Cisco Secure Firewall でのブランチおよび WAN の簡素化の使用例

初版：2023 年 4 月 4 日

最終更新：2023 年 8 月 2 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

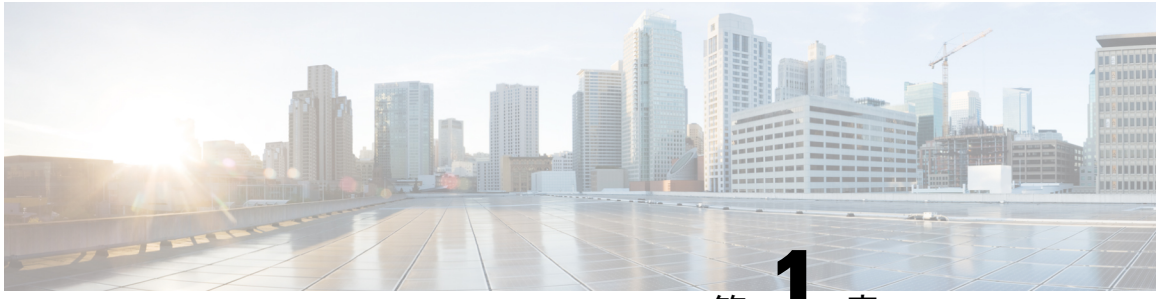
Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2023 Cisco Systems, Inc. All rights reserved.

目 次



第 1 章

使用する前に

この章では、Cisco Secure Firewall の機能と、サポートされているブランチおよび WAN の機能の概要について説明します。

この資料について

このガイドでは、Cisco Secure Firewall でサポートされているブランチおよび WAN の機能を使用する主な使用例について詳しく説明します。

各アプローチは、ネットワークで考えられるすべてのニーズに対応するものではありません。ネットワークを構築するときのモデルとして使用してください。例で示されている機能を使用せずに、実際のニーズに合うように機能を追加したり置き換えたりすることもできます。

このガイドは、Cisco Secure Firewall に精通していることを前提としています。設定の詳細については、『Cisco Secure Firewall Management Center Administration Guide, 7.3』および『Cisco Secure Firewall Management Center Device Configuration Guide, 7.3』を参照してください。

Cisco Secure Firewall

Cisco Secure Firewall は、Snort IPS、URL フィルタリング、マルウェア防御などの最先端機能を備えた、非常に堅牢なファイアウォール ソリューションです。

この包括的な製品により、物理、プライベート、およびパブリッククラウド環境で一貫したセキュリティポリシーを適用することで、脅威からの保護が大幅に簡素化されます。

さらに、ネットワークインフラストラクチャを広範囲に可視化し、潜在的な脅威の発生源とアクティビティを迅速に特定します。この情報を活用することで、攻撃によって運用が中断される前に、攻撃を阻止するための措置を迅速に講じることができます。

従来のファイアウォール機能に加えて、次の機能が提供されます。

1. アプリケーションの可視化と制御
2. ユーザーアイデンティティの認識と制御
3. 侵入防止と侵入検知
4. SSL/TLS の復号
5. レピュテーションベースのブロッキング
6. ファイルとマルウェアの防御
7. バーチャル プライベート ネットワーク（VPN）

ネットワーク展開のセキュリティを向上させるために、Cisco Secure Firewall は、以降のリリースで次のような追加のセキュリティ機能を提供します。

- 暗号化された可視性エンジン（EVE）。完全な中央のメインシステム（MITM）の復号を導入することなく、暗号化されたトラフィックの検査を強化します。
- エレファントフローの検出。エレファントフロー（通常は 1 GB/10 秒を超えるフロー）を検出して修復し、高い CPU 使用率とパケットドロップを回避します。
- Cisco Secure Dynamic Attribute Connector（CSDAC）。従来の IP/ネットワークベースのポリシー設定ではなく、ポリシー設定用のタグとラベルを活用することで、セキュリティポリシー管理に俊敏性とインテリジェンスをもたらします。

ブランチの簡素化の概要

組織が複数のブランチロケーションに業務を拡大するにつれて、セキュアで合理化された接続を確保することが最優先されるようになります。セキュアなブランチ ネットワーク インフラストラクチャを展開するには、複雑な設定と管理のプロセスが必要です。これには時間がかかり、適切に処理しないとセキュリティの脆弱性が発生しやすくなります。ただし、組織はセキュアなファイアウォール ソリューションを活用して、簡素化されたセキュアなブランチ展開を実現することで、これらの課題を克服できます。

このガイドでは、堅牢なファイアウォール ソリューションを使用した、セキュアなブランチ展開の簡素化の概念について説明します。セキュアなファイアウォールをブランチ ネットワーク アーキテクチャの基本コンポーネントとして統合することで、組織は展開プロセスを簡素化しながら、強力なセキュリティベースラインを確立することができます。このアプローチにより、組織は統合されたセキュリティポリシーを適用し、トラフィックルーティングを最適化し、復元力のある接続を確保することができます。

Cisco Secure Firewall でサポートされているブランチおよび WAN の簡素化機能の一部を次に示します。

- **セキュアで柔軟な接続**：
  - 本社（ハブ）とブランチ（スポーク）の間のルートベース（VTI）VPN トンネル
  - VTI を介した IPv4 および IPv6 BGP、IPv4 および IPv6 OSPFv2/v3、IPv4 EIGRP

- スタティックまたはダイナミック IP を持つスポークのための DVTI のサポート

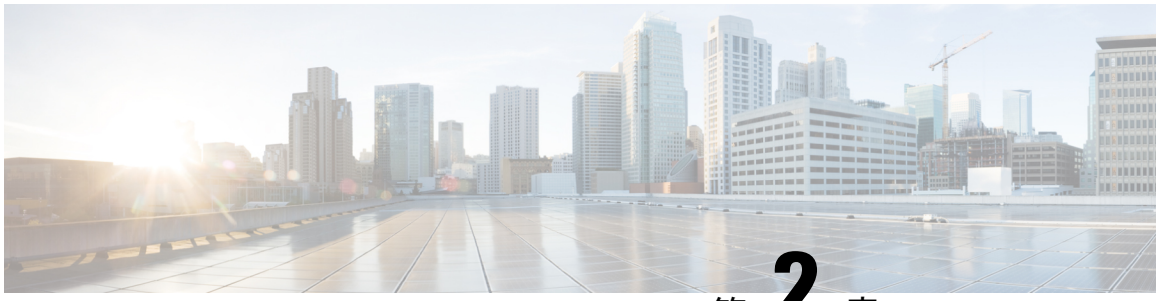
- **ネットワークのダウンタイムがほぼゼロの高可用性**：
  - デュアル ISP 設定
  - アプリケーションベースのインターフェイス モニタリングに基づく最適なパス選択
- **使用可能帯域幅の増加**：
  - 複数の ISP にまたがるロードバランシングのための ECMP のサポート
  - SVTI のための ECMP のサポート
  - PBR を使用したアプリケーションベースのロードバランシング
- **パブリッククラウドおよびゲストユーザーのダイレクト インターネット アクセス**：
  - 一致基準としてアプリケーションを使用したポリシーベースルーティング
  - Cisco Umbrella のためのローカルトンネル ID のサポート
- **シンプルな管理**：
  - SASE：Cisco Umbrella 自動トンネルの展開
  - DVTI ハブスポークトポロジの簡素化

機能

次の表に、一般的に使用される WAN 機能の一部を示します

機能	導入されたリリース
VTI のループバック インターフェイス サポート	リリース 7.3
サイト間 VPN を使用したダイナミック VTI（DVTI）のサポート	リリース 7.3
Cisco Umbrella 自動トンネル	リリース 7.3
VTI の IPv4 および IPv6 BGP、IPv4 および IPv6 OSPFv2/v3、IPv4 EIGRP のサポート	リリース 7.3
ハブアンドスポークトポロジを使用したルートベースのサイト間 VPN	リリース 7.2
パスのモニタリングによるポリシーベースのルーティング	リリース 7.2
サイト間 VPN 監視ダッシュボード	リリース 7.1

機能	導入されたリリース
ダイレクト インターネット アクセス/ポリシーベースルーティング	リリース 7.1
WAN インターフェイスを使用した Equal-Cost-Multi-Path（ECMP）ゾーン	リリース 7.1
VTI インターフェイスを使用した Equal-Cost-Multi-Path（ECMP）ゾーン	リリース 7.1
ルートベースのサイト間 VPN 向けバックアップ用 VTI	リリース 7.0
サイト間 VPN を使用したスタティック VTI（SVTI）のサポート	リリース 6.7



第 2 章

ダイナミック仮想トンネルインターフェイス（DVTI）を使用したブランチからハブへの通信の簡素化

この章では、ハブアンドスポークトポロジでの DVTI の実践的な応用について詳しく説明します。この使用例では、シナリオ、ネットワークトポロジ、ベストプラクティス、および前提条件について詳しく説明します。また、シームレスな導入のための包括的なエンドツーエンドの手順も提供します。

ハブアンドスポークトポロジでのルートベースの VPN

Cisco Secure Firewall Management Center は、仮想トンネルインターフェイス（VTI）と呼ばれるルーティング可能な論理インターフェイスをサポートしています。このインターフェイスを使用して、スタティックおよびダイナミック ルーティング ポリシーを適用できます。VTI を使用すると、静的暗号マップのアクセスリストを設定してインターフェイスにマッピングする必要がなくなります。すべてのリモート サブネットを追跡し、暗号マップのアクセス リストに含める必要がなくなります。

VTI を使用してピア間に VPN トンネルを作成できます。VTI は、各トンネルの終端に IPsec プロファイルが付加されたルートベースの VPN をサポートします。VTI ではスタティックまたはダイナミックルートが使用されます。Threat Defense デバイスは、トンネルインターフェイスとの間のトラフィックを暗号化または復号し、ルーティングテーブルに従って転送します。

