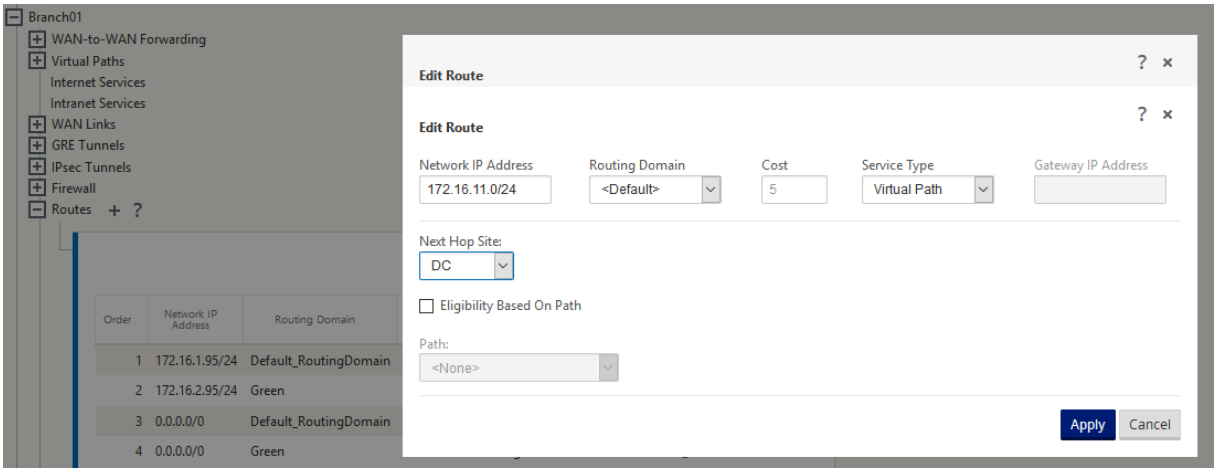
1. 動的仮想パスは構成されていません。常に、中間サイトは 2 つのサイト間のトラフィックをすべて認識します。
2. WAN から WAN への転送グループには参加しません。

   WAN から WAN への転送とヘアピンの配置は、相互に排他的です。任意の時点で設定できるのは、そのうちの 1 つだけです。

   Citrix SD-WAN SE/PE および VPX（仮想）アプライアンスは、ヘアピンの展開をサポートします。0.0.0.0/0 ルートを設定して、追加のロケーションに影響を与えずに 2 つのロケーション間のトラフィックをヘアピンできるようになりました。イントラネットトラフィックにヘアピニングを使用する場合、特定のイントラネットルートがクライアントサイトに追加され、仮想パスを通じてヘアピンサイトにイントラネットトラフィックを転送します。ヘアピン機能を実現するために WAN から WAN への転送を有効にする必要はなくなりました。

ヘアピンの展開は、構成エディターから Citrix SD-WAN Web 管理インターフェースを使用して構成できます。





Palo Alto Networks SD-WAN 1100 プラットフォーム上のファイアウォール統合

May 10, 2021

Citrix SD-WAN は、Palo Alto Networks の次世代仮想マシンのホスティングをサポートしています (VM) SD-WAN 1100 プラットフォーム上のシリーズファイアウォール. サポートされている仮想マシンモデルは次のとおりです。

- VM 50
- VM 100

Palo Alto Networks 仮想マシンシリーズのファイアウォールは、SD-WAN 1100 プラットフォーム上で仮想マシンとして動作します。ファイアウォール仮想マシンは **Virtual Wire** モードで統合され、2 つのデータ仮想インターフェイスが接続されています。SD-WAN でポリシーを構成することで、必要なトラフィックをファイアウォール仮想マシンにリダイレクトできます。

長所

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

- 支店デバイスの統合:SD-WAN と高度なセキュリティの両方を実行する単一のアプライアンス
- LAN-to-LAN、LAN-インターネット、およびインターネット-LAN のトラフィックを保護するオンプレム NGFW（次世代ファイアウォール）によるブランチオフィスのセキュリティ

構成の手順

Palo Alto Networks 仮想マシンを SD-WAN に統合するには、以下の構成が必要です。

- ファイアウォール仮想マシンのプロビジョニング
- セキュリティ仮想マシンへのトラフィックリダイレクトを有効にする

> 注:
>
> トラフィックのリダイレクトを有効にする前に、ファイアウォール仮想マシンを最初にプロビジョニングする必要があります。

Palo Alto Networks 仮想マシンのプロビジョニング

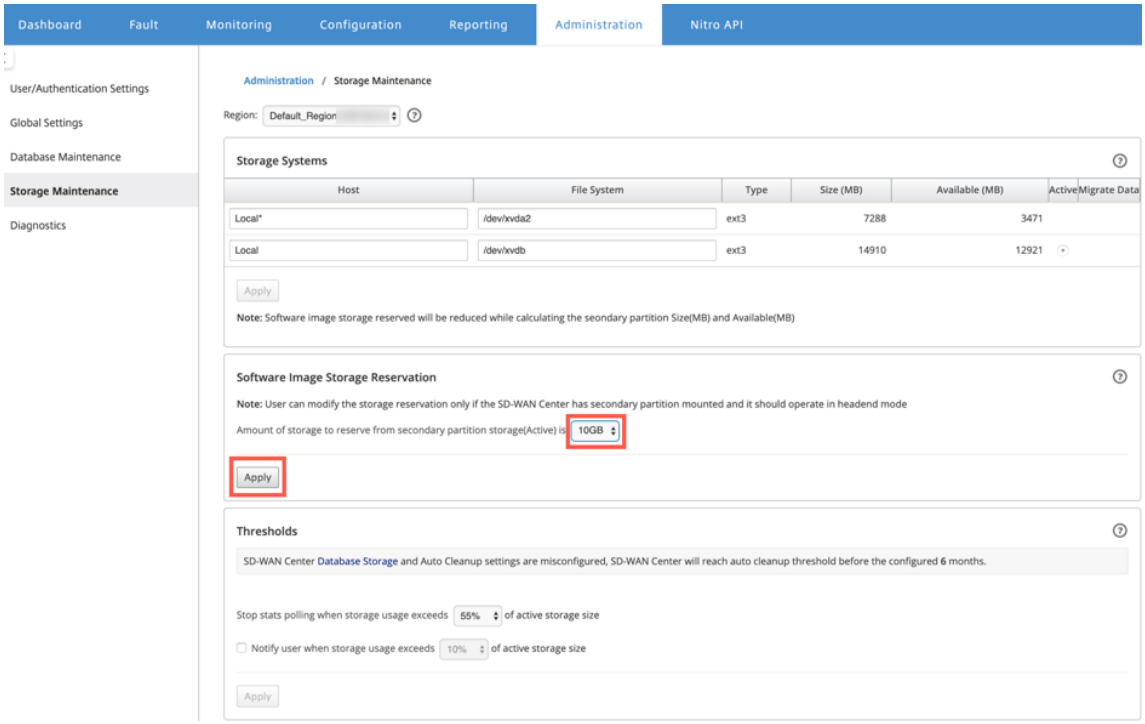
ファイアウォール仮想マシンをプロビジョニングするには、次の 2 つの方法があります。

- SD-WAN センターによるプロビジョニング
- SD-WAN アプライアンス GUI によるプロビジョニング

SD-WAN センターを介したファイアウォール仮想マシンの **Provisioning**

前提条件

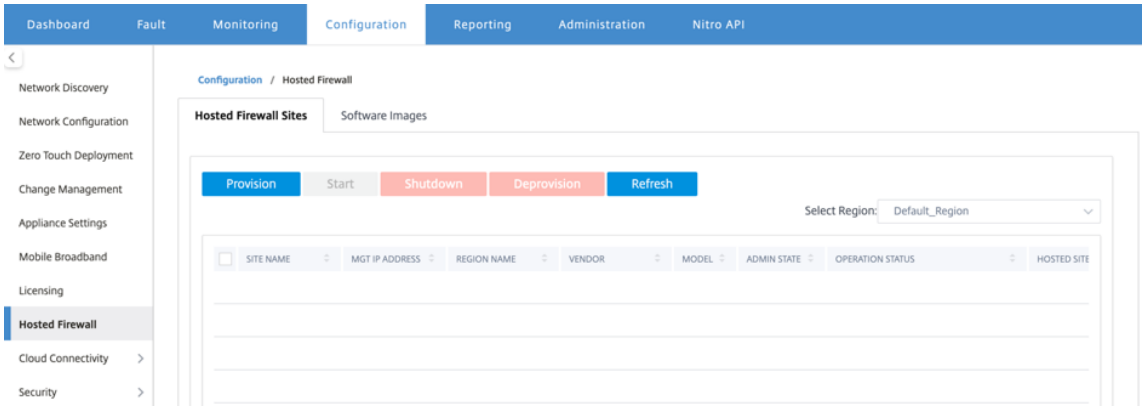
- セカンダリストレージを SD-WAN Center に追加して、ファイアウォール VM イメージファイルを保存します。詳しくは、「システム要件とインストール」を参照してください。
- ファイアウォール VM イメージファイル用にセカンダリパーティションからストレージを予約します。ストレージ制限を設定するには、[管理**] > [**ストレージのメンテナンス] に移動します。
  - リストから必要なストレージ量を選択します。
  - ［適用］をクリックします。



> 注:
>
> ストレージは、条件が満たされた場合にアクティブであるセカンダリパーティションから予約されています。

SD-WAN Center プラットフォーム経由でファイアウォール仮想マシンを Provisioning するには、次の手順を実行します。

1. Citrix SD-WAN Center GUI で、［構成］ > ［ホストされたファイアウォール］を選択します。



   ドロップダウンリストから [Region] を選択すると、選択したリージョンのプロビジョニングされたサイトの詳細を表示できます。

2. ソフトウェアイメージをアップロードします。

> 注:
>
> ソフトウェアイメージをアップロードするのに十分なディスク領域があることを確認してください。

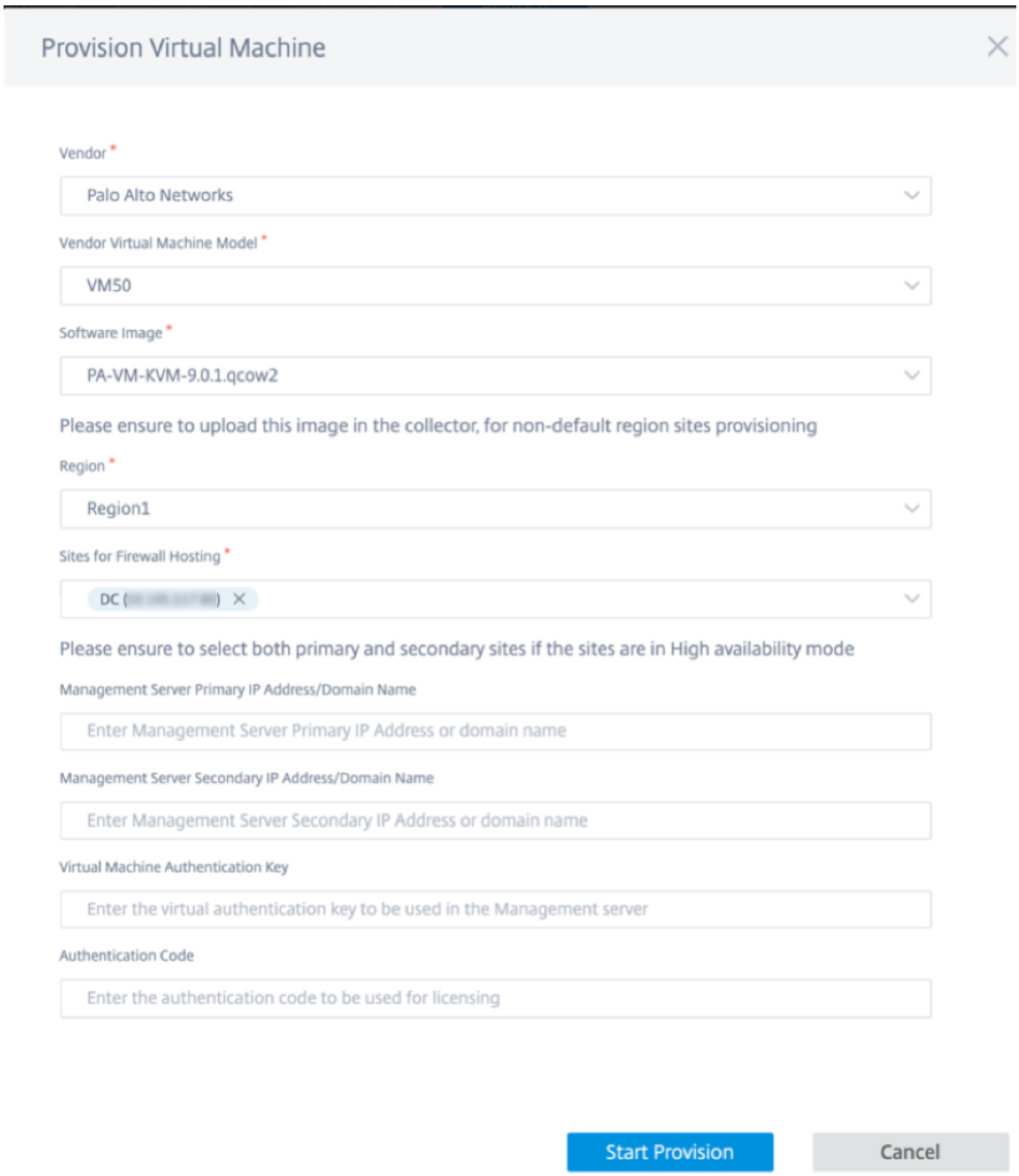
[設定] > [ホストファイアウォール**] > [**ソフトウェアイメージ] に移動し、ドロップダウンリストから [Palo Alto Networks] としてベンダー名を選択します。アップロードするボックスに、ソフトウェアイメージファイルをクリックまたはドロップします。

進行中のアップロード処理を示すステータスバーが表示されます。イメージファイルが 100% アップロードされたと表示されるまで、[**Refresh**] をクリックしたり、その他のアクションを実行したりしないでください。

- 更新: [更新] オプションをクリックして、最新のイメージファイルの詳細を取得します。
- 削除: 既存のイメージファイルを削除するには、[削除] オプションをクリックします。

> 注
>
> - デフォルト以外のリージョンのサイトでファイアウォール仮想マシンをプロビジョニングするには、各コレクタノードにイメージファイルをアップロードします。
> - Palo Alto VM イメージを SDWAN センターから削除すると、SDWAN センターストレージからイメージが削除され、アプライアンスからは削除されません。

3. プロビジョニングについては、[ホストされたファイアウォールサイト] タブに戻り、[プロビジョニング] をクリックします。

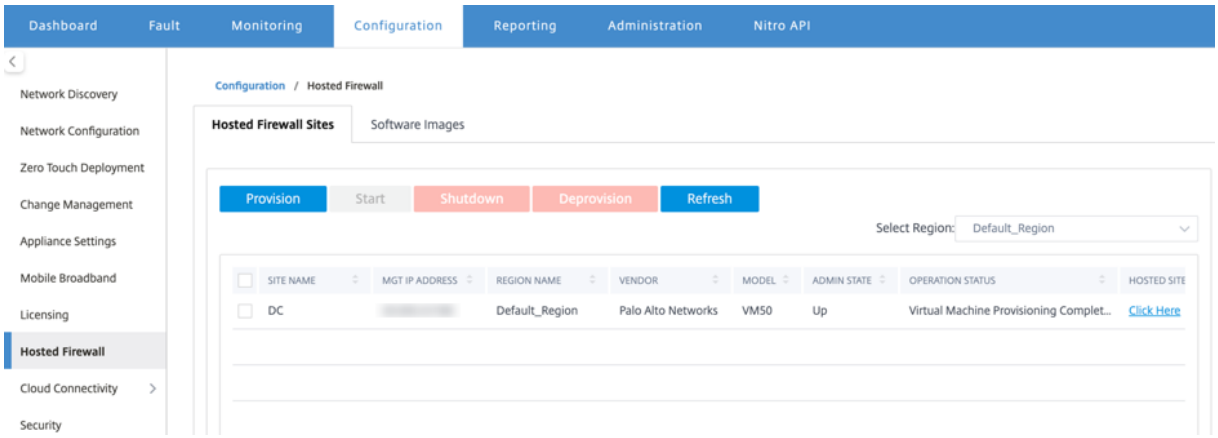


- ベンダー: ドロップダウンリストから [**Palo Alto Networks**] としてベンダー名を選択します。
- ベンダー仮想マシンモデル: リストから仮想マシンのモデル番号を選択します。
- ソフトウェアイメージ: プロビジョニングするイメージファイルを選択します。
- リージョン: リストからリージョンを選択します。
- [ファイアウォールホスティングのサイト]: ファイアウォールホスティングのリストのサイトを選択します。サイトが高可用性モードの場合は、プライマリサイトとセカンダリサイトの両方を選択する必要があります。

- 管理サーバーのプライマリ **IP** アドレス/ドメイン名：管理プライマリ IP アドレスまたは完全修飾ドメイン名を入力します（オプション）。
- 管理サーバーのセカンダリ **IP** アドレス/ドメイン名：管理サーバーのセカンダリ IP アドレスまたは完全修飾ドメイン名を入力します（オプション）。
- 仮想マシン認証キー: 管理サーバーで使用する仮想認証キーを入力します。
- 認証コード：ライセンスに使用する仮想認証コードを入力します。

4. 「プロビジョニングの開始」をクリックします。
5. 最新のステータスを取得するには、[**Refresh**] をクリックします。Palo Alto Networks 仮想マシンが完全に起動すると、SD-WAN Center UI に反映されます。

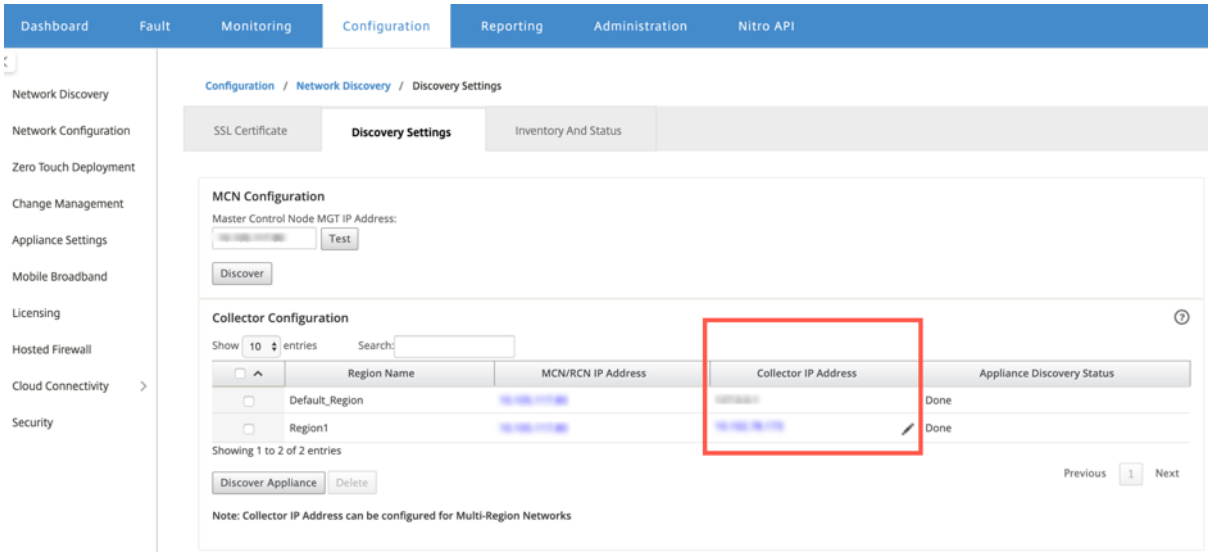
必要に応じて 、仮想マシンを開始、シャットダウン、プロビジョニング解除 できます。



- サイト名: サイト名が表示されます。
- 管理 **IP**: サイトの管理 IP アドレスを表示します。
- リージョン名: リージョン名が表示されます。
- ベンダー: ベンダー名 (パロアルトネットワーク) を表示します。
- モデル：モデル番号（VM50/VM100）が表示されます。
- 管理状態：ベンダー仮想マシンの状態（アップ/ダウン）。
- 操作ステータス: 操作ステータスメッセージを表示します。
- ホストサイト: Palo Alto Networks 仮想マシンの GUI にアクセスするには、**[**ここをクリック**]** リンクを使用します。

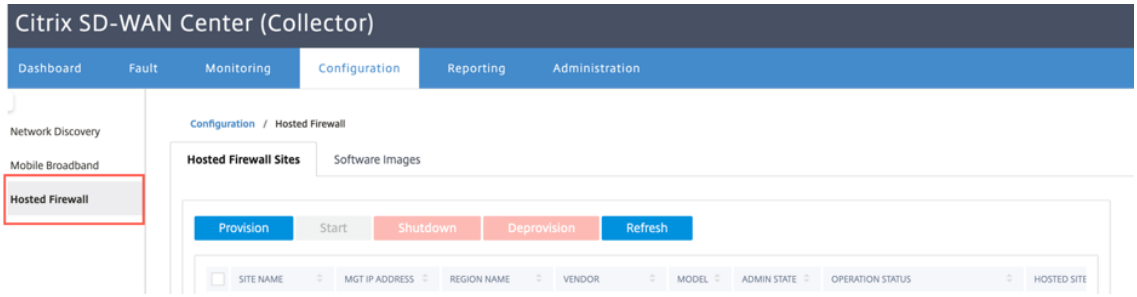
デフォルト以外のリージョンサイトをプロビジョニングするには、SD-WAN Center Collector にソフトウェアイメージをアップロードする必要があります。Palo Alto Networks は、SD-WAN Center ヘッドエンド GUI または SD-WAN Center コレクタから両方ともプロビジョニングできます。

SD-WAN Center コレクタの IP アドレスを取得するには、[構成**] > [**ネットワーク探索**] >** [探索の設定] タブを選択します。

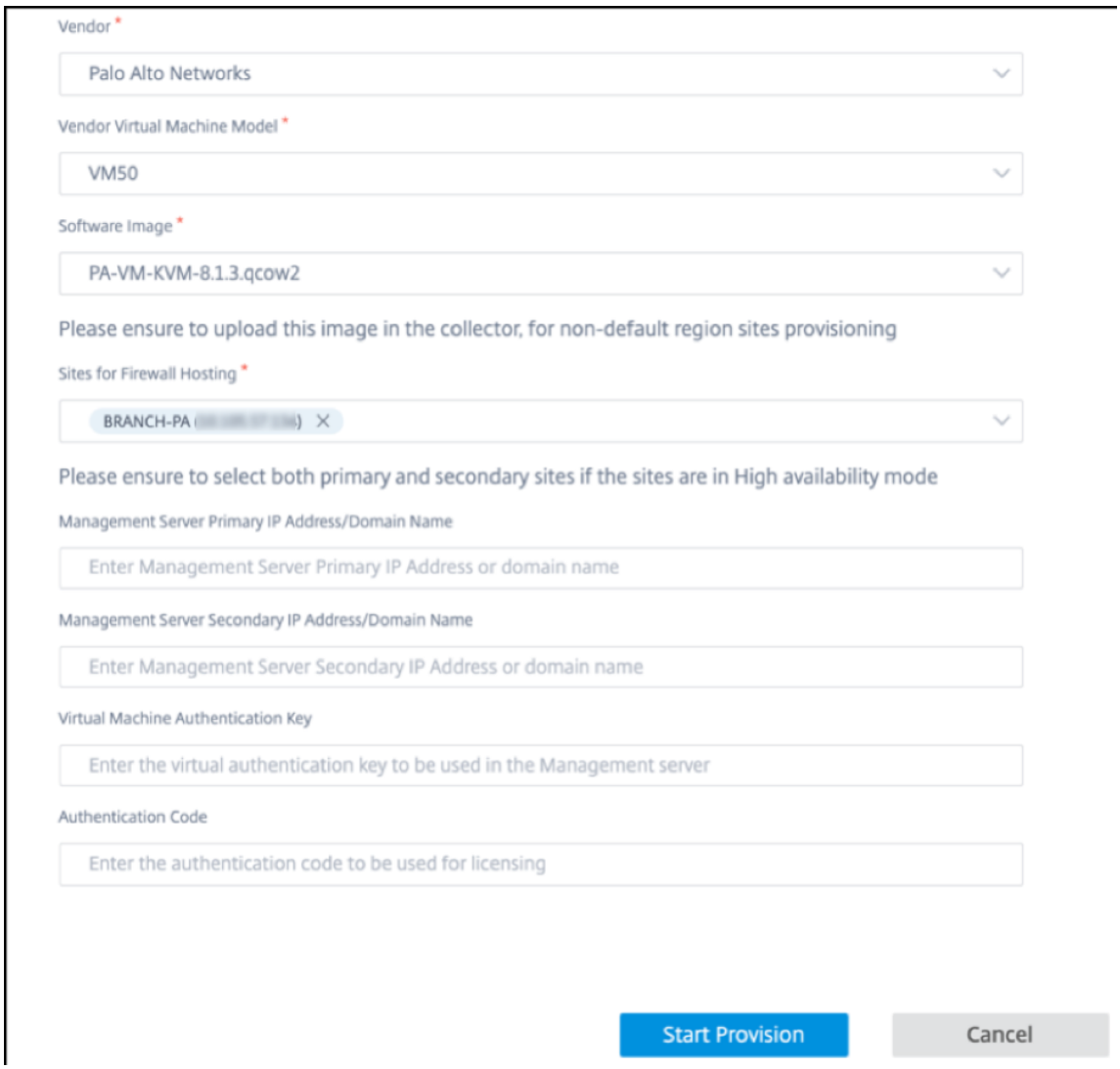


SD-WAN コレクタから Palo Alto Networks をプロビジョニングするには:

1. SD-WAN Collector GUI から、[構成] に移動し、[ホストされたファイアウォール] を選択します。



2. ソフトウェアイメージタブに移動して、ソフトウェアイメージをアップロードします。
3. [ホストされたファイアウォールサイト] タブの [プロビジョニング] をクリックします。
4. 次の詳細を入力し、「プロビジョニングの開始」をクリックします。



- ベンダー: ドロップダウンリストから [**Palo Alto Networks**] としてベンダー名を選択します。
- ベンダー仮想マシンモデル: リストから仮想マシンのモデル番号を選択します。
- ソフトウェアイメージ: プロビジョニングするイメージファイルを選択します。
- リージョン: リストからリージョンを選択します。
- [ファイアウォールホスティングのサイト]: ファイアウォールホスティングのリストのサイトを選択します。サイトが高可用性モードの場合は、プライマリサイトとセカンダリサイトの両方を選択する必要があります。
- 管理サーバーのプライマリ **IP** アドレス/ドメイン名: 管理プライマリ IP アドレスまたは完全修飾ドメイン名を入力します（オプション）。
- 管理サーバーのセカンダリ **IP** アドレス/ドメイン名: 管理サーバーのセカンダリ IP アドレスまたは完全修飾ドメイン名を入力します（オプション）。
- 仮想マシン認証キー: 管理サーバーで使用する仮想認証キーを入力します。

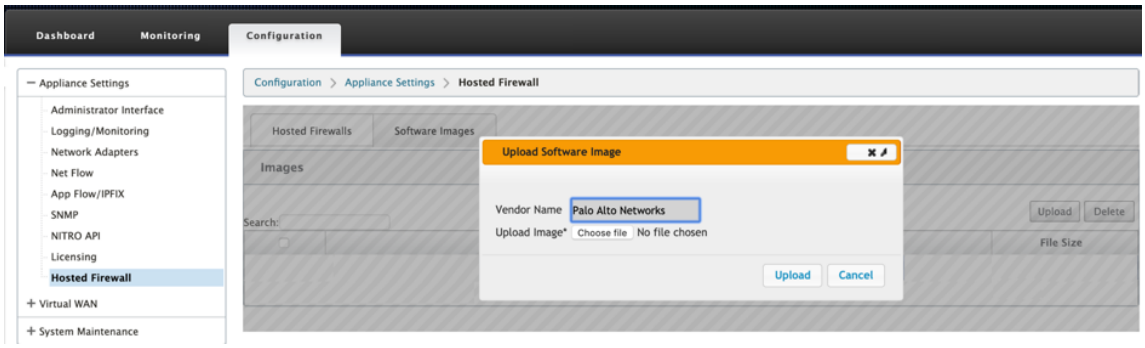
- 認証コード：ライセンスに使用する仮想認証コードを入力します。

5.「プロビジョニングの開始」をクリックします。

SD-WAN アプライアンスの GUI によるファイアウォール仮想マシンの Provisioning

SD-WAN プラットフォームで、ホストされた仮想マシンをプロビジョニングして起動します。Provisioning の手順は、次のとおりです。

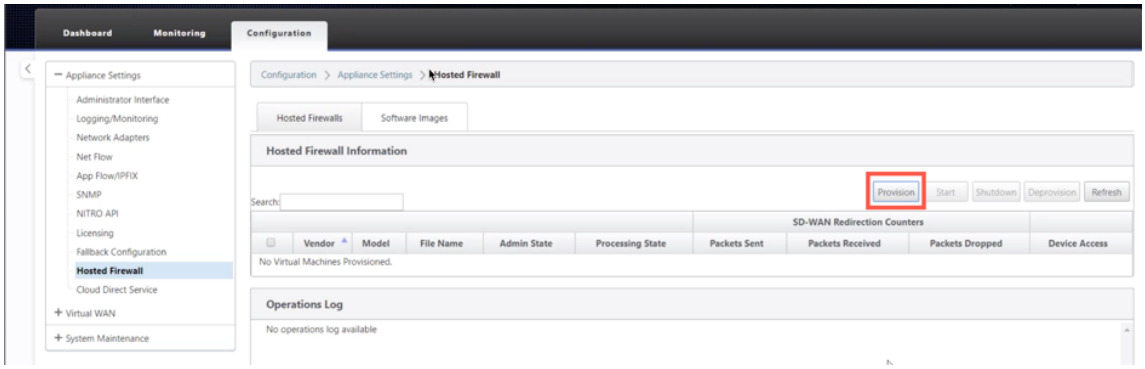
1. Citrix SD-WAN GUI で、［構成］**>**［アプライアンスの設定］の順に 展開し、［ホストされたファイアウォール］を選択します。
2. ソフトウェアイメージをアップロードします。
   - ［ソフトウェアイメージ］タブを選択します。[**Palo Alto Networks**] としてベンダー名を選択します。
   - ソフトウェアイメージファイルを選択します。
   - ［アップロード］をクリックします。



> 注：
> アップロードできるソフトウェアイメージは最大 2 つです。Palo Alto Networks 仮想マシンイメージのアップロードには、帯域幅の可用性によっては、時間がかかる場合があります。

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

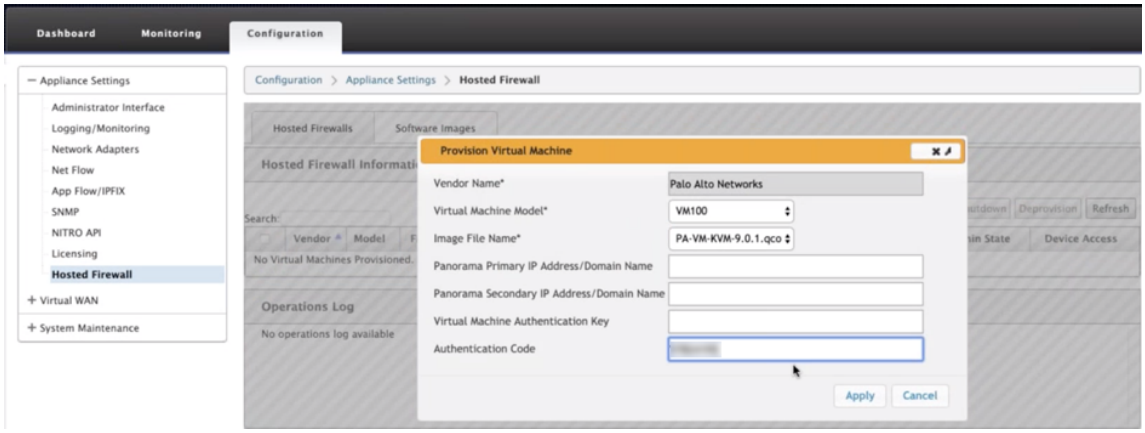
3. プロビジョニングの場合は、[ホストされたファイアウォール] タブを選択し、[プロビジョニング] ボタンをクリックします。



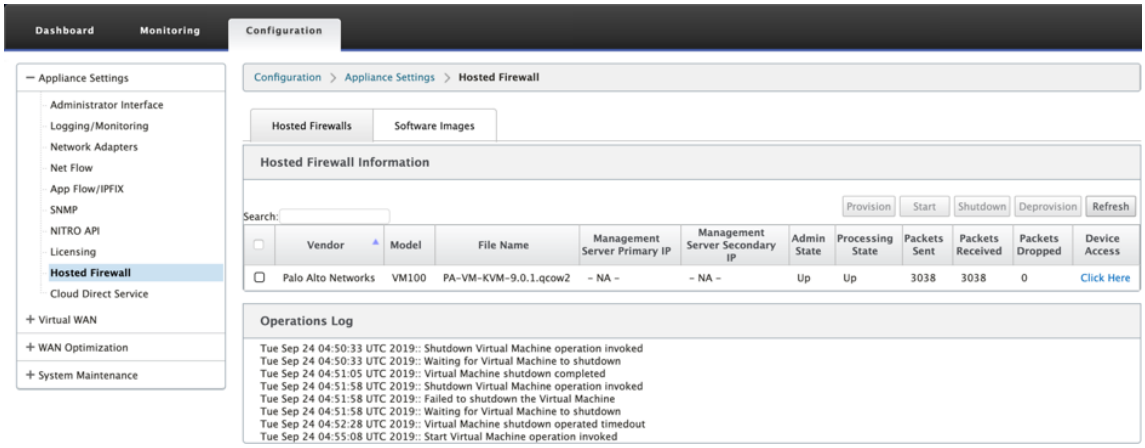
4. Provisioning について次の詳細を入力します。

   - ベンダー名: **Palo Alto** ネットワークとしてベンダーを選択します。
   - 仮想マシンモデル: リストから仮想マシンのモデル番号を選択します。
   - イメージファイル名: イメージファイルを選択します。
   - パノラマプライマリ **IP** アドレス/ドメイン名: パノラマプライマリ IP アドレスまたは完全修飾ドメイン名を指定します (オプション)。
   - パノラマセカンダリ **IP** アドレス/ドメイン名: パノラマセカンダリ IP アドレスまたは完全修飾ドメイン名を指定します (オプション)。
   - 仮想マシン認証キー: 仮想マシン認証キーを指定します (オプション)。

     Palo Alto Networks 仮想マシンをパノラマに自動登録するには、仮想マシン認証キーが必要です。
   - 認証コード: 認証コード（仮想マシンライセンスコード）を入力します（オプション）。
   - [適用] をクリックします。



5. 最新のステータスを取得するには、[**Refresh**] をクリックします。Palo Alto Networks 仮想マシンが完全に起動すると、操作ログの詳細とともに SD-WAN UI に反映されます。



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

必要に応じて 、仮想マシンを開始、シャットダウン、プロビジョニング解除できます。ここをクリック オプションを使用して、Palo Alto Networks 仮想マシンの GUI にアクセスするか、管理 IP と 4100 ポート (管理 IP: 4100) を使用します。

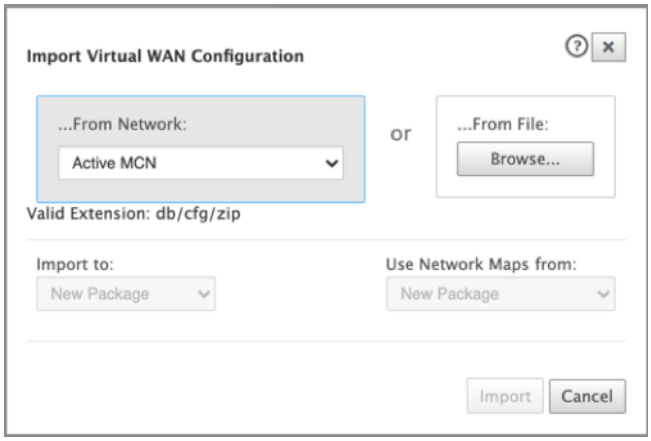
> 注
> パロアルトネットワークスの GUI にアクセスするには、常にシークレットモードを使用してください。

トラフィックリダイレクト

トラフィックリダイレクトの設定は、MCN の構成エディターまたは SD-WAN Center の構成エディターを使用して行うことができます。

SD-WAN センターで構成エディター内を移動するには、次の手順を実行します。

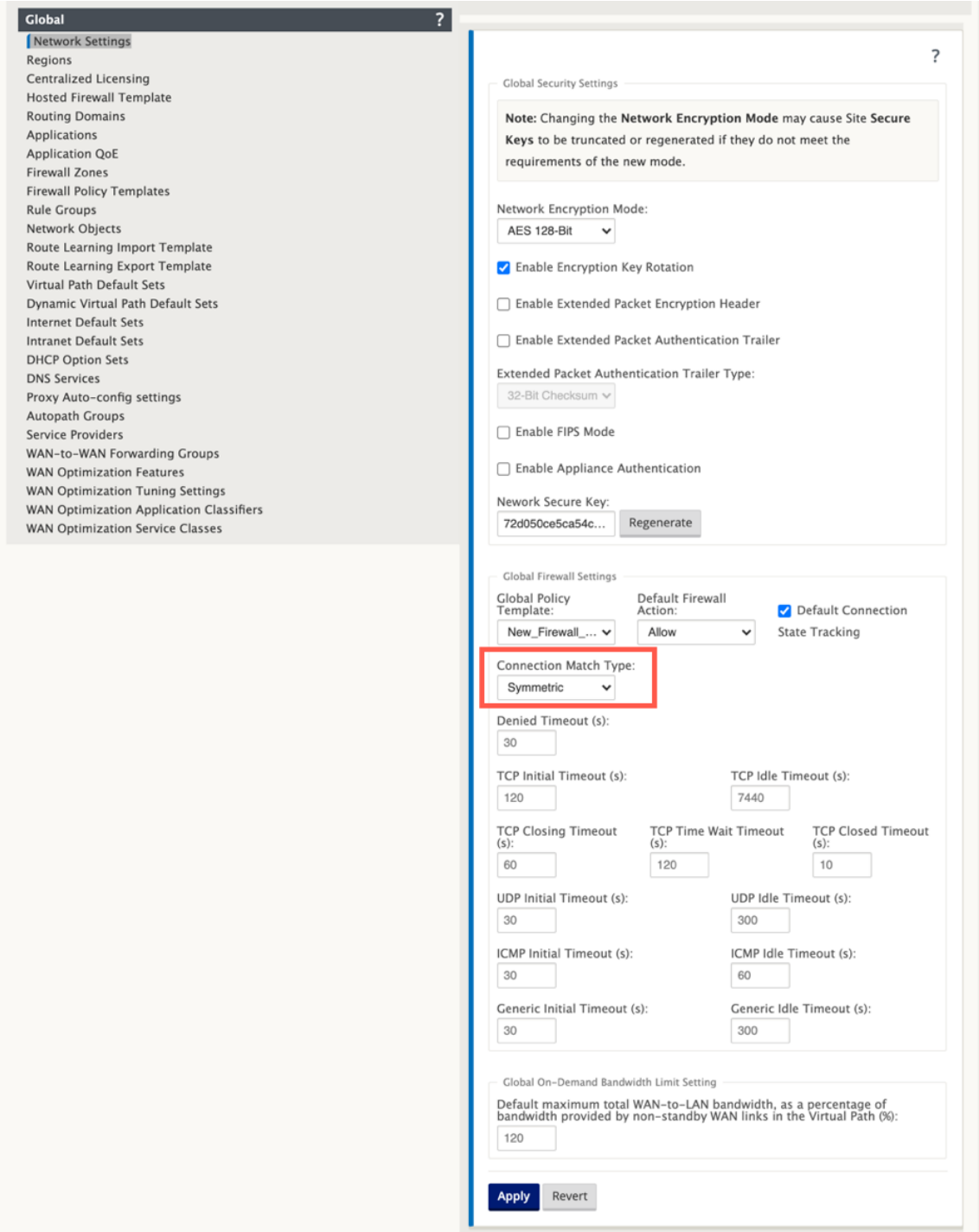
1. Citrix SD-WAN Center UI を開き、［構成］**>**［ネットワーク構成のインポート］に移動します。アクティブ MCN から仮想 WAN 設定をインポートし、[**Import**] をクリックします。



残りの手順は、MCN を介したトラフィックリダイレクション設定と同様です。

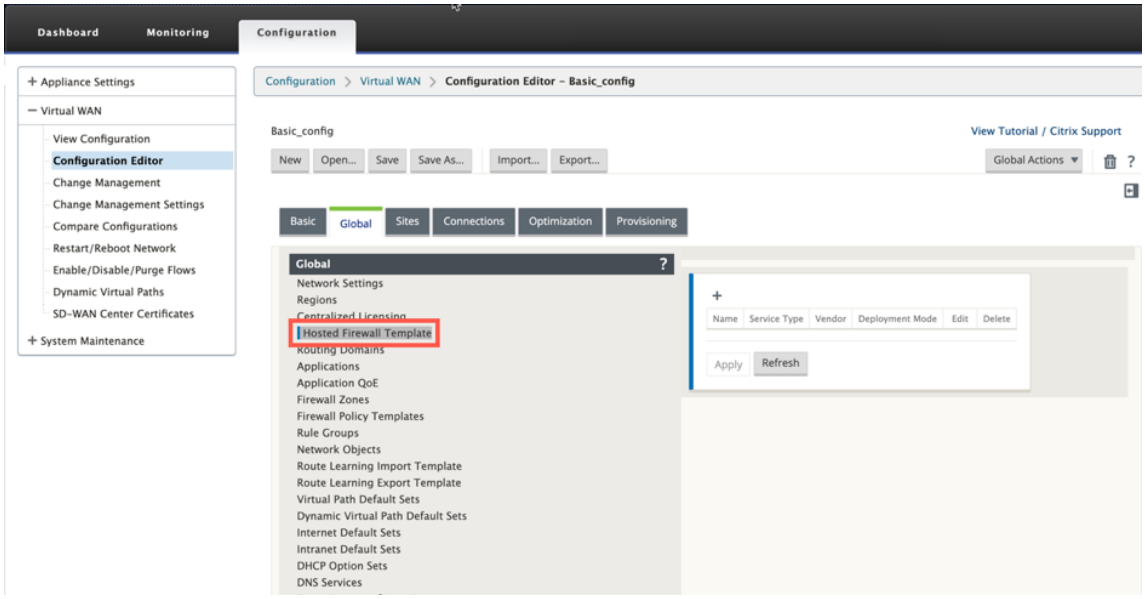
MCN の構成エディタ内を移動するには、次の手順を実行します。

1. [グローバル**] > [**ネットワーク設定] で [接続の一致タイプ] を対称に設定します。

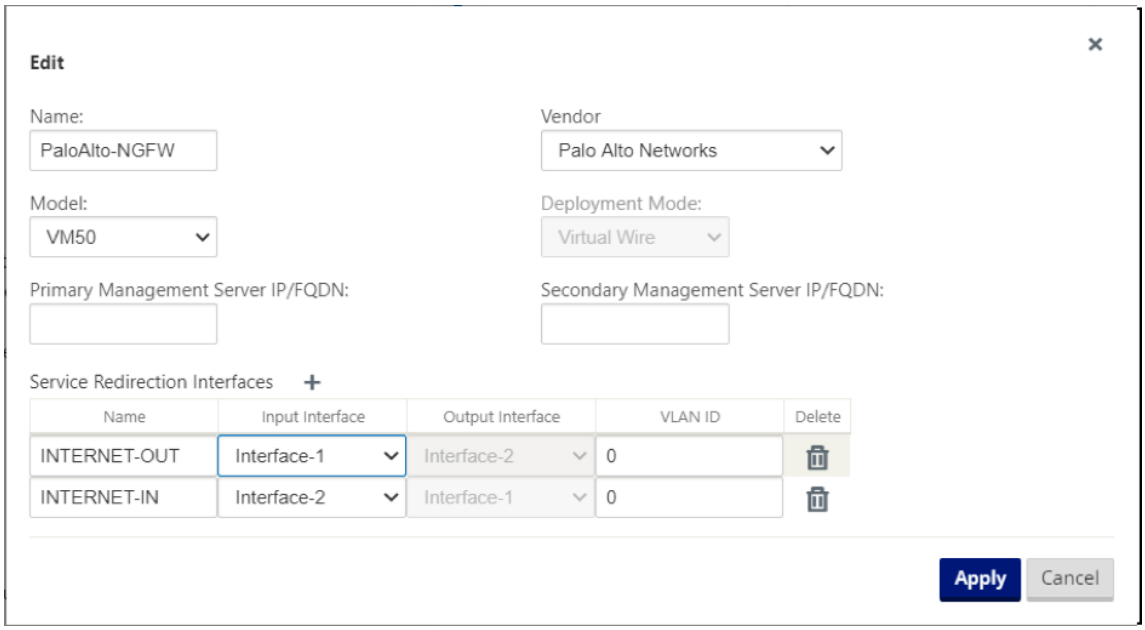


デフォルトでは、SD-WAN ファイアウォールポリシーは方向固有です。対称マッチタイプは、指定された一致基準を使用して接続に一致し、両方向にポリシーアクションを適用します。

2. **Citrix SD-WAN UI** を開き、［構成］**>** ［仮想 **WAN** ］を展開し、［構成エディタ］を選択し、［グローバル］セクションで［ホストされたファイアウォールテンプレート］を選択します。



3. [**+**] をクリックし、次のスクリーンショットで必要な情報を入力し、[**Hosted Firewall**] テンプレートを追加し、[**Add**] をクリックします。



ホストされたファイアウォールテンプレートを使用すると、SD-WAN アプライアンスでホストされているファイアウォール仮想マシンへのトラフィックリダイレクトを構成できます。テンプレートを構成するために必要な入力は次のとおりです。

- **[** 名前]: ホストされているファイアウォールテンプレートの名前。
- ベンダー: ファイアウォールベンダーの名前。
- 配置モード: [配置モード] フィールドは自動的に入力され、グレー表示されます。**Palo Alto** ネットワークスのベンダーの場合、展開モードは **Virtual Wire** です。

- モデル: ホストされたファイアウォールの仮想マシンモデル。Palo Alto Networks ベンダーの場合、仮想マシンのモデル番号を VM 50/VM 100 として選択できます。
- プライマリ管理サーバ **IP/FQDN**: パノラマのプライマリ管理サーバ IP/FQDN。
- セカンダリ管理サーバ **IP/FQDN**: パノラマのセカンダリ管理サーバ IP/FQDN。
- サービスリダイレクトインターフェイス: SD-WAN とホストされたファイアウォール間のトラフィックリダイレクトに使用される論理インターフェイスです。

Interface-1、Interface-2 は、ホストされているファイアウォールの最初の 2 つのインターフェイスを指します。トラフィックリダイレクションに VLAN を使用する場合は、ホストされたファイアウォールで同じ VLAN を設定する必要があります。トラフィックリダイレクション用に設定された VLAN は、SD-WAN およびホステッドファイアウォールの内部にあります。

> 注
>
> リダイレクション入力インターフェイスは、接続イニシエータの方向から選択する必要があります。リダイレクションインターフェイスは、応答トラフィック用に自動的に選択されます。たとえば、発信インターネットトラフィックが Interface-1 でホストされているファイアウォールにリダイレクトされると、応答トラフィックは Interface-2 でホストされているファイアウォールに自動的にリダイレクトされます。インターネットインバウンドトラフィックがない場合、上記の例では Interface-2 は必要ありません。

Palo Alto Networks ファイアウォールをホストするには、物理インターフェイスが 2 つだけ割り当てられます。複数のゾーンからのトラフィックをホストされたファイアウォールにリダイレクトする必要がある場合は、内部 VLAN を使用して複数のサブインターフェイスを作成し、ホストされたファイアウォールの異なるファイアウォールゾーンに関連付けることができます。

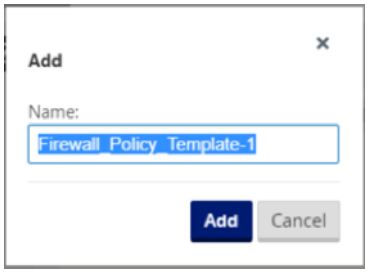
SD-WAN ファイアウォールポリシーまたはサイトレベルのポリシーを使用して、すべてのトラフィックを Palo Alto Networks 仮想マシンにリダイレクトできます。

> 注
>
> SD-WAN ファイアウォールポリシーが自動的に作成され、ホストされているファイアウォール管理サーバーとの間のトラフィック を許可 します。これにより、ホストされたファイアウォール宛ての管理トラフィック（または）がリダイレクトされるのを回避できます。

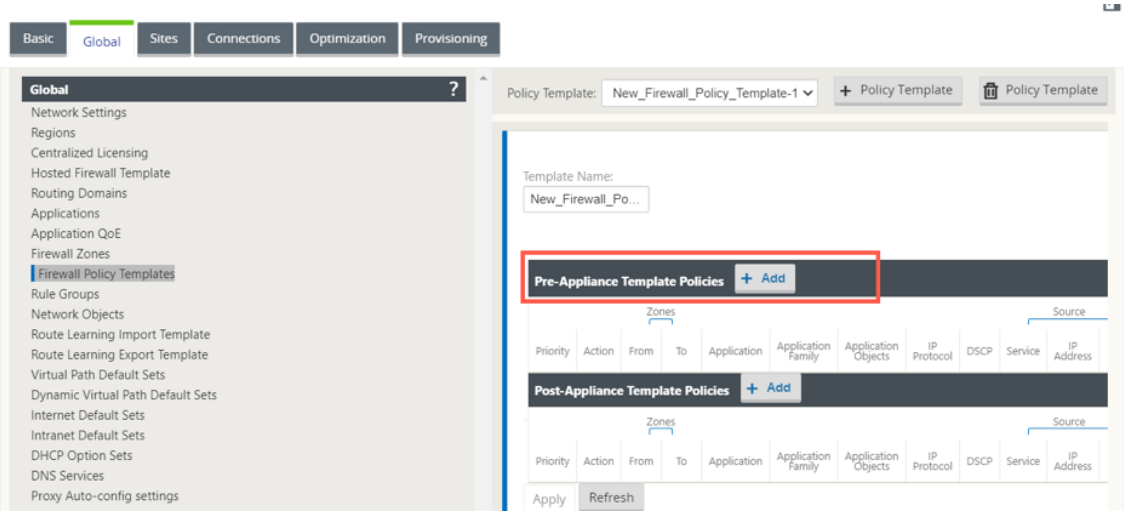
ファイアウォール仮想マシンへのトラフィックのリダイレクトは、SD-WAN ファイアウォールポリシーを使用して実行できます。SD-WAN ファイアウォールポリシーを作成するには、グローバルセクションのファイアウォールポリシーテンプレートまたはサイトレベルのどちらを使用するかの 2 つの方法があります。

方法**-1**

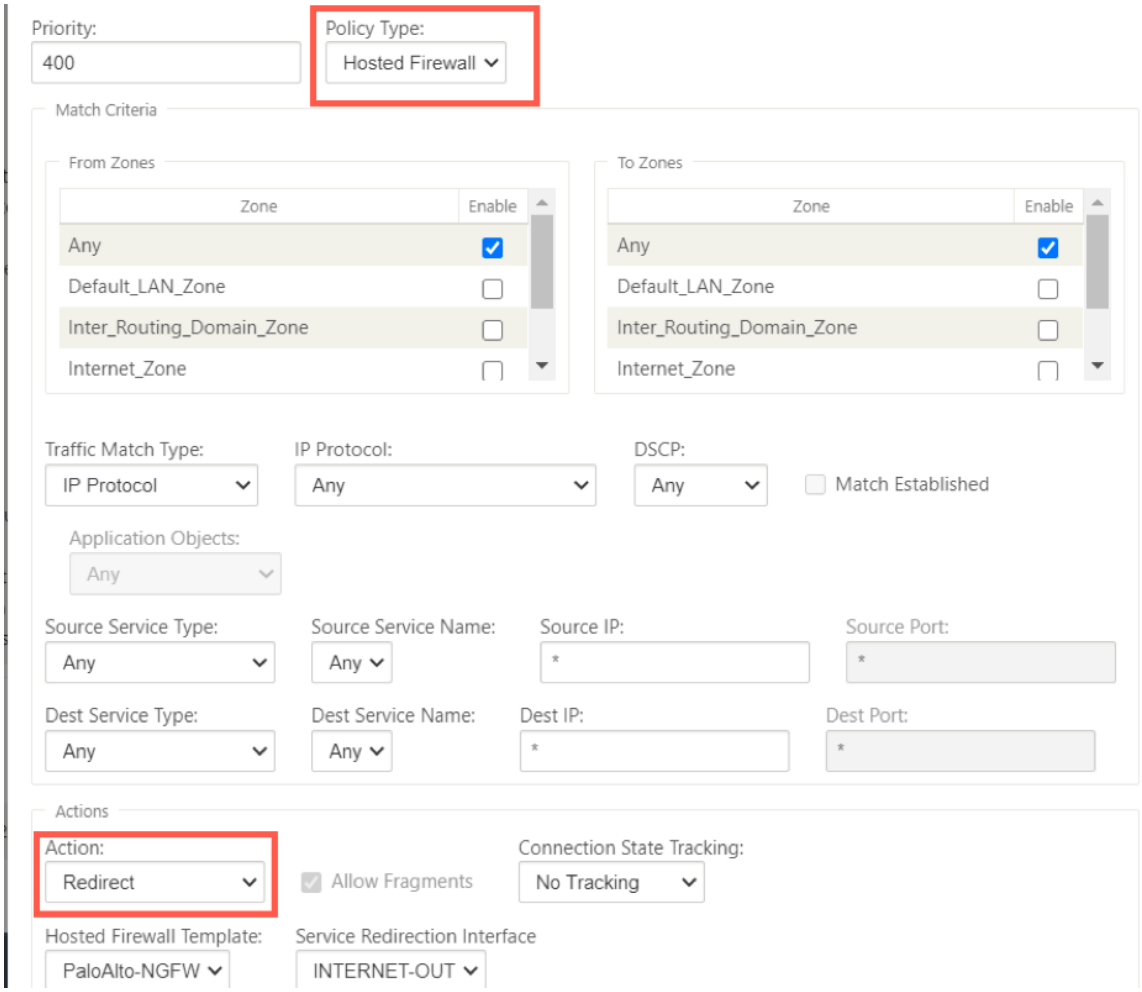
1. Citrix SD-WAN GUI から、［構成］**>**［仮想 **WAN**］を展開し、［構成エディタ］に移動します。[グローバル] タブに移動し、[ファイアウォールポリシーテンプレート] を選択します。[**+** ポリシーテンプレート] をクリックします。ポリシーテンプレートに名前を指定し、[**Add**] をクリックします。



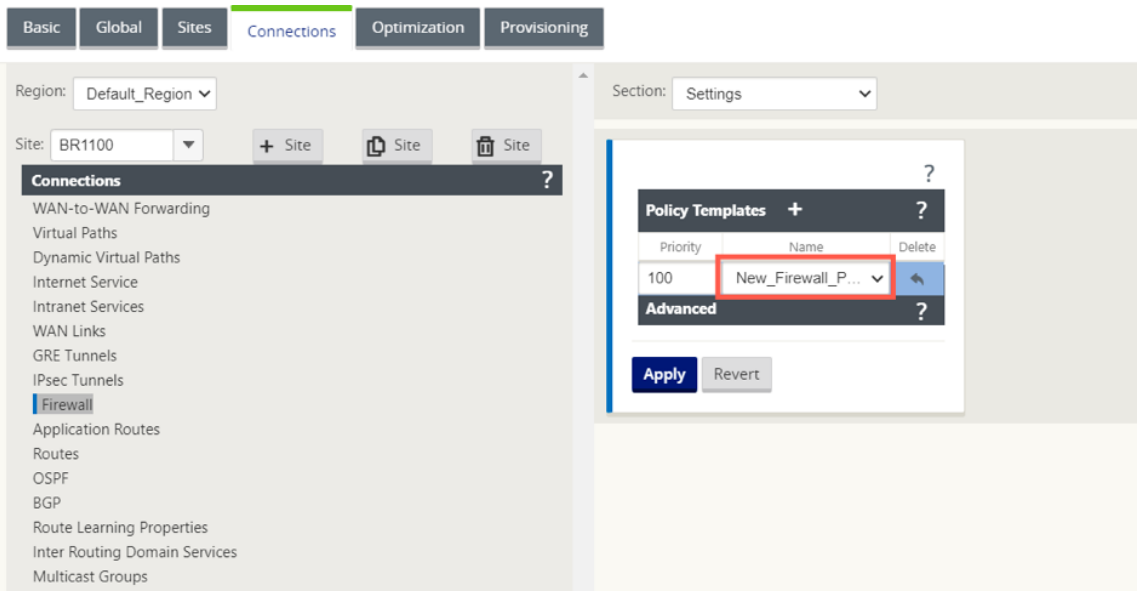
2. ［プレアプライアンステンプレートポリシー］の横にある［**+** 追加］をクリックします。



3. ポリシータイプを **[**ホストされたファイアウォール] に変更します。アクションフィールドは、リダイレクトに自動入力されます。ドロップダウンリストから、****** ホストされたファイアウォールテンプレートとサービスリダイレクトインターフェイスを選択します ****** 。必要に応じて、他の一致基準を入力します。

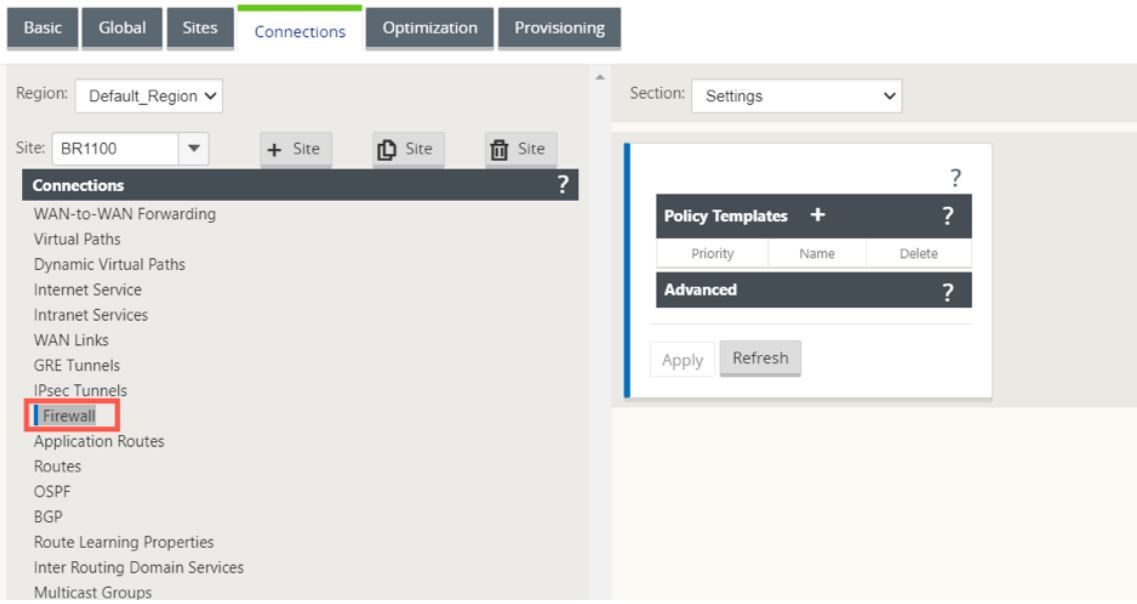


4. [接続] **>** [ファイアウォール] に移動し、[名前] フィールドで (作成した) ファイアウォールポリシーを選択します。[適用] をクリックします。

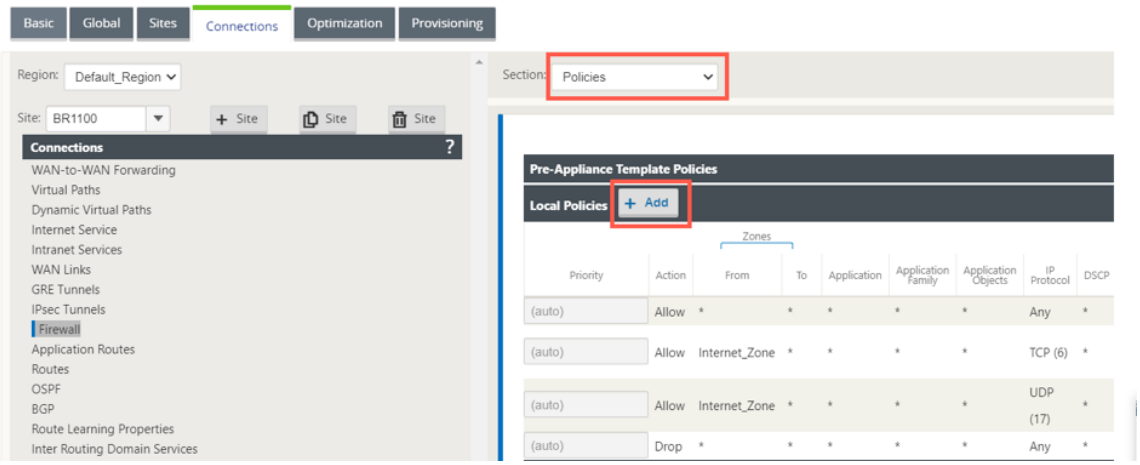


方法**-2**

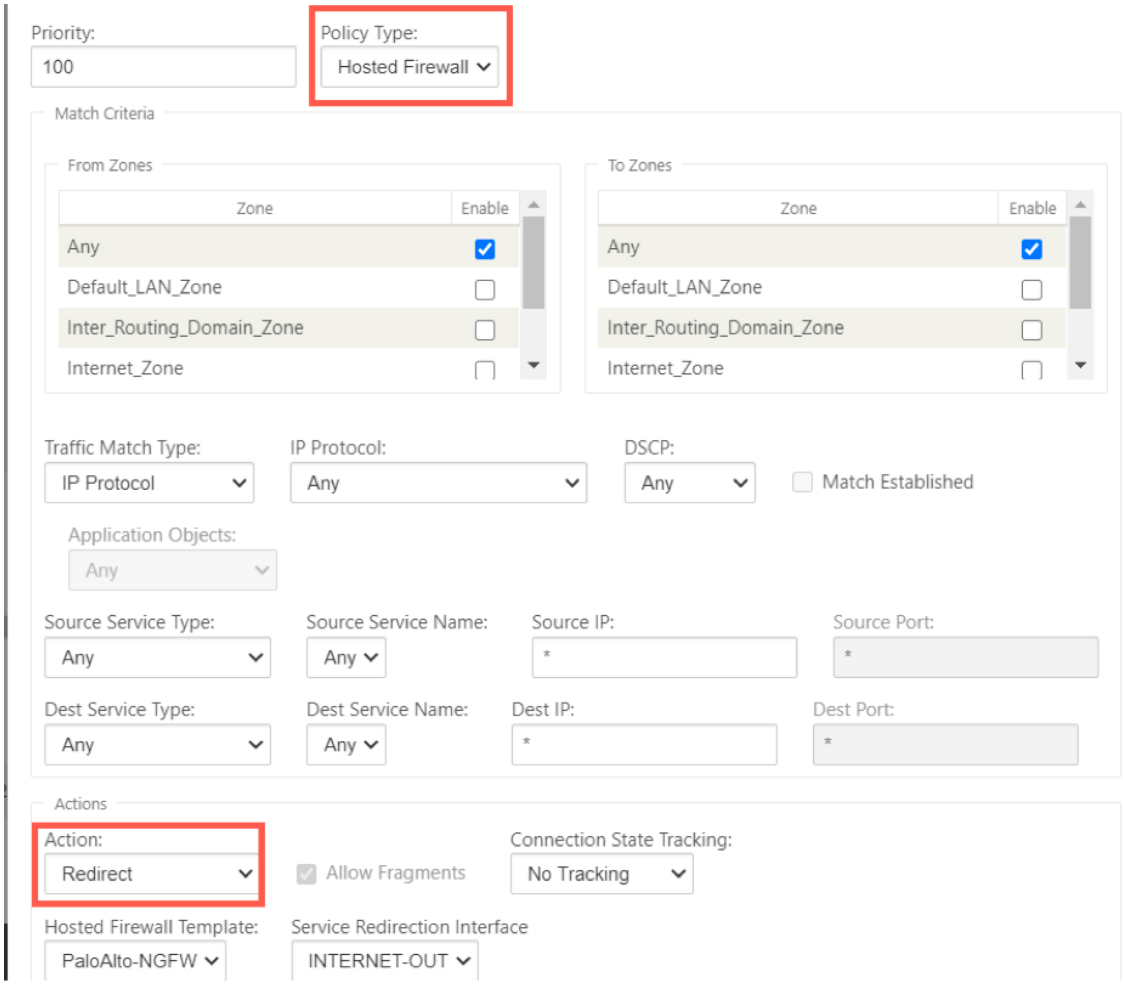
1. すべてのトラフィックをリダイレクトするには、[構成エディタ**] > [**仮想 **WAN**] で、[接続] タブに移動し、[ファイアウォール] を選択します。



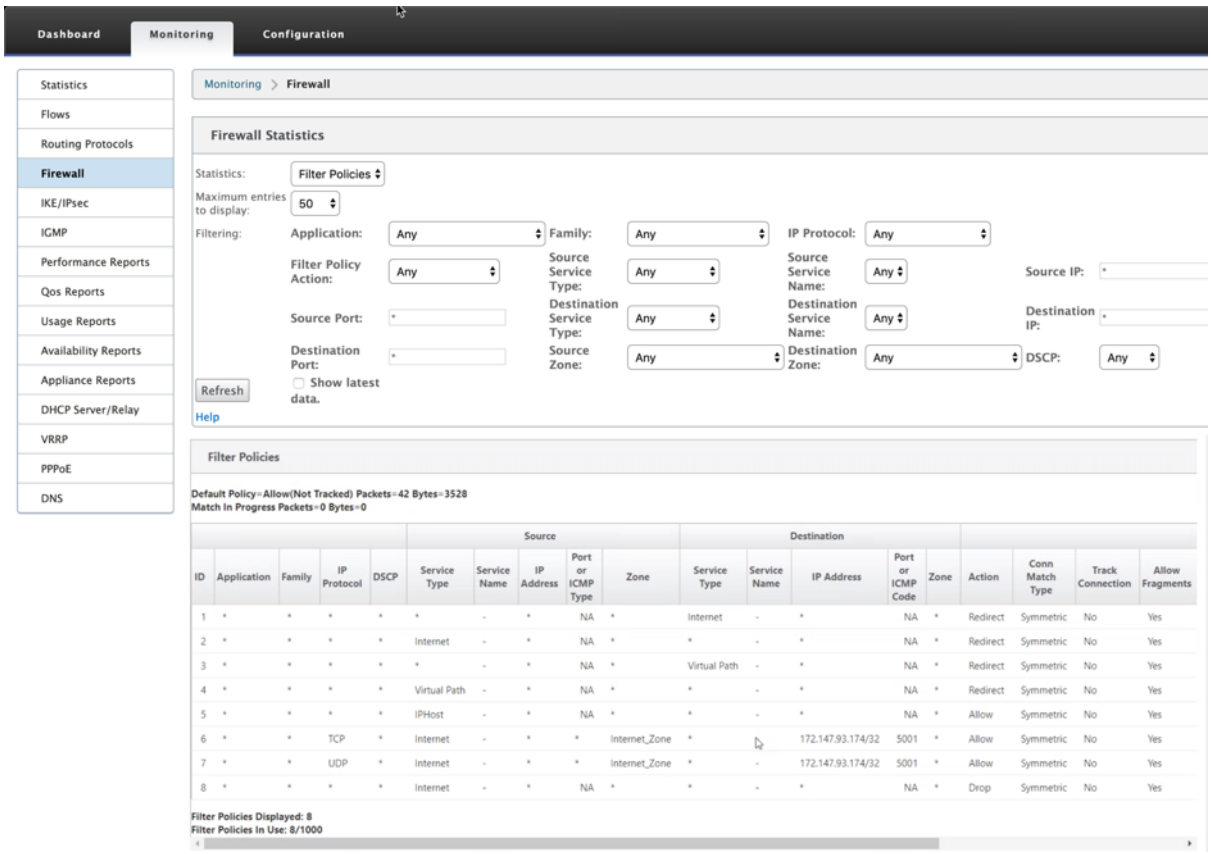
2. [セクション] ドロップダウンリストから [ポリシー] を選択し、[**+** 追加] をクリックして新しいファイアウォールポリシーを作成します。



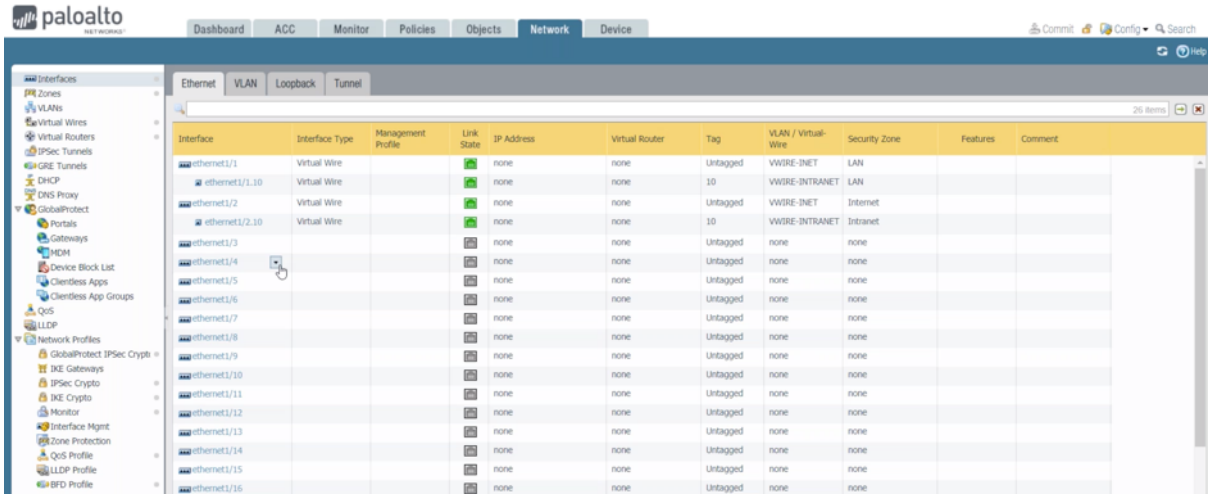
3. ポリシータイプを **[**ホストされたファイアウォール] に変更します。アクションフィールドは、リダイレクトに自動入力されます。ドロップダウンリストから、****** ホストされたファイアウォールテンプレートとサービスリダイレクトインターフェイスを選択します ****** 。[追加] をクリックします。



すべてのネットワーク構成が起動して実行モードになっている間は、[監視] **>** [ファイアウォール] **>** [統計 リスト] の [フィルタポリシー] を選択して接続を監視できます。



Palo Alto Networks UI を使用して、SD-WAN サービスチェーンテンプレートで行った設定と Palo Alto Networks 設定のマッピングを検証できます。



メモ

1100 アプライアンスでクラウドダイレクトまたは **SD-WAN WANOP**（**PE**）がすでにプロビジョニングされている場合は、Palo Alto ネットワークスの仮想マシンをプロビジョニングできません。

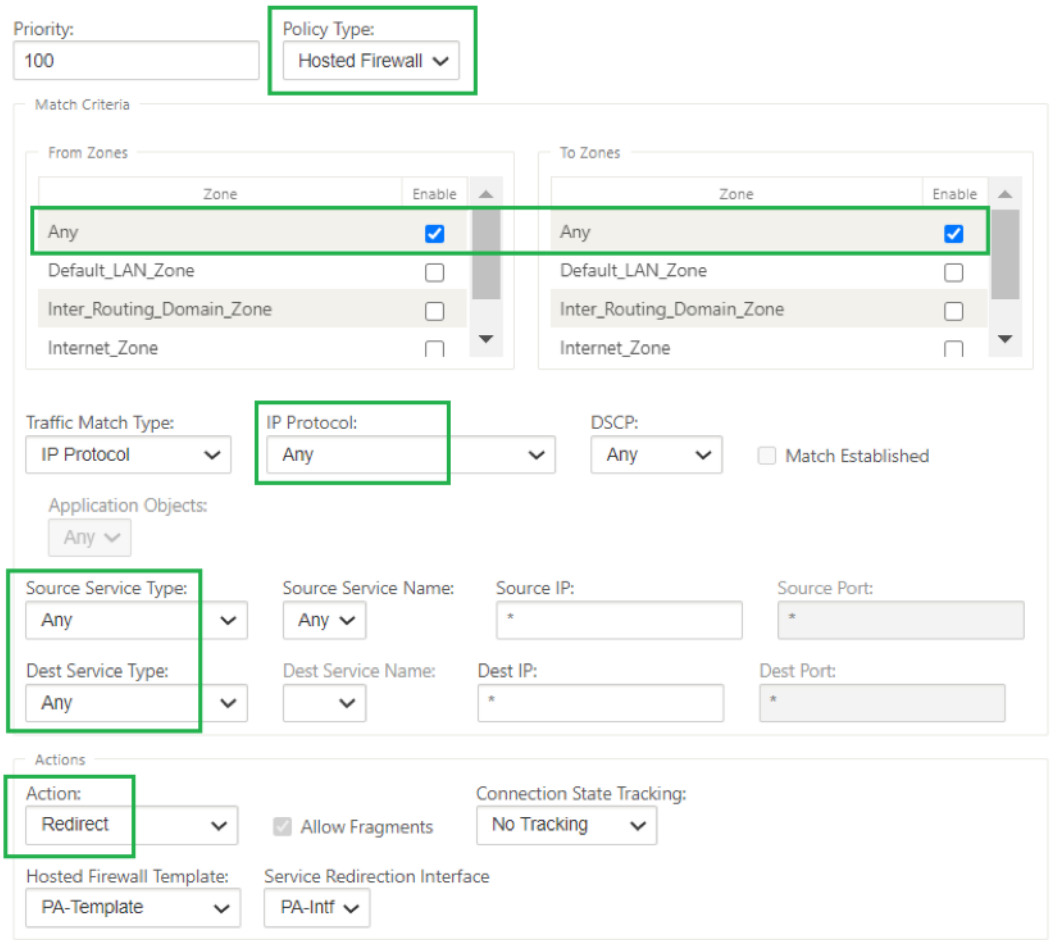
ユースケース—**SD-WAN 1100** 上のホスト型ファイアウォール

Citrix SD-WAN 1100 アプライアンスを使用して実装されたユースケースシナリオを次に示します。

ユースケース **1**: すべてのトラフィックをホストファイアウォールにリダイレクトする

このユースケースは、すべてのトラフィックが Hosted 次世代ファイアウォールによって処理される小規模なブランチユースケースに適用されます。リダイレクトされたトラフィックのスループットの量は 100 Mbps に制限されるため、帯域幅要件を考慮する必要があります。

これを実現するには、次のスクリーンショットに示すように、トラフィックに一致するファイアウォールルールを作成し、[****** リダイレクトとしてアクション ****] を使用します。

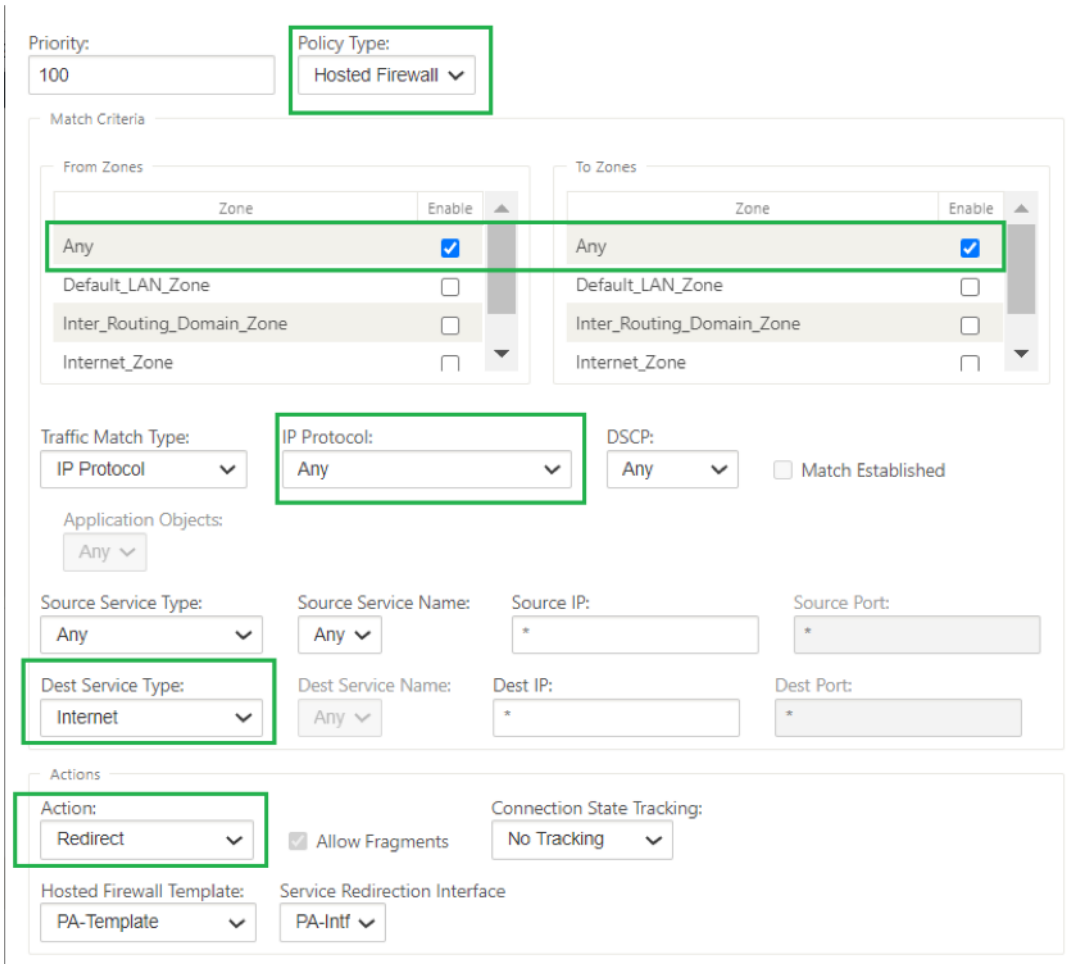


ユースケース **2:** インターネットトラフィックのみをホスト型ファイアウォールにリダイレクトする

このユースケースは、インターネットにバインドされたトラフィックが、サポートされているリダイレクトされたトラフィックのスループットの量を超えないすべてのブランチサイトに適用されます。この場合、データセンターへの

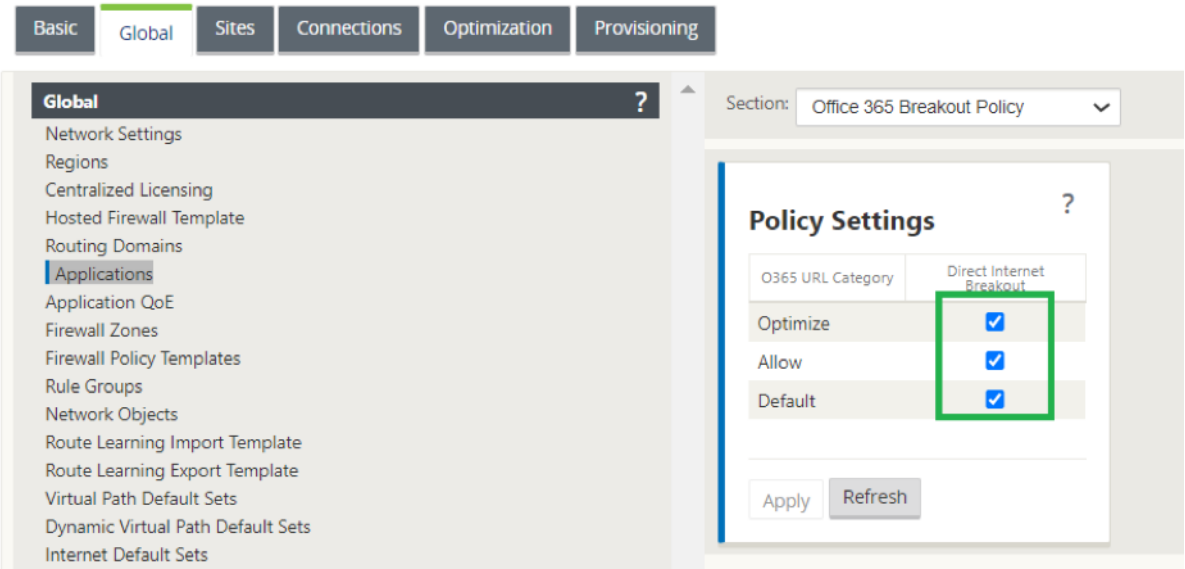
ブランチトラフィックは、データセンターにデプロイされたセキュリティアプライアンス/サービスによって処理されます。

これを実現するには、次のスクリーンショットに示すように、任意のトラフィックに一致するファイアウォールルールを作成し、** リダイレクトとしてアクションを使用します ** 。

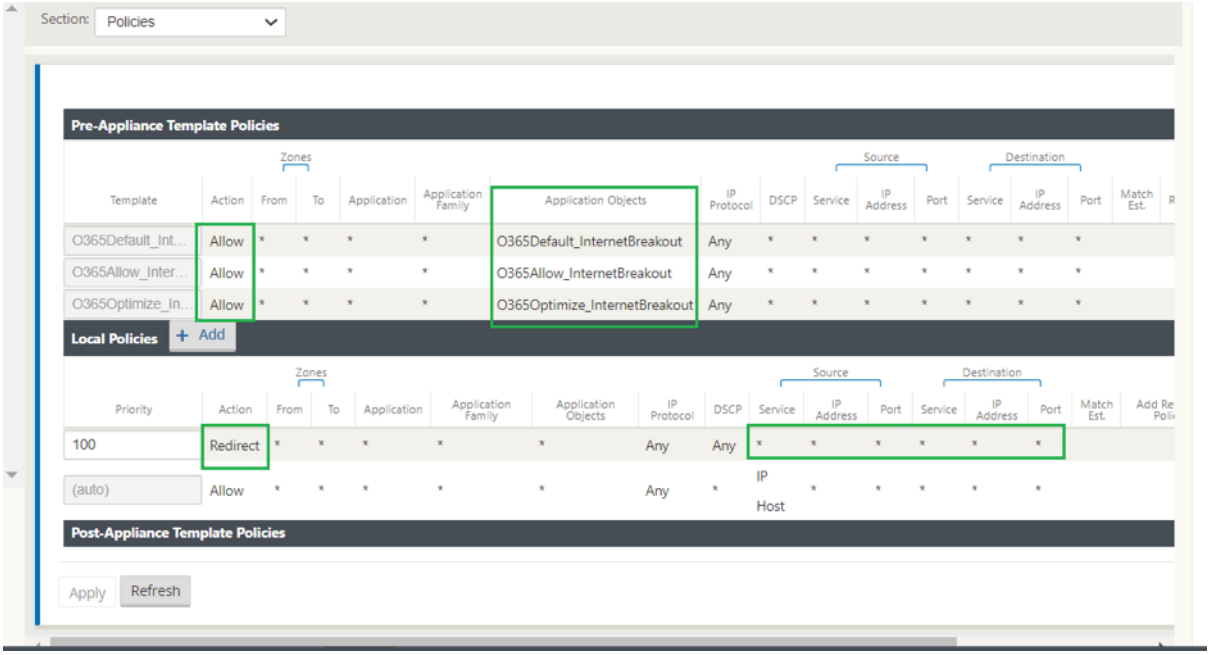


ユースケース **3:** 信頼できるインターネット **SaaS** アプリケーション用のインターネットブレークアウトを直接送信し、残りのすべてのトラフィックを **Hosted VM** にリダイレクトする

このユースケースでは、Office 365 などの信頼できる SaaS アプリケーションに対して直接インターネットブレイクアウトを実行するためのファイアウォール規則が追加されます。次のスクリーンショットに示すように、まず Office 365 ブレークアウトポリシーを有効にします。



これにより、次のスクリーンショットに示すように、Office 365 トラフィックを許可する事前アプライアンステンプレートポリシーが自動的に追加されます。次に、以下に述べるように、残りのすべてのトラフィックをホストされたファイアウォールにリダイレクトするファイアウォールルールを追加します。



> 注:
>
> ホストされたファイアウォール構成は、Citrix SD-WAN の構成とは無関係です。したがって、ホストされたファイアウォールは、企業のセキュリティ要件に従って構成できます。

リンク集約グループ

November 8, 2021

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

Citrix SD-WAN リリース 11.0 では、単純な LAG（ACTIVE-BACKUP）がサポートされています。802.3ad LACP プロトコルベースのネゴシエーションは、現在のリリースではサポートされていません。アクティブなポートは 1 つだけで、他のポートはバックアップモードになります。アクティブサポートおよびバックアップサポートは、LAG 機能についてデータプレーン開発キット (DPDK) パッケージに依存しています。LAG 機能は、次の DPDK でサポートされているプラットフォームでのみ使用できます。

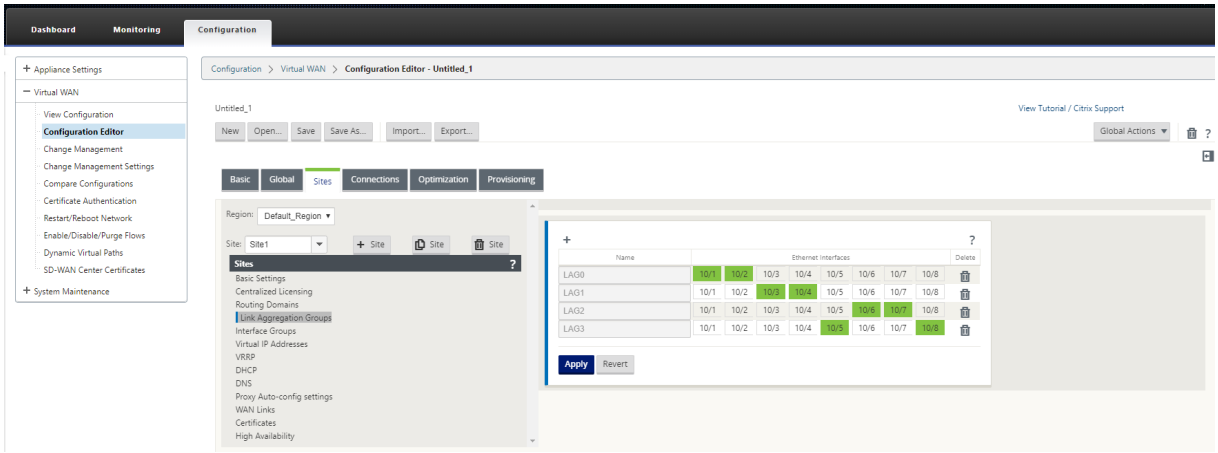
- Citrix SD-WAN 110 SE
- Citrix SD-WAN 210 SE
- Citrix SD-WAN 410 SE
- Citrix SD-WAN 1100 SE/PE
- Citrix SD-WAN 4000、4100、5100 SE
- Citrix SD-WAN 6100 SE

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

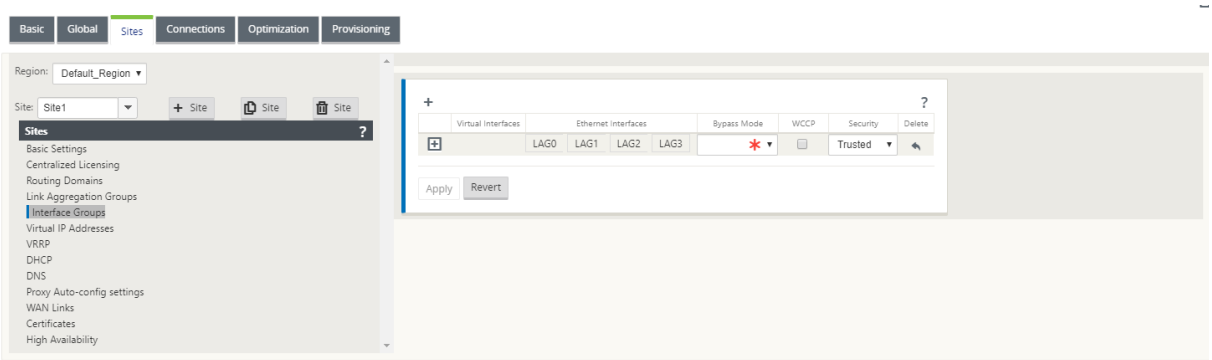
Citrix SD-WAN アプライアンスの各 LAG にグループ化された最大 4 つのポートを持つ最大 4 つの LAG を作成できます。

> 注
>
> Citrix SD-WAN 210 および 410 アプライアンスの場合、最大 3 つのポートをグループ化した LAG を 1 つだけ作成できます。

リンク集約グループを構成するには、構成エディタで、[サイト] > [リンク集約グループ] に移動します。使用可能なすべての物理ポートとイーサネットインターフェイスを表示できます。[**+**] をクリックして LAG を作成します。



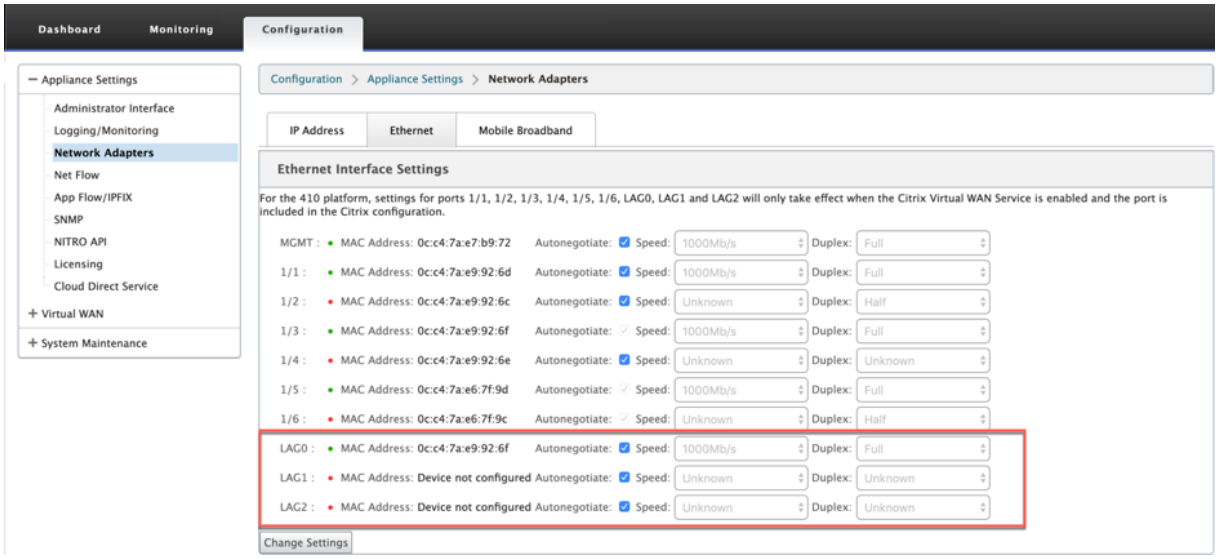
メンバーポートを選択し、[**Apply**] をクリックします。ポートが LAG に追加されると、メンバーポートではなく、インターフェイスグループ内の LAG だけが表示されます。



LAG を使用して仮想インターフェイスを作成できます。これらのインターフェイスは、LAN/WAN リンクおよび HA の設定にさらに使用されます。

> 注
>
> LAG がインターフェイスグループのイーサネットインターフェイスとして使用される場合、リンクステート伝播（LSP） 機能はサポートされません。

アクティブおよびスタンバイ LAG ポートを表示し、設定 > ** アプライアンスの設定 ** > ネットワークアダプタ > イーサネットにナビゲートできます。



> 注
>
> 個々のメンバポートの設定は変更できません。LAG に対する構成の変更は、メンバポートに自動的にプッシュされます。

リンク状態の伝播

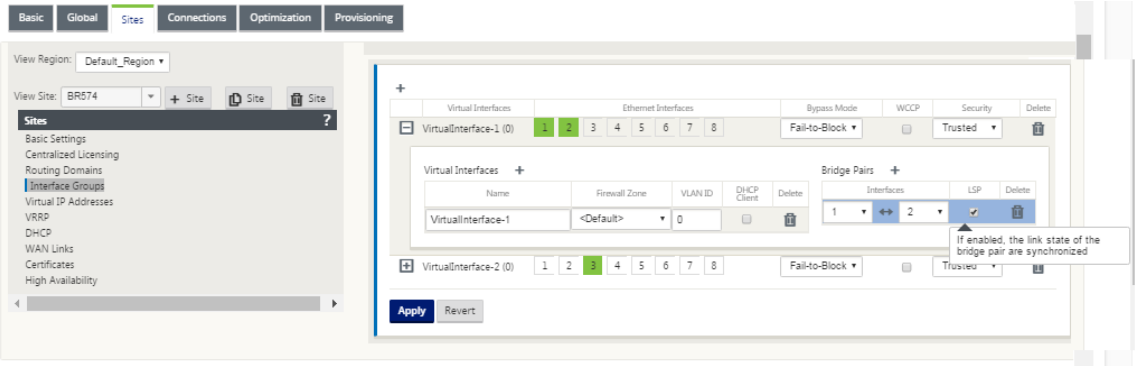
May 10, 2021

Link State Propagation（LSP; Link State Propagation）機能を使用すると、ネットワーク管理者はバイパスペアのリンクステートを同期化しておき、リンクの反対側の接続デバイスが、リンクが非アクティブであるときに表示できるようになります。バイパスペアの 1 つのポートが非アクティブになると、結合されたリンクは管理上非アクティブになります。ネットワークアーキテクチャにパラレルフェールオーバーネットワークが含まれている場合、トラフィックは強制的にそのネットワークに移行します。中断されたリンクが復元されると、対応するリンクが自動的にアクティブになります。

リンク状態の伝播を構成する方法

リンク状態の伝播を構成するには、次の手順を実行します。

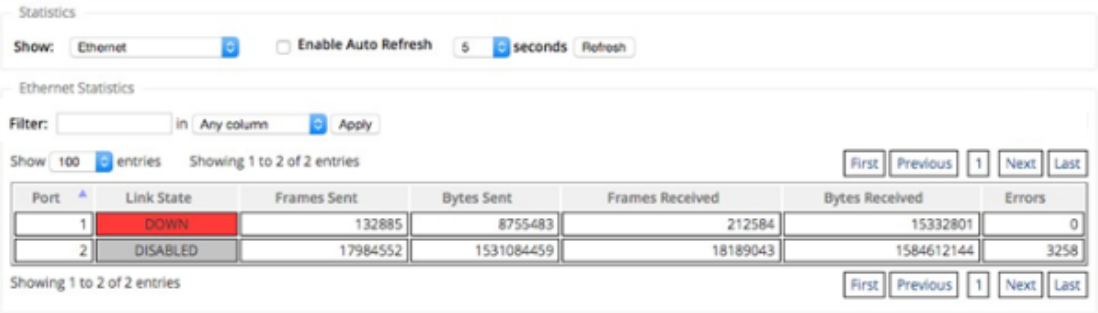
1. [構成エディタ] > [サイト**] > [**サイト **[**名**]**] > [インターフェイスグループ] に移動します。
2. [仮想インターフェイス] を展開し、[ブリッジペア] で [**LSP**] チェックボックスをクリックして、ブリッジペアの リンクステート伝播 を有効にします。[適用] をクリックして設定を保存します。



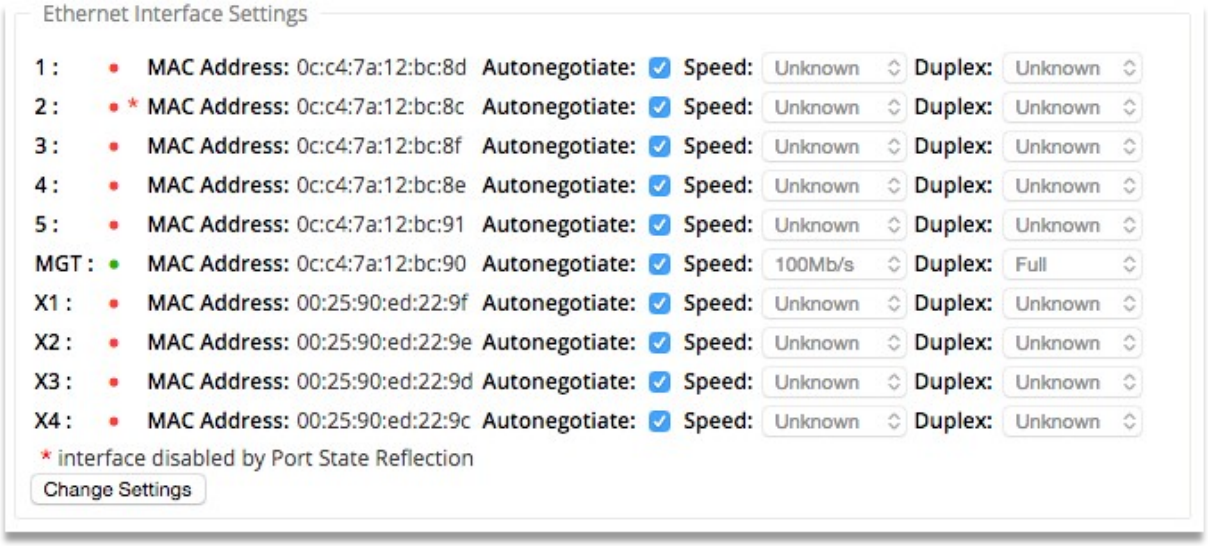
リンク統計情報のモニタリング

リンク統計情報を監視するには、次の手順を実行します。

1. **[Monitor] > [Statistics**] ページで、[**Show**] ドロップダウンメニューから [**Ethernet**] を選択して、リンク状態伝播を有効にしたバイパスポートペアのステータスを表示します。LAN 側リンクがダウンし、後でバイパスペアの WAN 側リンクが管理上 Disabled になっていることに注意します。



2. 構成 **>** アプライアンスの設定 **>** ネットワークアダプタ **>** イーサネットタブに移動します。管理上ダウンしているポートは、[**Ethernet Interface Settings]** リストに赤色のアスタリスク（*）で示されます。



メータリングおよびスタンバイ **WAN** リンク

May 10, 2021

Citrix SD-WAN では、従量制課金リンクの有効化がサポートされています。これは、使用可能な他のすべての WAN リンクが無効になっているときに、ユーザーのトラフィックが特定のインターネット WAN リンクでのみ転送されるように構成できます。

従量制課金リンクは、使用量に基づいて請求されるリンクの帯域幅を節約します。従量制課金リンクを使用すると、リンクを [Last Resort] リンクとして設定できます。これにより、他のすべての従量制課金リンクが停止または低下するまで、リンクの使用が許可されません。[最後のリゾート設定] は、通常、サイトへの WAN リンク (MPLS、ブロードバンドインターネット、4G/LTE) が 3 つあり、WAN リンクの 1 つが 4G/LTE であり、必要でない限り使用を許可するにはコストがかかりすぎる可能性があります。メータリングはデフォルトでは有効になっていないため、任意のアクセスタイプ（パブリックインターネット、プライベート MPLS、プライベートイントラネット）の WAN リンクで有効にできます。メータリングが有効な場合は、必要に応じて次の項目を設定できます。

- データキャップ
- 請求サイクル（週次/月次）
- 開始日
- スタンバイモード
- 優先度
- Active heartbeat interval：少なくともハートビート間隔の間パス上にトラフィック（ユーザー/コントロール）がない場合に、アプライアンスから仮想パスの反対側のピアにハートビートメッセージが送信される間隔

ローカルの従量制課金リンクでは、アプライアンスのダッシュボードの下部に **WAN** リンクメータリング テーブルが表示され、メータリング情報が示されます。

ローカルの従量制課金リンクでの帯域幅使用率は、設定されたデータキャップに対して追跡されます。使用量が構成済みデータ上限の 50%、75%、または 90% を超えると、アプライアンスはユーザーに警告するイベントを生成し、アプライアンスのダッシュボードの上部に警告バナーが表示されます。この使用状況アラートイベントは、SD-WAN Center でも表示できます。従量制課金パスは、1 つまたは 2 つの従量制課金リンクで形成できます。2 つの従量制課金リンク間にパスが形成されている場合、従量制課金パスで使用されるアクティブハートビートインターバルは、リンクで設定された 2 つのアクティブハートビートインターバルのうち大きい方になります。

従量制課金パスは非スタンバイパスであり、常にユーザトラフィックに適格です。GOOD 状態にある非従量制課金パスが少なくとも 1 つある場合、従量制課金パスは制御トラフィックの量を削減し、フォワーディングプレーンがパスを検索するときに回避されます。

スタンバイモード

WAN リンクのスタンバイモードは、デフォルトで無効になっています。スタンバイモードを有効にするには、次の 2 つのモードのどちらでスタンバイリンクが動作するかを指定する必要があります。

- オンデマンド：いずれかの条件が満たされたときにアクティブになるスタンバイリンク。

  仮想パスで使用可能な帯域幅が、設定されたオンデマンド帯域幅制限よりも小さく、十分な使用量がある場合。十分な使用量は、現在の使用可能な帯域幅の 95% 以上（ON_DEMAND_USAGE_THRESHOLD_PCT）として定義されるか、現在の使用可能な帯域幅と現在の使用量の差が 250 kbps 未満（ON_DEMAND_THRESHOLD_GAP_KBPS）の場合、両方のパラメータは t2_variables を使用して変更できます。パスが無効になっているか、無効になっています。

- **Last-resort**： すべての非スタンバイリンクおよびオンデマンドスタンバイリンクがデッドまたは無効になったときにだけアクティブになるスタンバイリンク。

- スタンバイプライオリティは、スタンバイリンクが複数ある場合に、スタンバイリンクがアクティブになる順序を示します。

  - プライオリティ 1 のスタンバイリンクが先にアクティブになり、プライオリティ 3 のスタンバイリンクが最後にアクティブになります

  - 複数のスタンバイリンクに同じプライオリティを割り当てることができます

スタンバイリンクを設定する場合、スタンバイプライオリティと 2 つのハートビートインターバルを指定できます。

- アクティブハートビート間隔：スタンバイパスがアクティブなときに使用されるハートビート間隔（デフォルト 50ms/1s/2s/3s/4s/5s/6s/7s/8s/9s/10s）

- スタンバイハートビート間隔：スタンバイパスが非アクティブのときに使用されるハートビート間隔（デフォルトは 1s/2s/3s/4s/5s/6s/7s/8s/9s/10s/無効）

スタンバイパスは、1 つまたは 2 つのスタンバイリンクで形成されます。

- **On** -Demand：オンデマンドスタンバイパスは次の間で形成されます。

  - 非スタンバイリンクとオンデマンドスタンバイリンク
  - 2 つのオンデマンドスタンバイリンク

- **last-resort**： 最後のリゾートスタンバイパスは次の間に形成されます。

  - 非スタンバイリンクおよび最終リゾートスタンバイリンク
  - オンデマンドスタンバイリンクおよびラストリゾートスタンバイリンク
  - 2 つの最終リゾートスタンバイリンク

スタンバイパスで使用されるハートビートインターバルは、次のように決定されます。

- 2 つのリンクのうち少なくとも 1 つでスタンバイハートビートが無効になっている場合、非アクティブな間はスタンバイパスでハートビートが無効になります。
- いずれかのリンクでスタンバイハートビートが無効になっていない場合、スタンバイパスがスタンバイのときに 2 つの値のうち大きい方が使用されます。

- 両方のリンクでアクティブハートビートインターバルが設定されている場合、スタンバイパスがアクティブなときに 2 つの値のうち大きい方が使用されます。

ハートビート (キープアライブ) メッセージ:

- 非スタンバイパスでは、ハートビートメッセージが送信されるのは、少なくともハートビートインターバルの間にトラフィック（制御またはユーザ）がない場合だけです。ハートビート間隔は、パスの状態によって異なります。非スタンバイ、非従量制課金 パスの場合：
  - パス状態が GOOD の場合、50 ミリ秒
  - パス状態が BAD の場合、25 ミリ秒

スタンバイパスでは、使用されるハートビート間隔は、アクティビティ状態とパスの状態によって異なります。

- 非アクティブの間、ハートビートが無効になっていない場合、ハートビートメッセージは設定されたスタンバイハートビート間隔で定期的に送信されます。これは、他のトラフィックが許可されていないためです。
- パス状態が GOOD の場合に、設定されたアクティブハートビートインターバルが使用されます。
- パスの状態が BAD の場合、設定されたアクティブハートビートインターバル 1/2 が使用されます。
- 非スタンバイパスと同様に、アクティブ中は、少なくとも設定されたアクティブハートビートインターバルの間にトラフィック（制御またはユーザ）がない場合に限り、ハートビートメッセージが送信されます。
- パス状態が GOOD の場合に、設定されたスタンバイハートビートインターバルが使用されます。
- パスの状態が BAD の場合、設定されたスタンバイハートビートインターバルの 1/2 が使用されます。

非アクティブの場合、スタンバイパスはユーザトラフィックに対して適格ではありません。非アクティブなスタンバイパスで送信される制御プロトコルメッセージは、ハートビートメッセージだけです。ハートビートメッセージは、接続障害検出および品質メトリックの収集用です。スタンバイパスがアクティブの場合、時間コストを追加したユーザトラフィックに適格です。これは、フォワーディングパスの選択中に非スタンバイパスが使用可能な場合、そのパスが優先されるようにするために行われます。

非アクティブのハートビートが無効になっているスタンバイパスのパス状態は、GOOD であると見なされ、[**Monitoring**] の [Path Statistics] テーブルに GOOD と表示されます。アクティブになると、仮想パスピアから聞くまで DEAD 状態で開始される非スタンバイパスとは異なり、GOOD 状態で開始されます。仮想パスピアとの接続が検出されない場合、パスは BAD になり、次に DEAD になります。仮想パスピアとの接続が再確立されると、パスが BAD になり、その後再び GOOD になります。

このようなスタンバイパスが DEAD になってから非アクティブになった場合、パスの状態は（仮定）GOOD に変更されません。その代わり、すぐに使用できないように、時間の間 DEAD 状態に保たれます。これは、正常な DEAD パスを想定した低いプライオリティのパスグループと、実際に GOOD パスを持つ高いプライオリティのパスグループの間でアクティビティが振動するのを防ぐためです。この保留期間 (NO_HB_PATH_ON_HOLD_PERIOD_MS) は 5 分に設定され、t2_ 変数を使用して変更できます。

仮想パスでパス MTU 検出が有効になっている場合、パスがスタンバイ状態の間、スタンバイパスの MTU は仮想パスの MTU の計算に使用されません。スタンバイパスがアクティブになると、仮想パスの MTU は、スタンバイパス

の MTU を考慮して再計算されます。（仮想パスの MTU は、仮想パス内のすべてのアクティブパスの中で最小のパス MTU です）。

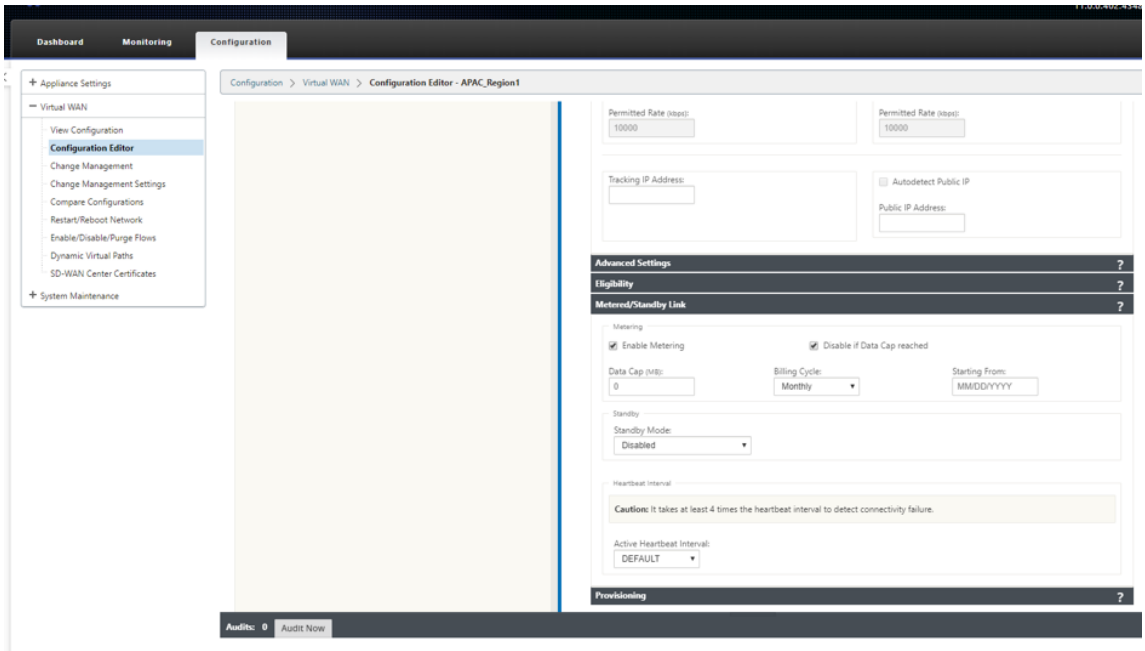
スタンバイパスがスタンバイとアクティブの間で移行すると、イベントとログメッセージが生成されます。

構成の前提条件：

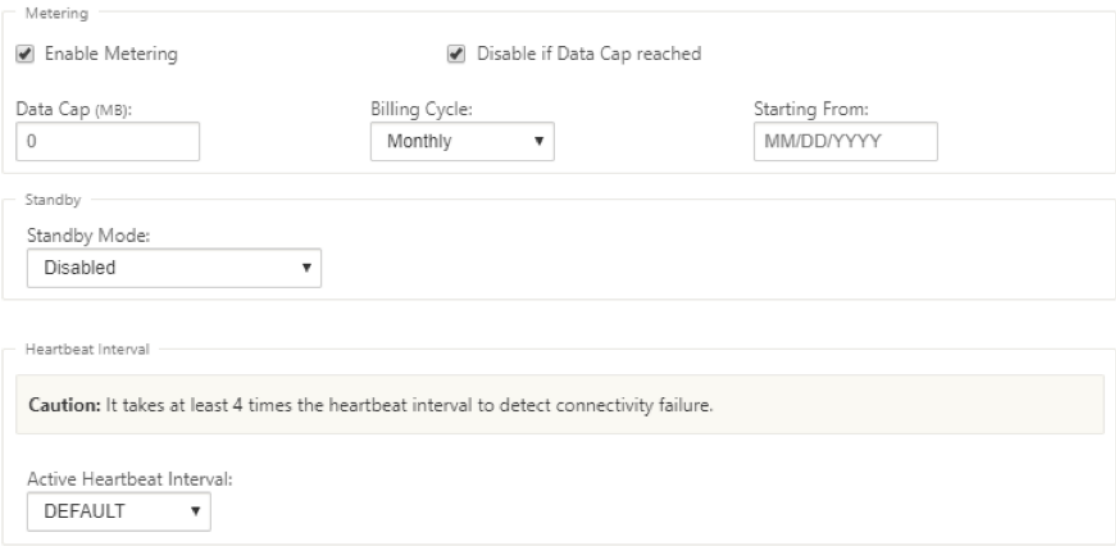
- メーターリンクは、任意のアクセスタイプである場合があります。
- サイトのすべてのリンクは、メータリングを有効にして構成できます。
- スタンバイリンクは、[パブリックインターネット] または [プライベートイントラネット] のアクセスタイプです。プライベート MPLS アクセスタイプの WAN リンクは、スタンバイリンクとして設定できません。
- サイトごとに少なくとも 1 つの非スタンバイリンクを設定する必要があります。サイトごとに最大 3 つのスタンバイリンクがサポートされます。
- インターネット/イントラネットサービスは、オンデマンドスタンバイリンクで構成されていない可能性があります。オンデマンドスタンバイリンクは、仮想パスサービスのみをサポートします。
- インターネットサービスは、last-resort スタンバイリンクで設定されている場合がありますが、サポートされているのは負荷分散モードだけです。
- イントラネットサービスは、ラストリゾートスタンバイリンクで構成されている可能性がありますが、サポートされているのはセカンダリモードのみで、プライマリ再要求を有効にする必要があります。

従量制課金リンクを設定するには:

1. SD-WAN Web 管理インターフェイスで、[構成**] > [**仮想 **WAN]** の順に選択し、[構成エディタ**] >** を選択し、ドロップダウンリストから [サイト] を追加または選択し、[**WAN** リンク**] >** [**Metered/Standby Link**] タブをクリックして.it を拡張します。



2. [メータリングを有効にする] チェックボックスをオンにします。[データ上限]、[請求サイクルの開始日]、および [アクティブハートビート間隔] の値を指定できます。

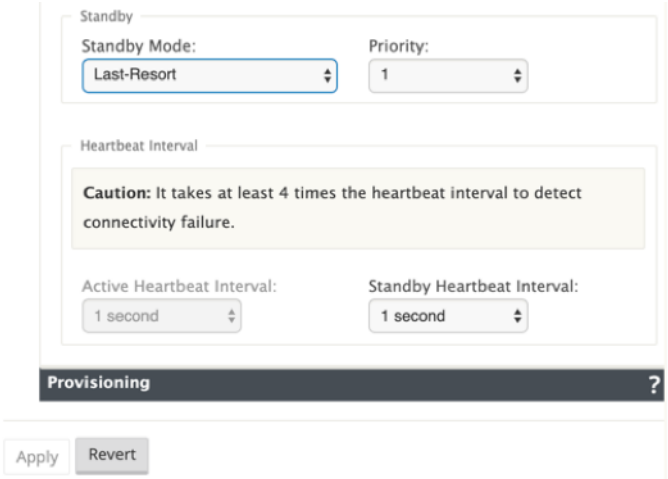


3. データ上限に達した場合は無効にします。

   - [データ上限に達した場合に無効にする] チェックボックスがオンの場合、データ使用量がデータ上限に達すると、次回の請求サイクルまで、従量制課金リンクとその関連パスがすべて無効になります。
   - デフォルトでは、[データ上限に達した場合に無効にする] チェックボックスはオフの状態になります。このチェックボックスは、データ上限に達した後も次の請求サイクルまで継続される従量制課金リンクに設定された現在のモードまたは状態を保持します。

スタンバイリンクを設定するには、次の手順を実行します。

1. デフォルトでは、WAN リンクのスタンバイモードは無効です。WAN リンクをスタンバイとして設定するには、ドロップダウンリストからいずれかのスタンバイモード（Last-Resort/On-Demand）を選択します。

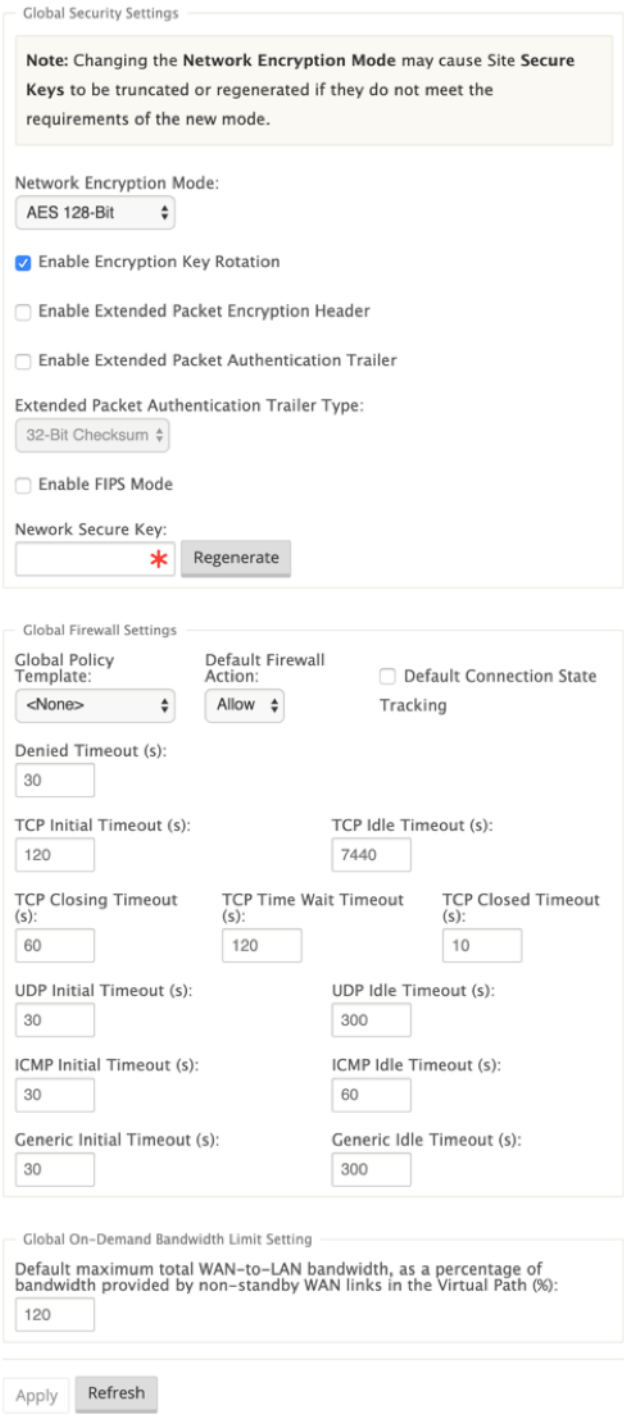


2. スタンバイモードを選択したら、スタンバイプライオリティ、アクティブハートビートインターバル、およびスタンバイハートビートインターバルを適宜選択します。[適用] をクリックして、設定を検証します。

3. オンデマンドスタンバイリンクが設定されている場合、グローバルなデフォルトのオンデマンド帯域幅制限（120%）が仮想パスに適用されます。これは、仮想パスで許可される WAN-to-LAN 帯域幅の最大値を指定し

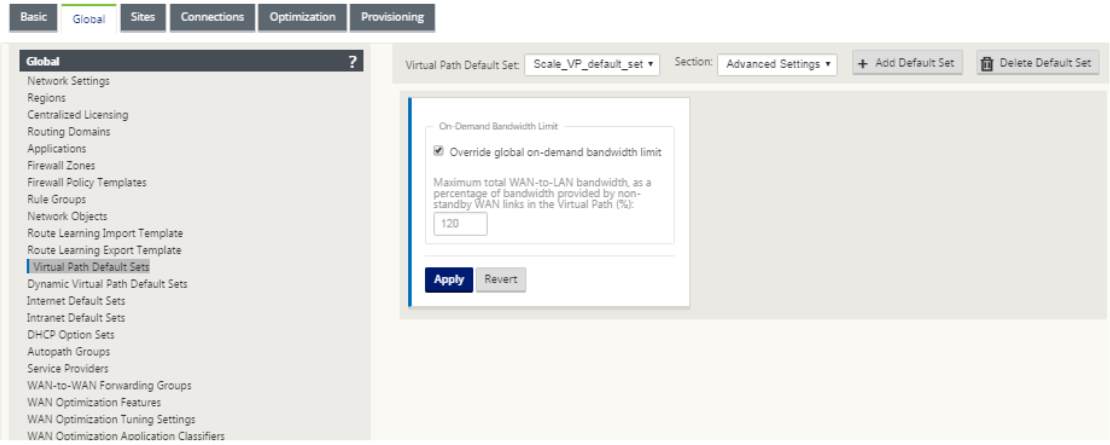
ます。これは、仮想パス内のすべての非スタンバイリンクによって提供される総帯域幅に対するパーセンテージで表されます。仮想パスで使用可能な帯域幅が制限を下回っている限り、十分な使用量があれば、アプライアンスは帯域幅を補完するためにオンデマンドパスをアクティブ化しようとします。

4. グローバルなデフォルトのオンデマンド帯域幅制限を表示または変更するには、[グローバル] > [仮想 **WAN** ネットワーク 設定] セクションを開きます。

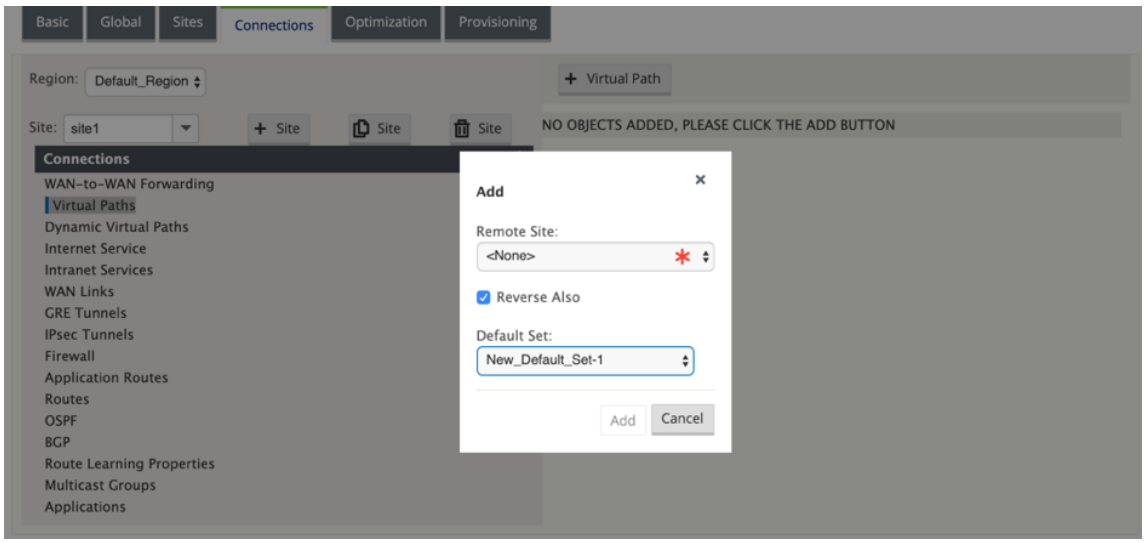


5. 仮想パスに固有のオンデマンド帯域幅制限を適用し、グローバルなデフォルト設定を変更しない場

合は、仮想パスのデフォルトセットを作成し、[詳細設定] でオンデマンド帯域幅制限を変更できます。



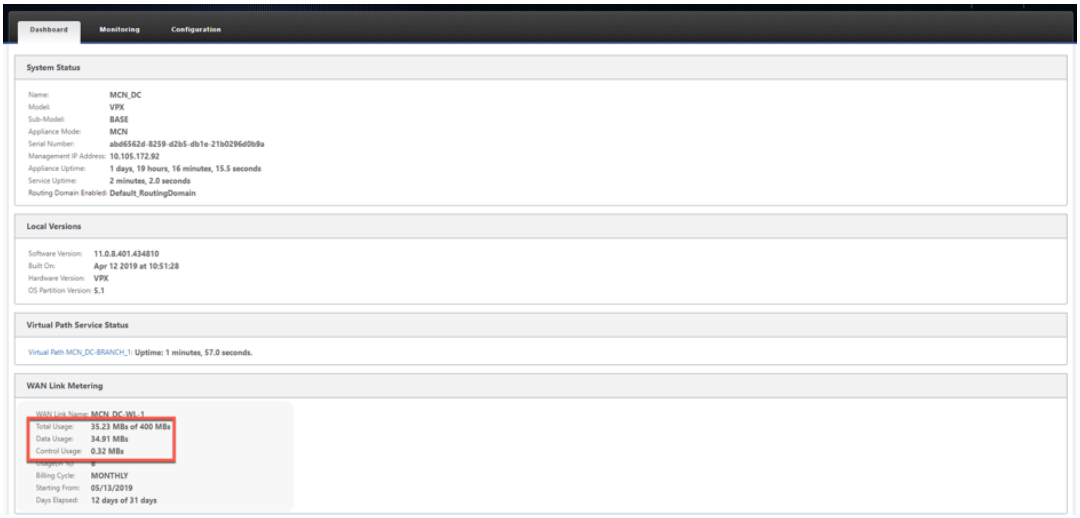
6. 特定の仮想パスに設定を適用するには、[接続] **>** [仮想パス] セクションに移動し、[**+** 仮想パス] をクリックします。



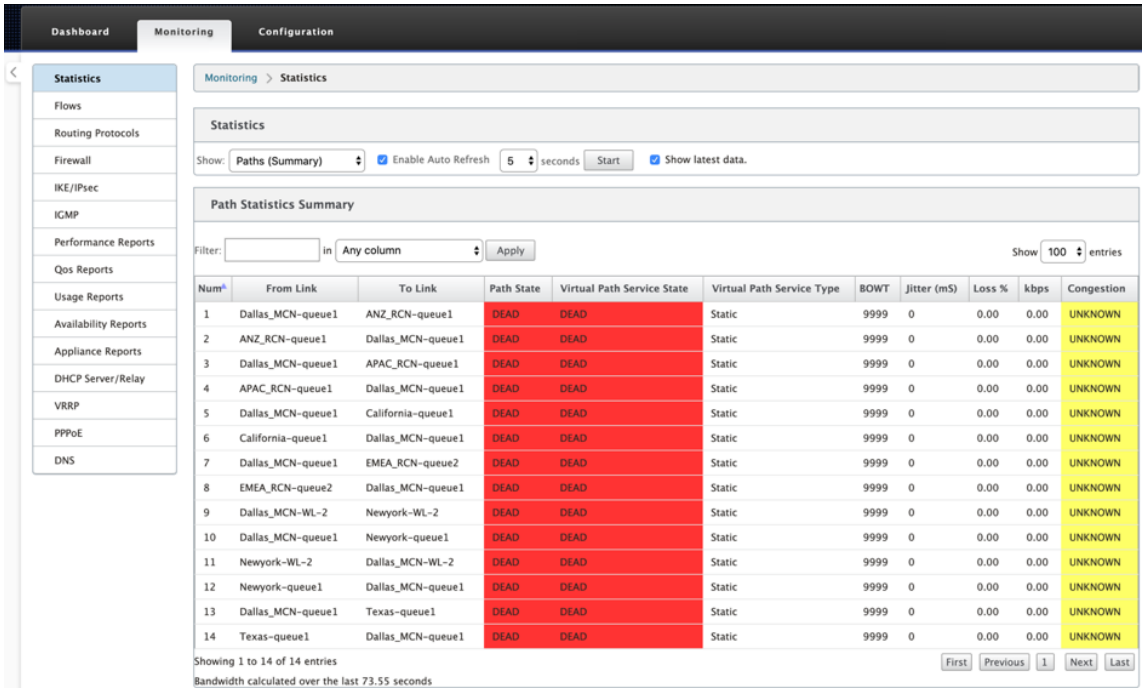
従量制課金およびスタンバイ **WAN** リンクの監視

- [ダッシュボード] ページには、次の **WAN** リンクメータリング 情報と使用値が表示されます。
  - **WAN** リンク名: WAN リンク名を表示します。
  - 合計使用量: 合計トラフィック使用量（データ使用量 + 制御使用量）が表示されます。
  - [データ使用状況]: ユーザートラフィック別の使用状況を表示します。
  - 制御の使用状況: 制御トラフィックごとの使用状況を表示します。
  - 使用量 **(%)**: 使用済みデータ上限値をパーセンテージ (合計使用量/データ上限値) x 100 で表示します。
  - 請求サイクル: 請求頻度 (週単位/月単位)

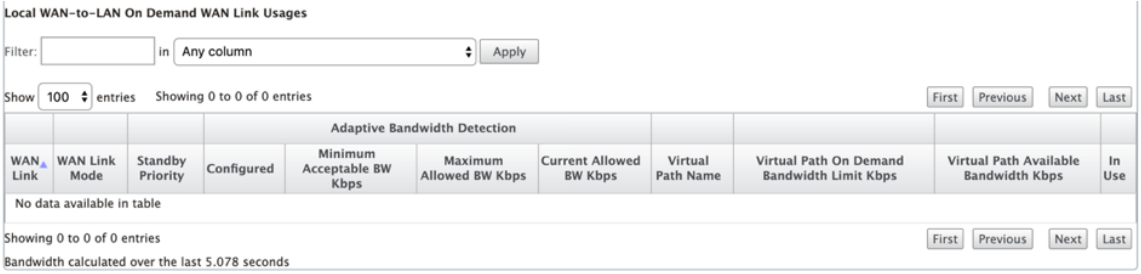
- 開始日: 請求サイクルの開始日
- 経過日数：経過時間（日、時、分、秒単位）



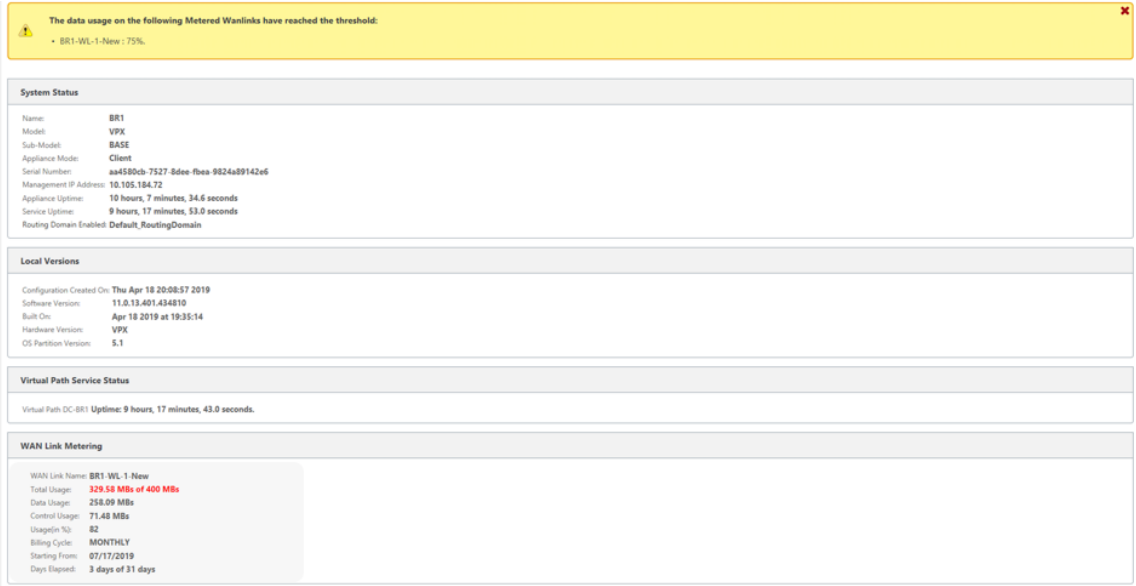
- パス統計（[モニタリング] > [統計] > [パス]）が表示されると、スクリーンショットのように従量制課金リンクとスタンバイリンクがマークされます。



- ローカルまたはリモートのオンデマンドスタンバイリンクを持つ仮想パスがアプライアンスに存在する場合、WAN リンクの使用状況の統計情報を表示すると、ページの下部にオンデマンド帯域幅を示す追加のテーブルが表示されます（[モニタリング] > [統計] > [**WAN** リンクの使用状況]）。



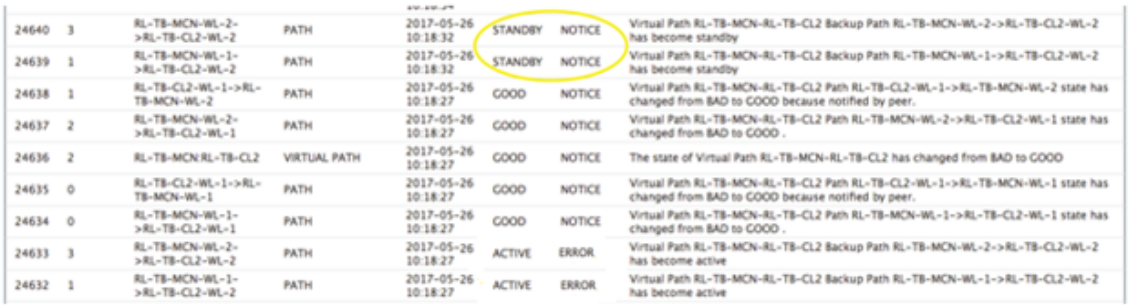
- 従量制課金リンクの使用量が、設定されたデータ上限の 50% を超えると、ダッシュボードの上部に警告バナーが表示されます。さらに、使用量が構成済みのデータ上限の 75% を超えると、ダッシュボードの下部に向けた数値計測情報が強調表示されます。



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

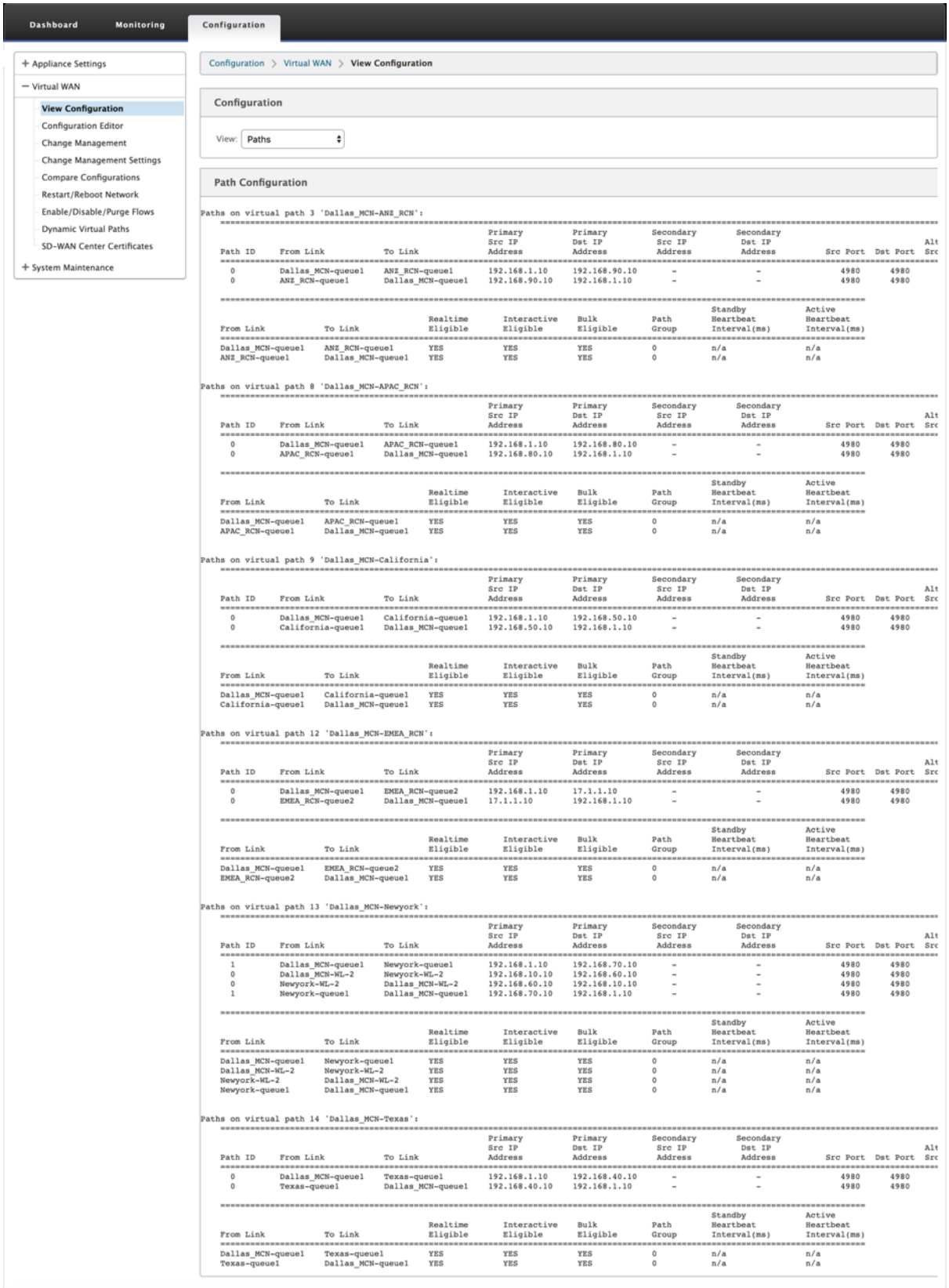
17654	1	RL-TB-CL1-WL-2	WAN LINK	2017-05-24 10:22:58	USAGE_3	WARNING	Total usage 1.84 GBytes used (91% of limit 2.00 GBytes) in 1 of 31 days in this billing cycle since 00:00:00 05/24/2017
17653	1	RL-TB-CL1-WL-2	WAN LINK	2017-05-24 10:17:58	USAGE_2	WARNING	Total usage 1.52 GBytes used (75% of limit 2.00 GBytes) in 1 of 31 days in this billing cycle since 00:00:00 05/24/2017
17652	1	RL-TB-CL1-WL-2	WAN LINK	2017-05-24 10:09:58	USAGE_1	WARNING	Total usage 1.00 GBytes used (50% of limit 2.00 GBytes) in 1 of 31 days in this billing cycle since 00:00:00 05/24/2017

1. スタンバイパスがスタンバイ状態とアクティブ状態の間で移行すると、アプライアンスによってイベントが生成されます。



24640	3	RL-TB-MCN-WL-2->RL-TB-CL2-WL-2	PATH	2017-05-26 10:18:32	STANDBY	NOTICE	Virtual Path RL-TB-MCN-RL-TB-CL2 Backup Path RL-TB-MCN-WL-2->RL-TB-CL2-WL-2 has become standby
24639	1	RL-TB-MCN-WL-1->RL-TB-CL2-WL-2	PATH	2017-05-26 10:18:32	STANDBY	NOTICE	Virtual Path RL-TB-MCN-RL-TB-CL2 Backup Path RL-TB-MCN-WL-1->RL-TB-CL2-WL-2 has become standby
24638	1	RL-TB-CL2-WL-1->RL-TB-MCN-WL-2	PATH	2017-05-26 10:18:27	GOOD	NOTICE	Virtual Path RL-TB-MCN-RL-TB-CL2 Path RL-TB-CL2-WL-1->RL-TB-MCN-WL-2 state has changed from BAD to GOOD because notified by peer.
24637	2	RL-TB-MCN-WL-2->RL-TB-CL2-WL-1	PATH	2017-05-26 10:18:27	GOOD	NOTICE	Virtual Path RL-TB-MCN-RL-TB-CL2 Path RL-TB-MCN-WL-2->RL-TB-CL2-WL-1 state has changed from BAD to GOOD .
24636	2	RL-TB-MCN:RL-TB-CL2	VIRTUAL PATH	2017-05-26 10:18:27	GOOD	NOTICE	The state of Virtual Path RL-TB-MCN-RL-TB-CL2 has changed from BAD to GOOD
24635	0	RL-TB-CL2-WL-1->RL-TB-MCN-WL-1	PATH	2017-05-26 10:18:27	GOOD	NOTICE	Virtual Path RL-TB-MCN-RL-TB-CL2 Path RL-TB-CL2-WL-1->RL-TB-MCN-WL-1 state has changed from BAD to GOOD because notified by peer.
24634	0	RL-TB-MCN-WL-1->RL-TB-CL2-WL-1	PATH	2017-05-26 10:18:27	GOOD	NOTICE	Virtual Path RL-TB-MCN-RL-TB-CL2 Path RL-TB-MCN-WL-1->RL-TB-CL2-WL-1 state has changed from BAD to GOOD .
24633	3	RL-TB-MCN-WL-2->RL-TB-CL2-WL-2	PATH	2017-05-26 10:18:27	ACTIVE	ERROR	Virtual Path RL-TB-MCN-RL-TB-CL2 Backup Path RL-TB-MCN-WL-2->RL-TB-CL2-WL-2 has become active
24632	1	RL-TB-MCN-WL-1->RL-TB-CL2-WL-2	PATH	2017-05-26 10:18:27	ACTIVE	ERROR	Virtual Path RL-TB-MCN-RL-TB-CL2 Backup Path RL-TB-MCN-WL-1->RL-TB-CL2-WL-2 has become active

2. 各パスに設定されたアクティブハートビート間隔とスタンバイハートビート間隔は、[構成**] > [** 仮想 WAN**] > [構成の ** 表示] > [パス] で確認できます。



Office 365 の最適化

May 10, 2021

Office 365 の最適化 機能は、Microsoft Office 365 のネットワーク接続に関する原則に準拠し Office 365 を最適化します。Office 365 は、グローバルに配置された複数のサービスエンドポイント (フロントドア) を通じてサービスとして提供されます。Office 365 トラフィックの最適なユーザーエクスペリエンスを実現するために、Microsoft では、Office 365 トラフィックをブランチ環境から直接インターネットにリダイレクトし、中央プロキシへのバックホールなどのプラクティスを回避することをお勧めします。これは、Outlook や Word などの Office 365 トラフィックが遅延の影響を受けやすく、バックホートラフィックによって遅延が増え、ユーザーエクスペリエンスが低下するためです。Citrix SD-WAN を使用すると、インターネットへの Office 365 トラフィックを突破するポリシーを構成できます。

Office 365 トラフィックは、世界中の Microsoft Office 365 インフラストラクチャのエッジに存在する最も近い Office 365 サービスエンドポイントに送信されます。トラフィックがフロントドアに到達すると、それは Microsoft のネットワークを経由し、実際の宛先に到達します。これにより、お客様のネットワークから Office 365 エンドポイントへの往復時間が短縮されるにつれて、待ち時間が最小限に抑えられます。

Office 365 エンドポイント

Office 365 エンドポイントは、ネットワークアドレスとサブネットのセットです。エンドポイントは、次の 3 つのカテゴリに分類されます。

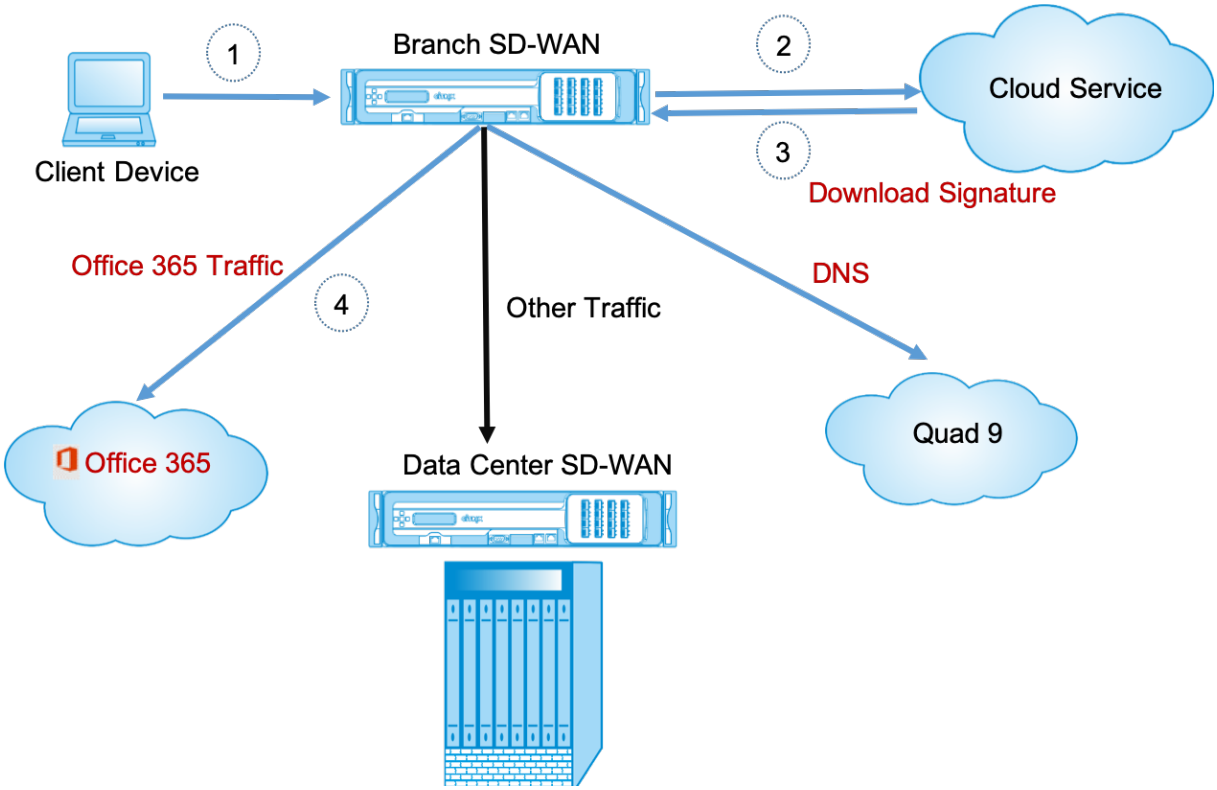
- 最適化 -これらのエンドポイントは、すべての Office 365 サービスと機能への接続を提供し、可用性、パフォーマンス、およびレイテンシーに非常に敏感です。Office 365 の帯域幅、接続、データ量の 75% 以上を占めています。すべての Optimize エンドポイントは、Microsoft データセンターでホストされます。これらのエンドポイントへのサービスリクエストは、ブランチからインターネットにブレークアウトし、データセンターを通過しないようにする必要があります。
- 許可 -これらのエンドポイントは、特定の Office 365 サービスおよび機能への接続のみを提供し、ネットワークのパフォーマンスと待ち時間にはそれほど敏感ではありません。Office 365 の帯域幅と接続数の表現も大幅に低くなっています。これらのエンドポイントは、Microsoft データセンターでホストされます。これらのエンドポイントへのサービスリクエストは、ブランチからインターネットにブレークアウトしたり、データセンターを経由したりする場合があります。
- デフォルト -これらのエンドポイントは、最適化を必要としない Office 365 サービスを提供し、通常のインターネットトラフィックとして扱うことができます。これらのエンドポイントの一部は、Microsoft データセンターでホストされていない可能性があります。このカテゴリのトラフィックは、遅延の変化の影響を受けません。したがって、このタイプのトラフィックを直接遮断しても、インターネットのブレイクアウトと比較してパフォーマンスが向上することはありません。また、このカテゴリのトラフィックが常に Office 365 トラフィックであるとは限りません。したがって、ネットワークで Office 365 ブレイクアウトを有効にする場合は、このオプションを無効にすることをお勧めします。

Office 365 の最適化の仕組み

Microsoft エンドポイントの署名は最大で 1 日に 1 回更新されます。アプライアンス上のエージェントは、毎日 Citrix サービス（sdwan-app-routing.citrixnetworkapi.net）をポーリングして、最新のエンドポイント署名のセットを取得します。SD-WAN アプライアンスは、アプライアンスの電源がオンになり、Office 365 の最適化が有効になっているときに、Citrix サービス（sdwan-app-routing.citrixnetworkapi.net）を毎日 1 回ポーリングします。使用可能な新しいシグニチャがある場合、アプライアンスはそのシグニチャをダウンロードし、データベースに保存します。シグニチャは、基本的に、どのトラフィックステアリングポリシーを構成できるかに基づいて Office 365 トラフィックを検出するために使用される URL と IP のリストです。

> 注:
>
> Office 365 トラフィックの最初のパケット検出と分類は、Office 365 ブレークアウト機能が有効な場合にのみ実行されます。

Office 365 アプリケーションの要求が到着すると、アプリケーション分類子は、最初のパケット分類子のデータベース検索を実行し、Office 365 トラフィックを識別し、マークします。Office 365 トラフィックが分類されると、自動作成されたアプリケーションルートとファイアウォールポリシーが有効になり、インターネットに直接トラフィックが遮断されます。Office 365 の DNS 要求は、Quad9 などの特定の DNS サービスに転送されます。詳しくは、「ドメイン・ネーム・システム」を参照してください。



署名は、クラウドサービス（sdwan-app-routing.citrixnetworkapi.net）からダウンロードされます。

Office 365 ブレークアウトを構成する

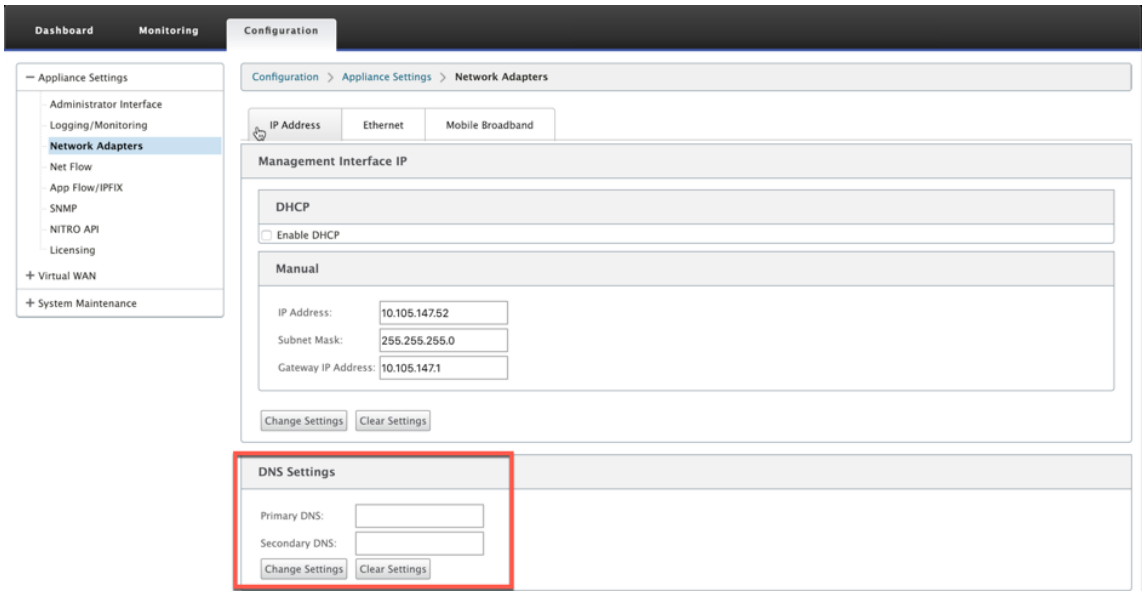
Office 365 ブレイクアウトポリシーでは、ブランチから直接抜け出すことができる Office 365 トラフィックのカテゴリを指定できます。Office 365 ブレークアウトを有効にして構成をコンパイルすると、DNS オブジェクト、アプリケーションオブジェクト、アプリケーションルート、およびファイアウォールポリシーテンプレートが自動的に作成され、インターネットサービスを持つブランチサイトに適用されます。

前提条件

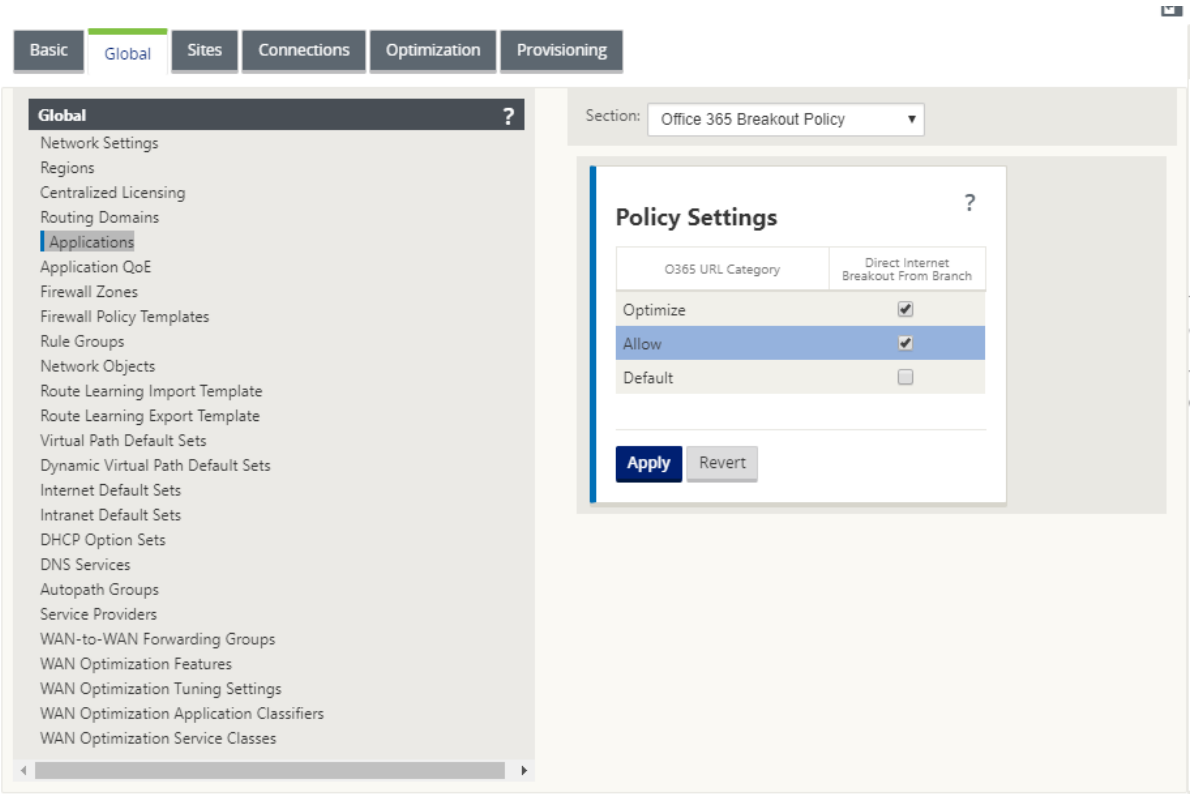
次の項目があることを確認します。

1. Office 365 のブレイクアウトを実行するには、アプライアンスでインターネットサービスを構成する必要があります。インターネットサービスの設定の詳細については、インターネットアクセスを参照してください。
2. 管理インターフェイスにインターネット接続があることを確認します。

   Citrix SD-WAN Web インターフェイスを使用して、管理インターフェイスの設定を構成できます。
3. 管理 DNS が設定されていることを確認します。管理インターフェイスの DNS を設定するには、[構成] **>** [アプライアンスの設定] **>** [ネットワークアダプタ] に移動します。[**DNS** 設定] セクションで、プライマリ DNS サーバーとセカンダリ DNS サーバーの詳細を指定し、[設定の変更] をクリックします。

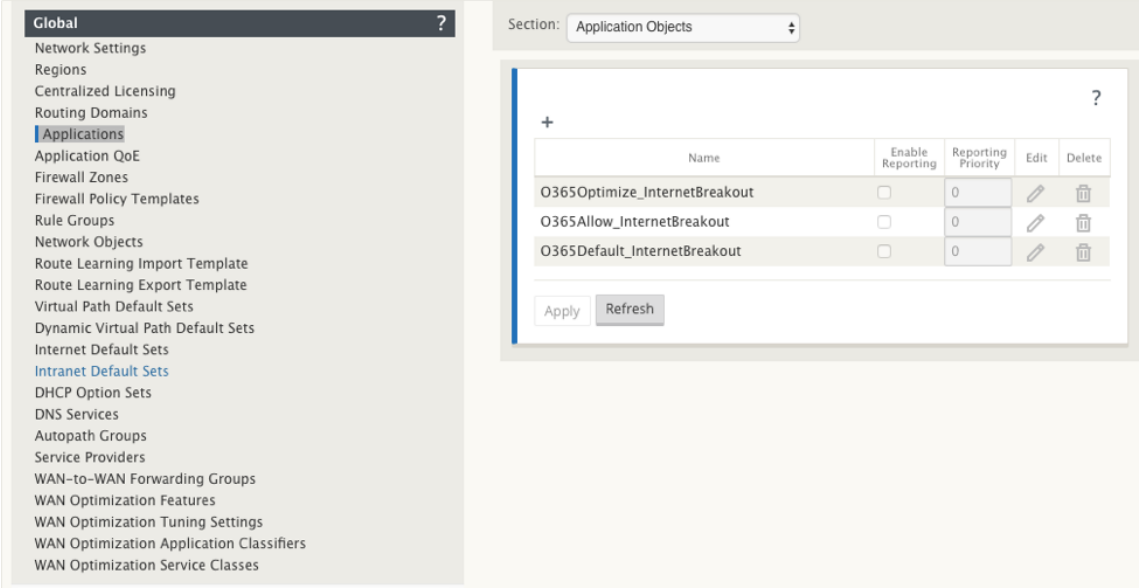


[**Office 365** ブレイクアウトポリシー] 設定は、[グローバル設定] の下で使用できます。インターネットブレイクアウトに必要な Office 365 カテゴリを選択し、[適用] をクリックします。

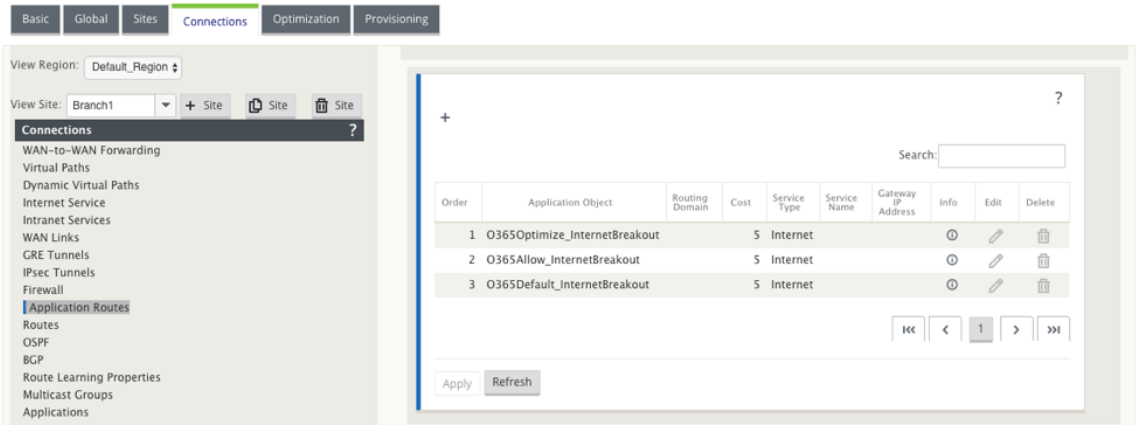


Office 365 を構成した後、ポリシー設定をブレークアウトし、構成をコンパイルします。次の設定は自動入力されます。

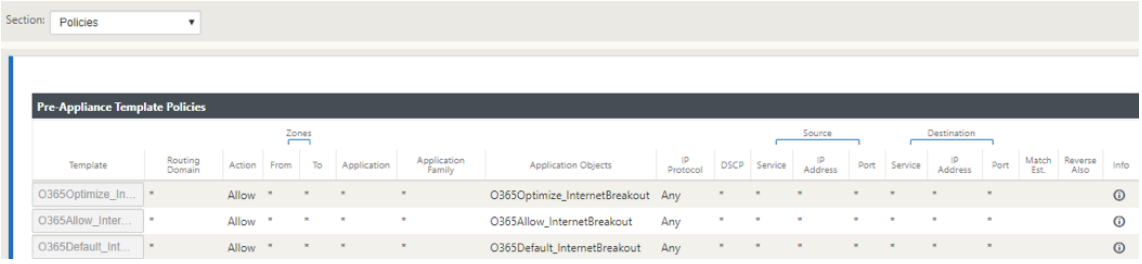
- **DNS** オブジェクト -DNS オブジェクトは、ユーザーが構成されている DNS サービスに転送するトラフィックの種類を指定します。DNS 要求はすべての信頼されたインターフェイスで受信され、DNS フォワーダーは Office 365 の DNS 要求を Quad9 サービスに送信するために含まれます。このフォワーダ規則は、最も高い優先順位を取ります。詳細については、「ドメインネームサービス」セクションを参照してください。
- アプリケーションオブジェクト -ユーザーが選択した Office 365 カテゴリを持つアプリケーションオブジェクトが作成されます。最適化、許可、およびデフォルトのカテゴリを選択した場合は、アプリケーション・オブジェクト **O365Optimize_InternetBreakout**、**O365Allow_InternetBreakout** 、**O365Default_InternetBreakout** が作成されます。



- アプリケーションルート: アプリケーションルートは、インターネットサービスの種類の Office 365 アプリケーションオブジェクトごとに作成されます。



- ファイアウォール事前アプライアンスポリシーテンプレート: 構成済みの Office 365 カテゴリごとに、グローバル事前アプライアンスポリシーテンプレートが作成されます。このテンプレートは、インターネットサービスを持つすべてのブランチサイトに適用されます。アプライアンスの前ポリシーは、ローカルおよびアプライアンスの後ポリシーテンプレートよりも優先されます。

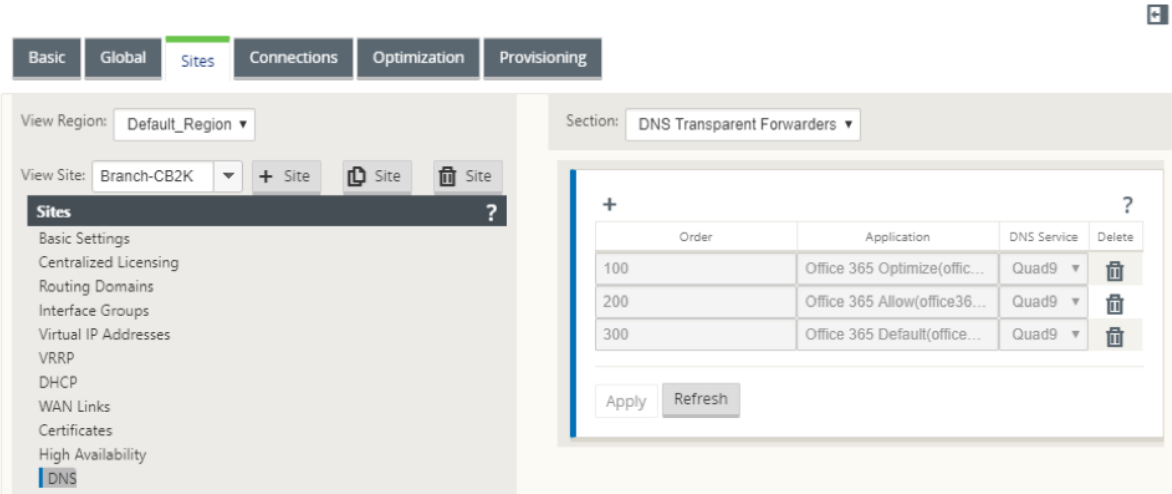


Office 365 の透過的なフォワーダー

Office 365 のブランチは、DNS 要求から始まります。Office 365 ドメインを経由する DNS 要求は、ローカルで操作する必要があります。Office 365 のインターネットブレークアウトを有効にすると、内部 DNS ルートが決定され、透過フォワーダーリストが自動的に設定されます。Office 365 の DNS 要求は、既定でオープンソースの DNS サービス Quad 9 に転送されます。Quad 9 DNS サービスは、安全でスケーラブルで、マルチポップな存在感を持っています。必要に応じて DNS サービスを変更できます。

Office 365 アプリケーション用の透過的なフォワーダーは、インターネットサービスと Office 365 ブレイクアウトが有効になっているすべてのブランチで作成されます。

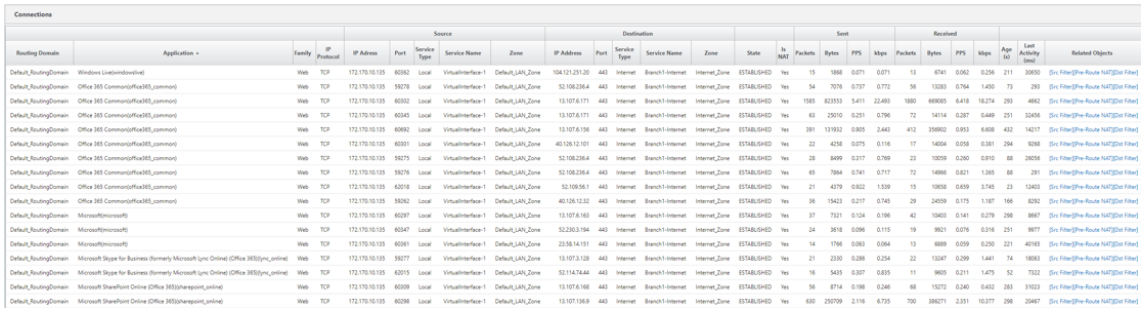
別の DNS プロキシを使用している場合、または SD-WAN が DNS プロキシとして構成されている場合、Office 365 アプリケーションのフォワーダーがフォワーダー一覧に自動的に入力されます。



監視

Office 365 アプリケーションの統計情報は、次の SD-WAN 統計レポートで監視できます。

- ファイアウォールの統計情報



- フロー

Flows Data

LAN to WAN Flows

Details	Routing Domain	Source IP Address	Dest IP Address	Source Port	Dest Port	IPP	Hit Count	Service Type	Service Name	Age (mS)	Packets	Bytes	PPS	Application ▲
	Optimize	172.147.100.146	52.98.65.178	57930	443	TCP	4	INTERNET	-	120979	3	156	0.000	outlook
	Optimize	172.147.100.146	13.107.18.11	57931	443	TCP	15	INTERNET	-	26513	14	1683	0.018	outlook
	Optimize	172.147.100.146	13.107.42.11	57891	443	TCP	20	INTERNET	-	8418	19	1903	0.036	outlook
	Optimize	172.147.100.146	40.100.136.146	57926	443	TCP	14	INTERNET	-	730	13	2118	0.036	outlook
	Optimize	172.147.100.146	40.97.229.82	57918	443	TCP	15	INTERNET	-	1229	14	2178	0.036	outlook
	Optimize	172.147.100.146	52.98.65.178	57929	443	TCP	4	INTERNET	-	121224	3	156	0.000	outlook
	Optimize	172.147.100.146	34.203.255.247	51236	443	TCP	5	INTERNET	-	599759	4	164	0.000	okta
	Optimize	172.147.100.146	34.203.255.247	51237	443	TCP	4	INTERNET	-	592420	3	123	0.000	okta
	Optimize	172.147.100.146	13.107.6.156	51298	443	TCP	29	INTERNET	-	42061	28	11416	0.018	office365_common
	Optimize	172.147.100.146	20.190.140.51	57935	443	TCP	16	INTERNET	-	24735	15	4184	0.018	office365_common
	Optimize	172.147.100.146	13.67.50.225	57897	443	TCP	3	INTERNET	-	2250	2	81	0.047	office365_common
	Optimize	172.147.100.146	13.67.50.225	51228	443	TCP	4	INTERNET	-	603355	3	123	0.000	office365_common
	Optimize	172.147.100.146	13.107.6.156	51255	443	TCP	249	INTERNET	-	377061	248	85307	0.000	office365_common
	Optimize	172.147.100.146	52.109.124.84	57939	443	TCP	20	INTERNET	-	22933	19	4679	0.018	office365_common
	Optimize	172.147.100.146	13.67.50.225	51346	443	TCP	3	INTERNET	-	5900	2	81	0.044	office365_common

- DNS 統計情報

Dashboard | Monitoring | Configuration

Statistics
Flows
Routing Protocols
Firewall
IKE/IPsec
IGMP
Performance Reports
Qos Reports
Usage Reports
Availability Reports
Appliance Reports
DHCP Server/Relay
VRRP
PPPoE
DNS

Monitoring > DNS

DNS Statistics

Refresh

Proxy Statistics

Search:

Proxy Name	Application Name	DNS Service Name	DNS Service Active	Hits
DNS_Proxy1	office365_optimize	Quad9	YES	2
DNS_Proxy1	office365_allow	Quad9	YES	8
DNS_Proxy1	office365_default	Quad9	YES	6
DNS_Proxy1	Any	Google	YES	17

Showing 1 to 4 of 4 entries

Transparent Forwarder Statistics

Search:

Application Name	DNS Service Name	DNS Service Active	Hits
office365_allow	Quad9	YES	0
office365_default	Quad9	YES	0
office365_optimize	Quad9	YES	0

Showing 1 to 3 of 3 entries

- アプリケーションルート統計情報

Monitoring > Statistics

Statistics

Show: Application Routes | Enable Auto Refresh | 5 seconds | Stop | Clear Counters on Refresh | Processing...

Application Route Statistics

Maximum allowed routes: 64000

Application Routes for routing domain : Default_RoutingDomain

Filter: in Any column Apply

Show 100 entries Showing 1 to 3 of 3 entries

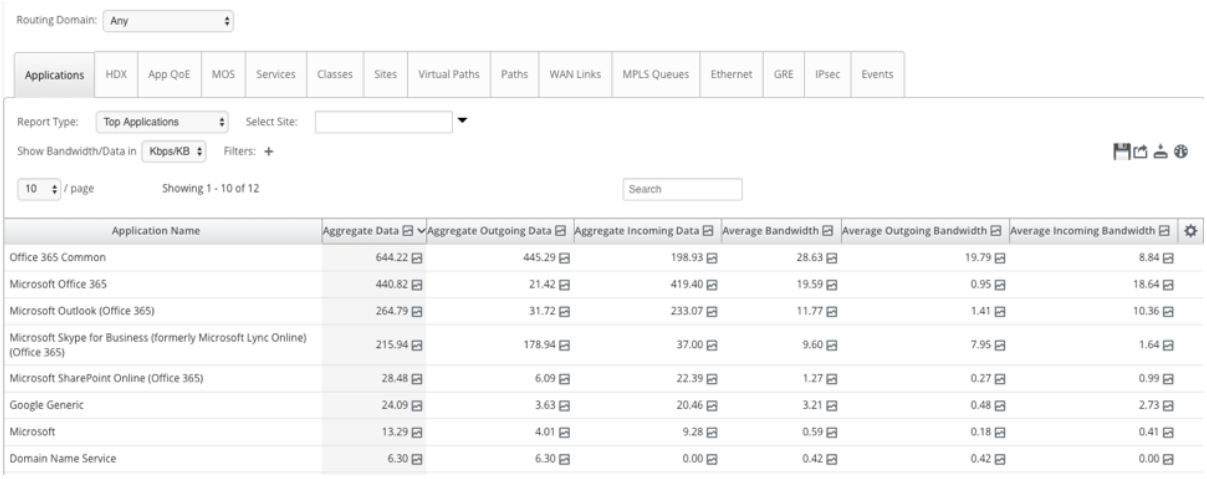
First Previous 1 Next Last

Num	Application Object	Gateway IP Address	Service	Firewall Zone	Reachable	Site	Type	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
0	O365Optimize_InternetBreakout	*	Internet	Internet_Zone	YES	Branch1	Static	5	1792	YES	N/A	N/A
2	O365Allow_InternetBreakout	*	Internet	Internet_Zone	YES	Branch1	Static	5	1395	YES	N/A	N/A
1	O365Default_InternetBreakout	*	Internet	Internet_Zone	YES	Branch1	Static	5	0	YES	N/A	N/A

Showing 1 to 3 of 3 entries

First Previous 1 Next Last

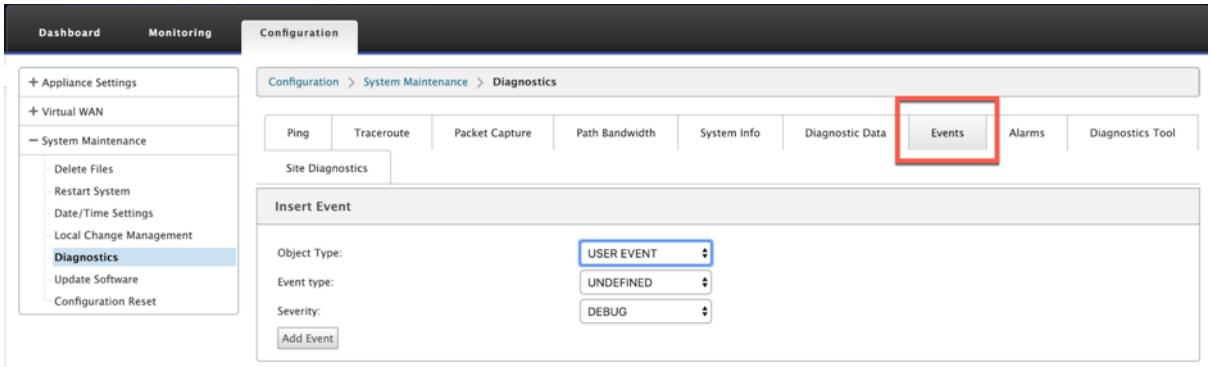
SD-WAN センターアプリケーションレポートで Office 365 アプリケーションの統計情報を表示することもできます。



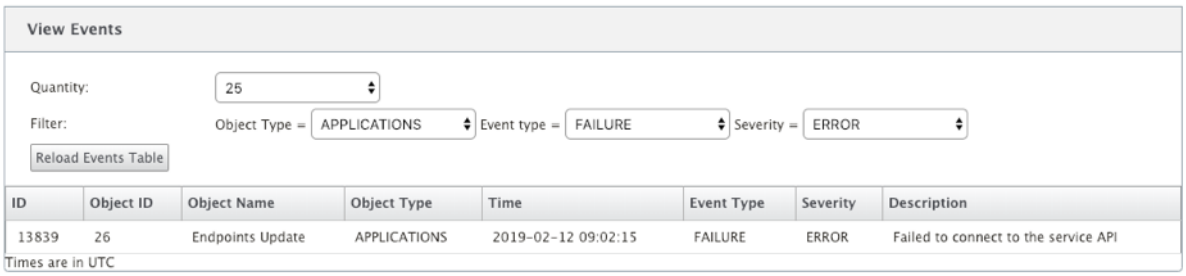
トラブルシューティング

サービスエラーは、SD-WAN アプライアンスの [イベント] セクションで確認できます。

エラーを確認するには、[構成**] > [**システムメンテナンス**] > [**診断**]** の順に選択し、[イベント] タブをクリックします。

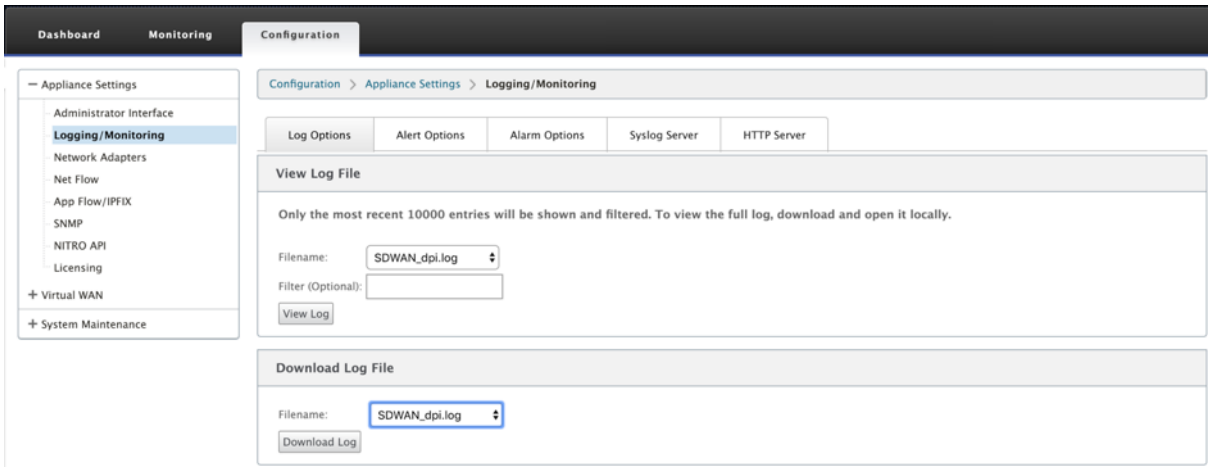


Citrix サービス（sdwan-app-routing.citrixnetworkapi.net）への接続に問題がある場合、エラーメッセージは［イベントの表示］テーブルに表示されます。



接続エラーも **SDWAN_DPI.log** に記録されます。ログを表示するには、［構成］**>**［アプライアンスの設定］**>**［ログ**/**監視］**>**［ログオプション］に移動します。ドロップダウンリストから **SDWAN_DPI.log** を選択し、[ログの表示] をクリックします。

ログファイルをダウンロードすることもできます。ログファイルをダウンロードするには、[Download Log file] セクションの下のドロップダウンリストから必要な ログファイルを選択し、**[Download Log]** をクリックします。



制限事項

- Office 365 のブレークアウトポリシーが構成されている場合、構成された IP アドレスのカテゴリ宛ての接続では、ディープパケットインスペクションは実行されません。
- 自動作成されたファイアウォールポリシーとアプリケーションルートは編集できません。
- 自動作成されたファイアウォールポリシーの優先順位が最も低く、編集できません。
- 自動作成されたアプリケーションルートのルートコストは 5 です。このルートは、低コストのルートで上書きできます。

PPPoE セッション

May 10, 2021

PPPoE（Point-to-Point Protocol over Ethernet）は、イーサネットローカルエリアネットワーク上の複数のコンピュータユーザーを、一般的な顧客構内のアプライアンス（Citrix SD-WAN など）を介してリモートサイトに接続します。PPPoE を使用すると、ユーザーは共通のデジタル加入者線 (DSL)、ケーブルモデム、またはインターネットへのワイヤレス接続を共有できます。PPPoE は、ダイヤルアップ接続で一般的に使用される Point-to-Point Protocol (PPP) と、ローカルエリアネットワークで複数のユーザをサポートするイーサネットプロトコルを組み合わせます。PPP プロトコル情報は、イーサネットフレーム内にカプセル化されます。

Citrix SD-WAN アプライアンスは、PPPoE を使用して、ダイヤルアップ接続とは異なり、継続的な DSL およびケーブルモデム接続をサポートするインターネットサービスプロバイダ（ISP）を提供します。PPPoE は、「検出」と呼ばれる初期交換を通じて互いのネットワークアドレスを学習するために、各ユーザリモートサイトセッションを提供します。個々のユーザーとリモートサイト (ISP プロバイダーなど) の間にセッションが確立されると、セッションを

監視できます。企業は、イーサネットと PPPoE を使用して、DSL 回線を介して共有インターネットアクセスを使用します。

Citrix SD-WAN は、PPPoE クライアントとして機能します。PPPoE サーバで認証し、ダイナミック IP アドレスを取得するか、固定 IP アドレスを使用して PPPoE 接続を確立します。

PPPoE セッションを正常に確立するには、次のことが必要です。

- 仮想ネットワークインターフェイス (VNI) を設定します。
- PPPoE セッションを作成するための一意の資格情報。
- WAN リンクを設定します。各 VNI に設定できる WAN リンクは 1 つだけです。
- 仮想 IP アドレスを設定します。各セッションは、指定された設定に基づいて、一意の IP アドレス（動的、または静的）を取得します。
- アプライアンスをブリッジモードで展開し、静的 IP アドレスで PPPoE を使用し、インターフェイスを「信頼済み」に設定します。
- スタティック IP は、サーバ提案の IP を強制的に設定することを推奨します。設定されたスタティック IP と異なる場合は、エラーが発生する可能性があります。
- アプライアンスをエッジデバイスとして展開し、ダイナミック IP で PPPoE を使用し、インターフェイスを「信頼できない」として構成します。
- サポートされている認証プロトコルは、PAP、CHAP、EAP-MD5、EAP-SRP です。
- 複数のセッションの最大数は、設定されている VNI の数によって異なります。
- インターフェイスグループごとに複数の PPPoE セッションをサポートするために、複数の VNI を作成します。

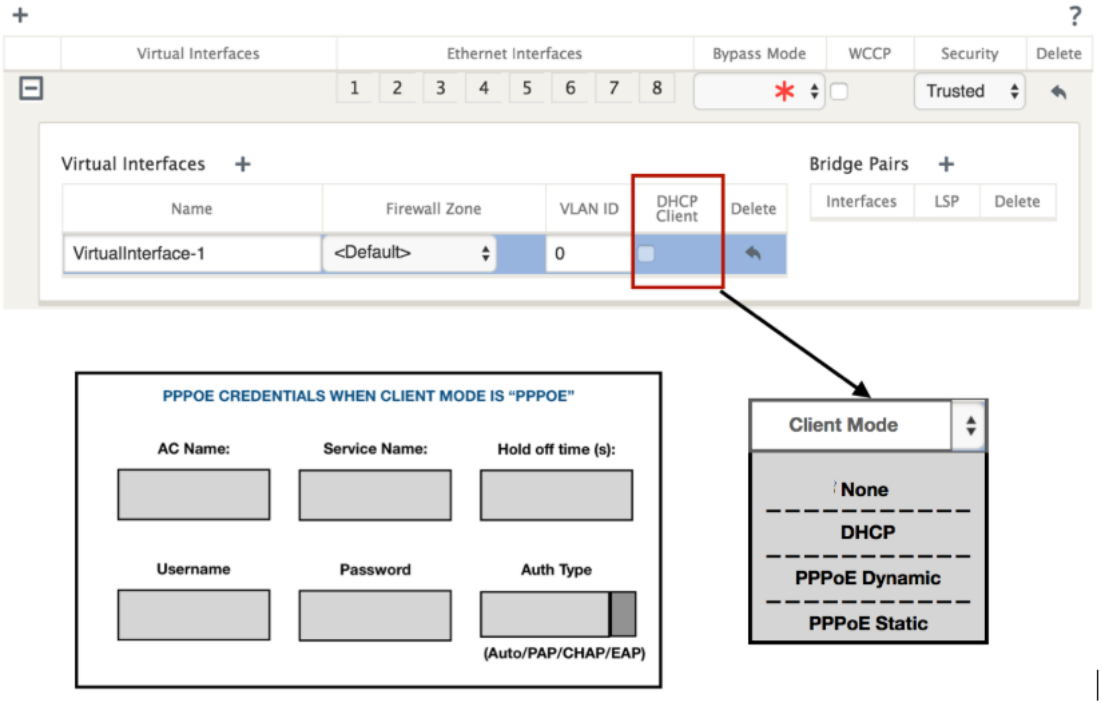
  > 注:
  >
  > 同じ 802.1Q VLAN タグを使用して複数の VNI を作成できます。

PPPoE 設定の制限事項

- 802.1q VLAN タギングはサポートされません。
- EAP-TLS 認証はサポートされていません。
- アドレス/制御圧縮
- 収縮圧縮。
- プロトコルフィールド圧縮ネゴシエーション
- 圧縮制御プロトコル。
- BSD 圧縮圧縮。
- IPv6 および IPX プロトコル。
- PPP マルチリンク。
- Van Jacobson スタイルの TCP/IP ヘッダー圧縮。

- Van Jacobson スタイルの TCP/IP ヘッダー圧縮の接続 ID 圧縮オプション。
- PPPoE は LTE インターフェイスではサポートされていません

PPPoE の設定を容易にするため、**DHCP** クライアント オプションは、[サイト 設定] の SD-WAN Web 管理インターフェイスの [クライアントモード] という新しいオプションに置き換えられます。



次の表に、MCN アプライアンスおよびブランチ SD-WAN アプライアンスで使用できるクライアントモード PPPoE 構成オプションを示します。

MCN

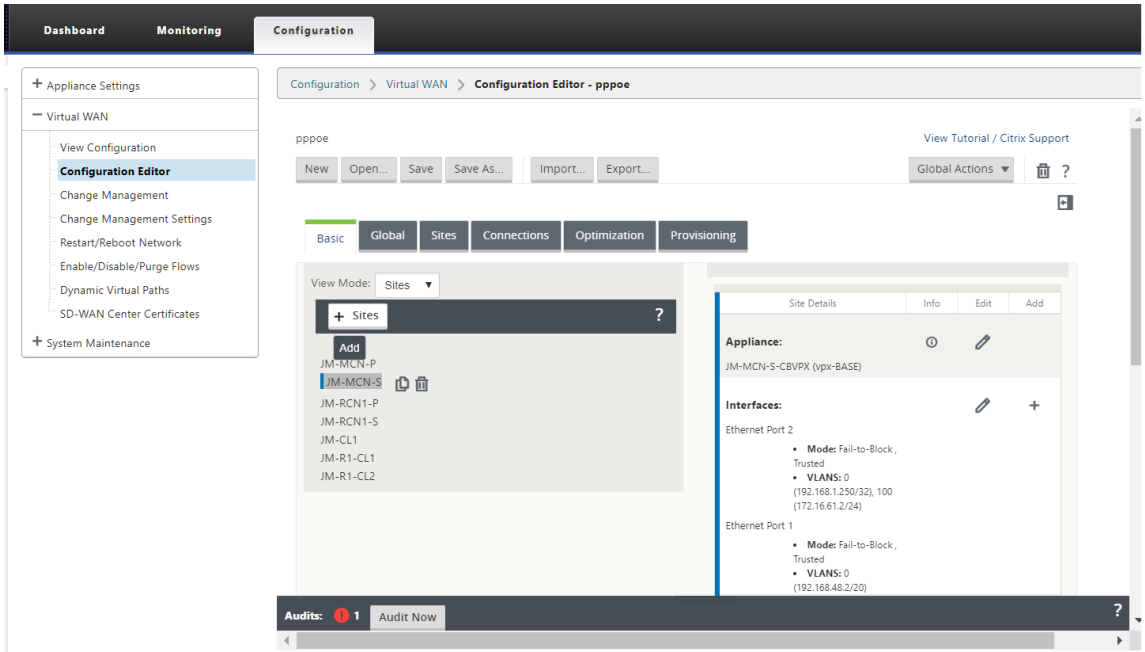
- なし
- PPPoE スタティック

ブランチ

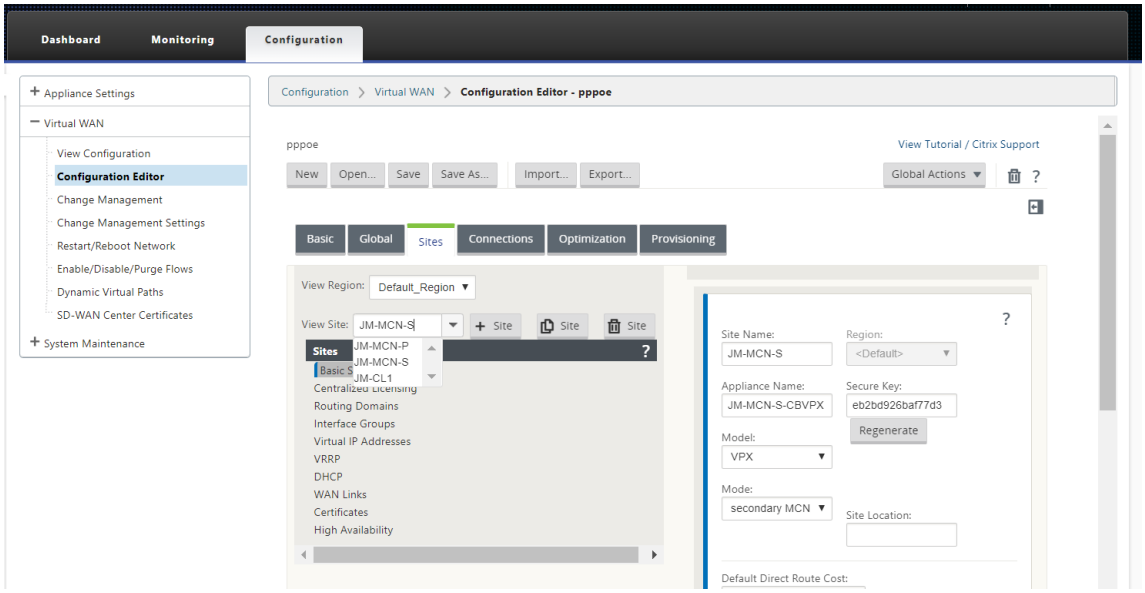
- なし
- PPPoE スタティック
- PPPoE ダイナミック
- DHCP

MCN アプライアンスの構成

1. SD-WAN MCN アプライアンス GUI で、[構成] > [仮想 **WAN**] > [構成エディタ] に移動します。[基本] タブの下にサイトを追加します。詳細については、MCN の構成のブランチノード構成を参照してください。



2. 新しいサイトが作成されたら、[サイト] タブを開きます。[サイトの 表示] ドロップダウンリストから、新しく作成したサイト を選択します。

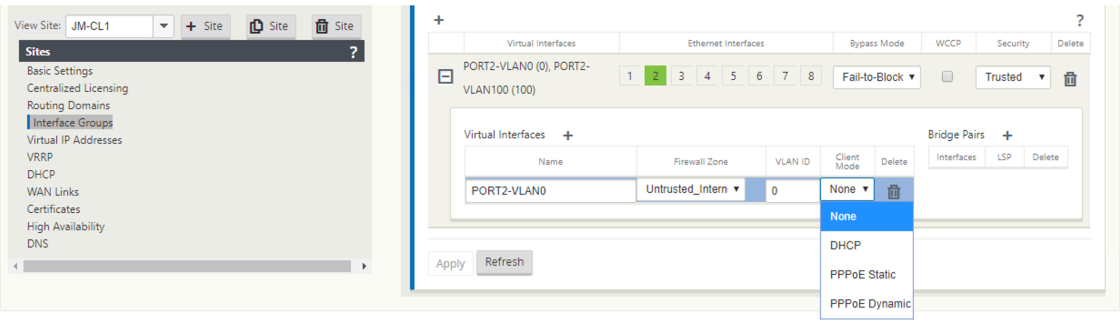


3. MCN サイトの [インターフェイスグループ] を選択します。以下を実行します:

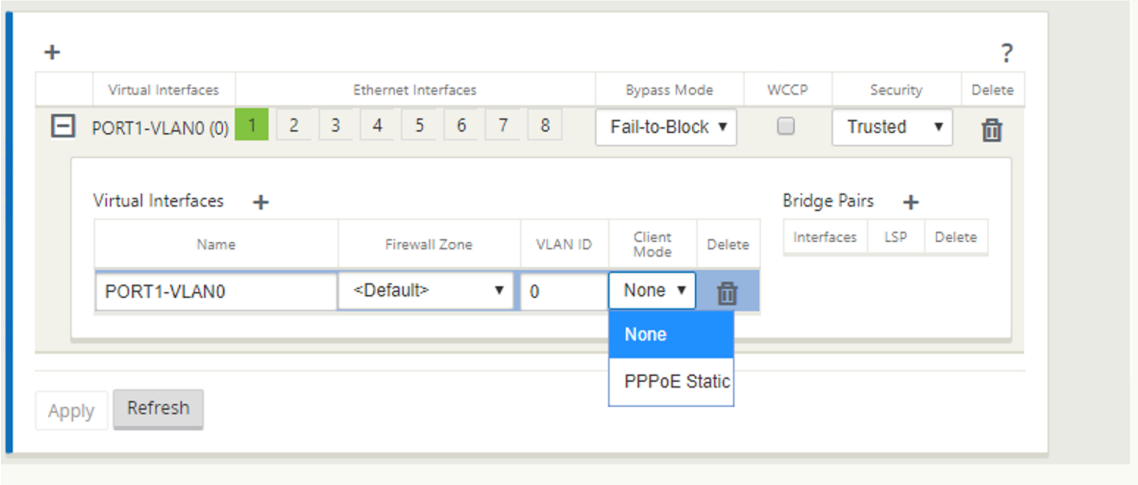
   - 仮想インターフェイスの追加
   - イーサネットインターフェイスを設定します。
   - バイパスモードを設定します。
   - 必要に応じて、**WCCP** を選択します。
   - [セキュリティ]-[信頼済み/信頼されていない] を選択します。

   仮想インターフェイスの場合:

- 名前、ファイアウォールゾーン、VALN ID、およびクライアントモードを設定します。
- 複数のインターフェイスが設定された VNI では、PPPoE 接続に使用できるインターフェイスは 1 つだけです。
- 複数のインターフェイスが設定された VNI で PPPoE 接続が異なるインターフェイスに変更された場合、モニタページを使用して既存のセッションを停止し、新しいセッションを開始すると、新しいインターフェイスで新しいセッションを確立できます。



4. MCN アプライアンスの [クライアントモード] オプションのネットワーク構成要件に基づいて、[**PPPoE** 静的] または [なし] を選択します。さらに次のオプションが表示されます。

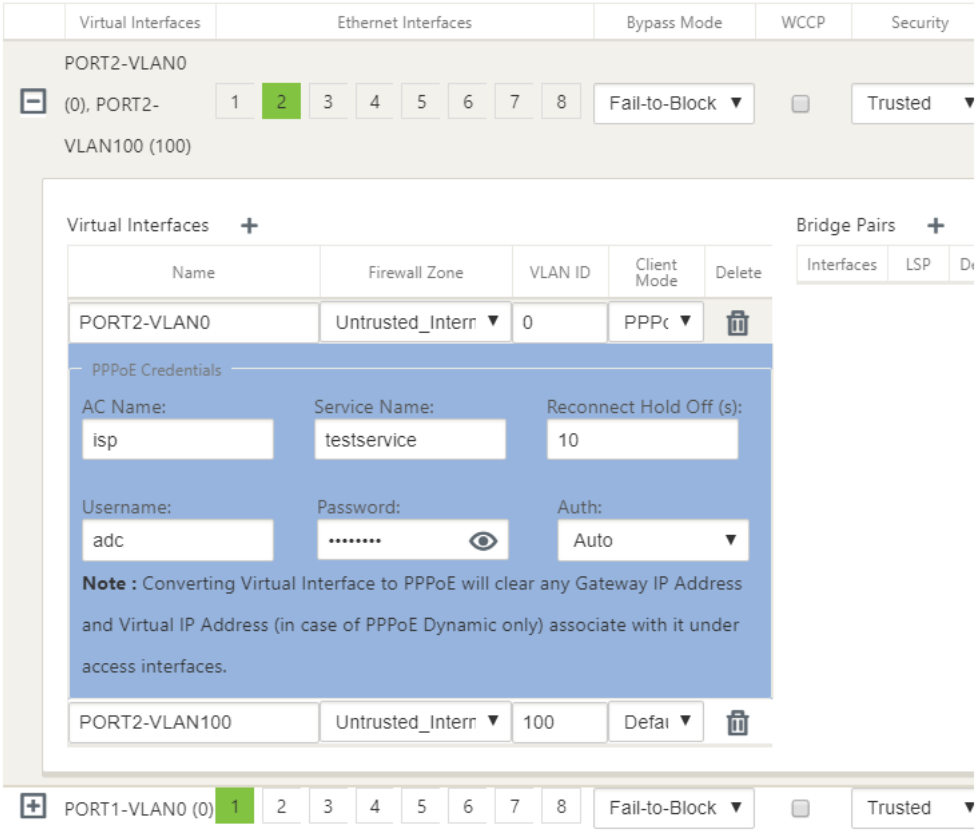


次の PPPoE パラメータを設定し、[**Apply**] をクリックします。

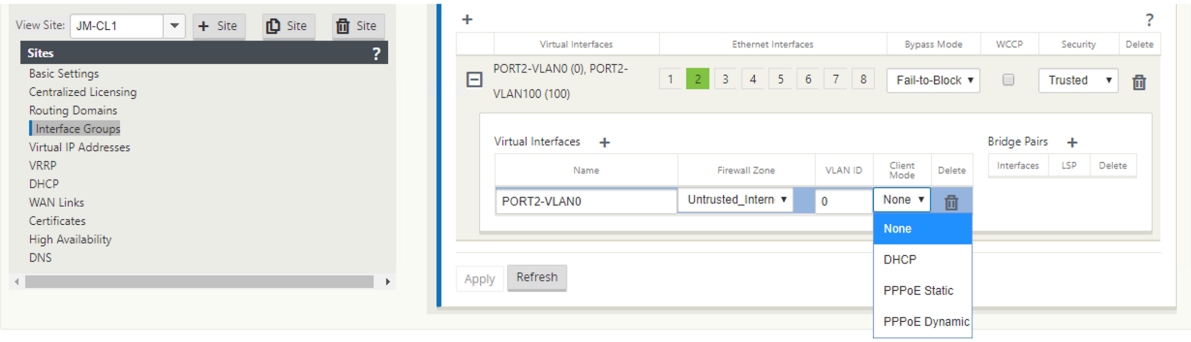
- [コンセントレータ (AC) 名] フィールドにアクセスします。
- サービス名。
- ホールドオフ再接続時間（デフォルトはただちに再接続されます。’0’）
- 認証タイプ-(AUTO/PAP/CHAP/EAP)。
  - Auth オプションが Auto に設定されている場合、SD-WAN アプライアンスは、サーバーから受信したサポートされている認証プロトコル要求を受け入れます。

  - Auth オプションが PAP/CHAP/EAP に設定されている場合、特定の認証プロトコルだけが適用されます。PAP が設定内にあり、サーバが CHAP を使用して認証要求を送信した場合、接続要求は拒否されます。サーバが PAP とネゴシエートしない場合、認証エラーが発生します。

- CHAP には、CHAP、Microsoft CHAP、および Microsoft CHAPv2 が含まれます。
- EAP は EAP-MD5 をサポートします。
- ユーザ名とパスワード。



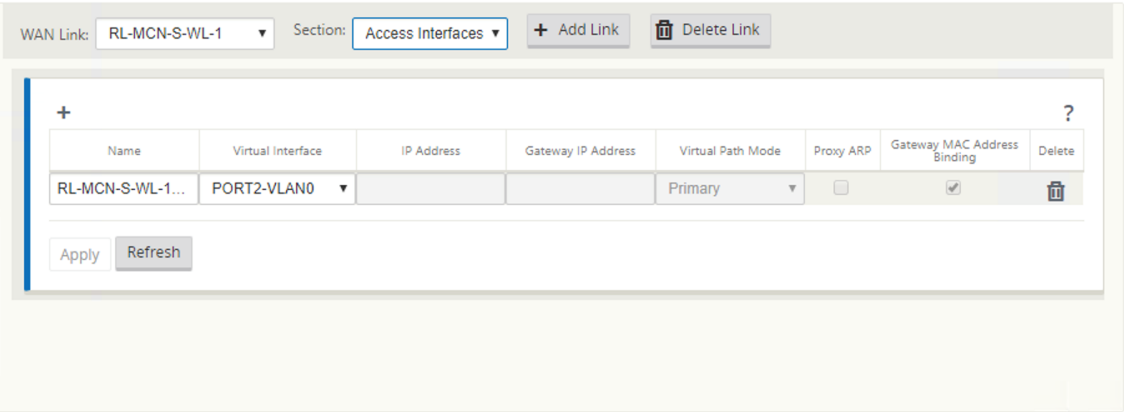
次の図は、ブランチ SD-WAN アプライアンスの PPPoE クライアントモードオプションを示しています。[PPPoE ダイナミック] が選択されている場合、VNI は「信頼できない」である必要があります。



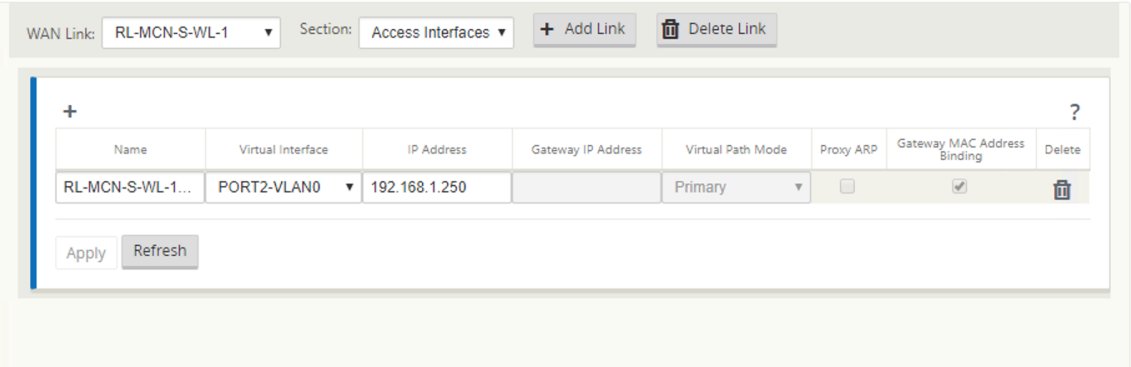
WAN リンクの設定

1. SD-WAN GUI で、[サイト**] > [WAN** リンク] に移動します。PPPoE スタティック VNI またはダイナミック VNI ごとに、WAN リンクの作成は 1 つだけ許可されます。WAN リンクの設定は、クライアントモードの VNI の選択によって異なります。
2. VNI に PPPoE ダイナミッククライアントモードが設定されている場合は、次の手順を実行します。
   - IP アドレスフィールドとゲートウェイ IP アドレスフィールドは非アクティブになります。
   - 仮想パスモードが「プライマリ」に設定されています。
   - プロキシ ARP は設定できません。

   デフォルトでは、[ゲートウェイ MAC アドレスバインディング] が選択されています。



3. VNI に PPPoE スタティッククライアントモードが設定されている場合は、IP アドレスを設定します。



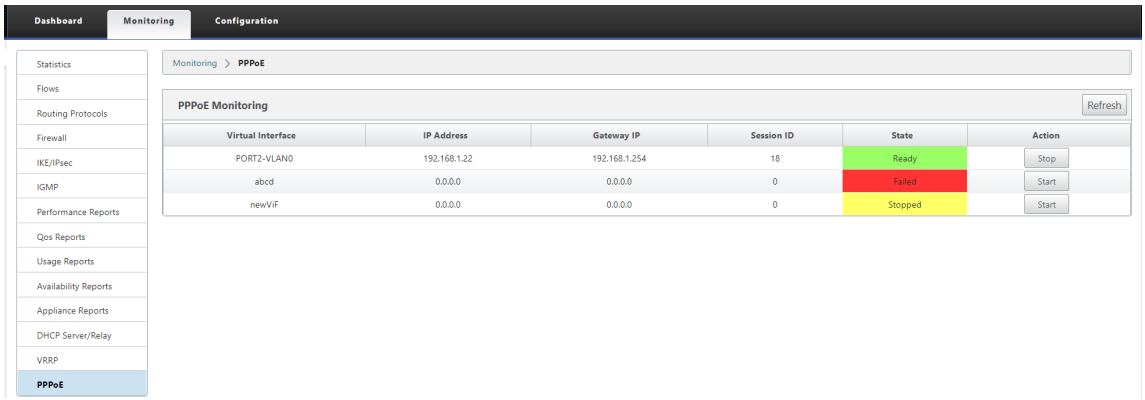
> 注:
>
> サーバが設定された静的 IP アドレスを尊重せず、別の IP アドレスを提供すると、エラーが発生します。PPPoE セッションは、サーバーが設定された IP アドレスを受け入れるまで、定期的に接続の再確立を試みます。

PPPoE セッションの監視

PPPoE セッションを監視するには、SD-WAN GUI の **[**モニタリング**] > [PPPoE**] ページに移動します。

PPPoE ページには、PPPoE スタティッククライアントモードまたはダイナミッククライアントモードが設定された VNI のステータス情報が表示されます。トラブルシューティングの目的で、手動でセッションを開始または停止できます。

- VNI が起動して準備ができている場合は、**IP** カラムと **Gateway IP** カラムにセッションの現在の値が表示されます。これは、最近受信した値であることを示します。
- VNI が停止しているか、障害状態の場合、値は最後に受信された値です。
- [Gateway IP] 列の上にマウスを置くと、セッションと IP の受信元の PPPoE アクセスコンセントレータの MAC アドレスが表示されます。
- 「状態」の値の上にマウスを置くとメッセージが表示され、「失敗」状態の方が便利です。



[**State**] 列には、緑、赤、黄、および値の 3 つのカラーコードを使用して PPPoE セッションのステータスが表示されます。次の表では、状態と説明について説明します。ステートの上にマウスポインタを置くと、説明が表示されます。

PPPoE セッションタイプ	色	説明
構成済み	黄	VNI には PPPoE が設定されています。これは初期状態です。
ダイヤル中	黄	VNI が設定されると、PPPoE ディスカバリを開始して PPPoE セッション状態がダイヤル状態に移行します。パケット情報がキャプチャされます。
セッション	黄	VNI は Discovery 状態からセッション状態に移行されます。動的な場合は IP の受信を待機するか、静的な場合は、アドバタイズされた IP のサーバからの確認応答を待機します。
準備完了	緑	IP パケットが受信され、VNI および関連する WAN リンクが使用可能になります。

PPPoE セッションタイプ	色	説明
失敗	赤	PPP/PPPoE セッションが終了しました。失敗の原因は、無効な構成または致命的なエラーが原因である可能性があります。セッションは 30 秒後に再接続を試みます。
停止しました	黄色	PPP/PPPoE セッションは手動で停止されます。
終了中	黄色	理由により終了する中間状態。この状態は、一定時間（通常のエラーの場合は 5 秒、致命的なエラーの場合は 30 秒）後に自動的に開始されます。
無効	黄色	SD-WAN サービスは無効です。

PPPoE セッション障害のトラブルシューティング

[Monitoring] ページで、PPPoE セッションの確立に問題がある場合、次の手順を実行します。

- [失敗] ステータスの上にマウスを置くと、最近の失敗の理由が表示されます。
- 新しいセッションを確立したり、アクティブな PPPoE セッションのトラブルシューティングを行うには、[監視] → [PPPoE] ページを使用してセッションを再起動します。
- PPPoE セッションを手動で停止した場合、手動で開始して構成の変更がアクティブになるか、サービスが再起動されるまで、PPPoE セッションを開始できません。

PPPoE セッションは、次の理由により失敗することがあります。

- 設定内のユーザ名/パスワードが正しくないために SD-WAN がピアに対して自身を認証できない場合
- PPP ネゴシエーションが失敗します。ネゴシエーションは、少なくとも 1 つのネットワークプロトコルが実行されているポイントに到達しません。
- システムメモリまたはシステムリソースの問題。
- 構成が無効または不正です（AC 名またはサービス名が間違っています）。
- オペレーティングシステムエラーのため、シリアルポートを開けませんでした。
- エコーパケットに対する応答が受信されない（リンクが不良であるか、サーバが応答していない）。
- 1 分以内に、が連続的に失敗したダイヤルセッションがいくつか発生しました。

10 回連続して失敗した後、失敗の理由が観察されます。

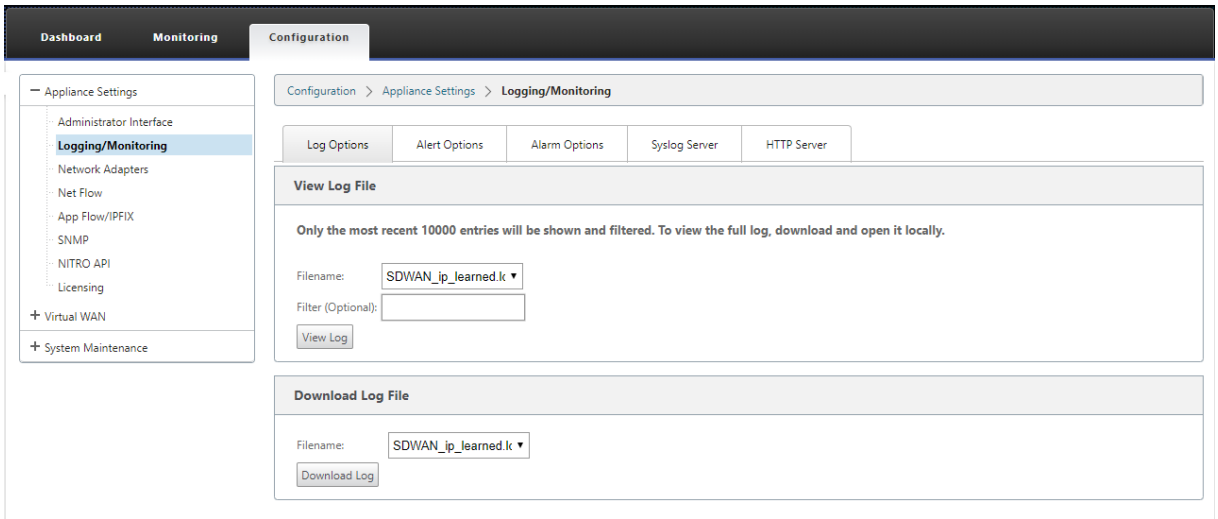
- 障害が正常であれば、すぐに再起動します。
- 失敗がエラーの場合、再起動は 10 秒間戻ります。
- 失敗が致命的である場合、再起動は 30 秒間戻ってから再起動します。

LCP Echo 要求パケットは、SD-WAN から 60 秒ごとに生成され、5 つのエコー応答を受信できなかった場合はリンク障害と見なされ、セッションが再確立されます。

PPPoE ログファイル

SDWAN_IP_learned.log ファイルには、PPPoE に関連するログが含まれています。

SD-WAN GUI から *SDWAN_IP_learned.log* ファイルを表示またはダウンロードするには、アプライアンスの設定 > ログ/監視 > ログオプションに移動します。*SDWAN_IP_learned.log* ファイルを表示またはダウンロードします。



サービス品質

May 10, 2021

オフィスの場所とデータセンターまたはクラウド間のネットワークでは、高品質のビデオやリアルタイムの音声など、多数のアプリケーションやデータを転送する必要があります。帯域幅に敏感なアプリケーションは、ネットワークの機能とリソースを拡張します。Citrix SD-WAN は、保証された、安全で、測定可能な、予測可能なネットワークサービスを提供します。これは、ネットワーク上の遅延、ジッタ、帯域幅、およびパケット損失を管理することによって実現されます。

Citrix SD-WAN ソリューションには、高度なアプリケーション QoS（サービス品質）エンジンが含まれており、アプリケーショントラフィックにアクセスし、重要なアプリケーションに優先順位を付けます。また、WAN ネットワーク品質の要件を理解し、品質特性に基づいてネットワークパスをリアルタイムで選択します。

次の項のトピックでは、QoS クラス、IP ルール、アプリケーション QoS ルール、およびアプリケーション QoS の定義に必要な、その他のコンポーネントについて説明します。

クラス

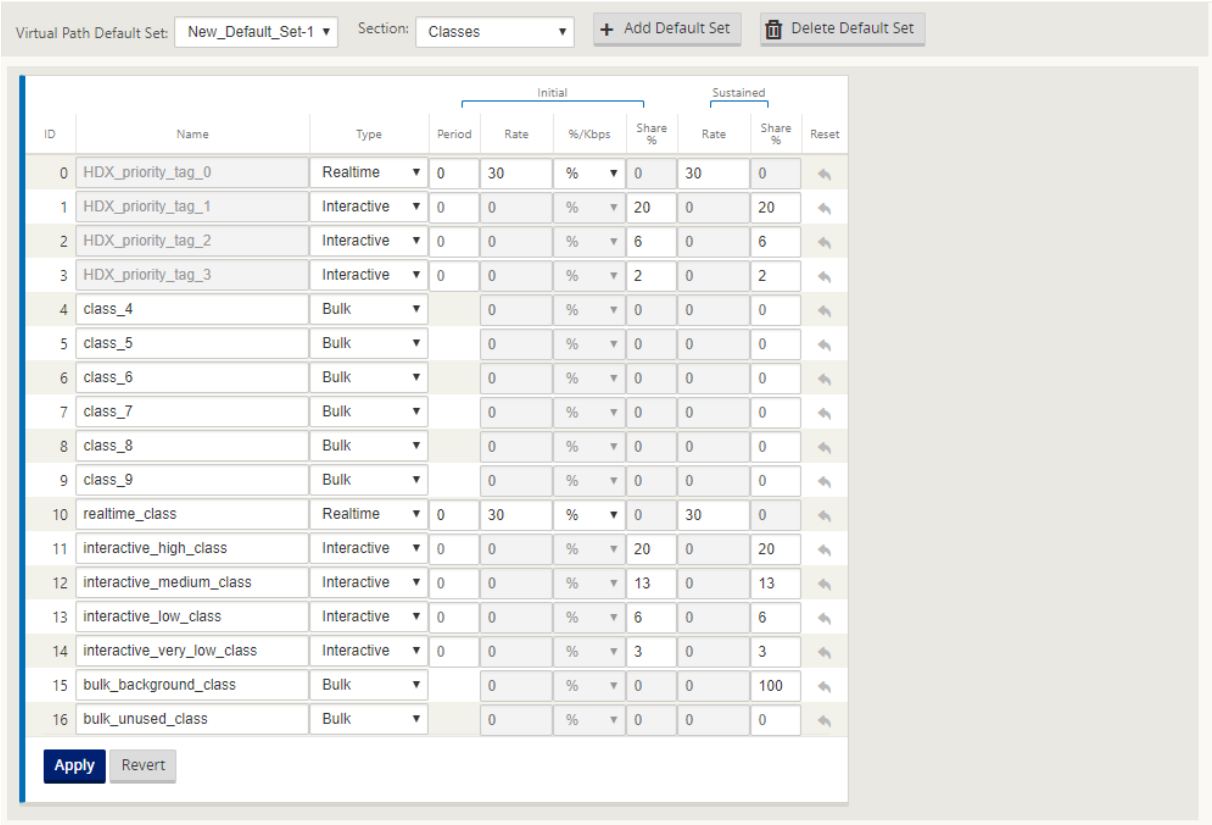
November 8, 2021

Citrix SD-WAN 構成では、仮想パスを通過するすべてのトラフィックに適用されるアプリケーションおよび IP/ポートベースの QoS ポリシーのデフォルトセットが提供されます。これらの設定は、展開のニーズに合わせてカスタマイズできます。

クラスは、トラフィックの優先順位付けに役立ちます。アプリケーションおよび IP/ポートベースの QoS ポリシーは、トラフィックを分類し、設定で指定された適切なクラスに配置します。

アプリケーションの QoS と IP アドレス/ポートベースの QoS の詳細については、アプリケーション名別のルール 、IP アドレスとポート番号によるルールをそれぞれ参照してください 。

SD-WAN は 17 のクラス（ID: 0 ～16）を提供します。以下は、すべての 17 クラスのデフォルト設定です。



ID	Name	Type	Initial Period	Initial Rate	Initial %/Kbps	Initial Share %	Sustained Rate	Sustained Share %	Reset
0	HDX_priority_tag_0	Realtime	0	30	%	0	30	0	
1	HDX_priority_tag_1	Interactive	0	0	%	20	0	20	
2	HDX_priority_tag_2	Interactive	0	0	%	6	0	6	
3	HDX_priority_tag_3	Interactive	0	0	%	2	0	2	
4	class_4	Bulk		0	%	0	0	0	
5	class_5	Bulk		0	%	0	0	0	
6	class_6	Bulk		0	%	0	0	0	
7	class_7	Bulk		0	%	0	0	0	
8	class_8	Bulk		0	%	0	0	0	
9	class_9	Bulk		0	%	0	0	0	
10	realtime_class	Realtime	0	30	%	0	30	0	
11	interactive_high_class	Interactive	0	0	%	20	0	20	
12	interactive_medium_class	Interactive	0	0	%	13	0	13	
13	interactive_low_class	Interactive	0	0	%	6	0	6	
14	interactive_very_low_class	Interactive	0	0	%	3	0	3	
15	bulk_background_class	Bulk		0	%	0	0	100	
16	bulk_unused_class	Bulk		0	%	0	0	0	

以下は、クラスの異なるタイプです。

- リアルタイム: 低遅延、低帯域幅、時間依存型のトラフィックに使用されます。リアルタイムアプリケーションは時間に依存しますが、実際には高帯域幅（Voice over IP など）を必要としません。リアルタイムアプリケーションは、レイテンシーとジッタの影響を受けますが、ある程度の損失を許容できます。
- **Interactive**：低～中レイテンシーおよび低～中帯域幅要件の対話型トラフィックに使用されます。通常、対話はクライアントとサーバーの間で行われます。通信は、高帯域幅を必要としない場合がありますが、損失や遅延に敏感です。
- バルク: 高帯域幅トラフィックおよび高遅延に耐えるアプリケーションに使用されます。ファイル転送を処理し、高帯域幅を必要とするアプリケーションは、バルククラスに分類されます。これらのアプリケーションは、人間の干渉をほとんど伴わず、ほとんどシステム自体によって処理されます。

クラス間の帯域幅共有

帯域幅は、クラス間で次のように共有されます。

- リアルタイム: リアルタイムクラスにヒットするトラフィックは低遅延であることが保証され、競合するトラフィックが存在する場合、帯域幅はクラスシェアまで制限されます。
- インタラクティブ**:** 対話型クラスに当たるトラフィックは、リアルタイムトラフィックを提供した後、残りの帯域幅を取得し、利用可能な帯域幅は、対話型クラス間で公平に共有されます。
- バルク: バルクがベストエフォートです。リアルタイムトラフィックおよびインタラクティブトラフィックを提供した後に残された帯域幅は、公平な共有ベースでバルククラスに与えられます。リアルタイムトラフィックおよびインタラクティブトラフィックが使用可能な帯域幅をすべて利用すると、バルクトラフィックが枯渇する可能性があります。

> 注:
>
> 競合がない場合、すべてのクラスが使用可能な帯域幅を使用できます。

次に、クラス設定に基づく帯域幅分散の例を示します。

仮想パス上に 10 Mbps の集約帯域幅があるとします。クラス設定が

- リアルタイム:30%
- インタラクティブハイ:40%
- インタラクティブ媒体:20%
- インタラクティブロー:10%
- バルク:100%。

帯域幅分布の結果は

- リアルタイムトラフィックは、必要に応じて 10Mbs（3 Mbps）の 30% を取得します。10% 未満で済む場合は、残りの帯域幅が他のクラスで使用可能になります。

- 対話型クラスは、残りの帯域幅をフェアシェアベース（4 Mbps: 2 Mbps: 1 Mbps）で共有します。
- リアルタイムのインタラクティブトラフィックが共有を完全に使用していないときに残ったものは、Bulk クラスに与えられます。

クラスをカスタマイズするには、次の手順に従います。

1. 仮想パスのデフォルトセットが使用されている場合は、[グローバル**] > [**仮想パスのデフォルトセット] でクラスを変更できます。

   > 注**:**
   >
   > 仮想パスレベル (接続**->** 仮想パス**->** クラス**)** でクラスを変更することもできます

2. 「デフォルトセットを追加」をクリックし、デフォルトセットの名前を入力して、「追加」をクリックします。[セクション] フィールドで、[クラス] を選択します。
3. [**Name**] フィールドで、デフォルト名をそのまま使用するか、任意の名前を入力します。
4. [タイプ] フィールドで、クラスタイプ ([リアルタイム]、[インタラクティブ]、[バルク]) を選択します。
5. リアルタイムクラスの場合、次の属性を指定できます。
   - 初期期間：持続レートに切り替える前に初期レートを適用する期間（ミリ秒単位）。
   - 初期レート：初期期間中にパケットがキューから出る最大レートまたはパーセンテージ。
   - 持続レート：最初の期間後にパケットがキューから出る最大レートまたはパーセンテージ。
6. 対話型クラスの場合、次の属性を指定できます。
   - [**Initial**Perioed]: 持続パーセンテージに切り替える前に、使用可能な帯域幅の初期パーセンテージを適用する期間（ミリ秒単位）。通常、20 ミリ秒
   - 初期共有**%**：初期期間中にリアルタイムにサービスを提供した後に残っている仮想パス帯域幅の最大シェアです。
   - 持続共有**%:** 初期期間の後にリアルタイムトラフィックを処理した後に残っている仮想パス帯域幅の最大シェアです。
7. バルククラスの場合は、リアルタイムおよび対話型トラフィックを処理した後にバルククラスに使用される残りの仮想パス帯域幅を決定する持続共有**%** だけを指定できます。
8. ［**Apply**］をクリックします。

> 注：
>
> 構成を保存し、変更管理の受信トレイにエクスポートし、変更管理プロセスを開始します。

IP アドレスとポート番号による規則

May 10, 2021

IP アドレスとポート番号によるルール機能を使用すると、ネットワークのルールを作成し、ルールに基づいてサービス品質（QoS）を決定するのに役立ちます。ネットワーク用のカスタムルールを作成できます。たとえば、次のルールを作成できます。—送信元 IP アドレスが 172.186.30.74、宛先 IP アドレスが 172.186.10.89 の場合は、送信モードを「永続パス、**LAN** を **WAN** クラスに 10 (realtime_class)」に設定します。

構成エディタを使用して、トラフィックフローのルールを作成し、そのルールをアプリケーションとクラスに関連付けることができます。フローのトラフィックをフィルタリングするための基準を指定し、一般的な動作、LAN から WAN への動作、WAN から LAN への動作、およびパケットインスペクション規則を適用できます。

ルールは、サイトレベルまたはグローバルレベルでローカルに作成できます。複数のサイトで同じルールが必要な場合は、[グローバル] > [仮想パスのデフォルトセット**] > [**ルール**]** で、ルールのテンプレートをグローバルに作成できます。このテンプレートは、ルールの適用が必要なサイトに添付できます。サイトがグローバルに作成されたルールテンプレートに関連付けられている場合でも、サイト固有のルールを作成できます。このような場合、サイト固有のルールが優先され、グローバルに作成されたルールテンプレートが上書きされます。

IP アドレスとポート番号によるルールの作成

1. SD-WAN 設定エディタで、[グローバル] > [仮想パスデフォルトセット**]** に移動します。

   > **注:**
   >
   > サイトレベルでルールを作成するには、**[**サイト**] > [**接続**] > [**仮想パス**] > [**ルール**]** に移動します。

2. 「デフォルトセットを追加」をクリックし、デフォルトセットの名前を入力して、「追加」をクリックします。「セクション」フィールドで「ルール」を選択し、「**+**」をクリックします。
3. [順序] フィールドに、他の規則に関連して規則が適用されるタイミングを定義する順序値を入力します。
4. [ルールグループ名] フィールドで、ルールグループを選択します。同じルールグループを持つルールの統計情報はグループ化され、まとめて表示できます。

   ルールグループを表示するには、[モニタリング**] > [**統計**]** に移動し、[表示] フィールドで [ルールグループ] を選択します。

   カスタムアプリケーションを追加することもできます。詳しくは、「ルールグループを追加して MOS を有効にする」を参照してください。
5. [**Routing Domain**] フィールドで、設定済みのルーティングドメインの 1 つを選択します。
6. ルール一致条件を定義して、以下に示すパラメータに基づいてサービスをフィルタリングできます。フィルタリングの後、ルール設定は、これらの基準に一致するサービスに適用されます。

- 送信元 **IP** アドレス：トラフィックと照合する送信元 IP アドレスおよびサブネットマスク。
- 宛先 **IP** アドレス：トラフィックと照合する宛先 IP アドレスおよびサブネットマスク。

  > 注
  >
  > [**Dest=Src**] チェックボックスが選択されている場合、送信元 IP アドレスは宛先 IP アドレスにも使用されます。

- プロトコル：トラフィックと照合するプロトコル。
- **[**Source Port]：トラフィックと照合する送信元ポート番号またはポート範囲。
- 宛先ポート：トラフィックと照合する宛先ポート番号またはポート範囲。

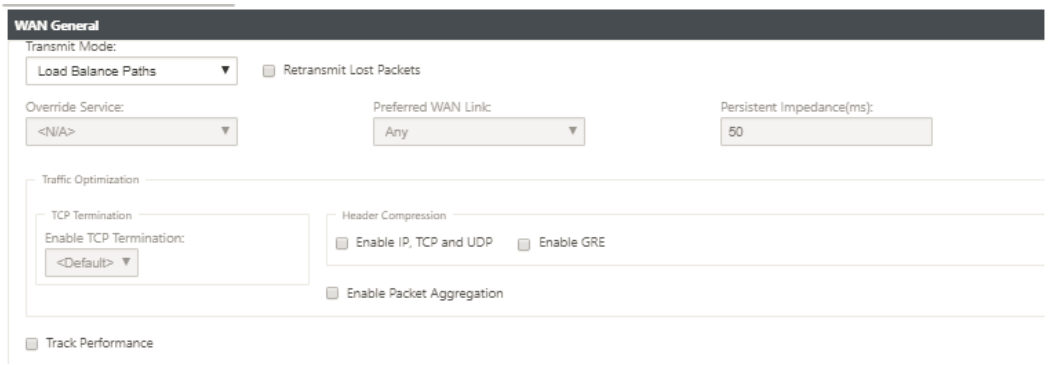
  > 注
  >
  > [**Dest=Src**] チェックボックスが選択されている場合、送信元ポートは宛先ポートにも使用されます。

- **DSCP**：トラフィックと照合する IP ヘッダー内の **DSCP** タグ。
- **VLAN**：トラフィックと照合する **VLAN ID** 。

7. 新しいルールの横にある追加（+）アイコンをクリックします。
8. [プロトコルを使用してプロパティを 初期化] をクリックして、ルールのデフォルトとプロトコルの推奨設定を適用して、ルールのプロパティを初期化します。これにより、デフォルトのルール設定が入力されます。次の手順に示すように、設定を手動でカスタマイズすることもできます。
9. [**WAN** 全般] タイルをクリックして、次のプロパティを構成します。

   - 送信モード：次のいずれかの送信モードを選択します。
     - ロードバランスパス: フローのトラフィックは、サービスの複数のパス間で分散されます。トラフィックは、そのパスが使用されるまで、最適パスを介して送信されます。残りのパケットは、次の最適パスを介して送信されます。
     - 永続パス：フローのトラフィックは、パスが使用できなくなるまで、同じパス上に残ります。
     - 重複パス：フローのトラフィックが複数のパス間で重複するため、信頼性が向上します。
     - オーバーライドサービス：フローのトラフィックは、別のサービスにオーバーライドされます。[オーバーライドサービス] フィールドで、サービスがオーバーライドするサービスタイプを選択します。たとえば、仮想パスサービスは、イントラネット、インターネット、またはパススルーサービスに上書きできます。
   - 失われたパケットの再送信：このルールに一致するトラフィックを、信頼できるサービス経由でリモートアプライアンスに送信し、失われたパケットを再送信します。
   - **TCP** 終端を有効にする：このフローのトラフィックの TCP 終端を有効にします。パケットの確認応答のラウンドトリップ時間が短縮されるため、スループットが向上します。

- 優先 **WAN** リンク：フローが最初に使用する WAN リンク。
- 永続インピーダンス：トラフィックが同じパス内に留まる最小時間（ミリ秒単位）。パスが設定値よりも長い待機時間になります。
- **IP**、**TCP**、および **UDP** を有効にする: IP、TCP、および UDP パケットのヘッダーを圧縮します。
- **GRE** を有効にする：**GRE** パケットのヘッダーを圧縮します。
- パケット集約を有効にする：小さなパケットを大きなパケットに集約します。
- パフォーマンスの追跡: このルールのパフォーマンス属性をセッションデータベースに記録します (損失、ジッタ、遅延、帯域幅など)。

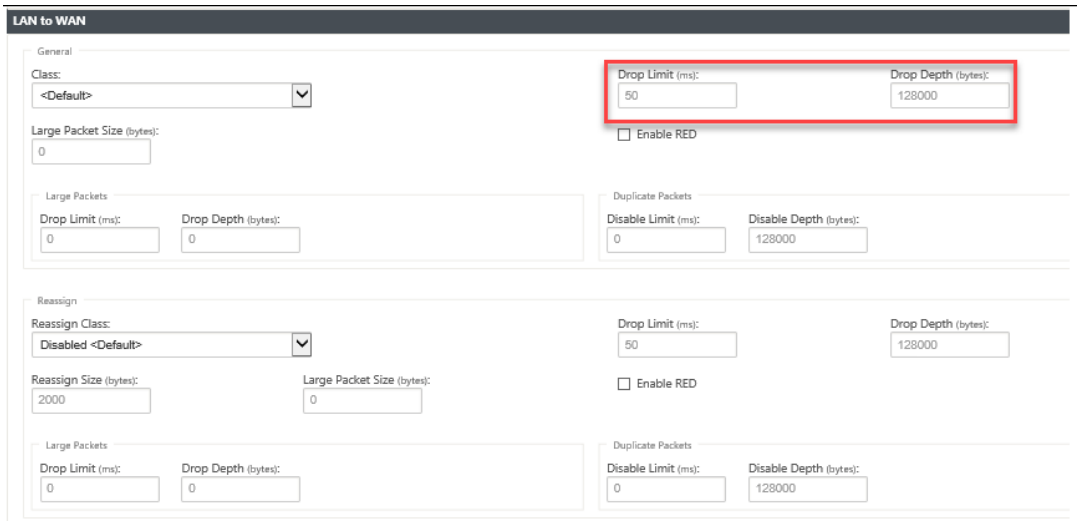


10. [**LAN to WAN**] タイルをクリックして、このルールの LAN から WAN への動作を構成します。

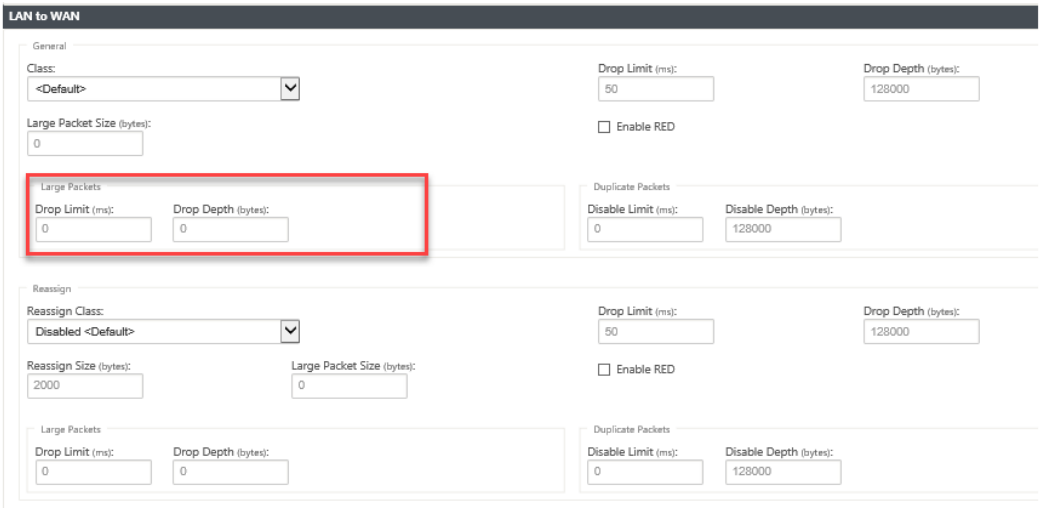
- クラス: このルールを関連付けるクラスを選択します。

> 注
>
> ルールを適用する前にクラスをカスタマイズすることもできます。詳細については、「クラスをカスタマイズする方法」を参照してください。

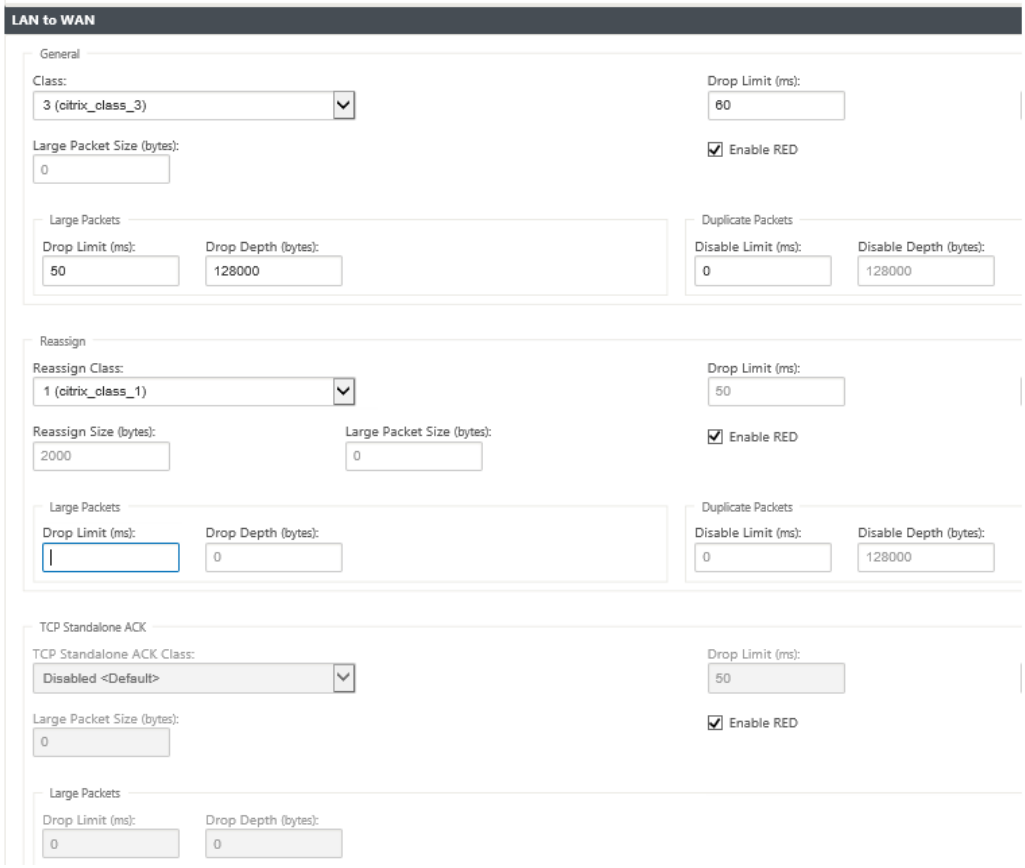
- **Large Packet Size**：このサイズ以下のパケットには、[**Class**] フィールドの右側にあるフィールドで指定された [**Drop **Limit**] および [Drop Depth**] の値が割り当てられます。



このサイズより大きいパケットには、画面の [Lar **ge** Packets] セクションのデフォルトの [**Drop Limit**] フィールドおよび [**Drop Depth**] フィールドで指定された値が割り当てられます。

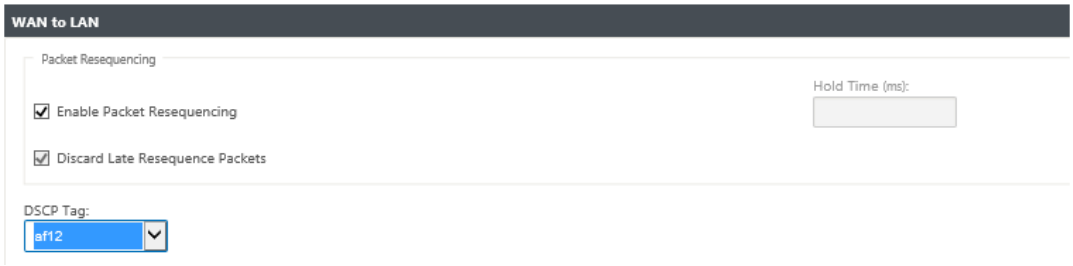


- [**Drop Limit**]：クラススケジューラで待機しているパケットがドロップされるまでの時間。バルククラスには適用されません。
- ドロップ深度：パケットがドロップされるキュー深度のしきい値。
- **RED** を有効にする：Random Early Detection（RED; ランダム早期検出）は、輻輳が発生したときにパケットを廃棄することにより、クラスリソースの公平な共有を保証します。
- **[Resassign Size**]：パケット長を超えると、[Reassign Class] フィールドで指定したクラスにパケットが再割り当てされます。
- **[Reassign**Class]：パケット長が [Reassign Size] フィールドで指定したパケット長を超えた場合に使用されるクラス。
- **Disable Limit**：重複パケットが帯域幅を消費するのを防ぐために重複を無効にできる時間。
- **Disable Dep**th：クラススケジューラのキューの深さ。この時点で、重複パケットは生成されません。
- **TCP** スタンドアロン **ACK** クラス: 大きなファイル転送中に TCP スタンドアロン確認がマッピングされる優先度の高いクラス。



11. [**WAN to LAN**] タイルをクリックして、このルールの WAN から LAN への動作を構成します。

    - パケットの再シーケンシングを有効にする：宛先で正しい順序でパケットを順序付けします。
    - **[Hold Time**]：パケットが再シーケンス処理のために保持され、その後パケットが LAN に送信される時間間隔。
    - 遅延再シーケンス処理パケットの破棄：再シーケンス処理に必要なパケットが LAN に送信された後に到着した順不同パケットを廃棄します。
    - **DSCP** タグ：LAN に送信する前に、このルールに一致するパケットに適用される DSCP タグ。



12. [ディープパケットインスペクション] タイルをクリックし、[パッシブ **FTP** 検出を有効にする] を選択して、FTP データ転送に使用されるポートをルールが検出し、検出されたポートにルール設定を自動的に適用できるようにします。

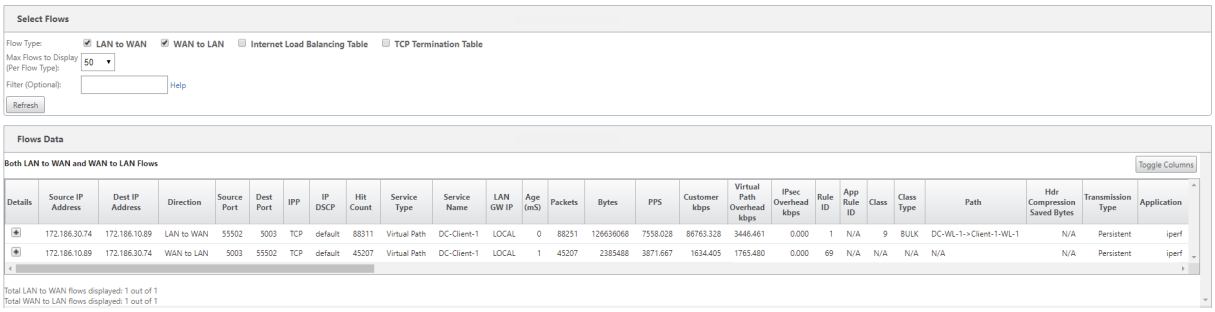
13. ［適用］をクリックします。

> 注
>
> 設定を保存し、変更管理の受信トレイにエクスポートして、変更管理プロセスを開始します。

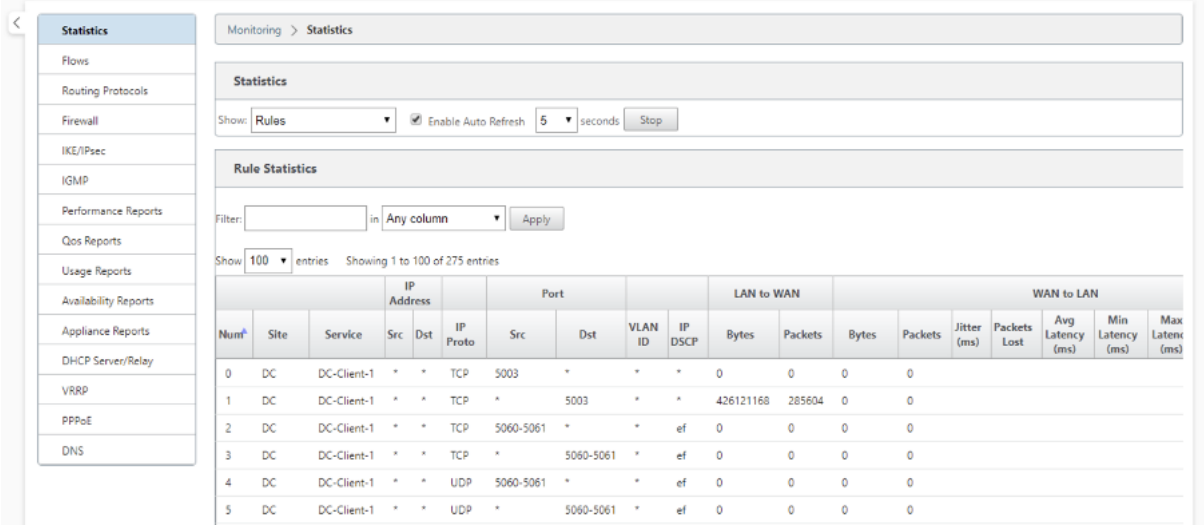
規則の確認

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

例：
「送信元 IP アドレスが 172.186.30.74、宛先 IP アドレスが 172.186.10.89 の場合、送信モードを永続パスに設定する」というルールには、次のフローデータが表示されます。



構成エディタで、[監視] **>** [統計] に移動し、構成済みのルールを確認します。



アプリケーション名別のルール

May 10, 2021

アプリケーション分類機能を使用すると、Citrix SD-WAN アプライアンスは着信トラフィックを解析し、特定のアプリケーションまたはアプリケーションファミリに属するものとして分類できます。この分類により、アプリケーションルールを作成して適用することにより、個々のアプリケーションファミリまたはアプリケーションファミリの QoS を強化できます。

アプリケーション、アプリケーションファミリ、またはアプリケーションオブジェクトマッチタイプに基づいてトラフィックフローをフィルタリングし、アプリケーションルールを適用できます。アプリケーションルールは、インターネットプロトコル (IP) ルールに似ています。IP 規則の詳細については、規則「IP アドレスとポート番号による」を参照してください。

すべてのアプリケーションルールに対して、転送モードを指定できます。使用可能な送信モードを次に示します。

- ロードバランスパス：フローのアプリケーショントラフィックは、複数のパス間で分散されます。トラフィックは、そのパスが使用されるまで、最適パスを介して送信されます。残りのパケットは、次の最適パスを介して送信されます。
- 永続パス：アプリケーショントラフィックは、パスが使用できなくなるまで同じパス上に残ります。
- 重複パス: アプリケーショントラフィックは複数のパス間で重複するため、信頼性が向上します。

アプリケーションルールはクラスに関連付けられています。クラスの詳細については、クラスのカスタマイズを参照してください。

デフォルトでは、以下の 5 つの事前定義されたアプリケーションルールが Citrix ICA アプリケーションで使用できます。

規則	クラス	送信モード	失われたパケットの再送信	パケット集約を有効にする	パケット再シーケンシングの有効化	リシーケンスの保持時間（ミリ秒）	レイトリシーケンスパケットの破棄	ドロップ制限 (ミリ秒)	ドロップ深度 (バイト)	RED を有効にする	無効限界 (ミリ秒)	深度の無効化 (バイト)
HDX_Priority_0 (HDX_priority_tag_0)	0	負荷分散パス	True	False	True	250	True	350	30000	True	0	128000
HDX_Priority_1 (HDX_priority_tag_1)	1	負荷分散パス	True	False	True	250	True	350	30000	True	0	128000

規則	クラス	送信モード	失われたパケットの再送信	パケット集約を有効にする	パケット再シーケンシングの有効化	リシーケンスの保持時間（ミリ秒）	レイトリシーケンスパケットの破棄	ドロップ制限 (ミリ秒)	ドロップ深度 (バイト)	RED を有効にする	無効限界 (ミリ秒)	深度の無効化 (バイト)
HDX_Priority_2	2 (HDX_priority_tag_2)	負荷分散パス	True	False	True	250	True	350	30000	True	0	128000
HDX_Priority_3	3 (HDX_priority_tag_3)	負荷分散パス	True	False	True	250	True	350	30000	True	0	128000
HDX	11 (interactive_high_class)	負荷分散パス	True	False	True	250	True	350	30000	True	0	128000

アプリケーションルールの適用方法

SD-WAN ネットワークでは、着信パケットが SD-WAN アプライアンスに到達すると、最初の少数のパケットが DPI 分類を受けません。この時点で、クラス、TCP 終端などの IP 規則属性がパケットに適用されます。DPI 分類後、Class、transmit モードなどのアプリケーションルールの属性は、IP ルールの属性を上書きします。

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

たとえば、SMTP プロトコルを使用する Google Mail などのウェブメールアプリケーションのアプリケーションルールを指定したとします。SMTP プロトコルの IP ルールセットは、最初に DPI 分類の前に適用されます。パケットを解析し、Google Mail アプリケーションに属するものとして分類した後、Google Mail アプリケーション用に指定されたアプリケーションルールが適用されます。

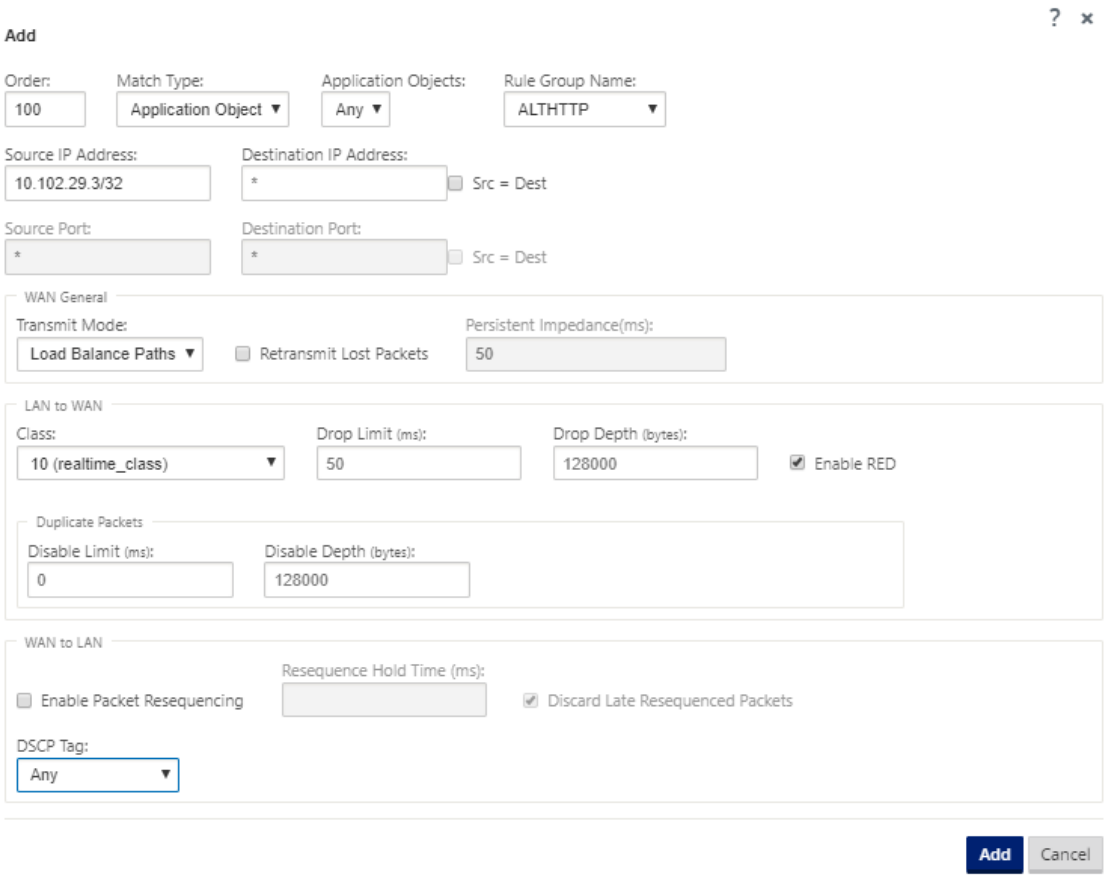
アプリケーションルールの作成

アプリケーション・ルールを作成する手順は、次のとおりです。

1. SD-WAN 設定エディタで、[グローバル] > [仮想パスデフォルトセット] に移動します。

2.「デフォルトセットを追加」をクリックし、デフォルトセットの名前を入力して、「追加」をクリックします。[セクション] フィールドで [アプリケーション **QoS**] を選択し、[**+**] をクリックします。

> 注
>
> [接続] > [仮想パス] **> [**アプリケーション **QoS]** または **[**** グローバル] > [動的仮想パスの ****** デフォルトセット] > [アプリケーション **QoS**] の順に選択して、アプリケーションルールを作成することもできます。



3. [順序] フィールドに、他の規則に関連して規則が適用されるタイミングを定義する順序値を入力します。

4. [**Match Type**] フィールドで、次のいずれかのマッチタイプを選択します。

   - [アプリケーション] —この一致タイプを選択した場合は、このフィルタの一致基準として使用するアプリケーションを指定します。
   - 「アプリケーションファミリ」—この一致タイプを選択した場合は、このフィルタの一致基準として使用するアプリケーションファミリを選択します。
   - 「アプリケーション・オブジェクト」—この一致タイプを選択した場合は、このフィルタの一致基準として使用するアプリケーション・オブジェクトを選択します。

アプリケーション、アプリケーションファミリ、およびアプリケーションオブジェクトの詳細については、「

アプリケーション分類」を参照してください。

5. [ルールグループ名] フィールドで、ルールグループを選択します。同じルールグループを持つルールの統計情報はグループ化され、まとめて表示できます。

   ルールグループを表示するには、[監視] > [統計] に移動し、[表示] フィールドで [ルールグループ] を選択します。

   カスタムルールグループを追加することもできます。詳しくは、「カスタムアプリケーションの追加と MOS の有効化」を参照してください。

6. アプリケーショントラフィックをフィルタリングするために、次のアプリケーションルールの一致基準を指定します。フィルタリングの後、ルール設定は、これらの基準に一致するサービスに適用されます。

   - 送信元 **IP** アドレス：トラフィックと照合する送信元 IP アドレスおよびサブネットマスク。
   - 宛先 **IP** アドレス：トラフィックと照合する宛先 IP アドレスおよびサブネットマスク。
   - **[**Source Port]：トラフィックと照合する送信元ポート番号またはポート範囲。
   - 宛先ポート：トラフィックと照合する宛先ポート番号またはポート範囲。

   > 注
   >
   > 送信元と宛先のインターネットプロトコルアドレスが同じ場合は、[**Src = Dest**] を選択します。

7. 次の一般的な WAN 設定を構成します。

   - [**Transmit Mode**] フィールドで、次のいずれかの送信モードを選択します。
     - ロードバランスパス：フローのアプリケーショントラフィックは、複数のパス間で分散されます。トラフィックは、そのパスが完全に使用されるまで、最適パスを介して送信されます。残りのパケットは、次の最適パスを介して送信されます。
     - 永続パス：アプリケーショントラフィックは、パスが使用できなくなるまで同じパス上に残ります。

       [**Persistent Impedance**] フィールドで、パス上の待機時間が設定された値よりも長くなるまで、トラフィックが同じパスに留まる最小時間をミリ秒単位で指定します。
     - 重複パス: アプリケーショントラフィックは複数のパス間で重複するため、信頼性が向上します。
   - [失われたパケットを再送信] をオンにすると、このルールに一致するトラフィックが信頼できるサービス経由でリモートアプライアンスに送信され、失われたパケットが再送信されます。

8. LAN から WAN への設定を構成します。

   - クラス: このルールを関連付けるクラスを選択します。

     ルールを適用する前にクラスをカスタマイズすることもできます。詳細については、「クラスのカスタマイズ」を参照してください。
   - [**Drop Limit**]：クラススケジューラで待機しているパケットがドロップされるまでの時間。バルククラスには適用されません。

- ドロップ深度：パケットがドロップされるまでのキューの深さのしきい値。
- **RED** を有効にする：Random Early Detection（RED; ランダム早期検出）は、輻輳が発生したときにパケットを廃棄することにより、クラスリソースの公平な共有を保証します。
- **Disable Limit**：重複パケットが帯域幅を消費するのを防ぐために、重複を無効にする時間。
- **Disable Dep**th：クラススケジューラのキューの深さ。この時点で、重複パケットは生成されません。

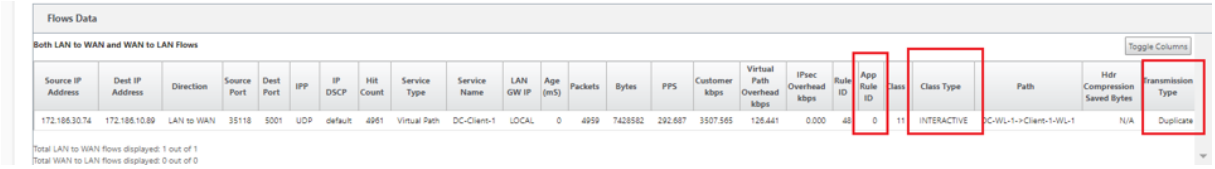
9. この規則に対して、次の WAN から LAN への動作を設定します。

- パケットの再シーケンシングを有効にする：宛先で正しい順序でパケットをシーケンスします。
- [**Resquence Hold Time**]：パケットがリシーケンシングのために保持され、その後パケットが LAN に送信される時間間隔。
- 遅延再シーケンス処理パケットの破棄：再シーケンス処理に必要なパケットが LAN に送信された後に到着した順不同パケットを廃棄します。

10. ［適用］をクリックします。

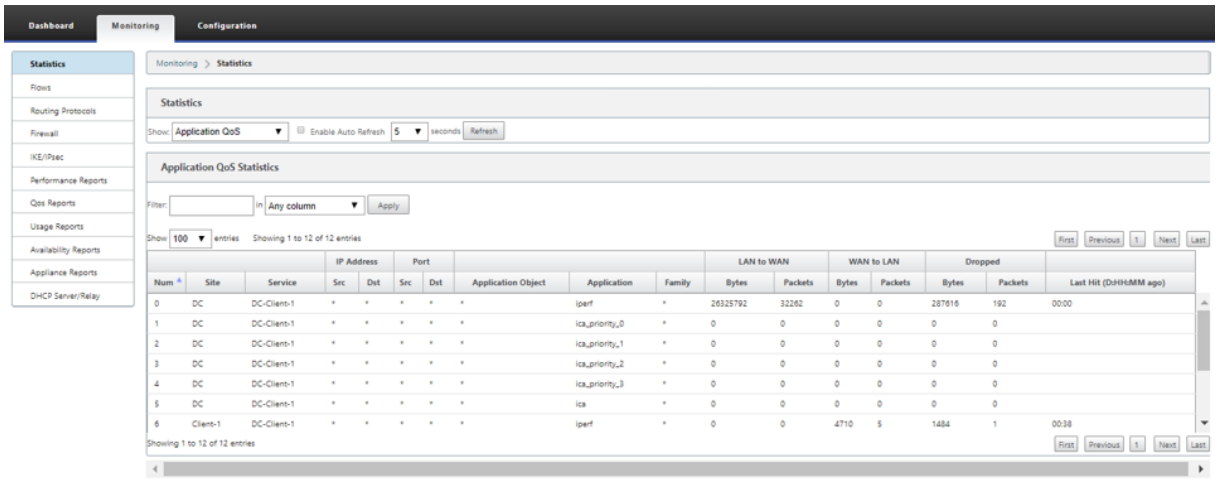
アプリケーションルールがトラフィックフローに適用されるかどうかを確認するには、**[**Monitoring**] > [Flows] に移動します。**

アプリのルール ID を書き留め、クラスタイプと送信モードがルール構成に従っているかどうかを確認します。



[Monitor **ing] > [**Statistics**] > [Application QoS] の順に選択すると、各サイトでアップロード、ダウンロード、ドロップされたパケット数やバイト数などの アプリケーション **QoS** を監視 ** できます。

Num パラメーターは、アプリルール ID を示します。フローから取得したアプリルール ID を確認します。



カスタムアプリケーションの作成

アプリケーション・オブジェクトを使用して、次の一致タイプに基づいてカスタム・アプリケーションを定義できます。

- IP プロトコル
- アプリケーション名
- アプリケーションファミリ

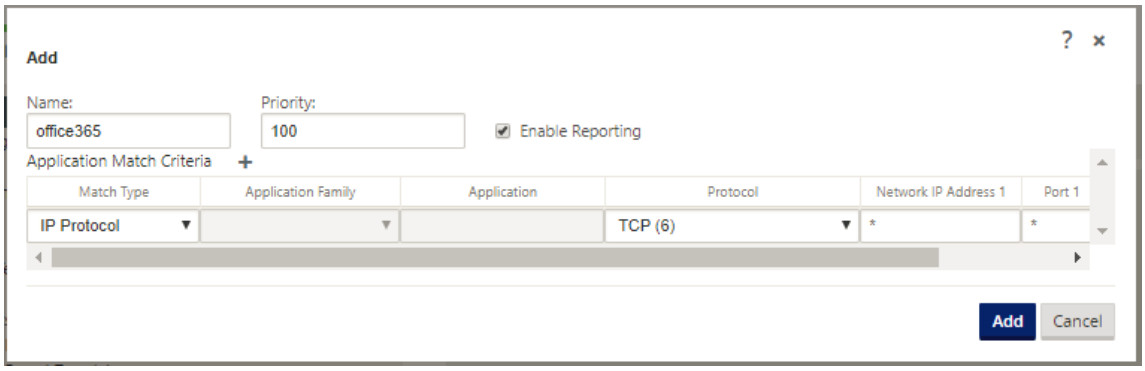
DPI 分類器は、着信パケットを分析し、指定された一致基準に基づいてアプリケーションとして分類します。これらの分類済みカスタムアプリケーションは、QoS、ファイアウォール、およびアプリケーションルーティングで使用できます。

> ヒント
>
> 1 つ以上のマッチタイプを指定できます。

SD-WAN Center では、分類されたカスタムアプリケーションのレポートを表示できます。詳しくは、「アプリケーションレポート」を参照してください。

カスタム・アプリケーションを作成するには、次の手順に従います。

1. 構成エディタで、「グローバル」>「アプリケーション」>「カスタムアプリケーション **」の順に選択し、「**+」をクリックします。



2. 次のパラメーターを設定します。

   - **[名前]:** カスタムアプリケーションの名前
   - レポートを有効にする**:** SD-WAN Center でカスタムアプリケーションレポートを表示できるようにします。詳しくは、「アプリケーションレポート」を参照してください。
   - 優先度: カスタムアプリケーションの優先度。着信パケットが 2 つ以上のカスタムアプリケーション定義と一致すると、最もプライオリティの高いカスタムアプリケーション定義が適用されます。

3. [アプリケーション一致条件] セクションの [+] をクリックします。

4. 次のいずれかのマッチタイプを選択します。

   - **IP** プロトコル: プロトコル、ネットワーク IP アドレス、ポート番号、および DSCP タグを指定します。

- アプリケーション: アプリケーション名、ネットワーク IP アドレス、ポート番号、および DSCP タグを指定します。
- アプリケーションファミリ: アプリケーションファミリを選択し、ネットワーク IP アドレス、ポート番号、および DSCP タグを指定します。

5. アプリケーションの一致基準を追加するには、[**+**] をクリックします。
6. ［適用］をクリックします。

ルールグループを追加して **MOS** を有効にする

May 10, 2021

ネットワーク内の特定のアプリケーションは、そのアプリケーションに適用される規則のグループによって定義できます。SD-WAN 構成エディタには、ルールグループのデフォルトリストが表示されます。また、カスタム規則グループを作成し、個別の IP 規則またはアプリケーション QoS 規則をアプリケーションにタグ付けすることもできます。

規則の詳細については、IP アドレスとポート番号による規則およびアプリケーション名による規則を参照してください。

同じルールグループを持つルールの統計情報は、グループ化され、まとめて表示できます。

ルールグループに基づいて統計情報を表示するには、[モニタリング**] > [**統計**]** に移動し、[表示**]** フィールドで [ルールグループ] を選択します。

平均オピニオンスコア（MOS）は、アプリケーションがエンドユーザーに提供するエクスペリエンスの品質の数値指標です。主に VoIP アプリケーションに使用されます。SD-WAN では、トラフィックを VoIP コールであるかのように判断することで、非 VoIP アプリケーションの品質を評価するためにも使用されます。

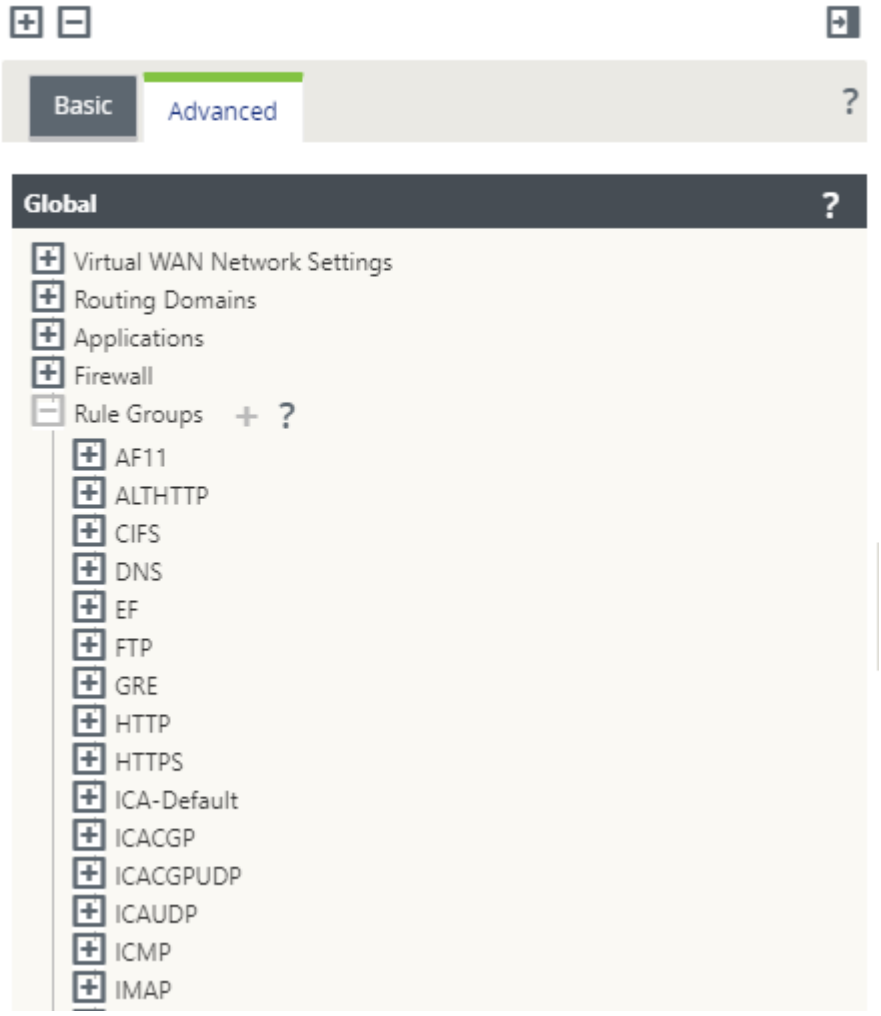
平均 MOS スコアは、サンプリング間隔が 1 分で計算されます。他のサードパーティ製ツールによって計算される MoS スコアは、使用するサンプリング間隔によって異なる場合があります。

SD-WAN Center には、仮想パスを通過する既存のトラフィックの MOS が表示されます。SD-WAN Center で MOS を表示する方法については、アプリケーション向け MOSを参照してください。

カスタム・ルール・グループを追加するには、次の手順に従います。

1. 構成エディタで、[グローバル] > [規則グループ**]** に移動します。。ルールグループのデフォルトリストが表示されます。
2. 追加 (+) アイコンをクリックします。
3. アプリケーション名を入力します。

4. 編集アイコンをクリックし、[**MOS** を有効にする] を選択します。



5. [適用] をクリックします。

> 注
>
> - [Enable MOS] を選択して、デフォルトアプリケーションの **MOS** 推定を有効にすることもできます。
> - アプリケーションの MOS を推定し、SD-WAN Center に表示するには、[ルール] の [パフォーマンスの追跡] オプションを有効にします。詳細については、アプリケーション向け MOSを参照してください。

アプリケーション分類

June 8, 2022

Citrix SD-WAN アプライアンスは、ディープ・パケット・インスペクション（DPI）を実行して、次の手法を使用してアプリケーションを識別および分類します。

- DPI ライブラリの分類
- シトリックス独自の独立コンピューティングアーキテクチャ（ICA）分類
- アプリケーションベンダー API (たとえば、Office 365 用の Microsoft REST API)
- ドメイン名ベースのアプリケーション分類

DPI ライブラリの分類

ディープパケットインスペクション (DPI) ライブラリは、数千もの商用アプリケーションを認識します。これにより、アプリケーションのリアルタイムの検出とクラス分けが可能になります。SD-WAN アプライアンスは DPI テクノロジーを使用して、着信パケットを分析し、トラフィックを特定のアプリケーションまたはアプリケーションファミリに属するものとして分類します。各接続のアプリケーション分類には、数個のパケットが必要です。

DPI ライブラリ分類を有効にするには、構成エディタで、[グローバル**] > [**アプリケーション**] > [DPI** 設定] に移動し、[ディープパケットインスペクションを有効にする] チェックボックスをオンにします。

ICA の分類

Citrix SD-WAN アプライアンスでは、Virtual Apps and Desktops の Citrix HDX トラフィックを識別および分類することもできます。Citrix SD-WAN は、ICA プロトコルの次のバリエーションを認識します。

- ICA
- ICA-CGP
- シングルストリーム ICA（SSI）
- マルチストリーム ICA（MSI）
- TCP 経由の ICA
- ICA オーバー UDP/EDT
- 非標準ポート経由の ICA（マルチポート ICA を含む）
- HDX アダプティブ トランスポート
- WebSocket 経由の ICA（HTML5 レシーバで使用）

> 注
>
> SSL/TLS または DTLS 経由で配信される ICA トラフィックの分類は、SD-WAN Standard Edition ではサポートされませんが、SD-WAN Premium Edition と SD-WAN WANOP Edition ではサポートされます。
>
> ネットワークトラフィックの分類は、初期接続またはフロー確立時に行われます。したがって、既存の接続は ICA に分類されません。接続テーブルを手動でクリアすると、接続の分類も失われます。
>
> Framehawk トラフィックとオーディオオーバー UDP/RTP は、HDX アプリケーションには分類されません。「UDP」または「不明なプロトコル」のいずれかとして報告されます。

> リリース 10 バージョン 1 以降、SD-WAN アプライアンスは、シングルポート構成であっても、マルチストリーム ICA の各 ICA データストリームを区別することができます。各 ICA ストリームは、優先順位付けのための独自のデフォルト QoS クラスを持つ個別のアプリケーションとして分類されます。
>
> - マルチストリーム ICA 機能を正しく動作させるには、SD-WANStandard Edition10.1 以降、または SD-WAN Premium Edition が必要です。
> - SDWAN-Center で HDX ユーザーベースのレポートを表示するには、SD-WANStandard Edition または Premium Edition 11.0 以降が必要です。
>
> HDX 情報仮想チャネルの最小ソフトウェア要件:
>
> - XenApp および XenDesktop 7.17 で前提となる機能が導入され、7.15 長期サービスリリースには含まれていないため、Citrix Virtual Apps and Desktops（旧 XenApp および XenDesktop）の 7～1912 長期サービスリリースまたは現行リリース。
> - マルチストリーム ICA および HDX インサイト情報仮想チャネル CTXNSAP をサポートする Citrix Workspace アプリ（またはその前身である Citrix Receiver）のバージョン。Citrix Workspace アプリの機能マトリックスで、**NSAP VC** およびマルチポート/マルチストリーム **ICA** を使用した **HDX Insight** を探します。現在サポートされているリリースバージョンについては、HDX インサイトを参照してください。

分類されると、ICA アプリケーションはアプリケーションルールで使用され、他の分類されたアプリケーションと同様のアプリケーション統計を表示できます。

ICA アプリケーションには、以下の優先順位タグに対して 5 つのデフォルトのアプリケーションルールがあります。

- 独立コンピューティングアーキテクチャ（Citrix）（ICA）
- ICA リアルタイム (ica_priority_0)
- ICA インタラクティブ (ica_priority_1)
- ICA バルクトランスファー (ica_prority_2)
- ICA の背景 (ica_priority_3)

詳しくは、「アプリケーション名による規則」を参照してください。

マルチストリーム ICA をサポートしていないソフトウェアを 1 つのポート上で組み合わせて実行している場合、QoS を実行するには、ICA ストリームごとに 1 つずつ、複数のポートを設定する必要があります。
XA/XD サーバーポリシーで構成された非標準ポートで HDX を分類するには、これらのポートを ICA ポート構成に追加する必要があります。また、これらのポートのトラフィックを有効な IP ルールに一致させるには、ICA IP ルールを更新する必要があります。

ICA IP とポートリストで、XA/XD ポリシーで使用する非標準ポートを指定して、HDX 分類を処理できます。IP アドレスは、ポートを特定の宛先にさらに制限するために使用されます。任意の IP アドレス宛てのポートには ‘*’ を使用します。SSL ポートを組み合わせた IP アドレスは、トラフィックが最終的に ICA に分類されない場合でも、トラフィックが ICA である可能性が高いことを示すためにも使用されます。この表示は、Citrix Application Delivery

Management でマルチホップレポートをサポートするために L4 AppFlow レコードを送信するために使用されます。

ICA ベースの分類を有効にするには、構成エディタで［グローバル］**>**［アプリケーション］**>**［**DPI** 設定］に移動し、［**Citrix ICA** アプリケーションのディープパケットインスペクションを有効にする］チェックボックスをオンにします。

アプリケーションベンダー **API** ベースの分類

Citrix SD-WAN では、次のアプリケーションベンダー API ベースの分類がサポートされています。

- Office 365。詳しくは、「Office 365 の最適化」を参照してください。
- Citrix Cloud および Citrix Gateway サービス。詳しくは、「ゲートウェイサービスの最適化」を参照してください。

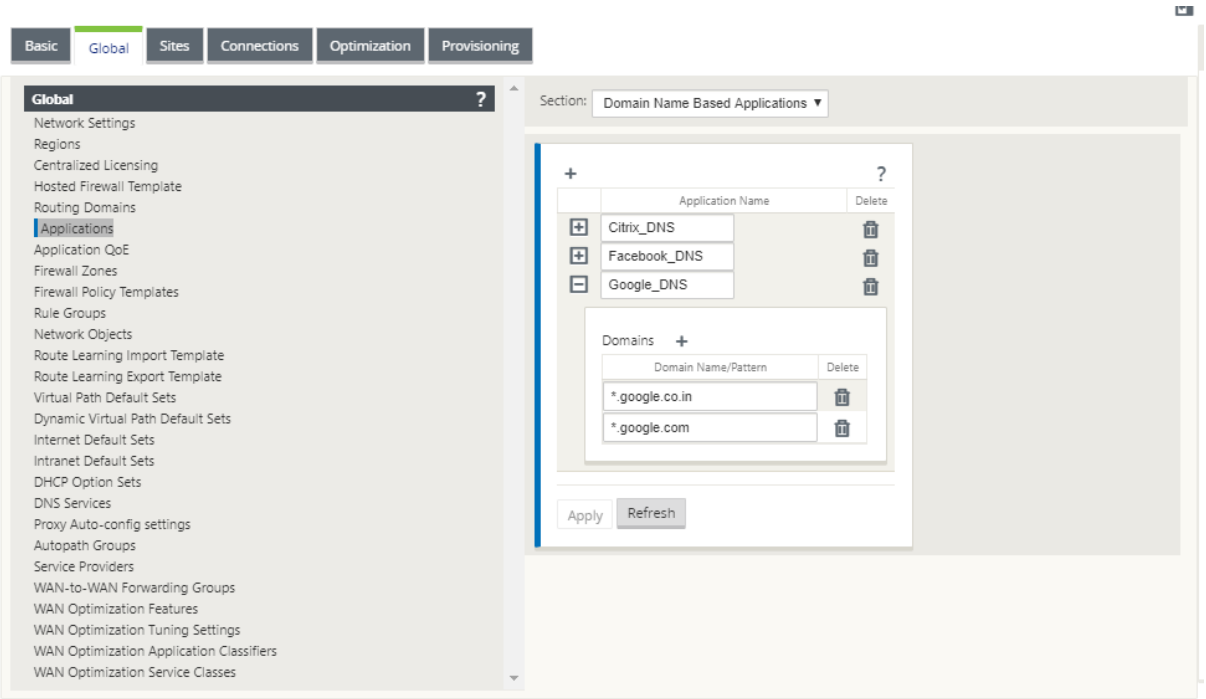
ドメイン名ベースのアプリケーション分類

DPI 分類エンジンが拡張され、ドメイン名とパターンに基づいてアプリケーションを分類できるようになりました。DNS フォワーダが DNS 要求を代行受信して解析した後、DPI エンジンは IP 分類子を使用して最初のパケット分類を実行します。さらに DPI ライブラリと ICA 分類が行われ、ドメイン名ベースのアプリケーション ID が追加されます。

ドメイン名ベースのアプリケーション機能を使用すると、複数のドメイン名をグループ化し、単一のアプリケーションとして扱うことができます。ファイアウォール、アプリケーションステアリング、QoS、およびその他のルールを簡単に適用できます。最大 64 のドメイン名ベースのアプリケーションを構成できます。

ドメイン名ベースのアプリケーションを定義するには、構成エディタで [グローバル] > [アプリケーション] > [ドメイン名ベースのアプリケーション] に移動します。アプリケーション名を入力し、必要なドメイン名またはパターンを追加します。完全なドメイン名を入力することも、先頭にワイルドカードを使用することもできます。次のドメイン名の形式を使用できます。

- example.com
- *.example.com



分類されたドメイン名ベースのアプリケーションは、次の設定に使用されます。

- DNS プロキシ
- DNS トランスペアレントフォワーダ
- アプリケーションオブジェクト
- アプリケーションルート
- ファイアウォールポリシー
- アプリケーション QoS ルール
- アプリケーション QoE

制限事項

- ドメイン名ベースのアプリケーションに対応する DNS 要求/応答がない場合、DPI エンジンはドメイン名ベースのアプリケーションを分類しないため、ドメイン名ベースのアプリケーションに対応するアプリケーションルールを適用しません。
- ポート範囲にポート 80 および/またはポート 443 が含まれ、ドメイン名ベースのアプリケーションに対応する特定の IP アドレス一致タイプが含まれるようにアプリケーションオブジェクトが作成された場合、DPI エンジンはドメイン名ベースのアプリケーションを分類しません。
- 明示的な Web プロキシが設定されている場合は、DNS 応答が必ず同じ IP アドレスを返すとは限らないように、すべてのドメイン名パターンを PAC ファイルに追加する必要があります。
- ドメイン名ベースのアプリケーション分類は、設定のアップグレード時にリセットされます。再分類は、DPI ライブラリ分類、ICA 分類、ベンダーアプリケーション API ベースの分類など、11.0.2 以前のリリース分類手法に基づいて行われます。

- ドメイン名ベースのアプリケーション分類によって学習されたアプリケーションシグニチャ（宛先 IP アドレス）は、設定の更新時にリセットされます。
- 標準 DNS クエリとその応答のみが処理されます。
- AAAA レコードまたは IPv6 レコードはサポートされていません。
- 複数のパケットに分割された DNS 応答レコードは処理されません。単一のパケット内の DNS 応答のみが処理されます。
- TCP 経由の DNS はサポートされていません。
- ドメイン名のパターンとしてサポートされるのは、トップレベルドメインのみです。

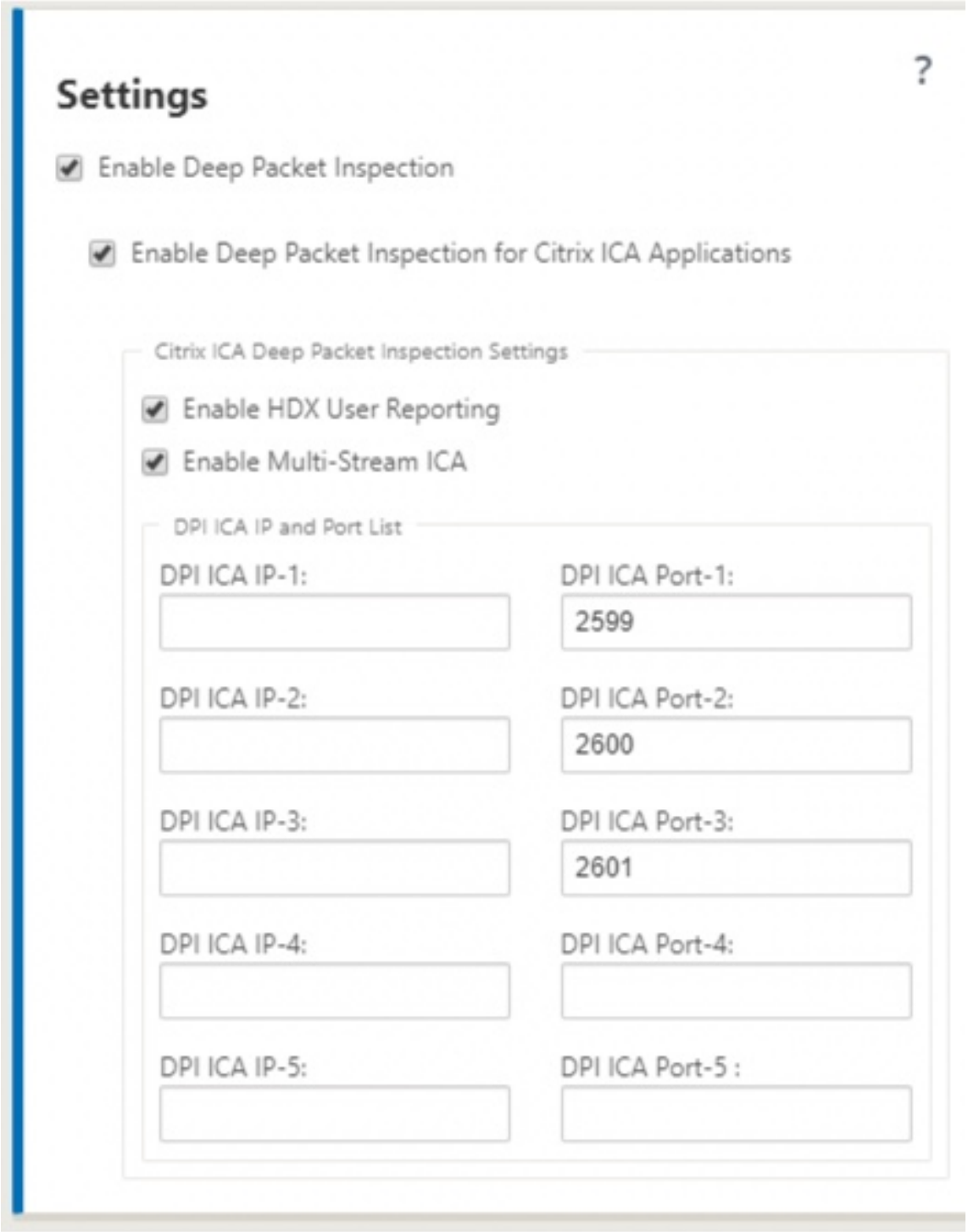
暗号化されたトラフィックの分類

Citrix SD-WAN アプライアンスは、アプリケーションレポートの一部として暗号化されたトラフィックを次の 2 つの方法で検出してレポートします。

- HTTPS トラフィックの場合、DPI エンジンは SSL 証明書を検査して、サービスの名前 (たとえば Facebook、Twitter) を含む共通名を読み取ります。アプリケーションアーキテクチャによっては、複数のサービスタイプ (たとえば、電子メール、ニュースなど) に 1 つの証明書だけが使用されることがあります。異なるサービスで異なる証明書を使用する場合、DPI エンジンはサービスを区別できます。
- 独自の暗号化プロトコルを使用するアプリケーションの場合、DPI エンジンはフロー内のバイナリパターンを検索します。たとえば、Skype の場合、DPI エンジンは証明書内のバイナリパターンを検索し、アプリケーションを決定します。

アプリケーション分類設定を構成するには、次の手順に従います。

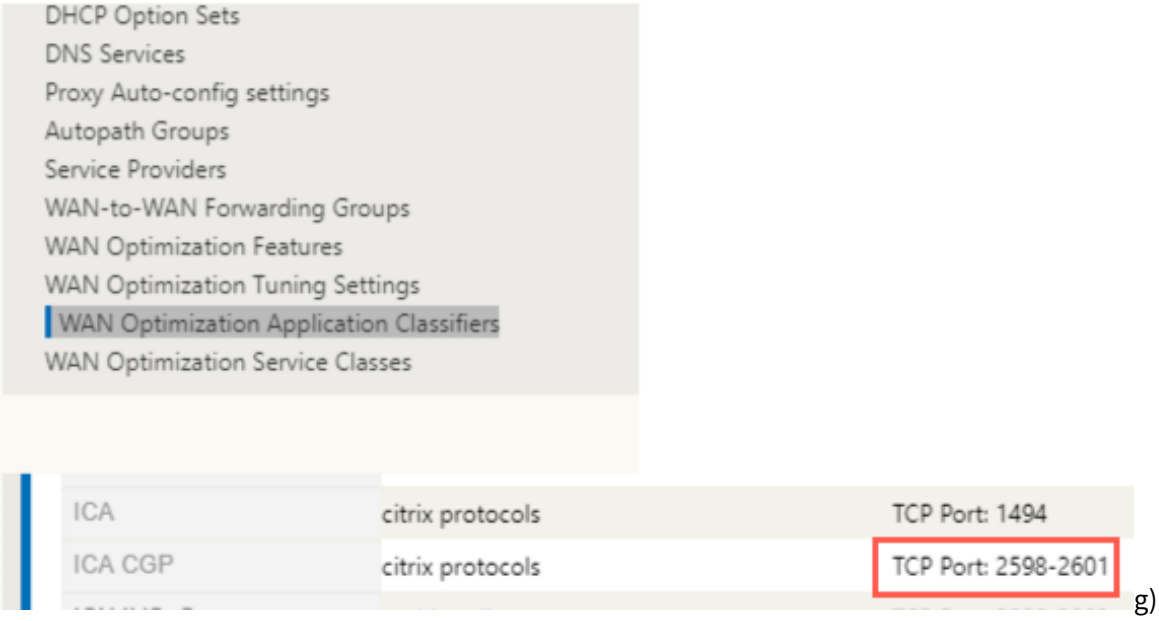
1. 構成エディタで、[グローバル] > [アプリケーション] > [設定] をクリックします。



注

マルチポート展開用に追加の ICA ポートを追加する場合は、WAN 最適化アプリケーション分類子でこれらのポートを追加する必要があります。そうしないと、3 つの追加ポートのトラフィックは wanop に転送されません。ICA が最適化するように構成されている場合、デフォルトの 2598 ポートのみが転

> 送されます。

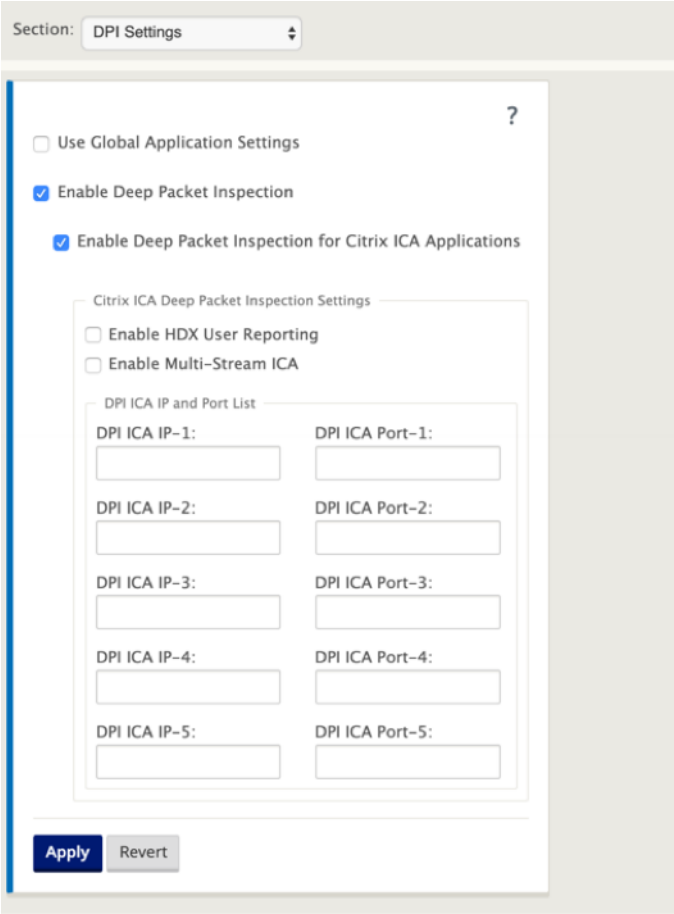


2. [ディープパケットインスペクションを有効にする] を選択します。これにより、アプライアンスでアプリケーションの分類が可能になります。SD-WAN Center では、アプリケーションの統計情報を表示、監視できます。詳しくは、「アプリケーションレポート」を参照してください。

> 注
>
> デフォルトでは、ディープパケットインスペクションの有効化（**Enable Deep Packet Inspection** ）は、分類されたデータの統計情報を収集します。

3. ［**Citrix ICA** アプリケーションのディープ・パケット・インスペクションを有効にする］を選択します。これにより、Citrix ICA アプリケーションの分類が可能になり、ユーザー、セッション、フロー数の統計が収集されます。このオプションを有効にしないと、HDX トラフィックのフレーバーの一部が分類され、QoE が計算されますが、SD-WAN Center の統計情報は利用できません。SD-WAN Center では、ICA アプリケーションの統計情報を表示、監視できます。このオプションは、デフォルトで有効になっています。詳しくは、「HDX レポート」を参照してください。

4. ［**HDX** ユーザーレポートを有効にする］を選択して、新しく追加されたユーザーベースのレポート（[HDX サマリー]、[HDX ユーザーセッション]、[**HDX** アプリ]）を生成します。これらのレポートは、SD-WAN Center で使用できます。これは、**HDX** サイト統計 レポートには適用されません。このオプションは、DPI オプションを有効にするのと同様に、グローバルレベルおよびサイトレベルで使用できます。サイトレベルで **HDX** ユーザーレポートを有効にするには、構成エディターで［接続］**>**［アプリケーション］をクリックします。



5. **DPI ICA** ポートで、HDX 分類を処理する XA/XD ポリシーで使用される非標準ポートを指定します。標準ポート番号 2598 または 1494 は、内部的にすでに含まれているため、このリストには含めないでください。
6. **DPI ICA IP** で、ポートを特定の宛先にさらに制限するために使用する IP アドレスを指定します。

   > 注
   >
   > 任意の IP アドレス宛てのポートには ‘*’ を使用します。

7. [適用] をクリックします。

アプリケーション分類の設定は、各サイトで個別に構成できます。[接続] をクリックし、サイトを選択して、[アプリケーション設定] をクリックします。また、グローバルアプリケーション設定を使用することもできます。

アプリケーションの検索

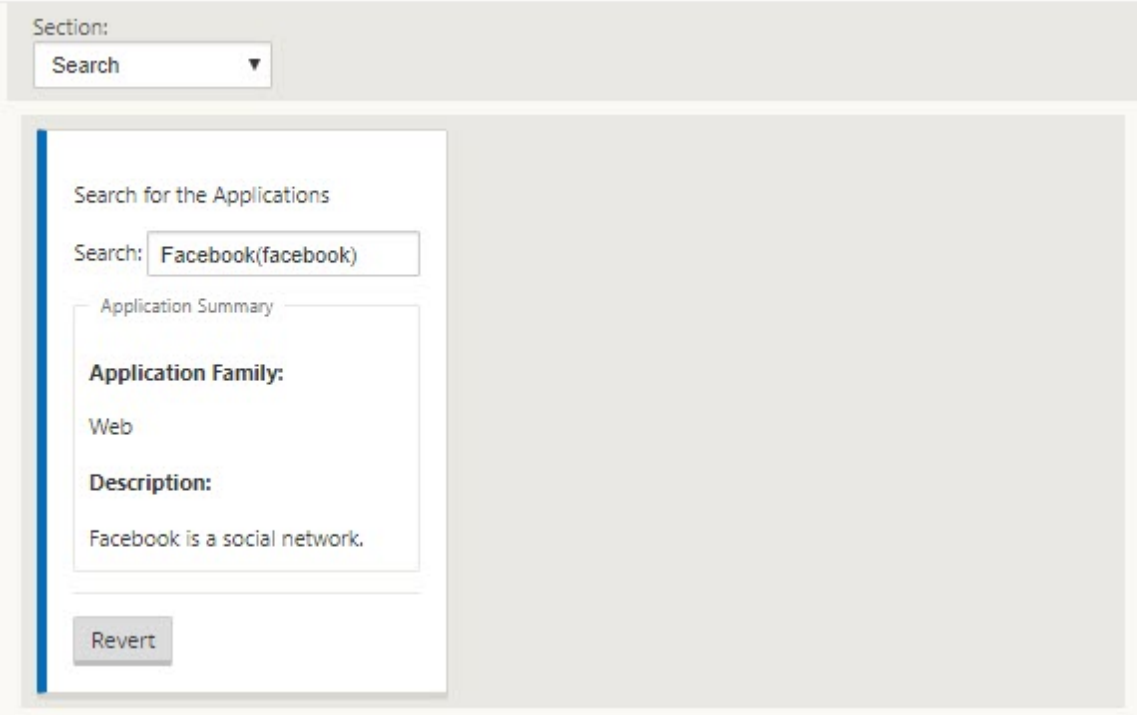
アプリケーションを検索して、アプリケーション・ファミリ名を特定できます。アプリケーションの簡単な説明も提供されます。

アプリケーションを検索する手順は、次のとおりです。

1. 構成エディターで、[グローバル] > [アプリケーション] > [検索] をクリックします。

2. [Search] フィールドにアプリケーションの名前を入力し、[Enter] をクリックします。

   アプリケーションとアプリケーション・ファミリ名の簡単な説明が表示されます。



次の機能は、マッチタイプとしてアプリケーションを使用します。

- ファイアウォールポリシー
- アプリケーション QoS ルール
- アプリケーション QoE

> 注
>
> ディープパケットインスペクションを使用して SD-WAN アプライアンスが識別できるアプリケーションについては、アプリケーション署名ライブラリを参照してください。

アプリケーションオブジェクト

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

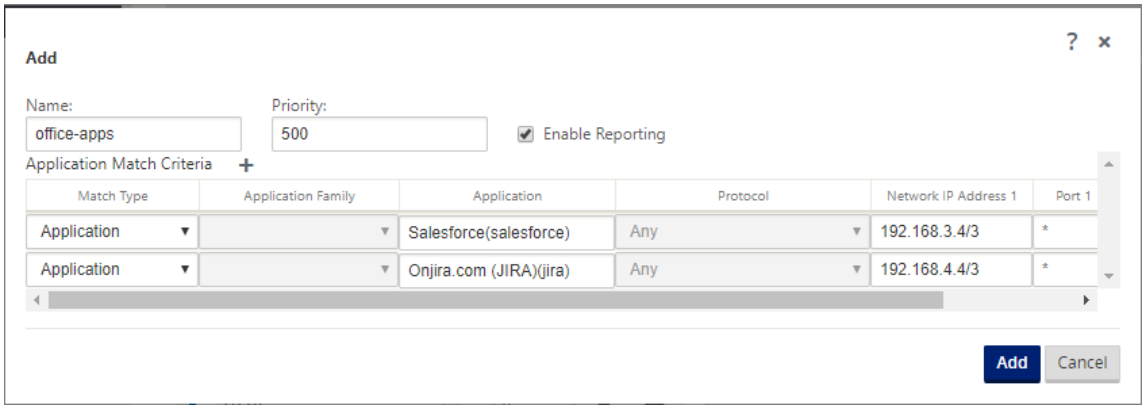
次の機能では、アプリケーションオブジェクトを一致タイプとして使用します。

- アプリケーションルート
- ファイアウォールポリシー

- アプリケーション QoS ルール
- アプリケーション QoE

アプリケーション・オブジェクトを作成する手順は、次のとおりです。

1. 構成エディターで、「グローバル」>「アプリケーション」>「アプリケーションオブジェクト」をクリックします。
2. [追加] をクリックし、[名前] フィールドにオブジェクトの名前を入力します。

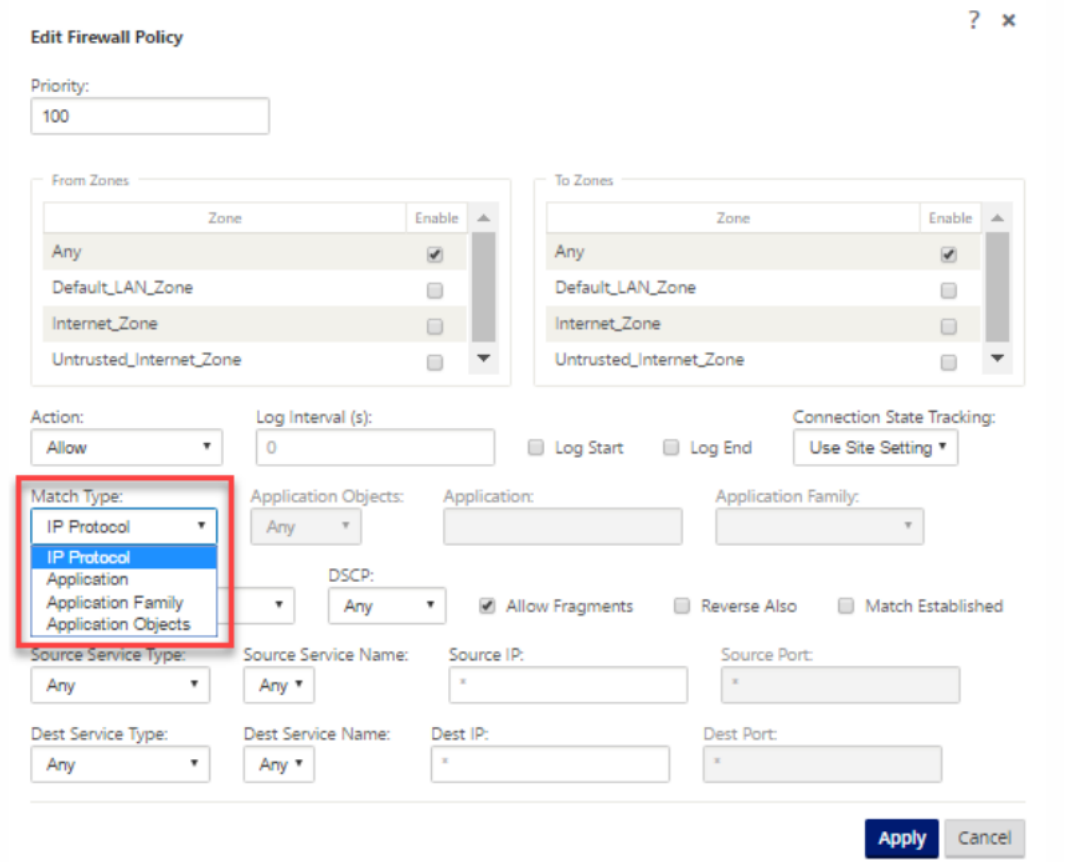


3. **Citrix SD-WAN Center** でカスタムアプリケーションレポートを表示できるようにするには、［レポートを有効にする］を選択します。詳しくは、「アプリケーションレポート」を参照してください。
4. [**Priority**] フィールドに、アプリケーションオブジェクトの優先度を入力します。着信パケットが 2 つ以上のアプリケーションオブジェクト定義と一致すると、プライオリティが最も高いアプリケーションオブジェクトが適用されます。
5. [アプリケーション一致基準] セクションで [**+**] をクリックします。
6. 次のいずれかのマッチタイプを選択します。
   - **IP** プロトコル: プロトコル、ネットワーク IP アドレス、ポート番号、および DSCP タグを指定します。
   - アプリケーション: アプリケーション名、ネットワーク IP アドレス、ポート番号、および DSCP タグを指定します。
   - アプリケーションファミリ: アプリケーションファミリを選択し、ネットワーク IP アドレス、ポート番号、および DSCP タグを指定します。
7. アプリケーションの一致基準を追加するには、[**+**] をクリックします。
8. ［追加］をクリックします。

ファイアウォールでのアプリケーション分類の使用

トラフィックをアプリケーション、アプリケーションファミリ、またはドメイン名として分類すると、アプリケーション、アプリケーションファミリ、およびアプリケーションオブジェクトを一致タイプとして使用して、トラフィッ

クをフィルタリングし、ファイアウォールポリシーとルールを適用できます。これは、すべてのプレポリシー、ポストポリシー、およびローカルポリシーに適用されます。ファイアウォールの詳細については、ステートフルファイアウォールと NAT のサポートを参照してください。



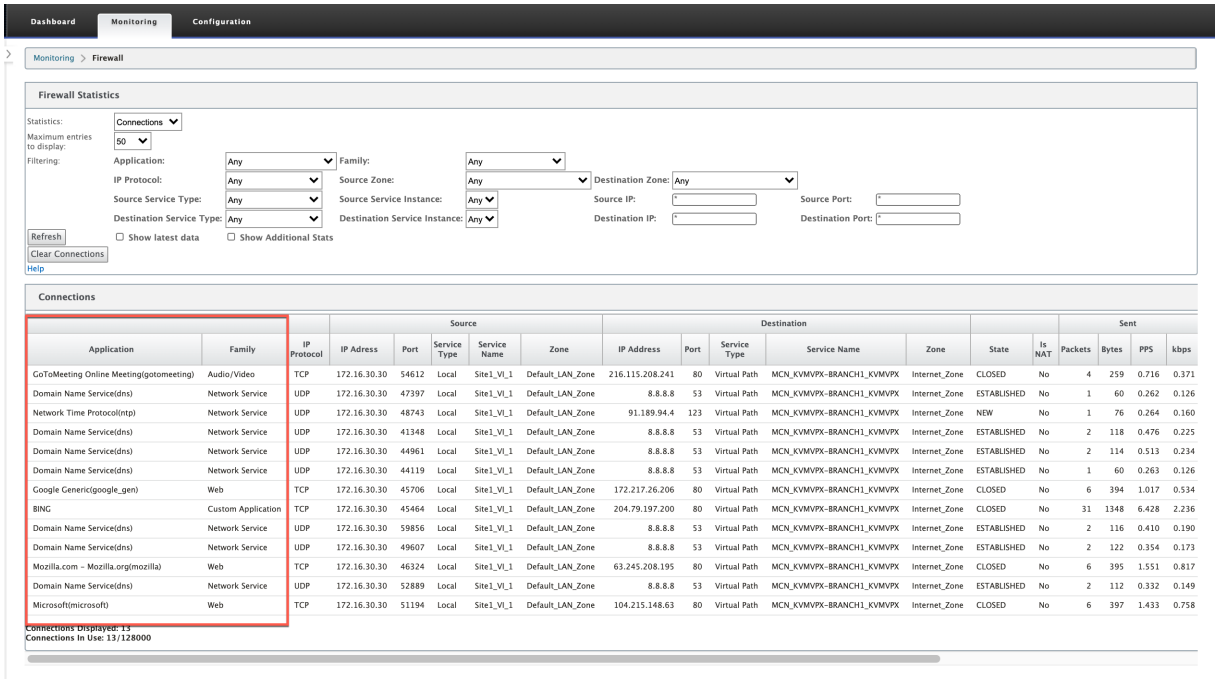
アプリケーション分類の表示

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

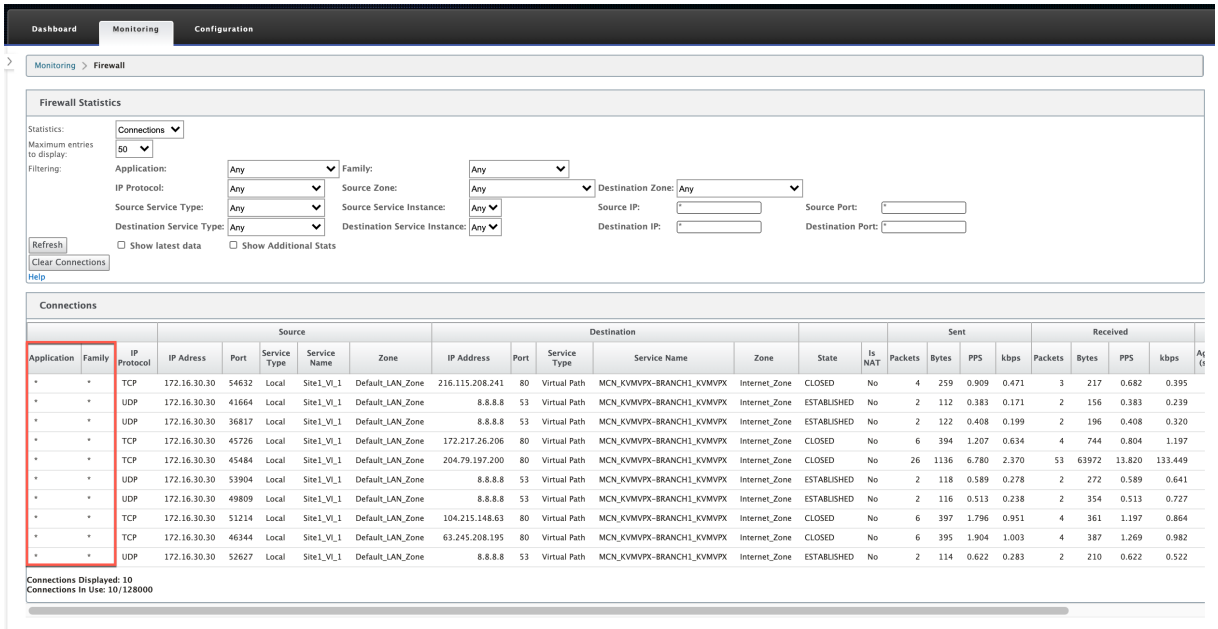
- ファイアウォール接続の統計情報
- フロー情報
- アプリケーション統計

ファイアウォール接続の統計情報

構成エディタで、**[監視] > [ファイアウォール]** に移動します。[接続] セクションの [アプリケーション] 列と [ファミリ] 列には、アプリケーションとその関連ファミリが一覧表示されます。

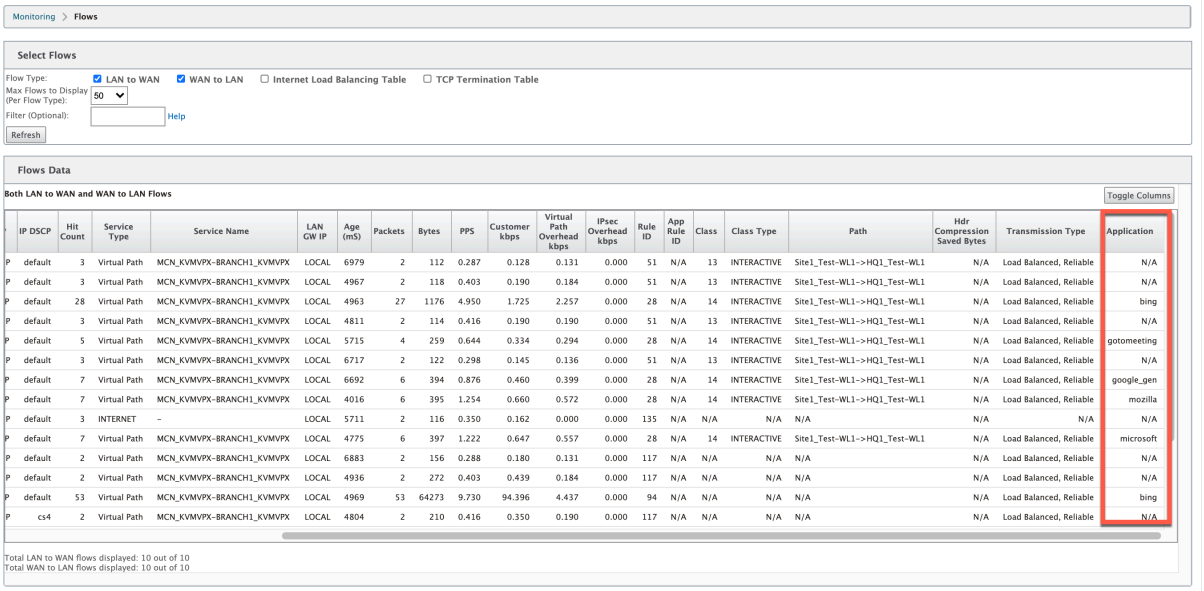


アプリケーションの分類を使用可能にしない場合、「アプリケーション」列と「ファミリ」列にはデータが表示されません。



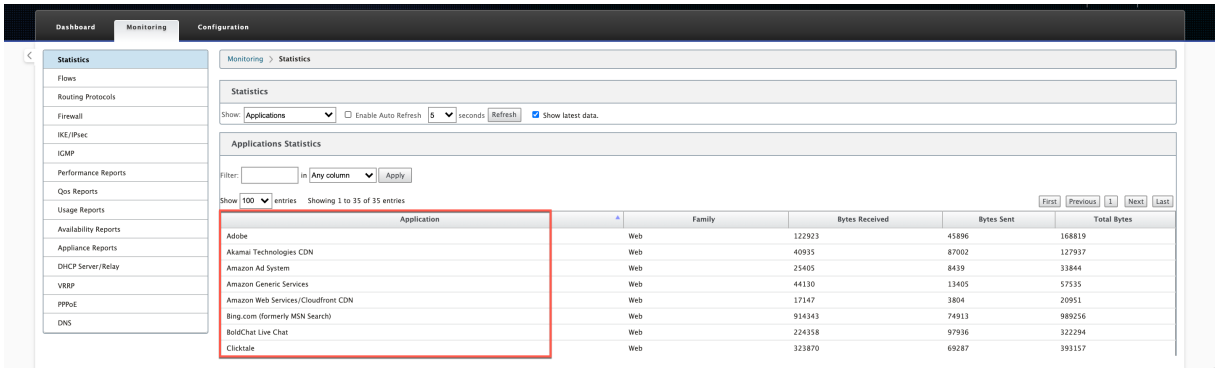
フロー情報

構成エディタで、**[監視] > [フロー]** に移動します。「フロー・データ」セクションの「アプリケーション」列にアプリケーションの詳細がリストされます。



アプリケーション統計

構成エディタで、**[監視] > [統計]** に移動します。[アプリケーション統計] セクションの [アプリケーション] 列に、アプリケーションの詳細が表示されます。



トラブルシューティング

アプリケーションの分類を有効にした後、[**Monitoring**] セクションの下にレポートを表示し、アプリケーションの詳細が表示されることを確認できます。詳しくは、「アプリケーション分類の表示」を参照してください。

予期しない動作が発生した場合は、問題が発生している間に STS 診断バンドルを収集し、Citrix サポートチームと共有します。

STS バンドルは、**[構成] > [システムメンテナンス] > [診断] > [診断情報]** を使用して作成およびダウンロードできます。

QoS 公平性（RED）

May 10, 2021

QoS 公平性機能は、QoS クラスと Random Early Detection（RED; ランダム早期検出）を使用して、複数の仮想パスフローの公平性を向上させます。仮想パスは、16 種類のクラスのいずれかに割り当てることができます。クラスは、次の 3 つの基本タイプのいずれかになります。

- リアルタイムクラスは、特定の帯域幅制限までプロンプトサービスを要求するトラフィックフローを提供します。総スループットよりも低レイテンシが推奨されます。
- インタラクティブクラスの優先順位は、リアルタイムよりも低くなりますが、バルクトラフィックよりも絶対的な優先順位を持ちます。
- バルククラスは、リアルタイムおよび対話型クラスから残っているものを取得します。これは、バルクトラフィックにとってレイテンシーはあまり重要ではないためです。

ユーザは、クラスごとに異なる帯域幅要件を指定します。これにより、仮想パススケジューラは、同じタイプの複数のクラスから競合する帯域幅要求を調停できます。スケジューラは、クラス間の公平性を達成するために、階層公平サービス曲線（HFSC）アルゴリズムを使用します。

HFSC は、先入れ先出し (FIFO) の順序でクラスを提供します。パケットをスケジューリングする前に、Citrix SD-WAN はパケットクラスの保留中のトラフィック量を調べます。過剰なトラフィックが保留中の場合、パケットはキューに入れられずにドロップされます（テールドロップ）。

TCP がキューイングを引き起こすのはなぜですか?

TCP では、ネットワークがデータを送信できる速度を制御できません。帯域幅を制御するために、TCP は帯域幅ウィンドウの概念を実装しています。これは、ネットワークで許可される未確認トラフィックの量です。最初は小さなウィンドウから始まり、確認応答が受信されるたびに、そのウィンドウのサイズが 2 倍になります。これをスロースタートまたは指数関数的な成長フェーズと呼びます。

TCP は、ドロップされたパケットを検出することによってネットワークの輻輳を識別します。TCP スタックが 250 ms の遅延をもたらすパケットのバーストを送信する場合、TCP はパケットが廃棄されない場合に輻輳を検出しないため、ウィンドウのサイズは増加し続けます。待機時間が 600 ～800 ミリ秒に達するまで、この処理が続けられる場合があります。

TCP がスロースタートモードでない場合、パケット損失が検出されると帯域幅が半分になり、受信確認応答ごとに 1 パケットずつ許可帯域幅が増加します。したがって、TCP は、帯域幅を上向きに圧力をかけることとバッキングオフを交互に行います。残念ながら、パケット損失が検出されるまでに待機時間が 800 ミリ秒に達すると、帯域幅の削減によって伝送遅延が発生します。

QoS の公平性への影響

TCP 伝送遅延が発生すると、仮想パスクラス内で何らかの公平性保証を提供することは困難です。仮想パススケジューラは、大量のトラフィックが保持されないように、テールドロップ動作を適用する必要があります。TCP 接続の性質は、少数のトラフィックが仮想パスを満たすため、新しい TCP 接続で帯域幅の公平なシェアを得ることが困難になるようなものです。帯域幅を公平に共有するには、新しいパケットを送信するために帯域幅が使用可能であることを確認する必要があります。

ランダム早期検出

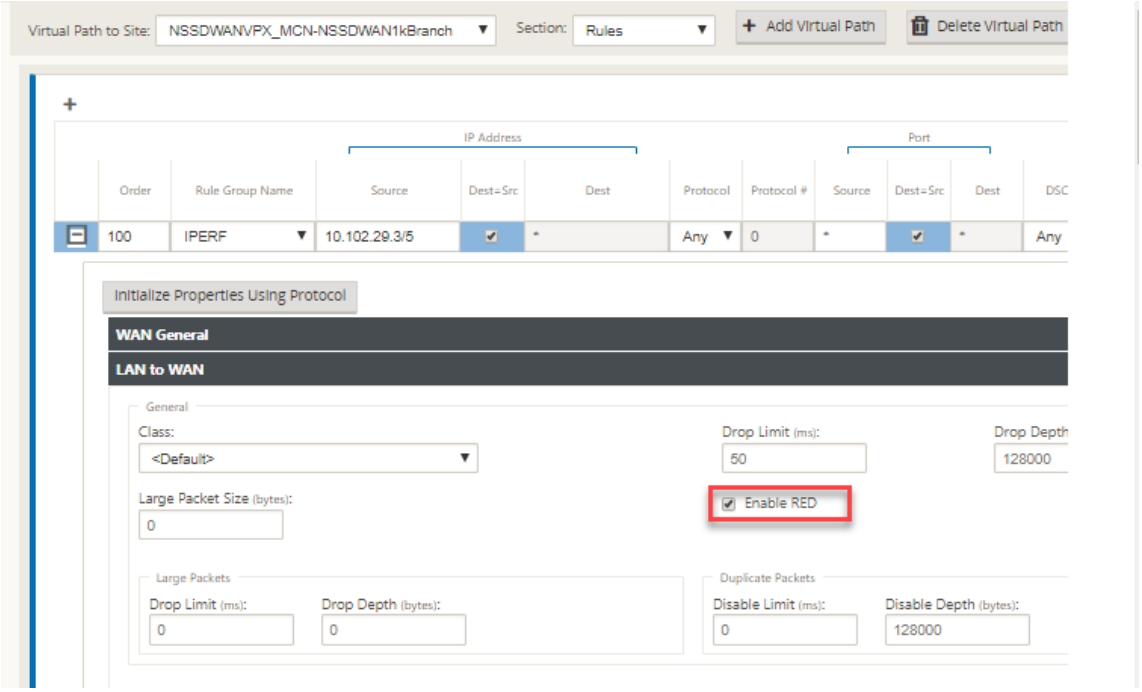
Random Early Detection（RED; ランダム早期検出）は、トラフィックキューがいっぱいになり、テールドロップこれにより、TCP 接続が達成できるスループットに影響を与えずに、仮想パススケジューラによる不必要なキューイングを防止できます。

RED の使い方

1. TCP セッションを開始して、仮想パスを作成します。RED を有効にすると、そのクラスの待機時間が定常状態で約 50 ミリ秒に留まることを確認します。
2. 2 番目の TCP セッションを開始し、両方の TCP セッションで仮想パスの帯域幅が均等に共有されていることを確認します。クラスの待機時間が定常状態のままであることを確認します。
3. 構成エディタを使用して RED を有効または無効にできること、およびパラメータに正しい値が表示されることを確認します。
4. SD-WAN GUI の [設定の表示] ページに、ルールに対して RED が有効になっているかどうかが表示されていることを確認します。

RED を有効にする方法

1. 構成エディタ > 接続 > 仮想パス **>** 仮想パスの **[**選択**]>** ルール > ルールの選択 **(VOIP)** などに移動します。
2. [**LAN** から **WAN** へ] ペインを展開します。[**LAN to WAN**] セクションで、[**RED** を有効にする] チェックボックスをオンにして、TCP ベースのルールに対して有効にします。



MPLS キュー

May 10, 2021

この機能を使用すると、マルチプロトコルレイヤスイッチング（MPLS）WAN リンクを追加するときに SD-WAN 設定を簡単に作成できます。以前は、各 MPLS キューに 1 つの WAN リンクを作成する必要がありました。各 WAN リンクには、WAN リンクを作成するための一意の仮想 IP アドレス (VIP) と、プロバイダのキューイングスキームに対応する一意の Differented Services Code Point (DSCP) タグが必要です。各 MPLS キューに WAN リンクを定義した後、特定のキューにマッピングするイントラネットサービスが定義されます。

現在、新しい MPLS 固有の WAN リンク定義（アクセスタイプ）が使用可能です。新しいプライベート MPLS アクセスタイプを選択すると、WAN リンクに関連付けられた MPLS キューを定義できます。これにより、MPLS WAN リンクに対するプロバイダのキューイング実装に対応する複数の DSCP タグを持つ 1 つの VIP を使用できます。これにより、イントラネットサービスが 1 つの MPLS WAN リンク上の複数の MPLS キューにマッピングされます。

MPLS プロバイダーが DSCP マーキングに基づいてトラフィックを識別できるようにして、プロバイダーがサービスクラスを適用できるようにします。

> 注
>
> 既存の MPLS 構成があり、プライベート MPLS アクセスタイプを実装する場合は、Citrix サポートにお問い合わせください。

プライベート **MPLS WAN** リンクの設定

1. WAN リンクアクセスタイプをプライベート MPLS として定義します。
2. サービスプロバイダー MPLS キューに対応する MPLS キューを定義します。
3. 仮想パスサービスの WAN リンクを有効にします（プライベート MPLS WAN リンクではデフォルトで有効）。
4. WAN リンクの仮想パスから、Autopath グループを割り当てます。

   > 注
   >
   > 自動パスグループが WAN リンクレベルから割り当てられている場合、SD-WAN は、一致する DSCP タグに基づいて MCN キューとクライアント MPLS キューの間にパスを自動的に作成します。自動パスグループが MPLS キューレベルから割り当てられている場合、SD-WAN は DSCP タグが一致しているかどうかにかかわらず、パスを自動的に作成します。

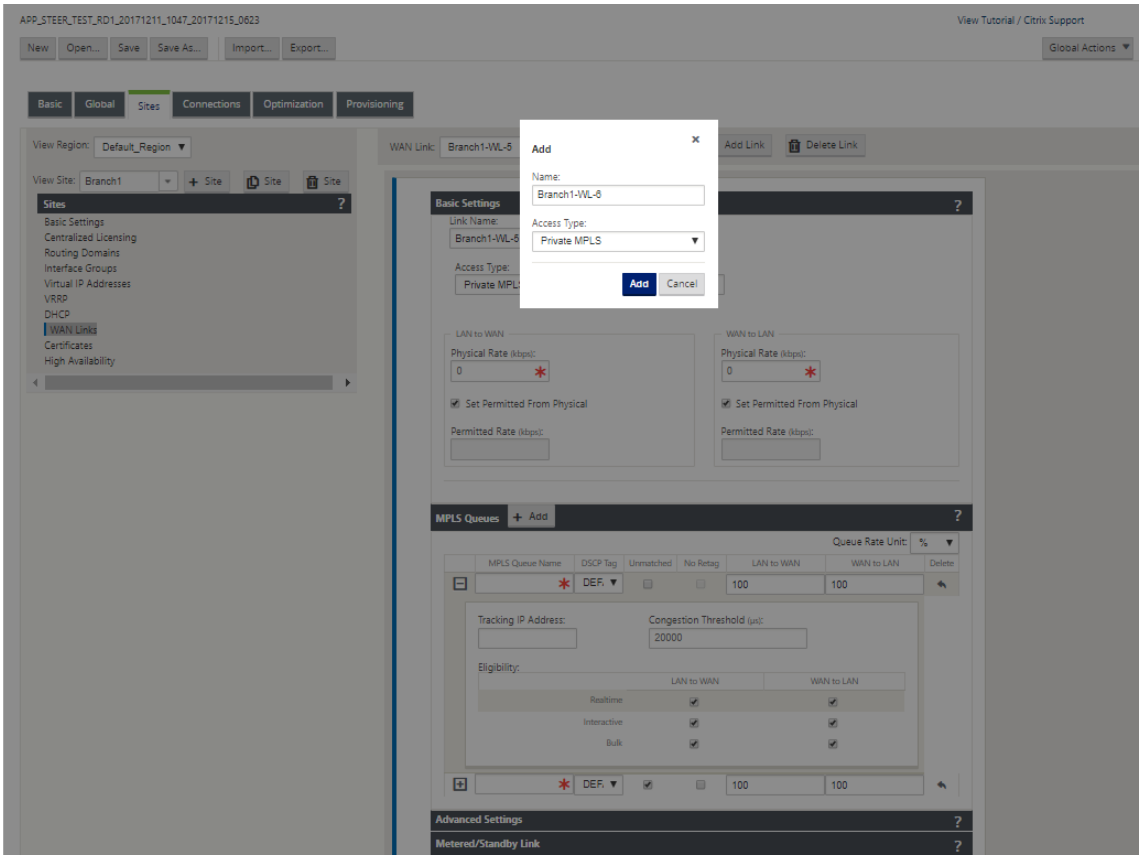
5. MCN とクライアントで同じ Autopath Group が構成されていることを確認します。
6. WAN リンクのパスが自動的に構築されていることを確認します。
7. 必要に応じて、イントラネットサービスを特定のキューに割り当てます。

> 注
>
> SD-WAN 設定では、プロバイダーベースのキューに対して 1 対 1 のマッピングがない場合があります。これは、特定の展開シナリオに基づいています。異なるプライベートアクセスタイプ間で自動パスグループを作成することはできません。たとえば、プライベートインターネットアクセスタイプとプライベート MPLS アクセスタイプの間に自動パスグループを作成することはできません。

プライベート **MPLS WAN** リンクの追加方法

プライベート MPLS 用の新しい WAN リンクアクセスタイプを設定するには、次の手順を実行します。

1. 構成エディタで、[サイト] > [サイト **[**名**]**] > [**WAN** リンク**]** に移動します。[リンクを追加**]** をクリックします。WAN リンク名を入力し、アクセスタイプとして [プライベート **MPLS**] を選択します。



2. [基本設定] の下に、新しい [**MPLS** キュー] タブが追加されました。[+ Add] をクリックして、特定の MPLS キューを追加します。これらは、サービスプロバイダによって定義されたキューに対応している必要があります。

フィールド	説明
MPLS キュー名	MPLS キュー名
DSCP タグ	キューに対するサービスプロバイダの DSCP タグ設定。
一致しません	有効にすると、構成ファイル内の定義されたタグと一致しない着信フレームは、このキューおよびこのキューに定義された帯域幅にマッピングされます。
LAN から WAN への許可レート（kbps）	SD-WAN デバイスがアップロードに使用できる帯域幅の量。これは、WAN リンクの定義された物理アップロードレートを超えることはできません。
WAN から WAN への許可レート（kbps）	SD-WAN デバイスがダウンロードに使用できる帯域幅の量。これは、WAN リンクの定義された物理ダウンロードレートを超えることはできません。

[+] をクリックして [MPLS キュー定義] を展開すると、その他のオプションが表示されます。これらのオプシ

ョンには、次のものがあります。

フィールド	説明
IP アドレスの追跡	WAN リンクトラッキングアドレス
輻輳しきい値	MPLS キューによってパケット送信が抑制され、輻輳が回避されるまでに定義された輻輳時間（マイクロ秒）。輻輳が設定しきい値を超えると、SD-WAN は送信レートをバックオフします。
参加資格	特定のトラフィッククラスを処理する MPLS キューの適格性。特定のトラフィッククラスに対して適格性が無効になっている場合、ネットワーク条件によって要求されない限り、そのトラフィッククラスが MPLS キューを通過することはほとんどありません。

既存のサービスプロバイダー WAN リンクキュー定義に対応する MPLS キューを設定します。

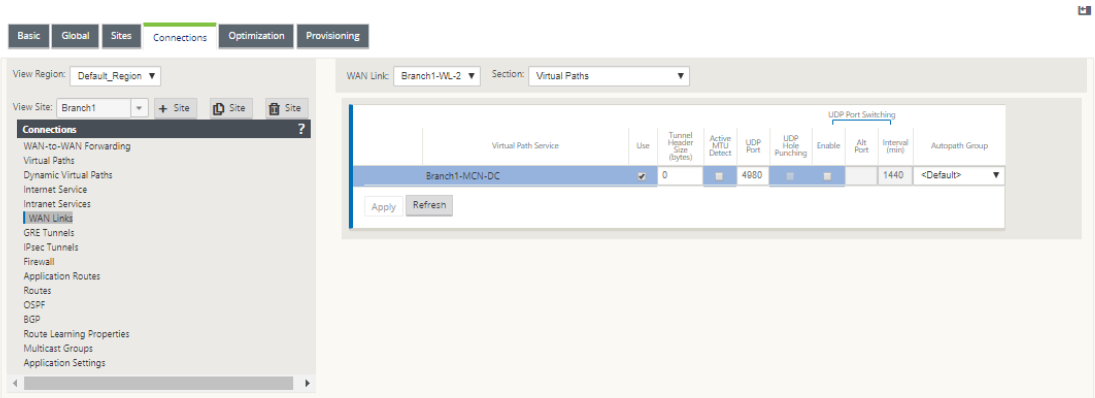
> 注
>
> SD-WAN 9.1 より前に設定された既存の MPLS WAN リンクは影響を受けません。

プライベート **MPLS** の **WAN** リンクプロパティの定義

MPLS キューを持つプライベート MPLS WAN リンクを定義したら、特定の仮想パス定義の下で WAN リンクに自動パスグループを割り当てる必要があります。

autopath グループを割り当てるには、次の手順に従います。

1. **[** 接続**] >[**名**]>[WAN** リンク**]>**[**MPLS WAN** リンク名]> **[**仮想パス**]>**[仮想パス名]>[ローカルサイト]>**[WAN** リンク**]** に移動し **[Edit]** をクリックします。
2. 「**Autopath Group** 」ドロップダウンメニューをクリックし、使用可能なグループから選択します。デフォルトでは、MPLS キューは MPLS WAN リンクに割り当てられた自動パスグループを継承します。選択した Autopath Group を継承するように個々の MPLS キューを設定するか、各 MPLS キューの [Autopath Group] ドロップダウンメニューから代替を選択するかを選択できます。



> 注
>
> ローカルサイトのキューとリモートサイトのキュー間で DSCP タグに基づく 1 対 1 のマッピングがない場合は、MPLS キューを特定の Autopath Group にマッピングする必要があります。MPLS WAN リンクから自動パスグループを継承すると、一致する DSCP タグを持つキュー間のパスが自動的に生成されます。

仮想パス **WAN** リンクへの自動パスグループの割り当て

定義された Autopath Group は、MCN アプライアンスとクライアントアプライアンスで同じです。これにより、システムは自動的にパスを構築できます。MCN サイトでは、仮想パスに関連付けられた WAN リンクを展開することもできます。

WAN リンクの許可レートと輻輳の表示

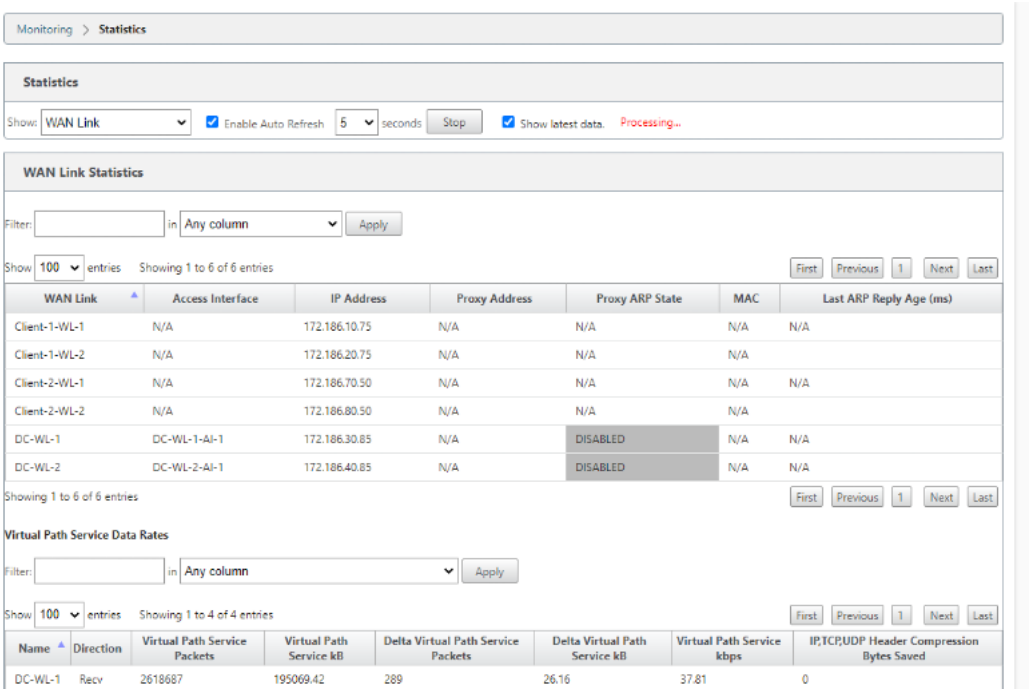
SD-WAN Web インターフェイスでは、WAN リンクおよび WAN リンク使用率の許可レート、および WAN リンク、パス、または仮想パスが輻輳状態であるかどうかを表示できるようになりました。以前のリリースでは、この情報は SD-WAN ログファイルおよび CLI 経由でのみ入手できました。トラブルシューティングに役立つように、Web インターフェイスでこれらのオプションが使用できるようになりました。

許可された料金を表示

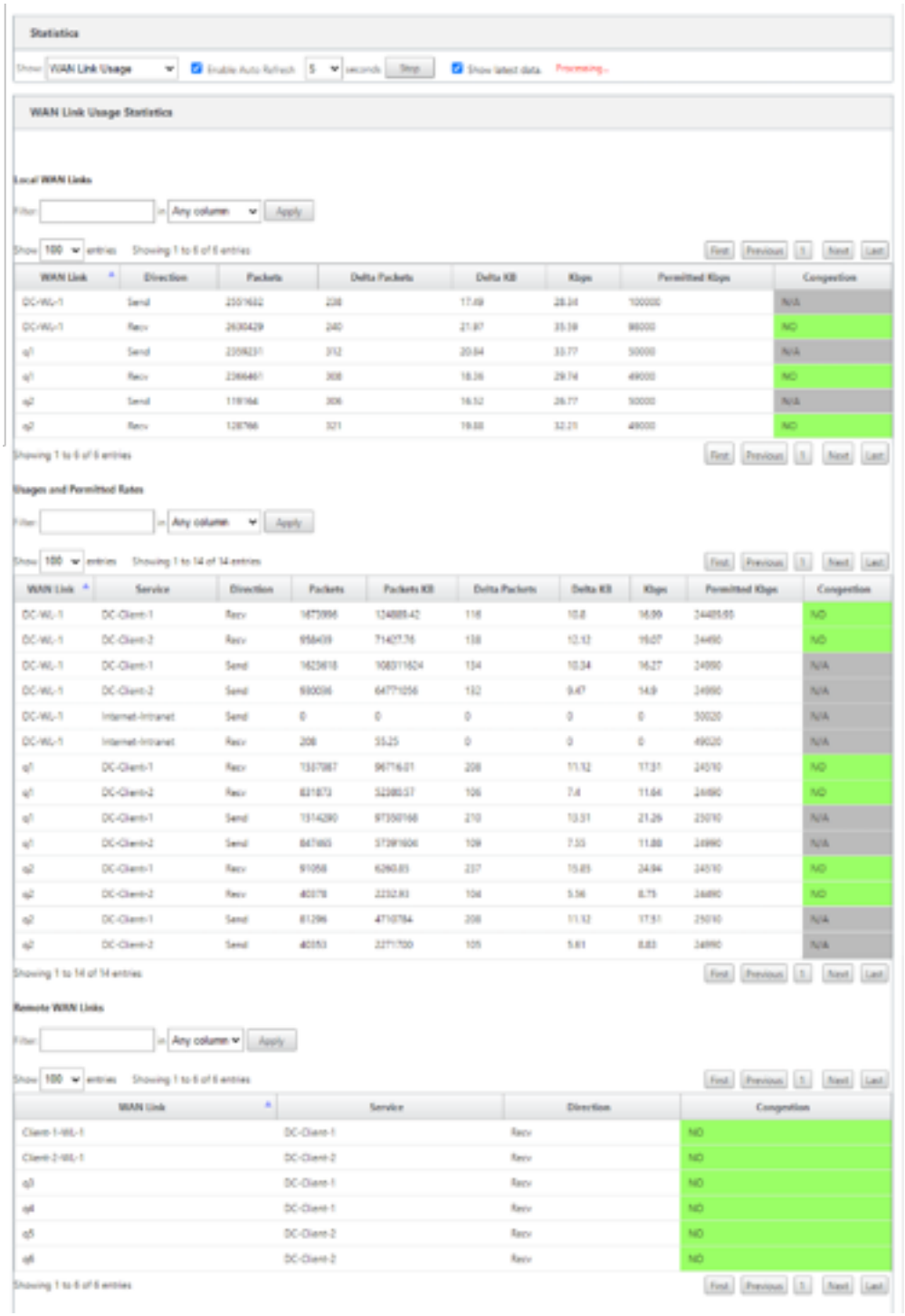
許可レートは、特定の WAN リンク、仮想パスサービス、イントラネットサービス、またはインターネットサービスが、特定の時点で使用できる帯域幅の量です。WAN リンクの許可レートはスタティックで、SD-WAN 設定で明示的に定義されます。仮想パスサービス、イントラネットサービス、またはインターネットサービスの許可率は、輻輳、ユーザーの要求、公正な共有に応じて時間の経過とともに変動しますが、常にサービスの最小予約帯域幅以上になります。

WAN リンクの監視

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

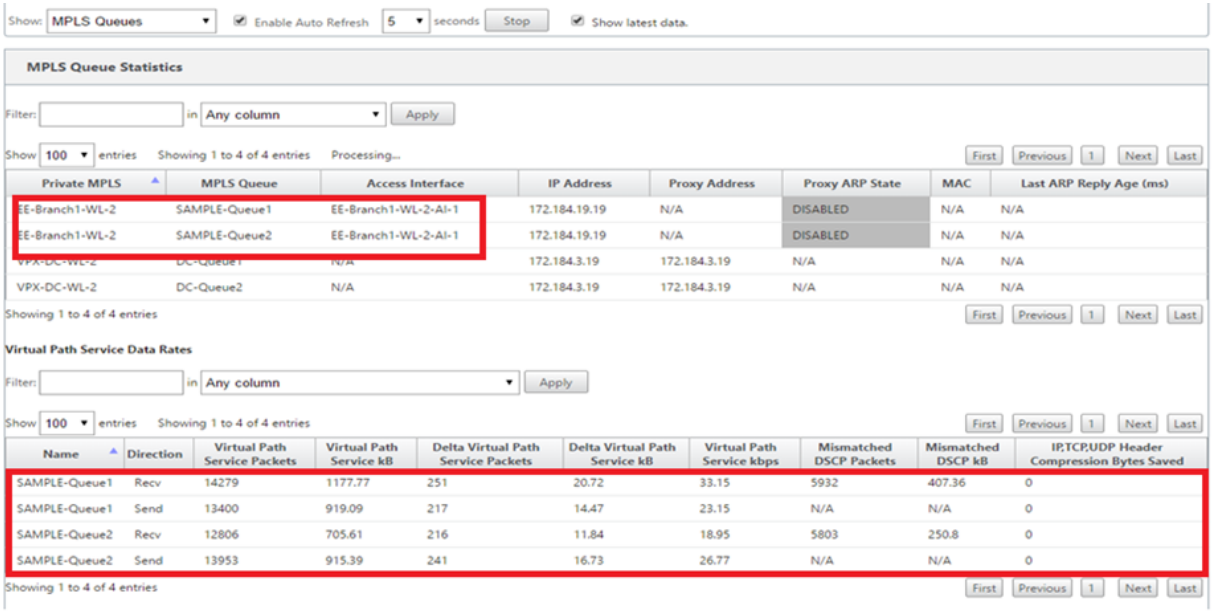


[モニター**] > [**統計] の順に選択し、[表示] ドロップダウンリストから [**WAN** リンクの使用状況] を選択します。



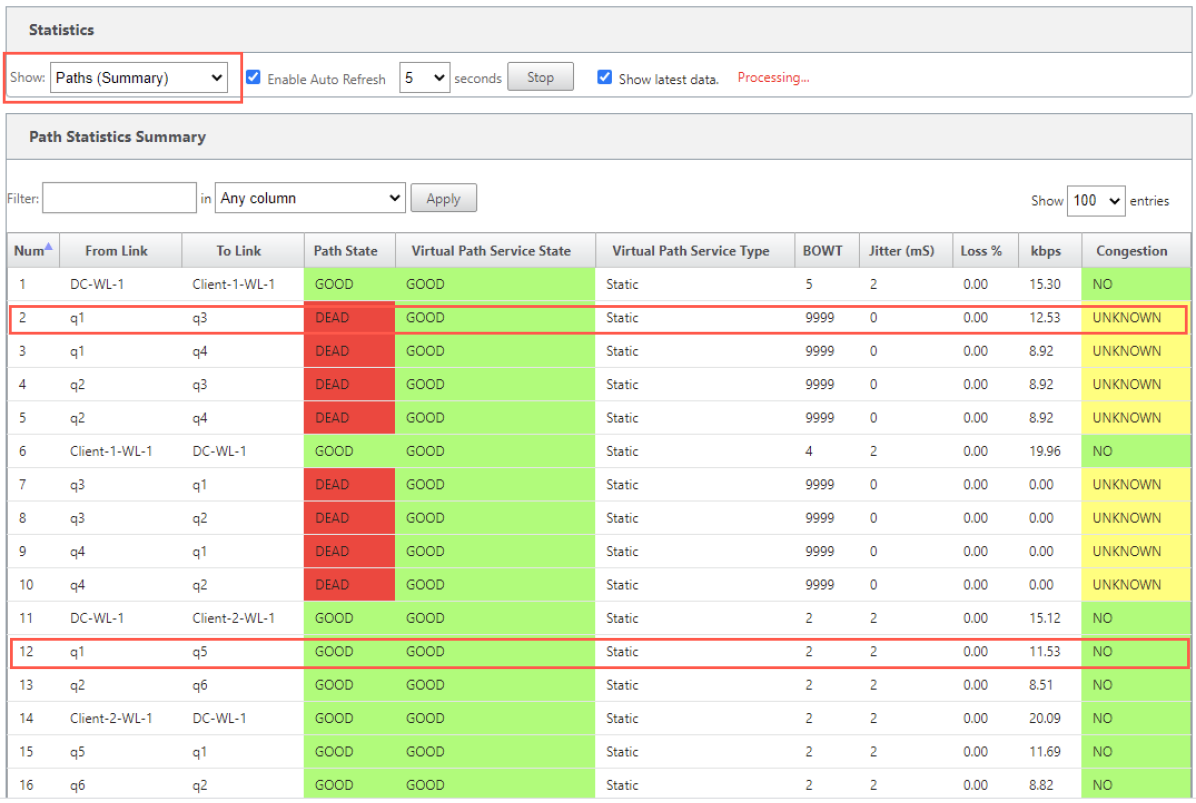
MPLS キューの監視

[モニタ] > [統計] に移動し、[表示] ドロップダウンリストから [**MPLS** キュー] を選択します。



MPLS キューのトラブルシューティング

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

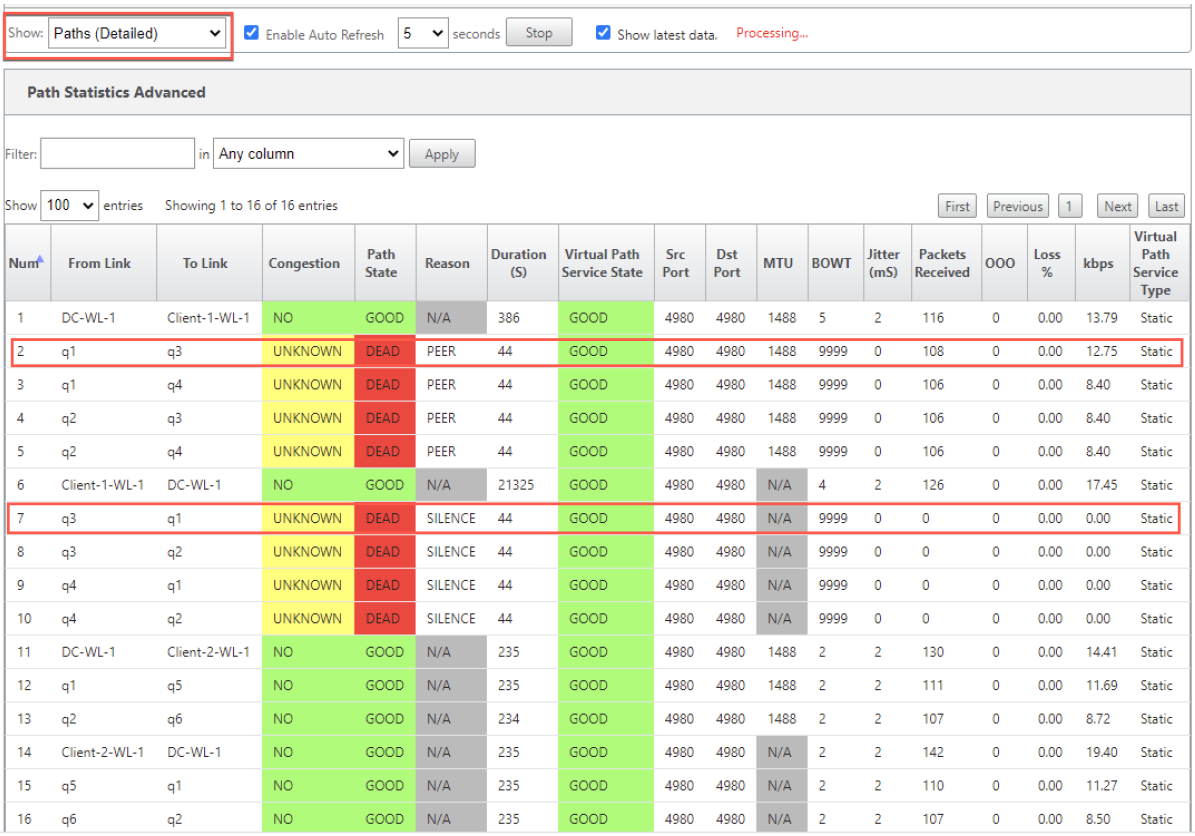


Num	From Link	To Link	Path State	Virtual Path Service State	Virtual Path Service Type	BOWT	Jitter (mS)	Loss %	kbps	Congestion
1	DC-WL-1	Client-1-WL-1	GOOD	GOOD	Static	5	2	0.00	15.30	NO
2	q1	q3	DEAD	GOOD	Static	9999	0	0.00	12.53	UNKNOWN
3	q1	q4	DEAD	GOOD	Static	9999	0	0.00	8.92	UNKNOWN
4	q2	q3	DEAD	GOOD	Static	9999	0	0.00	8.92	UNKNOWN
5	q2	q4	DEAD	GOOD	Static	9999	0	0.00	8.92	UNKNOWN
6	Client-1-WL-1	DC-WL-1	GOOD	GOOD	Static	4	2	0.00	19.96	NO
7	q3	q1	DEAD	GOOD	Static	9999	0	0.00	0.00	UNKNOWN
8	q3	q2	DEAD	GOOD	Static	9999	0	0.00	0.00	UNKNOWN
9	q4	q1	DEAD	GOOD	Static	9999	0	0.00	0.00	UNKNOWN
10	q4	q2	DEAD	GOOD	Static	9999	0	0.00	0.00	UNKNOWN
11	DC-WL-1	Client-2-WL-1	GOOD	GOOD	Static	2	2	0.00	15.12	NO
12	q1	q5	GOOD	GOOD	Static	2	2	0.00	11.53	NO
13	q2	q6	GOOD	GOOD	Static	2	2	0.00	8.51	NO
14	Client-2-WL-1	DC-WL-1	GOOD	GOOD	Static	2	2	0.00	20.09	NO
15	q5	q1	GOOD	GOOD	Static	2	2	0.00	11.69	NO
16	q6	q2	GOOD	GOOD	Static	2	2	0.00	8.82	NO

パスの詳細については、[表示] ドロップダウンリストから [パス **(**詳細**)**] を選択します。状態の理由、継続時間、送信元ポート、宛先ポート、MTU などのパスに関する情報は、

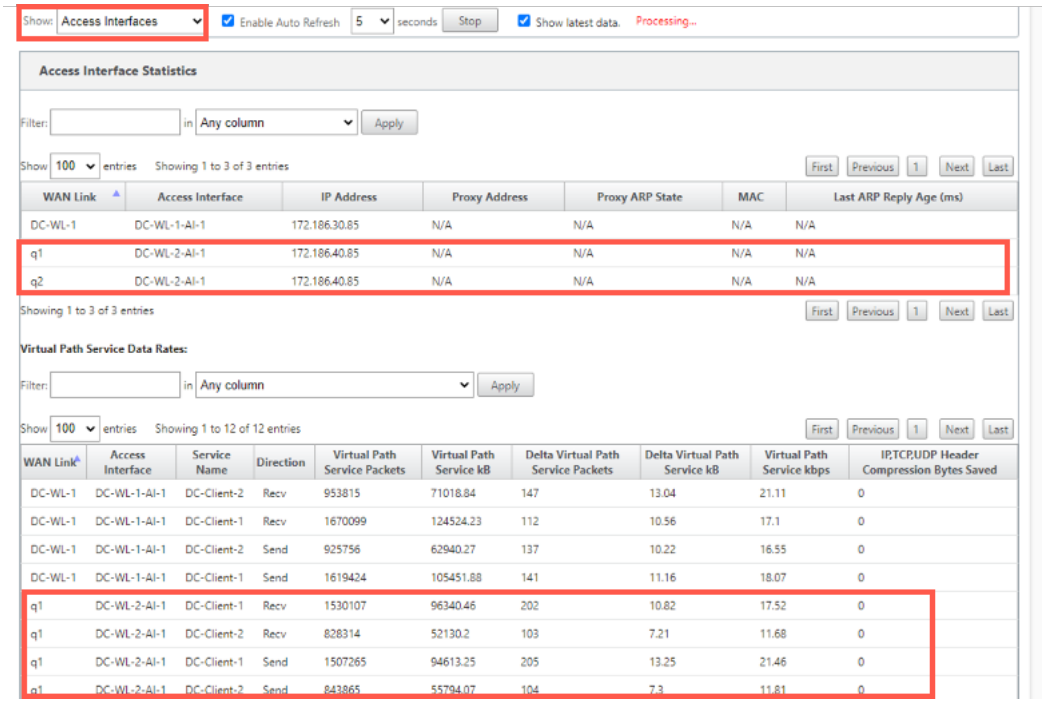
次の例では、MPLS キュー「q1」から「q3」へのパスが DEAD 状態であり、その理由は PEER です。MPLS キュー「q3」から「q1」へのパスは停止しており、その理由は SILENCE です。次の表に、利用可能な理由のリストとその説明を示します。

理由	説明
GATEWAY	アプライアンスがゲートウェイに到達または検出できないため、パスは DEAD です
SILENCE	アプライアンスがピアサイトからパケットを受信していないため、パスは BAD または DEAD です
LOSS	パケット損失のためにパスが不正です
PEER	ピアサイトがパスが不正であると報告している

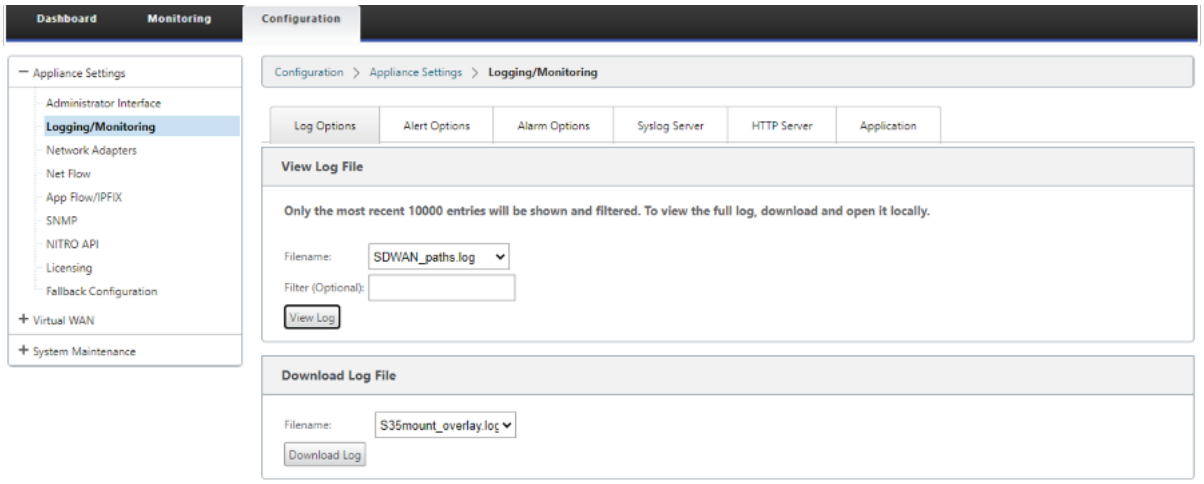


Num	From Link	To Link	Congestion	Path State	Reason	Duration (S)	Virtual Path Service State	Src Port	Dst Port	MTU	BOWT	Jitter (mS)	Packets Received	OOO	Loss %	kbps	Virtual Path Service Type
1	DC-WL-1	Client-1-WL-1	NO	GOOD	N/A	386	GOOD	4980	4980	1488	5	2	116	0	0.00	13.79	Static
2	q1	q3	UNKNOWN	DEAD	PEER	44	GOOD	4980	4980	1488	9999	0	108	0	0.00	12.75	Static
3	q1	q4	UNKNOWN	DEAD	PEER	44	GOOD	4980	4980	1488	9999	0	106	0	0.00	8.40	Static
4	q2	q3	UNKNOWN	DEAD	PEER	44	GOOD	4980	4980	1488	9999	0	106	0	0.00	8.40	Static
5	q2	q4	UNKNOWN	DEAD	PEER	44	GOOD	4980	4980	1488	9999	0	106	0	0.00	8.40	Static
6	Client-1-WL-1	DC-WL-1	NO	GOOD	N/A	21325	GOOD	4980	4980	N/A	4	2	126	0	0.00	17.45	Static
7	q3	q1	UNKNOWN	DEAD	SILENCE	44	GOOD	4980	4980	N/A	9999	0	0	0	0.00	0.00	Static
8	q3	q2	UNKNOWN	DEAD	SILENCE	44	GOOD	4980	4980	N/A	9999	0	0	0	0.00	0.00	Static
9	q4	q1	UNKNOWN	DEAD	SILENCE	44	GOOD	4980	4980	N/A	9999	0	0	0	0.00	0.00	Static
10	q4	q2	UNKNOWN	DEAD	SILENCE	44	GOOD	4980	4980	N/A	9999	0	0	0	0.00	0.00	Static
11	DC-WL-1	Client-2-WL-1	NO	GOOD	N/A	235	GOOD	4980	4980	1488	2	2	130	0	0.00	14.41	Static
12	q1	q5	NO	GOOD	N/A	235	GOOD	4980	4980	1488	2	2	111	0	0.00	11.69	Static
13	q2	q6	NO	GOOD	N/A	234	GOOD	4980	4980	1488	2	2	107	0	0.00	8.72	Static
14	Client-2-WL-1	DC-WL-1	NO	GOOD	N/A	235	GOOD	4980	4980	N/A	2	2	142	0	0.00	19.40	Static
15	q5	q1	NO	GOOD	N/A	235	GOOD	4980	4980	N/A	2	2	110	0	0.00	11.27	Static
16	q6	q2	NO	GOOD	N/A	235	GOOD	4980	4980	N/A	2	2	107	0	0.00	8.50	Static

MPLS キューに関連付けられたアクセスインターフェイスおよび IP アドレスを確認するには、[**Show**] ドロップダウンリストから [**Access Interfaces**] を選択します。



詳細なトラブルシューティングのために、ログファイルをダウンロードできます。[構成**] > [**ログ**/**監視] に移動し、[ログオプション] タブで [**SDWAN_paths.log**] または [**SDWAN_common.log**] を選択します。



レポート

May 10, 2021

アプリケーション QoE

複数のネットフローコレクタ

アプリケーション **QoE**

June 8, 2022

アプリケーション **QoE** とは、SD-WAN ネットワークにおけるアプリケーションの経験の品質を測定する指標です。2 つの SD-WAN アプライアンス間の仮想パスを通過するアプリケーションの品質を測定します。アプリケーション **QoE** スコアは 0 ～10 の値です。該当するスコア範囲によって、アプリケーションの品質が決まります。

品質	範囲
高	8–10
標準	4–8
低	0–4

アプリケーション **QoE** スコアは、アプリケーションの品質を測定し、問題のある傾向を特定するために使用できます。

QoE プロファイルを使用して、リアルタイムおよび対話型アプライアンスの品質しきい値を定義し、これらのプロファイルをアプリケーションまたはアプリケーションオブジェクトにマッピングできます。

> 注:
>
> アプリケーション QoE を監視するには、ディープパケットインスペクションを有効にすることが不可欠です。詳しくは、「アプリケーション分類」を参照してください。

リアルタイムアプリケーション **QoE**

リアルタイムアプリケーションのアプリケーション QoE 計算では、MOS スコアから派生した Citrix の革新的な手法が使用されます。

デフォルトのしきい値は次のとおりです。

- レイテンシしきい値：160
- ジッタしきい値：30 ミリ秒
- パケット損失しきい値:2%

遅延、損失、およびジッタに関するしきい値を満たすリアルタイムアプリケーションのフローは、品質が良いと見なされます。

リアルタイムアプリケーションの QoE は、しきい値を満たすフローの割合をフローサンプルの合計数で割った値から決定されます。

リアルタイムの QoE =（しきい値を満たすフローサンプル数/フローサンプルの合計数）* 100

これは、0 から 10 の範囲の QoE スコアとして表されます。

カスタムしきい値を使用して QoE プロファイルを作成し、アプリケーションまたはアプリケーションオブジェクトに適用できます。

> 注:
>
> ネットワーク条件がリアルタイムトラフィックに設定されたしきい値を超えている場合、QoE 値はゼロになります。

対話型アプリケーション **QoE**

対話型アプリケーションのアプリケーション QoE では、パケット損失とバーストレートのしきい値に基づいて Citrix の革新的な技術を使用しています。

対話型アプリケーションは、パケット損失とスループットに影響されます。したがって、フロー内のパケット損失率、および入出力トラフィックのバーストレートを測定します。

設定可能なしきい値は、次のとおりです。

- パケット損失率。
- 入力バーストレートと比較して、予想される出力バーストレートのパーセンテージ。

デフォルトのしきい値は次のとおりです。

- パケット損失しきい値:1%
- バーストレート:60%

次の条件が満たされている場合、フローの品質は良好です。

- フローの損失の割合は、設定されたしきい値より小さくなります。
- 出力バーストレートは、少なくとも入力バーストレートに設定されたパーセンテージです。

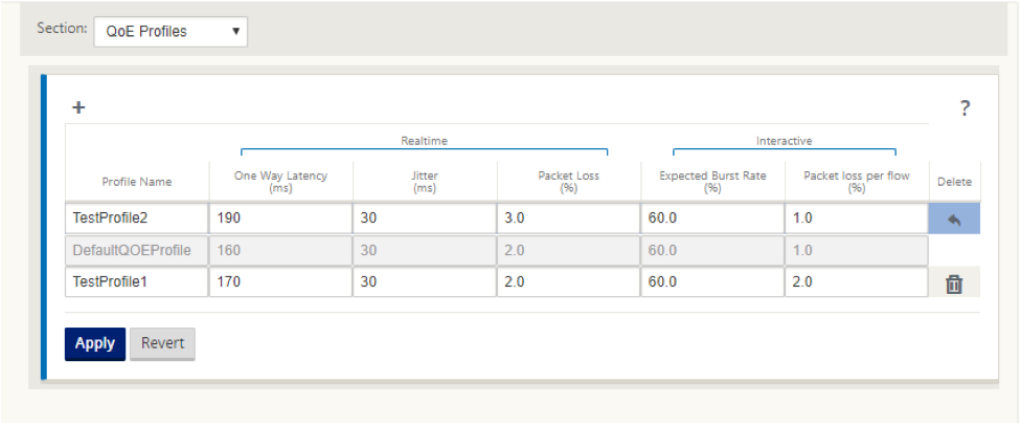
アプリケーション **QoE** の設定

アプリケーションまたはアプリケーションオブジェクトをデフォルトまたはカスタム QoE プロファイルにマッピングします。
リアルタイムおよび対話型トラフィック用のカスタム QoE プロファイルを作成できます。

カスタム QoE プロファイルを作成するには、次の手順を実行します。

1. 構成エディタで、[グローバル**] > [**アプリケーション **QoE] > [QoE** プロファイル] に移動し、[**+**] をクリックします。
2. 次のパラメータの値を入力します。

- **Profile Name**: リアルタイムトラフィックおよびインタラクティブトラフィックのしきい値を設定するプロファイルを識別する名前。
- **Real-Time**: リアルタイム QoS ポリシーにヒットするトラフィックフローのしきい値を設定します。遅延、損失、およびジッタに関するしきい値を満たすリアルタイムアプリケーションのフローは、品質が良いと見なされます。
  - 片道レイテンシ: レイテンシのしきい値 (ミリ秒単位)。デフォルトの QoE プロファイル値は 160 ミリ秒です。
  - ジッタ: ジッタしきい値（ミリ秒単位)。デフォルトの QoE プロファイル値は 30 ミリ秒です。
  - パケット損失: パケット損失の割合。デフォルトの QoE プロファイル値は 2% です。
- **Interactive**: 対話型 QoS ポリシーにヒットするトラフィックフローのしきい値を設定します。バースト率とパケット損失のしきい値を下回っていることを満たすインタラクティブアプリケーションのフローは、品質が良いと見なされます。
  - 予想バーストレート: 予想バーストレートのパーセンテージ。出力バーストレートは、入力バーストレートの設定済みパーセンテージ以上でなければなりません。デフォルトの QoE プロファイル値は 60% です。
  - フローあたりのパケット損失率: パケット損失の割合。デフォルトの QoE プロファイル値は 1% です。

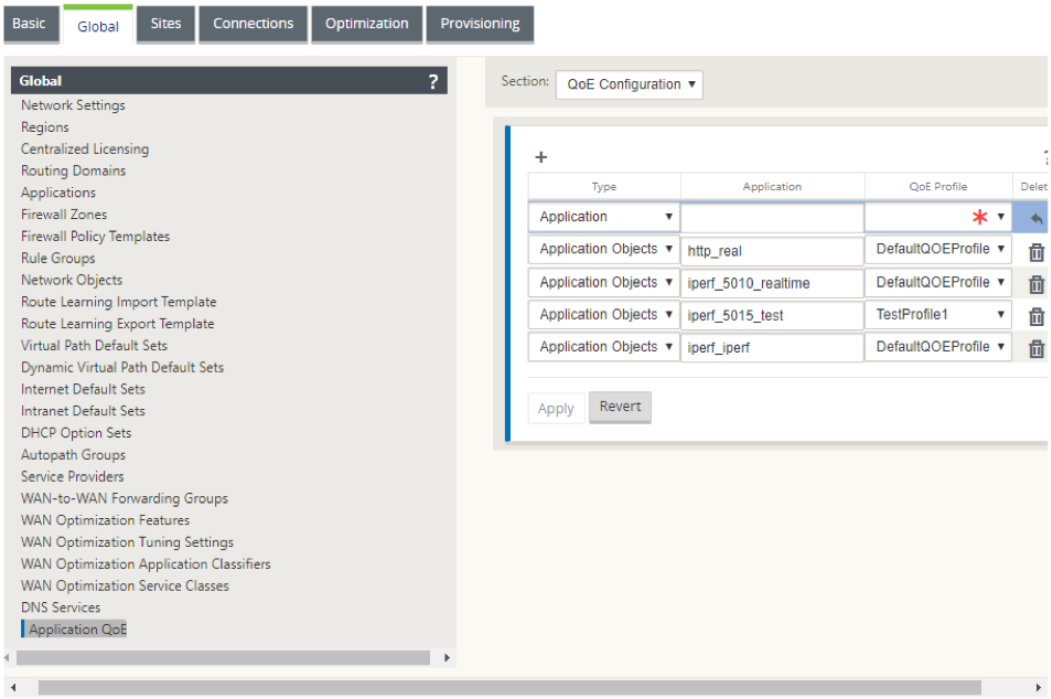


3. ［適用］をクリックします。

QoE プロファイルを使用してアプリケーションまたはアプリケーション・オブジェクトをマップするには、次の手順に従います。

1. 構成エディタで、[グローバル**] > [**アプリケーション **QoE] > [QoE** 設定] に移動し、[**+**] をクリックします。
2. 次のパラメータの値を選択します。
   - 型: DPI アプリケーションまたはアプリケーションオブジェクト。
   - **Application**: 選択したタイプに基づいて、アプリケーションまたはアプリケーション・オブジェクトを検索して選択します。

- **QoE** プロファイル：アプリケーションまたはアプリケーション・オブジェクトにマッピングする QoE プロファイルを選択します。



3. ［適用］をクリックします。

QoE プロファイルを使用して、最大 10 個のアプリケーションまたはアプリケーションオブジェクトをマッピングできます。SD-WAN Center でアプリケーション QoE レポートを表示できます。詳細については、アプリケーション QOE レポートレポートを参照してください。

HDX QoE

May 10, 2021

レイテンシー、ジッタ、パケットドロップなどのネットワークパラメーターは、HDX ユーザーのユーザーエクスペリエンスに影響します。経験の品質（QoE）は、ユーザーが ICA の経験の質を理解し、確認するのに役立つように導入されています。QoE は計算されたインデックスで、ICA トラフィックのパフォーマンスを示します。ユーザーは、QoE を向上させるために、ルールとポリシーを調整できます。

QoE は 0 ～100 の数値で、値が大きいほどユーザーエクスペリエンスが向上します。QoE は、すべての ICA/HDX アプリケーションでデフォルトで有効になっています。

QoE の計算に使用されるパラメータは、クライアントとサーバー側にある 2 つの SD-WAN アプライアンス間で測定され、クライアントまたはサーバーアプライアンス自体の間で測定されません。遅延、ジッタ、およびパケットドロップはフローレベルで測定され、リンクレベルの統計情報とは異なる場合があります。エンドホスト（クライアント

またはサーバ）アプリケーションは、WAN でパケット損失があることを認識しません。再送信が成功すると、フローレベルのパケット損失レートはリンクレベルの損失よりも低くなります。ただし、その結果、レイテンシーとジッタが少し増加する可能性があります。

HDX トラフィックのデフォルト設定では、SD-WAN でパケットを再送信できるため、ネットワーク内のパケット損失により失われた QoE インデックス値が向上します。

SD-WAN Center ダッシュボードでは、HDX アプリケーションの全体的な品質をグラフィカルに表示できます。HDX アプリケーションは、次の 3 つの品質カテゴリに分類されます。

品質	QoE 範囲
高	80–100
標準	50–80
低	0–50

QoE が最も低い下位 5 つのサイトのリストも、Citrix SD-WAN Center ダッシュボードに表示されます。

異なる時間間隔での QoE のグラフィック表示により、各サイトで HDX アプリケーションのパフォーマンスを監視できます。

詳しくは、「SD-WAN Center ダッシュボード」を参照してください。

また、Citrix SD-WAN Center で各サイトの詳細な HDX レポートを表示することもできます。詳しくは、「HDX レポート」を参照してください。

> 注
>
> - *WAN* リンク遅延、ジッタ、およびパケットドロップが常にアプリケーションの遅延、ジッタ、およびパケットドロップと一致することを想定しないでください。*WAN* リンク損失は実際の *WAN* パケット損失と相関しますが、アプリケーションの損失は再送信後に発生し、*WAN* リンク損失よりも低くなります。
> - *GUI* に表示される *WAN* リンクの待ち時間は、*BOWT*（ベストワンウェイタイム）です。これは、リンクの健全性を測定する手段として、リンクの最適なメトリックです。アプリケーション *QoE* は、そのアプリケーションのすべてのパケットの合計および平均遅延を追跡し、計算します。これは、多くの場合、リンク *BOWT* と一致しません。
> - *MSI* セッションが開始されると、*ICA* ハンドシェイク中に、セッションが一時的に *1* つの *MSI* ではなく *4* つの *SSI* としてカウントされることがあります。ハンドシェイクが完了すると、*1 MSI* に収束します。*SQL* テーブルが更新される前に変換が行われると、その分の *ICA_Summary* に表示されます。
> - セッションの再接続では、初期プロトコル情報が交換されないため、*SD-WAN* は *MSI* を識別できないため、各接続は *SSI* 情報としてカウントされます。
> - *UDP* 接続の場合、接続が閉じられた後、*ICA_Summary* で接続が閉じられ、更新されるまでに最大 *5* 分かかる場合があります。*TCP* 接続の場合、接続が閉じられた後、*ICA_Summary* で閉じていると表示されるまでに最大 *2* 分かかることがあります。

> - *TCP セッションと UDP セッションの QoE は、TCP と UDP の間で本質的に異なるため、同じパス上で同じではない場合があります。*
> - *1 人のユーザーが 2 つの仮想デスクトップを起動すると、ユーザー数が 2 つと打ち消されます。*

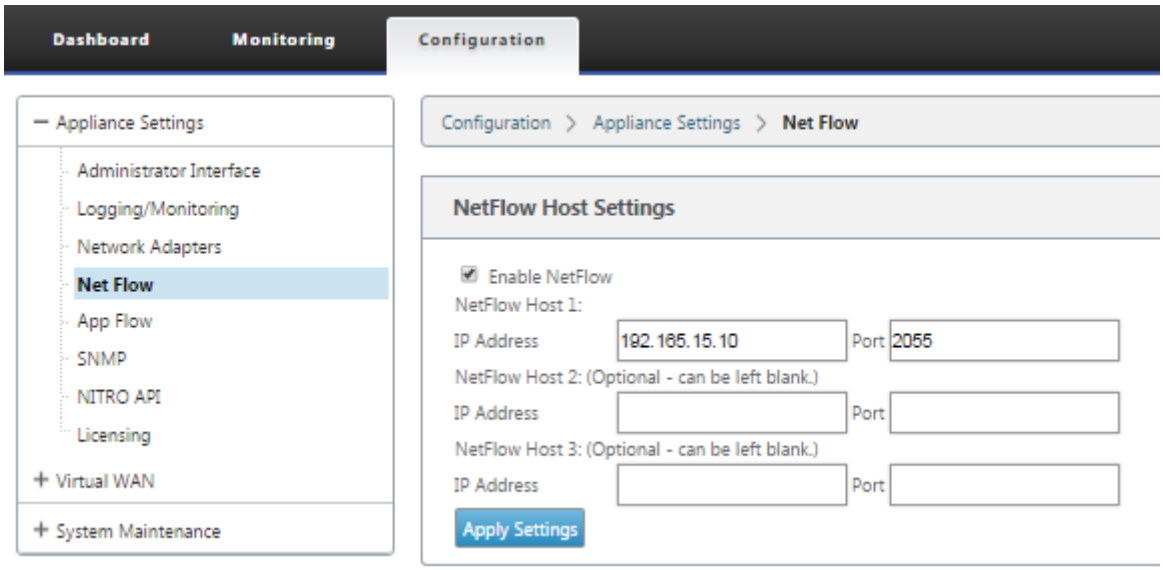
複数のネットフローコレクタ

November 8, 2021

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

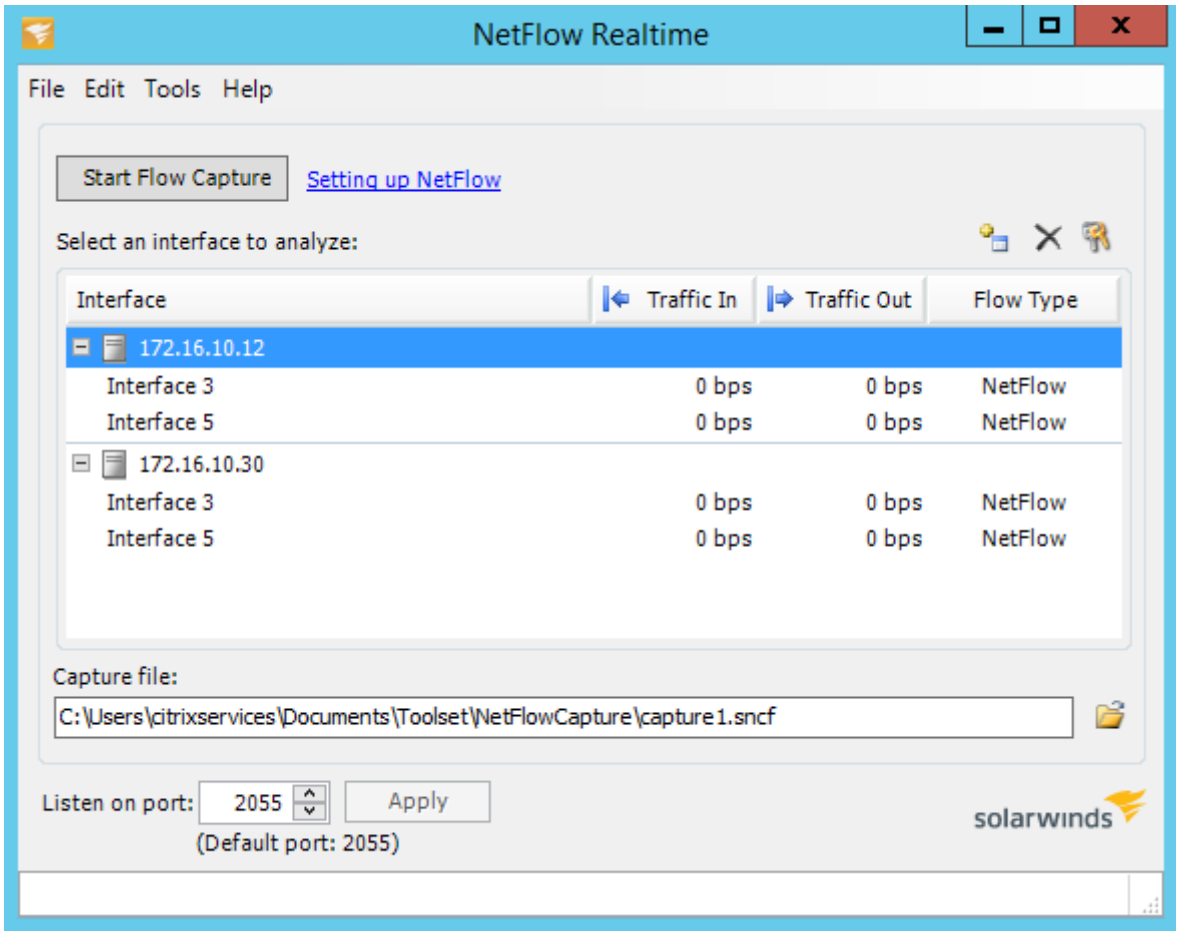
Net Flow ホストを設定するには、次の手順を実行します。

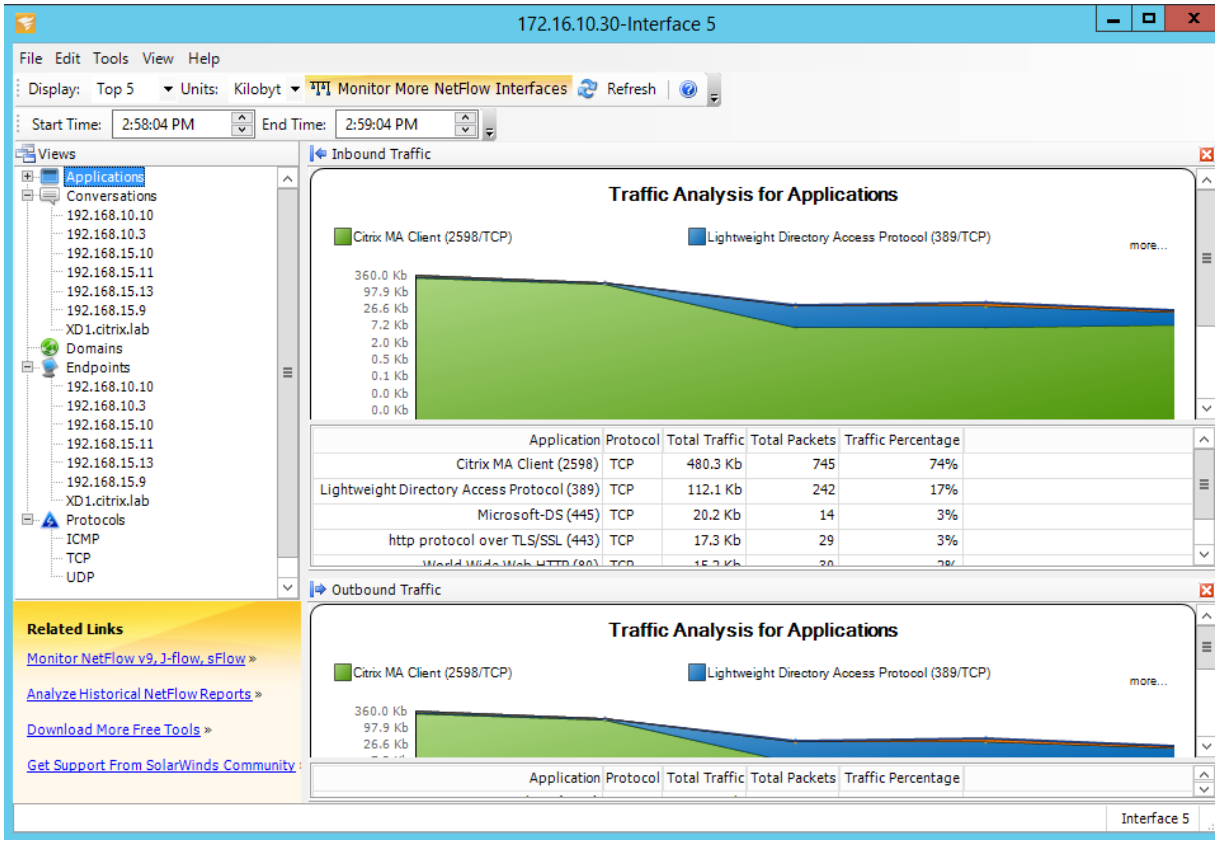
[構成] **>** [アプライアンス設定] **>** [ネットフロー] ****[**Netflow** ホスト設定] ページに移動します。[**NetFlow** を有効にする（Enable NetFlow）] チェックボックスをクリックし、最大 3 つのネットフローホストの **IP** アドレスとポート番号を入力し ****** 、[設定の適用（****Apply Settings** ）] をクリックして変更を保存します。



NetFlow エクスポート

Net Flow データは SD-WAN デバイスの管理ポートからエクスポートされます。SNMP が設定されていない場合、Net Flow コレクタツールでは、SD-WAN デバイスが設定された管理 IP アドレスとしてリストされます。インターフェイスは、着信用 1 つ、発信用 2 つ（仮想パストラフィック）としてリストされます。





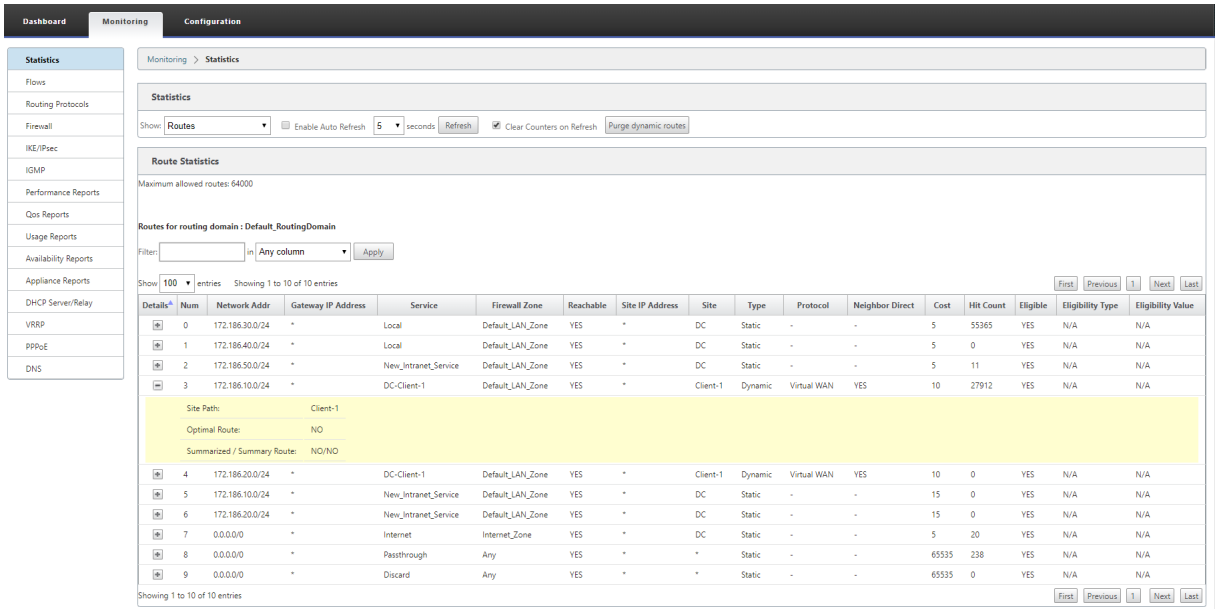
NetFlow の制限事項

- SD-WAN Standard Edition および Premium （Enterprise）Edition アプライアンスで Netflow を有効にすると、仮想パスデータは指定された Netflow コレクタにストリーミングされます。この制限の 1 つは、SD-WAN で使用されている物理 WAN リンクを区別できないことです。ソリューションでは、集約された仮想パス情報（仮想パスは複数の個別の WAN パスで構成されている場合があります）がレポートされるため、個別の WAN パスの Netflow レコードをフィルタリングする方法はありません。
- TCP 制御ビットは N/A として報告されます。これは、SD-WAN が、TCPControlBits（IANA ）の要素 ID 6 を持つ RFC 7011に基づく Netflow エクスポートのインターネット標準に従っていないことを示します。TCP フラグがないと、フローデータのラウンドトリップ時間（RTT）、遅延、ジッタ、およびその他のパフォーマンスメトリックを計算できません。セキュリティ側から、TCP フラグがないと、ネットフローコレクタは、FIN、ACK/RST、または SYN スキャンが発生しているかどうかを判別できません。

ルート統計情報

May 10, 2021

SD-WAN アプライアンスのルート統計情報を表示するには、SD-WAN GUI で [モニタリング] > [統計] > [ルート] に移動します。



次のパラメータを表示できます。

- ネットワークアドレス: ルートのネットワークアドレスとサブネットマスク。
- 詳細: [+] をクリックすると、次の情報が表示されます。
  - サイトパス: サイトパスは、受信したプレフィックスの真実のメトリックのソースです。これは、WAN から WAN への転送が複数のデバイスおよびメッシュ展開で有効になっている状況で使用されます。このようなプレフィクスが複数受信され、管理者はサイトパスを表示することでプレフィクスの属性を判断できます。

    たとえば、Geo MCN とともに Branch1、Branch2、および MCN の単純なトポロジを考えます。Branch1 にはプレフィックス 172.16.1.0/24 があり、Branch2 に到達する必要があります。Geo MCN および MCN では、WAN から WAN への転送が有効になっています。

    接頭辞 172.16.1.0/24 は、Branch1-MCN-Branch2、Branch1-Geo-Branch2、Branch1-MCN-Geo-Branch2 を経由して Branch2 に到達できる。これらの個別のプレフィクスごとに、ルーティングテーブルがサイトパスメトリックで更新されます。サイトパスメトリックは、ルートプレフィクスの起点と、Branch2 に到達するためのコストを示します。
  - **Optimal R**oute: Optimal Route は、ルートが他のすべてのルートと比較してそのサブネットに到達するのに最適なルートであるかどうかを示します。この最適ルートは、他のサイトにエクスポートされます。
  - **Summarized/Su**mmary Route：サマリールートは、スーパーネットに含まれる複数のプレフィクスを要約するために、管理者が明示的に設定したルートです。集約ルートは、集約ルートに含まれるプレフィクスです。

たとえば、サマリールート 172.16.0.0/16 があるとします。これはサマリールートだけであり、サマリールートではありません。サマリールートには、サマリー ‘YES’ とサマリー ‘NO’ があります。172.16.1.0/24、172.16.2.0/24、172.16.3.0/24 のような他のサブネットが少ない場合、これらの 3 つのルートはサマリールートまたはスーパーネットに該当するため、サマリールートと呼ばれます。集約されたルートには、集約された「YES」と集約された「NO」があります。

- **Gateway IP** アドレス: このルートに到達するために使用されるゲートウェイ/ルートの IP アドレス。
- サービス：Citrix SD-WAN サービスのタイプ。
- ファイアウォールゾーン：ルートによって使用されるファイアウォールゾーン。
- 到達可能: ルートが到達可能かどうか。
- サイト **IP** アドレス: サイトの IP アドレス。
- サイト: サイトの名前。
- タイプ: ルートのタイプは、ルート学習のソースによって異なります。LAN 側のルートと、設定時に手動で入力したルートは、スタティックルートです。SD-WAN またはダイナミックルーティングピアから学習されたルートは、ダイナミックルートです。
- プロトコル：プレフィクスのプロトコル。
  - ローカル：アプライアンスのローカル仮想 IP。
  - 仮想 **WAN**：ピア SD-WAN アプライアンスから学習されたプレフィクス。
  - **OSPF**：OSPF ダイナミックルーティングピアから学習されたプレフィクス。
  - **BGP**：**BGP** ダイナミックルーティングピアから学習されたプレフィクス。
- **Neighbor Direct**：サブネットが、ルートがアプライアンスに到達したブランチに接続されているかどうかを示します。
- コスト：宛先ネットワークへの最適なパスを決定するために使用されるコスト。
- ヒット数：そのサブネットにパケットを転送するためにルートがヒットした回数。
- 適格：ルートが適格であることを示します。トラフィック処理中にヒットしたプレフィクスへのパケットの転送またはルーティングに使用されます。
- 適格タイプ: 次の 2 つの適格タイプを使用できます。
  - **Gateway** の適格：ゲートウェイが到達可能かどうかを判断します。
  - パスの適格性：パスが DEAD か否かを決定します。
- 適格値: ルートがシステムに作成されているときに、Gateway または構成内のパスに対して選択された値。たとえば、パス MCN-WL-1->BR1-WL-2 に基づいてルートを適格に呼び出すことができます。したがって、ルートセクションのこのルートの適格性値は MCN-WL-1->BR1-WL-2 の値です。

ルーティング

May 10, 2021

動的ルーティング

Citrix SD-WAN では、ダイナミックルーティング機能の下に、既知のルーティングプロトコルのサポートが導入されます。この機能により、LAN サブネットの検出が容易になり、仮想パスルートが BGP および OSPF プロトコルを使用してネットワーク内でよりシームレスに動作するようにアドバタイズされます。これにより、スタティックルート設定や正常なルータフェールオーバーを必要とせずに、SD-WAN を既存の環境にシームレスに展開できます。

ルートフィルタリング

ルート学習が有効なネットワークの場合、Citrix SD-WAN により、ルーティングネイバーにアドバタイズされる SD-WAN ルートと、ルーティングネイバーから受信されるルートをより詳細に制御できます。

- エクスポートフィルタは、特定の一致基準に基づいて OSPF および BGP プロトコルを使用してアドバタイズメント用のルートを含めるか除外するために使用されます。
- インポートフィルタは、特定の一致基準に基づいて OSPF および BGP ネイバーを使用して受信したルートを受け入れるか、受け付けないかに使用します。

ルートフィルタリングは、SD-WAN ネットワーク（データセンター/ブランチ）の LAN ルートおよび仮想パスルートに実装され、BGP と OSPF を使用して SD-WAN 以外のネットワークにアドバタイズされます。

ルート集約

ルート集約により、ルータが維持する必要のあるルートの数が減少します。サマリールートは、複数のルートを表すために使用される 1 つのルートです。1 つのルートアドバタイズメントを送信することで帯域幅を節約し、ルータ間のリンク数を削減します。1 つのルートアドレスだけが維持されるため、メモリを節約できます。CPU リソースは、再帰的なルックアップを避けることによって、より効率的に使用されます。

VRRP

Virtual Router Redundancy Protocol（VRRP）仮想ルータ冗長プロトコル）は、デバイスの冗長性を提供し、スタティックデフォルトルーティング環境に固有の単一障害点を排除する、広く使用されているプロトコルです VRRP を使用すると、1 つのグループを形成するように 2 つ以上のルータを設定できます。このグループは、1 つの仮想 IP アドレスと 1 つの仮想 MAC アドレスを持つ単一のデフォルト Gateway として表示されます。

Citrix SD-WAN（リリースバージョン 10.0 以降）は、VRRP バージョン 2 およびバージョン 3 をサポートし、サードパーティのルーターとの相互動作をサポートします。SD-WAN アプライアンスはマスタールータとして機能し、サイト間で仮想パスサービスを使用するようにトラフィックを誘導します。仮想インターフェイス IP を VRRP IP として設定し、手動でプライオリティをピアルータよりも高い値に設定することで、SD-WAN アプライアンスを VRRP マスターとして設定できます。アドバタイズメント間隔と preempt オプションを設定できます。

CLI を使用したルーティング機能へのアクセス

ダイナミックルーティングおよびプロトコルステータスに関連する追加情報を表示できます。次のコマンドと構文を入力して、ルーティングデーモンにアクセスし、コマンドのリストを表示します。

‘

dynamic_routing?