Management Center は、VTI またはルートベースの VPN を設定するためのデフォルトのサイト間 VPN ウィザードをサポートしています。

ハブアンドスポークトポロジでルートベースの VPN を導入する場合、ダイナミック仮想トンネルインターフェイス（DVTI）はハブで設定され、スタティック仮想トンネルインターフェイス（SVTI）はスポークで設定されます。

ダイナミック VTI では、IPsecインターフェイスの動的なインスタンス化および管理のために、仮想テンプレートが使用されます。仮想テンプレートは、VPNセッションごとに固有の仮想アクセスインターフェイスを動的に生成します。ダイナミック VTI は、複数の IPsec セキュリティアソシエーションをサポートし、スポークによって提案された複数の IPsec セレクターを受け入れます。

Cisco Secure Firewall Threat Defense は、ルートベース（VTI）VPN のバックアップトンネルの設定をサポートし、リンクの冗長性を提供します。プライマリ VTI（プライマリトンネル）がトラフィックをルーティングできない場合、VPN内のトラフィックはバックアップVTI（セカンダリトンネル）を介してトンネリングされます。

利点

ハブアンドスポークトポロジで VTI ベースの VPN を使用する利点は次のとおりです。

1. **設定の簡素化**：VTIは、トンネル自体を表す論理インターフェイスを提供することで、VPN トンネルの設定を簡素化します。これにより、通常は従来の VPN 設定に伴う複雑なクリプトマップまたはアクセスリストの設定が不要になります。
2. **管理の簡素化**：大企業のハブアンドスポーク展開のピア設定を簡単に管理できます。スポークで設定された複数のスタティック VTI に対して、ハブでは 1 つのダイナミック VTI のみが設定されます。
3. **拡張性**：VTI により、簡単に拡張することができます。新しいスポークを追加しても、ハブで追加の VPN 設定を行う必要はありません。設定によっては、NAT およびルーティングの設定の更新が必要になる場合があります。

4. **ダイナミックルーティングのサポート**：VTI は、Open Shortest Path First（OSPF）などのダイナミック ルーティング プロトコルをサポートしているため、VPN エンドポイント間でルーティング情報をダイナミックに交換できます。これにより、リアルタイムのネットワーク状態に基づいた効率的なルーティングの決定が可能になります。
5. **デュアル ISP の冗長性**：SVTI はバックアップ VTI トンネルをサポートしています。
6. **ロードバランシング**：SVTI は ECMP を使用した VPN トラフィックのロードバランシングをサポートしています。

この使用例の対象者

このDVTIハブアンドスポーク設定の対象者には、組織のネットワーク インフラストラクチャの設計と管理を担当するネットワークアーキテクト、IT管理者、およびネットワーク技術者が含まれます。この使用例は、リモートスポークサイトに接続するセキュアなトンネルを備えた集中型ハブを導入することで、ネットワーク接続の最適化、データセキュリティの確保、およびネットワーク管理の合理化を求めるユーザーのために役立ちます。

シナリオ

複数の都市に複数の分散拠点を持つ中規模企業が、これらのブランチを中央の本社と接続するためのセキュアで効率的なネットワーク インフラストラクチャを確立したいと考えています。会社の IT 管理者である Alice が、ネットワークの設定と管理を担当しています。

リスクがあるもの

現在のネットワーク設定では、各分散拠点と中央の本社の間にある複数のポイントツーポイント接続を手動で設定する必要があります。このアプローチは時間がかかり、エラーが発生しやすく、すべての場所でネットワーク設定の一貫性を維持することが困難です。Alice は、設定プロセスを簡素化し、集中管理を提供するソリューションを必要としています。

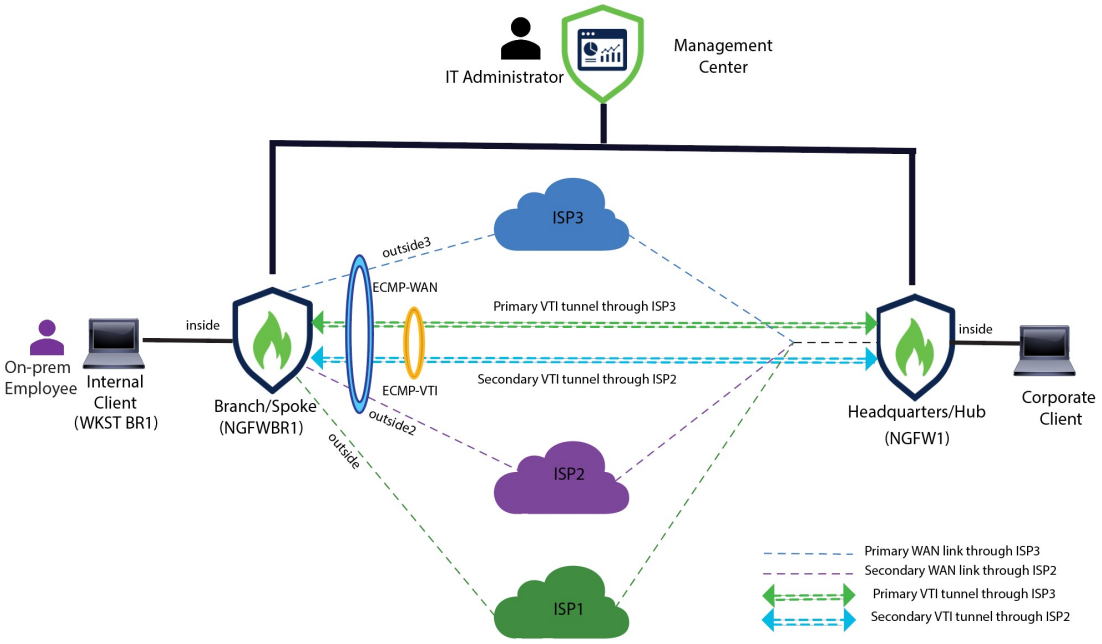
ブランチ（スポーク）と本社（ハブ）の間のルートベース VPN による問題の解決方法

1. 集中型設定：AliceはDVTIハブアンドスポークトポロジを導入し、ハブでの設定と管理を一元化します。これにより、すべての場所でのネットワーク設定が簡素化されます。
2. ダイナミックルーティング：Alice はルーティング情報の交換を自動化するダイナミック ルーティング プロトコル（OSPF など）を設定します。スタティックルートの手動設定が不要になり、ネットワーク管理が簡素化されます。
3. 迅速なプロビジョニング：DVTI により、Alice はスポークルータを設定し、ハブとのセキュアなトンネルを確立することで、新しい分散拠点を迅速にプロビジョニングできます。これにより、プロビジョニングプロセスが簡素化され、ネットワークの拡張性がサポートされます。

DVTIを導入することで、Aliceはネットワーク設定を簡素化し、管理を一元化し、一貫性を確保し、企業のネットワークでの効率的なプロビジョニングと拡張性を実現します。

ネットワーク トポロジ

このハブスポークトポロジでは、Threat Defense デバイスがブランチロケーションに展開されます。次の図では、内部クライアントまたはブランチワークステーションには WKST BR というラベルが付けられ、ブランチ（スポーク）の Threat Defense には NGFWBR1 というラベルが付けられています。本社（ハブ）は NGFW1 としてラベル付けされ、企業のネットワークに接続されています。VPN トンネルは NGFWBR1 と NGFW1 の間に設定されます。リンクの冗長性と VPN トラフィックのロードバランシングのために、ブランチノードのプライマリおよびセカンダリのスタティック VTI インターフェイスで ECMP ゾーンが設定されます。



ベストプラクティス

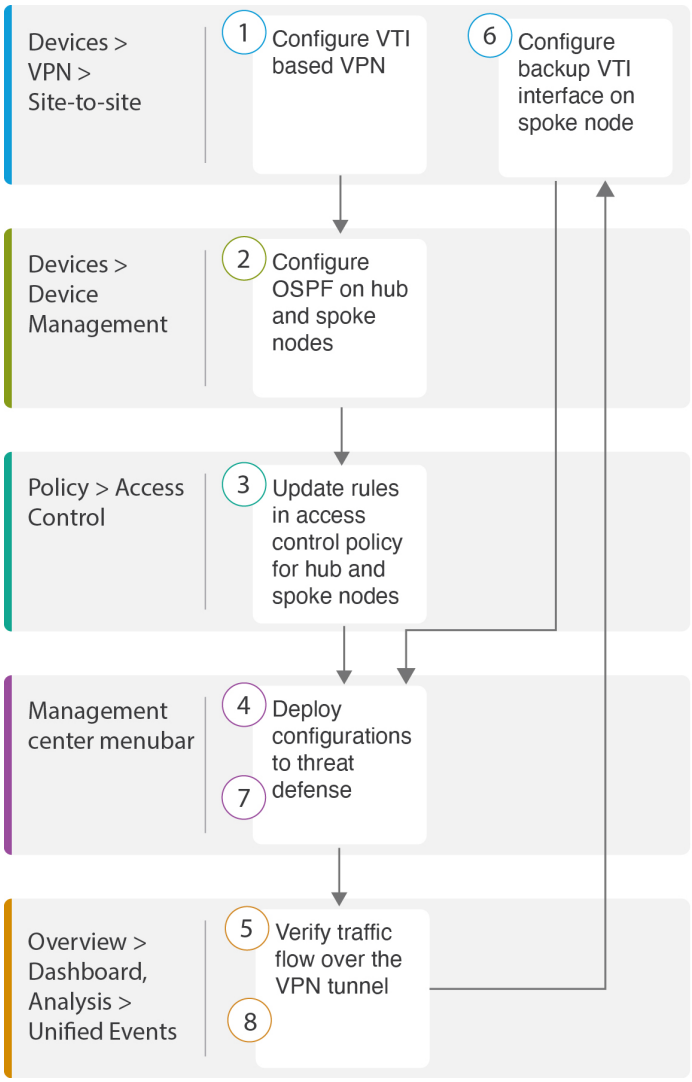
- Cisco Secure Firewall Threat Defense がバージョン 6.7 以降で実行されていることを確認します。
- VTI はルーテッドモードのみでサポートされています。
- ループバック インターフェイスから動的インターフェイスの借用 IP を設定します。
- VTI 経由のトラフィックを制御するために、VTI インターフェイスにアクセスルールを適用していることを確認します。
- VTI トラフィックをロードバランシングするために、SVTI の ECMP ゾーンを設定します。

前提条件

- Device Manager を使用した Threat Defense の初期設定の完了
- デバイスへのライセンスの割り当て
- インターネットアクセスのルートの追加。「スタティックルートの追加」を参照してください
- 脅威に対する防御のための NAT の設定
- 基本的なアクセス コントロール ポリシーの作成

ルートベース VPN（ハブアンドスポークトポロジ）を設定するためのエンドツーエンドの手順

次のフローチャートは、Cisco Secure Firewall Management Center でハブスポークトポロジのルートベース VPN を設定するためのワークフローを示しています。



ステップ	説明
1	VTI ベースの VPN を設定します。参照先 • ルートベースのサイト間 VPN の作成 （11 ページ） • ハブノードのエンドポイントの設定 （12 ページ） • スポークノードのエンドポイントの設定 （14 ページ）
2	ハブノードとスポークノードで OSPF を設定します。参照先 • ハブノードでの OSPF の設定 （16 ページ） • スポークノードでの OSPF の設定 （18 ページ）

ステップ	説明
3	ハブノードとスポークノードのアクセス コントロール ポリシーのルールを更新します。アクセス コントロール ポリシーの設定 （20 ページ）を参照してください。
4	設定を Threat Defense に展開します。設定の展開 （23 ページ）を参照してください。
5	VPN トンネルを介したトラフィックフローを確認します。VPN トンネルを介したトラフィックフローの確認 （23 ページ）を参照してください。
6	スポークノードでバックアップ VTI を設定します。スポークノードでのバックアップ VTI インターフェイスの設定 （27 ページ）を参照してください。
7	設定を Threat Defense に展開します。設定の展開 （23 ページ）を参照してください。
8	セカンダリトンネルを介したトラフィックフローを確認します。プライマリトンネルとセカンダリトンネルの確認 （30 ページ） を参照してください。

ルートベースのサイト間 VPN の作成

2 つのノード間にルートベースのサイト間 VPN を設定できます。VTI ベースの VPN を設定するには、トンネルの両方のノードに仮想トンネルインターフェイスが必要です。

管理対象スポークの場合、プライマリ VTIインターフェイスとともにバックアップのスタティック VTI インターフェイスを設定できます。

ステップ 1 [デバイス（Devices）] > [VPN] > [サイト間（Site To Site）] を選択します。

ステップ 2 [トポロジ名（Topology Name）] フィールドに名前として **Corporate-VPN** と入力します。

ステップ 3 トポロジタイプとして [ルートベース（VTI）（Route Based (VTI)）] を選択します。

ステップ 4 ハブノードのエンドポイントを設定します。ハブノードのエンドポイントの設定 （12 ページ）を参照してください。

ステップ 5 スポークノードのエンドポイントを設定します。スポークノードのエンドポイントの設定 （14 ページ）を参照してください。

ステップ 6 [IKE]、[IPsec]、および [詳細設定（Advanced）] タブでは、デフォルト設定が使用されます。

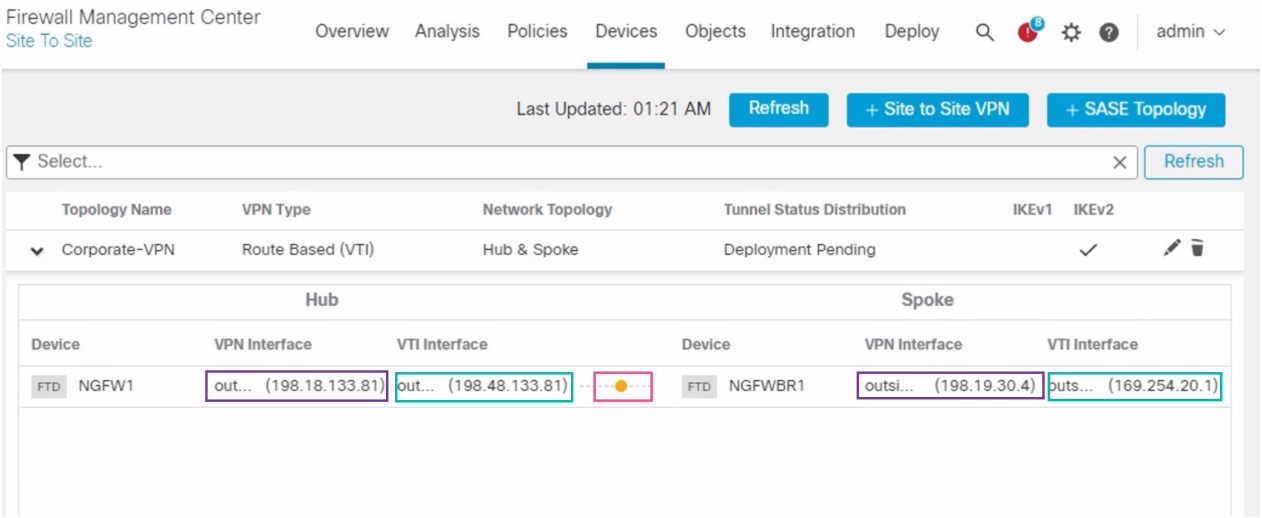
ステップ 7 [保存（Save）] をクリックします。

Corporate-VPN トポロジが正常に作成されます。

ステップ 8 [デバイス（Devices）]>[サイト間VPN（Site-to-site VPN）]に移動すると、[サイト間VPN（Site-to-site VPN）]の一覧ページで VPN トポロジを表示できます。

（注） 作成した VPN トポロジが表示されない場合は、[更新（Refresh）] をクリックします。

ステップ 9 [Corporate-VPN] ノードを展開して、トポロジ内のすべてのトンネルを表示します。**NGFW1** ハブと **NGFWBR1** スポークが、物理ソースと VTI インターフェイスの詳細とともに表示されます。設定がまだ展開されていないため、[導入保留中（Deployment Pending）]と表示され、トンネルのステータスがオレンジで表示されます。



次のタスク

両方のデバイスで VTI インターフェイスと VTI トンネルを設定したら、次のものを設定する必要があります。

- VTI トンネルを介してデバイス間で VTI トラフィックをルーティングするルーティングプロトコル。ハブノードでの OSPF の設定 （16 ページ）およびスポークノードでの OSPF の設定 （18 ページ）を参照してください。
- 暗号化されたトラフィックを許可するアクセスコントロールルール。アクセス コントロール ポリシーの設定 （20 ページ） を参照してください。

ハブノードのエンドポイントの設定

トンネルタイプを「ダイナミック」として指定し、関連パラメータを設定すると、Management Center はダイナミック仮想テンプレートを生成します。仮想テンプレートは、VPN セッションごとに固有の仮想アクセスインターフェイスを動的に生成します。

ステップ 1 [ハブノード（Hub Nodes）] セクションで、[+] をクリックします。[エンドポイントの追加（Add Endpoint）] ダイアログボックスが表示されます。

ステップ 2 [デバイス（Device）] ドロップダウンリストからハブとして [NGFW1] を選択します。

（注） ソフトウェアバージョン 7.3 以降で実行されているデバイスである必要があります。

ステップ 3 [ダイナミック仮想トンネルインターフェイス（Dynamic Virtual Tunnel Interface）] ドロップダウンリストの横にある [+] をクリックして新しいダイナミック VTI を追加します。

[仮想トンネルインターフェイスの追加（Add Virtual Tunnel Interface）] ダイアログボックスが表示され、次の事前入力されたデフォルト設定が示されます。

- [トンネルタイプ（Tunnel Type）] には [ダイナミック（Dynamic）] が自動的に入力されます。
- [名前（Name）] は <*tunnel_source interface logical name*>+ dynamic_vti +<*tunnel ID*> として自動入力されます。たとえば、**outside_dynamic_vti_1** となります。
- [有効（Enabled）] チェックボックスはデフォルトでオンになります。
- [セキュリティゾーン（Security Zone）]：このインターフェイスのセキュリティゾーンを定義するには、ドロップダウンリストから [新規…（New…）] を選択します。[新規セキュリティゾーン（New Security Zone）] ダイアログボックスで名前として **Tunnel_Zone** と入力し、[OK] をクリックします。このトンネルインターフェイスのセキュリティゾーンとして [Tunnel_Zone] を選択します。
- [テンプレートID（Template ID）] には、DVTI インターフェイスの一意の ID が自動入力されます。
- [トンネルの送信元（Tunnel Source）] は、DVTI の送信元である物理インターフェイスであり、デフォルトで自動入力されます。この使用例では、DVTI の明示的なトンネルの送信元を設定しません。ドロップダウンリストから [インターフェイスの選択（Select Interface）] を選択して、選択をクリアします。
- [IPsecトンネルモード（IPsec Tunnel Mode）] は、デフォルトでは IPv4 に設定されます。
- DVTI はテンプレート インターフェイスであるため、[IPアドレス（IP address）] をスタティック IP アドレスにすることはできません。ループバック インターフェイスから動的インターフェイスの借用 IP を設定することをお勧めします。ループバック インターフェイスを追加するには、[IPの借用（IPアンナンバード）（Borrow IP (IP unnumbered)）] ドロップダウンリストの横にある [+] をクリックします。[ループバックインターフェイスの追加（Add Loopback Interface）] ダイアログボックスで、次の手順を実行します。