‘

SD-WAN オーバーレイルーティング

May 10, 2021

Citrix SD-WAN は、リモートサイト、データセンター、クラウドネットワーク間の耐障害性と堅牢な接続を提供します。SD-WAN ソリューションでは、ネットワーク内の SD-WAN アプライアンス間にトンネルを確立することで、既存のアンダーレイネットワークにオーバーレイするルートテーブルを適用することで、サイト間の接続が可能になります。SD-WAN ルートテーブルは、既存のルーティングインフラストラクチャと完全に置き換えたり、共存したりできます。

Citrix SD-WAN アプライアンスは、可用性、損失、遅延、ジッタ、輻輳特性の観点から単方向で利用可能なパスを測定し、パケットごとに最適なパスを選択します。つまり、サイト A からサイト B まで選択したパスは、必ずしもサイト B からサイト A まで選択したパスである必要はありません。特定の時間における最適なパスは、各方向で個別に選択されます。Citrix SD-WAN では、パケットベースのパス選択により、ネットワークの変更に迅速に対応できます。SD-WAN アプライアンスは、2 つまたは 3 つのパケットが欠落した後でパスの停止を検出できるため、アプリケーショントラフィックを次善の WAN パスにシームレスにフェールオーバーできます。SD-WAN アプライアンスは、すべての WAN リンクステータスを約 50 ミリ秒で再計算します。次の記事では、Citrix SD-WAN ネットワーク内の詳細なルーティング構成について説明します。

Citrix SD-WAN ルートテーブル

SD-WAN 設定では、特定のサイトのスタティックルートエントリと、サポートされているルーティングプロトコル（OSPF、eBGP、iBGP など）を介してアンダーレイネットワークから学習されたルートエントリが許可されます。ルートは、ネクストホップだけでなく、サービスタイプによって定義されます。これにより、ルートの転送方法が決まります。以下は、使用中の主なサービスの種類です。

- ローカルサービス： SD-WAN アプライアンスにローカルなルートまたはサブネットを示します。これには、仮想インターフェイスサブネット（ローカルルートを自動的に作成）、およびルートテーブルに定義されたローカルルート（ローカルネクストホップを使用）が含まれます。ルートは、このローカルサイトへの仮想パスを持つ他の SD-WAN アプライアンスにアドバタイズされます。このルートは、パートナーとして信頼されている場合に構成されます。

> 注
>
> デフォルトルートとサマリールートをローカルルートとして追加する場合は、注意が必要です。これらのルートは、他のサイトで仮想パスルートになることがあります。常にルートテーブルをチェックして、正しいルーティングが有効であることを確認します。

- **[Virtual Path]**： リモート SD-WAN サイトから学習されたローカルルートを示します。これは、仮想パスから到達可能なものです。これらのルートは通常自動ですが、仮想パスルートはサイトで手動で追加できます。このルートのトラフィックはすべて、この宛先ルート（サブネット）に対して定義された仮想パスに転送されます。
- イントラネット：プライベート WAN リンク（MPLS、P2P、VPN など）を介して到達可能なルートを示します。たとえば、MPLS ネットワーク上にあり、SD-WAN アプライアンスを持たないリモートブランチなどです。これらのルートは、特定の WAN ルータに転送する必要があることを前提としています。イントラネットサービスは既定では有効になっていません。このルート（サブネット）に一致するトラフィックは、SD-WAN ソリューションを持たないサイトに配信するために、このアプライアンスのイントラネットとして分類されます。

> 注
>
> イントラネットルートを追加する場合、ネクストホップはなく、イントラネットサービスへの転送があります。サービスは、指定された WAN リンクに関連付けられています。

- インターネット—イントラネットに似ていますが、プライベート WAN リンクではなくパブリックインターネット WAN リンクに流れるトラフィックを定義するために使用されます。1 つのユニークな違いは、インターネットサービスを複数の WAN リンクに関連付けて、負荷分散（フローごと）に設定するか、アクティブ/バックアップに設定できることです。インターネットサービスが有効の場合（デフォルトではオフになっています）、デフォルトのインターネットルートが作成されます。このルート（サブネット）に一致するトラフィックは、パブリックインターネットリソースに配信するために、このアプライアンスのインターネットとして分類されます。

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

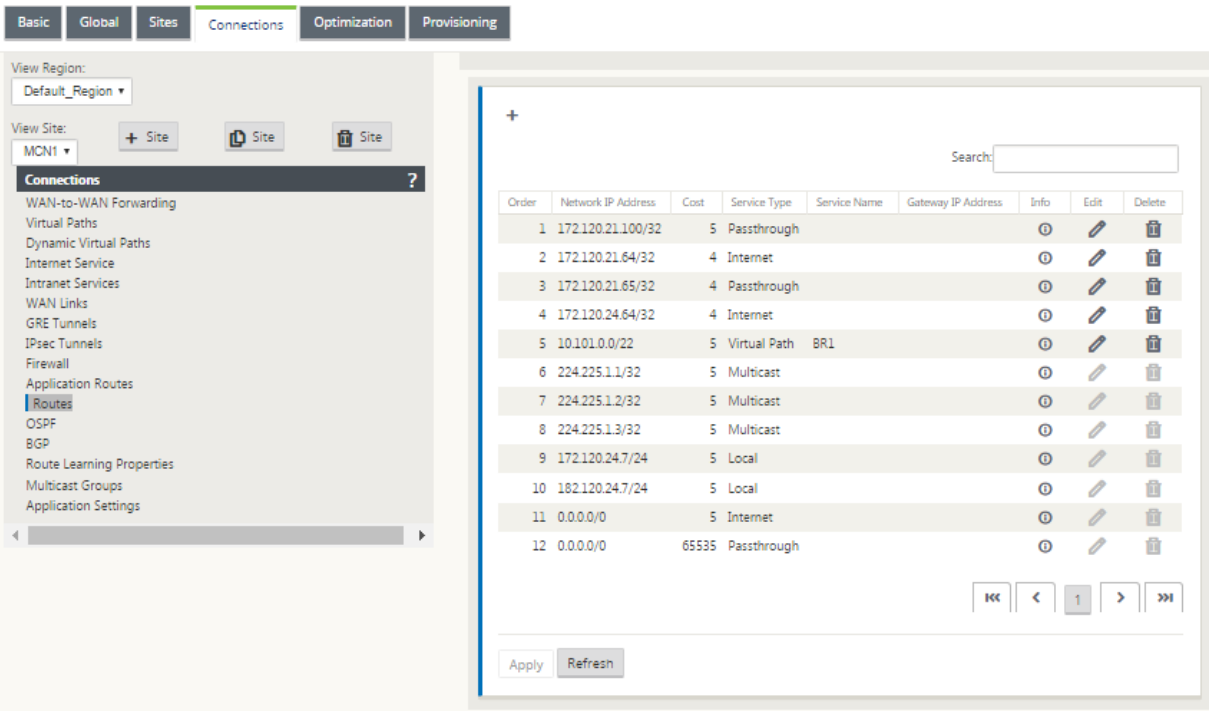
- パススルー—アプライアンスがインラインモードの場合、このサービスは最後の手段または上書きサービスとして機能します。宛先 IP アドレスが他のルートと一致しない場合、SD-WAN アプライアンスはそのアドレス

を WAN リンクネクストホップに転送するだけです。デフォルトルート：0.0.0.0/0 コスト 16 パススルールートが自動的に作成されます。SD-WAN アプライアンスがパス外またはエッジ/ゲートウェイモードで展開されている場合、パススルーは機能しません。このルート（サブネット）に一致するトラフィックはすべて、このアプライアンスのパススルーとして分類されます。パススルートラフィックは可能な限り制限されることを推奨します。

> 注
>
> パススルーは、POC の実行時に多数のルーティングを設定する必要がない場合に役立ちます。ただし、SD-WAN はパススルーに送信されるトラフィックの WAN リンク利用率を考慮しないため、本番環境では注意が必要です。また、問題をトラブルシューティングする場合や、仮想パスを介して特定の IP フローを配信できないようにする場合にも役立ちます。

- **Discard**：これはサービスではなく、一致した場合にパケットをドロップする最後の手段ルートです。通常、SD-WAN アプライアンスがパスの外に展開されている場合、この動作は期待されません。すべてのキャッチルートとして、イントラネットサービスまたはローカルルートが必要です。それ以外の場合、パススルーサービスが存在しないため、トラフィックは破棄されます (パススルーデフォルトルートが存在する場合でも)。

  SD-WAN 構成エディタでは、使用可能なサイトごとにルートテーブルをカスタマイズできます。



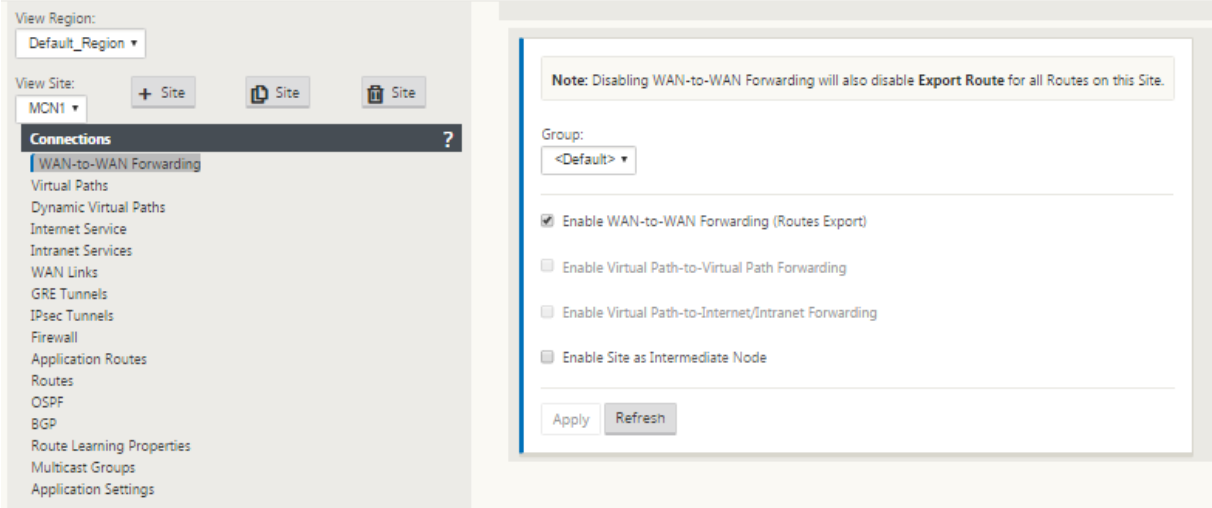
ルートテーブルエントリは、さまざまな入力から設定されます。

- 設定された仮想 IP アドレス（VIP）は、サービスタイプローカルルートとして自動入力されます。構成エディタは、異なるサイトノードへの同じ VIP 割り当てを防止します。
- ローカルサイトで有効になっているインターネットサービスは、直接インターネットブレイクアウトのためにデフォルトルート (0.0.0.0/0) をローカルに自動入力します。

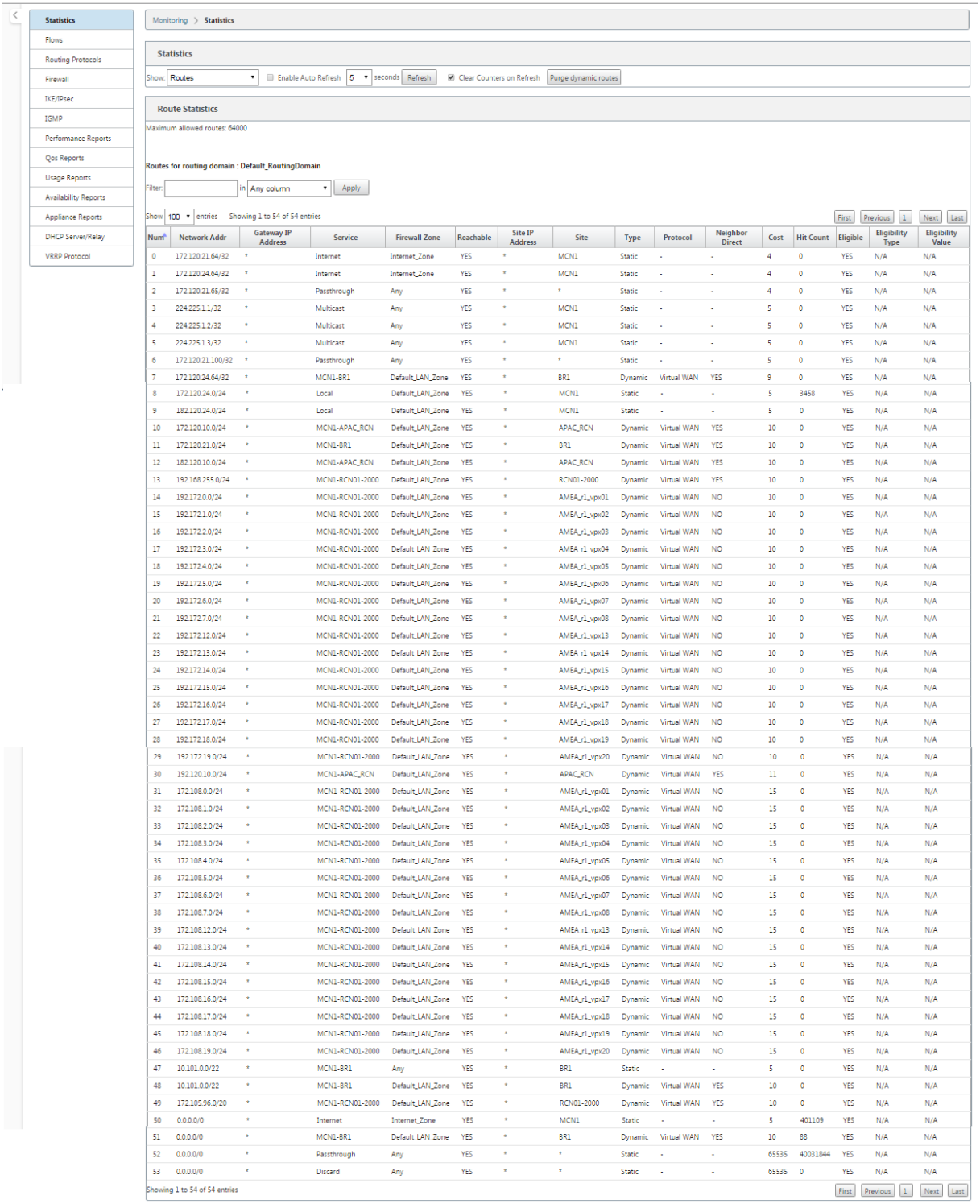
- 管理者は、サイトごとにスタティックルートを定義しました。スタティックルートは、サービスタイプローカルルートとしても定義されます。
- デフォルト（0.0.0.0/0）では、コスト 16 がパススルーとして定義されたすべてのルートがキャッチされます。

管理者は、上記のルートの 1 つを設定できますが、ルートコストに加えて、サービスタイプに応じてサービスタイプ、ネクストホップ、または Gateway を含めることもできます。デフォルトのルートコストは、各ルートタイプに自動的に追加されます (デフォルトのルートコストについては、次の表を参照してください)。また、信頼されたルートだけが他の SD-WAN アプライアンスにアドバタイズされます。信頼できないルートは、ローカルアプライアンスでのみ使用されます。

クライアントノードルートは、デフォルトでは MCN ノードにのみアドバタイズされ、他のクライアントノードはアドバタイズされません。クライアントノードルートを別のクライアントノードに表示するには、MCN ノードで WAN から WAN への転送を有効にする必要があります。



グローバル設定で WAN-to-WAN 転送（ルートエクスポートテンプレート）が有効になっている場合、MCN サイトは SD-WAN オーバーレイに参加しているすべてのクライアントにアドバタイズされたルートを共有します。この機能をオンにすると、MCN を通過する通信で、異なるクライアントノードサイトにあるホスト間の IP 接続が可能になります。ローカルクライアントノードのルートテーブルは、[**Monitoring] > [**Statistics**] ページで、[**Show**] ドロップダウンリストで [ルート] を選択して監視できます ** 。



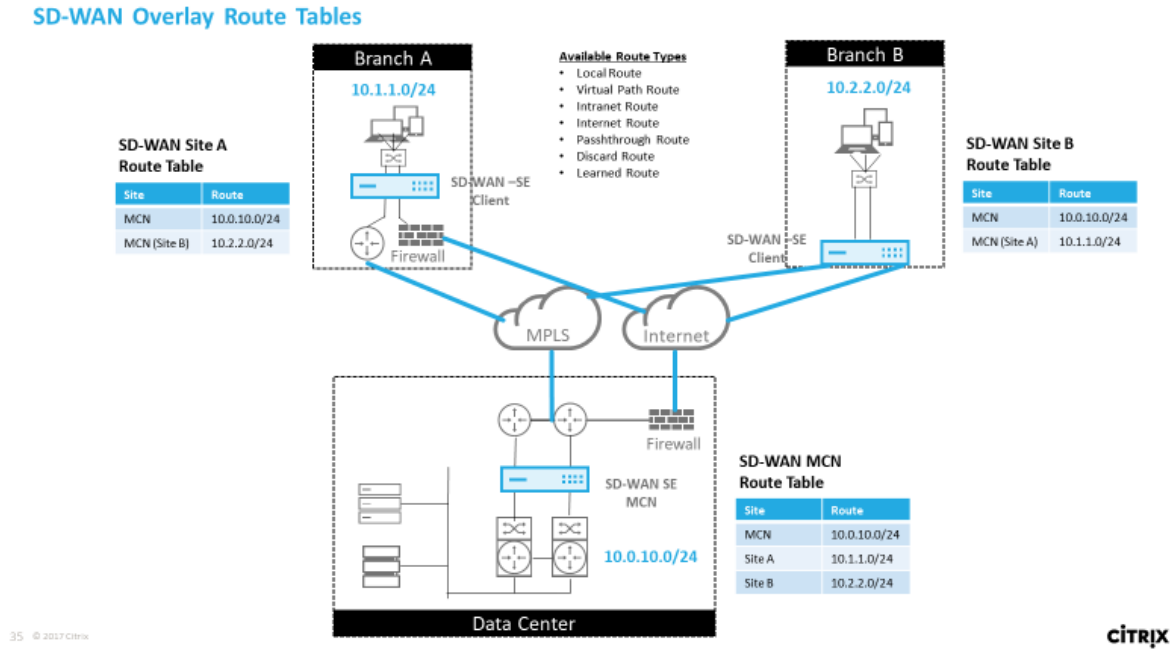
Num	Network Addr	Gateway IP Address	Service	Firewall Zone	Reachable	Site IP Address	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
0	172.120.21.64/32	*	Internet	Internet_Zone	YES	*	MCN1	Static	-	-	4	0	YES	N/A	N/A
1	172.120.24.64/32	*	Internet	Internet_Zone	YES	*	MCN1	Static	-	-	4	0	YES	N/A	N/A
2	172.120.21.65/32	*	Passthrough	Any	YES	*	*	Static	-	-	4	0	YES	N/A	N/A
3	224.225.1.1/32	*	Multicast	Any	YES	*	MCN1	Static	-	-	5	0	YES	N/A	N/A
4	224.225.1.2/32	*	Multicast	Any	YES	*	MCN1	Static	-	-	5	0	YES	N/A	N/A
5	224.225.1.3/32	*	Multicast	Any	YES	*	MCN1	Static	-	-	5	0	YES	N/A	N/A
6	172.120.21.100/32	*	Passthrough	Any	YES	*	*	Static	-	-	5	0	YES	N/A	N/A
7	172.120.24.64/32	*	MCN1-BR1	Default_LAN_Zone	YES	*	BR1	Dynamic	Virtual WAN	YES	9	0	YES	N/A	N/A
8	172.120.24.0/24	*	Local	Default_LAN_Zone	YES	*	MCN1	Static	-	-	5	3458	YES	N/A	N/A
9	182.120.24.0/24	*	Local	Default_LAN_Zone	YES	*	MCN1	Static	-	-	5	0	YES	N/A	N/A
10	172.120.10.0/24	*	MCN1-APAC_RCN	Default_LAN_Zone	YES	*	APAC_RCN	Dynamic	Virtual WAN	YES	10	0	YES	N/A	N/A
11	172.120.21.0/24	*	MCN1-BR1	Default_LAN_Zone	YES	*	BR1	Dynamic	Virtual WAN	YES	10	0	YES	N/A	N/A
12	182.120.10.0/24	*	MCN1-APAC_RCN	Default_LAN_Zone	YES	*	APAC_RCN	Dynamic	Virtual WAN	YES	10	0	YES	N/A	N/A
13	192.168.255.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	RCN01-2000	Dynamic	Virtual WAN	YES	10	0	YES	N/A	N/A
14	192.172.0.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx01	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
15	192.172.1.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx02	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
16	192.172.2.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx03	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
17	192.172.3.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx04	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
18	192.172.4.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx05	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
19	192.172.5.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx06	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
20	192.172.6.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx07	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
21	192.172.7.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx08	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
22	192.172.12.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx13	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
23	192.172.13.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx14	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
24	192.172.14.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx15	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
25	192.172.15.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx16	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
26	192.172.16.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx17	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
27	192.172.17.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx18	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
28	192.172.18.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx19	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
29	192.172.19.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx20	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
30	192.120.10.0/24	*	MCN1-APAC_RCN	Default_LAN_Zone	YES	*	APAC_RCN	Dynamic	Virtual WAN	YES	11	0	YES	N/A	N/A
31	172.108.0.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx01	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
32	172.108.1.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx02	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
33	172.108.2.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx03	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
34	172.108.3.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx04	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
35	172.108.4.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx05	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
36	172.108.5.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx06	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
37	172.108.6.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx07	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
38	172.108.7.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx08	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
39	172.108.12.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx13	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
40	172.108.13.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx14	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
41	172.108.14.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx15	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
42	172.108.15.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx16	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
43	172.108.16.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx17	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
44	172.108.17.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx18	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
45	172.108.18.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx19	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
46	172.108.19.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx20	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
47	10.101.0.0/22	*	MCN1-BR1	Any	YES	*	BR1	Static	-	-	5	0	YES	N/A	N/A
48	10.101.0.0/22	*	MCN1-BR1	Default_LAN_Zone	YES	*	BR1	Dynamic	Virtual WAN	YES	10	0	YES	N/A	N/A
49	172.105.96.0/20	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	RCN01-2000	Dynamic	Virtual WAN	YES	10	0	YES	N/A	N/A
50	0.0.0.0/0	*	Internet	Internet_Zone	YES	*	MCN1	Static	-	-	5	401109	YES	N/A	N/A
51	0.0.0.0/0	*	MCN1-BR1	Default_LAN_Zone	YES	*	BR1	Dynamic	Virtual WAN	YES	10	88	YES	N/A	N/A
52	0.0.0.0/0	*	Passthrough	Any	YES	*	*	Static	-	-	65535	40031844	YES	N/A	N/A
53	0.0.0.0/0	*	Discard	Any	YES	*	*	Static	-	-	65535	0	YES	N/A	N/A

Showing 1 to 54 of 54 entries
First Previous 1 Next Last

リモートブランチオフィスのサブネットの各ルートは、MCN 経由で接続する仮想パスを介してサービスとしてアドバタイズされます。[サイト] 列には、宛先がローカルサブネットとして存在するクライアントノードが表示されます。

次の例では、**WAN** ツー **WAN** 転送（ルートエクスポート）が有効の場合、支店 A は MCN を経由する支店 B サブネ

ット（10.2.2.0/24）のルートテーブルエントリをネクストホップとして持っています。



定義されたルートで **Citrix SD-WAN** トラフィックが一致する方法

Citrix SD-WAN で定義されたルートの照合プロセスは、宛先サブネットの最長のプレフィックス一致に基づきます（ルーターの操作に似ています）。ルートの具体性が高いほど、マッチングされるルートの変化が高くなります。ソートは次の順序で行われます。

1. 最長プレフィクス一致
2. コスト
3. サービス

したがって、/32 ルートは、常に /31 ルートの前にあります。2 つの /32 ルートの場合、コスト 4 ルートは常にコスト 5 ルートの前にあります。2 つの /32 コスト 5 ルートの場合、ルートは順序付けされた IP ホストに基づいて選択されます。サービスの順序は次のとおりです。ローカル、仮想パス、イントラネット、インターネット、パススルー、破棄。

例として、次の 2 つのルートを考える。

- 192.168.1.0/24 コスト 5
- 192.168.1.64/26 コスト 10

192.168.1.65 ホスト宛てのパケットは、コストが高い場合でも、後者のルートを使用します。これに基づいて、パススルーサービスへのデフォルトルートなど、すべてのルートをキャッチする他のトラフィックと、Virtual Path オーバーレイを介して配信されるルートのみの設定を行うことが一般的です。

ルートは、同じプレフィックスを持つサイトノードルートテーブルで構成できます。タイブレークは、ルートコスト、サービスタイプ（仮想パス、イントラネット、インターネットなど）、およびネクストホップ IP に移動します。

Citrix SD-WAN ルーティングパケットフロー

- LAN から WAN（仮想パス）のトラフィックルート照合：
  1. 着信トラフィックは LAN インターフェイスによって受信され、処理されます。
  2. 受信したフレームは、最長プレフィクス一致のルートテーブルと比較されます。
  3. 一致が見つかった場合、フレームはルールエンジンによって処理され、フローデータベースにフローが作成されます。
- WAN から LAN（仮想パス）のトラフィックルート照合：
  1. 仮想パストラフィックはトンネルから SD-WAN によって受信され、処理されます。
  2. アプライアンスは、ソース IP アドレスを比較して、ソースがローカルであるかどうかを確認します。
     - 「はい」の場合：WAN は適格で、IP 宛先をルーティングテーブル/仮想パスに一致させます。
     - 「いいえ」の場合、WAN から WAN への転送が有効になります。
  3. （WAN から WAN への転送は無効）ローカルルートに基づいて LAN に転送します。
  4. （WAN から WAN への転送が有効）ルートテーブルに基づいて仮想パスに転送します。
- 非仮想パストラフィック：
  1. 着信トラフィックは LAN インターフェイスで受信され、処理されます。
  2. 受信したフレームは、最長プレフィクス一致のルートテーブルと比較されます。
  3. 一致が見つかった場合、フレームはルールエンジンによって処理され、フローデータベースにフローが作成されます。

Citrix SD-WAN ルーティングプロトコルのサポート

Citrix SD-WAN リリース 9.1 では、OSPF および BGP ルーティングプロトコルを構成に導入しました。SD-WAN にルーティングプロトコルを導入すると、ルーティングプロトコルがアクティブに使用されている、より複雑なアンダーレイネットワークに SD-WAN を簡単に統合できます。同じルーティングプロトコルを SD-WAN で有効にすると、SD-WAN オーバーレイを利用するように示すサブネットの設定が容易になりました。さらに、ルーティングプロトコルにより、SD-WAN サイトと非 SD-WAN サイト間の通信が可能になり、共通のルーティングプロトコルを使用して既存のカスタマーエッジルータに直接通信できます。アンダーレイネットワークで動作するルーティングプ

ロトコルに参加する Citrix SD-WAN は、SD-WAN の展開モード（インラインモード、仮想インラインモード、エッジ/ゲートウェイモード）に関係なく実行できます。また、SD-WAN は「学習専用」モードで展開できます。この場合、SD-WAN はルートを受信できますが、ルートをアンダーレイにアドバタイズすることはできません。これは、ルーティングインフラストラクチャが複雑または不確実であるネットワークに SD-WAN ソリューションを導入する場合に便利です。

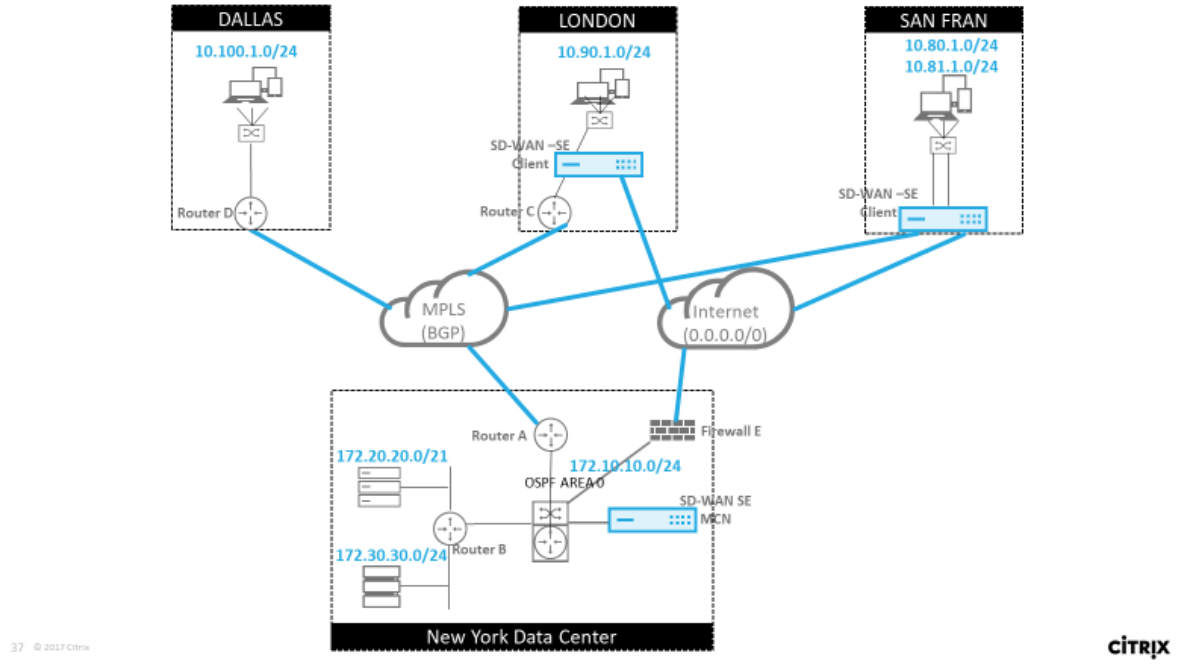
> 重要
>
> 気をつけなければ、不要なルートを漏らすのは簡単です。

SD-WAN 仮想パスルートテーブルは、BGP（サイト間と考える）と同様に、外部ゲートウェイプロトコル（EGP）として機能します。たとえば、SD-WAN が SD-WAN アプライアンスから OSPF へのルートをアドバタイズする場合、通常はサイトおよびプロトコルの外部と見なされます。

> 注
>
> インフラストラクチャ全体にわたって（WAN 経由で）IGP が存在する環境は、SD-WAN アドバタイズされたルートの使用方法が複雑になるため、注意してください。EIGRP は市場で広く使用されており、SD-WAN はそのプロトコルと相互運用できません。

SD-WAN 配置にルーティングプロトコルを導入する際の課題の 1 つは、SD-WAN サービスが有効になり、ネットワーク内で動作するまでルートテーブルを使用できないことです。そのため、最初に SD-WAN アプライアンスからのルートのアドバタイズを有効にすることは推奨されません。SD-WAN でルーティングプロトコルを段階的に導入するには、インポートフィルタとエクスポートフィルタを使用します。

私たちは、次の例を見直すことによって詳しく見てみましょう：



この例では、ルーティングプロトコルの使用例を調べます。前述のネットワークには、ニューヨーク、ダラス、ロンドン、サンフランシスコの 4 つの拠点があります。SD-WAN アプライアンスをこれらの 3 つの場所に導入し、SD-WAN を使用してハイブリッド WAN ネットワークを作成します。このネットワークでは、MPLS とインターネット WAN リンクを使用して仮想化 WAN を提供します。ダラスには SD-WAN デバイスがないため、アンダーレイと SD-WAN オーバーレイネットワーク間の完全な接続を確保するために、そのサイトへの既存のルートプロトコルとの統合方法を検討する必要があります。

ネットワーク例では、MPLS ネットワーク上の 4 つのロケーションすべて間で eBGP が使用されます。各ロケーションには、独自の自律システム番号（ASN）があります。

New York データセンターでは、コアデータセンターサブネットをリモートサイトにアドバタイズし、New York Firewall（E; ニューヨークファイアウォール）からのデフォルトルートをアナウンスするために OSPF が実行されています。この例では、ロンドン支店とサンフランシスコ支店にインターネットへのパスがあるにもかかわらず、すべてのインターネットトラフィックがデータセンターにバックホールされます。

また、サンフランシスコのサイトには、ルータがないことにも注意する必要があります。SD-WAN はエッジ/Gateway モードで展開され、そのアプライアンスはサンフランシスコサブネットのデフォルトゲートウェイであり、MPLS への eBGP にも参加します。

- New York データセンターでは、SD-WAN が仮想インラインモードで展開されていることに注意してください。この目的は、既存の OSPF ルーティングプロトコルに参加して、トラフィックを優先 Gateway としてアプライアンスに転送することです。
- London サイトは、従来のインラインモードで展開されます。アップストリーム WAN ルータ（C）は、引き続き London サブネットのデフォルト Gateway になります。
- サンフランシスコサイトはこのネットワークに新しく導入されたサイトであり、SD-WAN は Edge/Gateway モードで展開され、新しい San Francisco サブネットのデフォルトゲートウェイとして機能する予定です。

SD-WAN を実装する前に、既存のアンダーレイルートテーブルの一部を確認してください。

ニューヨークコアルータ **B**:

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

O>* 0.0.0.0/0 [110/10] via 172.10.10.3, eth1, 00:08:56
O>* 10.90.1.0/24 [110/20] via 172.10.10.1, eth1, 00:21:02
O>* 10.100.1.0/24 [110/20] via 172.10.10.1, eth1, 00:21:02
C>* 127.0.0.0/8 is directly connected, lo
O   172.10.10.0/24 [110/10] is directly connected, eth1, 1d20h00m
C>* 172.10.10.0/24 is directly connected, eth1
C>* 172.20.20.0/24 is directly connected, eth2
C>* 172.30.30.0/24 is directly connected, eth3
C>* 192.168.65.0/24 is directly connected, eth0
```

ローカル New York サブネット（172.x.x.x）は、直接接続されたルータ B で使用でき、ルートテーブルから、デフ

ォルトルートが 172.10.10.3（ファイアウォール E）であることが特定されます。また、ダラス（10.90.1.0/24）とロンドン（10.100.1.0/24）のサブネットが 172.10.10.1（MPLS ルータ A）を介して利用可能であることがわかります。ルートコストは、eBGP から学習されたことを示します。

> 注
>
> この例では、サンフランシスコはルートとしてリストされていません。これは、SD-WAN のサイトをエッジ/ゲートウェイモードで展開していないためです。

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

O>* 0.0.0.0/0 [110/10] via 172.10.10.3, eth1, 00:09:52
B>* 10.90.1.0/24 [20/1] via 192.168.10.2, eth2, 1d23h09m
B>* 10.100.1.0/24 [20/1] via 192.168.10.3, eth2, 1d23h10m
C>* 127.0.0.0/8 is directly connected, lo
O   172.10.10.0/24 [110/10] is directly connected, eth1, 1d20h01m
C>* 172.10.10.0/24 is directly connected, eth1
O>* 172.20.20.0/24 [110/20] via 172.10.10.2, eth1, 00:21:58
O>* 172.30.30.0/24 [110/20] via 172.10.10.2, eth1, 00:21:58
C>* 192.168.10.0/24 is directly connected, eth2
O   192.168.65.0/24 [110/20] via 172.10.10.2, 1d19h57m
C>* 192.168.65.0/24 is directly connected, eth0
```

New York WAN ルータ（A）では、OSPF によって学習されたルートと、eBGP を介して MPLS 経由で学習されたルートがリストされます。工順コストに注意してください。BGP は、OSPF 110/10 と比較して、デフォルトで 20/1 の低い管理ドメインとコストです。

ダラス・ルータ **D**:

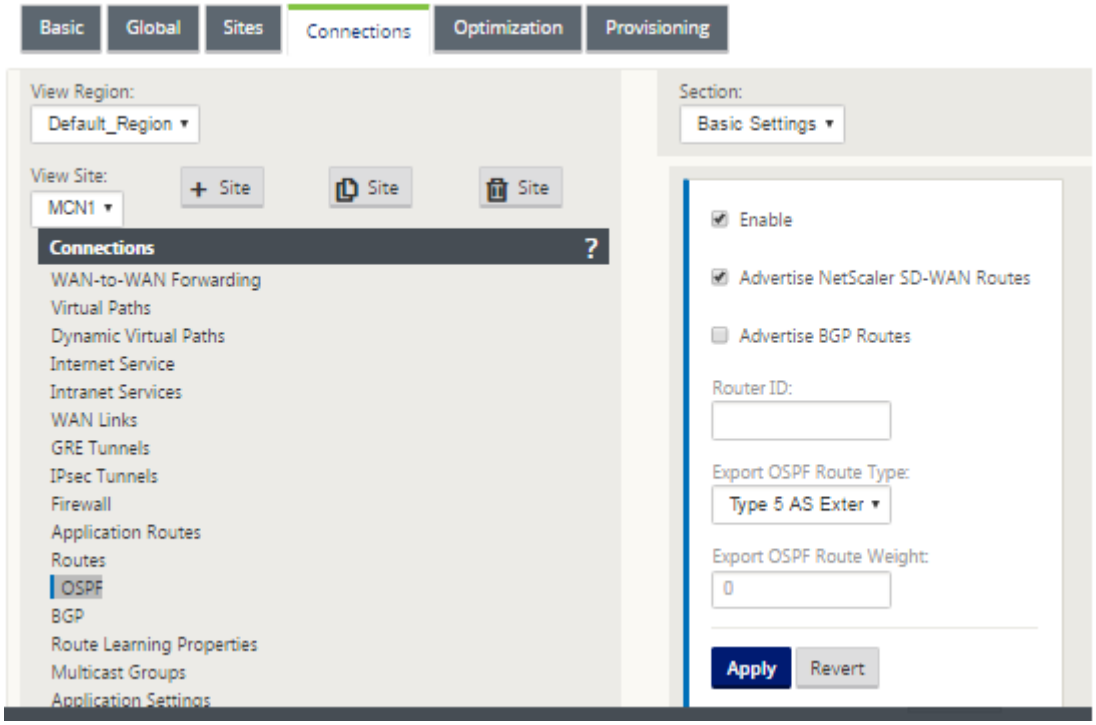
ダラス WAN ルータ（D）では、すべてのルートが MPLS 経由で学習されます。

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

B>* 0.0.0.0/0 [20/10] via 192.168.10.1, eth2, 00:10:17
B>* 10.90.1.0/24 [20/1] via 192.168.10.2, eth2, 1d23h10m
C>* 10.100.1.0/24 is directly connected, eth1
C>* 127.0.0.0/8 is directly connected, lo
B>* 172.10.10.0/24 [20/1] via 192.168.10.1, eth2, 1d23h10m
B>* 172.20.20.0/24 [20/20] via 192.168.10.1, eth2, 00:22:17
B>* 172.30.30.0/24 [20/20] via 192.168.10.1, eth2, 00:22:17
C>* 192.168.10.0/24 is directly connected, eth2
C>* 192.168.65.0/24 is directly connected, eth0
```

> 注
>
> この例では、192.168.65.0/24 サブネットを無視できます。これは管理ネットワークであり、この例には関連

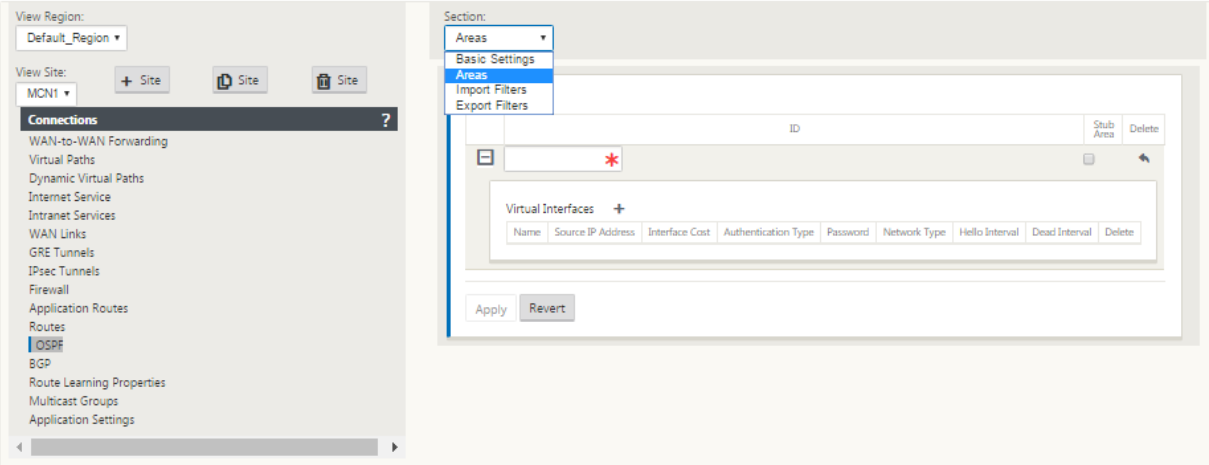
> していません。すべてのルータは管理サブネットに接続されますが、どのルーティングプロトコルでもアドバタイズされません。

Citrix SD-WAN では、我々は、接続 > サイトの 表示 > OSPF > 基本設定 の下で、ニューヨークのサイトにある SD-WAN 上で **OSPF** を有効にすることにより、SD-WAN オーバーレイを追加することができます:



> 注
>
> エクスポート **OSPF** ルートタイプは、デフォルトでタイプ 5 外部です。これは、SD-WAN ルーティングテーブルが OSPF プロトコルの外部と見なされるため、OSPF は内部（エリア内）で学習されたルートを優先するため、SD-WAN によってアドバタイズされるルートが優先されない可能性があるためです。

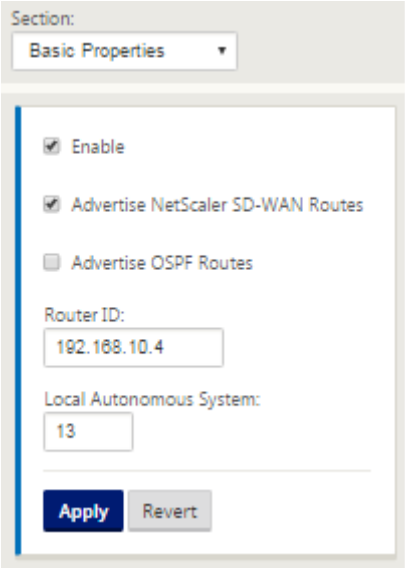
OSPF が WAN 全体（つまり MPLS ネットワーク）で使用されている場合、これをタイプ 1 のエリア内に変更できます。OSPF エリアは、次のように設定できます。

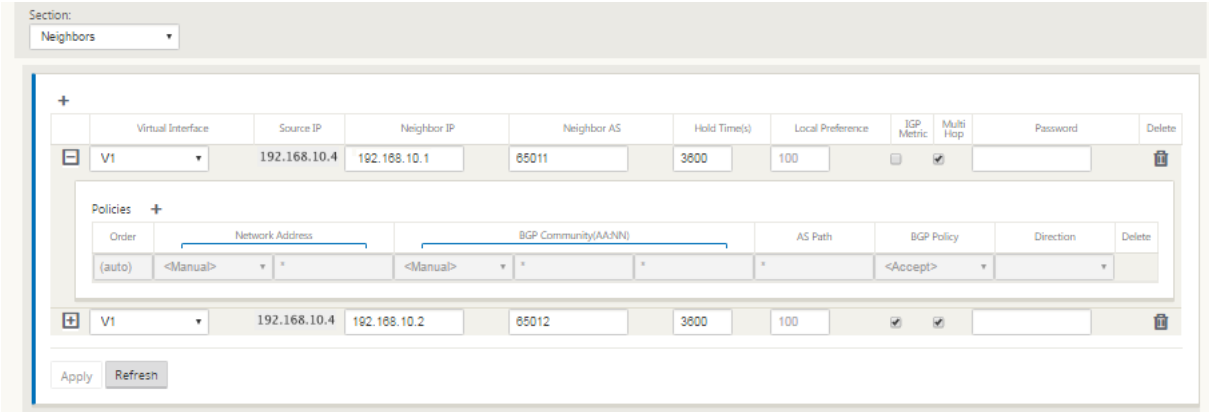


仮想インターフェイス（172.10.10.0）から派生したローカルネットワークで追加されたエリア 0 は、その他の設定はすべてデフォルトのままです。

新しい San Francisco サイトでは、eBGP が MPLS ネットワークに直接接続され、サイトのカスタマーエッジルートとして動作するため、eBGP を有効にする必要があります。BGP は、[接続] > [サイトの表示] > [**BGP**] > [基本設定] で有効にできます。

自律システム番号 13 に注意してください。





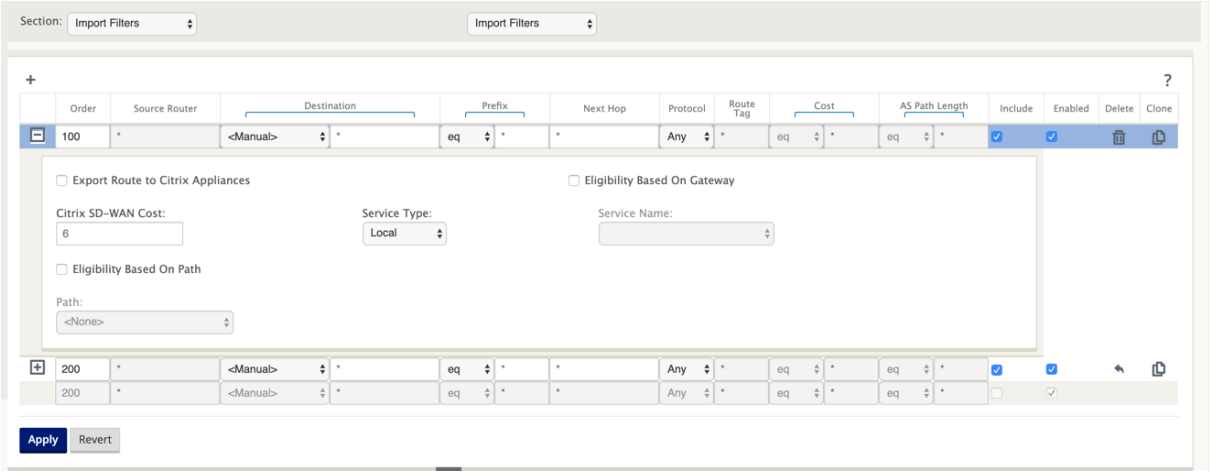
eBGP は、他のロケーションとピアリングします。各 ASN は異なります。

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

- サンフランシスコロケーションには、2 つのローカルサブネット **10.80.1.0/24** と **10.81.1.0/24** があります。ダラスなどのサイトがアンダーレイネットワーク経由でサンフランシスコのサイトに到達し、ロンドンやニューヨークなどのサイトが Virtual Path オーバーレイネットワーク経由でサンフランシスコに到達できる

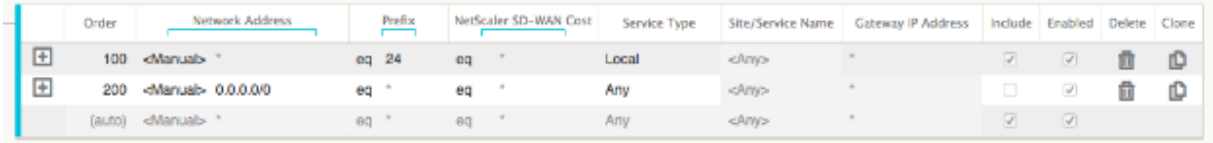
ように、eBGP を通じてこれらのサイトを宣伝したいと考えています。また、SD-WAN 仮想パスオーバーレイがダウンし、環境が MPLS だけの使用にフォールバックする必要がある場合に備えて、すべてのサイトへの eBGP 到達可能性について学習します。また、SD-WAN が eBGP から SD-WAN ルータに学習する内容を再評価する必要もありません。このためには、フィルタを次のように構成する必要があります。

- eBGP からすべてのルートをインポートします。SD-WAN アプライアンスにルートを再読み込み/エクスポートしないでください。



- ローカルルートを eBGP にエクスポートする

エクスポートのデフォルトのルールは、すべてをエクスポートすることです。ルール 200 は、ルートを再検証しないようにフォールトルールを上書きするために使用されます。任意のプレフィクス SD-WAN に一致するすべてのルートが、仮想パスを通って学習しました。



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

ダラスルータ **D:**


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

B>* 0.0.0.0/0 [20/10] via 192.168.10.1, eth2, 00:00:01
B>* 10.80.1.0/24 [20/0] via 192.168.10.4, eth2, 3d19h07m
B>* 10.81.1.0/24 [20/0] via 192.168.10.4, eth2, 3d19h07m
B>* 10.90.1.0/24 [20/1] via 192.168.10.2, eth2, 4d23h38m
C>* 10.100.1.0/24 is directly connected, eth1
C>* 127.0.0.0/8 is directly connected, lo
B>* 172.10.10.0/24 [20/1] via 192.168.10.1, eth2, 4d23h38m
B>* 172.20.20.0/24 [20/20] via 192.168.10.1, eth2, 00:00:01
B>* 172.30.30.0/24 [20/20] via 192.168.10.1, eth2, 00:00:01
B   192.168.10.0/24 [20/0] via 192.168.10.4 inactive, 3d19h07m
C>* 192.168.10.0/24 is directly connected, eth2
C>* 192.168.65.0/24 is directly connected, eth0
```

さらに、Citrix SD-WAN ルートテーブルは、［モニタリング］>［統計］>［ルートの表示］ページで確認できます。

サンフランシスコの **Citrix SD-WAN**:

Routes for routing domain : Default_RoutingDomain

Filter: in Any column Apply

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

Num	Network Addr	Gateway IP Address	Service	Reachable	Site IP Address	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
0	10.81.1.0/24	10.80.1.20	Local	YES	*	SFO	Static	-	-	5	0	YES	N/A	N/A
1	10.80.1.0/24	*	Local	YES	*	SFO	Static	-	-	5	0	YES	N/A	N/A
2	192.168.10.0/24	*	Local	YES	*	SFO	Static	-	-	5	122	YES	N/A	N/A
3	172.10.10.0/24	*	NYC-SFO	YES	*	NYC	Static	-	-	5	0	YES	N/A	N/A
4	172.30.30.0/24	192.168.10.1	Local	YES	*	SFO	Dynamic	BGP	-	6	0	YES	N/A	N/A
5	172.20.20.0/24	192.168.10.1	Local	YES	*	SFO	Dynamic	BGP	-	6	0	YES	N/A	N/A
6	172.10.10.0/24	192.168.10.1	Local	YES	*	SFO	Dynamic	BGP	-	6	0	YES	N/A	N/A
7	10.100.1.0/24	192.168.10.3	Local	YES	*	SFO	Dynamic	BGP	-	6	0	YES	N/A	N/A
8	10.90.1.0/24	192.168.10.2	Local	YES	*	SFO	Dynamic	BGP	-	6	0	YES	N/A	N/A
9	172.20.20.0/24	*	NYC-SFO	YES	*	NYC	Dynamic	Virtual WAN	YES	6	0	YES	N/A	N/A
10	10.100.1.0/24	*	NYC-SFO	YES	*	NYC	Dynamic	Virtual WAN	YES	6	0	YES	N/A	N/A
11	172.30.30.0/24	*	NYC-SFO	YES	*	NYC	Dynamic	Virtual WAN	YES	6	0	YES	N/A	N/A
12	0.0.0.0/0	192.168.10.1	Local	YES	*	SFO	Dynamic	BGP	-	6	0	YES	N/A	N/A
13	0.0.0.0/0	*	NYC-SFO	YES	*	NYC	Dynamic	Virtual WAN	YES	6	0	YES	N/A	N/A
14	0.0.0.0/0	*	Passthrough	YES	*	*	Static	-	-	16	0	YES	N/A	N/A
15	0.0.0.0/0	*	Discard	YES	*	*	Static	-	-	16	0	YES	N/A	N/A

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

Citrix SD-WAN は、仮想パスオーバーレイを介して利用可能なルートを含め、学習されたすべてのルートを表示します。

私たちは、ニューヨークのデータセンターにある 172.10.10.0/24 を考えてみましょう。このルートは、次の 2 つの方法で学習されています。

- 仮想パスルート（番号 3）として、サービス = コストが 5 の NYC-SFO で、static と入力します。これは、ニューヨークの SD-WAN アプライアンスによってアドバタイズされるローカルサブネットです。アプライアンスに直接接続されているか、または設定に入力された手動スタティックルートであるという点ではスタティックです。サイト間の仮想パスが稼働状態/稼働状態にあるため、到達可能です。

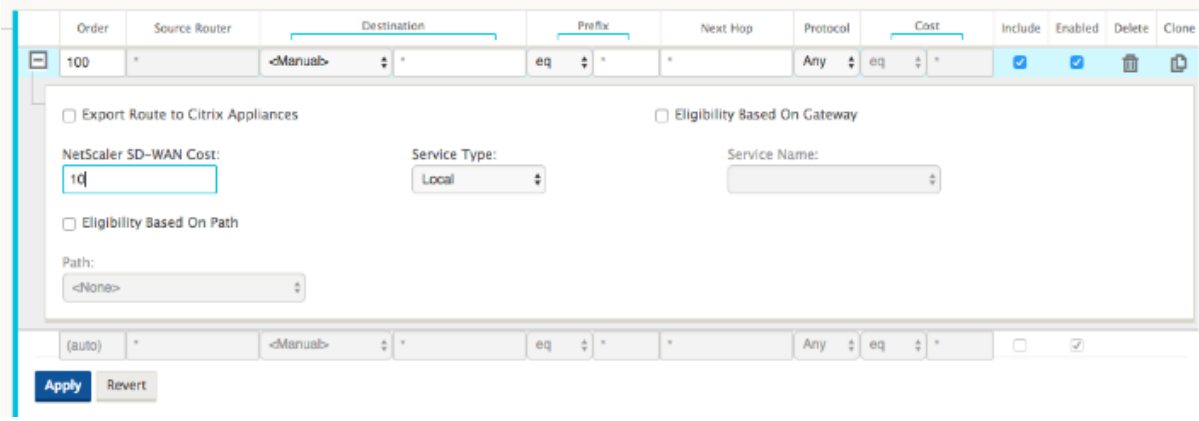
- BGP（番号 6）を介してアドバタイズされたルートとして、コストは 6 です。これは現在、フォールバックルートと見なされます。

プレフィクスが等しく、コストが異なるため、SD-WAN は仮想パスルートを使用できない限り、仮想パスルートを使用します。この場合、フォールバックルートは BGP を介して学習されます。

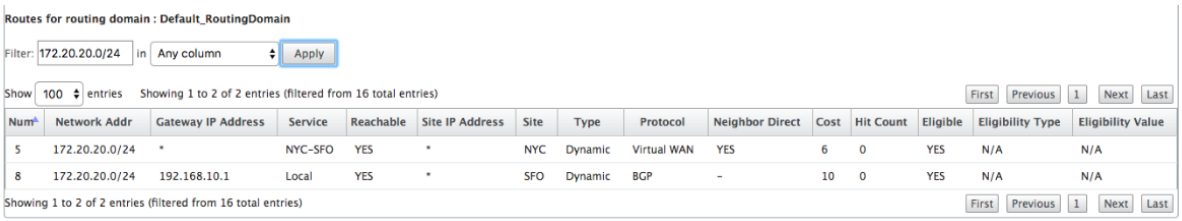
さて、ルート 172.20.20.0/24 を考えてみましょう。

- これは仮想パスルート（番号 9）として学習されますが、ダイナミックタイプでコストは 6 です。これは、リモート SD-WAN アプライアンスがルーティングプロトコル（この場合は OSPF）を介してこのルートを学習したことを意味します。デフォルトでは、ルートコストは高くなります。
- SD-WAN は、同じコストで BGP を介してこのルートを学習するため、この場合、このルートは仮想パスルートよりも優先されます。

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



調整を行った後、San Francisco アプライアンスの SD-WAN ルートテーブルを更新して、調整されたルートコストを確認できます。フィルタオプションを使用して、表示されているリストにフォーカスします。



最後に、サンフランシスコ SD-WAN で学習されたデフォルトルートを見てみましょう。私たちは、すべてのインターネットトラフィックをニューヨークにバックホールしたいと考えています。仮想パスを使用して送信するか、またはフォールバックとして MPLS ネットワークを介して送信することがわかります。

Routes for routing domain : Default_RoutingDomain

Filter: 0.0.0.0/0 in Any column Apply

Show 100 entries Showing 1 to 4 of 4 entries (filtered from 16 total entries) First Previous 1 Next Last

Num	Network Addr	Gateway IP Address	Service	Reachable	Site IP Address	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
12	0.0.0.0/0	*	NYC-SFO	YES	*	NYC	Dynamic	Virtual WAN	YES	6	0	YES	N/A	N/A
13	0.0.0.0/0	192.168.10.1	Local	YES	*	SFO	Dynamic	BGP	-	10	0	YES	N/A	N/A
14	0.0.0.0/0	*	Passthrough	YES	*	*	Static	-	-	16	0	YES	N/A	N/A
15	0.0.0.0/0	*	Discard	YES	*	*	Static	-	-	16	0	YES	N/A	N/A

Showing 1 to 4 of 4 entries (filtered from 16 total entries) First Previous 1 Next Last

また、コスト 16 のパススルーおよび廃棄ルートも表示されます。これらは、削除できない自動ルートです。デバイスがインラインの場合、パススルールートは最後の手段として使用されるため、パケットをより特定のルートと照合できない場合、SD-WAN はそのパケットをインターフェイスグループのネクストホップに渡します。SD-WAN がパス外またはエッジ/ゲートウェイモードの場合、パススルーサービスは存在しません。この場合、SD-WAN はデフォルトの廃棄ルートを使用してパケットをドロップします。Hit Count は、各ルートにヒットしているパケットの数を示します。このパケットは、トラブルシューティングの際に役立ちます。

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

New York のサイトには、複数のサブネットがあります。

- 172.10.10.0/24（直接接続）
- 172.20.20.0/24（コアルータ B から OSPF 経由でアドバタイズされる）
- 172.30.30.0/24（コアルータ B から OSPF 経由でアドバタイズされる）

また、MPLS を介してダラス（10.100.1.0/24）へのトラフィックフローを提供する必要があります。

最後に、すべてのインターネット接続トラフィックが 172.10.10.3 を経由して、ネクストホップとしてファイアウォール E にルーティングされるようにします。SD-WAN は、OSPF を介してこのデフォルトルートを学習し、仮想パスを介してアドバタイズします。ニューヨークのサイトのフィルタは次のとおりです。

Order	Source Router	Destination	Prefix	Next Hop	Protocol	Cost	Include	Enabled	Delete	Clone
100	*	<Manual> 192.168.65.0/24	eq *	*	Any	eq *	☐	☑		
200	*	<Manual> 192.168.10.0/24	eq *	*	Any	eq *	☐	☑		
300	*	<Manual> *	eq *	*	Any	eq *	☑	☑		
(auto)	*	<Manual> *	eq *	*	Any	eq *	☐	☑		

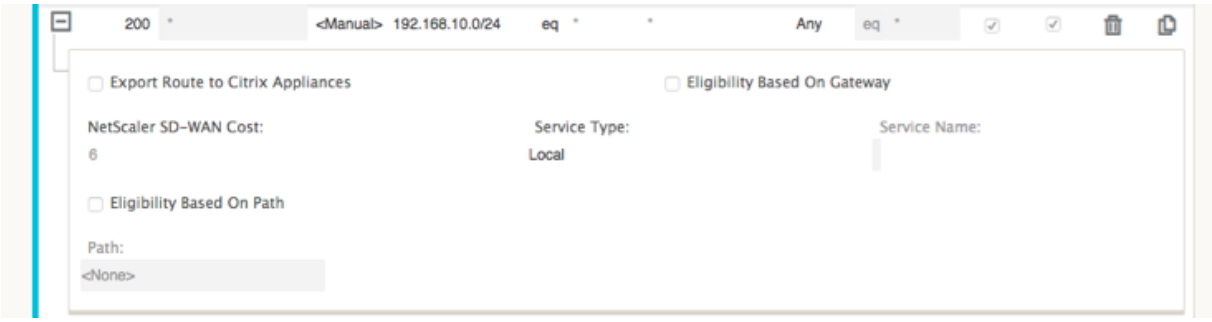
☐ Export Route to Citrix Appliances ☐ Eligibility Based On Gateway

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

☐ Eligibility Based On Path

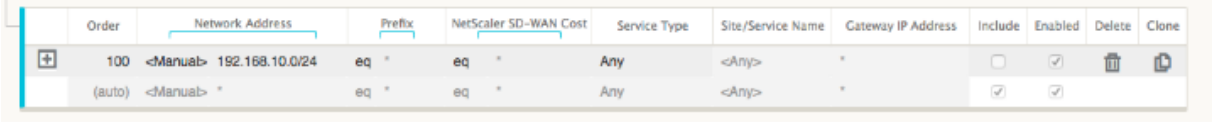
Path: <None>

New York SD-WAN サイトは、管理ネットワークのすべてのルートをインポートします。これは無視してもかまいません。フィルタ 200 に集中できます。



フィルタ 200 は、到達可能性のために 192.168.10.0/24（MPLS コア）をインポートするために使用されますが、仮想パスにはエクスポートされません。［含める］チェックボックスをオンにし、［**Citrix** アプライアンスへのルートをエクスポート］チェックボックスがオフになっていることを確認します。その後、他のすべてのルートが含まれます。

エクスポートフィルタでは、192.168.10.0/24 のルートを除外できます。これは、サンフランシスコサイト内で直接接続されたサブネットとして、このルートをソースでフィルタリングできないため、この終端では抑制されるためです。



次に、New York サイトのコアルートから更新されたルートテーブルを確認してみましょう。

ニューヨークルータ **B:**

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

O>* 0.0.0.0/0 [110/10] via 172.10.10.3, eth1, 4d22h22m
O>* 10.80.1.0/24 [110/15] via 172.10.10.10, eth1, 3d19h49m
O>* 10.81.1.0/24 [110/15] via 172.10.10.10, eth1, 3d19h49m
O>* 10.90.1.0/24 [110/15] via 172.10.10.10, eth1, 3d19h50m
O>* 10.100.1.0/24 [110/20] via 172.10.10.1, eth1, 4d22h22m
C>* 127.0.0.0/8 is directly connected, lo
O   172.10.10.0/24 [110/10] is directly connected, eth1, 4d22h22m
C>* 172.10.10.0/24 is directly connected, eth1
C>* 172.20.20.0/24 is directly connected, eth2
C>* 172.30.30.0/24 is directly connected, eth3
C>* 192.168.65.0/24 is directly connected, eth0
```

サンフランシスコ（10.80.1.0 および 10.81.1.0）およびロンドン（10.90.1.0）のサブネットが、New York SD-WAN アプライアンス（172.10.10.10）を介してアドバタイズされていることがわかります。ルート 10.100.1.0/24 は、まだアンダーレイ MPLS ルータ A を介してアドバタイズされています。ここでは、New York サイトの SD-WAN ルートテーブルを確認します。

ニューヨークのサイト **SD-WAN** ルートテーブル：

Routes for routing domain : Default_RoutingDomain

Filter: in Any column Apply

Show 100 entries Showing 1 to 11 of 11 entries First Previous 1 Next Last

Num	Network Addr	Gateway IP Address	Service	Reachable	Site IP Address	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
0	172.10.10.0/24	*	Local	YES	*	NYC	Static	-	-	5	0	YES	N/A	N/A
1	10.90.1.0/24	*	NYC-LON	YES	*	LON	Static	-	-	5	0	YES	N/A	N/A
2	10.81.1.0/24	10.80.1.20	NYC-SFO	YES	*	SFO	Static	-	-	5	0	YES	N/A	N/A
3	10.80.1.0/24	*	NYC-SFO	YES	*	SFO	Static	-	-	5	0	YES	N/A	N/A
4	192.168.10.0/24	*	NYC-SFO	YES	*	SFO	Static	-	-	5	0	YES	N/A	N/A
5	172.30.30.0/24	172.10.10.2	Local	YES	*	NYC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
6	172.20.20.0/24	172.10.10.2	Local	YES	*	NYC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
7	10.100.1.0/24	172.10.10.1	Local	YES	*	NYC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
8	0.0.0.0/0	172.10.10.3	Local	YES	*	NYC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
9	0.0.0.0/0	*	Passthrough	YES	*	*	Static	-	-	16	0	YES	N/A	N/A
10	0.0.0.0/0	*	Discard	YES	*	*	Static	-	-	16	0	YES	N/A	N/A

OSPF を介して学習されたローカルサブネット、MPLS ルータ A から学習されたダラスサイトへのルート、およびサンフランシスコサイトとロンドンサイトのリモートサブネットの両方の正しいルートを確認できます。MPLS ルータ A を見てみましょう。このルータは OSPF および BGP に参加しています。

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

O>* 0.0.0.0/0 [110/10] via 172.10.10.3, eth1, 00:04:12
O   10.80.1.0/24 [110/15] via 172.10.10.10, 00:04:13
B>* 10.80.1.0/24 [20/0] via 192.168.10.4, eth2, 00:05:09
O   10.81.1.0/24 [110/15] via 172.10.10.10, 00:04:13
B>* 10.81.1.0/24 [20/0] via 192.168.10.4, eth2, 00:05:09
O   10.90.1.0/24 [110/15] via 172.10.10.10, 00:04:13
B>* 10.90.1.0/24 [20/1] via 192.168.10.2, eth2, 00:05:11
S>* 10.90.1.10/32 [5/0] via 192.168.10.2, eth2
B>* 10.100.1.0/24 [20/1] via 192.168.10.3, eth2, 00:04:28
C>* 127.0.0.0/8 is directly connected, lo
O   172.10.10.0/24 [110/10] is directly connected, eth1, 00:05:24
C>* 172.10.10.0/24 is directly connected, eth1
O>* 172.20.20.0/24 [110/20] via 172.10.10.2, eth1, 00:04:12
O>* 172.30.30.0/24 [110/20] via 172.10.10.2, eth1, 00:04:12
B   192.168.10.0/24 [20/0] via 192.168.10.4 inactive, 00:05:09
C>* 192.168.10.0/24 is directly connected, eth2
O   192.168.65.0/24 [110/20] via 172.10.10.2, 00:04:12
C>* 192.168.65.0/24 is directly connected, eth0
```

ルートテーブルから、このルータ A は BGP および OSPF を介してリモートサブネットを学習しています。BGP ルートのアドミニストレーティブディスタンスとコスト（20/5）が OSPF（110/10）よりも低いため、優先されます。この例では、コアルートが 1 つしかないネットワークでは、これは問題にならない可能性があります。ただし、ここに着信するトラフィックは、SD-WAN アプライアンス（172.10.10.10）に送信されるのではなく、MPLS ネットワーク経由で配信されます。ルーティングの対称性を完全に維持する場合は、eBGP 経由で学習したルートではなく、172.10.10.10 からのルートからのルート優先が得られるように、AD/メトリックコストを調整するルートマップが必要です。

また、「バックドア」ルートを設定して、ルータが BGP ルート経由で OSPF ルートを優先するようにすることもできます。SD-WAN 仮想 IP アドレスがロンドンサイトの SD-WAN アプライアンスへのスタティックルートに注目してください。

```
S>* 10.90.1.10/32 [5/0] via 192.168.10.2, eth2
```

これは、MPLS パスがダウンした場合に、仮想パスが New York サイトの SD-WAN アプライアンスに再ルーティングされるようにするために必要です。10.90.1.0/24 のルートが 172.10.10.10（ニューヨーク SD-WAN）経由でアドバタイズされるためです。また、仮想パスがそれ自体に戻らないように、SD-WAN アプライアンスで UDP 4,980 パケットをドロップするオーバーライドサービスルールを作成することをお勧めします。

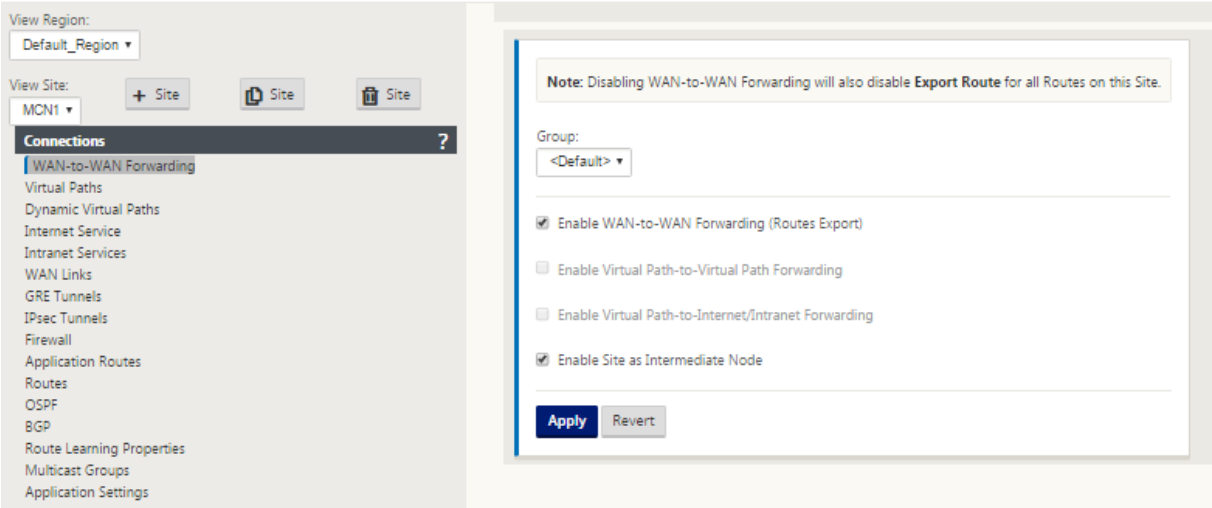
動的仮想パス

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

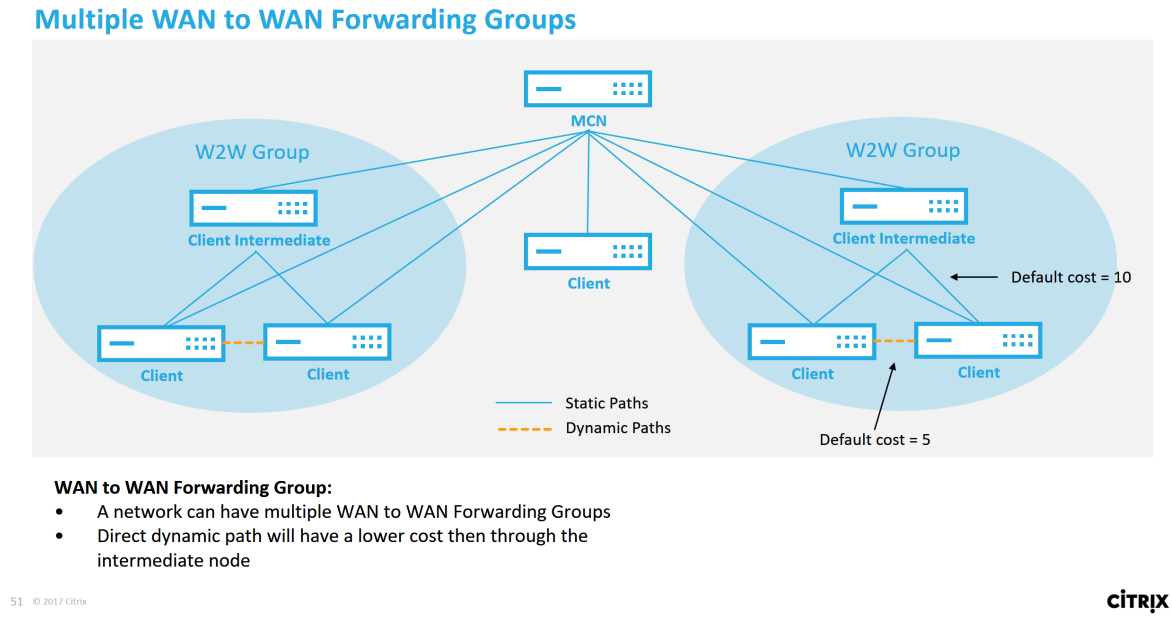
動的仮想パスのしきい値が満たされると、クライアントノードは、サイト間で利用可能なすべての WAN パスを使用して相互の仮想パスを動的に作成し、次のようにそのパスをフル活用します。

- バルクデータが存在する場合は送信し、損失がないことを確認し、
- 対話型データを送信し、損失がないことを確認してから
- バルクデータおよびインタラクティブデータが安定していると見なされた後にリアルタイムデータを送信する（損失なし、許容レベルなし）
- 一括データまたは対話型データがない場合、動的仮想パスが一定期間安定した後、リアルタイムデータを送信する
- ユーザーデータがユーザー定義の期間に設定されたしきい値を下回ると、動的仮想パスは破棄されます。

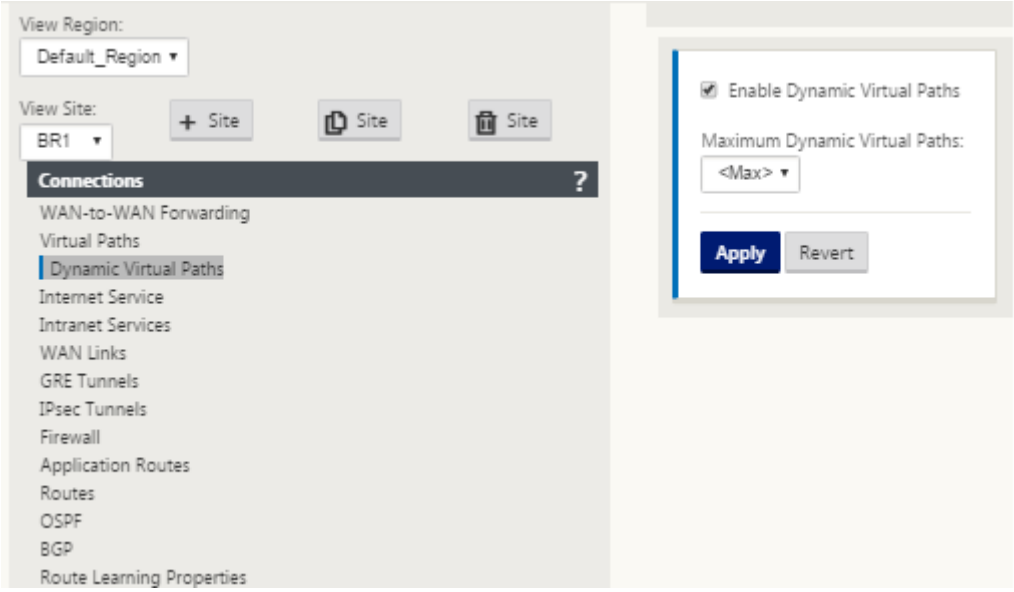
  動的仮想パスには、中間サイトの概念があります。中間サイトは、MCN サイト、または静的仮想パスが構成され、2 つ以上の他のクライアントノードに接続されているネットワーク内の他のサイトです。もう 1 つの設計上の考慮事項の要件は、WAN-to-WAN 転送を有効にして、すべてのサイトからのすべてのルートを動的仮想パスが必要なクライアントノードにアドバタイズできるようにすることです。クライアントノード通信を監視し、動的パスを確立して切断する必要がある時期を指示するには、この中間サイトに対して WAN ツー WAN 転送に加えて、**[**サイトを中間ノードとして有効にする**]** を有効にする必要があります。



SD-WAN 構成では複数の WAN-to-WAN フォワーディンググループを使用できるため、特定のクライアントノード間のパス確立に対するフルコントロールが可能になります。



クライアントノードを中間サイトとして動作させるには、その **WAN-to-WAN** フォワーディンググループに関連付けられているクライアントとの間で、静的な仮想パスを構成する必要があります。さらに、クライアントノードでは、クライアントノードごとに [動的仮想パスの有効化] オプションをオンにする必要があります。



各 SD-WAN デバイスには、それぞれ固有のルートテーブルがあり、各ルートに次の詳細が定義されています。

- Num：一致プロセスに基づくこのアプライアンスのルートの順序（最下位の Num が最初に処理される）
- ネットワーク・アドレス：サブネットまたはホスト・アドレス
- 必要に応じてゲートウェイ
- サービス：このルートに適用されるサービス
- ファイアウォールゾーン—ルートのファイアウォールゾーン分類
- 到達可能：このサイトの仮想パスの状態がアクティブ
- サイト—ルートが存在することが予想されるサイトの名前
- Type：ルートタイプの識別（スタティックまたはダイナミック）
- ネイバーダイレクト
- コスト-特定のルートのコスト
- [Hit Count]：パケットごとにルートが使用された回数。これは、ルートが正しくヒットしていることを確認するために使用されます。
- 対象外
- 適格性タイプ
- 適格性値

次に、SD-WAN サイトルートテーブルの例を示します。

Routes for routing domain : Default_RoutingDomain

Filter: in Any column Apply

Show 100 entries Showing 1 to 13 of 13 entries First Previous 1 Next Last

Num	Network Addr	Gateway IP Address	Service	Firewall Zone	Reachable	Site IP Address	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
0	172.16.10.0/24	192.168.15.1	DC-AWS	Default_LAN_Zone	YES	*	DC	Static	-	-	4	0	YES	N/A	N/A
1	192.168.100.0/24	*	Local	Default_LAN_Zone	YES	*	AWS	Static	-	-	5	0	YES	N/A	N/A
2	192.168.15.0/24	*	DC-AWS	Default_LAN_Zone	YES	*	DC	Static	-	-	5	0	YES	N/A	N/A
3	172.16.250.0/24	*	DC-AWS	Default_LAN_Zone	YES	*	DC	Static	-	-	5	0	YES	N/A	N/A
4	172.16.150.0/24	*	DC-AWS	Default_LAN_Zone	YES	*	DC	Static	-	-	5	0	YES	N/A	N/A
5	192.168.200.0/24	*	DC-AWS	Default_LAN_Zone	NO	*	Azure	Static	-	-	15	0	YES	N/A	N/A
6	192.168.10.0/24	*	DC-AWS	Default_LAN_Zone	YES	*	Branch	Static	-	-	15	0	YES	N/A	N/A
7	172.16.200.0/24	*	DC-AWS	Default_LAN_Zone	YES	*	Branch	Static	-	-	15	0	YES	N/A	N/A
8	172.16.100.0/24	*	DC-AWS	Default_LAN_Zone	YES	*	Branch	Static	-	-	15	0	YES	N/A	N/A
9	172.16.30.0/24	*	DC-AWS	Default_LAN_Zone	YES	*	Branch	Static	-	-	15	0	YES	N/A	N/A
10	0.0.0.0/0	*	Internet	Untrusted_Internet_Zon	YES	*	*	Static	-	-	5	1	YES	N/A	N/A
11	0.0.0.0/0	*	Passthrough	Any	YES	*	*	Static	-	-	16	0	YES	N/A	N/A
12	0.0.0.0/0	*	Discard	Any	YES	*	*	Static	-	-	16	0	YES	N/A	N/A

Showing 1 to 13 of 13 entries First Previous 1 Next Last

前述の SD-WAN ルートテーブルから、従来のルータでは通常使用できない要素が増えています。最も注目すべきは「到達可能」列です。この列は、WAN パスの状態に応じて、ルートをアクティブまたは非アクティブ（yes/no）にします。ここにリストされているルートは、サービスのさまざまな状態（例として仮想パスがダウンしている）に基づいて抑制されます。ルートを強制的に不適格にする可能性があるその他のイベントには、パスダウン状態、ネクストホップ到達不能、または WAN リンクダウンがあります。

前の表から、14 の定義されたルートを見ることができます。ルートまたはルートのグループの説明は、次のように記述されます。

- Route 0：MCN では、これは DC サイトに存在するホストサブネットルートです。172.16.10.0/24 は DC LAN にあり、192.168.15.1 は LAN 上の Gateway で、そのサブネットに到達するネクストホップです。
- Route 1：ルートテーブルを表示するこの SD-WAN デバイスへのローカルルートです。
- Route 2—4：DC サイト SD-WAN 用に設定された仮想インターフェイスの一部であるサブネットです。これらのサブネットは、定義された信頼された仮想インターフェイスから派生します。
- Route 5：これは、MCN によって共有される別のクライアントノードへの共有ルートで、そのサイトと MCN 間の仮想パスがダウンしているため、到達可能性ステータスが No です。
- Route 6—9：これらのルートは、別のクライアントサイトに存在します。このルートでは、仮想パス上のリモートサイト宛ての WAN 入力トラフィックを照合するために、仮想パスルートが作成されます。
- Route 10 —インターネットサービスが定義されている場合、システムは、このローカルサイトの直接インターネットブレイクアウトのキャッチオールルートを追加します。
- Route 11：パススルーは、既存のルートに一致しない場合にパケットが通過できるようにシステムによって常に追加されるデフォルトのルートです。パススルーはクリーンアップされません。通常、ローカルブロードキャストと ARP トラフィックはこのサービスにマッピングされます。
- Route 12：Discard は、未定義のものをドロップするためにシステムによって常に追加されるデフォルトのルートです。

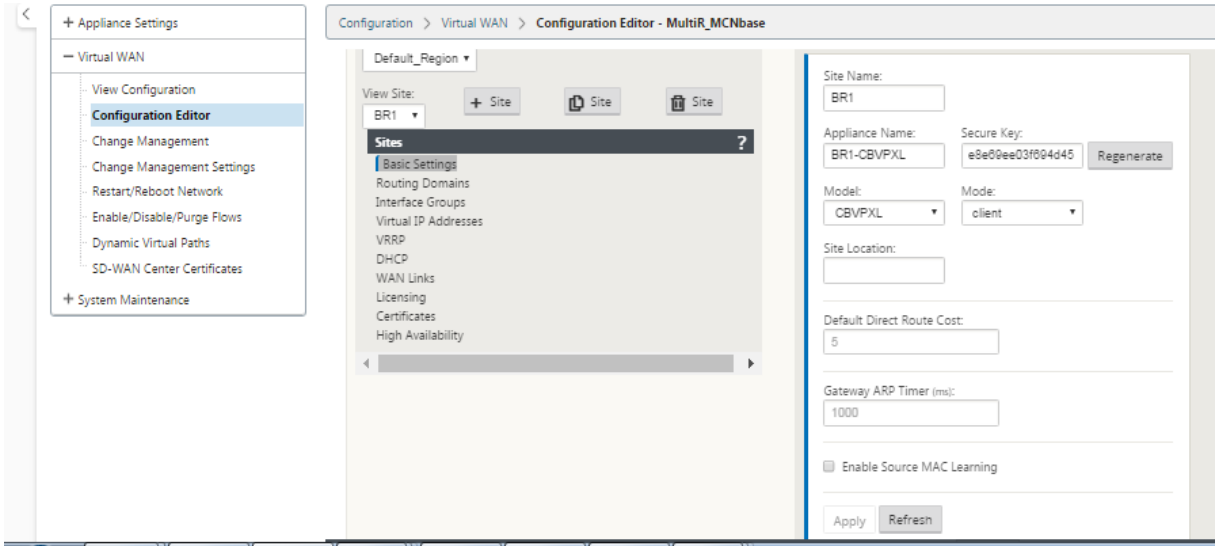
デフォルトのルートコスト値:

- WAN から WAN への転送—10
- デフォルトの直接ルートコスト—5
- 自動生成されたルート—5
- 仮想パス—5
- ローカル—5
- イントラネット—5
- インターネット—5
- パススルー—5
- オプション：ルートはサービスレベルとして定義される 0.0.0.0/0 です。

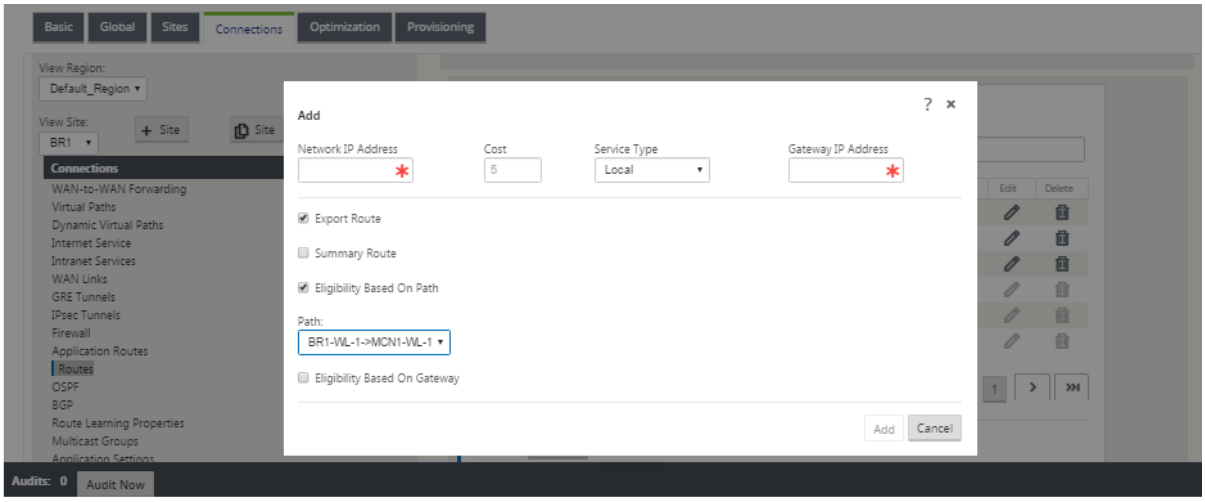
これらのルートを定義したら、定義されたルートを使用してトラフィックがどのように流れるかを理解することが重要です。これらのトラフィックフローは、次のフローに分割されます。

- LAN から WAN（仮想パス）：SD-WAN オーバーレイトンネルに入るトラフィック
- WAN から LAN（仮想パス）：SD-WAN オーバーレイトンネルに存在するトラフィック
- 非仮想パストラフィック：アンダーレイネットワークにルーティングされるトラフィック

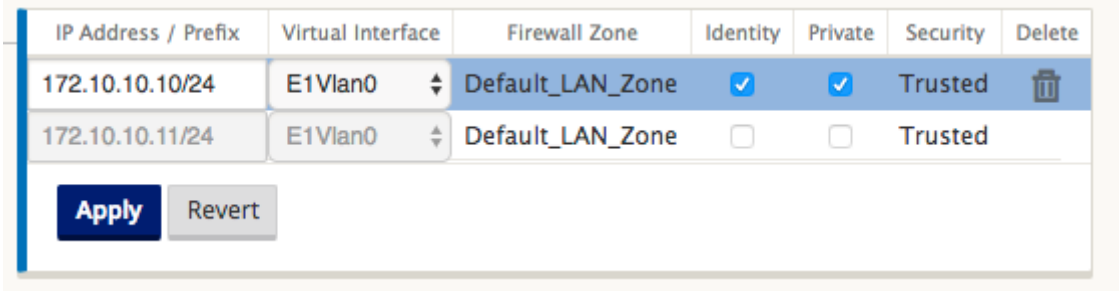
デフォルトのルートコストは、サイトごとに変更できます。構成は、[サイトの表示] > [基本設定] で確認できます。



スタティックルートは、[接続] > [サイト] > [ルート] ノードで サイトごとに定義できます。



ルートは、仮想パスまたはゲートウェイ IP 可用性に結び付けることができます。インターネットルートは、目的の動作に応じて仮想パスオーバーレイにエクスポートすることも、エクスポートしないこともできます。また、SD-WAN にアドバタイズされるプレフィクス（つまり、最終手段のコストの高いルート）を取得していない場合でも、スタティック仮想パスルートを作成して、トラフィックを仮想パスに強制することもできます。SD-WAN は、仮想 IP アドレス (VIP) をプライベートにすることで、ローカルサブネットのアドバタイズを抑制することもできます。



> 注
>
> 設定では、各ルートドメインに少なくとも 1 つの非プライベート VIP が必要です。

イントラネットとインターネットルート

イントラネットサービスタイプおよびインターネットサービスタイプでは、これらのタイプのサービスをサポートするために SD-WAN リンクを定義しておく必要があります。これは、これらのサービスのいずれかに定義されたルートのための前提条件です。WAN リンクがイントラネットサービスをサポートするように定義されていない場合、WAN リンクはローカルルートと見なされます。イントラネット、インターネット、パススルールートは、構成されているサイト/アプライアンスにのみ関連します。

イントラネット、インターネット、またはパススルールートを定義する場合、設計上の考慮事項は次のとおりです。

- WAN リンクにサービスが定義されている必要があります (イントラネット/インターネット—必須)
- イントラネット/インターネットには、WAN リンク用に Gateway が定義されている必要があります。

- ローカル SD-WAN デバイスに関連します
- イントラネット・ルートは仮想パスを介して学習できますが、それは高コストで学習できます
- インターネットサービスでは、自動的にデフォルトルートが作成され（0.0.0.0/0）、最大コストですべてのルートをキャッチします
- パススルーが動作すると仮定しないでください。テスト/検証する必要があります。また、仮想パスをダウン/無効にしてテストして目的の動作を確認します
- ルートテーブルは、ルート学習機能が有効でない限り、スタティックです

次に、複数のルーティングパラメータでサポートされる最大制限を示します。

- 最大ルーティングドメイン:255
- WAN リンクあたりの最大アクセスインターフェイス:64
- サイトあたりの BGP ネイバーの最大数：255
- サイトあたりの最大 OSPF エリア:255
- OSPF エリアあたりの仮想インターフェイスの最大数:255
- サイトあたりのルートラーニングインポートフィルタの最大数:512
- サイトあたりのルートラーニングエクスポートフィルタの最大数:512
- BGP ルーティングポリシーの最大数:255
- BGP コミュニティストリングオブジェクトの最大数：255

ルーティングドメイン

May 10, 2021

Citrix SD-WAN では、ルーティングドメインを使用することにより、ネットワークのセグメント化によりセキュリティと管理が容易になります。たとえば、ゲストネットワークトラフィックを従業員のトラフィックから分離したり、大規模な企業ネットワークをセグメント化するために個別のルーティングドメインを作成したり、トラフィックをセグメント化して複数のカスタマーネットワークをサポートしたりできます。各ルーティングドメインには独自のルーティングテーブルがあり、IP サブネットのオーバーラップをサポートできます。

Citrix SD-WAN アプライアンスは、ルーティングドメイン用の OSPF および BGP ルーティングプロトコルを実装し、ネットワークトラフィックを制御およびセグメント化します。

仮想パスは、アクセスポイントの定義に関係なく、すべてのルーティングドメインを使用して通信できます。これは、SD-WAN カプセル化にパケットのルーティングドメイン情報が含まれているためです。したがって、両方のエンドネットワークは、パケットがどこに属しているかを認識します。ルーティングドメインごとに WAN リンクまたはアクセスインターフェイスを作成する必要はありません。

ルーティングドメイン機能を設定するときに考慮すべきポイントのリストを次に示します。

- デフォルトでは、ルーティングドメインは MCN で有効になっています。
- ルーティングドメインは、ブランチサイトで有効になります。
- 有効な各ルーティングドメインには、仮想インターフェイスと仮想 IP が関連付けられている必要があります。
- ルーティングの選択は、次のすべての設定の一部です。
  - インターフェイスグループ
  - 仮想 IP
  - GRE
  - WAN リンク-> アクセスインターフェイス
  - IPSec トンネル
  - ルート
  - 規則
- ルーティングドメインは、複数のドメインが作成された場合に限り、Web インターフェイス設定で公開されます。
- パブリックインターネットリンクの場合、作成できるプライマリアクセスインターフェイスとセカンダリアクセスインターフェイスは 1 つだけです。
- プライベートイントラネット/MPLS リンクの場合、ルーティングドメインごとに 1 つのプライマリおよびセカンダリアクセスインターフェイスを作成できます。

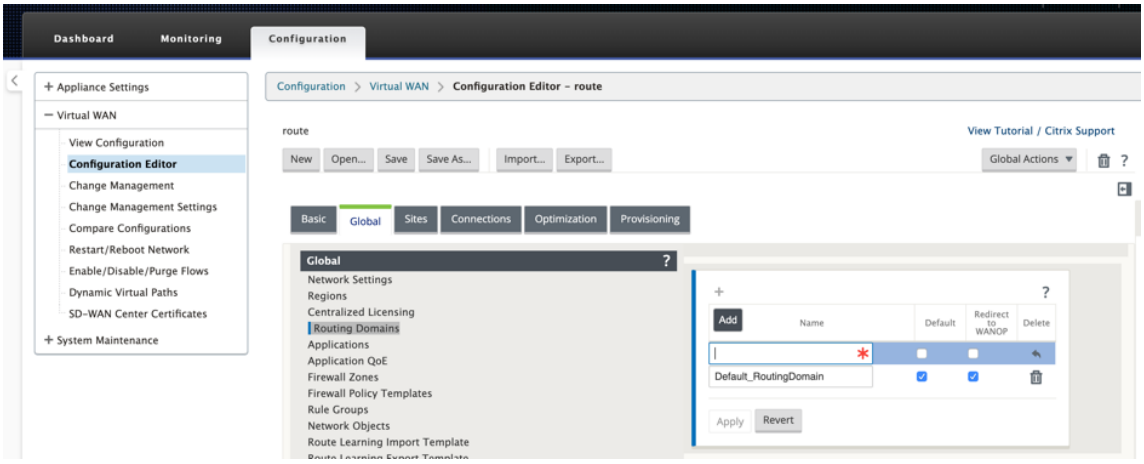
ルーティングドメインの構成

May 10, 2021

Citrix SD-WAN アプライアンスは、ルーティングプロトコルを構成して、企業ネットワーク、支店ネットワーク、データセンターネットワークを管理するための単一の管理ポイントを提供します。最大 254 個のルーティングドメインを設定できます。

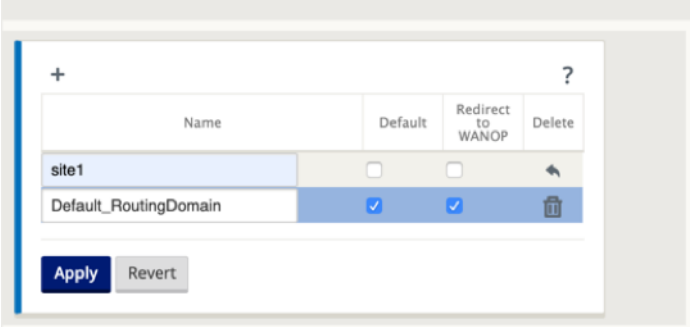
ルーティングドメインを構成するには、次の手順を実行します。

1. SD-WAN Web インターフェイスで、[構成] > [仮想 **WAN**] > [構成エディタ] に移動します。構成エディターで、「グローバル」>「ルーティングドメイン」に移動し、「追加」**(+)** をクリックして、新しいルーティングドメインの名前を入力します。



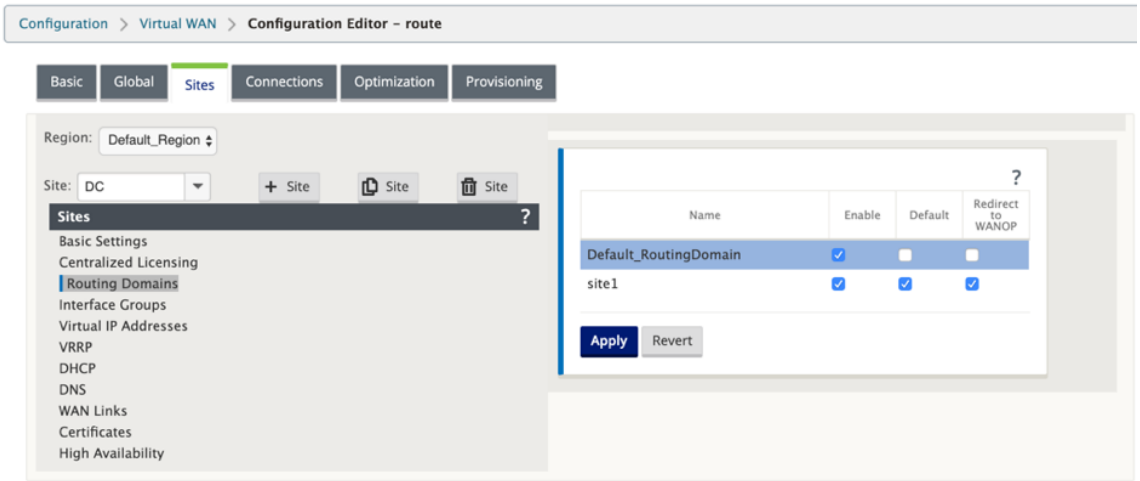
2. このルーティングドメインをデフォルトに設定する場合は、[デフォルト] チェックボックスをオンにします。[適用] をクリックして変更を保存します。単一のルーティングドメインを実装する場合は、明示的な設定は必要ありません。

   すべての新しい設定には、デフォルトのルーティングドメインが自動的に設定されます。



3. 「サイト」→「**[**クライアントサイト名**]** 」>「ルーティングドメイン」に移動します。[**Enable**] チェックボックスをクリックして、サイトに対して構成済みのルーティングドメインを有効にします。

4. [デフォルト] チェックボックスをクリックして、そのルーティングドメインをサイトのデフォルトにします。[適用] をクリックして変更を保存します。



> 注
>
> 「ルーティングドメインに対して 有効 にする」をオフにすると、サイトで使用できなくなります。

11.0.2 リリースでは、ルーティング可能な仮想 **IP**（**VIP**）を持たないルーティングドメイン は、次の機能で許可されます。

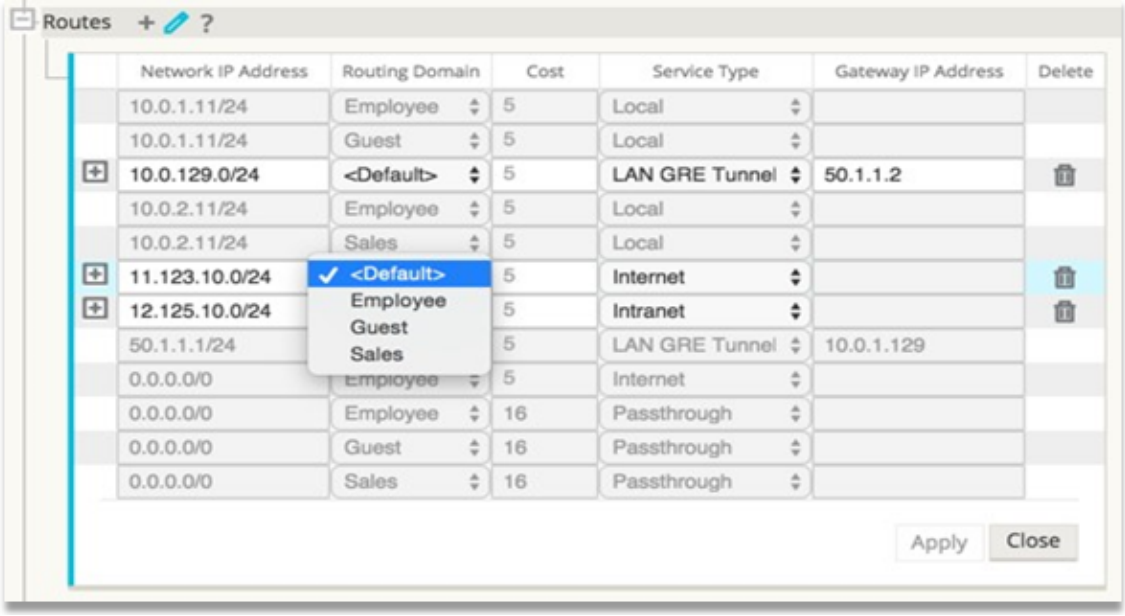
- デバイスに、信頼できないインターフェイスまたはインターフェイスがないルーティングドメインを持たせるようにします。
- 中間サイトに物理的な存在がないルーティングドメインを介して、ブランチが相互に通信できるようにします。

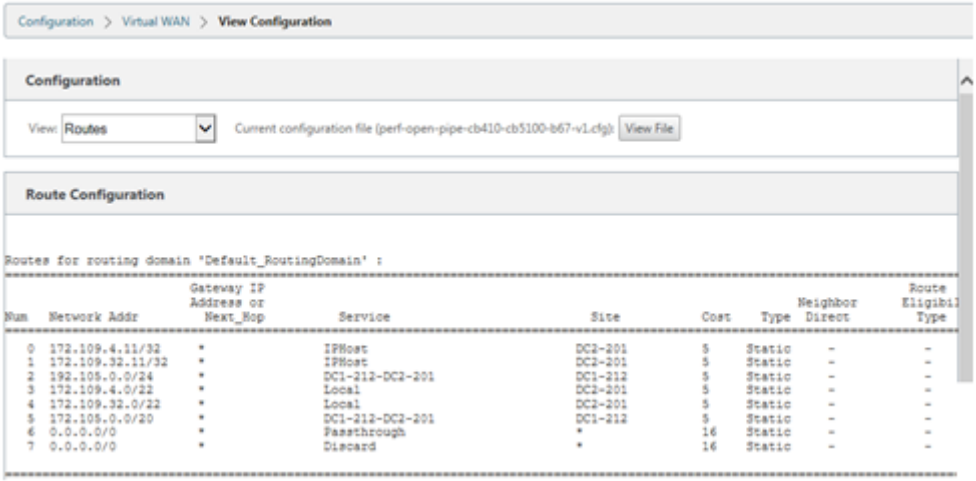
ルートの設定

May 10, 2021

ルートを構成するには、次の手順に従います。

1. 構成エディタで、**[**接続] > [**[**サイト名**]**] > [ルート] に移動します。
2. ドロップダウンメニューから ルーティングドメイン を選択します。新しいルートは、デフォルトのルーティングドメインに自動的に関連付けられます。詳細な手順については、ルートの設定を参照してください。





ルートを設定したら、[構成] > [仮想 **WAN**] > [表示] > [ルート] に移動して、設定 済みのルーティングドメインのルートテーブルを検証します。

CLI を使用してルーティングにアクセスする

May 10, 2021

Citrix SD-WAN リリースバージョン 10.0 では、動的ルーティングとプロトコルの状態に関連する追加情報を表示できます。次のコマンドと構文を入力して、ルーティングデーモンにアクセスし、コマンドの一覧を表示します。

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

動的ルーティング

May 10, 2021

Citrix SD-WAN では、次の 2 つの動的ルーティングプロトコルがサポートされています。

- Open Shortest Path First (OSPF)
- Border Gateway Protocol（BGP）

OSPF

OSPF は、Internet Engineering Task Force (IETF) の Interior Gateway Protocol (IGP) グループによってインターネットプロトコル (IP) ネットワーク向けに開発されたルーティングプロトコルである。これは、OSI の中間シ

ステム（IS-IS）ルーティングプロトコルの初期バージョンが含まれています。

OSPF プロトコルはオープンです。つまり、その仕様はパブリックドメイン（RFC 1247）にあります。OSPF は、ダイクストラと呼ばれる最短パスファースト (SPF) アルゴリズムに基づいています。これは、リンクステートルーティングプロトコルで、同じ階層領域内の他のすべてのルータに Link-State Advertising（LSA; リンクステートアドバタイズメント）を送信するようコールします。接続されているインターフェイス、使用されるメトリック、およびその他の変数に関する情報は、OSPF LSA に含まれます。OSPF ルータは、各ノードへの最短パスを計算するために SPF アルゴリズムによって使用されるリンクステート情報を蓄積します。

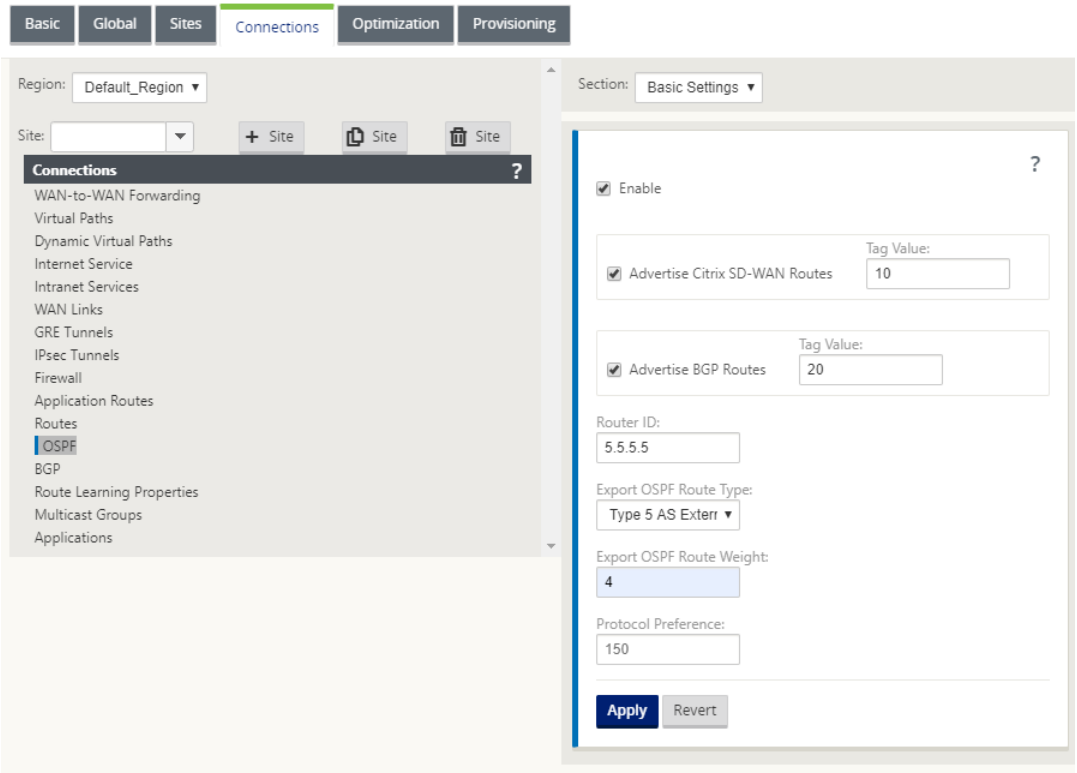
Citrix SD-WAN アプライアンス（Standard Edition と Premium （Enterprise）Edition）を構成して、OSPF を使用してルートを学習し、ルートをアドバタイズできるようになりました。

> 注
>
> - Citrix SD-WAN アプライアンスは、デフォルトの DR 優先順位が「0」に設定されているため、各マルチアクセスネットワーク上で代表ルータ（DR）および BDR（バックアップ代表ルータ）として参加しません。
> - Citrix SD-WAN アプライアンスは、エリア境界ルータ（ABR）としての要約をサポートしていません。

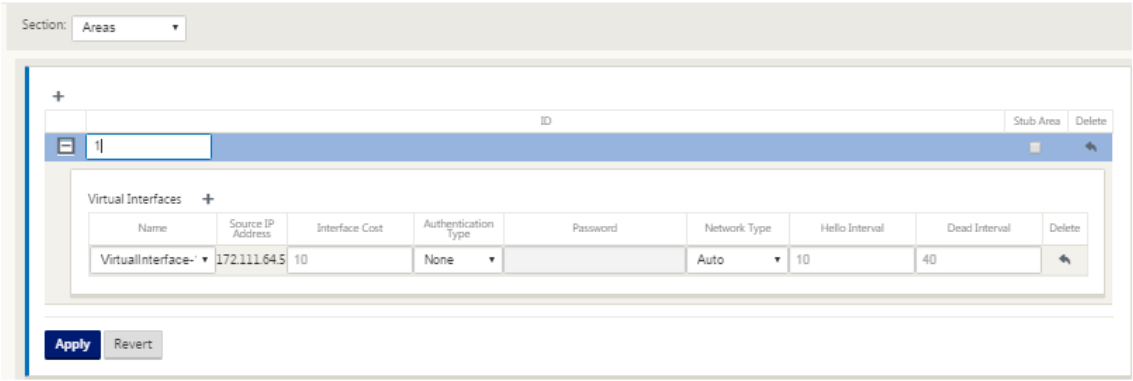
OSPF の設定

OSPF を設定するには、次の手順を実行します。

1. 構成エディタで、[接続**] > [**リージョン**] > [**サイト**] > [OSPF] > [**基本設定**]** に移動します。
2. 「有効化」(Enable) をクリックし、次のパラメータを選択または入力して、「適用」**(Apply**) をクリックします。
   - **Citrix SD-WAN** ルートのアドバタイズ：OSPF 経由で Citrix SD-WAN ルートをアドバタイズできるようにします。OSPF 再配布用のタグを指定することもできます。
   - **BGP** ルートのアドバタイズ：BGP ピアから学習したルートを OSPF 経由でアドバタイズできるようにします。OSPF 再配布用のタグを指定することもできます。
   - ルータ **ID**：一意のルータ ID。ルータは OSPF アドバタイズメントに使用されます。ルータ ID が指定されていない場合は、SD-WAN ネットワークでホストされている最下位の仮想 IP として自動的に選択されます。
   - **OSPF** ルートタイプのエクスポート：Citrix SD-WAN ルートをエリア内ルートまたは外部ルートとして OSPF ピアにアドバタイズします。
   - **OSPF** ルート重みのエクスポート：Citrix SD-WAN ルートを OSPF にエクスポートする場合、この重みを各ルートの Citrix SD-WAN コストに追加します。
   - **Protocol Preference**：プレフィクスが複数のルーティングプロトコルによって学習される場合、プロトコルプリファレンス値によってルーティングプロトコルの選択が決定されます。詳しくは、「プロトコルプリファレンス」を参照してください。



3. [**OSPF**] → [エリア] を展開し、[編集] をクリックします。



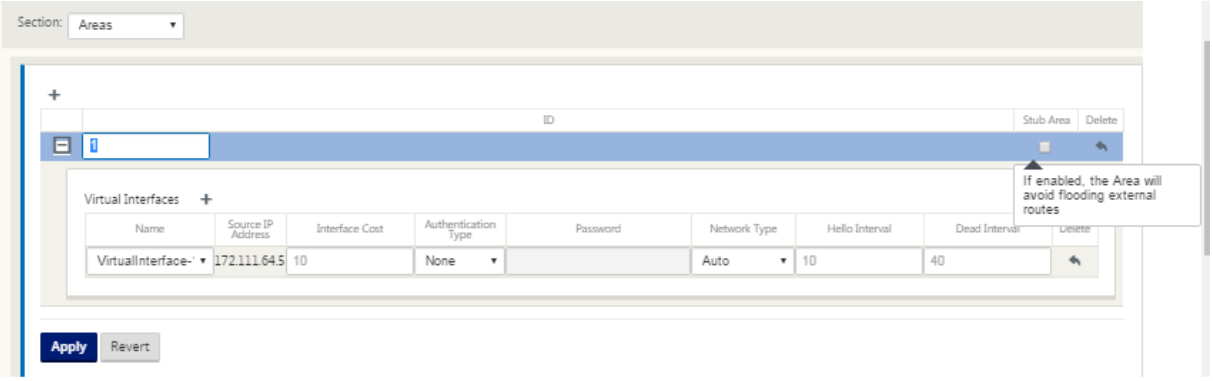
4. ルートを学習し、アドバタイズする エリア **ID** を入力します。
5. 特定の仮想 IP アドレスの ID がチェックされていない場合、関連付けられた仮想インターフェイスは IP サービスで使用できません。
6. [**Name**] メニューから使用可能な仮想インターフェイスを 1 つ選択します。仮想インターフェイスは、送信元 **IP** アドレスを決定します。
7. インタフェース・コスト を入力します（デフォルトは 10 です）。
8. メニューから「認証タイプ」を選択します。
9. 手順 8 で「パスワード」または「**MD5** 」を選択した場合は、「パスワード関連テキスト」フィールドに入力します。

10. [**Hello Interval**] フィールドに、直接接続されたネイバーに Hello プロトコルパケットを送信するまでの待機時間を入力します（デフォルトは 10 秒）。
11. [**Dead Interval**] フィールドに、ルータをデッドとしてマークするまでの待機間隔を入力します。デフォルトのデッドインターバルは 40 秒です。
12. ［適用］をクリックして変更を保存します。

スタブエリア

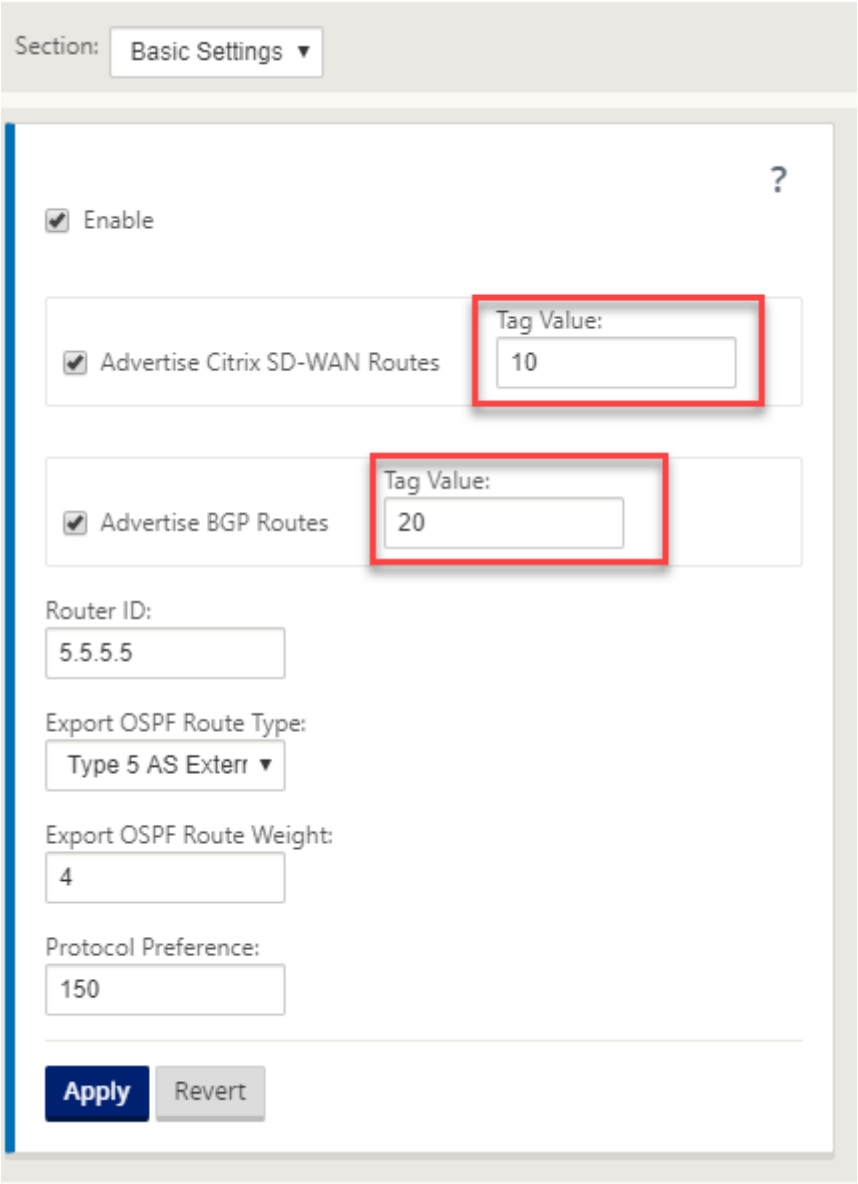
スタブエリアは外部ルートからシールドされ、同じ OSPF ドメインの他のエリアに属するネットワークに関する情報を受信します。

[スタブエリア] チェックボックスをオンにします。



OSPF 再配布タグ

OSPF タグを使用すると、OSPF と他のプロトコル間の相互再配布中にルーティングループが発生しないようにできます。OSPF ドメインで、同じサブネットへの SD-WAN および BGP で学習されたルートがある場合、OSPF ループ防止メカニズムはそのルートをループとして識別し、ルートを無視します。SD-WAN ルートと BGP 学習ルートに異なるタグを指定すると、これらのルートを OSPF ルーティングテーブルにインストールできます。
SD-WAN および BGP を通じて学習されたルートの OSPF 再配布タグは、[OSPF の基本設定] セクションで設定 できます。



BGP

BGP は、自律システム間ルーティングプロトコルです。自律ネットワークまたはネットワークのグループは、共通の管理下および共通のルーティングポリシーで管理されます。BGP は、インターネットのルーティング情報を交換するために使用され、ISP 間で使用されるプロトコルです。カスタマーネットワークは、RIP や OSPF などの内部 Gateway プロトコルを展開して、ネットワーク内のルーティング情報を交換します。カスタマーは ISP に接続し、ISP は BGP を使用してカスタマーと ISP のルートを交換します。自律システム（AS）間で BGP を使用する場合、プロトコルは External BGP（EBGP）と呼ばれます。サービスプロバイダーが BGP を使用して AS 内でルートを交換している場合、このプロトコルは Interior BGP（IBGP）と呼ばれます。

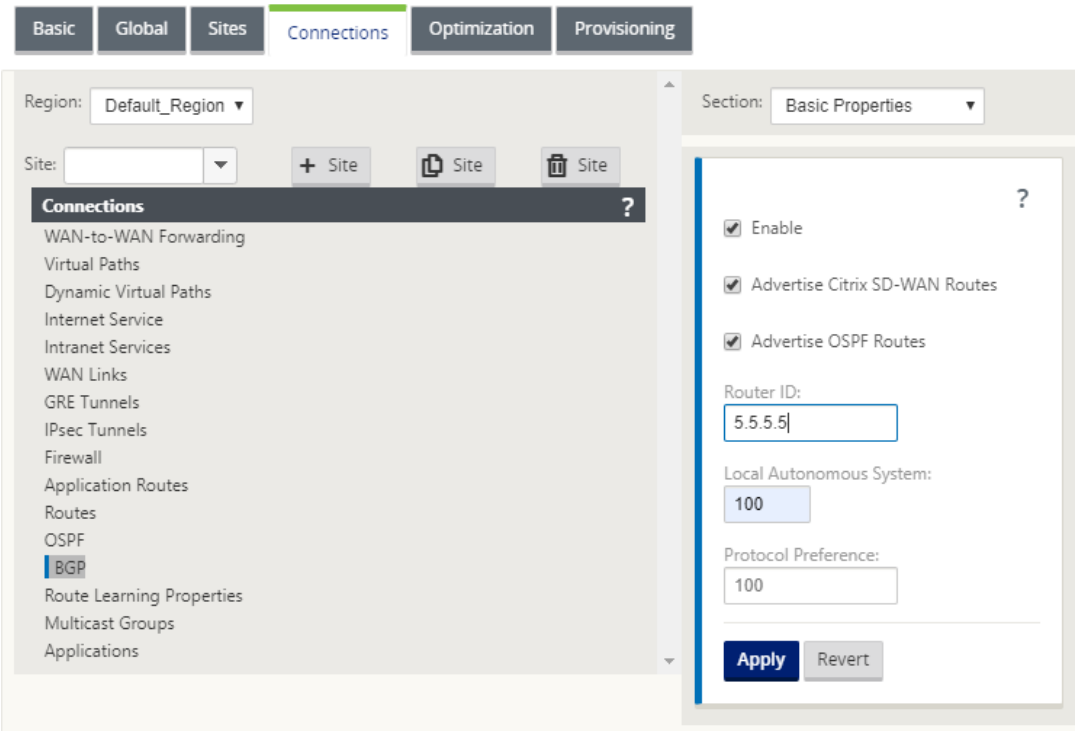
BGP は、インターネット上に展開される堅牢でスケーラブルなルーティングプロトコルです。スケーラビリティを実

現するために、BGP は属性と呼ばれる多数のルートパラメータを使用して、ルーティングポリシーを定義し、安定したルーティング環境を維持します。BGP ネイバーは、ネイバー間の TCP 接続が最初に確立されたときに、完全なルーティング情報を交換します。ルーティングテーブルへの変更が検出されると、BGP ルータは、変更されたルートだけをネイバーに送信します。BGP ルータは定期的なルーティングアップデートを送信せず、宛先ネットワークへの最適パスのみをアドバタイズします。ルートを学習し、BGP を使用してルートをアドバタイズするように、Citrix SD-WAN アプライアンスを構成できます。

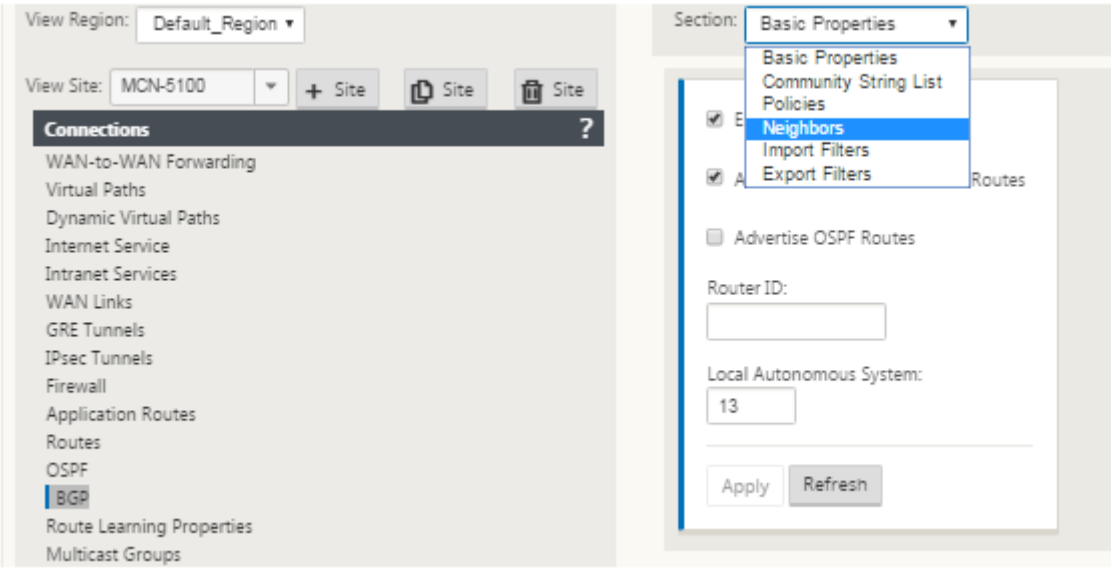
BGP の設定

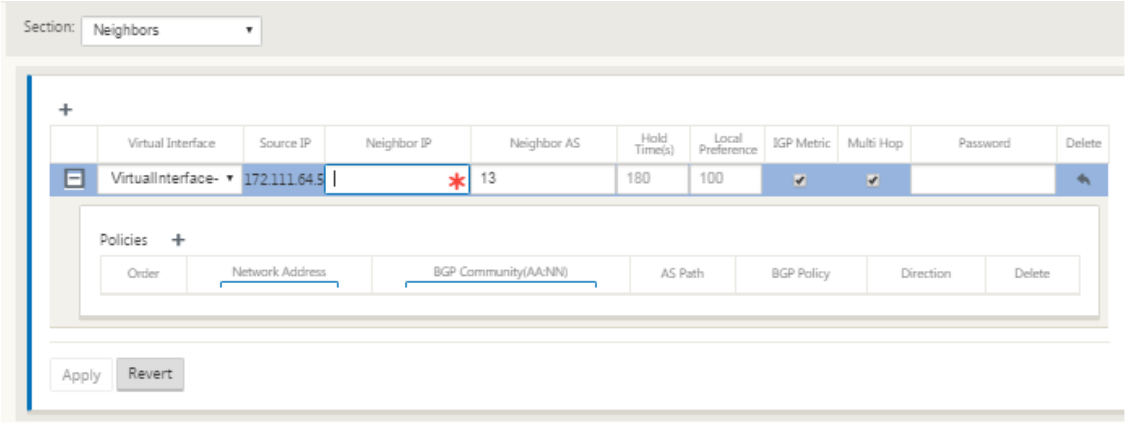
BGP を設定するには、次の手順を実行します。

1. 構成エディタで、[接続**] > [**リージョン**] > [**サイト**] > [BGP] > [**基本設定**]** に移動します。
2. 「有効化」(Enable) をクリックし、次のパラメータを選択または入力して、「適用」**(Apply**) をクリックします。
   - **Citrix SD-WAN** ルートのアドバタイズ：BGP 経由で Citrix SD-WAN ルートをアドバタイズできるようにします。
   - **OSPF** ルートのアドバタイズ：OSPF ピアから学習したルートを BGP 経由でアドバタイズできるようにします。
   - ルータ **ID**：一意のルータ ID。ルータは OSPF アドバタイズメントに使用されます。ルータ ID が指定されていない場合は、SD-WAN ネットワークでホストされている最下位の仮想 IP として自動的に選択されます。
   - ローカル自律システム：ルートが学習され、アドバタイズされるローカル自律システム番号。自律システム番号は、ネイバールータ上の自律システム番号と一致する必要があります。
   - **Protocol Preference**：プレフィクスが複数のルーティングプロトコルによって学習される場合、プロトコルプリファレンス値によってルーティングプロトコルの選択が決定されます。詳細については、「プロトコルプリファレンス」を参照してください。



3. [基本設定] **>** [ネイバー] を展開し、[追加] **(+)** アイコンをクリックします。





複数のルーティングドメインを持つサイトの場合、ルーティングドメインを選択します。ルーティングドメインは、使用可能な仮想インターフェイスを決定します。

4. メニューから 仮想インターフェイスを 選択します。仮想インターフェイスによって送信元 IP アドレスが決定されます。
5. [ネイバー **IP]** フィールドに **IBGP** ネイバールータの **IP** アドレスを、[ネイバー AS] フィールドにローカル自律システム 番号を入力します。
6. [**Hold Time (s)**] フィールドに、ネイバーがダウンしたと宣言されるまでの待機時間を秒単位で入力します（デフォルトは 180）。
7. [**Local Preference (s)**] フィールドに、複数の BGP ルートからの選択に使用される Local Preference 値を秒単位で入力します（デフォルトは 100）。
8. [**IGP Metric**] チェックボックスをクリックして、内部距離の比較を有効にして、最適ルートを計算します。
9. [**Multi-hop**] チェックボックスをオンにして、ルートの複数のホップを有効にします。
10. [**P** assword] フィールドに、BGP セッションの MD5 認証用のパスワードを入力します（認証は不要です）。

> 注
>
> iBGP のルートリフレクタおよびコンフェデレーションの設定は、SD-WAN ネットワークではサポートされていません。

外部 **BGP**（**eBGP**）

Citrix SD-WAN アプライアンスは、LAN 側のスイッチ、WAN 側のルーターに接続します。SD-WAN テクノロジーが企業のネットワーク展開に不可欠になり始めるにつれ、SD-WAN アプライアンスがルーターを置き換えます。SD-WAN は eBGP ダイナミックルーティングプロトコルを実装して、専用のルーティングデバイスとして機能します。

SD-WAN アプライアンスは、eBGP を使用して WAN 側へのピアルータとのネイバーシップを確立し、ピアとの間でルートを学習し、アドバタイズできます。eBGP 学習ルートのインポートとエクスポートは、ピアデバイス上で選

択できます。また、SD-WAN スタティック、仮想パスラーニングされたルートを eBGP ピアにアドバタイズするように設定することもできます。

詳細については、次のユースケースを参照してください。

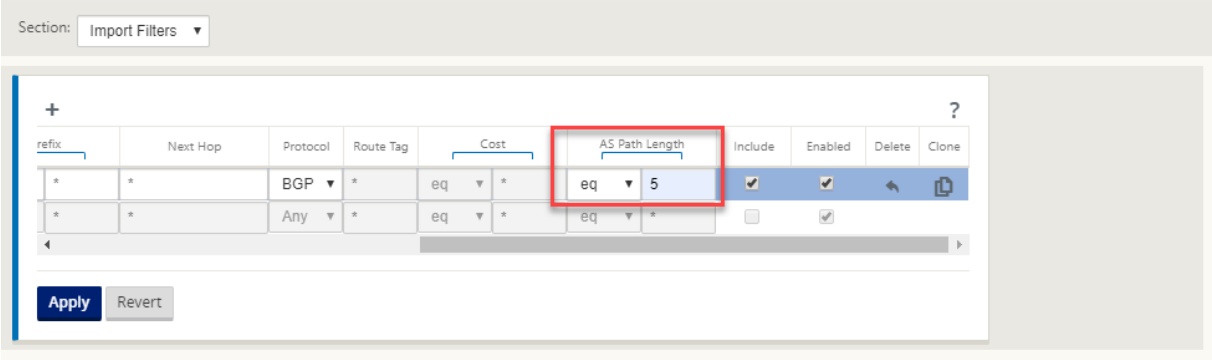
- eBGP 経由で非 SD-WAN サイトと通信する SD-WAN サイト
- 仮想パスと eBGP を使用した SD-WAN サイト間の通信
- ワンアームトポロジでの OSPF の実装
- MPLS ネットワークでの OSPF タイプ 5 からタイプ 1 への配置
- SD-WAN および非 SD-WAN（サードパーティ）アプライアンスの OSPF 展開
- 高可用性セットアップで SD-WAN ネットワークを使用した OSPF の実装

AS パスの長さ

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

非 SD-WAN アプライアンスは、AS パスの長さに基づいてルートをインポートすることにより、トラフィックをプライマリ DC またはセカンダリ DC SD-WAN アプライアンスにルーティングできます。また、ルータ上のプライマリ DC アプライアンスの AS パス長を増やすだけで、ルータからセカンダリ DC へのトラフィックを動的に誘導することもできます。ルートコストを変更し、設定の更新を実行する必要がなくなります。

インポートフィルタで AS パス長を設定するには、プロトコルとして BGP を選択し、述語を選択して **AS** パス長を入力します。詳しくは、「ルートフィルタリング」を参照してください。



ルート統計情報のモニタリング

[モニタ] > [統計] に移動します。[表示] ドロップダウンメニューから [ルート] を選択します。

Citrix SD-WAN ネットワークでは、ルートが動的か静的かに関係なく、該当するルートのすべての機能がサポートされています。

Monitoring > Statistics

Statistics

Show: Routes | Enable Auto Refresh | 5 seconds | Refresh | Clear Counters on Refresh | Purge dynamic routes

Route Statistics

Maximum allowed routes: 16000

Routes for routing domain : Default_RoutingDomain

Filter: in Any column Apply

Show 100 entries Showing 1 to 28 of 28 entries First Previous 1 Next Last

Num	Network Addr	Gateway IP Address	Service	Reachable	Site IP Address	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
0	115.1.1.0/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
1	115.168.0.16/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
2	115.168.0.12/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
3	115.168.0.8/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
4	115.168.0.4/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
5	115.168.0.0/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
6	115.14.14.0/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
7	115.13.13.0/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
8	115.12.12.0/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
9	115.10.10.0/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
10	115.9.9.16/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
11	115.8.8.12/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
12	115.7.7.8/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
13	115.6.6.4/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
14	115.5.5.0/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
15	115.4.4.0/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
16	115.3.3.0/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
17	115.2.2.0/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
18	182.120.1.0/24	*	Local	YES	*	pod2_DC	Static	-	-	5	0	YES	N/A	N/A
19	172.120.1.0/24	*	Local	YES	*	pod2_DC	Static	-	-	5	0	YES	N/A	N/A
20	182.120.2.0/24	*	pod2_DC-pod3_Br	YES	*	pod3_Br	Static	-	-	5	0	YES	N/A	N/A
21	172.120.2.0/24	*	pod2_DC-pod3_Br	YES	*	pod3_Br	Static	-	-	5	0	YES	N/A	N/A
22	182.120.0.0/24	*	pod2_DC-pod1_Br	YES	*	pod1_Br	Static	-	-	5	0	YES	N/A	N/A
23	172.120.0.0/24	*	pod2_DC-pod1_Br	YES	*	pod1_Br	Static	-	-	5	0	YES	N/A	N/A
24	192.120.1.0/24	172.120.1.2	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	75612	YES	N/A	N/A
25	192.120.0.0/24	*	pod2_DC-pod1_Br	YES	*	pod1_Br	Dynamic	Virtual WAN	YES	6	75612	YES	N/A	N/A
26	0.0.0.0/0	*	Passthrough	YES	*	*	Static	-	-	16	0	YES	N/A	N/A
27	0.0.0.0/0	*	Discard	YES	*	*	Static	-	-	16	0	YES	N/A	N/A

Showing 1 to 28 of 28 entries First Previous 1 Next Last

OSPF

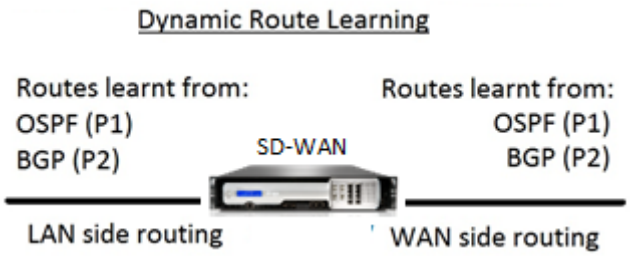
May 10, 2021

LAN 側：ダイナミックルートラーニング

ゲートウェイモードで展開された Citrix SD-WAN アプライアンスの LAN ポートで実行されている OSPF:

Citrix SD-WAN アプライアンスは、必要なルーティングプロトコル（OSPF および BGP）ごとに、ローカルカスタマーネットワーク（ブランチとデータセンターの両方）内でレイヤー 3 ルーティングアドバタイズメントのルート検出を実行します。学習されたルートは動的にキャプチャされ、表示されます。

これにより、SD-WAN 管理者は、SD-WAN ネットワークの一部である各アプライアンスの LAN 側のネットワーク環境を静的に定義する必要がなくなります。



WAN 側**:** ダイナミックルート共有

タイプ 5 AS-外部 LSA の学習を制限することにより、STUB エリアとして定義されたエリアを持つ Citrix SD-WAN アプライアンス。

Citrix SD-WAN アプライアンスは、ローカルで学習された動的ルートを MCN でアドバタイズできます。MCN は、これらのルートをネットワーク内の他の SD-WAN アプライアンスに中継できます。この情報を動的に交換することで、変化するネットワーク全体でサイト間の接続を維持できます。

OSPF 展開モード

以前のリリースでは、SD-WAN からの OSPF インスタンス学習ルートは、タイプ 5 LSA のみの外部ルートとして扱われていました。これらのルートは、タイプ 5 外部 LSA のネイバールータにアドバタイズされました。その結果、SD-WAN ルートは、OSPF パス選択アルゴリズムに従って、あまり優先されないルートになりました。

最新リリースでは、SD-WAN はルートをエリア内ルート（LSA タイプ 1）としてアドバタイズし、OSPF パス選択アルゴリズムを使用してルートコストに従って優先権を取得できるようになりました。ルートコストを設定し、ネイバールータにアドバタイズできます。これにより、SD-WAN アプライアンスを以下に説明するワンアームモードで展開できます。

ワンアームトポロジでの **OSPF** の実装

ワンアーム設定では、OSPF 配置でルータに複雑な PBR または WCCP 設定が必要です。デフォルトのエクスポートルートタイプをタイプ 5 からタイプ 1 に変更することで、この展開を簡素化できます。SD-WAN ルートがコストの

少ないエリア内ルートとしてアドバタイズされ、SD-WAN アプライアンスがアクティブになると、ネイバールータは SD-WAN ルートを選択し、SD-WAN ネットワーク経由のトラフィックの転送を自動的に開始します。PBR または WCCP の追加設定は不要です。

前提条件:

- DC サイトおよびブランチサイトの SD-WAN アプライアンスは、最新のリリースバージョンを実行している必要があります。
- エンドツーエンドの IP 接続を構成し、正常に動作する必要があります。
- OSPF はすべてのサイトで有効になっています。

OSPF タイプ 1 を設定するには、次の手順を実行します。

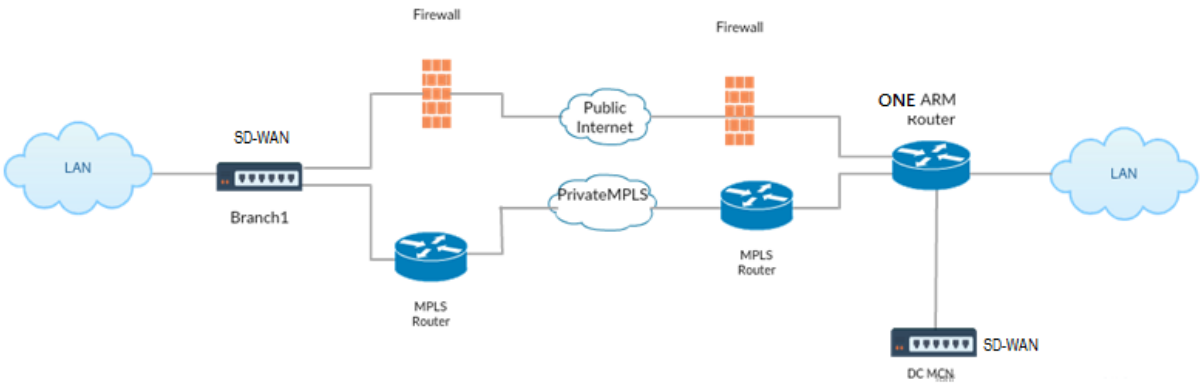
1. DC サイトとブランチサイトの両方で 仮想インターフェイス と **WAN** リンク を設定し、それらの間に仮想パスを作成できるようにします。
2. [接続] >[**MCN**] > [ルート学習] > [**OSPF**] > [基本設定] で、[**OSPF** ルートタイプを **** タイプ **1** イントラエリア としてエクスポート **] を選択します。
3. 構成を保存し、ステージングし、構成をアクティブにします。

[
OSPF ルートタイプのエクスポート] で、次のルートタイプが表示されている必要があります。

- タイプ 5 AS 外部
- タイプ 1 イントラエリア

タイプ **5 AS** 外部ルートを設定できる必要があります。

変更された設定をアクティブ化した後、**[**設定**]** > **[** 仮想 **WAN]** > **[** 設定の表示**]** > **[** ダイナミックルーティング**]** で、ルートタイプの変更を確認する必要があります。

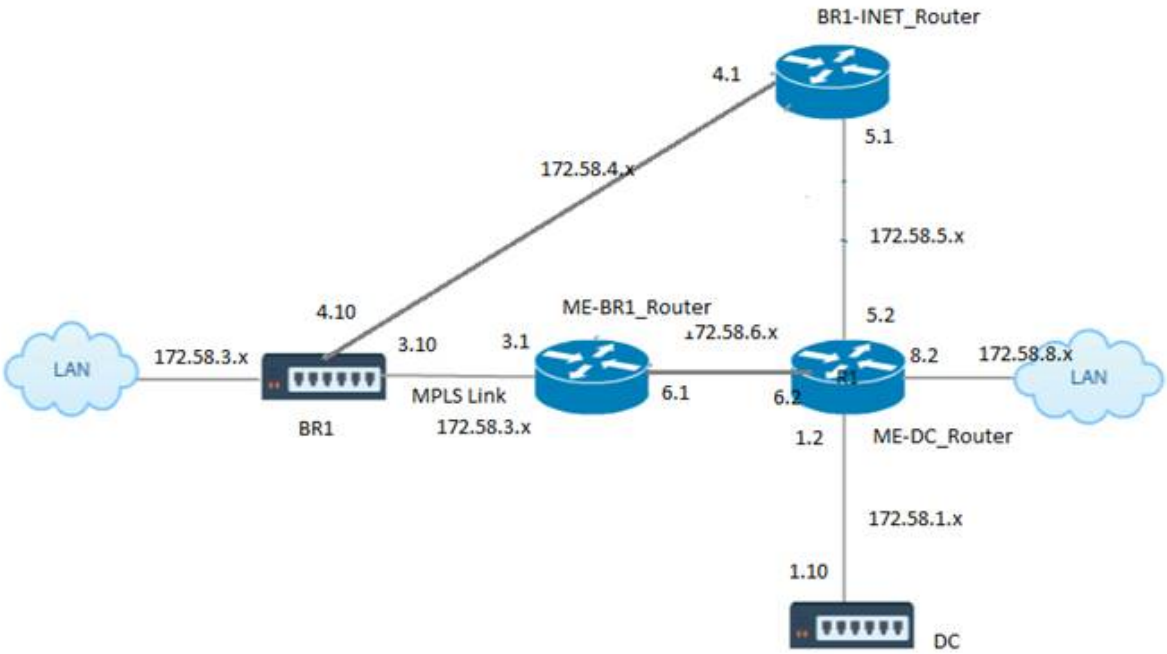


上の図に示すように、DC MCN はワンアームトポロジで展開されます。DC サイトがアップしている場合、ワンアームルータは、ローカル LAN から他のサイト（たとえば、宛先 IP アドレスが同じサブネット内にある支店のローカル LAN など）にすべてのトラフィックを転送します。次に、SD-WAN アプライアンスはすべてのパケットをラップし、すべてのパケット宛先 IP でルータに送信します。アドレスを、ブランチ仮想 IP アドレスに入力します。ルータは、これらのパケットを WAN に転送します。

DC サイトがダウンしている場合、ルータは、ローカル LAN から他のサイト（ブランチサイトのローカル LAN、宛先 IP はサブネット内）へのすべてのトラフィックを SD-WAN アプライアンスではなく、直接 WAN に転送します。

MPLS ネットワークにおける **OSPF** タイプ **5** からタイプ **1** への配置

SD-WAN アプライアンスを使用して設定された MPLS ネットワークでのループ形成を回避するために、次の展開モードが用意されています。次の図は、標準的な MPLS ネットワーク実装を示しています。



上の図では、次のようになります。

- OSPF は、エリア 0 の *ME-BR1_router* と *ME-DC_router* の間で設定されます。
- OSPF は、エリア 0 の *ME-DC_router* と *DC* の間で設定されます。

推奨構成**:**

- エリア 0 上の DC VW および ME-DC_Router
- エリア 0 上の ME-BR1_Router および ME-DC_Router
- エリア 0 上の BR1 VW および ME-BR1_Router

Me-DC_Router では、次の操作を行います。

1. 172.58.3.10/32（MPLS リンク用の BR1 の仮想 IP）から 172.58.6.1 までのスタティックルートを追加
2. 172.58.4.10/32（INET 用 BR1 の仮想 IP）から 172.58.5.1 までのスタティックルートを追加

スタティックルートを追加すると、ME-DC_router と DC SD-WAN アプライアンスの間のループ形成を防ぐことができます。スタティックルートを追加しない場合、MCN は ME-DC Router にトラフィックを転送し、ルータから MCN に戻して、ループを継続的に作成します。

PBR ルートではなく、宛先ホスト IP ベースのルートであるスタティックルートは、選択したパスおよびその後実行されるカプセル化に基づいて DC 側から選択される正しいリンクに向かって通過します。したがって、これらのスタティックルートが設定されている場合、BR1 SD-WAN アプライアンスの任意の宛先仮想 IP を持つカプセル化されたパケットは、DC MCN によって選択された最適パスに従ってこれらのリンクを使用します。

IPHOST ルートがインストールされている場合（スタティック仮想 IP が設定されていない場合）、ループ形成を回避するために ACL を追加します。

- BR1 SD-WAN アプライアンスによってアドバタイズされる IPHOST ルートが MCN ルータ *ME-DC_Router* によってインストールされ、上記のようにスタティックルートとして追加されていない場合、ME-BR1_Router と ME-DC_Router 間の OSPF 参加インターフェイス（172.58.6.x）がダウンすると、ループが形成される可能性があります。これは、このインターフェイスがダウンしていると、IPHOST ルートが ME-DC_router のルーティングテーブルからフラッシュされるためです。
- この場合、MCN は BR1 VIP 宛てのカプセル化されたパケットを ME-DC ルータに転送し、ルータから MCN に戻してループを継続的に行います。

ME-BR1_Router では、次のようにします。

ME-BR1_Router <-> ME-DC_router と **ME-DC_Router <-> DC**（**SD-WAN**）の間で同じ **AREA-ID** が使用されている場合、**DC** によって同じネットワークに対してアドバタイズされたコストよりも高いコストで **172.58.3.x** ネットワークを **ME-DC_Router** にアドバタイズします。

- OSPF 10^8/BW のコストメトリック計算に基づいて、ルートプレフィクスのコストはインターフェイスタイプに基づいています。SD-WAN アプライアンスは、デフォルトの SD-WAN コストが 5 で、仮想パスと仮想 WAN 固有のスタティックルートを外部ルータまたはピアルータにアドバタイズします。
- ME-BR1_router が 172.58.3.0/24 を内部 OSPF タイプ 1 ルートとして DC（SD-WAN）とともにアドバタイズし、内部 OSPF タイプ 1 ルートと同じプレフィクスをアドバタイズする場合、コスト計算に従って、デフォルトで ME-BR1_router のルートが設定されます。これは、コストが SD-WAN のデフォルトのコストは 5 です。これを回避し、SD-WAN アプライアンスを最初に優先ルートとして選択するには、ME-BR1_Router で上位になるようにインターフェイスコスト（172.58.3.1）を操作して、DC SD-WAN ルートが ME-DC_router のルーティングテーブルで設定されるようにする必要があります。

これにより、DC SD-WAN アプライアンスに障害が発生しても、ME-BR1_router を次の優先 Gateway として使用する代替ルートによって、中断のないトラフィックフローが保証されます。

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

このルートを使用すると、DC SD-WAN は、カプセル解除後に LAN サブネットを認識しているアップストリームルータにパケットを送信できます。DC SD-WAN がダウンした場合、レガシールーティングインフラストラクチャは、

ME-BR1_router が 172.58.8.x ネットワークに到達するネクストホップとして ME-DC_router を使用するのに役立ちます。

OSPF エクスポートされたルートを [基本 **OSPF** 設定] で Type1 として設定するには、次の手順を実行します。

1. DC サイトとブランチサイトの両方で仮想インターフェイスと **WAN** リンクを構成して、それらの間に仮想パスを作成します。
2. **[**接続**]**>[**MCN**]>**[**ルート学習**]>[OSPF]>[**基本設定**]** で、**[OSPF** ルートタイプのエクスポート**]** で **[**タイプ **1** イントラエリア**]** を選択します。
3. 設定、ステージを保存し、同じことをアクティブにします。[**OSPF** ルートタイプのエクスポート**]** で、次の **2** つのルートタイプが表示されている必要があります。
   - タイプ 5 AS 外部
   - タイプ 1 イントラエリア

変更した設定をアクティブ化すると、[設定] > [仮想 **WAN**] > [設定の表示] > [動的ルーティング] でルートタイプの変更を確認できます。

ルートは、SD-WAN アプライアンスによってタイプ 5 外部 AS としてアドバタイズされる必要があります。SD-WAN を介して学習されたルートは、ネイバールータでタイプ 5 AS 外部ルートとして表示する必要があります。

[基本的な **OSPF** 設定] で OSPF エクスポートされたルートウェイトを設定するには、次の手順を実行します。

1. DC サイトとブランチサイトの両方で仮想インターフェイスと WAN リンクを構成して、それらの間に仮想パスを作成します。
2. [接続]>[**MCN**]> [ルート学習] > [**OSPF**] > [基本設定**]** で、**[OSPF** ルートウェイトのエクスポート] を設定します。
3. 設定、ステージを保存し、同じことをアクティブにします。
4. ここで、[OSPF ルートウェイトのエクスポート] を **1** ～**65529** までの任意の数値に設定します。
5. 変更した設定をアクティブ化すると、[設定] > [仮想 **WAN**] > [設定の表示] > [ダイナミックルーティング] でルートの重みを確認できます。エクスポートされるデフォルトのルートウェイトは 0 でなければなりません。ルートの実際のコストは SD-WAN のコストだけである必要があります。

[エクスポートフィルタ設定] で OSPF でエクスポートされたルートを Type1 として設定するには、次の手順を実行します。

1. DC とブランチの両方で仮想インターフェイスと **WAN** リンクを設定し、それらの間に仮想パスを作成できるように 1。[接続] > [**[MCN]**] > [ルート学習] > [**OSPF**] > [エクスポートフィルタ] でエクスポートフィルタを設定します。
2. フィルタを展開します。**[OSPF** ルートタイプのエクスポート**]** を **[**タイプ **1** イントラエリア 内ルート] に設定します。
3. 設定、ステージを保存し、同じことをアクティブにします。[**OSPF** ルートタイプのエクスポート] で、次の 2 つのルートタイプが表示されている必要があります。

- タイプ 5 AS 外部
- タイプ 1 イントラエリア

変更された設定をアクティブ化した後、ユーザは **[**構成**]** > **[** 仮想 **WAN]** > **[**設定の表示**]** で、ルートタイプの変更を確認できる必要があります。ルートタイプは、タイプ 5 AS External として表示する必要があります。

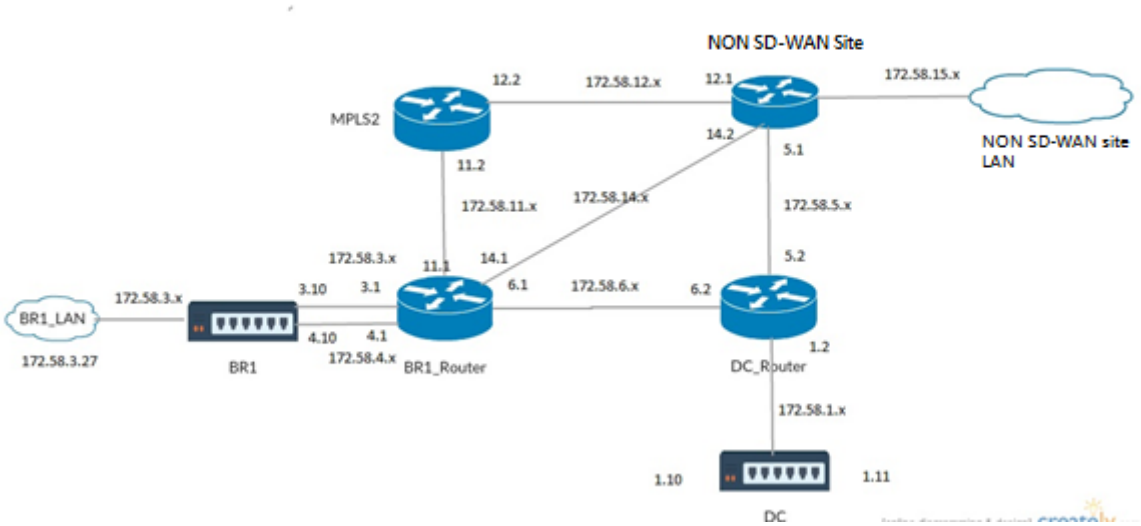
[エクスポートフィルタ] 設定で OSPF でエクスポートされたルートウェイトを設定するには、次の手順を実行します。

1. DC と Branch の両方で仮想インターフェイスと WAN リンクを設定して、それらの間に仮想パスを作成できるようにします。
2. [接続]>[**MCN**]> [ルート学習] > [**OSPF**] > [エクスポートフィルタ] で、エクスポートフィルタを設定します。
3. フィルタを展開します。[OSPF ルートウェイトのエクスポート] を **1** ～**65529** までの任意の数値に設定します。
4. 設定、ステージを保存し、同じことをアクティブにします。

変更された設定をアクティブ化した後、ユーザは **[**構成**]** > **[** 仮想 **WAN]** > **[**設定の表示**]** で、ルートタイプの変更を確認できる必要があります。
[エクスポートフィルタ] で設定されたルートウェイトは、[基本 **OSPF** 設定] で設定された重みよりも優先する必要があります。

SD-WAN およびサードパーティ（**SD-WAN** 以外）アプライアンスの展開

下の図に示すように、サードパーティのアプライアンスサイトは、サイト B に直接トラフィックを送信することで、サイト B の LAN にアクセスすることができます。トラフィックを直接送信できない場合、フォールバックルートはサイト A に送信され、DC からブランチサイト間の仮想パスを使用してブランチに到達します。失敗した場合は、MPLS2 を使用してブランチサイトにアクセスしてください。



構成手順**:**

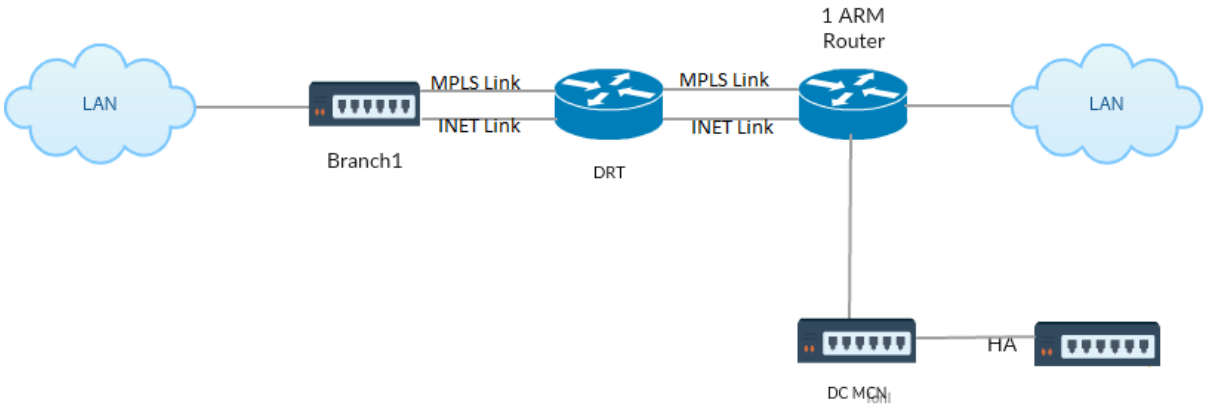
1. サイト間に仮想パスが作成されるように、**DC** とブランチの両方で仮想インターフェイスと **WAN** リンクを設定します。
2. SD-WAN アプライアンスで、エクスポートルートタイプをタイプ **1** に設定し、コストを **195** として割り当てます。
3. 設定を保存、ステージングし、アクティブ化します。
4. DC サイトとブランチサイトのエンドホスト間でトラフィックを送信します。
5. R1 と R2 の間のリンクをシャットダウンします。
6. DC サイトとブランチサイトのエンドホスト間でトラフィックを送信します。
7. R1 と R2 の間のリンクを解除します。
8. DC サイトとブランチサイトのエンドホスト間でトラフィックを送信します。
9. 仮想パスがダウンするように、DC サイトで仮想 WAN サービスを無効にします。
10. DC サイトとブランチサイトのエンドホスト間でトラフィックを送信します。

設定の確認:

1. 最初は、ステップ 4 で、すべてのトラフィックが SD-WAN アプライアンスを通過します。
2. ステップ 6 では、R1 と R2 の間のリンクが切断されると、トラフィックは R3 を介して SD-WAN にルーティングされます。
3. ステップ 8 では、トラフィックは、LAN ルータ R1 のネクストホップとして R2 を持つ SD-WAN アプライアンスを通過します。
4. ステップ 10 では、DC アプライアンスと BR1 アプライアンス間で仮想 WAN パスがダウンし、SD-WAN ネットワークが設定される前と同じようにトラフィックが正常に流れる必要があります。

トラフィックフローは、SD-WAN GUI の [モニタリング] > [フロー] で確認できます。

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



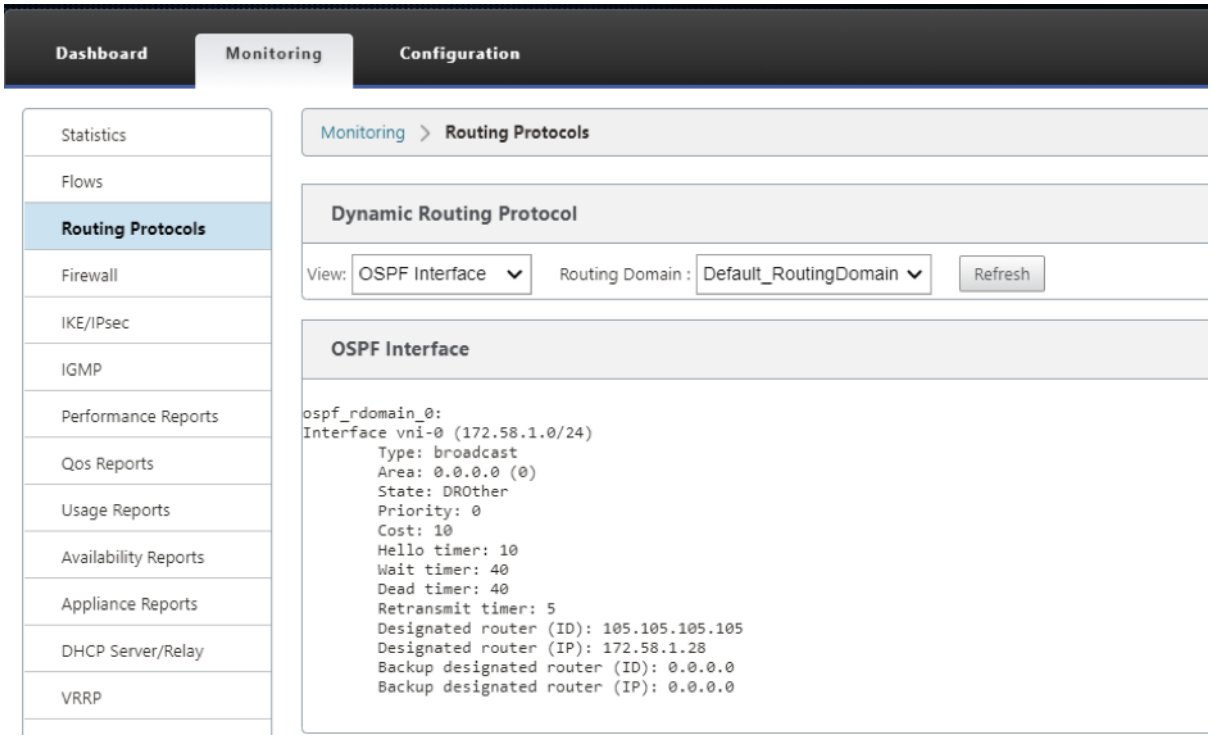
スタンバイアプライアンスへのフェールオーバー中に高可用性サイトを持つ OSPF Type-5 から Type-1 への高可用性セットアップで展開されます。

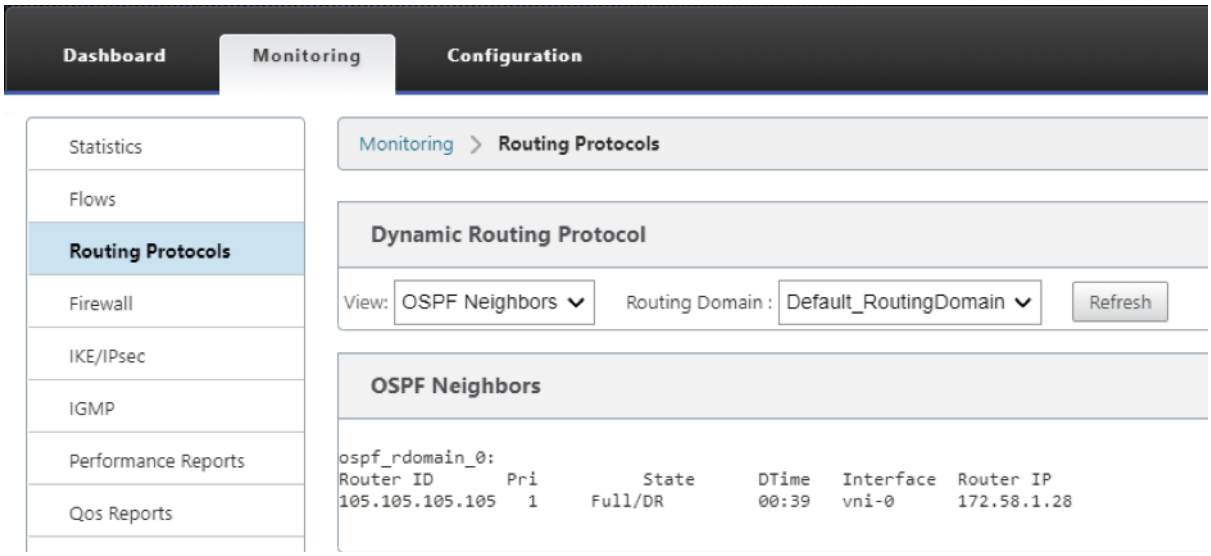
HA 展開で OSPF を設定するには、次の手順を実行します。

1. DC とブランチの両方で仮想インターフェイスと **WAN** リンクを設定して、それらの間に仮想パスを作成します。
2. 高可用性のセットアップ
3. ルートタイプをタイプ **1** に設定し、ルートウェイト を **50** に設定してエクスポートします。
4. 設定、ステージを保存し、同じことをアクティブにします。
5. トラフィックフローを開始します。
6. [**Monitor**] > [**Statistics**] > [**Routes**] で、コストが最も少ない OSPF ルートのヒットカウントが増加することを確認します。
7. アクティブ MCN をダウンさせ、動作を確認します。
8. 元のアクティブ MCN をバックアップします。
9. [ダッシュボード] > [高可用性ステータス] が HA ローカルアプライアンス、およびピアアプライアンスがアクティブおよびスタンバイの場合は正しく表示されます。
10. [設定] > [設定の表示] > [ダイナミックルーティング] では、OSPF が有効になり、**export_ospf_route_type** が **Type1** 、**export_ospf_route_weight** が **50** と表示されます。
11. フェールオーバー後でも、高可用性ステータスは、ローカルアプライアンスとピアアプライアンスの正しい OSPF 設定を示します。
12. 表示 モニター > 統計 > ルート。最小のコストで OSPF ルートのヒットカウントが増加します。
13. フェールバック後、高可用性ステータスは、ローカルおよびピアアプライアンスの正しい OSPF 設定を示します。
14. [**Monitor**] > [**Statistics**] > [Routes] で、低コストの OSPF ルートのヒットカウントが増加することを確認します。

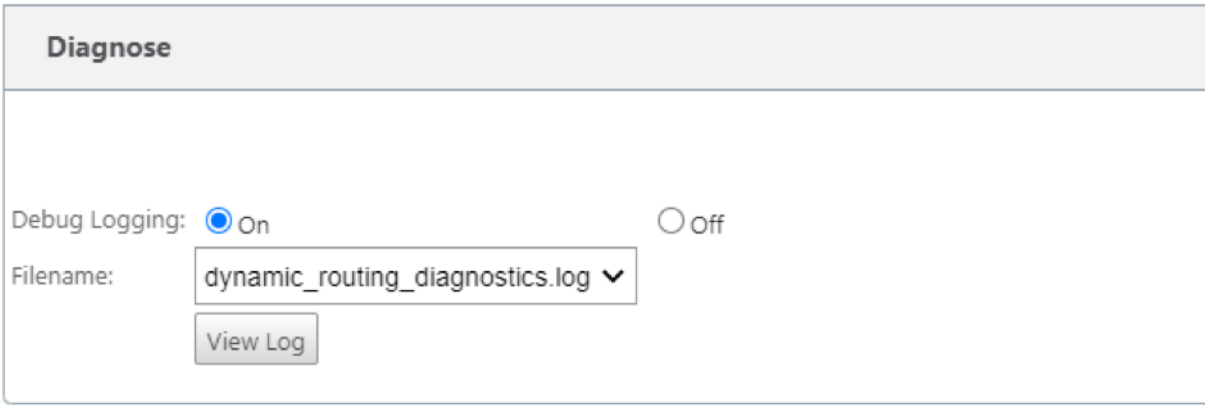
トラブルシューティング

OSPF パラメータは、[モニタリング**] > [**ルーティングプロトコル] の下に表示されます。





また、ダイナミックルーティングログを確認して、OSPF コンバージェンスに問題がないかどうかを確認することもできます。



BGP

May 10, 2021

SD-WAN BGP ルーティング機能を使用すると、次のことが可能になります。

- ネイバーまたは他のピアルータ（iBGP または eBGP）の AS 番号を設定します。
- いずれかの方向（インポートまたはエクスポート）で、ネイバーごとにネットワークセットに選択的に適用する BGP ポリシーを作成します。SD-WAN アプライアンスは、サイトごとに 8 つのポリシーをサポートし、1 つのポリシーには最大 8 つのネットワークオブジェクト（または 8 つのネットワーク）が関連付けられています。
- ユーザは、ポリシーごとに、複数のコミュニティストリング、AS-PATH-PREPEND、MED 属性を設定できます。ユーザーは、ポリシーごとに最大 10 の属性を設定できます。

> 注:
>
> パスの選択と操作には、ローカルプリファレンスと IGP メトリックだけが許可されます。

ポリシーの設定

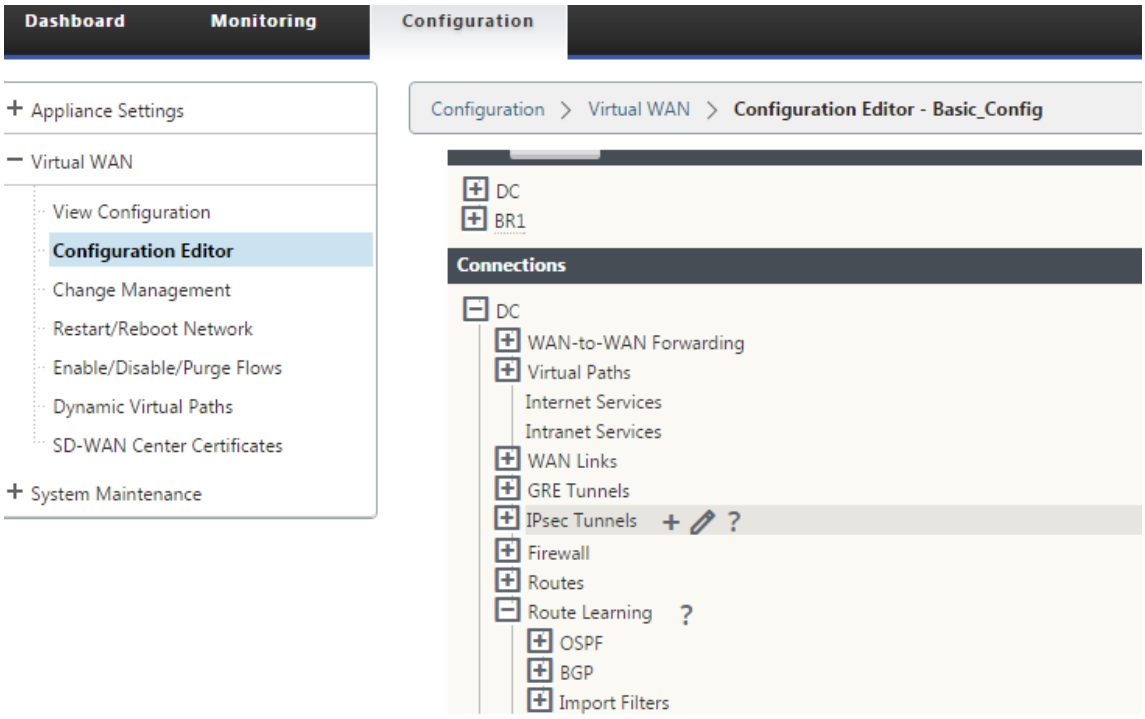
SD-WAN Web 管理インターフェイスでは、構成エディタに **[R **oute Learning**] > [BGP] の下に BGP ポリシーという新しいセクションが追加されました。** このセクションでは、ポリシーを構成する BGP 属性を追加できます。コミュニティストリングの追加、AS パスの先頭追加、および MED の設定がサポートされています。

各コミュニティストリングを手動で設定するか、ドロップダウンメニューから [アドバタイズなし] または [エクスポートコミュニティストリングなし] を選択できます。手動設定の場合、AS 番号とコミュニティを入力できます。[**Insert/Remove**] を選択して、ルートにタグを付けたり、ルートからコミュニティを削除したりできます。

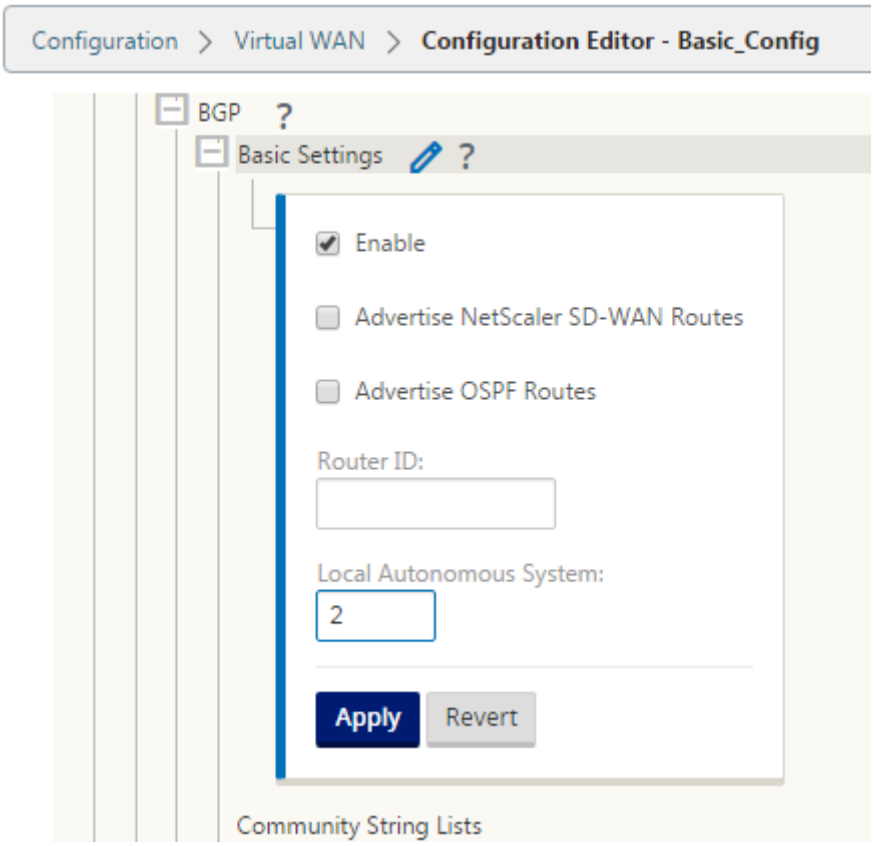
ローカルネットワークの外部をアドバタイズする前に AS パスにローカル AS を付加する回数を設定できます。ルートを照合するために MED を設定できます。

BGP ポリシーを設定するには、次の手順を実行します。

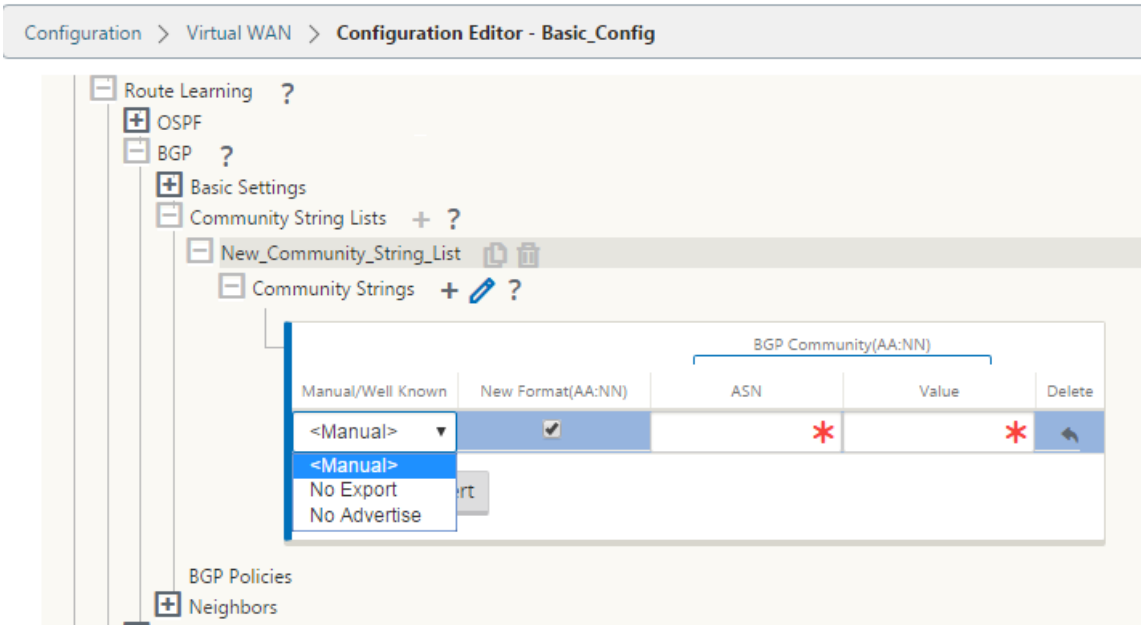
1. NetScaler SD-WAN Web 管理インターフェイスで、［構成］ **>** ［仮想 WAN］ **>** ［構成エディタ］ の順に選択します。既存の構成パッケージを開きます。[サイト] > [**DC** または 支店 の設定] に移動します。



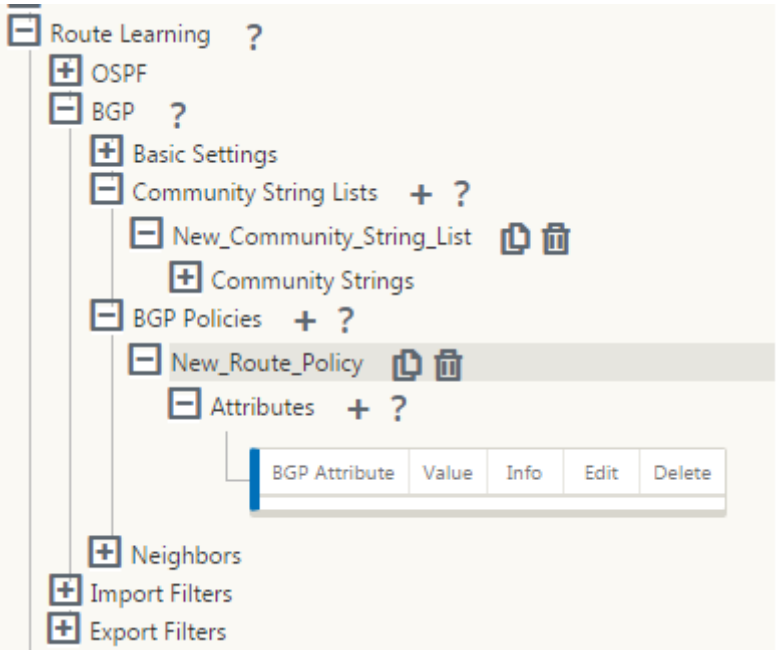
2. [**BGP**] を展開し、[基本設定] の [有効] をクリックします。ルータ **ID** と ローカル自律システム 値を入力し、[**Apply**] をクリックします。



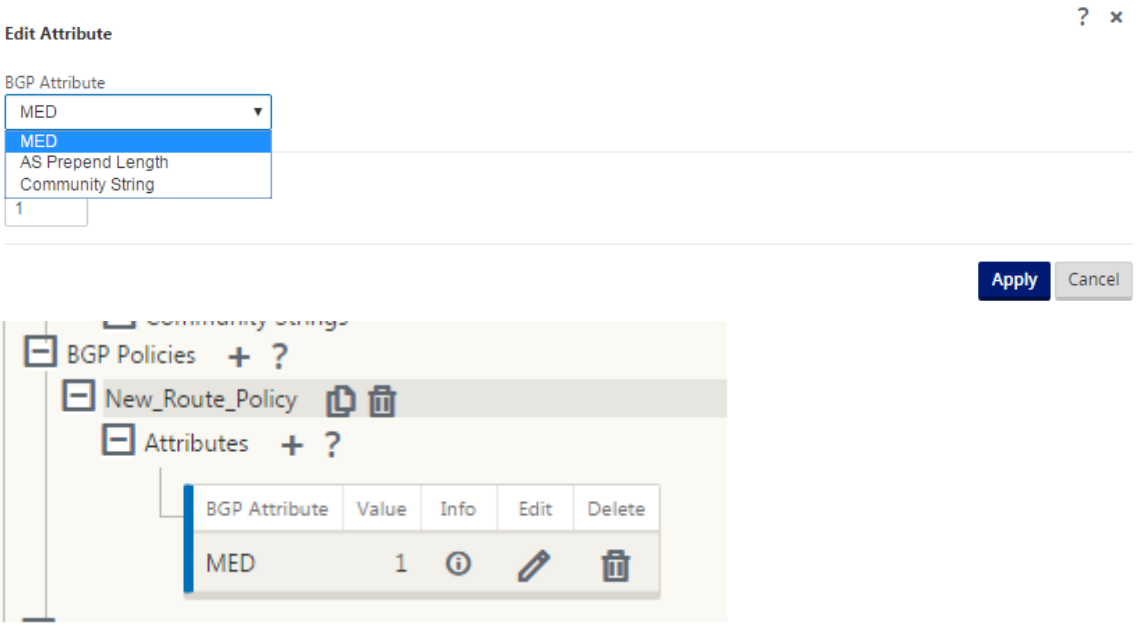
3. [コミュニティストリングリスト] の横にある [**+**] 記号をクリックします。各コミュニティストリングを手動で設定するか、ドロップダウンメニューから [アドバタイズなし] または [エクスポートコミュニティストリングなし] を選択します。手動設定の場合、AS 番号とコミュニティを入力できます。コミュニティストリングを含むルートに [**Insert/Rem** ove taging] を選択するか、ピアから受信したルートからコミュニティストリングを削除できます。



4. BGP ポリシーを展開して、**BGP** ポリシーを設定します。BGP アトリビュートを 新しいルートポリシーに追加します。



5. BGP アトリビュート を編集するには、[Attributes] の横の [**+**] 記号をクリックします。「属性の編集」ウィンドウが表示されます。ドロップダウンメニューから目的の BGP 属性を選択します。選択に従って、[**MED]**、**[AS** プリペンド長]、または [コミュニティストリング] に値を入力します。[適用] をクリックします。



> 注
>
> どのポリシーでも、1 つの属性の出現は 1 つだけであり、同じ属性を複数回出現することはできません。2 台の MED または 2 台の AS パスの先頭にすることはできません。先頭に MED/AS-PATH を追加/コミュニティストリング、またはその組み合わせを指定できます。

ネイバーの設定

eBGP を設定するには、既存の BGP ネイバーセクションにカラムを追加して、ネイバー AS 番号を設定します。SD-WAN 9.2 構成エディタを使用して以前の設定をインポートすると、このフィールドにはローカル AS 番号があらかじめ入力されています。

また、ネイバー設定には、オプションの詳細セクション（展開可能な行）があり、各ネイバーのポリシーを追加できます。

アドバンストネイバーの設定

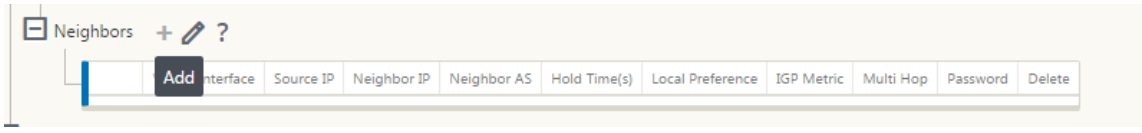
このオプションを使用すると、ネットワークオブジェクトを追加し、そのネットワークオブジェクトに設定された BGP ポリシーを追加できます。これは、特定のルートを照合するルートマップと ACL を作成し、そのネイバーの BGP 属性を設定するのと似ています。このポリシーが着信ルートまたは発信ルートに適用されているかどうかを示す方向を指定できます。

デフォルトのポリシー <accept> はすべてのルートに適用されます。承認ポリシーと拒否ポリシーはデフォルトで、変更できません。

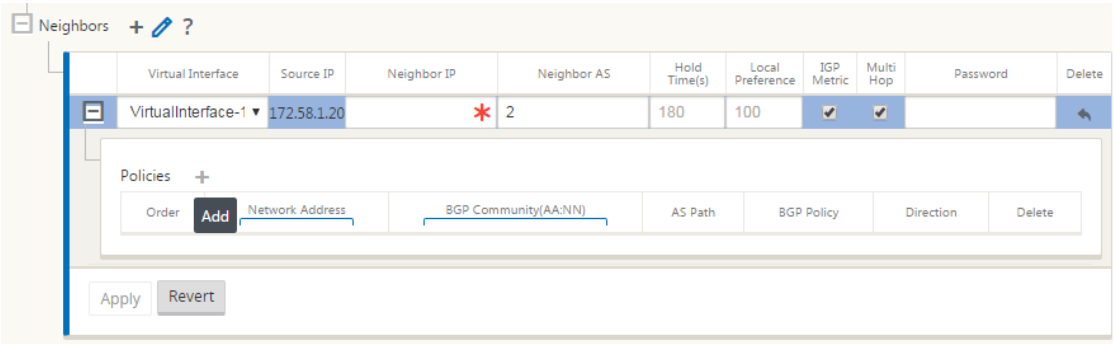
ネットワークアドレス（宛先アドレス）、AS パス、コミュニティストリングに基づいてルートを照合し、ポリシーを割り当てて適用するポリシーの方向を選択できます。

ネイバーを設定するには、次の手順を実行します。

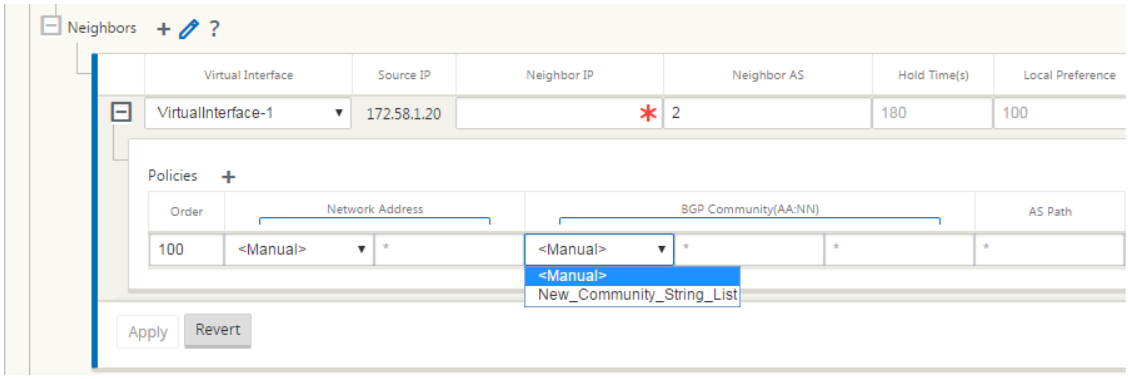
1. 次に示すように、[**Add**] をクリックしてネイバーを設定します。

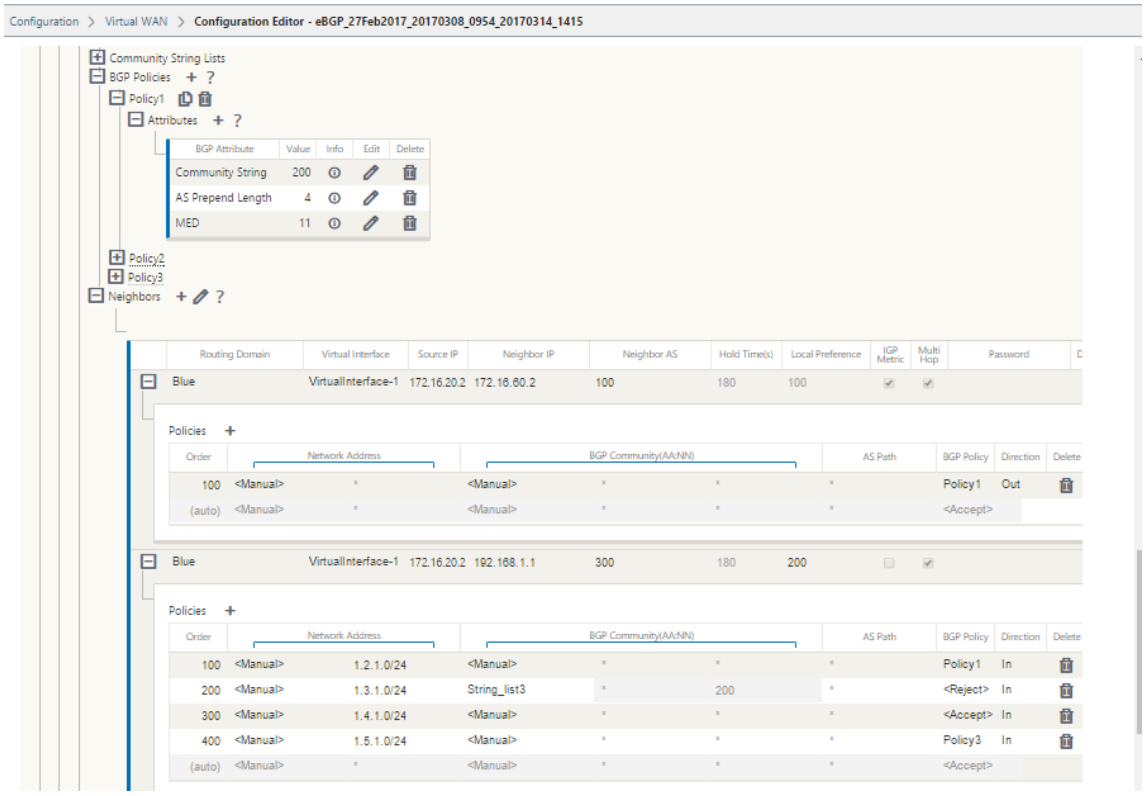


2. **+** 記号をクリックします。仮想インターフェイスを選択します。ネイバー **IP** アドレスを入力します。



3. ポリシーを追加します。必要に応じて、[ネットワークアドレス]、[**BGP** コミュニティ]、および [**AS** パスの詳細] を選択します。[適用] をクリックします。





4. [モニタリング] > [ルーティングプロトコル] > [ダイナミックルーティングプロトコル] の順に選択し、DC またはブランチサイトアプライアンスに設定された BGP ポリシーとネイバーを監視します。

デバッグロギングを有効にし、ルーティング用のログファイルを表示するには、[**Monitor**] > [Rout **ing Protocol]** ページを使用します。ルーティングデーモンのログは、別々のログファイルに分割されます。標準ルーティング情報は d *ynamic_routing.log* に格納され、動的ルーティングの問題は d *ynamic_routing_diagnostics.log* に格納されます。この情報は、ルーティングプロトコルの監視から参照できます。

BGP ソフト再設定

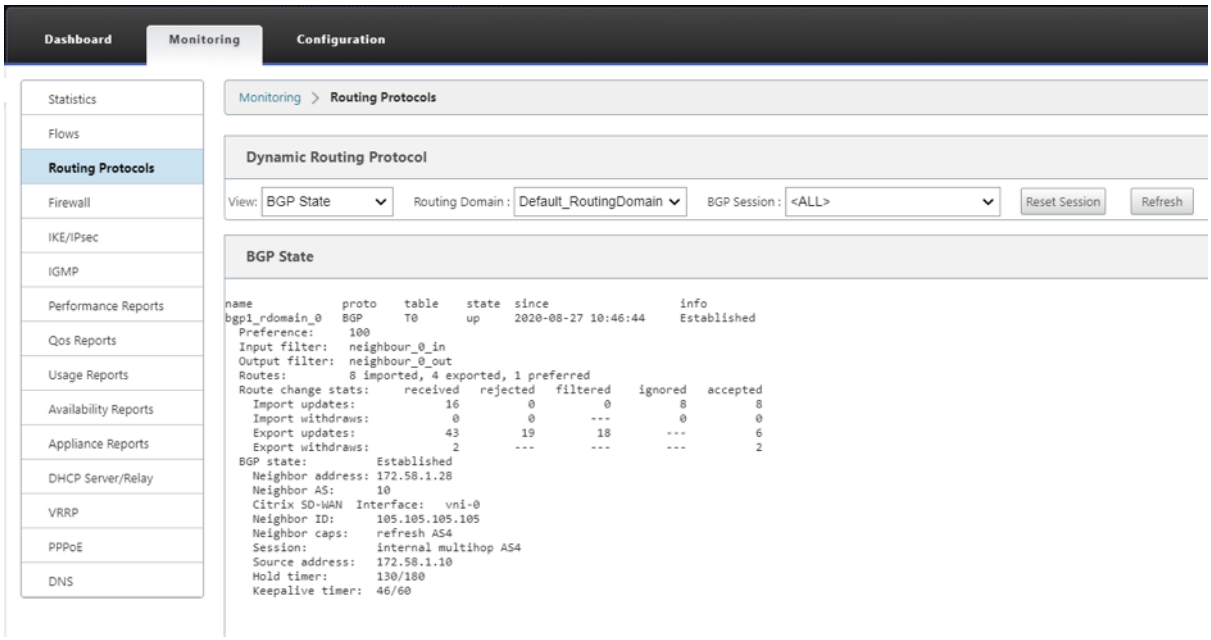
BGP ピアのルーティングポリシーには、インバウンドまたはアウトバウンドルーティングテーブルの更新に影響する可能性のあるルートマップ、配布リスト、プレフィクスリスト、フィルタリストなどの設定が含まれます。ルーティングポリシーに変更があった場合、新しいポリシーを有効にするには、BGP セッションをクリアまたはリセットする必要があります。

ハードリセットを使用して BGP セッションをクリアすると、キャッシュが無効になり、キャッシュ内の情報が利用できなくなると、ネットワークの動作に悪影響が生じます。

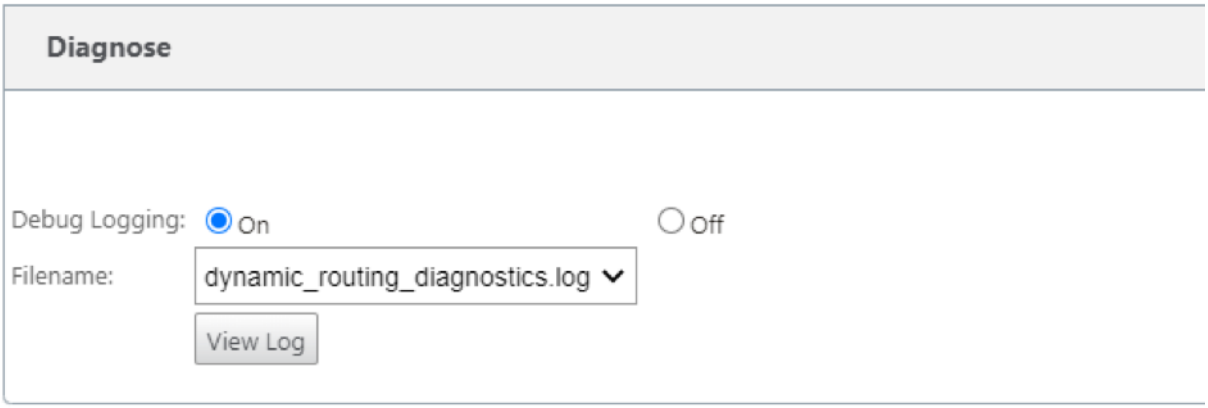
BGP ソフトリセット拡張機能は、格納されているルーティングテーブルの更新情報に依存しない着信 BGP ルーティングテーブルアップデートのダイナミックソフトリセットを自動的にサポートします。

トラブルシューティング

BGP パラメータを表示するには、[モニタリング] **>** [ルーティングプロトコル] に移動し、[**View**] フィールドから [**BGP State**] を選択します。



ダイナミックルーティングログを確認して、BGP コンバージェンスに問題がないかどうかを確認できます。



iBGP

May 10, 2021

iBGP が LAN 側に、eBGP が WAN 側に Citrix SD-WAN アプライアンス:

Citrix SD-WAN アプライアンスは、LAN 側に iBGP、WAN 側に eBGP を使用して展開すると、NEXT HOP SELF を使用して IGP ドメインに学習されたすべての eBGP ルートをアドバタイズします。

リニアネットワークトポロジー内の複数の iBGP LAN ルーターは、ダイレクトピアリング機能を持ち、Citrix SD-WAN でメッシュ化されています。

制限事項:

- AS パスプリペンド、Med、およびコミュニティ属性はサポートされていません。
- 再配布中の OSPF と BGP 間のルートフィルタリングはサポートされていません。OSPF から学習されたルートはすべて BGP ピアにアドバタイズされるか（または)、その逆も同様です。
- ルート集約はサポートされていません。
- 最大 16 の BGP ピア（iBGP および eBGP を含む）だけを設定できます。

eBGP

May 10, 2021

eBGP 経由で非 SD-WAN サイトと通信する SD-WAN サイト

SD-WAN アプライアンスのないサイトが、単一の WAN パスで SD-WAN アプライアンス（サイト A）を使用する別のサイトと通信している場合（インターネットのみが使用可能)、SD-WAN アプライアンスのあるサイト（サイト A) がインターネット接続を失った場合、SD-WAN を使用しないサイトは、別の SD-WAN を介してサイト A と通信できます。アプライアンスサイト (サイト B) で設定します。サイト B は、SD-WAN アプライアンスのないサイトからサイト A にトラフィックをファネルします。

仮想パスと eBGP を使用した SD-WAN サイト間の通信

Virtual WAN アプライアンスが稼動している間に、2 つのサイト間で仮想パスがダウンしている場合に、リモートサイトのローカルサブネットと通信するためのアンダーレイルートラーニングを提供します。

アプリケーションルート

May 10, 2021

一般的なエンタープライズネットワークでは、ブランチオフィスはオンプレミスデータセンター、クラウドデータセンター、または SaaS アプリケーション上のアプリケーションにアクセスします。アプリケーションルーティング機能により、ネットワークを介してアプリケーションを簡単かつコスト効率よく操作できます。たとえば、ブランチサイトのユーザーが SaaS アプリケーションにアクセスしようとすると、ブランチオフィスが最初にデータセンターを経由することなく、インターネット上の SaaS アプリケーションに直接アクセスできるように、トラフィックをルーティングできます。

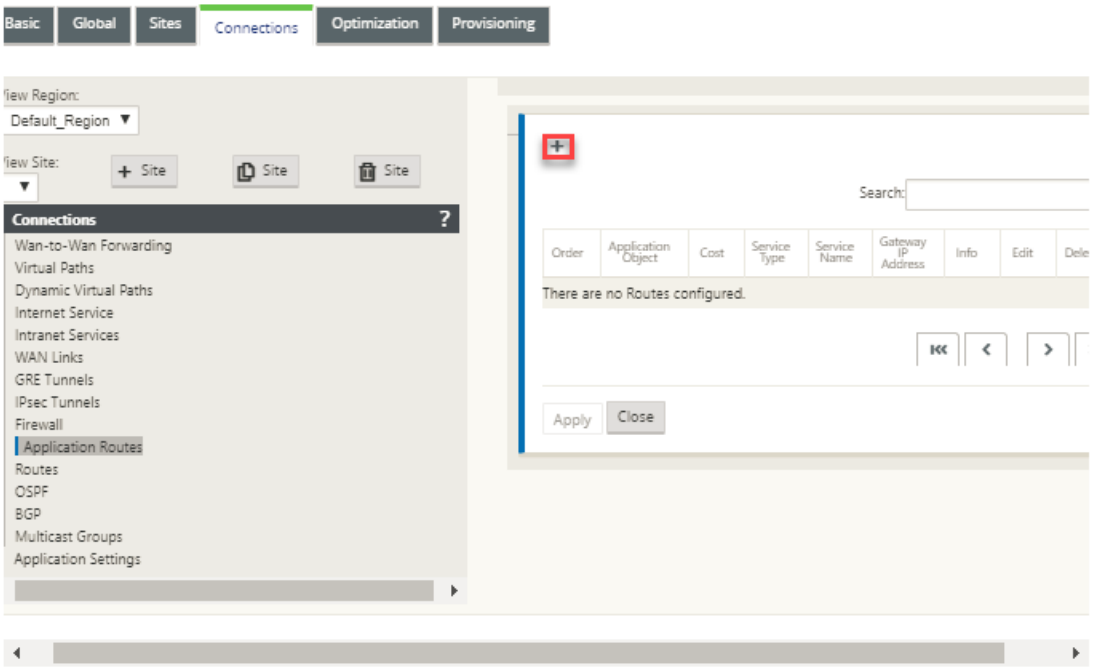
Citrix SD-WAN では、次のサービスのアプリケーションルートを定義できます。

- 仮想パス：このサービスは、仮想パスを通過するトラフィックを管理します。仮想パスは、2 つの WAN リンク間の論理リンクです。これは、2 つの SD-WAN ノード間で高いサービス・レベル通信を提供するために結合された WAN パスの集合で構成されます。SD-WAN アプライアンスは、パス単位でネットワークを測定し、変化するアプリケーション需要や WAN 条件に適応します。仮想パスは、スタティック（常に存在）またはダイナミック（2 つの SD-WAN アプライアンス間のトラフィックが設定されたしきい値に達した場合のみ存在）のいずれかになります。
- インターネット：このサービスは、エンタープライズサイトとパブリックインターネット上のサイト間のトラフィックを管理します。インターネットトラフィックはカプセル化されません。輻輳が発生すると、SD-WAN は、仮想パス、およびイントラネットトラフィックに対するレート制限によって、帯域幅を積極的に管理します。
- イントラネット: このサービスは、仮想パス経由の送信用に定義されていないエンタープライズイントラネットトラフィックを管理します。イントラネットトラフィックはカプセル化されません。SD-WAN は、輻輳時にこのトラフィックを他のサービスタイプと比較してレート制限することにより、帯域幅を管理します。特定の条件下では、イントラネットフォールバックが仮想パス上に構成されている場合、通常は仮想パスを通過するトラフィックは、代わりにイントラネットトラフィックとして扱うことができます。
- ローカル：このサービスは、他のサービスと一致しないサイトへのローカルトラフィックを管理します。SD-WAN は、ローカルルートを送信元および宛先とするトラフィックを無視します。
- **GRE** トンネル：このサービスは、GRE トンネル宛の IP トラフィックを管理し、サイトで設定された LAN GRE トンネルと一致します。GRE トンネル機能を使用すると、LAN 上の GRE トンネルを終了するように SD-WAN アプライアンスを設定できます。サービスタイプ GRE Tunnel のルートの場合、Gateway はローカル GRE トンネルのトンネルサブネットの 1 つに存在する必要があります。
- **LAN IPsec** トンネル**:** このサービスは、LAN IPsec トンネル宛の IP トラフィックを管理し、サイトで構成された LAN IPsec トンネルと一致します。LAN IPsec トンネル機能を使用すると、LAN または WAN 側で IPsec トンネルを終了するように SD-WAN アプライアンスを構成できます。

アプリケーションのサービスステアリングを実行するには、最初のパケット自体でアプリケーションを識別することが重要です。最初は、トラフィックが分類され、アプリケーションが認識されると、パケットは IP ルートを通過します。対応するアプリケーションルートが使用されます。最初のパケット分類は、アプリケーションオブジェクトに関連付けられた IP サブネットとポートを学習することによって達成されます。これらは、DPI 分類器の履歴分類結果とユーザ設定の IP ポート一致タイプを使用して取得されます。

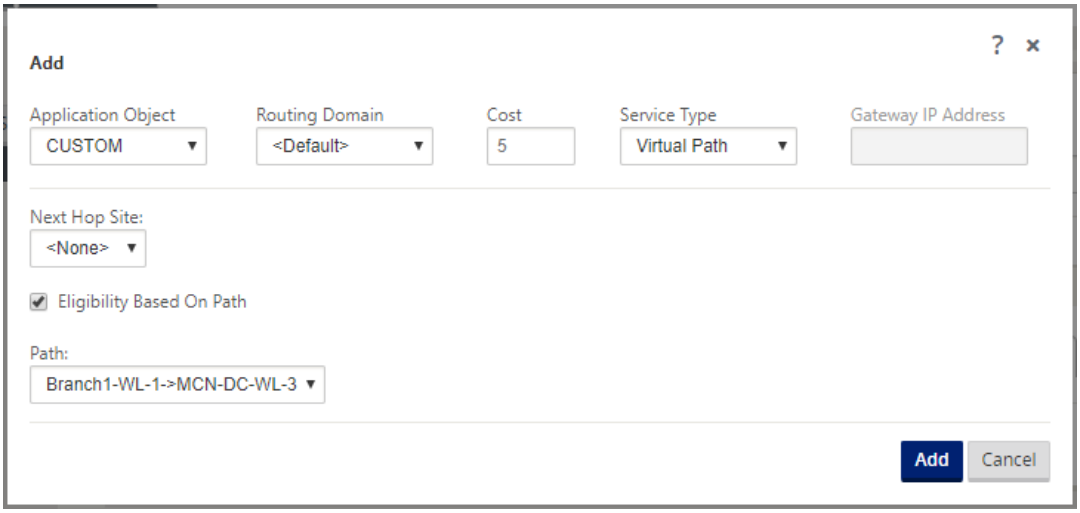
アプリケーション・ルーティングを構成するには、次の手順に従います。

1. 構成エディタで、「接続」>「アプリケーションルート」に移動し、「+」をクリックします。



2. [追加] ページで、次のパラメータを設定します。

- アプリケーション・オブジェクト: 操作するアプリケーション・オブジェクト。ここで作成したアプリケーションオブジェクトが一覧表示されます。詳細については、アプリケーション分類トピックの「アプリケーションオブジェクト」セクションを参照してください。



- ルーティングドメイン: アプリケーションルートで使用されるルーティングドメイン。設定済みのルーティングドメインの 1 つを選択します。
- コスト: このルートのルート優先度を決定する重み。低コストのルートは、高コストのルートよりも優先されます。指定できる範囲は 1 ～65534 です。デフォルト値は 5 です。
- サービスタイプ**:** 次のサービスのいずれかを選択します。これにより、アプリケーションがサービスに

マッピングされます。

- 仮想パス：アプリケーショントラフィックを仮想パストラフィックとして識別し、仮想パスルールに基づいて仮想パスを照合します。[**Next Hop Site**] フィールドに、仮想パスパケットの送信先となるネクストホップリモートサイトを入力します。

  > 注
  >
  > 仮想パスアプリケーションルートに到達するフローは、ダイナミック仮想パスを通過しません。

- インターネット：アプリケーショントラフィックをインターネットトラフィックとして識別し、インターネットサービスと照合します。
- [イントラネット]: アプリケーショントラフィックをイントラネットトラフィックとして識別し、イントラネットルールに基づいてイントラネットサービスと照合します。[イントラネットサービス] フィールドで、ルートに使用するイントラネットサービスを選択します。
- [ローカル]: アプリケーショントラフィックをサイトに対してローカルとして識別し、サービスと一致しません。ローカルルートをソースおよび宛先とするトラフィックは無視されます。

  > 注
  >
  > ローカルサービスタイプの場合、DPI 分類が完了すると、設定された IP ルートがルーティング決定を行います。

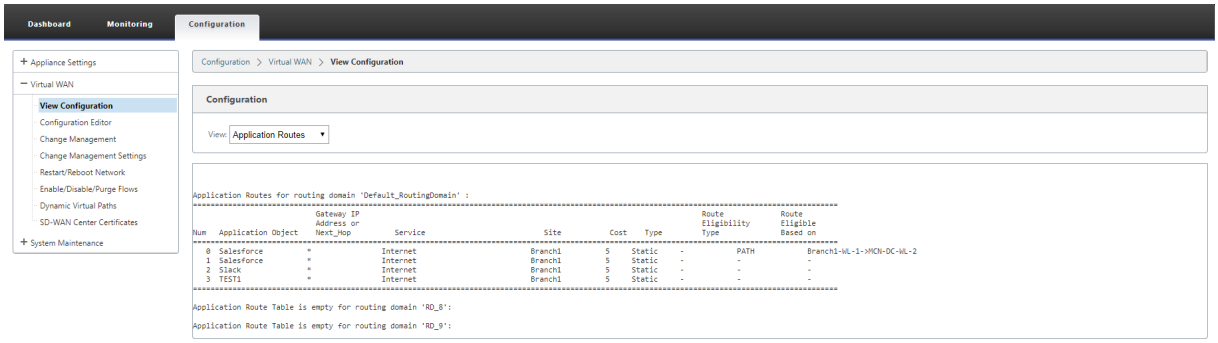
- **GRE** トンネル：アプリケーショントラフィックが GRE トンネルの宛先であると識別され、サイトで設定された LAN GRE トンネルと一致します。**[Gateway IP Address**] フィールドに、LAN GRE トンネルのサブネット内にある必要のあるゲートウェイの IP アドレスを入力します。ゲートウェイに到達できないときにルートがトラフィックを受信しないようにするには、**[**ゲートウェイに基づく適格性] を選択します。
- **LAN IPsec** トンネル：アプリケーショントラフィックが LAN IPsec トンネル宛てであると識別され、サイトで構成された LAN IPsec トンネルと一致します。[**IPSec Tunnel**] フィールドで、設定済みの IPSec トンネルの 1 つを選択します。トンネルに到達できないときにルートがトラフィックを受信しないようにするには、**[**トンネルに基づく適格性] を選択します。

  > 注
  >
  > カスタムアプリケーションのサービスを選択したら、そのサービスを変更しないでください。

- [パスに基づく適格性**]:** 指定したパスがダウンしたときにルートがトラフィックを受信しないようにする場合に選択します。[**Path**] フィールドで、ルートの適格性の決定に使用するパスを指定します。

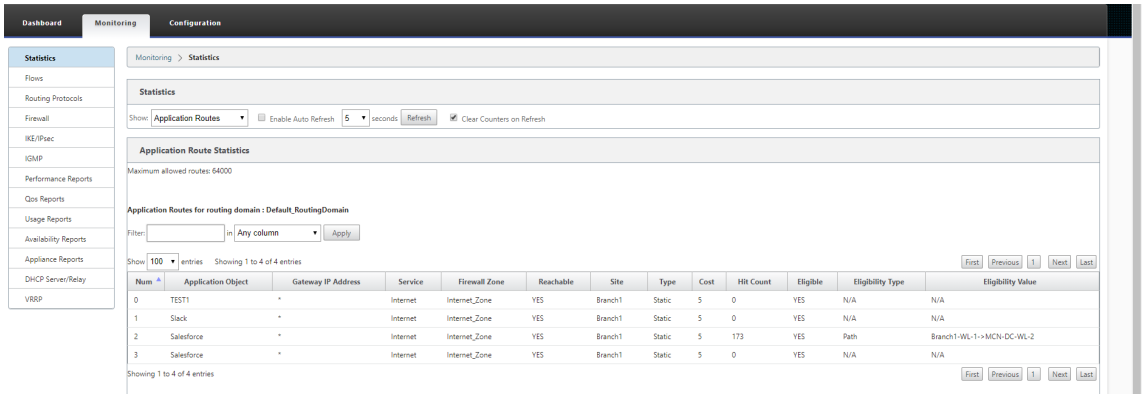
3. ［適用］をクリックします。

SD-WAN アプライアンスに構成されているアプリケーションルートを表示する。SD-WAN GUI で、[設定] > [仮想 **WAN**] > [設定の表示] に移動します。[表示] ドロップダウンメニューから [アプリケーションルート] を選択します。



アプリケーション・ルートの統計データを表示する手順は、次のとおりです。

1. SD-WAN GUI で、[モニタリング] > [統計] に移動します。
2. [表示] ドロップダウンリストから、[アプリケーションルート] を選択します。



次の統計を表示できます。

- アプリケーション・オブジェクト: アプリケーション・オブジェクトの名前。
- **Gateway IP** アドレス: GRE トンネルサービスタイプのアプリケーションオブジェクトで使用されるゲートウェイ IP アドレス。
- サービス: アプリケーション・オブジェクトにマップされたサービス・タイプ。
- ファイアウォールゾーン: このルートが属するファイアウォールゾーン。
- 到達可能: アプリケーションルートのステータス。
- サイト: サイトの名前。
- **[Type]**: ルートが静的か動的かを示します。
- コスト: ルートの優先度。
- **Hit Count**: トラフィックを処理するためにアプリケーションルートが使用される回数。
- 適格: アプリケーションルートがトラフィックを送信できるかどうかを示します。
- 適格タイプ: この工順に適用される工順適格条件のタイプ。適格性タイプは、パス、ゲートウェイ、またはトンネルです。
- 適格値: 工順適格条件に対して指定された値。

> 注
>
> 現在のリリースでは、アプリケーションファミリに属するアプリケーションは、アプリケーションオブジェクトで定義されている一致タイプで操作できません。

トラブルシューティング

アプリケーションルートを作成したら、[**Monitoring**] セクションを使用して、目的のサービスにアプリケーションが正しくルーティングされていることを確認できます。

アプリケーションが目的のサービスに正しくルーティングされているかどうかを確認するには、次のページに移動します。

- モニタリング **>** 統計 **>** アプリケーションルート
- モニタリング **>** フロー
- モニタリング **>** ファイアウォール

予期しないルーティング動作が発生した場合は、問題が発生している間に STS 診断バンドルを収集し、Citrix サポートチームと共有します。

STS バンドルは、**[**構成**] > [**システムメンテナンス**] > [**診断**] > [**診断情報**]** を使用して作成およびダウンロードできます。

ルートフィルタリング

May 10, 2021

ルート学習が有効なネットワークの場合、Citrix SD-WAN により、ルーティングネイバーにアドバタイズされる SD-WAN ルートと、ルーティングネイバーから受信されるルートをより詳細に制御できます。

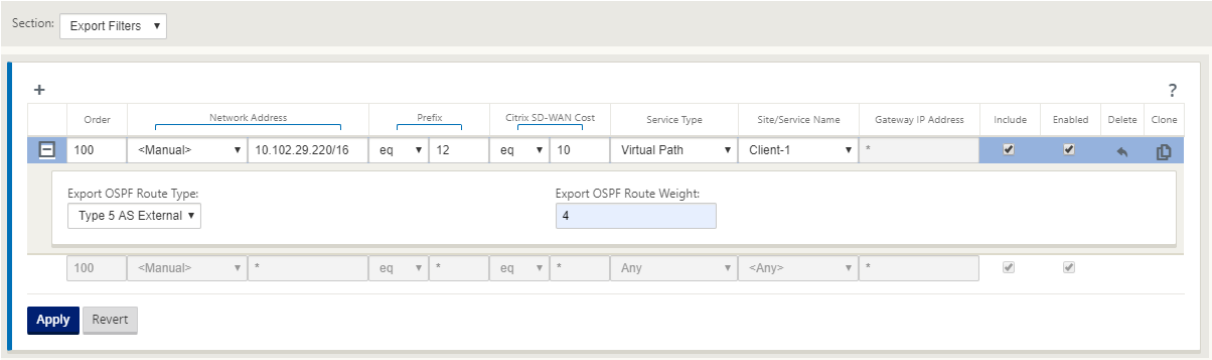
- エクスポートフィルタは、特定の一致基準に基づいて OSPF および BGP プロトコルを使用してアドバタイズメント用のルートを含めるか除外するために使用されます。エクスポートフィルタルールは、ダイナミックルーティングプロトコルで SD-WAN ルートをアドバタイズするときに満たす必要があるルールです。デフォルトでは、すべてのルートがピアにアドバタイズされます。
- インポートフィルタは、特定の一致基準に基づいて OSPF および BGP ネイバーを使用して受信したルートを受け入れるか、受け付けないかに使用します。インポートフィルタルールは、ダイナミックルートを SD-WAN ルートデータベースにインポートする前に満たす必要があるルールです。デフォルトでは、ルートはインポートされません。

ルートフィルタリングは、SD-WAN ネットワーク（データセンター/ブランチ）の LAN ルートおよび仮想パスルートに実装され、BGP と OSPF を使用して SD-WAN 以外のネットワークにアドバタイズされます。

最大 512 のエクスポートフィルタと 512 のインポートフィルタを設定できます。これは、ルーティングドメインごとの制限ではなく、全体的な制限です。

エクスポートフィルタの構成

構成エディタで、[接続] **>** [リージョン] **>** [サイト] **>** [**OSPF**] または [**BGP**] **>** [フィルタのエクスポート] に移動します。



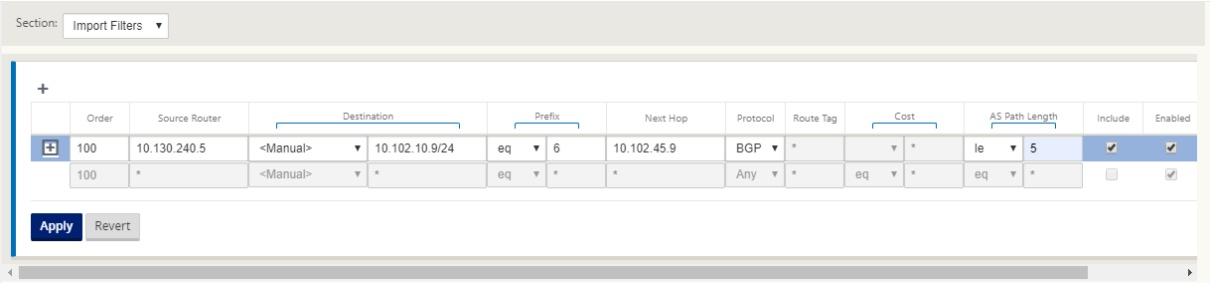
作成する各エクスポートフィルタを作成するには、次の基準を使用します。

フィールド条件	説明	値
Order	フィルタが優先される順序。ルートが一致する最初のフィルタは、そのルートに適用されます	100, 200, 300, 400, 500, 600
ネットワークアドレス	ルートのネットワークを記述する設定済みの Network Object の **IP** アドレス とサブネットマスクを入力します。	• IP アドレス
前	プレフィクスでルートを照合するには、メニューから一致述語を選択し、隣接するフィールドに Route プレフィクスを入力します。	• eq: 等しい,- lt: より小さい,- le: より小さい,- gt: より大きい,- ge: より大きい
Citrix SD-WAN コスト	エクスポートされたルートの選択を絞り込むために使用される方法（述語）と SD-WAN ルートコスト	数値
サービスの種類	Citrix SD-WAN サービスのリストから、一致するルートに割り当てられるサービスタイプを選択します。	任意、ローカル、仮想パス、インターネット、イントラネット、LAN GRE トンネル、LAN IPsec トンネル

フィールド条件	説明	値
サイト/サービス名	イントラネット、LAN GRE トンネル、および LAN IPsec トンネルの場合は、使用する構成済みのサービスタイプの名前を指定します。	テキスト文字列
Gateway IP アドレス	サービスタイプとして LAN GRE トンネルを選択した場合は、トンネルの Gateway IP を入力します。	IP アドレス
含める	[このフィルタに一致するルートを含める] チェックボックスをオンにします。それ以外の場合、一致するルートは無視されます	なし
有効です	[このフィルタを有効にする] チェックボックスをオンにします。それ以外の場合、フィルタは無視されます	なし
削除	このフィルタを削除するには、削除アイコンを選択します。	なし
複製	既存のフィルターのコピーを作成するには、クローンアイコンをクリックします。	なし

インポートフィルタの構成

構成エディタで、[接続**] > [**リージョン**] > [**サイト**] > [OSPF]** または [**BGP] > [**フィルタのインポート**]** に移動します。



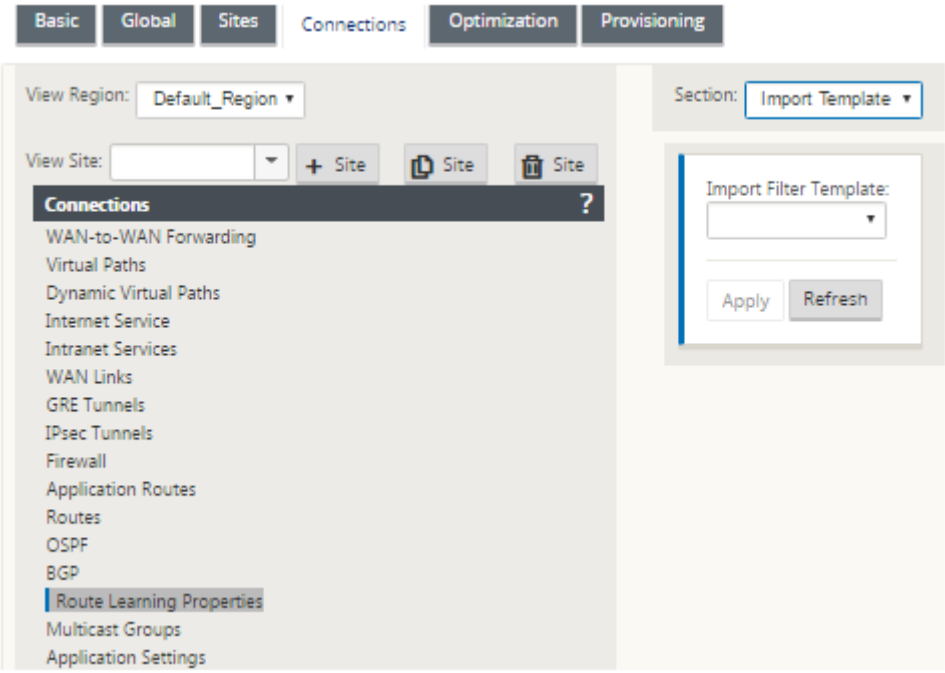
作成する各エクスポートフィルタを作成するには、次の基準を使用します。

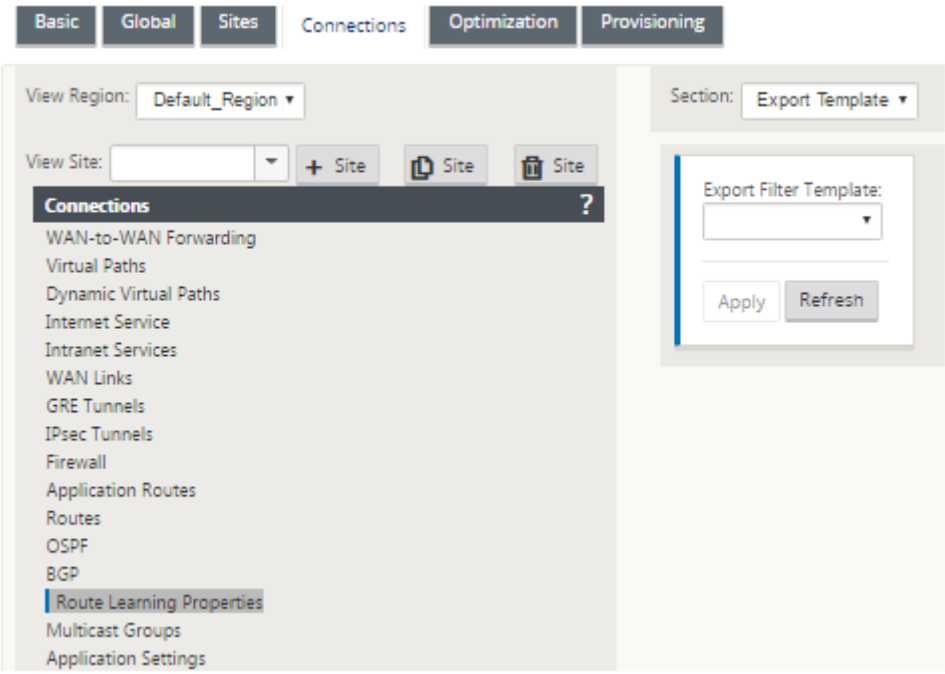
フィールド条件	説明	値
Order	フィルタが優先される順序。ルートが一致する最初のフィルタは、そのルートに適用されます	100, 200, 300, 400, 500, 600
送信元ルータ	送信元ルータの IP アドレス。iBGP だけに適用されます。	• IP アドレス
接続先	ルートの宛先の IP アドレスとサブネットマスク	• IP アドレス
前	プレフィクスでルートを照合するには、メニューから一致述語を選択し、隣接するフィールドに Route プレフィクスを入力します。	• eq: 等しい,- lt: より小さい,- le: より小さい,- gt: より大きい,- ge: より大きい
次ホップ	ネクストホップの IP アドレス	• IP アドレス
プロトコル	ルートの学習に使用するルーティングプロトコル	OSPF または BGP
ルートタグ	フィルタが一致する OSPF ルートタグ。OSPF ルートタグにより、OSPF と他のプロトコル間の相互再配布中のルーティングループを防止	数値
コスト	インポート用の OSPF ルートの照合に使用されるルートコスト	数値
AS パスの長さ	インポート用の BGP ルートの照合に使用される AS パスの長さ	数値
含める	[このフィルタに一致するルートを含める] チェックボックスをオンにします。それ以外の場合、一致するルートは無視されます	なし
有効です	[このフィルタを有効にする] チェックボックスをオンにします。それ以外の場合、フィルタは無視されます	なし
削除	このフィルタを削除するには、[削除] アイコンをクリックします。	なし
複製	既存のフィルターのコピーを作成するには、クローンアイコンをクリックします。	なし