  1. [全般（General）] タブで、[名前（Name）] を **HUB_Tunnel_IP**、[ループバックID（Loopback ID）] を **1** として入力します。
  2. [IPv4] タブで、IP アドレスを **198.48.133.81/32** として入力します。
  3. [OK] をクリックして、ループバック インターフェイスを保存します。

  [IPの借用（Borrow IP）] は [ループバック1（HUB_Tunnel_IP）（Loopback 1(HUB_Tunnel_IP)）] に設定されます。

[OK] をクリックして、DVTI を保存します。VTI が正常に作成されたことを確認するメッセージが表示されます。[OK] をクリック

[ダイナミック仮想トンネルインターフェイス（Dynamic Virtual Tunnel Interface）] は [outside_dynamic_vti_1（198.48.133.81）（outside_dynamic_vti_1(198.48.133.81)）] に設定されます。

ステップ 4 [トンネルの送信元（Tunnel Source）] ドロップダウンリストから [GigabitEthernet 0/0（outside）（GigabitEthernet 0/0 (outside)）] を選択します。外部インターフェイスの IP アドレス（**198.18.133.81**）が次のフィールドに自動入力されます。

ステップ 5 [詳細設定（Advanced Settings）] を展開して、デフォルト設定を表示します。

ステップ 6 [OK] をクリック

NGFW1 がハブノードとして正常に設定されました。

スポークノードのエンドポイントの設定

ステップ 1 [スポークノード（Spoke Nodes）] セクションで、[+] をクリックします。[エンドポイントの追加（Add Endpoint）] ダイアログボックスが表示されます。

ステップ 2 [デバイス（Device）] ドロップダウンリストからハブとして [NGFWBR1] を選択します。

（注） ソフトウェアバージョン 7.3 以降で実行されているデバイスである必要があります。

ステップ 3 [スタティック仮想トンネルインターフェイス（Static Virtual Tunnel Interface）] ドロップダウンリストの横にある [+] をクリックして新しいスタティック VTI を追加します。

[仮想トンネルインターフェイスの追加（Add Virtual Tunnel Interface）] ダイアログボックスが表示され、次の事前入力されたデフォルト設定が示されます。

- [トンネルタイプ（Tunnel Type）] には [スタティック（Static）] が自動的に入力されます。
- [名前（Name）] は <*tunnel_source interface logical name*>+ static_vti +<*tunnel ID*> として自動入力されます。たとえば、**outside_static_vti_1** となります。
- [有効（Enabled）] チェックボックスはデフォルトでオンになります。
- [セキュリティゾーン（Security Zone）] ドロップダウンリストから [Tunnel_Zone] を選択します。
- [トンネルID（Tunnel ID）] には、1 の値が自動入力されます。
- [トンネルの送信元（Tunnel Source）] ドロップダウンリストから [GigabitEthernet0/4（outside3）（GigabitEthernet0/4 (outside3)）] を選択します。その横にあるドロップダウンリストから、outside3 インターフェイスの IP アドレスとして [198.19.30.4] を選択します。
- [IPsecトンネルモード（IPsec Tunnel Mode）] は、デフォルトでは IPv4 に設定されます。

- [IPアドレス（IP address）] は、スタティック IP アドレスまたは借用 IP のいずれかです。ループバック インターフェイスから静的インターフェイスの借用 IP を設定することをお勧めします。ループバック インターフェイスを追加するには、[IPの借用（IPアンナンバード）（Borrow IP (IP unnumbered)）] ドロップダウンリストの横にある [+] をクリックします。[ループバックインターフェイスの追加（Add Loopback Interface）] ダイアログボックスで、次の手順を実行します。

  1. [全般（General）] タブで、[名前（Name）] を **Spoke_Tunnel_IP**、[ループバック ID（Loopback ID）] を **1** として入力します。
  2. [IPv4] タブで、IP アドレスを **169.254.20.1/32** として入力します。
  3. [OK] をクリックして、ループバック インターフェイスを保存します。

  [IPの借用（Borrow IP）] は [ループバック 1（Spoke_Tunnel_IP）（Loopback 1(Spoke_Tunnel_IP)）] に設定されます。

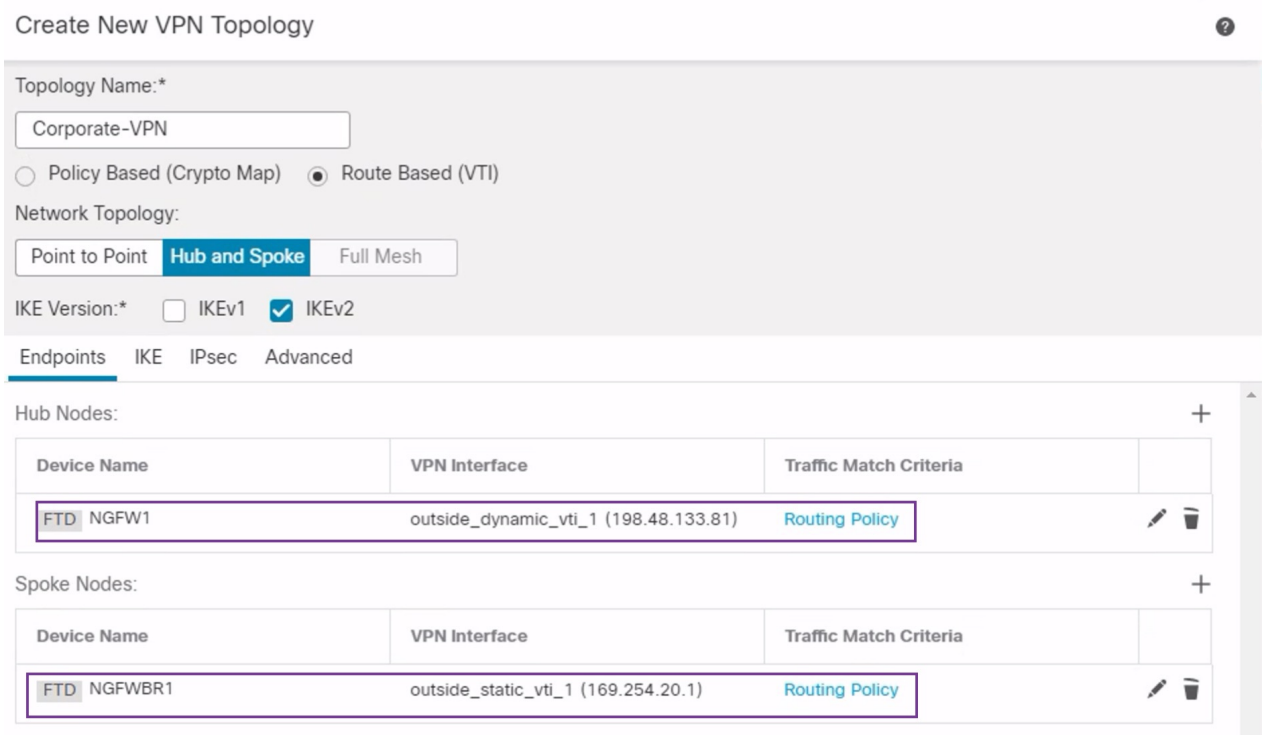
[OK] をクリックして、SVTI を保存します。VTI が正常に作成されたことを確認するメッセージが表示されます。[OK] をクリック

スタティック仮想トンネルインターフェイスが [outside_static_vti_1（169.254.20.1）（outside_static_vti_1(169.254.20.1)）] に設定されます。

ステップ 4 [詳細設定（Advanced Settings）] を展開して、デフォルト設定を表示します。両方のチェックボックスをオンにする必要があります。

ステップ 5 [OK] をクリック

NGFWBR1 がスポークノードとして正常に設定されました。



ハブノードでの OSPF の設定

OSPF は、VPN トンネルを介してトラフィックを送信できるように、ハブとスポークのデバイス間で設定されます。参考までに、スタティックルーティングはアンダーレイであり、その上にスポークからハブへのトンネルが確立され、OSPF はオーバーレイと見なされます。

ステップ 1 ハブノードを編集するには、[デバイス（Devices）] > [デバイス管理（Device Management）] を選択し、NGFW1 ノードの [編集（Edit）]（✎） アイコンをクリックします。

ステップ 2 [インターフェイス（Interfaces）] タブで、以前に作成された、DVTI インターフェイスの IP アドレスとして機能する **Loopback1** インターフェイスを確認します。

ステップ 3 [Routing] をクリックします。

ステップ 4 左側のパネルで [OSPF] をクリックします。

ステップ 5 [プロセス1（Process 1）] チェックボックスをオンにして、OSPF インスタンスを有効にします。

ステップ 6 [インターフェイス（Interface）] タブをクリックします。

ステップ 7 [追加（Add）] をクリックします。[Add Interface] ダイアログボックスが表示されます。次のフィールドを変更します。

- [インターフェイス（Interface）]：ドロップダウンリストから DVTI インターフェイスの [outside_dynamic_vti_1] を選択します。