ルートポリシーフィルタテンプレートの設定

さまざまなフィルタルールを使用して複数のインポートフィルタテンプレートまたはエクスポートフィルタテンプレートを作成し、各サイトでテンプレートを関連付けることができます。

ユーザーが作成したサイトレベルのインポート/エクスポートフィルタルールがより優先されます。テンプレートルールは、接続の R **oute Learning** セクションでサイトに関連付けられると、ユーザが作成したルールに従います。





ルート集約

May 10, 2021

企業ネットワークのサイズが大きくなるにつれて、ルータはルーティングテーブル内の多数のルートを維持する必要があります。ルータでは、大規模なルーティングテーブルを検索し、個々のルートを維持するために、CPU、メモリ、および帯域幅のリソースを増やす必要があります。サマリールートには、ローカルサービスタイプと廃棄サービスタイプを設定できます。このサマリールートは、ネクストホップデバイスにアドバタイズされます。

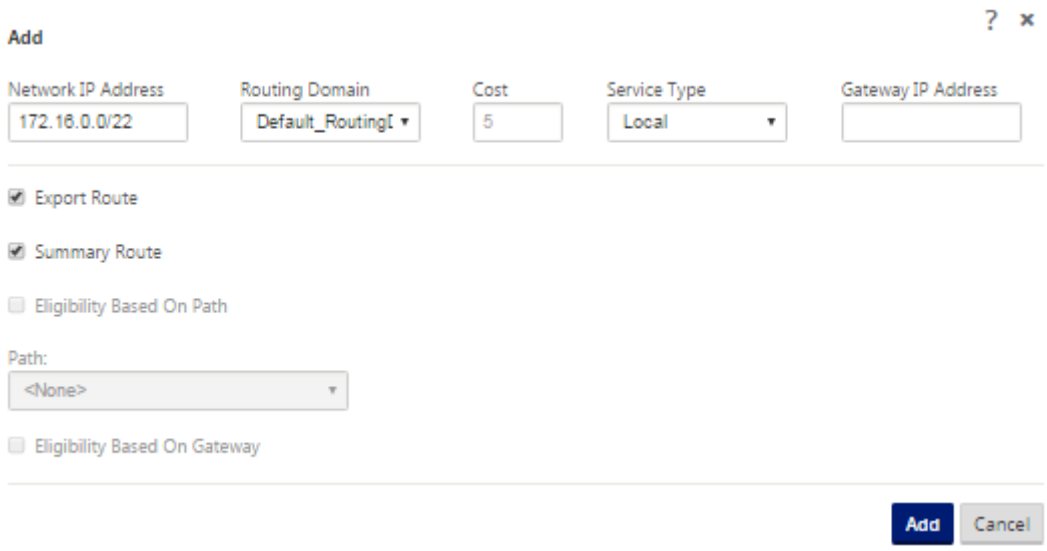
ローカルサブネットのサマリールートを設定するには、次の手順を実行します。

1. 設定エディタで、[接続] > [ルート] に移動し、[**+**] をクリックしてルートを追加します。
2. [ルートの追加] ページで、次のパラメータを設定し、[追加] をクリックします。

- ネットワーク **IP** アドレス: 計算されたサマリールート IP アドレス。
- コスト: このルートのルート優先度を決定する重み。低コストのルートは、高コストのルートよりも優先されます。指定できる範囲は 1 ～65534 です。
- ルーティングドメイン: 企業ネットワーク、ブランチオフィスネットワーク、またはデータセンターネットワークを管理するための単一管理ポイントを提供するルーティングプロトコル。
- [サービスタイプ**]:** [ローカルサービスタイプ] を選択します。

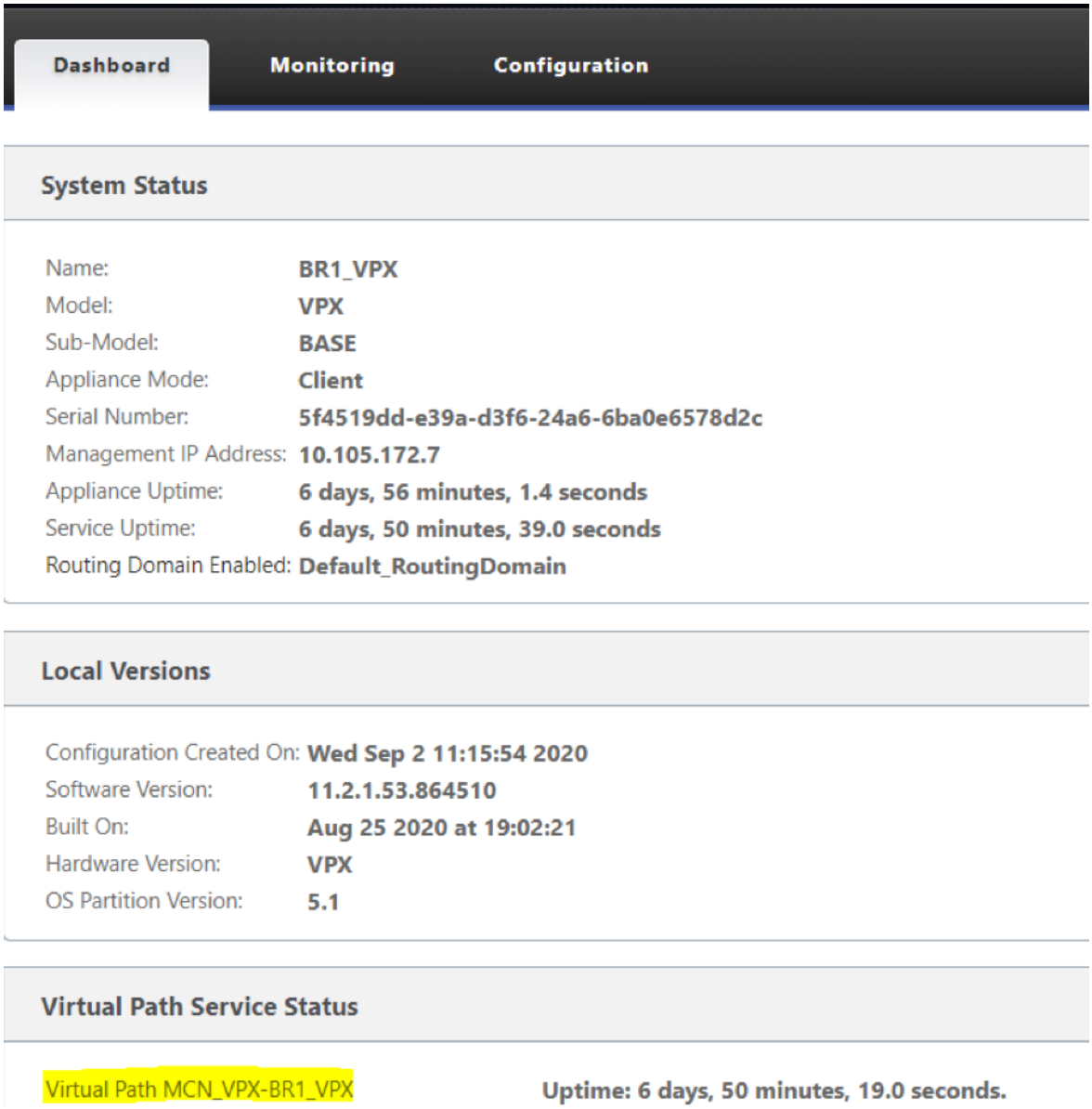
> 注
>
> サマリールートには、ローカル サービスタイプと 廃棄 サービスタイプだけを選択できます。

- ゲートウェイ **IP** アドレス**:** このルートのゲートウェイ IP アドレス。
- **[** ルートをエクスポート**]:** ルートを他の接続されたサイトにエクスポートします。
- **Summary Rout**e：他のすべての一致するサブネットではなく、接続されている他のデバイスに、ルートを 1 つのサマリールートとしてアドバタイズします。



トラブルシューティング

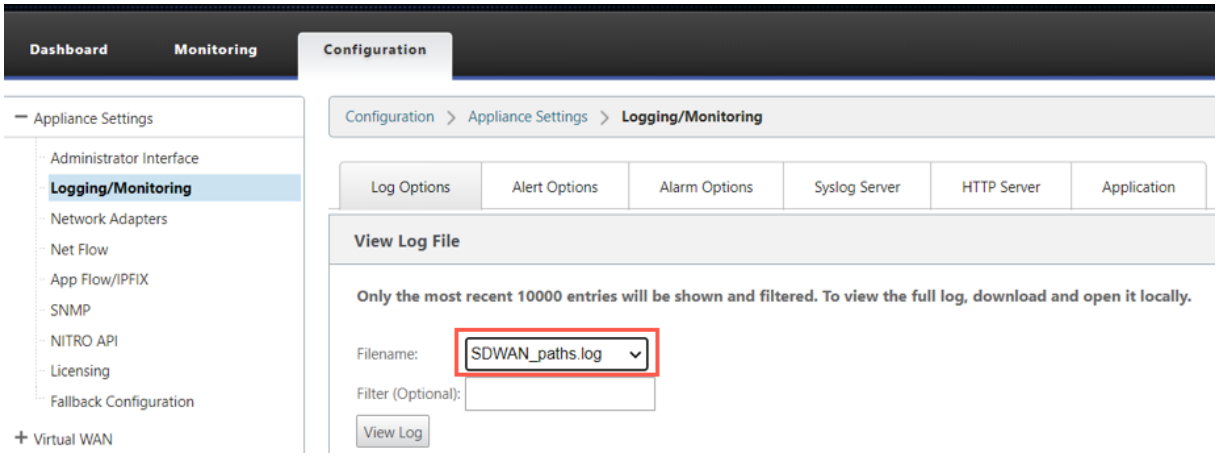
MCN で設定された集約ルートは、仮想パスを経由してブランチに送信されます。ブランチのルートテーブルに仮想パスの詳細が表示されない場合は、ブランチダッシュボードを確認します。ダッシュボードには、MCN とブランチ間の仮想パスのステータスが表示されます。



仮想パスがダウンしている場合は、[構成] **>** [ログ/監視] で、その理由を確認します。

[ファイル名] ドロップダウンリストから、次のいずれかのファイルを選択して、検証します。

- SDWAN_paths.log
- SDWAN_common.log



プロトコルプリファレンス

May 10, 2021

プロトコルの優先設定は、Citrix SD-WAN 固有の機能です。これは、ルータのアドミニストレーティブディスタンスに似ています。

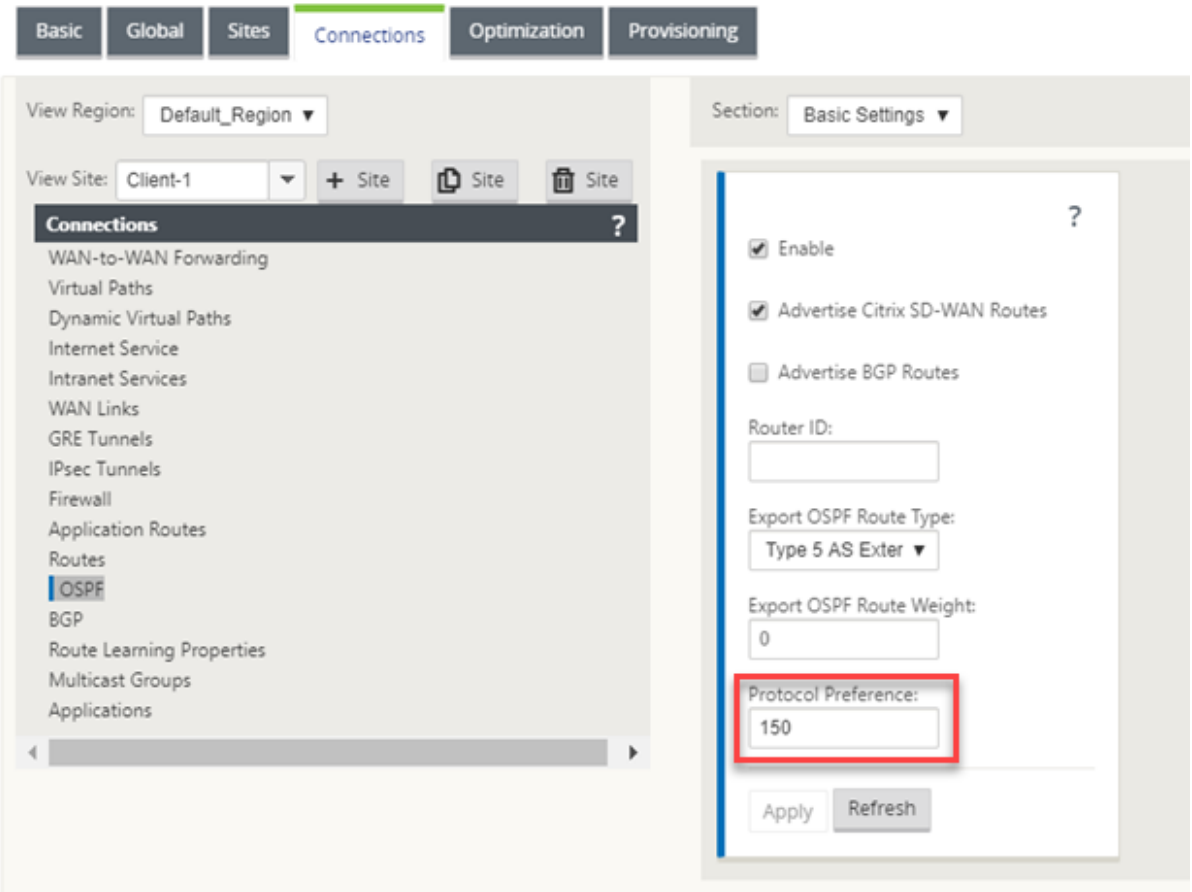
Citrix SD-WAN が仮想パス、OSPF プロトコル、または BGP プロトコルを介してルートプレフィクスを同時に学習する場合、次のデフォルトの優先順位に従います。

- OSPF-150
- BGP-100
- SD-WAN-250

優先順位が最も高いプロトコルが最も優先されます。プロトコルプリファレンス値が最も高いプロトコルを使用するルート

また、BGP または OSPF プロトコルを設定しながら、プロトコルプリファレンス値を設定することで、OSPF プロトコル上で BGP プロトコルを使用することもできます。100 ～200 の範囲でプリファレンスを指定できます。

プロトコルの優先順位情報は Citrix SD-WAN アプライアンスのローカルであり、ピアネットワーク要素にはアドバタイズされません。



マルチキャストルーティング

May 10, 2021

マルチキャストルーティングにより、1 対多のトラフィックを効率的に配信できます。マルチキャスト送信元は、マルチキャストトラフィックを 1 つのストリームでマルチキャストグループに送信します。マルチキャストグループには、マルチキャスト通信に IGMP プロトコルを使用するホストや隣接ルータなどのレシーバが含まれます。Voice over IP、ビデオオンデマンド、IP テレビ、およびビデオ会議は、マルチキャストルーティングを使用する一般的なテクノロジの一部です。Citrix SD-WAN アプライアンスでマルチキャストルーティングを有効にすると、アプライアンスはマルチキャストルーターとして機能します。

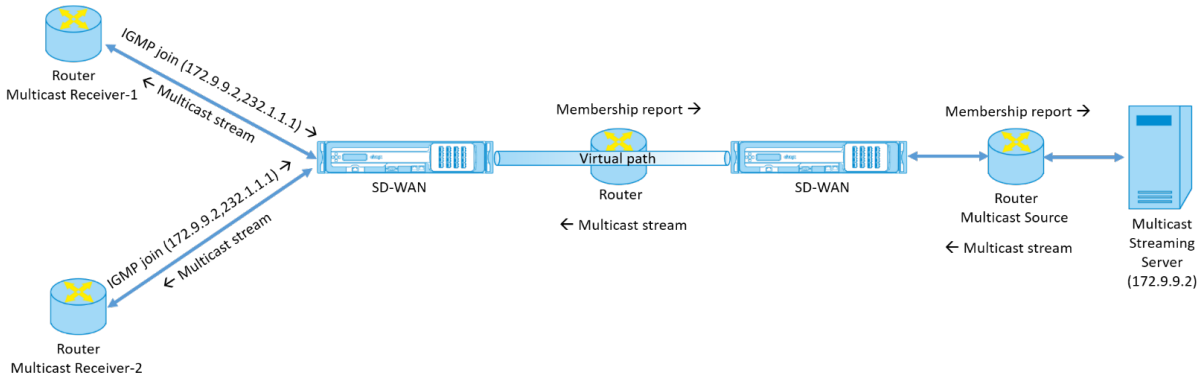
送信元固有のマルチキャスト

通常、マルチキャストプロトコルを使用すると、マルチキャストレシーバは任意の送信元からマルチキャストトラフィックを受信できます。Source Specific Multicast（SSM; ソース固有マルチキャスト）では、レシーバがマルチキャストトラフィックを受信する送信元を指定できます。これにより、レシーバは、マルチキャストストリームを送信

するすべてのソースに対してオープンリスナーではなく、特定のマルチキャストソースをリッスンすることを保証します。SSM は、考えられるすべての送信元からのトラフィックの消費に使用されるリソースのコストを削減します。また、受信者が既知の送信者からのトラフィックを確実に受信することによって、セキュリティ層を提供します。

次のトポロジは、ブランチサイトの 2 つのマルチキャストレシーバと、データセンターの 1 つのマルチキャストサーバ（172.9.9.2）を示しています。マルチキャストサーバは特定のグループ（232.1.1.1）でトラフィックをストリーミングし、レシーバはグループに参加します。マルチキャストグループでストリーミングされるトラフィックは、グループに加入したすべてのレシーバに中継されます。

> 注
>
> SSM が機能するためには、マルチキャストグループ IP が 232.0.0.0/8 の範囲内にある必要があります。



1. マルチキャストレシーバは、IP IGMP Join 要求を送信します。これは、レシーバがマルチキャストグループに加入し、送信元からマルチキャストストリームを受信することを示します。IGMP Join には、マルチキャスト送信元とグループ（S, G）の 2 つの属性が含まれます。IGMP バージョン 3 は、マルチキャスト送信元および受信側の SSM に使用され、一部の include 特定の送信元アドレスをリレーします。SSM を使用すると、レシーバは特定のマルチキャストサーバからストリームを明示的に受信できます。その送信元アドレスは、JOIN 要求の一部としてレシーバによって明示的に提供されます。この例では、IGMP v3 Join 要求が、ソース 172.9.9.2 を含む明示的なインクルード送信元リストを使用してトリガーされ、グループ 232.1.1.1 経由でマルチキャストストリームを送信するアドレスになります。
2. 支店の Citrix SD-WAN は、これらの受信機からのすべての IGMP 要求をリッスンし、それをメンバーシップレポートに変換し、仮想パス経由でデータセンターの SD-WAN アプライアンスに送信します。
3. データセンターの Citrix SD-WAN アプライアンスは、仮想パスを介してメンバーシップレポートを受信し、マルチキャストソースに転送し、制御チャネルを確立します。
4. マルチキャスト送信元は、仮想パスを介してマルチキャストストリームをマルチキャストレシーバに送信します。

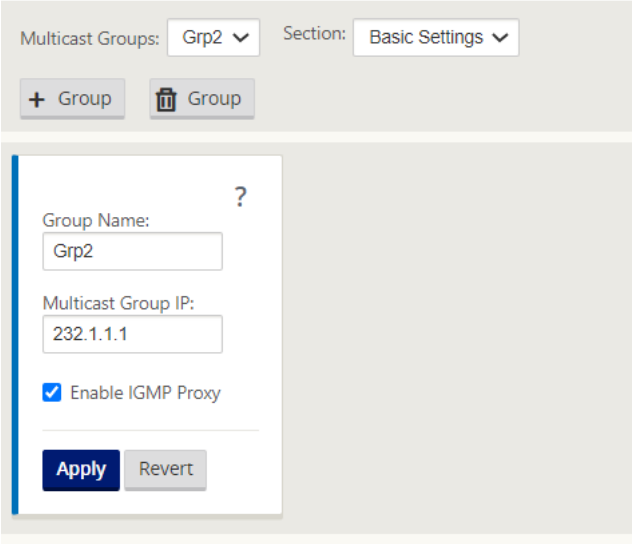
コントロールチャネルトラフィックとマルチキャストストリームは、ブランチとデータセンター間の確立された仮想パスを通過します。Citrix SD-WAN オーバーレイパスにより、マルチキャストトラフィックが WAN の劣化やリンクの停止を防ぐことができます。

マルチキャストの構成

マルチキャストを設定するには、送信元と宛先の両方で SD-WAN アプライアンスで次の操作を実行します。

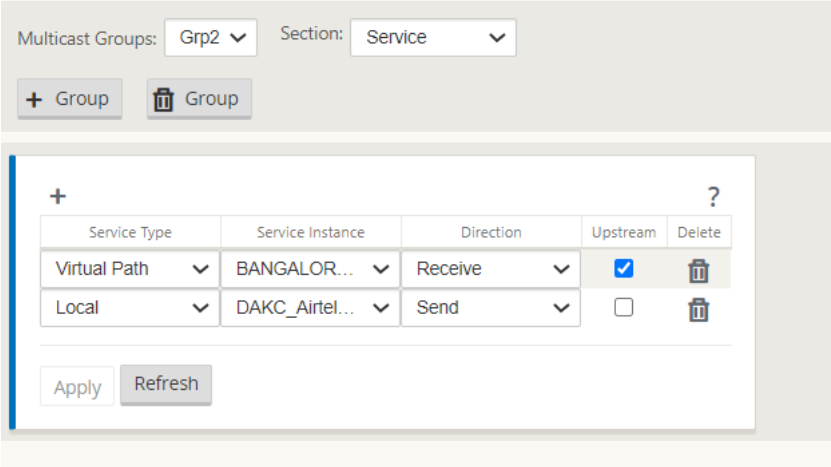
1. マルチキャストグループの作成：マルチキャストグループの名前と IP アドレスを指定します。マルチキャストグループ IP は、送信元固有のマルチキャストに対して 232.0.0.0/8 の範囲内にある必要があります。
2. IGMP プロキシを有効にする—Citrix SD-WAN アプライアンスを IGMP プロキシとして構成し、マルチキャストルーティング用の IGMP 制御チャネル情報を伝送できます。IGMP V3 は、単一送信元マルチキャストに必要です。
3. アップストリームおよびダウンストリームサービスの定義：アップストリームインターフェイスにより、IGMP PROXY は、トラフィックをストリームする実際のマルチキャストソースに近い SD-WAN アプライアンスに接続できます。ダウンストリームインターフェイスを使用すると、IGMP Proxy は、トラフィックをストリームする実際のマルチキャストソースから遠く離れたホストに接続できます。
   アップストリームとダウンストリームのサービスは、ソースのアプライアンスとデスティネーションのアプライアンスで異なります。

Citrix SD-WAN アプライアンスでマルチキャストを構成するには、[接続] > [マルチキャストグループ] に移動します。マルチキャストグループの名前と IP アドレスを指定して、マルチキャストグループを作成します。[**IGMP** プロキシを有効にする] をクリックします。

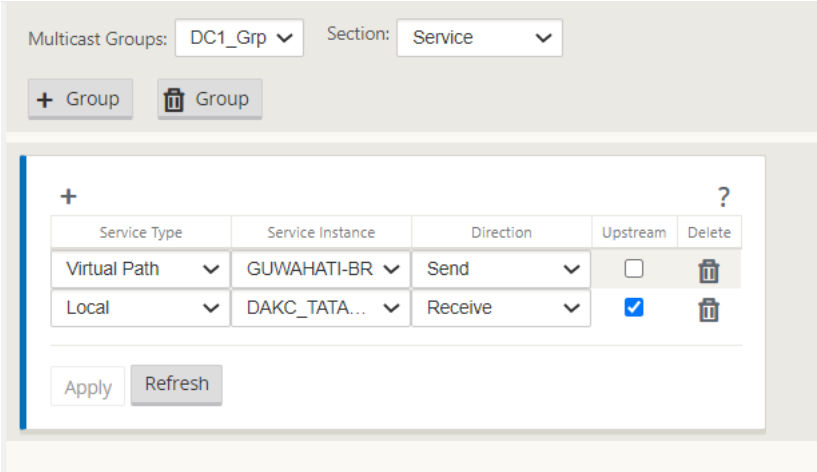


ブランチアプライアンスおよびデータセンターアプライアンスのアップストリームパスとダウンストリームパスを設定します。

アプライアンスがマルチキャストレシーバ（ブランチ）に近い場合、アプライアンスは仮想パスインターフェイスでマルチキャストトラフィックを受信し、ローカルインターフェイス上のトラフィックを受信者に送信します。



アプライアンスがマルチキャストソース（データセンター）に近い場合、アプライアンスはローカルインターフェイスでマルチキャストトラフィックを受信し、仮想パスインターフェイス上でトラフィックを送信します。

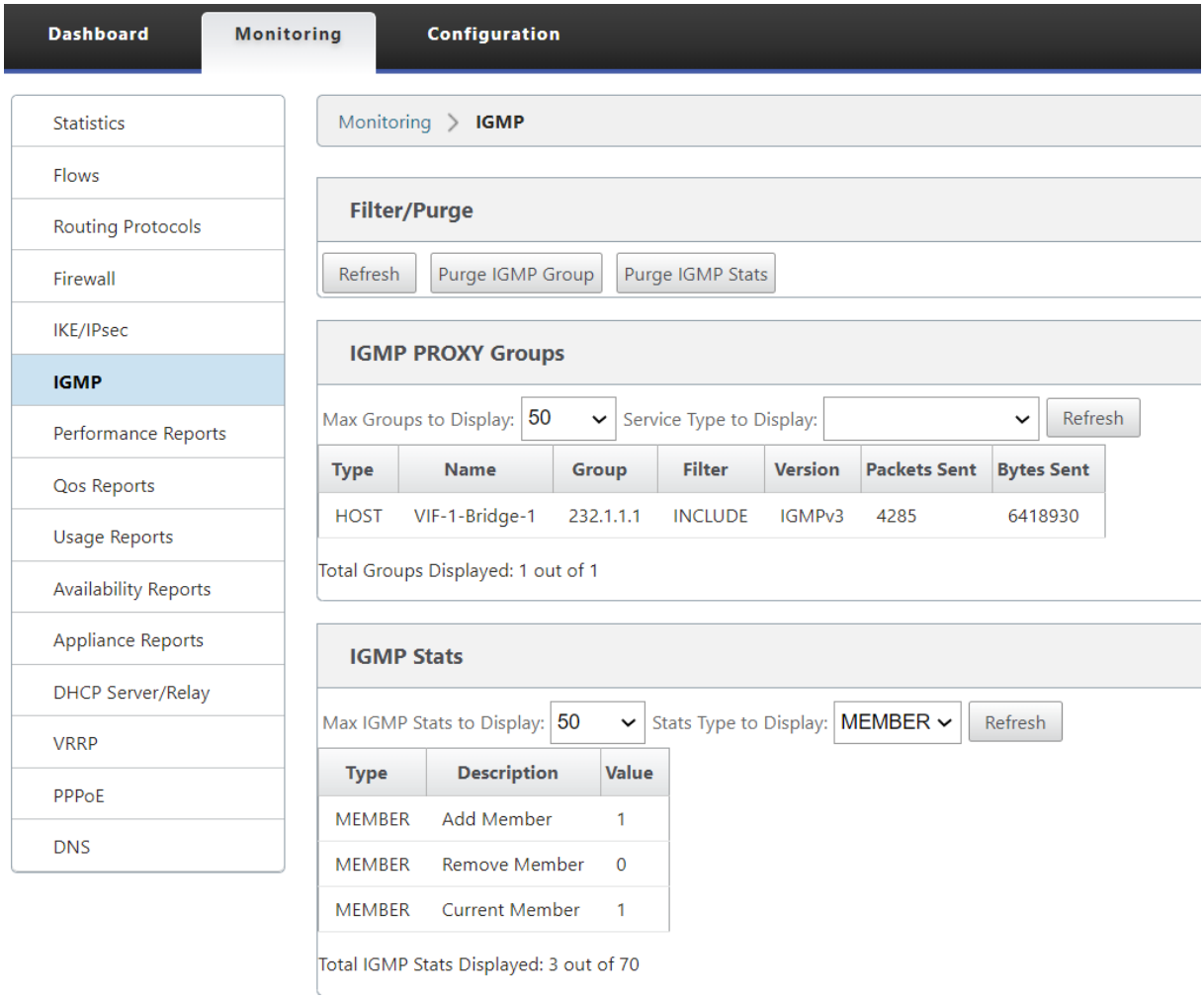


監視

IGMP 統計情報

マルチキャストレシーバが加入グループ要求を開始すると、アプライアンスの [**Monitoring**] > [**IGMP**] でレシーバの詳細を確認できます。この情報は、発信元と宛先の両方のアプライアンスで確認できます。

次の図は、IGMP バージョン 3 の加入が開始され、特定の送信元アドレスを含めるためにフィルタタイプの INCLUDE が使用されていることを示しています。IGMP メンバーの統計情報も確認できます。



仮想パスルートコストの構成

May 10, 2021

Citrix SD-WAN では、データセンター管理に関連する次のルーティング機能強化がサポートされています。

たとえば、北米とヨーロッパの 2 つのデータセンターを持つ SD-WAN ネットワークを考えます。北米のすべてのサイトで北米のデータセンターを経由するトラフィックをルーティングし、ヨーロッパのすべてのサイトで欧州のデータセンターを使用したいとします。これまでは、SD-WAN 9.3 以前のリリースバージョンでは、データセンター管理のこの機能はサポートされていませんでした。これは、仮想パスルートコストの導入によって実装されます。

- 仮想パスルートコスト：ルートがリモートサイトから学習されたときにルートコストに追加される個々の仮想パスに対して、仮想パスルートコストを設定できます。

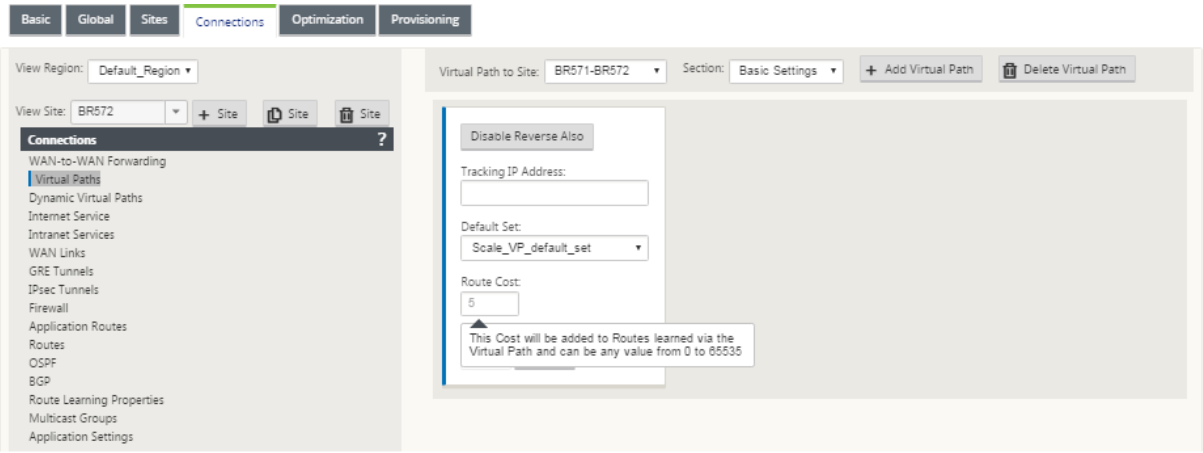
この機能により、WAN から WAN への転送コストが無効化または削除されます。

- OSPF ルートコスト：インポートフィルタで [OSPF ルートコストのコピー**]** を有効にすると、**OSPF** ルートコスト（タイプ 1 メトリック）をインポートできるようになりました。OSPF ルートコストは、SD-WAN コストではなく、ルート選択で考慮されます。15 ではなく 65534 までのコストがサポートされますが、ルートがリモートサイトから学習された場合に追加される適切な仮想パスルートコストに対応することをお勧めします。
- BGP-MED への VP コスト：SD-WAN ルートを BGP ピアにエクスポート（再配布）するときに、SD-WAN ルートの仮想パスルートコストを BGP MED 値にコピーできるようになりました。これは、BGP ポリシーを作成し、各ネイバーの「OUT」方向に適用することで、個々のネイバーに対して設定できます。
- どのサイトも、他のサイトへの複数の仮想パスを持つことができます。場合によっては、より多くの仮想パスを経由してサービスに接続できるブランチがある場合、ブランチサイトから 2 つの仮想パスが存在することがあります。一方の仮想パスは DC1 を経由し、もう一方の仮想パスは DC2 を経由します。DC1 は MCN であり、DC2 は Geo-MCN であり、静的仮想パスを持つ別のサイトとして構成できます。
- 各 VP の既定のコストを 1 として追加します。仮想パスルートコストは、サイトの各仮想パスにコストを関連付けるのに役立ちます。これは、デフォルトのサイトコストではなく、特定の仮想パス上のルート交換/更新を操作するのに役立ちます。これにより、トラフィックを送信するためにどのデータセンターを優先するかを操作できます。
- 各 VP の小さい範囲（1 ～10 など）でコストを設定できます。
- ダイナミックルーティングで学習したルートを含め、ルーティングプリファレンスを示すために、ネイバーサイトと共有するすべてのルートに仮想パスコストを追加する必要があります。
- 静的仮想パスは、動的仮想パスよりも低コストである必要はありません。

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

仮想パスルートコストの設定方法

仮想パスルートは、SD-WAN GUI で、[接続] > [リージョンの表示**] > [**サイトの表示**] > [**仮想パス**] > [**基本設定**]** の下で構成できます。すべてのルートは、基本的な Citrix SD-WAN コスト +VP のルートコストとともにインストールされ、複数の仮想パスのルートコストに影響を与えます。



ユースケース:

たとえば、サブネット 172.16.2.0/24 と 172.16.3.0/24 があります。両方のサブネットを使用して SD-WAN にトラフィックを送信するデータセンターの DC1 と DC2 が 2 つあるとします。デフォルトの仮想パスルートコストでは、ルーティングに影響を与えることはできません。これは、最初にインストールされたルートによって、最初に DC2 または DC1 のいずれかになることができるからです。

仮想パスを使用すると、DC2 仮想パスのほうが仮想パスルートコスト（10 など）が大きくなり、DC1 のデフォルト VP ルートコストは 5 になります。この操作は、DC1 を最初に、DC2 を次に、両方のルートをインストールするのに役立ちます。

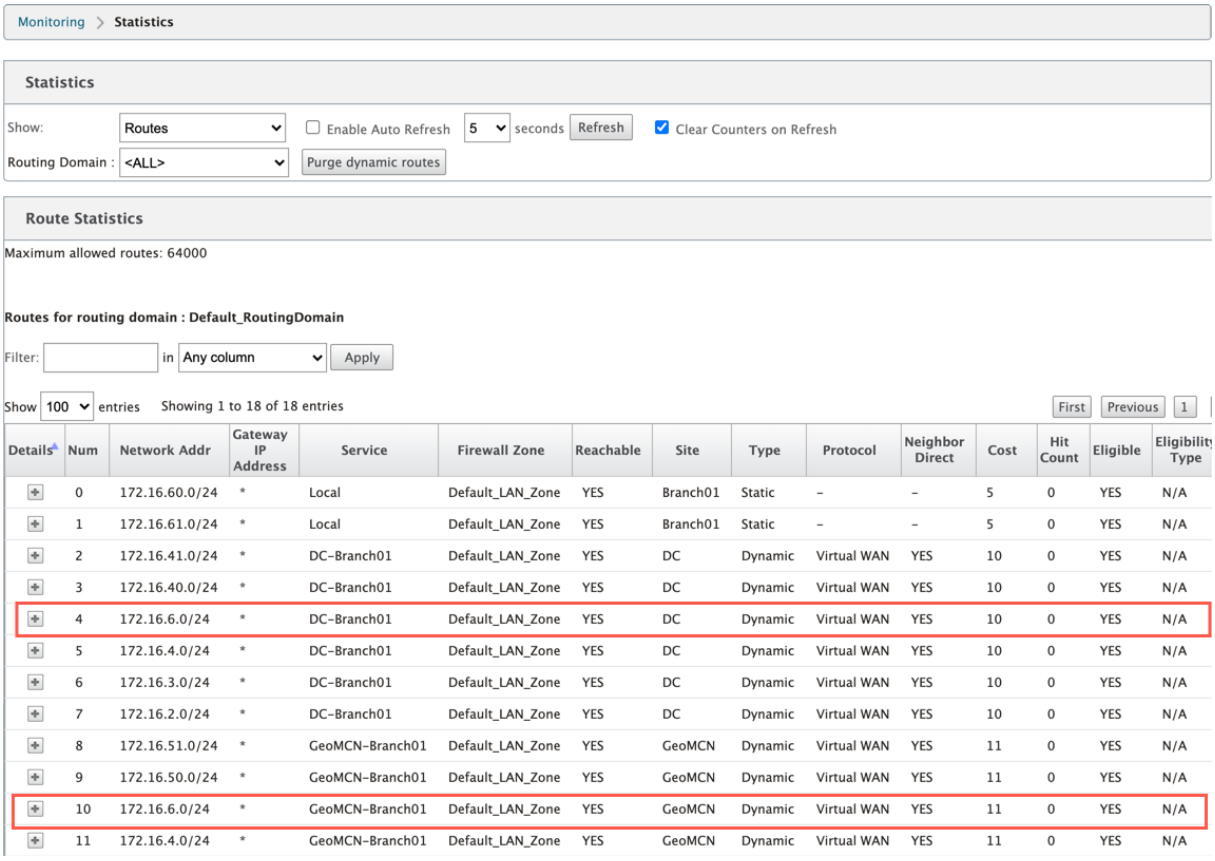
4 つのルートがあり、2 つのルートは 172.16.2.0/24 までです。1 つは低コストで DC1 経由で、1 つは高コストで DC2 経由で、172.16.3.0/24 の場合はさらに 2 つです。

監視とトラブルシューティング

ルーティングテーブルには、仮想パス経由でブランチサイトに接続されている 2 つのサイトによってアドバタイズされた同じサブネットが、仮想パスのルートコストを追加したコストよりも優先してインストールされる方法が表示されます。

ルートコストおよびルーティングテーブルで使用されているルートを確認するには、[モニタリング**] > [**統計**] >** [表示] フィールドの下に移動し、[ルート] を選択します。ルートコストとヒット数は、同じページで確認できます。

次の図は、同じルートの 2 つの異なるコストを持つルートテーブルを示しています。このコストは 172.16.6.0/24 で、サービス **DC-Branch01** と GEOMCN-Branch01** のコストは 10 と 11 です。



Details	Num	Network Addr	Gateway IP Address	Service	Firewall Zone	Reachable	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type
	0	172.16.60.0/24	*	Local	Default_LAN_Zone	YES	Branch01	Static	-	-	5	0	YES	N/A
	1	172.16.61.0/24	*	Local	Default_LAN_Zone	YES	Branch01	Static	-	-	5	0	YES	N/A
	2	172.16.41.0/24	*	DC-Branch01	Default_LAN_Zone	YES	DC	Dynamic	Virtual WAN	YES	10	0	YES	N/A
	3	172.16.40.0/24	*	DC-Branch01	Default_LAN_Zone	YES	DC	Dynamic	Virtual WAN	YES	10	0	YES	N/A
	4	172.16.6.0/24	*	DC-Branch01	Default_LAN_Zone	YES	DC	Dynamic	Virtual WAN	YES	10	0	YES	N/A
	5	172.16.4.0/24	*	DC-Branch01	Default_LAN_Zone	YES	DC	Dynamic	Virtual WAN	YES	10	0	YES	N/A
	6	172.16.3.0/24	*	DC-Branch01	Default_LAN_Zone	YES	DC	Dynamic	Virtual WAN	YES	10	0	YES	N/A
	7	172.16.2.0/24	*	DC-Branch01	Default_LAN_Zone	YES	DC	Dynamic	Virtual WAN	YES	10	0	YES	N/A
	8	172.16.51.0/24	*	GeoMCN-Branch01	Default_LAN_Zone	YES	GeoMCN	Dynamic	Virtual WAN	YES	11	0	YES	N/A
	9	172.16.50.0/24	*	GeoMCN-Branch01	Default_LAN_Zone	YES	GeoMCN	Dynamic	Virtual WAN	YES	11	0	YES	N/A
	10	172.16.6.0/24	*	GeoMCN-Branch01	Default_LAN_Zone	YES	GeoMCN	Dynamic	Virtual WAN	YES	11	0	YES	N/A
	11	172.16.4.0/24	*	GeoMCN-Branch01	Default_LAN_Zone	YES	GeoMCN	Dynamic	Virtual WAN	YES	11	0	YES	N/A

仮想ルータ冗長プロトコルの設定

May 10, 2021

Virtual Router Redundancy Protocol（VRRP）仮想ルータ冗長プロトコル）は、デバイスの冗長性を提供し、スタティックデフォルトルーティング環境に固有の単一障害点を排除する、広く使用されているプロトコルです VRRP を使用すると、1 つのグループを形成するように 2 つ以上のルータを設定できます。このグループは、1 つの仮想 IP アドレスと 1 つの仮想 MAC アドレスを持つ単一のデフォルト Gateway として表示されます。

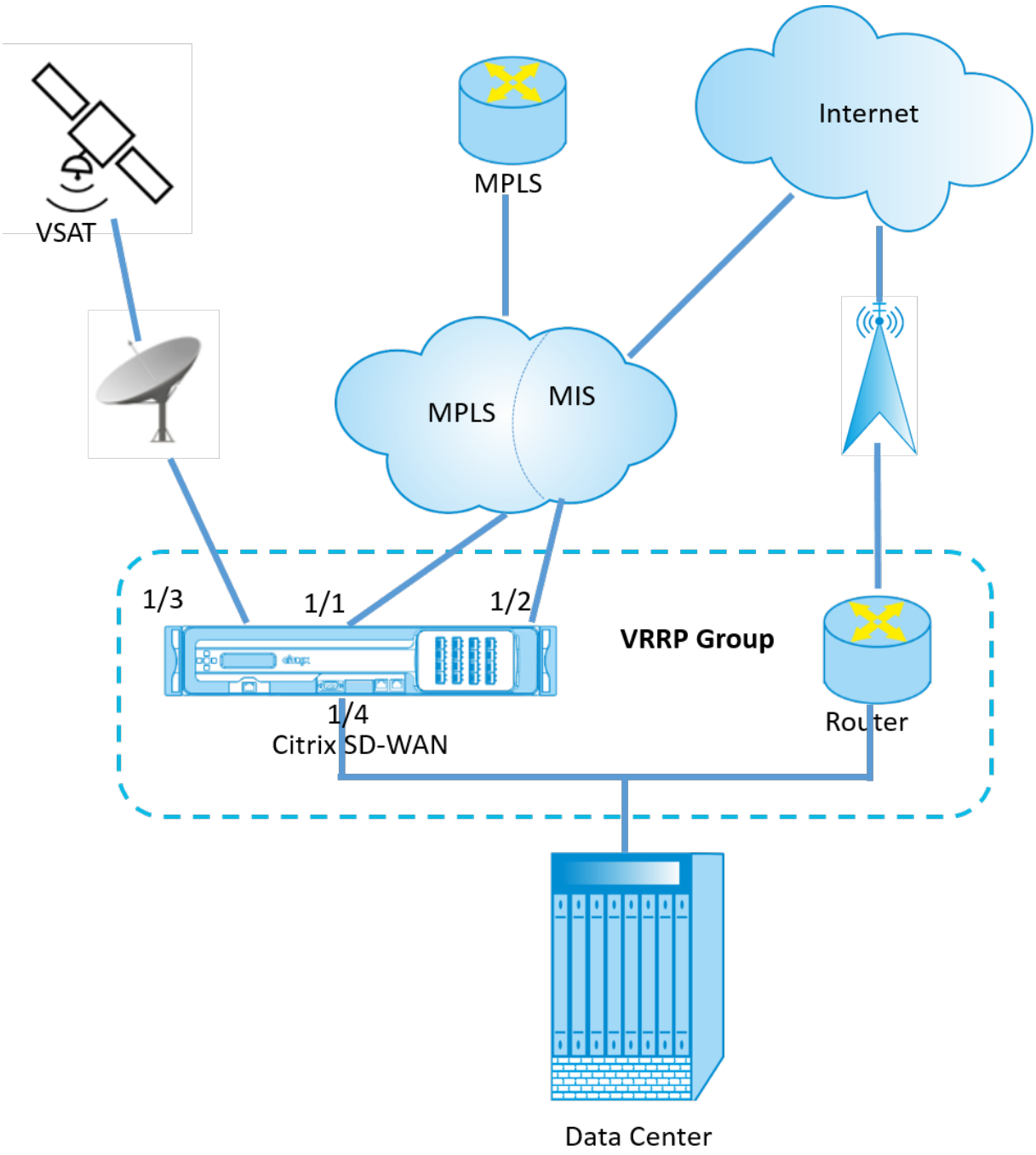
プライマリ/マスタールータに障害が発生すると、バックアップルータが自動的に引き継ぎます。VRRP 設定では、マスタールータは、アドバタイズメントと呼ばれる VRRP パケットをバックアップルータに送信します。マスタールータがアドバタイズメントの送信を停止すると、バックアップルータはインターバルタイマーを設定します。この保留期間内にアドバタイズメントが受信されない場合、バックアップルータはフェールオーバールーチンを開始します。

VRRP は、プライオリティが最も高いルータがマスターになる選択プロセスを指定します。ルータ間でプライオリティが同じ場合、IP アドレスの最も大きいルータがマスターになります。他のルータはバックアップ状態です。マスターに障害が発生した場合、新しいルータがグループに加入した場合、または既存のルータがグループを離れると、再び選出プロセスが開始されます。

VRRP は、すべてのエンドホストでダイナミックルーティングまたはルータディスカバリプロトコルを設定せずに、高可用性デフォルトパスを保証します。

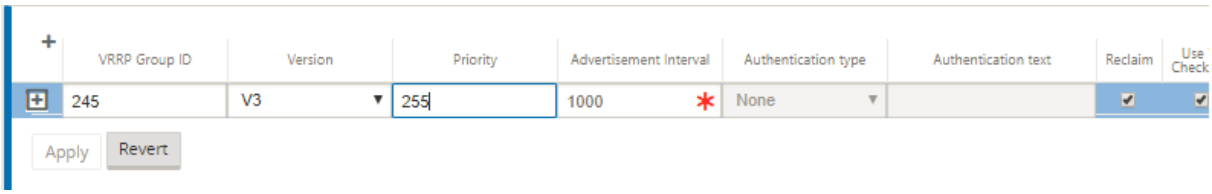
Citrix SD-WAN リリースバージョン 10.1 では、VRRP バージョン 2 およびバージョン 3 がサポートされ、サードパーティ製のルーターとの相互動作が可能です。SD-WAN アプライアンスはマスタールータとして機能し、サイト間で仮想パスサービスを使用するようにトラフィックを誘導します。仮想インターフェイス IP を VRRP IP として設定し、手動でプライオリティをピアルータよりも高い値に設定することで、SD-WAN アプライアンスを VRRP マスターとして設定できます。アドバタイズメント間隔と preempt オプションを設定できます。

以下のネットワーク図は、Citrix SD-WAN アプライアンスと VRRP グループとして構成されたルーターを示しています。SD-WAN アプライアンスはマスターとして設定されています。SD-WAN アプライアンスに障害が発生した場合、バックアップルータはミリ秒以内に停止し、ダウンタイムが発生しないようにします。



VRRP インスタンスを設定するには、次の手順を実行します。

1. 構成エディタで、[サイト] > [サイト名**] > [VRRP**] に移動し、[**+**] をクリックします。



1. VRRP インスタンスを設定します。次のフィールドに値を入力します。

- **VRRP** グループ **ID**: VRRP グループ ID。グループ ID は、1 ～255 の値の範囲である必要があります。バックアップルータでも同じグループ ID を設定する必要があります。

> 注
>
> 現時点では、最大 4 つのグループしか構成できません。

- バージョン: VRRP プロトコルのバージョン。VRRP プロトコル V2 と V3 のいずれかを選択できます。
- 優先度: VRRP グループの Citrix SD-WAN アプライアンスの優先度。プライオリティの範囲は 1 ～254 です。SD-WAN アプライアンスをマスターにするには、この値を maximum（254）に設定します。

> 注
>
> ルータが VRRP IP アドレスの所有者である場合、プライオリティはデフォルトで 255 に設定されます。

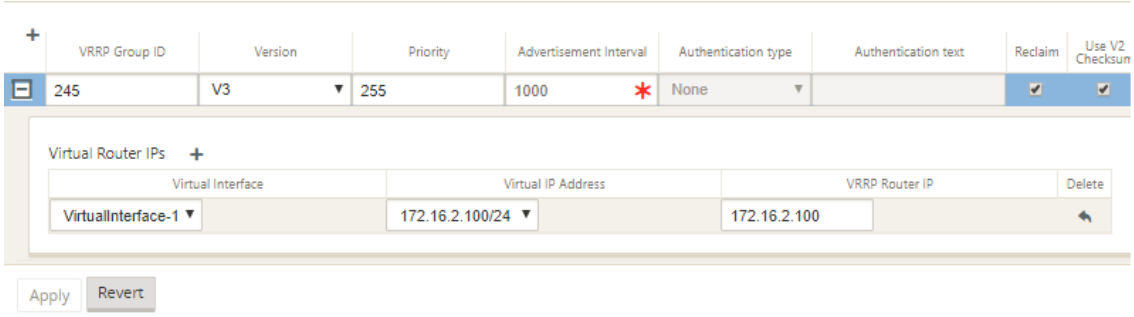
- **Advertisement Interval**: SD-WAN アプライアンスがマスターであるときに VRRP アドバタイズメントが送信される頻度（ミリ秒単位）。デフォルトのアドバタイズメント間隔は 1 秒です。
- 認証タイプ**:** [プレーンテキスト] を選択して、認証文字列を入力できます。認証文字列は、VRRP アドバタイズメントで暗号化なしでプレーンテキストとして送信されます。認証を設定しない場合は、[**None**] を選択します。
- 認証テキスト: VRRP アドバタイズメントで送信される認証文字列。このオプションは、認証の種類 が プレーンテキストの場合に有効になります。

> 注
>
> 認証は VRRPv2 でのみサポートされます。

- 再利用: VRRP グループで SD-WAN アプライアンスのプライオリティが最も高い場合に、プリエンプションを有効にします。これは VRRP 選定プロセスで使用されます。
- **V2** チェックサムを使用: VRRPv3 のサードパーティネットワークデバイスとの互換性を有効にします。デフォルトでは、VRRPv3 は v3 チェックサム計算方式を使用します。一部のサードパーティデバイスでは、VRRPv2 チェックサム計算しかサポートされない場合があります。そのような場合は、このオプションを有効にします。

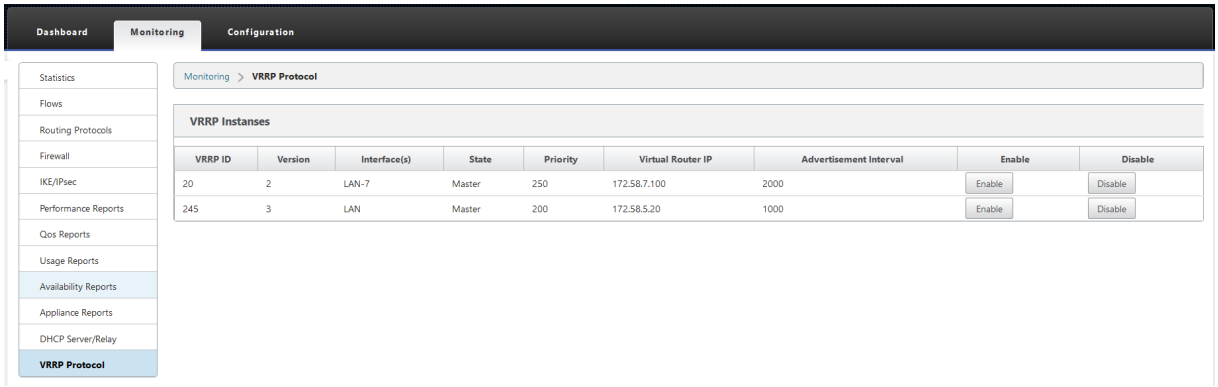
VRRP IP アドレスを設定します。次のフィールドに値を入力し、[適用] をクリックします。

- 仮想インターフェイス: VRRP に使用される仮想インターフェイス。設定済みの仮想インターフェイスの 1 つを選択します。
- 仮想 **IP** アドレス: 仮想インターフェイスに割り当てられた仮想 IP アドレス。仮想インターフェイスに設定済みの仮想 IP アドレスのいずれかを選択します。
- **VRRP** ルータ **IP**: VRRP グループの仮想ルータ IP アドレス。デフォルトでは、SD-WAN アプライアンスの仮想 IP アドレスが仮想ルータ IP アドレスとして割り当てられます。



VRRP 統計情報

VRRP 統計情報は、[モニタリング] > [**VRRP** プロトコル] の下に表示されます。



次の統計データを表示できます。

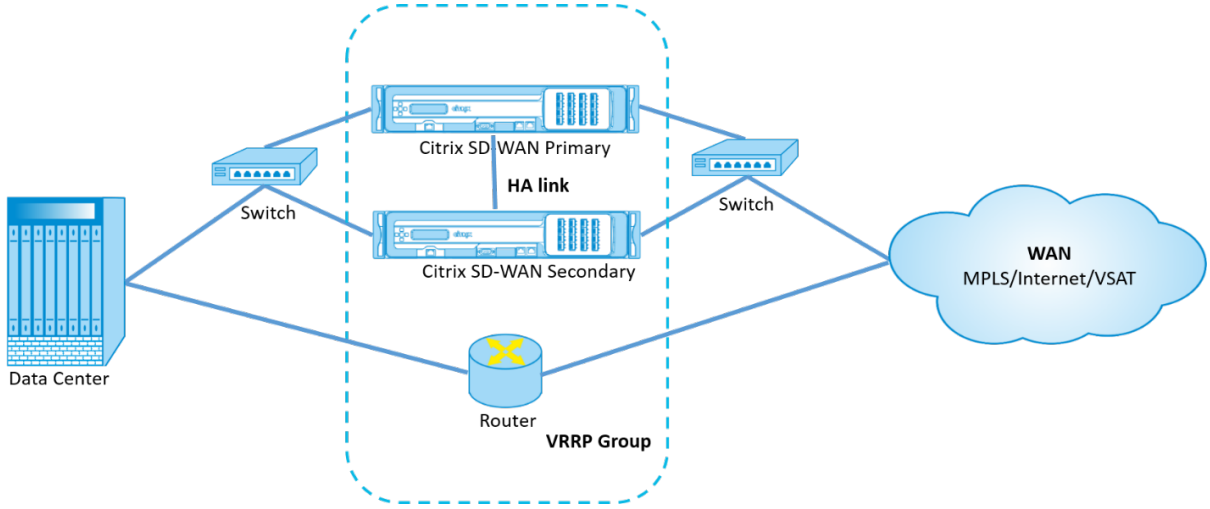
- **VRRP ID**： VRRP グループ ID
- バージョン： VRRP プロトコルのバージョン。
- インターフェイス： VRRP に使用される仮想インターフェイス。
- 状態： SD-WAN アプライアンスの VRRP 状態。アプライアンスがマスターかバックアップかを示します。
- プライオリティ： VRRP グループの SD-WAN アプライアンスのプライオリティ
- 仮想ルータ **IP**： VRRP グループの仮想ルータ IP アドレス。
- アドバタイズメント間隔： VRRP アドバタイズメントの頻度。
- [**Enable**]： SD-WAN アプライアンスで VRRP インスタンスを有効にする場合は、これを選択します。
- [無効]**:** SD-WAN アプライアンスの VRRP インスタンスを無効にする場合は、これを選択します。

制限事項

- VRRP は、ゲートウェイモード配置でのみサポートされます。
- 最大 4 つの VRRP ID（VRID）を設定できます。
- VRID には、最大 16 個の仮想ネットワークインターフェイスを使用できます。

高可用性および **VRRP**

SD-WAN ネットワーク上の高可用性機能と VRRP 機能の両方を利用することで、ネットワークのダウンタイムとトラフィックの中断を大幅に削減できます。アクティブ/スタンバイの役割で Citrix SD-WAN アプライアンスのペアをスタンバイルーターとともに展開し、VRRP グループを形成します。このグループは、1 つの仮想 IP アドレスと 1 つの仮想 MAC アドレスを持つ単一のデフォルト Gateway として表示されます。



上記の展開では、次の 2 つのケースがあります。

1 番目のケース：**SD-WAN** での高可用性フェールオーバータイマーは、**VRRP** フェールオーバータイマーと同じです。

予想される動作は、VRRP スイッチオーバーの前に高可用性スイッチオーバーが発生することです。つまり、トラフィックは新しい Active SD-WAN アプライアンスを引き続き通過します。この場合、SD-WAN は VRRP マスターロールを継続します。

2 番目のケース：**VRRP** フェールオーバータイマーよりも大きい **SD-WAN** での高可用性フェールオーバータイマーです。

想定される動作は、ルータへの VRRP スイッチオーバーが発生することです。つまり、ルータが VRRP マスターになり、トラフィックが SD-WAN アプライアンスをバイパスして、ルータを一時的に流れる可能性があります。

ただし、高可用性スイッチオーバーが発生すると、SD-WAN が再び VRRP マスターになります。つまり、トラフィックは新しいアクティブ SD-WAN アプライアンスを通過します。

高可用性デプロイモードの詳細については、高可用性を参照してください。

ネットワークオブジェクトの構成

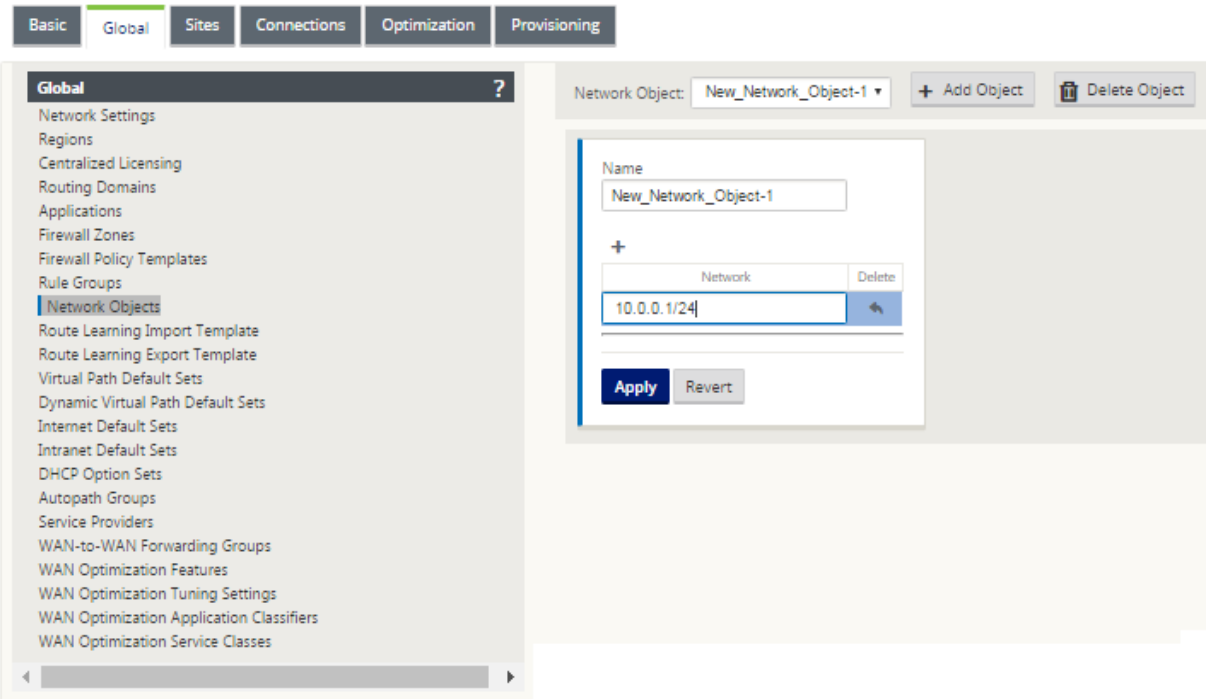
May 10, 2021

Citrix SD-WAN では、構成エディタの［グローバル］パネルにネットワークオブジェクトを追加するオプションが導入されています。ルートフィルタを定義するときに、サブネットごとにフィルタを作成するのではなく、複数のサブネットをまとめてグループ化し、1 つのネットワークオブジェクトを参照できます。

ネットワーク・オブジェクトを構成するには、次の手順に従います。

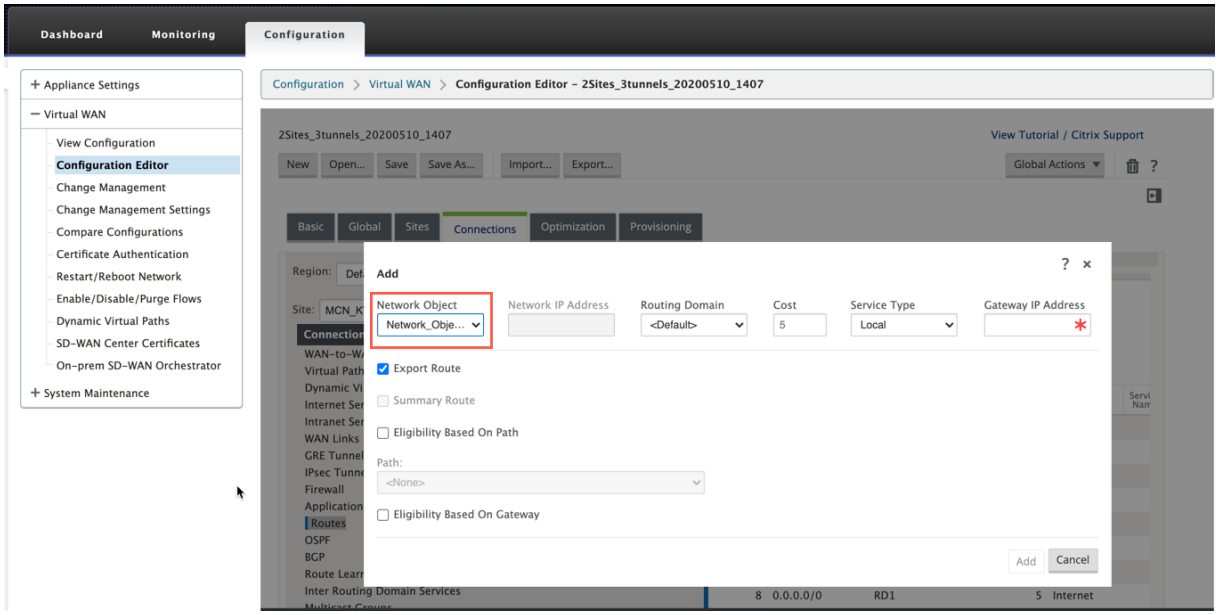
1. 設定エディタで、グローバル → ネットワークオブジェクトに移動し、追加（**+**）をクリックします。
2. [ネットワーク] の下の [追加] **(+)** をクリックします。
3. 新しいネットワークオブジェクトの **IP** アドレス と サブネット を入力します。
4. [適用] をクリックして設定を保存します。

ネットワークオブジェクトの名前を編集するには、ネットワークオブジェクトの名前をクリックし、新しい名前を入力します。

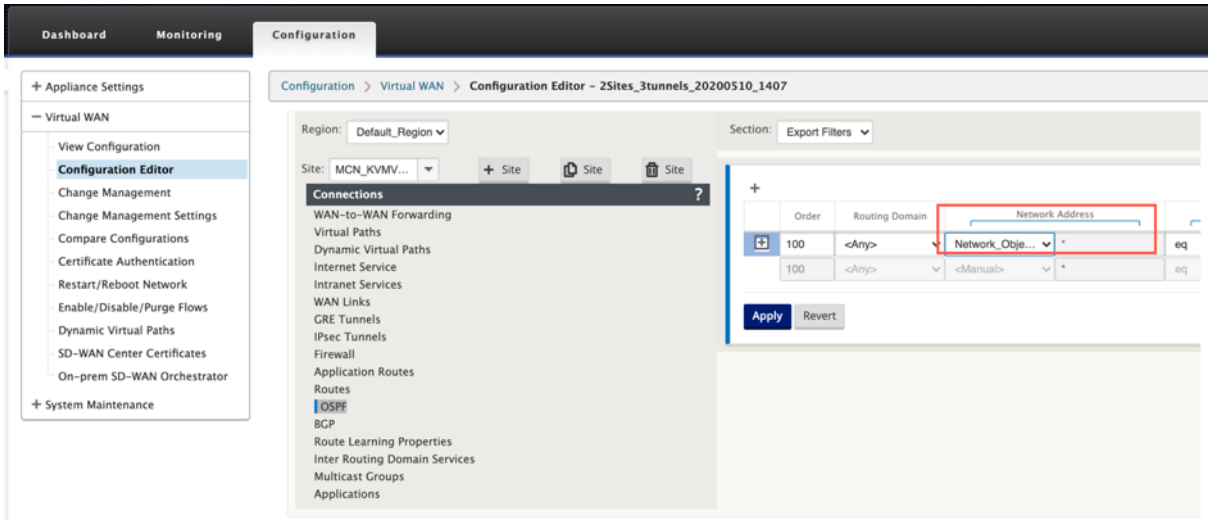


次の機能は、ネットワークオブジェクトを利用しています。

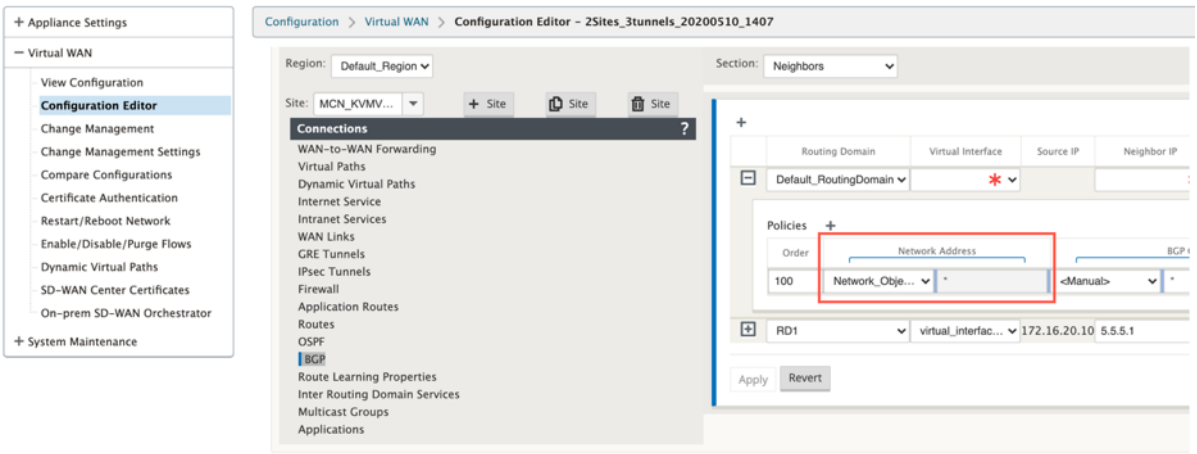
- ルート（設定エディタ **>** 接続 **>** ルート **>+** をクリック > ネットワークオブジェクト）



- BGP および OSPF インポートおよびエクスポートフィルタ（コンフィギュレーションエディタ **>** 接続 **> BGP/OSPF >** エクスポート/インポートフィルタ **>+** をクリック **>** ネットワークアドレス）



- BGP ネイバーポリシー（コンフィギュレーションエディタ **>** 接続 **> BGP >** ネイバー **>** ポリシー **>+** をクリック **>** ネットワークアドレス）



LAN セグメンテーションのルーティングサポート

May 10, 2021

SD-WAN Standard および Premium (Enterprise) Edition アプライアンスは、いずれかのアプライアンスが展開されている個別のサイト間で LAN セグメンテーションを実装します。アプライアンスは、使用可能な LAN 側 VLAN の記録を認識して維持し、別の SD-WAN 標準または Premium（Enterprise）Edition アプライアンスと遠隔地で接続できる他の LAN セグメント（VLAN）に関するルールを構成します。

上記の機能は、SD-WAN Standard または Premium（Enterprise）Edition アプライアンスで維持される Virtual Routing and Forwarding（VRF; 仮想ルーティングおよび転送）テーブルを使用して実装されます。このテーブルは、ローカル LAN セグメントにアクセス可能なリモート IP アドレス範囲を追跡します。この VLAN 間トラフィックは、2 つのアプライアンス間で確立された同じ仮想パスを経由して WAN を通過します（新しいパスを作成する必要はありません）。

この機能のユースケースの例として、WAN 管理者は VLAN を介してローカルブランチネットワーク環境をセグメント化でき、それらのセグメント（VLAN）の一部をインターネットにアクセスできる DC 側の LAN セグメントに提供する一方で、そのようなアクセスを取得できない場合もあります。VLAN と VLAN の関連付けの設定は、SD-WAN 管理 Web インターフェイスの MCN の構成エディタを使用して行います。

安全なピアリング

May 10, 2021

Premium (Enterprise) Edition アプライアンスはデータセンターにインストールでき、自動または手動によるセキュアピアリングの開始、SSL プロファイルの作成、サービスクラスの関連付け、Windows ドメインコントローラ

へのアプライアンスの参加が可能なため、ユーザー/管理者がスタンドアロン WANOP の拡張された豊富な機能を使用できます。アプライアンス。

次に、自動セキュアピアリングと手動セキュアピアリングでサポートされている展開モードを示します。

自動セキュアピアリングの展開:

「DC サイトのスタンドアロン WANOP/SDWAN SE/WANOP から PE アプライアンスへの自動セキュアピアリングを実行するには」を参照してください。

この展開を開始する手順:

- WANOP DC アプライアンスはリスニングオンモード(2312/非標準ポート)で、ブランチ PE は CONNECT-TO モードです。
- WANOP DC は PE アプライアンスへの自動セキュアピアリングを開始します。このピアリングは、プライベート CA 証明書と CERT キーペアをインストールし、WANOPs LISTEN-ON IP を使用して PE アプライアンスに CONNECT-TO を設定します。

「DC サイトおよびブランチサイト PE アプライアンスで PE アプライアンスから開始される自動セキュアピアリングを実行するには」を参照してください。

この展開を開始する手順:

- PE DC アプライアンスは、リスニングオンモード（ポート 443）です。ブランチ PE は CONNECT-to モードです。
- PE DC アプライアンスは、PE ブランチアプライアンスへの自動セキュアピアリングを開始します。このアプライアンスは、プライベート CA 証明書と CERT キーペアをインストールし、DC PE の LISTEN-ON IP を使用して PE ブランチアプライアンスに CONNECT-TO を設定します。
- PE の LISTEN-ON IP は、「WANOP にリダイレクト」が有効になっているルーティングドメインに関連付けられたインターフェイス IP にあります。

自動セキュアピアリングは、WANOP/SDWAN SE アプライアンスで DC サイトおよびブランチの PE アプライアンスから開始されます。

この展開を開始する手順:

- PE DC アプライアンスは、リスニングオンモード（ポート 443）です。ブランチ WANOP/SD-WAN SE は、接続モードです。
- PE DC アプライアンスは、ブランチ WANOP または SD-WAN SE アプライアンスへの自動セキュアピアリングを開始します。このアプライアンスは、プライベート CA 証明書と CERT キーペアをインストールし、DC PE の LISTEN-ON IP を使用して PE アプライアンスに CONNECT-TO を設定します。

セキュアピアリングの手動展開:

「DC サイトの PE アプライアンスからブランチ PE アプライアンスへの手動セキュアピアリングを開始」を参照してください。

この展開を開始する手順:

- PE DC アプライアンスは、リスニングオンモード（ポート 443）です。ブランチ PE は CONNECT-to モードです。
- PE の LISTEN-ON IP は、「WANOP にリダイレクト」が有効になっているルーティングドメインに関連付けられたインターフェイス IP にあります。
- 認証局の認証元から取得した CA と Cert Key のペア証明書を手動でアップロードします。

DC サイトの PE アプライアンスからブランチ WANOP/SDWAN-SE アプライアンスへの手動セキュアピアリングが開始されます。

この展開を開始する手順:

- PE DC アプライアンスは、リスニングオンモード（ポート 443）です。ブランチ WANOP/SD-WAN SE は、接続モードです。
- PE の LISTEN-ON IP は、「WANOP にリダイレクト」が有効になっているルーティングドメインに関連付けられたインターフェイス IP 内にある
- 認証局の認証元から取得した CA と Cert Key のペア証明書を手動でアップロードします。

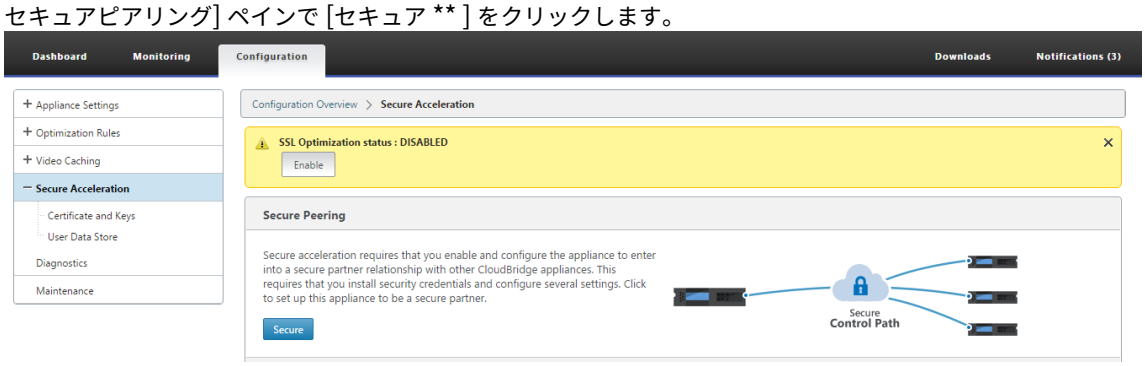
DC サイトのスタンドアロン SD-WAN SE および WANOP アプライアンスから PE アプライアンスへの自動セキュアピアリング

May 10, 2021

DC 側のスタンドアロンの SD-WAN SE および WANOP アプライアンスから PE アプライアンスで自動セキュアピアリングを実行するには、次の手順を実行します。

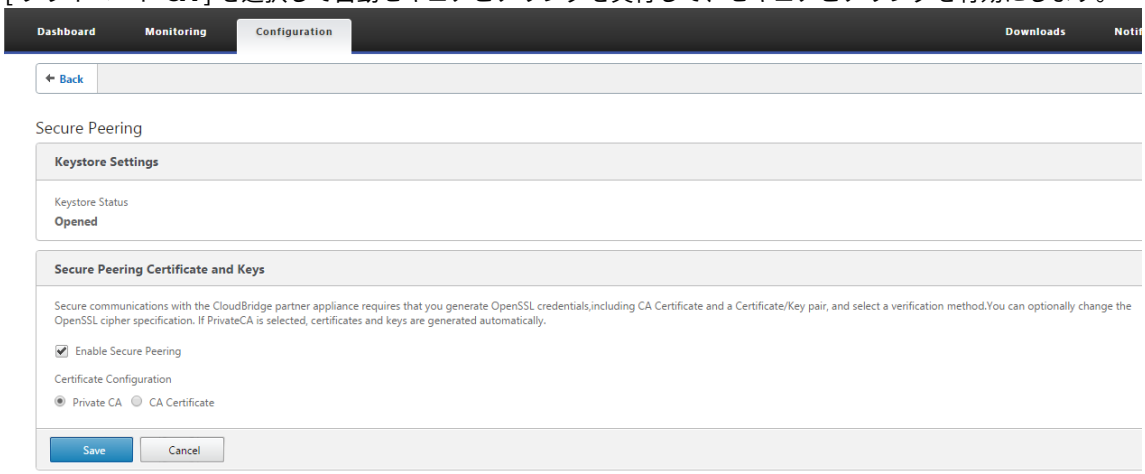
- WANOP DC アプライアンスは、リスニングオンモード（2312/非標準ポート）です。
- ブランチ PE アプライアンスは CONNECT-to モードです。
- WANOP DC は PE アプライアンスへの自動セキュアピアリングを開始します。このピアリングは、プライベート CA 証明書と CERT キーペアをインストールし、WANOPs LISTEN-ON IP を使用して PE アプライアンスに CONNECT-TO を設定します。

1. データセンターのスタンドアロン WANOP アプライアンスで、[セキュアアクセラレーション] ページの **[** セキュアピアリング]** ペインで [セキュア **] をクリックします。



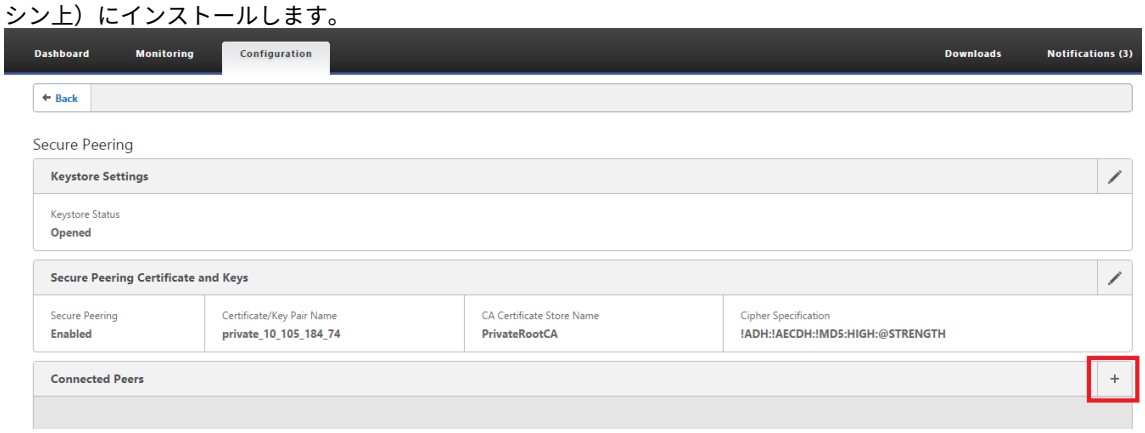
2. キーストアの パスワードを入力するか、キーストア を無効にして、キーストア設定を構成します。

3. [プライベート **CA**] を選択して自動セキュアピアリングを実行して、セキュアピアリングを有効にします。



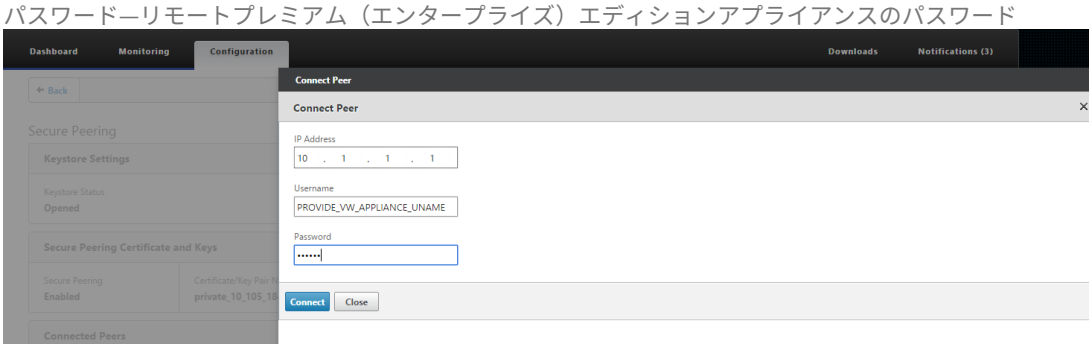
4. アプライアンスレベルの CA 証明書とプライベート証明書とキーがローカル WANOP で生成され、AUTO セキュアピアリングを実行する REMOTE PEER を追加するためのテーブルが表示されます。

5.「**+**」アイコンをクリックすると、ユーザー名とパスワードの付いた IP アドレスを追加するためのポップアップウィンドウが表示されます。資格情報を指定したリモート IP による認証が成功すると、要求がリモートマシンに送信されます。リモートマシンでは、CA Certificate と Private 証明書とキーをローカル（リモートマシン上）にインストールします。

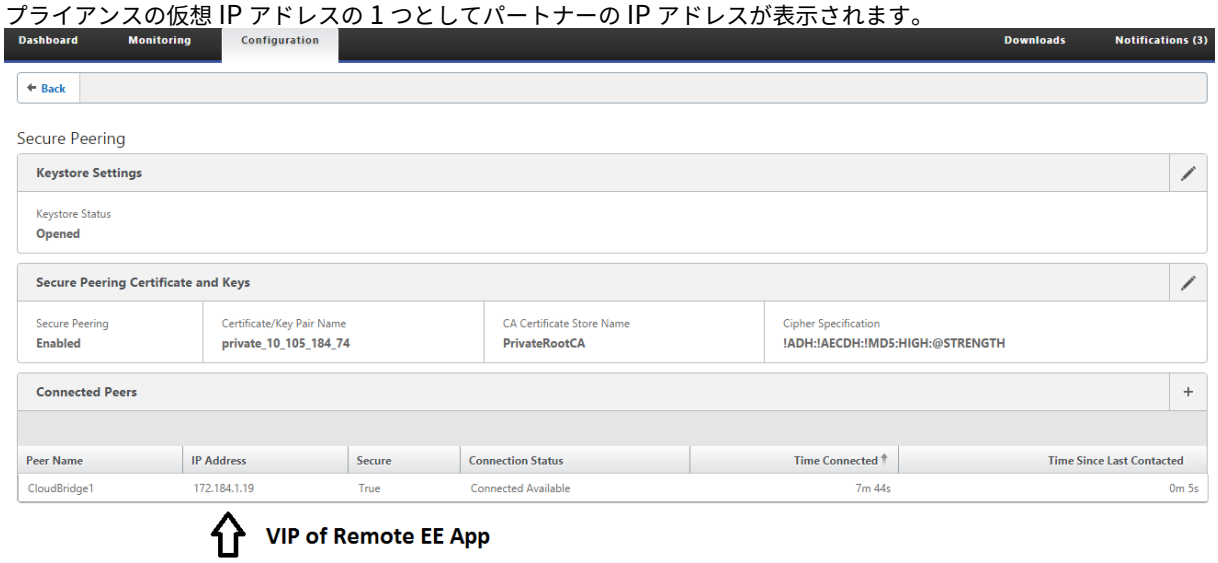


注

- IP アドレス—リモート PREMIUM (ENTERPRISE) EDITION アプライアンス管理 IP の IP アドレス
- ユーザー名—リモート PREMIUM (ENTERPRISE) EDITION アプライアンスのユーザー名
- パスワード—リモートプレミアム（エンタープライズ）エディションアプライアンスのパスワード



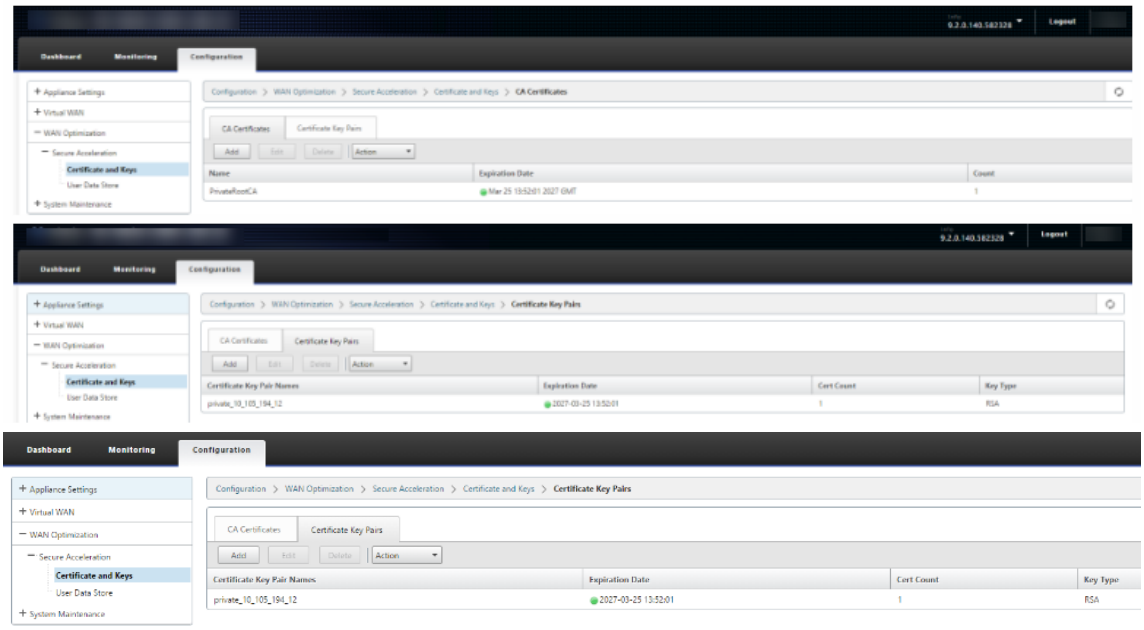
認証に成功すると、セキュアピアリングが TRUE になり、リモートプレミアム（エンタープライズ）エディションアプライアンスの仮想 IP アドレスの 1 つとしてパートナーの IP アドレスが表示されます。



監視

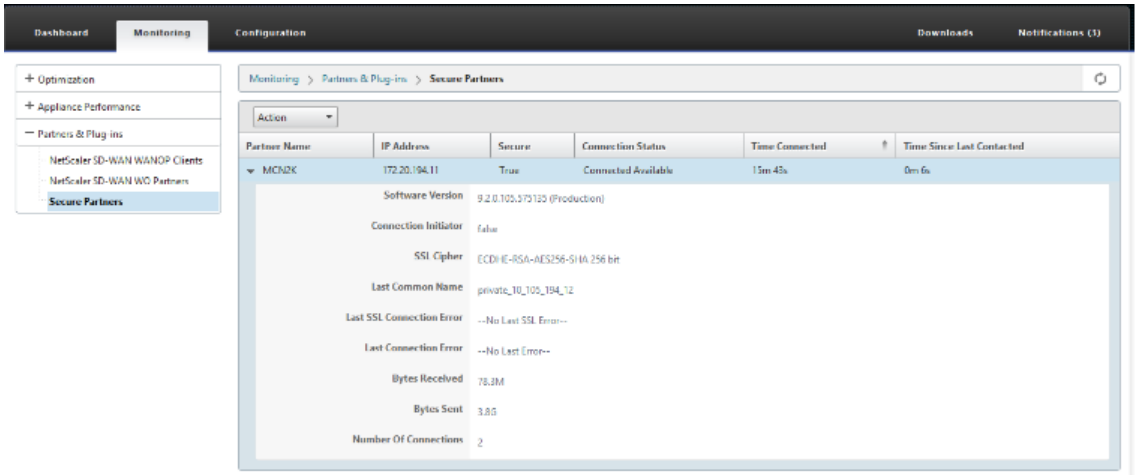
［監視］ページの［**WANOptimization** ］>［パートナー］の下にある、プレミアム（エンタープライズ）エディションアプライアンスのセキュアパートナー 情報を表示します。

1. データストアの暗号化は、Premium (Enterprise) Edition アプライアンスの [最適化] ノードにある MCN から機能を有効化することで、Premium (Enterprise) Edition アプライアンス上で実行できます。
2. Premium (Enterprise) Edition アプライアンスの場合、セキュアピアリングは常に有効になります。
3. プライベート **CA** とプライベート証明書キーの ペアが正常に生成されたかどうかを確認するには、次の情報を確認します。



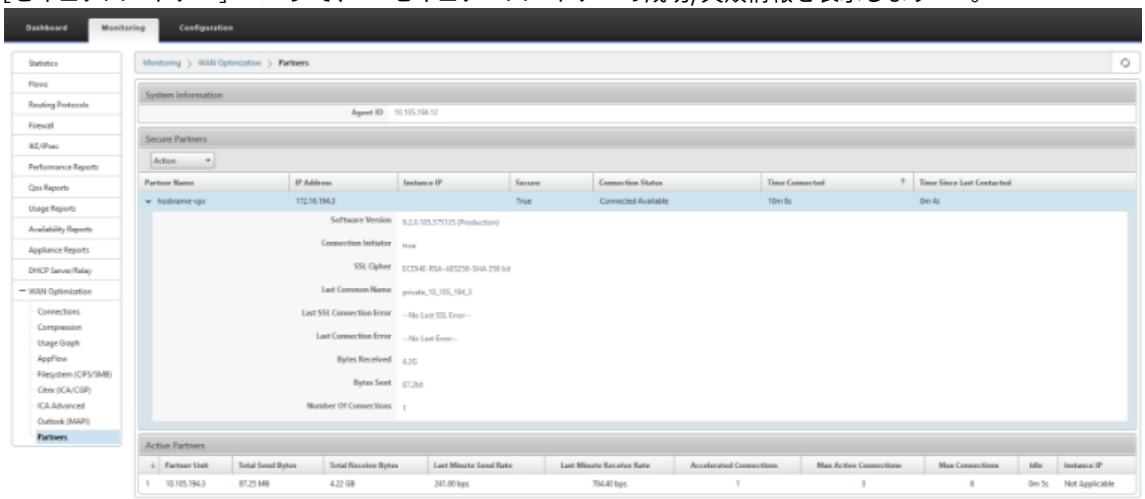
4. Premium (エンタープライズ) エディションアプライアンスの [監視] > [**WAN** 最適化] > [パートナー] ページで、セキュアパートナー情報を表示します。

5. パートナーアプライアンスの **[** 監視] > [パートナーとプラグイン] > [**セキュアパートナー] ページで、Premium (Enterprise) エディションアプライアンスのセキュアパートナー情報を表示します ** 。

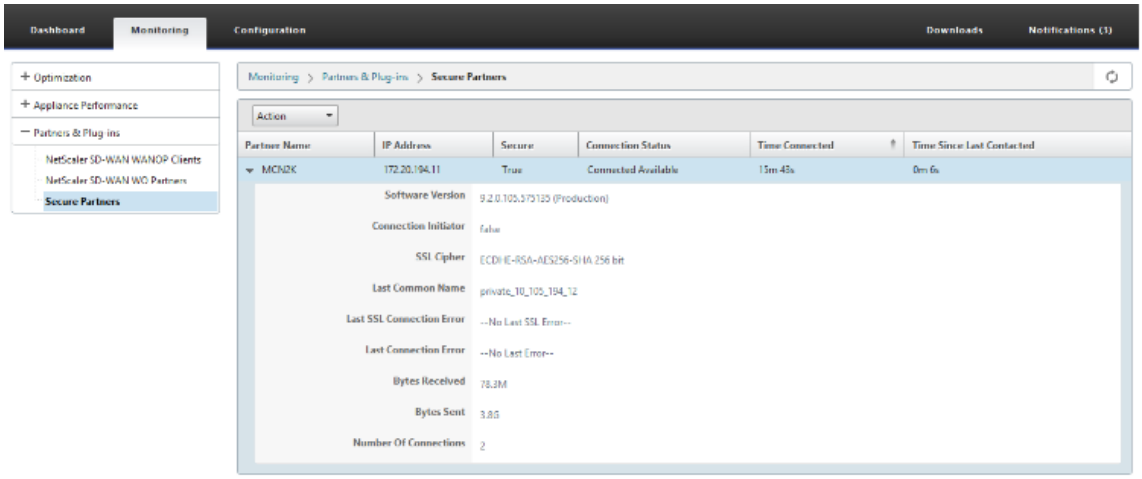


トラブルシューティング

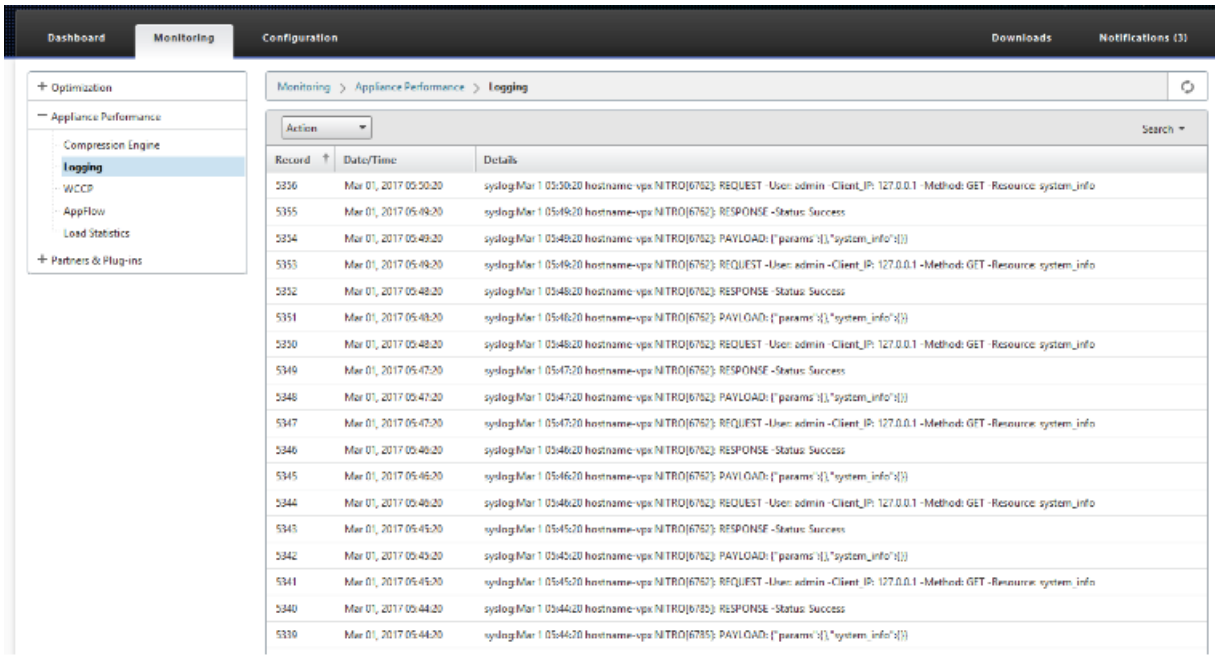
1. Premium（エンタープライズ）エディションアプライアンスの［監視］>［**WAN** 最適化］>［パートナー］**>**［セキュアパートナー］ページで、****** セキュア・パートナーの成功/失敗情報を表示します ****** 。



2. パートナーアプライアンスで、Premium（エンタープライズ）エディションアプライアンスの［監視］>［パートナーとプラグイン］**>**［セキュアパートナー］ページで、セキュアパートナー情報を表示します。



3. パートナーアプライアンスで、Premium（エンタープライズ）エディションアプライアンスの［監視］>［アプライアンスのパフォーマンス］>［ログ］ページの［セキュア・パートナー情報］を表示します。



DC サイトおよびブランチサイトの **PE** アプライアンスから、自動セキュアピアリングが開始されます

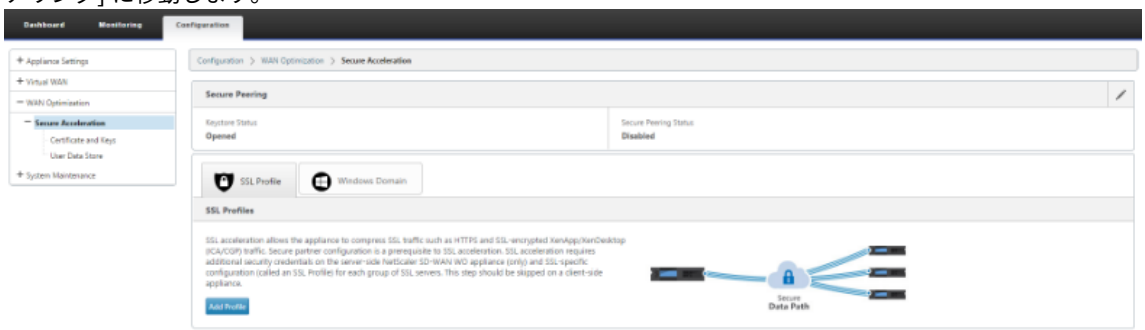
May 10, 2021

構成

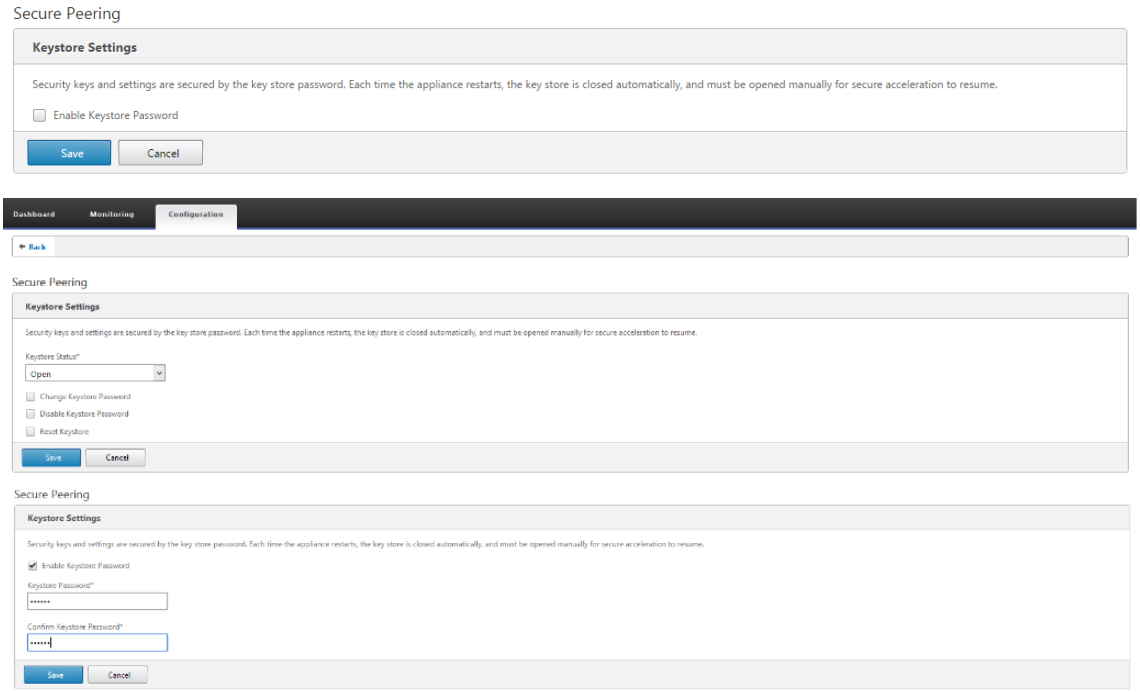
DC の新しい Premium (Enterprise) Edition アプライアンスで自動セキュアピアリングを構成するには、次の手順を実行します。

- PE DC アプライアンスは、リスニングオンモード（ポート 443）です。ブランチ PE アプライアンスは CONNECT-to モードです。
- PE DC アプライアンスは、PE ブランチアプライアンスへの自動セキュアピアリングを開始します。このアプライアンスは、プライベート CA 証明書と CERT キーペアをインストールし、DC EE の LISTEN-ON IP を使用して PE ブランチアプライアンスに CONNECT-TO を設定します。
- PE アプライアンスの LISTEN-ON IP は、「WANOP にリダイレクト」が有効になっているルーティングドメインに関連付けられたインターフェイス IP にあります。

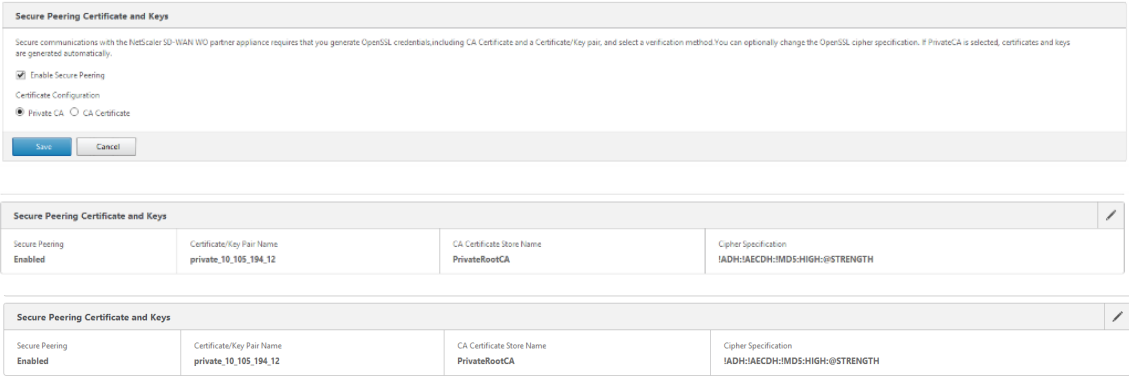
1. SD-WAN Web GUI で、[構成] > [**WAN Optimization**] > [セキュアアクセラレーション] > [セキュアピアリング] に移動します。



2. キーストアのパスワードを入力するか、キーストアを無効にして、キーストアを構成します。

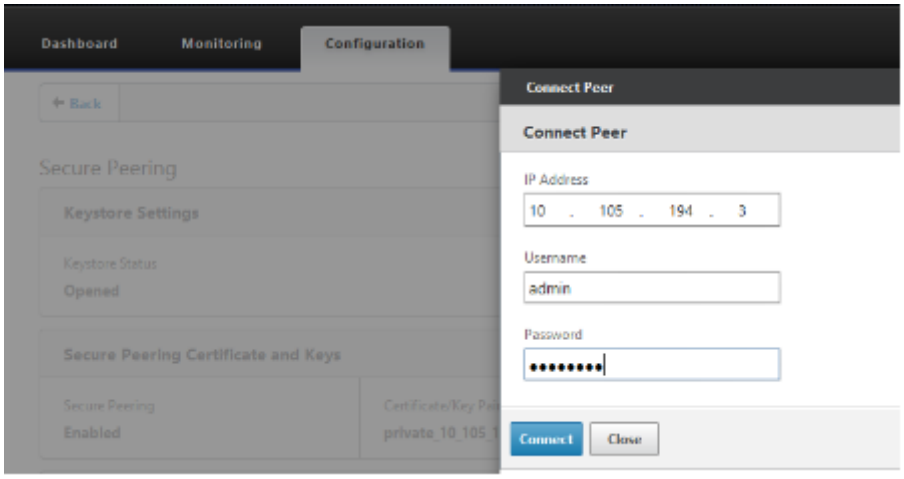


3. 自動 セキュアピアリング を実行するには、[プライベート **CA**] を選択して、セキュアピアリングを有効にします。



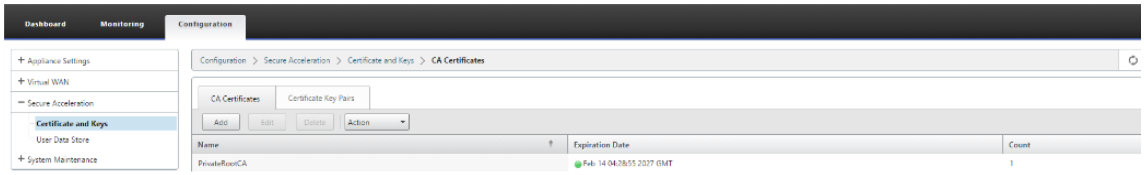
4.「+」アイコンをクリックし、ユーザー名とパスワードで IP を追加します。指定されたリモート IP とクレデンシャルを使用した認証が成功すると、要求がリモートマシンに送信され、CA 証明書とプライベート証明書とキーがリモートマシンにローカルにインストールされます。

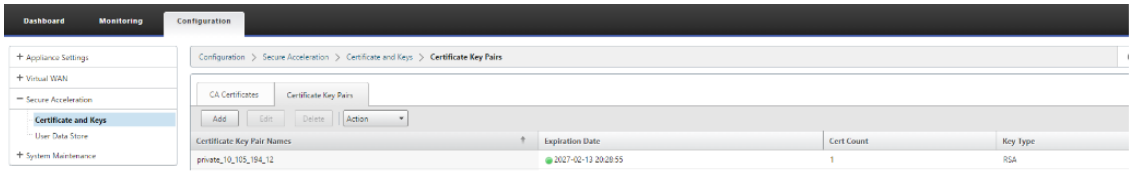
> 注
>
> IP アドレス—リモート EE アプライアンス管理 IP の IP アドレス
>
> ユーザー名—リモート EE アプライアンスのユーザー名
>
> パスワード—リモート EE アプライアンスのパスワード



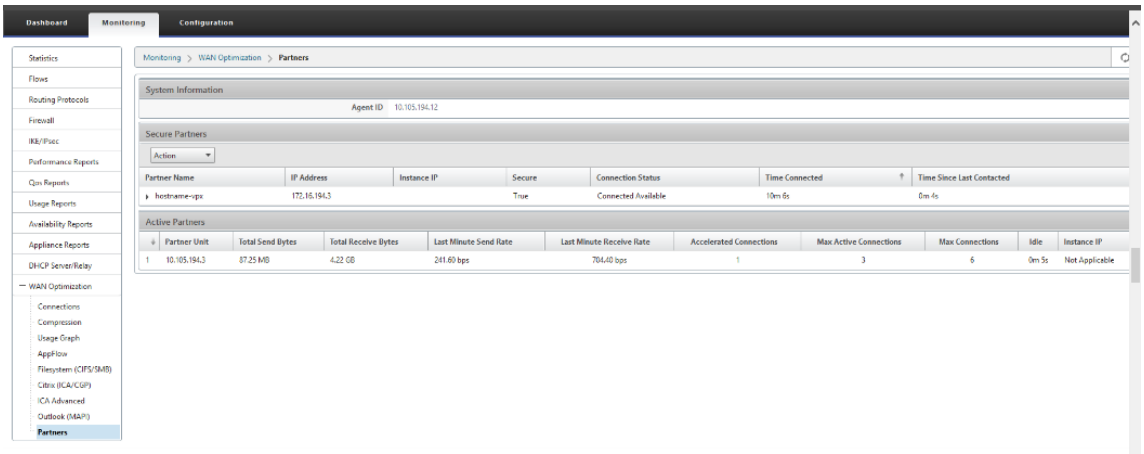
監視

1. プライベート CA とプライベート証明書キーのペアが正常に生成されたかどうかを確認するには、以下に表示される情報を確認します。

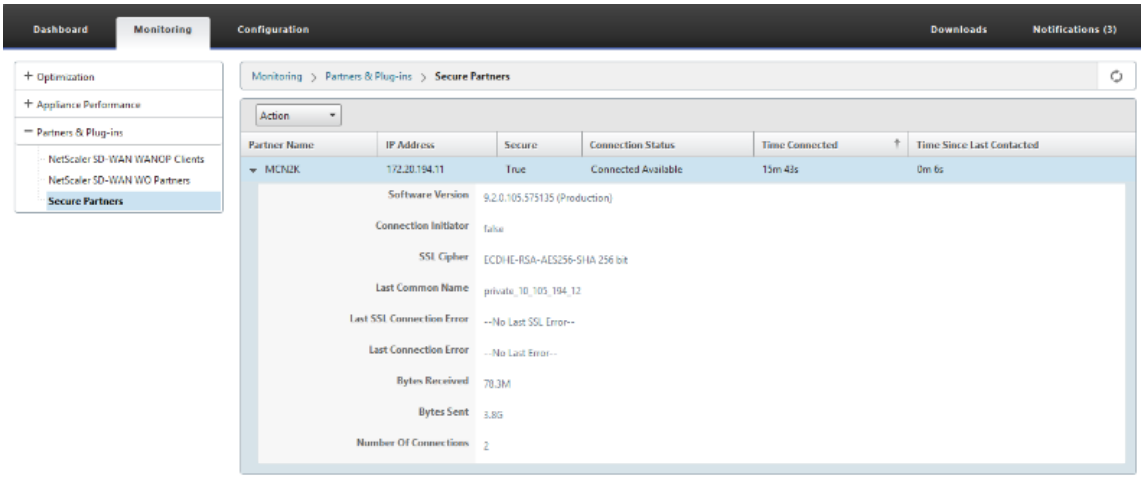




2. Premium (エンタープライズ) エディションアプライアンスの [監視] > [**WAN** 最適化] > [パートナー] ページで、セキュアパートナー情報を表示します。

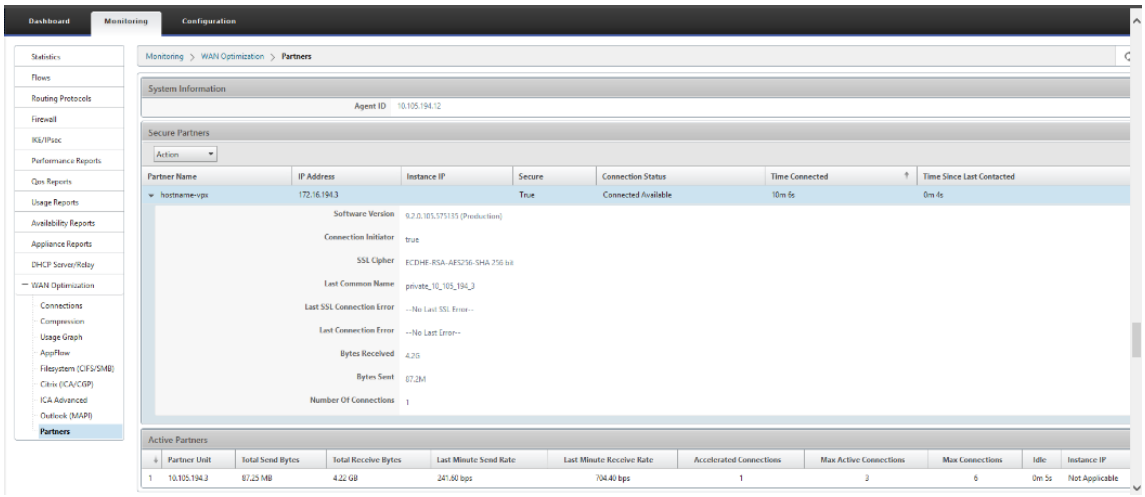


3. パートナーアプライアンスで、Premium (Enterprise) Edition アプライアンスの [監視] > [パートナーとプラグイン] > [セキュアパートナー] ページの [セキュアパートナー 情報] を表示します。

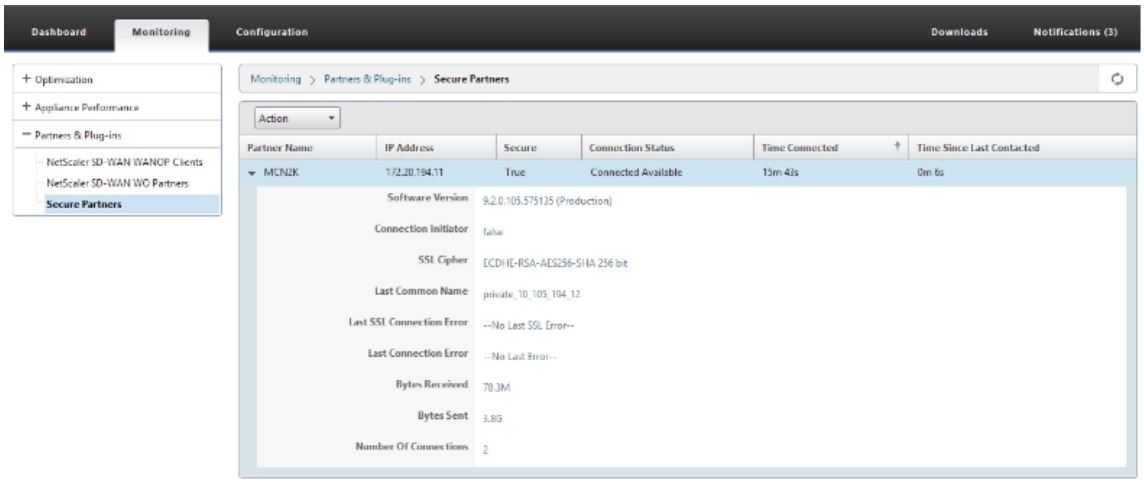


トラブルシューティング

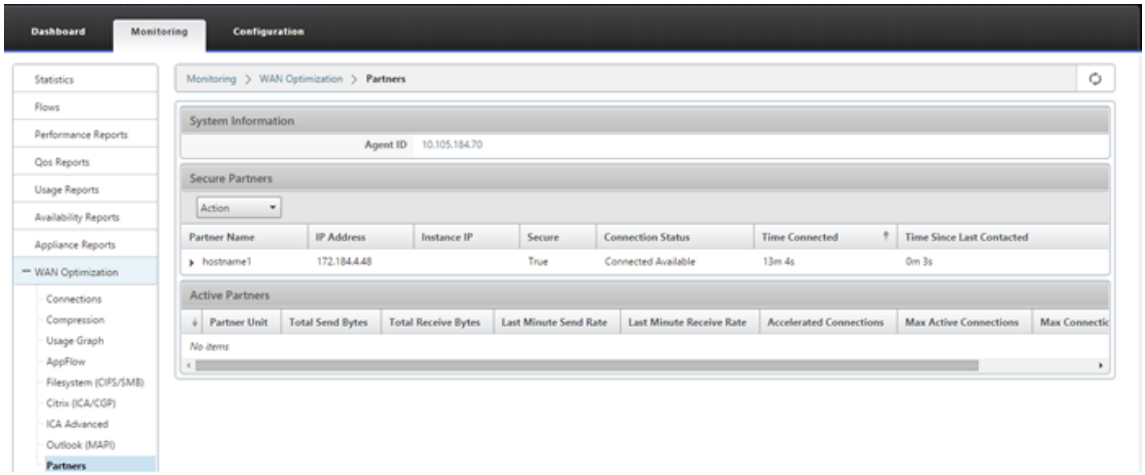
1. Premium（エンタープライズ）エディションアプライアンスの［監視］>［**WAN** 最適化］>［パートナー］>［セキュアパートナー］ページで、セキュア・パートナーの成功/失敗情報を表示します。

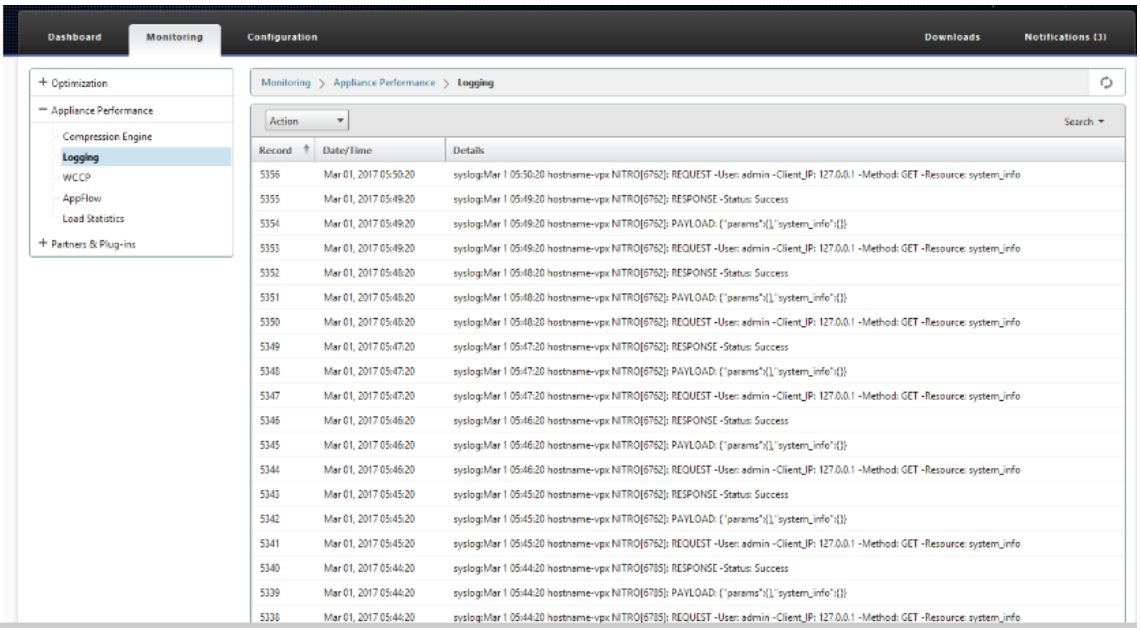


2. パートナーアプライアンスで、Premium (Enterprise) Edition アプライアンスの [監視] > [パートナーとプラグイン] > [セキュアパートナー] ページの [セキュアパートナー 情報] を表示します。



3. パートナーアプライアンスで、Premium (Enterprise) Edition アプライアンスの [監視] > [アプライアンスのパフォーマンス] > [ログ] ページの [セキュリティで保護されたパートナー情報] を表示します。





スタンドアロンの **SD-WAN SE** および **WANOP** アプライアンスを使用して、**DC** サイトおよびブランチの **PE** アプライアンスから自動セキュアピアリングを開始

May 10, 2021

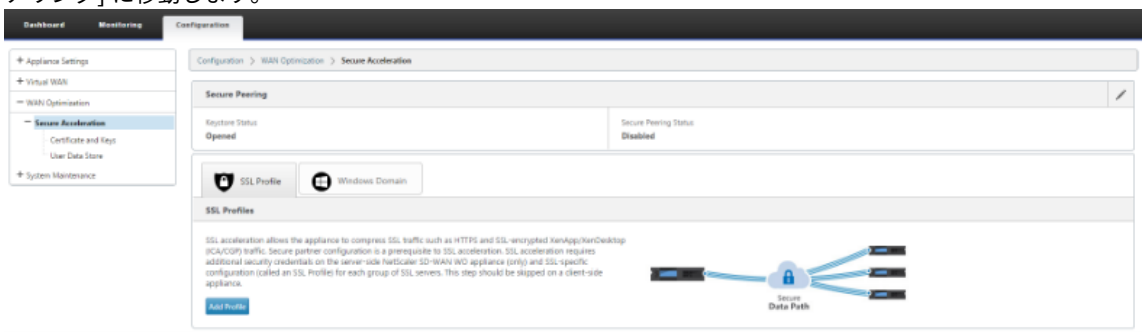
構成

スタンドアロン SD-WAN および WANOP アプライアンスを使用して、DC サイトおよびブランチで自動セキュアピアリング機能を備えた新しい Premium (Enterprise) Edition アプライアンスを構成するには、次の手順を実行し

ます。

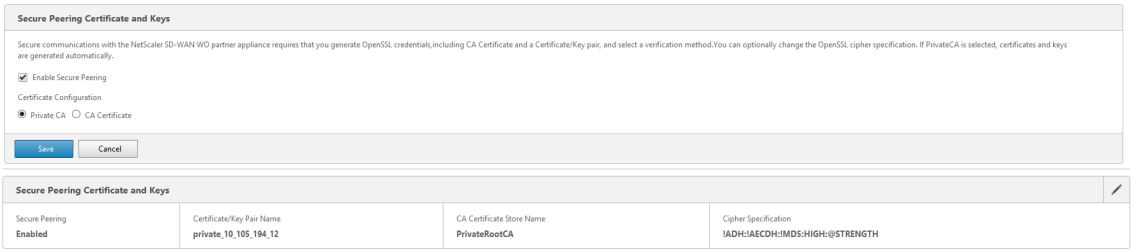
- PE DC アプライアンスは、リスニングオンモード（ポート 443）です。
- ブランチスタンドアロンの SD-WAN SE および WANOP は CONNECT-to モードです。
- PE DC アプライアンスは、ブランチスタンドアロンの SD-WAN SE および WANOP アプライアンスへの自動セキュアピアリングを開始します。このアプライアンスは、プライベート CA 証明書と CERT キーペアをインストールし、DC EE の LISTEN-ON IP を使用して PE アプライアンスに CONNECT-TO を設定します。

1. SD-WAN Web GUI で、[構成] > [**WAN Optimization**] > [セキュアアクセラレーション] > [セキュアピアリング] に移動します。



2. キーストアのパスワードを入力するか、キーストアを無効にして、キーストアを構成します。

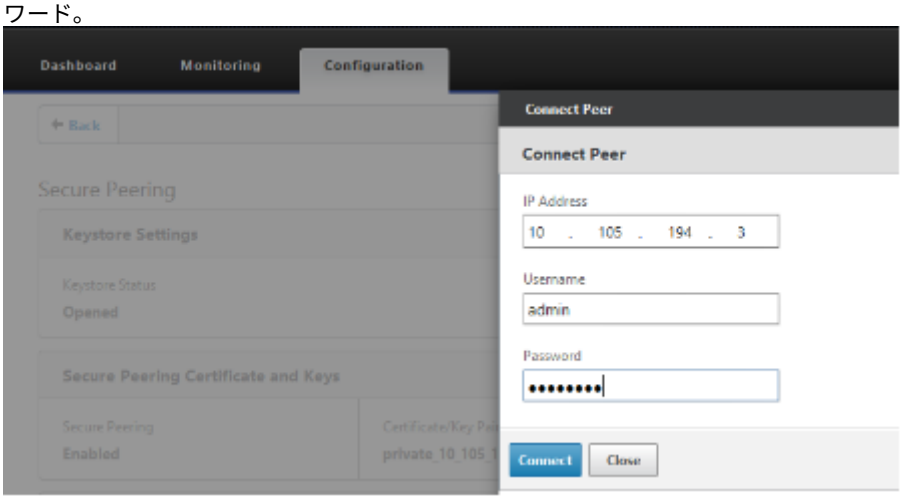
3. 自動 セキュアピアリング を実行するには、[プライベート **CA**] を選択して、セキュアピアリングを有効にします。



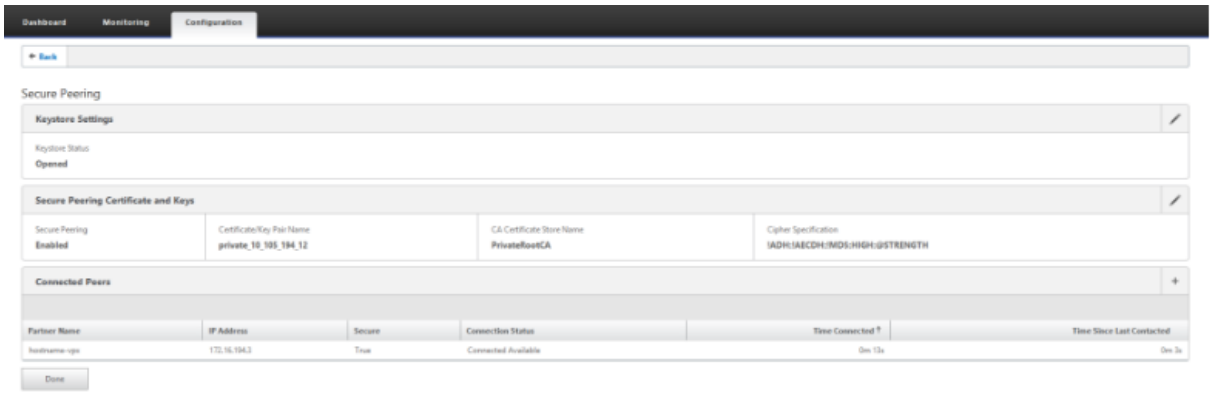
4.「+」アイコンをクリックし、ユーザー名とパスワードで IP を追加します。指定されたリモート IP とクレデン

シャルを使用した認証が成功すると、要求がリモートマシンに送信され、CA 証明書とプライベート証明書とキーがリモートマシンにローカルにインストールされます。

- IP アドレス—リモート WANOP スタンドアロンまたは Standard Edition のアプライアンス管理 IP の IP アドレス。
- ユーザー名—リモート WANOP スタンドアロンまたは Standard Edition アプライアンスのユーザー名。
- パスワード—リモート WANOP スタンドアロンまたはスタンダードエディションアプライアンスのパスワード。

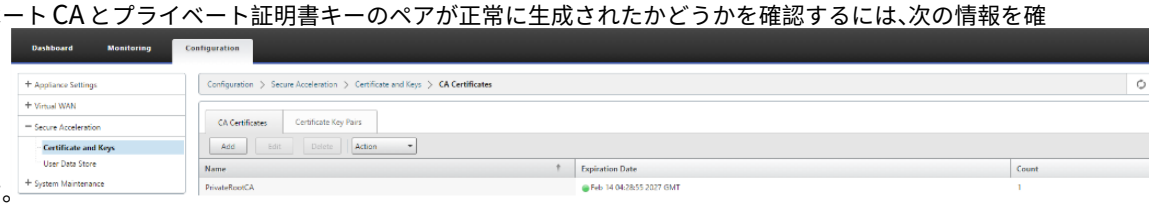


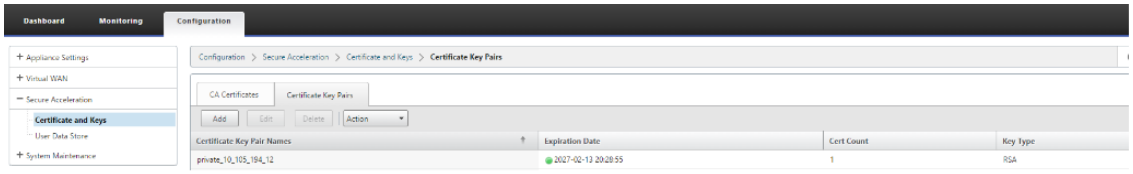
認証が成功すると、セキュアピアリングを TRUE として、パートナー IP をリモート WANOP スタンドアロンアプライアンスの仮想 IP の 1 つとして表示できます。



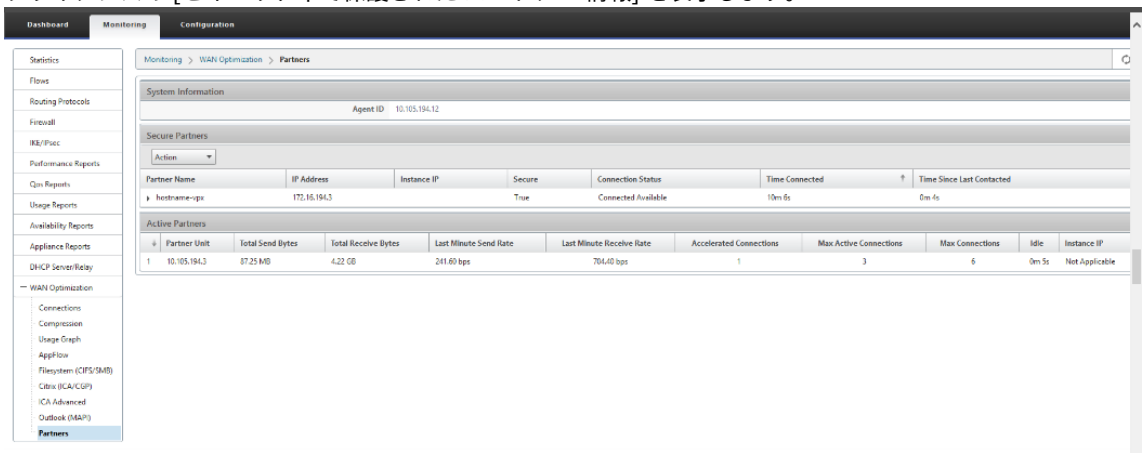
監視

1. プライベート CA とプライベート証明書キーのペアが正常に生成されたかどうかを確認するには、次の情報を確認します。

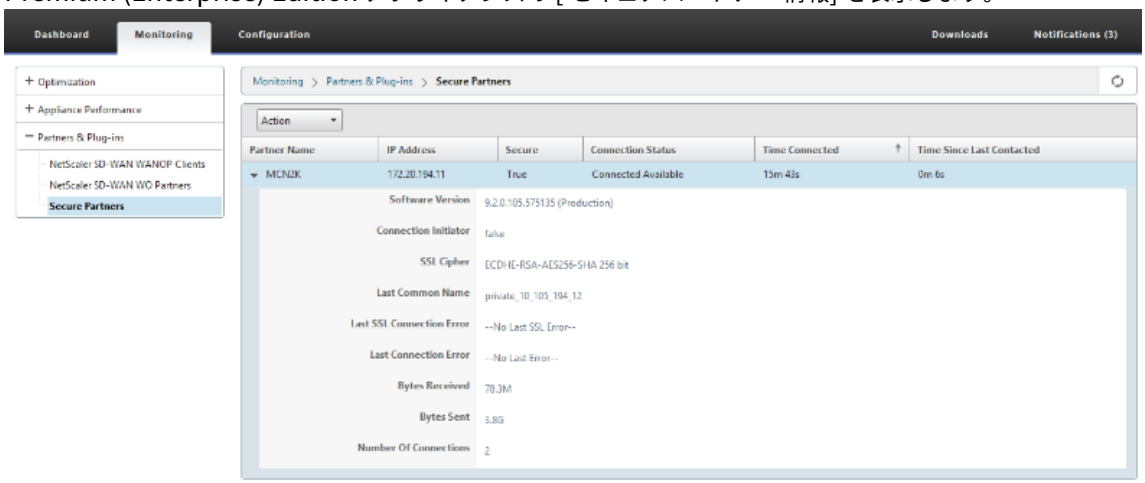




2. [監視] > [**WAN Optimization**] > [パートナー] ページで、プレミアム (エンタープライズ) エディションアプライアンスの [セキュリティで保護された パートナー 情報] を表示します。

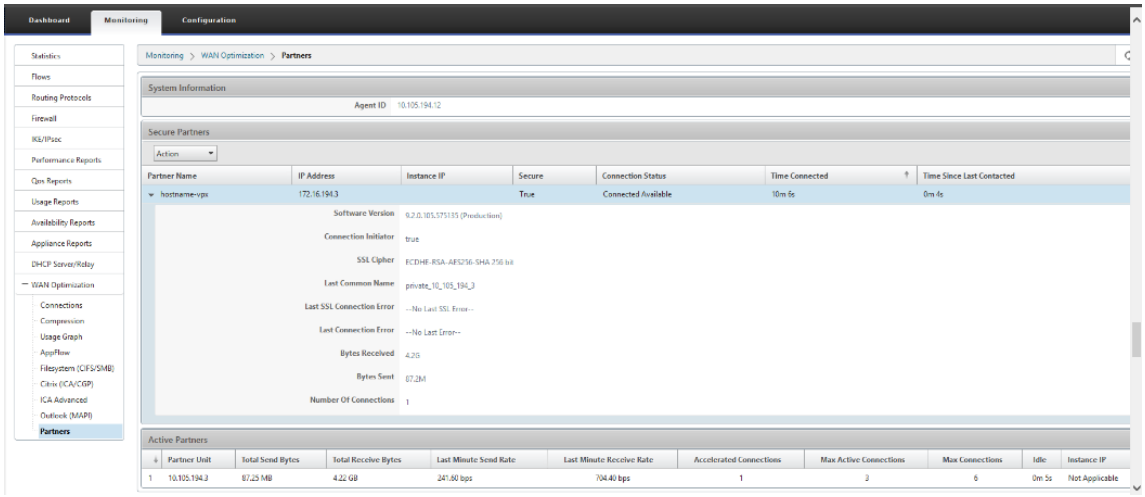


3. パートナーアプライアンスで、[監視] > [パートナーと プラグイン] > [セキュアパートナー] ページで Premium (Enterprise) Edition アプライアンスの [セキュアパートナー 情報] を表示します。

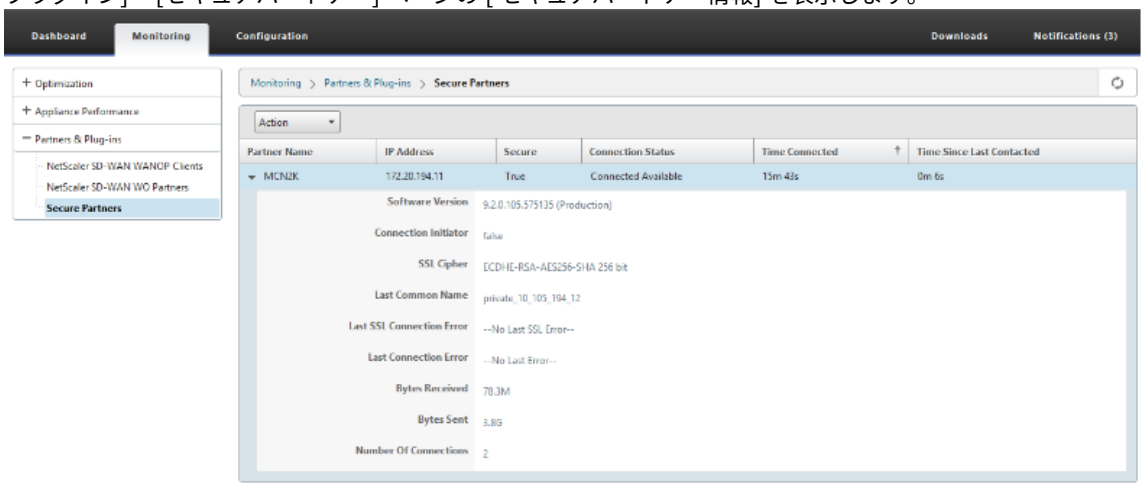


トラブルシューティング

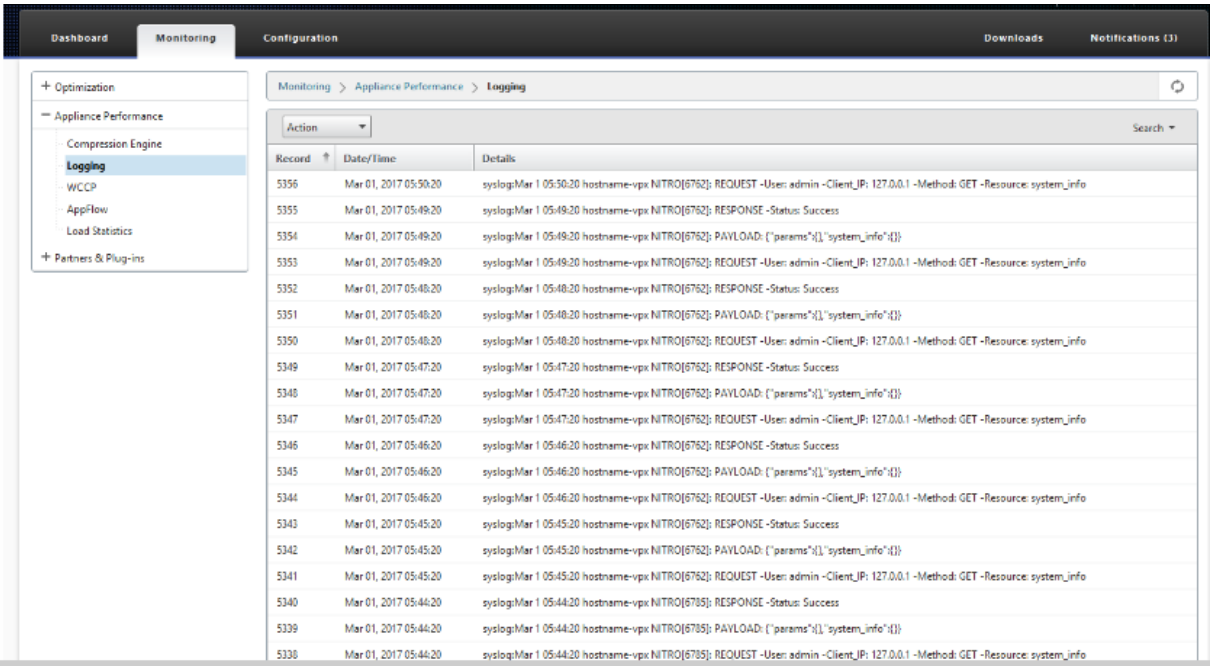
1. [監視] > [**WAN Optimization**] > [パートナー] > [セキュアパートナー] ページの Premium (Enterprise) Edition アプライアンスで、セキュア パートナーの 成功/失敗情報を表示します。



2. パートナーアプライアンスで、Premium (Enterprise) Edition アプライアンスの [監視] > [パートナーとプラグイン] > [セキュアパートナー] ページの [セキュアパートナー情報] を表示します。



3. パートナーアプライアンスで、Premium (Enterprise) Edition アプライアンスの [監視] > [アプライアンスのパフォーマンス] > [ログ] ページの [セキュアパートナー情報] を表示します。



DC サイトおよびブランチ PE アプライアンスの PE アプライアンスから、手動によるセキュアピアリングを開始

May 10, 2021

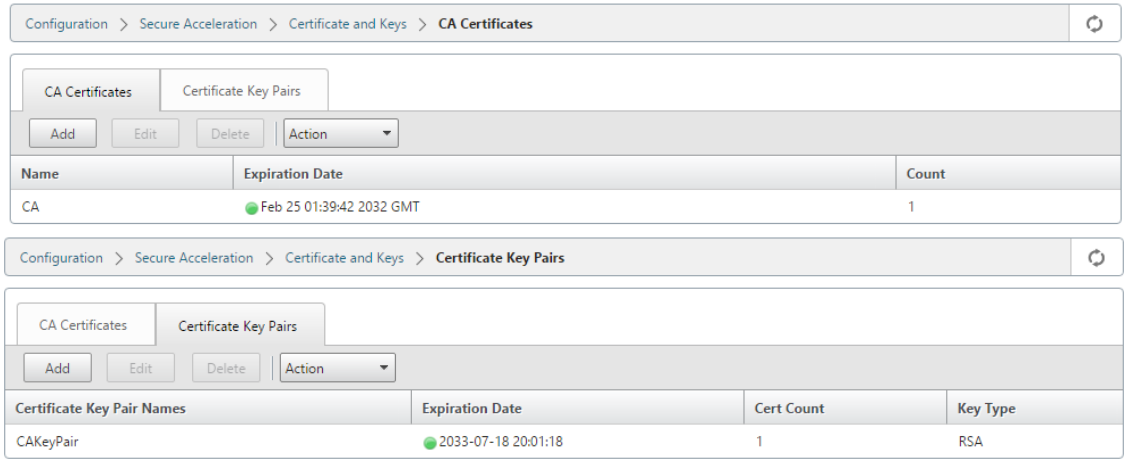
この展開では、DC サイト PE アプライアンスがリスニングオンモードで構成され、ブランチサイト PE アプライアンスが接続先モードで構成されます。

- PE DC アプライアンスは、リスニングオンモード（ポート 443）です。
- ブランチ PE アプライアンスは CONNECT-to モードです。
- PE の LISTEN-ON IP は、「WANOP にリダイレクト」が有効になっているルーティングドメインに関連付けられたインターフェイス IP にあります。
- 認証局の認証元から取得した CA と Cert Key のペア証明書を手動でアップロードします。

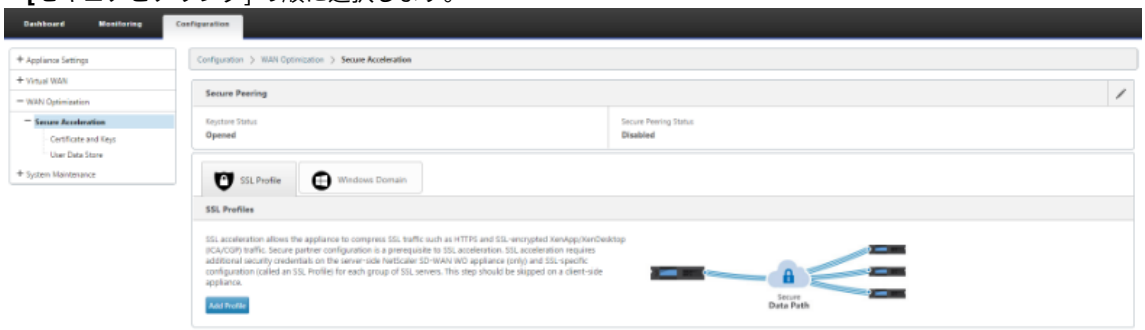
構成

DC サイトの PE アプライアンスおよびブランチサイトの PE アプライアンスから開始される自動セキュアピアリングを設定するには、次の手順を実行します。

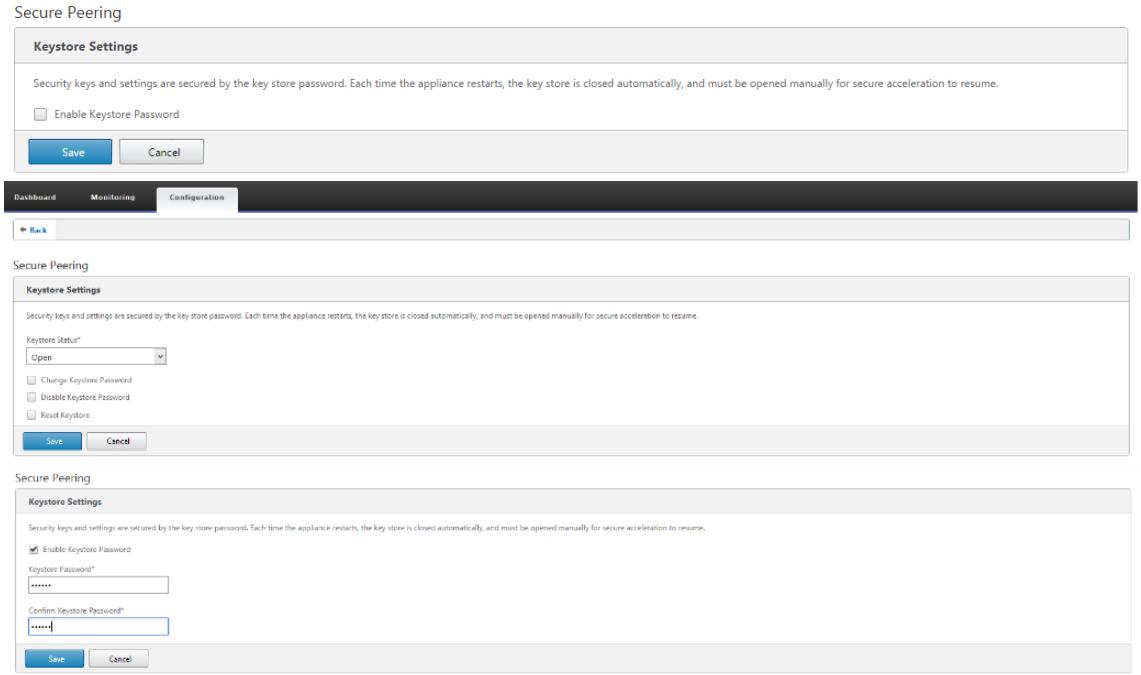
1. 本物の 証明書 から取得した **CA** 証明書と **CA** キー証明書 をアップロードし、以下に示すように SD-WAN に提供します。



2. DC サイトの新しい PE アプライアンスで、SD-WAN Web GUI で、[設定] **> [**セキュアアクセラレーション**] > [**セキュアピアリング] の順に選択します。

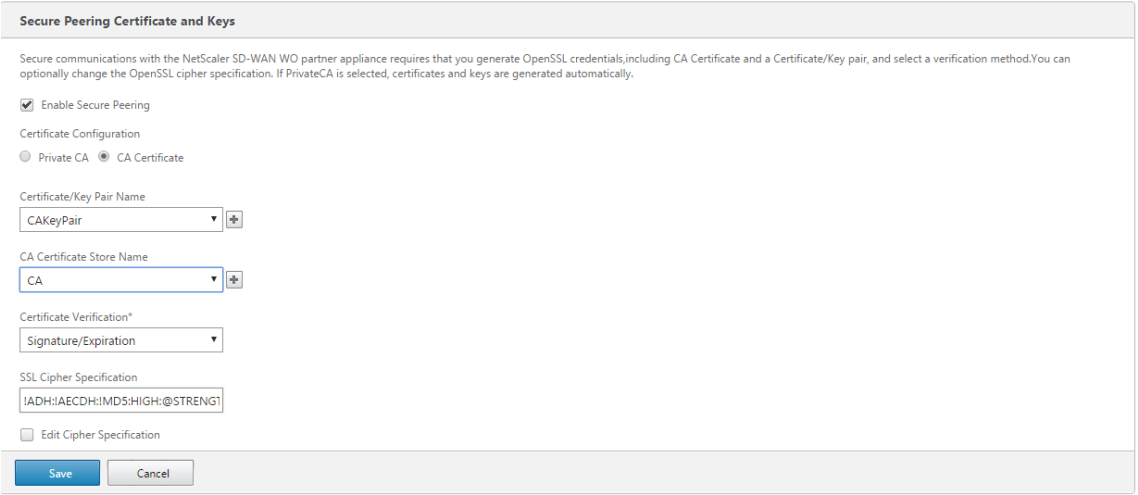


3. キーストアのパスワードを入力するか、キーストアを無効にして、キーストアを構成します。

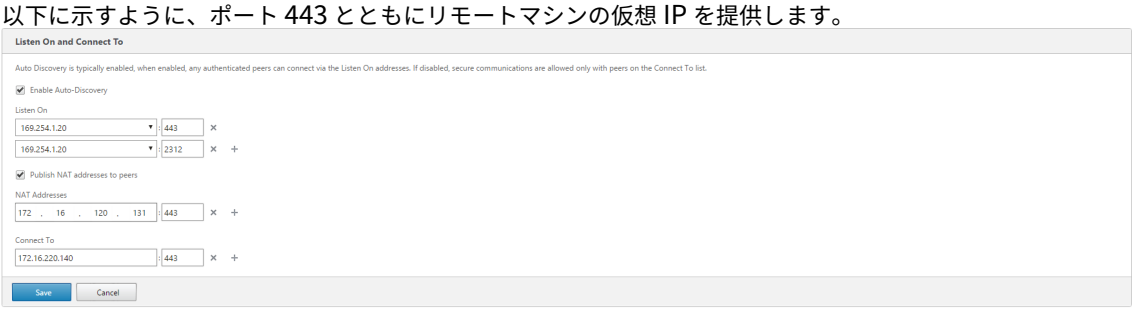


4. [**CA Cert** ificate] オプションボタンを選択し、アップロードされた CA と CA キーのペア証明書を以下に示

すように適切に提供することで、セキュアピアリングを有効にします。

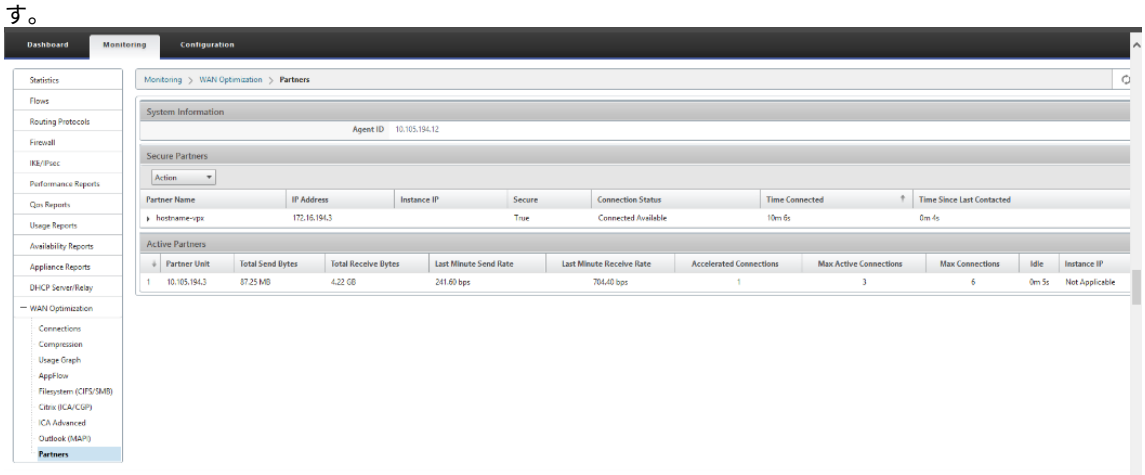


5. 以下に示すように、ポート 443 とともにリモートマシンの仮想 IP を提供します。

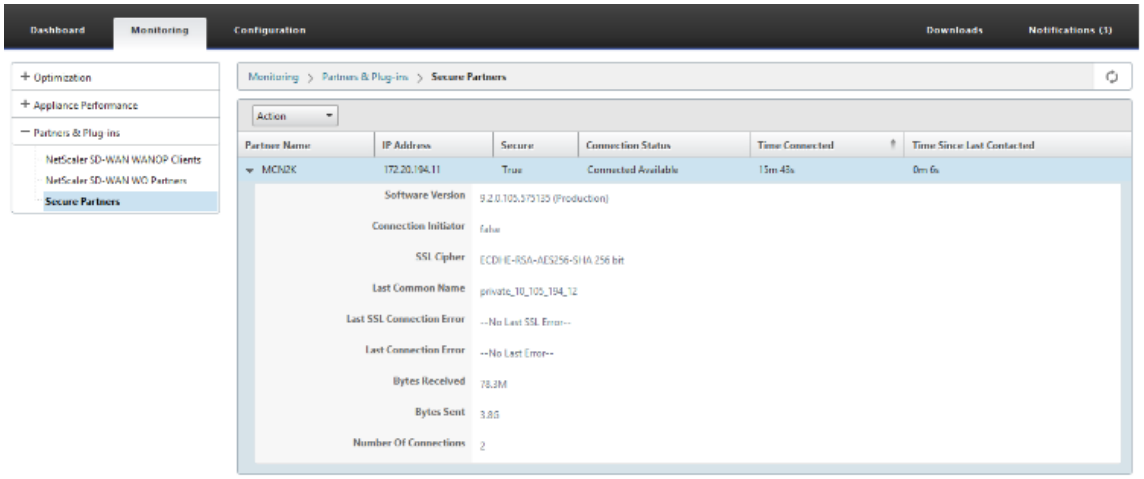


監視

1. プライベート **CA** と秘密証明書キーのペアが正常に生成されたかどうかを検証するには、次の情報を確認します。

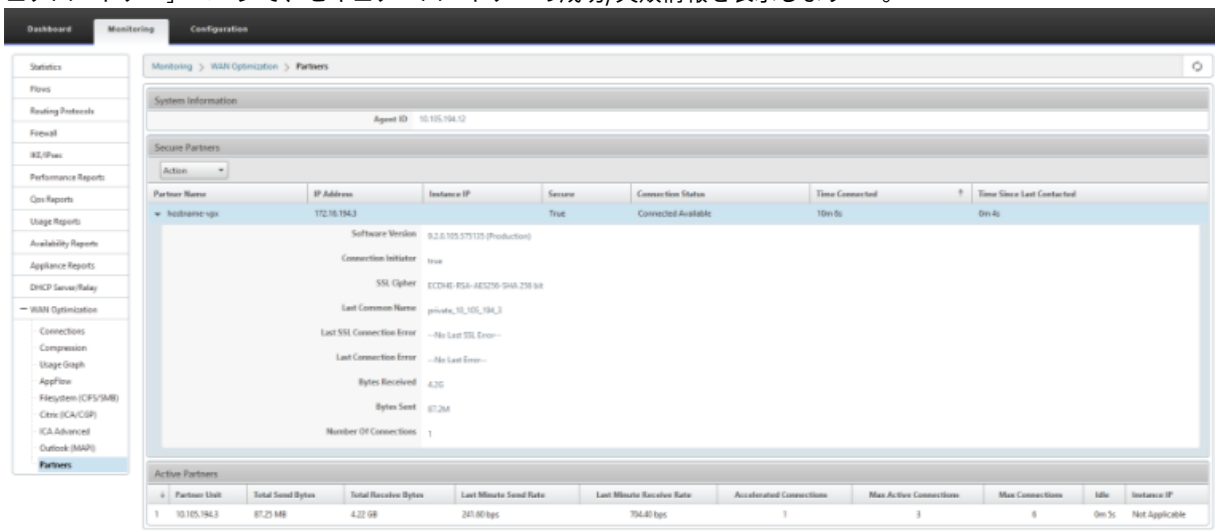


2. パートナーアプライアンスで、Premium（エンタープライズ）エディションアプライアンスの［監視］>［パートナー］**>**［セキュアパートナー］ページの［****** セキュアパートナー情報］を表示します ****** 。



トラブルシューティング

Premium（エンタープライズ）エディションアプライアンスの［監視］>［**WAN** 最適化］>［パートナー］**>**［セキュアパートナー］ページで、セキュア・パートナーの成功/失敗情報を表示します **。



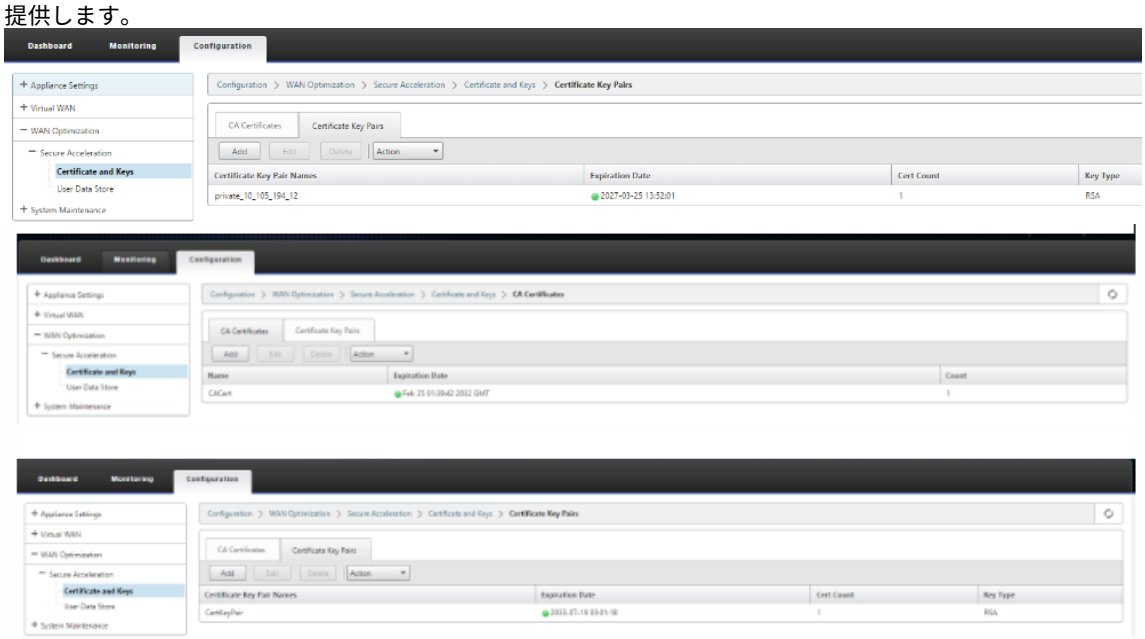
DC サイトの **PE** アプライアンスから、ブランチスタンドアロン **SD-WAN SE** および **WANOP** アプライアンスへの手動セキュアピアリング

May 10, 2021

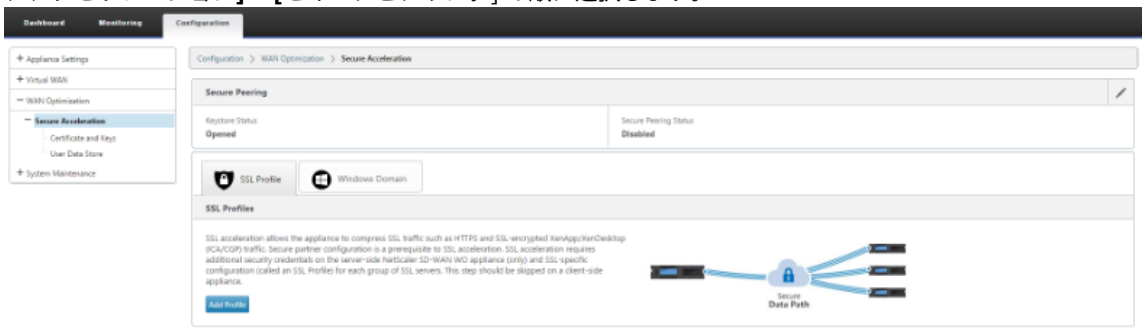
- PE DC アプライアンスは、リスニングオンモード（ポート 443）です。
- ブランチ PE アプライアンスは CONNECT-to モードです。

- PE の LISTEN-ON IP は、「WANOP にリダイレクト」が有効になっているルーティングドメインに関連付けられたインターフェイス IP にあります。
- 認証局の本格的なソースから取得した CA 証明書と Cert Key ペアの証明書を手動でアップロードします。

1. 本物の 証明書 から取得した **CA** 証明書と **CA** キー証明書 をアップロードし、以下に示すように SD-WAN に提供します。

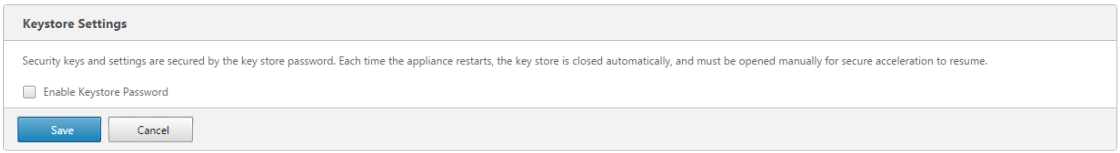


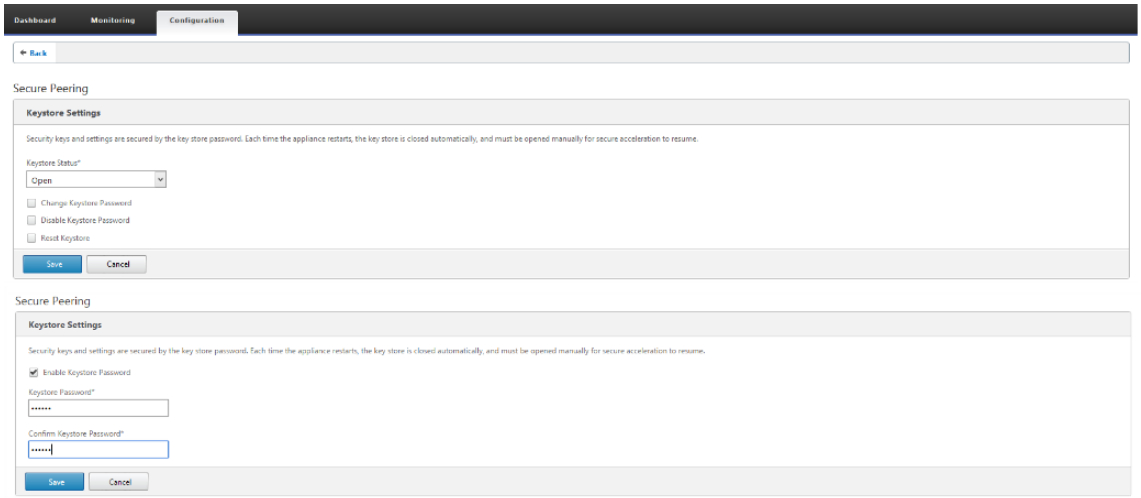
2. DC サイトの新しい PE（Premium Edition）アプライアンスで、SD-WAN Web GUI で、[構成] > [セキュアアクセラレーション**] > [**セキュアピアリング] の順に選択します。



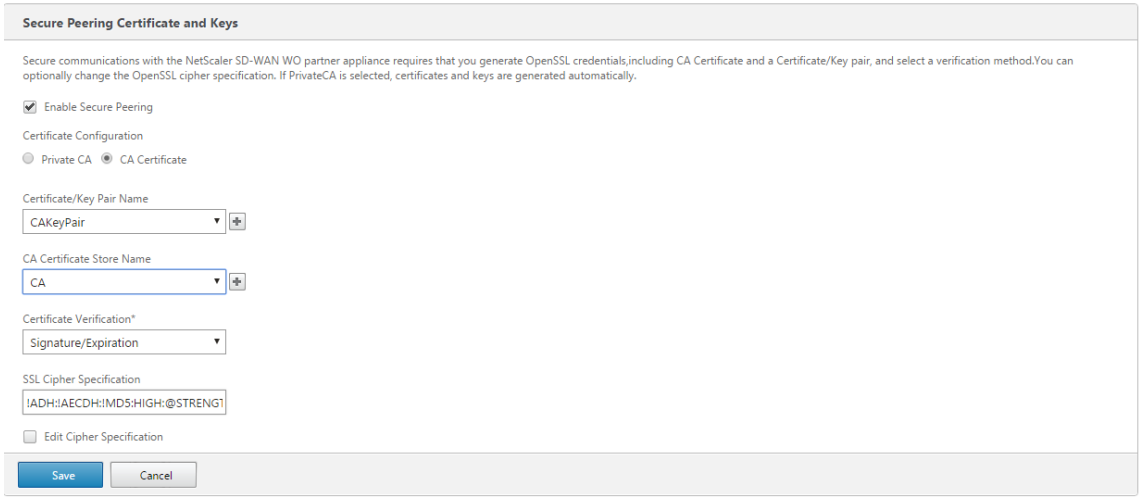
3. キーストアの パスワードを入力してキーストア を有効にするか、キーストアを無効にします。

Secure Peering





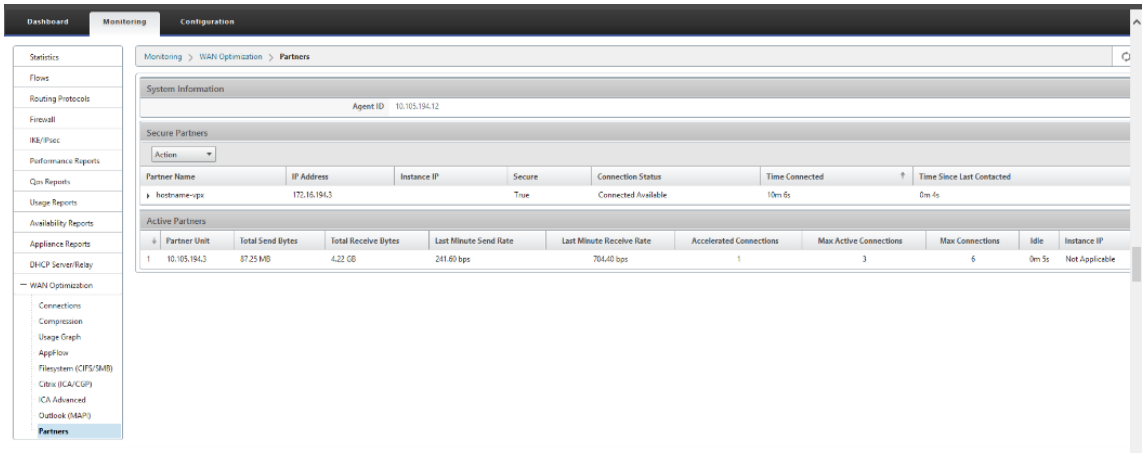
4. [**CA Cert** ificate] オプションボタンを選択し、アップロードされた CA と CA キーのペア証明書を以下に示すように適切に提供することで、セキュアピアリングを有効にします。



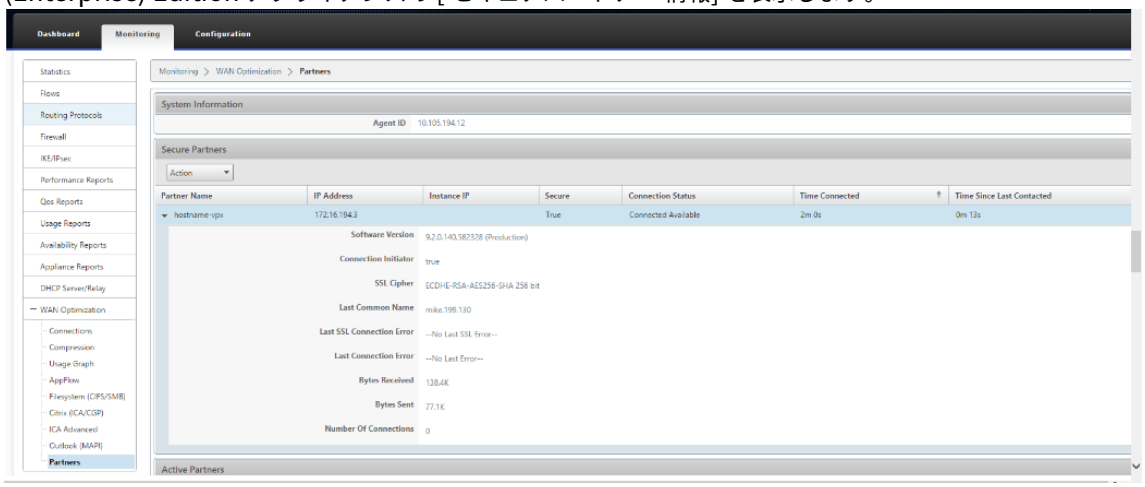
5. 以下に示すように、ポート 443 とともにリモートマシンの仮想 IP を提供します。

監視

1. [監視] > [**WAN Optimization**] > [パートナー] ページで、プレミアム (エンタープライズ) エディションアプライアンスの [セキュリティで保護された パートナー 情報] を表示します。

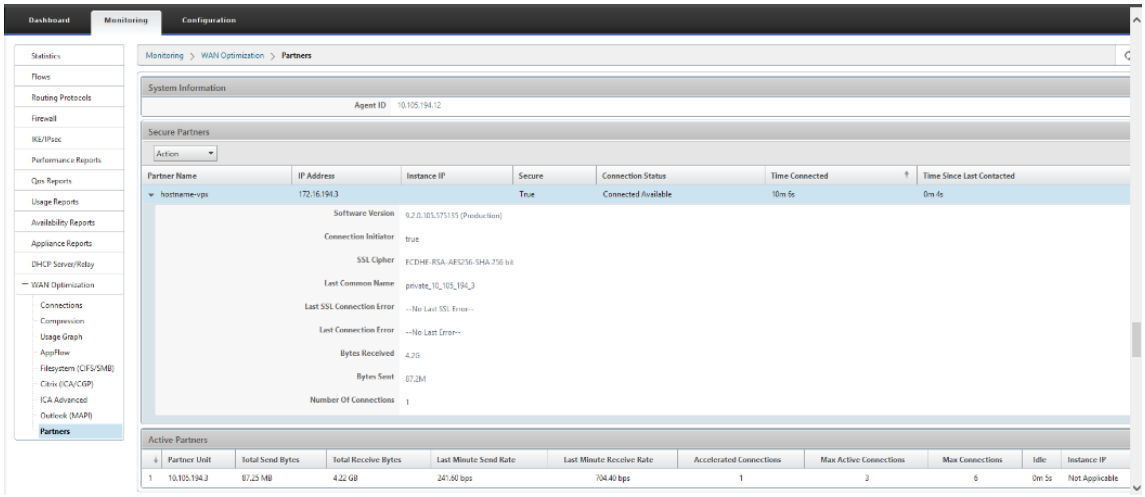


2. パートナーアプライアンスで、**[** 監視] > [パートナー] > [セキュアパートナー] ページで Premium (Enterprise) Edition アプライアンスの [セキュアパートナー 情報] を表示します。**

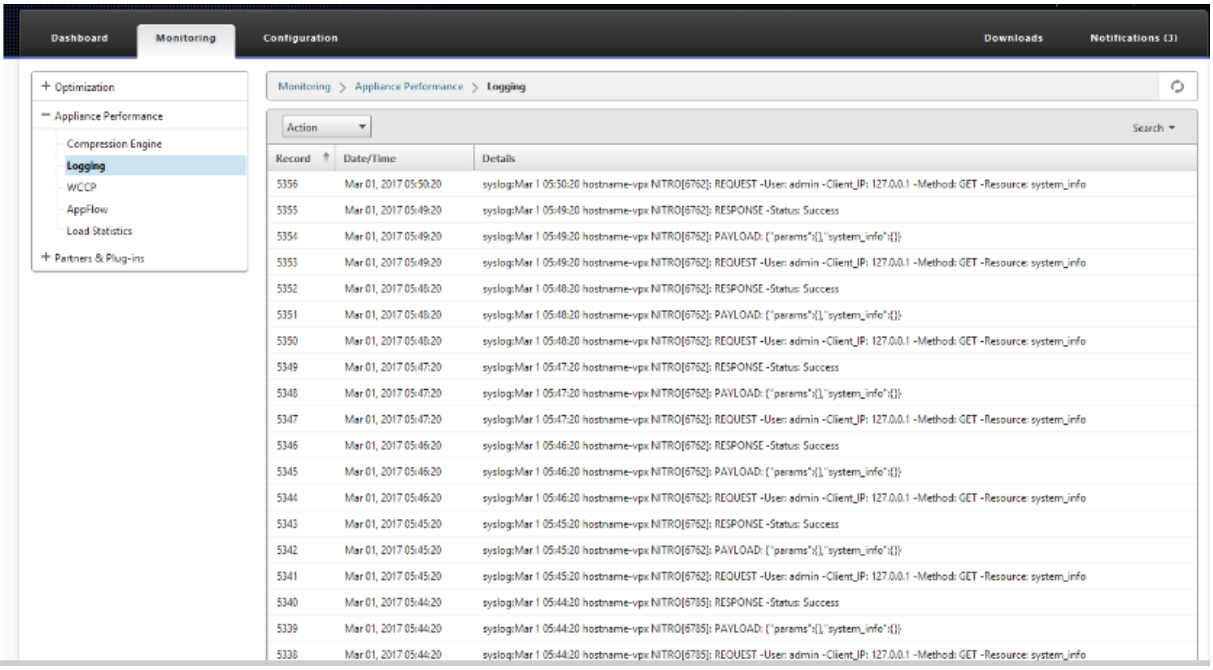


トラブルシューティング

1. [監視] > [**WAN Optimization**] > [パートナー**] > [**セキュアパートナー**]** ページの **Premium (Enterprise) Edition** アプライアンスで、**** セキュアパートナーの **** 成功 / 失敗情報 を表示します。



2. パートナーアプライアンスで、Premium (Enterprise) Edition アプライアンスの [監視] > [アプライアンスのパフォーマンス] > [ログ] ページの [セキュアパートナー情報] を表示します。



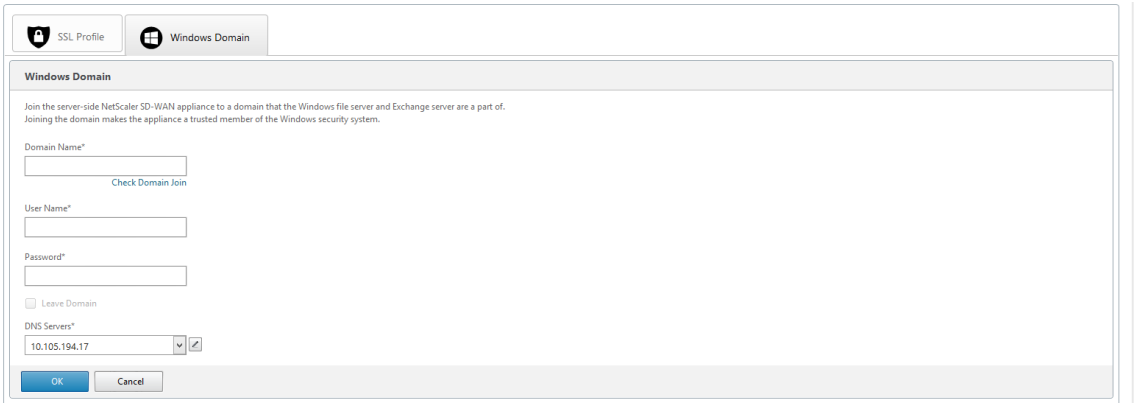
ドメイン参加と代理ユーザーの作成

May 10, 2021

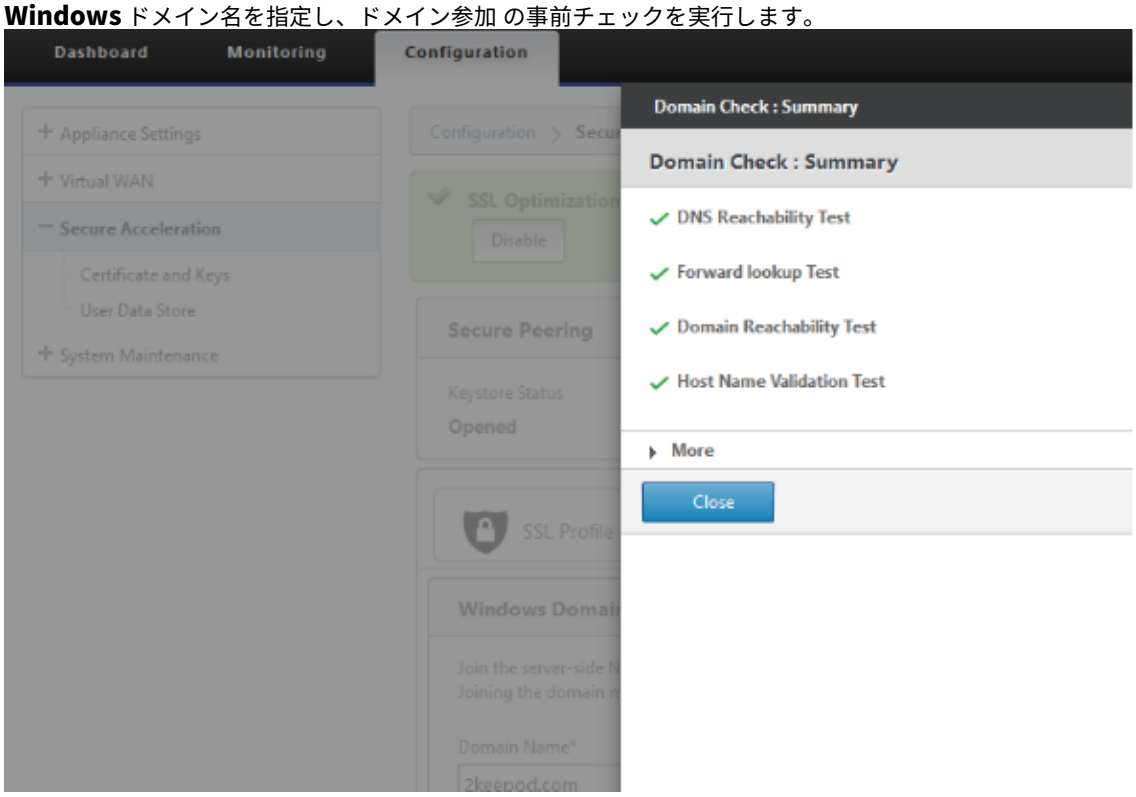
DC から **windows** ドメインに新しいプレミアム（エンタープライズ）エディション（**PE**）アプライアンスを設定するには:

1. SD-WAN Web GUI で [Windows ドメイン] に移動し、[構成] > [セキュアアクセラレーション] に移動し、[

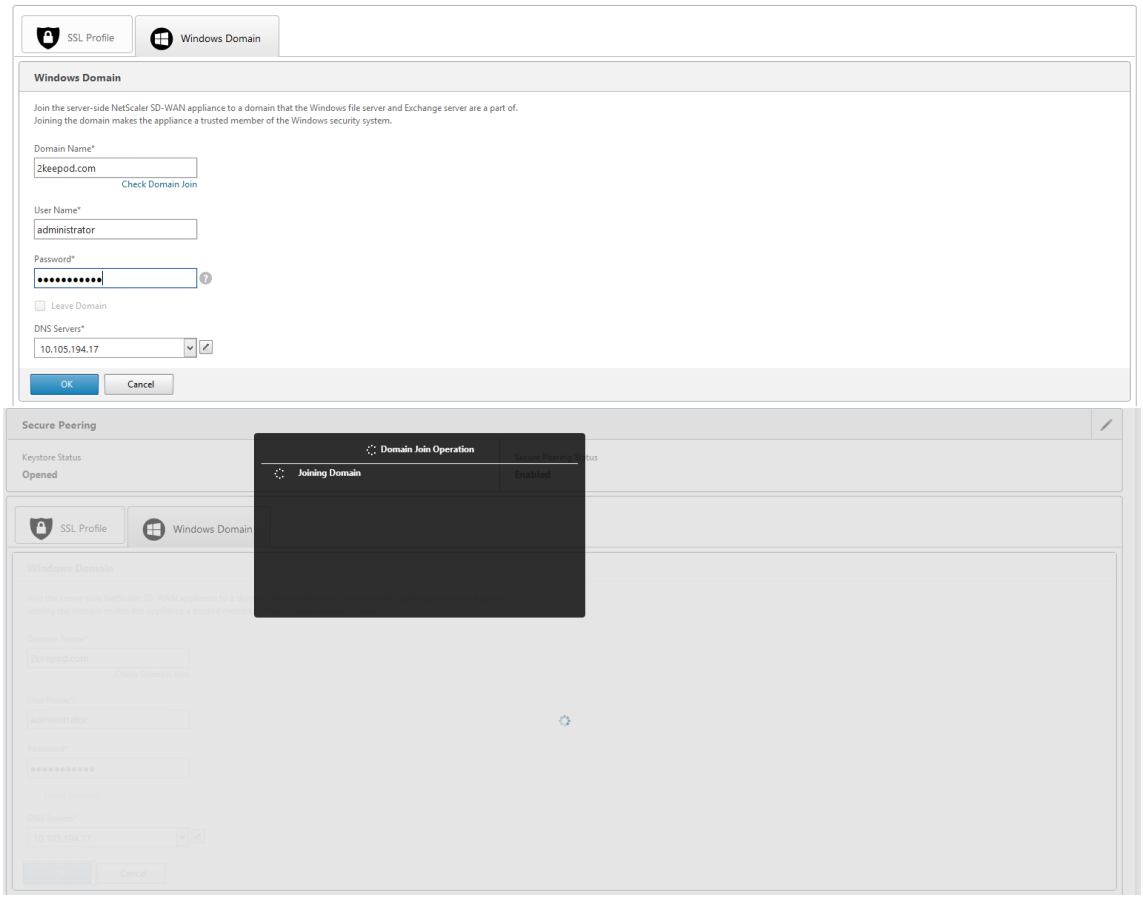
Windows ドメインに参加] をクリックします。



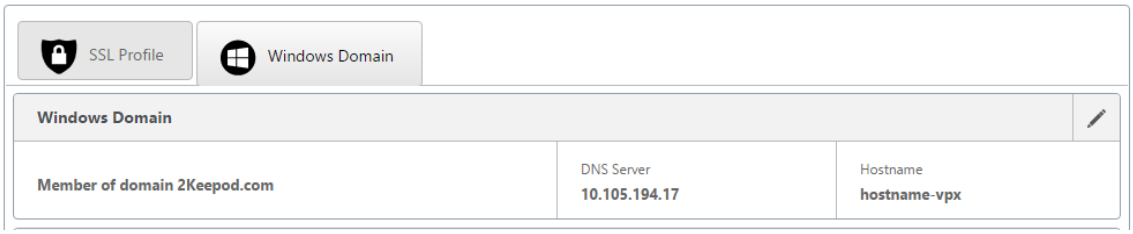
2. **Windows** ドメイン名を指定し、ドメイン参加 の事前チェックを実行します。



3. 事前チェックの概要が正常に表示されたら、ドメインコントローラの資格情報を入力します。

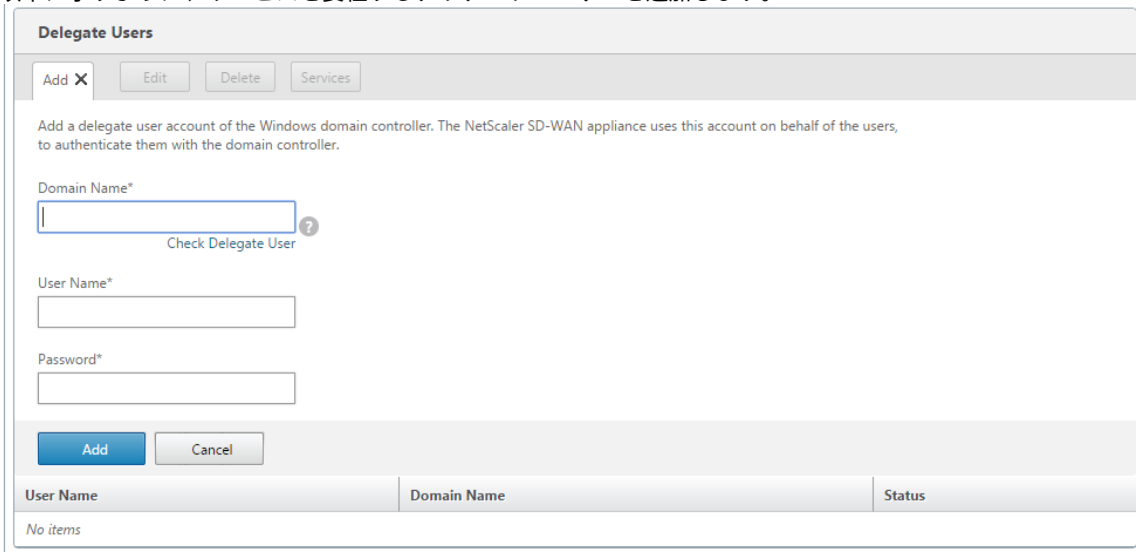


4. ドメイン参加に成功すると、次の出力が得られます。

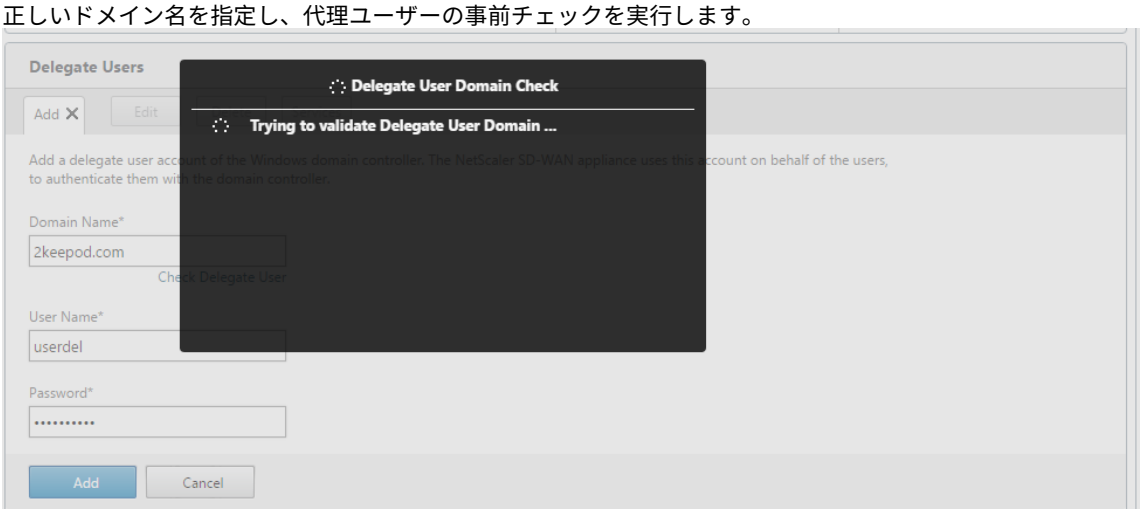


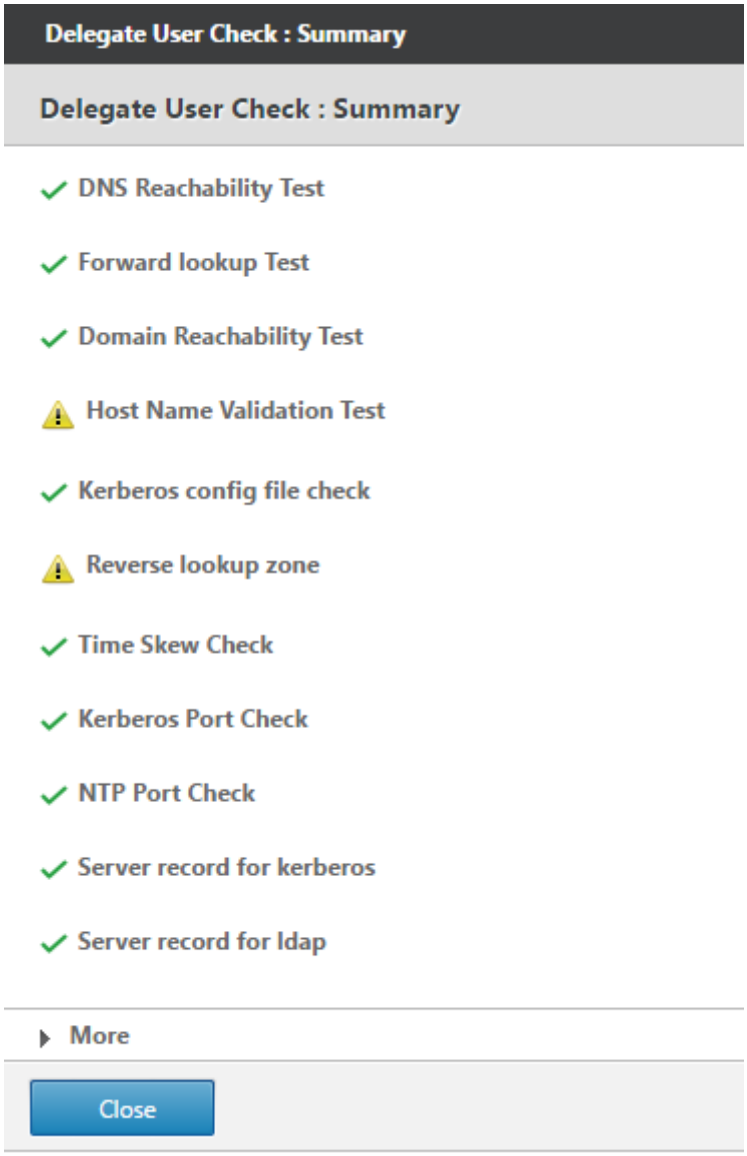
ユーザーを委任する

1. 以下に示すように、サービスを委任するデリゲートユーザーを追加します。

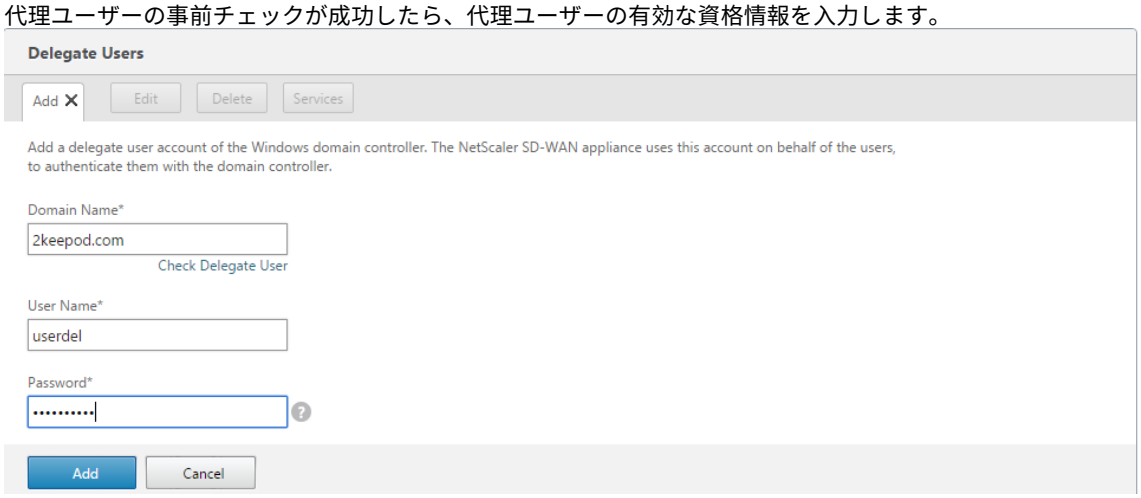


2. 正しいドメイン名を指定し、代理ユーザーの事前チェックを実行します。



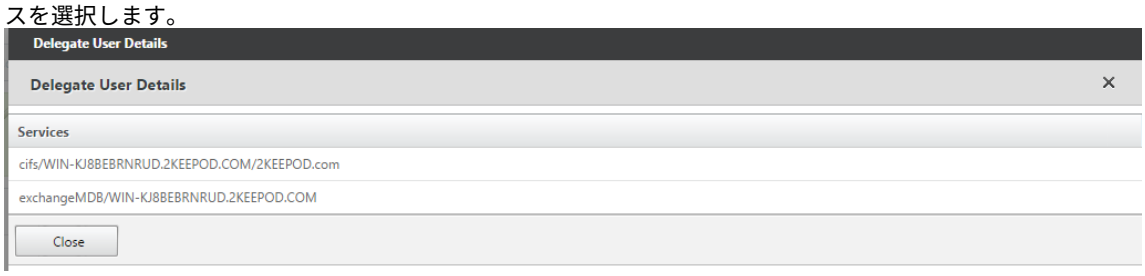


3. 代理ユーザーの事前チェックが成功したら、代理ユーザーの有効な資格情報を入力します。



4. 代理ユーザが SD-WAN に正常に追加されると、成功メッセージが表示されます。

5. 委任ユーザーによって委任されているすべてのサービスを確認するには、そのユーザーをポイントし、サービスを選択します。



セキュリティ

May 10, 2021

このセクションのトピックでは、Citrix SD-WAN 展開に関する一般的なセキュリティガイダンスを提供します。

Citrix SD-WAN 展開のガイドライン

展開ライフサイクルを通じてセキュリティを維持するには、次のセキュリティを考慮することをお勧めします。

- 物理的セキュリティ
- アプライアンスのセキュリティ
- ネットワークセキュリティ
- 管理と管理

次のリンクで説明するトピックでは、を使用して SD-WAN ネットワークのセキュリティを設定する方法について詳しく説明します。

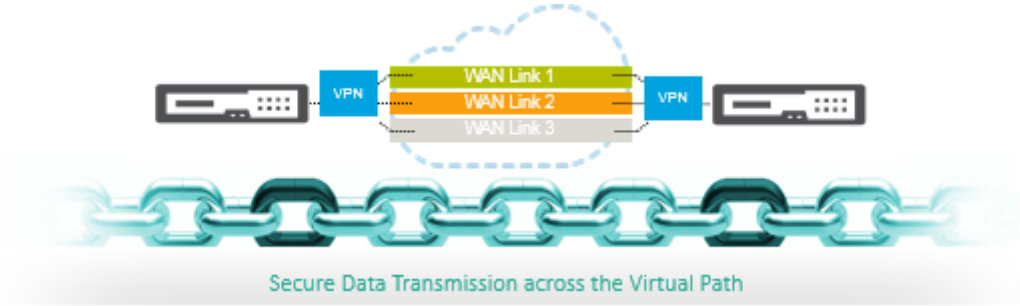
- IPSec トンネル
- ファイアウォール

IPsec トンネル終了

May 10, 2021

Citrix SD-WAN は IPsec 仮想パスをサポートしているため、サードパーティ製のデバイスが、Citrix SD-WAN アプライアンスの LAN または WAN 側で IPsec VPN トンネルを終了できます。140-2 レベル 1 FIPS 認定の IPSec 暗号化バイナリを使用して、SD-WAN アプライアンスで終端するサイト間の IPSec トンネルを保護できます。

また、Citrix SD-WAN は、差別化された仮想パストンネリングメカニズムを使用した耐障害性 IPSec トンネリングもサポートします。



Citrix SD-WAN と AWS トランジットゲートウェイとの統合

May 10, 2021

アマゾンウェブサービス（**AWS**）トランジット **Gateway** サービスを使用すると、Amazon 仮想プライベートクラウド（VPC）とオンプレミスのネットワークを 1 つのゲートウェイに接続できます。AWS で実行されるワークロードの数が増えるにつれて、複数のアカウントと Amazon VPC にまたがってネットワークを拡張し、その増加に対応できます。

ピアリングを使用して Amazon VPC のペアを接続できるようになりました。ただし、多くの Amazon VPC 間でポイントツーポイント接続を管理するには、接続ポリシーを一元管理する機能がないと、運用上のコストがかかり、煩雑になる可能性があります。オンプレミスの接続では、AWS VPN を個々の Amazon VPC にアタッチする必要があります。このソリューションは構築に時間がかかり、VPC の数が数百個に増えると、管理が難しい場合があります。

AWS Transit Gateway では、中央ゲートウェイからネットワーク経由で各 Amazon VPC、オンプレミスのデータセンター、またはリモートオフィスへの 1 つの接続を作成および管理するだけでかまいません。Transit Gateway は、スポークのように動作するすべての接続ネットワーク間でトラフィックがどのようにルーティングされるかを制御するハブとして機能します。このハブアンドスポークモデルでは、管理が大幅に簡素化され、運用コストが削減されます。これは、各ネットワークはトランジットゲートウェイにのみ接続し、他のすべてのネットワークには接続しないためです。新しい VPC はトランジットゲートウェイに接続され、トランジットゲートウェイに接続されている他のすべてのネットワークで自動的に利用できるようになります。この接続性の容易さにより、成長に合わせてネットワークの拡張が容易になります。

企業が増加するアプリケーション、サービス、インフラストラクチャをクラウドに移行するにつれ、SD-WAN を迅速に導入して、ブロードバンド接続のメリットを享受し、ブランチサイトのユーザーをクラウドリソースに直接接続します。インターネット転送サービスを使用してグローバルなプライベートネットワークを構築および管理し、地理的

に分散した場所とユーザーを近位ベースのクラウドリソースで接続するという複雑さには、多くの課題があります。**AWS** トランジットゲートウェイネットワークマネージャー は、このパラダイムを変更します。現在、AWS を使用する Citrix SD-WAN のお客様は、Citrix SD-WAN ブランチアプライアンスの AWS Transit Gateway を統合することにより、Citrix SD-WAN を AWS トランジットゲートウェイとともに使用できるようになりました。これにより、トランジットゲートウェイに接続されたすべての VPC に手を差し伸べる機能を持つユーザーに最高品質のエクスペリエンスを提供できます。

次に、Citrix SD-WAN と AWS トランジットゲートウェイを統合する手順を示します。

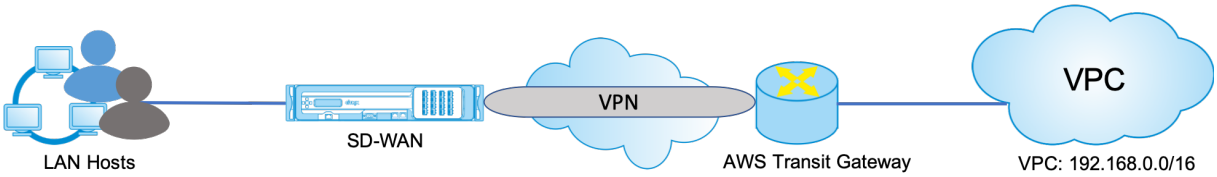
1. AWS トランジットゲートウェイを作成します。
2. VPN を中継ゲートウェイ（既存の VPN または新しい VPN のいずれか）に接続します。
3. オンプレミスまたは任意のクラウド（AWS、Azure、または GCP）にある SD-WAN サイトで VPN が設定されたトランジットゲートウェイに VPN を接続します。
4. Citrix SD-WAN から AWS Transit Gateway と IPsec トンネルを介したボーダーゲートウェイプロトコル（BGP）ピアリングを確立し、トランジットゲートウェイに接続されたネットワーク（VPC）を学習します。

使用例

ユースケースは、ブランチ環境から AWS 内（任意の VPC 内）にデプロイされたリソースに手を差し伸べます。AWS Transit Gateway を使用すると、トラフィックは BGP ルートを処理せずに、Transit Gateway に接続されたすべての VPC に到達できます。これを実現するには、次の方法を実行します。

- ブランチの Citrix SD-WAN アプライアンスから AWS トランジットゲートウェイへの IPSec を確立します。この展開方法では、トラフィックが IPsec を通過するため、SD-WAN の利点をすべて得ることはありません。
- AWS 内に Citrix SD-WAN アプライアンスをデプロイし、仮想パスを介してオンプレミスの Citrix SD-WAN アプライアンスに接続します。

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

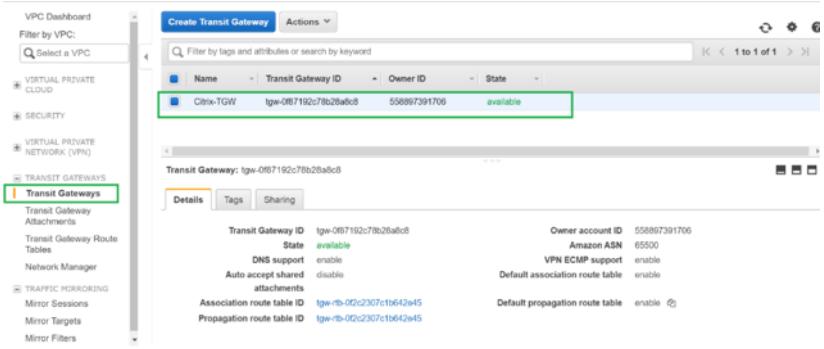


AWS トランジットゲートウェイの設定

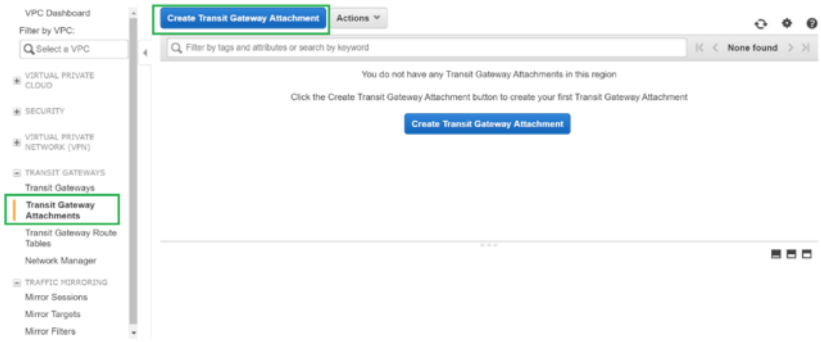
AWS トランジットゲートウェイを作成するには、VPC ダッシュボードに移動し、[トランジットゲートウェイ] セクションに移動します。