- [ポイントツーポイント（Point-to-point）]：このチェックボックスをオンにして、VPN トンネル経由で OSPF ルートを送信します。

  残りのフィールドではデフォルト値を使用します。

- [OK] をクリック

[インターフェイス（Interface）] タブに **outside_dynamic_vti_1** の行が追加されます。

ステップ 8 [エリア（Area）] タブをクリックします。

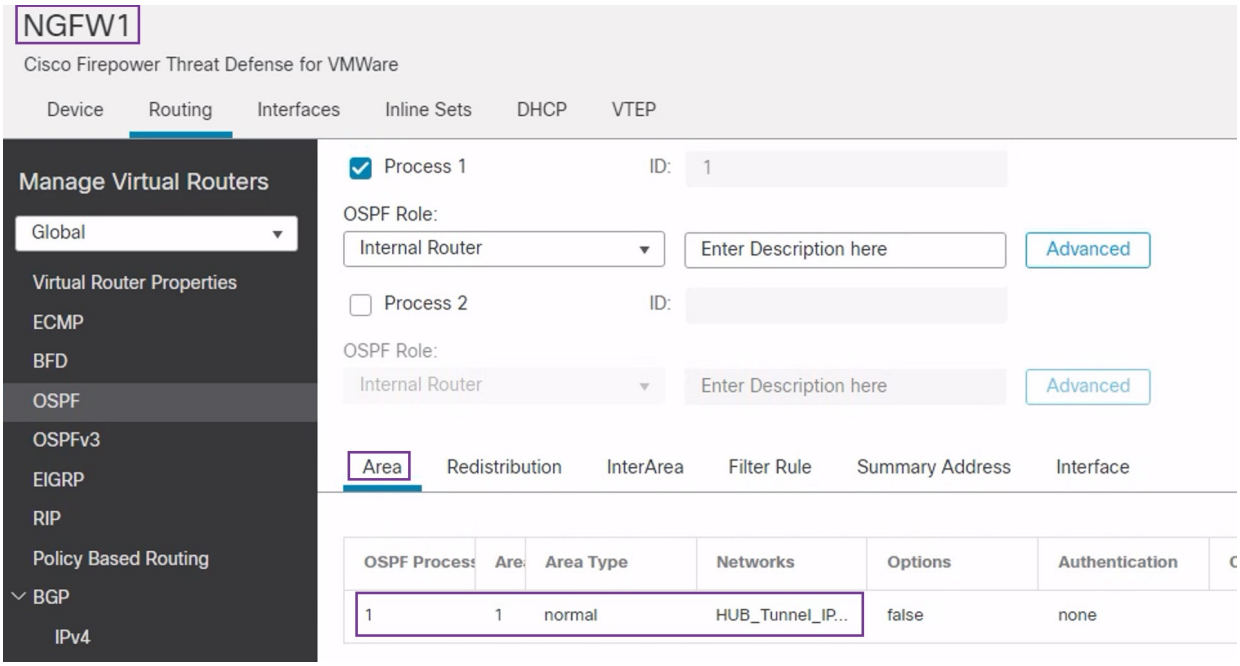
ステップ 9 [追加（Add）] をクリックします。[エリアの追加（Add Area）] ダイアログボックスが表示されます。次のフィールドを変更します。

- [OSPFプロセス（OSPF Process）]：プロセス ID として 1 を選択します。
- [エリアID（Area ID）]：値が 1 であることを確認します。

  残りのフィールドではデフォルト値を使用します。

- [使用可能なネットワーク（Available Network）]：トンネルを介してアドバタイズされるネットワークを追加するために、次の手順を実行します。
  - 新しいネットワークオブジェクトを追加するには、＋をクリックします。次の詳細を入力します。
    - [名前（Name）]：名前として **HUB_Tunnel_IP** と入力します。
    - [ネットワーク（Network）]：[ホスト（Host）] オプションを選択し、ホスト IP として **198.48.133.81** と入力します。
    - [保存（Save）] をクリックします。
  - [使用可能なネットワーク（Available Network）] フィールドの検索エリアに **HUB** と入力します。新しく追加されたネットワークオブジェクト（**HUB_Tunnel_IP**）が表示されます。このオブジェクトを選択して [追加（Add）] をクリックし、[選択したネットワーク（Selected Network）] リストに追加します。
  - [使用可能なネットワーク（Available Network）] フィールドの検索エリアに **Corporate** と入力します。**Corporate_LAN** ネットワークオブジェクトが表示されます。このオブジェクトを選択して [追加（Add）] をクリックし、[選択したネットワーク（Selected Network）] リストに追加します。
- [OK] をクリック

[エリア（Area）] タブに行が追加されます。



ステップ 10 [保存（Save）] をクリックして、ハブノードの OSPF 設定を保存します。

スポークノードでの OSPF の設定

ステップ 1 スポークノードを編集するには、[デバイス（Devices）]>[デバイス管理（Device Management）] を選択し、NGFWBR1 ノードの [編集（Edit）]（✎） アイコンをクリックします。

ステップ 2 [インターフェイス（Interfaces）] タブで、次の手順を実行します。

- スポーク設定で以前に作成された **Tunnel1** インターフェイスの詳細を確認します。
- 以前に作成された、Tunnel1 の IP アドレスとして機能する **Loopback1** インターフェイスの詳細を確認します。

ステップ 3 [Routing] をクリックします。

ステップ 4 左側のパネルで [OSPF] をクリックします。

ステップ 5 [プロセス1（Process 1）] チェックボックスをオンにして、OSPF インスタンスを有効にします。

ステップ 6 [エリア（Area）] タブをクリックします。

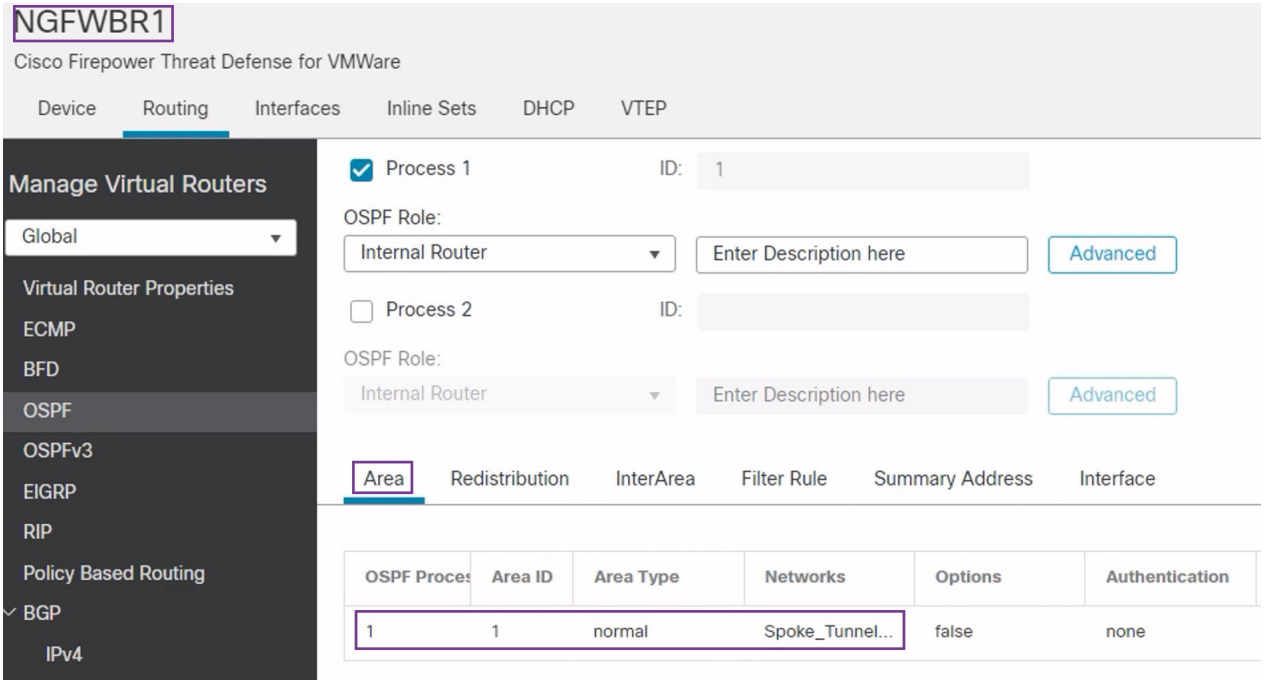
ステップ 7 [追加（Add）] をクリックします。[エリアの追加（Add Area）] ダイアログボックスが表示されます。次のフィールドを変更します。

- [OSPFプロセス（OSPF Process）]：プロセス ID として 1 を選択します。
- [エリアID（Area ID）]：値が 1 であることを確認します。

残りのフィールドではデフォルト値を使用します。

- [使用可能なネットワーク（Available Network）]：トンネルを介してアドバタイズされるネットワークを追加するために、次の手順を実行します。
  - 新しいネットワークオブジェクトを追加するには、＋をクリックします。次の詳細を入力します。
    - [名前（Name）]：名前として **Spoke_Tunnel_IP** と入力します。
    - [ネットワーク（Network）]：[ホスト（Host）] オプションを選択し、ホスト IP として **169.254.20.1** と入力します。
    - [保存（Save）] をクリックします。
  - [使用可能なネットワーク（Available Network）] フィールドの検索エリアに **Spoke** と入力します。新しく追加されたネットワークオブジェクト（**Spoke_Tunnel_IP**）が表示されます。このオブジェクトを選択して [追加（Add）] をクリックし、[選択したネットワーク（Selected Network）] リストに追加します。
  - [使用可能なネットワーク（Available Network）] フィールドの検索エリアに **Branch** と入力します。**Branch_LAN** ネットワークオブジェクトが表示されます。このオブジェクトを選択して [追加（Add）] をクリックし、[選択したネットワーク（Selected Network）] リストに追加します。
- [OK] をクリック

[エリア（Area）] タブに行が追加されます。



ステップ 8 [保存（Save）] をクリックして、スポークノードの OSPF 設定を保存します。

アクセス コントロール ポリシーの設定

続行する前に、**NGFW1** ノードと **NGFWBR1** ノードの VTI インターフェイスが、**Tunnel_Zone** というラベルの付いた新しいゾーンに関連付けられていることを確認します。