1. 次のスクリーンショットで強調表示されているとおりにトランジットゲートウェイ名、説明、Amazon ASN 番号を指定し、[**Create Transit Gateway**] をクリックします。

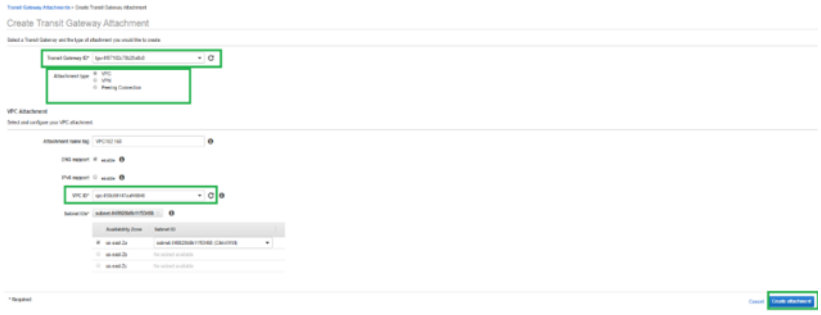
トランジットゲートウェイの作成が完了すると、ステータスが [**Available**] として表示されます。



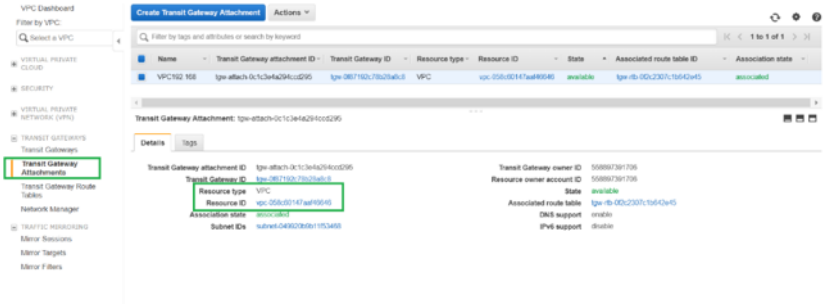
2. トランジットゲートウェイの 添付ファイルを作成するには、「トランジットゲートウェイ」 **>**「トランジットゲートウェイの添付ファイル」に移動し、「トランジットゲートウェイの添付ファイルの作成」をクリックします。



3. ドロップダウンリストから作成したトランジットゲートウェイを選択し、**VPC** としてアタッチメントタイプを選択します。添付ファイル名タグを指定し、作成したトランジットゲートウェイにアタッチする VPC ID を選択します。選択した VPC のサブネットの 1 つが自動選択されます。[アタッチメントを作成] をクリックして、VPC をトランジットゲートウェイにアタッチします。

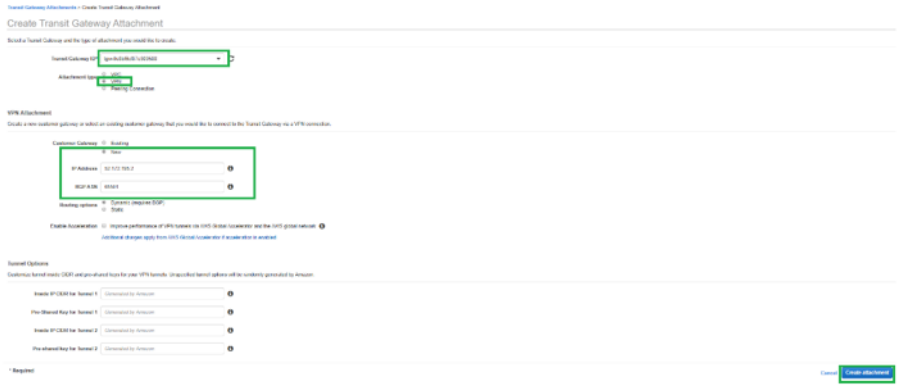


4. VPC をトランジット Gateway にアタッチすると、リソースタイプ **VPC** がトランジットゲートウェイに関連付けられていることがわかります。

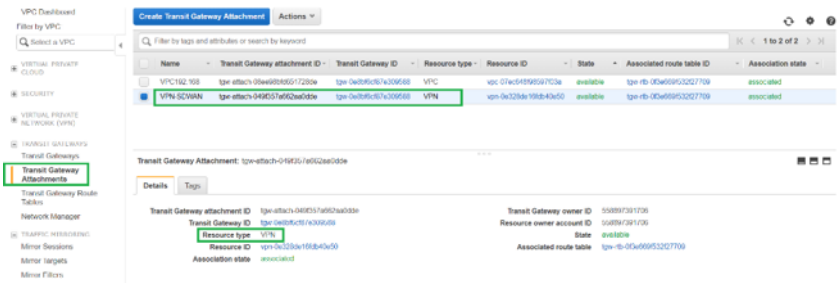


5. VPN を使用して SD-WAN をトランジットゲートウェイに接続するには、ドロップダウンリストから トランジットゲートウェイ **ID** を選択し、[**Attachment type**] を **VPN** として選択します。正しいトランジットゲートウェイ ID を選択していることを確認します。

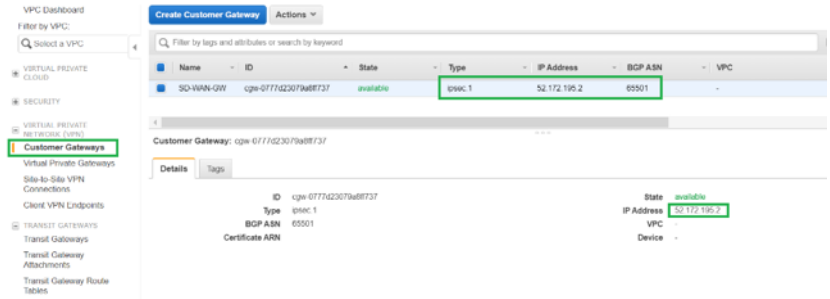
   SD-WAN リンクのパブリック IP アドレスと BGP ASN 番号を指定して、新しい VPN カスタマーゲートウェイを接続します。[添付ファイルの作成] をクリックして、VPN をトランジットゲートウェイにアタッチします。



6. 次のスクリーンショットに示すように、VPN は、トランジットゲートウェイに接続したら、あなたは詳細を表示することができます。

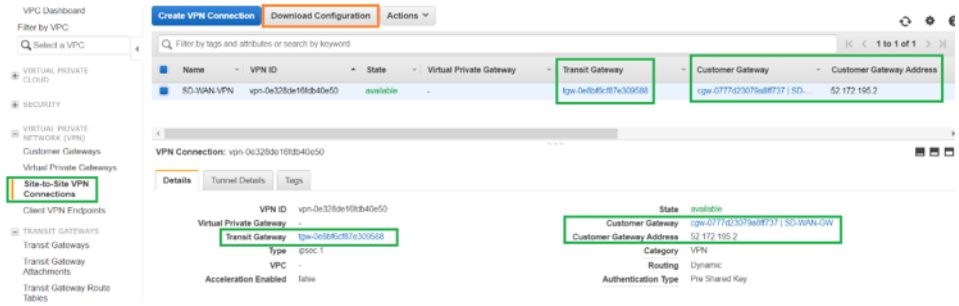


7. [カスタマーゲートウェイ] で、SD-WAN カスタマーゲートウェイとサイト間 VPN 接続は、トランジットゲートウェイへの VPN 添付ファイルの一部として作成されます。SD-WAN カスタマーゲートウェイが、SD-WAN の WAN リンクパブリック IP アドレスを表すこのカスタマーゲートウェイの IP アドレスとともに作成されていることがわかります。

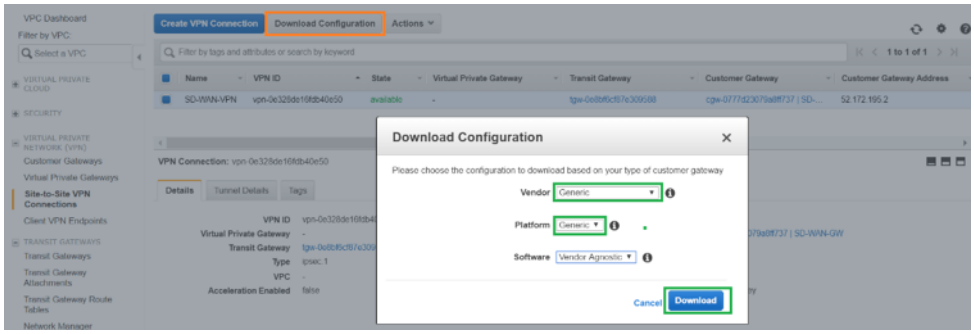


8. サイト間 **VPN** 接続 に移動し、**SD-WAN** カスタマーゲートウェイ **VPN** 設定をダウンロードします。この構成ファイルには、BGP ピア情報とともに 2 つの IPsec トンネル詳細があります。冗長性のために、SD-WAN からトランジットゲートウェイへの 2 つのトンネルが作成されます。

   SD-WAN リンクのパブリック IP アドレスがカスタマーゲートウェイアドレスとして設定されていることがわかります。



9. [設定のダウンロード] をクリックし、VPN 構成ファイルをダウンロードします。**[**** ベンダー]、[プラットフォーム]、[ベンダーに依存しないソフトウェア] を選択します。**



ダウンロードした構成ファイルには、次の情報が含まれています。

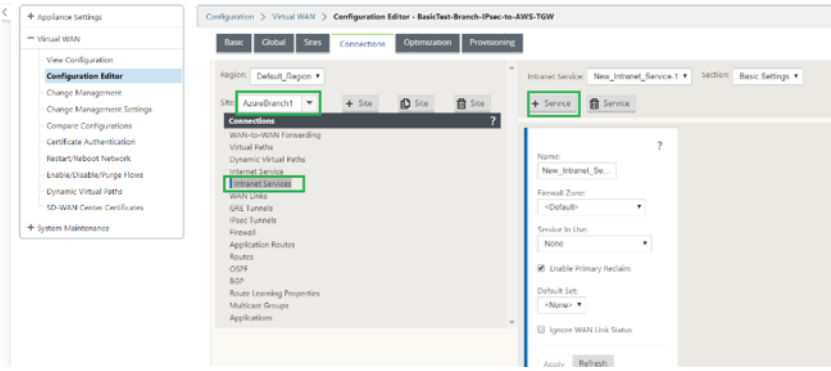
- IKE 設定
- AWS トランジットゲートウェイの IPsec 設定
- トンネルインターフェイス構成
- BGP 構成

この情報は、高可用性（HA）用の 2 つの IPsec トンネルで使用できます。SD-WAN で設定する場合は、両方のトンネルエンドポイントを設定してください。参考のために次のスクリーンショットを参照してください。

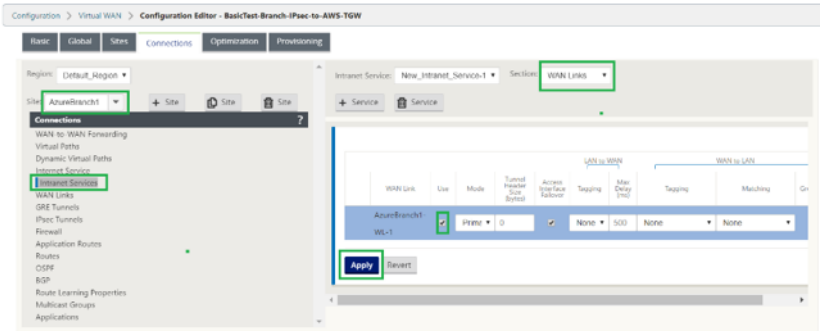
```
#3: Tunnel Interface Configuration

Your Customer Gateway must be configured with a tunnel interface that is
associated with the IPSec tunnel. All traffic transmitted to the tunnel
interface is encrypted and transmitted to the Virtual Private Gateway.


The Customer Gateway and Virtual Private Gateway each have two addresses that relate
to this IPSec tunnel. Each contains an outside address, upon which encrypted
traffic is exchanged. Each also contain an inside address associated with
the tunnel interface.

The Customer Gateway outside IP address was provided when the Customer Gateway
was created. Changing the IP address requires the creation of a new
Customer Gateway.

The Customer Gateway inside IP address should be configured on your tunnel
interface.

Outside IP Addresses:
  - Customer Gateway                    : 52.172.195.2
  - Virtual Private Gateway             : 3.133.37.22

Inside IP Addresses
  - Customer Gateway                    : 169.254.216.178/30
  - Virtual Private Gateway             : 169.254.216.177/30

Configure your tunnel to fragment at the optimal size:
  - Tunnel interface MTU     : 1436 bytes
```

SD-WAN でイントラネットサービスを構成する

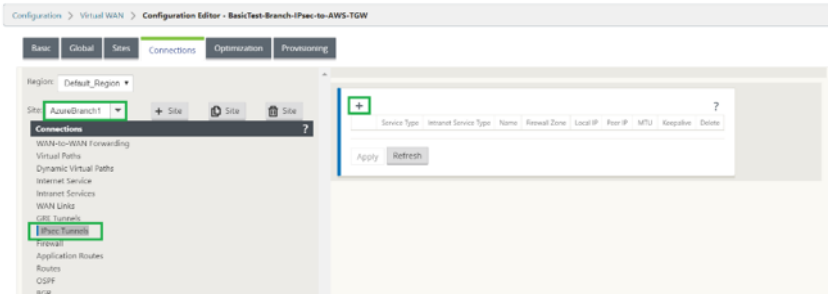
1. SD-WAN の IPSec トンネル構成で使用されるイントラネットサービスを構成するには、[構成エディタ] **>** **[**接続**]** の順に選択し、ドロップダウンリストからサイトを選択し、[イントラネットサービス] を選択します。[**+** サービス] をクリックして、新しいイントラネットサービスを追加します。



2. イントラネットサービスの追加後、このサービスに使用される WAN リンクを選択します (これを使用して、トランジットゲートウェイへのトンネルを確立します)。

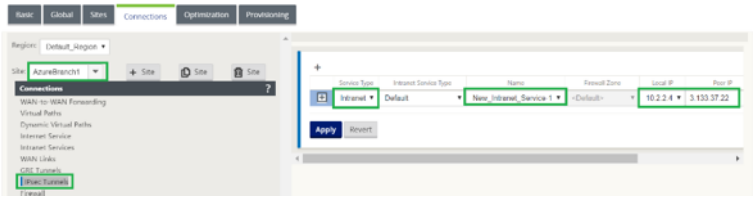


3. AWS Transit Gateway への IPsec トンネルを設定するには、[設定エディタ**] > [**接続] に移動し、ドロップダウンリストから [サイト] を選択し、[**IPsec Tun**nels] をクリックします。IPSec トンネルを追加するには、[**+**] オプションをクリックします。

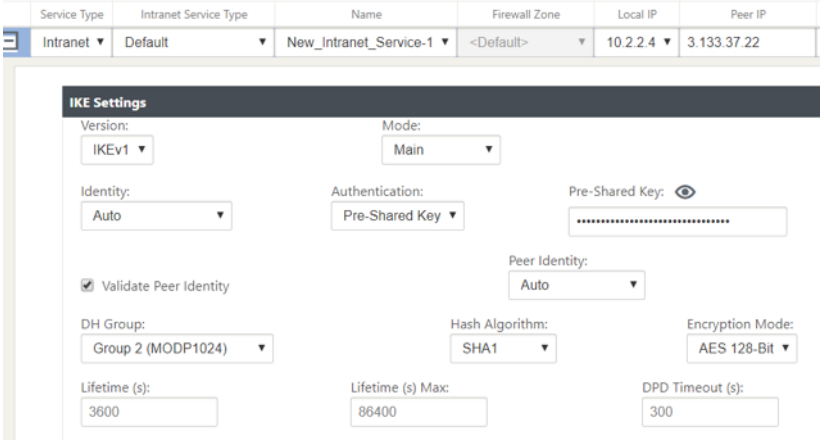


4. [サービスタイプ] を [イントラネット] として選択し、追加した [イントラネットサービス名] を選択します。[ローカル **IP** アドレス] を [WAN リンク IP アドレス] として、[ピア アドレス] を [トランジットゲートウェイ仮想プライベートゲートウェイ IP アドレス] として選択します。

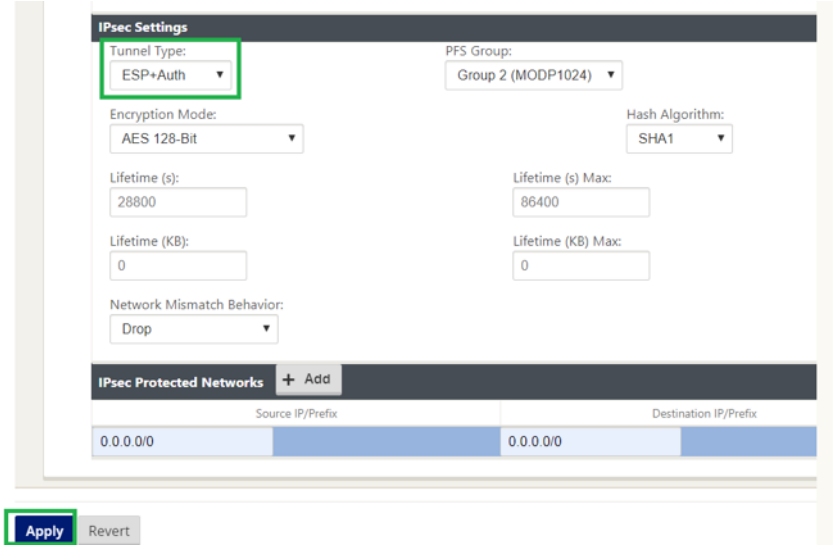
   設定のアクティブ化後すぐに SD-WAN によってトンネルが開始されるようにするには、[**Keepalive**] チェックボックスをオンにします。



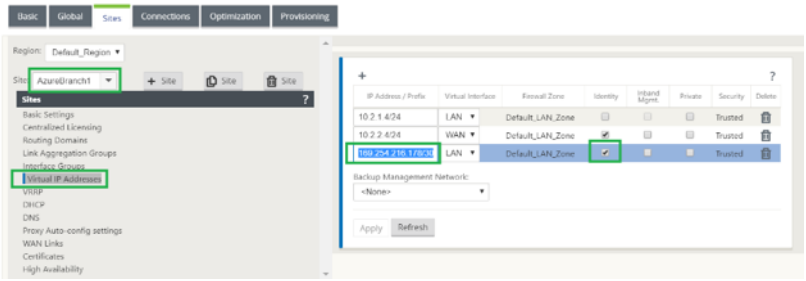
5. AWS からダウンロードした VPN 設定ファイルに基づいて IKE パラメータを設定します。



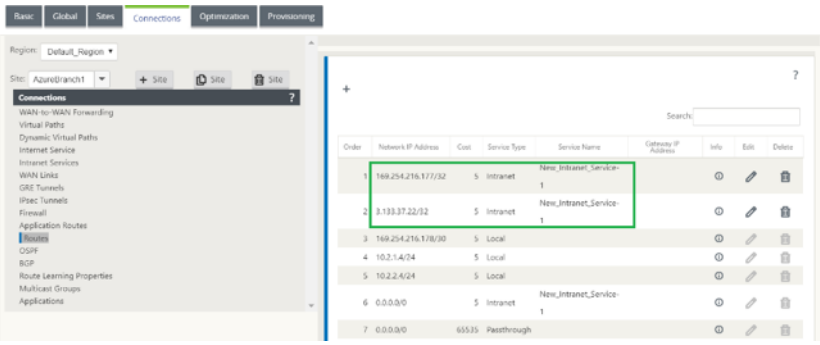
6. AWS からダウンロードした VPN 設定ファイルに基づいて IPSec パラメータを設定します。また、トンネルを介して送信する ネットワークに基づいて、**IPsec** 保護された ネットワークを構成します。IPsec トンネル経由のトラフィックを許可するように構成されていることがわかります。



7. カスタマーゲートウェイの内部 **IP** アドレスを SD-WAN 上の仮想 IP アドレスの 1 つとして設定します。ダウンロードされた VPN 設定ファイルから、Tunnel-1 に関連する IP アドレス内のカスタマー Gateway を見つけます。このカスタマー Gateway の IP アドレスを SD-WAN 上の仮想 IP アドレスのいずれかとして設定し、[**ID**] チェックボックスをオンにします。

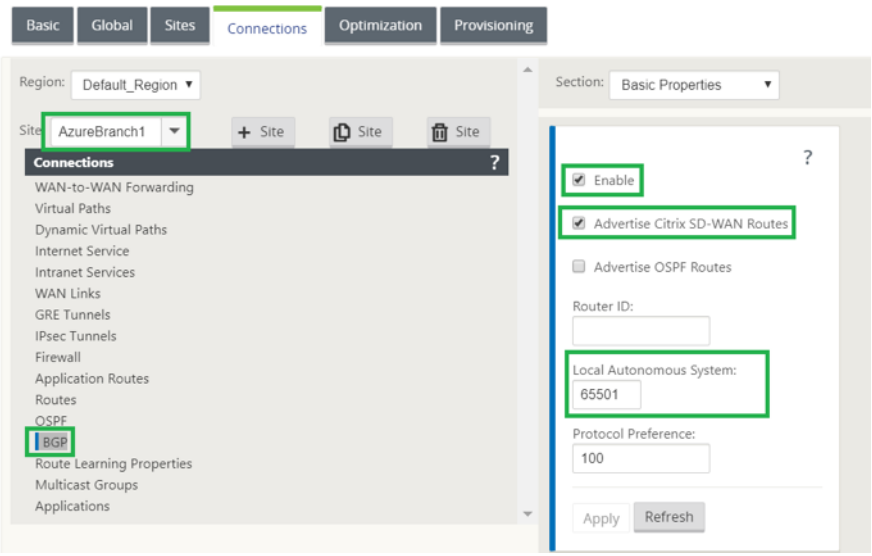


8. SD-WAN に ルート を追加して、トランジット ゲートウェイの仮想プライベート ゲートウェイに到達します。ダウンロードされた VPN 設定ファイルから、Tunnel-1 に関連する仮想プライベートゲートウェイの内側および外部 IP アドレスを検索します。サービスタイプ を イントラネット として仮想プライベートゲートウェイの内部と外部の IP アドレスにルートを追加し、上記の手順で作成したイントラネットサービスを選択します。



9. SD-WAN で **BGP** を設定します。適切な ASN 番号で BGP を有効にします。ダウンロードした VPN 構成ファイルから、Tunnel-1 に関連する BGP 構成オプションを探します。これらの詳細を使用して、SD-WAN に BGP ネイバーを追加します。

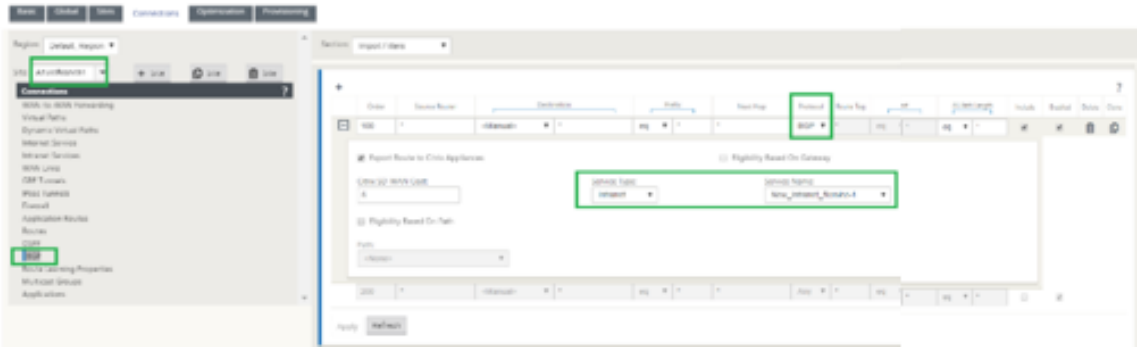
   SD-WAN で BGP を有効にするには、[接続] に移動して、ドロップダウンリストからサイトを選択し、[**BGP**] を選択します。BGP を有効にするには、[Enable] チェックボックスをオンにします。[**Citrix SD-WAN** ルートのアド バタイズ] チェックボックスをクリックして、SD-WAN ルートをトランジットゲートウェイにアドバタイズします。BGP 設定オプションから カスタマーゲートウェイ **ASN** を使用し、ローカル自律システムとして設定します。



10. SD-WAN に BGP ネイバー を追加するには、[接続] に移動して、ドロップダウンリストからサイトを選択し、[**BGP**] を選択します。[ネイバー] セクションをクリックし、[**+**] オプションをクリックします。

    ネイバーを追加するときに、**BGP** 設定オプションからネイバー **IP** アドレス と 仮想プライベートゲートウェイ **ASN** を使用します。送信元 **IP** は、AWS からダウンロードした設定ファイルの カスタマーゲートウェイ 内部 IP アドレス（SD-WAN で仮想 IP アドレスとして設定）と一致する必要があります。SD-WAN で マルチホップ が有効になっている BGP ネイバーを追加します。

11. インポートフィルタ を追加して BGP ルートを SD-WAN にインポートするには、[接続] に移動し、ドロップダウンリストからサイトを選択し、[**BGP**] を選択して [**Import Filters**] セクションをクリックします。[**+**] オプションをクリックして、[インポート] フィルタを追加します。[**Protocol**] を [**BGP**] として選択し、[any] に一致させ、すべての BGP ルートをインポートします。[サービスタイプ] を [イントラネット] として選択し、作成したイントラネットサービスを選択します。これは、サービスタイプの BGP ルートをイントラネットとしてインポートするためです。

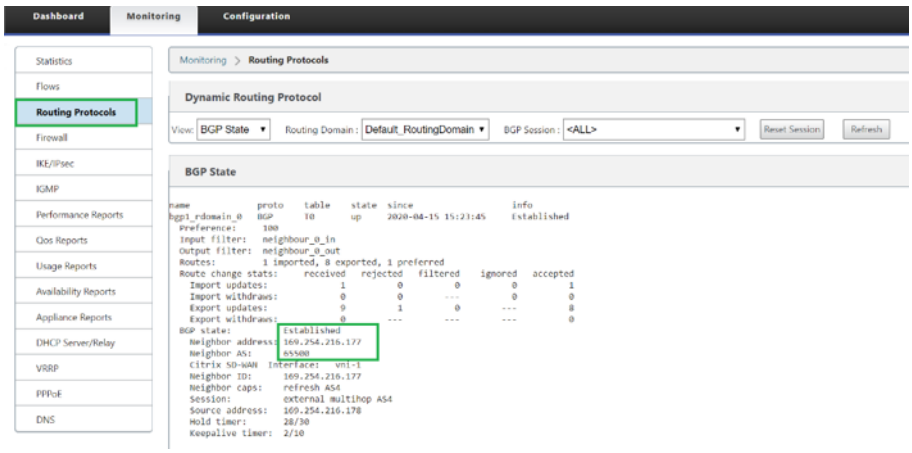


SD-WAN でのモニタリングとトラブルシューティング

1. SD-WAN で IPsec トンネル確立ステータスを確認するには、[モニタリング**] > [**統計情報**] > [IPsec** トンネル**]** に移動します。次のスクリーンショットでは、IPsec トンネルが SD-WAN から AWS Transit Gateway に向けて確立され、状態が **GO**OD であることがわかります。
   また、この IPsec トンネルを介して送受信されるトラフィックの量を監視することもできます。

   ![SD-WAN での監視とトラブルシューティング] (/en-us/citrix-sd-wan/11/media/monitoring-and-troubleshooting-on-sdwan.png)

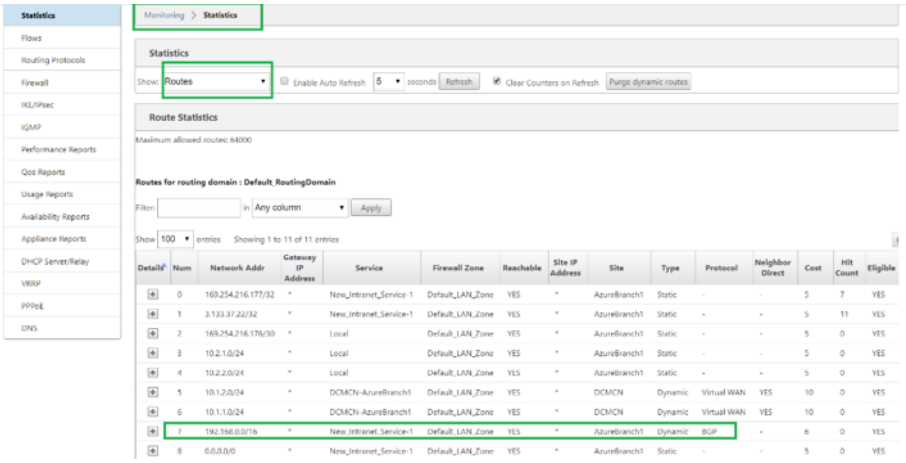
2. SD-WAN の **BGP** ピアリング ステータスを確認するには、[モニタリング**] > [**ルーティングプロトコル] に移動し、[**BGP** ステート] を選択します。BGP 状態が [確立 済み] として報告され、ネイバー **IP** アドレスとネイバー **ASN** が AWS BGP ネイバーの詳細と一致していることがわかります。これにより、IPsec トンネルを介して SD-WAN から AWS トランジットゲートウェイへの BGP ピアリングが確立されたことを確認できます。



   VPC（192.168.0.0）が AWS トランジットゲートウェイにアタッチされています。SD-WAN は、この VPC ネットワーク（192.168.0.0）を AWS Transit Gateway から BGP
   経由で学習しました。このルートは、上記の手順で作成したインポートフィルタに従って、サービスタイプがイントラネットで SD-WAN にインストールされました。

3. SD-WAN への BGP ルートのインストールを確認するには、**[Monitoring] > [Statistics] > [** Routes] の順に選択し、サービスタイプがイントラネットの BGP ルートとしてインストールされたネットワーク

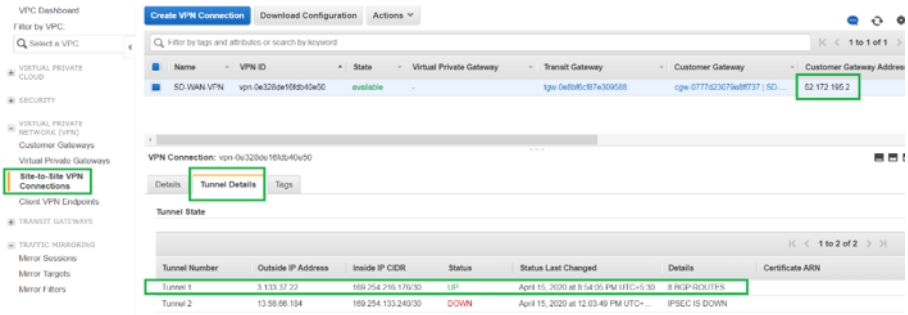
192.168.0.0/16 を確認します。つまり、AWS Transit Gateway にアタッチされたネットワークを学習し、確立された IPsec トンネルを介してこれらのネットワークと通信できます。



AWS でのモニタリングおよびトラブルシューティング

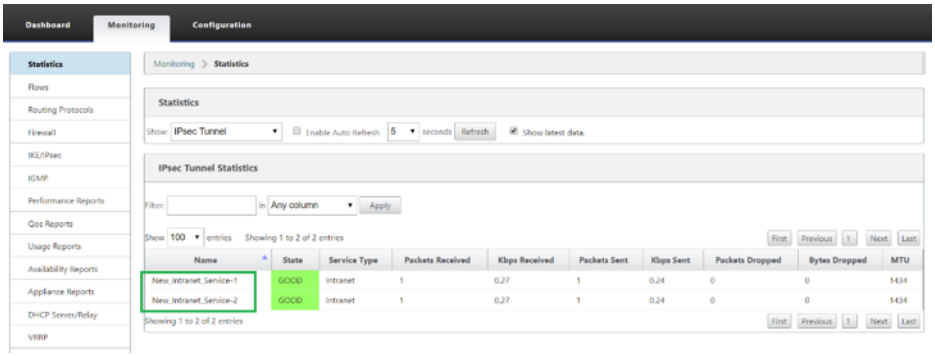
1. AWS で IPsec トンネルの確立ステータスを確認するには、仮想プライベートネットワーク（**VPN**）**>** サイト間 **VPN** 接続に移動します。次のスクリーンショットでは、カスタマーゲートウェイアドレスは、あなたがトンネルを確立している使用して SD-WAN リンクのパブリック IP アドレスを表していることを確認することができます。

   トンネルのステータスは **UP** と表示されます。また、AWS が SD-WAN から **8** つの **BGP** ルート を学習していることも観察できます。つまり、SD-WAN は AWS Transit Gateway を使用してトンネルを確立でき、BGP 経由でルートを交換することもできます。

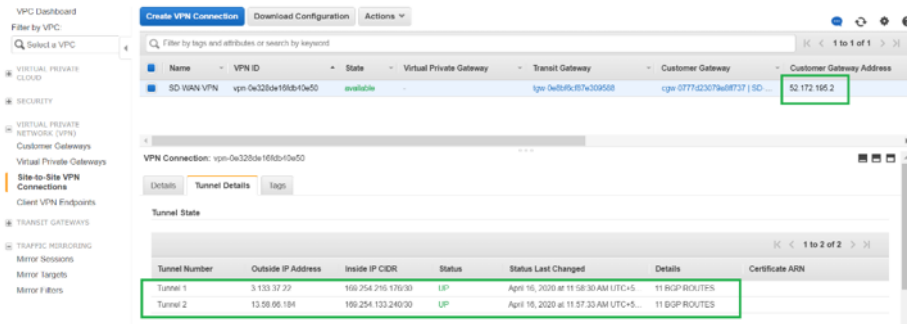


2. SD-WAN にダウンロードした構成ファイルに基づいて、2 番目のトンネルに関連する IPSec および BGP の詳細を設定します。

   SD-WAN では、次のように、両方のトンネルに関連するステータスを監視できます。



3. 両方のトンネルに関連するステータスは、AWS で次のように監視できます。

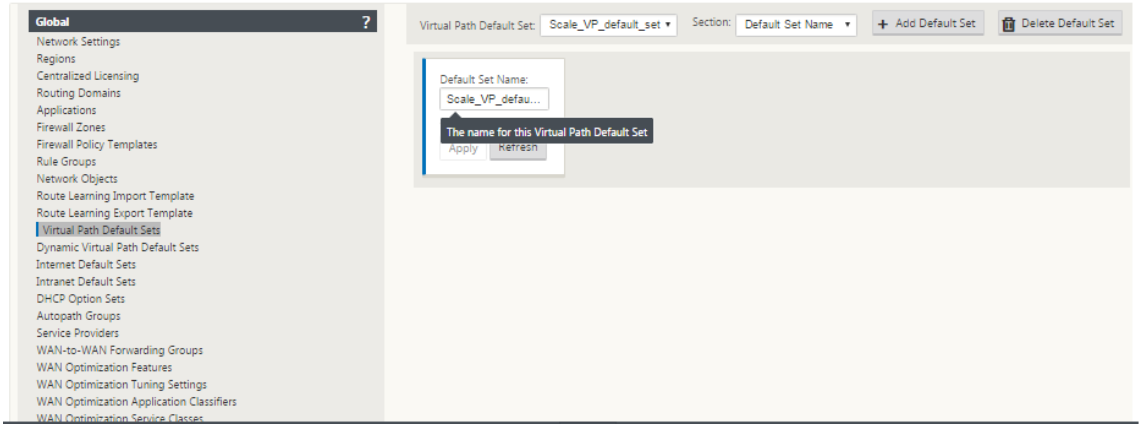


仮想パスおよびダイナミックパスの **IPSec** トンネルを構成する方法

May 10, 2021

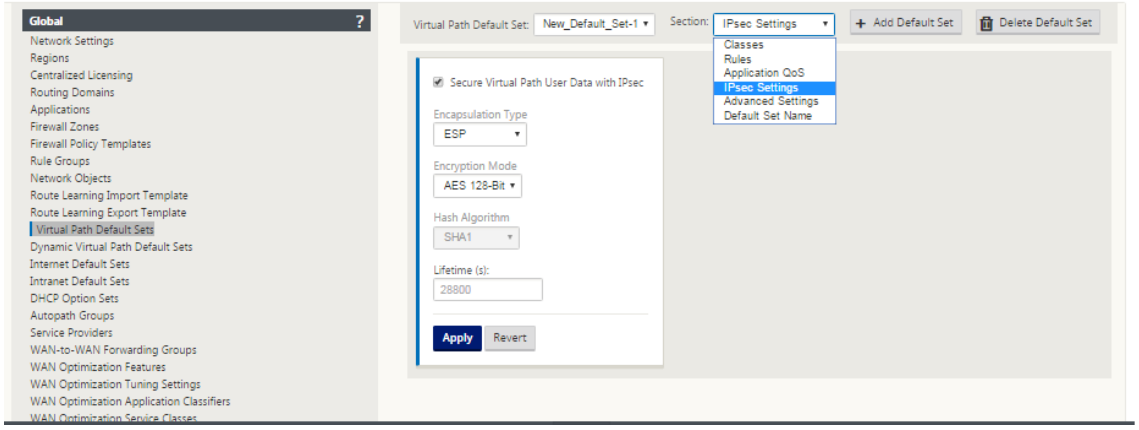
Citrix SD-WAN ブランチサイト間の仮想パスおよび動的仮想パスの IPsec トンネルを構成するには:

1. [グローバル**] > [**仮想パスのデフォルトセット] または [動的仮想パスのデフォルトセット**]** に移動します。



2. 新しいデフォルトセット（仮想または動的仮想パス）を作成し、**IPsec** を使用してセキュア仮想パスユーザーデータを有効にします。

3. IPsec 暗号化に使用できるオプションの 1 つを選択します。
    - カプセル化タイプ:ESP、AH、または ESP+AH
    - 暗号化モード:AES-CBC、AES 128、または 256 ビット
    - ハッシュアルゴリズム：SHA1 または SHA-256
4. 作成した仮想パスのデフォルトセットを MCN ノードに適用します。これにより、MCN への仮想パスを持つすべてのクライアント・ノードに、同じデフォルト・セットが自動的に適用されます。

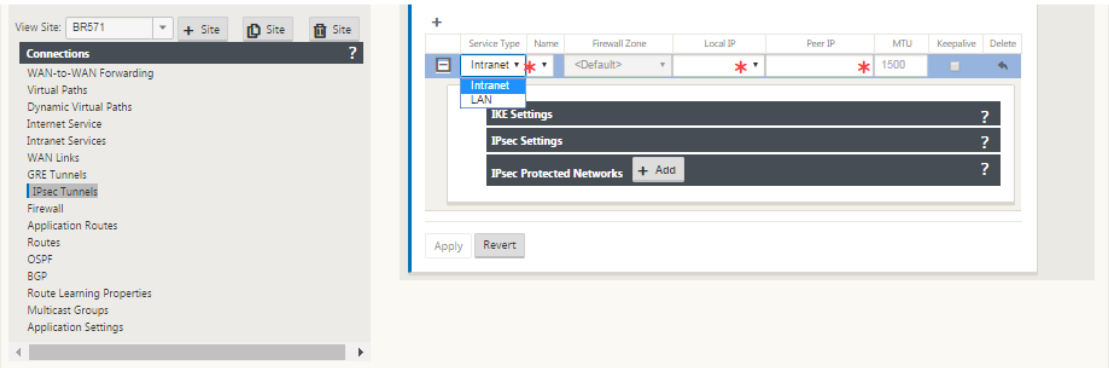


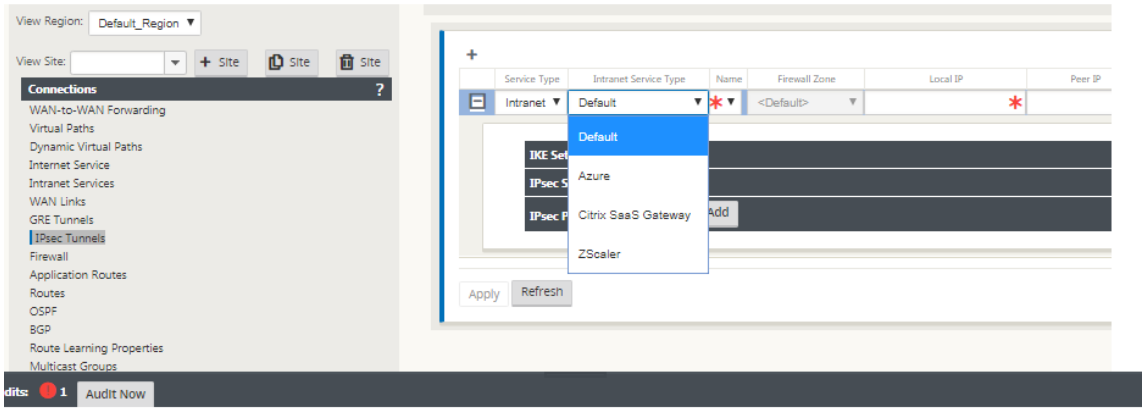
SD-WAN とサードパーティデバイス間の IPsec トンネルを構成する方法

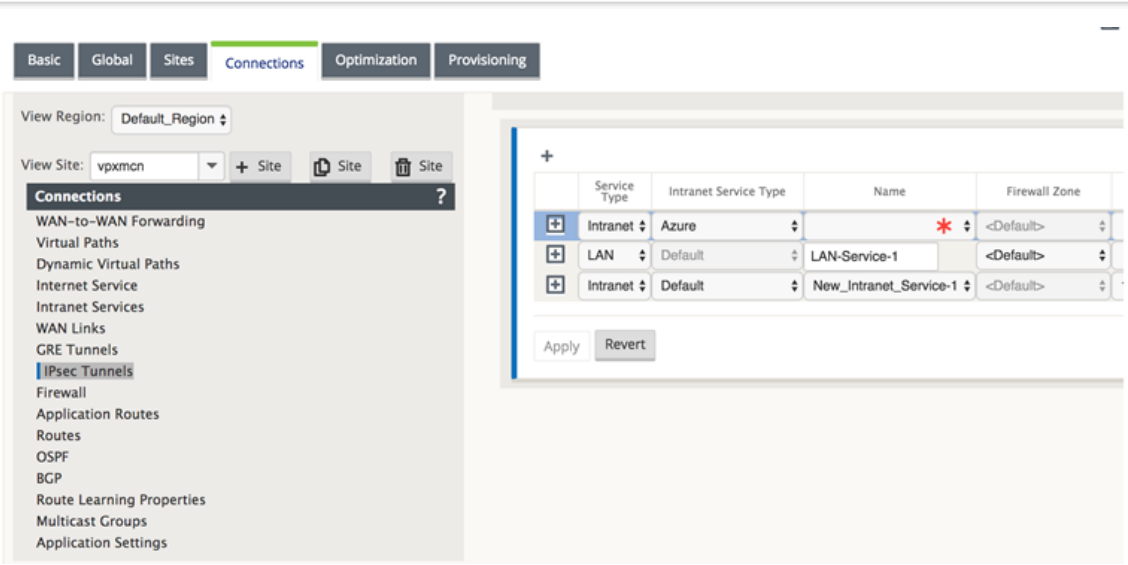
May 10, 2021

イントラネットまたは LAN サービスの IPSec トンネルを構成するには、次の手順を実行します。

1. 構成エディタで、[接続] > [サイトの表示**] > [**サイト **[**名**]**] > [**IPsec** トンネル] に移動します。サービスタイプ（LAN またはイントラネット）を選択します。
2. サービス・タイプの「名前」を入力します。イントラネットサービスの種類では、構成されたイントラネットサーバーによって、使用できるローカル IP アドレスが決まります。
3. 使用可能なローカル **IP** アドレスを選択し、ピアに使用する仮想パスのピア **IP** アドレスを入力します。

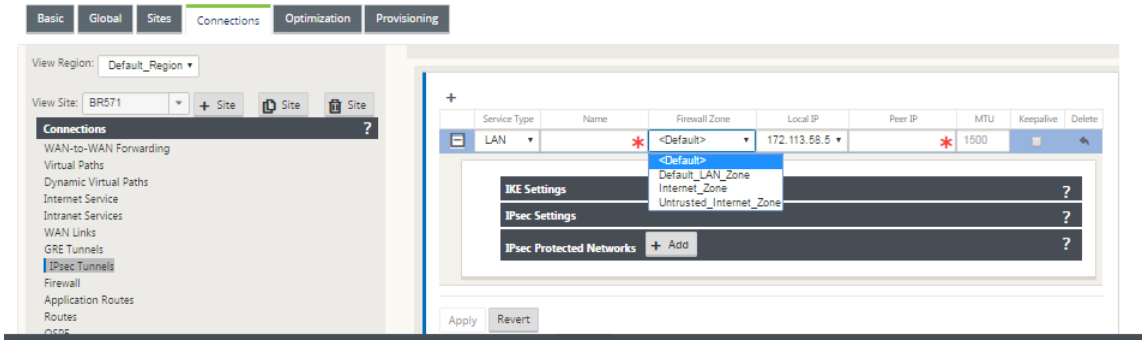






注

[サービスタイプ] が [イントラネット] の場合、IP アドレスは選択したイントラネットサービスによって事前に決定されます。



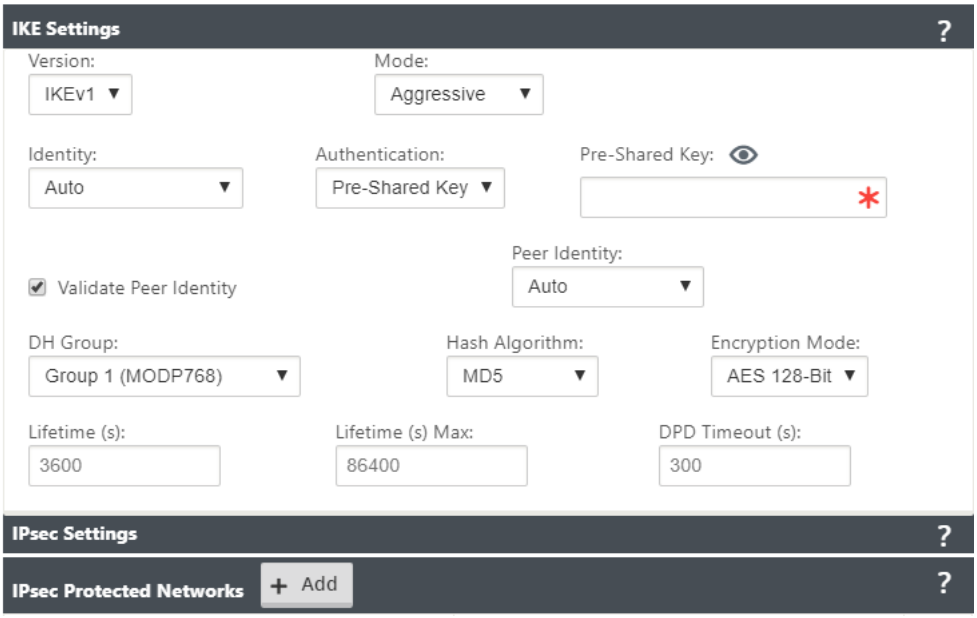
4. 次の表に示す条件を適用して、IPSec 設定を構成します。完了したら、[適用] をクリックして設定を保存します。

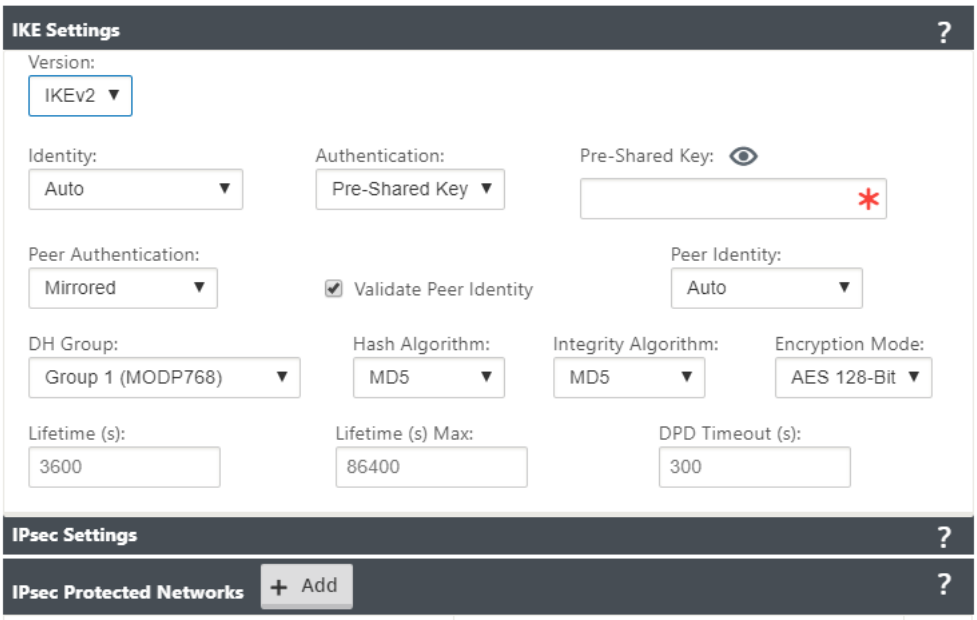
フィールド	説明	値
サービスの種類	ドロップダウンメニューからサービスタイプを選択します。	イントラネット、LAN
名前	サービスの種類が [イントラネット] の場合は、ドロップダウンメニューで構成されたイントラネットサービスのリストから選択します。サービスタイプが LAN の場合は、一意の名前を入力します。	テキスト文字列
ローカル IP	このサイトで構成されている使用可能な仮想 IP アドレスのドロップダウンメニューから、IPSec トンネルのローカル IP アドレスを選択します。	IP アドレス
ピア IP	IPsec トンネルのピア IP アドレスを入力します。	IP アドレス
MTU	IKE および IPsec フラグメントをフラグメント化するための **MTU** を入力します。	デフォルト:1500
IKE 設定	バージョン: ドロップダウンメニューから IKE バージョンを選択します。	IKEv1 IKEv2
モード	ドロップダウンメニューからモードを選択します	FIPS 準拠: メイン、非 FIPS 準拠: アグレッシブ
ID	ドロップダウンメニューから ID を選択します	自動 IP アドレス手動 IP アドレスユーザ FQDN

フィールド	説明	値
認証	ドロップダウンメニューから認証タイプを選択します	事前共有キー: 事前共有キーを使用している場合は、このフィールドにコピーして貼り付けます。眼球（）アイコンをクリックして、事前共有キーを表示します。証明書:ID 証明書を使用している場合は、ドロップダウンメニューから選択します。
ピア ID の検証	IKE のピアを検証するには、このチェックボックスをオンにします。ピアの ID タイプがサポートされていない場合は、この機能を有効にしないでください。	なし
DH グループ	ドロップダウンメニューから、IKE キー生成に使用する Diffie-Hellman グループを選択します。	非 FIPS 準拠: グループ 1、FIPS 準拠: グループ 2 グループ 5 グループ 14 グループ 15 グループ 16 グループ 19 グループ 20 グループ 21
ハッシュアルゴリズム	ドロップダウンメニューからアルゴリズムを選択して、IKE メッセージを認証します。	非 FIPS 準拠:MD5 FIPS 準拠:SHA1 SHA-256
暗号化モード	ドロップダウンメニューから IKE メッセージの 暗号化モード を選択します。	AES 128 ビット AES 192 ビット AES 256 ビット
ライフタイム	IKE セキュリティアソシエーションが存在するための優先期間を秒単位で入力します。	3600 秒（デフォルト）
最大寿命	IKE セキュリティアソシエーションの存在を許可する最大優先時間を秒単位で入力します。	86400 秒（デフォルト）
DPD タイムアウト	VPN 接続の デッドピア検出タイムアウトを秒単位で入力します。	300 秒（デフォルト）
IKEv2	ピア認証：ドロップダウンメニューから「ピア認証」を選択します。	ミラー化された事前共有キー証明書
IKE2-事前共有キー	ピア事前共有キー：認証のために、IKEv2 ピア事前共有キーをこのフィールドに貼り付けます。眼球（）アイコンをクリックして、事前共有キーを表示します	テキスト文字列

フィールド	説明	値
整合性アルゴリズム	ドロップダウンメニューから、HMAC 検証に使用するハッシュアルゴリズムとしてアルゴリズムを選択します	非 FIPS 準拠:MD5 FIPS 準拠:SHA1 SHA-256

> 注:
>
> 終端側の IPsec ルータの設定にハッシュベースメッセージ認証コード（HMAC）が含まれている場合は、**SHA1** としてハッシュアルゴリズムを使用して IPsec モードを **EXP+Auth** に変更します。



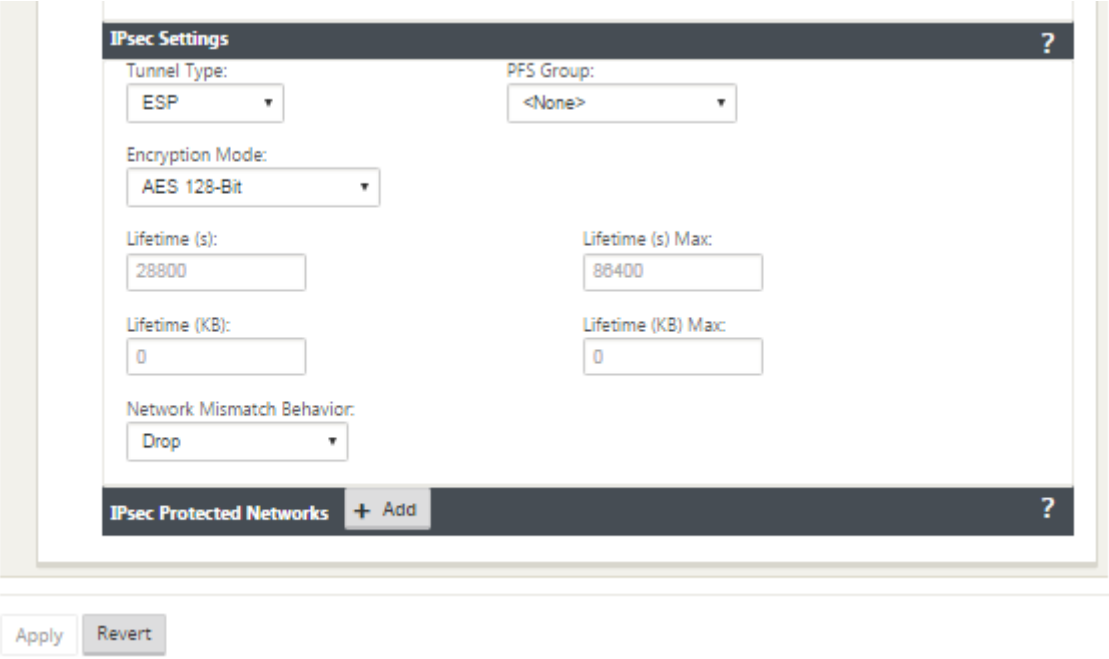


IPsec および IPsec で保護されたネットワーク設定

フィールド	説明	値
トンネルタイプ	ドロップダウンメニューから [トンネルタイプ] を選択します。	ESP ESP+Auth ESP+NULL AH
PFS グループ	ドロップダウンメニューから [Diffie-Hellman] グループを選択して、完全な前方秘密鍵生成に使用します。	なしグループ 1 グループ 2 グループ 5 グループ 14 グループ 15 グループ 16 グループ 19 グループ 20 グループ 21

フィールド	説明	値
暗号化モード	ドロップダウンメニューから IPsec メッセージの 暗号化モード を選択します。	[ESP] または [ESP+ 認証] を選択した場合は、次のいずれかを選択します。AES 128 ビット、AES 192 ビット、AES 256 ビット、AES 128 ビット GCM 64 ビット、AES 192 ビット GCM 64 ビット、AES 256 ビット GCM 64 ビット、AES 128 ビット GCM 96 ビット、AES 128 ビット GCM 96 ビット、AES 192 ビット GCM 96 ビット、AES 256 ビット GCM 96 ビット、AES 128 ビット GCM 128 ビット、AES 192 ビット GCM 128 ビット、AES 256 ビット GCM 128 ビット。AES 128/192/256 ビットは CBC をサポートしています。
ライフタイム	IPsec セキュリティアソシエーションの存在を許可する時間を秒単位で入力します。	28800 秒（デフォルト）
最大有効期間	IPSec セキュリティアソシエーションの存在を許可する最大時間を秒単位で入力します。	86400 秒（デフォルト）
ライフタイム (KB)	IPsec セキュリティアソシエーションが存在するデータ量をキロバイト単位で入力します。	キロバイト
最大寿命（KB）	IPSec セキュリティアソシエーションの存在を許可するデータの最大量をキロバイト単位で入力します。	キロバイト
ネットワークの不一致動作	パケットが IPsec トンネルの保護ネットワークと一致しない場合に実行するアクションをドロップダウンメニューから選択します。	ドロップ、暗号化されていない送信、非 IPSec ルートの使用
IPSec 保護ネットワーク	送信元 **IP /**プレフィックス**:[**追加**] (+ [**追加**])** ボタンをクリックした後、**IP**Sec トンネルが保護するネットワークトラフィックの 送信元 **IP** とプレフィックスを入力します。	IP アドレス

フィールド	説明	値
IPSec 保護ネットワーク	宛先 **IP /**プレフィックス**:IPsec** トンネルが保護するネットワークトラフィックの宛先 **IP** とプレフィックスを入力します。	IP アドレス



IPsec トンネルの監視

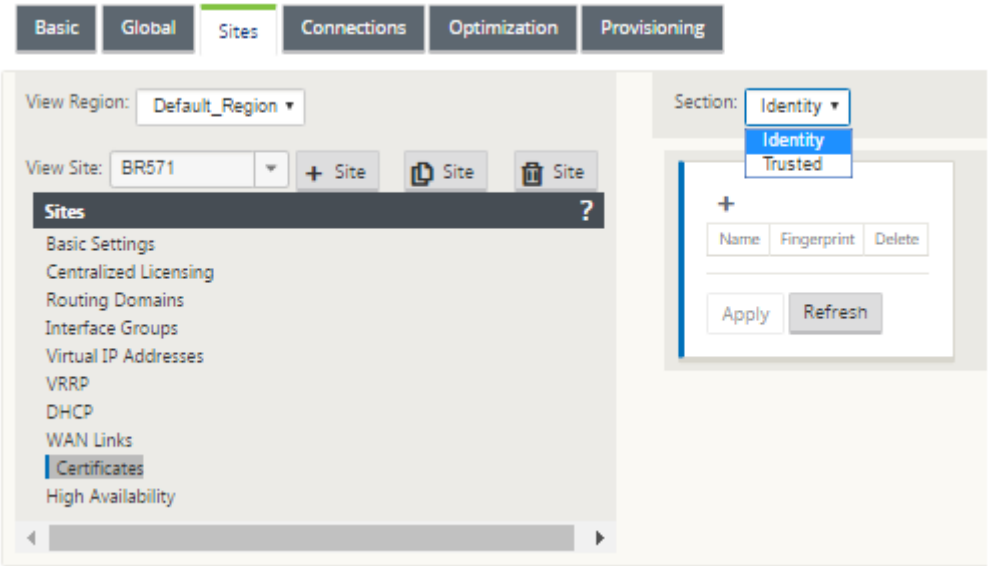
SD-WAN アプライアンスの GUI で「監視」**>**「**IKE/IPSec** 」に移動し、IPSec トンネル設定を表示および監視します。

IKE 証明書を追加する方法

May 10, 2021

IKE ネゴシエーション用の証明書を実装するには、次の手順を実行します

1. [サイト] > [証明書] に移動し、必要な証明書を追加します。

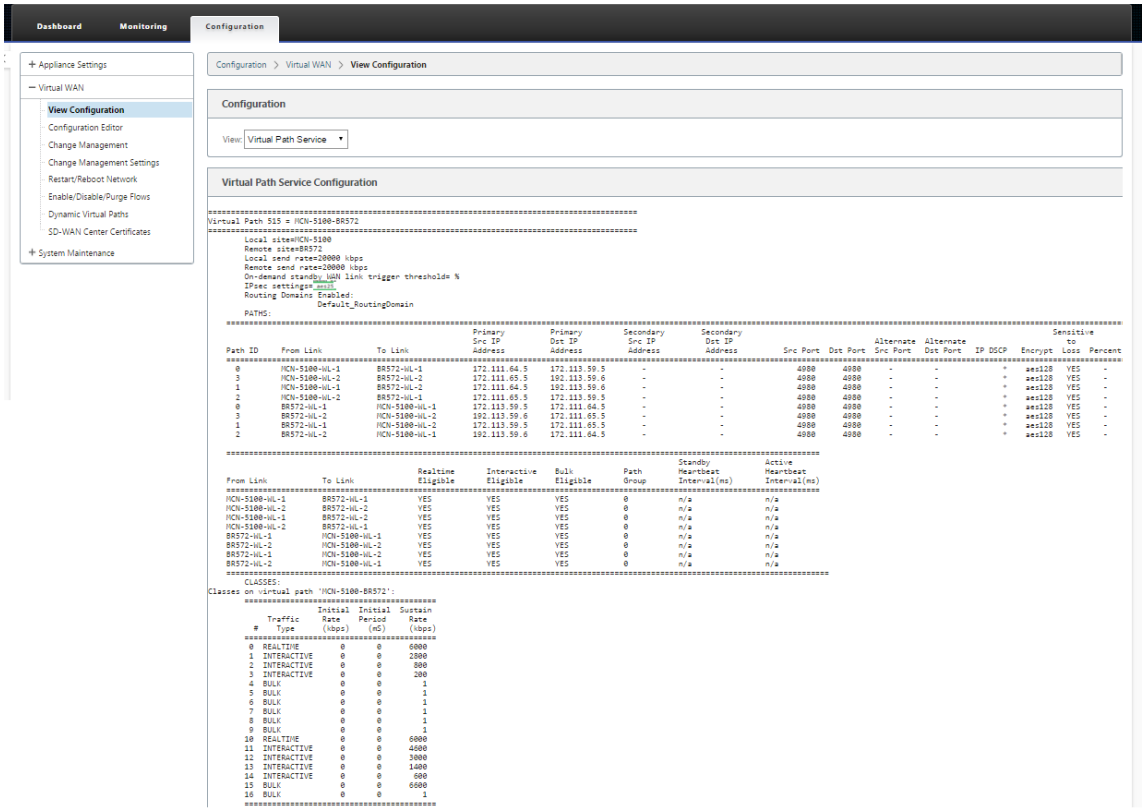


IPsec トンネルの設定を表示する方法

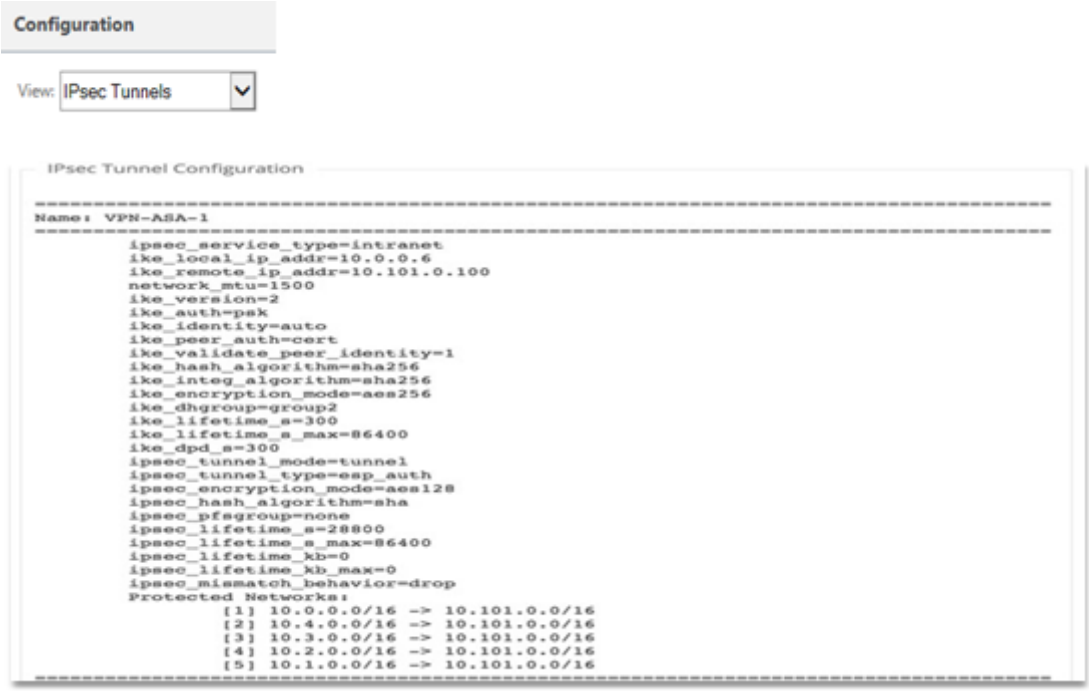
May 10, 2021

ipsec トンネルの設定を表示するには、次の手順を実行します。

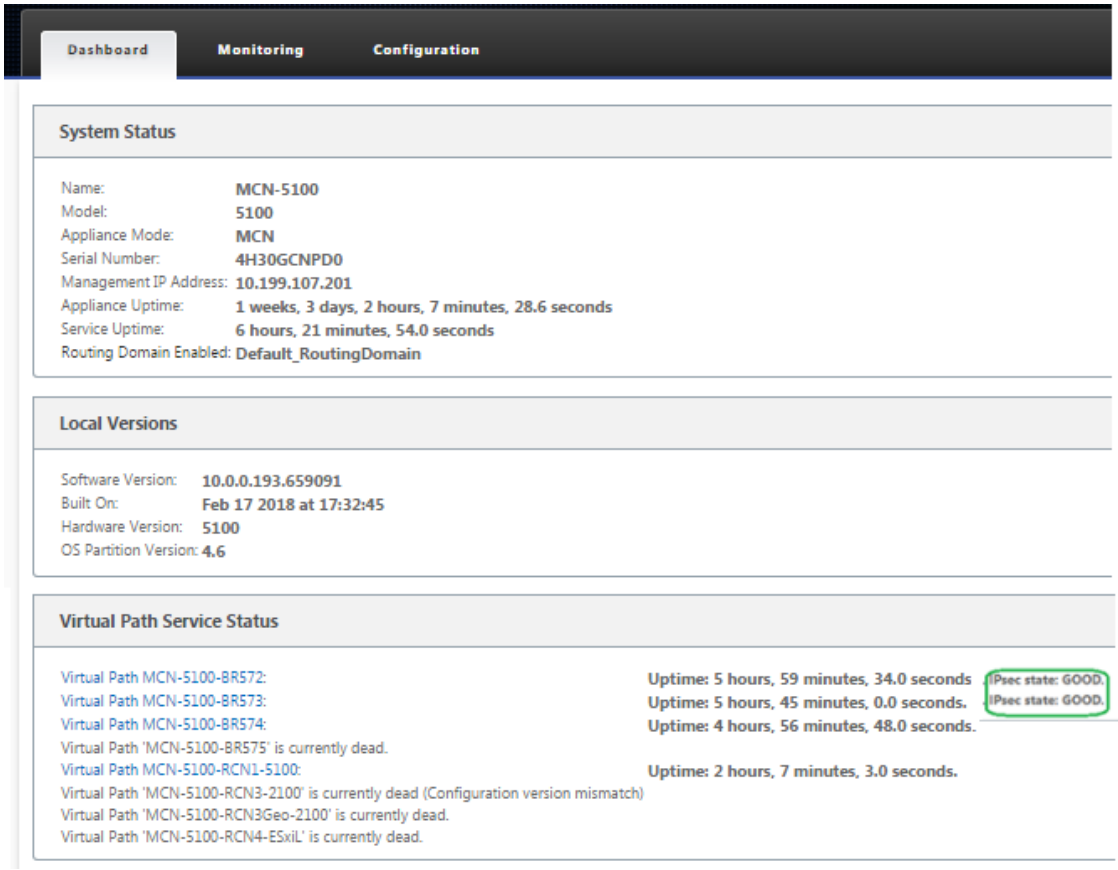
1. [構成**] > [**仮想 **WAN**] > [構成の表示] に移動します。
2. ドロップダウンメニューから [仮想パスサービス] を選択します。IPsec 設定は、構成エディタで IPsec が有効になっている場合にのみ表示されます。



3. ドロップダウンメニューから [**IPSec** トンネル] を選択して、IPSec トンネル設定を表示します。



4. 各仮想パスは、次に示すように、独自の IPsec トンネルのステータスを表示します。

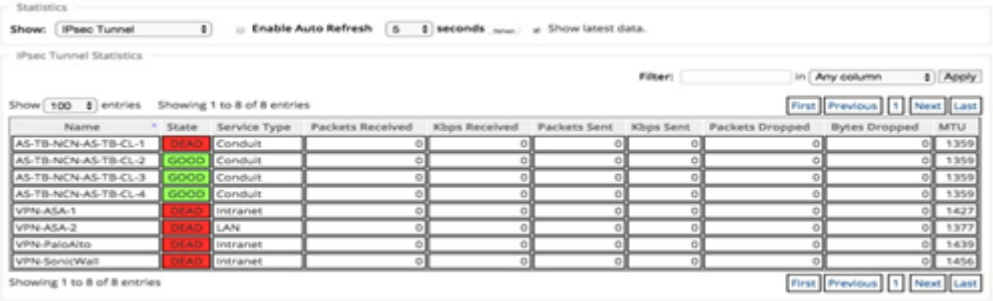


IPsec の監視とログ

May 10, 2021

IPsec トンネルの統計情報を監視するには:

1. [監視] **>** [統計] に移動します。[**Show**] ドロップダウンメニューから [**IPSec Tunnel**] を選択します。

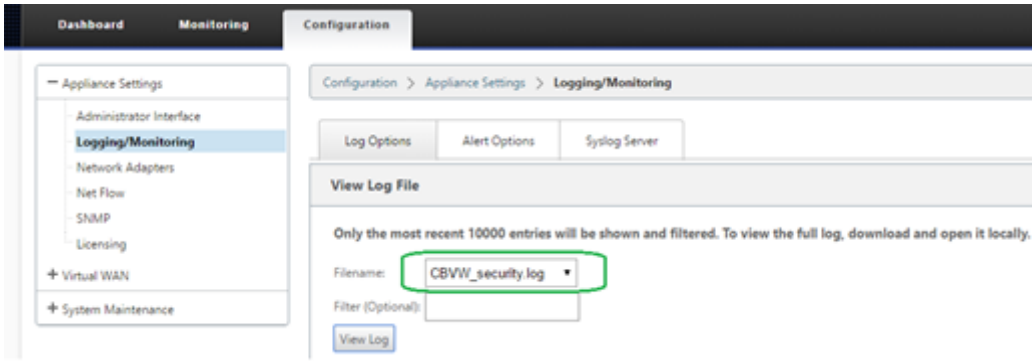


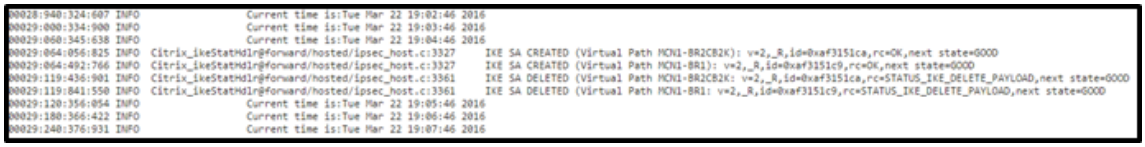
2. [モニター] > [**IKE/IPSec**] に移動します。設定された IPSec トンネル、SD-WAN ネットワーク内に設定された 2 つのエンドポイントまたはモード VPN エンドポイント間の IKE および IPSec サービスアソシエーションを確認します。

ipec ログを監視する方法

1. 「構成」>「アプライアンスの設定」>「ログ/監視」に移動します。ドロップダウンメニューから [ファイル名] を選択し、[ログの表示] をクリックします。IPsec トンネルの次のログ詳細を表示できます。

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

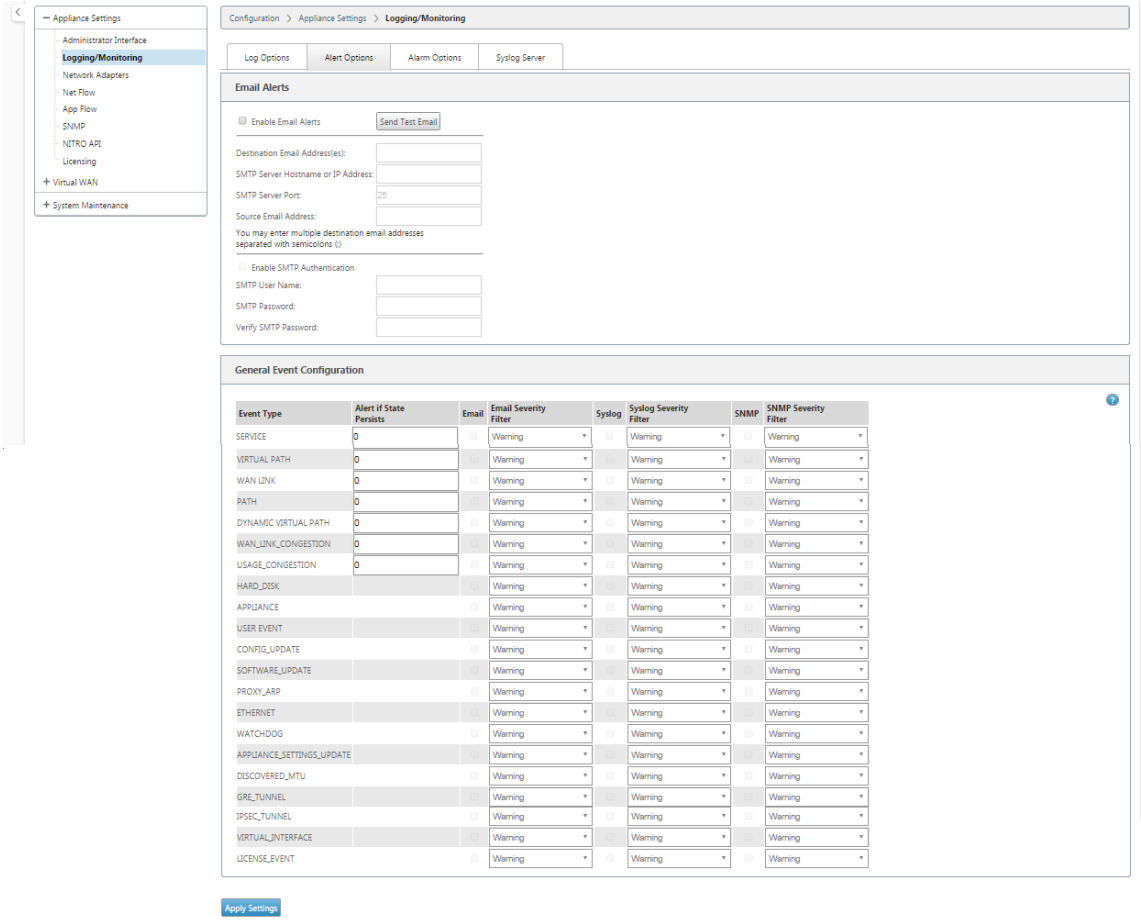




IPsec トンネルアラートを表示する方法

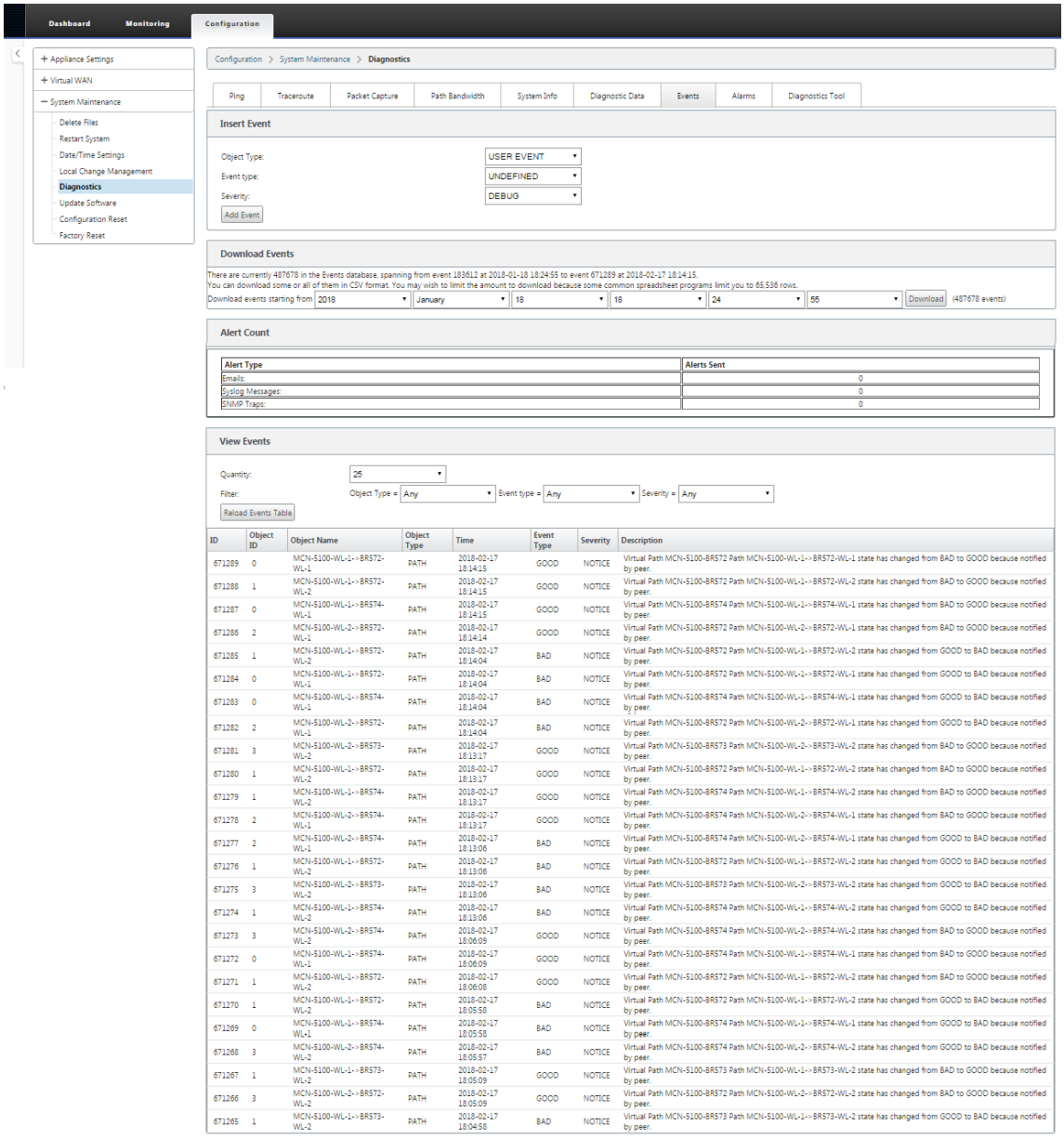
1. 「構成」>「アプライアンスの設定」**>**「ログ/監視」>「アラート・オプション」に移動します。
2. IPsec トンネルの状態レポート用の電子メールおよび Syslog アラートを作成します。

   - IPSEC_TUNNEL をイベントタイプの 1 つとしてサポートし、電子メールおよび Syslog 重大度フィルタを設定できます。



IPsec トンネルイベントの監視方法

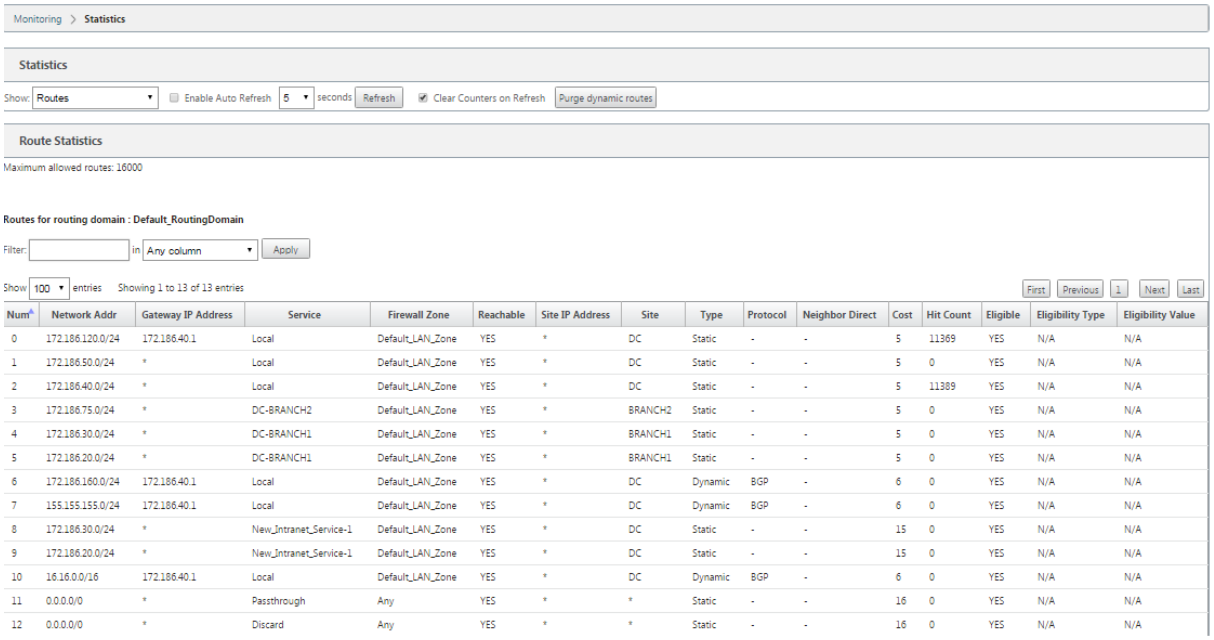
1. [構成**] > [**システムメンテナンス**] >** [診断] > [イベント] に移動します。
2. **IPSEC_TUNNEL** オブジェクトタイプ に基づいてイベントを追加します。すべての IPSec 関連イベントのフィルタを作成します。



IPsec 非仮想パスルートの適格性

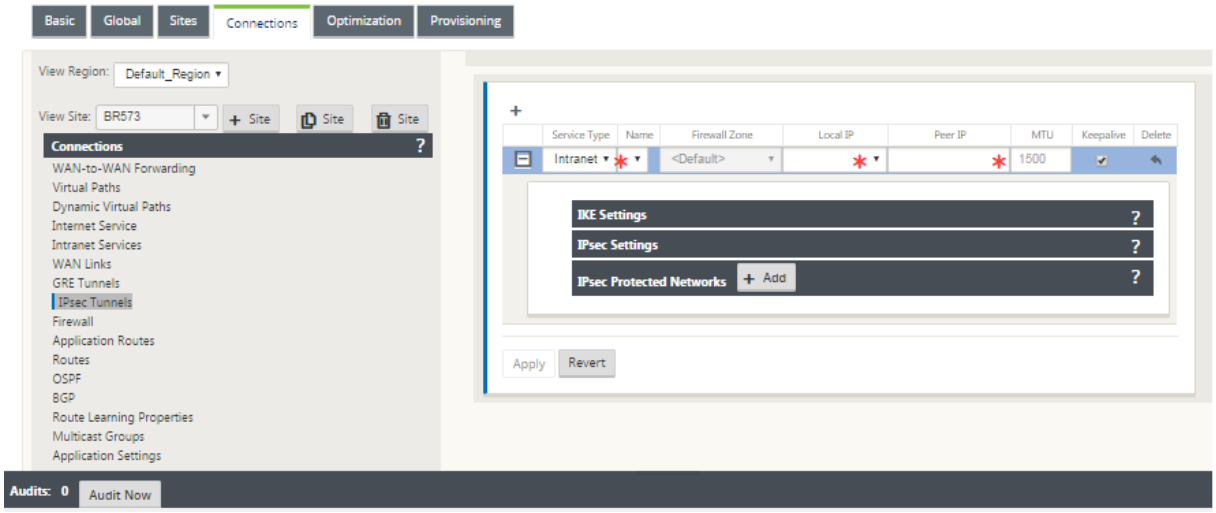
May 10, 2021

以前のリリースでは、トンネルが使用できなくなった場合でも、IPsec トンネルルートはルートテーブルに残っていました。



Num	Network Addr	Gateway IP Address	Service	Firewall Zone	Reachable	Site IP Address	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
0	172.186.120.0/24	172.186.40.1	Local	Default_LAN_Zone	YES	*	DC	Static	-	-	5	11369	YES	N/A	N/A
1	172.186.50.0/24	*	Local	Default_LAN_Zone	YES	*	DC	Static	-	-	5	0	YES	N/A	N/A
2	172.186.40.0/24	*	Local	Default_LAN_Zone	YES	*	DC	Static	-	-	5	11389	YES	N/A	N/A
3	172.186.75.0/24	*	DC-BRANCH2	Default_LAN_Zone	YES	*	BRANCH2	Static	-	-	5	0	YES	N/A	N/A
4	172.186.30.0/24	*	DC-BRANCH1	Default_LAN_Zone	YES	*	BRANCH1	Static	-	-	5	0	YES	N/A	N/A
5	172.186.20.0/24	*	DC-BRANCH1	Default_LAN_Zone	YES	*	BRANCH1	Static	-	-	5	0	YES	N/A	N/A
6	172.186.160.0/24	172.186.40.1	Local	Default_LAN_Zone	YES	*	DC	Dynamic	BGP	-	6	0	YES	N/A	N/A
7	155.155.155.0/24	172.186.40.1	Local	Default_LAN_Zone	YES	*	DC	Dynamic	BGP	-	6	0	YES	N/A	N/A
8	172.186.30.0/24	*	New_Intranet_Service-1	Default_LAN_Zone	YES	*	DC	Static	-	-	15	0	YES	N/A	N/A
9	172.186.20.0/24	*	New_Intranet_Service-1	Default_LAN_Zone	YES	*	DC	Static	-	-	15	0	YES	N/A	N/A
10	16.16.0.0/16	172.186.40.1	Local	Default_LAN_Zone	YES	*	DC	Dynamic	BGP	-	6	0	YES	N/A	N/A
11	0.0.0.0/0	*	Passthrough	Any	YES	*	*	Static	-	-	16	0	YES	N/A	N/A
12	0.0.0.0/0	*	Discard	Any	YES	*	*	Static	-	-	16	0	YES	N/A	N/A

[接続] [サイト名] > [**IPsec** トンネル] の **[**キープアライブ**]** オプションを使用すると、この動作が強化され、**IPsec** トンネル が使用できなくなったときに IPsec 非仮想パスルートが不適格と見なされるようになりました。キープアライブオプションが有効の場合、SA は自動的に作成されます。トラフィックはトンネル経由で送信されません。

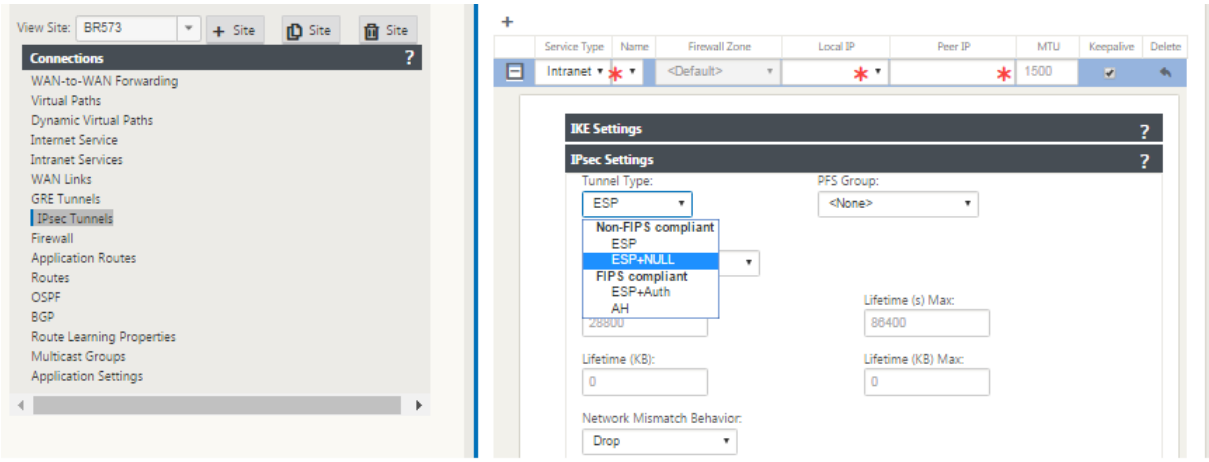


IPsec ヌル暗号化

May 10, 2021

以前のリリースでは、トンネルタイプ ESP+NULL が導入されました。IPsec ESP プロトコルを使用する場合、トラフィックは通常、暗号化および認証されます。ただし、Null 暗号化を使用すると、暗号化を使用しないように選択できます。ESP + NULL トンネルタイプでは、パケットは認証されますが、暗号化されません。

IPsec トンネルは、設定エディタの [IP **sec** 設定] セクションの ESP+NULL トンネルタイプで設定できます。



FIPS 準拠

May 10, 2021

Citrix SD-WAN では、FIPS モードでは、ユーザーは IPSec トンネルおよび仮想パスの IPSec 設定に FIPS 準拠の設定を構成する必要があります。

- FIPS 準拠の IKE モードを表示します。
- FIPS 準拠の IKE DH グループを表示します。このグループから、アプライアンスを FIPS 準拠モード（2,5,14～21）に設定するために必要なパラメータを選択できます。
- 仮想パスの IPSec 設定で FIPS 準拠の IPSec トンネルの種類を表示します
- IKE ハッシュおよび（IKEv2）整合性モード、IPsec 認証モード。
- FIPS ベースのライフタイム設定に対する監査エラーの実行

Citrix SD-WAN GUI を使用して FIPS コンプライアンスを有効にするには、次の手順に従います。

1. [構成] > [仮想 **WAN**] > [構成エディタ] > [グローバル] の順に選択し、[**FIPS** モードを有効にする] を選択します。

FIPS モードを有効にすると、設定中にチェックが実行され、IPSec 関連のすべての設定パラメータが FIPS 標準に準拠しているかどうかが確認されます。IPsec を構成するには、監査エラーと警告が表示されます。

仮想パス IPsec 設定を構成するには、次の手順を実行します。

- FIPS 準拠が必要なすべての仮想パスに対して、仮想パス IPSec トンネルを有効にします。仮想パスの IPsec 設定は、デフォルトセットによって制御されます。

- IPsec モードを AH または ESP+ 認証に変更してメッセージ認証を構成し、FIPS 承認ハッシュ機能を使用します。SHA1 は FIPS によって受け入れられますが、SHA256 を強く推奨します。
- IPsec ライフタイムは、8 時間（28,800 秒）以下に設定する必要があります。

仮想 WAN は、事前共有キーを持つ IKE バージョン 2 を使用して、次の設定を使用して、仮想パスを経由する IPSec トンネルをネゴシエートします。

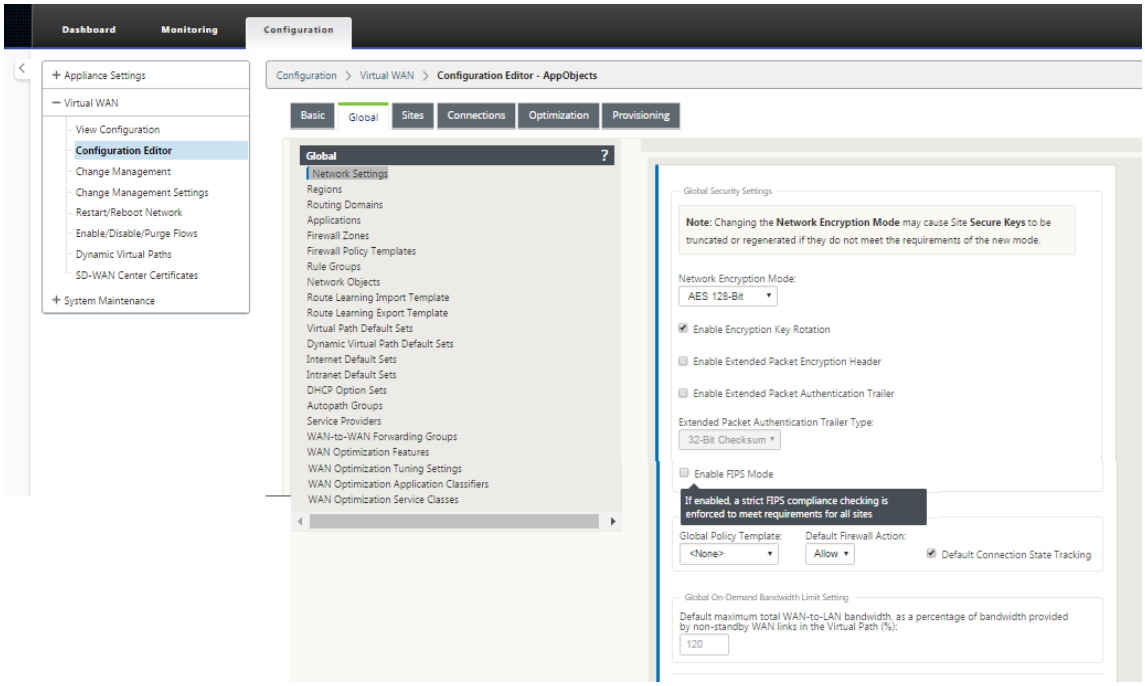
- DH グループ 19: キーネゴシエーションのための ECP256 (256 ビット楕円曲線)
- 256 ビット AES-CBC 暗号化
- メッセージ認証のための SHA256 ハッシュ
- メッセージの整合性のための SHA256 ハッシュ
- DH Group 2: MODP-1024 Perfect Forward Secrecy

サードパーティの IPSec トンネルを構成するには、次の設定を使用します。

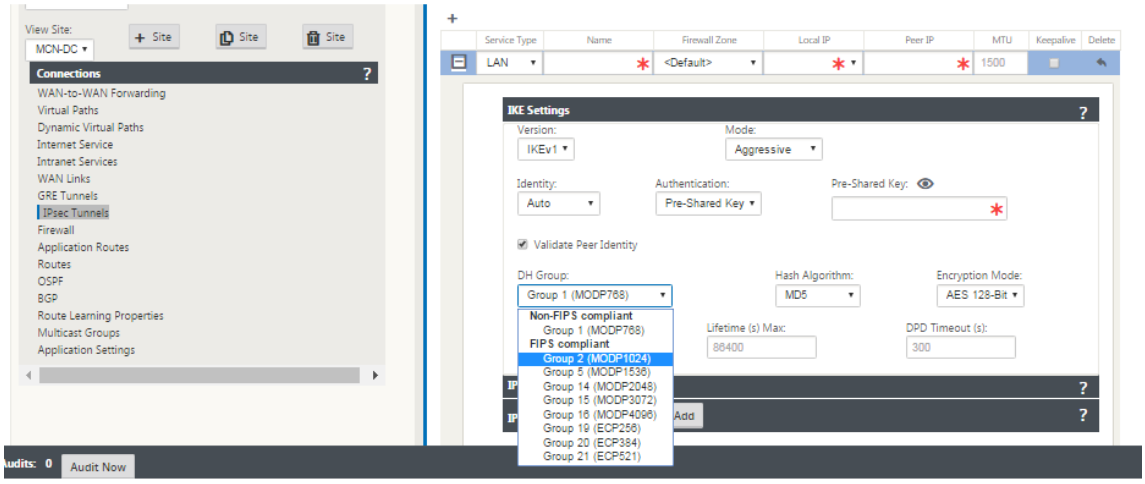
1. FIPS 承認済みの DH グループを構成します。グループ 2 と 5 は FIPS では許可されますが、グループ 14 以上を強く推奨します。
2. FIPS 承認ハッシュ関数を設定します。SHA1 は FIPS によって受け入れられますが、SHA256 を強くお勧めします。
3. IKEv2 を使用する場合は、FIPS 承認の整合性機能を設定します。SHA1 は FIPS によって受け入れられますが、SHA256 を強くお勧めします。
4. IKE ライフタイムおよび最大ライフタイムを 24 時間（86,400 秒）以下に設定します。
5. IPSec モードを AH または ESP+ 認証に変更して IPSec メッセージ認証を構成し、FIPS 承認ハッシュ機能を使用します。SHA1 は FIPS によって受け入れられますが、SHA256 を強く推奨します。
6. IPSec ライフタイムおよび最大ライフタイムを 8 時間（28,800 秒）以下に設定します。

IPSec トンネルを設定するには、次の手順を実行します。

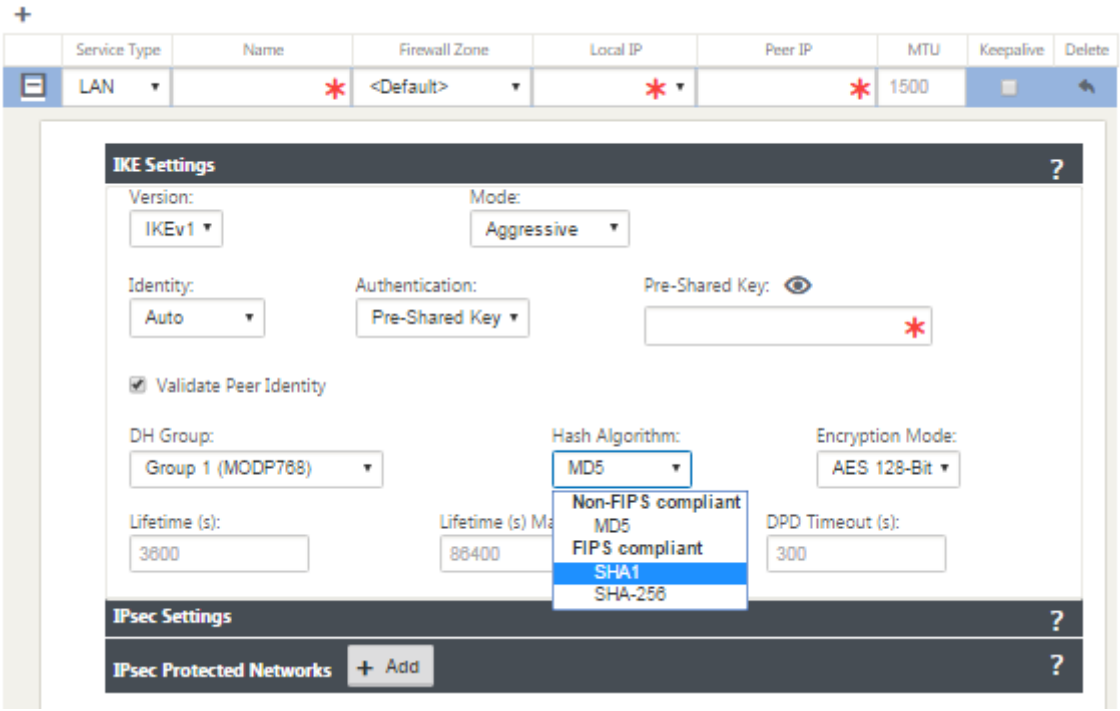
1. MCN アプライアンスで、[構成] > [仮想 **WAN**] > [構成エディタ] の順に選択します。既存の構成パッケージを開きます。「接続」>「**IPsec** トンネル」の順に選択します。



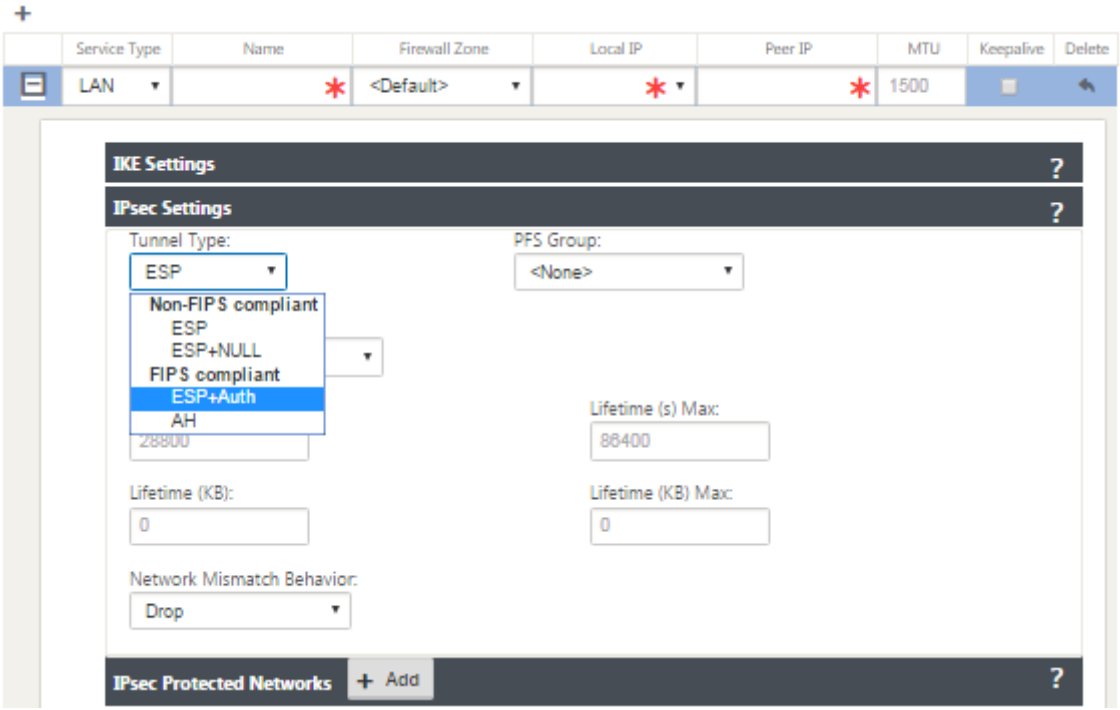
2. 「接続」>「**IPsec** トンネル」の順に選択します。[**LAN**] または [イントラネットトンネル] を選択すると、画面で IKE 設定の FIPS 準拠のグループと非準拠のグループが区別されるため、FIPS 準拠を簡単に構成できます。



画面には、次の図に示すように、ハッシュアルゴリズムが FIPS に準拠しているかどうかも表示されます。



IPSec 設定の FIPS 準拠オプション



IPSec 構成が有効になっているときに FIPS 標準に準拠していない場合、監査エラーが発生する可能性があります。以下は、GUI に表示される監査エラーの種類です。

- の場合、FIPS モードが有効になり、非 FIPS 準拠オプションが選択されます。
- の場合、FIPS モードが有効になり、誤ったライフタイム値が入力されます。

- の場合、FIPS モードが有効になり、仮想パスのデフォルトセットの IPSec 設定も有効になり、不正なトンネルモードが選択されます (ESP 対 ESP_auth/AH)。
- FIPS モードを有効にすると、仮想パスのデフォルトセットの IPSec 設定も有効になり、誤ったライフタイム値が入力されます。

Citrix SD-WAN Secure Web Gateway

May 10, 2021

トラフィックを保護し、ポリシーを適用するために、企業は多くの場合、MPLS リンクを使用して、ブランチトラフィックを企業のデータセンターにバックホールします。データセンターは、セキュリティポリシーを適用し、セキュリティアプライアンスを介してトラフィックをフィルタリングしてマルウェアを検出し、トラフィックを ISP 経由でルーティングします。プライベート MPLS リンクを介したこのようなバックホールは高価です。また、レイテンシーが大きくなるため、ブランチサイトでのユーザーエクスペリエンスが低下します。また、ユーザーがセキュリティ制御をバイパスするリスクもあります。

バックホールに代わる方法として、支店にセキュリティアプライアンスを追加する方法があります。ただし、複数のアプライアンスをインストールして、サイト全体で一貫したポリシーを維持するにつれて、コストと複雑さが増大します。また、多くの支社がある場合、コスト管理は実用的ではありません。

Zscaler:

コスト、複雑さ、待ち時間を追加せずにセキュリティを強化する理想的なソリューションは、すべてのブランチインターネットトラフィックを Citrix SD-WAN アプライアンスから ZScaler Cloud セキュリティプラットフォームにルーティングすることです。その後、中央の Zscaler コンソールを使用して、ユーザーに詳細なセキュリティポリシーを作成できます。ポリシーは、ユーザーがデータセンターにいるかブランチサイトにいるかにかかわらず、一貫して適用されます。Zscaler セキュリティソリューションはクラウドベースであるため、ネットワークにセキュリティアプライアンスを追加する必要はありません。

FIPS コンプライアンス:

アメリカ国立標準技術研究所（NIST）は、自主基準が存在しない地域で連邦情報処理基準（FIPS）を開発しています。FIPS は、次の問題を解決します。

- 異なるシステム間の互換性。
- データとソフトウェアの移植性。
- コスト効率に優れたコンピュータセキュリティと機密情報のプライバシー

FIPS は、セキュリティシステムで使用される暗号化モジュールのセキュリティ要件を指定します。これらのセキュリティ標準を Citrix SD-WAN アプライアンスの処理に適用するには、FIPS モードを構成します。

フォースポイント:

Citrix SD-WAN を使用すると、ファイアウォールリダイレクト（宛先 NAT による透過プロキシ）機能を使用して、エンタープライズエッジにある SD-WAN アプライアンスから、Forcepoint クラウドホスト型セキュリティモジュールにインターネット（HTTP および HTTPS）トラフィックをリダイレクトできます。HTTP トラフィックをポート 80 からポート 8081 に、HTTPS トラフィックをポート 443 から最も近い Forcepoint クラウドプロキシサーバーのポート 8443 にリダイレクトできます。

GRE トンネルと IPsec トンネルを使用した Zscaler 統合

November 8, 2021

Zscaler Cloud Security Platform は、世界中の 100 以上のデータセンターで一連のセキュリティチェックの投稿として機能します。インターネットトラフィックを Zscaler にリダイレクトするだけで、店舗、支店、遠隔地をすぐに保護できます。Zscaler はユーザーとインターネットを接続し、暗号化または圧縮されている場合でも、トラフィックのすべてのバイトを検査します。

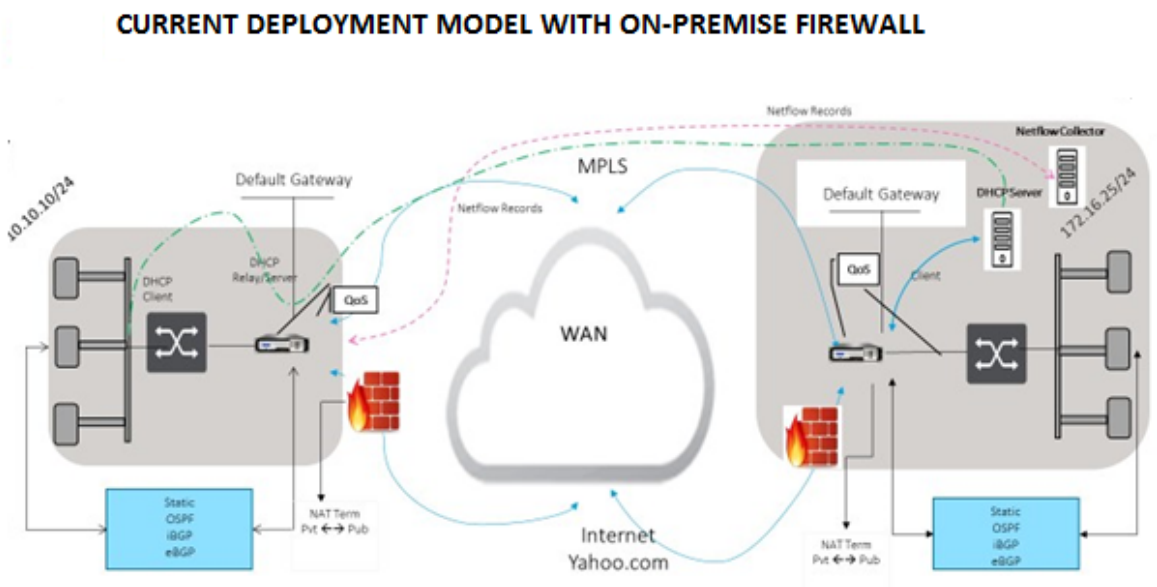
Citrix SD-WAN アプライアンスは、お客様のサイトの GRE トンネルを介して ZScaler クラウドネットワークに接続できます。SD-WAN アプライアンスを使用した Zscaler の展開では、次の機能がサポートされています。

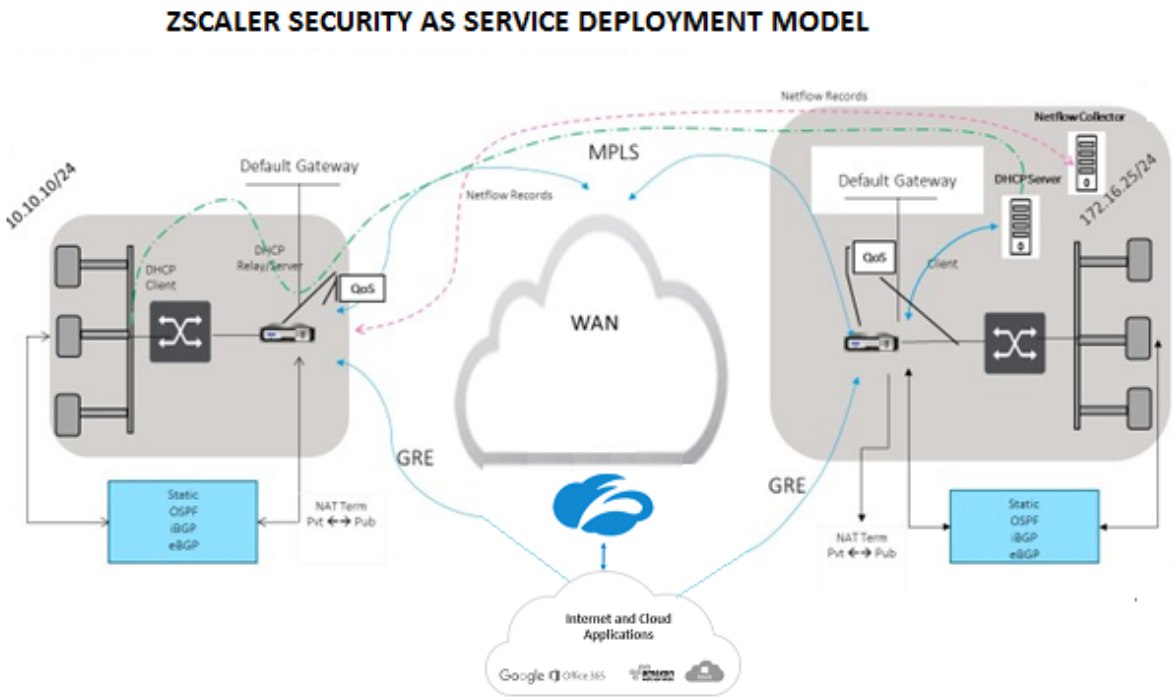
- すべての GRE トラフィックを Zscaler に転送することで、直接インターネットブレイクアウトが可能になります。
- 顧客サイトごとに Zscaler を使用した直接インターネットアクセス（DIA）。
  - 一部のサイトでは、DIA にオンプレミスのセキュリティ機器を提供し、Zscaler を使用しない場合があります。
  - 一部のサイトでは、インターネットアクセス用に別の顧客サイトへのトラフィックのバックホールを選択する場合があります。
- 仮想ルーティングと転送の展開。
- インターネットサービスの一部としての 1 つの WAN リンク。

Zscaler はクラウドサービスです。サービスとして設定し、基になる WAN リンクを定義する必要があります。

- データセンターでインターネットサービスを設定し、GRE 経由でブランチします。
- 信頼できるパブリックインターネットリンクを、データセンターおよびブランチサイトで構成します。

トポロジ





GRE トンネルまたは IPsec トンネルトラフィック転送を使用するには、次の手順を実行します。

1. Zscaler ヘルプポータルにログインします https://help.zscaler.com/submit-ticket。
2. チケットを発行し、GRE トンネルまたは IPsec トンネルの送信元 IP アドレスとして使用する静的パブリック IP アドレスを指定します。

Zscaler は、送信元 IP アドレスを使用してカスタマーの IP アドレスを識別します。送信元 IP はスタティックパブ

リック IP である必要があります。ZScaler は、トラフィックを送信する 2 つの ZEN IP アドレス（プライマリとセカンダリ）で応答します。GRE キープアライブメッセージを使用して、トンネルの健全性を判断できます。

Zscaler は、送信元 IP アドレス値を使用してカスタマーの IP アドレスを識別します。この値は、静的なパブリック IP アドレスである必要があります。Zscaler は、トラフィックのリダイレクト先となる 2 つの ZEN IP アドレス [DR1] で応答します。GRE キープアライブメッセージを使用して、トンネルの健全性を判断できます。

サンプル **IP** アドレス

プライマリ

内部ルータの IP アドレス:172.17.6.241/30
内部 ZEN IP アドレス:172.17.6.242/30

セカンダリ

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

インターネットサービスの設定

インターネットサービスを構成するには、次の操作を行います。

1. [接続]-[インターネットサービス] に移動します。インターネットサービスを構成します。
2. [**+** サービス] を選択し、必要に応じて設定 (基本設定、WAN リンク、およびルール) を有効にします。
3. ［適用］を選択します。

サイトのインターネットサービスを有効にする方法の詳細については、「統合ファイアウォールを使用したブランチでの直接インターネットブレイクアウト」を参照してください。

インターネットサービスでは、次の設定を構成できます。

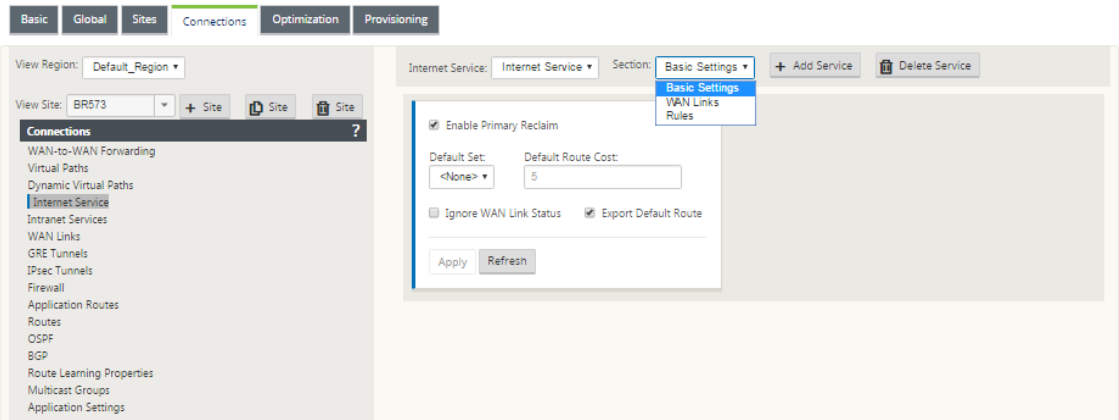
- 基本設定
- WAN リンク
- 規則

基本設定

ファイアウォールゾーンの設定は、インターネットサービスには構成できません。インターネットサービスが信頼されている場合は、**Internet_Zone** に割り当てられます。インターネットサービスが信頼されていない場合は、**Untrusted_Internet_Zone** に割り当てられます。

構成可能な基本設定は次のとおりです。

- プライマリ再利用を有効にする：有効にすると、WAN リンク上のこのサービスに関連付けられている（使用 = プライマリ）使用状況は、その WAN リンク上のアクティブサービスとして強制的にステータスを再利用します。
- デフォルトセット: サイトのインターネットサービスのルールを設定するインターネットのデフォルトセットの名前。
- デフォルトルートコスト: デフォルト（0.0.0.0/0）インターネットルートに関連付けられたルートコスト。
- **WAN** リンクステータスを無視：有効にすると、このサービス宛てのパケットは、このサービスのすべての WAN リンクが利用できない場合でも、このサービスを選択します。
- デフォルトルートのエクスポート: 有効にすると、WAN-to-WAN 転送が有効になっている場合、インターネットサービスのデフォルトルート 0.0.0.0/0 が他のサイトにエクスポートされます。



WAN リンク

設定可能な WAN リンクの設定は次のとおりです。

- 使用: サービスにこの WAN リンクの使用を許可します。[使用] (Use) が無効になっていると、他のすべてのオプションは使用できなくなります。
- **Mode**：トラフィックの冗長性または負荷分散のためのサービスモード（プライマリ、セカンダリ、またはバランス）。
- トンネルヘッダーサイズ **(**バイト**)**: トンネルヘッダーのサイズ（バイト単位）（該当する場合）。
- アクセスインターフェイスフェールオーバー：有効にした場合、VLAN が一致しないインターネットまたはイントラネットパケットは引き続きサービスを使用できます。

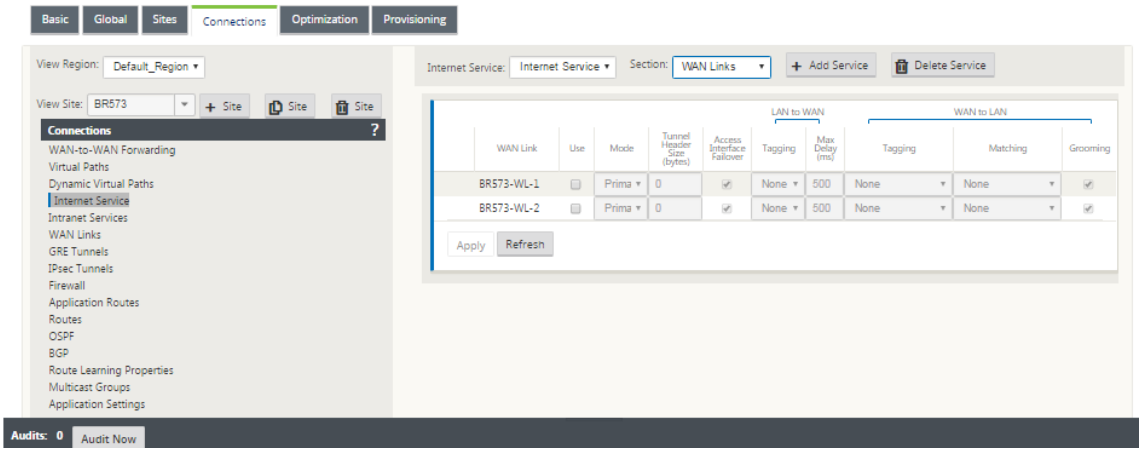
LAN から **WAN**

- タグ付け: サービス上の LAN から WAN へのパケットに適用する DSCP タグ。

- **Max Delay (ms)**: WAN リンクの帯域幅を超えたときにパケットをバッファリングする最大時間（ミリ秒単位）。

WAN から **LAN** へ

- タグ付け: サービス上の WAN から LAN へのパケットに適用する DSCP タグ。
- 一致: このタグに一致するインターネット WAN から LAN へのパケットがサービスに割り当てられます。
- グルーミング: 有効にすると、WAN から LAN へのトラフィックがサービスのプロビジョニングされた帯域幅を超えないように、パケットはランダムにドロップされます。



規則

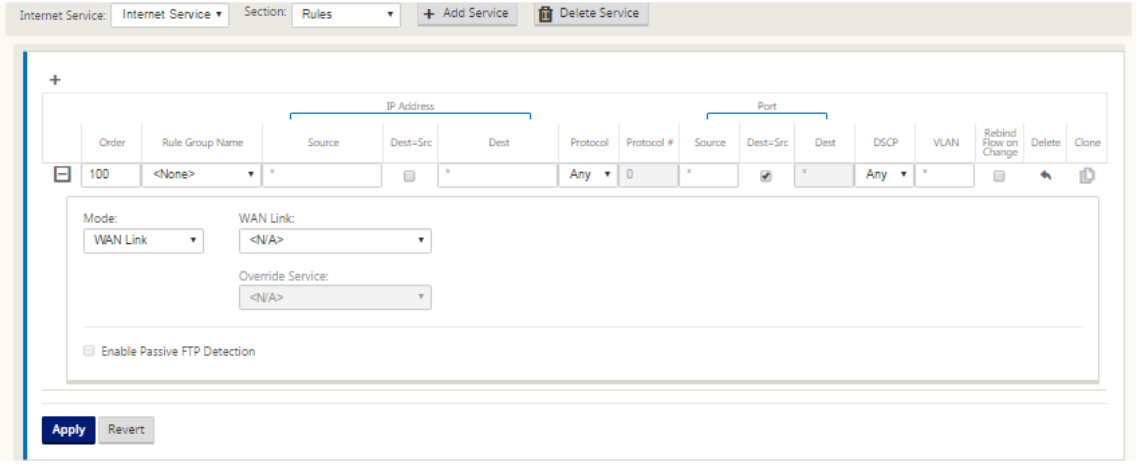
インターネットトラフィックは、定義されたルールに基づいて識別されます。ルール定義は、特定のトラフィックフローを照合するために使用されます。一致したら、トラフィックフローに適用するアクションを定義する必要があります。

使用可能なルールのリストは次のとおりです。

- 順序: ルールが適用され、自動的に再配布される順序。
- ルールグループ名: ルール統計の表示時にグループ単位で集計できるようにするルールに付けられる名前。同じルールグループ名を持つルールのすべての統計情報をまとめて表示できます。
- 送信元: ルールと一致する送信元 IP アドレスとサブネットマスク。
- **Dest-Src**: 有効にすると、送信元 IP アドレスが宛先 IP アドレスとしても使用されます。
- **Dest**: ルールと一致する宛先 IP アドレスとサブネットマスク。
- プロトコル: フィルタと一致するプロトコル名。
- **Protocol #**: フィルタと一致するプロトコル番号。
- **DSCP**: ルールと一致する IP ヘッダー内の DSCP タグ。

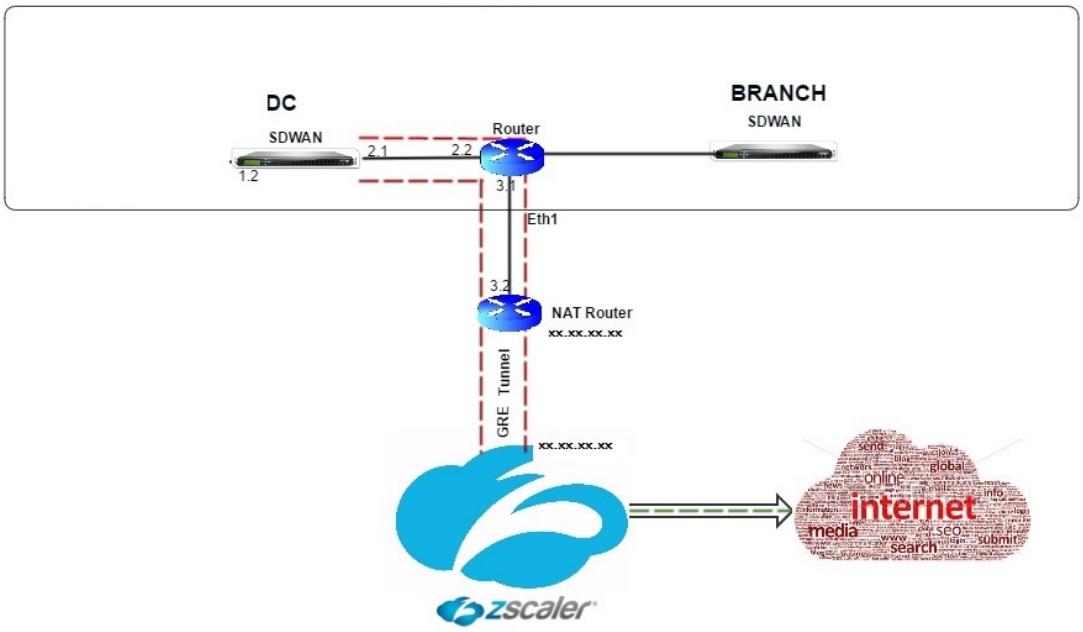
使用可能なアクションのリストを以下に示します。

- **WAN** リンク: インターネット負荷分散が有効な場合に、ルールに一致するフローによって使用される WAN リンク。
- **Override Service**: ルールに一致するフローの宛先サービス。
  - **Discard**: トラフィックをドロップします。
  - パススルー: フローをパススルーにマッピングし、トラフィックが変更されずにアプライアンスを通過できるようにします。



GRE トンネルの設定

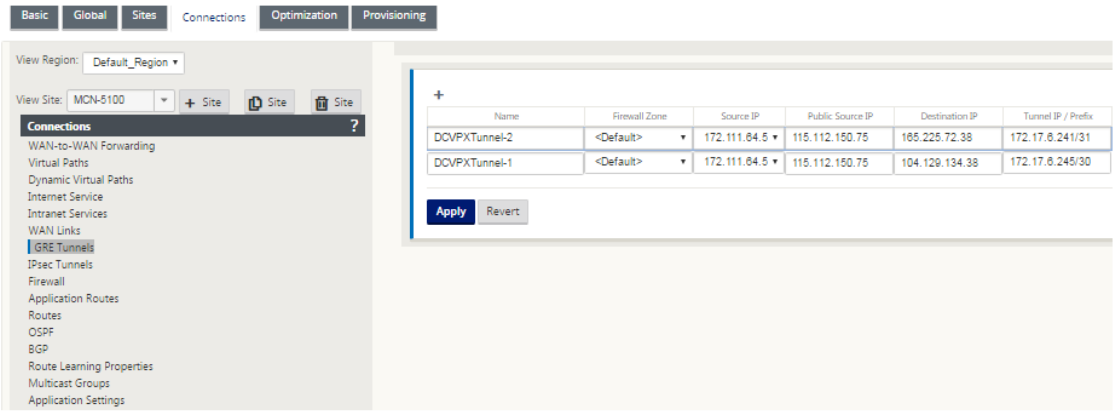
1. 送信元 IP アドレスは、トンネルの送信元 IP アドレスです。トンネル送信元 IP アドレスが NATted の場合、別の中間デバイスで NATted されている場合でも、パブリック送信元 IP アドレスはパブリックトンネル送信元 IP アドレスになります。
2. 宛先 IP アドレスは、ZScaler が提供する ZEN IP アドレスです。
3. 元のペイロードがカプセル化されている場合、送信元 IP アドレスと宛先 IP アドレスはルータ GRE ヘッダーです。
4. トンネル IP アドレスおよびプレフィックスは、GRE トンネル自体の IP アドレッシングです。これは、GRE トンネル経由でトラフィックをルーティングする場合に便利です。trafic は、この IP アドレスを Gateway アドレスとして必要とします。



GRE トンネルを設定するには、次の手順を実行します。

1. 構成エディタで、[接続] > [サイト] > [**GRE** トンネル] に移動し、インターネットプレフィックスサービスを Zscaler GRE トンネルに転送するルートを設定します。

   送信元 IP アドレスは、信頼できるリンクの仮想ネットワークインターフェイスからのみ選択できます。GRE トンネルの設定方法を参照してください。



GRE トンネルのルートの設定

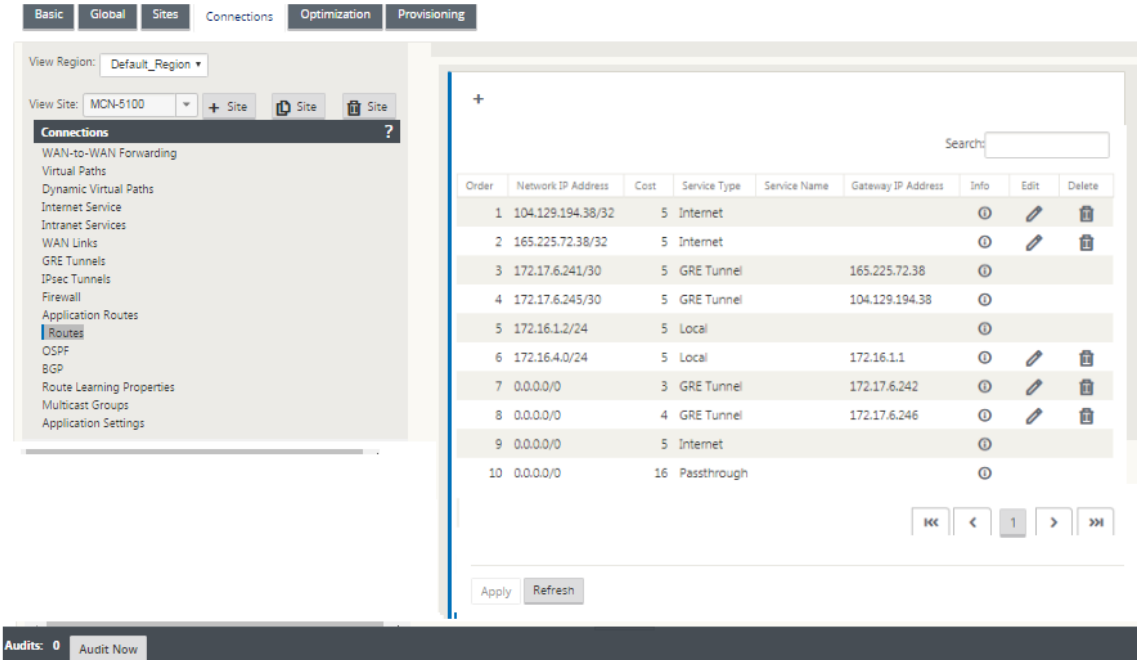
インターネットプレフィックスサービスを Zscaler GRE トンネルに転送するルートを設定します。

- ZEN IP アドレス（トンネルの宛先 IP、上の図の 104.129.194.38）は、サービスタイプインターネットに設定する必要があります。これは、Zscaler 宛てのトラフィックがインターネットサービスから計上されるようにするために必要です。

- Zscaler 宛てのすべてのトラフィックは、デフォルトルート 0/0 と一致し、GRE トンネルを介して送信する必要があります。[DR1] GRE トンネルに使用される 0/0 ルートが、パススルーまたは他のサービスタイプよりも低コストであることを確認します。
- 同様に、Zscaler へのバックアップ GRE トンネルのコストは、プライマリ GRE トンネルのコストよりも高い必要があります。
- ZEN IP アドレスの非再帰ルートが存在することを確認します。

GRE トンネルのルートを設定するには、次の手順を実行します。

1. [接続] > [サイト] > [ルート] に移動し、ルートの作成手順については、ルートの設定で説明されている手順に従います 。



注

Zscaler IP アドレスに特定のルートがない場合は、ZEN IP アドレスと一致するようにルートプレフィクス 0.0.0.0/0 を設定し、GRE トンネルのカプセル化ループを介してルーティングします。この設定では、アクティブバックアップモードでトンネルを使用します。上の図に示す値を使用すると、トラフィックは Gateway IP アドレス 172.17.6.242 のトンネルに自動的に切り替わります。必要に応じて、バックホール仮想パスルートを設定します。それ以外の場合は、バックアップトンネルのキープアライブ間隔をゼロに設定します。これにより、Zscaler へのトンネルが両方とも失敗しても、サイトへの安全なインターネットアクセスを可能にします。

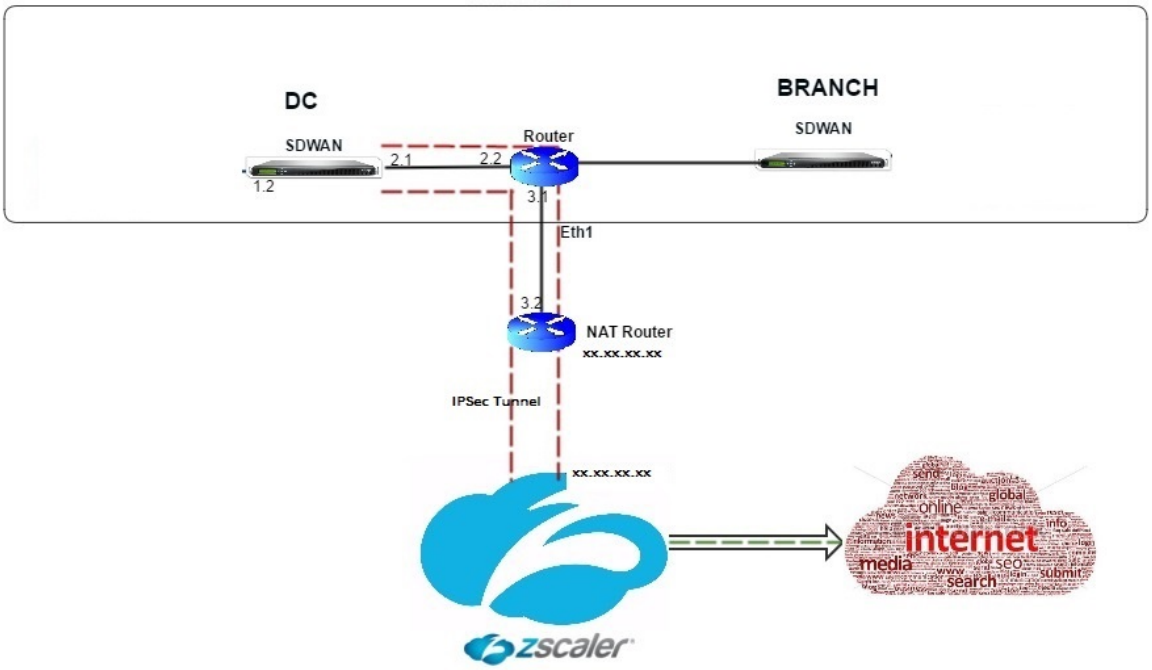
GRE キープアライブメッセージがサポートされています。**GRE** 送信元アドレスの **NAT** アドレスを提供するパブリックソース **IP** という新しいフィールドが、Citrix SD-WAN GUI インターフェイスに追加されます（SD-WAN アプライアンスのトンネルソースが中間デバイスによって NAT 接続されている場合）。Citrix SD-WAN GUI には、パブリックソース IP というフィールドが含まれています。このフィー

> ルドには、Citrix SD-WAN アプライアンスのトンネルソースが中間デバイスによって NAT 変換されたときに、GRE ソースアドレスの NAT アドレスを提供します。

制限事項

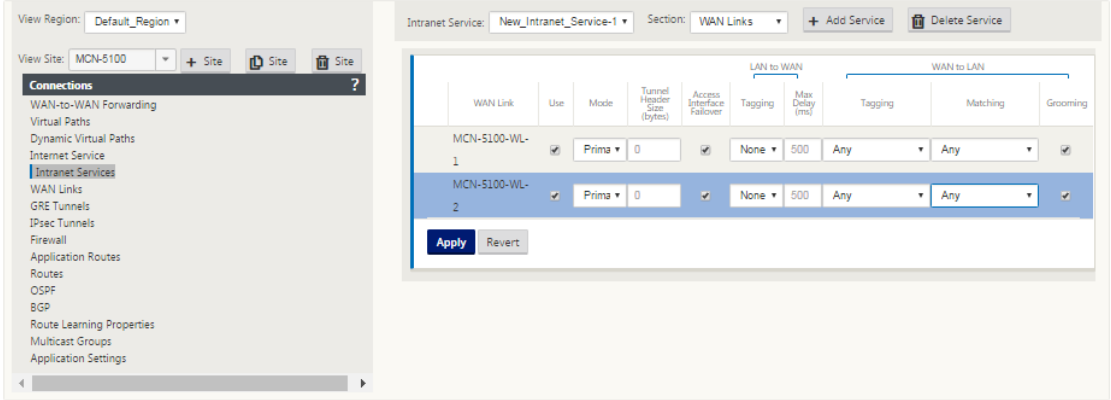
- 複数の VRF 配置はサポートされていません。
- プライマリバックアップ GRE トンネルは、高可用性設計モードでのみサポートされます。

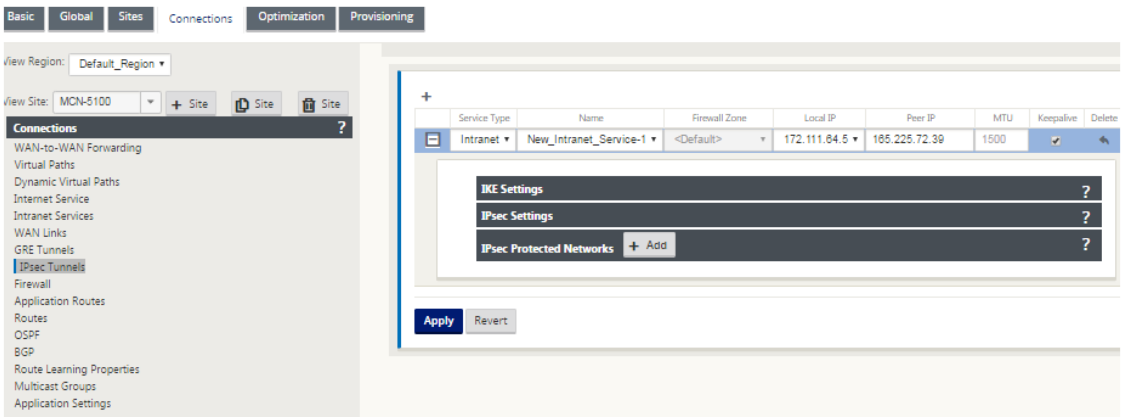
IPSec トンネルを構成する



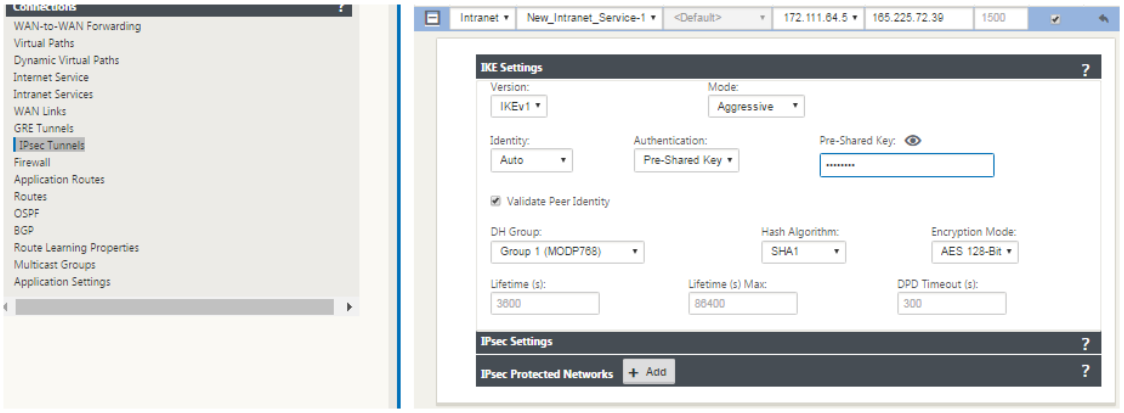
Citrix SD-WAN アプライアンス GUI でイントラネットまたは LAN サービス用の IPsec トンネルを構成するには、以下の手順に従ってください。

1. 設定エディタで、[接続] > [**SiteName**] > [**IPsec** トンネル] に移動し、サービスタイプ（LAN またはイントラネット）を選択します。
2. サービス・タイプ の「名前」を入力します。イントラネットサービスの種類では、構成されたイントラネットサーバーによって、使用できるローカル IP アドレスが決まります。
3. 使用可能なローカル IP アドレスを選択し、リモートピアへの仮想パスのピア IP アドレスを入力します。



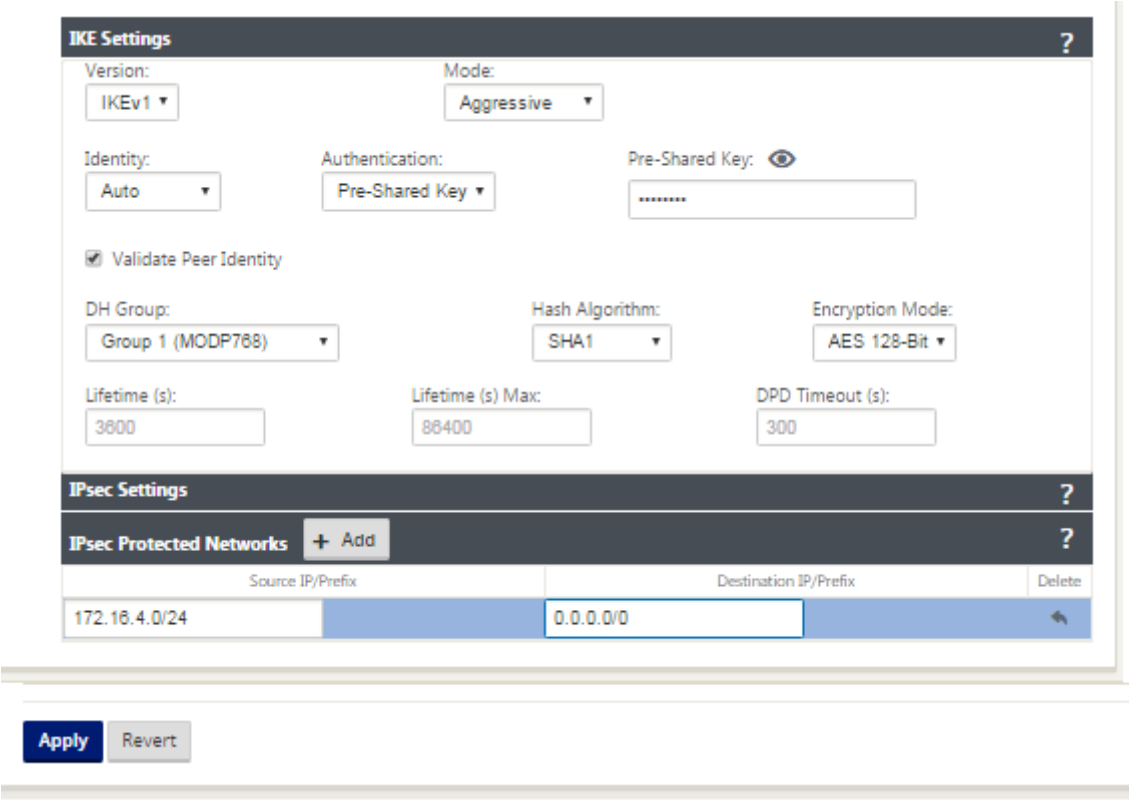


4. **IKE** 設定で **[**IKEv1****] を選択します。Zscaler は IKEv1 のみをサポートしています。



5. [IPsec 設定] で、[トンネルの種類] に [**ESP-NULL**] を選択し、IPsec トンネルを介してトラフィックを Zscaler にリダイレクトします。IPsec トンネルはトラフィックを暗号化しません。

6. インターネットトラフィックはリダイレクトされるため、宛先 IP/プレフィックスには任意の IP アドレスを使用できます。



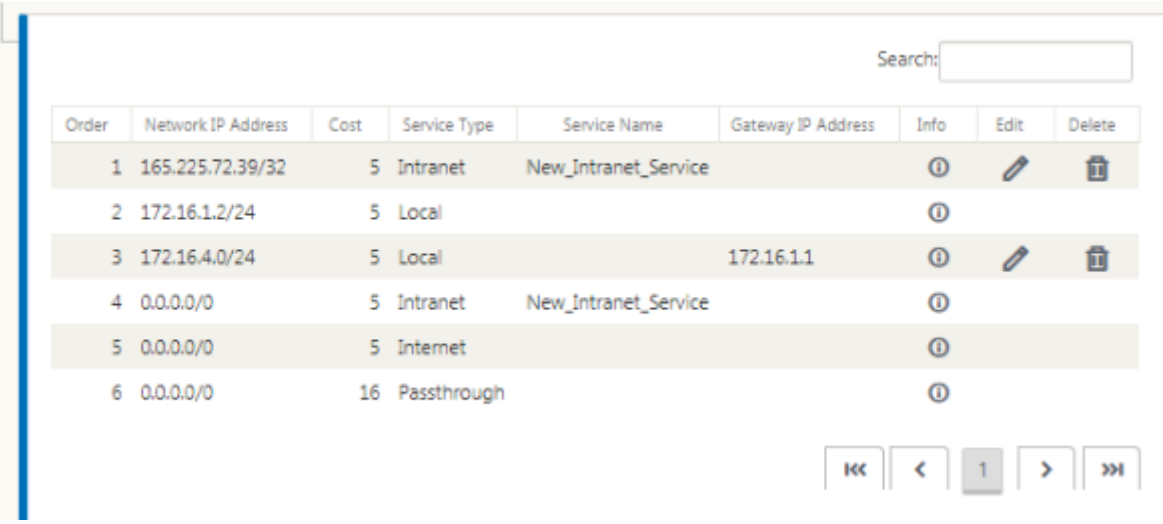
Citrix SD-WAN Web インターフェイスを使用した IPSec トンネルの構成の詳細については、「IPSec トンネル」ト

ピックを参照してください。

IPsec トンネルのルートの設定

IPSec ルートを設定するには、次の手順を実行します。

1. [接続] > [**DC**] > [ルート] に移動し、ルートの作成手順については、ルートの設定で説明されている手順に従います 。



GRE および IPsec トンネルの統計情報をモニタするには、

SD-WAN Web インターフェイスでは、モニタリング > **IPsec** トンネル]。
統計情報 > [**GRE** トンネルにナビゲートして下さい

詳細については、を参照してください。IPsec トンネルのモニタリングおよびGRE トンネルのトピック 。

Citrix SD-WAN での **Forcepoint** を使用したファイアウォールトラフィックリダイレクトのサポート

May 10, 2021

Forcepoint は次の機能をサポートしますが、SD-WAN はファイアウォールリダイレクト機能のみをサポートします。

- PKI を使用した IPSec
- PSK を使用した IPSec

- PAC ファイル設定を使用したプロキシチェーン
- 標準ヘッダーによるプロキシ連鎖
- 独自のヘッダーによるプロキシチェーンにより、クライアントの IP 範囲 (パートナーシップ/開発) を構成する必要がなくなります
- ファイアウォールリダイレクト（宛先 NAT による透過プロキシ）

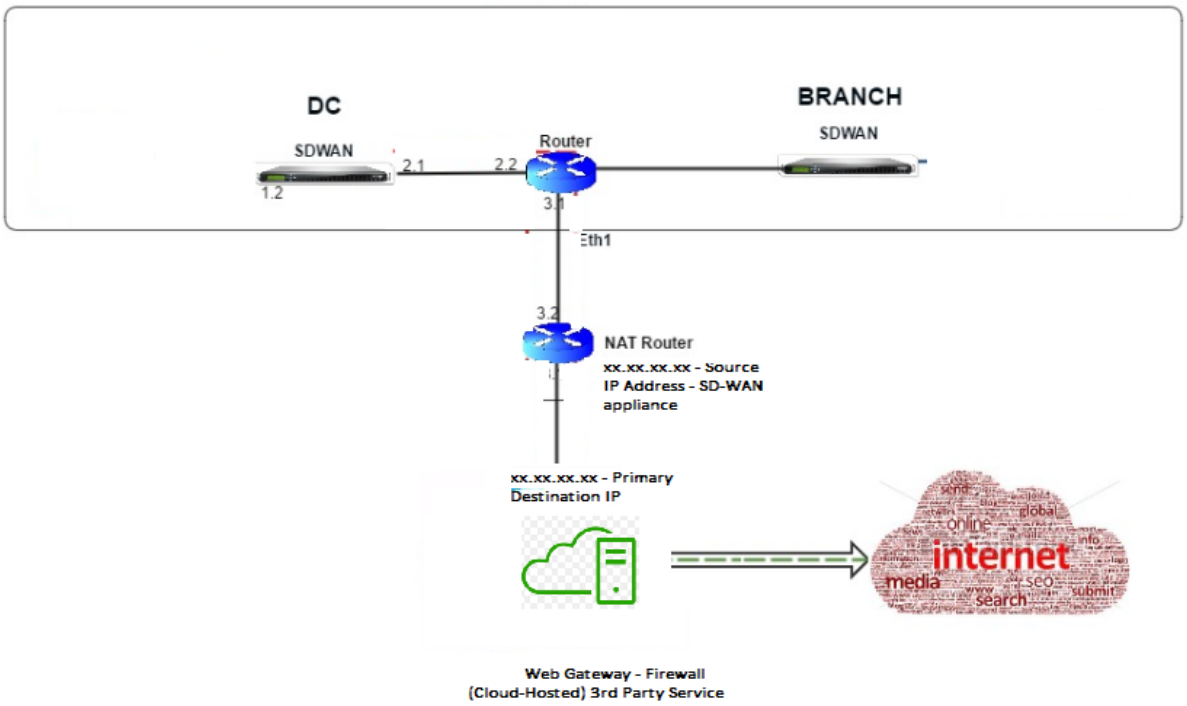
Destination NAT ポリシーを使用すると、企業は ForcePoint を使用してクラウドでホストされたセキュリティサービスを通じてインターネットトラフィックをルーティングできます。

SD-WAN アプライアンスで Destination NAT を構成し、安全なクラウドベースのファイアウォールサービスを通じてインターネットトラフィックをリダイレクトする方法を理解するには、次のユースケースを参照してください。

前提条件:

1. Forcepoint ポータルサイトにログインします。インターネットトラフィックを Forcepoint にリダイレクトする必要があるエンタープライズパブリック IP アドレスを指定して、ポリシーを作成します。インターネットトラフィックのリダイレクト先となるプライマリ IP アドレスとセカンダリ IP アドレスを取得します。
2. SD-WAN GUI で、DC サイトの SD-WAN アプライアンスで、WAN リンクに関連付けられたインターネットサービスを設定します。
3. 宛先 NAT は、インターネットトラフィックの宛先 IP アドレスを使用して実行されます。この宛先アドレスは、Forcepoint パブリック IP アドレスに変更されます。
4. 送信元 IP アドレスとプライマリ IP アドレスを指定して、宛先 NAT ポリシーを設定します。送信元 IP は、ポート 80 (http) および 443 (https) 内の SD-WAN アプライアンスのインターネット IP アドレスです。このアドレスは、外部ポート 8081 (http) および 8443 (https) で、クラウドベースのファイアウォール Gateway のプライマリ宛先 IP アドレスにリダイレクト/変換されます。
5. DNAT ポリシーを設定した後、DC で設定されたルートで、SD-WAN ネットワーク IP アドレスに対してインターネットサービスタイプが選択されていることを確認します。

Citrix SD-WAN での NAT サポートの詳細については、以下のトピック「NAT の設定」を参照してください



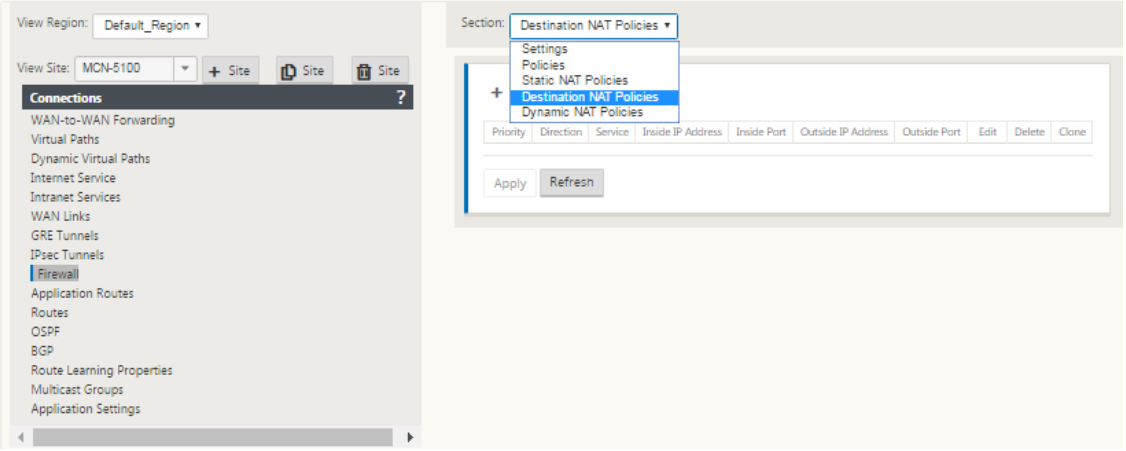
宛先 **NAT**（**DNAT**）の設定

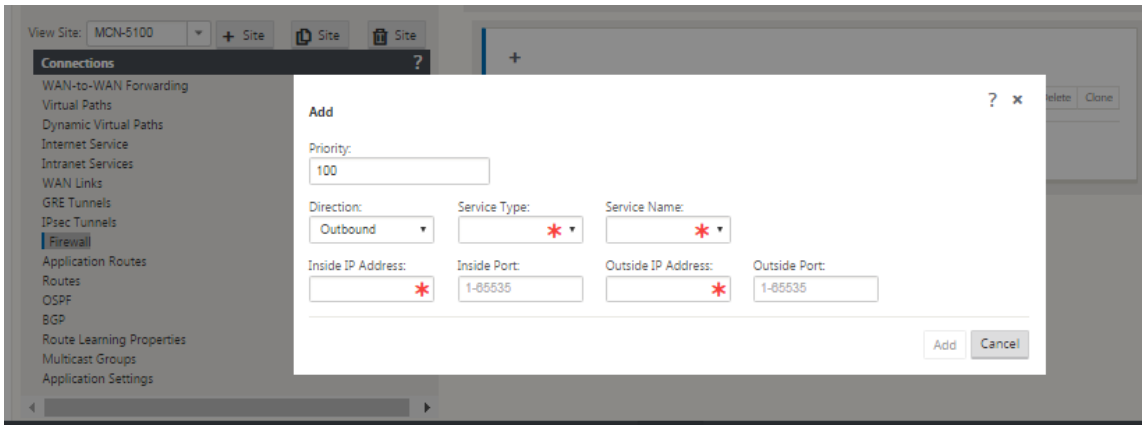
Citrix SD-WAN GUI を使用して、宛先 NAT（DNAT）を構成します。設定で、特定の宛先 IP アドレスおよびポートに一致するトラフィックをリダイレクトする、1 つ以上の DNAT ポリシーを追加します。

宛先 NAT を設定するには、次の手順を実行します。

SD-WAN SE/VPX GUI で、[構成] → [仮想 **WAN**] → [構成エディタ] に移動します。[開く] をクリックして、既存のパッケージを開きます。保存済みの構成パッケージを選択します。また、ネットワーク構成の構築中に DNAT ルールを作成することもできます。

1. DC (MCN) で、インターネットサービスを構成します。[接続]-> [ファイアウォール] に移動します。
2. [**+** 追加] をクリックして、DNAT ポリシーを追加します。
3. [宛先 **NAT** ポリシーの追加] ダイアログボックスで、次の情報を入力します。
    - 優先度
    - 方向
    - サービスの種類
    - サービス名
    - 内部 IP アドレス
    - インサイドポート
    - 外部 IP アドレス
    - 外部ポート





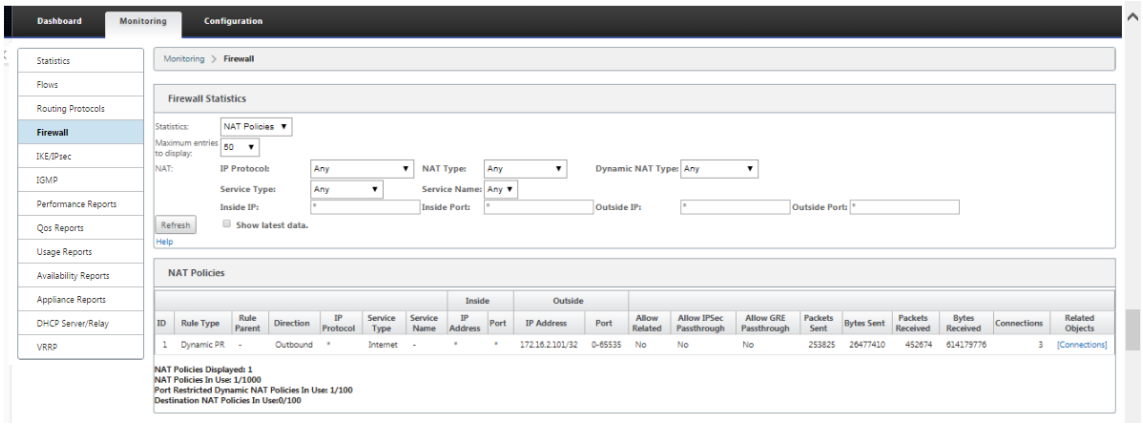
4. スタティック NAT と同様に、ファイアウォールトラフィックリダイレクト用の宛先 NAT ルールをプロビジョニングします。
5. 一致基準と、NAT する宛先 IP/ポートを入力します。
6. 統計情報を使用して、DNAT 規則の接続照合を実行します。
7. 構成の更新中に DNAT ルールを削除または更新します。

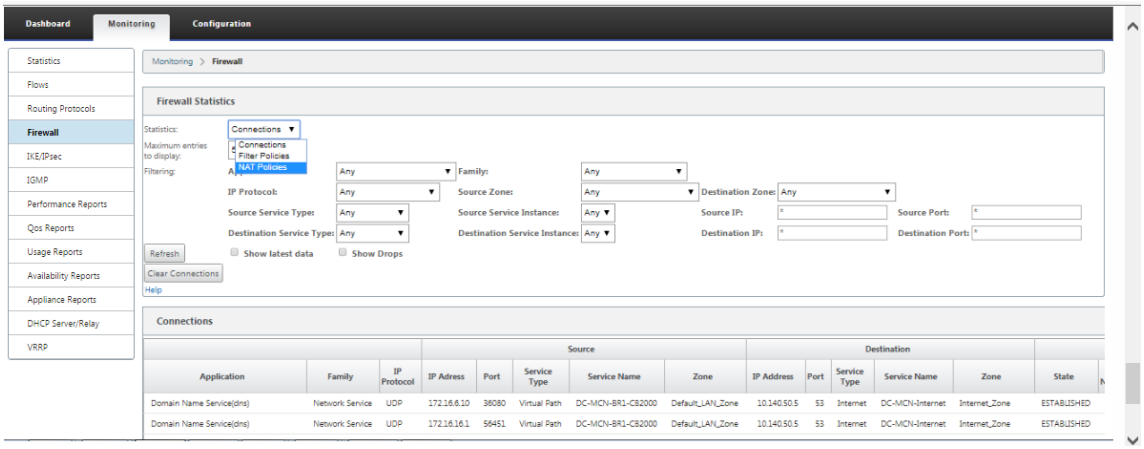
宛先 **NAT** ポリシー（ファイアウォール）のモニタリング

Citrix SD-WAN GUI を使用して、現在の DNAT ポリシー構成を監視することもできます。

現在の宛先 NAT ポリシー設定をモニタするには、次の手順を実行します。

1. Citrix SD-WAN GUI で、［監視］＞［ファイアウォール］＞［**NAT** ポリシー］に移動します。
2. 監視する統計情報を含むタブを選択します。





IPsec トンネルを使用した Palo Alto 統合

May 10, 2021

Palo Alto Networks は、リモートネットワークを保護するためのクラウドベースのセキュリティインフラストラクチャを提供します。組織が SD-WAN ファブリックを保護する地域的なクラウドベースのファイアウォールをセットアップできるようにすることで、セキュリティを提供します。

リモートネットワーク用の Prisma Access サービスを使用すると、リモートネットワークロケーションをオンボードし、ユーザーにセキュリティを提供できます。すべてのリモートロケーションでのデバイスの設定と管理の複雑さを取り除きます。

このサービスは、新しいリモートネットワークロケーションを簡単に追加し、これらのロケーションのユーザーが常に接続してセキュリティを確保することで、運用上の問題を最小限に抑えるための効率的な方法を提供します。

Prisma Access サービスでは、パノラマからポリシーを一元管理して、リモートネットワークの場所に対して一貫性と合理化されたセキュリティを確保することもできます。

リモートネットワークロケーションを Prisma Access サービスに接続するには、Palo Alto Networks 次世代ファ

イアウォール、またはサービスへの IPsec トンネルを確立できる
SD-WAN を含むサードパーティの IPSec 準拠デバイスを使用できます。

- リモートネットワーク用の Prisma アクセスサービスの計画
- リモートネットワーク用の Prisma Access サービスの構成
- 設定インポートを備えたオンボードリモートネットワーク

Citrix SD-WAN ソリューションは、ブランチからのインターネットトラフィックを分割する機能をすでに提供しています。これは、各ブランチで高価なセキュリティスタックの導入を回避しながら、信頼性が高く、低レイテンシのユーザーエクスペリエンスを提供するために重要です。Citrix SD-WAN と Palo Alto Networks は、分散企業に、ブランチ内のユーザーをクラウド内のアプリケーションに接続するためのより信頼性が高く安全な方法を提供します。

Citrix SD-WAN アプライアンスは、最小限の構成で SD-WAN アプライアンスの場所から IPsec トンネルを介して Palo Alto クラウドサービス（Prisma Access Service）ネットワークに接続できます。Palo Alto Networks は、Citrix SD-WAN センターで構成できます。

リモートネットワーク用の Prisma Access Service の設定を開始する前に、次の構成を準備しておき、サービスを正常に有効にし、リモートネットワークロケーションのユーザにポリシーを適用できることを確認します。

1. サービス接続—ユーザーの認証や重要なネットワーク資産へのアクセスを可能にするために、リモートネットワークのロケーションが企業本社のインフラストラクチャにアクセスする必要がある場合、本社とリモートネットワークのロケーションが接続されています。

リモートネットワークの場所が自律的で、他の場所にあるインフラストラクチャにアクセスする必要がない場合は、サービス接続を設定する必要はありません（モバイルユーザーがアクセスを必要とする場合を除く）。

1. テンプレート—プリズマアクセスサービスは、リモートネットワーク用のプリズマアクセスサービスのテンプレートスタック (Remote_Network_Template_Stack) と最上位テンプレート (Remote_Network_Template) を自動的に作成します。

   リモートネットワーク用の Prisma Access Service を構成するには、トップレベルのテンプレートを最初から構成するか、Palo Alto Networks ファイアウォールをオンプレミスで既に実行している場合は、既存の構成を活用します。

   テンプレートには、リモートネットワークの場所とリモートネットワーク用の Prisma Access サービス、セキュリティポリシーで参照できるゾーン、およびログ転送プロファイル間のプロトコルネゴシエーションのための IPsec トンネルとインターネットキーエクスチェンジ（IKE）構成を確立するための設定が必要です。リモートネットワークの Prisma Access サービスからログサービスにログを転送できること。

2. 親デバイスグループ—リモートネットワーク用の Prisma Access サービスでは、セキュリティポリシー、セキュリティプロファイル、およびその他のポリシーオブジェクト (アプリケーショングループ、オブジェクト、アドレスグループなど)、および認証ポリシーを含む親デバイスグループを指定する必要があります。リモートネットワーク用の Prisma Access サービスは、IPSec トンネルを介してリモートネットワークの Prisma Access サービスにルーティングされるトラフィックに対して、ポリシーを一貫して適用できます。

Panorama でポリシールールとオブジェクトを定義するか、既存のデバイスグループを使用して、リモートネットワークロケーションのユーザを保護する必要があります。

> 注:
>
> ゾーンを参照する既存のデバイスグループを使用する場合は、ゾーンを定義する対応するテンプレートを Remote_Network_Template_Stack に追加してください。

これにより、Prisma Access Service for Remote Networks を構成するときにゾーンマッピングを完了することができます。

3. **IP** サブネット—Prisma Access サービスがトラフィックをリモートネットワークにルーティングするには、Prisma Access サービスを使用してセキュリティ保護するサブネットワークのルーティング情報を指定する必要があります。リモートネットワークの場所で各サブネットワークへの静的ルートを定義するか、サービス接続場所と Prisma Access サービスの間に BGP を構成するか、両方の方法を組み合わせて使用できます。

   スタティックルートを設定し、BGP を有効にすると、スタティックルートが優先されます。リモートネットワークロケーションにサブネットワークが少数しかない場合は、スタティックルートを使用すると便利ですが、サブネットが重複する多数のリモートネットワークがある大規模な展開では、BGP を使用すると簡単に拡張できます。

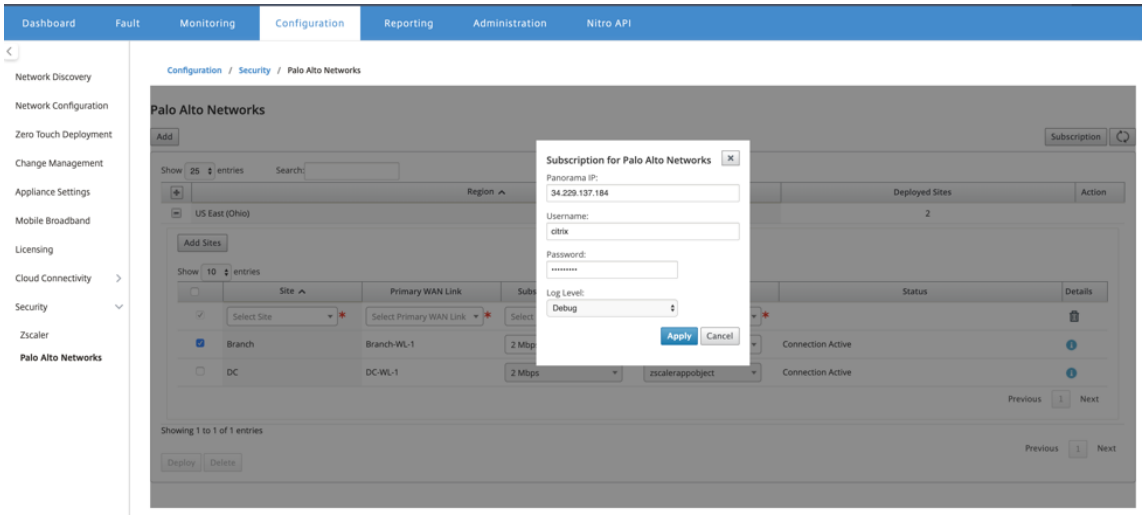
SD-WAN Center の Palo Alto Networks

以下の前提条件が満たされていることを確認してください。

- PRISMA ACCess サービスからパノラマ IP アドレスを取得します。
- PRISMA ACCESS サービスでユーザー名とパスワードを取得します。
- SD-WAN アプライアンス GUI で IPsec トンネルを構成します。
- サイトが、Citrix-IKE-暗号化デフォルト/Citrix-IPsec 暗号化デフォルト以外の IKE/IPsec プロファイルで構成された別のサイトがあるリージョンにオンボードされていないことを確認します。
- SD-WAN センターによって設定を更新するときに、Prisma Access の設定が手動で変更されていないことを確認します。

Citrix SD-WAN Center の GUI で、Palo Alto のサブスクリプション情報を入力します。

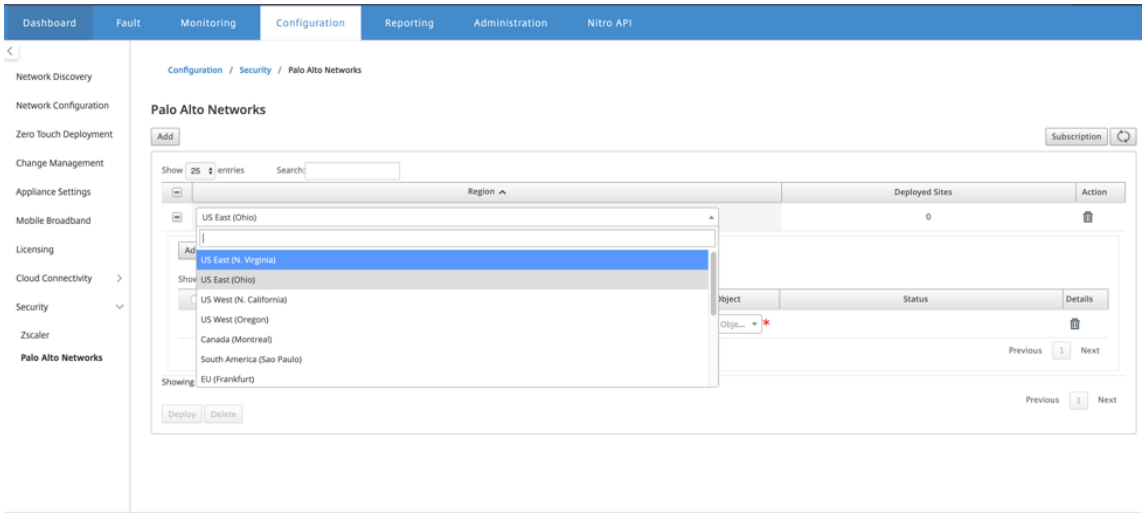
- パノラマ IP アドレスを設定します。この IP アドレスは Palo Alto（PRISMA ACCESS サービス）から取得できます。
- PRISMA ACCESS サービスで使用するユーザー名とパスワードを設定します。

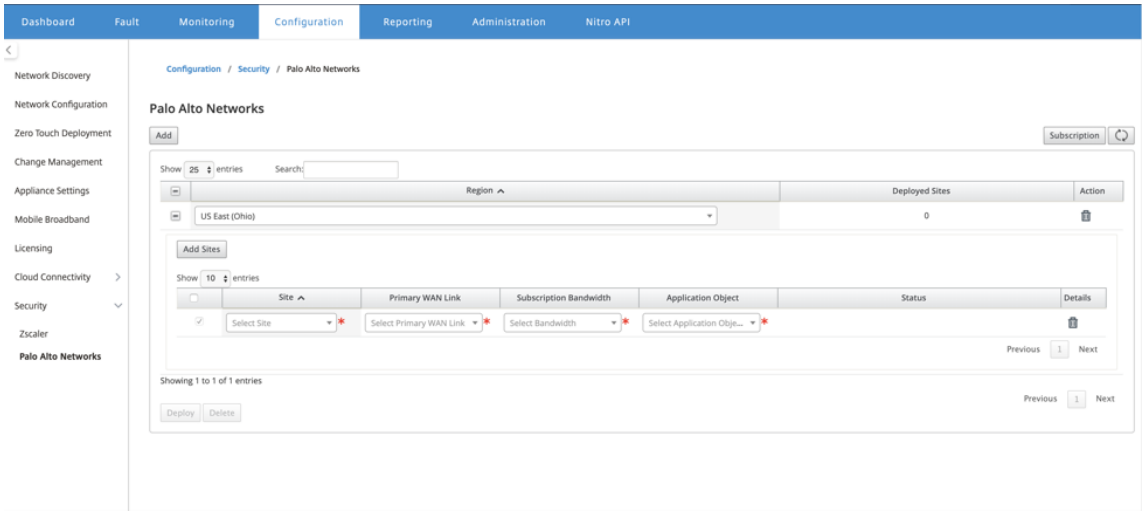


サイトを追加して展開する

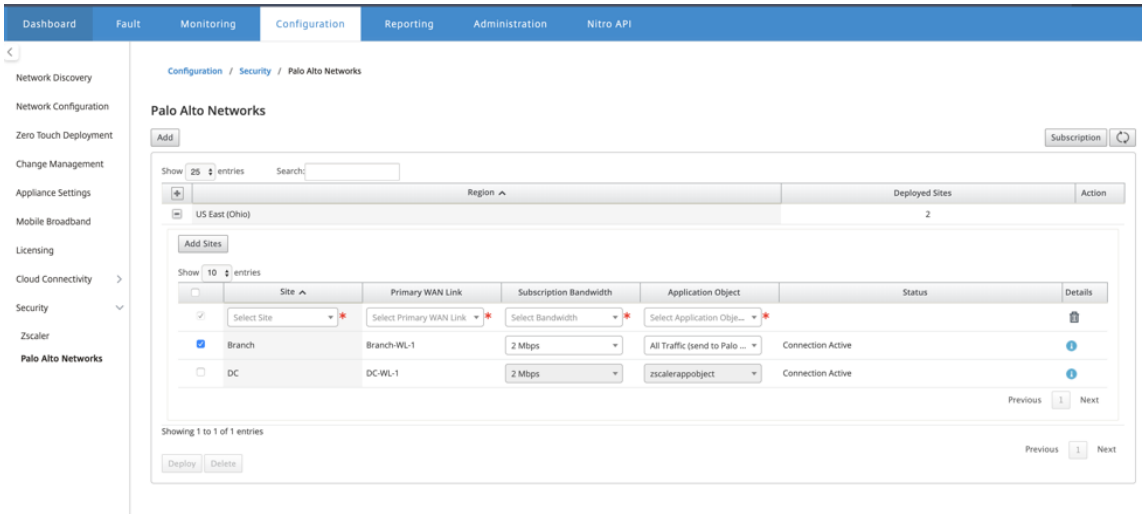
1. サイトをデプロイするには、PRISMA ACCESS ネットワークリージョンと Prisma Access リージョン用に構成する SD-WAN サイトを選択し、サイト WAN リンク、帯域幅、およびトラフィック選択用のアプリケーションオブジェクトを選択します。

   > 注:
   >
   > 選択した帯域幅が使用可能な帯域幅範囲を超えると、トラフィックフローが影響を受けます。
   >
   > [アプリケーションオブジェクト] の選択の下にある [すべてのトラフィック] オプションを選択すると、インターネットにバインド されたすべてのトラフィック を PRISMA Access サービスにリダイレクトできます。

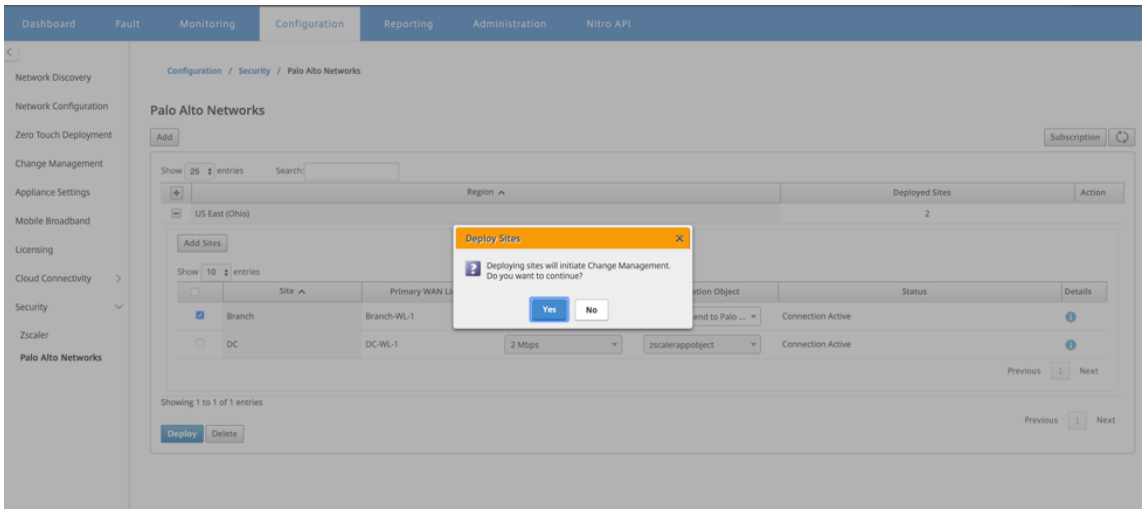




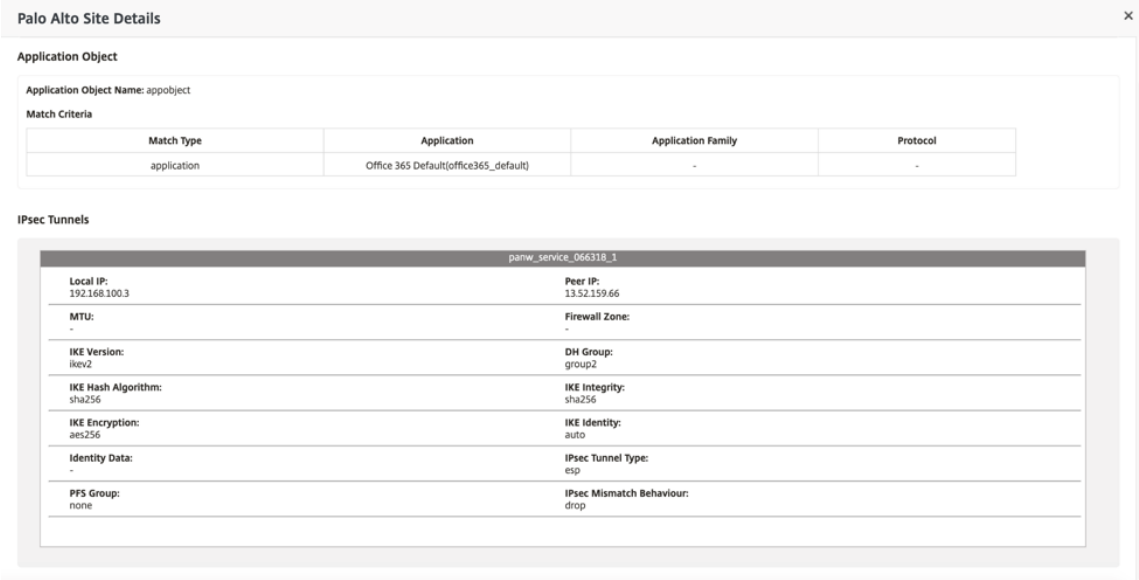
2. 必要に応じて、引き続き SD-WAN ブランチサイトを追加できます。



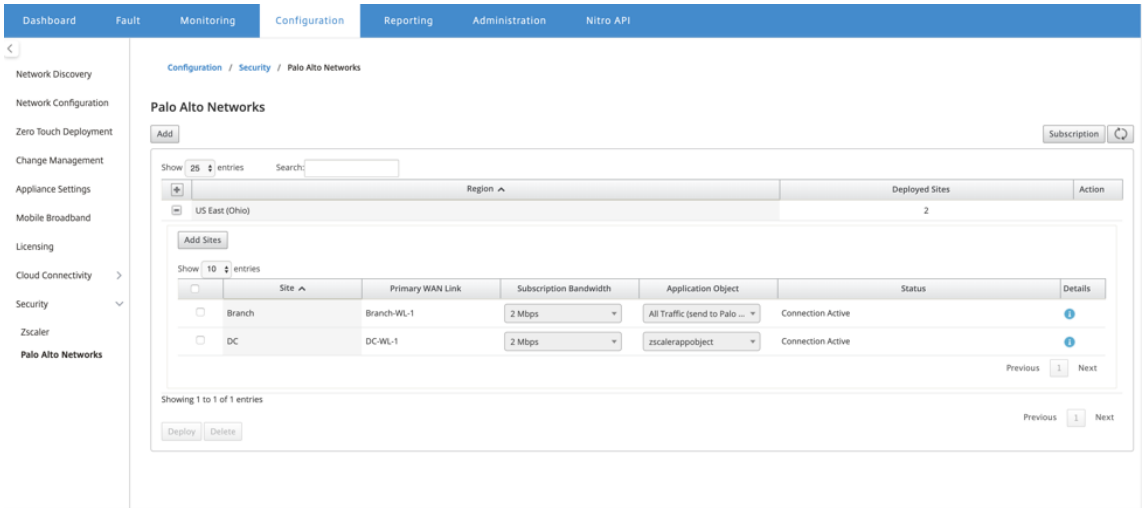
3. ［展開］をクリックします。変更管理プロセスが開始されます。［**Yes**］をクリックして続行します。



展開後、トンネルの確立に使用される IPsec トンネル構成は次のとおりです。



ランディングページには、さまざまな SD-WAN リージョンで構成およびグループ化されたすべてのサイトのリストが表示されます。



エンドツーエンドのトラフィック接続を確認します。

- ブランチの LAN サブネットから、インターネットリソースにアクセスします。
- トラフィックが Citrix SD-WAN IPsec トンネルを通過して Palo Alto Prisma Access に到達することを確認します。
- [Monitoring] タブで、Palo Alto セキュリティポリシーがトラフィックに適用されていることを確認します。
- インターネットからブランチ内のホストへの応答が通過することを確認します。

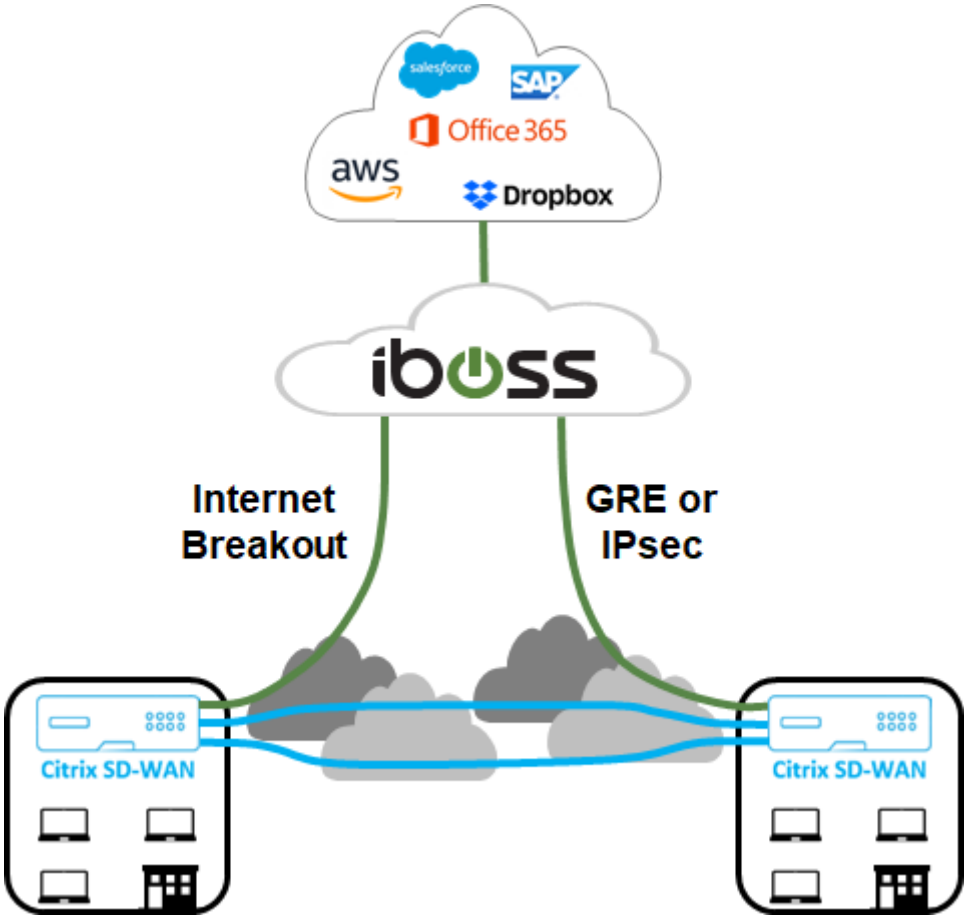
Citrix SD-WAN と iboss クラウドの統合

May 10, 2021

Citrix SD-WAN は、ブランチからインターネットへの直接アクセスを許可または拒否できるローカルのブランチからインターネットへのブレークアウトをセキュアに有効にし、企業がクラウドへの移行を支援します。Citrix SD-WAN は、個々の SaaS アプリケーションを含め、4,500 を超えるアプリケーションの統合データベースを組み合わせてアプリケーションを識別し、ディープパケット検査技術を使用してアプリケーションのリアルタイム検出と分類を行います。このアプリケーション知識を使用して、ブランチからインターネット、クラウド、SaaS へのトラフィックをインテリジェントに誘導します。

iboss クラウドは、クラウド内の任意の場所から、任意のデバイス上のインターネットアクセスを保護します。iboss は、インターネットブレイクアウトを介してプライベートオフィスの接続からインターネットトラフィックがオフロードされるブランチオフィスにクラウド内のセキュリティを提供します。ユーザーは、コンプライアンス、Web フィルタリング、SSL 検査、ファイルおよびストリームベースのセキュリティ、マルウェア防御、データ損失防止など、最高のインターネット保護を受けることができます。トラフィックはクラウドでセキュリティ保護され、すべてのブランチオフィスで一元化されたセキュリティポリシーと、帯域幅の増加に応じて瞬時に拡張できます。

Citrix SD-WAN と iboss Cloud を組み合わせることで、企業は WAN を安全に変えることができます。全体的なソリューションアーキテクチャを次の図に示します。

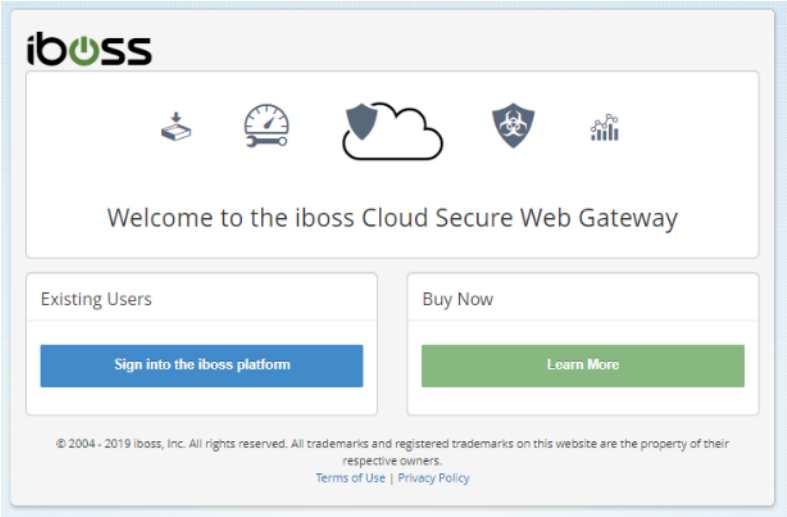


iboss 構成

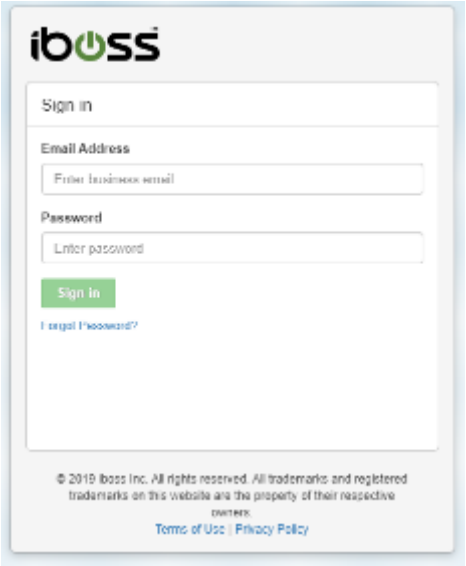
ログイン

iboss 設定は iboss ダッシュボード GUI を使用してプロビジョニングされます。

管理インターフェイスにログインするには、インターネットブラウザを使用して www.ibosscloud.com に移動します。

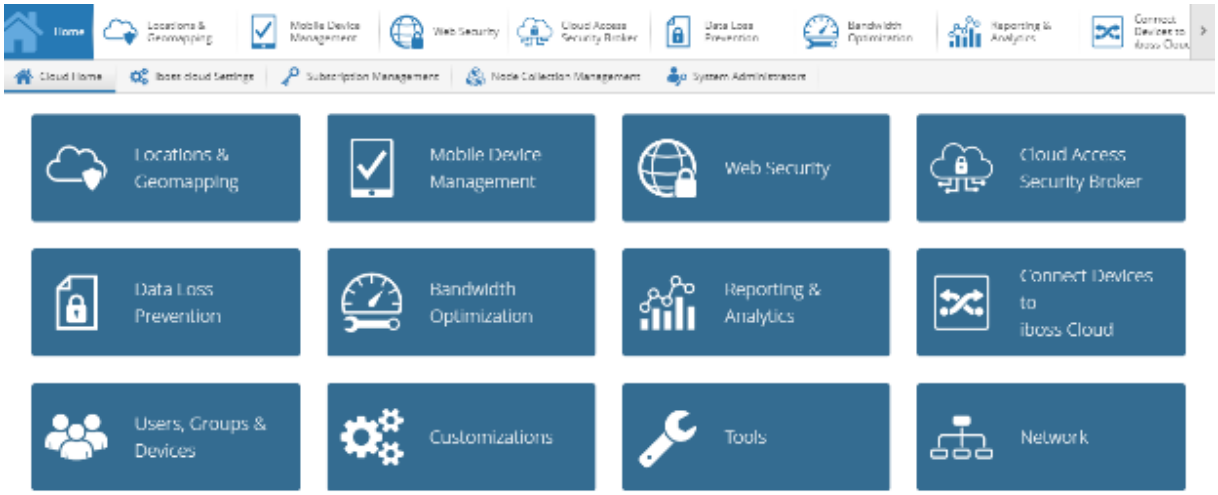


iboss プラットフォームにサインイン をクリックし、認証情報を入力します。

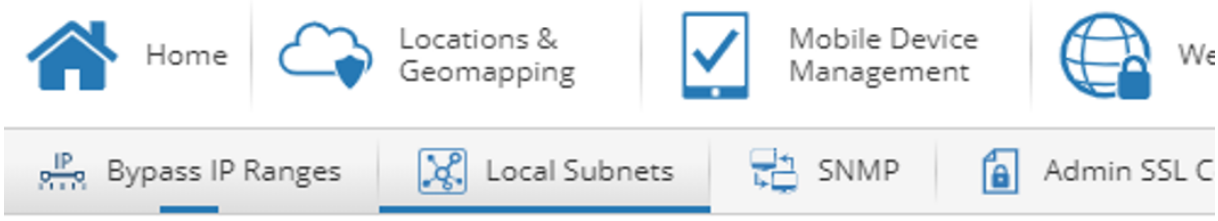


ネットワーク・サブネット

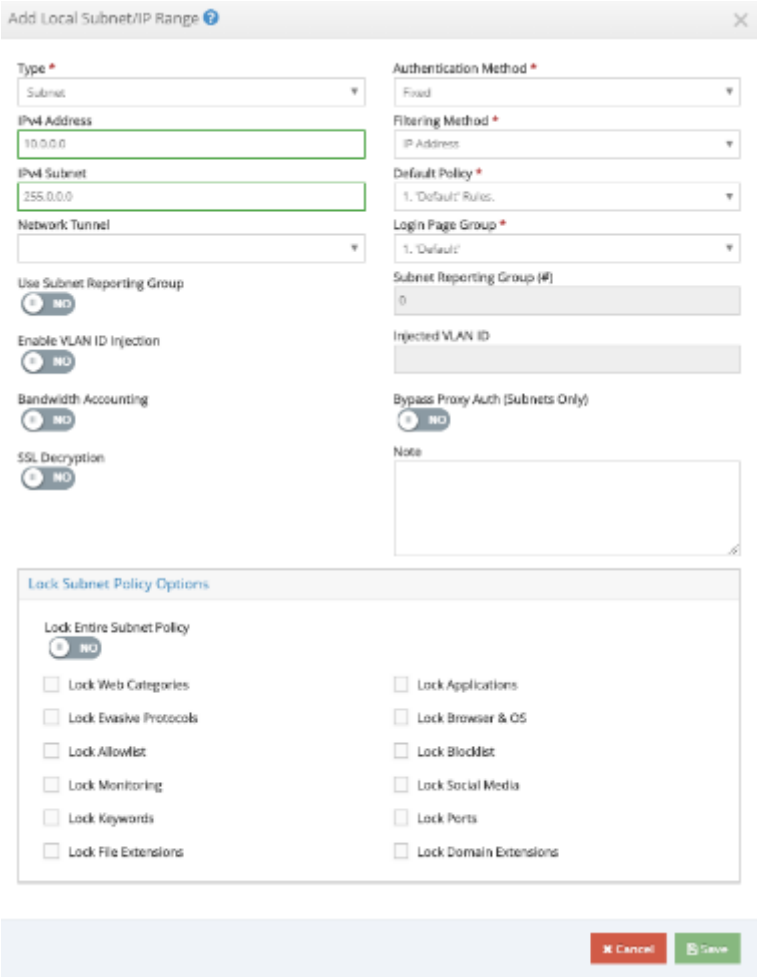
多くのお客様は、ブランチネットワークサブネットに基づいて SD-WAN 展開のポリシーを作成します。ネットワークで使用されるプライベート範囲（10.0.0.0/255.0.0.0 など）ごとにブランケットサブネットを追加し、必要に応じてより具体的なサブネットを作成することをお勧めします。ネットワークサブネットを作成するには、ホームページから [ネットワーク] タイルを選択します。



[ローカルサブネット**] > [+** 新しいローカルサブネット**/IP** 範囲] に移動します。



必須フィールドの値を入力または選択し、「保存」をクリックします。

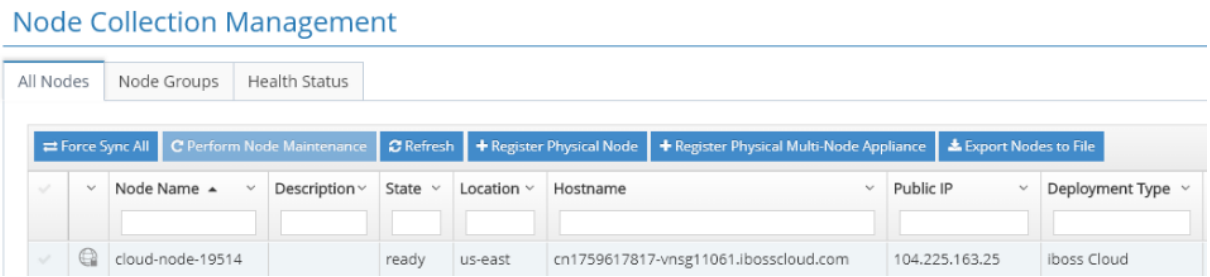


トンネル

ネットワークサブネットがプロビジョニングされた後、必要に応じて GRE トンネルまたは IPsec トンネルを使用して、ブランチオフィスを iboss Cloud に接続できます。以下の手順は、単一の iboss SWG ノードへの単一のトンネルを設定する方法を示しています。ステップを複製して、単一のブランチアプライアンスまたは複数の iboss Gateway ノードから複数のトンネルを提供できます。

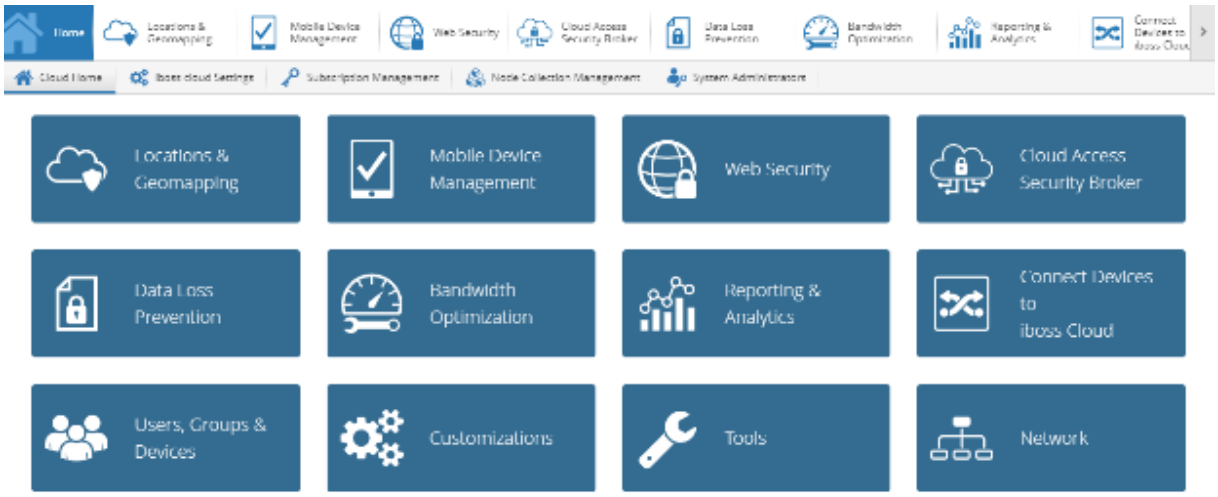
Citrix SD-WAN アプライアンスからの GRE または IPsec トンネルは、ibossGateway ノードのパブリック IP アドレスで終了します。iboss Gateway ノードのパブリック IP アドレスを識別するには、ホームページに戻り、[ノードコレクション管理] をクリックします。

[**All Nodes**] タブでは、Gateway ノードの パブリック **IP** アドレスがトンネルの外部 IP アドレスになります。以下の例では、iboss 側のトンネルの外部 IP は 104.225.163.25 です。

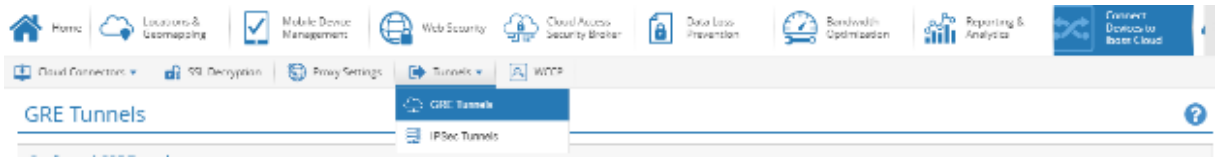


GRE

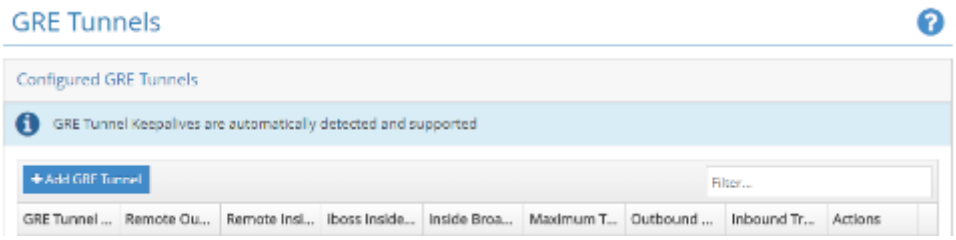
特定の場所から GRE トンネルを追加するには、ホームページに戻り、[デバイスを **iboss Cloud** に接続] をクリックします。



[トンネル] をクリックし、[**GRE** トンネル] を選択します。



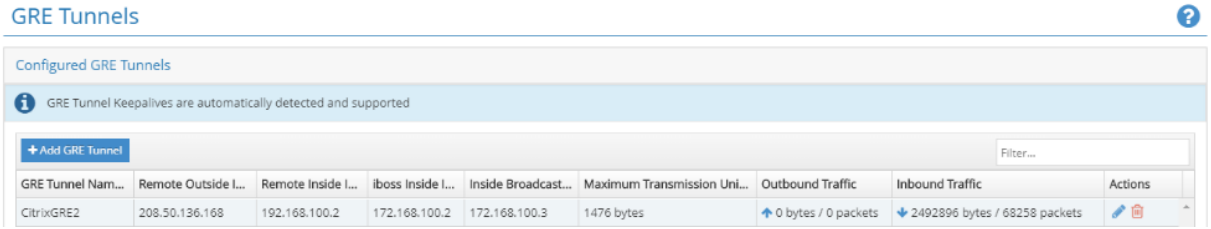
[**+ GRE** トンネルの追加] をクリックし、必要な情報を入力します。



内部トンネルサブネットは、トンネルごとに一意である必要があります（たとえば、169.254.1.0/30、169.254.1.4/30 など）。複数のサイト間で重複するサブネットには、一意の iboss ノードを使用する必要があります。たとえば、サイ

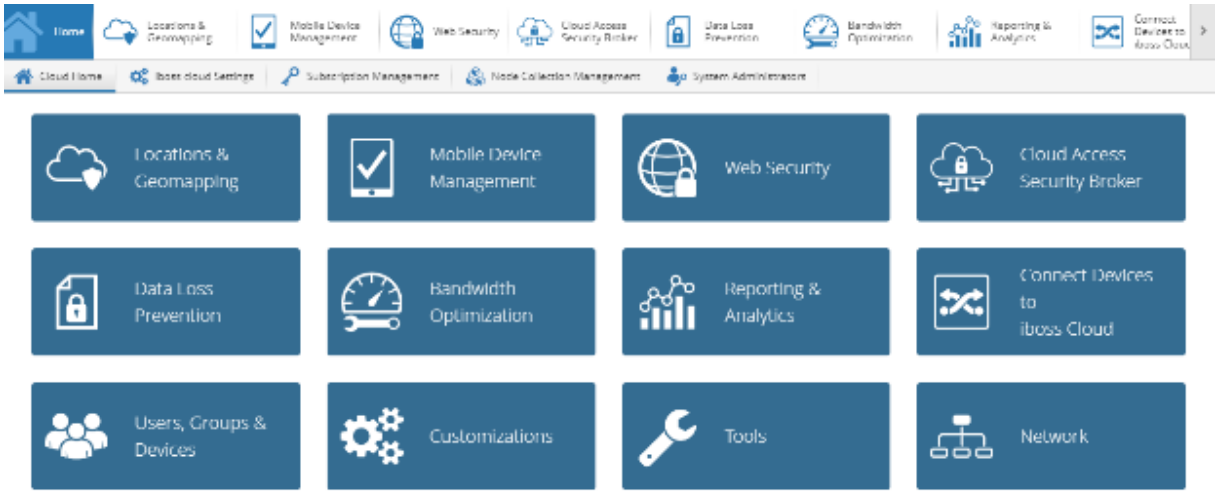
ト「A」とサイト「B」が 192.168.1.0/24 サブネットを使用する場合、これらのサイトごとに GRE トンネル設定を異なる iboss ノードで実行する必要があります。

［保存］をクリックします。トンネル情報は、要約として表示されます。必要に応じて編集することができます。

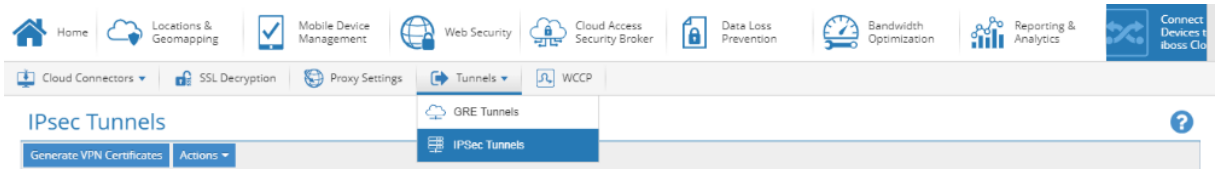


IPsec

特定の場所から IPsec トンネルを追加するには、ホームページに戻り、[デバイスを **iboss Cloud** に接続] をクリックします。



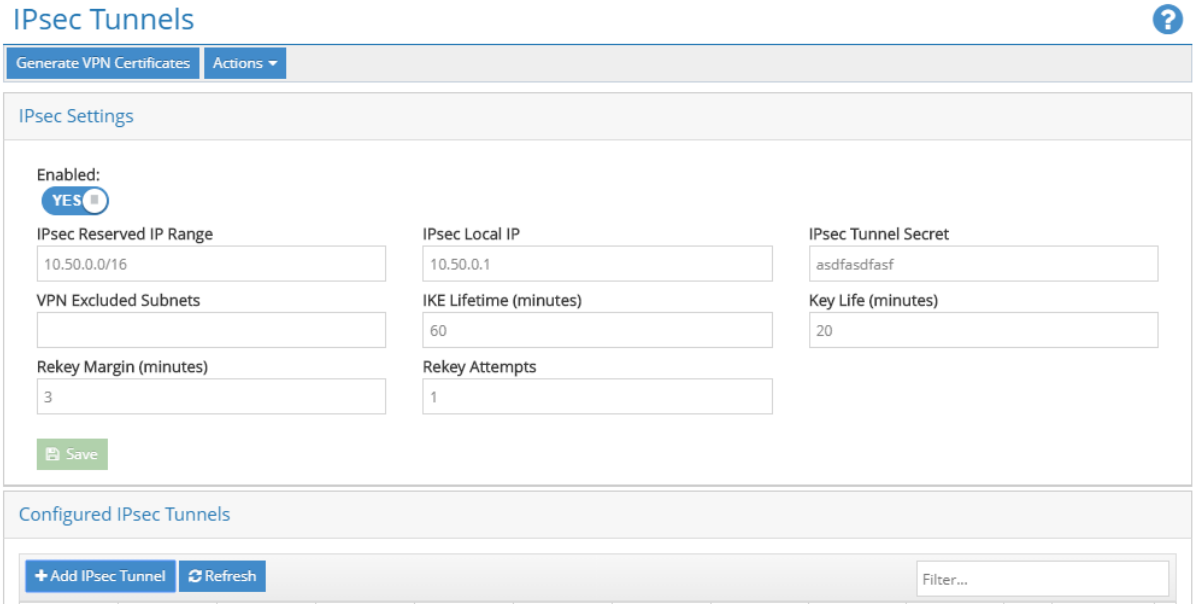
[トンネル] をクリックし、[**IPSec** トンネル] を選択します。



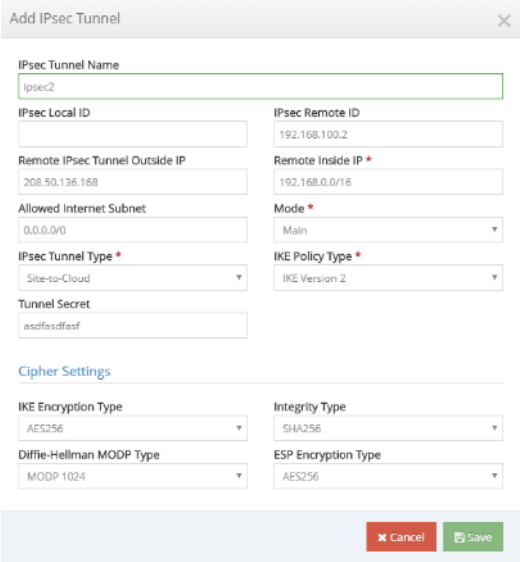
Citrix SD-WAN アプライアンスからトンネルを接続する場合は、すべてのトンネルで共通する次の IPsec 設定をお勧めします。

- IKE ライフタイム（分）: 60
- キーライフ（分）: 20
- キー再生成マージン（分）: 3
- キー再生成の試行:1

他のすべての設定（IPsec トンネルシークレットなど）は、展開固有のものです。



[**+ IPSec** トンネルの追加] をクリックして、必要に応じてトンネルを作成します。

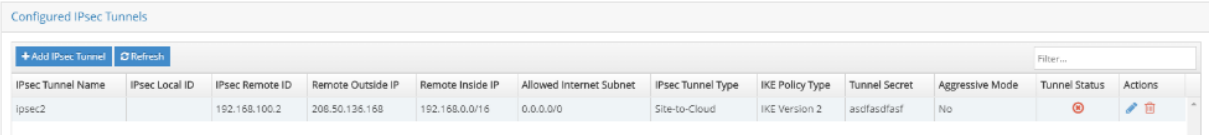


必要な情報を入力します。Citrix SD-WAN アプライアンスからの IPsec トンネルの場合、すべてのトンネルに次の IPsec 設定をお勧めします。

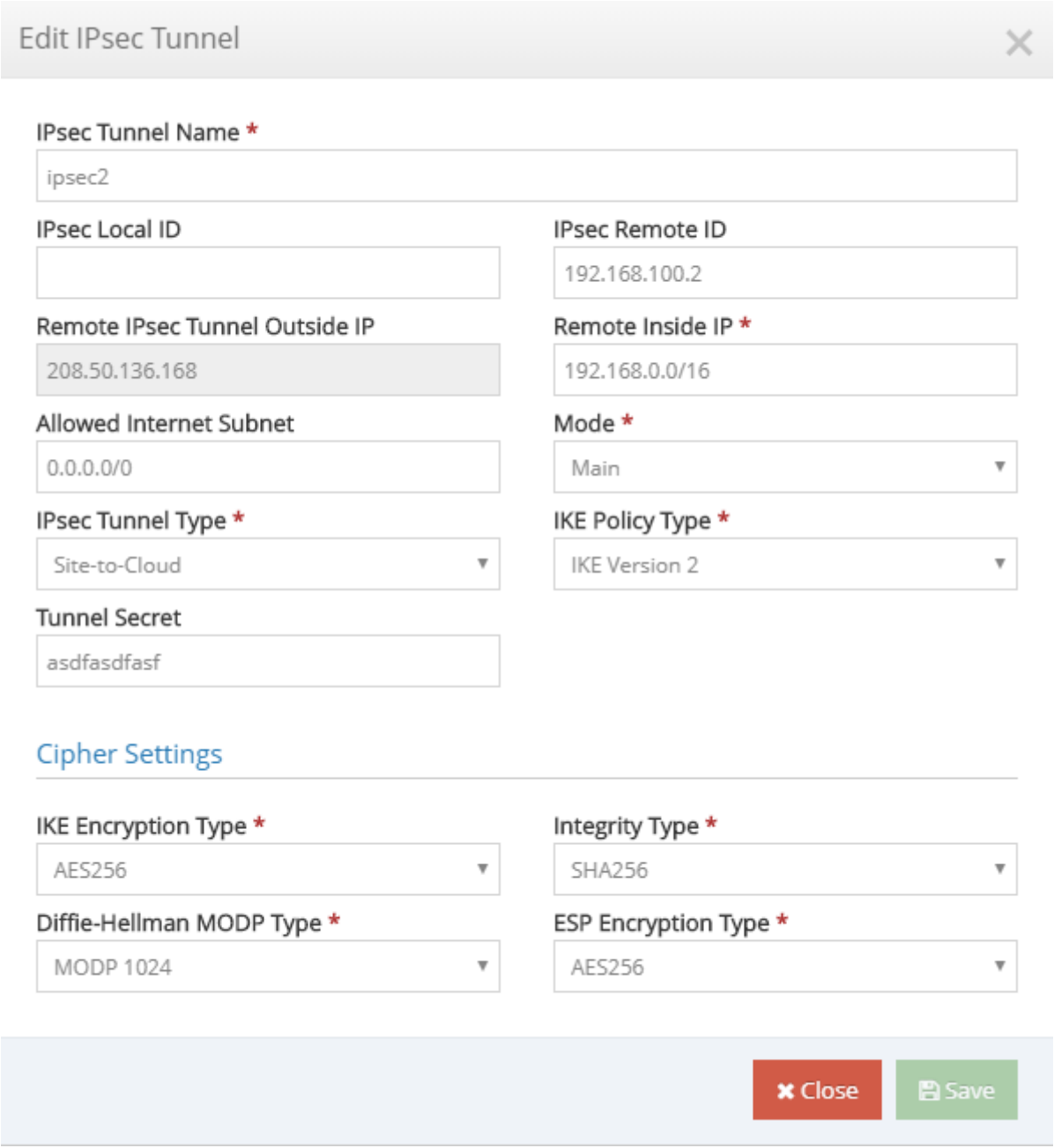
- モード: メイン
- IPsec トンネルの種類: サイト間クラウド
- IKE ポリシータイプ: IKE バージョン 2
- IKE 暗号化タイプ:AES256
- 整合性タイプ:SHA256
- Diffie-Hellman MODP タイプ:MODP 1024
- ESP 暗号化タイプ:AES256

他のすべての設定（たとえば、リモート IPsec トンネル IP 外部など）は、展開固有のものである場合があります。内部トンネルサブネットは、トンネルごとに一意である必要があります（たとえば、169.254.1.0/30、169.254.1.4/30 など）。複数のサイト間で重複するサブネットには、一意の iboss ノードを使用する必要があります。たとえば、サイト「A」とサイト「B」の両方がサブネット 192.168.1.0/24 を使用する場合、これらのサイトのトンネル設定は異なる iboss ノードで実行する必要があります。

［保存］をクリックします。トンネル情報は、要約として表示されます。



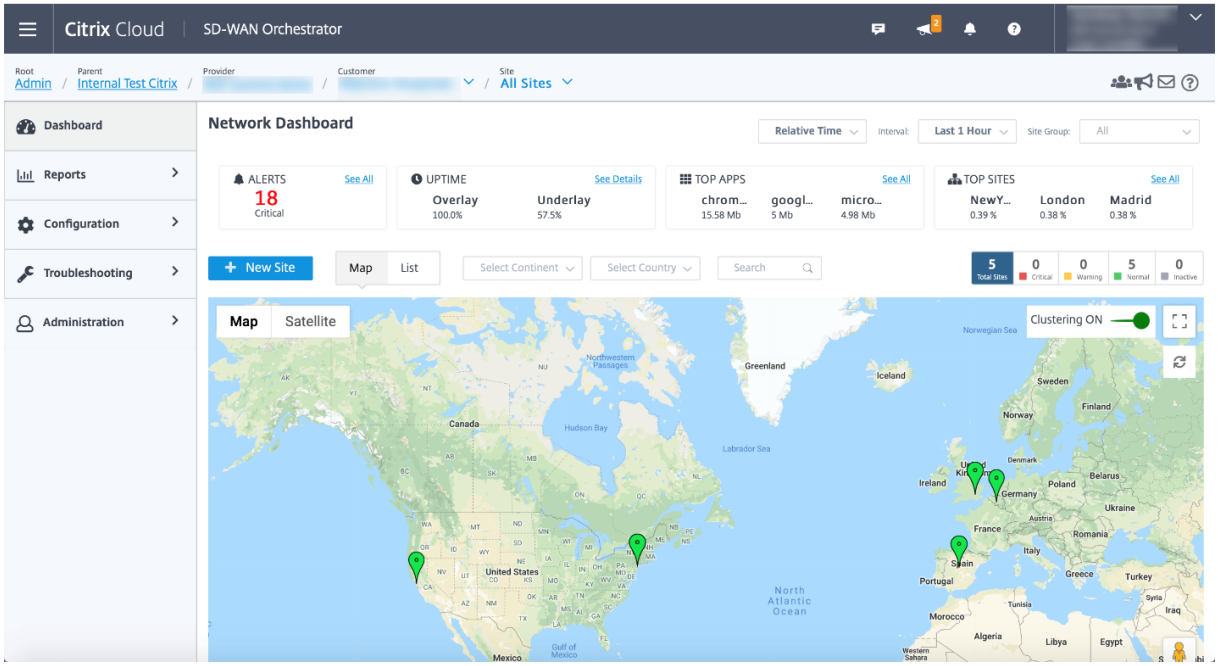
IP の外側のリモート **IPsec** トンネルを除く、トンネルのすべての設定パラメータを編集できます。



Citrix SD-WAN 構成

Citrix SD-WAN ネットワークは、Citrix Cloud ベースの管理サービス Citrix SD-WAN Orchestrator を介して管理されます。アカウントをお持ちでない場合は、「Citrix SD-WAN Orchestrator のオンボーディング」を参照してください。

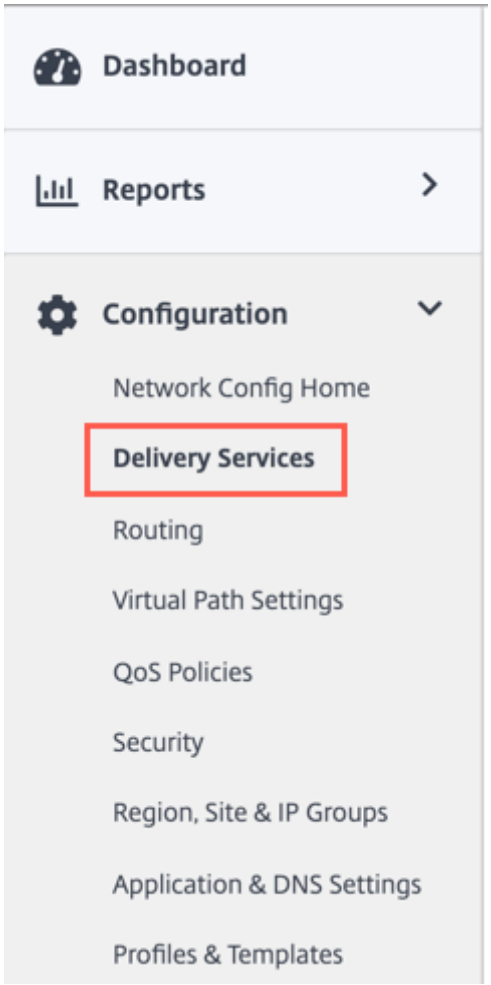
オンボーディングプロセスが正常に完了すると、SD-WAN Orchestrator にアクセスできます。



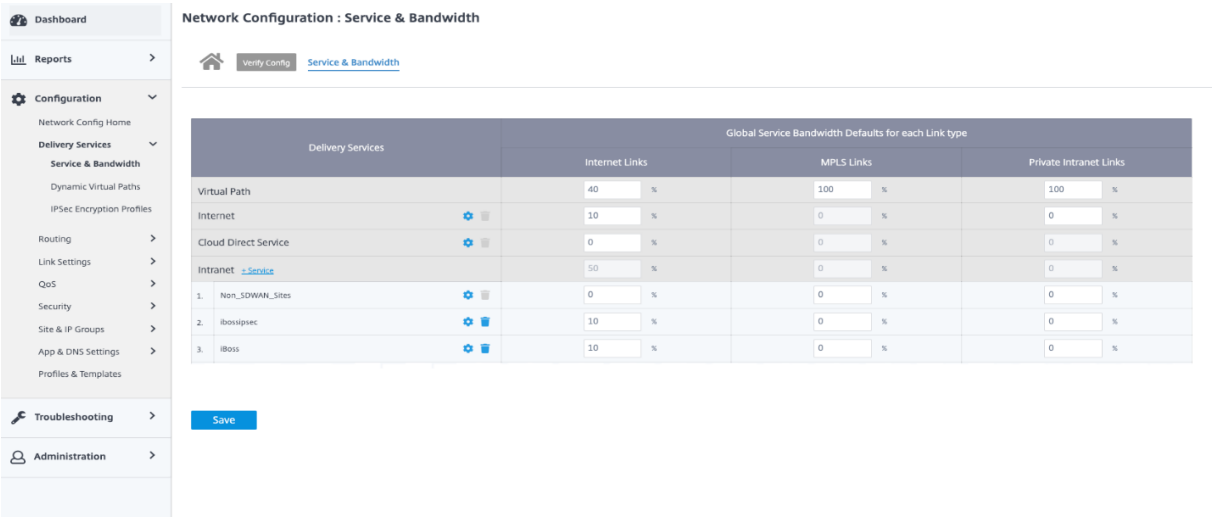
Citrix SD-WAN サイトがすでに構成されており、ブランチおよびネットワークに接続されていることを確認します。構成の詳細については、「ネットワーク構成」を参照してください。

配送サービス

配信サービスを使用すると、インターネット、イントラネット、IPsec、GRE などの配信サービスを構成できます。配信サービスはグローバルに定義され、必要に応じて個々のサイトの WAN リンクに適用されます。



iboss クラウドは、GRE または IPsec サービスを介して Citrix SD-WAN から接続できます。前のセクションの iboss が推奨する設定を使用してください。



GRE サービス

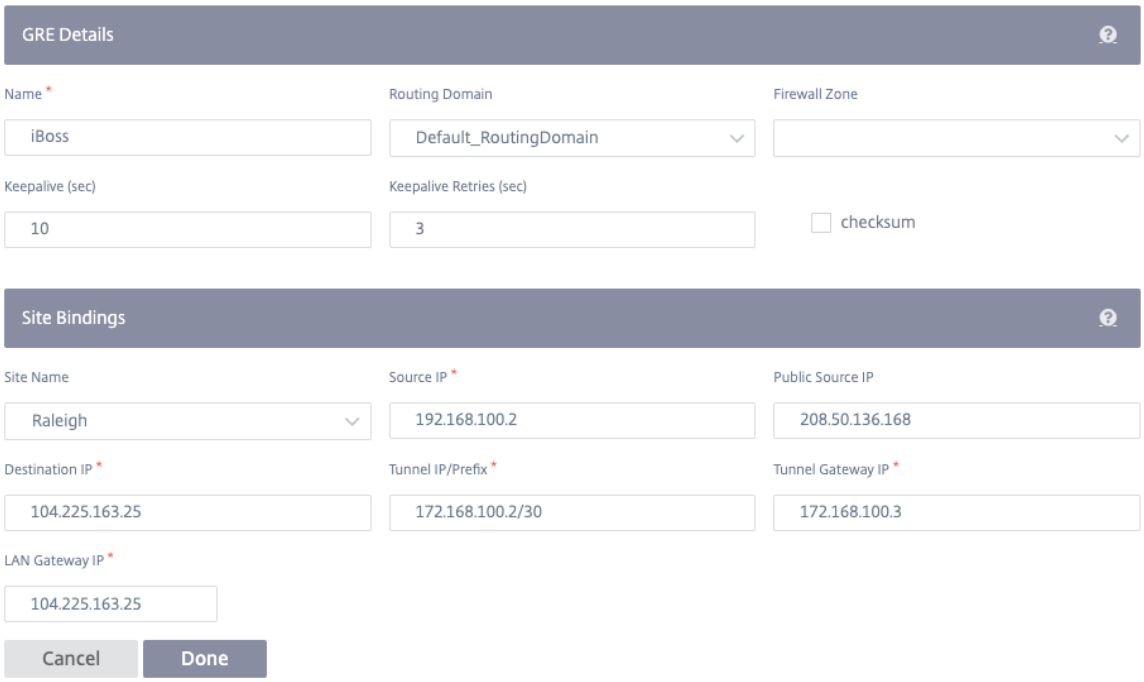
GRE トンネルを終了するように SD-WAN アプライアンスを設定できます。次の設定を行います。

GRE の詳細:

- 名前: GRE サービスの名前。
- ルーティングドメイン：GRE トンネルのルーティングドメイン。
- ファイアウォールゾーン：トンネル用に選択されたファイアウォールゾーン。デフォルトでは、トンネルは Default_LAN_Zone に配置されます。
- キープアライブ：キープアライブメッセージを送信する間隔。0 に設定すると、キープアライブパケットは送信されませんが、トンネルはアップ状態のままです。
- キープアライブ再試行：Citrix SD-WAN アプライアンスが応答なしでキープアライブパケットを送信してからトンネルダウンを行う回数。
- チェックサム：トンネルの GRE ヘッダーのチェックサムを有効または無効にします。

サイトバインディング:

- サイト名：GRE トンネルをマッピングするサイト。
- 送信元 **IP**：トンネルの送信元 IP アドレス。これは、このサイトで設定されている仮想インターフェイスの 1 つです。選択したルーティングドメインによって、使用可能な送信元 IP アドレスが決まります。
- パブリック送信元 **IP**：トンネルトラフィックが NAT を通過する場合の送信元 IP。
- 宛先 **IP**：トンネルの宛先 IP アドレス。
- トンネル **IP/**プレフィクス：GRE トンネルの IP アドレスとプレフィクス。
- トンネルゲートウェイ **IP**：トンネルトラフィックをルーティングするためのネクストホップ IP アドレス。
- **LAN** ゲートウェイ **IP**：LAN トラフィックをルーティングするためのネクストホップ IP アドレス。



IPSec サービス

Citrix SD-WAN アプライアンスは、LAN または WAN 側のサードパーティのピアと固定 IPSec トンネルをネゴシエートできます。トンネルエンドポイントを定義し、サイトをトンネルエンドポイントにマッピングできます。

セキュリティプロトコルと IPsec 設定を定義する IPsec セキュリティプロファイルを選択して適用することもできます。

IPsec 暗号化プロファイルを追加するには、[構成] > [デリバリーサービス] > [**IPsec** 暗号化プロファイル] タブを選択します。

IPsec プロファイルは、IPsec サービスを配信サービスセットとして構成するときに使用されます。[IPsec セキュリティプロファイル] ページで、[IP **sec** 暗号化プロファイル]、[**IKE** 設定]、および [**IPsec** 設定] に必要な値を入力します。

IPsec 暗号化プロファイル情報

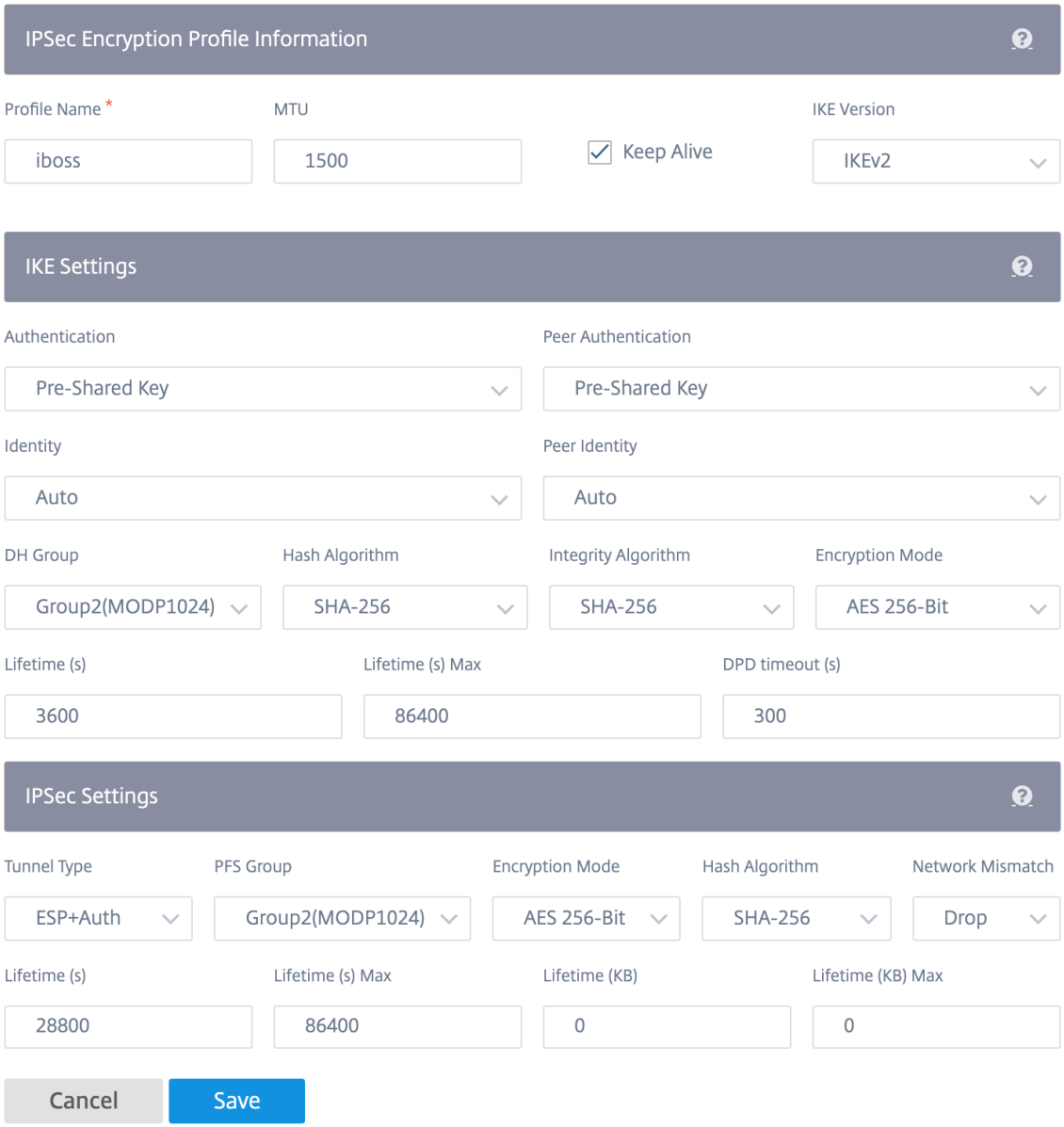
- プロファイル名: プロファイルの名前。
- **MTU**: IKE または IPsec の最大パケットサイズ（バイト単位）。
- **Keep Alive**: トンネルをアクティブに保ち、ルートの適格性を有効にします。
- **IKE** バージョン: IKE プロトコルのバージョン。

IKE 設定:

- モード：IKE フェーズ 1 ネゴシエーションモードには、メインモードまたはアグレッシブモードを選択します。
  - メイン: ネゴシエーション中に潜在的な攻撃者に情報は公開されませんが、アグレッシブモードよりも遅くなります。
  - アグレッシブ：ネゴシエーション中に一部の情報（ネゴシエーション中のピアの識別情報など）が潜在的な攻撃者に公開されますが、メインモードよりも高速です。
- 認証：認証タイプ、証明書、または事前共有キー。
- アイデンティティ: アイデンティティメソッド。
- ピア **ID**：ピア ID メソッド。
- **DH** グループ：IKE キーの生成に使用できる Diffie-Hellman（DH）グループ。
- ハッシュアルゴリズム：IKE メッセージを認証するためのハッシュアルゴリズム。
- 暗号化モード：IKE メッセージの暗号化モード。
- **Lifetime (s)**：IKE セキュリティアソシエーションが存在するのに推奨される期間（秒単位）。
- [**Lifetime (s) Max**]: IKE セキュリティアソシエーションの存在を許可する最大優先期間（秒単位）。
- **DPD** タイムアウト: VPN 接続のデッドピア検出タイムアウト (秒単位)。

IPSec 設定:

- トンネルタイプ：トンネルカプセル化タイプ。
  - **ESP**：ユーザーデータのみを暗号化します。
  - **ESP+** 認証：ユーザーデータを暗号化し、HMAC を含みます。
  - **ESP+NULL**：パケットは認証されますが、暗号化されません。
  - **AH**: HMAC のみが含まれています。
- **PFS** グループ：完全なフォワード秘密鍵生成に使用する Diffie—Hellman グループ。
- 暗号化モード: ドロップダウンメニューから IPsec メッセージの暗号化モード。
- ハッシュアルゴリズム: MD5、SHA1、および SHA-256 ハッシュアルゴリズムは、HMAC 検証に使用できます。
- ネットワークの不一致: パケットが IPsec トンネルの保護ネットワークと一致しない場合に実行するアクション。
- ライフタイム: IPsec セキュリティアソシエーションが存在するまでの時間 (秒単位)。
- **Lifetime (s) Max**:IPsec セキュリティアソシエーションが存在するための最大時間 (秒単位)。
- ライフタイム **(KB)**: IPsec セキュリティアソシエーションが存在するデータの量 (キロバイト単位)。
- ライフタイム **(KB)** 最大: IPsec セキュリティアソシエーションが存在できるデータの最大量 (KB 単位)。



IPSec トンネルを設定するには、次の手順を実行します。

1. サービスの詳細を指定します。

    - サービス名: IPSec サービスの名前。
    - サービスタイプ: IPSec トンネルが使用するサービス。
    - ルーティングドメイン: LAN 経由の IPsec トンネルの場合は、ルーティングドメインを選択します。IPsec トンネルがイントラネットサービスを使用する場合、イントラネットサービスはルーティングドメインを決定します。
    - ファイアウォールゾーン: トンネルのファイアウォールゾーン。デフォルトでは、トンネルは Default_LAN_Zone に配置されます。

2. トンネルエンドポイントを追加します。

   - 名前: [サービスタイプ] が [イントラネット] の場合、トンネルが保護するイントラネットサービスを選択します。それ以外の場合は、サービスの名前を入力します。
   - ピア **IP**：リモートピアの IP アドレス。
   - **IPsec** プロファイル: セキュリティプロトコルと IPsec 設定を定義する IPsec セキュリティプロファイル。
   - 事前共有キー：IKE 認証に使用される事前共有キー。
   - ピア事前共有キー：IKEv2 認証に使用される事前共有キー。
   - アイデンティティデータ: 手動アイデンティティタイプまたはユーザー FQDN タイプを使用する場合に、ローカル ID として使用されるデータ。
   - ピア **ID** データ: 手動の ID またはユーザー FQDN タイプを使用する場合に、ピア ID として使用されるデータ。
   - 証明書：IKE 認証として [証明書] を選択した場合は、設定された証明書から選択します。

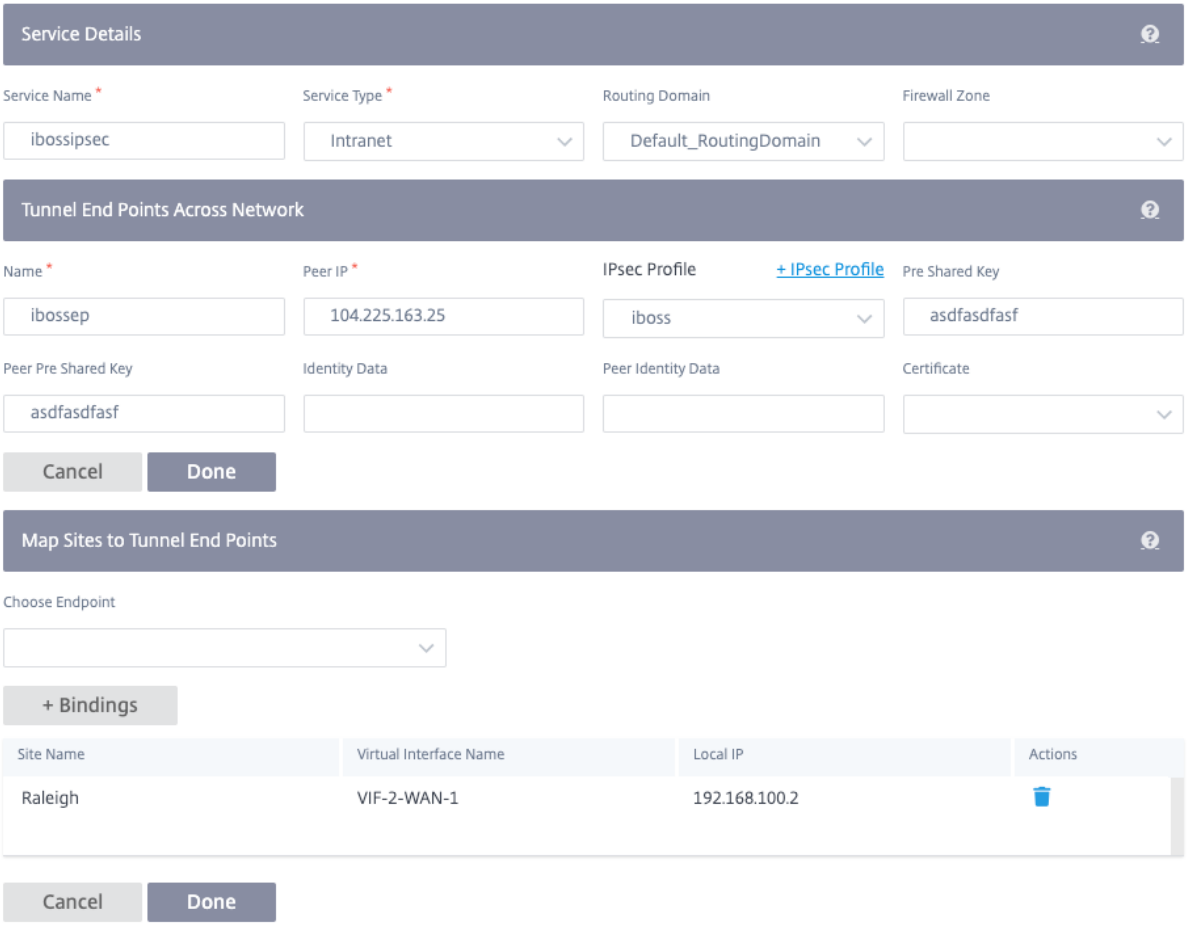
3. サイトをトンネルエンドポイントにマッピングします。

   - **Choose Endpoint**: サイトにマップするエンドポイント。
   - サイト名: エンドポイントにマップされるサイト。
   - 仮想インターフェイス名: エンドポイントとして使用するサイトの仮想インターフェイス。
   - ローカル **IP**：ローカルトンネルエンドポイントとして使用するローカル仮想 IP アドレス。

4. 保護されたネットワークを作成します。

   - 送信元ネットワーク **IP/**プレフィックス：IPsec トンネルが保護するネットワークトラフィックの送信元 IP アドレスとプレフィックス。
   - 宛先ネットワーク **IP/**プレフィックス：IPsec トンネルが保護するネットワークトラフィックの宛先 IP アドレスとプレフィックス。

5. IPsec 構成がピアアプライアンスにミラーリングされていることを確認します。



IPsec は安全なトンネルを提供します。Citrix SD-WAN は IPsec 仮想パスをサポートしているため、サードパーティ製のデバイスが、Citrix SD-WAN アプライアンスの LAN または WAN 側で IPsec VPN トンネルを終了できます。140-2 レベル 1 FIPS 認定の IPSec 暗号化バイナリを使用して、SD-WAN アプライアンスで終端するサイト間の IPSec トンネルを保護できます。

また、Citrix SD-WAN は、差別化された仮想パストンネリングメカニズムを使用した耐障害性 IPSec トンネリングもサポートします。

GRE および IPSec トンネルの監視

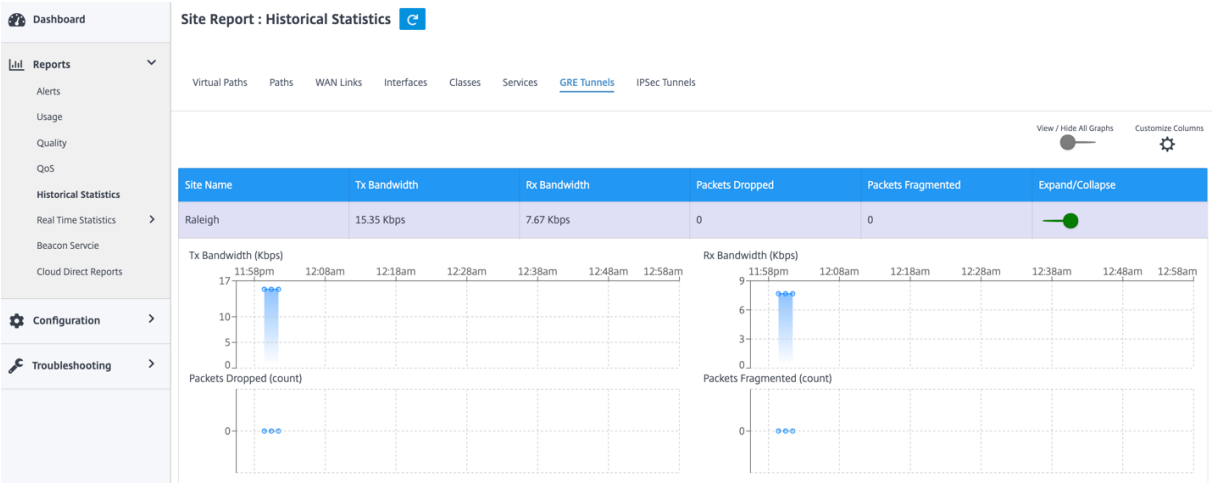
GRE トンネル

トンネリングメカニズムを使用して、あるプロトコルのパケットを別のプロトコル内で転送できます。他のプロトコルを伝送するプロトコルはトランスポートプロトコルと呼ばれ、伝送されたプロトコルはパッセンジャープロトコルと呼ばれます。Generic Routing Encapsulation（GRE）は、トランスポートプロトコルとして IP を使用し、さまざまなパッセンジャープロトコルを伝送できるトンネリングメカニズムです。

トンネルの送信元アドレスと宛先アドレスは、トンネル内の仮想ポイントツーポイントリンクの 2 つのエンドポイントを識別するために使用されます。

GRE トンネルの統計情報を表示するには、[レポート] > [統計] > [**GRE** トンネル] に移動します。
次のメトリックを表示できます。

- サイト名: サイト名。
- **Tx** 帯域幅: 送信帯域幅。
- **Rx** 帯域幅：受信された帯域幅。
- **Packet Drop**ed：ネットワークの輻輳のためにドロップされたパケット数。
- フラグメント化されたパケット：フラグメント化されたパケットの数。パケットはフラグメント化されて、元のデータグラムよりも小さい MTU を持つリンクを通過できる小さなパケットを作成します。フラグメントは受信ホストによって再構成されます。
- 展開/折りたたみ：必要に応じてデータを展開または折りたたむことができます。



IPSec トンネル

IP セキュリティ（IPsec）プロトコルは、機密データの暗号化、認証、再生に対する保護、IP パケットのデータ機密性などのセキュリティサービスを提供します。カプセル化セキュリティペイロード (ESP) および認証ヘッダー (AH) は、これらのセキュリティサービスを提供するために使用される 2 つの IPsec セキュリティプロトコルです。

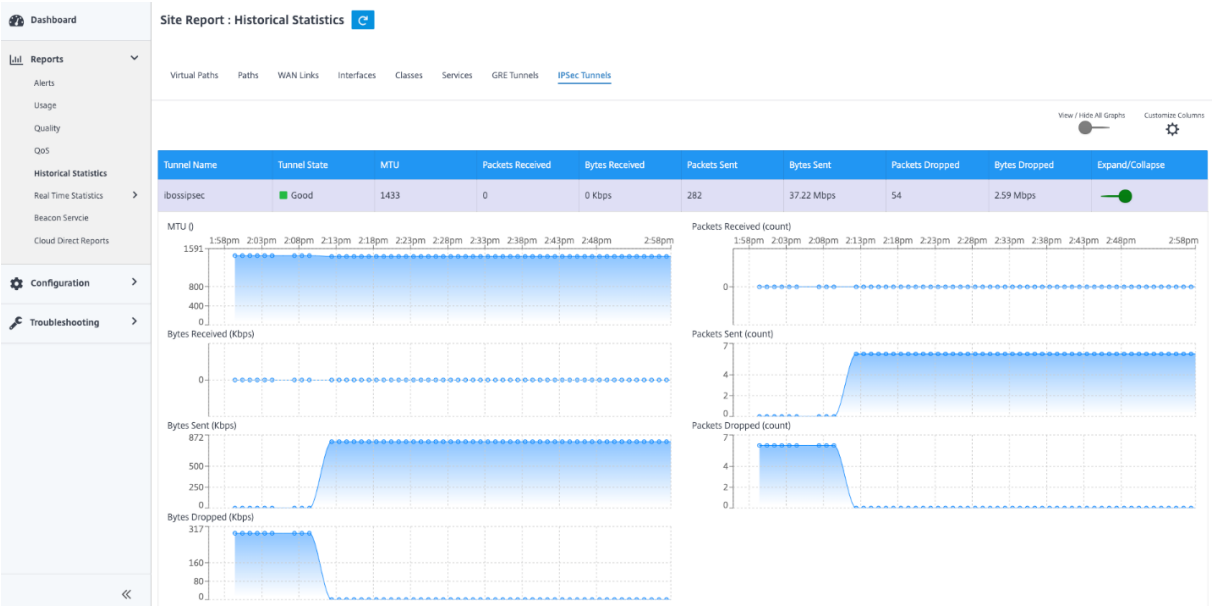
IPsec トンネルモードでは、元の IP パケット全体が IPsec によって保護されます。元の IP パケットはラップおよび暗号化され、VPN トンネルを介してパケットを送信する前に新しい IP ヘッダーが追加されます。

IPsec トンネルの 統計情報を表示するには、[レポート] > [統計] > [**IPsec** トンネル] に移動します。

次のメトリックを表示できます。

- トンネル名：トンネル名。
- トンネルの状態：IPSec トンネルの状態。
- **MTU**：最大伝送単位：特定のリンクを介して転送できる最大の IP データグラムのサイズ。

- 受信パケット：受信されたパケット数。
- 送信済みパケット：送信済みパケット数。
- **Packet Drop**ed：ネットワークの輻輳のためにドロップされたパケット数。
- ドロップされたバイト数：ドロップされたバイト数。
- 展開/折りたたみ：必要に応じてデータを展開または折りたたむことができます。



ステートフルファイアウォールと **NAT** のサポート

May 10, 2021

この機能は、SD-WAN アプリケーションに組み込まれたファイアウォールを提供します。ファイアウォールは、サービスとゾーン間のポリシーを許可し、スタティック NAT、ダイナミック NAT (PAT)、およびポートフォワーディングによるダイナミック NAT をサポートします。ファイアウォール機能には、次のようなものがあります。

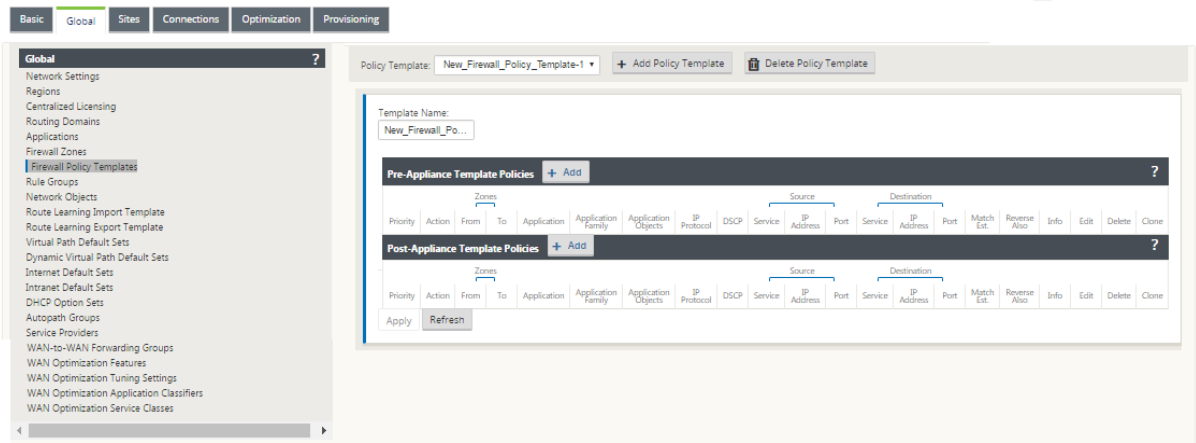
- SD-WAN ネットワーク内のユーザートラフィックのセキュリティを提供 (エンタープライズおよびサービスプロバイダー)
- （可能性）外部機器の削減（企業・サービスプロバイダー）
- 複数の顧客に対して同じ IP アドレス空間を使用する:NAT 機能 (サービスプロバイダー)
- グローバルな視点から複数のファイアウォールを適用する（サービスプロバイダ）
- ゾーン間のトラフィックフローのフィルタリング
- ゾーン内のサービス間のトラフィックのフィルタリング
- 異なるゾーンに存在するサービス間のトラフィックのフィルタリング
- サイトのサービス間のトラフィックのフィルタリング
- フローを許可、拒否、または拒否するフィルタポリシーの定義

- 選択したフローのフロー状態の追跡
- グローバルポリシーテンプレートの適用
- 信頼できないポート上のインターネットへのトラフィックに対するポートアドレス変換のサポート、およびポートフォワーディングのインバウンドとアウトバウンドのサポート
- スタティックネットワークアドレス変換 (スタティック NAT) の提供
- ダイナミックネットワークアドレス変換 (ダイナミック NAT) の提供
- ポートアドレス変換（PAT）
- ポートフォワーディング

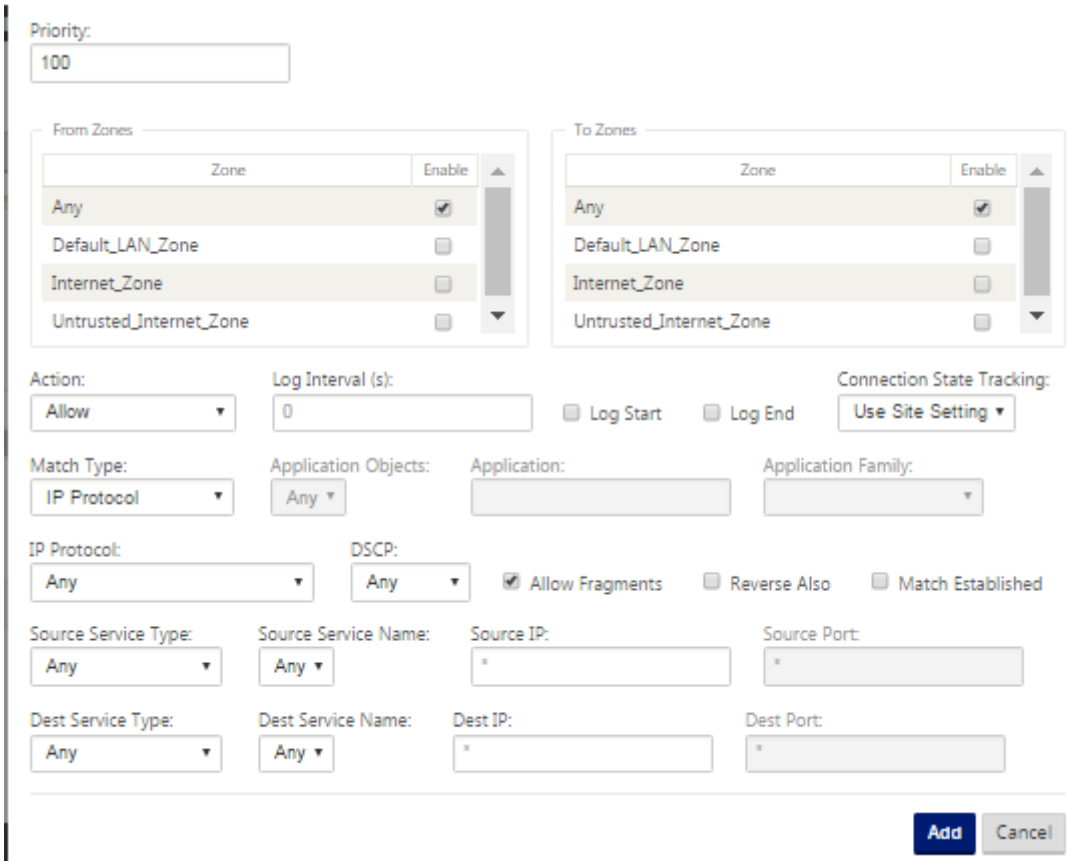
構成プロセスを簡素化するために、ファイアウォールポリシーはグローバル構成レベルで作成されます。このグローバル構成は、SD-WAN ネットワーク内のすべてのサイトに適用できる、アプライアンス前およびアプライアンス後のサイトのポリシーテンプレートで構成されます。

> 注
>
> セキュリティ上の理由により、Fail-to-Wire インラインモードでファイアウォールを使用することは推奨されません。

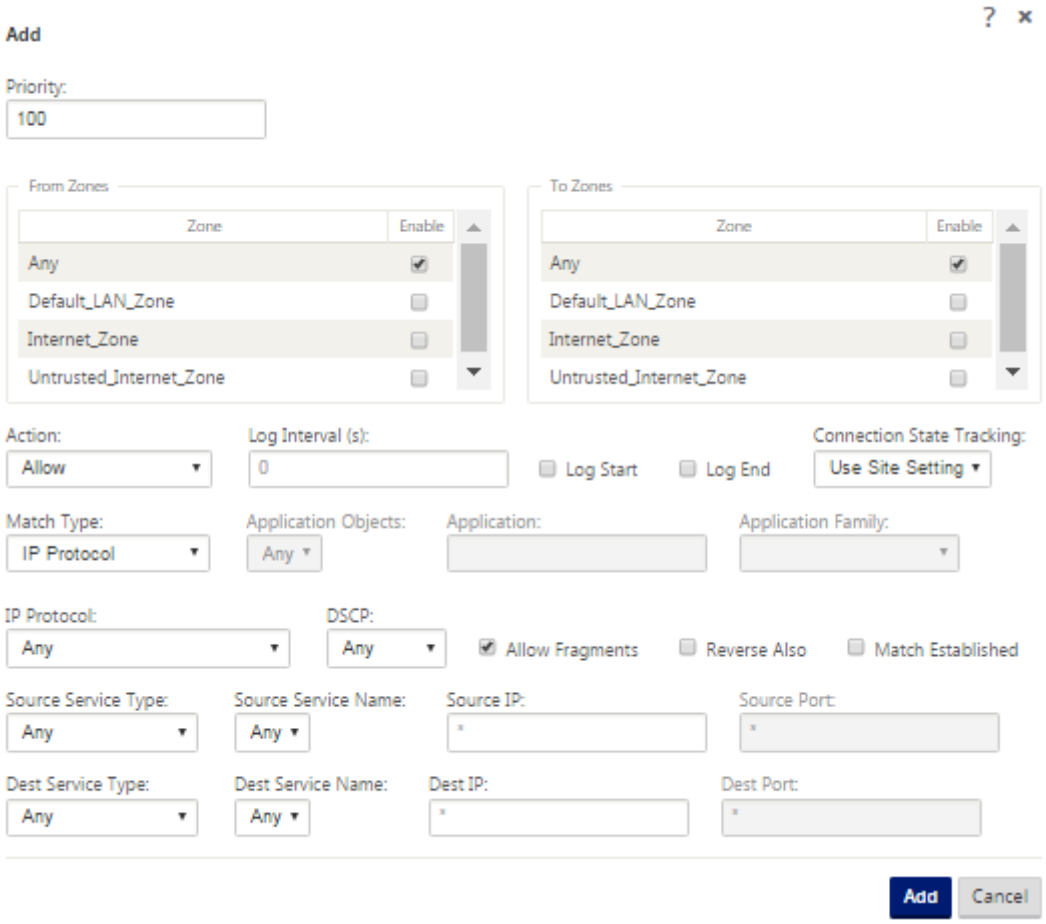
グローバルポリシーテンプレート



事前ポリシーテンプレート



ポストポリシーテンプレート



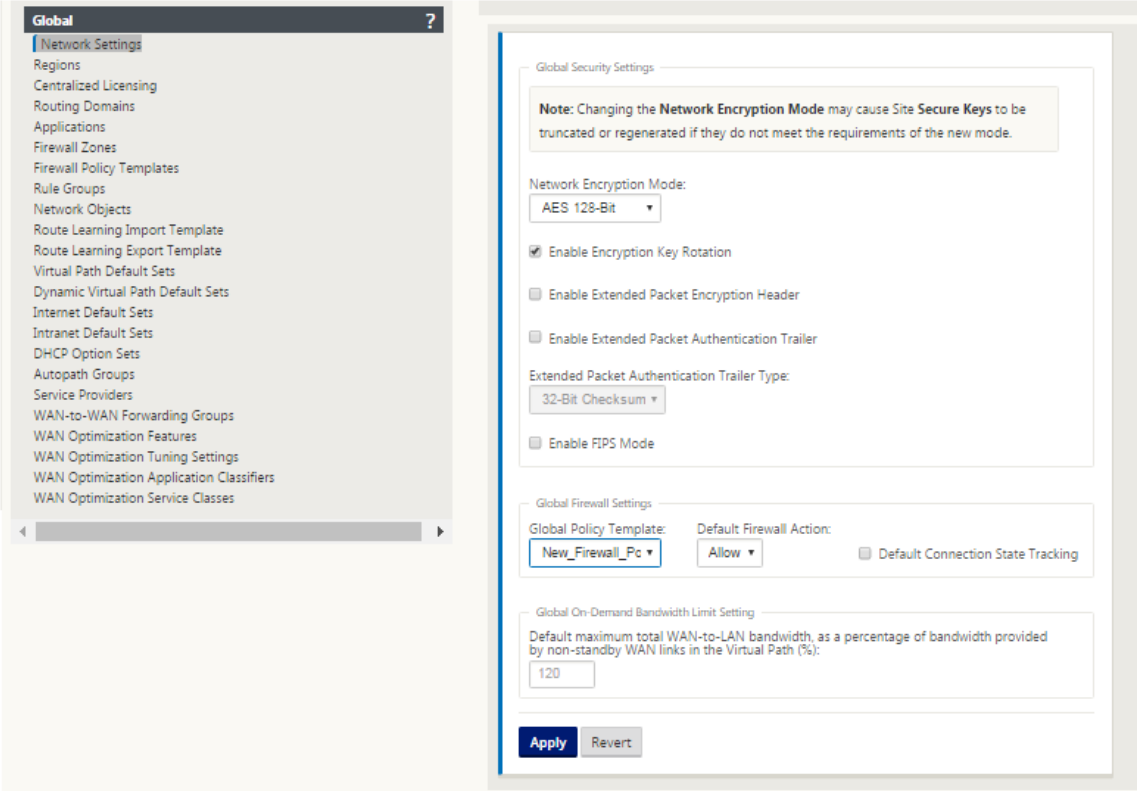
グローバルファイアウォールの設定

May 10, 2021

ファイアウォールポリシーテンプレートを作成したら、このポリシーを使用して NetScaler SD-WAN ネットワークのファイアウォール設定を構成できます。グローバルファイアウォール設定を使用すると、グローバルファイアウォールパラメータを構成できます。これらの設定は仮想 WAN ネットワーク上のすべてのサイトに適用されます。

グローバルファイアウォール設定を構成するには、次の手順を実行します。

1. 構成エディタで、[グローバル] > [ネットワーク設定] に移動し、編集アイコンをクリックします。



2. [グローバルファイアウォール設定] セクションで、次のオプションの値を選択します。
   - グローバルポリシーテンプレート -SD-WAN ネットワーク内のすべてのアプライアンスに適用するファイアウォールポリシーテンプレートの選択、デフォルトのファイアウォールアクション -フィルタポリシーに一致しないパケットを許可するには、[Allow] を選択します。フィルタポリシーに一致しないパケットをドロップするには、[Drop, **Default Connection State Tracking**] を選択します。これにより、フィルタポリシーまたは NAT 規則に一致しない TCP、UDP、および ICMP フローに対して、方向接続状態追跡が有効になります。これにより、ファイアウォールポリシーが定義されていない場合でも、非対称フローがブロックされます。
3. ［適用］をクリックします。

> 注
>
> これらの設定をサイトレベルで構成することもできます。この設定は、グローバル設定よりも優先されます。

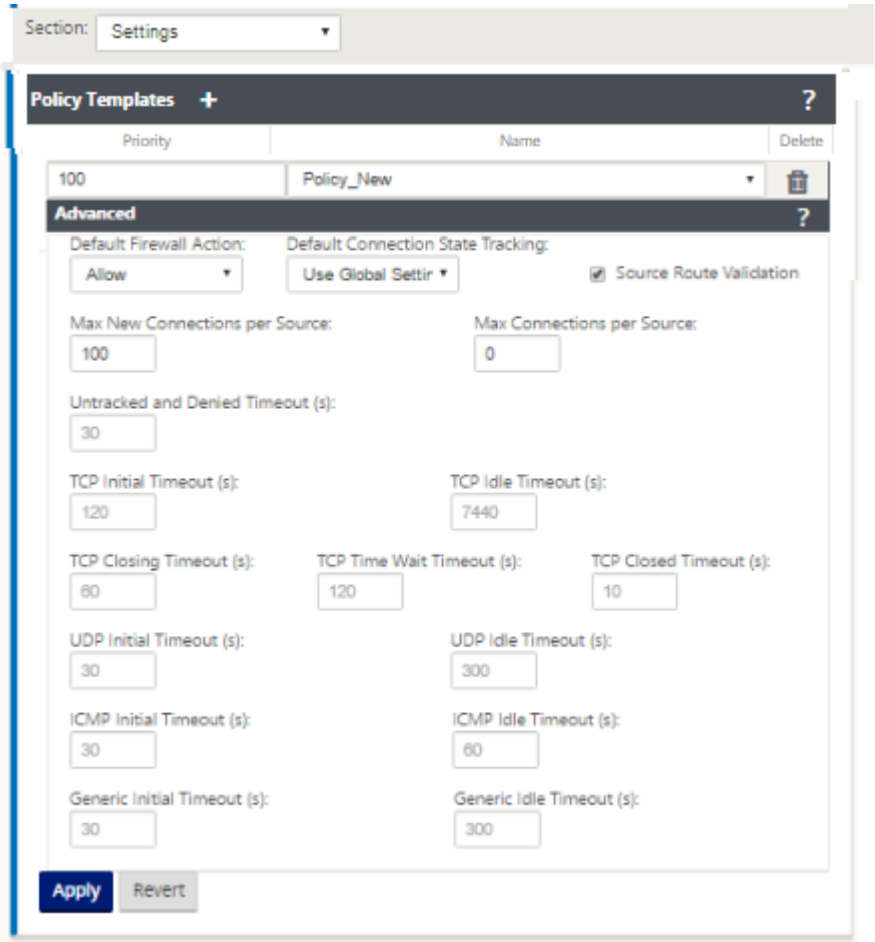
ファイアウォールの詳細設定

May 10, 2021

ファイアウォールの詳細設定は、サイトごとに個別に構成できます。これにより、グローバル設定が上書きされます。

ファイアウォールの詳細設定を構成するには

1. 構成エディタで、[接続] > [サイトの表示] > [ファイアウォール] > [設定] に移動します。



2. [ポリシーテンプレート] セクションで、[追加] をクリックします。次のパラメータの値を入力します。

   - 優先度 -ポリシーがサイトに適用される順序。
   - 名前：サイトで使用するポリシーテンプレートの名前。

3. [詳細設定] をクリックします。次のパラメーターの値を入力します。

   - デフォルトのファイアウォール操作 -次のいずれかのオプションを選択します。
     - グローバル設定の使用-NetScaler SD-WAN 設定で構成されたグローバル設定を使用します。
     - **Allow**-どのフィルタポリシーにも一致しないパケットも許可されます。
     - **Drop**：どのフィルタポリシーにも一致しないパケットはドロップされます。
   - 「デフォルトの接続状態の追跡」—次のいずれかのオプションを選択します。
     - グローバル設定の使用 -NetScaler SD-WAN 設定で構成されたグローバル設定を使用します。
     - **No Tracking**：双方向接続状態追跡は、どのフィルタポリシーにも一致しないパケットでは実行されません。

  - **Track** -双方向接続状態追跡は、どのフィルタポリシーまたは NAT 規則にも一致しない TCP、UDP、および ICMP パケットに対して実行されます。これにより、ファイアウォールポリシーが定義されていない場合でも、非対称フローがブロックされます。

- **Source Route Validation**: 有効にすると、送信元 IP アドレスによって決定される、パケットのルートとは異なるインターフェイスで受信したときにパケットがドロップされます。パケットが現在一致しているルートだけが考慮されます。
- ソースごとの最大新規接続数**:** ソース IP アドレスごとに許可される未確立接続の最大数。0 は無制限を意味します。この設定を使用して、ファイアウォールに対するサービス拒否攻撃を防止します。
- ソースあたりの最大接続数**:** ソース IP アドレスごとに許可される接続の最大数。0 は無制限を意味します。この設定を使用して、ファイアウォールに対するサービス拒否攻撃を防止します。

4. さまざまなタイムアウト設定を構成し、[**Apply**] をクリックします。

ゾーン

May 10, 2021

ネットワーク内のゾーンを構成し、トラフィックがゾーンに出入りする方法を制御するポリシーを定義できます。デフォルトでは、次のゾーンが作成されます。

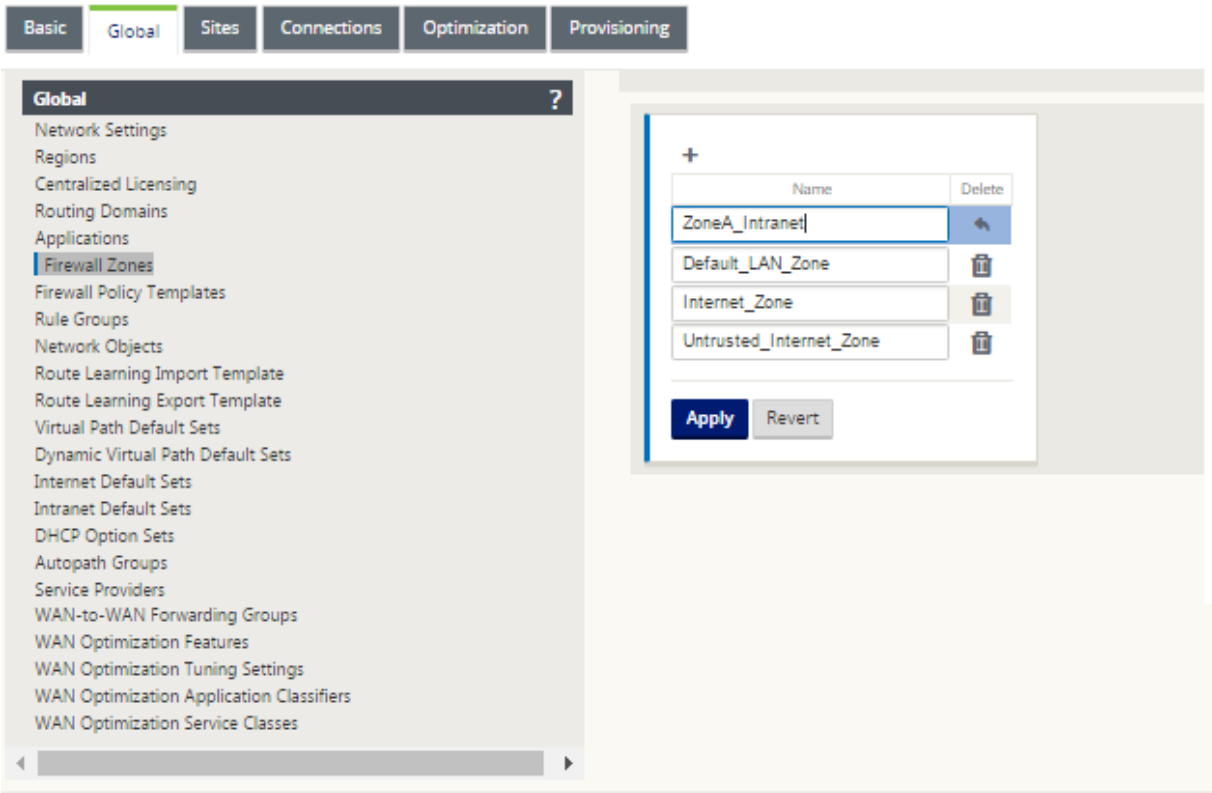
- Zone
  - 信頼されたインターフェイスを使用するインターネットサービスとの間で送受信されるトラフィックに適用されます。
- Untrusted_Internet_Zone
  - 信頼できないインターフェイスを使用するインターネットサービスとの間で送受信されるトラフィックに適用されます。
- Default_LAN_Zone
  - ゾーンが設定されていない設定可能なゾーンを持つオブジェクトへのトラフィックまたはオブジェクトからのトラフィックに適用されます。

独自のゾーンを作成し、次のタイプのオブジェクトに割り当てることができます。

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

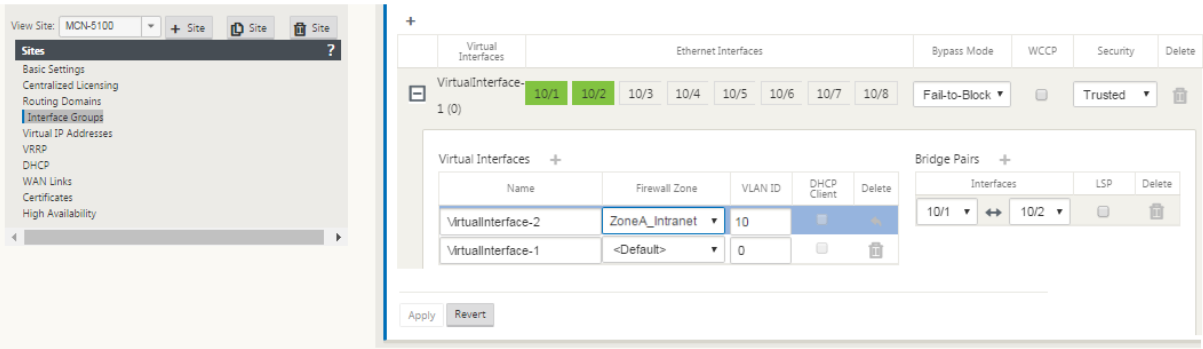
- LAN IPsec トンネル

次の図に、事前構成された 3 つのゾーンを示します。さらに、必要に応じて独自のゾーンを作成することもできます。この例では、ゾーン「zonea_ イントラネット」はユーザーが作成したゾーンです。SD-WAN アプライアンスのバイパスセグメント（ポート 1 および 2）の仮想インターフェイスに割り当てられます。



パケットの送信元ゾーンは、パケットが受信されるサービスまたは仮想ネットワークインターフェイスによって決まります。ただし、仮想パストラフィックは例外です。トラフィックが仮想パスに入ると、パケットはトラフィックを発信したゾーンでマークされ、その送信元ゾーンは仮想パスを介して伝送されます。これにより、仮想パスの受信側は、元のソースゾーンが仮想パスに入る前にポリシーを決定できます。

たとえば、ネットワーク管理者は、サイト A の VLAN 30 からのトラフィックだけがサイト B で VLAN 10 に入るようにポリシーを定義することができます。管理者は、各 VLAN にゾーンを割り当てて、これらのゾーン間のトラフィックを許可し、他のゾーンからのトラフィックをブロックするポリシーを作成できます。次のスクリーンショットは、ユーザーが「zonea_ イントラネット」ゾーンを VLAN 10 に割り当てる方法を示しています。この例では、「ZoneA_ イントラネット」ゾーンは、仮想インターフェイス「VirtualInterface2」に割り当てるためにユーザーによって事前に定義されています。

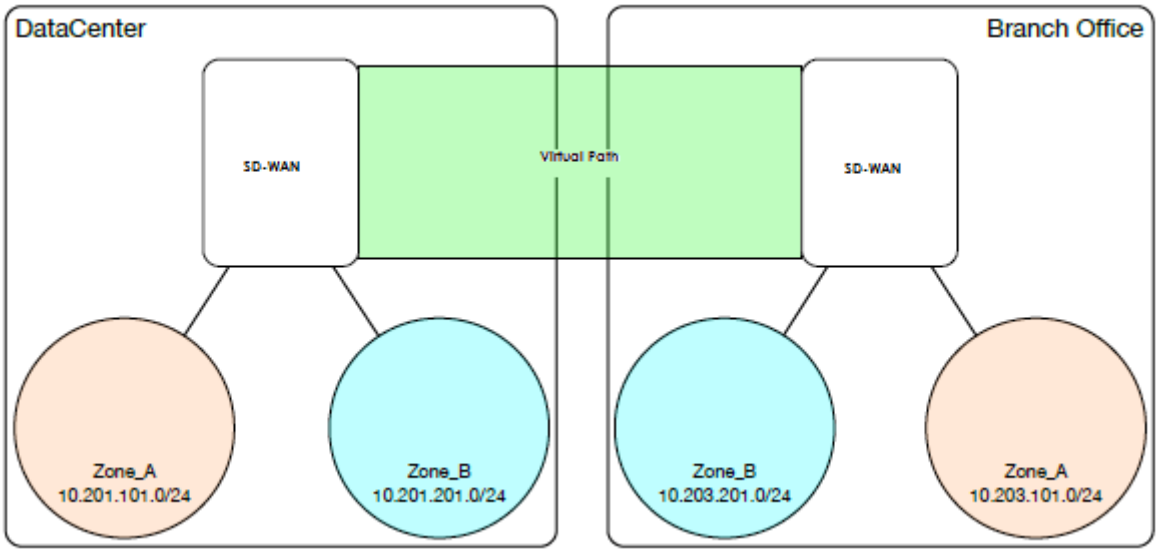


パケットの宛先ゾーンは、宛先ルートの一致に基づいて決定されます。SD-WAN アプライアンスがルートテーブルで宛先サブネットを検索すると、パケットはルートと一致します。ルートにはゾーンが割り当てられています。

- ソースゾーン
  - 非仮想パス：で受信した仮想ネットワークインターフェイスパケットを介して決定されます。
  - 仮想パス：パケットフローヘッダーのソースゾーンフィールドを介して決定されます。
  - 仮想ネットワークインターフェイス-送信元サイトでパケットを受信しました。
- 宛先ゾーン
  - パケットの宛先ルート検索により決定。

SD-WAN 内のリモートサイトと共有されるルートは、ダイナミックルーティングプロトコル（BGP、OSPF）を通じて学習されたルートなど、宛先ゾーンに関する情報を保持します。このメカニズムを使用すると、ゾーンは SD-WAN ネットワークでグローバルな重要性を獲得し、ネットワーク内でエンドツーエンドのフィルタリングを可能にします。ゾーンを使用すると、ネットワーク管理者は、顧客、事業部門、または部門に基づいてネットワークトラフィックを効率的にセグメント化できます。

SD-WAN ファイアウォールの機能を使用すると、次の図に示すように、1 つのゾーン内のサービス間のトラフィックをフィルタリングしたり、異なるゾーン内のサービス間で適用できるポリシーを作成したりできます。以下の例では、Zone_A と Zone_B があり、それぞれに LAN 仮想ネットワークインターフェイスがあります。



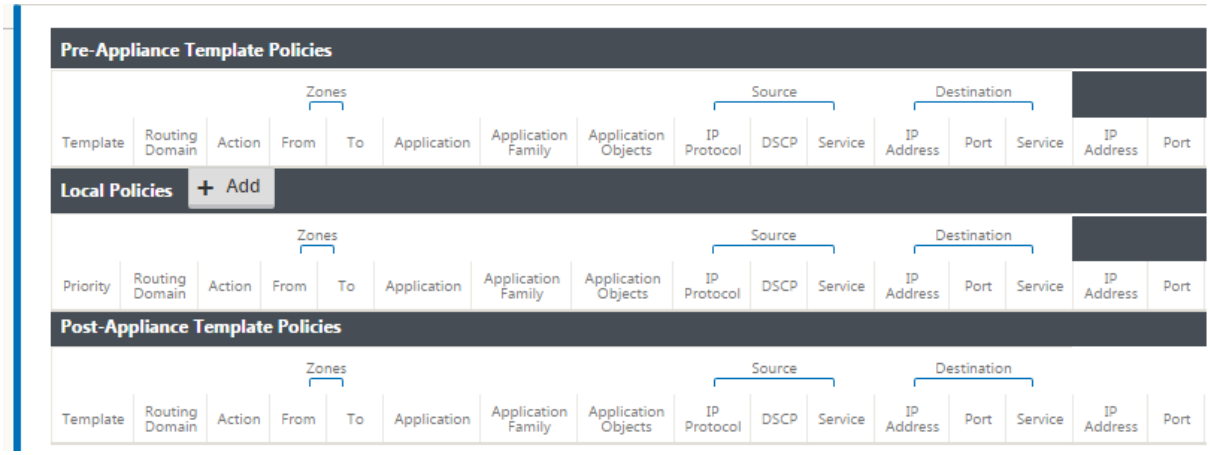
下のスクリーンショットは、割り当てられた仮想ネットワークインターフェイス（VNI）からの仮想 IP（VIP）のゾーンの継承を示しています。

IP Address / Prefix	Virtual Interface	Firewall Zone	Identity	Private	Security	Delete
172.16.187.11/24	VirtualInterface-1	Default_LAN_Zone	✓		Trusted	🗑
172.16.187.12/24	VirtualInterface-1	Default_LAN_Zone			Trusted	

ポリシー

May 10, 2021

ポリシーを使用すると、特定のトラフィックフローの許可、拒否、またはカウントおよび継続を行うことができます。SD-WAN ネットワークが拡大するにつれて、これらのポリシーを各サイトに個別に適用することは困難になります。この問題を解決するには、ファイアウォールポリシーテンプレートを使用してファイアウォールフィルターのグループを作成できます。ファイアウォールポリシーテンプレートは、ネットワーク内のすべてのサイトに適用することも、特定のサイトにのみ適用することもできます。これらのポリシーは、アプライアンス前のテンプレート・ポリシーまたはアプライアンス後のテンプレート・ポリシーとして順序付けられます。ネットワーク全体のアプライアンス前およびアプライアンス後のテンプレート・ポリシーは、どちらもグローバル・レベルで構成されます。ローカルポリシーは、[接続] の下のサイトレベルで構成され、その特定のサイトにのみ適用されます。



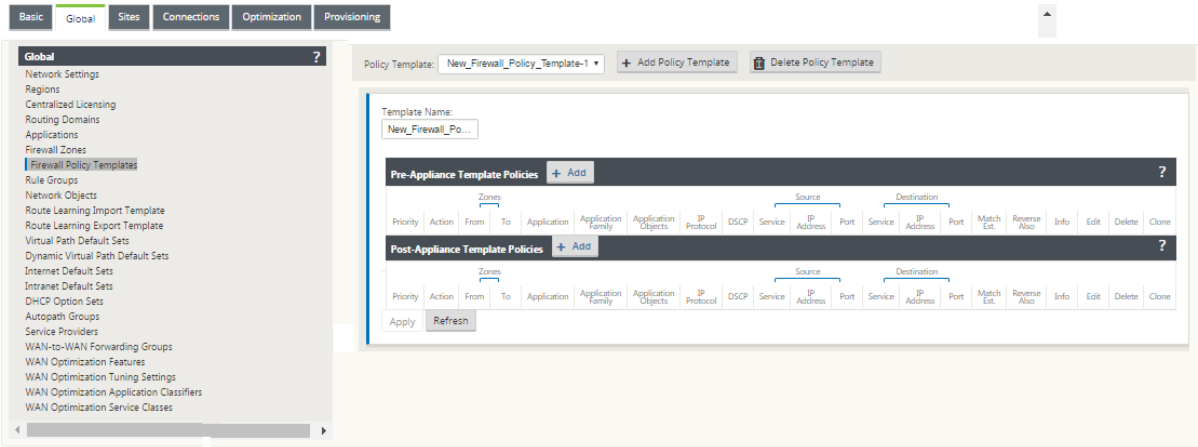
アプライアンスの前テンプレートポリシーは、ローカルサイトポリシーの前に適用されます。次に、ローカルサイトポリシーが適用されます。次に、アプライアンスポストテンプレートポリシーが適用されます。目標は、サイト固有のポリシーを適用する柔軟性を維持しながら、グローバルポリシーを適用できるようにすることで、構成プロセスを簡素化することです。

フィルタポリシー評価順序

1. Pre-templates —すべてのテンプレート「PRE」セクションからコンパイルされたポリシー。
2. Pre-Global —グローバル「PRE」セクションからコンパイルされたポリシー。
3. Local：アプライアンスレベルのポリシー。
4. [ローカル自動生成]：自動的にローカルに生成されたポリシー。
5. ポストテンプレート—すべてのテンプレート「POST」セクションからコンパイルされたポリシー。
6. ポストグローバル—グローバル「POST」セクションからコンパイルされたポリシー。

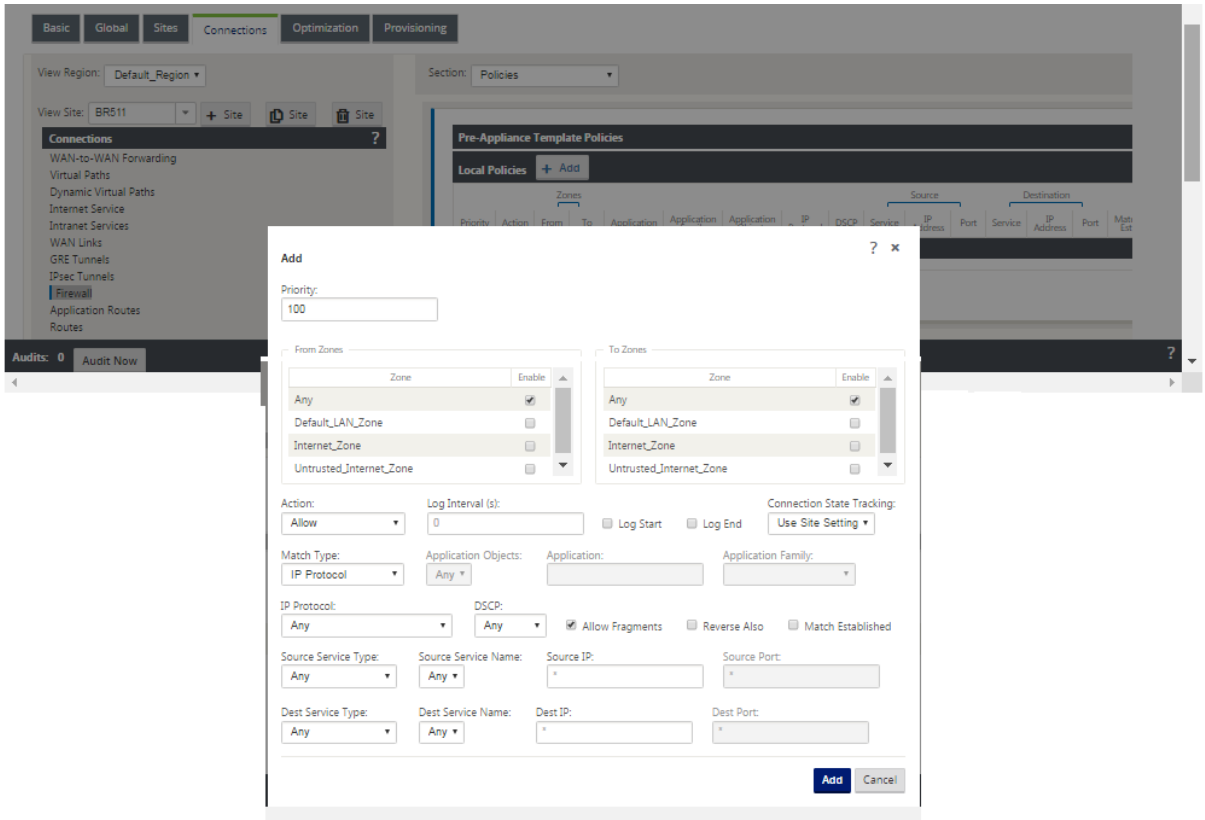
ポリシー定義-グローバルおよびローカル (サイト)

アプライアンス前およびアプライアンス後のテンプレート・ポリシーは、グローバル・レベルで構成できます。ローカルポリシーは、アプライアンスのサイトレベルで適用されます。



上のスクリーンショットは、SD-WAN ネットワークにグローバルに適用されるポリシーテンプレートを示しています。ネットワーク内のすべてのサイトにテンプレートを適用するには、[グローバル] > [ネットワーク設定**] > [**グローバルポリシーテンプレート**]** に移動し、特定のポリシーを選択します。サイトレベルでは、ポリシーテンプレートを追加したり、サイト固有のポリシーを作成できます。

ポリシーの特定の設定可能な属性は、以下のスクリーンショットに表示されます。これらの属性は、すべてのポリシーで同じです。



ポリシー属性

- **Priority**： 定義されたすべてのポリシー内でポリシーが適用される順序。優先順位の低いポリシーは、優先順位の高いポリシーの前に適用されます。
- **Zone**： フローには送信元ゾーンと宛先ゾーンがあります。
  - [**From Z** one]：ポリシーの送信元ゾーン。
  - **[** 宛先 **Z** one]：ポリシーの宛先ゾーン。
- **[Act** ion]：一致したフローに対して実行するアクション。
  - **Al** low：ファイアウォールを通過するフローを許可します。
  - [**D** rop]：パケットをドロップすることにより、ファイアウォールを通過するフローを拒否します。
  - **Reject**：ファイアウォールを通過するフローを拒否 し、プロトコル固有の応答を送信します。TCP はリセットを送信し、ICMP はエラーメッセージを送信します。
  - **Count and Continue**： このフローのパケット数とバイト数をカウントしてから、ポリシーリストを続けます。
- **Log Interval**： ポリシーに一致するパケットの数をファイアウォールログファイルまたは syslog サーバに記録する間隔（設定されている場合）。
  - **[Log Start**]：選択すると、新しいフローのログエントリが作成されます。
  - **Log End** —フローが削除されたときに、フローのデータをログに記録します。

> 注
>
> デフォルトの Log Interval の値である 0 は、ロギングがないことを意味します。

- [**Tr** ack]：ファイアウォールがフローの状態を追跡し、この情報を [**Monitoring**] > [**Firewall**] > [**Connections**] テーブルに表示できるようにします。フローがトラッキングされていない場合、状態は NOT_TRACKED と表示されます。以下のプロトコルに基づく状態追跡については、表を参照してください。[ファイアウォール] > [設定] > [詳細設定] > [既定の追跡] でサイトレベルで定義された設定を使用します。
  - **No Track**： フロー状態が有効になっていません。
  - [**Track**]：（このポリシーに一致した）フローの現在の状態を表示します。
- 「一致タイプ」(Match Type)-次のいずれかの一致タイプを選択します。
  - [**IP** プロトコル]：この一致タイプを選択した場合、フィルタが照合する IP プロトコルを選択します。オプションには、任意、TCP、UDP ICMP などがあります。
  - [アプリケーション] —この一致タイプを選択した場合は、このフィルタの一致基準として使用するアプリケーションを指定します。

- 「アプリケーションファミリ」—この一致タイプを選択した場合は、このフィルタの一致基準として使用するアプリケーションファミリを選択します。
- 「アプリケーション・オブジェクト」—この一致タイプを選択した場合は、このフィルタの一致基準として使用するアプリケーション・ファミリを選択します。

アプリケーション、アプリケーションファミリ、およびアプリケーションオブジェクトの詳細については、「アプリケーション分類」を参照してください。

- **DSCP**： ユーザが DSCP タグ設定を照合できるようにします。
- フラグメントを許 可：このフィルタポリシーに一致する IP フラグメントを許可します。

> 注
>
> ファイアウォールは、断片化されたフレームを再構成しません。

- **Re** verse Atho：ソースとデスティネーションの設定を逆にしたこのフィルタポリシーのコピーを自動的に追加します。
- **Match** 確立 済み：発信パケットが許可された接続の着信パケットを照合します。
- ソースサービスタイプ—SD-WAN サービスを参照して、ローカル（アプライアンス）、仮想パス、イントラネット、IPHost、またはインターネットがサービスタイプの例です。
- **IPHost** オプション -ファイアウォールの新しいサービスタイプで、SD-WAN アプリケーションによって生成されるパケットに使用されます。たとえば、SD-WAN の Web UI から ping を実行すると、SD-WAN 仮想 IP アドレスからパケットが送信されます。この IP アドレスのポリシーを作成する場合、ユーザーは IPHost オプションを選択する必要があります。
- ソース・サービス名：サービス・タイプに関連付けられたサービスの名前。たとえば、「ソース・サービス・タイプ」で仮想パスが選択されている場合、これは特定の仮想パスの名前になります。これは必ずしも必要ではなく、選択したサービスタイプによって異なります。
- 送信元 **IP** アドレス—フィルタが照合に使用する一般的な IP アドレスとサブネットマスク。
- **Source Port**： 特定のアプリケーションが使用するソース・ポート。
- デスティネーション・サービス・タイプ -SD-WAN サービスに関するサービス-ローカル（アプライアンス）、仮想パス、イントラネット、IPHost、またはインターネットがサービスタイプの例です。
- 宛先サービス名：サービス・タイプに関連付けられたサービスの名前。これは必ずしも必要ではなく、選択したサービスタイプによって異なります。
- 宛先 **IP** アドレス -フィルタが照合に使用する一般的な IP アドレスとサブネットマスク。
- 宛先ポート—特定のアプリケーションが使用する宛先ポート (TCP プロトコル用の HTTP 宛先ポート 80)。

track オプションは、フローの詳細を提供します。状態テーブルで追跡される状態情報を以下に示します。

トラックオプションのステートテーブル

一貫性のある状態は、ごくわずかです。

- **INIT-** 接続が作成されましたが、最初のパケットは無効です。
- **O_DENIED-** 接続を作成したパケットは、フィルタポリシーによって拒否されます。
- **R_DENIED-** 応答側からのパケットは、フィルタポリシーによって拒否されます。
- **NOT_TRACKED-** 接続はステートフルに追跡されませんが、それ以外の場合は許可されます。
- **CLOSED-** 接続がタイムアウトしたか、プロトコルによって閉じられました。
- **DELETED-** 接続は削除中です。DELETED 状態はほとんど見られません。

その他の状態はすべてプロトコル固有であり、ステートフルトラッキングを有効にする必要があります。

TCP は、次の状態を報告できます。

- **SYN_SENT** -最初の TCP SYN メッセージが表示されます。
- **SYN_SENT2** -双方向で認識される SYN メッセージ。SYN+ACK なし（別名同時オープン）。
- **SYN_ACK_RCVD** -SYN+ACK を受信しました。
- **ESTABLISHED-** 2 番目の ACK を受信し、接続は完全に確立されています。
- **FIN_WAIT** - 最初に見られた FIN メッセージ。
- **CLOSE_WAIT** -両方向に表示される FIN メッセージ。
- **TIME_WAIT** -両方向で最後に確認された ACK。接続は再度開くのを待って閉じられました。

その他すべての IP プロトコル（特に ICMP および UDP）には、次の状態があります。

- **NEW** -一方向で表示されるパケット。
- 確立 済み-両方向で認識されるパケット。

ネットワークアドレス変換 (NAT)

May 10, 2021

ネットワークアドレス変換 (NAT) は、IP アドレスの保存を実行して、登録された IPv4 アドレスの限られた数を維持します。これにより、未登録の IP アドレスを使用するプライベート IP ネットワークがインターネットに接続できるようになります。Citrix SD-WAN の NAT 機能は、プライベート SD-WAN ネットワークをパブリックインターネットに接続します。内部ネットワーク内のプライベートアドレスを、合法的なパブリックアドレスに変換します。また、NAT は、ネットワーク全体のアドレスを 1 つだけインターネットにアドバタイズし、内部ネットワーク全体を隠すことで、セキュリティを強化します。Citrix SD-WAN では、次の種類の NAT がサポートされます。

- スタティック 1 対 1 NAT
- ダイナミック NAT（PAT-ポートアドレス変換）
- ポートフォワーディングルールを使用したダイナミック NAT

> 注
>
> NAT 機能は、サイトレベルでのみ設定できます。NAT のグローバル構成（テンプレート）はありません。すべての NAT ポリシーは、ソース NAT（「SNAT」）変換から定義されます。対応する宛先 NAT（「DNAT」）規則は、ユーザーに対して自動的に作成されます。

静的 NAT

May 10, 2021

スタティック NAT は、SD-WAN ネットワーク内のプライベート IP アドレスまたはサブネットを、SD-WAN ネットワーク外のパブリック IP アドレスまたはサブネットに 1 対 1 のマッピングです。スタティック NAT を設定するには、内部 IP アドレスと変換先の外部 IP アドレスを手動で入力します。スタティック NAT は、ローカル、仮想パス、インターネット、イントラネット、およびルーティング間ドメインサービスに対して構成できます。

インバウンドおよびアウトバウンド NAT

接続の方向は、内側から外側、または外側から内側にできます。NAT ルールが作成されると、方向一致タイプに応じて両方の方向に適用されます。

- Inbound: 送信元アドレスは、サービスで受信したパケットに対して変換されます。宛先アドレスは、サービス上で送信されるパケットに対して変換されます。たとえば、インターネットサービスから LAN サービスへ—受信したパケット（インターネットから LAN へ）の場合、送信元 IP アドレスが変換されます。送信されたパケット（LAN からインターネットへ）では、宛先 IP アドレスが変換されます。
- Outbound: 宛先アドレスは、サービスで受信したパケットに対して変換されます。送信元アドレスは、サービス上で送信されるパケットに対して変換されます。たとえば、LAN サービスからインターネットサービスへ—送信されたパケット（LAN からインターネット）の場合、送信元 IP アドレスが変換されます。受信パケット（インターネットから LAN へ）の場合、宛先 IP アドレスが変換されます。

ゾーン派生

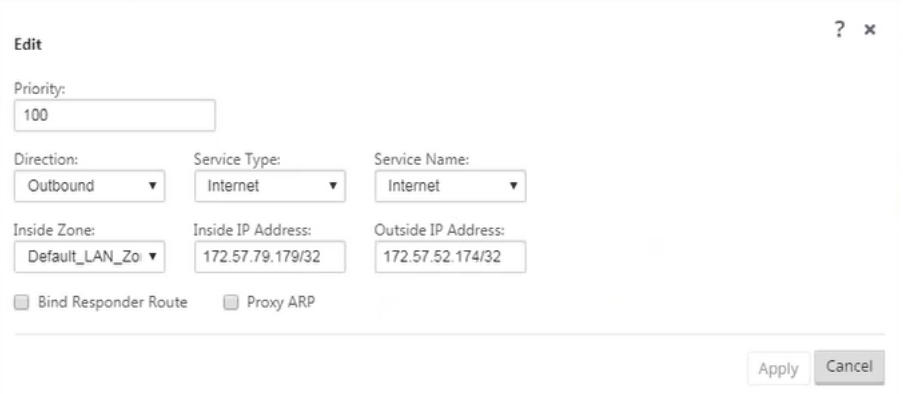
インバウンドまたはアウトバウンドトラフィックの送信元および宛先ファイアウォールゾーンは、同じであってはなりません。送信元と宛先の両方のファイアウォールゾーンが同じ場合、トラフィックに対して NAT は実行されません。

発信 NAT の場合、外部ゾーンはサービスから自動的に派生します。デフォルトでは、SD-WAN 上のすべてのサービスがゾーンに関連付けられます。たとえば、信頼できるインターネットリンク上のインターネットサービスは、信頼できるインターネットゾーンに関連付けられています。同様に、着信 NAT の場合、内部ゾーンはサービスから取得されます。

仮想パスサービスの場合、NAT ゾーンの導出が自動的に行われないため、内部ゾーンと外部ゾーンを手動で入力する必要があります。NAT は、これらのゾーンに属するトラフィックに対してのみ実行されます。仮想パスのサブネット内に複数のゾーンが存在する可能性があるため、仮想パスのゾーンは派生できません。

スタティック **NAT** ポリシーの設定

スタティック NAT ポリシーを設定するには、設定エディタで、[接続] > [ファイアウォール] > [スタティック **NAT** ポリシー] に移動します。

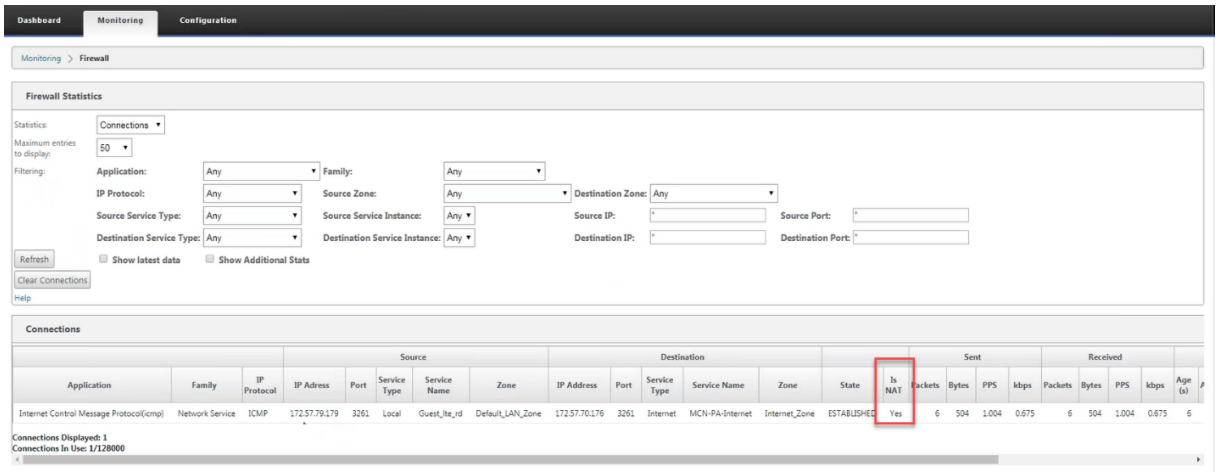


- **Priority**: 定義されたすべてのポリシー内でポリシーが適用される順序。優先順位の低いポリシーは、優先順位の高いポリシーの前に適用されます。
- 方向：仮想インターフェイスまたはサービスから見たトラフィックが流れている方向。インバウンドトラフィックまたはアウトバウンドトラフィックのいずれかになります。
- サービスタイプ：NAT ポリシーが適用される SD-WAN サービスタイプ。スタティック NAT の場合、サポートされるサービスの種類は、ローカル、仮想パス、インターネット、イントラネット、およびインタールーティングドメインサービスです。
- サービス名: サービスタイプに対応する構成済みのサービス名を選択します。
- **Inside Zone**: 変換を許可するために、パケットの送信元となる必要がある内部ファイアウォールゾーンのマッチタイプ。
- **Outside Zone**: 変換を許可するために、パケットの送信元となる必要がある外部ファイアウォールゾーンのマッチタイプ。
- 内部 **IP** アドレス：一致基準が満たされた場合に変換する必要がある内部 IP アドレスおよびプレフィクス。
- 外部 **IP** アドレス：一致基準が満たされた場合に内部 IP アドレスが変換される外部 IP アドレスおよびプレフィクス。
- 応答側ルートのバインド: 非対称ルーティングを回避するために、応答トラフィックが受信されたサービスと同じサービスで送信されるようにします。

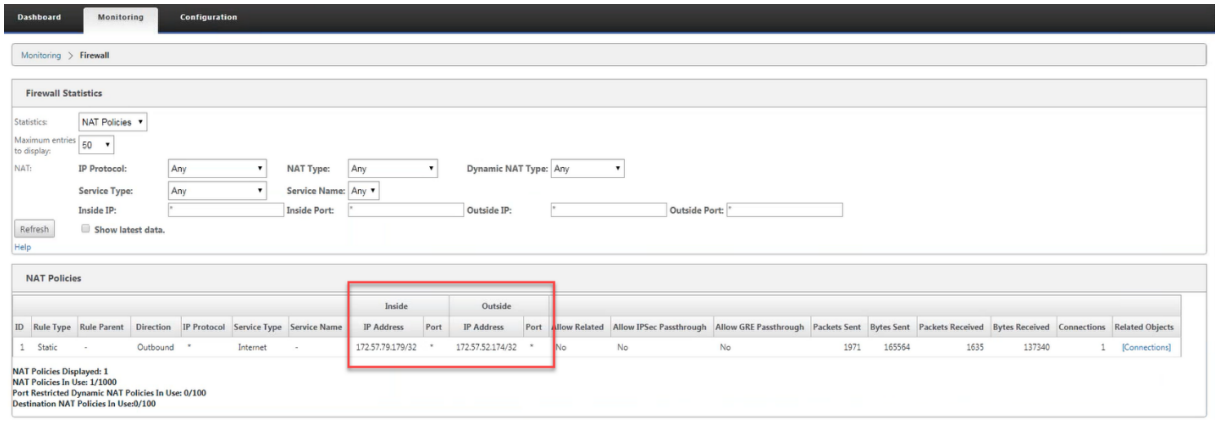
- プロキシ **ARP**: アプライアンスが外部 IP アドレスに対するローカル ARP 要求に応答することを保証します。

監視

NAT を監視するには、[監視] > [ファイアウォール統計] > [接続] に移動します。接続では、NAT が完了しているかどうかを確認できます。

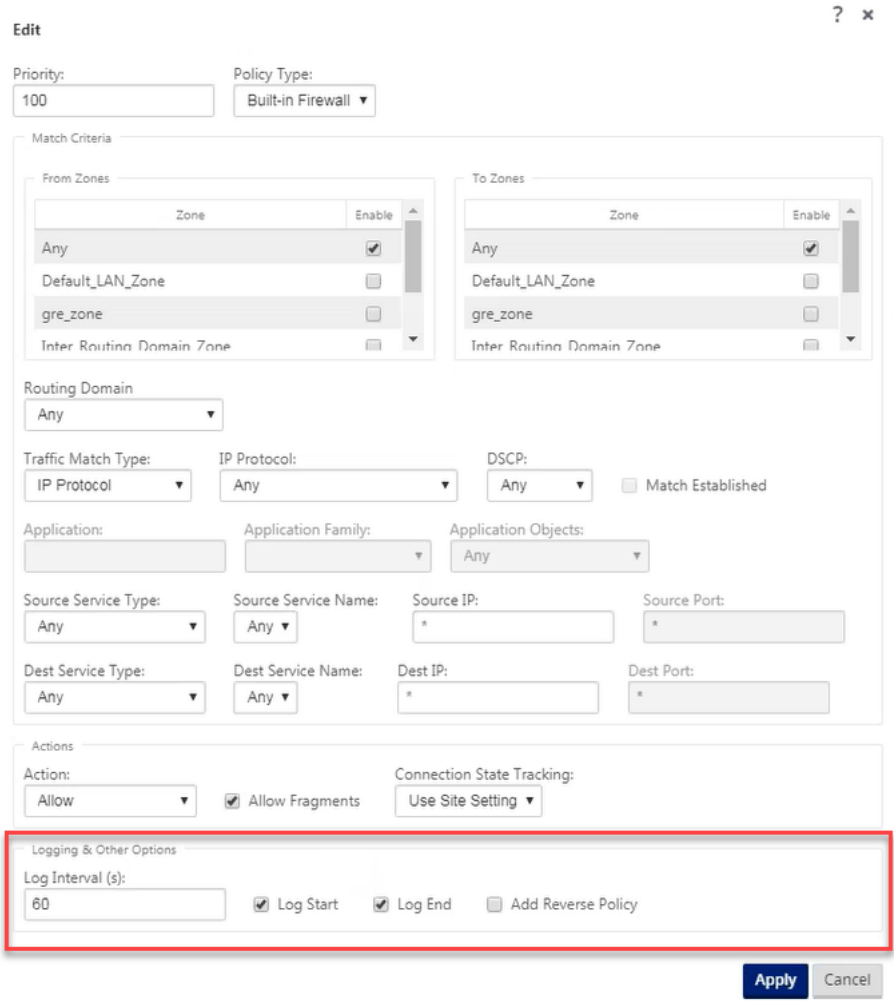


内部 IP アドレスと外部 IP アドレスのマッピングをさらに確認するには、[関連オブジェクト] の [ルート後 **NAT**] をクリックするか、[モニタリング] > [ファイアウォール統計] > [**NAT** ポリシー] に移動します。

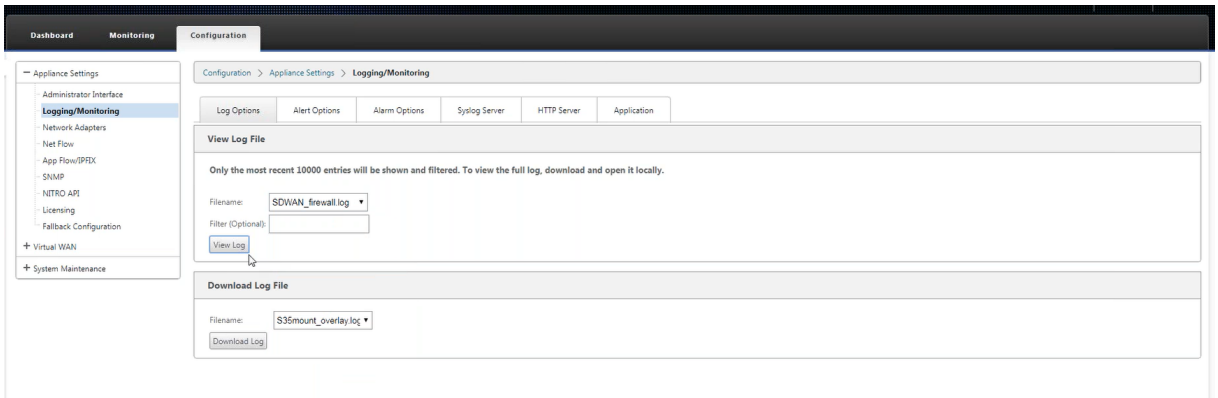


ログ

NAT に関連するログは、ファイアウォールログで表示できます。NAT のログを表示するには、NAT ポリシーに一致するファイアウォールポリシーを作成し、ファイアウォールフィルタでロギングが有効になっていることを確認します。



[ログ/監視] > [ログオプション] に移動し、[**SDWAN_firewal.log**] を選択し、[ログの表示] をクリックします。



NAT 接続の詳細がログファイルに表示されます。


```
2020-05-11T10:14:19.861597+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.79.179-->172.57.70.176 (ID:10743)
2020-05-11T10:15:19.166668+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.70.176-->172.57.79.179 (ID:10743)
2020-05-11T10:15:19.986378+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.79.179-->172.57.70.176 (ID:10743)
2020-05-11T10:15:44.749959+0000 INFO    conn_clear_all@forward/firewall/connection.c:8704      Removed 1 Connections
2020-05-11T10:15:44.750109+0000 INFO    t2_firewall_monitor.pl   NAT Connection DELETED for (Routing Domain Default_RoutingDomain) ICMP 172.57.70.176-->172.57.79.179 (ID:10743)
2020-05-11T10:16:16.981504+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 21 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.70.176-->172.57.79.179 (ID:10743)
2020-05-11T10:16:20.108292+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 21 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.79.179-->172.57.70.176 (ID:10743)
2020-05-11T10:16:21.299055+0000 INFO    t2_firewall_monitor.pl   NAT Connection CREATED for (Routing Domain Default_RoutingDomain) ICMP 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:16:22.112286+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 1 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:16:22.112650+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 1 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:17:21.768837+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:17:22.255262+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:18:22.235843+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 56 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:18:22.371729+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:19:21.353441+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:19:22.483705+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:20:22.374898+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:20:22.598370+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:21:20.464917+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:21:22.716765+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:22:20.474915+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 50 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:22:22.846123+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 54 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:23:09.456757+0000 INFO    t2_firewall_monitor.pl   NAT Connection DELETED for (Routing Domain Default_RoutingDomain) ICMP 172.57.79.179-->172.57.70.176 (ID:3261)
```

ダイナミック **NAT**

May 10, 2021

ダイナミック NAT は、SD-WAN ネットワーク内のプライベート IP アドレスまたはサブネットを、SD-WAN ネットワーク外のパブリック IP アドレスまたはサブネットに多対 1 のマッピングです。LAN セグメント内の信頼できる (内部) IP アドレス経由の異なるゾーンおよびサブネットからのトラフィックは、単一のパブリック (外部) IP アドレス経由で送信されます。

ダイナミック **NAT** タイプ

ダイナミック NAT は、IP アドレス変換とともにポートアドレス変換（PAT）を行います。ポート番号は、どのトラフィックがどの IP アドレスに属しているかを識別するために使用されます。すべての内部プライベート IP アドレスに 1 つのパブリック IP アドレスが使用されますが、各プライベート IP アドレスには異なるポート番号が割り当てられます。PAT は、1 つのパブリック IP アドレスを使用して複数のホストがインターネットに接続できるようにする費用対効果の高い方法です。

- ポート制限：ポート制限 NAT は、内部 IP アドレスとポートのペアに関連するすべての変換に同じ外部ポートを使用します。このモードは、通常、インターネット P2P アプリケーションを許可するために使用されます。
- 対称：対称 NAT は、内部 IP アドレス、内部ポート、外部 IP アドレス、および外部ポートタプルに関連するすべての変換に同じ外部ポートを使用します。通常、このモードは、セキュリティを強化したり、NAT セッションの最大数を拡張するために使用されます。

インバウンドおよびアウトバウンド **NAT**

接続の方向は、内側から外側、または外側から内側にできます。NAT ルールが作成されると、方向一致タイプに応じて両方の方向に適用されます。

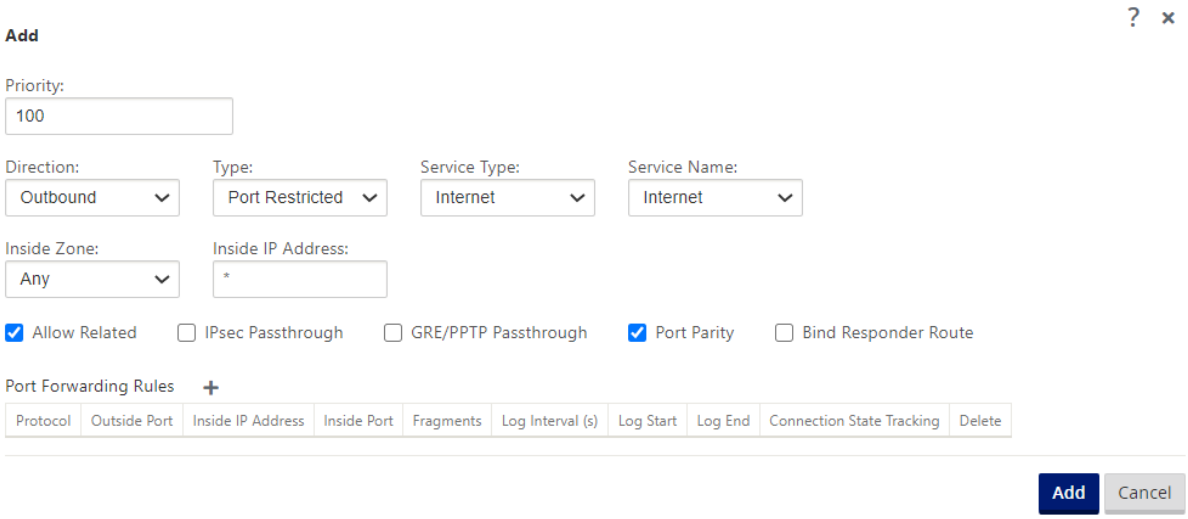
- **Outbound**: サービスで受信したパケットについて、宛先アドレスが変換されます。送信元アドレスは、サービス上で送信されるパケットに対して変換されます。発信ダイナミック NAT は、ローカル、インターネット、

イントラネット、およびルーティング間ドメインサービスでサポートされます。インターネットサービスやイントラネットサービスなどの WAN サービスの場合、構成された WAN リンク IP アドレスが外部 IP アドレスとして動的に選択されます。ローカルおよびインタールーティングドメインサービスの場合は、外部 IP アドレスを指定します。Outside ゾーンは、選択したサービスから取得されます。アウトバウンドダイナミック NAT の一般的な使用例は、LAN 内の複数のユーザーが、単一のパブリック IP アドレスを使用してインターネットに安全にアクセスできるようにすることです。

- **Inbound**: サービスで受信したパケットについて、送信元アドレスが変換されます。宛先アドレスは、サービス上で送信されるパケットに対して変換されます。インバウンドダイナミック NAT は、インターネットやイントラネットなどの WAN サービスではサポートされません。同じことを示す明示的な監査エラーがあります。インバウンドダイナミック NAT は、ローカルおよびインタールーティングドメインサービスでのみサポートされます。変換先の外部ゾーンと外部 IP アドレスを指定します。インバウンドダイナミック NAT の一般的な使用例は、外部ユーザーがプライベートネットワークでホストされている電子メールまたはウェブサーバーにアクセスできるようにすることです。

ダイナミック **NAT** ポリシーの設定

ダイナミック NAT ポリシーを設定するには、構成エディタで、[接続] > [ファイアウォール] > [ダイナミック **NAT** ポリシー] に移動します。



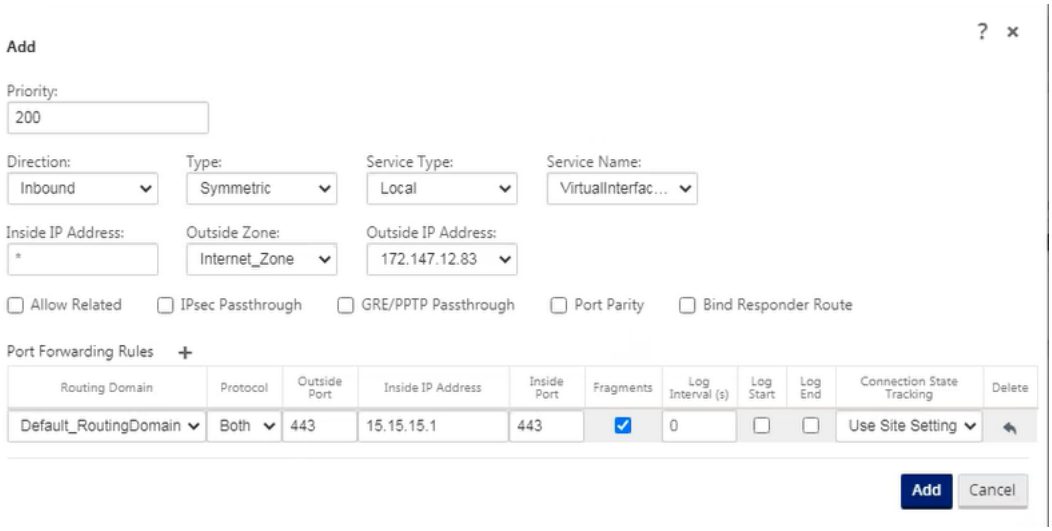
- **Priority**: 定義されたすべてのポリシー内でポリシーが適用される順序。優先順位の低いポリシーは、優先順位の高いポリシーの前に適用されます。
- 方向: 仮想インターフェイスまたはサービスから見たトラフィックが流れている方向。インバウンドトラフィックまたはアウトバウンドトラフィックのいずれかになります。
- タイプ: 実行するダイナミック NAT のタイプ、ポート制限、または対称。
- サービスタイプ: ダイナミック NAT ポリシーが適用される SD-WAN サービスタイプ。インバウンドダイナミック NAT は、ローカルおよびインタールーティングドメインサービスでサポートされます。発信ダイナミック NAT は、ローカル、インターネット、イントラネット、およびルーティングドメインサービスでサポートさ

れます。

- サービス名: サービスタイプに対応する構成済みのサービス名を選択します。
- **Inside Zone**: 変換を許可するために、パケットの送信元となる必要がある内部ファイアウォールゾーンのマッチタイプ。
- [**Outside Zone**]: インバウンドトラフィックの場合、変換を許可するためにパケットの送信元となる必要がある外部ファイアウォールゾーンのマッチタイプを指定します。
- 内部 **IP** アドレス: 一致基準が満たされた場合に変換する必要がある内部 IP アドレスおよびプレフィクス。「*」と入力して、内部 IP アドレスを指定します。
- 外部 **IP** アドレス: 一致基準が満たされた場合に内部 IP アドレスが変換される外部 IP アドレスおよびプレフィクス。インターネットサービスおよびイントラネットサービスを使用する発信トラフィックでは、構成された WAN リンク IP アドレスが外部 IP アドレスとして動的に選択されます。
- **[** 関連を許可]: ルールに一致するフローに関連するトラフィックを許可します。たとえば、ポリシーに一致する特定のフローに関連する ICMP リダイレクション（フローに関連する何らかのタイプのエラーがある場合）。
- **IPsec** パススルー: IPSec (AH/ESP) セッションの変換を許可します。
- **GRE/PPTP** パススルー: GRE/PPTP セッションの変換を許可します。
- ポートパリティ: 有効の場合、NAT 接続の外部ポートはパリティを維持します（内部ポートが偶数であっても、外部ポートが奇数の場合は奇数）。
- 応答側ルートのバインド: 非対称ルーティングを回避するために、応答トラフィックが受信されたサービスと同じサービスで送信されるようにします。

ポートフォワーディング

ポートフォワーディングを使用したダイナミック NAT では、特定のトラフィックを定義済みの IP アドレスにポート転送できます。これは、通常、Web サーバなどの内部ホストで使用されます。ダイナミック NAT を設定したら、ポートフォワーディングポリシーを定義できます。IP アドレス変換用のダイナミック NAT を設定し、外部ポートを内部ポートにマッピングするポートフォワーディングポリシーを定義します。ダイナミック NAT ポートフォワーディングは、通常、リモートホストがプライベートネットワーク上のホストまたはサーバーに接続できるようにするために使用されます。より詳細なユースケースについては、Citrix SD-WAN ダイナミック NAT の説明を参照してください。



- プロトコル: TCP、UDP、またはその両方。
- 外部ポート: 内部ポートにポート転送される外部ポート。
- 内部 **IP** アドレス: 一致するパケットを転送する内部アドレス。
- 内部ポート: 外部ポートが転送される内部ポート。
- [フラグメント] : フラグメント化されたパケットの転送を許可します。
- ログ間隔: ポリシーに一致するパケット数を syslog サーバにロギングする間隔（秒）。
- ログ開始: 選択すると、新しいフローの新しいログエントリが作成されます。
- ログ終了: フローが削除されたときにフローのデータをログに記録します。

  > 注
  >
  > デフォルトの Log Interval の値である 0 は、ロギングがないことを意味します。

- 追跡: 規則に一致する TCP、UDP、および ICMP パケットに対して、双方向接続状態トラッキングが実行されます。この機能は、非対称ルーティングまたはチェックサムの失敗、プロトコル固有の検証のために、非合法に見えるフローをブロックします。状態の詳細は、[監視] > [ファイアウォール] > [接続] の下に表示されます。
- [トラッキングなし]: ルールに一致するパケットでは、双方向接続状態トラッキングは実行されません。

すべてのポートフォワーディングルールには、親 NAT ルールがあります。外部 IP アドレスは、親 NAT ルールから取得されます。

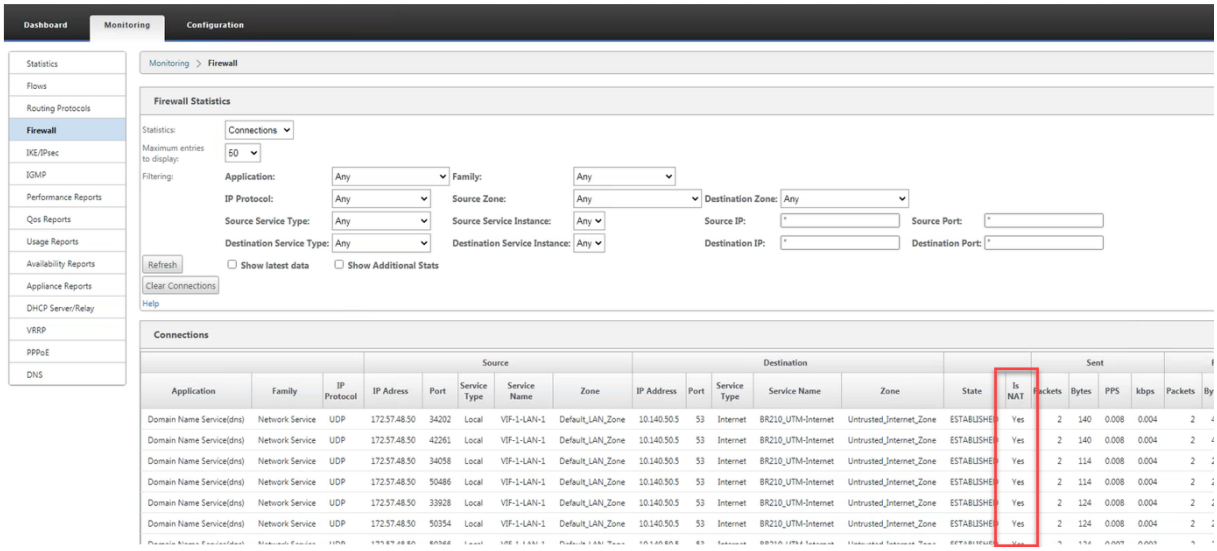
自動作成されたダイナミック **NAT** ポリシー

インターネットサービスのダイナミック NAT ポリシーは、次の場合に自動的に作成されます。

- 信頼できないインターフェイス（WAN リンク）でのインターネットサービスの設定
- 単一の WAN リンク上のすべてのルーティングドメインに対するインターネットアクセスを有効にします。詳しくは、「ファイアウォールセグメンテーションの構成」を参照してください。
- SD-WAN での DNS フォワーダーまたは DNS プロキシの設定詳しくは、「ドメイン・ネーム・システム」を参照してください。

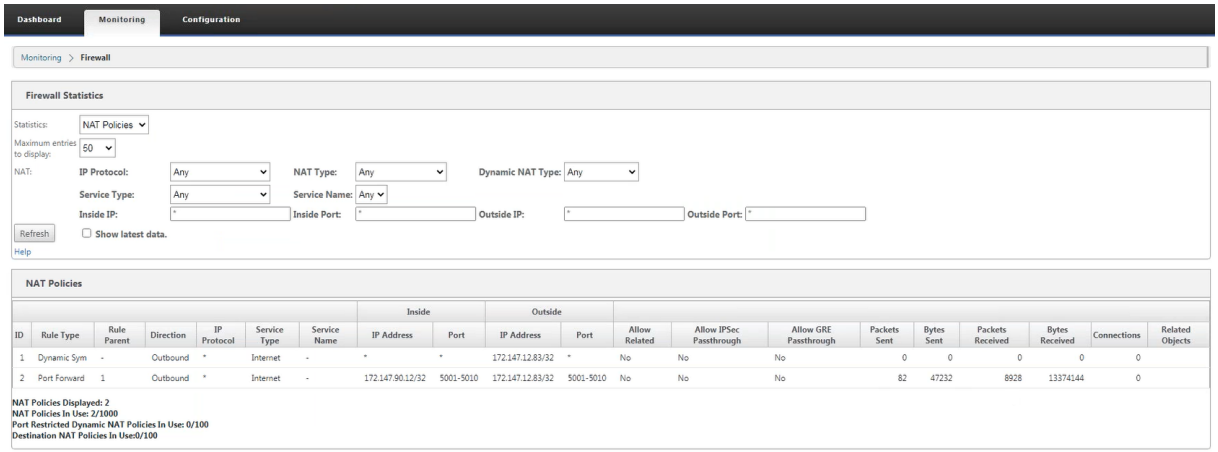
監視

ダイナミック NAT を監視するには、[監視] > [ファイアウォール統計] > [接続] に移動します。接続では、NAT が完了しているかどうかを確認できます。

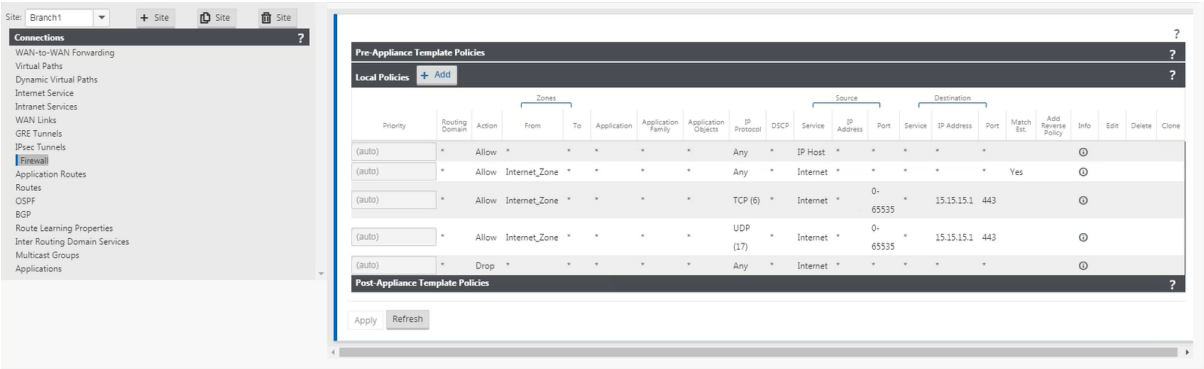


内部 IP アドレスと外部 IP アドレスのマッピングをさらに確認するには、[関連オブジェクト] の [ルーティング前 **NAT**] または [ポストルート **NAT**] をクリックするか、[モニタリング] > [ファイアウォール統計] > [**NAT** ポリシー] に移動します。

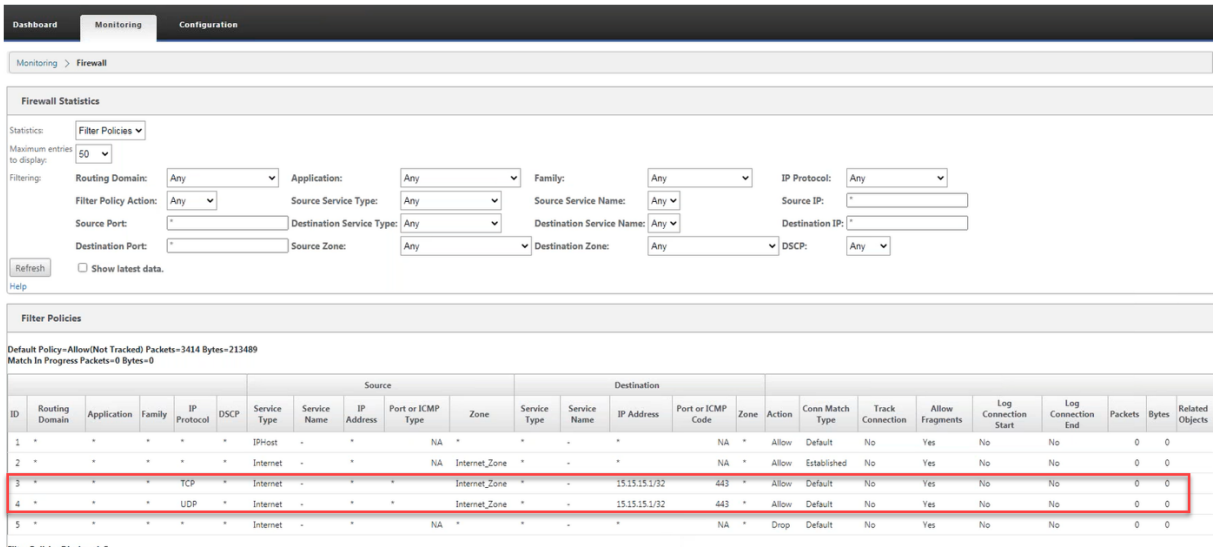
次のスクリーンショットは、タイプシンメトリックダイナミック NAT 規則とそれに対応するポート転送規則の統計を示しています。



ポート転送規則が作成されると、対応するファイアウォール規則も作成されます。

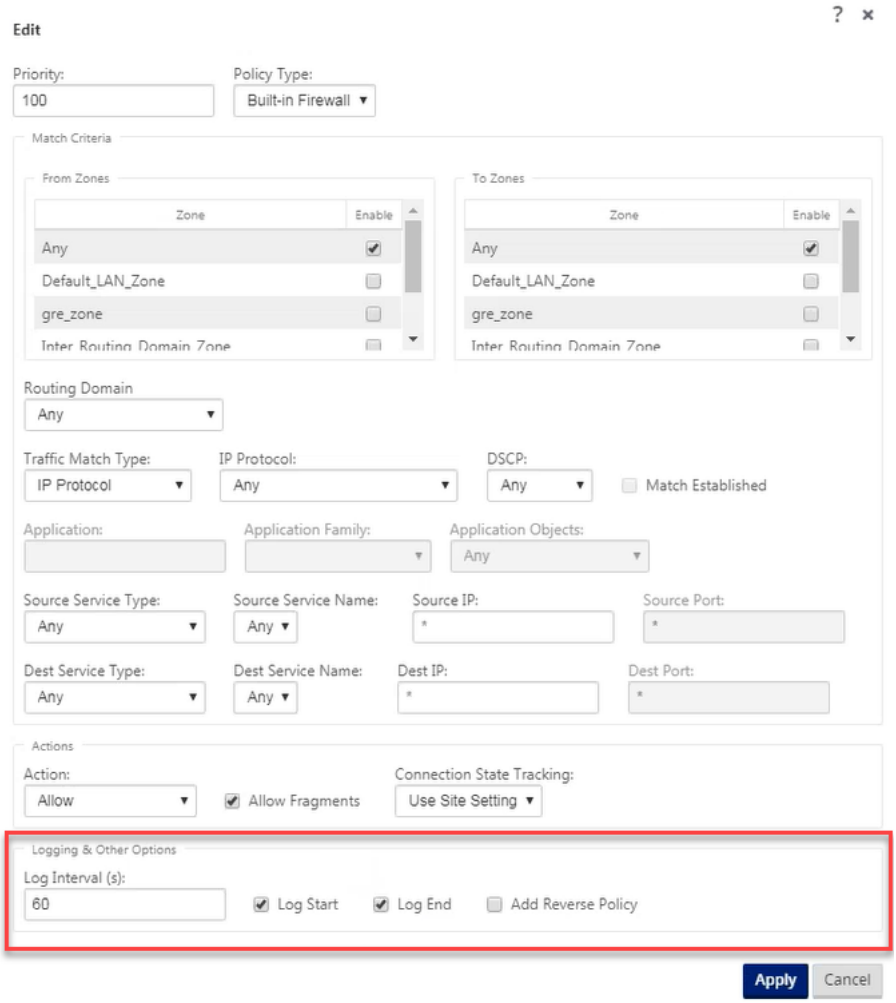


[監視] > [ファイアウォール統計] > [フィルタポリシー] に移動すると、フィルタポリシーの統計を表示できます。

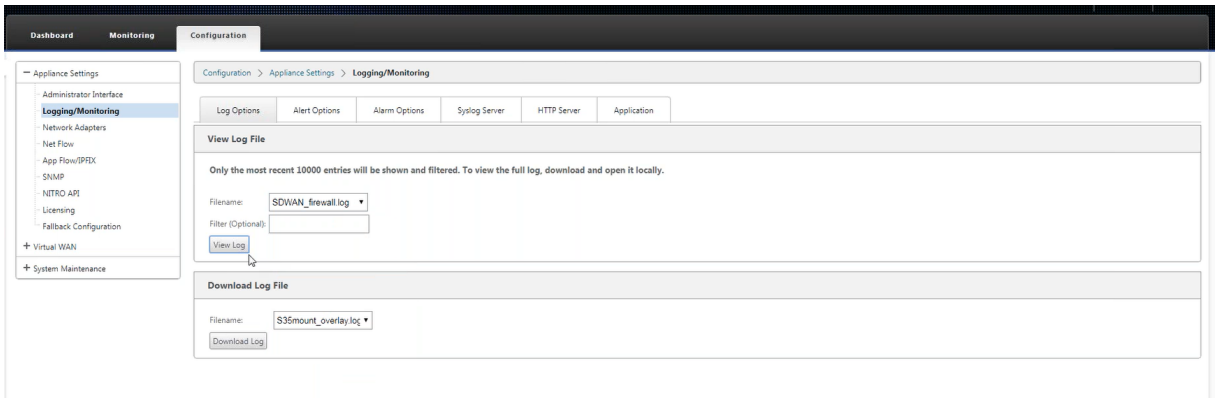


ログ

NAT に関連するログは、ファイアウォールログで表示できます。NAT のログを表示するには、NAT ポリシーに一致するファイアウォールポリシーを作成し、ファイアウォールフィルタでロギングが有効になっていることを確認します。



[ログ/監視] > [ログオプション] に移動し、[**SDWAN_firewal.log**] を選択し、[ログの表示] をクリックします。



NAT 接続の詳細がログファイルに表示されます。


```
2020-05-11T10:14:19.861597+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.79.179-->172.57.70.176 (ID:10743)
2020-05-11T10:15:19.166668+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.70.176-->172.57.79.179 (ID:10743)
2020-05-11T10:15:19.986378+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.79.179-->172.57.70.176 (ID:10743)
2020-05-11T10:15:44.749959+0000 INFO    conn_clear_all@forward/firewall/connection.c:8704:      Removed 1 Connections
2020-05-11T10:15:44.750109+0000 INFO    t2_firewall_monitor.pl   NAT Connection DELETED for (Routing Domain Default_RoutingDomain) ICMP 172.57.70.176-->172.57.79.179 (ID:10743)
2020-05-11T10:16:16.981504+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 21 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.70.176-->172.57.79.179 (ID:10743)
2020-05-11T10:16:20.108292+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 21 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.79.179-->172.57.70.176 (ID:10743)
2020-05-11T10:16:21.299055+0000 INFO    t2_firewall_monitor.pl   NAT Connection CREATED for (Routing Domain Default_RoutingDomain) ICMP 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:16:22.112286+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 1 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:16:22.112650+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 1 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:17:21.768837+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:17:22.255262+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:18:22.235843+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 56 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:18:22.371729+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:19:21.353441+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:19:22.483705+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:20:22.374898+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:20:22.598370+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:21:20.464917+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:21:22.716765+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:22:20.474915+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 50 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:22:22.846123+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 54 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:23:09.456757+0000 INFO    t2_firewall_monitor.pl   NAT Connection DELETED for (Routing Domain Default_RoutingDomain) ICMP 172.57.79.179-->172.57.70.176 (ID:3261)
```

仮想 **WAN** サービスの構成

May 10, 2021

Citrix SD-WAN 構成では、Citrix SD-WAN ネットワークのトポロジーについて説明し、定義します。SD-WAN ネットワークを展開する前に、仮想 WAN 構成を定義する必要があります。これを行うには、MCN アプライアンスの Citrix SD-WAN 管理 Web インターフェイスで構成エディターを使用します。

セキュリティと暗号化

SD-WAN の暗号化の有効化（仮想パス用）はオプションです。この機能の設定手順については、仮想 WAN セキュリティおよび暗号化の有効化と設定（オプション）を参照してください。

暗号化が有効な場合、SD-WAN は高度暗号化標準（AES）を使用して、仮想パスを通るトラフィックをセキュリティで保護します。AES 128 ビット暗号と 256 ビットの暗号の両方（キーサイズ）は SD-WAN アプライアンスでサポートされており、設定可能なオプションです。管理制御ノード (MCN) の管理 Web インターフェイスの構成エディタを使用して、これらの暗号化オプションおよびその他の暗号化オプションを選択、有効化、および構成できます。設定を変更し、SD-WAN ネットワーク全体に変更を配布するには、MCN に対する管理アクセス権が必要です。MCN がセキュリティで保護されると、暗号化設定とその配布もセキュリティで保護されます。

サイト間の認証は、仮想 WAN 構成で機能します。
ネットワーク構成には、各サイトの秘密キーがあります。各仮想パスについて、ネットワーク構成は、仮想パスの各端にあるサイトの秘密キーを組み合わせて、キーを生成します。仮想パスの最初のセットアップ後に発生する最初のキー交換は、その結合されたキーを使用してパケットを暗号化および復号化する能力に依存します。

仮想 **WAN** サービスの有効化

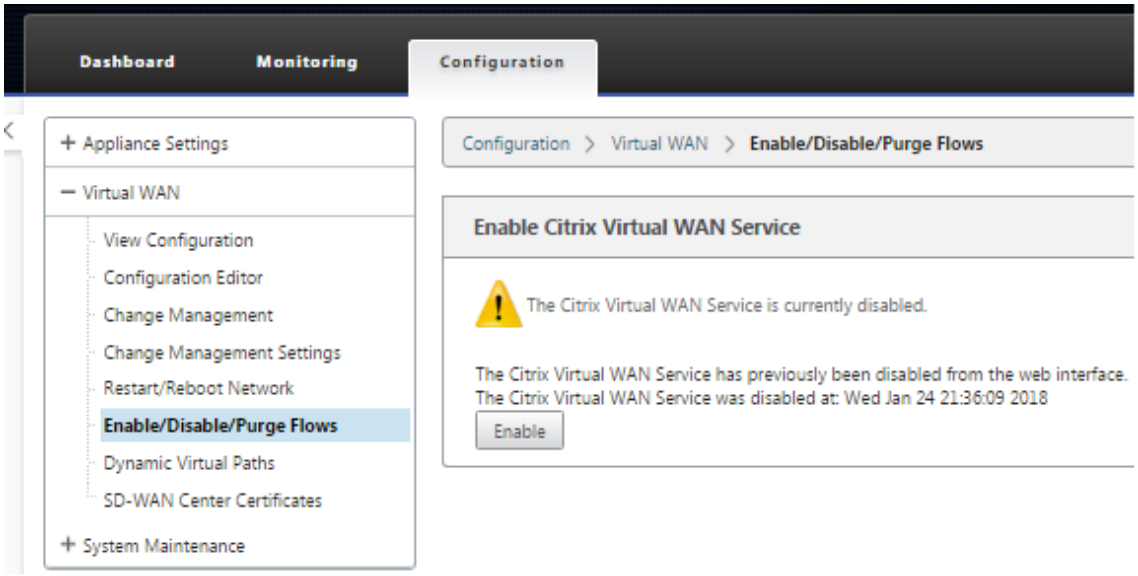
これが初期インストールおよび構成の場合、最後の手順として、ネットワーク内の各 SD-WAN アプライアンスで Virtual WAN サービスを手動で有効にする必要があります。サービスを有効にすると、仮想 WAN デーモンが有効になり、起動します。

> 注
>
> 既存の展開を再構成する場合、MCN は更新された Appliance Packages をクライアントサイトに配布するときに、サービスを自動的に有効にします。この場合、この最後のステップはスキップできます。

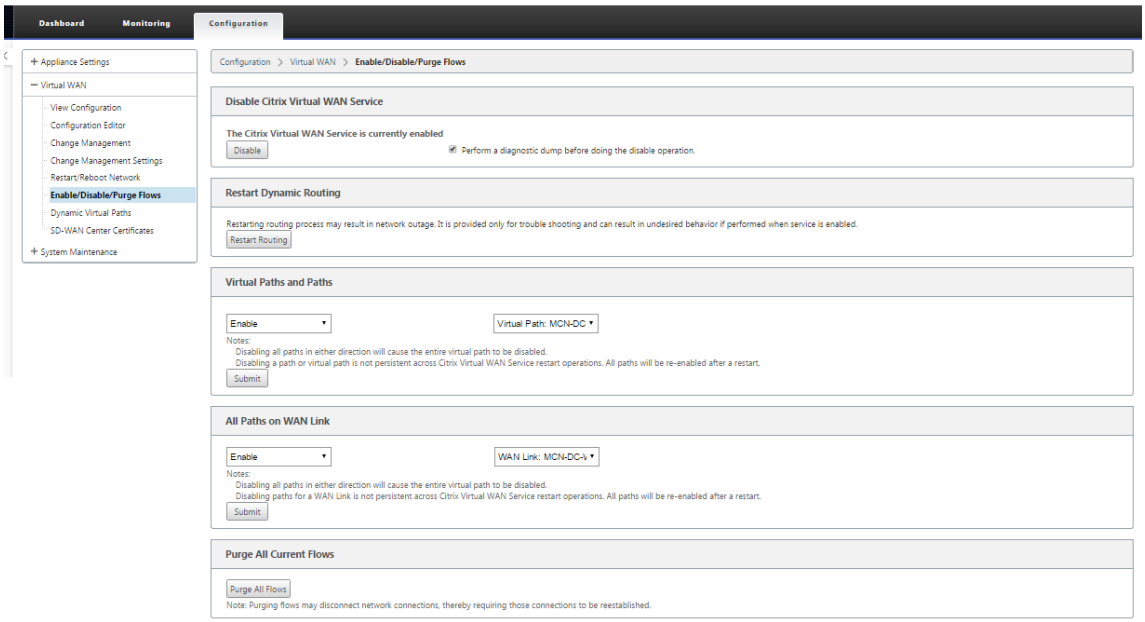
アプライアンスで仮想 WAN サービスを手動で有効にするには、次の手順を実行します。

1. アクティブ化するアプライアンスの管理 Web Interface にログインします。
2. [構成] タブを選択します。
3. ナビゲーションペインで、Virtual WAN ブランチを開き、[フローの有効化/無効化/パージ] を選択します。

   仮想 WAN サービスを無効にすると、次に示すように [仮想 WAN サービスの有効化] ページが表示されます。サービスがすでに有効になっている場合は、「フローの有効化/無効化/パージ・フロー」ページが表示されます。



4. [有効] をクリックします。これにより、サービスが有効になり、「フローの有効化」、「無効化」、「パージ」ページが表示されます。



Virtual WAN サービスを有効にすると、その旨を示すステータスメッセージがページの上部セクションに表示されます。

> 注
>
> このページでは、ネットワーク内の特定のパスと仮想パスを有効/無効にするオプション、およびすべてのフローを消去するオプションも表示されます。

これで、MCN およびブランチサイトクライアントアプライアンスでの SD-WAN のインストールとアクティベーションが完了します。[Monitoring] ページを使用して、アクティブ化を確認し、既存または潜在的な構成問題を診断できます。

ファイアウォールセグメンテーションの構成

May 10, 2021

Virtual Route Forwarding（VRF; バーチャルルートフォワーディング）ファイアウォールセグメンテーションでは、複数のルーティングドメインが共通のインターフェイスを介してインターネットにアクセスでき、各ドメインのトラフィックは他のドメインのトラフィックから分離されます。たとえば、従業員とゲストは、互いのトラフィックにアクセスすることなく、同じインターフェイスを介してインターネットにアクセスできます。

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

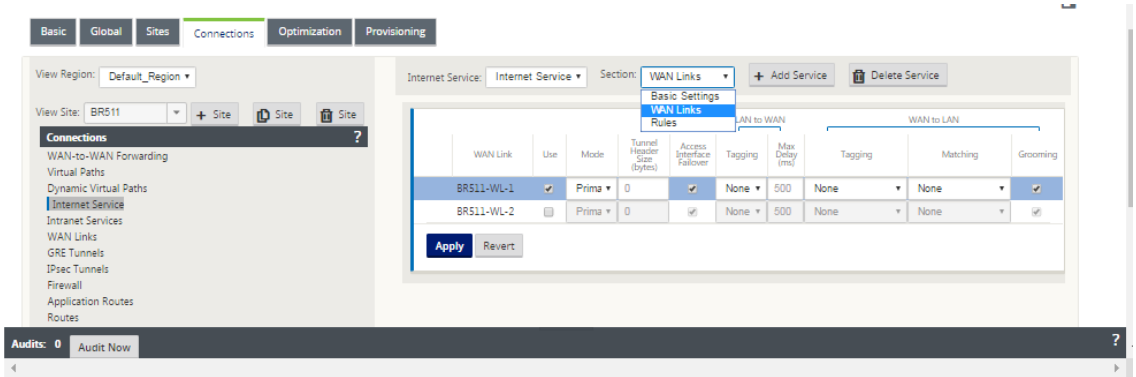
- 有効にすると、この機能はすべてのルーティングドメインに適用されます。

また、複数のアクセスインターフェイスを作成して、個別のパブリック向け IP アドレスを収容することもできます。どちらのオプションでも、各ユーザグループに必要なセキュリティが提供されます。

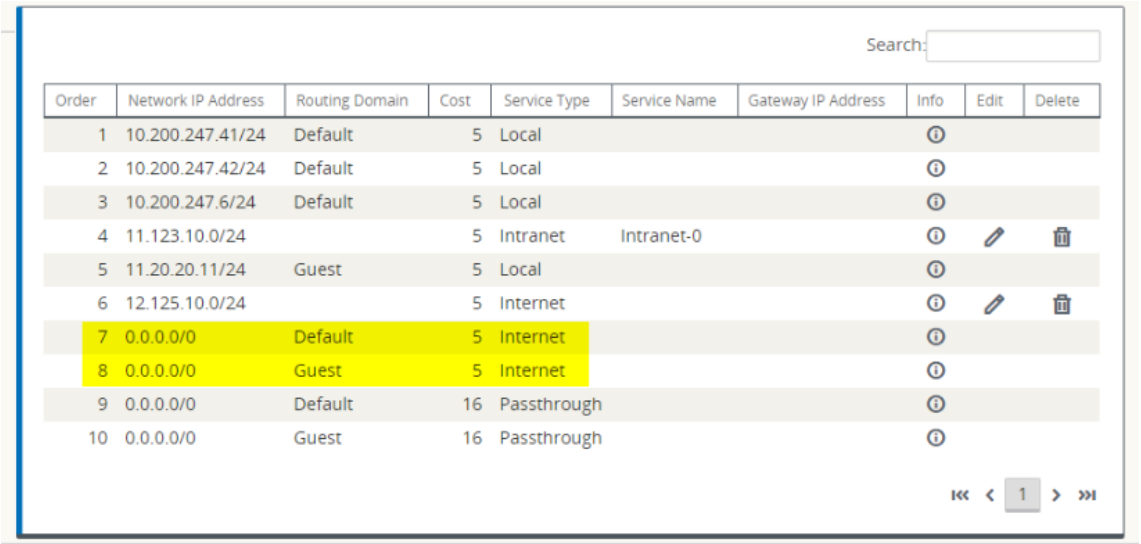
> 注
>
> 詳細については、「VRF の設定」を参照してください。

すべてのルーティングドメインに対してインターネットサービスを構成するには、次の手順を実行します。

1. サイトのインターネットサービスを作成します。[接続] > [リージョンの表示] > [サイトの表示] [サイト名] > [インターネットサービス] **> [**セクション**] > [WAN** リンク] に移動し、[WAN リンク] で [使用] チェックボックスをオンにします。

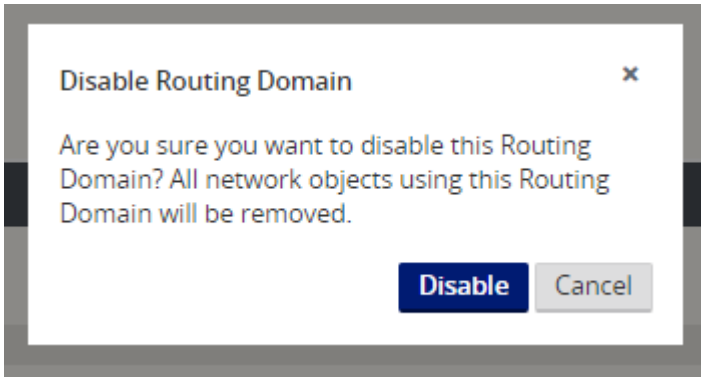


> 注
>
> [接続] > [リージョンの表示] **> [**** サイトの表示 **] >[サイト名]>**[**ルート**]** の下に、ルーティングドメインごとに 1 つずつ 0.0.0.0/0 ルートが追加されていることがわかります。

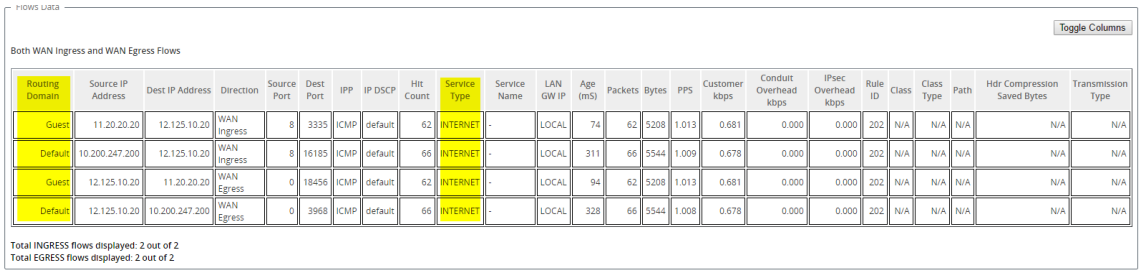


MCN ですべてのルーティングドメインを有効にする必要はなくなりました。

2. MCN でルーティングドメインを無効にすると、ドメインがブランチサイトで使用されている場合は、次のメッセージが表示されます。



3. 各ルーティングドメインがインターネットサービスを使用していることを確認するには、**[**Monitor**] > [Flows] の下の Web 管理インターフェイスの [Flows] テーブルにある [Routing Domain] 列を確認します。**



Flows Data

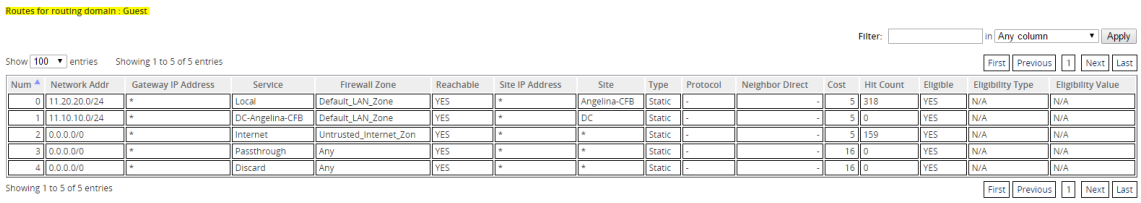
Toggle Columns

Both WAN Ingress and WAN Egress Flows

Routing Domain	Source IP Address	Dest IP Address	Direction	Source Port	Dest Port	IPP	IP DSCP	Hit Count	Service Type	Service Name	LAN GW IP	Age (mS)	Packets	Bytes	PPS	Customer kbps	Conduit Overhead kbps	IPsec Overhead kbps	Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type
Guest	11.20.20.20	12.125.10.20	WAN Ingress	8	3335	ICMP	default	62	INTERNET	-	LOCAL	74	62	5208	1.013	0.681	0.000	0.000	202	N/A	N/A	N/A	N/A	N/A
Default	10.200.247.200	12.125.10.20	WAN Ingress	8	16185	ICMP	default	66	INTERNET	-	LOCAL	311	66	5544	1.009	0.678	0.000	0.000	202	N/A	N/A	N/A	N/A	N/A
Guest	12.125.10.20	11.20.20.20	WAN Egress	0	18456	ICMP	default	62	INTERNET	-	LOCAL	94	62	5208	1.013	0.681	0.000	0.000	202	N/A	N/A	N/A	N/A	N/A
Default	12.125.10.20	10.200.247.200	WAN Egress	0	3968	ICMP	default	66	INTERNET	-	LOCAL	328	66	5544	1.008	0.678	0.000	0.000	202	N/A	N/A	N/A	N/A	N/A

Total INGRESS flows displayed: 2 out of 2
Total EGRESS flows displayed: 2 out of 2

4. [モニター] > [統計] > [ルート] で、各ルーティングドメインのルーティングテーブルを確認することもできます。



Routes for routing domain : Guest

Filter: in Any column Apply

Show 100 entries Showing 1 to 5 of 5 entries First Previous 1 Next Last

Num	Network Addr	Gateway IP Address	Service	Firewall Zone	Reachable	Site IP Address	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
0	11.20.20.0/24	*	Local	Default_LAN_Zone	YES	*	Angelina-CFB	Static	-	-	5	318	YES	N/A	N/A
1	11.10.10.0/24	*	DC-Angelina-CFB	Default_LAN_Zone	YES	*	DC	Static	-	-	5	0	YES	N/A	N/A
2	0.0.0.0/0	*	Internet	Untrusted_Internet_Zon	YES	*	*	Static	-	-	5	159	YES	N/A	N/A
3	0.0.0.0/0	*	Passthrough	Any	YES	*	*	Static	-	-	16	0	YES	N/A	N/A
4	0.0.0.0/0	*	Discard	Any	YES	*	*	Static	-	-	16	0	YES	N/A	N/A

Showing 1 to 5 of 5 entries First Previous 1 Next Last

使用例

以前の Citrix SD-WAN リリースでは、仮想ルーティングと転送には以下の問題がありましたが、これらの問題は解決されています。

- ブランチサイトに複数のルーティングドメインがある場合、データセンター (MCN) のすべてのドメインを含める必要はありません。さまざまな顧客のトラフィックを安全な方法で分離する能力が必要
- 1 つのサイトでインターネットにアクセスするには、複数のルーティングドメインに対して、アクセス可能なファイアウォール付きパブリック IP アドレスを 1 つ持つ必要があります（VRF lite を超えて拡張）。
- お客様は、異なるサービスをサポートするルーティングドメインごとにインターネットルートが必要です。

- ブランチサイトでの複数のルーティングドメイン
- 異なるルーティングドメインのインターネットアクセス。

ブランチサイトでの複数のルーティングドメイン

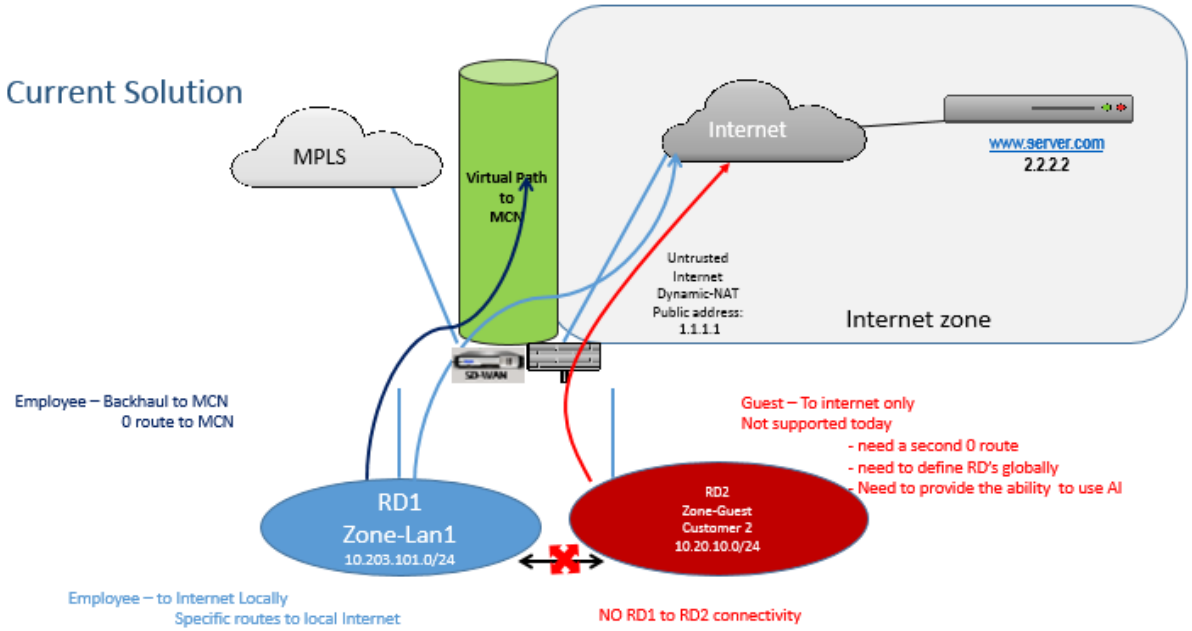
仮想転送およびルーティングファイアウォールのセグメント化機能強化により、次のことが行えます。

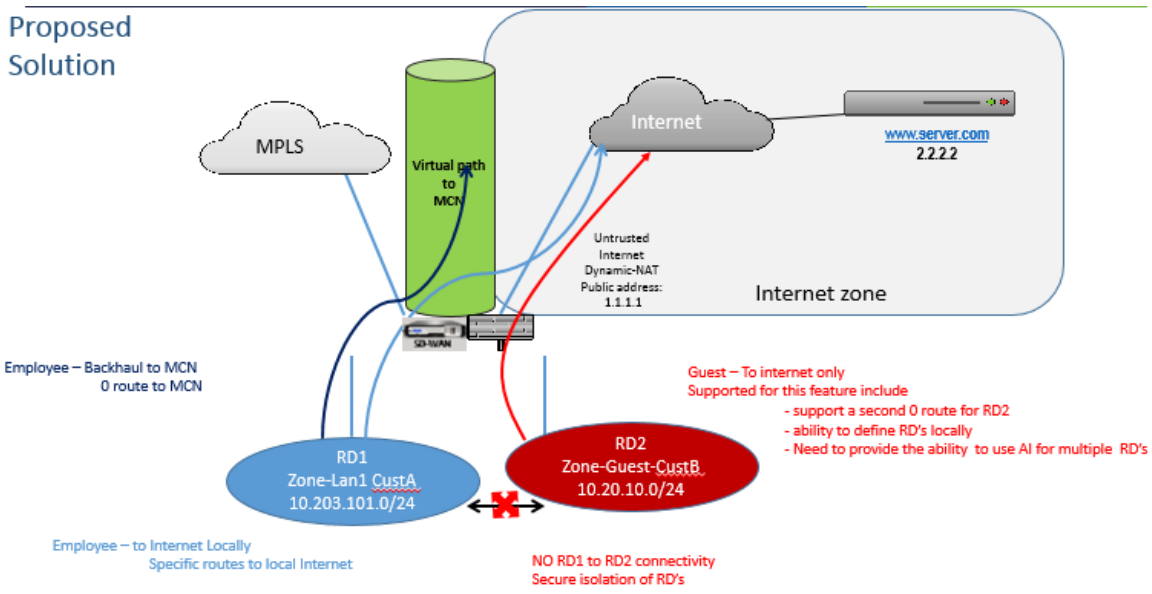
- 従業員やゲストなど、少なくとも 2 つのユーザーグループの安全な接続をサポートするインフラストラクチャをブランチサイトで提供します。このインフラストラクチャは、最大 16 のルーティングドメインをサポートできます。
- 各ルーティングドメインのトラフィックを、他のルーティングドメインのトラフィックから分離します。
- 各ルーティングドメインにインターネットアクセスを提供し、
  - 共通のアクセスインターフェイスが必要であり、許容される
  - 個別のパブリック向け IP アドレスを持つ各グループのアクセスインターフェイス
- 従業員のトラフィックは、ローカルインターネット（特定のアプリケーション）に直接ルーティングできます
- 従業員のトラフィックは、広範なフィルタリング（0 ルート）のために MCN にルーティングまたはバックホールできます
- ルーティングドメインのトラフィックは、ローカルインターネット (0 ルート) に直接ルーティングできます。
- 必要に応じて、ルーティングドメインごとに特定のルートをサポート
- ルーティングドメインは VLAN ベースです
- RD を MCN に配置する必要の要件を削除
- ルーティングドメインをブランチサイトでのみ構成できるようになりました
- アクセスインターフェイスに複数の RD を割り当てることができます (一度有効にすると)
- 各 RD には 0.0.0.0 のルートが割り当てられます
- RD に特定のルートを追加できるようにします
- 同じアクセスインターフェイスを使用して、異なる RD からのトラフィックがインターネットに出ることを許可します。
- RD ごとに異なるアクセスインターフェイスを構成できます。
- 一意のサブネットでなければならない（RD は VLAN に割り当てられる）
- 各 RD では、同じ FW デフォルトゾーンを使用できます。
- トラフィックは、ルーティングドメインを介して分離されます
- アウトバウンドフローには、フローヘッダーのコンポーネントとして RD があります。SD-WAN がリターンフローを正しいルーティングドメインにマッピングできるようにします。

複数のルーティングドメインを設定するための前提条件

- インターネットアクセスが構成され、WAN リンクに割り当てられます。
- NAT 用に設定されたファイアウォールと正しいポリシーが適用されます。
- 2 番目のルーティングドメインがグローバルに追加されました。
- 各ルーティングドメインがサイトに追加されました。
- [サイト] > [サイト名] > [W **AN** リンク **[**名前名前**]**] > [WL2] > [アクセスインターフェイス] で、チェックボックスが使用可能であり、インターネットサービスが正しく定義されていることを確認します。このチェックボックスを選択できない場合、インターネットサービスは定義されていないか、サイトの WAN リンクに割り当てられていません。

展開シナリオ





制限事項

- すべてのルーティングドメインでインターネットアクセスを有効にするには、インターネットサービスを WAN リンクに追加する必要があります。(このオプションを有効にするまで、このオプションを有効にするチェックボックスはグレー表示されます)。

  すべてのルーティングドメインでインターネットアクセスを有効にしたら、Dynamic-NAT ルールを自動的に追加します。

- サイトあたり最大 16 のルーティングドメイン。
- アクセスインターフェイス (AI): サブネットごとに単一の AI。
- 複数の AI では、AI ごとに個別の VLAN が必要です。
- サイトに 2 つのルーティングドメインがあり、1 つの WAN リンクがある場合、両方のドメインは同じパブリック IP アドレスを使用します。
- すべてのルーティングドメインのインターネットアクセスが有効になっている場合、すべてのサイトがインターネットにルーティングできます。(1 つのルーティングドメインでインターネットアクセスを必要としない場合は、ファイアウォールを使用してトラフィックをブロックできます)。
- 複数のルーティングドメインで同じサブネットはサポートされません。
- 監査機能はありません
- WAN リンクは、インターネットアクセス用に共有されます。
- ルーティングドメインごとの QoS はありません。先着順です。

証明書認証

May 10, 2021

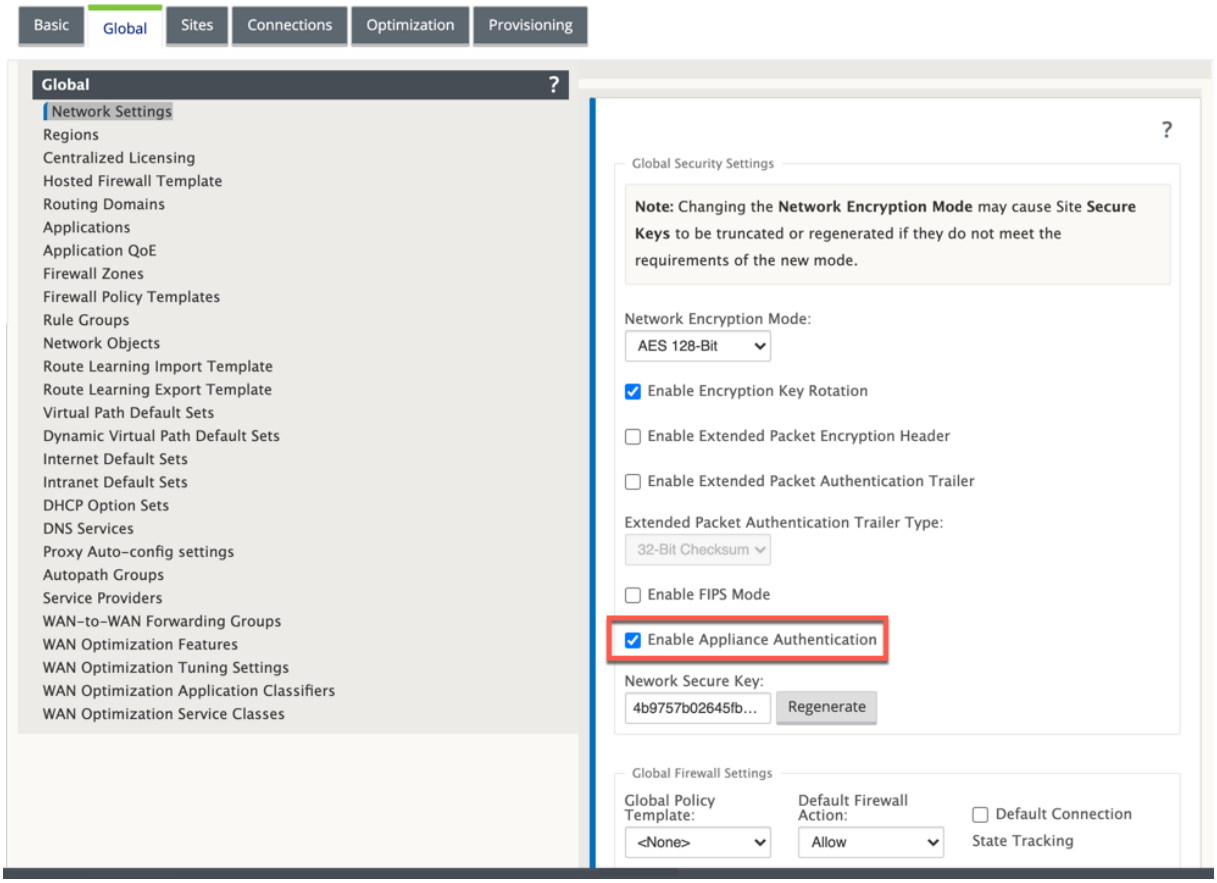
Citrix SD-WAN は、ネットワーク暗号化や仮想パスの IPSec トンネルなどのセキュリティ技術を使用して、SD-WAN ネットワーク上のアプライアンス間で安全なパスを確立します。Citrix SD-WAN 11.0.2 では、既存のセキュリティ対策に加えて、証明書ベースの認証が導入されています。

証明書認証。組織は、プライベート認証局（CA）によって発行された証明書を使用してアプライアンスを認証できます。アプライアンスは、仮想パスを確立する前に認証されます。たとえば、ブランチアプライアンスがデータセンターに接続しようとしたときに、ブランチからの証明書がデータセンターで想定される証明書と一致しない場合、仮想パスは確立されません。

CA によって発行された証明書は、公開鍵をアプライアンスの名前にバインドします。公開キーは、証明書で識別されるアプライアンスが所有する対応する秘密キーで動作します。

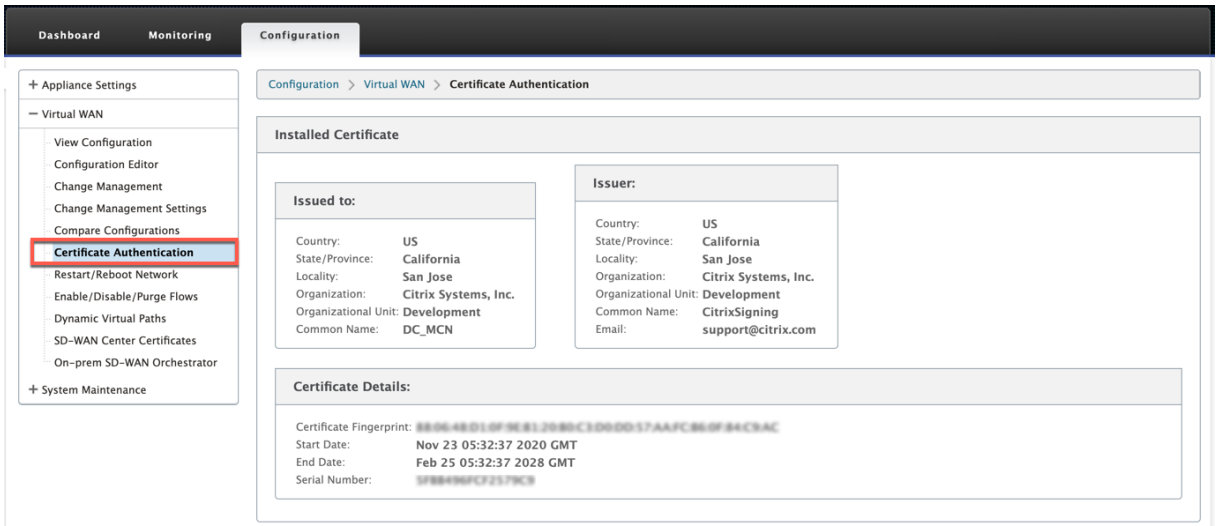
> 注
>
> 現在のリリースでは、CA 証明書をネットワーク内のすべてのアプライアンスに手動でアップロードする必要があります。将来のリリースには、ネットワーク証明書の自動配布が含まれます。

アプライアンス認証を有効にするには、構成エディターで [グローバル] > [ネットワーク設定] に移動し、[アプライアンス認証を有効にする] を選択します。



構成をステージングして適用すると、[構成] > [仮想 **WAN**] の下に新しい 証明書認証オプションが表示されます。

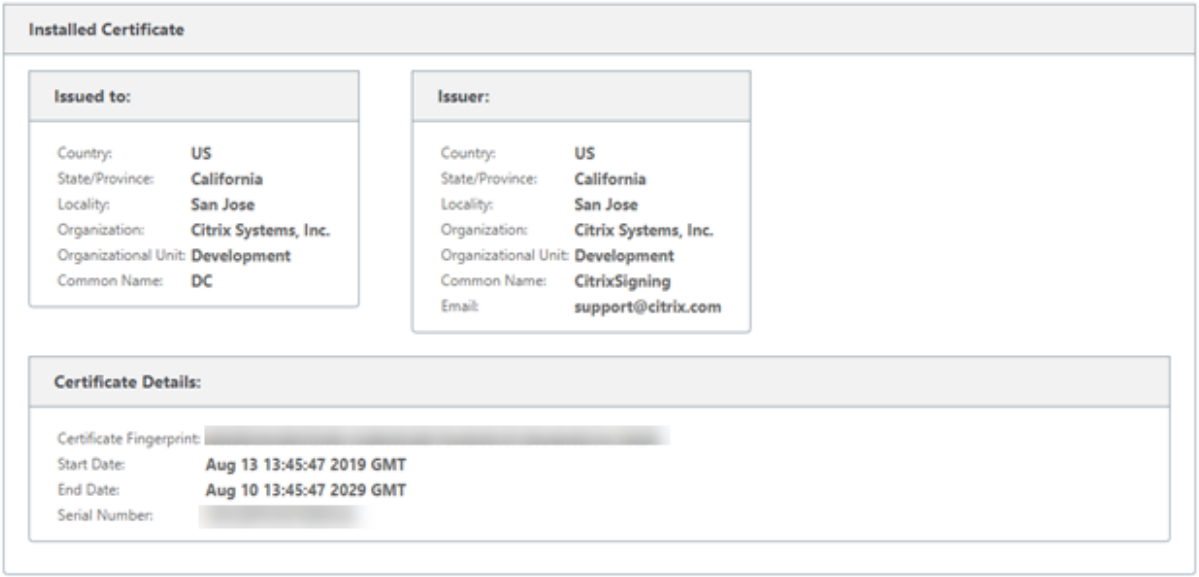
[証明書認証] ページから、仮想パス認証に使用されるすべての 証明書 を管理できます。



インストール済みの証明書

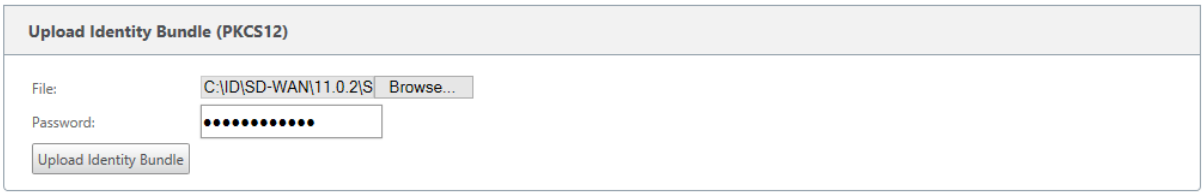
「インストールされた証明書」セクションには、アプライアンスにインストールされている証明書の概要が表示されます。アプライアンスは、この証明書を使用してネットワーク内で自身を識別します。

[発行先] セクションには、証明書の発行元に関する詳細が表示されます。証明書はアプライアンス 名にバインドされているため、証明書の共通 名はアプライアンスの名前と一致します。[発行者] セクションには、証明書に署名した認証局の詳細が表示されます。証明書の詳細には、証明書のフィンガープリント、シリアル番号、および証明書の有効期間が含まれます。



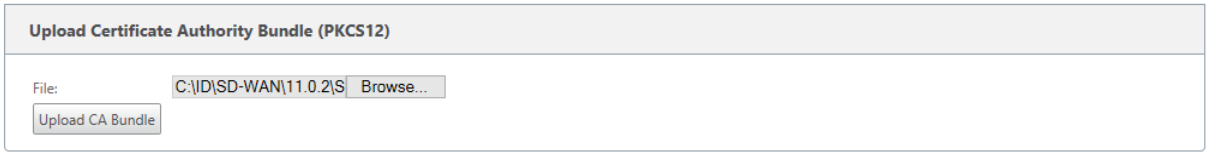
ID バンドルをアップロード

Identity バンドルには、秘密鍵と秘密鍵に関連付けられた証明書が含まれます。CA によって発行されたアプライアンス証明書をアプライアンスにアップロードできます。証明書バンドルは PKCS 12 ファイルで、拡張子は.p12 です。パスワードで保護することを選択できます。パスワードフィールドを空白のままにすると、パスワード保護なしとして扱われます。



認証局バンドルのアップロード

証明書署名機関に対応する PKCS 12 バンドルをアップロードします。認証局バンドルには、シグネチャの完全なチェーン、ルート、およびすべての中間署名機関が含まれます。



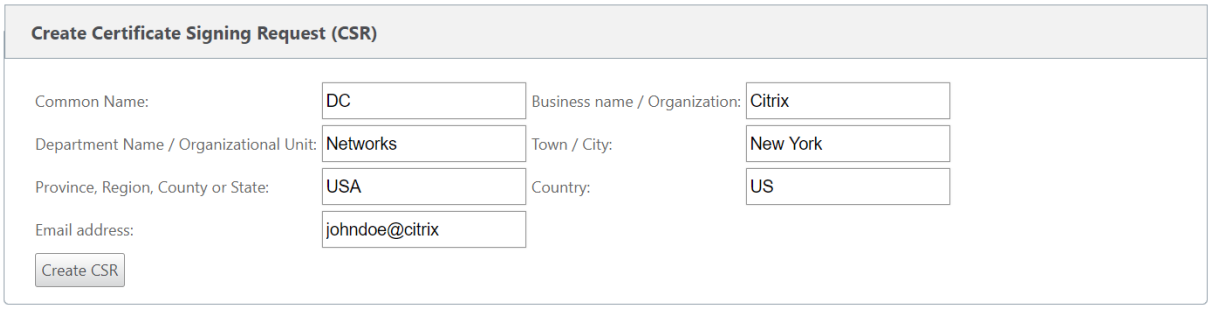
ネットワーク証明書のアップロード

1 つの.PEM ファイルに連結されているすべてのネットワーク証明書をアップロードします。ネットワーク証明書は、ネットワーク内の各アプライアンスにアップロードする必要があります。サイトが仮想パス接続を開始すると、その証明書を含むメッセージが応答側に送信されます。応答側は、イニシエータ証明書をネットワーク証明書 PEM ファイルと照合します。イニシエータ証明書がデータベース上の証明書と一致する場合、仮想パス接続が確立されます。

> 注
>
> 現在のリリースでは、CA 証明書をネットワーク内のすべてのアプライアンスに手動でアップロードする必要があります。将来のリリースには、ネットワーク証明書の自動配布が含まれます。

証明書署名リクエストの作成

アプライアンスは、署名されていない証明書を生成し、証明書署名要求（CSR）を作成できます。CA は、アプライアンスから CSR をダウンロードし、署名して、PEM または DER 形式でアプライアンスにアップロードし直すことができます。これは、アプライアンスのアイデンティティ証明書として使用されます。アプライアンスの CSR を作成するには、アプライアンスの共通名、組織の詳細、およびアドレスを指定します。

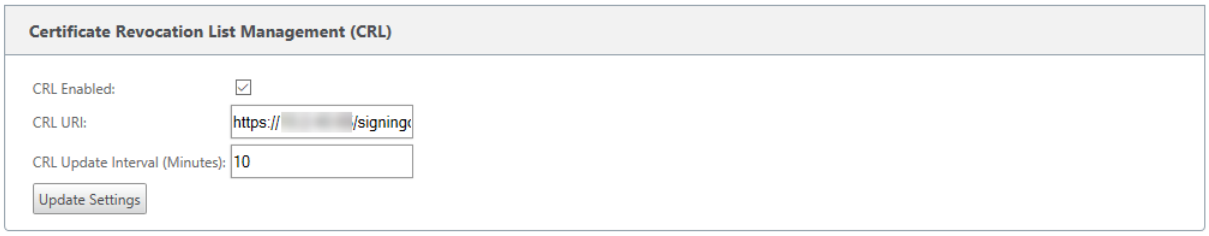


証明書失効リストマネージャ

証明書失効リスト (CRL) は、ネットワークで有効でなくなった証明書のシリアル番号の公開リストです。CRL ファイルは定期的にダウンロードされ、すべてのアプライアンスにローカルに保存されます。証明書が認証されると、応

答側は CRL を調べて、イニシエータ証明書がすでに失効しているかどうかを確認します。Citrix SD-WAN は現在、PEM および DER 形式のバージョン 1 の CRL をサポートしています。

CRL を有効にするには、[CRL 有効] オプションを選択します。CRL ファイルが維持される場所を指定します。HTTP、HTTPS、および FTP の場所がサポートされています。CRL ファイルを確認およびダウンロードする間隔を指定します。範囲は 1 ～1440 分です。



> 注
>
> virtua1 パスの再認証期間は 10 ～15 分です。CRL 更新間隔が短い期間に設定されている場合、更新された CRL リストには現在アクティブなシリアル番号が含まれる場合があります。アクティブ失効した証明書をネットワーク内で短時間利用できるようにする。

AppFlow と IPFIX

September 26, 2023

AppFlow および IPFIX は、ネットワークインフラストラクチャ内のアプリケーションおよびトランザクションデータを識別および収集するために使用されるフローエクスポート標準です。このデータにより、アプリケーショントラフィックの使用率とパフォーマンスの可視性が向上します。

収集されたデータは、フローレコードと呼ばれ、1 つ以上の IPv4 コレクタに送信されます。コレクターはフローレコードを集約し、リアルタイムレポートまたは履歴レポートを生成します。

AppFlow

AppFlow は、HDX/ICA 接続のみのフローレベルデータをエクスポートします。HDX データセットテンプレートの TCP のみを有効にすることも、HDX データセットテンプレートを有効にすることもできます。HDX データセット用の TCP のみマルチホップデータを提供します。HDX データセットがHDX インサイトデータを提供します。

> 注
>
> HDX テンプレートは、Citrix SD-WAN PE エディションおよび 2 ボックスアプライアンスでのみ使用できます。これは、データセンターアプライアンス上で有効にする必要があります。

Splunk や Citrix ADM などの AppFlow コレクターには、これらのテンプレートを解釈して表示するためのダッシュボードがあります。

IPFIX

IPFIX は、すべての接続のフローレベルデータをエクスポートするために使用されるコレクタエクスポートプロトコルです。どの接続でも、パケット数、バイト数、サービスの種類、フロー方向、ルーティングドメイン、アプリケーション名などの情報を表示できます。IPFIX フローは、管理インターフェイスを介して送信されます。ほとんどのコレクタは IPFIX フローレコードを受信できますが、IPFIX テンプレートを解釈するためにカスタムダッシュボードを構築する必要がある場合があります。

IPFIX バージョン 10 は、Citrix SD-WAN リリース 10 バージョン 2 以降でサポートされています。

アーキテクチャの変更がいくつかあり、これらのプロトコルがリソースを再利用するときに Net Flow、AppFlow、および IPFIX を一緒に有効にすると、パフォーマンスへの影響が少なくなっています。

制限事項

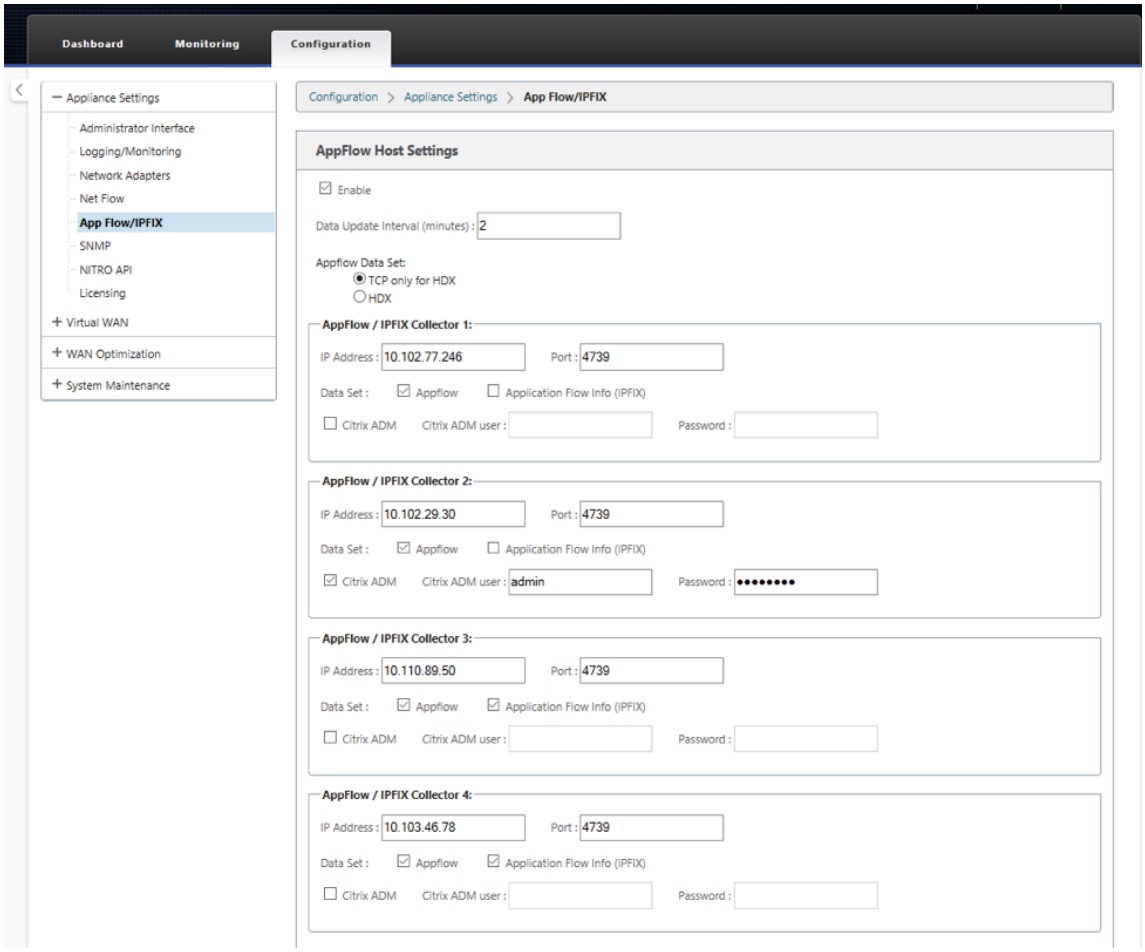
- Net Flow のエクスポート間隔が 15 秒から 60 秒に増加します。
- AppFlow/IPfix フローは UDP 経由で送信され、接続が失われた場合、すべてのデータが再送信されるわけではありません。エクスポート間隔が X 分に設定されている場合、アプライアンスは X 分のデータのみを保存します。接続損失の X 分後に再送信されます。
- Citrix SD-WAN では、リリース 10 バージョン 2 では、**AppFlow** の設定はすべてのアプライアンスにローカルに設定されていますが、以前のリリースではグローバル設定でした。SD-WAN ソフトウェアリリースが以前のリリースのいずれかにダウングレードされ、いずれかのアプライアンスで AppFlow が設定されている場合は、すべてのアライアンスにグローバルに適用されます。

AppFlow/IPFIX の設定

AppFlow/IPFIX を個別の SD-WAN アプライアンスで構成することも、SD-WAN Center で構成して、アプライアンスグループに構成をプッシュすることもできます。

SD-WAN アプライアンスで AppFlow /IPFIX を構成するには:

1. Citrix SD-WAN SE/PE Web インターフェイスで、［構成］**>**［**AppFlow/IPFIX**］に移動します。
2. [有効] をクリックします。



3. [**Data Update Interval**] フィールドで、フローレポートを AppFlow/IPFix コレクタにエクスポートする時間間隔を分単位で指定します。最大間隔は 10 分です。

4. **AppFlow** データセット テンプレートを選択すると、次のいずれかのデータセットテンプレートを選択できます。

   - **HDX** 専用（**AppFlow**）: ICA 接続のマルチホップデータを収集して AppFlow コレクターに送信するための AppFlow データセットテンプレート。
   - **HDX**（**AppFlow**）: ICA 接続の HDX インサイトデータを収集して AppFlow コレクターに送信するための AppFlow データセットテンプレート。

   > 注
   >
   > **HDX** テンプレートは、Citrix SD-WAN PE および Two Box アプライアンスでのみ使用できます。

5. 最大 4 つの AppFlow または IPFIX コレクタを設定できます。各コレクタに対して、次のパラメータを指定します。

   - **IP** アドレス: 外部 AppFlow /IPFIX コレクタ・システムの IP アドレス。

- ポート：外部 AppFlow /IPFIX コレクタ・システムがリッスンするポート番号。デフォルト値は 4739 です。
- アプリケーションフロー情報（**IPFIX**）：すべての接続のフローレコードを収集し、IPFIX コレクタに送信する IPFIX テンプレート。
- **Citrix ADM**：Citrix ADM を AppFlow コレクターとして使用するには、これを選択します。

> 注
>
> Citrix ADM は現在、IPFIX 収集をサポートしていません。

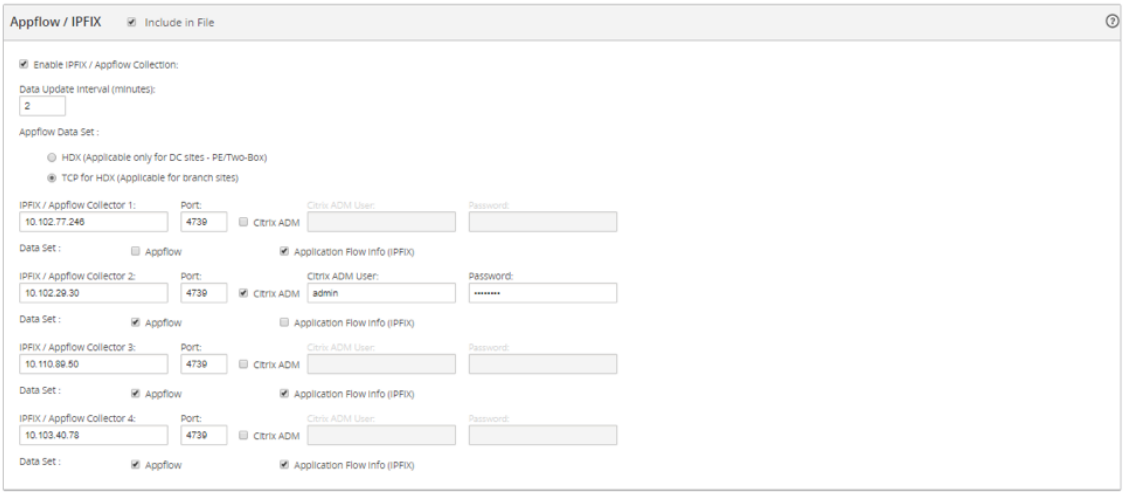
- **Citrix ADM** ユーザー：Citrix ADM コレクターのユーザー名
- パスワード：Citrix ADM コレクタのパスワード。

ユーザー名とパスワードは、Citrix ADM にシームレスにログインしてフローデータを保存するために使用されます。

6. [設定の適用] をクリックします。

SD-WAN Center を使用して **AppFlow /IPFIX** コレクタを構成するには：

1. Citrix SD-WAN Center 管理 UI で、［構成］**>**［アプライアンスの設定］に移動します。
2.「**AppFlow/IPFIX** 」セクションに移動し、「ファイルに含める」を選択します。
3. [**IPFIX /AppFlow** 収集を有効にする] を選択します。



4. [データ更新間隔] フィールドで、AppFlow レポートが AppFlow/IPFIX コレクターにエクスポートされる時間間隔を分単位で指定します。
5. **AppFlow** データセット テンプレートを選択すると、次のいずれかのデータセットテンプレートを選択できます。

   - **HDX** のみの **TCP**：ICA 接続のマルチホップデータを収集して AppFlow コレクターに送信する AppFlow データセットテンプレート。

- **HDX**: ICA 接続の HDX インサイトデータを収集して AppFlow ow コレクターに送信するための AppFlow データセットテンプレート。

> 注
>
> **HDX** テンプレートは、Citrix SD-WAN PE および Two Box アプライアンスでのみ使用できます。

6. 最大 4 つの AppFlow または IPFIX コレクタを設定できます。各コレクタに対して、次のパラメータを指定します。

   - **IPFIX/AppFlow** コレクタ: 外部 AppFlow/IPFIX コレクタシステムの IP アドレス。
   - ポート: 外部 AppFlow /IPFIX コレクタ・システムがリッスンするポート番号。デフォルト値は 4739 です。
   - アプリケーションフロー情報: すべての接続のフローレコードを収集し、IPFIX コレクタに送信する IPFIX テンプレート。
   - **Citrix ADM**: Citrix ADM を AppFlow コレクターとして使用するには、これを選択します。

     > 注
     >
     > Citrix ADM は現在、IPFIX 収集をサポートしていません。

   - **Citrix ADM** ユーザー: Citrix ADM コレクターのユーザー名。
   - パスワード: Citrix ADM コレクタのパスワード。

     ユーザー名とパスワードは、Citrix ADM にシームレスにログインしてフローデータを保存するために使用されます。

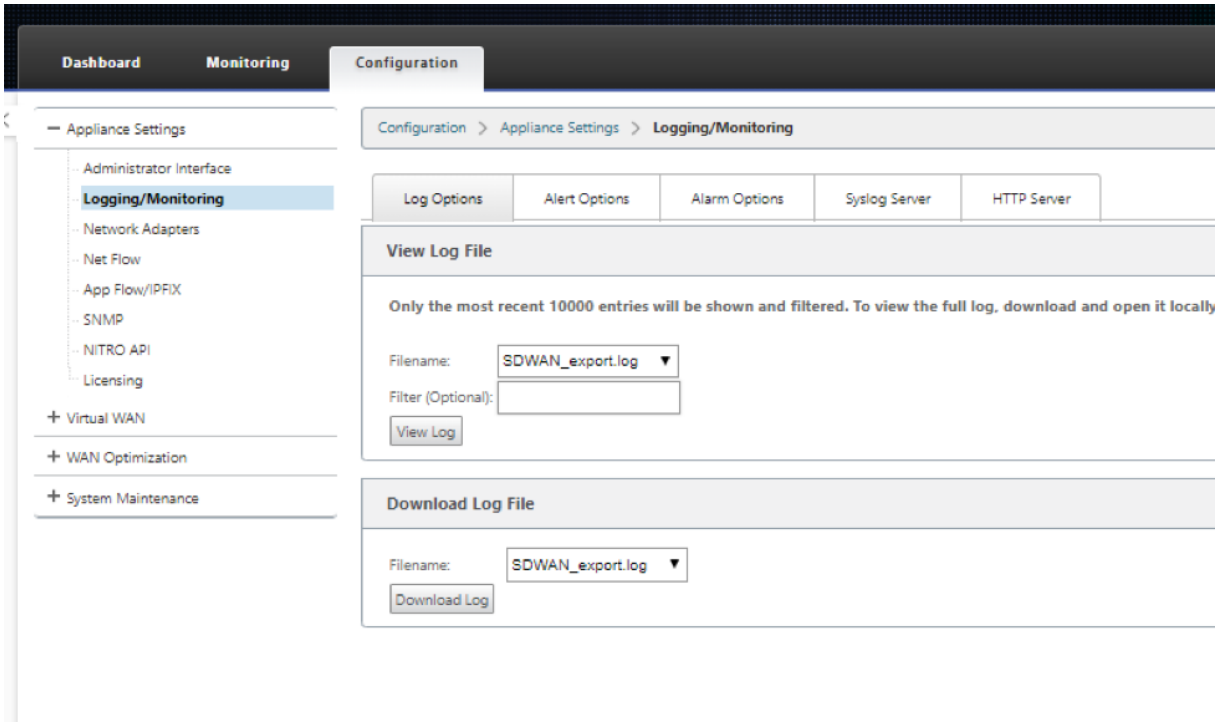
7. 設定を保存 し、管理アプライアンスに エクスポート します。

> 注
>
> SD-WAN Center のバージョンが 10.2 より低く、SD-WAN アプライアンスのバージョンが 10.2 以降の場合は、次の条件を満たすことができます。
>
> - アプライアンスでローカルコレクタが有効になっている場合、SD-WAN Center からプッシュされた AppFlow および IPFIX 設定は既存の設定に影響しません。
> - アプライアンスでローカルコレクタが有効になっていない場合、SD-WAN Center からプッシュされた AppFlow/IPFIX 設定がアプライアンスに適用されます。
> - SD-WAN Center 構成でグローバルな AppFlow/IPFix 構成が有効になっている場合、アプライアンスですべてのローカルコレクタが有効になります。

ログファイル

AppFlow/IPFIX エクスポートプロトコルに関連する問題のトラブルシューティングについては、SD-WAN_export.log ファイルを表示およびダウンロードできます。[構成] **>** [ログ記録/監視] に移動し、

SDWAN_Export.log ファイルを選択します。



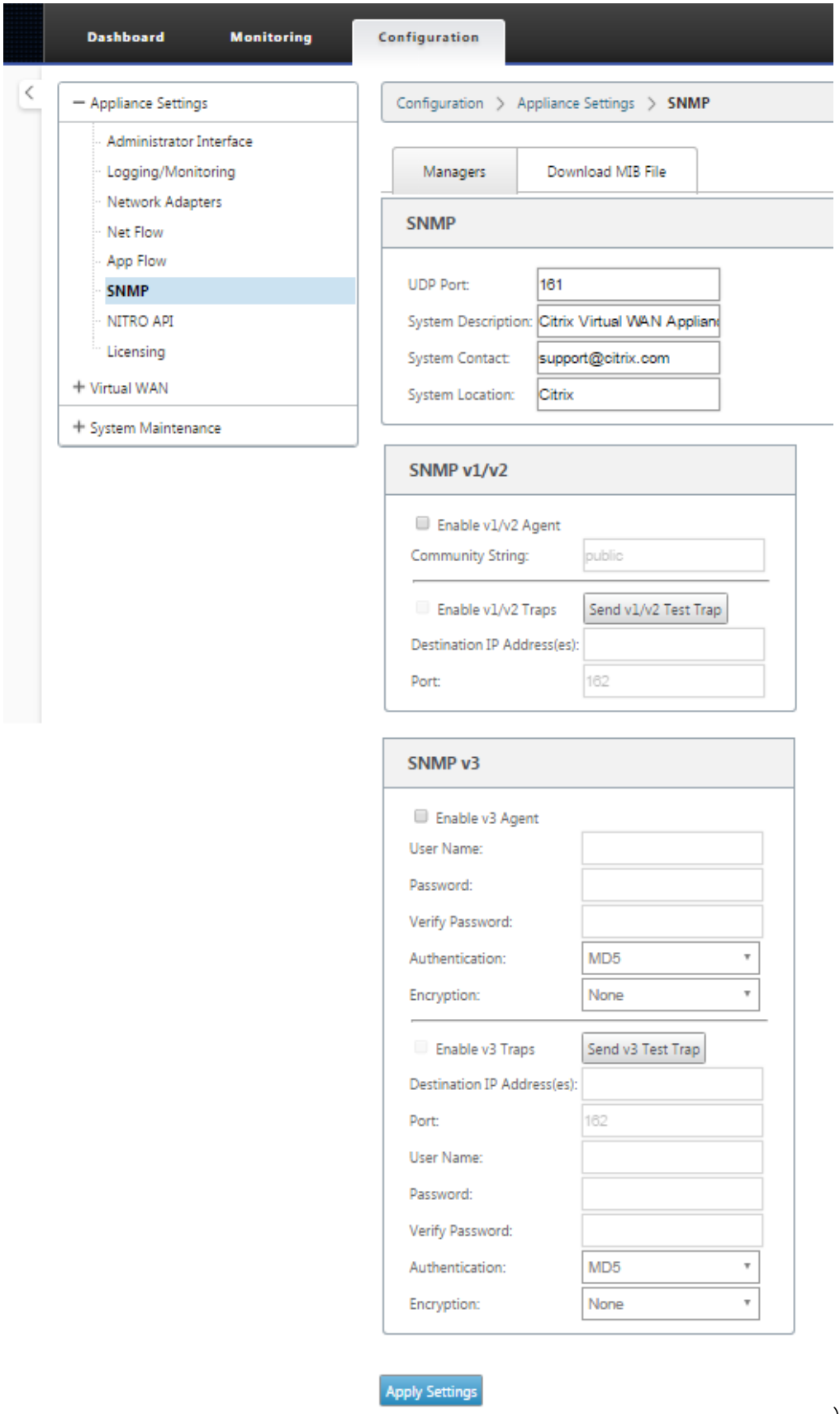
SNMP

November 17, 2022

Citrix SD-WAN は、SNMPV1/V2 機能をサポートし、SNMPv3 機能ごとに 1 つのユーザーアカウントのみをサポートします。この制限により、次の利点があります。

- ネットワークデバイスの SNMPv3 コンプライアンスの確保
- SNMPv3 機能の検証
- SNMPv3 の容易な設定

SNMPv3 のポーリングおよびトラップを構成するには、［構成］＞［アプライアンスの設定］＞［**SNMP** ］ページの［SNMPv3］セクションに移動し、必要に応じてフィールドに入力します。



)

標準 **MIB** サポート

SD-WAN アプライアンスでは、次の標準 MIB がサポートされています。

MIB	RFC (定義リンク)
DISMAN-EVENT-MIB	https://www.ietf.org/rfc/rfc2981.txt
IF-MIB	https://www.ietf.org/rfc/rfc2863.txt
IP-FORWARD-MIB	https://www.ietf.org/rfc/rfc4292.txt
IP-MIB（部分）	https://www.ietf.org/rfc/rfc4293.txt
Q-BRIDGE-MIB（部分）	http://www.ieee802.org/1/files/public/MIBs/IEEE8021-Q-BRIDGE-MIB-201112120000Z.mib
RFC1213-MIB	https://www.ietf.org/rfc/rfc1213.txt
SNMPv2-MIB	https://www.ietf.org/rfc/rfc3418.txt
TCP-MIB	https://www.ietf.org/rfc/rfc4022.txt
P-BRIDGE-MIB.txt	http://www.icir.org/fenner/mibs/extracted/P-BRIDGE-MIB-rfc2674.txt
RMON2-MIB.txt	https://www.ietf.org/rfc/rfc3273.txt
TOKEN-RING-RMON-MIB.txt	http://www.icir.org/fenner/mibs/extracted/TOKEN-RING-RMON-MIB-rmonmib-01.txt

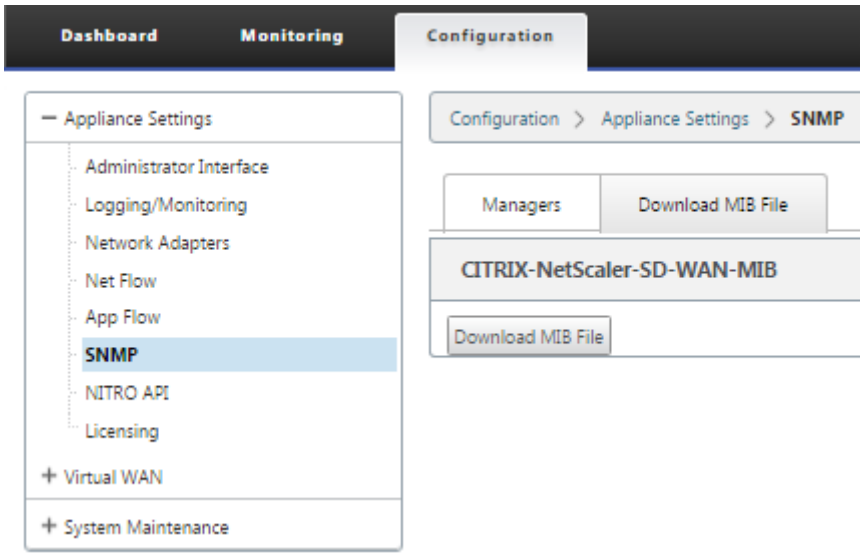
Citrix SD-WAN アプライアンスの監視を開始する前に、次の SNMP ファイルをダウンロードする必要があります。

- CITRIX-COMMON-MIB.txt
- APPACCELERATION-SMI.txt
- APPACCELERATION-PRODUCTS-MIB.txt
- APPACCELERATION-TC.txt
- APPACCELERATION-STATUS-MIB.txt
- APPCACHE-MIB.txt
- SDX-MIB-smiv2.mib

MIB ファイルは、SNMPv3 マネージャおよび SNMPv3 トラップリスナーによって使用されます。このファイルには、SD-WAN アプライアンスのエンタープライズ MIB が含まれており、SD-WAN 固有のイベントが提供されます。MIB ファイルをダウンロードするには、SD-WAN Web 管理インターフェイスで次の手順を実行します。

1. 「構成」>「アプライアンスの設定」>「**SNMP** 」>「**MIB** ファイルのダウンロード」ページに移動します。
2. 必要な **MIB** ファイルを選択します。
3. [表示] をクリックします。

   MIB ファイルが MIB ブラウザで開きます。



> 注
>
> - これらの MIB のサポートは、Linux システム上の **net-snmpd** デーモンプロセスによってデフォルトで提供されます。MIB は、ネットワーク管理アプリケーションをサポートするための基礎となります。
> - イーサネットポートパケットおよびバイトカウンタは、**ifTable** 内の **IF-MIB** にあります。システム情報は、システムオブジェクトにあります。
> - イーサネットポートは **ifTable** に含まれています。したがって、SNMP サブシステムが動作していることを確認するには、この作業で十分です。
> - **Q-BRIDGE-MIB** および **IP-MIB** のサポートにより、ネットワークマッピングアプリケーションのサポートが提供されます。

SNMP マネージャーの追加、SNMP ビュー/アラームの設定、および SNMP サーバーの追加の詳細については、次の CloudBridge 7.4 のドキュメントを参照してください。CloudBridge。

WAN の最適化

May 10, 2021

Citrix SD-WAN WANOP アプライアンスは、WAN リンクを最適化し、最大限の応答性とスループットを確保します。Citrix SD-WAN WANOP アプライアンスは、リンクの両端で 1 つずつペアで動作し、リンク上のトラフィックを高速化します。以下に、Citrix SD-WAN WANOP の機能の一部を示します。

- 圧縮
- TCP プロトコルアクセラレーション
- トラフィック管理
- アプリケーションアクセラレーション
- Citrix の XenApp/XenDesktop（HDX）アクセラレーション
- 統合
- 監視と管理

Citrix SD-WAN WANOP 10.2 のインストール、展開、および機能の構成については、Citrix SD-WAN WANOP ドキュメントを参照してください。Citrix SD-WAN WANOP 10.2 の機能と手順は、Citrix SD-WAN WANOP リリースに記載されている手順と似ています。

Citrix SD-WANPremium エディションで WAN 最適化機能を有効にして構成できます。詳細については、Citrix SD-WAN「Premium Edition」を参照してください。

WANOP Client Plug-in ソフトウェアを使用して、リモート Windows のラップトップまたはワークステーションでネットワークアクセラレーションを実現できます。詳しくは、「WANOP クライアントプラグイン」を参照してください。