[ポリシー（Policies）]>[アクセス制御（Access Control）] に移動して、アクセス コントロール ポリシーを確認します。トンネルとの間の VPN トラフィックを許可するには、ハブとスポークの両方で次のアクセス コントロール ポリシーを更新する必要があります。

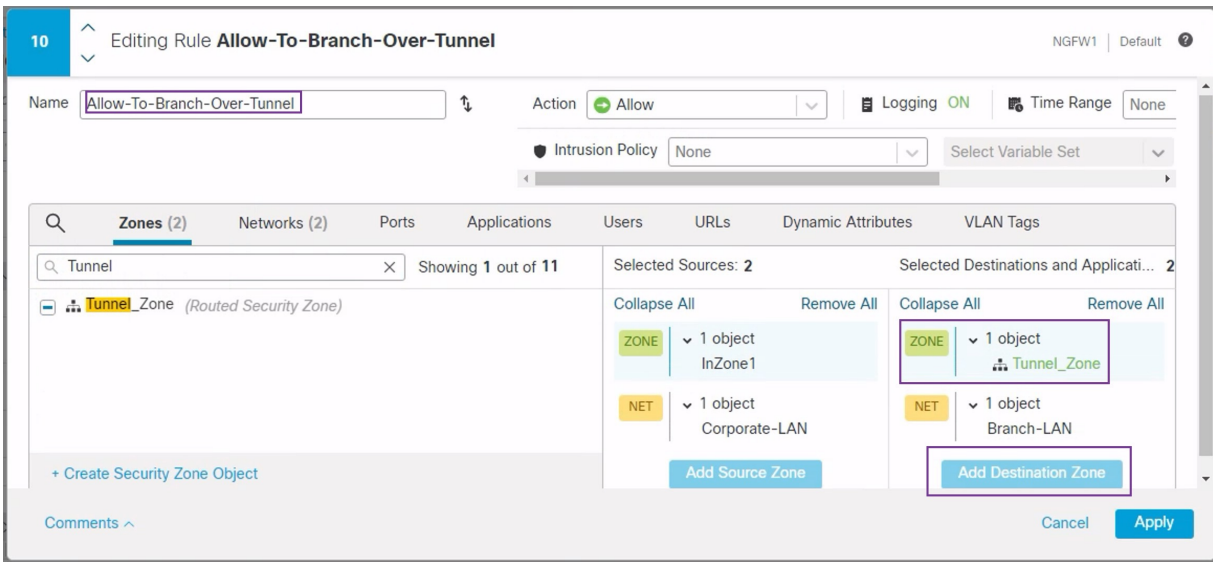
- **NGFW1**：ハブノード（NGFW1）のアクセス コントロール ポリシー
- **ブランチのアクセスコントロール**：スポークノード（NGFWBR1）のアクセス コントロール ポリシー

ステップ 1 ハブノード（NGFW1）の AC ポリシーを編集するには、[編集（Edit）]（✎）アイコンをクリックします。

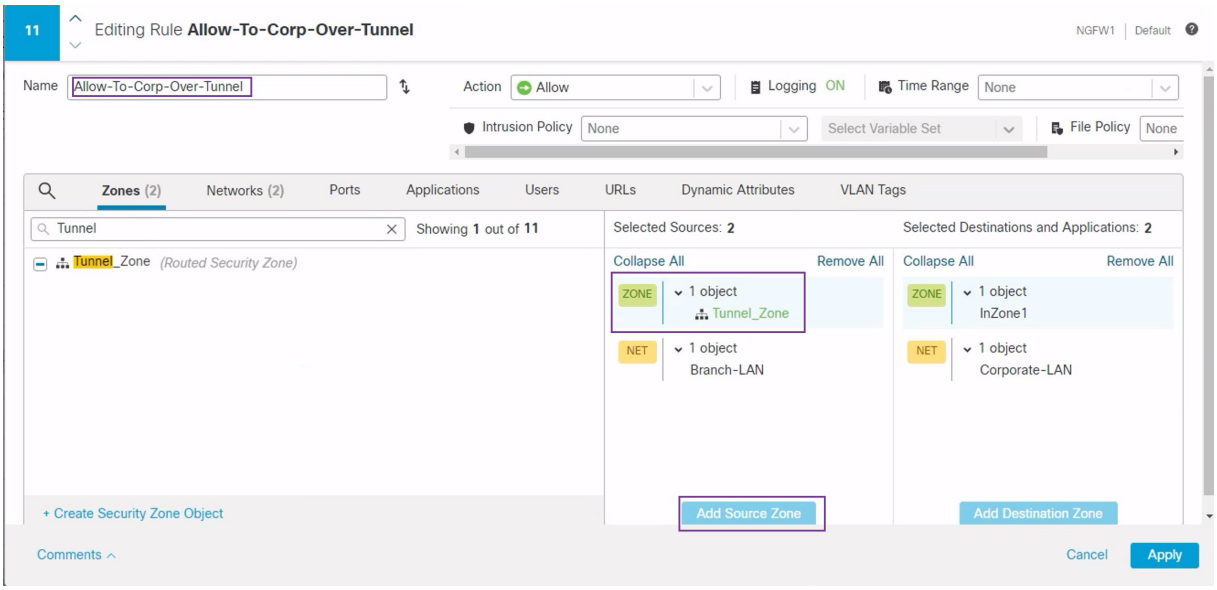
この使用例で変更する必要がある既存のルールは次のとおりです。

- **Allow-To-Branch-Over-Tunnel**
- **Allow-To-Corp-Over-Tunnel**

1. **Allow-To-Branch-Over-Tunnel** ポリシーを編集するには、[編集（Edit）]（✎） アイコンをクリックします。
2. [ゾーン（Zones）] タブで、**Tunnel_Zone** を検索して選択し、[宛先ゾーンを追加（Add Destination Zone）] をクリックします。



3. [適用（Apply）] をクリックして、ルールを保存します。
4. **Allow-To-Corp-Over-Tunnel** ポリシーを編集するには、[編集（Edit）]（✎） アイコンをクリックします。
5. [ゾーン（Zones）] タブで、**Tunnel_Zone** を検索して選択し、[送信元ゾーンを追加（Add Source Zone）] をクリックします。



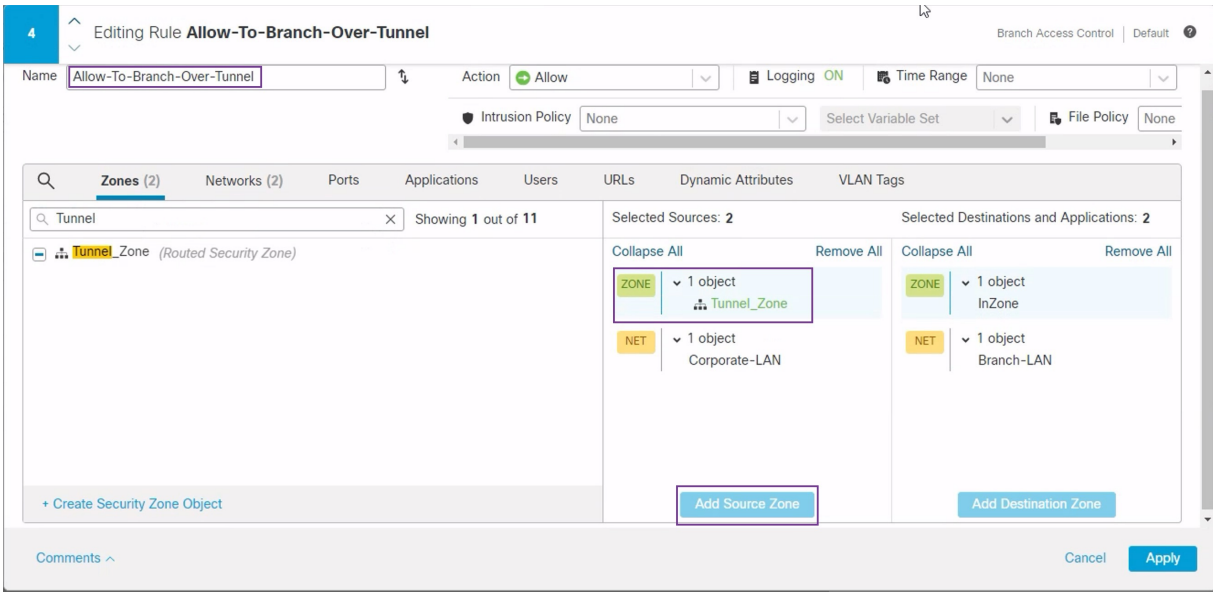
6. [適用（Apply）] をクリックして、ルールを保存します。
7. NGFW1 で更新されたルールを確認します。
8. [保存（Save）] をクリックして、AC ポリシーを保存します。
9. [アクセスコントロールポリシー管理に戻る（Return to Access Control Policy Management）] をクリックして、ポリシーページに戻ります。

ステップ 2 スポークノード（NGFWBR1）の AC ポリシーを編集するには、[編集（Edit）]（✎） アイコンをクリックします。

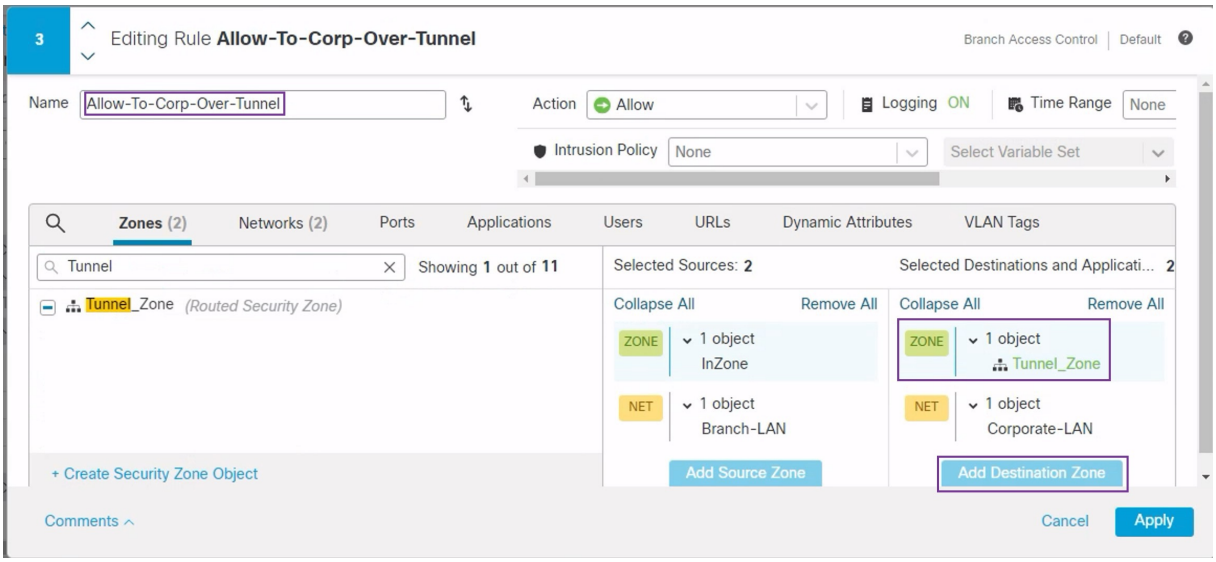
この例で編集する必要があるルールは次のとおりです。

- **Allow-To-Branch-Over-Tunnel**
- **Allow-To-Corp-Over-Tunnel**

1. **Allow-To-Branch-Over-Tunnel** ポリシーを編集するには、[編集（Edit）]（✎） アイコンをクリックします。
2. [ゾーン（Zones）] タブで、**Tunnel_Zone** を検索して選択し、[送信元ゾーンを追加（Add Source Zone）] をクリックします。



3. [適用（Apply）] をクリックして、ルールを保存します。
4. **Allow-To-Corp-Over-Tunnel** ポリシーを編集するには、[編集（Edit）]（✎） アイコンをクリックします。
5. [ゾーン（Zones）] タブで、**Tunnel_Zone** を検索して選択し、[宛先ゾーンを追加（Add Destination Zone）] をクリックします。



6. [適用（Apply）] をクリックして、ルールを保存します。
7. NGFWBR1 で更新されたルールを確認します。

8. [保存（Save）] をクリックして、AC ポリシーを保存します。

設定の展開

すべての設定が完了したら、管理対象デバイスに設定を展開します。

ステップ 1 Management Center メニューバーで、[展開（Deploy）] をクリックします。展開準備が完了しているデバイスのリストが表示されます。

ステップ 2 設定の変更を展開する NGFWBR1 と NGFW1 の横にあるチェックボックスをオンにします。

ステップ 3 [展開（Deploy）] をクリックします。[展開（Deploy）] ダイアログボックスで展開が [完了（Completed）] とマークされるまで待ちます。

ステップ 4 展開する変更に関するエラーや警告がシステムによって識別された場合は、[検証エラー（Validation Errors）] または [検証の警告（Validation Warnings）] ウィンドウにその内容が表示されます。完全な詳細を表示するには、[検証エラー（Validation Errors）] または [検証の警告（Validation Warnings）] リンクをクリックします。

次の選択肢があります。

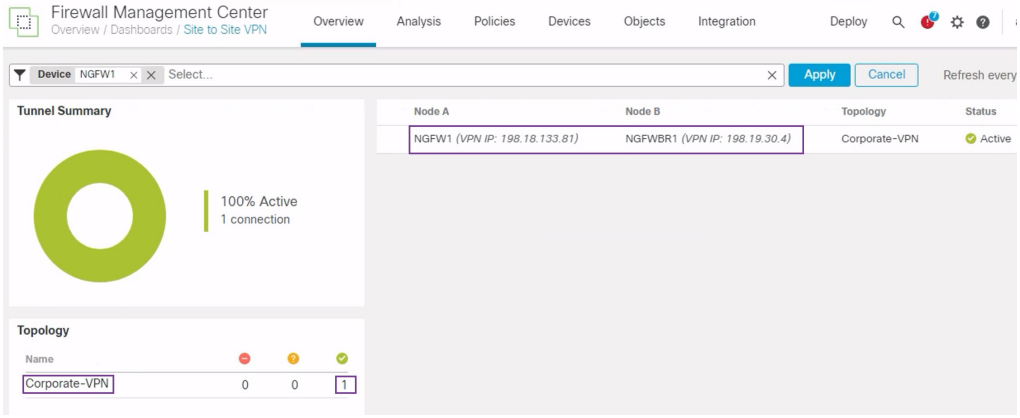
- [展開の続行（Proceed with Deploy）]：警告状態を解決せずに展開を続行します。システムがエラーを確認した場合は続行できません。
- [閉じる（Close）]：展開せずに終了します。エラーおよび警告状態を解決し、設定の再展開を試行します。

VPN トンネルを介したトラフィックフローの確認

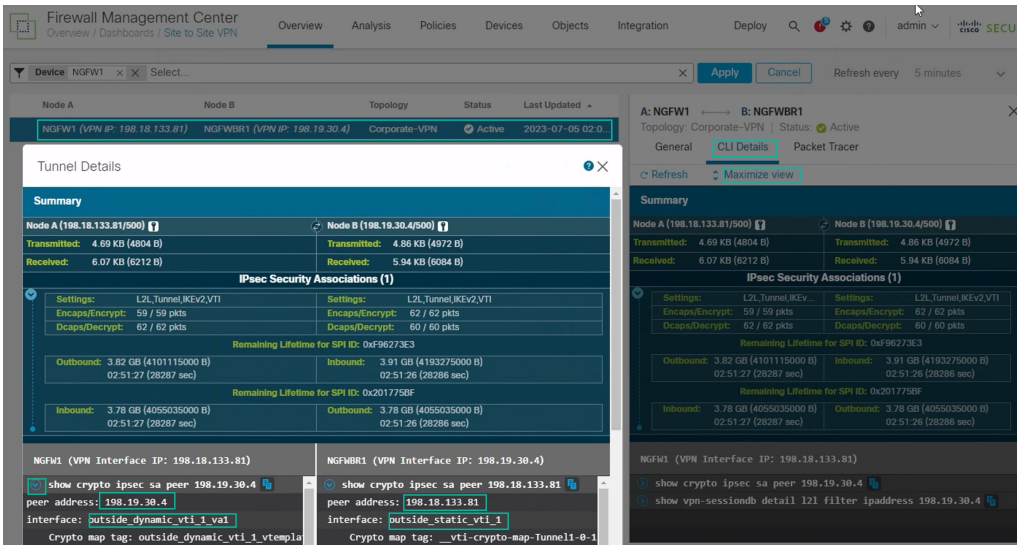
VPN トンネルに対して次の確認を行います。

- **[サイト間VPN（Site-to-site VPN）] ダッシュボードでのトンネルステータスの確認**

1. VPN トンネルが稼働していて緑であることを確認するために、[概要（Overview）] > [ダッシュボード（Dashboards）] > [サイト間VPN（Site-to-site VPN）] を選択します。



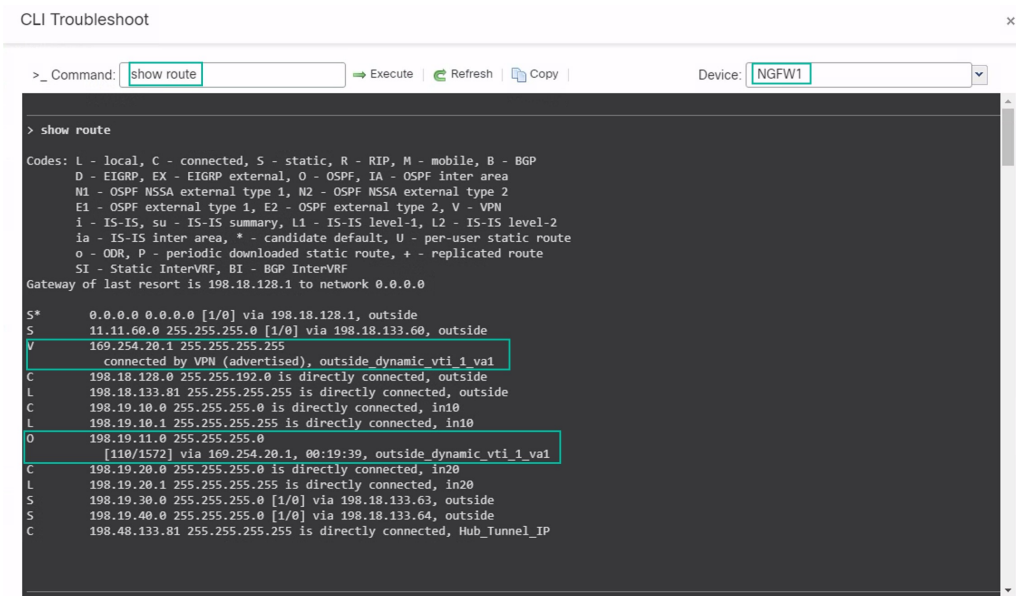
2. NGFW1 にカーソルを合わせます。[すべての情報を表示（View Full Information）] アイコンが NGFW1 の横に表示されます。
3. [すべての情報を表示（View Full Information）] アイコンをクリックします。トンネルの詳細と追加のアクションを含むサイドペインが表示されます。
4. サイドペインの [CLIの詳細（CLI Details）] タブをクリックします。
5. [ビューの最大化（Maximize View）] をクリックして、IPSec セキュリティ アソシエーションの詳細を含む、最大化されたダイアログボックスを表示します。
6. ダイアログボックスの下部にある show コマンドの CLI を展開すると、デバイスの VTI インターフェイスを表示できます。