Citrix SD-WAN Premium Edition

May 10, 2021

このセクションでは、仮想 WAN に対して SD-WAN Premium（エンタープライズ）エディションの WAN Optimization 機能を有効にして構成する手順を説明します。これを行うには、MCN の Web 管理インターフェイスで、構成エディター の [最適化] セクションフォームを使用します。

> 注
>
> 仮想 WAN の WAN Optimization 機能へのアクセス、有効化、構成、およびアクティブ化を行うには、SD-WAN Premium（Enterprise）Edition ライセンスをインストールしておく必要があります。SD-WAN Standard Edition では、これらの機能はサポートされていません。

最適化 セクションセットとパラメータを設定するには、最上位レベルの 2 つのステップがあります。これらは、依存性の順にリストされています。

1. WAN Optimization を有効にして、デフォルト 設定をカスタマイズするか、デフォルトをそのまま使用します。

   デフォルト 構成は、WAN **Optimization** の対象となるすべてのサイトの基本最適化構成として使用されます。デフォルト の設定は事前に設定されており、カスタマイズできます。

   > 注:
   >
   > 手順については、最適化の有効化とデフォルト設定の構成を参照してください。

2. （オプション）個々のブランチサイトごとに WAN Optimization 設定をカスタマイズするか、それぞれの **Defaults** セットと設定をそのまま使用します。

   デフォルトでは、デフォルト 構成は、WAN Optimization の対象となる各ブランチサイトに最初に適用されます。WAN Optimization は、1000-EE（Premium Edition）および 2000-EE（Premium Edition）のハードウェアアプライアンスでのみサポートされます。サポートされているブランチサイトごとに、既定の セットと設定の組み合わせ、またはこれらのサブセットを受け入れるか変更するかを選択できます。手順については、「ブランチサイトの最適化の構成」を参照してください。

   これらの手順を完了するには、構成フォームの設定エディターの [最適化] セクションを使用します。「最適化」セクションは次のように構成されています。

   - **Defaul** ts —**Default** s ブランチには、次の子ブランチが含まれます。子ブランチには、それぞれのセットと設定を構成するための 1 つ以上のフォームが含まれます。
     - 既定の機能
     - デフォルトのチューニング設定
     - デフォルトアプリケーション分類子 **(**セット**)**
     - デフォルトのサービスクラス（セット）
   - **** <Client Site Name>**—****Optimization** セクション構成ツリーには、**WAN Optimization** をサポートする各クライアントノード（ブランチサイト）のブランチが含まれています。クライアントノードがサポートされていないアプライアンスモデルの場合、サイトは **Optimiz** ation セクション構成ツリーに含まれません。ツリー内の各ブランチには、次の子ブランチが含まれています。これらの子ブランチには、それぞれのセットと設定を構成するための 1 つ以上のフォームが含まれます。
     - 既定の機能
     - デフォルトのチューニング設定
     - デフォルトのアプリケーション分類子 (セット)
     - デフォルトのサービスクラス（セット）

     次のセクションでは、仮想 WAN で WAN Optimization を有効にし、デフォルトの セットと設定を構成する方法について説明します。

最適化を有効化し、デフォルトの機能設定を構成する

May 10, 2021

仮想 WAN で WAN Optimization を有効にするには、次の手順を実行します。

1. [最適化] セクションの **[** 機能] 設定で WAN Optimization を有効にします。**

   このセクションには、プロセスのこの部分の手順が記載されています。

2. **[** サービスクラス**]** テーブルで、該当するサービスクラスごとに **[** アクセラレーション] ポリシー設定を構成します。**

   この手順は、残りの 最適化 構成を完了した後、でさらに実行されます。手順については、「最適化のデフォルトサービスクラスの設定」の項を参照してください。この時点で、構成で WAN Optimization が有効になっていますが、仮想 WAN ではまだ有効になっていません。仮想 WAN で WAN Optimization を有効にしてアクティブ化するには、このガイドの以降の章で説明するように、仮想 WAN 構成を完了し、展開内の適格なサイトで仮想 WAN アプライアンスパッケージを生成し、ステージングし、アクティブ化する必要があります。

   WAN Optimization を有効にして、[既定] セクションの [機能] 設定を構成するには、次の手順を実行します。

   a) 必要に応じて、管理 Web インターフェイスにログインし直して、構成エディタを開きます。

      構成エディタを開くには、次の操作を行います。

      i. ページ上部の［構成］タブを選択して、［構成］ナビゲーション・ツリー（左ペイン）を開きます。

      ii. ナビゲーションツリーで、**Virtual WAN** ブランチの左側にある [**+**] をクリックして、そのブランチを開きます。

      iii. [仮想 **WAN**] ブランチで、[構成エディタ**]** を選択します。

   b) 変更する構成パッケージを開きます。

      [開く] をクリックして [構成パッケージを開く] ダイアログボックスを表示し、[保存されたパッケージ**]** ドロップダウンメニューからパッケージ を選択します。

      これにより、選択したパッケージが 構成エディタ にロードされ、編集用に開きます。
      WAN Optimization 機能を含む有効な現在のライセンスをお持ちの場合は、構成エディタ の [最適化] セクションを使用できます。

      > 注
      >
      > [最適化] セクションが表示されない場合は、仮想 WAN に SD-WAN プレミアム (エンタープライズ) エディションのライセンスをインストールしていることを確認してください。SD-WAN Standard Edition は、WAN Optimization 機能をサポートしていません。

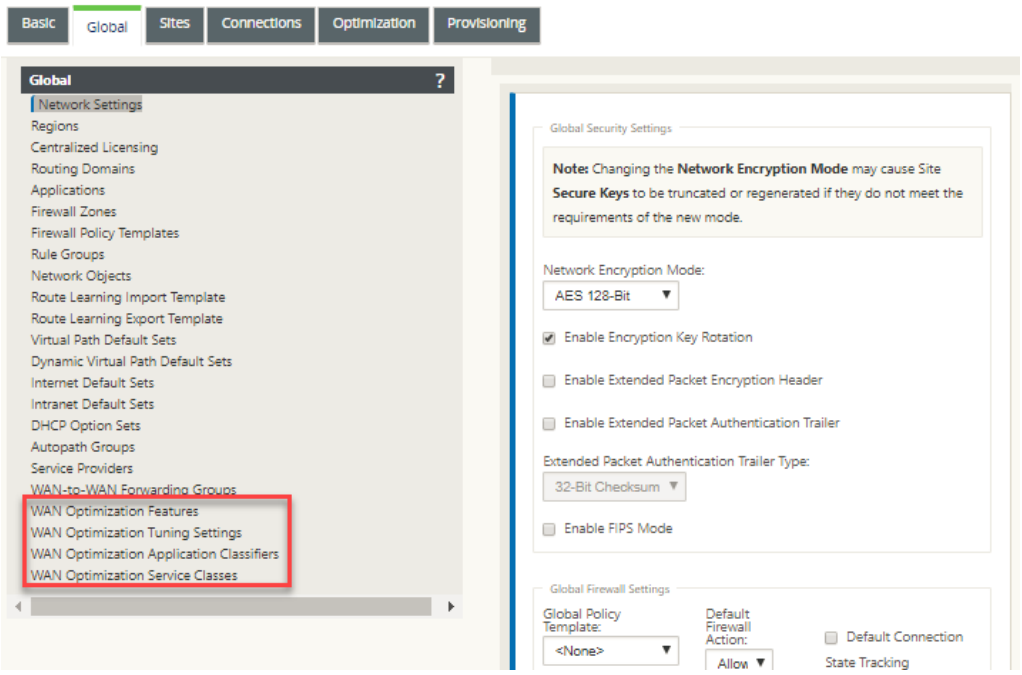
      詳細と手順については、次のセクションを参照してください。

- SD-WAN エディション
- ライセンス

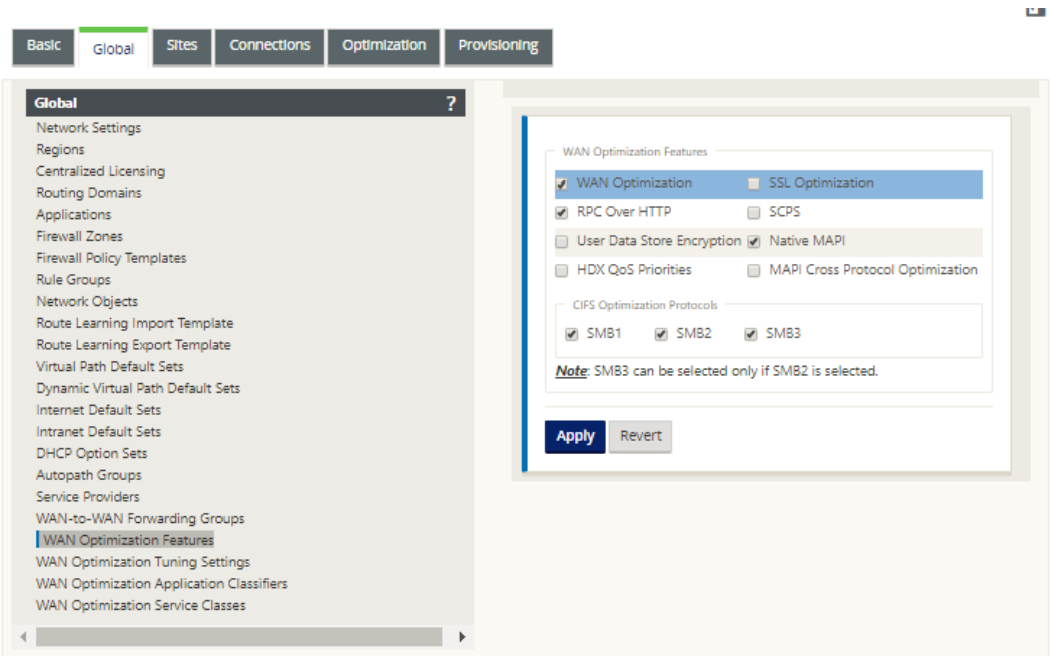
c) [グローバル] タブをクリックします。

[**Global**] タブから、WAN 最適化の次のデフォルト設定を構成できます。

- WAN Optimization 機能
- WAN Optimization チューニング設定
- WAN Optimization アプリケーション分類子
- WAN Optimization サービスクラス



d) [**WAN Optimization** 機能] をクリックします。



e) [**WAN Optimization**] チェックボックスをオンにします。

[**WAN Optimization**] チェックボックスは、[**WAN Optimization** 機能] セクションの左上隅にあります。これにより、フォームを編集できるようになり、[適用] ボタンと [元に戻す] ボタンが表示されます。

> 注
>
> この機能は有効にするためにのみ選択されます。WAN Optimization は、機能の 構成を完了した後、[適用] をクリックするまで、[最適化] セクションまたは構成パッケージで有効になりません。さらに、最適化構成プロセスでさらに指示されているように、「サービスクラス」テーブルで、適用可能な各サービスクラスの「アクセラレーション」設定も構成する必要があります。（手順については、最適化のデフォルトサービスクラスの設定セクションに記載されています）最後に、仮想 WAN 構成全体を完了してから、仮想 WAN で WAN Optimization が有効化されず、有効化されません。仮想 WAN の適格なサイトで仮想 WAN アプライアンス・パッケージを生成し、ステージングし、配布し、アクティブ化します。

f) [機能] 設定を構成します。

チェックボックスをクリックして、オプションを選択または選択解除します。フォームで事前に選択されたデフォルト設定を受け入れるか、設定をカスタマイズできます。

> 注
>
> デフォルトでは、[グローバル] タブで構成した設定は、ツリーに含まれる各ブランチサイトに自動的に適用されます。ただし、「ブランチサイトの最適化の構成」の項で説明されているように、特定のブランチの 最適化 設定をカスタマイズできます。

機能 設定フォームには、次の 2 つのセクションがあります。

- **WAN Optimization** 機能
- **CIFS Optimization** プロトコル

W **AN Optimization** 機能 の設定は次のとおりです。

- 「**WAN Optimization** 」—この構成で WAN Optimization を有効にするには、チェックボックスをオンにします。これにより、圧縮、重複除外、TCP プロトコル最適化も可能になります。

  > 注
  >
  > 他の [最適化] セクションのオプションを使用するには、[WAN 最適化] オプションを選択する必要があります。

- 「**SCPS** 」—サテライトリンクの TCP プロトコルの最適化を有効にするには、チェックボックスをオンにします。
- **HDX QoS** 優先度—HDX サブチャネルの優先順位付けに基づいて ICA トラフィックの最適化を有効にするには、チェックボックスをオンにします。
- [**MAPI** クロスプロトコル最適化] —Microsoft Outlook (MAPI) トラフィックのクロスプロトコル最適化を有効にするには、このチェックボックスをオンにします。
- 「**SSL Optimization** 」—SSL 暗号化を使用したトラフィックストリームの最適化を有効にするには、チェックボックスをオンにします。
- [**RPC over HTTP]** — RPC over HTTP を使用する Microsoft Exchange トラフィックの最適化を有効にするには、このチェックボックスをオンにします。
- 「ユーザーデータストアの暗号化」— WAN Optimization の圧縮履歴の暗号化によるデータのセキュリティ強化を有効にするには、チェックボックスをオンにします。
- [ネイティブ **MAPI**] —Microsoft Exchange トラフィックの最適化を有効にするには、このチェックボックスをオンにします。

  CIFS Optimization プロトコルの オプションは次のとおりです。

  - [**SMB1**] —Windows ファイル共有の最適化 (SMB1) を有効にするには、このチェックボックスをオンにします。
  - [**SMB2**] —Windows ファイル共有の最適化 (SMB2) を有効にするには、このチェックボックスをオンにします。
  - [**SMB3**] —[Windows ファイル共有 (SMB3) の最適化] を有効にするには、このチェックボックスをオンにします。**SMB**3 を選択する前に、まず SMB**2** オプションを選択する必要があります。

g) [適用] をクリックして、選択した 既定の機能 を有効にして構成パッケージに追加します。

次のステップは、最適化 のデフォルトの チューニング設定を構成することです。

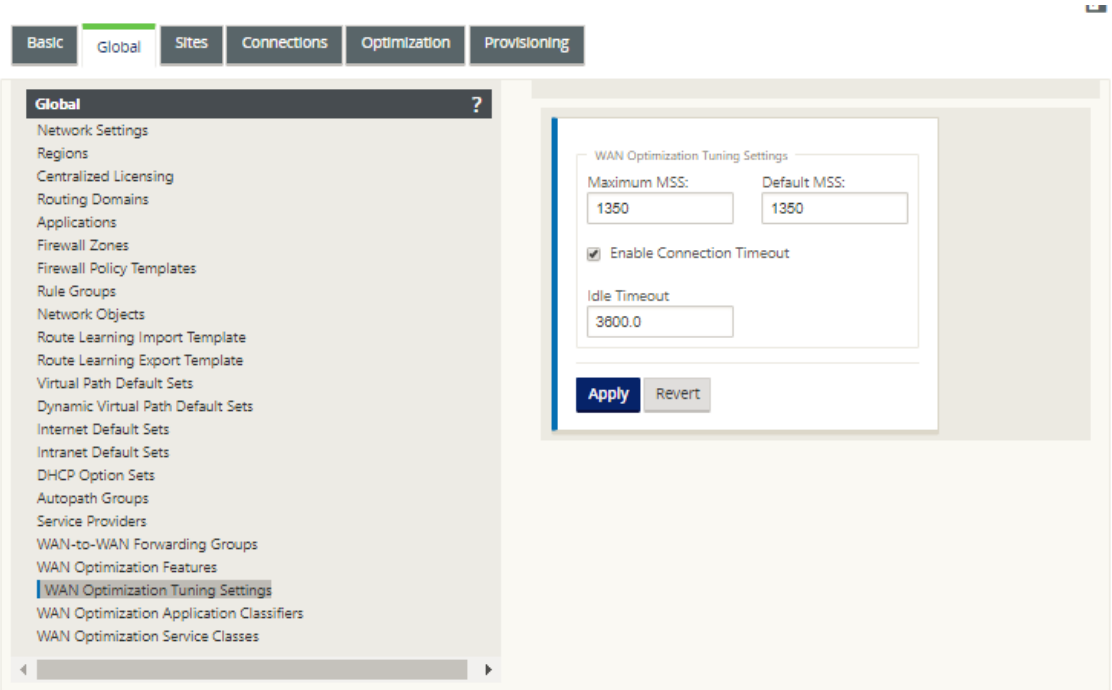
最適化のデフォルトチューニング設定の構成

May 10, 2021

[**Global**] タブで、WAN 最適化のデフォルトのチューニング設定を構成できます。

WAN Optimization のデフォルトの チューニング設定を構成するには、次の手順を実行します。

1. [グローバル] タブで、[**WAN Optimization** チューニング設定] をクリックします。



2. チューニング設定を選択して構成します。

   「チューニング設定」オプションは次のとおりです。

   - 「最大 **MSS** 」—TCP セグメントの最大セグメントサイズ（MSS）の最大サイズ（バイト単位）を入力します。
   - 「デフォルト **MSS**」—TCP セグメントの MSS のデフォルトサイズ（オクテット単位）を入力します。
   - 「接続タイムアウトの有効 化」—アイドルしきい値を超えたときに接続の自動終了を有効にする場合に選択します。
   - 「**Idle Timeout** 」—アイドル接続が終了するまでのアイドル時間の長さを指定するしきい値（秒単位）を入力します。このフィールドを構成するには、まず [接続タイムアウトの有効化] を選択する必要があります。

3. ［適用］をクリックします。

これにより、変更された チューニング設定が グローバル設定に適用されます。

次の手順では、WAN Optimization アプリケーション分類子のデフォルトセットを設定します。

最適化の既定のアプリケーション分類子の構成

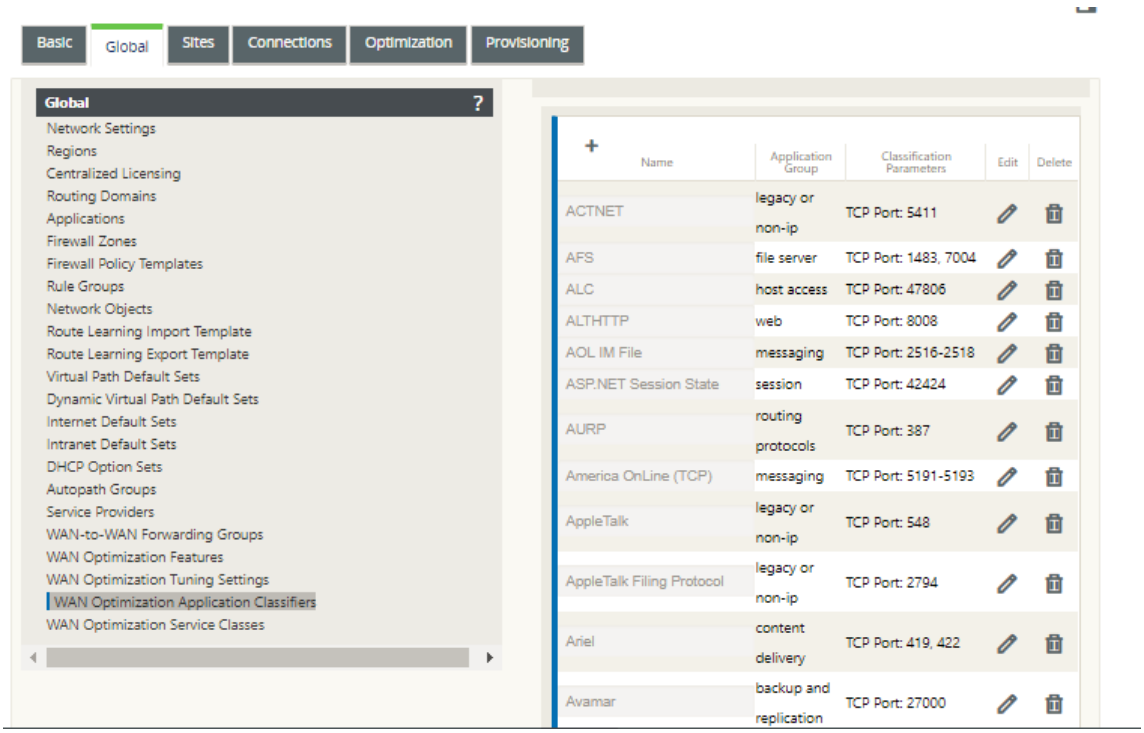
May 10, 2021

[**Global**] タブで、WAN 最適化のデフォルトのアプリケーション分類子設定を構成できます。

WAN Optimization アプリケーション分類子のデフォルトセットを設定するには、次の手順を実行します。

1. [グローバル] タブで、[**WAN Optimization** アプリケーション分類子] をクリックします。

   「アプリケーション分類子」(Application Classifiers) テーブルが開き、アプリケーション分類子のデフォルトのセットが表示されます。



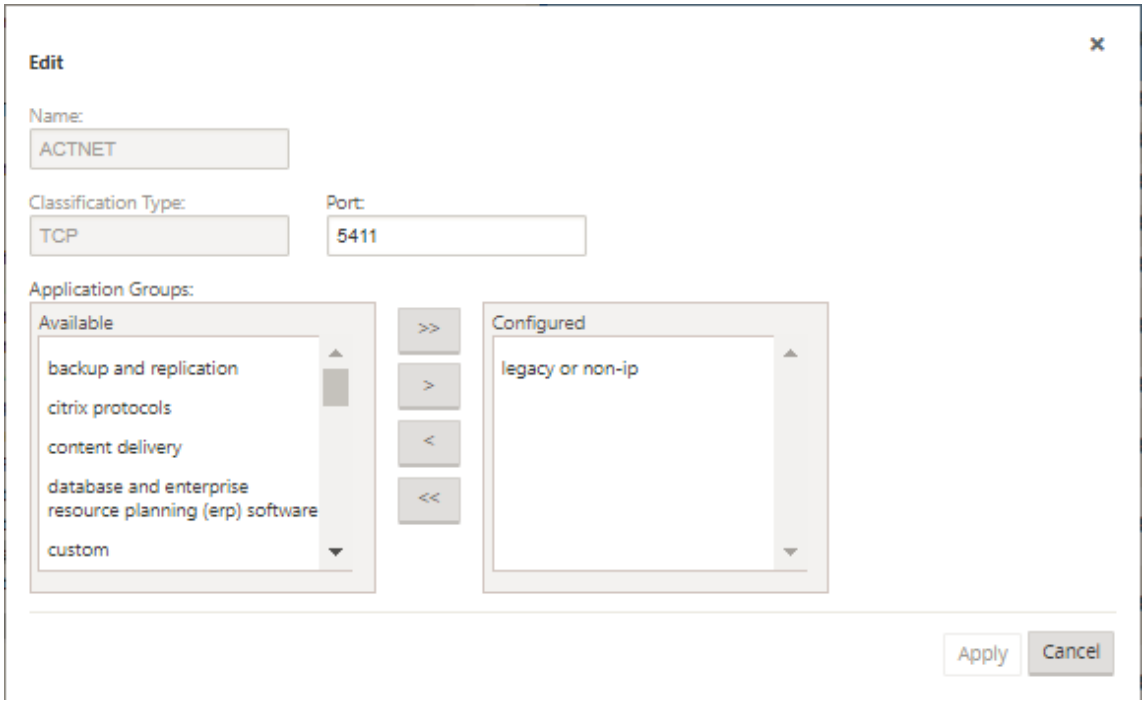
このテーブルは、設定フォームでもあります。このフォームを使用して、アプリケーション分類子を設定（編集）、削除、および追加して、カスタマイズされた既定のセットを作成できます。変更されたデフォルトの アプリケーション分類子 セットおよび構成する個々のアプリケーション分類子設定は、最適化 セクションツリーに含まれるブランチサイトにデフォルトとして自動的に適用されます。

> 注
>
> また、特定のブランチサイトごとに、アプリケーション分類子の セットと設定をカスタマイズすること

> もできます。手順については、ブランチサイトの最適化の構成を参照してください。

2. 既存のアプリケーション分類子を設定するには、その分類子エントリの [Edit] 列にある [**Edit**]（鉛筆アイコン）をクリックします。

   選択したアプリケーション分類子を設定するためのポップアップ設定の 編集 フォームが開きます。



3. [**Port**] フィールドに、アプリケーション分類子のポート番号を入力するか、デフォルトをそのまま使用します。

4. ［構成済み］ の一覧でアプリケーショングループを追加または削除するか、デフォルトを受け入れます。

   - 一覧にアプリケーショングループを追加するには、左側の [アプリケーショングループ 一覧] でアプリケーショングループを選択し、右矢印 (>) をクリックして、右側の [構成済み] リストにグループを追加します。すべての アプリケーショングループ を一覧に一度に追加するには、[すべて追加] 二重右矢印 (») をクリックします。
   - リストからアプリケーショングループを削除するには、右側の ［構成済み］ リストでアプリケーショングループを選択し、［削除］ 左矢印（<）をクリックします。一覧からすべての アプリケーショングループ を一度に削除するには、[すべて削除] 二重左矢印 («) をクリックします。

5. ［適用］ をクリックします。

   これにより、変更内容がアプリケーション分類子に適用され、**[設定の編集]** フォームが解除されます。

6. （オプション）デフォルトの アプリケーション分類子 セットをカスタマイズします。

   次のように、アプリケーション分類子を追加または削除して、デフォルトのセットをカスタマイズできます。

   - アプリケーション分類子をセットから削除する手順は、次のとおりです。

アプリケーション分類子の エントリの「削除」列にあるゴミ箱アイコンをクリックして、テーブルからそのエントリを削除します。

- アプリケーション分類子をセットに追加する手順は、次のとおりです。

  a) [アプリケーション分類子] ブランチラベルの右側にある [**+**] をクリックします。

     [設定の 追加] フォームが表示されます。

  b) [Name] フィールドと [Port] フィールドにアプリケーション分類子の 名前とポート番号 を入力します。

  c) ［構成済み］の一覧でアプリケーショングループを追加または削除します。

     一覧にアプリケーショングループを追加するには、左側の [アプリケーショングループ 一覧] でアプリケーショングループを選択し、右矢印 (>) をクリックして、右側の [構成済み] リストにグループを追加します。すべての アプリケーショングループ を一覧に一度に追加するには、[すべて追加] 二重右矢印 (») をクリックします。

     リストからアプリケーショングループを削除するには、右側の［構成済み］リストでアプリケーショングループを選択し、［削除］左矢印（<）をクリックします。一覧からすべての アプリケーショングループ を一度に削除するには、[すべて削除] 二重左矢印 («) をクリックします。

  d) ［適用］をクリックします。

     これにより、新しいアプリケーション分類子がセットに追加され、[**Add configuration]** フォームが中止されます。

     次のステップでは、WAN Optimization サービスクラスのデフォルトセットを構成します。

最適化のデフォルトサービスクラスを構成する

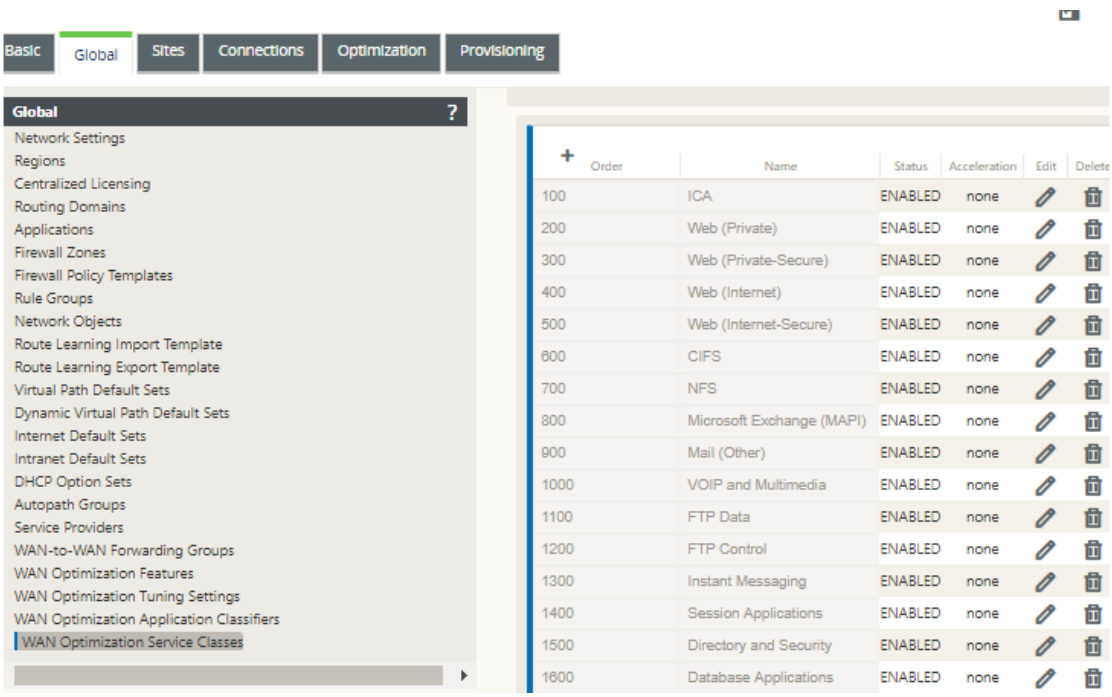
May 10, 2021

[**Global**] タブで、WAN 最適化のデフォルトサービスクラス設定を構成できます。

WAN Optimization サービスクラスのデフォルトセットを構成するには、次の手順を実行します。

1. [グローバル] タブで、[**WAN Optimization** サービスクラス**]** をクリックします。

   「サービスクラス」**(Service Class** es) テーブルが開き、デフォルトのサービスクラスセットが表示されます。

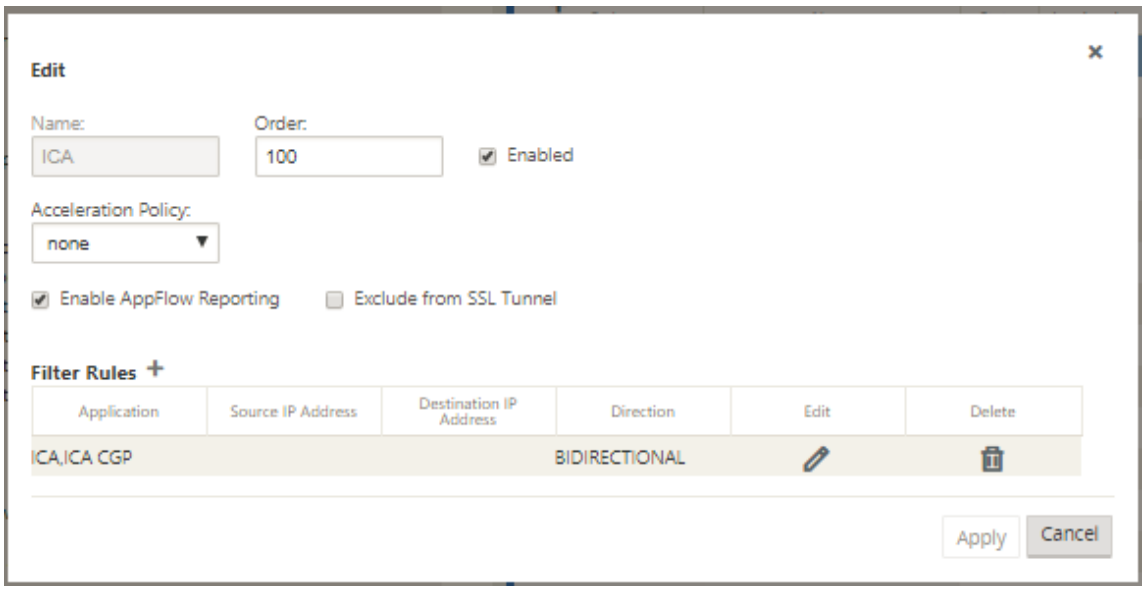


このテーブルは、設定フォームでもあります。このフォームを使用して、サービスクラスを設定（編集）、削除、および追加して、カスタマイズされた既定のセットを作成できます。変更されたデフォルトの サービスクラ ス・セットおよび構成した個々のサービスクラスの設定は、最適化 セクション・ツリーに含まれるブランチ・サイトにデフォルトとして自動的に適用されます。

> 注
>
> また、特定のブランチサイトごとに サービスクラス セットと設定をカスタマイズすることもできます。ブランチサイトの 最適化 設定をカスタマイズする手順については、「ブランチサイトの最適化の構成」の項を参照してください。

2. 既存のサービスクラスを設定するには、[Service Class] テーブルでそのクラスエントリの [**Edit**] 列にある [Edit]（鉛筆アイコン）をクリックします。

   選択したサービスクラスを設定するためのポップアップ設定 を編集 フォームが開きます。



3. サービスクラスの基本設定を構成します。

   基本的な設定は次のとおりです。

   - 「有効」—新しいサービスクラスを有効にする場合に選択します。このクラスはデフォルトで有効になっています。
   - 「アクセラレーションポリシー」—「アクセラレーションポリシー」ドロップダウンメニューからポリシーを選択します。使用できるオプションは、次のとおりです:
     - **disk** —圧縮に使用するトラフィック履歴を保存する場所としてアプライアンスディスクを指定する場合は、このポリシーを選択します。これにより、このサービスクラスのディスクベース圧縮（DBC）ポリシーが有効になります。一般的に、アプライアンスは、トラフィックに適した ** ディスク ** または メモリ をストレージの場所として自動的に選択するため、通常はディスクのポリシーが最適です。
     - **none**： このサービスクラスに対してアクセラレーションポリシーを有効にしない場合は、このオプションを選択します。通常、**none** というポリシーは、圧縮不可能な暗号化トラフィックとリアルタイムビデオにのみ使用されます。
     - **flow control Only**： 圧縮を無効にしますが、フロー制御アクセラレーションを有効にするには、このポリシーを選択します。常に暗号化されるサービス、および FTP 制御チャネルの場合はこれを選択します。
     - **memory**： 圧縮に使用されるトラフィック履歴を保存する場所としてメモリを指定するには、このポリシーを選択します。
   - 「**AppFlow** レポートを有効にする」—このサービスクラスに対して AppFlow レポートを有効にする場合は、これを選択します。AppFlow は、ネットワークインフラストラクチャによって処理されるアプリケーショントランザクションデータのロックを解除するための業界標準です。WAN Optimization AppFlow インターフェイスは、任意の AppFlow コレクタと連携してレポートを生成します。コレク

タは、AppFlow オープン標準（http://www.appflow.org）を使用して、アプライアンスから詳細情報を受け取ります。

AppFlow の詳細については、Citrix ドキュメントポータルhttp://docs.citrix.com/にある Citrix CloudBridge 7.4 製品ドキュメントを参照してください。

> 注
>
> WAN Optimization AppFlow レポートを表示するには、[モニタリング] タブを選択し、ナビゲーションツリー (左ペイン) で [**WAN Optimization**] ブランチを開き、[**AppFlow]** を選択します。「仮想 WAN の監視」も参照してください。

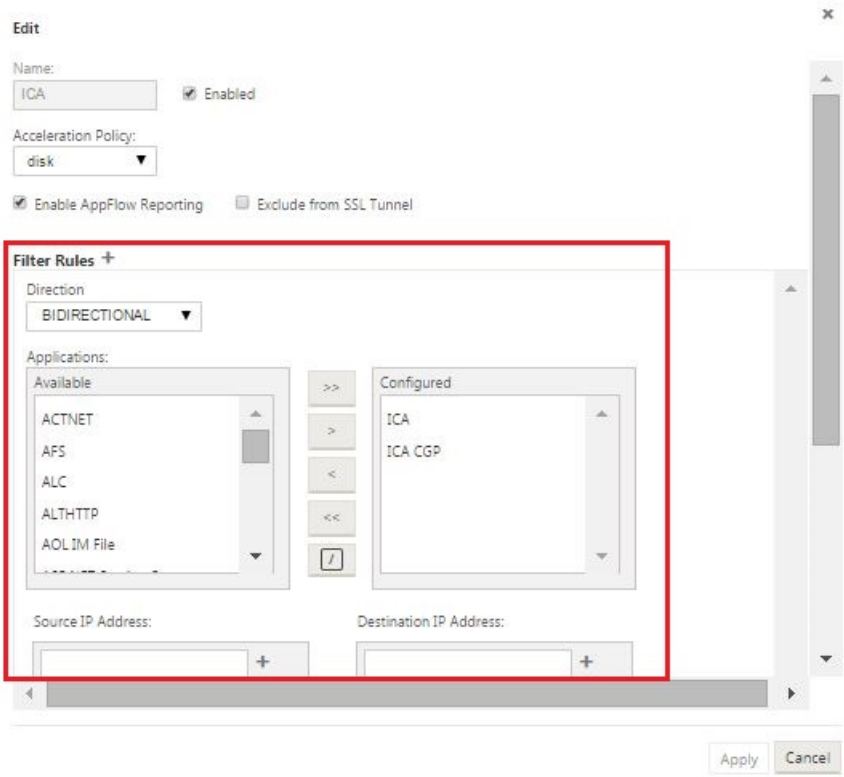
- 「**SSL** トンネルから除外」—サービスクラスに関連付けられたトラフィックを SSL トンネリングから除外する場合に選択します。

4. サービスクラスの フィルタ規則 を設定します。

既存のルールを編集するには、次の操作を行います。

a) [フィルタルール] テーブル (フォームの下部) で、編集するルールの [編集] 列にある [編集] (鉛筆のアイコン) をクリックします。

これにより、選択したフィルタ規則のフィルタ規則設定が表示されます。



b) [方向] ドロップダウンメニューからフィルタの方向を選択します。

次のいずれかのオプションを選択します:

- 双方向
- 単方向

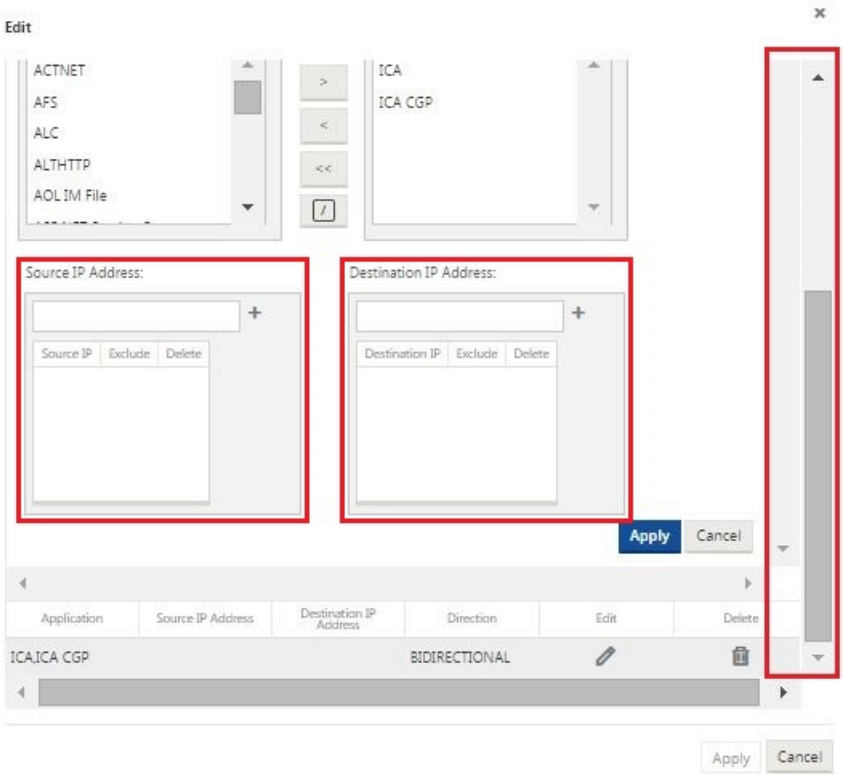
c) [構成済み] の一覧でアプリケーションを追加または削除します。

リストにアプリケーションを追加するには、左側の [アプリケーション] リストでアプリケーションを選択し、右矢印 (**>**) をクリックして、右側の [構成済み] リストにグループを追加します。すべてのアプリケーションを一覧に一度に追加するには、[すべて追加] 二重右矢印 (**»**) をクリックします。

リストからアプリケーションを削除するには、右側の［構成済み］リストでアプリケーションを選択し、［削除］左矢印 （**<**）をクリックします。一覧からすべての アプリケーションを 一度に削除するには、[すべて削除] 二重左矢印 (**«**) をクリックします。

d) 下にスクロールして、フォームの切り捨てられた部分を表示します。

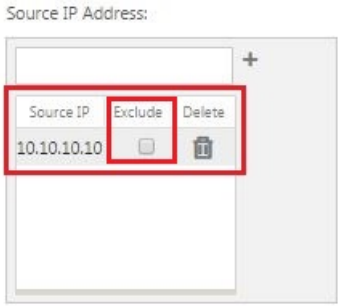
[**Filter Rules**] の設定セクションは多少長いため、スクロールバーを使用してフォームの切り捨てられた部分を表示する必要があります。



e) [送信元 IP アドレス] フィールドに 送信元 **IP** アドレスを入力します。

f) 入力した送信元 IP アドレスの右側にある [**+**] をクリックします。

これにより、指定した IP アドレスが 送信元 **IP** アドレス テーブルに追加されます。



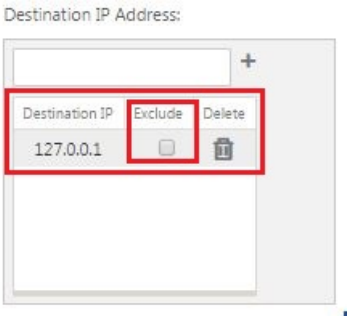
g) このフィルタ規則の送信元 IP アドレスを含めるか除外するかを指定します。

[除外] チェックボックスをオンにして、指定した送信元 IP アドレスをこのフィルタ規則から除外します。アドレスを含めるには、チェックボックスの選択を解除します。

h) [宛先 IP アドレス] フィールドに 宛先 **IP** アドレスを入力します。

i) 先ほど入力した [宛先 IP アドレス] の右側にある [**+**] をクリックします。

これにより、指定した IP アドレスが 送信元 **IP** アドレス テーブルに追加されます。



j) このフィルタ規則の宛先 IP アドレスを含めるか除外するかを指定します。

[除外] チェックボックスをオンにして、指定した宛先 IP アドレスをこのフィルタ規則から除外します。アドレスを含めるには、チェックボックスの選択を解除します。

k) [適用] をクリックします。

これにより、変更内容がルールに適用され、[フィルタルール 設定] セクションが非表示になります。

5. （オプション）デフォルトの サービスクラス セットをカスタマイズします。

次のように、サービスクラスを追加または削除して、デフォルトセットをカスタマイズできます。

- セットからサービスクラスを削除する手順は、次のとおりです。

  テーブル内のサービスクラス・エントリの「削除」(**Delete**) 列にあるゴミ箱アイコンをクリックして、そのエントリを削除します。

- サービスクラスをセットに追加するには、次の手順に従います。

  a) [サービスクラス] ブランチのラベルの右側にある [**+**] をクリックします。

  [設定の 追加] フォームが表示されます。

b)「名前」フィールドに新しいサービスクラスの名前を入力します。

c) 新しいサービスクラスを設定します。

新しいサービスクラスを設定する手順は、既存のサービスクラスを変更する場合と同じです。手順については、このセクションの前の手順を参照してください。

“3. サービスクラスの基本設定を行います。

“4. サービスクラスのフィルタ規則を設定します。

d) [**Add**] をクリックして、新しいサービスクラスをデフォルトセットに追加し、[**Add configuration]** フォームを閉じます。

6.（オプション、推奨）構成パッケージ を保存します。

これで、グローバル WAN Optimization 構成が完了し、ブランチサイトの 最適化 セットと設定の構成を開始できます。

ブランチサイトの最適化を構成する

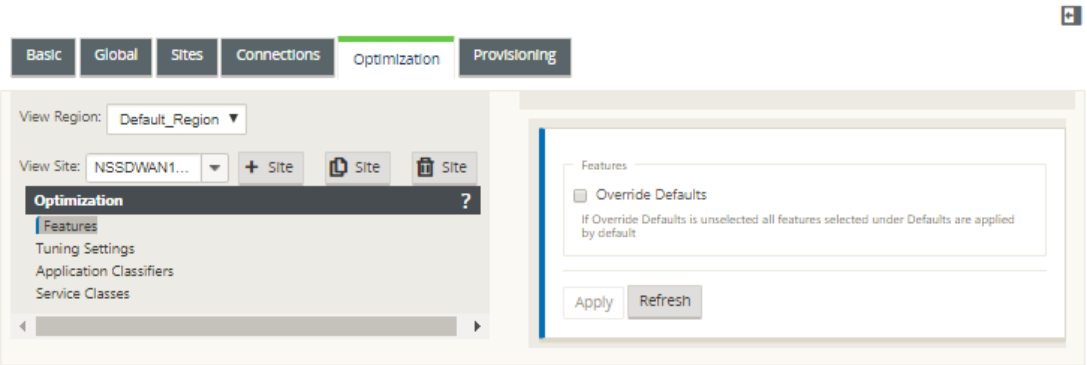
May 10, 2021

デフォルトのグローバル構成が完了したら、各ブランチサイトのセットと設定をカスタマイズできます。

構成したグローバル設定は、[最適化] セクションに含まれる各ブランチサイトに自動的に適用されます。デフォルトを受け入れるか、特定のブランチの設定をカスタマイズするかを選択できます。ブランチサイトの 最適化 セットと設定の構成手順は、グローバルデフォルトの設定と同じですが、いくつかの小さな違いがあります。

ブランチサイトの 最適化 構成をカスタマイズするには、次の手順を実行します。

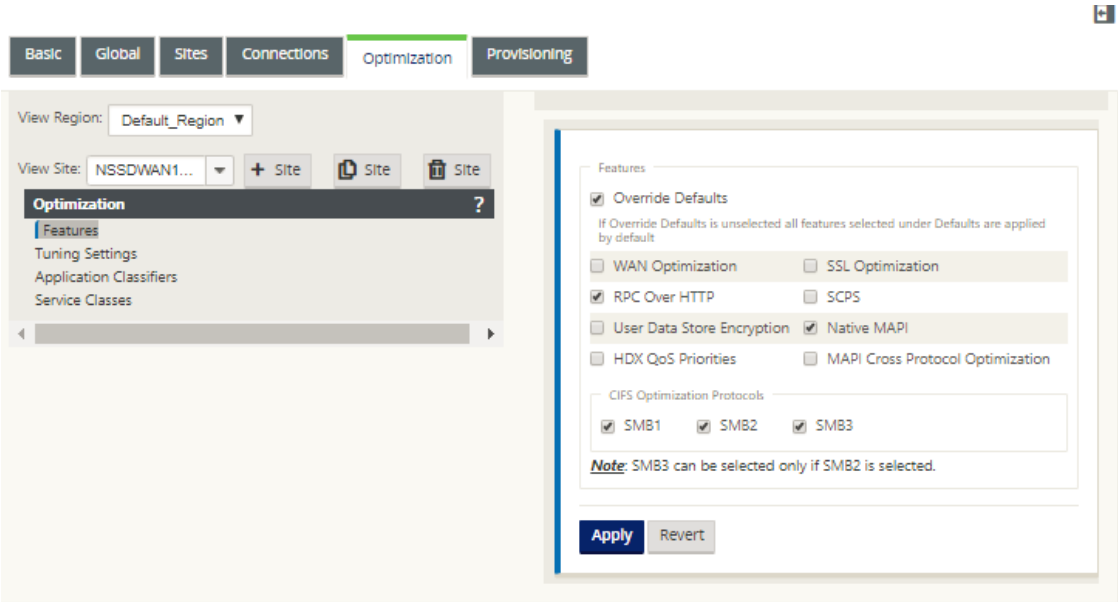
1. [最適化] タブの [サイトの表示] フィールドで、サイトを選択します。



2.「デフォルトを上書き」チェックボックスを選択します。

これにより、その構成カテゴリの最上位の設定フォームが表示され、編集用に開きます。

下の画像は、トップレベル設定設定フォームの例を示しています。この例では、機能 セットです。



3. 設定の変更を入力します。

   この時点から、各ブランチサイトの **Optimization** カテゴリの構成プロセスは、対応するグローバルセクションカテゴリと同じになります。特定のカテゴリのセットまたは設定を構成する方法については、以下の該当するセクションを参照してください。

   - 最適化の有効化と既定の機能設定の構成
   - 「最適化のデフォルト・チューニング設定の構成」を参照してください。
   - 「最適化のデフォルトアプリケーション分類子の設定」を参照してください。
   - 「最適化のデフォルトサービスクラスの設定」を参照してください。

4. （オプション、推奨）構成パッケージ を保存します。

   これで、仮想 WAN の 最適化 セクションセットと設定の構成が完了しました。

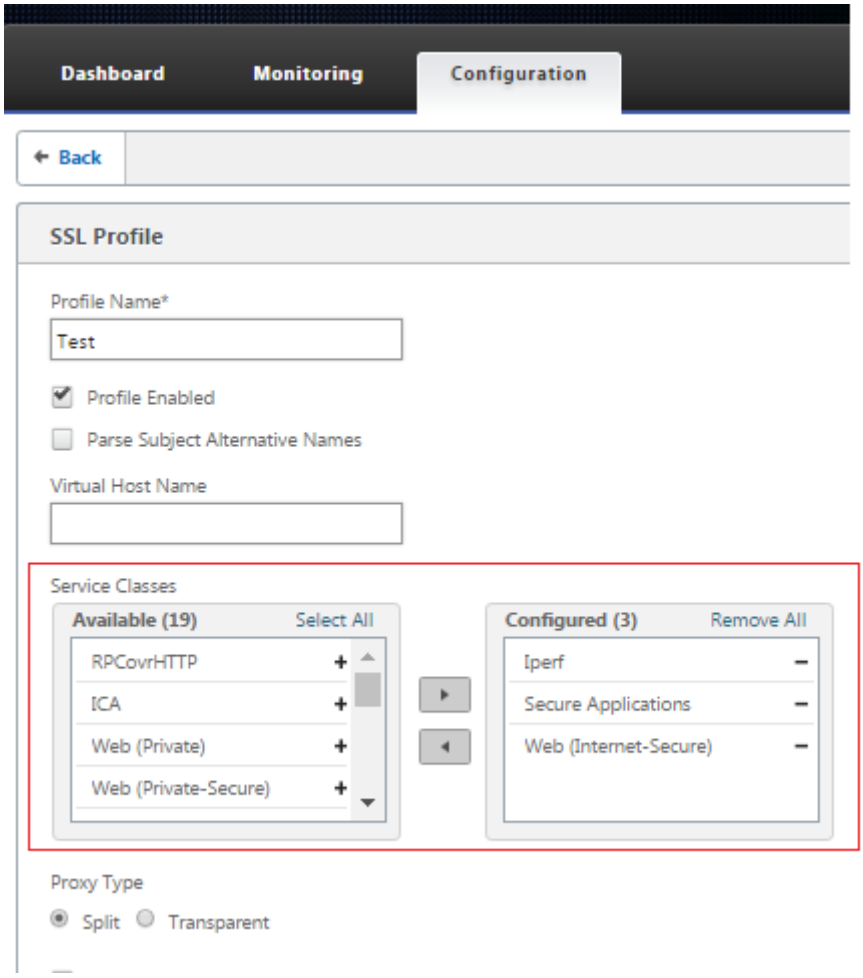
SSL プロファイルの設定

May 10, 2021

セキュリティと使いやすさのために、すべての SSL 関連の設定は、アプライアンスの新しい設定エディタから利用できます。SD-WAN Premium (Enterprise) エディションおよび 2 ボックスデプロイでは、サービスクラスは構成エディタから構成されるため、SSL プロファイルをアタッチすることはできません。サービスクラスへの SSL プロファイルマッピングの式に対応するために、SSL プロファイルのワークフローが変更され、プロファイルノードにサービスクラスをアタッチできるようになります。

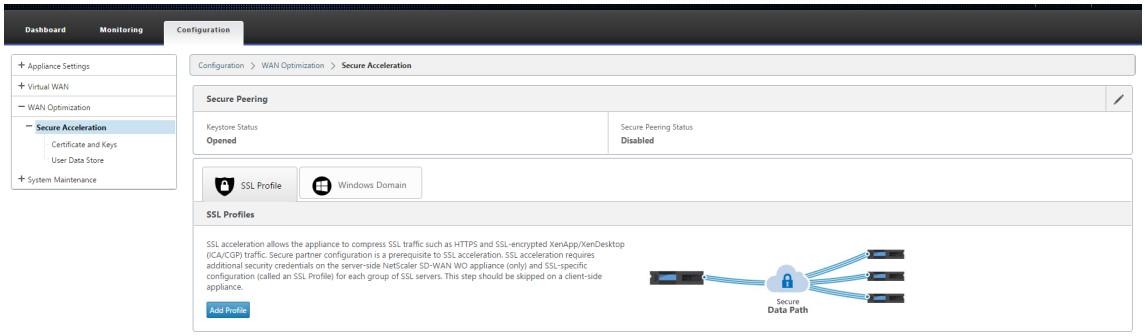
制限の 1 つは、SSL プロファイルがサービスクラス内のすべてのルールにアタッチされることです。SSL プロファイルを特定のルールに選択的にアタッチする必要がある場合、サービスクラス設定は詳細ルールに分割され、さらに選択できるようになります。

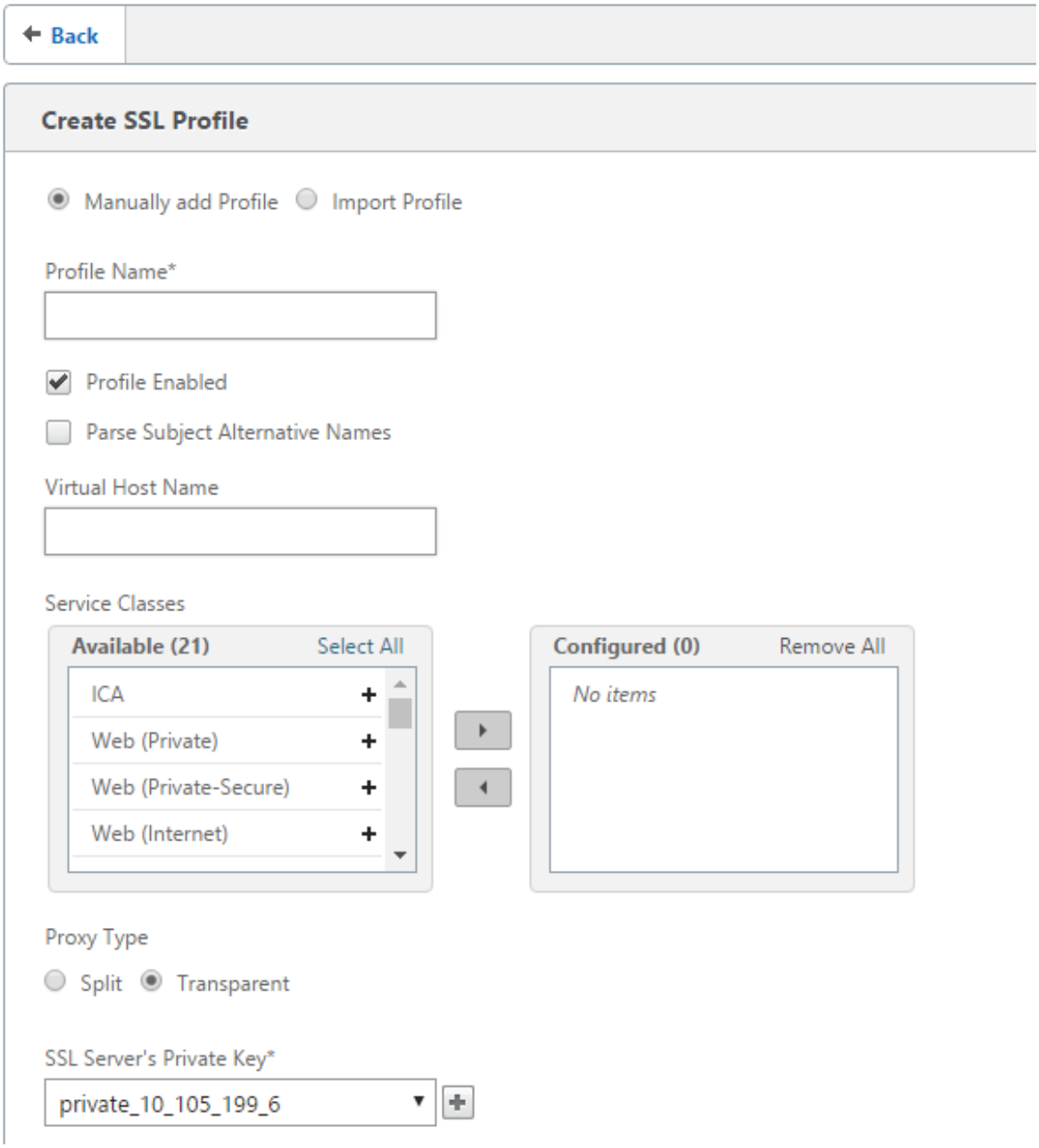
> 注
>
> SSL プロファイルに関連付けることができるのは、フィルタールールの方向が単方向に設定されているサービスクラスのみです。



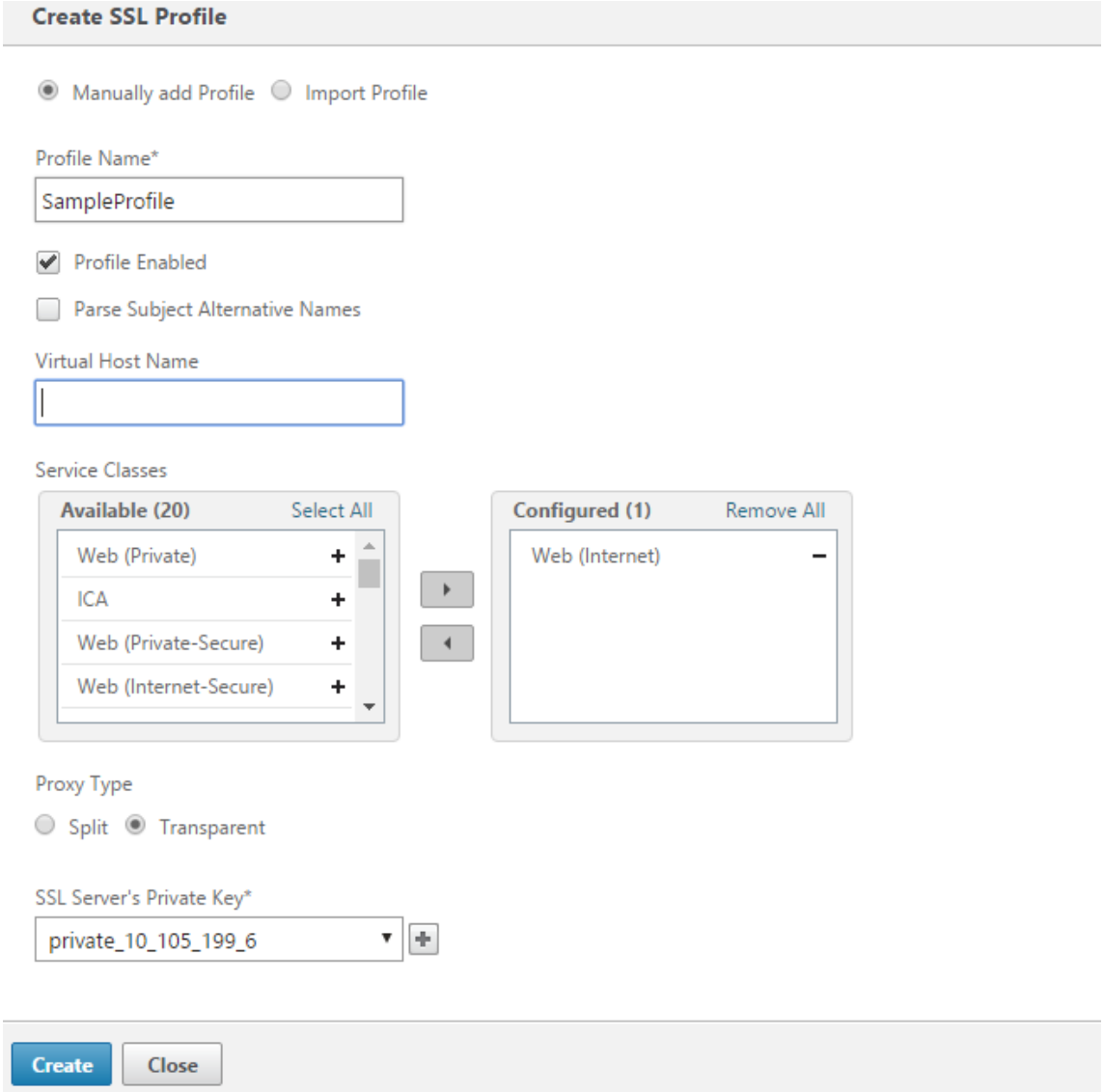
データセンターで新しい Premium (Enterprise) Edition アプライアンスで SSL プロファイルを作成するには:

1. SD-WAN Web GUI で、[設定] > [セキュアアクセラレーション] ページに移動します。[プロファイルの追加] をクリックします。**SSL** プロファイルを作成します。

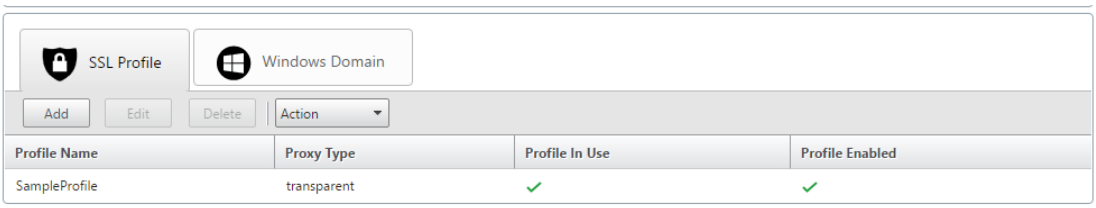




2. [**SSL** プロファイルの作成] ページで、プロファイル名を指定し、このプロファイルに関連付ける [サービスクラス] を選択します。[プロキシタイプ] を選択し、関連データを入力して [作成] をクリックします。



3. SSL プロファイルが正常に作成され、サービスクラスが関連付けられた後、以下に示すように、SSL プロファイル情報を表示します。



Citrix WAN 最適化クライアントプラグイン

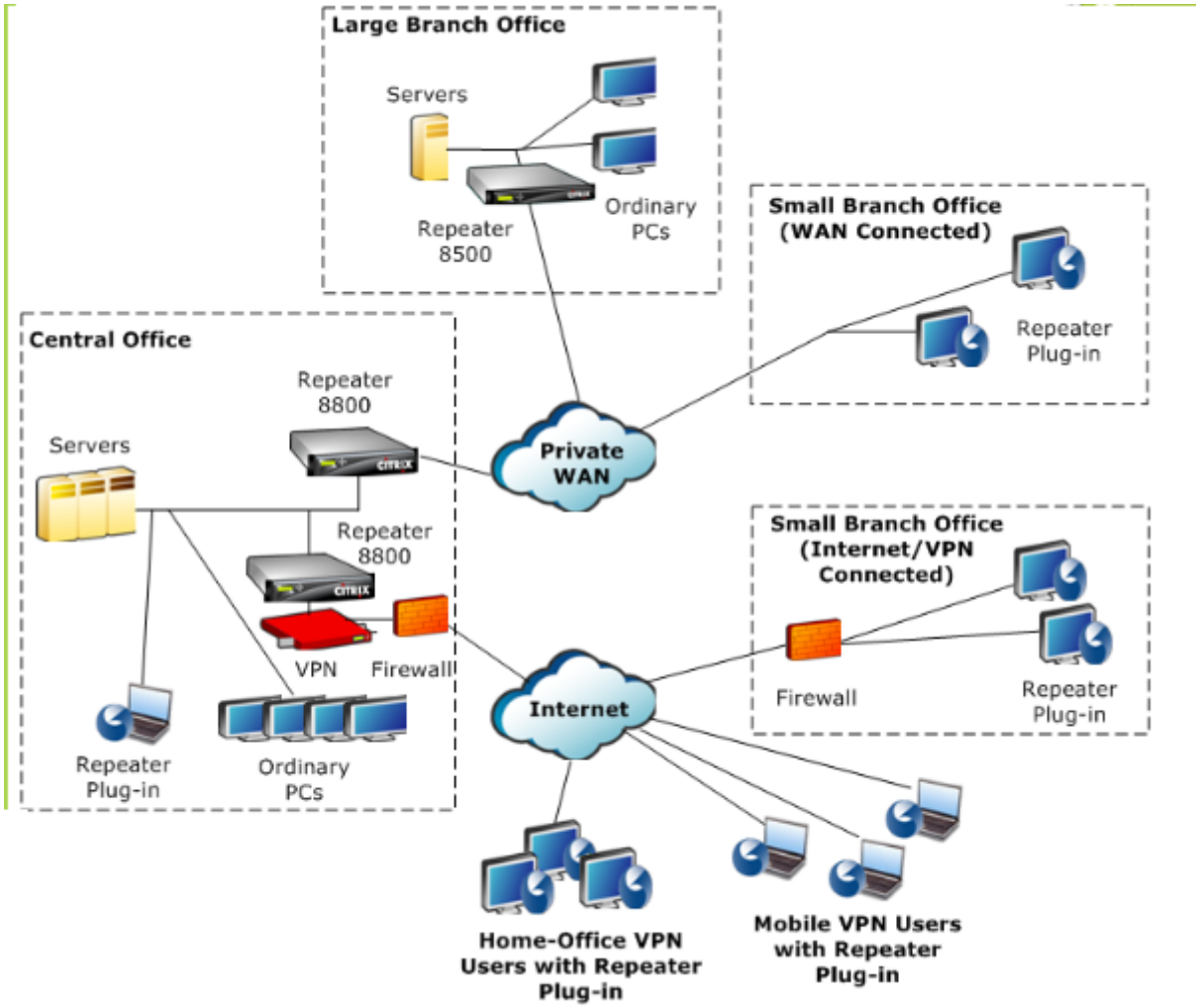
May 10, 2021

Citrix WANOP クライアントプラグインは、Windows ノートパソコンやワークステーションで動作するソフトウェアベースのネットワークアクセラレータで、WANOP クライアントプラグインアプライアンスを使用するオフィスだけでなく、どこでもアクセラレーションを提供します。リンクのもう一方の端にある Citrix WANOP クライアントプラグインアプライアンスに接続します。

WANOP クライアントプラグインの動作原理は、通常、WANOP クライアントプラグインアプライアンスの原理と同じです。プラグインのドキュメントに含まれていないトピックについては、より大きなドキュメントセットを参照してください。

プラグインは、標準の Microsoft インストールファイル（MSI）として配布されます。プラグインの展開では、リンクの反対側に WANOP Client Plug-in アプライアンスのプラグイン固有の設定が必要です。WANOP Client Plug-in アプライアンスの DNS または IP アドレス、およびその他のいくつかのパラメータを使用して MSI ファイルをカスタマイズする場合、ユーザーは Windows コンピューターにプラグインをインストールするときに構成情報を入力する必要はありません。

図 1：WANOP クライアントプラグインを示す典型的な WANOP クライアントプラグインネットワーク



> 注
>
> プラグインは Citrix Receiver 1.2 以降でサポートされており、Citrix Receiver で配布および管理できます。

ハードウェアとソフトウェアの要件

May 10, 2021

アクセラレーションリンクのクライアント側では、
WANOP Client Plug-in は Windows デスクトップおよびノートブックシステムではサポートされますが、ネットブックやシンクライアントではサポートされません。WANOP クライアントプラグインを実行するコンピューターには、以下の最低限のハードウェア仕様をお勧めします。

- Pentium4 クラス CPU

- 2GB の RAM
- 2GB の空きディスク容量

WANOP クライアントプラグインは Windows10 プラットフォームでサポートされており、次のシステム要件が必要です。

- 4GB RAM
- 10GB の空きディスク容量

WANOP クライアントプラグインは、次のオペレーティングシステムでサポートされています。

- Windows XP Home
- Windows XP Professional
- Windows Vista（Home Basic、Home Premium、Business、Enterprise、Ultimate のすべての 32 ビットバージョン）
- Windows 7（Home Basic、Home Premium、Professional、Enterprise、および Ultimate のすべての 32 ビットおよび 64 ビットバージョン）
- Windows 8 (32 ビット版と 64 ビット版の Premium エディション)
- Windows 10 (32 ビット版と 64 ビット版の Premium エディション)

サーバー側では、次のアプライアンスが現在、WANOP クライアントプラグインのデプロイメントをサポートしています。

- Repeater 8500 Series
- Repeater 8800 Series
- WANOP クライアントプラグイン VPX
- WANOP クライアントプラグイン 2000
- WANOP クライアントプラグイン 3000
- WANOP クライアントプラグイン 4000
- WANOP クライアントプラグイン 5000

WANOP プラグインの仕組み

May 10, 2021

WANOP クライアントプラグイン製品は既存のものを使用します WAN/VPN インフラ。プラグインがインストールされているコンピューターは、プラグインのインストール前と同じように、LAN、WAN、およびインターネットに引

き続きアクセスします。ルーティングテーブル、ネットワーク設定、クライアントアプリケーション、またはサーバーアプリケーションを変更する必要はありません。

Citrix Access Gateway VPN には、少量の WANOP クライアントプラグイン固有の構成が必要です。

プラグインとアプライアンスによる接続の処理方法には、トランスペアレントモードとリダイレクタモード ** の *2* つのバリエーションがあります。リダイレクタは、新しい展開では推奨されないレガシーモードです。

- プラグインからアプライアンスへのアクセラレーションの透過モード は、アプライアンスからアプライアンスへのアクセラレーションと非常によく似ています。WANOP クライアントプラグインアプライアンスは、プラグインとサーバー間を移動するときにパケットがたどるパス内にある必要があります。アプライアンス間のアクセラレーションと同様に、透過モードは透過プロキシとして動作し、接続の一方の端からもう一方の端までの送信元と宛先の IP アドレスとポート番号を保持します。
- リダイレクタモード（推奨されません）は、明示的なプロキシを使用します。プラグインは、発信パケットをアプライアンスのリダイレクタ IP アドレスに再アドレス指定します。次に、アプライアンスはパケットをサーバーに再アドレス指定し、リターンアドレスをプラグインではなく自身を指すように変更します。このモードでは、アプライアンスは WAN インターフェースとサーバー間のパスと物理的にインラインである必要はありません（これは理想的な展開ですが）。

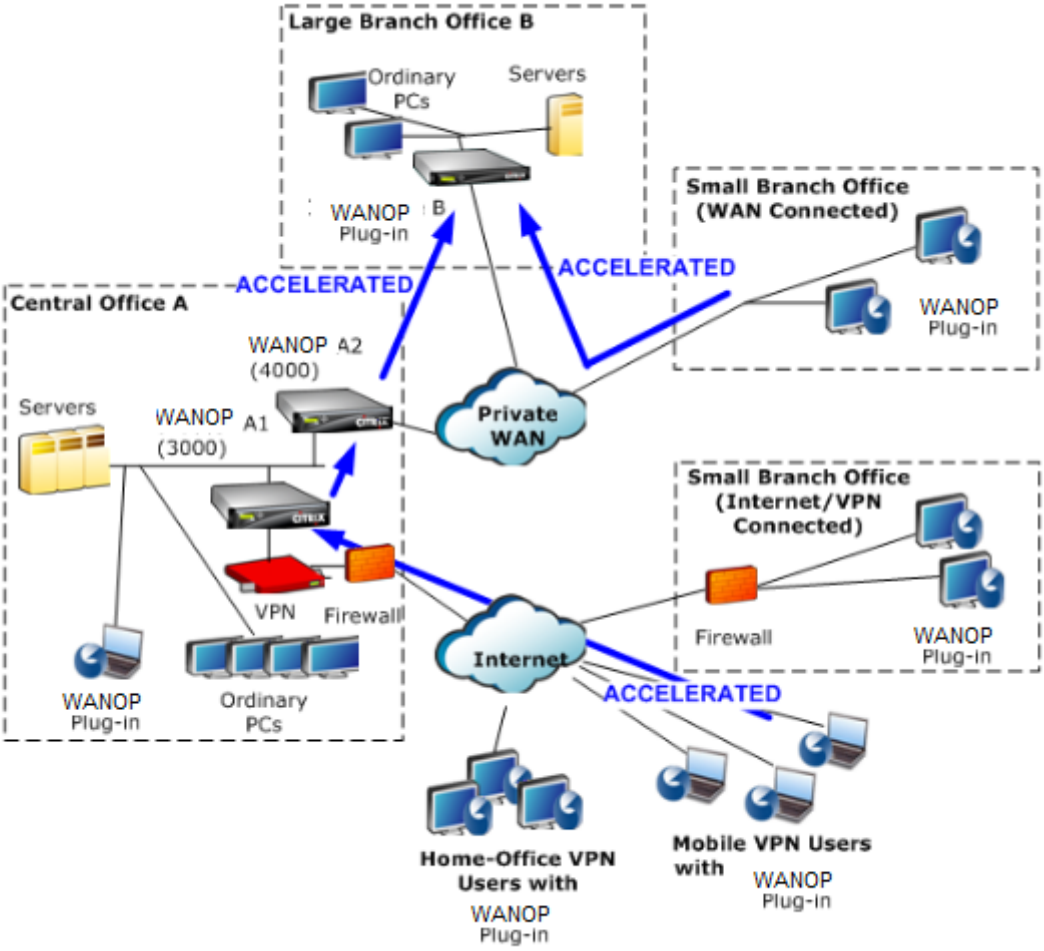
  ベストプラクティス：可能な場合は透過モードを使用し、必要な場合はリダイレクタモードを使用します。

透過モード

透過モードでは、高速化された接続のパケットは、アプライアンス間の高速化の場合と同様に、ターゲットアプライアンスを通過する必要があります。

プラグインは、アクセラレーションに使用できるアプライアンスのリストで構成されます。各アプライアンスへの接続を試み、シグナリング接続を開きます。シグナリング接続が成功すると、プラグインはアプライアンスからアクセラレーションルールをダウンロードし、アプライアンスがアクセラレーションできる接続の宛先アドレスを送信します。

図 1：透過モード、3 つの加速パスを強調表示



注

- トラフィックフロー：トランスペアレントモードは、WANOP クライアントプラグインとプラグイン対応アプライアンスの間の接続を高速化します。
- ライセンス-アプライアンスには、必要な数のプラグインをサポートするためのライセンスが必要です。この図では、Repeater A1 はサイト A のプラグインアクセラレーションを提供するため、Repeater A2 にプラグインアクセラレーションのライセンスを付与する必要はありません。
- デイジーチェーン-接続がターゲットアプライアンスに向かう途中で複数のアプライアンスを通過する場合、中央のアプライアンスで「デイジーチェーン」を有効にする必要があります。そうしないと、アクセラレーションがブロックされます。この図では、大規模ブランチオフィス B を宛先とするホームオフィスおよびモバイル VPN ユーザからのトラフィックが、Repeater B によって加速されます。これを機能させるには、Repeater A1 および A2 でデイジーチェーンが有効になっている必要があります。

プラグインが新しい接続を開くたびに、加速ルールを参照します。宛先アドレスがいずれかのルールに一致する場合、プラグインは、接続の最初のパケット（SYN パケット）にアクセラレーションオプションを付加することにより、接続をアクセラレーションしようとします。プラグインに認識されているアプライアンスが SYN-ACK 応答パケットに

アクセラレーションオプションを接続すると、そのアプライアンスとのアクセラレーション接続が確立されます。

アプリケーションとサーバーは、高速接続が確立されたことを認識していません。プラグインソフトウェアとアプライアンスだけが、加速が行われていることを認識しています。

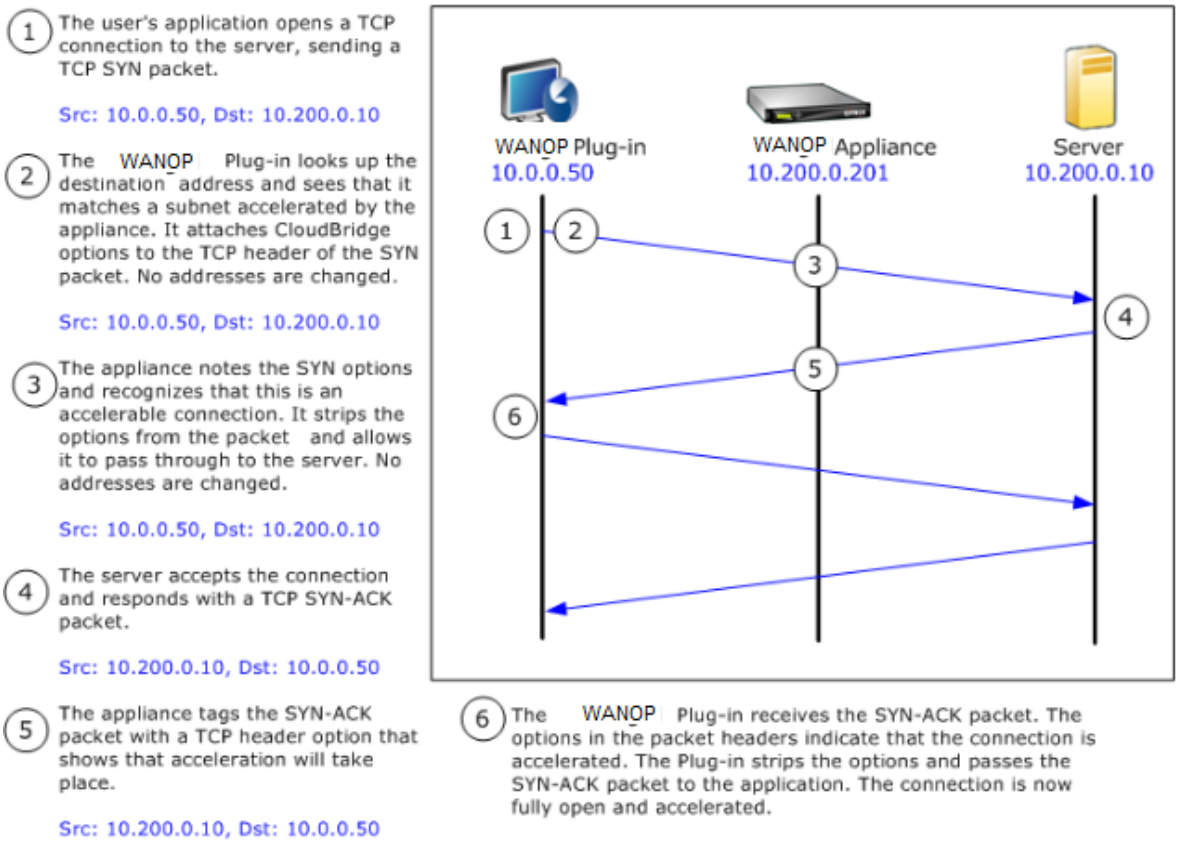
透過モードは、アプライアンス間のアクセラレーションに似ていますが、同じではありません。違いは次のとおりです。

- クライアントが開始する接続のみ-透過モードは、プラグインを備えたシステムによって開始される接続のみを受け入れます。プラグインを搭載したシステムをサーバーとして使用する場合、サーバー接続は高速化されません。一方、アプライアンス間のアクセラレーションは、どちらの側がクライアントでどちらがサーバーであるかに関係なく機能します。（アクティブモード FTP は、プラグインによって要求されたデータ転送を開始する接続がサーバーによって開かれるため、特殊なケースとして扱われます。）
- シグナリング接続-透過モードは、ステータス情報の送信にプラグインとアプライアンス間のシグナリング接続を使用します。アプライアンス間のアクセラレーションは、デフォルトで無効になっているセキュアなピア関係を除いて、シグナリング接続を必要としません。プラグインがシグナリング接続を開くことができない場合、アプライアンスを介した接続を高速化しようとはしません。
- デイジーチェーン接続-プラグインとその選択したターゲットアプライアンスの間のパスにあるアプライアンスの場合、［構成：チューニング］メニューでデイジーチェーンを有効にする必要があります。

透過モードは、VPN でよく使用されます。WANOP クライアントプラグインプラグインは、ほとんどの IPSec および PPTP VPN、および Citrix Access GatewayVPN と互換性があります。

次の図は、透過モードでのパケットフローを示しています。このパケットフローは、接続の高速化を試みるかどうかの決定がシグナリング接続を介してダウンロードされた高速化ルールに基づくことを除いて、アプライアンス間の高速化とほぼ同じです。

図 2：透過モードでのパケットフロー



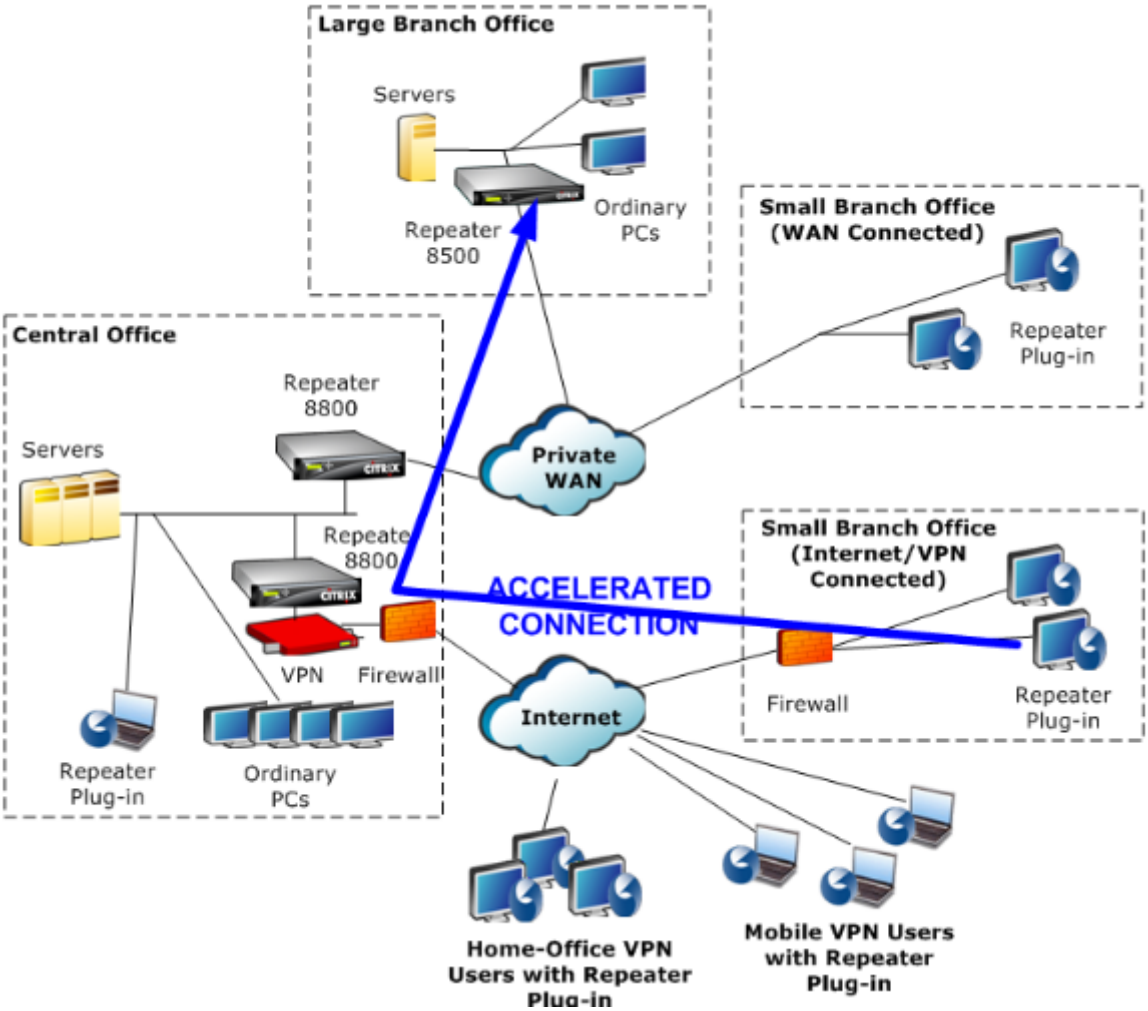
リダイレクタモード

リダイレクタモードは、次の点で透過モードとは動作が異なります。

- WANOP クライアントプラグインプラグインソフトウェアは、パケットをアプライアンスに明示的にアドレス指定することにより、パケットをリダイレクトします。
- したがって、リダイレクタモードアプライアンスは、すべての WAN リンクトラフィックを傍受する必要はありません。アクセラレーションされた接続は直接アドレス指定されるため、プラグインとサーバーの両方から到達できる限り、どこにでも配置できます。
- アプライアンスは最適化を実行してから、出力パケットをサーバーにリダイレクトし、パケット内の送信元 IP アドレスを独自のアドレスに置き換えます。サーバーの観点からは、接続はアプライアンスで開始されます。
- サーバーからのリターントラフィックはアプライアンスにアドレス指定されます。アプライアンスはリターン方向で最適化を実行し、出力パケットをプラグインに転送します。
- 宛先ポート番号は変更されないため、ネットワーク監視アプリケーションは引き続きトラフィックを分類できます。

次の図は、リダイレクタモードがどのように機能するかを示しています。

図 1: リダイレクタモード



次の図は、リダイレクタモードでのパケットフローとアドレスマッピングを示しています。

図 2：リダイレクタモードでのパケットフロー

1. The user's application opens a TCP connection to the server, sending a TCP SYN packet.

   Src: 10.0.0.50, Dst: 10.200.0.10

2. The Repeater Plug-in looks up the dst address and decides to redirect the connection to the appliance at 10.200.0.201.

   Src: 10.0.0.50, Dst: 10.200.0.201

   (10.200.0.10 is preserved in a TCP option field. Options 24-31 are used for various parameters.)

3. The appliance accepts the connection and forwards the packet to the server (using the dst address from the TCP options field), and giving itself as the src.

   Src: 10.200.0.201, Dst: 10.200.0.10

4. The server accepts the connection and responds with a TCP SYN-ACK packet.

   Src: 10.200.0.10, Dst: 10.200.0.201

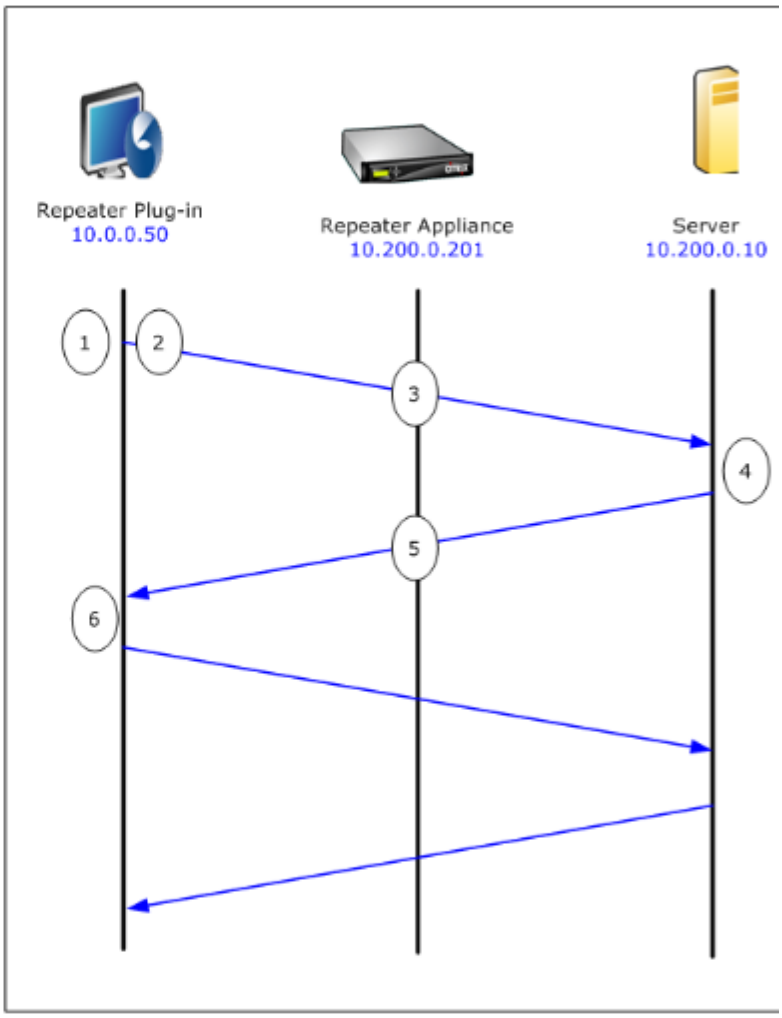
5. The appliance rewrites the addresses and forwards the packet to the Plug-in (placing the server address in an option field).

   Src: 10.200.0.201, Dst: 10.0.0.50

6. The connection is now fully open. The client and server send packets back and forth via the appliance.

   While the addresses are altered in Redirector mode, the destination port numbers are not (though the ephemeral port number may be). The data is not encapsulated. Redirector mode is a proxy, not a tunnel.

   There is no 1:1 relationship between packets (though in the end, the data received is always identical to the data sent). Compression may reduce many input packets into a single output packet. CIFS acceleration will perform speculative read-ahead and write-behind operations. Also, if packets are dropped between appliance and the Repeater Plug-in, the retransmission is handled by the appliance, not the server, using advanced recovery algorithms.



プラグインがアプライアンスを選択する方法

各プラグインは、高速接続を要求するために接続できるアプライアンスのリストで構成されています。

アプライアンスにはそれぞれ、アクセラレーション規則のリストがあります。これは、アプライアンスがアクセラレーション接続を確立できるターゲット・アドレスまたはポートのリストです。プラグインはこれらのルールをアプライアンスからダウンロードし、各接続の宛先アドレスとポートを各アプライアンスのルールセットと照合します。特定の接続を高速化するアプライアンスが 1 つしかない場合、選択は簡単です。複数のアプライアンスが接続を高速化することを提案している場合、プラグインはアプライアンスの 1 つを選択する必要があります。

アプライアンスの選択のルールは次のとおりです。

- 接続を高速化するために提供しているすべてのアプライアンスがリダイレクタモードアプライアンスである場合、プラグインのアプライアンスリストの左端のアプライアンスが選択されます。（アプライアンスが DNS アドレスとして指定されていて、DNS レコードに複数の IP アドレスがある場合、これらも左から右にスキャンされます。）
- 接続を高速化するために提供しているアプライアンスの一部がリダイレクタモードを使用し、一部が透過モードを使用している場合、透過モードアプライアンスは無視され、リダイレクタモードアプライアンスから選択が行われます。
- 接続を高速化するために提供しているすべてのアプライアンスが透過モードを使用している場合、プラグインは特定のモードを選択しません appliance. WANOP クライアントプラグイン SYN オプションを使用して接続を開始し、返される SYN-ACK パケットに適切なオプションをアタッチする候補アプライアンスが使用されます。これにより、実際にトラフィックと一致しているアプライアンスがプラグインに対して自身を識別できるようになります。ただし、プラグインは応答するアプライアンスとのオープンなシグナリング接続を備えている必要があります。そうでない場合、アクセラレーションは行われません。
- 一部の構成情報はグローバルと見なされます。この構成情報は、シグナリング接続を開くことができるリストの左端のアプライアンスから取得されます。

プラグインで使用するためのアプライアンスのデプロイ

May 10, 2021

クライアントアクセラレーションには、WANOP クライアントプラグインアプライアンスでの特別な構成が必要です。その他の考慮事項には、アプライアンスの配置が含まれます。プラグインは通常、VPN 接続用に展開されます。

可能な場合は専用のアプライアンスを使用してください

プラグインアクセラレーションとリンクアクセラレーションの両方に同じアプライアンスを使用しようとすると、多くの場合困難になります。これは、2 つの用途でアプライアンスをデータセンターの異なるポイントに配置する必要

があり、2 つの用途で異なるサービスクラスルールが必要になる場合があるためです。

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。単独で使用することも（透過モード）、リダイレクタモードと組み合わせて使用することもできます。

アプライアンスをネットワークの安全な部分に配置します

アプライアンスは、サーバーと同じように既存のセキュリティインフラストラクチャに依存します。ファイアウォール（および使用する場合は VPN ユニット）のサーバーと同じ側に配置する必要があります。

NAT の問題を回避する

プラグイン側のネットワークアドレス変換（NAT）は透過的に処理され、問題にはなりません。アプライアンス側では、NAT が面倒になる可能性があります。スムーズな展開を確実にするために、次のガイドラインを適用してください。

- アプライアンスをサーバーと同じアドレス空間に配置して、サーバーに到達するために使用されるアドレス変更もアプライアンスに適用されるようにします。
- アプライアンスがそれ自体に関連付けられていないアドレスを使用してアプライアンスにアクセスしないでください。
- アプライアンスは、プラグインユーザーが同じサーバーにアクセスするのと同じ IP アドレスを使用してサーバーにアクセス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。

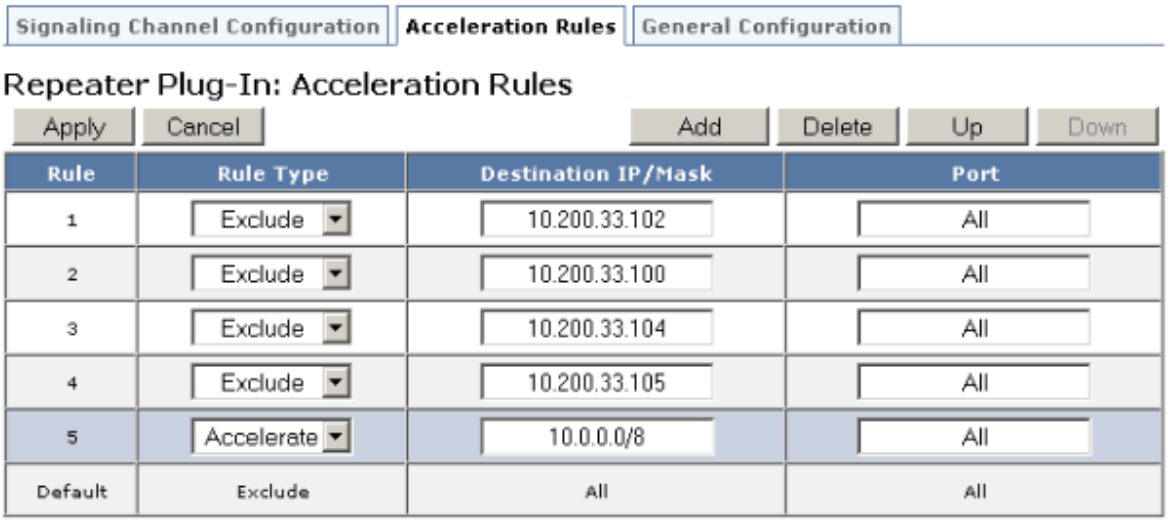
- VPN アクセラレータ-アプライアンスが VPN アクセラレータとして使用されており、すべての VPN トラフィックがアプライアンスを通過している場合、宛先に関係なく、すべての TCP トラフィックを高速化する必要があります。
- リダイレクタモード-トランスペアレントモードとは異なり、リダイレクタモードのアプライアンスは明示的なプロキシであるため、プラグインは、望ましくない場合でもトラフィックをリダイレクタモードアプライアンスに転送します。クライアントがサーバーから離れたアプライアンスにトラフィックを転送する場合、特にこの「三角形のルート」によって低速または信頼性の低いリンクが導入される場合、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。

Define the Rules-［構成］の［**WANOP** クライアントプラグイン］の［アクセラレーションルール］タブで、アクセラレーションルールを定義します。

ルールは順番に評価され、アクション（加速または除外）は最初に一致したルールから実行されます。接続を高速化するには、接続が高速化ルールに一致する必要があります。

デフォルトのアクションは加速しないことです。

図 1：アクセラレーションルールの設定



1. 構成：WANOP プラグイン：アクセラレーションルールタブ：
   - アプライアンスが到達できるローカル LAN サブネットごとに Accelerated ルールを追加します。つまり、[追加] をクリックし、[アクセラレート] を選択して、サブネットの IP アドレスとマスクを入力します。
   - アプライアンスに対してローカルなサブネットごとに繰り返します。
2. 含まれる範囲の一部を除外する必要がある場合は、除外ルールを追加して、より一般的なルールの上に移動します。たとえば、10.217.1.99 はローカルアドレスのように見えます。それが実際に VPN ユニットのローカルエンドポイントである場合は、次の Accelerate ルールの上の行に Exclude ルールを作成します。10.217.1.0/24.
3. HTTP のポート 80 など、単一のポートのみにアクセラレーションを使用する場合（非推奨）、[ポート] フィールドのワイルドカード文字を特定のポート番号に置き換えます。ポートごとに 1 つずつルールを追加することで、追加のポートをサポートできます。
4. 一般に、一般的なルールの前に狭いルール（通常は例外）をリストします。
5. ［適用］をクリックします。適用する前にこのページから移動した場合、変更は保存されません。

IP ポートの使用法

IP ポートの使用については、次のガイドラインを使用してください。

- **WANOP Client Plug-in Plug-in** との通信に使用されるポート：プラグインは、シグナリング接続を介してアプライアンスとのダイアログを保持します。デフォルトでは、ほとんどのファイアウォールで許可されているポート 443（HTTPS）にあります。

- サーバーとの通信に使用されるポート：WANOP Client Plug-in Plug-in Appliance 間の通信では、プラグインとアプライアンスが存在しない場合、クライアントがサーバーとの通信に使用するポートと同じポートが使用されます。つまり、クライアントがポート 80 で HTTP 接続を開くと、ポート 80 でアプライアンスに接続します。次に、アプライアンスはポート 80 でサーバーに接続します。

  リダイレクタモードでは、既知のポート（つまり、TCP SYN パケットの宛先ポート）のみが保持されます。エフェメラルポートは保持されません。透過モードでは、両方のポートが保持されます。

  アプライアンスは、クライアントが要求した任意のポートでサーバーと通信できると想定し、クライアントは、任意のポートでアプライアンスと通信できると想定します。これは、アプライアンスがサーバーと同じファイアウォールルールの対象である場合にうまく機能します。このような場合、直接接続で成功する接続はすべて、高速接続で成功します。

TCP オプションの使用法とファイアウォール

WANOP クライアントプラグインパラメータは、TCP オプションで送信されます。TCP オプションは任意のパケットで発生する可能性があり、接続を確立する SYN および SYN-ACK パケットに存在することが保証されています。

ファイアウォールが 24～31（10 進数）の範囲の TCP オプションをブロックしてはなりません。ブロックしないと、アクセラレーションを実行できません。ほとんどのファイアウォールはこれらのオプションをブロックしません。ただし、リリース 7.x ファームウェアを搭載した Cisco PIX または ASA ファイアウォールはデフォルトでそうする可能性があるため、設定を調整する必要がある場合があります。

プラグイン **MSI** ファイルをカスタマイズする

May 10, 2021

WANOP クライアントプラグイン配布ファイルでパラメーターを変更できます。配布ファイルは、標準の Microsoft インストーラ (MSI) 形式です。カスタマイズには、MSI エディタを使用する必要があります。

> 注
>
> 編集したパラメータの変更。MSI ファイルは、新規インストールにのみ適用されます。既存のプラグインユーザーが新しいリリースに更新しても、既存の設定は保持されます。したがって、パラメータを変更した後は、新しいバージョンをインストールする前に、古いバージョンをアンインストールするようにユーザーにアドバイスする必要があります。

ベスト・プラクティス：

最も近いプラグイン対応アプライアンスに解決される DNS エントリを作成します。たとえば、アプライアンスが 1 つしかない場合は、「Repeater.mycompany.com」を定義して、アプライアンスに解決させます。または、たとえば 5 つのアプライアンスがある場合は、Repeater.mycompany.com を 5 つのアプライアンスの 1 つに解決し、ク

ライアントまたは VPN ユニットへの近さに基づいてアプライアンスを選択します。たとえば、特定の VPN に関連付けられたアドレスを使用しているクライアントは、Repeater.mycompany.com がその VPN に接続されている WANOP クライアントプラグインアプライアンスの IP アドレスに解決されることを確認する必要があります。Orca などの MSI エディターを使用して、このアドレスをプラグインバイナリに組み込みます。アプライアンスを追加、移動、または削除するときに、DNS サーバーでこの単一の DNS 定義を変更すると、プラグインのアプライアンスリストが自動的に更新されます。

DNS エントリを複数のアプライアンスに解決することもできますが、プラグインはリストの左端のアプライアンスからその特性の一部を取得し、それらをグローバルに適用するため（SSL 圧縮特性を含む）、すべてのアプライアンスが同じように構成されていない限り、これは望ましくありません。。これは、特に DNS サーバーが各要求の IP アドレスの順序をローテーションする場合に、望ましくない混乱を招く結果につながる可能性があります。

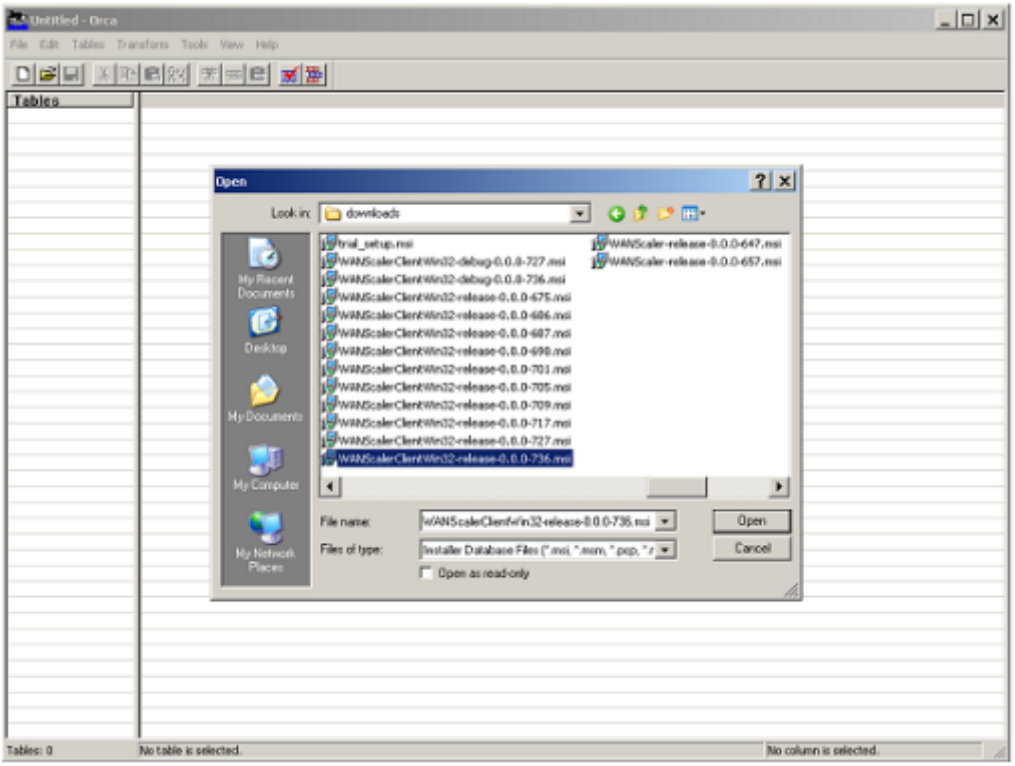
Orca MSI エディタをインストールします。

Orca など多くの MSI エディタが存在する。Orca は Microsoft の無償の Platform SDK の一部であり、Microsoft からダウンロードできる。

- Orca MSI エディタをインストールするには

  1. SDK の PSDK-x86.exe バージョンをダウンロードして実行します。インストール手順に従います。
  2. SDK をインストールしたら、Orca エディタをインストールする必要があります。これは、Microsoft プラットフォーム SDK\ Bin\ Orca.Msi の下になります。Orca.msi を起動して、実際の Orca エディタ（orca.exe）をインストールします。
  3. **Orca** の実行：Microsoft は Orca のドキュメントをオンラインで提供しています。次の情報は、最も重要な WANOP クライアント・プラグイン・パラメータを編集する方法について説明します。
  4. **[** スタート**] > [**すべてのプログラム**] > [**オルカ**]** で **Orca** を起動します。空の Orca ウィンドウが表示されたら、[ファイル] **> [**開く**]** で **WANOP** クライアントプラグイン **MSI** ファイルを開きます。

     図 **1**：**Orca** の使用



5. [テーブル] メニューの [プロパティ] をクリックします。.MSI ファイルの編集可能なすべてのプロパティのリストが表示されます。次の表に示すパラメーターを編集します。パラメータを編集するには、その値をダブルクリックし、新しい値 を入力して **[Enter]** を押します。

パラメーター	説明	デフォルト	コメント
WSAPPLIANCES	アプライアンスの一覧	なし	ここでは、WANOP アプライアンスの IP アドレスまたは DNS アドレスをカンマで区切って入力します。{appliance1, appliance2, appliance3} の形式で入力します。シグナリング接続に使用されるポートがデフォルト（443）と異なる場合は、Appliance1: port_number の形式でポートを指定します。

パラメーター	説明	デフォルト	コメント
DBCMINSIZE	圧縮に使用するディスク領域の最小量（メガバイト単位）	250	これを大きな値 (2000 など) に変更すると、圧縮のパフォーマンスは向上しますが、十分なディスク領域がない場合はインストールできなくなります。DBCMINSIZE に指定した値に加えて、少なくとも 100 MB の空きディスク容量がない限り、プラグインはインストールされません。
EKEYPEM	プラグインの秘密キー。SSL 圧縮で使用される証明書/キーペアの一部	なし	Orca の [セルを貼り付け] コマンドを使用します。通常の [貼り付け] 機能では、キーの形式は保持されません。PEM 形式の秘密キーである必要があります（—BEGIN RSA プライベートキー—で始まる）
X509CERTPEM	プラグインの証明書。SSL 圧縮で使用される証明書/キーペアの一部	なし	Orca の [セルを貼り付け] コマンドを使用します。通常の [貼り付け] 機能では、キーの形式は保持されません。PEM 形式の証明書である必要があります (—BEGIN Certificate —で始まる)
CACERTPEM	プラグインの証明機関証明書。SSL 圧縮で使用	なし	Orca の [セルを貼り付け] コマンドを使用します。通常の [貼り付け] 機能では、キーの形式は保持されません。PEM 形式の証明書である必要があります (—BEGIN Certificate —で始まる)

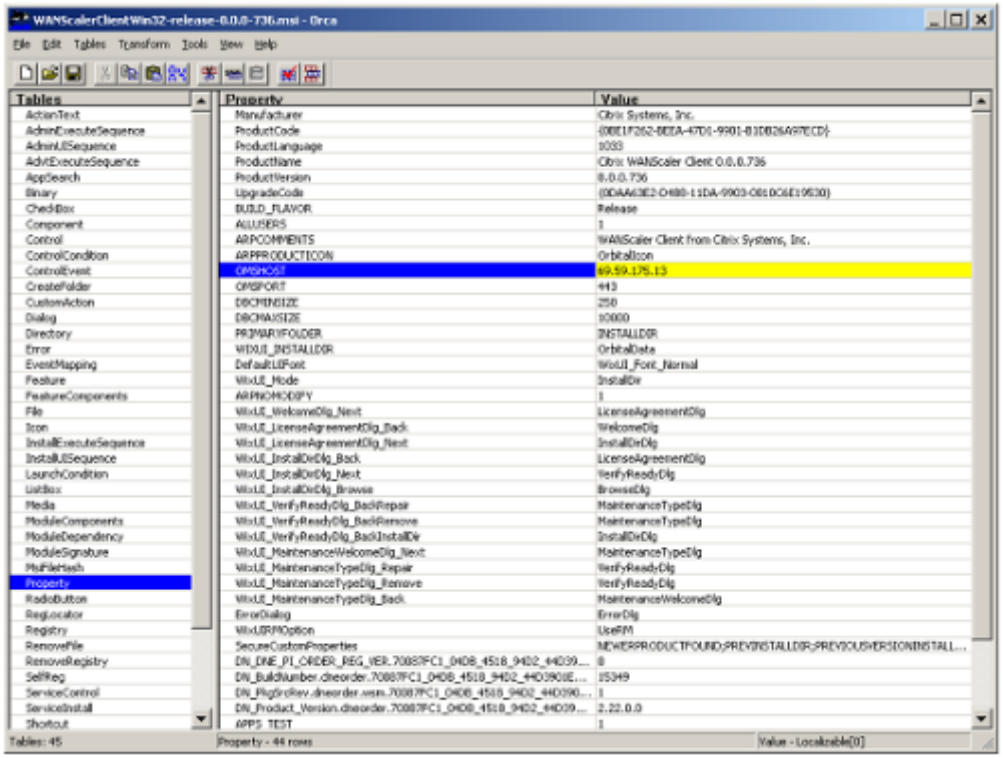
6. [テーブル] メニューで、[プロパティ] をクリックします。.MSI ファイルの編集可能なすべてのプロパティのリストが表示されます。次の表に示すパラメーターを編集します。パラメータを編集するには、その値をダブルクリックし、新しい値 を入力して **[Enter]** を押します。

パラメーター	説明	デフォルト	コメント
WSAPPLIANCES	アプライアンスの一覧	なし	WANOP クライアント・プラグイン・アプライアンスの IP または DNS アドレスをここに入力します。*{appliance1, appliance2, appliance3}* の形式でカンマ区切りのリストで入力します。シグナリング接続に使用されるポートがデフォルト（443）と異なる場合は、*Appliance1: port_number* の形式でポートを指定します。
DBCMINSIZE	圧縮に使用するディスク領域の最小量（メガバイト単位）	250	これを大きな値 (2000 など) に変更すると、圧縮のパフォーマンスは向上しますが、十分なディスク領域がない場合はインストールできなくなります。DBCMINSIZE に指定した値に加えて、少なくとも 100 MB の空きディスク容量がない限り、プラグインはインストールされません。
PRIVATEKEYPEM	プラグインの秘密キー。SSL 圧縮で使用される証明書/キーペアの一部	なし	Orca の [セルを貼り付け] コマンドを使用します。通常の [貼り付け] 機能では、キーの形式は保持されません。PEM 形式の秘密キーである必要があります（—BEGIN RSA プライベートキー—で始まる）

パラメーター	説明	デフォルト	コメント
X509CERTPEM	プラグインの証明書。SSL 圧縮で使用される証明書/キーペアの一部	なし	Orca の [セルを貼り付け] コマンドを使用します。通常の [貼り付け] 機能では、キーの形式は保持されません。PEM 形式の証明書である必要があります (—BEGIN Certificate —で始まる)
CACERTPEM	プラグインの証明機関証明書。SSL 圧縮で使用	なし	Orca の [セルを貼り付け] コマンドを使用します。通常の [貼り付け] 機能では、キーの形式は保持されません。PEM 形式の証明書である必要があります (—BEGIN Certificate —で始まる)

7. 完了したら、[ファイル**]: [**名前を付けて 保存] コマンドを使用して、編集したファイルを新しいファイル名 (test.msi など) で保存します。

   図 **2: Orca** のパラメータの編集:



8. 完了したら、[ファイル**]: [**名前を付けて 保存] コマンドを使用して、編集したファイルを新しいファイル名 (test.msi など) で保存します。

   これで、プラグインソフトウェアがカスタマイズされました。

   > 注
   >
   > 一部のユーザーは、ファイルを 1MB に切り捨てる orca のバグを確認しています。保存したファイルのサイズを確認してください。切り捨てられている場合は、元のファイルのコピーを作成し、[保存] コマンドを使用して元のファイルを上書きします。

   Orca を使用してアプライアンスリストをカスタマイズし、カスタマイズした MSI ファイルをユーザーに配布すると、ユーザーはソフトウェアのインストール時に構成情報を入力する必要がなくなります。

Windows システムにプラグインを展開する

May 10, 2021

WANOP クライアントプラグインは、他の Web 配布プログラムと同様にダウンロードしてインストールする実行可能な Microsoft インストーラー（MSI）ファイルです。このファイルは、Citrix.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 **Citrix** アクセラレーションプラグインマネージャーと呼んでいます。

プラグインに必要な唯一のユーザー構成は、アプライアンスアドレスのリストです。このリストは、IP アドレスまたは DNS アドレスのコンマ区切りのリストで構成できます。2 つの形式を混在させることができます。リストがデフォルトでアプライアンスを指すように、配布ファイルをカスタマイズできます。インストールすると、操作は透過的になります。アクセラレーションされたサブネットへのトラフィックは適切なアプライアンスを介して送信され、他のすべてのトラフィックはサーバーに直接送信されます。ユーザーアプリケーションは、これが発生していることに気づいていません。

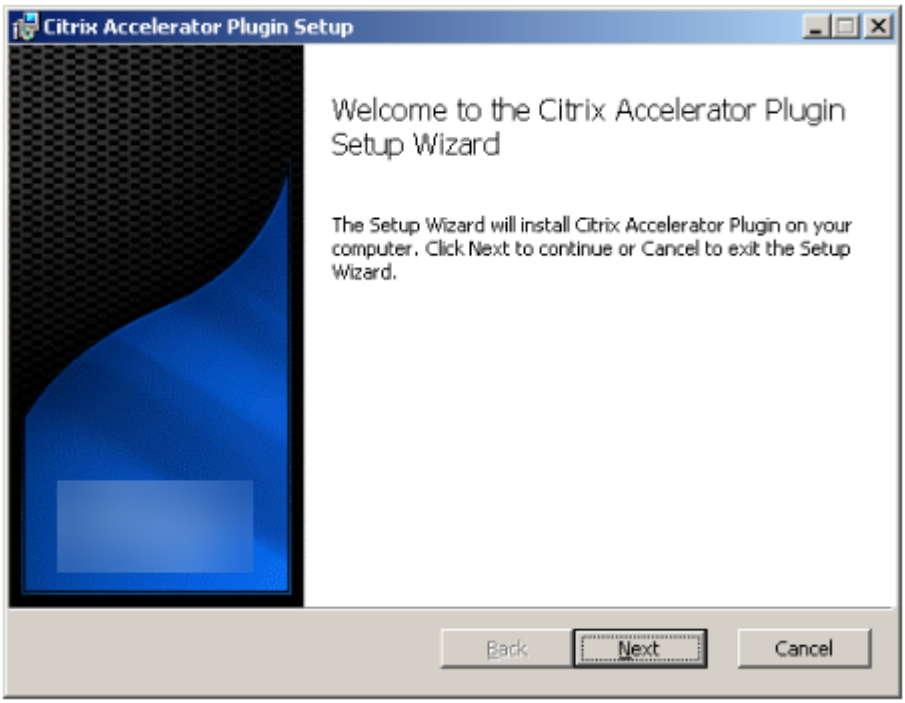
インストール

> 必須要件**:**
>
> Windows 10 では、エラーなしでインストールを実行するには、すべてのドライバに有効なデジタル署名が必要です。

WANOP クライアントプラグインプラグインアクセラレータを Windows システムにインストールするには:

1. Repeater*.msi ファイルはインストールファイルです。開いているすべてのアプリケーションとウィンドウを閉じて、通常の方法でインストーラを起動します（ファイルウィンドウをダブルクリックするか、run コマンドを使用します）。

   図 **1**: 初期インストール画面:



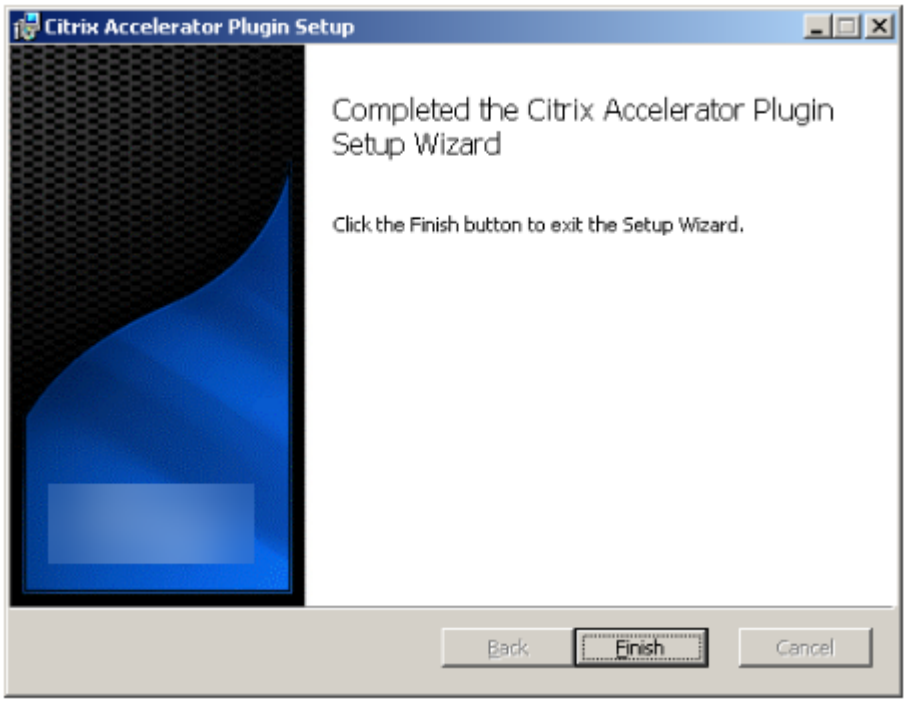
以下の手順は、インタラクティブインストール用です。サイレントインストールは、次のコマンドで実行できます。

「**msiexec /i client_msi_file /qn**」

2. インストールプログラムは、ソフトウェアをインストールする場所の入力を求めます。指定したディレクトリは、クライアントソフトウェアとデ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。

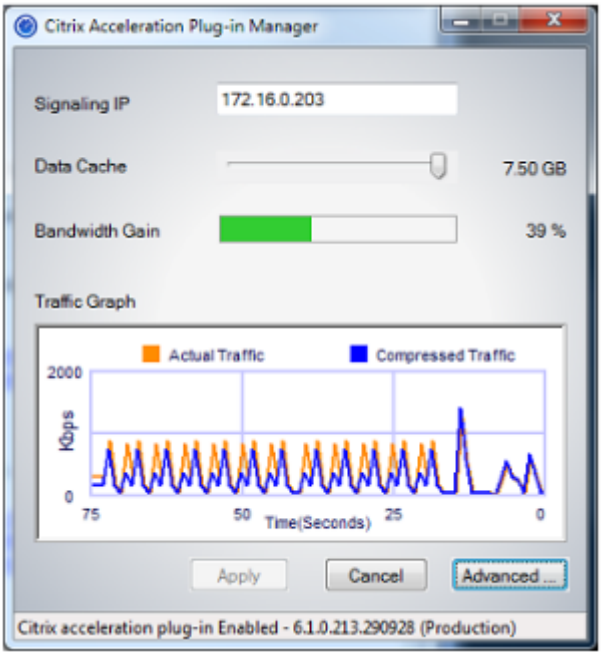
3. インストーラーが終了すると、システムを再起動するように求められる場合があります。再起動後、WANOP クライアントプラグインプラグインが自動的に起動します。

図 **2**：最終インストール画面



4. タスクバーのアクセラレータアイコンを右クリックし、［アクセラレータの管理］を選択して、Citrix Plug-in Accelerator Manager を起動します。

図 **3**：**Citrix** アクセラレータプラグインマネージャー、初期（基本）表示



5. .MSI ファイルがユーザー向けにカスタマイズされていない場合は、シグナリングアドレスと圧縮に使用するディスク容量を指定します。

   - [アプライアンス: シグナリングアドレス] フィールドに、アプライアンスのシグナリング IP アドレスを入力します。プラグイン対応アプライアンスが複数ある場合は、それらすべてをコンマで区切ってリストします。IP アドレスまたは DNS アドレスのいずれかを使用できます。
   - [データキャッシュ] スライダーを使用して、圧縮に使用するディスク容量を選択します。多いほど良いです。利用可能なディスク容量が多ければ、7.5GB はそれほど多くありません。
   - [適用] を押します。

     これで、WANOP クライアントプラグインアクセラレータが実行されます。加速されたサブネットへの今後のすべての接続は加速されます

     プラグインの [AdvancedRules] タブで、[Acceleration Rules] リストに、各アプライアンスが Connected として表示され、各アプライアンスの Accelerated サブネットが Accelerated として表示されます。そうでない場合は、Signaling Addresses IP フィールドと一般的なネットワーク接続を確認してください。

プラグインのトラブルシューティング

プラグインのインストールは一般的にスムーズに進みます。そうでない場合は、次の問題を確認してください。

一般的な問題:

- システムを再起動しないと、WANOP クライアントプラグインが正しく実行されません。

- 高度に断片化されたディスクは、圧縮パフォーマンスを低下させる可能性があります。
- アクセラレーションの失敗（[**Diagnostics**] タブにアクセラレーション接続が表示されない）は、通常、何かがアプライアンスとの通信を妨げていることを示します。プラグインの [構成**:** アクセラレーション規則] の一覧をチェックして、アプライアンスに正常に接続され、ターゲットアドレスがアクセラレーション規則の 1 つに含まれていることを確認します。接続障害の一般的な原因は次のとおりです。
  - アプライアンスが実行されていないか、アクセラレーションが無効になっています。
  - ファイアウォールは、プラグインとアプライアンスの間のある時点で WANOP クライアントプラグイン TCP オプションを削除しています。
  - プラグインはサポートされていない VPN を使用しています。

確定的ネットワークエンハンサーロックエラー

まれに、プラグインをインストールしてコンピューターを再起動した後、次のエラーメッセージが 2 回表示されます。

確定的ネットワークエンハンサーのインストールでは、ロックされたリソースを解放するために、最初に再起動する必要があります。コンピュータを再起動した後、このインストールを再度実行してください。

これが発生した場合は、次のようにします。

1. **[** プログラムの追加と削除**]** に移動し、WANOP クライアントプラグインがあれば削除します。
2. **[** コントロールパネル**] > [**ネットワークアダプタ] > [ローカルエリア接続] > [プロパティ] に移動し、[決定論的ネットワークエンハンサー] のエントリを探し、チェックボックスをオフにして、[**OK**] をクリックします。(ネットワークアダプタが「ローカルエリア接続」以外の名前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、c:\windows\inf (Windows を標準以外の場所にインストールしている場合は、同等のディレクトリ) に移動します。
4. 次のコマンドを入力します。

   「dne2000.cat」を見つける oem*.inf
5. 一致する行 (一致する行は CatalogFile= dne2000.cat) を返した最も高い番号の oem*.inf ファイルを検索し、編集します。次に例を示します:

   notepad oem13.inf
6. セミコロンで始まる上部の 3 行を除くすべてを削除してから、ファイルを保存します。これにより、不適切または廃止された設定がすべてクリアされ、次のインストールではデフォルト値が使用されます。
7. インストールを再試行してください。

その他のインストールの問題

WANOP クライアントプラグインのインストールに関する問題は、通常、既存のネットワーク、ファイアウォール、またはウイルス対策ソフトウェアがインストールを妨害した結果です。通常、インストールが完了すると、それ以上の問題は発生しません。

インストールが失敗した場合は、次の手順を試してください。

1. プラグインインストールファイルがローカルシステムにコピーされていることを確認してください。
2. アクティブなものをすべて切断します VPN/remote ネットワーククライアント。
3. ファイアウォールとウイルス対策ソフトウェアを一時的に無効にします。
4. これのいくつかが難しい場合は、できることをしてください。
5. WANOP クライアントプラグインを再インストールします。
6. それでも問題が解決しない場合は、システムを再起動してもう一度試してください。

WANOP プラグイン **GUI** コマンド

May 10, 2021

[**Citrix** アクセラレータプラグイン］アイコンを右クリックし、［アクセラレータの管理］を選択すると、**WANOP** クライアントプラグイン GUI が表示されます。GUI の基本画面が最初に表示されます。必要に応じて使用できる高度なディスプレイもあります。

基本表示

[基本] ページでは、次の 2 つのパラメーターを設定できます。

- Signaling Addresses フィールドは、プラグインが接続できる各アプライアンスの IP アドレスを指定します。アプライアンスを 1 つだけリストすることをお勧めしますが、コンマ区切りのリストを作成することもできます。これは順序付きリストであり、左端のアプライアンスが他のアプライアンスよりも優先されます。信号接続を確立できる左端のアプライアンスで加速が試行されます。DNS アドレスと IP アドレスの両方を使用できます。

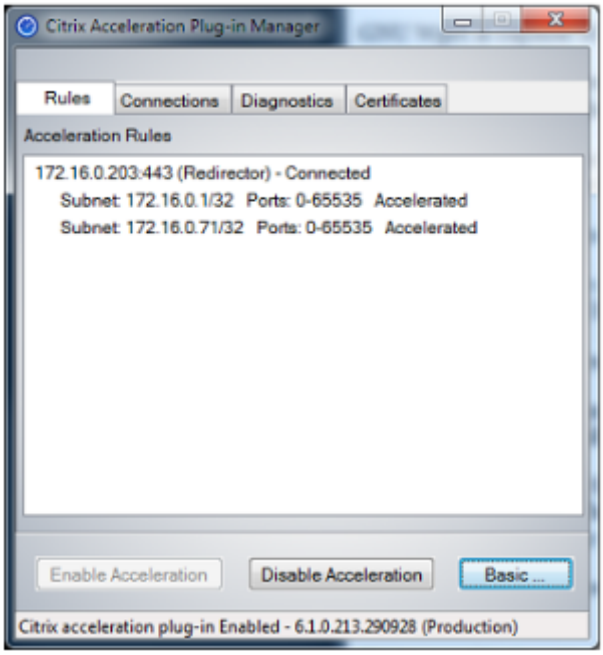
  例：10.200.33.200、ws.mycompany.com、ws2.mycompany.com

- データキャッシュスライダーは、プラグインのディスクベースの圧縮履歴に割り当てられるディスクスペースの量を調整します。多いほど良いです。

  さらに、詳細表示に移動するためのボタンがあります。

高度な表示

[詳細設定] ページには、[ルール]、[接続]、[診断]、および [証明書] の 4 つのタブがあります。



ディスプレイの下部には、アクセラレーションを有効にしたり、アクセラレーションを無効にしたり、基本ページに戻ったりするためのボタンがあります。

[ルール] タブ

[ルール] タブには、アプライアンスからダウンロードされたアクセラレーションルールの簡略リストが表示されます。各リスト項目には、アプライアンスのシグナリングアドレスとポート、アクセラレーションモード（リダイレクタまたはトランスペアレント）、接続状態が表示され、その後にアプライアンスのルールの概要が表示されます。

[接続] タブ

[接続] タブには、さまざまなタイプの開いている接続の数が表示されます。

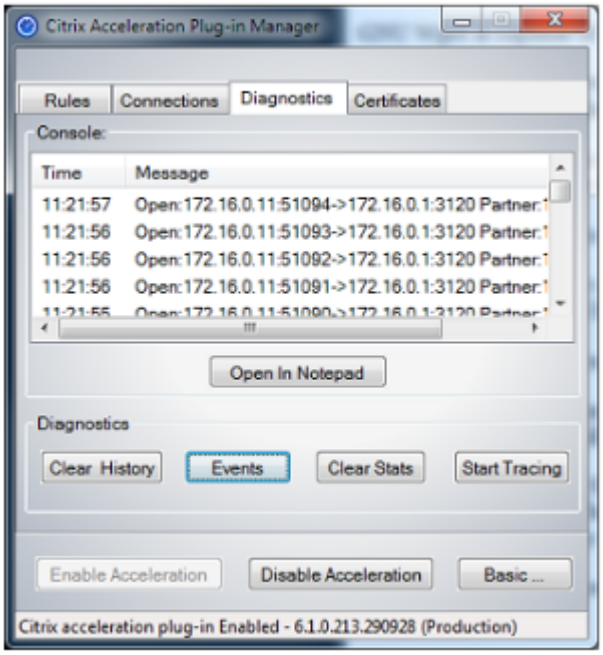
- アクセラレーテッド接続：WANOP クライアント・プラグインとアプライアンス間のオープン接続の数。この数には、アプライアンスごとに 1 つのシグナリング接続が含まれますが、高速化された CIFS 接続は含まれません。[詳細] をクリックすると、各接続の簡単な概要を示すウィンドウが開きます。（[その他] ボタンはすべて、サポートと共有する場合に、ウィンドウ内の情報をクリップボードにコピーできます。）
- **CIFS** 接続の高速化：CIFS（Windows ファイル・システム）サーバとのオープンで高速化された接続の数。これは通常、マウントされたネットワークファイルシステムの数と同じです。[詳細] をクリックすると、高速接続の場合と同じ情報に加えて、CIFS 接続が WANOP クライアントプラグインの特別な CIFS 最適化で実行されている場合にアクティブを報告するステータスフィールドが表示されます。

- 高速化された **MAPI** 接続：オープンで高速化された Outlook/Exchange 接続の数。
- アクセラレーション **ICA** 接続：ICA プロトコルまたは CGP プロトコルを使用して、オープンでアクセラレーションされた XenApp および XenDesktop 接続の数。
- アクセラレーションされていない接続：アクセラレーションされていない接続を開きます。[詳細] をクリックすると、接続が高速化されなかった理由の簡単な説明が表示されます。通常、この理由は、宛先アドレスを加速させるアプライアンスがないためです。このアドレスは、サービスポリシールールとして報告されます。
- 接続のオープン/クローズ：完全にオープンではないが、オープンまたはクローズ処理中の接続（TCP「ハーフオープン」または「ハーフクローズ」接続）。[詳細] ボタンには、これらの接続に関する追加情報が表示されます。

[診断] タブ

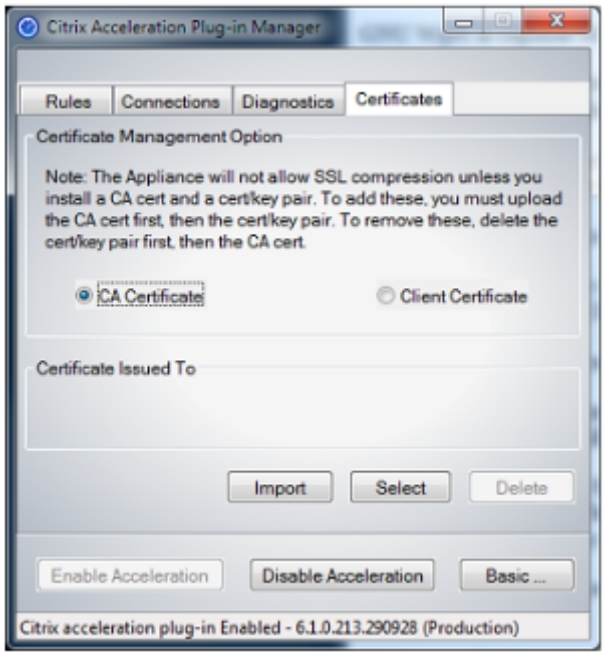
[診断] ページには、さまざまなカテゴリの接続数やその他の役立つ情報が報告されます。

- トレースの開始/トレースの停止：問題を報告した場合、Citrix の担当者が問題を特定するために接続トレースの実行を依頼することがあります。このボタンは、トレースを開始および停止します。トレースを停止すると、ポップアップウィンドウにトレースファイルが表示されます。Citrix の担当者が推奨する方法でそれらを送信します。
- 履歴のクリア：この機能は使用しないでください。
- **Clear Statistics**-このボタンを押すと、[Performance] タブの統計情報がクリアされます。
- **Console**：スクロール可能なウィンドウで、最近のステータスメッセージ（ほとんど接続オープンメッセージと接続クローズメッセージ、エラーメッセージやその他のステータスメッセージなど）が表示されます。



[証明書] タブ

[証明書] タブで、オプションのセキュアピアリング機能のセキュリティ資格情報をインストールできます。これらのセキュリティ資格情報の目的は、プラグインが信頼できるクライアントであるかどうかをアプライアンスが確認できるようにすることです。



CA 証明書と証明書とキーのペアをアップロードするには:

1. [CA 証明書管理] を選択します。
2. ［インポート］をクリックします。
3. CA 証明書をアップロードします。証明書ファイルは、サポートされているファイルタイプ（.pem、.crt、.cer、または.spc）のいずれかを使用する必要があります。使用する証明書ストアを選択するように求めるダイアログボックスが表示され、キーワードのリストが表示される場合があります。リストの最初のキーワードを選択します。
4. [クライアント証明書の管理] を選択します。
5. ［インポート］をクリックします。
6. 証明書とキーのペアの形式を選択します（PKCS12 または PEM/DER).
7. ［**Submit**］をクリックします。

> 注
>
> の場合 PEM/DER, 証明書とキー用に別々のアップロードボックスがあります。証明書とキーのペアが 1 つのファイルに結合されている場合は、ファイルを 2 回、各ボックスに 1 回指定します。

WANOP プラグインの更新

May 10, 2021

新しいバージョンの WANOP クライアントプラグインをインストールするには、プラグインを初めてインストールするときに使用したのと同じ手順に従います。

WANOP クライアントプラグインをアンインストールします

WANOP クライアントプラグインをアンインストールするには、Windows の [プログラムの追加と削除] ユーティリティを使用します。WANOP クライアントプラグインは、現在インストールされているプログラムのリストに、**Citrix** アクセラレーションプラグイン として表示されます。それを選択し、[削除] をクリックします。

クライアントのアンインストールを完了するには、システムを再起動する必要があります。

WANOP プラグインのトラブルシューティング

May 10, 2021

- 問題: シグナリングチャネルの接続の問題に直面しています。これらの問題を解決するにはどうすればよいですか?

  解決策: シグナリングチャネルの接続の問題を解決するには、次のトラブルシューティング手順を実行します。

  - シグナリング IP アドレスが正しく構成されていることを確認します。これを行うには、シグナリング IP アドレスに ping を実行し、応答を確認します。
  - WANOP アプライアンスでシグナリングステータスが有効になっていることを確認します。
  - ネットワークにインストールされているファイアウォールが WANOP TCP オプションを削除しないことを確認します。
  - 有効な WANOP プラグインライセンスが WANOP アプライアンスにインストールされていることを確認します。
  - シグナリングチャネルソースフィルタリング構成がクライアントソース IP アドレスをブロックしないことを確認します。
  - LAN 検出を有効にしている場合は、WANOP プラグインと WANOP アプライアンス間のラウンドトリップ時間が許容値であることを確認してください。

- 問題: WANOP 4000 アプライアンスで、WANOP プラグインを無効にできません。

  原因: これは既知の問題です。

解決策: なし。WANOP4000 アプライアンスで WANOP プラグインを無効にすることはできません。

- 問題: WANOP プラグインを使用して WANOP アプライアンスに接続すると、次のエラーメッセージエントリが [Alerts] タブに記録されます。

  <Number> このアプライアンスに接続しようとした WANOP プラグインの現在の制限を超えています。

  原因: WANOP アプライアンスへの接続数が、ライセンスされたユーザー制限を超えました。

  解決策: ユーザーが接続を切断するのを待つか、接続を終了します。

- 問題: WANOP 4000 または 5000 アプライアンスで正しくないシグナリング IP アドレスが設定されています。

  解決策: WANOP 4000 または 5000 アプライアンスのシグナリング IP アドレスを更新するには、次の手順を実行します。

  1. WANOP アプライアンスの NetScaler インスタンスにログオンします。
  2. [トラフィック管理] > [負荷分散] > [仮想サーバー] > [BR_LB_VIP_SIG] ページに移動します。
  3. シグナリング IP アドレスを更新します。
  4. 構成を保存します。

- 問題: CIFS と ICA のトラフィックが加速されない。

  解決策: この問題を解決するには、次のトラブルシューティング手順を実行します。

  - IP アドレスとポート番号のアクセラレーションルールが WANOP プラグインに対して正しく定義されていることを確認します。
  - シグナリング接続が成功した後、CIFS または ICA 接続が確立されていることを確認します。
  - 使用されているサービスクラスのアクセラレーションポリシーを確認します。

SMB 3.1.1 接続

May 10, 2021

サーバーメッセージブロック (SMB) プロトコルは、ネットワークファイル共有プロトコルです。プロトコルの特定のバージョンを定義するメッセージパケットは、ダイアレクトと呼ばれます。共通インターネットファイルシステム (CIFS) プロトコルは、SMB の方言です。

Citrix SD-WAN リリース 10 バージョン 1 では、SMB 3.1.1 プロトコルが Citrix SD-WAN WANOP および Premium エディションプラットフォームで導入されています。

Citrix SD-WAN WANOP は、SMB 3.1.1 接続をサポートします。SMB 3.1.1 接続は、クライアントが Windows 10 で、サーバーが Windows Server 2016 の場合に適用されます。

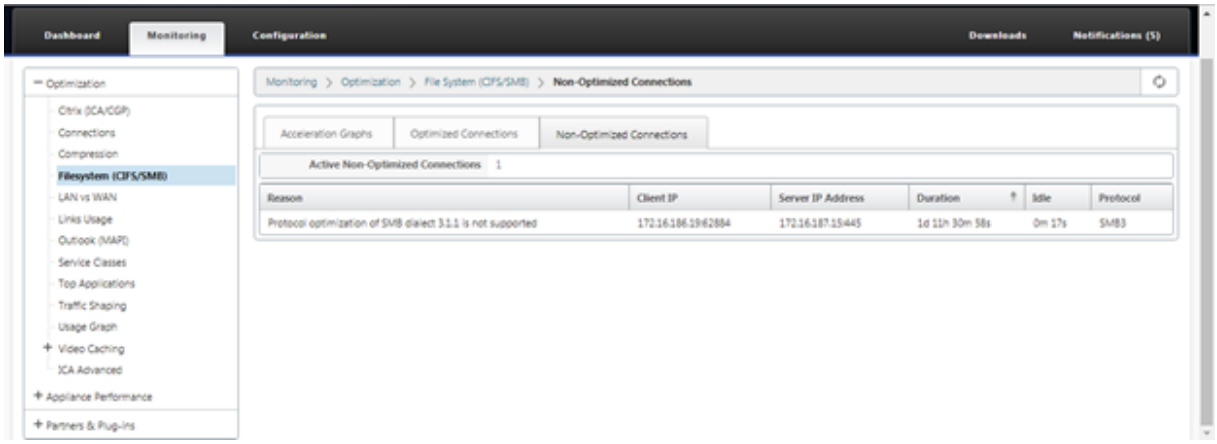
SMB 3.1.1 トラフィックが WANOP モジュールを通過する場合:

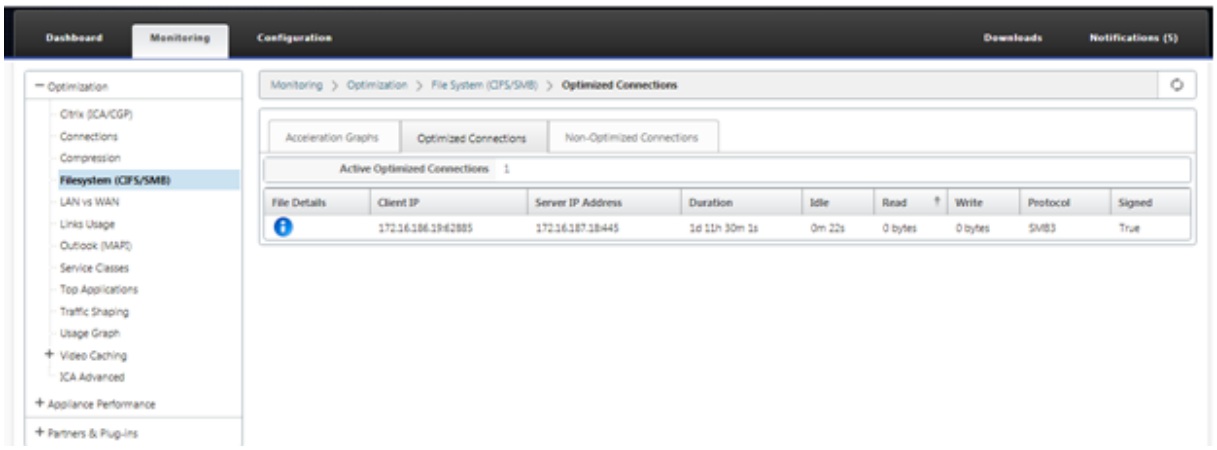
- SMB 3.1 CIFS 最適化されていない接続の一部としてカウント/認識可能
- 次のトレースメッセージが表示されます、「SMB 3.1.1 としてこの接続を渡すはサポートされていません」。

クライアント	サーバー	SMB バージョン
Windows 10	Win 2016, 2012R2	SMB 3.1.1, 3.0.2
Windows 8.1	SMB 3.0	SMB 3.0
Windows 7	SMB 3.0	SMB 3.0

最適化されていない接続の場合、Citrix SD-WAN WANOP アプライアンスの GUI に SMB 3.1.1 のメッセージが表示されます。

Citrix SD-WAN WANOP アプライアンスの GUI で、[監視] > [ファイルシステム（**CIFS/SMB**)] に移動します。[非最適化された接続] タブをクリックすると、次のメッセージが表示されます。*SMB* ダイアレクト *3.1.1* のプロトコル最適化はサポートされていません。使用可能なログエントリはありません。また、SD-WAN WANOP では、これをサポートするための新しい設定は必要ありません。





ハウツー記事

May 10, 2021

「How-to-Articles」では、Citrix SD-WAN でサポートされる機能を構成する手順について説明します。これらの記事には、次の重要な機能の一部に関する情報が含まれています。

以下の機能名をクリックすると、その機能に関するハウツー記事のリストが表示されます。

- 仮想ルーティングと転送
- QoS 公平性のための RED の有効化
- 構成
- 動的ルーティング
- DHCP サーバーと DHCP リレー
- ルートフィルタ
- IPSec の終了とモニタリング
- Secure Web Gateway
- QoS
- FIPS 準拠の動作-IPSec トンネル
- ダイナミック NAT 設定
- 適応型帯域幅検出
- アクティブ帯域幅テスト
- BGP の拡張機能
- SSL プロファイルとサービスクラスの関連付け
- セキュアピアリングと手動セキュアピアリング
- ゼロタッチ展開
- ツーボックスモードの展開

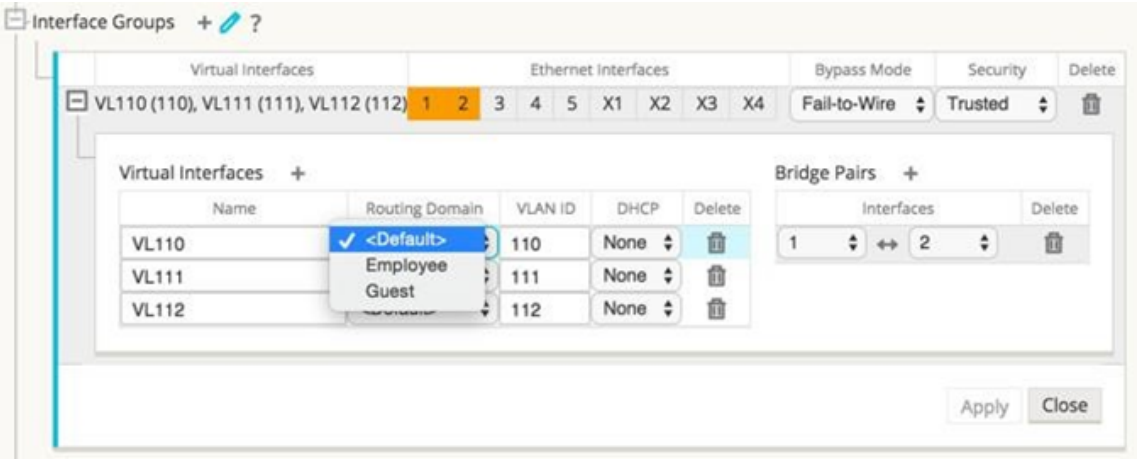
インターフェイスグループ

May 10, 2021

インターフェイスグループを設定するには、次の手順を実行します。

1. 構成エディターで、[サイト] > [**[**クライアントサイト名**]**] > [インターフェイスグループ] に移動し、仮想インターフェイスを設定するときにドロップダウンメニューから ルーティングドメイン を選択します。詳しい手順については、設定, インターフェイスグループを参照してください。

> 注
>
> 仮想インターフェイスが特定のルーティングドメインに関連付けられると、そのルーティングドメインを使用する場合、それらのインターフェイスだけが使用可能になります。



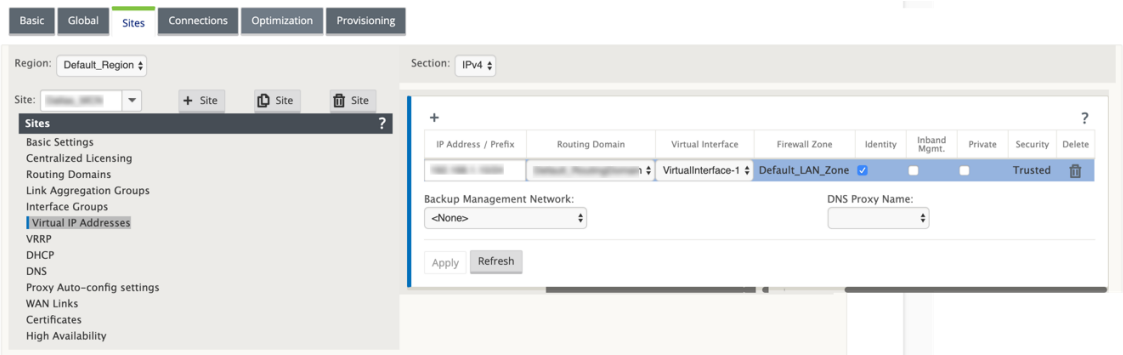
仮想 **IP** アドレス **ID** の設定

May 10, 2021

仮想ネットワークインターフェイスは、同じサブネットまたは異なるサブネットで複数の IP アドレスをホストできます。ただし、ID が true に設定されている仮想 IP は 1 つだけ選択できます。仮想 IP は、BGP/OSPF、DHCP サーバ/リレー、およびインバンド管理などのダイナミックルーティングプロトコルに使用できます。

仮想 IP アドレス ID を構成するには、次の手順を実行します。

1. 構成エディタで、[サイト**] > [**サイト **[**名**]**] > [仮想 **IP** アドレス] に移動します。
2. 仮想 IP アドレスの [**Identity**] チェックボックスをクリックして、IP サービスに使用します。



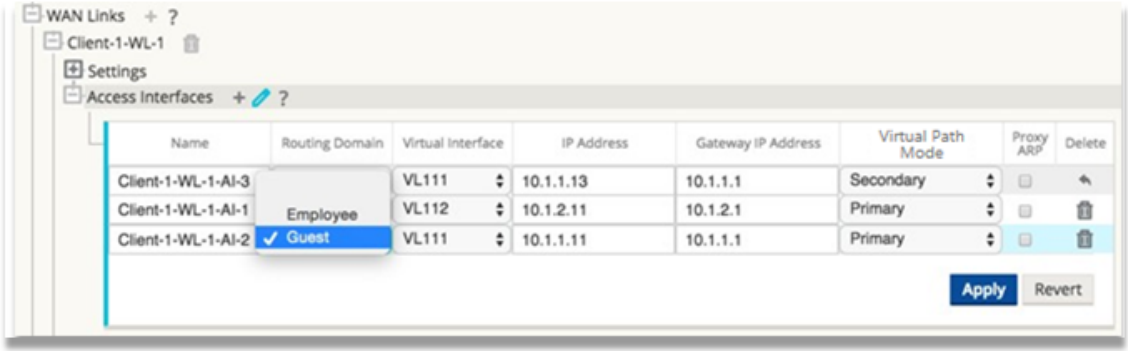
アクセスインターフェイスの設定

September 26, 2023

アクセスインターフェイスを構成するには、次の手順を実行します。

1. 構成エディターで、[サイト] > [クライアント **[サイト] 名 **] > [**WAN** リンク] > [W **[AN** リンク名**]**] > [アクセスインターフェイス] に移動します。
2. アクセスインターフェイスを設定するときに、ドロップダウンメニューから ルーティングドメイン を選択します。

   詳細な手順については、MCN の設定トピックの「アクセスインターフェイスの構成方法」を参照してください。



仮想 **IP** アドレスの構成

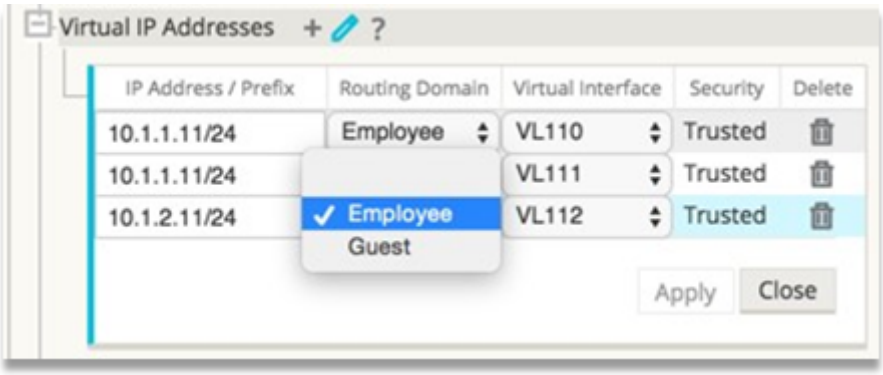
May 10, 2021

仮想 IP アドレスを構成するには

1. 構成エディターで、[サイト] **> [[**クライアントサイト名**]] > [**仮想 **IP** アドレス] に移動します。
2. 仮想 IP アドレスを設定するときに、ドロップダウンメニューから ルーティングドメイン を選択します。

   詳しい手順については、構成, 仮想 IP アドレスを参照してください。

選択したルーティングドメインによって、ドロップダウンメニューから使用できる仮想インターフェイスが決まります。



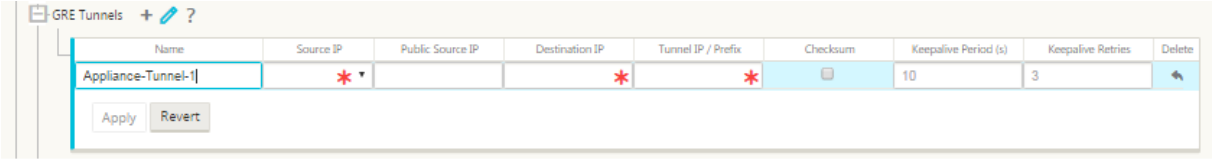
GRE トンネルの設定

May 10, 2021

GRE トンネルを設定するには、次の手順を実行します。

1. 構成エディタで、[接続] > [サイト] > [**GRE** トンネル] に移動します。送信元 IP アドレスは、信頼できるリンクの仮想ネットワークインターフェイスからのみ選択できます。
2. GRE トンネルの名前を入力します。
3. ドロップダウンメニューから使用可能な 送信元 **IP** アドレスを選択します。ルーティングドメインは、ドロップダウンメニューから使用できる送信元 IP アドレスを決定します。
4. （オプション）パブリックソース **IP** を選択します。このアドレスが送信元 IP と同じ場合、このフィールドは空にできます。
5. GRE トンネルの 宛先 **IP** アドレスを入力します。
6. GRE トンネルのトンネル **IP/**プレフィクス アドレスを入力します。
7. **GRE** トンネルヘッダーでチェックサムを使用する場合は、**[**チェックサム**]** をクリックします。
8. キープアライブ期間の 値を秒単位で入力します。0 を設定すると、キープアライブパケットは送信されませんが、GRE トンネルはアクティブになります。
9. キープアライブの再試行値を入力します。この値は、SD-WAN アプライアンスが GRE トンネルを非アクティブにするまでにキープアライブの再試行試行回数を決定します。

詳細については、MCN サイトのGRE トンネルの設定を参照してください。



GRE トンネルを使用した Web Gateway のセキュリティ保護の詳細については、Secure Web Gatewayを参照してください。

ブランチ間通信用の動的パスを設定する

May 10, 2021

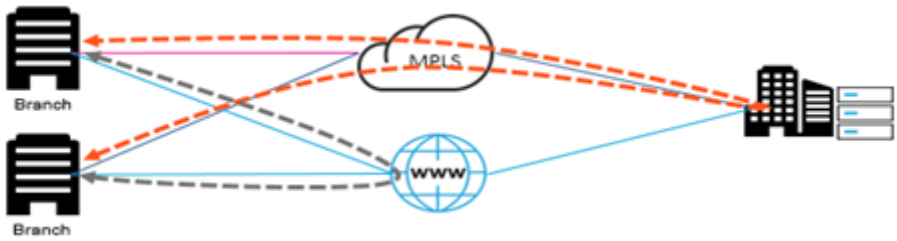
VoIP とビデオ会議の需要により、トラフィックはオフィス間を移動するようになっています。データセンターを介して完全なメッシュ接続を設定することは効率的ではありません。これには時間がかかることがあります。

Citrix SD-WAN では、すべてのオフィス間のパスを構成する必要はありません。ダイナミックパス機能を有効にすると、SD-WAN ソリューションは必要に応じてオフィス間のパスを自動的に作成します。セッションでは、最初に既存の固定パスが使用されます。また、帯域幅と時間のしきい値が満たされると、新しいパスが固定パスよりも優れたパフォーマンス特性を持つ場合、パスは動的に作成されます。セッショントラフィックは、新しいパスを介して送信されます。これにより、リソースの効率的な使用が可能になります。パスは、必要な場合にのみ存在し、データセンターとの間で送受信されるトラフィックの量を削減します。

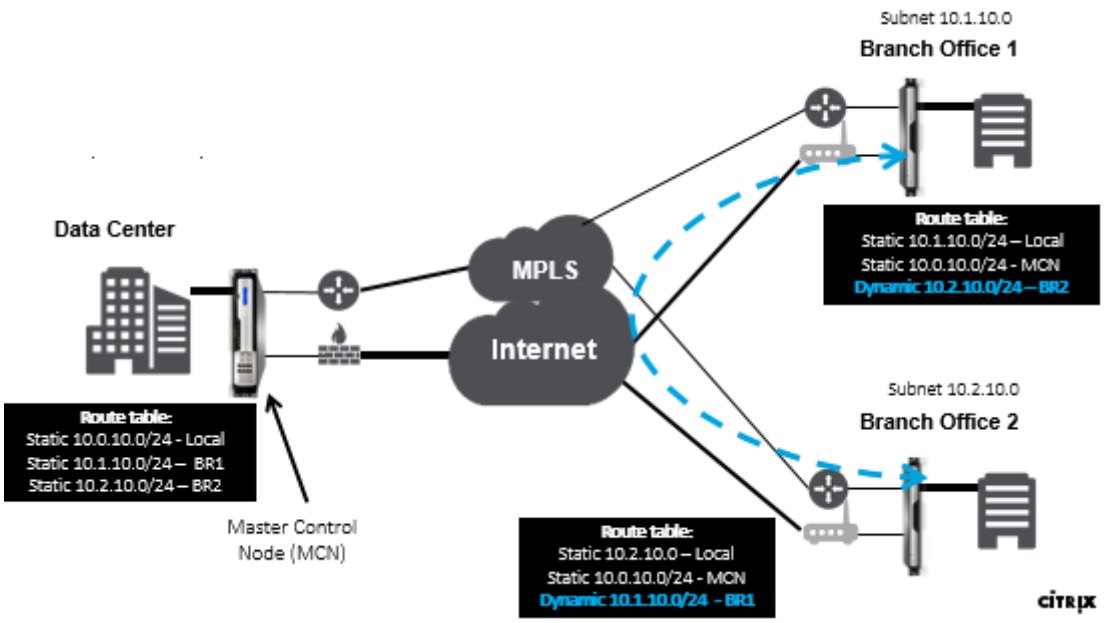
SD-WAN ネットワークのその他の利点は次のとおりです。

- ブランチ間の接続を許可する帯域幅と PPS のしきい値
- レーテンシーを最小限に抑えながら、データセンター内外の帯域幅要件を軽減
- オンデマンドで作成されるパスは、設定されたしきい値に依存
- 必要のない場合にネットワークリソースを動的に解放する
- マスターコントロールノードの負荷とレイテンシを軽減

動的仮想パスを使用したブランチとブランチ間の通信:



動的パスを持つ SD-WAN ネットワーク:

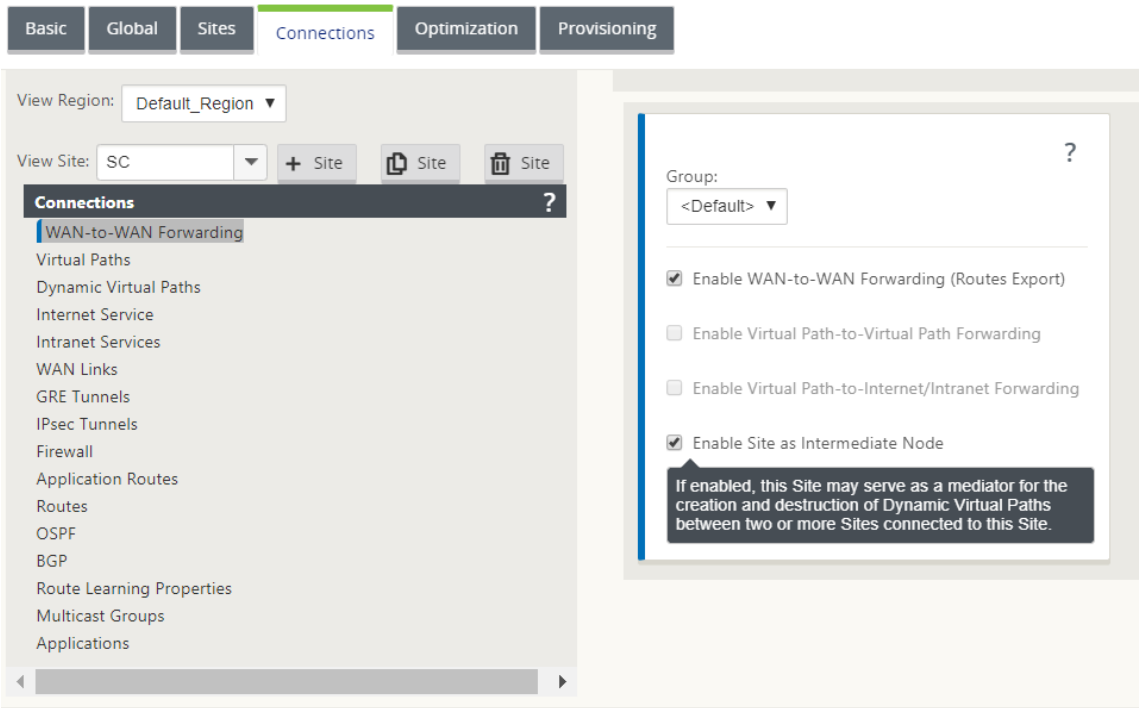


- 動的仮想パスは、エンタープライズなどの大規模な展開に使用されます。
- 小規模な展開では、静的仮想パスと Any-to-any 仮想パスを使用する
- 2 つのデータセンター間 (DC から DC へ) の静的仮想パスを常に使用
- 動的仮想パスを使用するためにすべての WAN パスを構成する必要はありません
- 各 SD-WAN アプライアンスには、構成可能な動的仮想パスの数が制限されています（動的最小制限 8 個、静的最小制限 8 個 = 合計 16 個）。

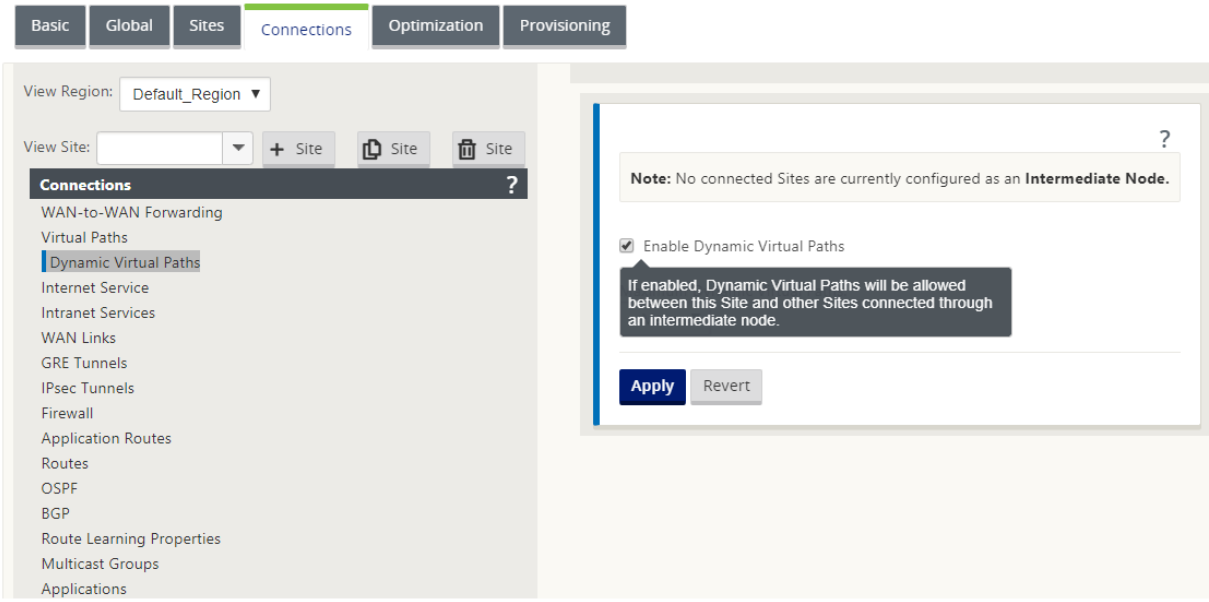
SD-WAN GUI で動的仮想パスを有効にする方法

動的仮想パスを有効にする手順は、次のとおりです。

1. Citrix SD-WAN GUI の［接続］ペインで、WAN から WAN への転送グループを作成します。
2. [接続**] > [[**クライアントサイト名**]] > [WAN** から **WAN** への転送] に移動します。
3. **WAN** から **WAN** への転送を有効にして、サイトがマルチホップサイト間プロキシとして機能できるようにします。
4. サイトを中間ノードとして有効にする
5. [接続**] > [**リモートサイト**] > [WAN** から **WAN** への転送] に移動します。
6. サイトがマルチホップサイト間プロキシとして機能できるようにするには、WAN から WAN への転送を有効にします。



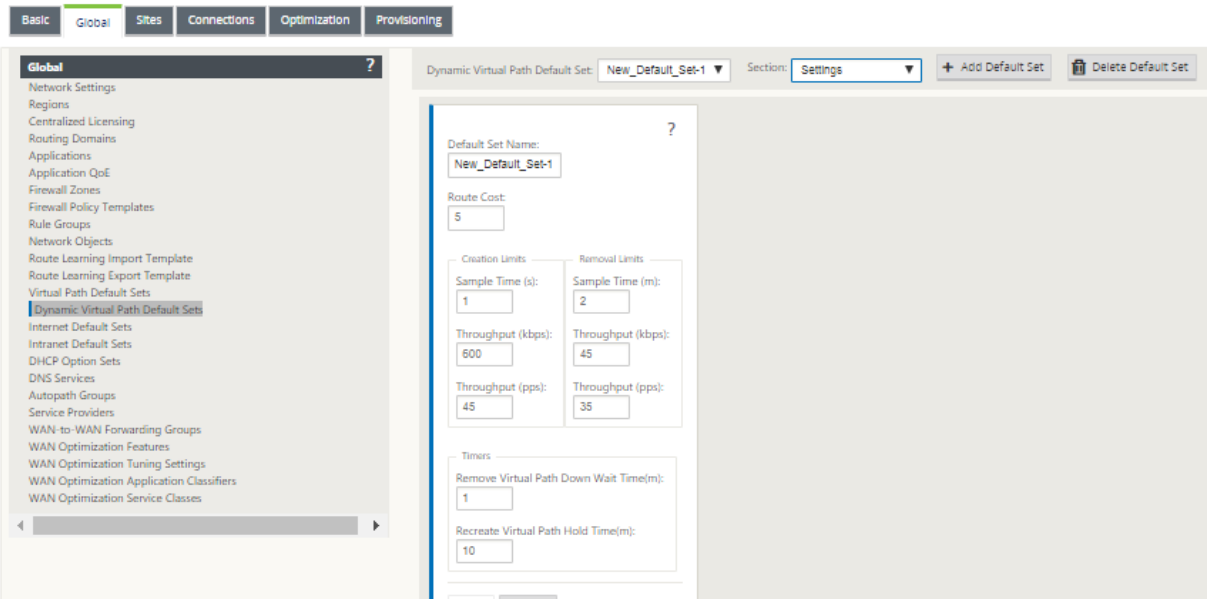
7. [接続] **>** [リモートサイト] **>** [仮想パス] **>** [動的仮想パス] に移動します。
8. 動的仮想パスを有効にします。
9. ダイナミックパスの最大数を設定します。



動的仮想パスの作成方法

- 構成では、動的仮想パスがアクティブかダウンするかを決定します。

- 時間枠内のサンプルパケットカウント（pps）または帯域幅（kbps）を設定します。
- グローバルに設定することも、中間ノードで WAN リンクを設定することもできます。



WAN から WAN への転送

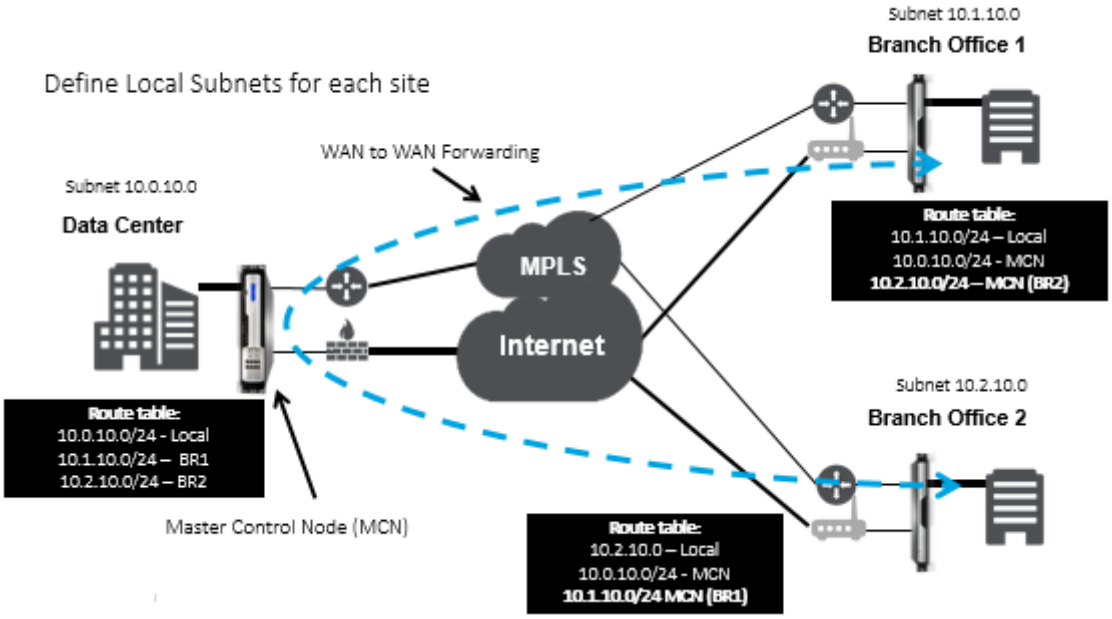
May 10, 2021

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

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

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

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



監視とトラブルシューティング

May 10, 2021

Citrix SD-WAN アプライアンスの Web 管理インターフェイスを使用して、サポートされている機能を監視およびトラブルシューティングできます。以下は、Citrix SD-WAN アプライアンスに適用される監視およびトラブルシューティングのトピックへのリンクです。

仮想 WAN の監視

統計情報の表示

フロー情報の表示

レポートの表示

ファイアウォールの統計情報の表示

診断ツール

パス・マッピングと帯域幅の向上

管理 IP のトラブルシューティング

アクティブ帯域幅テスト

適応型帯域幅検出

仮想 **WAN** の監視

May 10, 2021

アプライアンスの基本情報の表示

ブラウザを使用して、監視するアプライアンスの管理 Web インターフェイスに接続し、［ダッシュボード］タブをクリックして、そのアプライアンスの基本情報を表示します。

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

システムステータス:

- 名前—アプライアンスをシステムに追加したときに割り当てた名前です。
- モデル—これは仮想 WAN アプライアンスのモデル番号です。
- **Appliance Mode**： このアプライアンスがプライマリ MCN またはセカンダリ MCN として構成されているか、またはクライアントアプライアンスとして構成されているかを示します。
- 管理 **IP** アドレス—アプライアンスの管理 IP アドレスです。
- **Appliance Uptime** —前回の再起動以降、アプライアンスが稼働していた期間を指定します。
- ［**Service Uptime**]：前回の再起動以降、仮想 WAN サービスが実行されている期間を指定します。

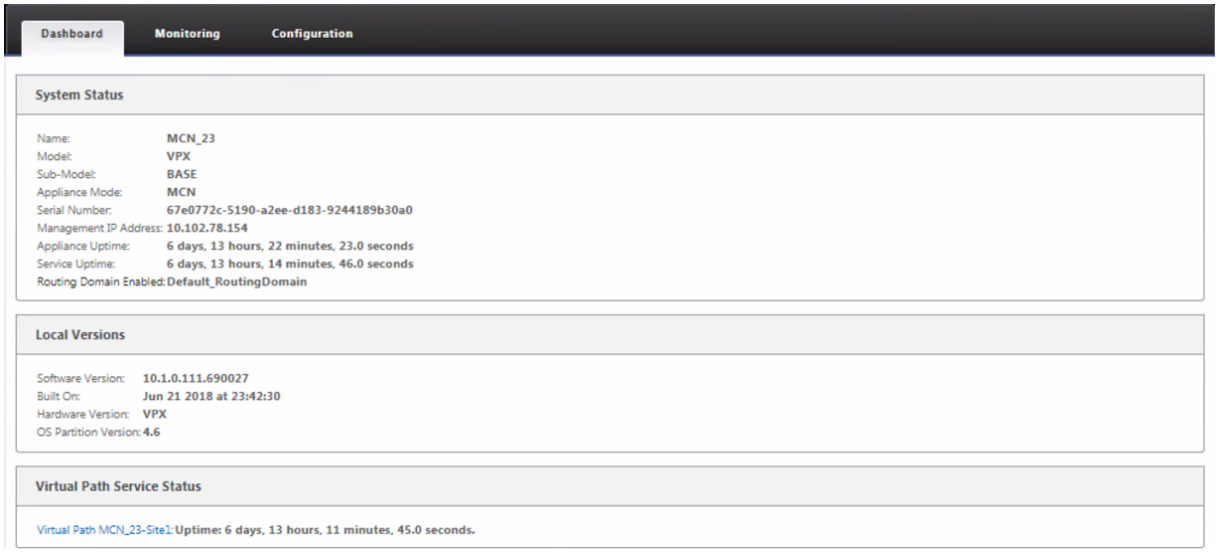
仮想パスサービスのステータス**:**

仮想パス **[**サイト名**]** —このアプライアンスに関連付けられているすべての仮想パスのステータスが表示されます。仮想 WAN サービスが有効になっている場合は、このセクションがページに含まれます。Virtual WAN サービスが無効な場合、このセクションの代わりに、アラートアイコン（ゴールデンロッドのデルタ）とアラートメッセージが表示されます。

ローカルバージョン情報**:**

- ソフトウェアのバージョン—これは、アプライアンス上で現在アクティブになっている CloudBridge Virtual Path ソフトウェアパッケージのバージョンです。
- **Build on** —ローカルアプライアンス上で現在実行されている製品バージョンのビルド日です。
- ハードウェアバージョン—これは、アプライアンスのハードウェアモデル番号とバージョンです。
- **OS** パーティションのバージョン—アプライアンス上で現在アクティブな OS パーティションのバージョンです。

下の図は、サンプルのダッシュボードページを示しています。



統計情報の表示

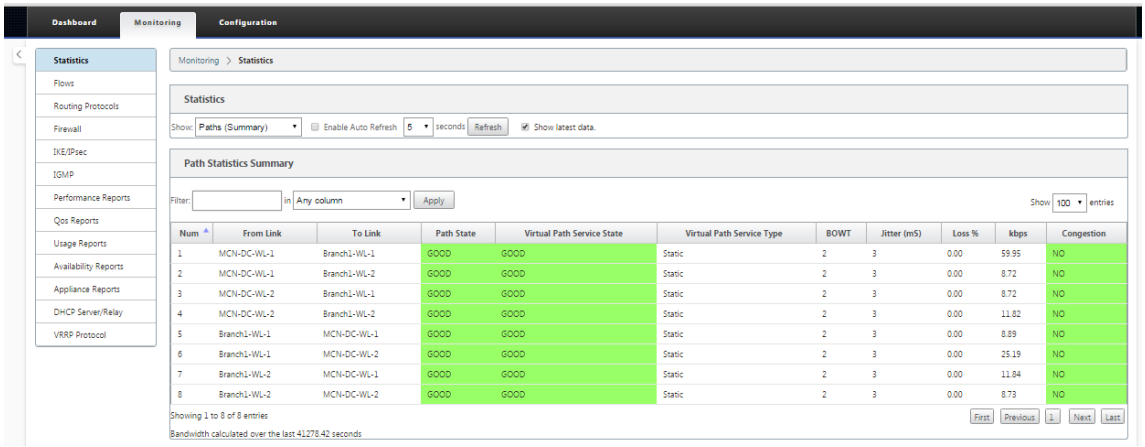
May 10, 2021

ここでは、仮想 WAN 統計情報を表示する基本的な手順について説明します。

1. MCN の管理 Web インターフェイスにログインします。
2. ［モニタリング］タブを選択します。

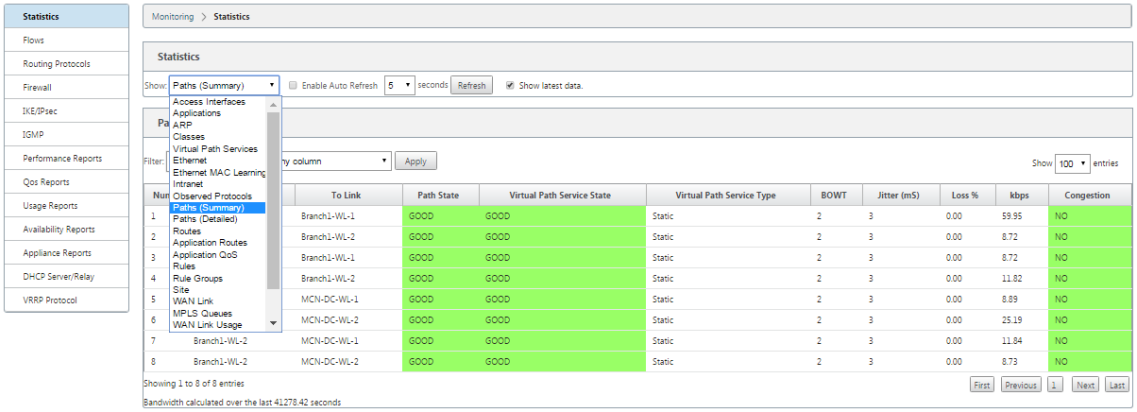
   これにより、左側のペインに [**Monitoring**] ナビゲーションツリーが開きます。デフォルトでは、[表示] フィールドで [パス] があらかじめ選択された [統計] ページも表示されます。これには、パスの統計情報の詳細なテーブルが含まれます。

   > 注
   >
   > 別の [**Monitoring**] ページ（[**Flow**s] など）に移動した場合は、[Monit **or** ing] ナビゲーション・ツリー（左側のペイン）で [**Statistics**] を選択することで、このページに戻ることができます。



3. [**Show**] フィールドの横にある [**Show**] ドロップダウンメニューを開きます。

   [表示] メニューには、パスの統計情報の他に、統計情報のフィルタリングと表示のためのオプションがいくつか用意されています。



4.「表示」メニューからフィルタを選択して、そのトピックの統計情報の表を表示します。

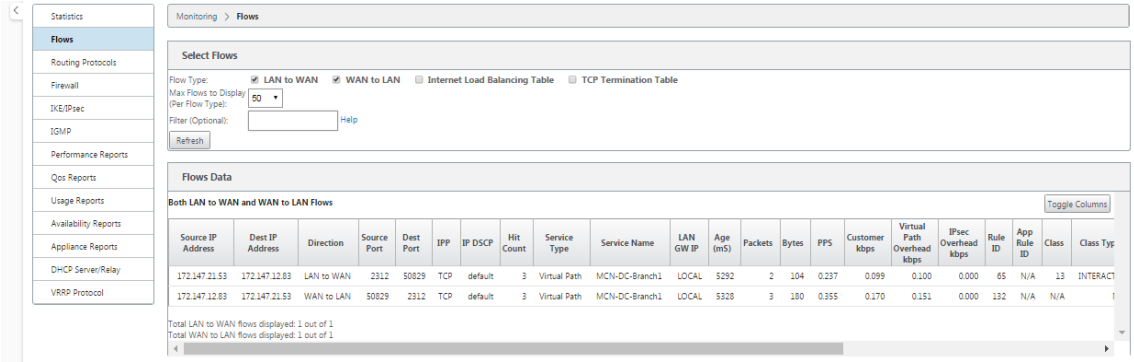
フロー情報の表示

May 10, 2021

ここでは、仮想 WAN フロー情報を表示する基本的な手順について説明します。

フロー情報を表示するには、次の手順を実行します。

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



3. [フロータイプ] を選択します。**[**** フロータイプ] フィールドは、[フロー] ページの上部にある **[**フローの選択**]** セクションにあります。**[**** フロータイプ] フィールドの横には、表示するフロー情報を選択するためのチェックボックスオプションの行があります。1 つまたは複数のチェックボックスをオンにして、表示する情報をフィルタできます。

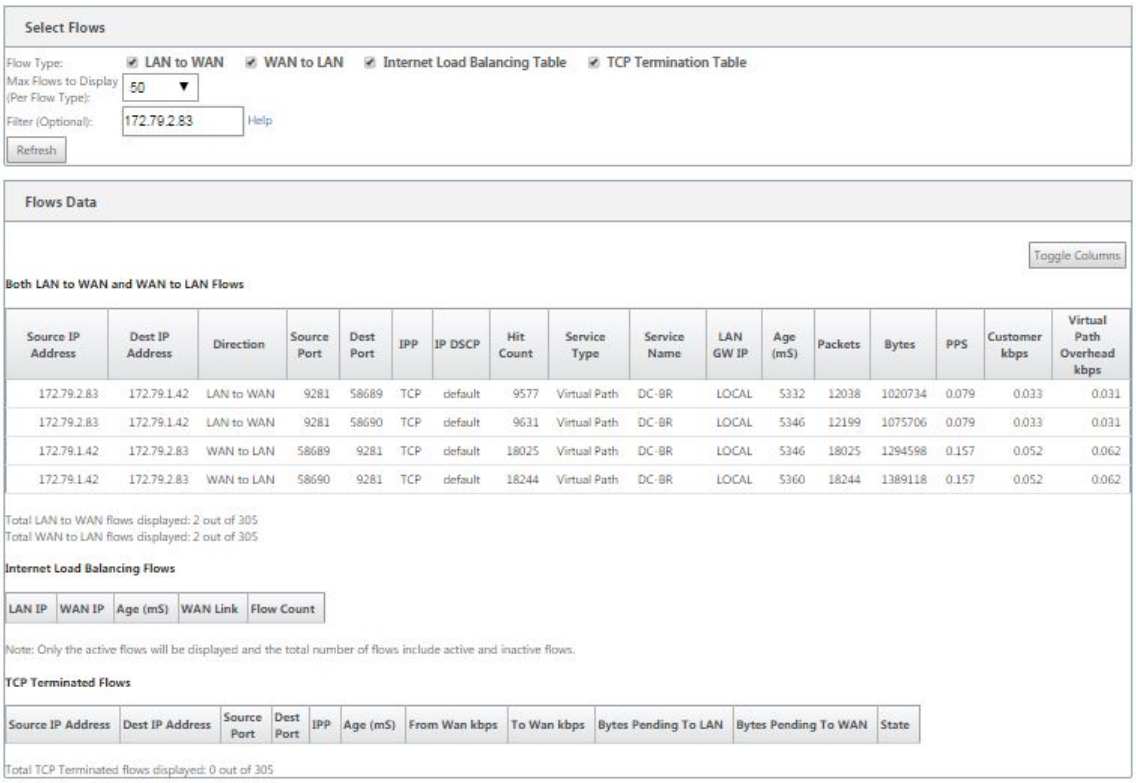
4. フィールドの横にあるドロップダウンメニューから [表示する最大フロー] を選択します。

5. これは、フロー テーブルに表示するエントリの数を決定します。オプションは、**50**、**100**、**1000** です。

6. （オプション）[**Filter**] フィールドに検索テキストを入力します。検索テキストを含むエントリのみがテーブルに表示されるように、テーブルの結果をフィルタリングします。

   > ヒント
   >
   > フィルタを使用して フロー テーブルの結果を絞り込む詳細な手順を表示するには、[フィルタ] フィールドの右側にある [ヘルプ] をクリックします。ヘルプ表示を閉じるには、[**Select Flows]** セクションの左下隅にある **[Refresh**] をクリックします。

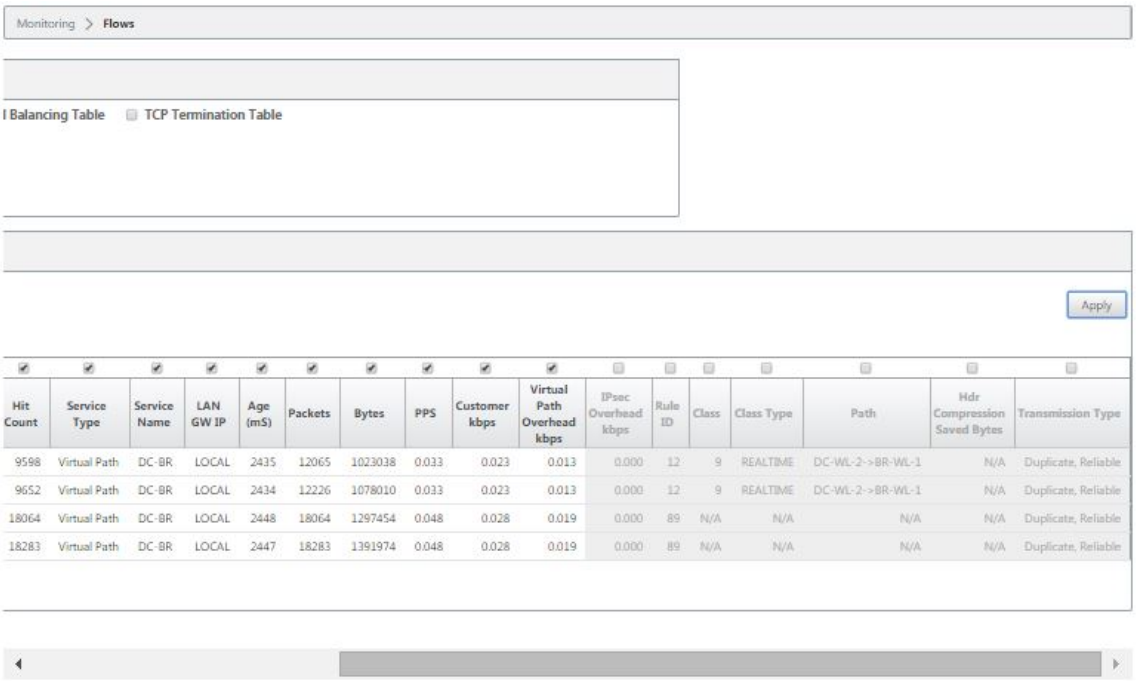
7. 「リフレッシュ」をクリックして、フィルタ結果を表示します。この図は、すべての フロー タイプを選択した状態で、フィルタリングされたフローページのサンプルを示しています。



8. （オプション）テーブルに含める列を選択します。以下を実行します:

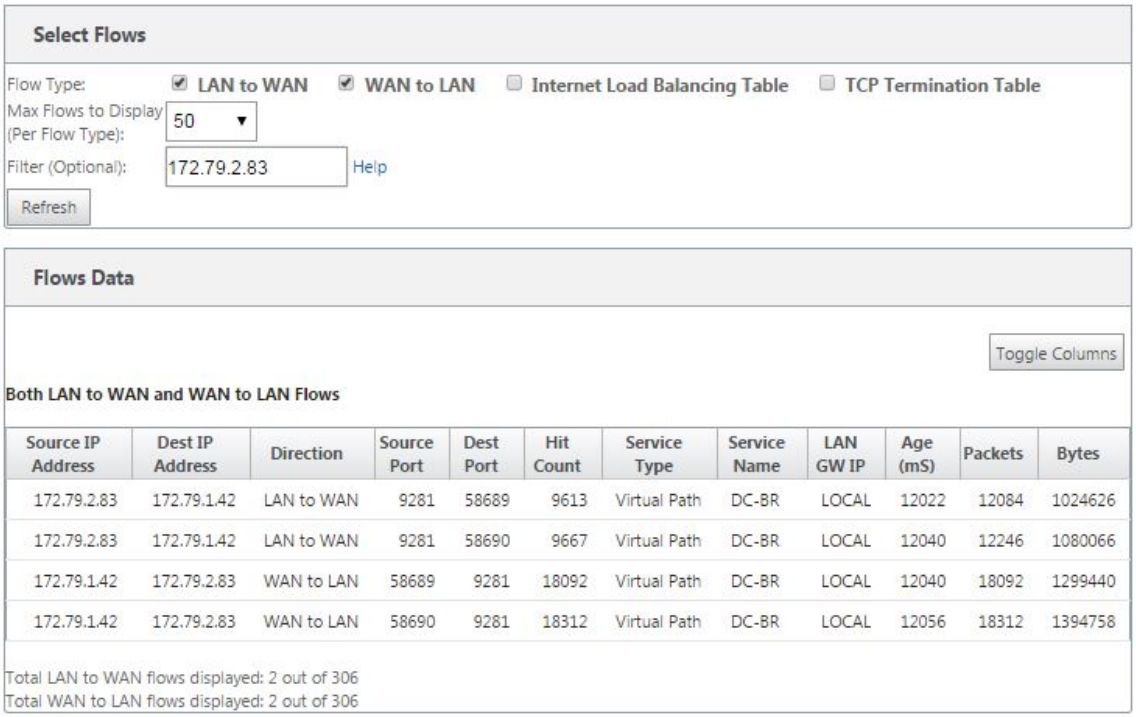
9. [列の 切り替え] をクリックします。**[** 列の切り替え] ボタンは、[フロー] テーブルの右上隅のすぐ上にあります。選択されていない列が表示され、各列の上にあるチェックボックスが開き、その列を選択または選択解除できます。選択解除された列は、図に示すように、グレー表示されます。

> 注
>
> デフォルトでは、すべての列が選択されています。これにより、表示でテーブルが切り捨てられ、[列の切り替え] ボタンが表示されなくなります。その場合は、テーブルの下に水平スクロールバーが表示されます。スクロールバーを右にスライドして表の切り捨てられたセクションを表示し、**[**列の切り替え] ボタンを表示します。スクロールバーが利用できない場合は、スクロールバーが表示されるまでブラウザウィンドウの幅を変更してみてください。



Hit Count	Service Type	Service Name	LAN GW IP	Age (mS)	Packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type
9598	Virtual Path	DC-BR	LOCAL	2435	12065	1023038	0.033	0.023	0.013	0.000	12	9	REALTIME	DC-WL-2->BR-WL-1	N/A	Duplicate, Reliable
9652	Virtual Path	DC-BR	LOCAL	2434	12226	1078010	0.033	0.023	0.013	0.000	12	9	REALTIME	DC-WL-2->BR-WL-1	N/A	Duplicate, Reliable
18064	Virtual Path	DC-BR	LOCAL	2448	18064	1297454	0.048	0.028	0.019	0.000	89	N/A	N/A	N/A	N/A	Duplicate, Reliable
18283	Virtual Path	DC-BR	LOCAL	2447	18283	1391974	0.048	0.028	0.019	0.000	89	N/A	N/A	N/A	N/A	Duplicate, Reliable

10. チェックボックスをクリックして、列を選択または選択解除します。
11. [適用] (テーブルの右上隅) をクリックします。選択オプションが解除され、選択した列のみが含まれるようにテーブルが更新されます。



Source IP Address	Dest IP Address	Direction	Source Port	Dest Port	Hit Count	Service Type	Service Name	LAN GW IP	Age (mS)	Packets	Bytes
172.79.2.83	172.79.1.42	LAN to WAN	9281	58689	9613	Virtual Path	DC-BR	LOCAL	12022	12084	1024626
172.79.2.83	172.79.1.42	LAN to WAN	9281	58690	9667	Virtual Path	DC-BR	LOCAL	12040	12246	1080066
172.79.1.42	172.79.2.83	WAN to LAN	58689	9281	18092	Virtual Path	DC-BR	LOCAL	12040	18092	1299440
172.79.1.42	172.79.2.83	WAN to LAN	58690	9281	18312	Virtual Path	DC-BR	LOCAL	12056	18312	1394758

SD-WAN Center の DPI アプリケーション

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

データ・パスは 1 分で収集されたすべてのアプリケーションに関する情報を提供しますが、1 分単位の統計レポートによって上位 100 個のアプリケーションが決定され、他のすべてのアプリケーションの集計が「その他」とレポートされます。ネットワーク内に追跡可能なアプリケーションの多様性が高い場合、データの明瞭さに影響を与える可能性があります。特に、アプリケーションの使用状況を追跡/グラフ化したい場合に、アプリケーションが上位 100 の制限から外れることがあります。

パス・マッピングと帯域幅の使用率の向上

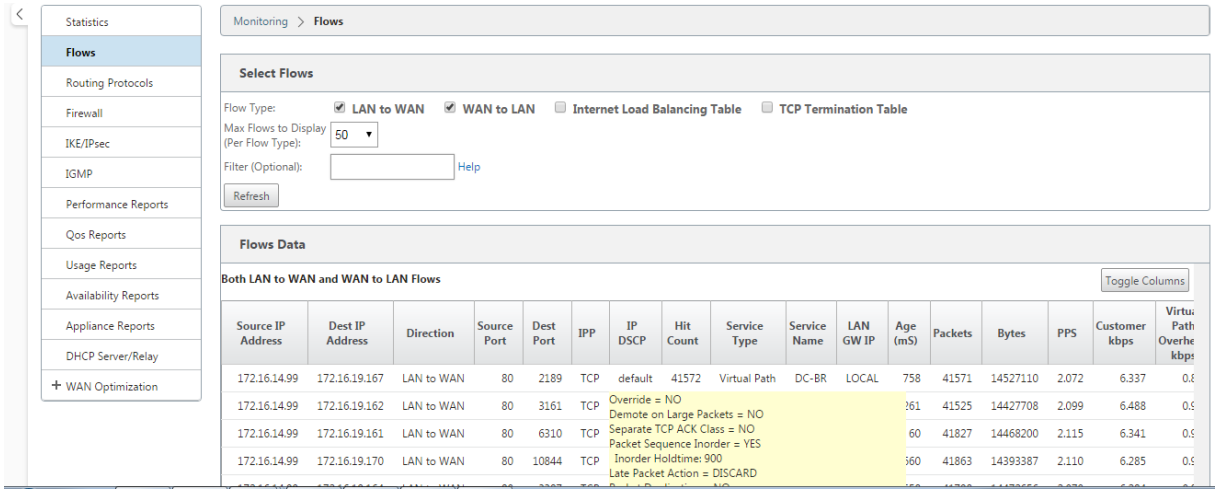
May 10, 2021

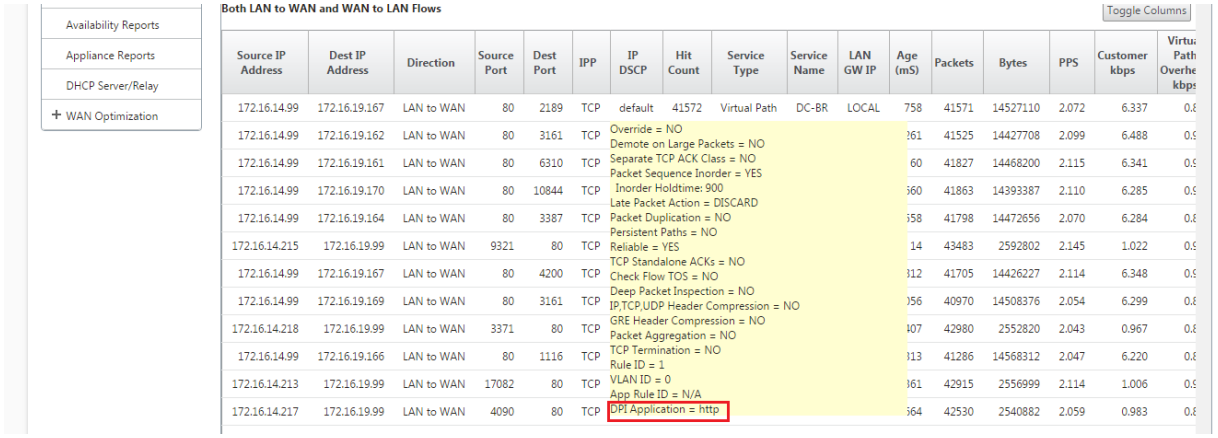
[Monitoring] タブでは、パスマッピングと帯域幅使用率の拡張が実装され、トラフィックフローが表示されます。たとえば、1 つの仮想パスだけがネットワーク接続を提供していて、その仮想パスが非アクティブになると、新しい最適パスが選択され、最初のパスが最後の最適パスになります。このシナリオは、帯域幅の需要が少なく、パスが 1 つしか選択されていない場合に実装されます。

複数の仮想パスが 1 つの接続を提供している場合、1 つの現在の最適パスと次の最適パス (使用可能な場合) が表示されます。トラフィックを処理するパスが 1 つだけ存在する場合、トラフィックを処理するパスが 3 つ以上存在し、パステーブルが 2 つのパスで更新されている場合、フローの SD-WAN GUI の [Monitoring] タブには、現在の最適パスが最初のパスとして表示され、次のカンマで区切られたパスが最後の最適パスとして表示されます。このシナリオは、帯域幅を必要とするパスを増やす必要がある場合に実装されます。

SD-WAN GUI による DPI アプリケーション情報の監視

モニタリングフローの DPI アプリケーションオブジェクト名は、SD-WAN GUI モニタリング -> フロー ページに格納され、表示されます。DPI アプリケーションを識別するためのツールチップが表示されます。





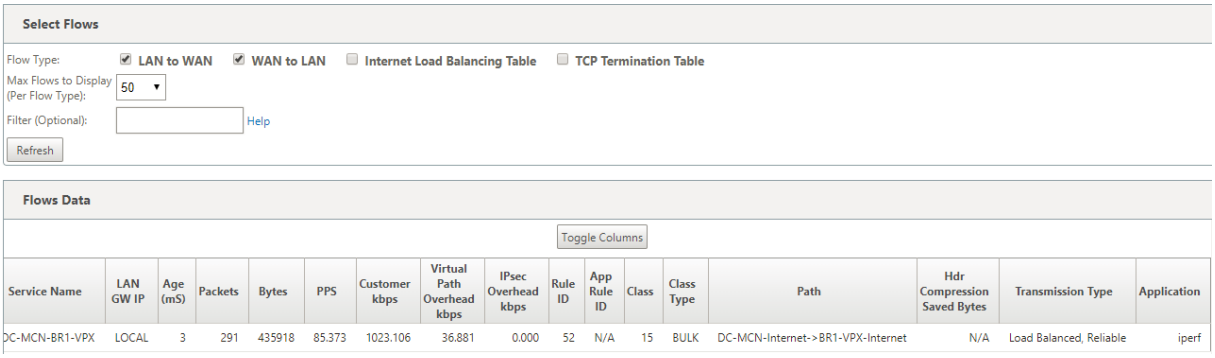
SD-WAN GUI でのトラフィックフローのパス情報のモニタリング

帯域幅を要求する着信トラフィックレートに基づいて、トラフィックを処理するために 1 つ以上のパスが必要になることがあります。

パスマッピングの実行方法を決定するには、次のシナリオを確認してください。

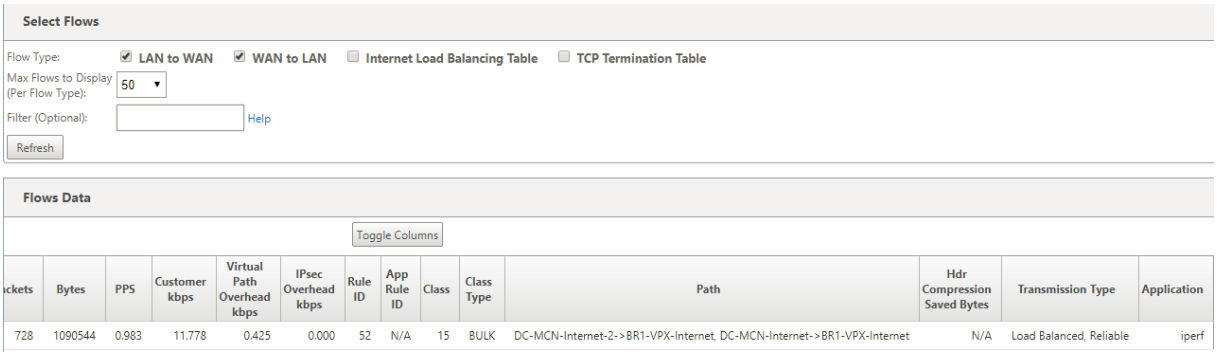
負荷分散伝送モード：

次の図は、トラフィックが開始され、すべてのパスが良好である場合、帯域幅需要が 1 つのパスによって処理されるのに十分なので、最適なパスが 1 つ選択されるシナリオを示しています。**DC-MCN-internet-> BR1-**VPX-inter**net** のパスが **1** つだけ選択され、伝送タイプのタイプが **Load Balanced** と表示されます。



次の図は、トラフィックが流れていて、そのパスの WAN 属性が低下しているときに、中断せずにトラフィックを処理するために新しいパスが選択されていることを示しています。この場合、パスマッピング機能を使用すると、トラフィックを処理する現在の最適パスが **DC-MCN-Internet2-> BR1-VPX-Internet** であり、トラフィックを処理した最後の最適パスが **DC-MCN-internet-> BR1-VPX-Internet** であることを指定できます。

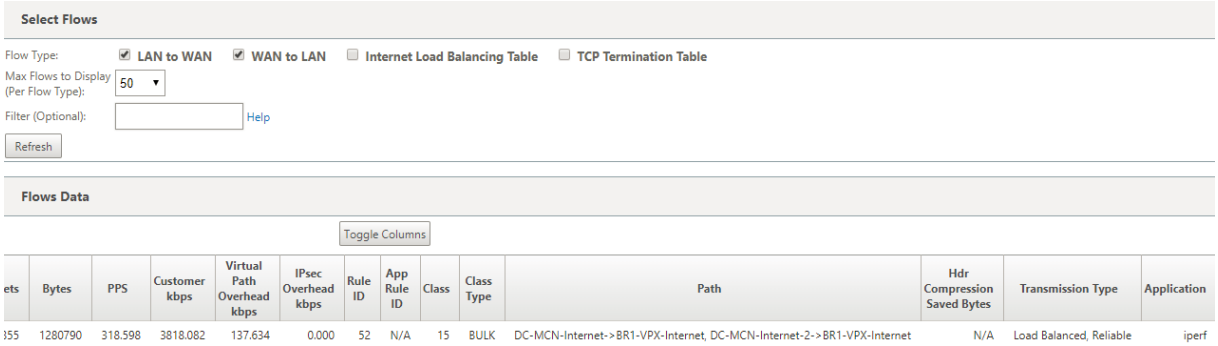
この例の最後の最適パスは、どのパスが以前に接続したかを示すインジケータです。



次の図は、トラフィックが継続中であり、帯域幅の需要によりトラフィック処理用に複数のパスが選択されている場合に、トラフィックの送信時に複数のパスが選択されていることを示しています。上記の場合とは異なり、ここではトラフィックを処理するパスが 3 つ以上ある場合がありますが、GUI では現在トラフィックを処理している最適なパスが 2 つだけ表示されます。

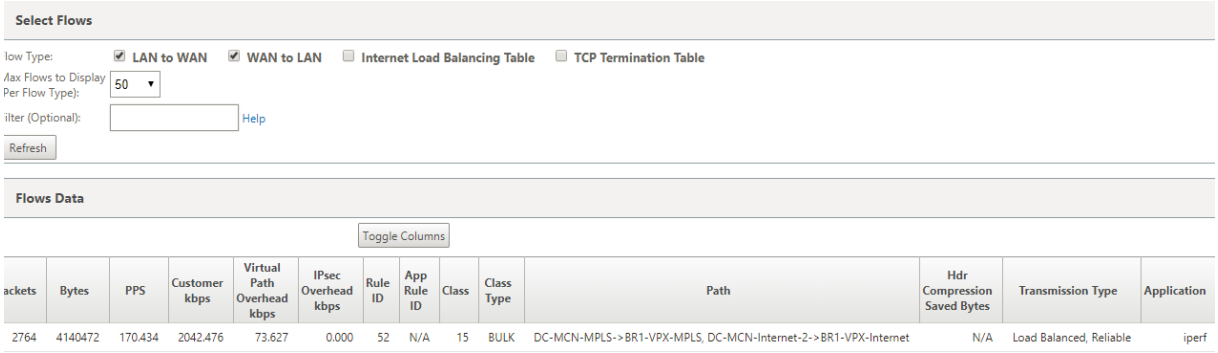
DC-MCN-インターネット**-> BR1-VPX-**インターネット、**DC-MCN-**インターネット **2-> BR1-VPX-**インターネット が、フローデータ テーブルに示されている 2 つのパスであることを確認します。

> 注
>
> 示されているように、フローテーブル内の最大 2 つのパスだけが表示されます。



次の図は、トラフィックが依然として流れているときに、**DC-MCN-Internet->BR1-VPX-Internet** である現在の最適パスが WAN アトリビュートで利用不可/非アクティブ/劣化している場合、選択された現在の最適パスが **Flows Data** テーブルのパスセクションで最初に表示されることを示しています。の後に、トラフィックを処理している最後の最適パスが続きます。

DC-MCN-インターネット**->BR1-VPX-**インターネット はもはや最適ではなかったので、新しい現在の最適パスが **DC-MCN-MPLS->BR1-VPX-MPLS** としてシステムによって選択されました。現在の最適パスとともにアクティブに接続を提供している最後の最適パスは、**DC-MCN-**インターネット **2->BR1-VPX-**です。両方のインターネット は、帯域幅の現在のトラフィック需要のために必要です。



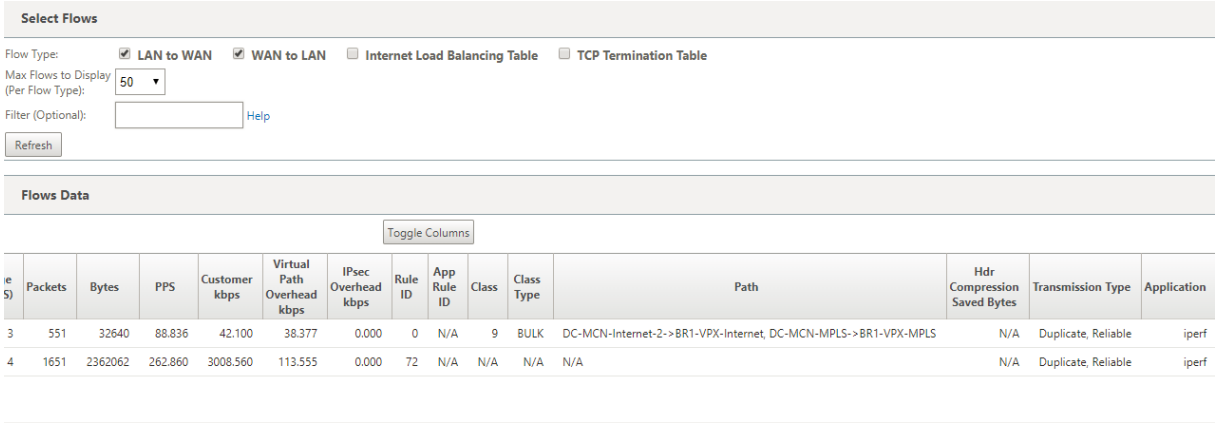
重複送信モード

一般的なパケット複製モードでは、2 つのパスが同じ接続のパケットを処理するために最初に使用され、2 つの別々のパス間でパケットを複製することによって信頼性の高い配信を保証します。

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

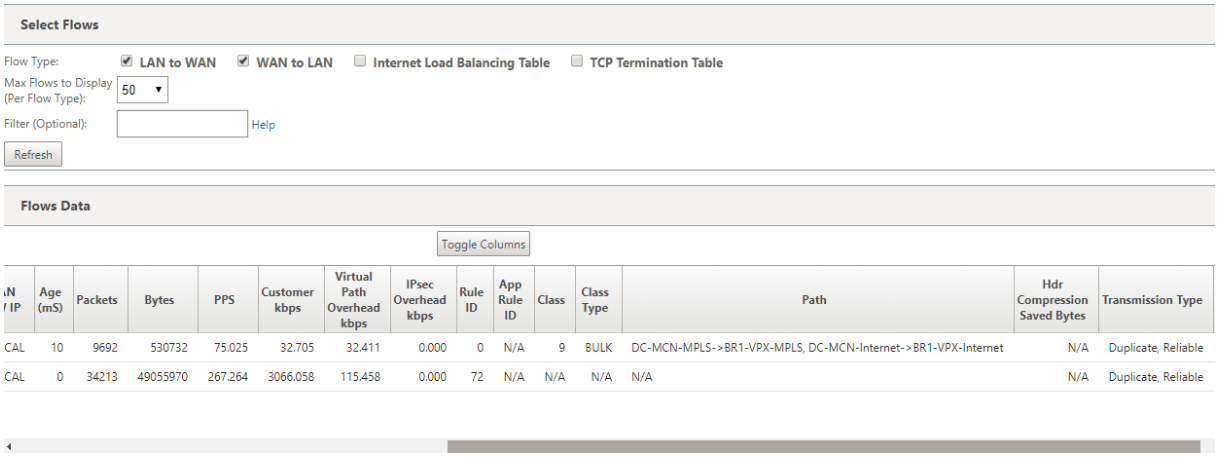
次の図は、wen トラフィックが流れていることを示しています。2 つのパスがトラフィックを処理していることがわかります。他のモードとは異なり、トラフィックが 1 つのパスだけで提供できる帯域幅が少なくても、このモードは常に 2 つのパス間でトラフィックを複製し、信頼性の高いアプリケーション配信を実現します。

次の図では、[フローデータ] テーブルのパスセクションに 2 つのパス（**DC-MCN-Internet2-> BR-VPX-**インターネット、**DC-MCN-MPLS-> BR1-VPX-MPLS**）があります。



Packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	App Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type	Application
551	32640	88.836	42.100	38.377	0.000	0	N/A	9	BULK	DC-MCN-Internet-2->BR1-VPX-Internet, DC-MCN-MPLS->BR1-VPX-MPLS	N/A	Duplicate, Reliable	iperf
1651	2362062	262.860	3008.560	113.555	0.000	72	N/A	N/A	N/A	N/A	N/A	Duplicate, Reliable	iperf

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

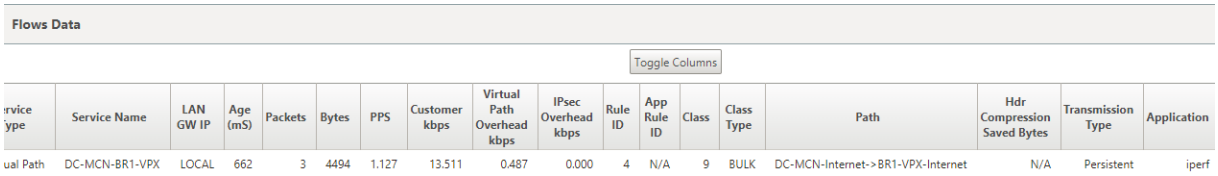


Age (mS)	Packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	App Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type
10	9692	530732	75.025	32.705	32.411	0.000	0	N/A	9	BULK	DC-MCN-MPLS->BR1-VPX-MPLS, DC-MCN-Internet->BR1-VPX-Internet	N/A	Duplicate, Reliable
0	34213	49055970	267.264	3066.058	115.458	0.000	72	N/A	N/A	N/A	N/A	N/A	Duplicate, Reliable

永続パス送信モード

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

次の図は、フローとそのパケットを現在処理している最適なパスである 1 つのパスだけを示しています。帯域幅の需要はなく、1 つのパスがすべてを供給します。現在、**DC-MCN-**インターネット**->BR1-VPX-**インターネットである最適なパスは **1** つだけです。



Service Name	LAN GW IP	Age (mS)	Packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	App Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type	Application
DC-MCN-BR1-VPX	LOCAL	662	3	4494	1.127	13.511	0.487	0.000	4	N/A	9	BULK	DC-MCN-Internet->BR1-VPX-Internet	N/A	Persistent	iperf

次の図は、パス **DC-MCN-internet->BR1-VPX-internet** が遅延が発生しやすくなったり、無効になったりすると、新しいパスが有効になり、現在のパス **DC-MCN-internet->BR1-VPX-inter** net が最後の最適パスになることを示しています。

したがって、新しいパスセクションには、**DC-MCN-MPLS->BR1-VPX-MPLS**、**DC-MCN-**インターネット**->BR1-VPX-**インターネットが表示されます。

Flows Data

Toggle Columns

N / IP	Age (mS)	Packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	App Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type	Application
CAL	950	41	61418	0.992	11.894	0.429	0.000	4	N/A	9	BULK	DC-MCN-MPLS->BR1-VPX-MPLS, DC-MCN-Internet->BR1-VPX-Internet	N/A	Persistent	iperf

永続モードでは、トラフィックを処理するために複数のパスを選択することができます。この場合、GUI は、トラフィックフローの先頭からフローテーブルの path セクションに、ベストパスとネクストベストパスの両方を表示します。

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

Flows Data

Toggle Columns

	Age (mS)	Packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	App Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type	Application
L	51	6368	367504	128.449	59.303	55.490	0.000	2	N/A	9	BULK	DC-MCN-Internet->BR1-VPX-Internet, DC-MCN-MPLS->BR1-VPX-MPLS	N/A	Persistent	iperf
L	1	9694	13894396	195.491	2241.576	84.452	0.000	74	N/A	N/A	N/A	N/A	N/A	Persistent	iperf

DC-MCN-internet の最良パスの 1 つが高遅延になるか、無効になっていると仮定します。これにより、新しいパスが表示され、その時点でのパス選択の決定に基づいて、新しいパスが最適パスになるか、2 番目の最適パスになることができます。

Flows Data

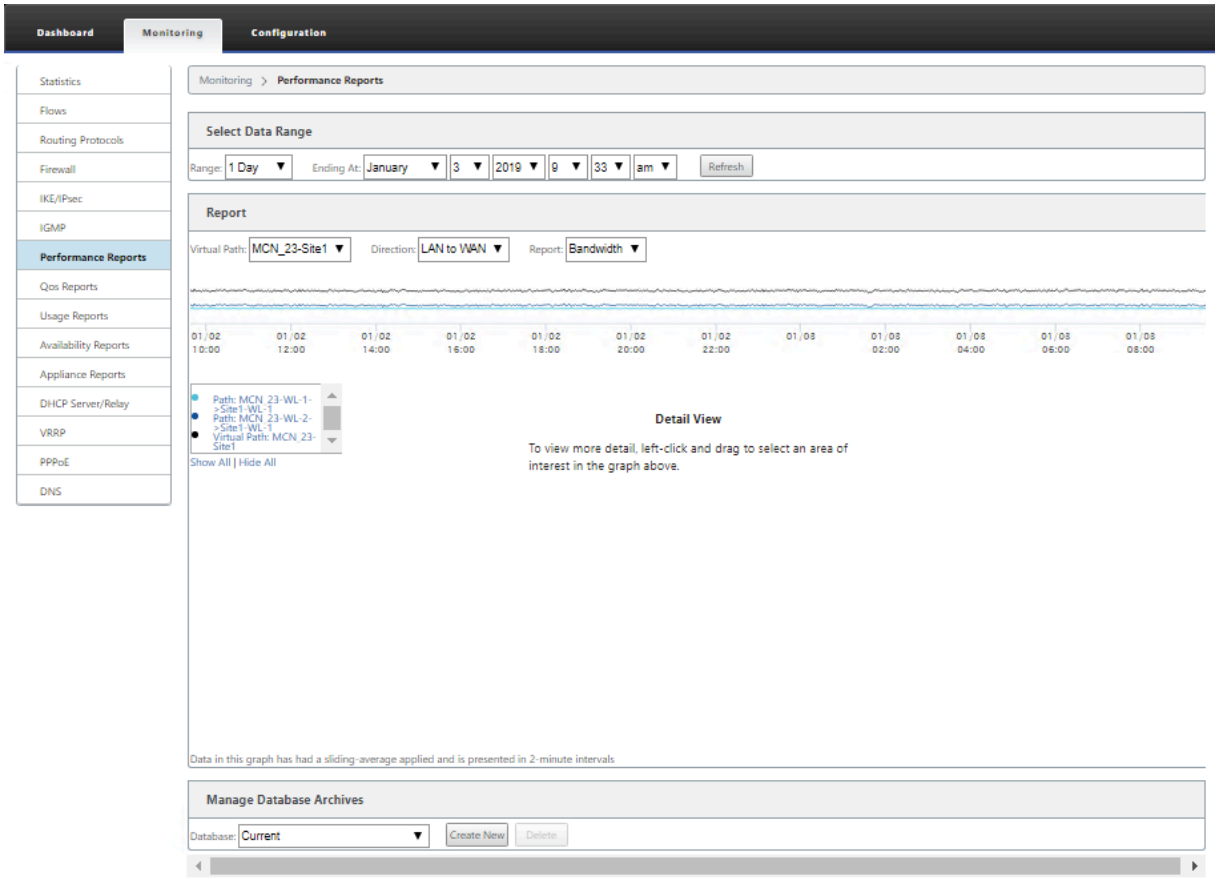
Toggle Columns

Age (mS)	Packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	App Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type	Application
2	79540	4709572	147.475	73.223	63.709	0.000	2	N/A	9	BULK	DC-MCN-MPLS->BR1-VPX-MPLS, DC-MCN-Internet-2->BR1-VPX-Internet	N/A	Persistent	iperf
0	119720	171655210	195.634	2233.531	84.514	0.000	74	N/A	N/A	N/A	N/A	N/A	Persistent	iperf

レポートの表示

May 10, 2021

このセクションでは、管理 Web Interface を使用してローカルアプライアンスに関する仮想 WAN レポートを生成および表示する基本的な手順について説明します。アプライアンスは、最大 30 個のアーカイブを保持し、30 個のエントリを超える最も古いアーカイブをパージできます。



> 注
>
> 管理 Web インターフェイスで生成されたレポートは、ローカルアプライアンスにのみ適用されます。仮想 WAN のレポートを生成および表示するには、仮想 WAN センター Web インターフェイスを使用します。

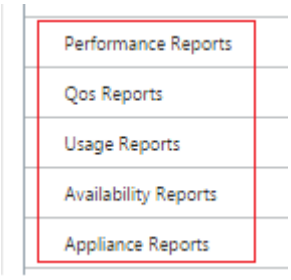
仮想 WAN レポートを生成および表示するには、次の手順を実行します。

1. MCN の管理 Web インターフェイスにログオンし、[モニタリング] タブを選択します。

   これにより、左側のペインに [**Monitoring**] ナビゲーションツリーが開きます。

2. ナビゲーション・ツリーからレポート・タイプを選択します。

   レポートタイプは、ナビゲーションツリーの [**Flow** s] ブランチのすぐ下にブランチとして表示されます。



   使用可能なレポートタイプは次のとおりです。

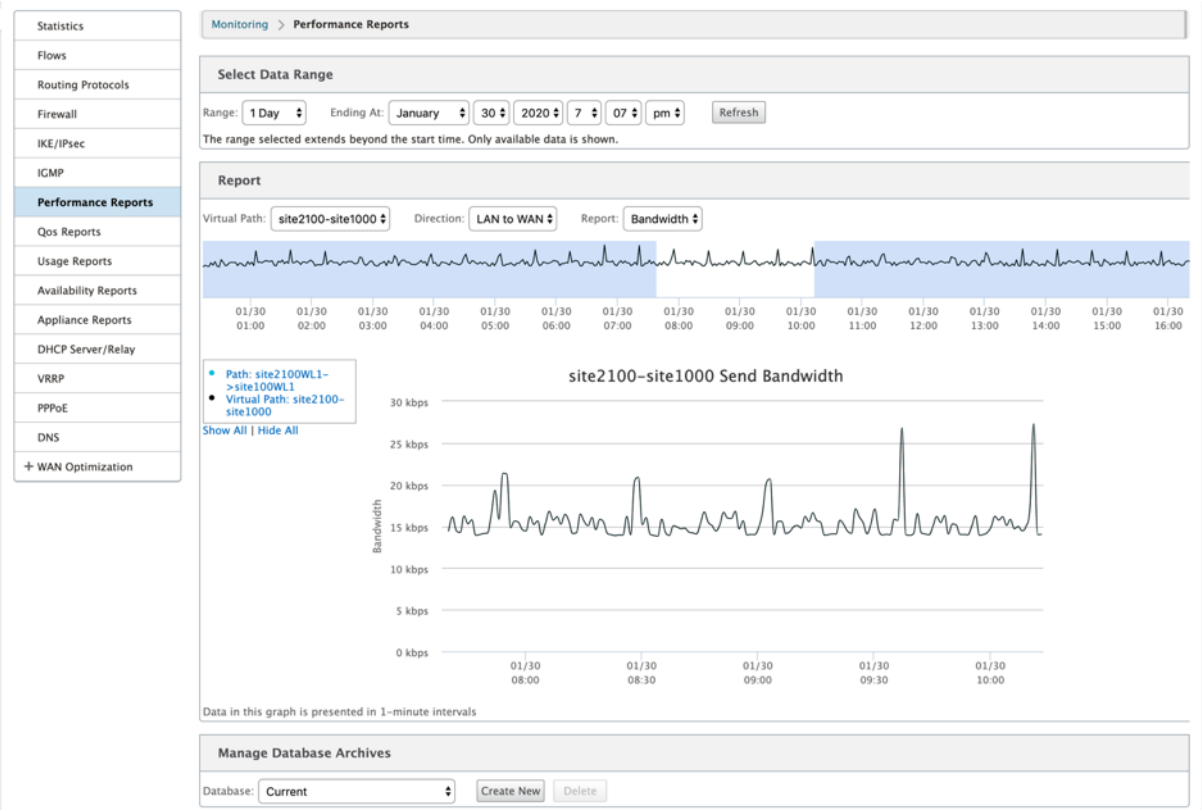
- パフォーマンスレポート
- **QoS** レポート
- 使用状況レポート
- 可用性レポート
- アプライアンス・レポート

3. レポートオプションを選択します。

さまざまなタイプのレポートに加えて、各レポートタイプには、レポート結果を絞り込むための多数のオプションとフィルタがあります。

パフォーマンス・レポート

Citrix SD-WAN では、サイト、仮想パス、または方向（LAN から WAN および WAN から LAN）レベルでパフォーマンス統計を表示できます。Citrix SD-WAN を使用すると、各リンクの効率をミリ秒単位で示すメトリックを収集できます。詳細を表示するには、左クリックしてグラフライン内のパスまたは時間枠の特定の領域を選択します。



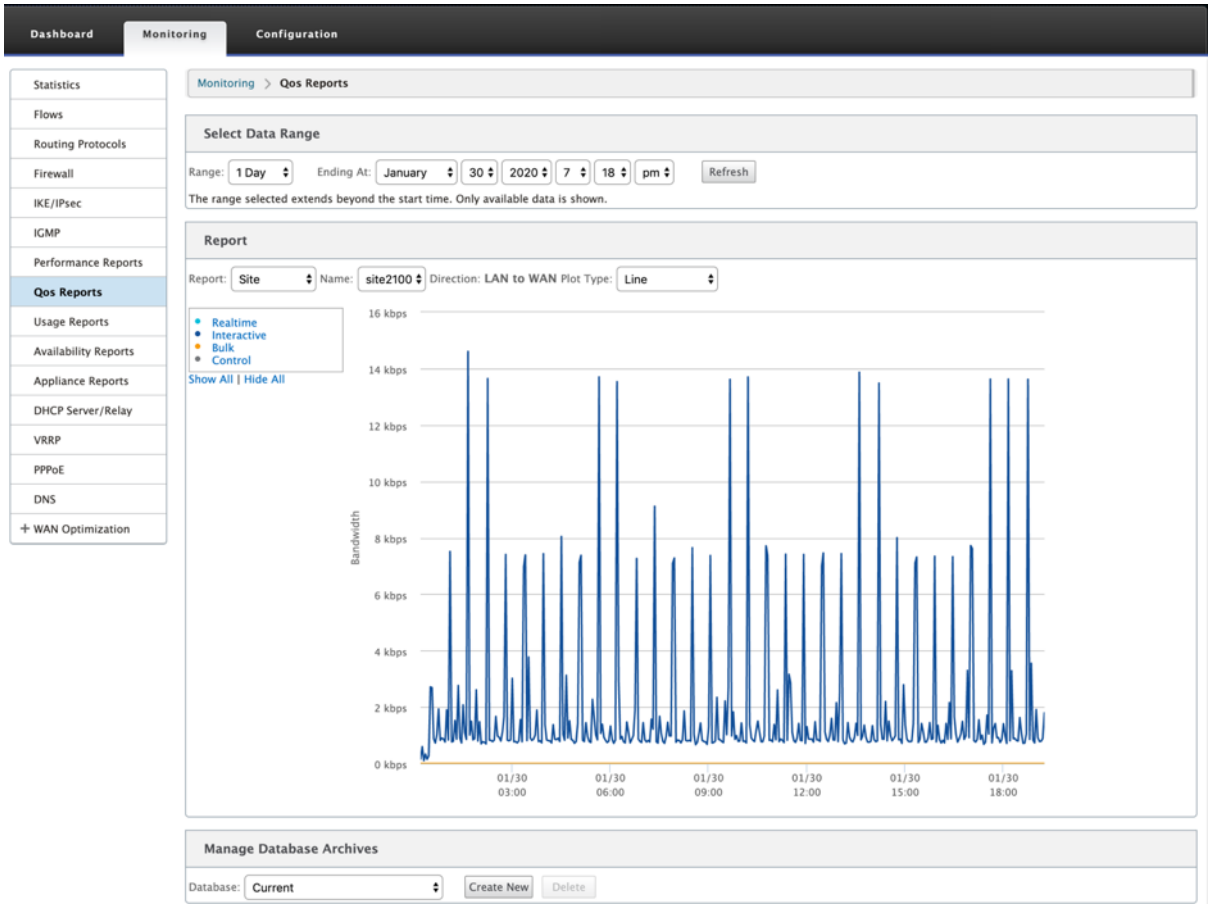
必要に応じてデータ範囲を選択し、次のフィールドを使用してパフォーマンス・レポートを表示できます。

- 仮想パス：ドロップダウンリストから仮想パスを選択します。
- 方向**:** 必要に応じて [方向] を選択します ([LAN から WAN へ] または [WAN から LAN へ])。

- レポート**:** レポート を表示するには、次のネットワークパラメータを選択します。
  - 帯域幅
  - 遅延
  - ジッタ ー
  - 損失
  - 品質

QoS レポート

アプリケーション QoS レポートは、各サイト、WAN リンク、仮想パス、パスレベルでアップロード、ダウンロード、ドロップされたパケット数またはバイト数などの監視できます。



次のメトリックを表示できます。

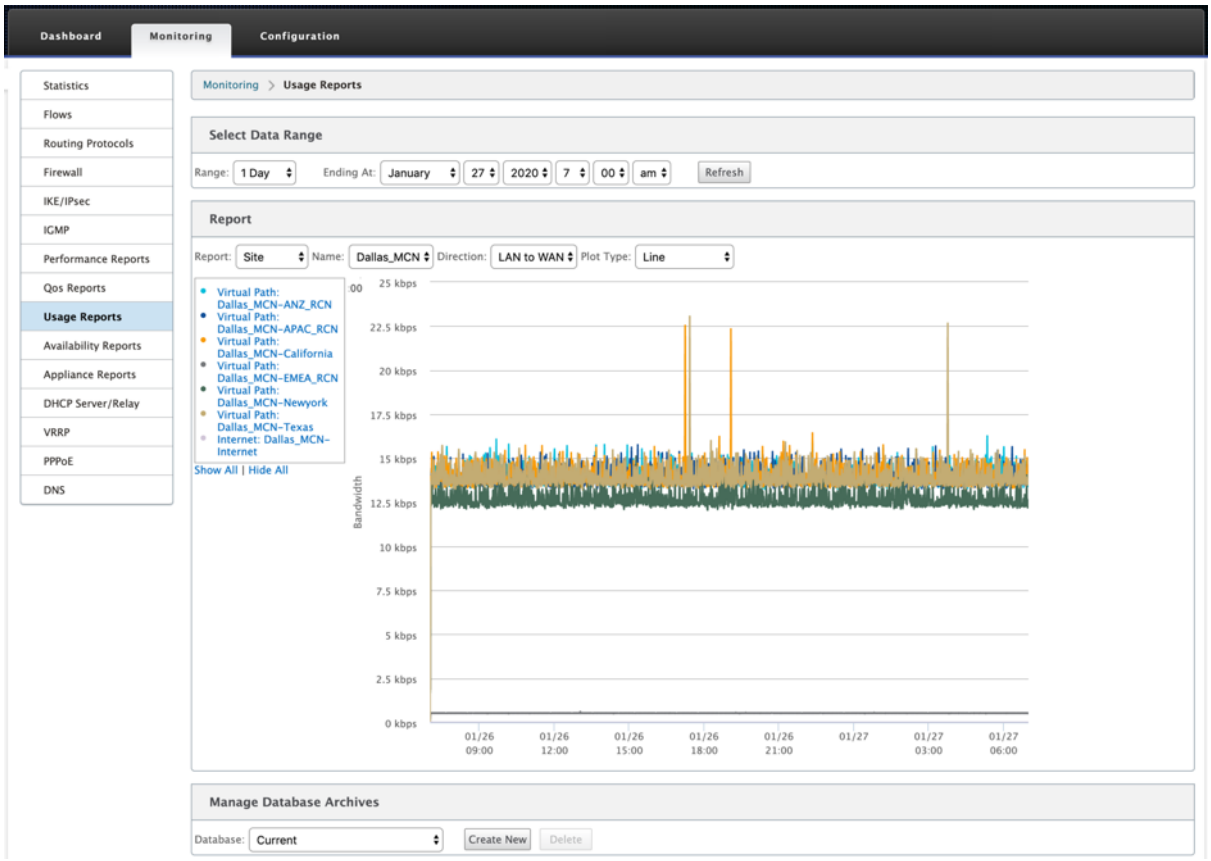
- リアルタイム： Citrix SD-WAN 構成でリアルタイムクラスの種類に属するアプリケーションによって消費される帯域幅。このようなアプリケーションのパフォーマンスは、ネットワーク遅延に大きく依存します。遅延したパケットは、失われたパケットよりも劣ります（たとえば、VoIP、Skype for Business）。
- インタラクティブ： Citrix SD-WAN 構成の対話型クラスの種類に属するアプリケーションによって消費される帯域幅。このようなアプリケーションのパフォーマンスは、ネットワーク遅延とパケット損失に大きく依存

します（たとえば、XenDesktop、XenApp）。

- **Bulk**： Citrix SD-WAN 構成でバルククラスタイプに属するアプリケーションによって消費される帯域幅。これらのアプリケーションは、人的介入がほとんどなく、ほとんどがシステム自体（FTP、バックアップ操作など）によって処理されます。
- コントロール**:** ルーティング、スケジューリング、およびリンクの統計情報を含む制御パケットの転送に使用される帯域幅。

使用状況レポート

使用状況レポートは、仮想パスの使用状況情報を提供します。

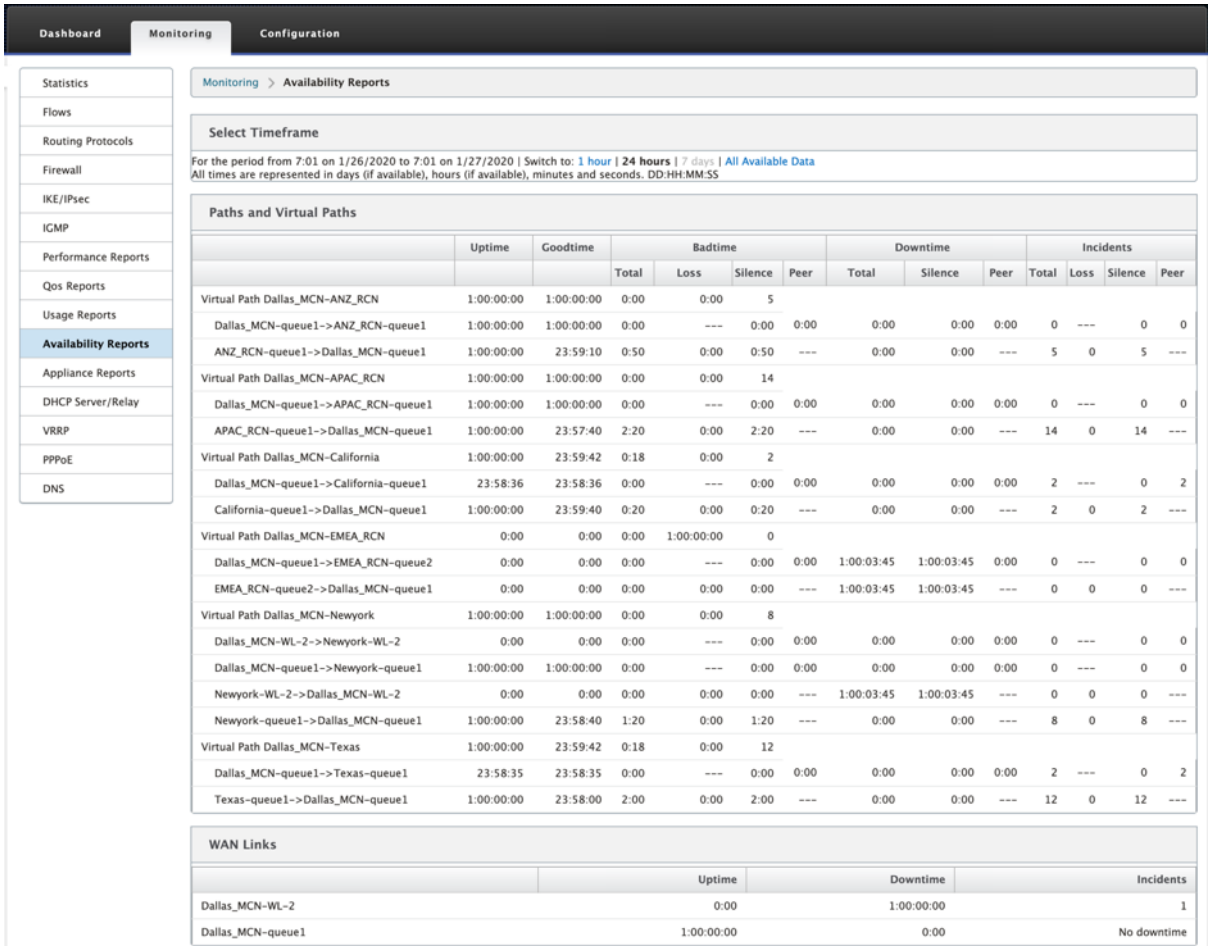


- レポート**:** ドロップダウンリストから [サイト] または [**WAN** リンク] を選択して、レポートを表示します。
- [名前]**:** ドロップダウンリストからサイトまたは WAN リンクの名前を選択します。
- 方向：必要に応じて方向を選択します（LAN から WAN または WAN から LAN）。
- [プロットタイプ]**:** ドロップダウンリストから [プロットタイプ] を選択します ([線分] または [面積])。

可用性レポート

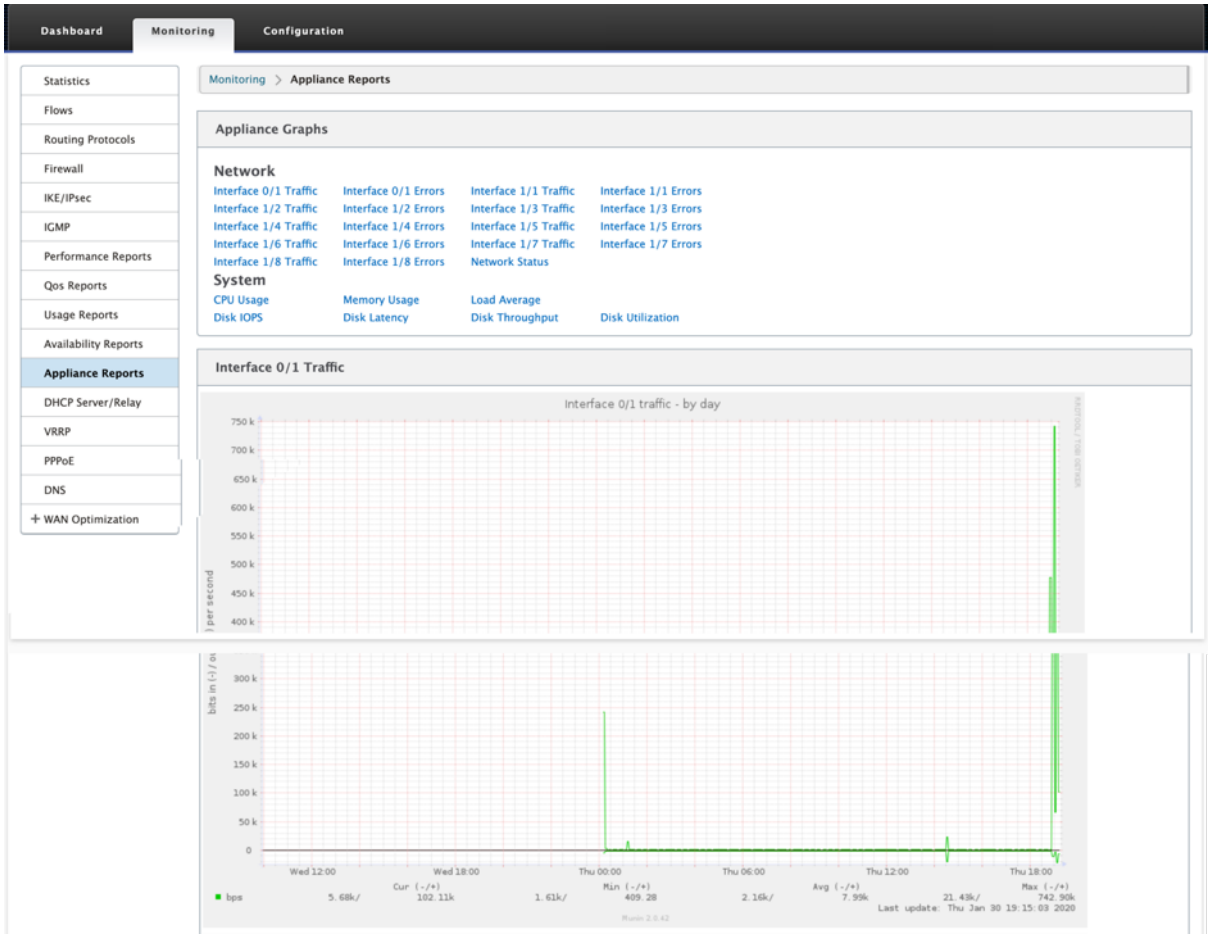
このレポートでは、WAN リンク、パス、仮想パスの可用性データを表示できます。また、1 時間、24 時間、7 日などの特定の時間枠に切り替えたり、選択して、利用可能なデータを表示することもできます。パスと仮想パスのデータ

は、**DD: HH: MM: SS** 形式で表されます。



アプライアンス・レポート

アプライアンス・レポートは、ネットワーク・トラフィックとシステム使用状況レポートを提供します。各リンクをクリックして、アプライアンスのグラフを日、週、月、年単位で表示または監視します。



ファイアウォールの統計情報の表示

May 10, 2021

ファイアウォールポリシーと NAT ポリシーを設定したら、接続、ファイアウォールポリシー、および NAT ポリシーの統計情報をレポートとして表示できます。さまざまなフィルタリングパラメータを使用して、レポートをフィルタリングできます。

ファイアウォールおよび NAT ポリシーの設定については、ステートフルファイアウォールと NAT のサポートを参照してください。

接続

ファイアウォールポリシーのアプリケーションの統計情報を確認できます。これにより、選択したアプリケーションと一致するすべての接続、接続元、接続先、および生成しているトラフィックの量を確認できます。ファイアウォールポリシーが、各アプリケーションのトラフィックに対してどのように動作しているかを確認できます。

次のパラメータを使用して、接続統計をフィルタリングできます。

- アプリケーション-接続のフィルタ条件として使用されるアプリケーション。
- ファミリ-接続のフィルタ条件として使用されるアプリケーションファミリ。
- IP プロトコル-接続によって使用される IP プロトコル。
- ソースゾーン-接続の発信元のゾーン。
- 宛先ゾーン-応答トラフィックの発信元ゾーン。
- ソースサービスタイプ-接続の発信元のサービス。
- ソースサービスインスタンス-接続の発信元であるサービスのインスタンス。
- [Source IP]：接続の発信元の IP アドレス。ドット付き 10 進表記で入力し、オプションのサブネットマスクを使用します。
- [Source Port]：接続元のポートまたはポートの範囲。「-」文字を使用して、単一のポートまたはポートの範囲を受け入れます。
- 宛先サービスタイプ：応答トラフィックの発信元となるサービス。
- 宛先サービスインスタンス-応答トラフィックの発信元となるサービスのインスタンス。
- Destination IP：応答デバイスの IP アドレス。ドット付き 10 進表記で入力し、オプションのサブネットマスクを使用します。
- 宛先ポート：応答するデバイスで使用されるポートまたはポートの範囲。「-」文字を使用して、単一のポートまたはポートの範囲を受け入れます。

フィルタポリシー

ポリシーを使用すると、トラフィックフローのアクションを指定できます。ファイアウォールフィルタのグループは、ファイアウォールポリシーテンプレートを使用して作成され、ネットワーク内のすべてのサイトに適用することも、特定のサイトにのみ適用することもできます。

すべてのフィルタポリシーの統計レポートを表示し、次のパラメータを使用してフィルタリングできます。

- アプリケーションオブジェクト-ファイアウォールポリシーのフィルタ条件として使用される Application オブジェクト。
- Application-ファイアウォールポリシーでフィルタ条件として使用されるアプリケーション
- Family-ファイアウォールポリシーでフィルタ条件として使用されるアプリケーションファミリ。
- [IP プロトコル]-フィルタポリシーが一致する IP プロトコル。
- DSCP：フィルタポリシーが一致する DSCP タグ。
- [フィルタポリシーアクション]-パケットがフィルタに一致したときにポリシーが実行するアクション。
- ソースサービスタイプ-接続の発信元のサービス。
- [ソースサービス名]-接続の発信元であるサービスのインスタンス。
- [Source IP]：接続の発信元の IP アドレス。ドット付き 10 進表記で入力し、オプションのサブネットマスクを使用します。
- [Source Port]：接続元のポートまたはポートの範囲。「-」文字を使用して、単一のポートまたはポートの範囲を受け入れます。

- 宛先サービスタイプ：応答するトラフィックが宛先となるサービス。
- [宛先サービス名]：該当する場合、応答トラフィックが宛先となるサービス。
- Destination IP：応答デバイスの IP アドレス。ドット付き 10 進表記で入力し、オプションのサブネットマスクを使用します。
- 宛先ポート：応答するデバイスで使用されるポートまたはポートの範囲。「-」文字を使用して、単一のポートまたはポートの範囲を受け入れます。
- [Source Zone]：フィルタポリシーに一致する発信元ゾーン。
- 宛先ゾーン-フィルタポリシーに一致する応答ゾーン。

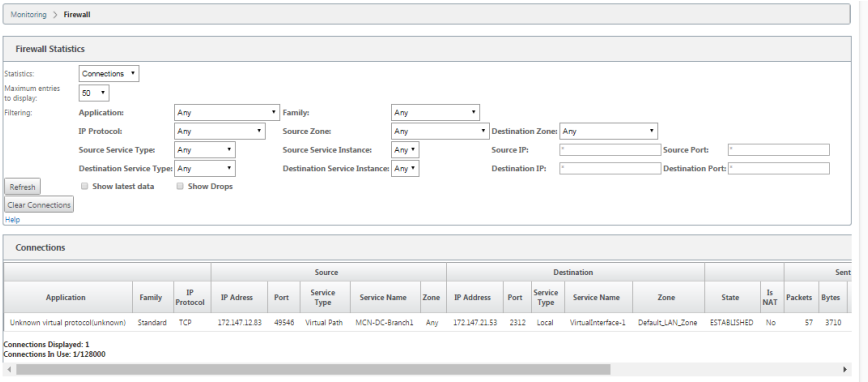
NAT ポリシー

すべてのネットワークアドレス変換（NAT）ポリシーの統計情報を表示し、次のパラメータを使用してレポートをフィルタリングできます。

- IP プロトコル-NAT ポリシーが一致する IP プロトコル。
- NAT タイプ-NAT ポリシーで使用されている NAT のタイプ。
- ダイナミック NAT タイプ：NAT ポリシーで使用中のダイナミック NAT のタイプ。
- サービスタイプ-NAT ポリシーで使用されるサービスタイプ。
- サービス名-NAT ポリシーで使用されるサービスのインスタンス。
- Inside IP-内部 IP アドレス。ドット付き 10 進表記で入力し、オプションのサブネットマスクを使用します。
- 内部ポート：NAT ポリシーで使用される内部ポート範囲。「-」文字を使用して、単一のポートまたはポートの範囲を受け入れます。
- Outside IP-外部 IP アドレス。ドット付き 10 進表記で入力し、オプションのサブネットマスクを使用します。
- [Outside Port]：NAT ポリシーで使用される外部ポート範囲。「-」文字を使用して、単一のポートまたはポートの範囲を受け入れます。

ファイアウォールの統計情報を表示するには

1. [監視] > [ファイアウォール**]** に移動します。
2. [Statistics] フィールドで、必要に応じて [接続]、[フィルタポリシー**]**、または **[NAT** ポリシー] を選択します。
3. フィルタ条件を必要として設定します。



4. [更新] をクリックします。

診断

September 26, 2023

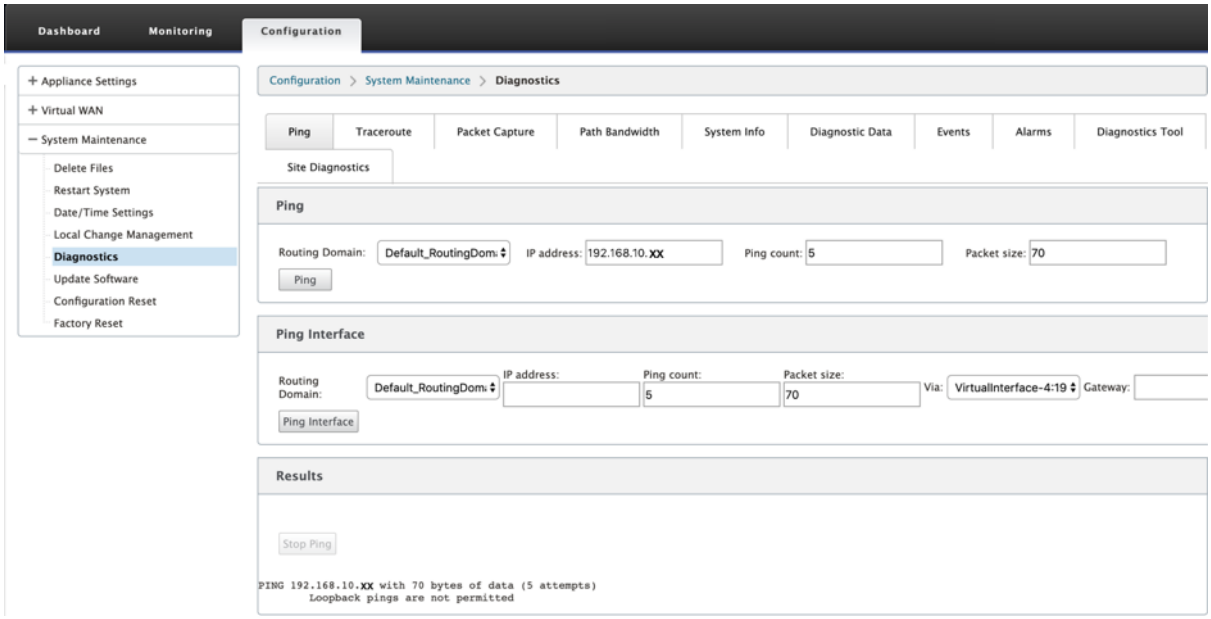
Citrix SD-WAN 診断ユーティリティには、接続の問題をテストおよび調査するための次のオプションが用意されています。

- Ping
- Traceroute
- パケットキャプチャ
- パス帯域幅
- システム情報
- 診断データ
- イベント
- alarms
- 診断ツール
- サイト診断

Citrix SD-WAN ダッシュボードの診断オプションは、データ収集を制御します。

Ping

Ping オプションを使用するには、[構成**] > [**診断] に移動し、[**Ping**] を選択します。Ping を使用して、ホストの到達可能性とネットワーク接続を確認できます。

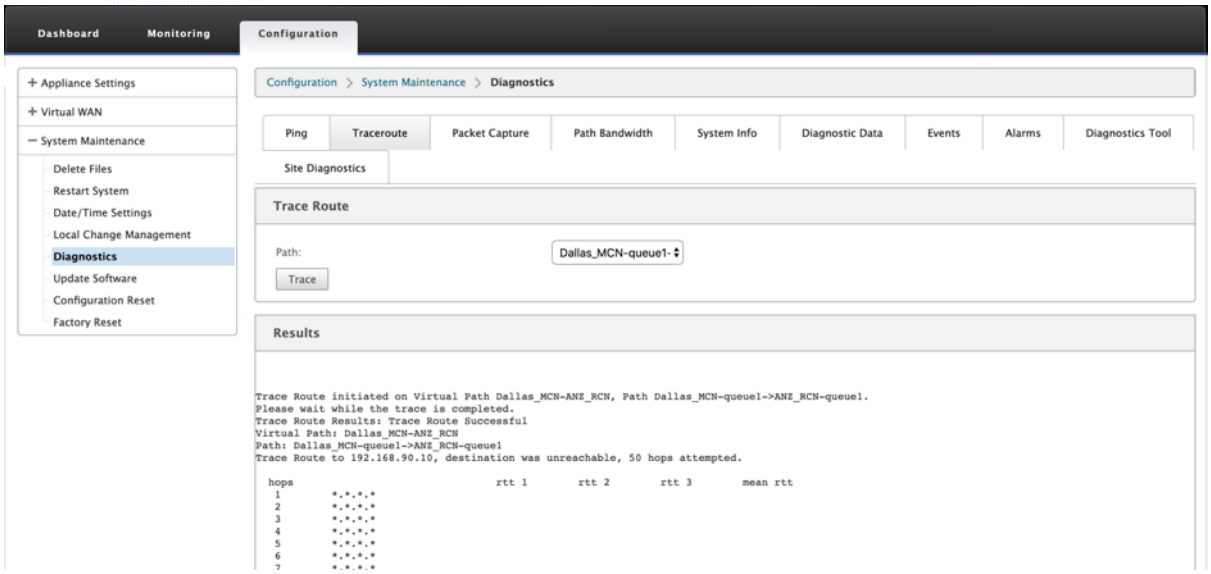


ルーティングドメインを選択します。有効な IP アドレス、ping カウント数 (ping 要求を送信する回数)、およびパケットサイズ (データバイト数) を指定します。[**Ping** の停止] をクリックして、進行中の ping 検索を停止します。

特定のインターフェイスから ping を実行できます。ルーティングドメインを選択し、IP アドレスと ping カウント、パケットサイズを指定し、ドロップダウンリストから仮想インターフェイスを選択します。

Traceroute

Traceroute オプションを使用するには、[構成] **> [**システムメンテナンス**] > [**診断**]** を展開し、[**traceroute**] を選択します。

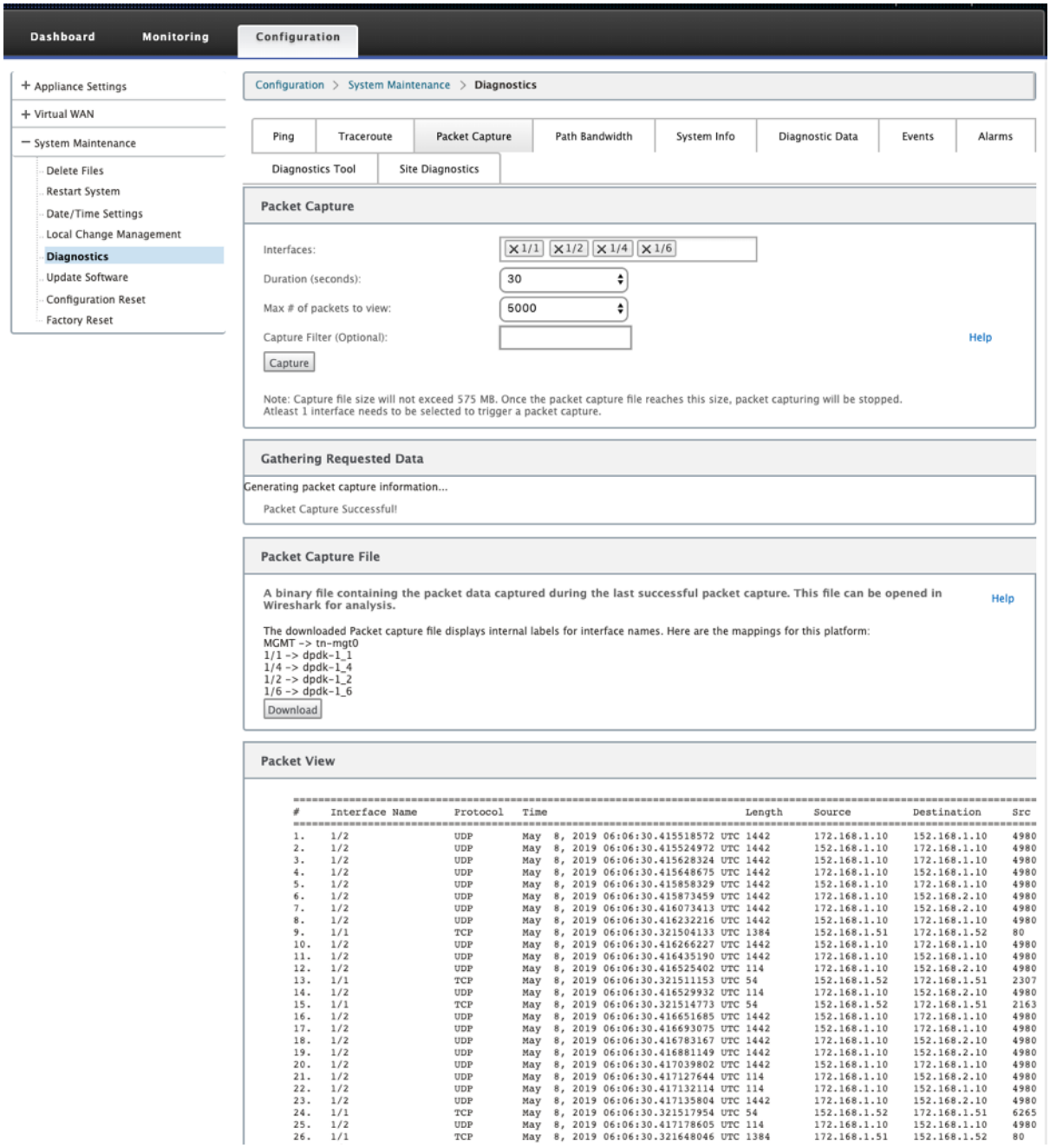


traceroute は、リモートサーバーへのパスまたはルートの検出と表示に役立ちます。**Traceroute** オプションをデバッグツールとして使用して、ネットワーク内の障害点を検出します。

ドロップダウンリストからパスを選択し、[トレース] をクリックします。[結果] セクションで詳細を表示できます。

Packet capture

[パケットキャプチャ（**Packet Capture** ）] オプションを使用すると、選択したサイトに存在する選択したアクティブインターフェイスを通過するリアルタイムデータパケットを代行受信できます。パケットキャプチャは、ネットワークの問題の分析とトラブルシューティングに役立ちます。



パケットキャプチャ操作に次の入力を提供します。

- インターフェイス -アクティブなインターフェイスは、SD-WAN アプライアンスのパケットキャプチャに使用できます。ドロップダウンリストからインターフェイスを選択するか、インターフェイスを追加します。パケットキャプチャをトリガーするには、少なくとも 1 つのインターフェイスを選択する必要があります。

  > 注:
  >
  > すべてのインターフェイスで同時にパケットキャプチャを実行する機能は、トラブルシューティングタスクのスピードアップに役立ちます。

- **Duration (**秒) —データをキャプチャする必要がある期間 (秒単位)。
- 表示するパケットの最大数: パケットキャプチャ結果に表示されるパケットの最大制限。
- **Capture Filter**（オプション）: オプションの Capture Filter フィールドは、キャプチャされるパケットを決定するために使用されるフィルタ文字列を受け入れます。パケットはフィルター文字列と比較され、比較結果が true の場合、パケットがキャプチャされます。フィルターが空の場合、すべてのパケットがキャプチャされます。詳細については、キャプチャフィルタを参照してください。

このキャプチャフィルターの例を以下に示します。

- **Ether proto\ ARP**： ARP パケットだけをキャプチャします。
- **Ether proto\ IP**： IPv4 パケットのみをキャプチャします
- **VLAN 100**： VLAN が 100 のパケットのみをキャプチャします。
- ホスト **10.40.10.20** -アドレスが 10.40.10.20 のホストとの間で送受信される IPv4 パケットのみをキャプチャします
- ネット **10.40.10.0** マスク **255.255.255.0** -10.40.10.0/24 サブネット内の IPv4 パケットだけをキャプチャします
- **IP** プロト **¥TCP** -IPv4/TCP パケットのみをキャプチャします。
- ポート **80**： ポート 80 との間で送受信される IP パケットのみをキャプチャします。
- ポート範囲 **20** ～**30**: ポート 20 ～30 との間で送受信される IP パケットだけをキャプチャします。

> 注
>
> キャプチャファイルの最大サイズ制限は最大 575 MB です。パケットキャプチャファイルがこのサイズに達すると、パケットキャプチャは停止します。

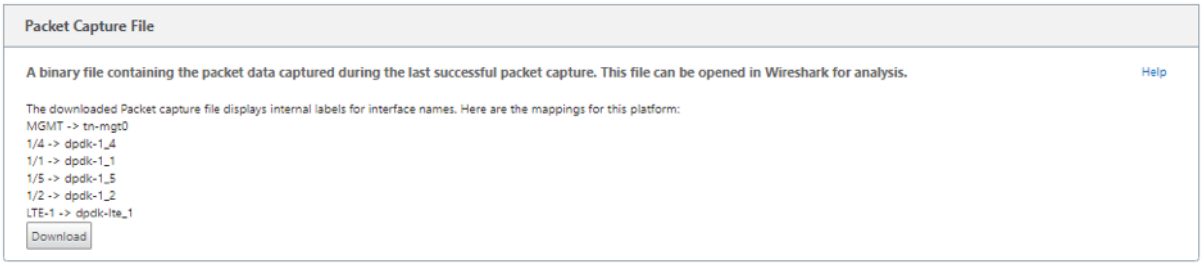
[**Capture**] をクリックして、パケットキャプチャ結果を表示します。最後に成功したパケットキャプチャ中にキャプチャされたパケットデータを含むバイナリファイルをダウンロードすることもできます。

リクエストされたデータの収集

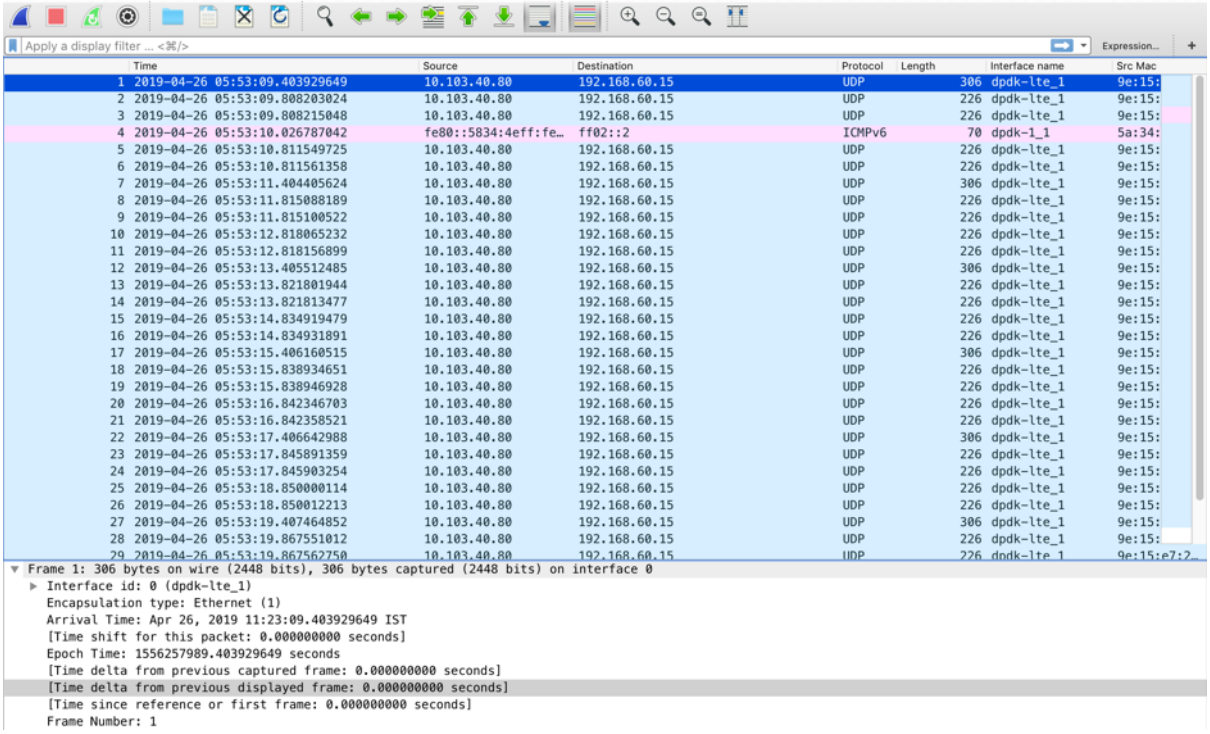
この表では、パケットキャプチャ情報の生成のステータス（パケットキャプチャが成功したかどうか、パケットキャプチャがないかどうか）を確認できます。

パケットキャプチャファイル

パケットは、最後に成功したパケットキャプチャ中に、バイナリデータとしてキャプチャされます。バイナリファイルをダウンロードして、パケット情報をオフラインで分析できます。インタフェース名は、GUI インタフェースと比較して、ダウンロードしたファイルでは異なります。内部インターフェイスのマッピングを表示するには、[Help] オプションをクリックします。



バイナリファイルを開いて読み込むには、**Wireshark** ソフトウェア 2.4.13 バージョン以上が必要です。

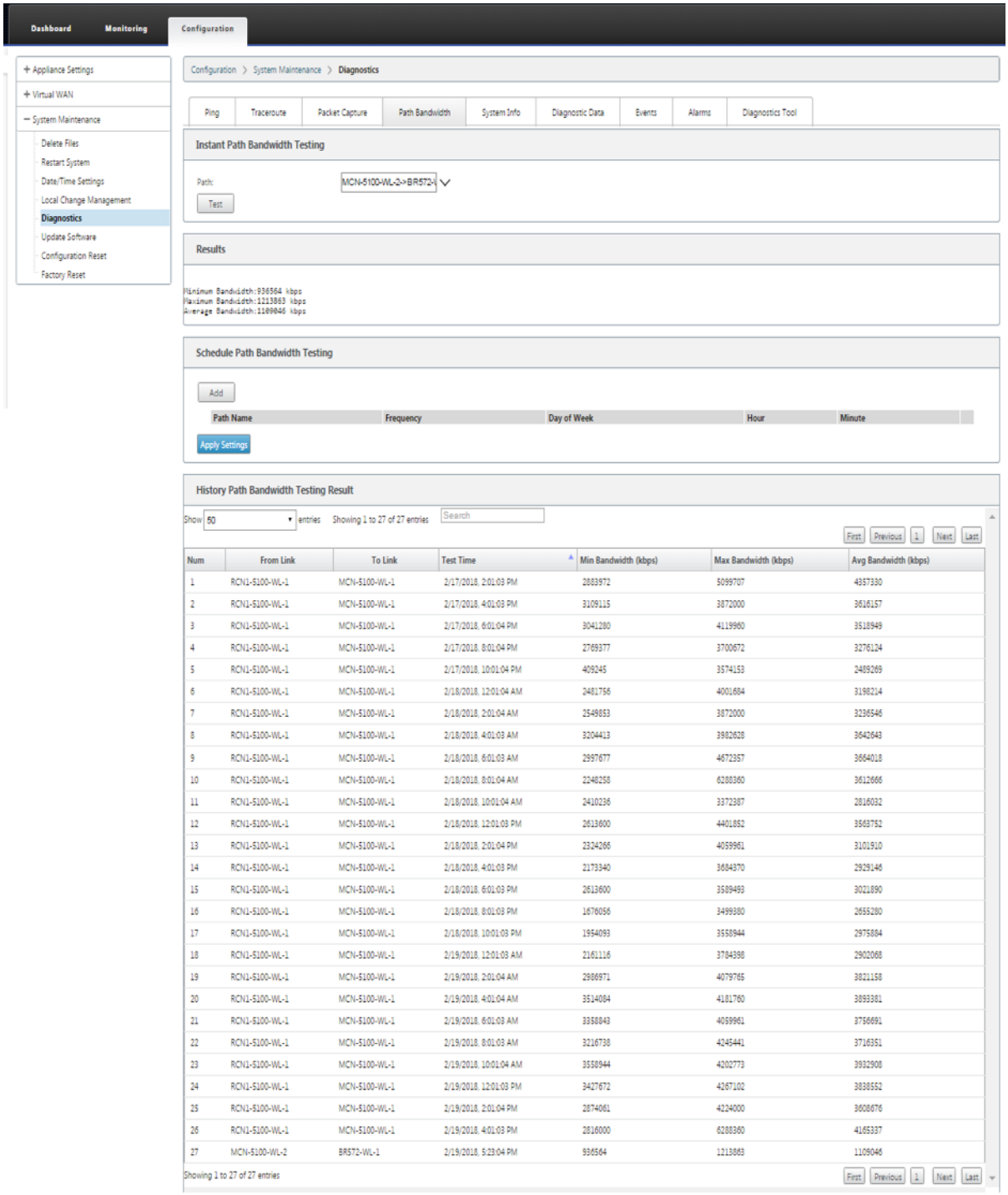


パケットビュー

パケットキャプチャファイルのサイズが大きければ、パケットビューのレンダリングプロセスを完了するのに時間がかかります。この場合、パケットビューの結果に頼るのではなく、ファイルをダウンロードして分析に **Wireshark** を使用することを推奨します。

パス帯域幅

パス帯域幅機能を使用するには、[設定] **>** [システムメンテナンス] **>** [診断] を展開し、[パス帯域幅] を選択します。



アクティブ帯域幅テストを使用すると、パブリックインターネット WAN リンクを介してインスタントパス帯域幅テストを発行したり、パブリックインターネット WAN リンク帯域幅テストを特定の時間に繰り返して完了するように

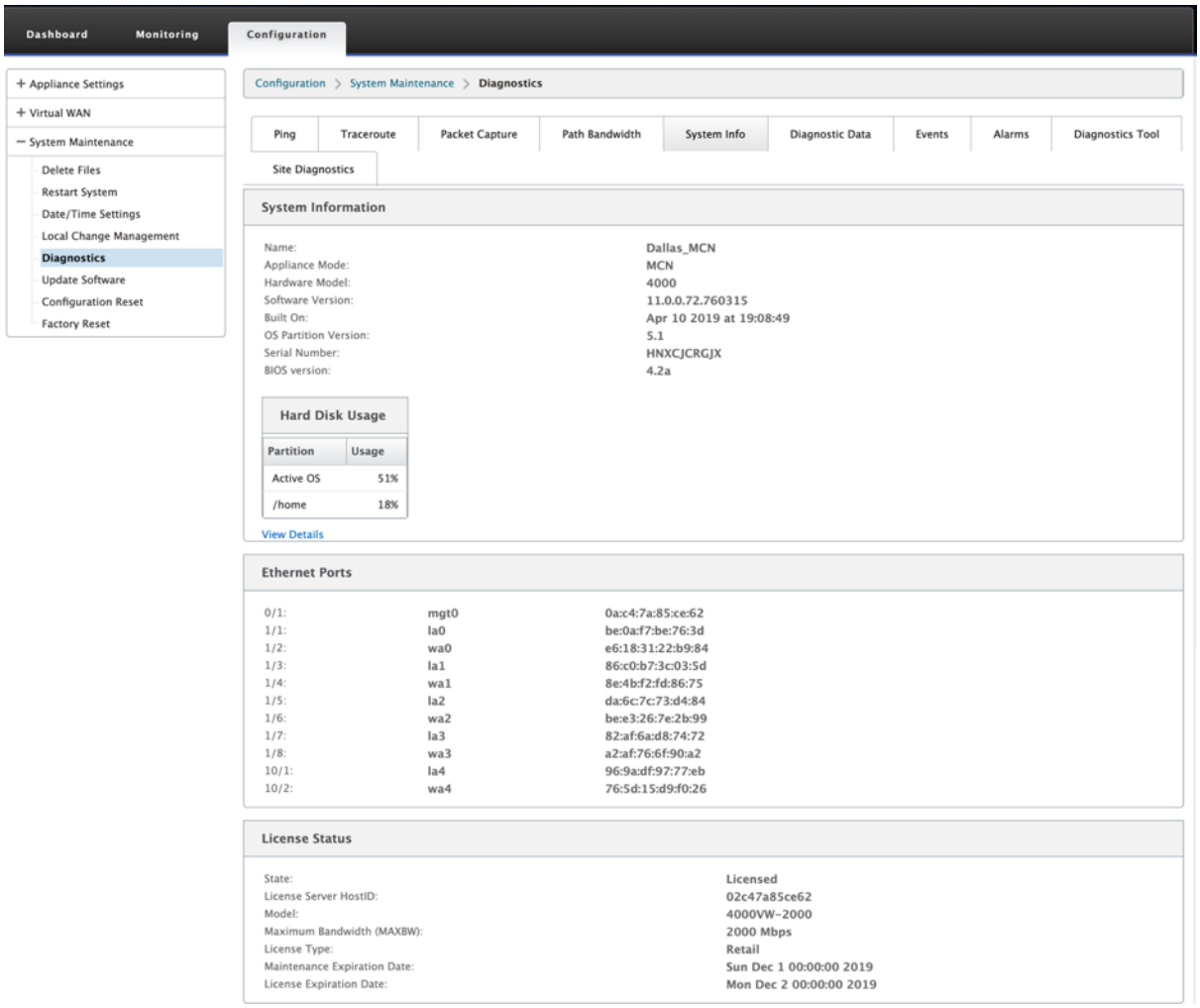
スケジュールしたりできます。

パス帯域幅機能は、新規および既存のインストール時に、2 つのロケーション間で使用可能な帯域幅の量を示すのに役立ちます。また、DSCP タグ設定や帯域幅許可レートの調整など、設定および確認の変更の結果を決定するためのパスをテストする場合にも使用できます。詳細については、アクティブ帯域幅テストを参照してください。

システム情報

[システム情報（**System Info** ）] ページには、システム情報、イーサネットポートの詳細、およびライセンスステータスが表示されます。

システム情報を表示するには、[構成**] > [**システムメンテナンス**] > [**診断**]** の順に展開し、[システム情報] を選択します。

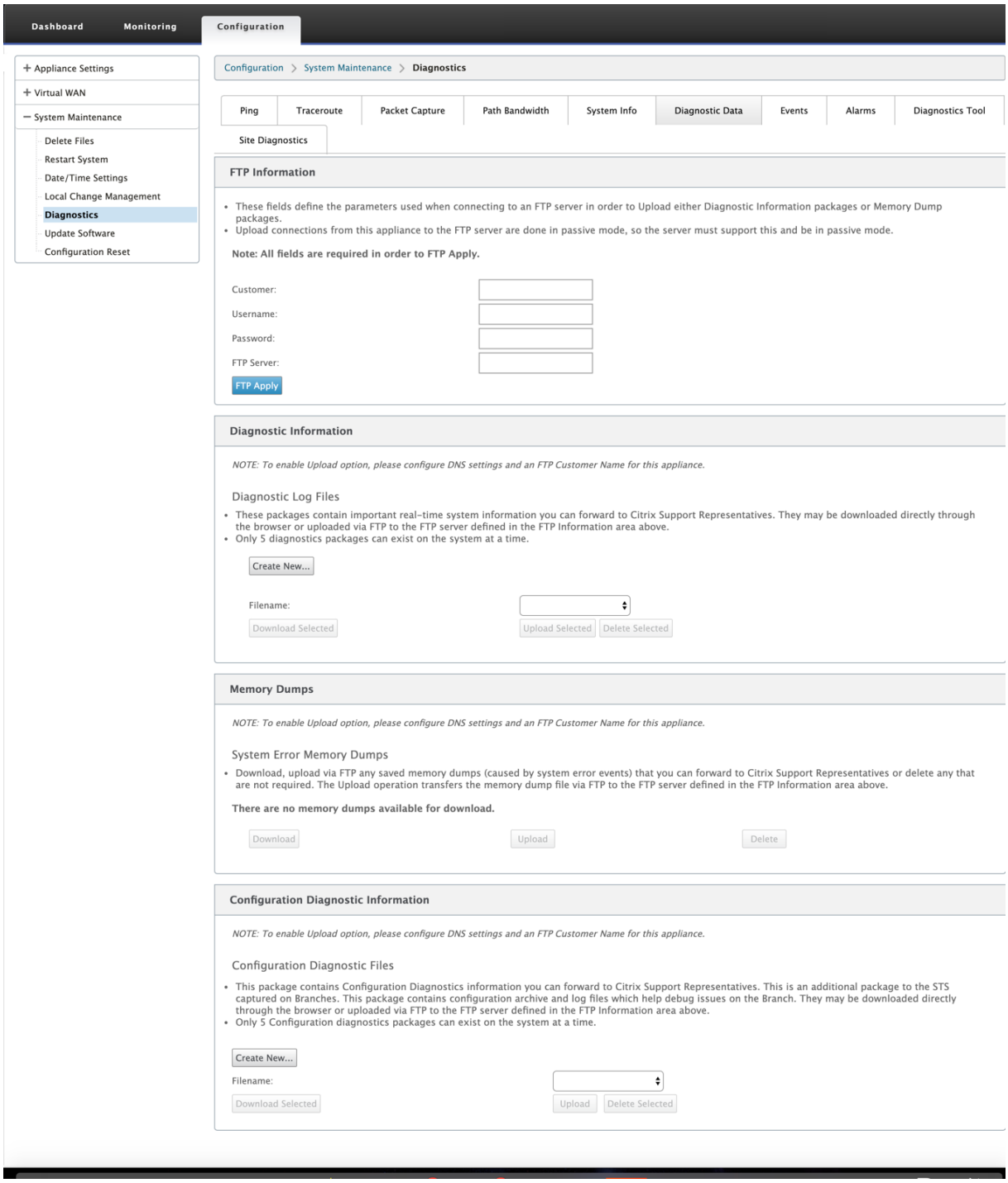


[システム情報（**System Info** ）] には、デフォルトに設定されていないすべてのパラメータが一覧表示されます。この情報は読み取り専用です。なんらかの設定ミスが疑われる場合にサポートが使用します。問題を報告すると、このページで 1 つ以上の値を確認するように求められる場合があります。

診断データ

診断データでは、Citrix サポートチームが分析する診断データパッケージを生成できます。診断ログファイルパッケージをダウンロードして、Citrix サポートチームと共有できます。

診断データを表示するには、[構成] **>** [システムメンテナンス] **>** [診断] の順に展開し、[診断データ] を選択します。



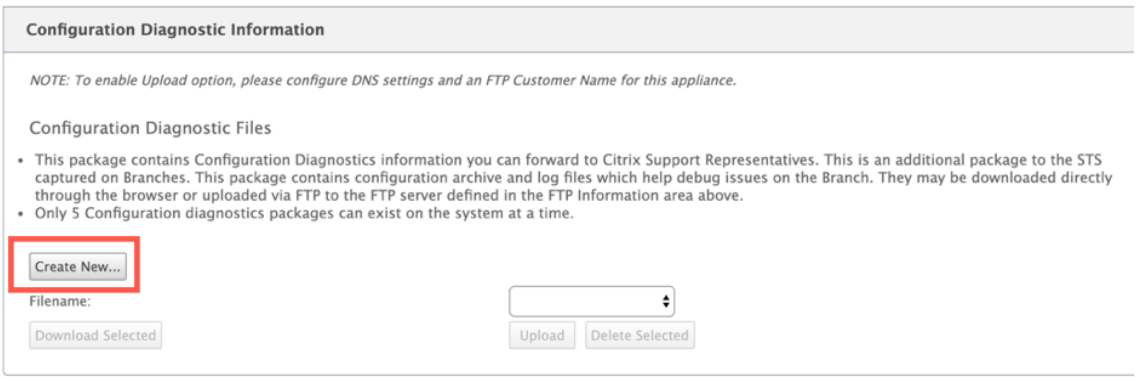
診断データには次のものが含まれます。

- 「**FTP** 情報」—FTP パラメータの詳細を入力し、「**FTP** 適用」をクリックします。診断情報パッケージをアップロードするために FTP サーバーに接続するのに必要な FTP 情報。
- 診断情報：診断ログファイルパッケージには、ブラウザからダウンロードしたり、FTP 経由で FTP サーバにアップロードしたりできるリアルタイムのシステム情報が含まれています。

  > 注:
  >
  > システムに同時に存在できる診断パッケージは 5 つだけです。

- 構成診断情報 -Citrix SD-WAN 11.0 リリースでは、ブランチ用に収集された診断情報でネットワーク構成ファイルを使用できません。サポートケースの場合は、ブランチの診断情報と、ブランチの接続先のコントロールノードからの構成診断情報を入力します。

  Control Node GUI から設定診断情報を収集するには、[構成] **>** [システムメンテナンス] **>** [診断] **>** [診断データ] > [構成診断情報] の下に移動し、[新規作成] をクリックします。

  構成診断情報の作成が完了したら、[選択したファイルのダウンロード] をクリックしてこのファイルを Citrix サポートに提供するか、同じページにある FTP 適用操作を使用してこのファイルを FTP 処理します。

- メモリダンプ—システムエラーメモリダンプファイルをダウンロードまたはアップロードして、Citrix サポートチームと共有できます。必要でない場合は、ファイルを削除することもできます。

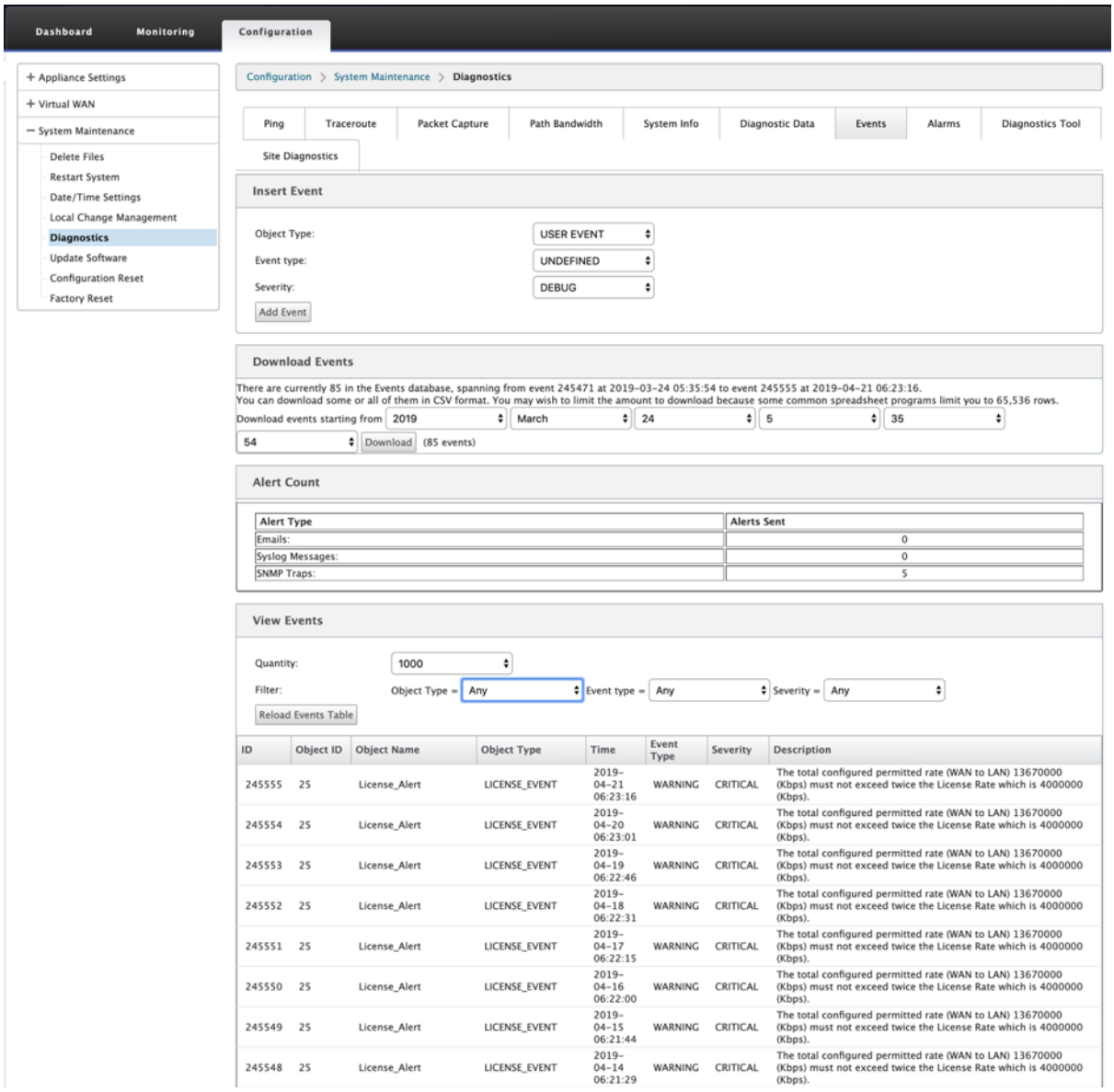
  > 注:
  >
  > デフォルトでは、[アップロード] オプションは無効モードになっています。これを有効にするには、このアプライアンスの **DNS** 設定と **FTP** カスタマー名を設定します。

イベント

イベント機能を使用して、生成されたイベントを追加、監視、および管理します。リアルタイムでイベントを特定し、問題を即座に解決し、Citrix SD-WAN アプライアンスを効果的に実行し続けるのに役立ちます。イベントは CSV 形式でダウンロードできます。

イベントを追加するには、ドロップダウンリストからオブジェクトタイプ、イベントタイプ、および重大度を選択し、[**Add Event**] をクリックします。

イベントを表示するには、[構成**] > [**システムメンテナンス**] ****[診断] の順に展開し ** 、[イベント] を選択します。



Citrix SD-WAN を構成して、さまざまなイベントタイプのイベント通知を電子メール、**SNMP** トラップ、または Syslog メッセージとして送信できます **。

電子メール、SNMP、および syslog 通知の設定が完了したら、さまざまなイベントタイプの重大度を選択し、イベント通知を送信するモード（電子メール、SNMP、syslog）を選択できます。

通知は、イベントタイプに指定された重大度レベル以上のイベントに対して生成されます。

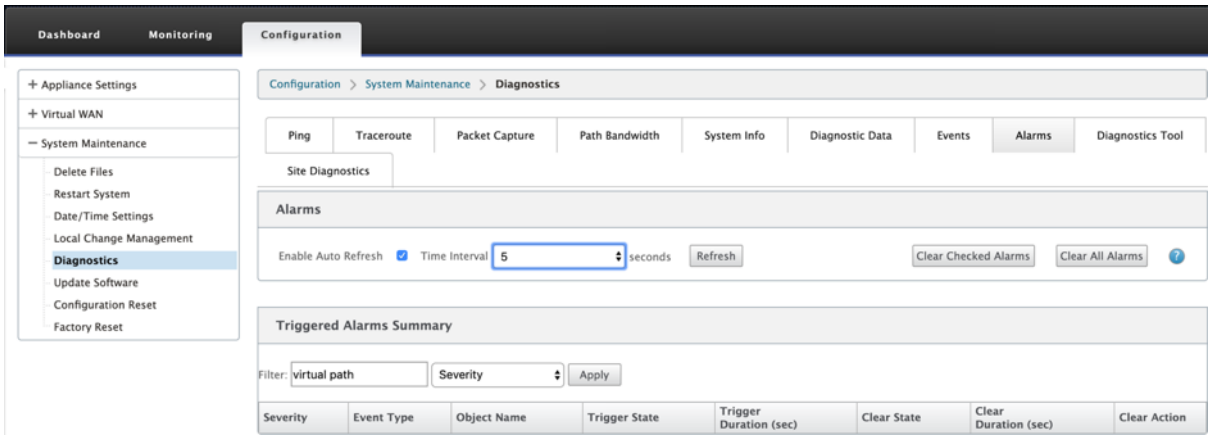
イベントの詳細は、[View **Events]** テーブルで確認できます。イベントの詳細には、次の情報が含まれます。

- **ID** —イベント ID。

- オブジェクト **ID** -イベントを生成するオブジェクトの ID。
- オブジェクト名 -イベントを生成するオブジェクトの名前。
- オブジェクトタイプ—イベントを生成するオブジェクトのタイプ。
- **Time** —イベントが生成された時刻。
- **Event Type** —イベント発生時のオブジェクトの状態。
- 重大度—イベントの重大度レベル。
- 説明—イベントの説明文です。

alarms

トリガーされたアラームを表示およびクリアできます。アラームを表示するには、[構成] に移動し、**[**システムメンテナンス**] > [**診断**]** を展開し、[アラーム] を選択します。



クリアするアラームを選択し、[チェック済みアラームのクリア（**Clear Alarms**）**]** をクリックするか、**[**すべてのアラームをクリア（**Clear All Alarms** ）] をクリックしてすべてのアラームをクリアします。

トリガーされたすべてのアラームの次のサマリーを表示できます。

- 重大度：重大度は、アラームがトリガーまたはクリアされたときに送信されるアラート、およびトリガーされたアラームの概要に表示されます。
- **Event Type** ： SD-WAN アプライアンスは、ネットワーク内の特定のサブシステムまたはオブジェクトに対してアラームをトリガーできます。これらのアラームは、イベントタイプと呼ばれます。
- **[**オブジェクト名] —イベントを生成するオブジェクトの名前。
- [**Trigger State**]：イベントタイプのアラームをトリガーするイベント状態。
- トリガー期間 **(**秒**)** —秒単位の期間によって、アプライアンスがアラームをトリガーする速度が決まります。
- [**Clear** State]：アラームがトリガーされた後にイベントタイプのアラームをクリアするイベント状態。
- [**Clear Duration (sec)**]：アラームをクリアするまでの待機時間を秒単位で指定します。
- [**Clear Action**]：アラームのクリア中に実行されるアクション。

診断ツール

診断ツールは、テストトラフィックを生成するために使用します。これにより、次のような結果になる可能性のあるネットワーク上の問題をトラブルシューティングできます。

- パス状態が良好から不良に頻繁に変化する。
- アプリケーションのパフォーマンスが低下します。
- パケット損失の増加

ほとんどの場合、これらの問題は、ファイアウォールとルータで設定されたレート制限、誤った帯域幅設定、低いリンク速度、ネットワークプロバイダーによって設定されたプライオリティキューなどが原因で発生します。診断ツールを使用すると、このような問題の根本原因を特定し、トラブルシューティングを行うことができます。

診断ツールは、データセンターおよびブランチホストに手動でインストールする必要がある iPerf などのサードパーティ製ツールへの依存性を排除します。これにより、送信される診断トラフィックのタイプ、診断トラフィックが流れる方向、および診断トラフィックが流れるパスをより詳細に制御できます。

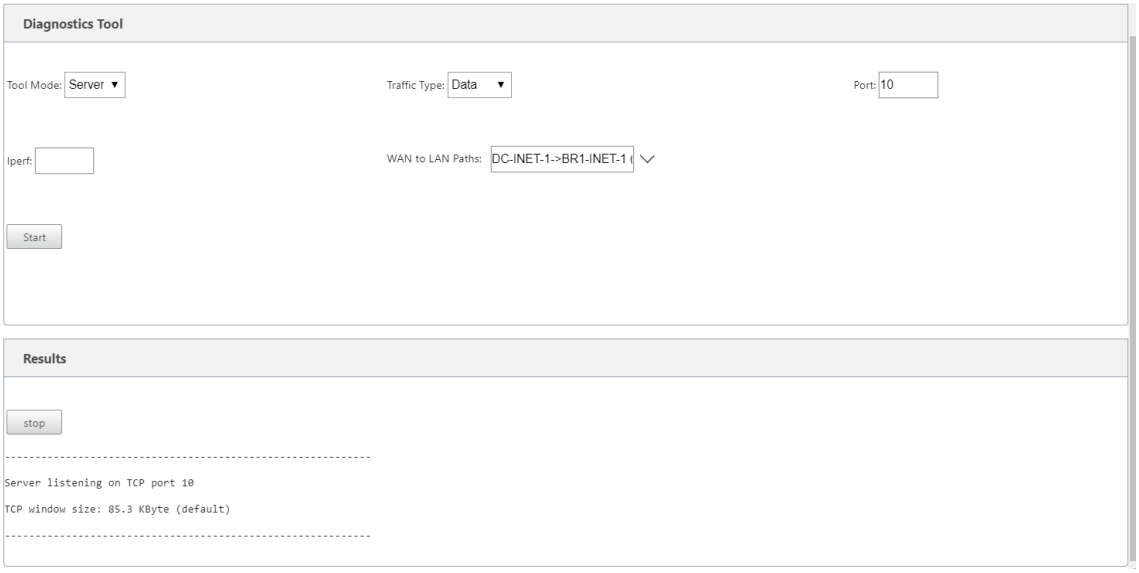
診断ツールでは、次の 2 種類のトラフィックを生成できます。

- 制御：パケットに QoS/スケジューリングが適用されていないトラフィックを生成します。その結果、そのパスが最適でない場合でも、UI で選択したパスでパケットが送信されます。このトラフィックは、特定のパスをテストするために使用され、ISP 関連の問題の特定に役立ちます。これを使用して、選択したパスの帯域幅を決定することもできます。
- データ:SD-WAN トラフィック処理でホストから生成されたトラフィックをシミュレートします。QoS/Scheduling がパケットに適用されるため、パケットは利用可能な最良のパスで送信されます。負荷分散が有効の場合、トラフィックは複数のパスで送信されます。このトラフィックは、QoS /スケジューラ関連の問題のトラブルシューティングに使用されます。

> 注
>
> パスで診断テストを実行するには、パスの両端でアプライアンスでテストを開始する必要があります。診断テストは、一方のアプライアンスのサーバとして、もう一方のアプライアンスのクライアントとして開始します。

診断ツールを使用するには、次の手順に従います。

1. 両方のアプライアンスで、構成 > システムメンテナンス > 診断 > 診断ツールをクリックします。

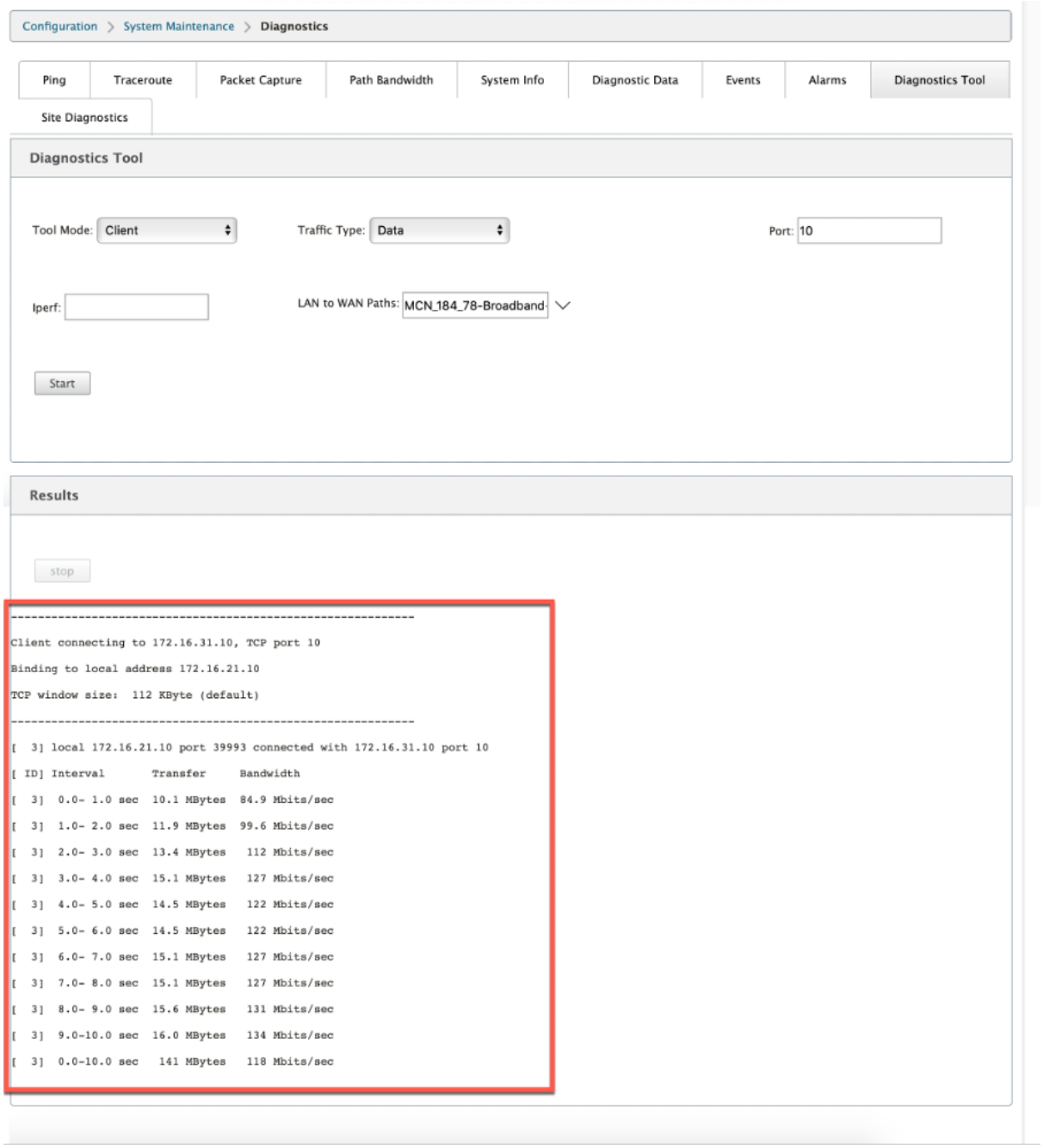


2. 「ツールモード」フィールドで、「アプライアンス上のサーバ」を選択し、選択したパスのリモートエンドに存在するアプライアンスで「クライアント」を選択します。
3. [トラフィックタイプ（Traffic Type）] フィールドで、診断トラフィックの種類（[制御] または [データ]）を選択します。両方のアプライアンスで同じトラフィックタイプを選択します。
4. [ポート（**Port**）**]** フィールドで、診断トラフィックを送信する **TCP/UDP** ポート番号を指定します。両方のアプライアンスで同じポート番号を指定します。
5. [**Iperf**] フィールドに、IPERF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

   > 注
   >
   > 次の IPERF コマンドラインオプションを指定する必要はありません。
   >
   > - -c: 診断ツールによってクライアントモードオプションが追加されます。
   > - -s：診断ツールによってサーバ・モード・オプションが追加されます。
   > - -B: IPERF を特定の IP/インターフェイスにバインドするには、選択したパスに応じて診断ツールを実行します。
   > - -p：ポート番号は診断ツールで提供されます。
   > - -i: 出力間隔 (秒)。
   > - -t: テストの合計時間 (秒)。

6. 診断トラフィックを送信する WAN から LAN へのパスを選択します。両方のアプライアンスで同じパスを選択します。
7. 両方のアプライアンスで [**Start**] をクリックします。

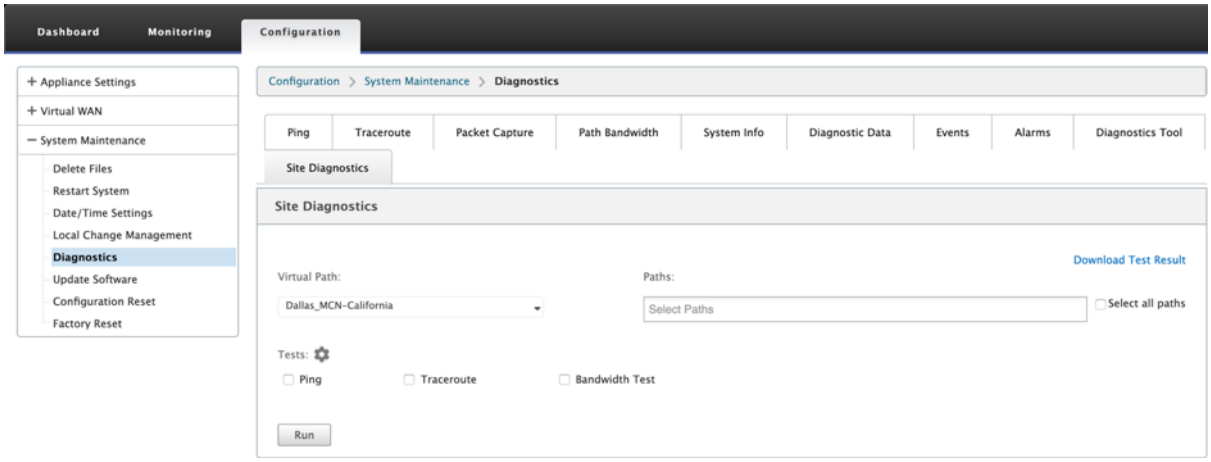
結果には、選択したアプライアンスのモード（クライアントまたはサーバー）と、テストが実行された TCP または UDP ポートが表示されます。テストの合計期間に達するまで、指定された間隔で転送されたデータおよび使用された帯域幅が定期的に表示されます。



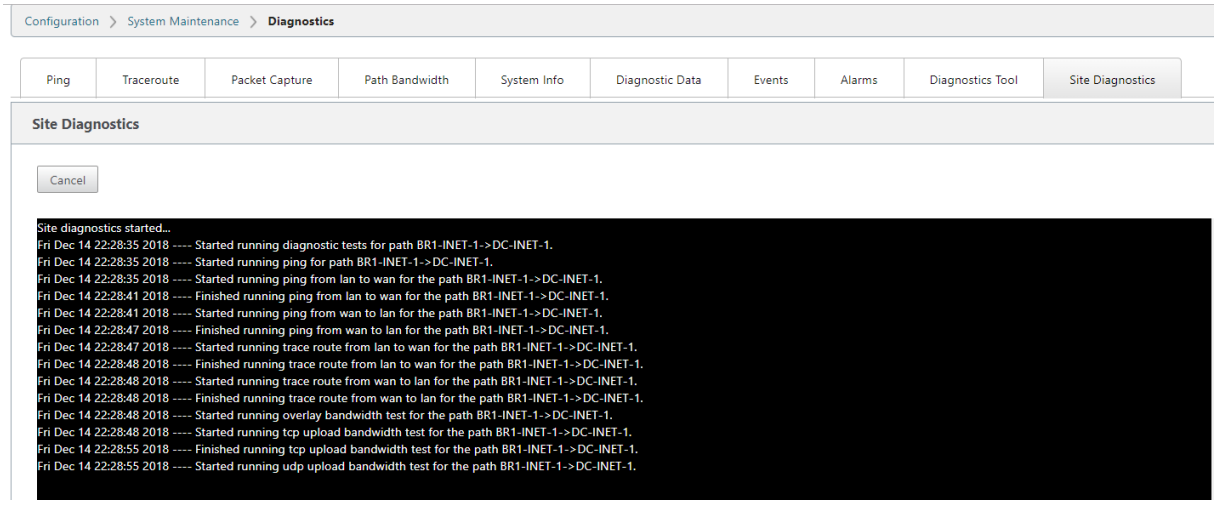
サイト診断

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

サイト診断を使用するには、[構成] **> [**システムメンテナンス**] ****[診断 **] を展開し、[診断ツール] を選択します。



- [**Interface Status**]: インターフェイスの名前、インターフェイスに関連付けられているファイアウォールゾーンの数、VLAN ID、および関連付けられているポートが表示されます。
- **[パスステータス]:** ターゲットプライベート IP、ゲートウェイ IP、ターゲットパブリック IP、パートナー IP、パートナーパブリック IP アドレスの詳細が表示されます。また、ゲートウェイ ARP とパス MTU のステータスも表示されます。
- **Ping Result: ping** の方向、ステータス、回数 (試行回数と失敗回数を含む)、および RTT が表示されます。
- **traceroute Result**: ホップの方向、ステータス、ホップ数、IP アドレスまたは RTT が表示されます。
- 帯域幅の結果:TCP と UDP のステータスと、オーバーレイおよびアンダーレイネットワークに使用されている帯域幅 (kbps 単位) が表示されます。UDP は帯域幅ベースであり、設定された帯域幅のみを使用するため、UDP と比較して TCP で使用される帯域幅は大きくなります。TCP はランプアッププロトコルです。基盤となるネットワーク構成によっては、使用状況によって、設定された帯域幅よりも高い帯域幅が報告される場合があります。



管理 IP のトラブルシューティング

May 10, 2021

DHCP IP アドレスを構成するときに発生する可能性のあるシナリオを次に示します。また、SD-WAN アプライアンスの展開時に DHCP 管理 IP アドレスを構成するためのベストプラクティスと推奨事項についても説明します。

これらの推奨事項は、SD-WAN のすべてのプラットフォームモデル（Standard Edition、WANOP、Premium（Enterprise）Edition（物理アプライアンスと仮想アプライアンス）に適用されます。

> 注
>
> SD-WAN アプライアンスのすべてのハードウェアモデルには、工場出荷時のデフォルトの管理 IP アドレスが付属しています。セットアッププロセス中に、アプライアンスに必要な DHCP IP アドレスを設定してください。
>
> SD-WAN アプライアンス（VPX モデル）および AWS 環境にデプロイできるアプライアンスのすべての仮想モデルには、工場出荷時のデフォルト IP アドレスが割り当てられていません。

DHCP サーバに到達できない状態でアプライアンスの電源を入れます。

- 原因:
  - イーサネット管理ケーブルが切断されている
  - 接続されているネットワークの DHCP サービスがダウンしています。
- 正常な動作
  - DHCP サービスを有効にしたアプライアンスは、300 秒ごとに DHCP 要求を再試行します（デフォルト値）。実際の間隔は約 7 分です
  - したがって、DHCP サービスを有効にしたアプライアンスは、DHCP サーバーが使用可能になってから 7 分以内に DHCP アドレスを取得します。遅延の範囲は 0 ～7 分

割り当てられた **DHCP** アドレスの有効期限が切れます。

- 予想される動作:
  - DHCP サービスを有効にしたアプライアンスは、アドレスの有効期限が切れる前にリースの更新を試みます
  - アプライアンスは新しい DHCP 検出で開始します（更新に失敗した場合）

DHCP サービスが有効になっているアプライアンスは、**DHCP** が有効なサブネットから別のサブネットに移動します。

- 原因: アプライアンスが割り当てられた DHCP サブネットから別の DHCP サブネットに移動する
- 予想される動作:
  - 永続的なリースの DHCP IP アドレスの割り当てでは、新しい DHCP サーバから IP アドレスを取得するために、アプライアンスの再起動が必要になる場合があります。

- DHCP リースの有効期限が切れると、現在の DHCP サーバーに到達できない場合、アプライアンスが DHCP 検出プロトコルを再開することがあります。
- アプライアンスは、8 分の遅延で新しい IP アドレスを取得します。Gateway IP アドレスは、GUI および CLI では変更されません。再起動プロセスが完了した後に更新されます。

推奨:

- Citrix SD-WAN アプライアンス（物理/仮想）に割り当てられた DHCP アドレスには、常に永続的なリースを割り当てます。これにより、アプライアンスは予測可能な管理 IP アドレスを持つことができます。

セッションベースの **HTTP** 通知

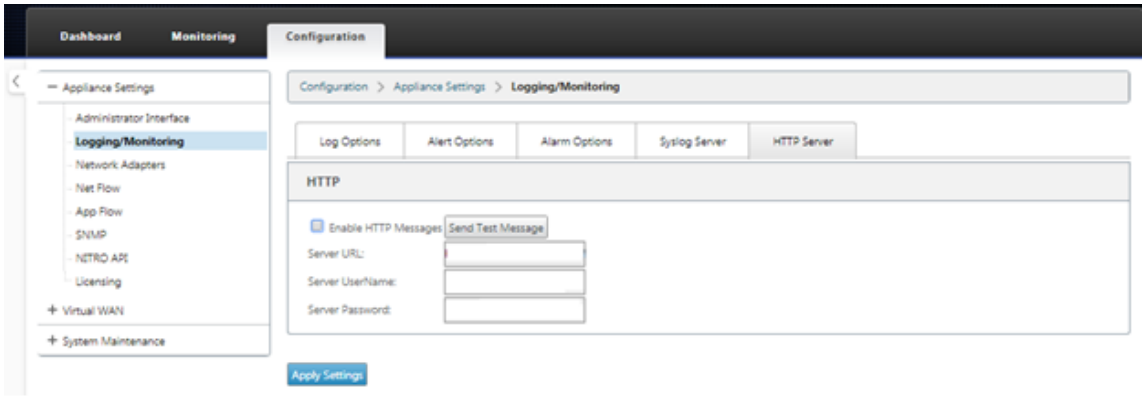
May 10, 2021

Citrix SD-WAN アプライアンスの GUI で、汎用 HTTP POST API サービス要求のイベントレポートとアラームレポートを構成できるようになりました。HTTP アラームおよびイベント通知の設定は、SD-WAN でサポートされるイベントおよびアラームの電子メールイベントおよび SNMP イベントに似ています。

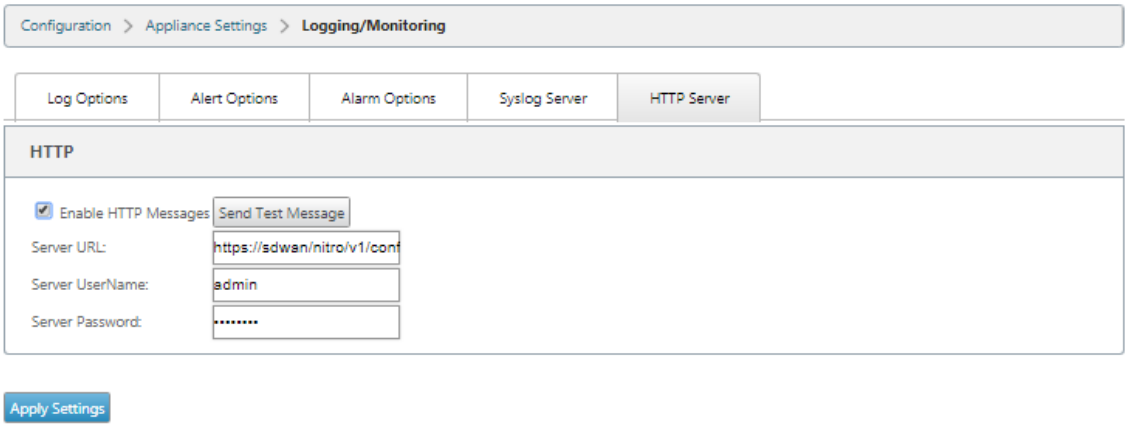
セッションベースの HTTP ポスト通知は、[Service Now] などの外部サービスに送信されます。HTTP サーバーのイベント通知は、Citrix SD-WAN アプライアンス GUI および Citrix SD-WAN Center で構成できます。

Citrix SD-WAN アプライアンス GUI で HTTP POST 通知を構成するには、以下の手順に従ってください。

1. [構成] > [ログ作成/監視] > [**HTTP** サーバー] に移動します。



2. [**HTTP** メッセージを有効にする] をクリックします。
3. 通知を受信する HTTP サーバのサーバ **URL** を入力します。サーバのユーザ名とサーバのパスワードを入力します。

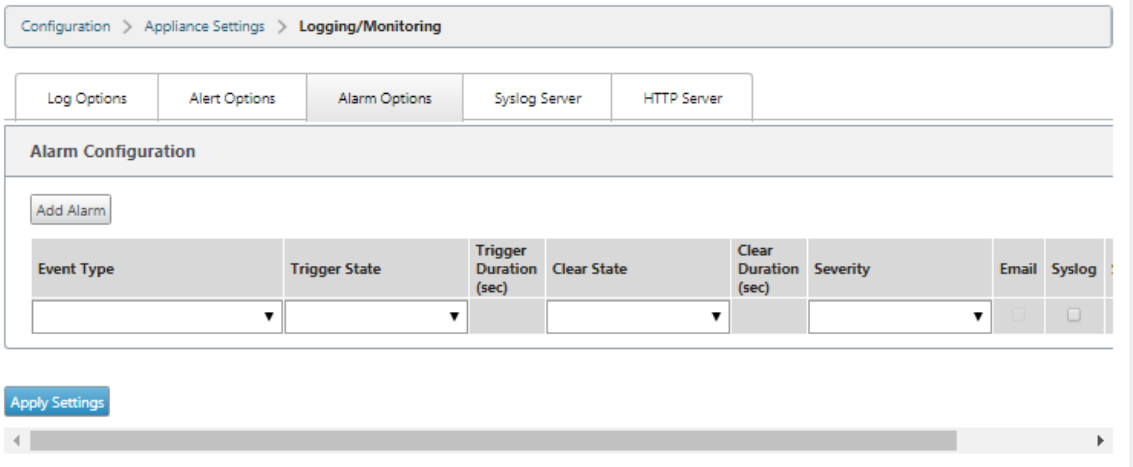


4. [設定の適用] をクリックします。HTTP サーバー通知設定が適用されると、ページが更新されます。

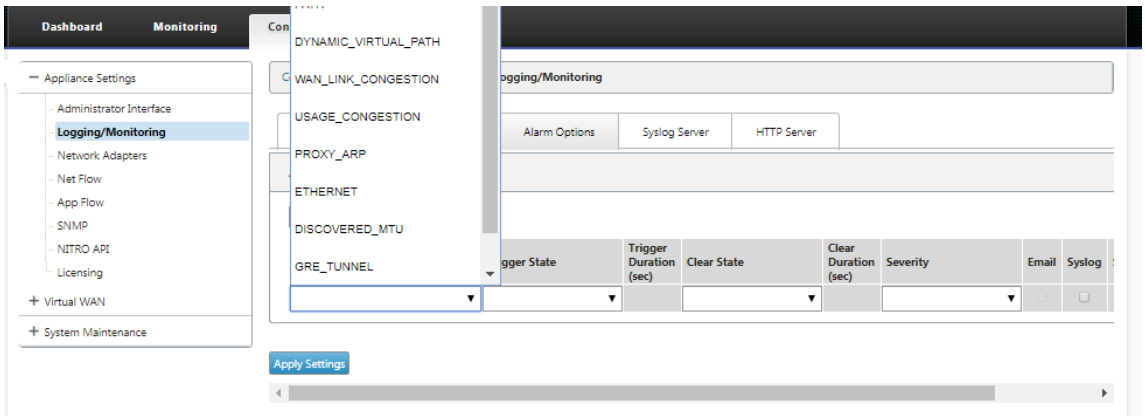
> 注
>
> [テストメッセージの送信] オプションを使用して、HTTP サーバー接続が成功したことを確認します。

HTTP サーバセッションにアラーム通知を追加するには、次の手順を実行します。

1. [ロギング/モニタリング] ページで、[アラームオプション] タブページに移動します。
2. [アラームの追加] をクリックします。

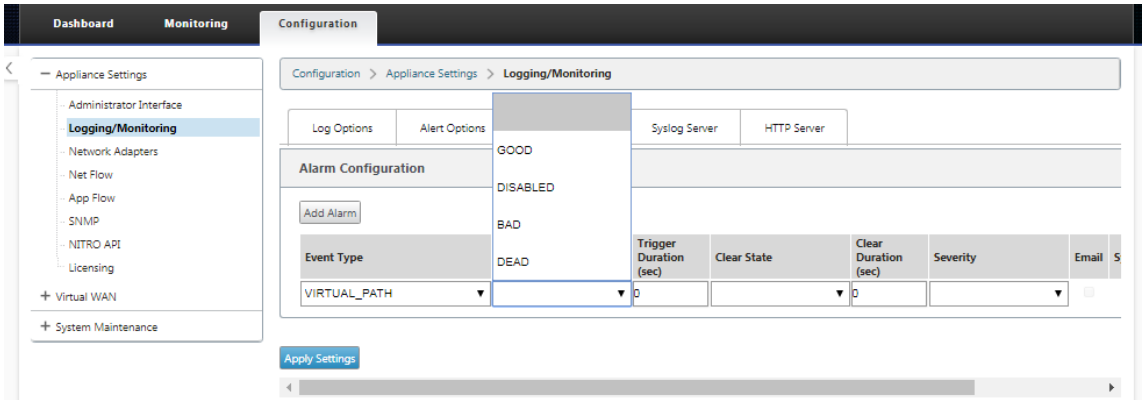


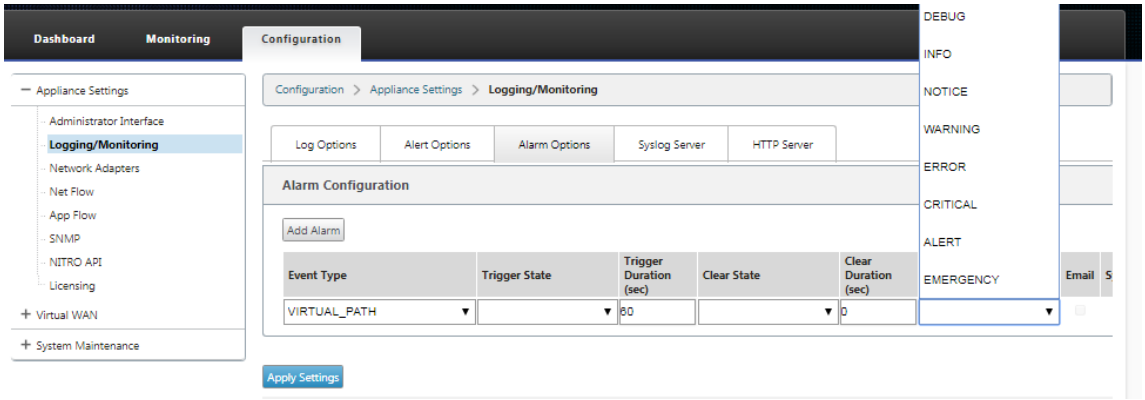
3. ドロップダウンリストから [イベントタイプ] を選択します。



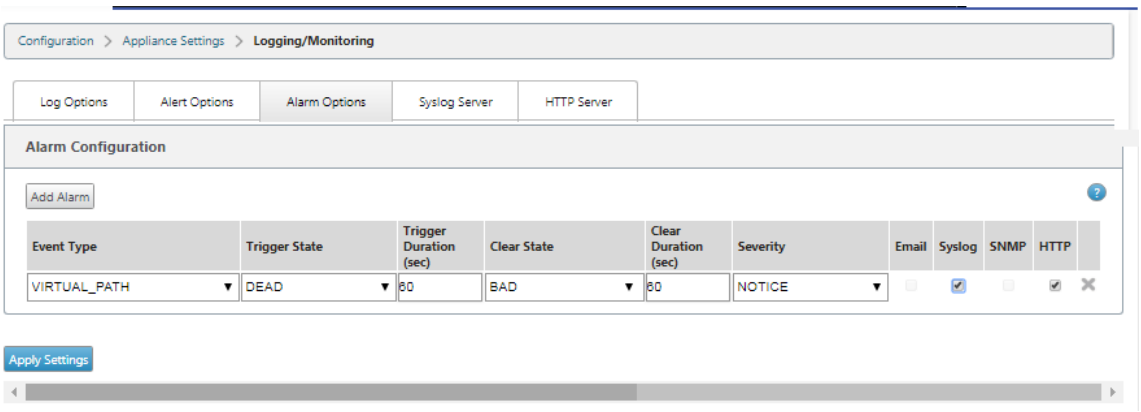
4. 選択した イベントタイプについて、次のアラーム通知状態を選択します。トリガー状態とクリア状態は、選択したイベントタイプに応じて変化します。

   - トリガー状態–GOOD, DISABLED, BAD, DEAD
   - トリガー時間—秒単位の時間
   - クリア状態 - GOOD, DISABLED, BAD, DEAD
   - クリア期間—秒単位の時間
   - 重大度—デバッグ、情報、通知、警告、エラー、重大、イベント、緊急





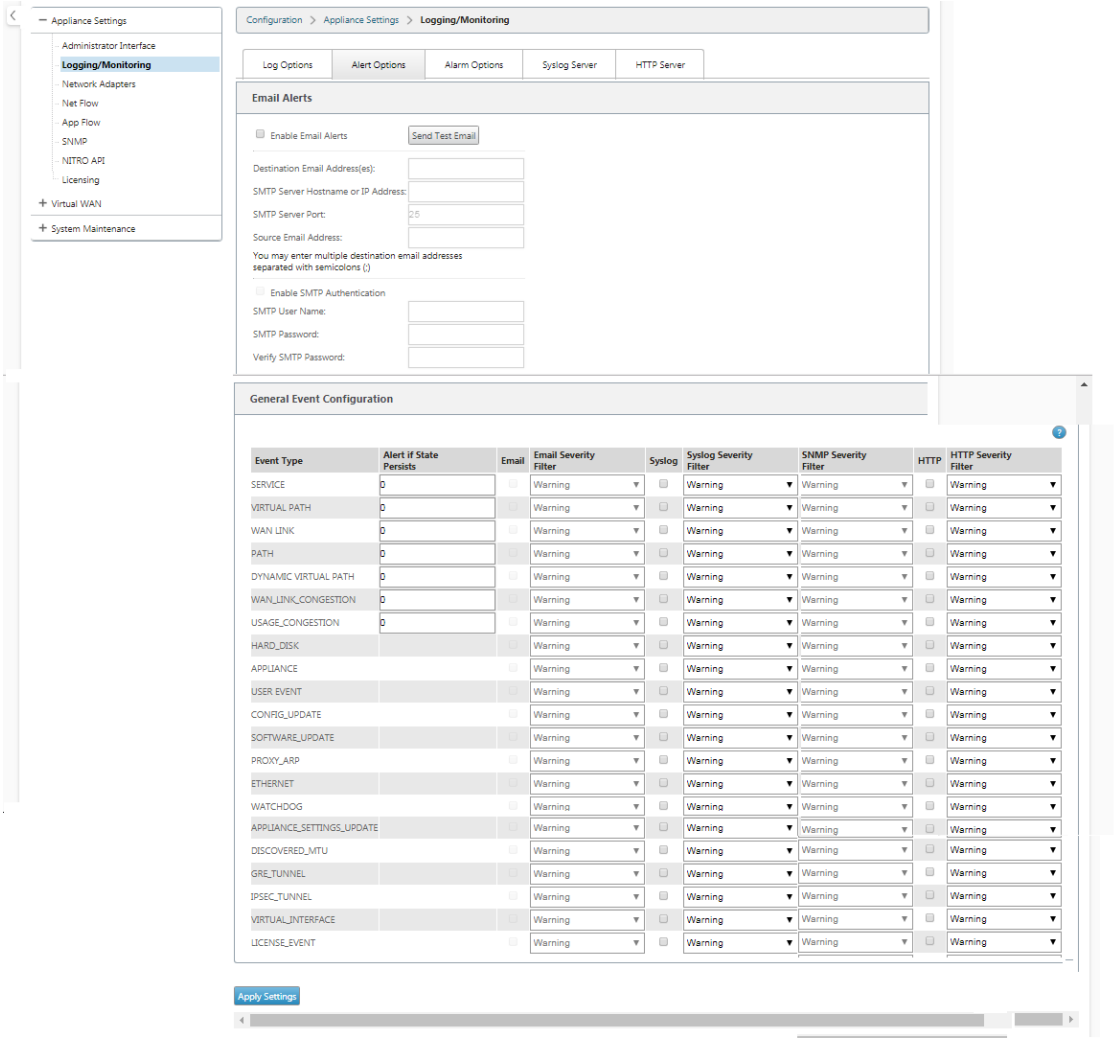
5. **Syslog** および **HTTP** サーバイベントに固有の通知を受信するには、[Syslog] および [HTTP] チェックボックスをオンにします。[設定の適用] をクリックします。



イベント・オプションを構成するには、次の手順に従います。

[アラートオプション] タブ・ページに移動します。[一般的なイベント構成] ページで、イベントタイプ の HTTP サーバー通知フィルタを選択し、[設定の適用] をクリックします。

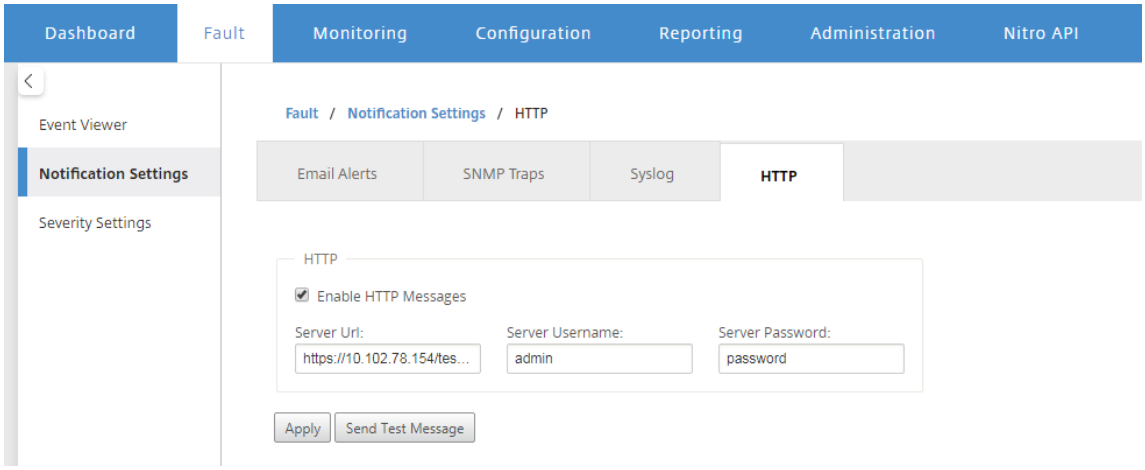
- HTTP
- HTTP 重大度フィルタ



Citrix SD-WAN Center で HTTP 通知を構成する

HTTP 通知を構成するには、次の手順を実行します。

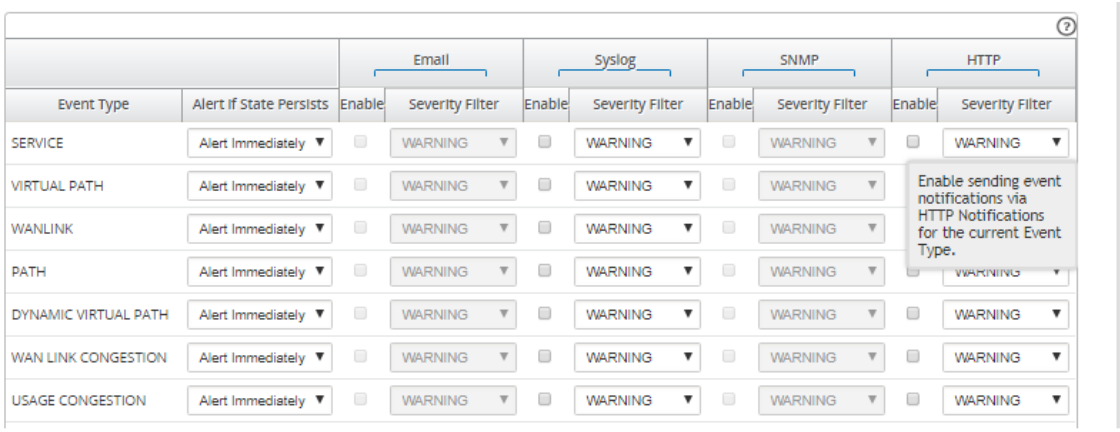
1. [障害] > [通知設定] > [**HTTP**] に移動します。



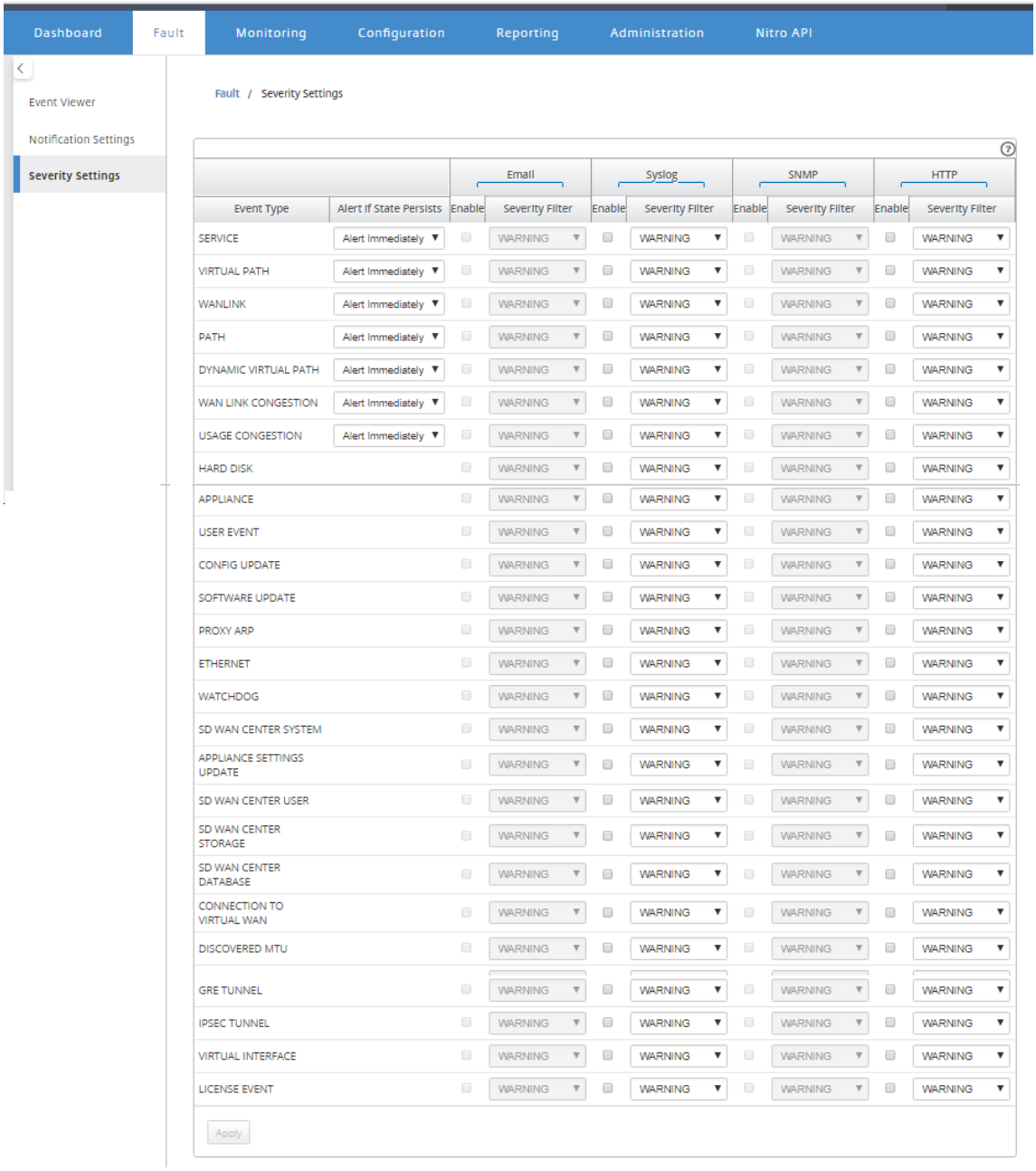
2. HTTP サーバの サーバ **URL**、サーバユーザ名、サーバパスワード を入力します。
3. [適用] をクリックします。

重大度設定を構成するには、次の手順に従います。

1. 重大度の設定 ページに移動します。[**Enable**] をクリックして、選択したイベントタイプの HTTP 通知の監視を開始します。



2. 次のイベントタイプについて、電子メール、Syslog、SNMP、および HTTP イベント通知を監視するように選択できます。[適用] をクリックします。



アクティブ帯域幅テスト

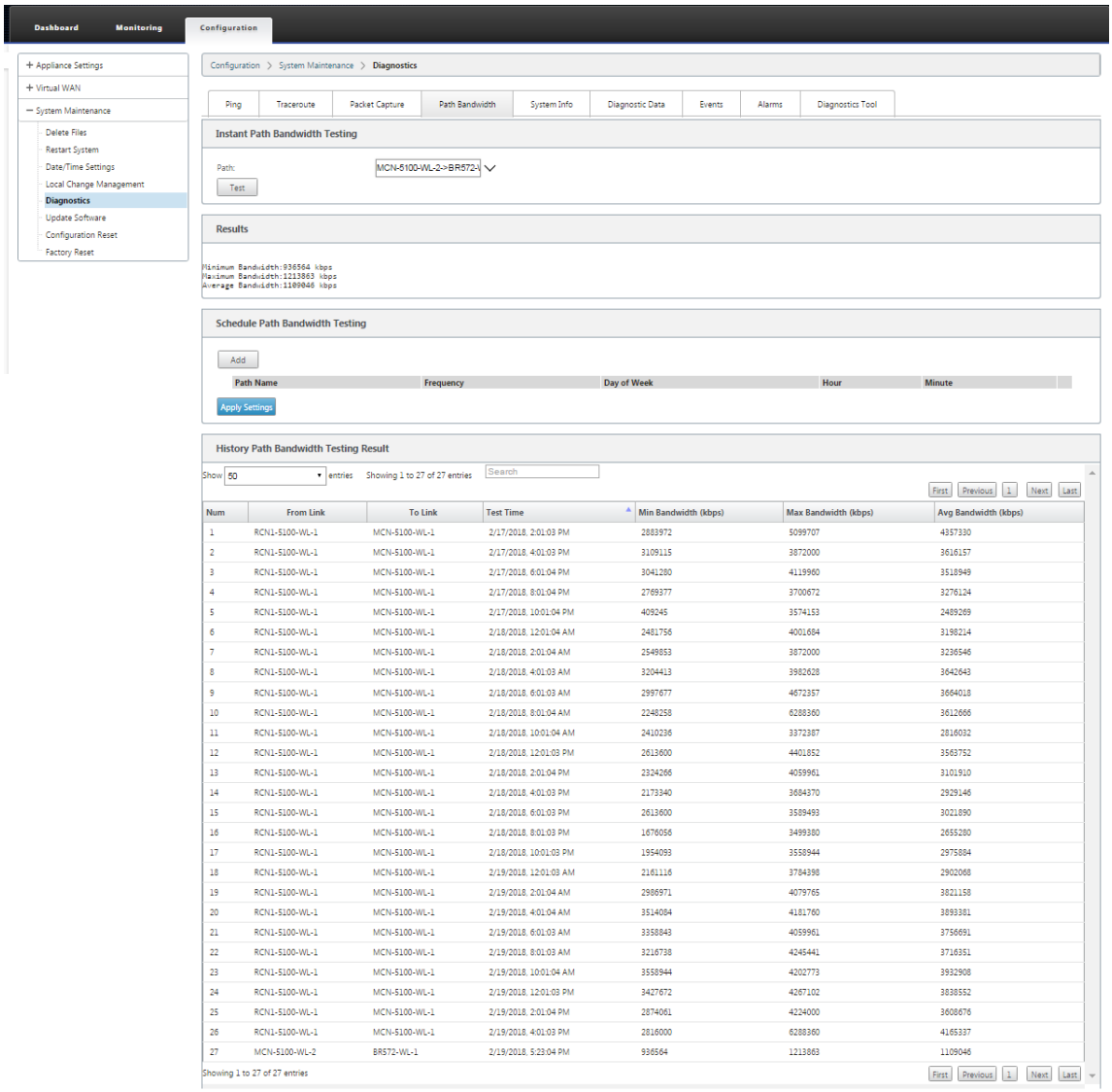
May 10, 2021

アクティブ帯域幅テストを使用すると、パブリックインターネット WAN リンクを介してインスタントパス帯域幅テストを発行したり、パブリックインターネット WAN リンク帯域幅テストを特定の時間に繰り返して完了するようにスケジュールしたりできます。この機能は、新規および既存のインストール中に 2 つのロケーション間で利用可能な

帯域幅の量を示す場合に便利です。また、DSCP タグ設定や帯域幅許可レートの調整など、設定および確認の変更の結果を判断するためのパスをテストする場合にも役立ちます。

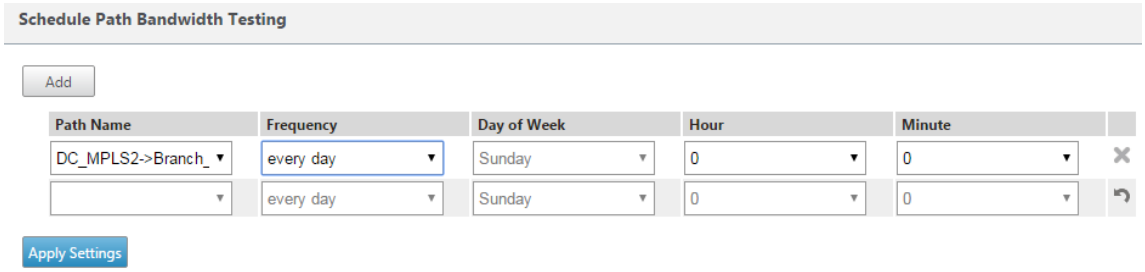
アクティブ帯域幅テスト機能を使用するには、次の手順を実行します。

1. [システムメンテナンス] > [診断] > [パス帯域幅] に移動します。
2. 目的の パスを 選択し、[テスト] をクリックします。



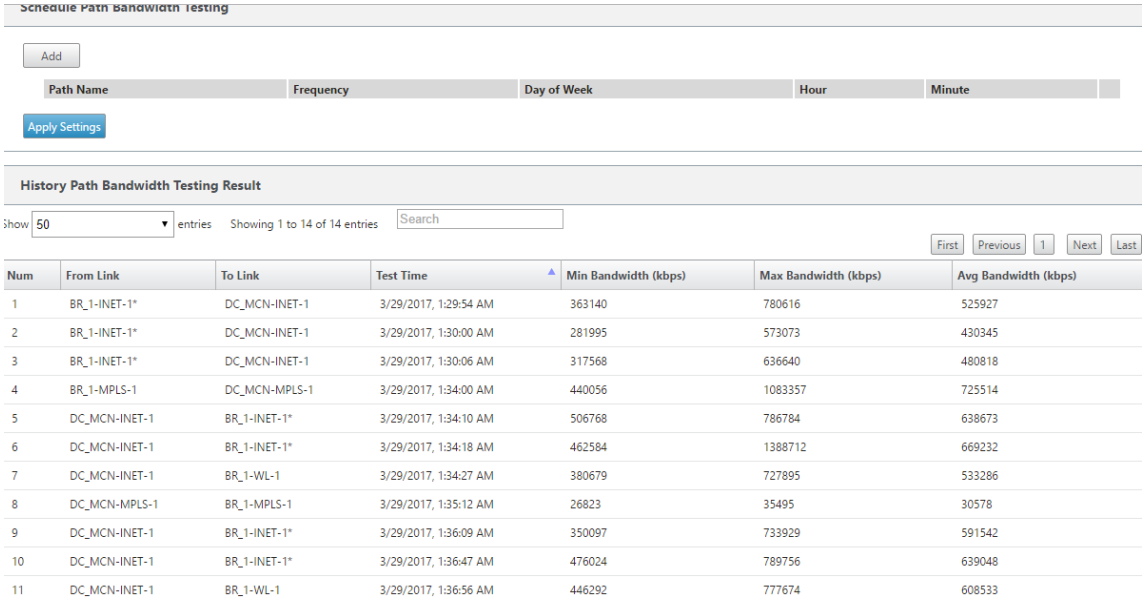
出力には、テストの WAN リンクの最小帯域幅および最大帯域幅結果の許可レートとして設定する値として使用された平均帯域幅が表示されます。帯域幅をテストする機能に加えて、学習した帯域幅を使用するように構成ファイルを変更できるようになりました。これは、[サイト] > [**WAN** リンク] [サイト名] > [WAN リンク名] [設定] の下にある [自動学習] オプションによって実現されます。有効にすると、システムは学習した帯域幅を使用します。

また、毎週、毎日、または毎時間の間隔で、パス帯域幅の繰り返しテストをスケジュールすることもできます。



注

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



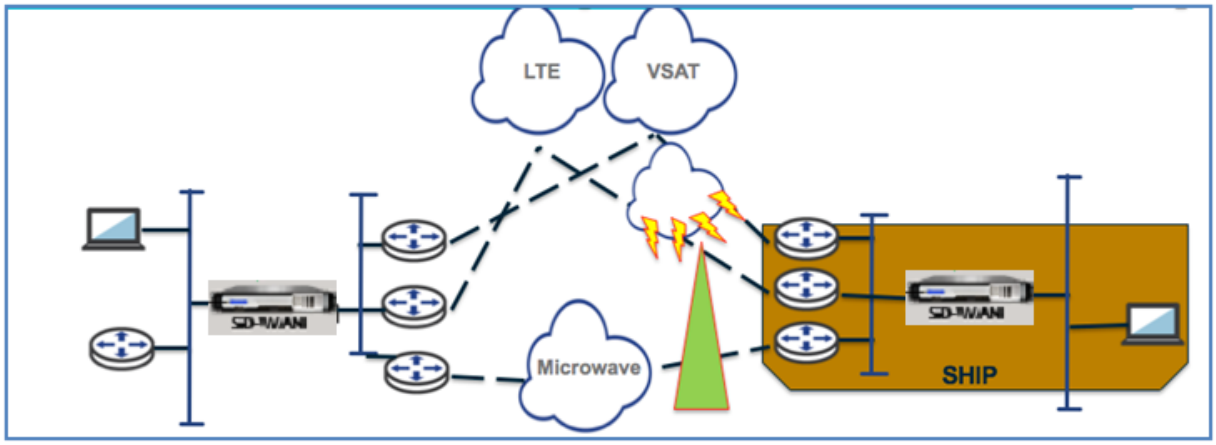
Num	From Link	To Link	Test Time	Min Bandwidth (kbps)	Max Bandwidth (kbps)	Avg Bandwidth (kbps)
1	BR_1-INET-1*	DC_MCN-INET-1	3/29/2017, 1:29:54 AM	363140	780616	525927
2	BR_1-INET-1*	DC_MCN-INET-1	3/29/2017, 1:30:00 AM	281995	573073	430345
3	BR_1-INET-1*	DC_MCN-INET-1	3/29/2017, 1:30:06 AM	317568	636640	480818
4	BR_1-MPLS-1	DC_MCN-MPLS-1	3/29/2017, 1:34:00 AM	440056	1083357	725514
5	DC_MCN-INET-1	BR_1-INET-1*	3/29/2017, 1:34:10 AM	506768	786784	638673
6	DC_MCN-INET-1	BR_1-INET-1*	3/29/2017, 1:34:18 AM	462584	1388712	669232
7	DC_MCN-INET-1	BR_1-WL-1	3/29/2017, 1:34:27 AM	380679	727895	533286
8	DC_MCN-MPLS-1	BR_1-MPLS-1	3/29/2017, 1:35:12 AM	26823	35495	30578
9	DC_MCN-INET-1	BR_1-INET-1*	3/29/2017, 1:36:09 AM	350097	733929	591542
10	DC_MCN-INET-1	BR_1-INET-1*	3/29/2017, 1:36:47 AM	476024	789756	639048
11	DC_MCN-INET-1	BR_1-WL-1	3/29/2017, 1:36:56 AM	446292	777674	608533

適応型帯域幅検出

May 10, 2021

この機能は、VSAT、LOS、マイクロ波、3G/4G/LTE WAN リンクを持つネットワークに適用できます。使用可能な帯域幅は、気象と大気の条件、場所、およびサイトの障害物によって異なります。これにより、SD-WAN アプライアンスは、定義された帯域幅範囲（最小および最大 WAN リンクレート）に基づいて WAN リンクの帯域幅レートを動的に調整し、パスに BAD マークを付けずに、使用可能な帯域幅の最大量を使用できます。

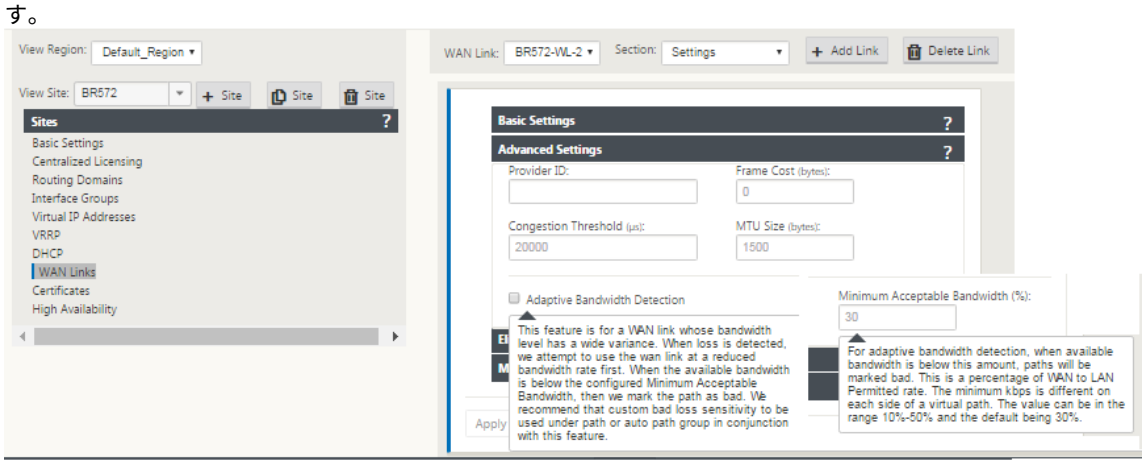
- 帯域幅の信頼性（VSAT 以上、マイクロ波、3G/4G、LTE 以上）
- ユーザーが構成した設定よりも適応型帯域幅の予測性が向上



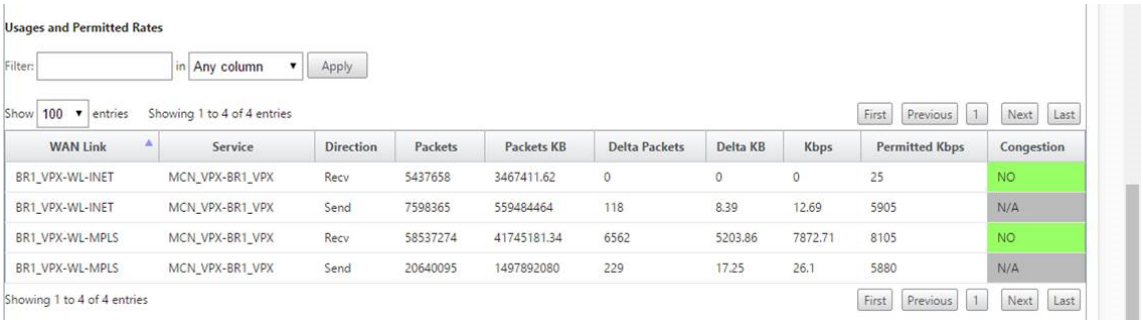
適応型帯域幅検出を有効にするには、次の手順を実行します。

この機能を使用するには、前提条件として [Bad Loss sensitivity] オプションを有効にする必要があります (デフォルト/カスタム)。**[** グローバル**] >[**自動パスグループ**] >**[自動パスグループ名]**>[** 不良ロスセンシティブ**]** で有効にすることができます。

1. **[** グローバル**]>[**自動パスグループ**]>**[自動パスグループ名]**>[**不良ロスセンシ ティブ**]** で、**[** 適応帯域幅検出**]** を有効にします。
2. **[** 構成エディタ**] >[** サイト**] >** [サイト名]**>[WAN** リンク**] >**[**WAN** リンク名]**>[** 設定**] >[** 詳細設定**]** に移動します。



3. [適応帯域幅検出] チェックボックスをオンにし、[最小許容帯域幅] フィールドに値を入力します。
4. [監視] > [統計] > [**WAN** リンク ****** の使用状況**] > [**使用量と許可されたレート] の順に移動して、[使用 ****** 量と許可されたレート] テーブルを表示します。



Usages and Permitted Rates

Filter: in Any column Apply

Show 100 entries Showing 1 to 4 of 4 entries First Previous 1 Next Last

WAN Link	Service	Direction	Packets	Packets KB	Delta Packets	Delta KB	Kbps	Permitted Kbps	Congestion
BR1_VPX-WL-INET	MCN_VPX-BR1_VPX	Recv	5437658	3467411.62	0	0	0	25	NO
BR1_VPX-WL-INET	MCN_VPX-BR1_VPX	Send	7598365	559484464	118	8.39	12.69	5905	N/A
BR1_VPX-WL-MPLS	MCN_VPX-BR1_VPX	Recv	58537274	41745181.34	6562	5203.86	7872.71	8105	NO
BR1_VPX-WL-MPLS	MCN_VPX-BR1_VPX	Send	20640095	1497892080	229	17.25	26.1	5880	N/A

Showing 1 to 4 of 4 entries First Previous 1 Next Last

ベストプラクティス

May 10, 2021

以下のトピックでは、ネットワークで Citrix SD-WAN ソリューションの設計、計画、実行を行う際に従うべきベストプラクティスを示します。

セキュリティ

ルーティング

QoS

WAN リンク

セキュリティ

May 10, 2021

この記事では、Citrix SD-WAN ソリューションのセキュリティのベストプラクティスについて説明します。Citrix SD-WAN 展開に関する一般的なセキュリティガイダンスを提供します。

Citrix SD-WAN 展開のガイドライン

展開ライフサイクルを通じてセキュリティを維持するには、次のセキュリティを考慮することをお勧めします。

- 物理的セキュリティ
- アプライアンスのセキュリティ
- ネットワークセキュリティ
- 管理と管理

物理的セキュリティ

セキュアサーバールームへの Citrix SD-WAN アプライアンスの展開-Citrix SD-WAN がインストールされているアプライアンスまたはサーバーは、セキュアなサーバールームまたは制限付きデータセンター施設に配置する必要があります。これにより、アプライアンスが不正アクセスから保護されます。少なくとも、アクセスは電子カードリーダーによって制御される必要があります。アプライアンスへのアクセスは、監査目的ですべてのアクティビティを継続的に記録する CCTV によって監視されます。侵入した場合, 電子監視システムは、即時応答のためのセキュリティ担当者にアラームを送信する必要があります.

フロントパネルとコンソールポートを不正アクセスから保護-物理キーのアクセス制御により、アプライアンスを大きなケージまたはラックに保護します。

電源の保護-アプライアンスが無停電電源装置（UPS）で保護されていることを確認します。

アプライアンスセキュリティ

アプライアンスのセキュリティを確保するには、Citrix SD-WAN 仮想アプライアンス（VPX）をホストするすべてのサーバーのオペレーティングシステムを保護し、リモートソフトウェア更新を実行し、安全なライフサイクル管理方法に従います。

- Citrix SD-WAN VPX アプライアンスをホストするサーバーのオペレーティングシステムのセキュリティ保護-Citrix SD-WAN VPX アプライアンスは、標準サーバー上で仮想アプライアンスとして動作します。標準サーバーへのアクセスは、ロールベースのアクセス制御と強力なパスワード管理で保護する必要があります。また、オペレーティングシステムの最新のセキュリティパッチを使用してサーバーを定期的に更新し、サーバー上の最新のウイルス対策ソフトウェアを更新することをお勧めします。
- リモートソフトウェア更新の実行-すべてのセキュリティ更新プログラムをインストールして、既知の問題を解決します。サインアップして最新のセキュリティアラートを受信するには、セキュリティ情報の Web ページを参照してください。
- Secure Lifecycle Management Practice に従う-RMA の再デプロイ時または開始時、機密データの廃棄時にアプライアンスを管理するには、アプライアンスから永続データを削除してデータ追従対策を完了します。

ネットワークセキュリティ

ネットワークセキュリティのために、デフォルトの SSL 証明書は使用しないでください。管理者インターフェイスにアクセスする場合は、Transport Layer Security (TLS) を使用し、アプライアンスのルーティング不可能な管理 IP アドレスを保護し、高可用性セットアップを構成し、展開に適した管理保護策を実装します。

- デフォルトの SSL 証明書を使用しない-信頼できる認証局からの SSL 証明書を使用すると、インターネットに直接接続する Web アプリケーションのユーザーエクスペリエンスを簡素化できます。自己署名証明書や評判の良い証明機関からの証明書の場合とは異なり、Web ブラウザーでは、Web サーバーへの安全な通信を開始するために、ユーザーは評判の良い証明機関からの証明書をインストールする必要はありません。

- 管理者インターフェイスにアクセスするときにトランスポート層セキュリティを使用する-管理 IP アドレスがインターネットからアクセスできないか、少なくともセキュリティで保護されたファイアウォールで保護されていることを確認してください。LOM IP アドレスがインターネットからアクセスできないか、少なくともセキュリティで保護されたファイアウォールで保護されていることを確認してください。
- 管理アカウントと管理アカウントの保護—別の管理者アカウントを作成し、管理者アカウントとビューアのアカウントに強力なパスワードを設定します。リモートアカウントアクセスを設定する場合は、RADIUS および TACAS を使用してアカウントの外部認証管理を設定することを検討してください。admin ユーザアカウントのデフォルトパスワードの変更、NTP の設定、デフォルトのセッションタイムアウト値の使用、SNMPv3 と SHA 認証および AES 暗号化を使用します。

Citrix SD-WAN オーバーレイネットワークは、SD-WAN オーバーレイネットワークを通過するデータを保護します。

セキュアな管理者インタフェース

安全な Web 管理アクセスを実現するには、信頼できる認証局から証明書をアップロードおよびインストールして、デフォルトのシステム証明書を置き換えます。**SD-WAN** アプライアンス **GUI** で、「構成」**>**「アプライアンスの設定」**>**「管理者インターフェース」の順に選択します。

ユーザーアカウント:

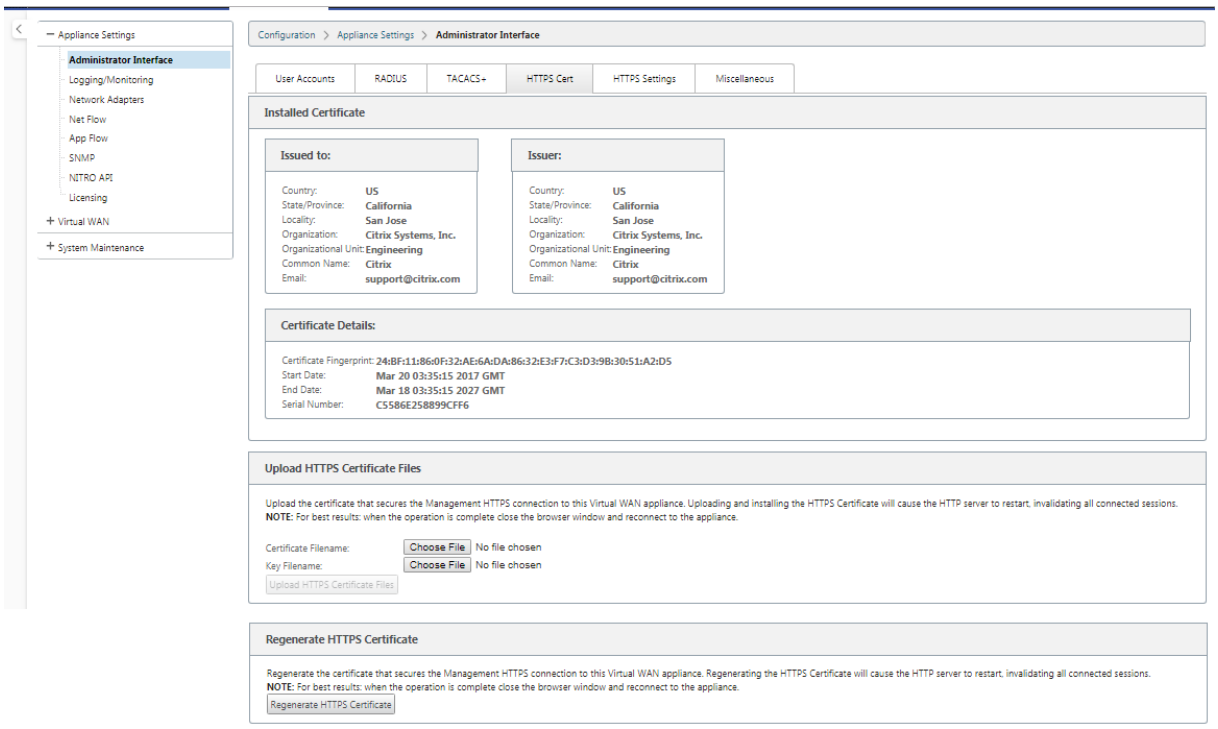
- ローカルユーザーパスワードの変更
- ユーザーの管理

HTTPS 証明書:

- 証明書
- キー

その他:

- Web コンソールのタイムアウト



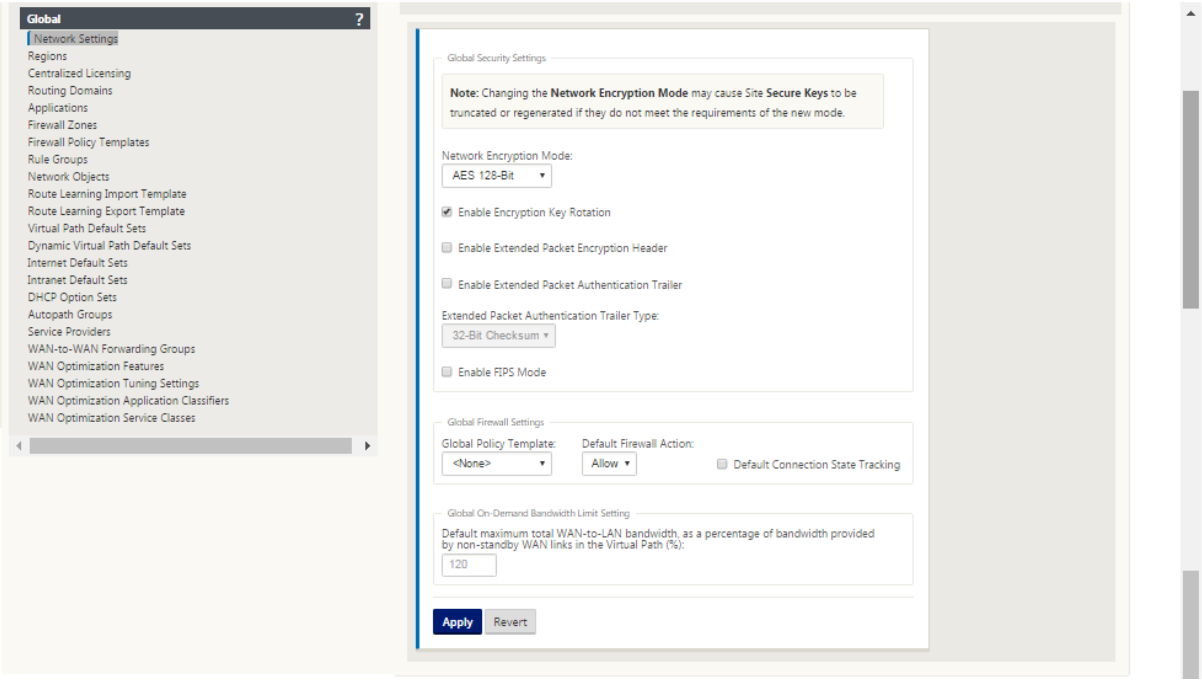
構成エディタ > グローバル > ネットワーク設定

グローバルファイアウォールの設定:

- グローバルポリシーテンプレート
- デフォルトのファイアウォールのアクション
- デフォルトの接続状態トラッキング

グローバル仮想パス暗号化設定:

- AES 128 ビット（デフォルト）
- 暗号化キーのローテーション (デフォルト)
- 拡張パケット暗号化ヘッダー
- 拡張パケット認証トレーラ



グローバル仮想パス暗号化設定

- AES-128 データ暗号化はデフォルトで有効になっています。パス暗号化には、AES-128 以上の保護を使用して AES-256 暗号化レベルを使用することを推奨します。「Enable Encryptic Key Rotation」が設定されており、楕円曲線 Diffie-Hellman 鍵交換を使用して、暗号化が有効になっているすべての仮想パスに対して鍵の再生成が 10 ～15 分間隔で行われるようにします。

ネットワークで機密性（つまりタンパープロテクション）に加えてメッセージ認証が必要な場合は、IPsec データ暗号化することをお勧めします。機密性のみが必要な場合は、拡張ヘッダーを使用することをお勧めします。

- Extended Packet Encryption Header を使用すると、暗号化されたメッセージの先頭にランダムにシードされたカウンタを追加できるようになります。暗号化されると、このカウンタはランダムな初期化ベクトルとして機能し、暗号化キーでのみ決定論的です。これにより、暗号化の出力がランダム化され、強力なメッセージが区別されません。このオプションを有効にすると、パケットのオーバーヘッドが 16 バイト増加することに注意してください。
- 拡張パケット認証トレーラーは、暗号化されたすべてのメッセージの最後に認証コードを追加します。このトレーラを使用すると、パケットが転送中に変更されていないことを確認できます。このオプションでは、パケットのオーバーヘッドが増加することに注意してください。

ファイアウォールのセキュリティ

推奨されるファイアウォールの構成では、まず「すべて拒否」というデフォルトのファイアウォールアクションが使用され、次に例外が追加されます。ルールを追加する前に、ファイアウォールルールの目的を文書化および確認しま

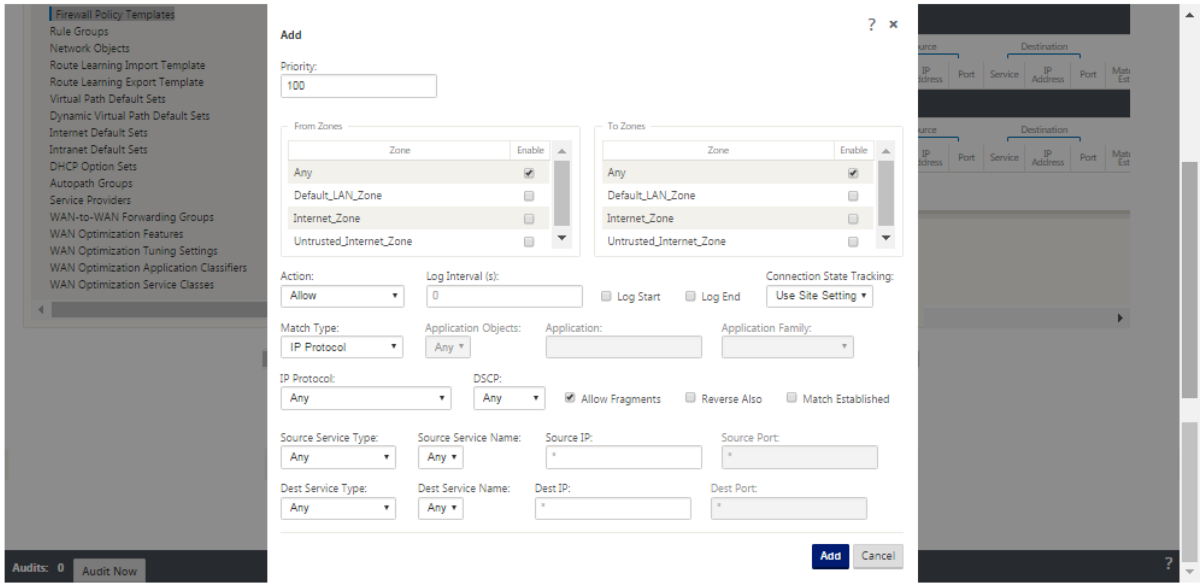
す。可能な場合は、ステートフル検査とアプリケーションレベル検査を使用します。ルールを簡素化し、冗長なルールを排除します。ファイアウォール 設定の変更を追跡して確認できる変更管理プロセスを定義し、遵守します。グローバル設定を使用してアプライアンスを経由する接続を追跡するように、すべてのアプライアンスのファイアウォールを設定します。接続のトラッキングは、パケットが適切に形成され、接続状態に適していることを確認します。組織のネットワークまたは機能領域の論理階層に適したゾーンを作成します。ゾーンは世界的に重要であり、地理的に異なるネットワークを同じセキュリティゾーンとして扱うことができることに注意してください。セキュリティホールのリスクを軽減する最も具体的なポリシーを作成し、許可ルールで [Any] を使用しないようにします。グローバルポリシーテンプレートを設定および管理して、ネットワーク内のすべてのアプライアンスの基本レベルのセキュリティレベルを作成します。ネットワーク内のアプライアンスの機能ロールに基づいてポリシーテンプレートを定義し、必要に応じて適用します。必要な場合のみ、個々のサイトでポリシーを定義します。

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

デフォルトのファイアウォールアクション—許可を有効にすると、どのフィルタポリシーにも一致しないパケットが許可されます。Deny は、どのフィルタポリシーにも一致しないパケットをドロップすることを有効にします。

[Default Connection State Tr acking]：フィルタポリシーまたは NAT 規則に一致しない TCP、UDP、および ICMP フローの双方向接続ステートトラッキングを有効にします。非対称フローは、ファイアウォールポリシーが定義されていない場合でも、これを有効にすると、ブロックされます。この設定は、グローバル設定よりも優先されるサイトレベルで定義できます。サイトで非対称フローが発生する可能性がある場合は、グローバルではなくサイトまたはポリシーレベルでこれを有効にすることをお勧めします。

ゾーン -ファイアウォールゾーンは、Citrix SD-WAN に接続されたネットワークの論理的なセキュリティグループを定義します。ゾーンは、仮想インターフェイス、イントラネットサービス、GRE トンネル、および LAN IPsec トンネルに適用できます。



WAN リンクセキュリティゾーン

信頼できないセキュリティゾーンは、パブリック (セキュリティで保護されていない) ネットワークに直接接続された WAN リンクで構成する必要があります。Untrusted は、WAN リンクを最も安全な状態に設定し、インターフェイスグループで暗号化、認証、および許可されたトラフィックだけを許可します。仮想 IP アドレスへの ARP および ICMP は、他に許可されるトラフィックタイプだけです。この設定により、暗号化されたトラフィックだけが、Interface グループに関連付けられたインターフェイスから送信されるようになります。

ルーティングドメイン

ルーティングドメインは、ネットワークトラフィックのセグメント化に使用される一連のルータを含むネットワークシステムです。新しく作成されたサイアーは、デフォルトのルーティングドメインに自動的に関連付けられます。

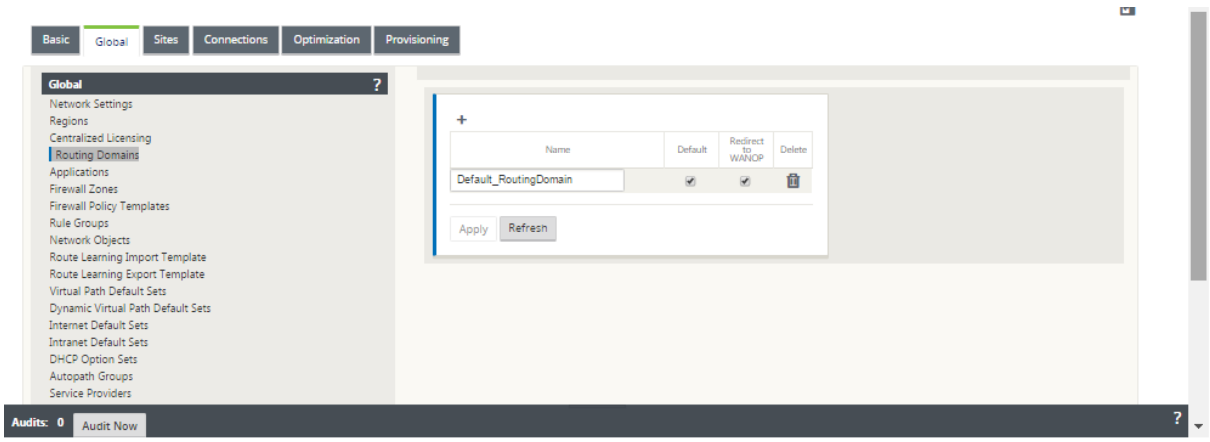
[構成エディタ**]** > [グローバル]

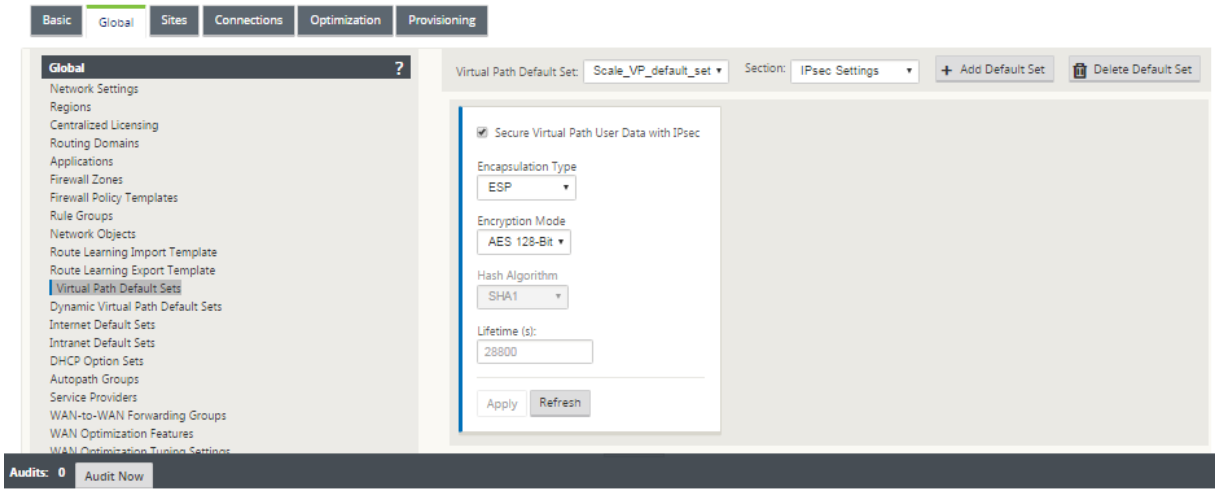
ルーティングドメイン

- RoutingDomain

IPsec トンネル

- デフォルト・セット
- IPsec による仮想パスユーザデータのセキュリティ保護





IPSec トンネル

IPsec トンネルは、ユーザデータとヘッダー情報の両方を保護します。Citrix SD-WAN アプライアンスは、LAN または WAN 側の固定 IPSec トンネルを非 SD-WAN ピアとネゴシエートできます。LAN 経由の IPSec トンネルでは、ルーティングドメインを選択する必要があります。IPsec トンネルがイントラネットサービスを使用する場合、ルーティングドメインは選択されたイントラネットサービスによって事前に決定されます。

IPsec トンネルは、SD-WAN オーバーレイネットワークを介してデータが流れる前に仮想パス上に確立されます。

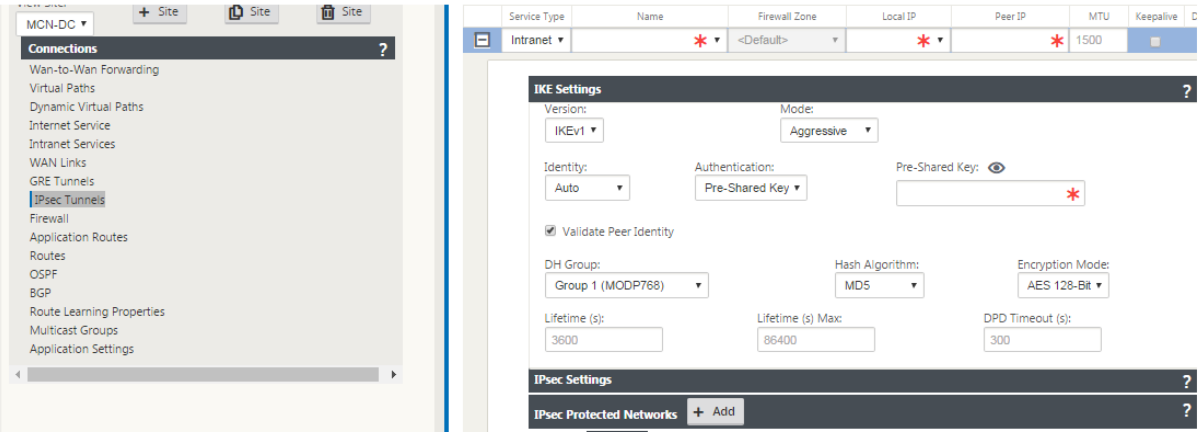
- [カプセル化タイプ] オプションには、ESP-データはカプセル化および暗号化、ESP+auth-データはカプセル化、暗号化、および HMAC で検証され、AH-データは HMAC で検証されます。
- 暗号化モードは、ESP が有効な場合に使用される暗号化アルゴリズムです。
- ハッシュアルゴリズムは、HMAC を生成するために使用されます。
- ライフタイムは、IPsec セキュリティアソシエーションが存在する場合に推奨される期間（秒単位）です。0 は無制限に使用できます。

IKE 設定

インターネットキーエクスチェンジ (IKE) は、セキュリティアソシエーション (SA) の作成に使用される IPSec プロトコルです。Citrix SD-WAN アプライアンスは、IKEv1 と IKEv2 の両方のプロトコルをサポートします。

- モードは、メインモードまたはアグレッシブモードのいずれかです。
- ID は、ピアを識別するために自動的に指定することも、IP アドレスを使用してピアの IP アドレスを手動で指定することもできます。
- 認証では、認証方法として事前共有キー認証または証明書が有効になります。
- [ピア ID の検証] では、ピアの ID タイプがサポートされている場合、IKE のピア ID の検証が有効になります。サポートされていない場合は、この機能を有効にしないでください。

- Diffie-Hellman グループは、グループ 1 が 768 ビット、グループ 2 が 1024 ビット、グループ 5 が 1536 ビットグループで IKE キー生成に使用できます。
- ハッシュアルゴリズムには、MD5、SHA1、および SHA-256 には、IKE メッセージ用のアルゴリズムが用意されています。
- 暗号化モードには、IKE メッセージに対して AES-128、AES-192、および AES-256 暗号化モードがあります。
- IKEv2 の設定には、ピア認証と整合性アルゴリズムが含まれます。



ファイアウォールの設定

アップストリームのルータとファイアウォールの設定を確認することで、次の一般的な問題を特定できます。

- MPLS キュー/QoS 設定：SD-WAN 仮想 IP アドレス間の UDP カプセル化トラフィックが、ネットワーク内の中間アプライアンス の **QoS** 設定によって影響を受けないことを確認します。
- SD-WAN ネットワーク上に構成された WAN リンク上のすべてのトラフィックは、適切なサービスタイプ（仮想パス、インターネット、イントラネット、ローカル）を使用して Citrix SD-WAN アプライアンスによって処理される必要があります。
- トラフィックが Citrix SD-WAN アプライアンスをバイパスし、同じ基になるリンクを使用する必要がある場合は、SD-WAN トラフィックの適切な帯域幅予約をルーター上で行う必要があります。また、SD-WAN 設定では、リンク容量を適宜設定する必要があります。
- 中間ルータ/ファイアウォールに UDP フラッディングや PPS の制限が適用されていないことを確認します。これにより、仮想パス（UDP カプセル化）を介して送信されるトラフィックが抑制されます。

ルーティング

May 10, 2021

この記事では、Citrix SD-WAN ソリューションのルーティングのベストプラクティスについて説明します。

インターネット/イントラネットルーティングサービス

インターネットサービスがインターネットにバインドされたトラフィックに対して構成されていない場合、ローカルルートまたは パススルー ルートのいずれかが Gateway ルータに到達するように構成されます。ルータは SD-WAN アプライアンスに設定された WAN リンクを使用し、リンクのオーバーサブスクリプションの問題につながります。

MCN でインターネットルートが **Local** として設定されている場合、すべてのブランチ SD-WAN サイトで学習され、デフォルトで 仮想パスルート として設定されます。これは、ブランチアプライアンスでインターネットにバインドされたトラフィックが、仮想パスを経由して MCN にルーティングされることを意味します。

ルーティングの優先順位

ルーティングの優先順位:

- プレフィックス一致: 最長プレフィックス一致。
- サービス: ローカル、仮想パスサービス、インターネット、イントラネット、パススルー
- ルートコスト

ルーティングの非対称性

ネットワークにルーティングの非対称性がないことを確認します（NetScaler SD-WAN アプライアンスがトラフィックを一方向のみ送信しています)。これにより、ファイアウォールの接続追跡とディープパケットインスペクションで問題が発生します。

QoS

May 10, 2021

QoS を設定する場合は、次の点を考慮してください。

- ネットワークトラフィックのパターンと要件を理解します。QoS 統計情報に示されているように、**QoS** クラス統計情報の確認、キュー深度の変更、またはデフォルトの QoS クラス共有パーセンテージの変更が必要になる場合があります。
- 特定のアプリケーション IP アドレスに対して Rules を作成するのではなく、設定を容易にするため、サブネット全体が Rule に追加されることがあります。サブネット全体をルールに追加すると、サブネット内のすべてのトラフィックが 1 つのルールに誤ってマッピングされます。したがって、そのルールに関連付けられた QoS クラスによって、テールドロップやアプリケーションパフォーマンスやユーザエクスペリエンスの低下につながる可能性があります。

WAN リンク

May 10, 2021

この記事では、Citrix SD-WAN ソリューションの WAN リンク構成のベストプラクティスについて説明します。

WAN リンクの設定時に覚えておくべきポイント

- 実際の WAN リンク帯域幅として、許可レートと物理 レートを設定します。WAN リンク容量全体が SD-WAN アプライアンスによって使用されることが想定されていない場合は、それに応じて 許可 レートを変更します。
- 帯域幅が不明な場合、およびリンクが信頼できない場合には、**Auto Learn** 機能を有効にできます。自動学習機能は、基礎となるリンク容量だけを学習し、今後同じ値を使用します。
- 基になるリンクが安定しておらず、固定帯域幅（4G リンクなど）を保証しない場合は、適応型帯域幅検出 機能を使用します。
- 同じ WAN リンク上で、自動学習 と 適応帯域幅検出 を有効にすることは推奨されません。
- 基になるリンクが安定していない場合は、次の [パス] 設定を変更します。
  - 損失の設定
  - 不安定性のセンシティブを無効にする
  - 沈黙の時間
- 診断ツールを使用して、リンクの正常性/容量を確認します。
- SD-WAN が ワンアーム モードで配置されている場合は、基礎となるリンクの物理容量を超過しないようにしてください。

ISP リンクのヘルスの確認

新しい展開の場合、SD-WAN 展開より前で、既存の SD-WAN 展開に新しい ISP リンクを追加する場合、次の手順を実行します。

- リンクタイプを確認します。たとえば、MPLS、ADSL、4G。
- ネットワーク特性たとえば、帯域幅、損失、遅延、ジッタなどです。

この情報は、要件に従って SD-WAN ネットワークを構成するのに役立ちます。

ネットワークトポロジ

通常、特定のネットワークトラフィックは Citrix SD-WAN アプライアンスをバイパスし、SD-WAN ネットワークで構成されているのと同じ基になるリンクを使用することが観察されます。SD-WAN では、リンク使用率を完全に可視

化できないため、SD-WAN がリンクをオーバーサブスクライブし、パフォーマンスと PATH の問題が発生する可能性があります。

プロビジョニング

SD-WAN の Provisioning 時に考慮すべきポイント

- デフォルトでは、すべてのブランチと WAN サービス (仮想パス/インターネット/イントラネット) は、同じ帯域幅のシェアを受け取ります。
- 接続するサイト間の帯域幅要件または可用性の面で大きな格差がある場合、プロビジョニングサイトを変更する必要があります。
- 使用可能な最大サイト間で動的仮想パスを有効にすると、DC への静的仮想パスと動的仮想パスの間で WAN リンク容量が共有されます。

よくあるご質問

May 10, 2021

高可用性

高可用性アプライアンスとセカンダリ（Geo）アプライアンスの違いは何ですか。

- 高可用性は、フォールトトレランスを保証しますセカンダリ (Geo) アプライアンスにより、ディザスタリカバリが可能になります。
- 高可用性は、MCN、RCN、およびブランチアプライアンスに対して設定できます。セカンダリ（Geo）アプライアンスは、MCN および RCN に対してのみ構成できます。
- 高可用性アプライアンスは、同じサイトまたは地理的な場所内で構成されます。地理的に異なる場所にあるブランチアプライアンスは、セカンダリ（Geo）MCN/RCN アプライアンスとして設定されます。
- 高可用性のプライマリアプライアンスとセカンダリアプライアンスは、同じプラットフォームモデルである必要があります。セカンダリ（Geo）アプライアンスは、プライマリ MCN/RCN と同じプラットフォームモデルである場合とそうでない場合があります。
- 高可用性は、セカンダリ（Geo）よりも高い優先順位です。アプライアンス（MCN/RCN）が高可用性およびセカンダリ（Geo）アプライアンスで構成されている場合、アプライアンスに障害が発生すると、セカンダリ高可用性アプライアンスがアクティブになります。両方の高可用性アプライアンスに障害が発生した場合や、データセンターサイトがクラッシュした場合は、セカンダリ（Geo）アプライアンスがアクティブになります。
- 高可用性では、プライマリ/セカンダリスイッチオーバーは、高可用性の展開に応じて、即座に、または 10 ～ 12 秒以内に発生します。プライマリ MCN/RCN からセカンダリ（Geo）MCN/RCN へのスイッチオーバーは、プライマリが非アクティブ状態の 15 秒後に発生します。

- 高可用性設定では、プライマリ再要求を設定できます。セカンダリ（Geo）アプライアンスのプライマリ再要求を設定することはできません。プライマリ再要求は、プライマリアプライアンスが戻り、ホールドタイマーが期限切れになると、自動的に行われます。

シングルステップアップグレード

> 注
>
> WANOP、SVM、および XenServer サプリメンタル/HF は、OS コンポーネントとして表示されます。

現在のバージョン（8.1.x 、*9.1.x*、*9.2.x*）から *9.3.x* にアップグレードするには、*.tar.gz*** を使用するか、*.zip* パッケージをシングルステップアップグレードする必要がありますか?

関連するプラットフォームの *.tar.gz* ファイルを使用して、SD-WAN ソフトウェアを 9.3.x にアップグレードします。SD-WAN ソフトウェアを 9.3.x バージョンにアップグレードしたら、*.zip* パッケージを使用して変更管理を実行し、OS コンポーネントソフトウェアパッケージを転送またはステージングします。アクティベーション後、MCN は関連するすべてのブランチの OS コンポーネントを転送/ステージングします。

シングルステップアップグレードパッケージ（.zip ファイル）を使用して 9.3.0 にアップグレードした後、実行する必要があります。各アプライアンスで *upg* アップグレードしますか?

いいえ。OS ソフトウェアの更新/アップグレードは、1 ステップのアップグレード *.zip* パッケージによって処理され、各サイトの変更管理設定に記載されているスケジュール詳細に従ってインストールされます。

9.3 より前のバージョンから 9.3.x にアップグレードするために、*.tar.gz*** に続いて*.zip* パッケージを使用する必要があるのはなぜですか? また、9.3.x の *.zip* パッケージを直接使用しないのはなぜですか?

シングルステップアップグレードパッケージは 9.3.0.161 以降でサポートされており、以前のリリースバージョン (リリース 9.3 以前) では、このパッケージは認識されません。シングルステップアップグレード *.zip* パッケージが Change Management の受信トレイにアップロードされると、パッケージが認識されないことを示すエラーがスローされます。したがって、まず SD-WAN ソフトウェアを 9.3 以上のバージョンにアップグレードしてから、を使用して変更管理を実行します。*zip* パッケージ。

OS コンポーネントは、1 ステップアップグレードでどのようにインストールされるのですか? *upg* のアップグレードが実行されませんか?

MCN は、シングルステップアップグレード *.zip* パッケージを使用して変更管理が完了した後、アプライアンスモデルに基づいて OS コンポーネントソフトウェアパッケージを転送またはステージングします。アクティベーション後、MCN は、スケジュールされた更新/アップグレードに必要なブランチの OS コンポーネントソフトウェアパッケージの転送/ステージングを開始します。

後でインストールするスケジュールを設定せずに、OS コンポーネントをインストールするにはどうすればよいですか?

OS コンポーネントをすぐにインストールするには、メンテナンスウィンドウ の値を「**0**」に設定します。

> 注
>
> インストールは、メンテナンスウィンドウ の値が「**0**」に設定されている場合でも、サイトに必要なすべてのパッケージがアプライアンスで受信された場合にのみ開始されます。

インストールのスケジュール設定にはどのようなものがありますか? スケジュール指示を使用して VW 単体でアップグレードすることはできますか?

スケジュールされたインストールは SD-WAN リリース 9.3 で導入され、OS コンポーネントにのみ適用され、VW ソフトウェアのアップグレードには適用されません。シングルステップアップグレードでは、OS コンポーネントのアップグレードを実行するために各アプライアンスにログインする必要はありません。スケジューリングオプションを使用すると、VW ソフトウェアバージョンアップグレード以外の時間に OS コンポーネントのインストールをスケジュールできます。

[変更管理設定] ページのスケジュール情報が、既定でスケジュール日を過ぎているのはなぜですか?

「変更管理設定」ページには、デフォルトのスケジュール情報が表示されます。「開始」*:*「*2016-05-21 21:20:00*」、「ウィンドウ」*: 1*、「繰り返し」*: 1*、「単位」*:*「日」です。日付が過去の日付の場合、スケジュールされたインストールは、日付ではなく、メンテナンスウィンドウ、リピートウィンドウ、ユニットなどの時間およびその他のパラメータに基づきます。

デフォルトのスケジュールインストール日時は何に設定されていますか。汎用アプライアンスとローカルアプライアンスに依存していますか。

デフォルトでは、スケジュールの詳細が *21:20:00* に「*2016-05-21*」に設定されています（メンテナンス期間は *1* 時間で、*1* 日ごとに繰り返されます）。この詳細は、ローカルアプライアンスサイトによって異なります。

メンテナンス/スケジュールされたウィンドウを待たずに、OS Components をすぐにインストールするにはどうすればよいですか?

「変更管理設定」ページで「メンテナンスウィンドウ」の値を「**0** 」に設定します。これにより、スケジュールされたインストール時間が上書きされます。

現在のソフトウェアバージョンが 9.3.x 以降の場合、アップグレードに使用するパッケージはどれですか?

現在のソフトウェアバージョン 9.3.x 以上の場合は、シングルステップアップグレード *.zip* パッケージを使用して、より高いバージョンにアップグレードします。

OS コンポーネントファイルはいつブランチに転送/ステージングされますか?

シングルステップアップグレード *.zip* パッケージを使用して Change Management を実行すると、アクティベーションが完了した後、OS コンポーネントファイルは関連するブランチに転送/ステージングされます。

どのアプライアンスが OS Components ファイルを受信するか、プラットフォームに依存するか、すべてのブランチがそれを受信しますか?

EE ライセンスで実行されている **SD-WAN-400**、**800**、**1000**、**2000 SE**、ベアメタル **SD-WAN-2100** などの Hypervisor ベースのアプライアンスは、アップグレードする OS コンポーネントを受け取ります。

スケジューリングはどのように機能しますか?

デフォルトでは、スケジュールの詳細は ***2016-05-21 21*** の ***21:20:00***（メンテナンス時間は ***1*** 時間で、***1*** 日ごとに繰り返される）に設定されています。これは、繰り返し値が **1** 日に設定され、メンテナンスが行われるため、新しいソフトウェアがインストール可能かどうかをシステムがチェックします。ウィンドウを **1** 時間表示すると、**2016-05-21** から **21:20:00**（ローカルアプライアンス時間）にインストールがトリガー/試行されます（新しいソフトウェアが使用可能な場合）

OS コンポーネントがアップグレードされたかどうかを知るにはどうすればよいですか?

[ステータス] 列には、緑色のチェックマークが表示されます。その上にカーソルを合わせると、「アップグレードは成功しました」というメッセージが表示されます。

RCN とそのブランチ用の OS コンポーネントのインストールをスケジュールするにはどうすればよいですか?

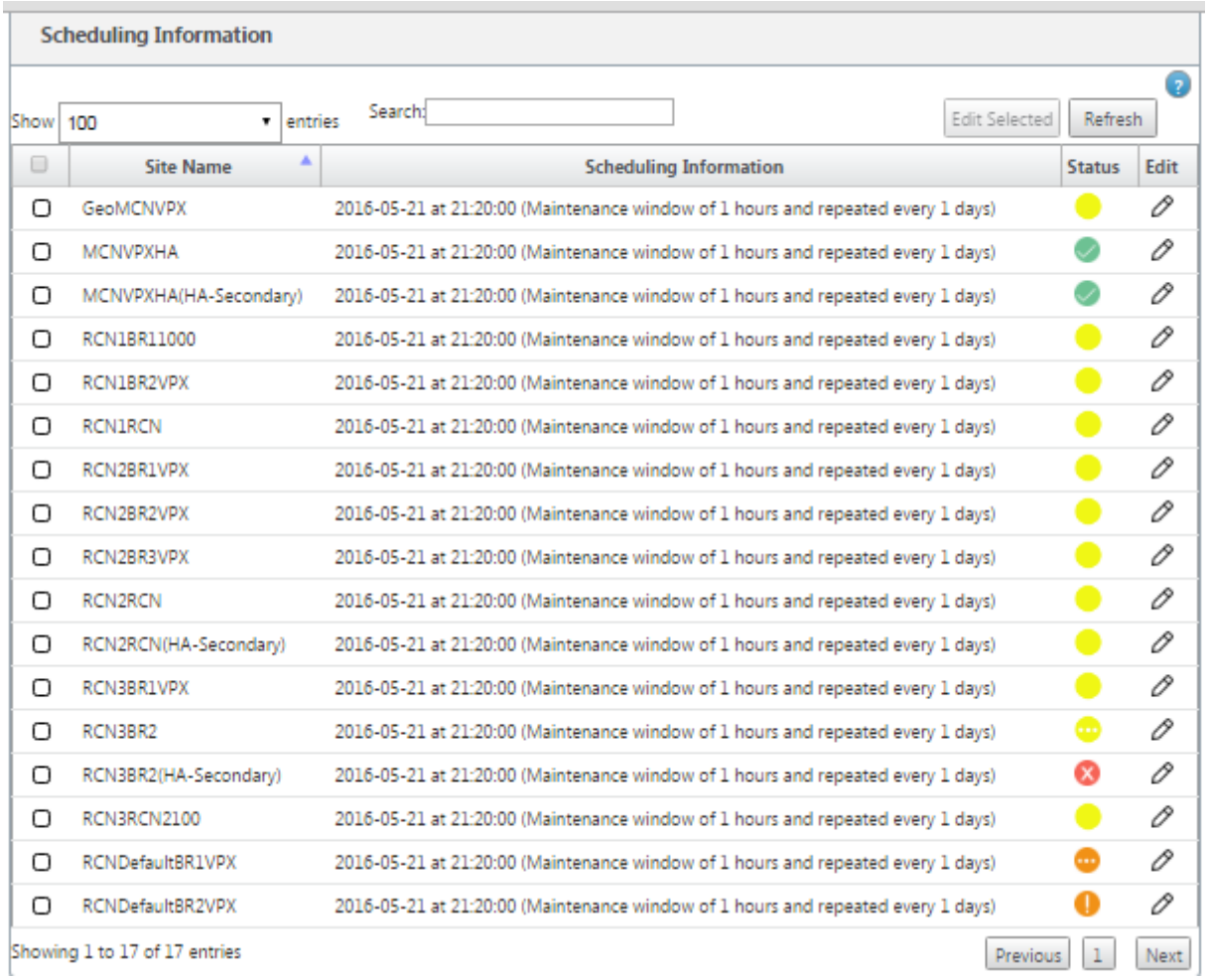
RCN のスケジューリングは、[MCN 変更管理設定] ページから実行されます。RCN ブランチの場合は、各 RCN にログインし、スケジュールの詳細を設定する必要があります。

スケジュールされたインストールのステータスはどこから入手できますか。

RCN のスケジュールされたインストールのステータスは、[MCN 変更管理設定] ページから取得できます。RCN ブランチの場合、ステータスを取得するには、各 RCN にログインする必要があります。

スケジュールされたインストールのステータスを取得するにはどうすればよいですか。

「変更管理設定」ページにある更新ボタンを使用して、MCN からステータスを取得し、デフォルトリージョンおよび RCN のブランチについては RCN からステータスを取得します。



Scheduling Information

Show 100 entries Search: Edit Selected Refresh

Site Name	Scheduling Information	Status	Edit
GeoMCNVPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
MCNVPXHA	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
MCNVPXHA(HA-Secondary)	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCN1BR11000	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCN1BR2VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCN1RCN	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCN2BR1VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCN2BR2VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCN2BR3VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCN2RCN	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCN2RCN(HA-Secondary)	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCN3BR1VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCN3BR2	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCN3BR2(HA-Secondary)	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCN3RCN2100	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCNDefaultBR1VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCNDefaultBR2VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		

Showing 1 to 17 of 17 entries Previous 1 Next

以前のソフトウェアアップグレードでシングルステップアップグレードが使用されたときに、*tar.gz* ファイルを使用して次のリリースにアップグレードできますか。

tar.gz ファイルを使用してアップグレードできますが、を使用してソフトウェアアップグレードを実行できるため、推奨されません。*upg* file. 該当する各アプライアンスにログインして、オペレーティングシステム (OS) コンポーネントソフトウェアをアップグレードするためにアップロードします。リリース 9.3 バージョン 1 から、「オペレーティングシステムソフトウェアの更新」ページは減価償却されます。その結果、*.zip* パッケージを使用して OS コンポーネントをアップグレードすることで、変更管理を実行できます。

現在実行中の OS コンポーネントのバージョンをどのように検証できますか?

現在、UI から OS コンポーネントの現在実行中のバージョンを検証できません。各コンソールからログインするか、STS にこの情報を表示できます。

ネットワークにベアメタルアプライアンスがある場合、どのような違いがありますか? スケジューリングはベアメタル/仮想アプライアンスに影響しますか?

SD-WAN のようなベアメタルアプライアンス—**410,2100,4100,5100 SD-WAN** は、SD-WAN ソフトウェアのみを実行します。ベアメタルアプライアンスには OS コンポーネントパッケージは必要ありません。これらのプラットフォームは、ソフトウェアの必要性の観点から、SD-WAN VPX-SE アプライアンスと同等の扱いを受けます。MCN

は OS コンポーネントパッケージをこれらのアプライアンスに転送しません。これらのアプライアンスには、アップグレードが必要な OS コンポーネントがないため、スケジュール情報の設定は有効になりません。

SSU は、高可用性環境/デプロイメントでどのように機能しますか?

MCN での高可用性展開では、変更管理中にアクティブな MCN スイッチがプライマリ MCN の役割を切り替え、スタンバイ/セカンダリ MCN が引き継ぐという制限があります。この場合、パッケージのアクティブな MCN 上の *.zip* パッケージを使用して変更管理を再度実行するか、アクティブな MCN のロールを切り替えてプライマリ MCN に切り替えて、元のプライマリ MCN が他の OS コンポーネントパッケージにステージングされる OS コンポーネントパッケージのロールを引き継ぐことができるように、プライマリ MCN に戻すことができます。枝。

高可用性環境/導入では、シングルステップアップグレードはどのように機能しますか。

高可用性展開でシングルステップアップグレードを実行すると、プライマリ MCN とスタンバイ MCN の役割が切り替わります。これは制限です。このような場合は、アクティブな MCN の *.zip* パッケージを使用して変更管理を再度実行します。または、アクティブ MCN の役割を切り替えて、元のプライマリ MCN が OS コンポーネントパッケージをブランチにステージングできるように、プライマリ MCN に切り替えることもできます。

アプライアンスを再起動するために、ゼロタッチ導入をワンステップでアップグレードできますか。

はい、使用できます。

スタンドアロン WANOP アプライアンスをアップグレードするためにシングルステップアップグレードを使用できますか?

いいえ。

シングルステップアップグレードを使用して、2 ボックスモードで展開されたスタンドアロン WANOP アプライアンスをアップグレードできますか?

なし 2 ボックスモードの一部である SD-WAN アプライアンスのみがアップグレードされ、WANOP スタンドアロンアプライアンスはアップグレードされません。

多層ネットワークにアップグレードするには、どのパッケージを使用すればよいですか?

<release-version> 現在のソフトウェアバージョンが 9.3.x 以上の場合は、シングルステップアップグレードパッケージ *ns-sdw-sw-.zip* ファイルを使用します。MCN は、それぞれのブランチに RCN と RCN ステージングソフトウェアパッケージにステージングパッケージの世話をします。

ns-sdw-sw-.zip <release-version> ファイルをアップロードした後、現在のソフトウェアでは 1 つのプラットフォームモデルしか表示されていませんか?

リリース 10.0 から、スケールアーキテクチャのサポートが導入され、シングルステップアップグレードの処理が高速化されました。現在のソフトウェアでは、MCN プラットフォームモデルのみを表示できます。[**Verif** y] ボタンまたは [**Stage Appliance]** ボタンを選択すると、その他のアプライアンス・パッケージがリスト/表示/処理されます。

VPX/VPXL/ベアメタルアプライアンスの場合、RCN 用にステージングされるパッケージはどれですか。

パッケージは RCN にステージングされます。RCN ブランチはどのプラットフォームモデルでもかまいません。したがって、彼らはすべてのパッケージを必要とします。

RCN が VPX アプライアンスで、ブランチがこれらのパッケージを必要とするアプライアンスである場合、RCN の背後にあるブランチサイトはどのように OS コンポーネントパッケージを取得しますか?

RCN は、SD-WAN VW ソフトウェアパッケージをアクティブ化した後、OS コンポーネントパッケージを必要とするブランチに、関連するパッケージをステージングします。

ステージング中に「未完了を無視」を選択し、変更管理の次のステージに進むことはできますか? このボタンを選択すると、ステージングが完了していないサイトに対してどのような影響がありますか。

はい、[不完全無視] をクリックできます。これにより、[次へ] ボタンが有効になり、進行状況バーが表示されます。このオプションは、サイトにアクセスできず、変更管理がこれらのサイトのステージングが完了するのを待っている場合に提供されます。そのため、ユーザーはステージの状態を無視して次のステージに進み、アクティブ化に進むことができます。サイトが起動すると、MCN はアクティベーション完了後にパッケージをステージングします。

部分的なソフトウェアアップグレード

部分的なサイトアップグレードとは何ですか? どのように使用できますか?

サイトソフトウェアの部分的なアップグレードは、リリース 10.0 で導入された新機能です。MCN からリリース 10.x の新しいバージョンをステージングし、選択したサイト/ブランチの **Local Change Management** ページからステージングされたソフトウェアバージョンをアクティブ化できます。サイト/ブランチでステージングされたソフトウェアをアクティブ化する前に、MCN のチェックボックスがオンになっていることを確認します。

- この機能はデフォルトでは無効になっています。既存の補正メカニズムにより、ネットワークの同期が維持されます。ユーザーは、［構成］>［管理設定の変更］ページでチェックボックスをオンにして、サイトの部分的なアップグレードを許可する必要があります。
- 部分的なソフトウェアアップグレードは、ブランチまたは RCN でのみ実行でき、MCN では実行できません。

サイトソフトウェアの部分的なアップグレードを使用できる場合のユースケース/シナリオを次に示します。

関連する変更を含むソフトウェアパッチが、特定のサイト (サイトの部分的なアップグレードが実行されている) に対して互換性があり、機能しているかどうかを検証します。アップグレードされたソフトウェアが予期したとおりに動作していることを確認します。これにより、ネットワーク全体を新しいソフトウェアでアップグレードする前に、新しいソフトウェアを検証し、特定のサイトで修正できます。

この機能を使用して次のものからアップグレードすることは可能ですが、

- 10.0 から 10.x
- 10.0.x から 10.0.y
- 11.0～11.y
- 11.0.x～11.0.y
- 上記のすべて

サイトソフトウェアの部分的なアップグレードは、アプライアンスがソフトウェアリリース 10.x 以降を実行している場合にのみ適用され、同じメジャーバージョンのソフトウェア内で使用できます。リリース 10.0 から 10.0.x/10.x の間で使用できます。サイトソフトウェアの部分的なアップグレードの一環として、構成を変更することはできません。

設定から機能を有効にすることで、部分的なソフトウェアアップグレードの一部としてテストする新機能をテストできますか。

いいえ。部分的なソフトウェアアップグレードでは、アクティブ構成とステージング構成を同一にする必要があります。変更できるのはソフトウェアバージョンのみです。

RCN の部分的なソフトウェアアップグレードを無効にすることはできますか。

いいえ。部分的なソフトウェアアップグレードは、MCN からのみ有効または無効にできます。RCN では、この機能は読み取り専用モードです。

9.3.x および 10.0.x をステージングした状態でアクティブになっている場合、部分的なソフトウェアアップグレードを使用できますか。

いいえ。アプライアンスはリリース 10.0 でアクティブなソフトウェアとして実行されている必要があります。

一部のブランチがこの機能を使用してすでにアップグレードされているときに、MCN から [Partial Software Upgrade] オプションが無効になっている場合はどうなりますか。

MCN は、Partial Software Upgrade 機能が無効になっているという通知をネットワーク内のすべてのアプライアンスに送信します。その後、ネットワーク内のすべてのアプライアンスが MCN によってアクティブおよびステージングされたバージョンに一致するように自動修正されます。ただし、MCN では、変更管理の [有効化] ページで [段階的有効化] オプションをクリックすることを期待しています。[Activate **Staged]** ボタンをクリックしてネットワークをアクティブ化するか、**[**Change Prepar** aged**] をクリックして確認を承認して状態をキャンセルするかを選択できます。

LTE ファームウェアのアップグレード

SSUP パッケージで LTE ファームウェアをアップグレードすることはできますか?

10.2.6 および 11.0.3 以降のリリースでは、LTE をサポートするその他のプラットフォーム上の SSUP パッケージを使用して LTE ファームウェアをアップグレードできます。

変更管理のロールバック

変更管理プロセスのロールバック機能とは何ですか?

リリース 9.3 から、変更管理ロールバック機能を使用すると、t2-app クラッシュや仮想パスの状態などの予期しないイベントが設定更新後に非アクティブになった場合に、作業構成にロールバックできます。ネットワークとアプライアンスは、設定の更新後 10 分間監視されます。この間、次の条件が満たされた場合（ユーザーがこの機能を有効に

している場合)、ステージングされた構成がアクティブになります。アクティブソフトウェアが [ステージング] にロールバックされます。

再起動する構成ロールバックの基準を教えてください。

ロールバックは、次のシナリオが発生した場合に発生します。

1. MCN-設定/ソフトウェアの変更後、30 分間隔でクラッシュにより t2_app サービスが無効になった場合。
2. MCN-構成/ソフトウェアの変更後、アクティベーション後 30 分以上仮想パスサービスがダウンしている場合。ロールバック機能は、サイトで開始されます。
3. サイト：構成/ソフトウェアの変更後、サイトが MCN との通信を失った場合、ロールバック機能が開始されます。
4. サイト-設定/ソフトウェア変更後、30 分間隔内にクラッシュしたため、t2_app サービスが無効になります。

ロールバック後はどうなりますか?

構成のロールバック後、障害のある構成/ソフトウェアが Staged ソフトウェアとして表示されます。

ロールバックが発生したことをユーザーにどのように通知しますか?

GUI の上部に、それぞれのエラーのために Config がロールバックされたという黄色のバナーが表示されます。また、あなたはそれが変更管理ステータステーブルである見ることができます。ロールバックが発生したサイトに対応する構成エラーまたはソフトウェアエラー が表示されます。

設定とソフトウェアの両方がロールバックされますか?

はい。構成とともにソフトウェアのアップグレードも実行され、ロールバックシナリオが発生すると、ソフトウェアもロールバックされます。

MCN に問題があり、すべてのサイトとの接続がクラッシュまたは切断された場合、どうなりますか。

MCN 以外のネットワーク全体がロールバックされます。通知が表示され、すべてのサイトの変更管理セクションにロールバック状態が表示されます。MCN の問題は手動で解決できます。

この機能を無効にすることはできますか?

はい、アクティブ化する直前にこの機能を無効にすることができます。ただし、この機能はデフォルトで有効になっています。

多層ネットワークがある場合、ロールバックは部分的なソフトウェアアップグレードとどのように相互作用しますか?

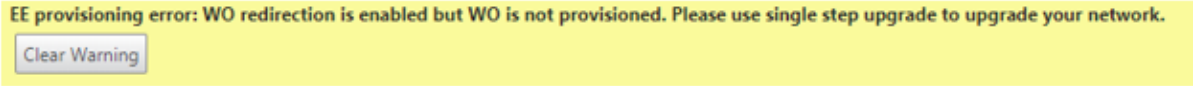
- 部分的なソフトウェアアップグレードが無効で、リージョン（または RCN）のサイトがロールバックすると、問題のあるリージョンがロールバックされ、完了すると、ロールバックは MCN に伝播されます。その結果、MCN とネットワークの残りの部分がロールバックされます。ロールバックしたリージョンの RCN と MCN の両方に、MCN が RCN でロールバックバナーを自動的に閉じることができないロールバックバナーが表示されます。
- 部分的なソフトウェアアップグレードが有効で、リージョン (または RCN) のサイトがロールバックされると、そのリージョンだけがロールバックされます。ロールバックイベントは MCN に伝播されません。その結果、

MCN は地域を離れます。MCN はロールバックバナーを表示せず、自身またはネットワークをロールバックしません。

どちらのシナリオでも、RCN はロールバックのバナーを表示します。なぜなら、MCN では自動解除できないからです。

2100 Premium（エンタープライズ）エディション

2100 EE アプライアンスがリリース 10.0 にアップグレードされた場合、次のメッセージは何を示していますか。



アプライアンスに EE ライセンスがあるか、MCN から WANOP リダイレクトが有効になっています。WANOP コンポーネントのインストールをスケジュールして、このプラットフォームで WANOP 機能の Provisioning を開始できます。

関連情報

- LTE を介したゼロタッチ展開
- HA でのセカンダリ MCN の設定

参考資料

May 10, 2021

アプリケーション署名ライブラリ

Citrix SD-WAN アプライアンスがディープパケットインスペクションを使用して識別できるアプリケーションのリストです。