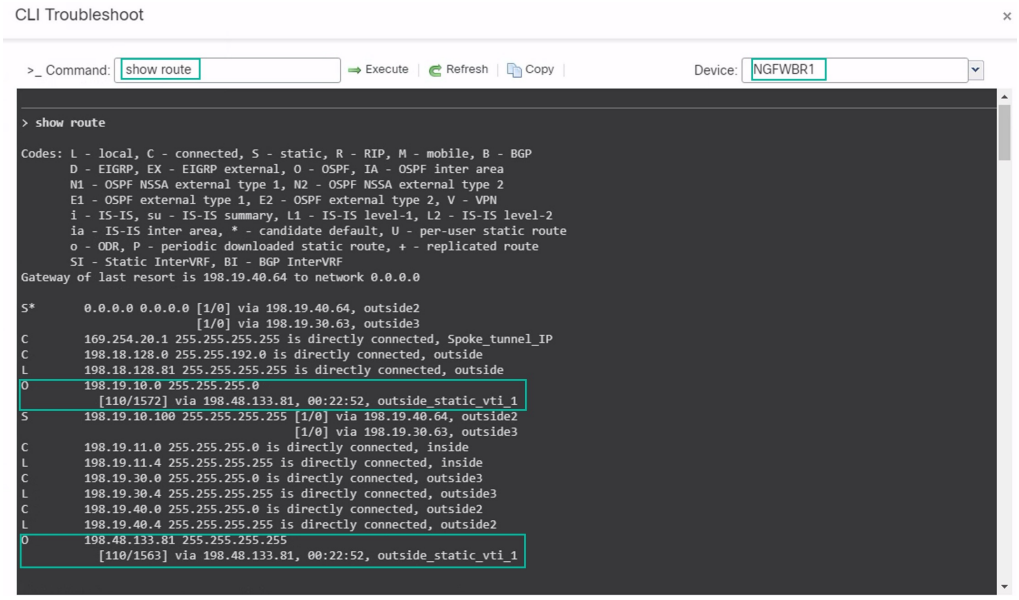
7. [閉じる（Close）] をクリックして [トンネルの詳細（Tunnel Details）] ウィンドウを終了します。

- **ハブノードとブランチノードでのルーティングの確認**：OSPF ルートが **NGFW1** および **NGFWBR1** ノードで正しく学習されていることを確認するために、次の手順を実行します。

1. [デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。
2. NGFW1 を編集するために、[編集（Edit）]（✎） アイコンをクリックします。
3. [デバイス（Device）] タブをクリックします。
4. [全般（General）] カードの [CLI] ボタンをクリックします。[CLIのトラブルシュート（CLI Troubleshoot）] ウィンドウが表示されます
5. [コマンド（Command）] フィールドに **show route** と入力し、[実行（Execute）] をクリックします。
6. NGFW1 ノードでルートを確認し、次の図に示すように、スポークの VTI IP（169.254.20.1）の VPN ルートと Branch_LAN（198.19.11.0/24）の OSPF 学習ルートを確認します。

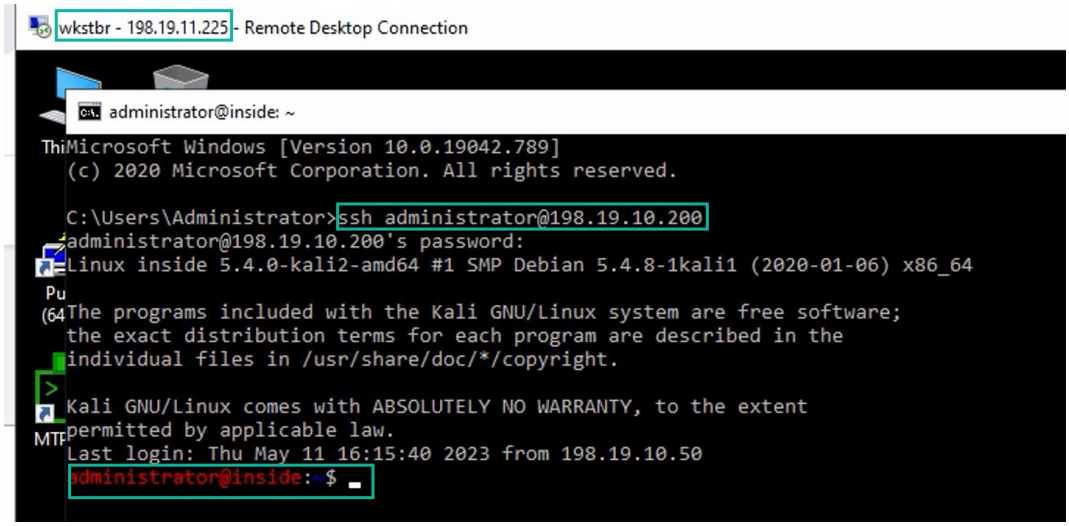


7. NGFWBR1 ノードに対してステップ 2 ～ 5 を繰り返します。
8. NGFWBR1 ノードでルートを確認します。次の図に示すように、ハブの VTI IP（198.48.133.81）および Corporate_LAN（198.19.10.0/24）の学習された OSPF ルートを確認します。



- スポークノードとハブノードの背後にある保護されたネットワーク間のトラフィックの確認

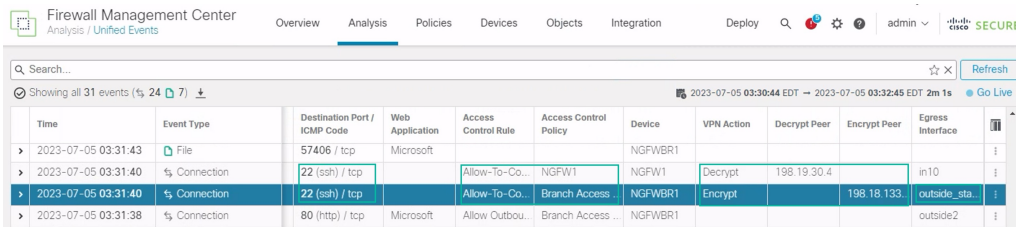
  WKST BR ワークステーション（198.19.11.225）にログインし、NGFW1 の背後にあるホスト（198.19.10.200）に SSH 接続します。ホストに正常に SSH 接続できることを確認します。



- 統合イベントを使用したブランチノードとスポークノードの間の接続の確認

  1. [分析（Analysis）] > [統合イベント（Unified Events）] を選択します。
  2. 列ピッカーを使用して、[VPNアクション（VPN Action）]、[ピアの暗号化（Encrypt Peer）]、[ピアの復号（Decrypt Peer）]、および [出力インターフェイス（Egress Interface）] の列を追加します。

3. 次の図に示すように、新しい列と、[宛先ポート/ICMPコード（Destination Port/ICMP Code）]、[アクセスコントロールルール（Access Control Rule）]、[アクセスコントロールポリシー（Access Control Policy）]、および[デバイス（Device）]の列を並べ替えてサイズ変更します。



4. **WKST BR** から**企業ホスト**への SSH 接続に関連するイベントを表示するには、[宛先ポート/ICMPコード（Destination Port/ICMP Code）]列で[22（ssh/tcp）（22 (ssh/tcp)）]の行を選択します。上の図に示すように、**outside_static_vti_1** インターフェイスを介した **NGFWBR1** での [暗号化（Encrypt）] アクションの後に、**NGFW1** での [復号（Decrypt）] アクションが続くことに注意してください。

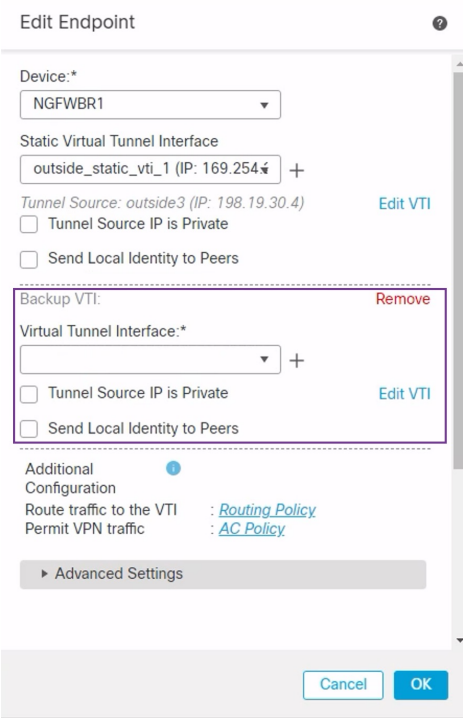
スポークノードでのバックアップ VTI インターフェイスの設定

Cisco Secure Firewall Threat Defense は、ルートベース（VTI）VPN のバックアップトンネルの設定をサポートします。プライマリ VTI がトラフィックをルーティングできない場合、VPN 内のトラフィックはバックアップ VTI を介してトンネリングされます。

ステップ 1 [デバイス（Devices）] > [サイト間VPN（Site-to-site VPN）] を選択し、設定された企業 VPN の VPN トポロジを表示し、[編集（Edit）]（✎）アイコンをクリックします。[VPNトポロジの編集（Edit VPN Topology）] ウィンドウが表示されます。

ステップ 2 [スポークノード（Spoke Nodes）] セクションで、**NGFWBR1** ノードの [編集（Edit）]（✎）アイコンをクリックします。[エンドポイントの編集（Edit Endpoint）] ダイアログボックスが表示されます。

ステップ 3 [バックアップVTIの追加（Add Backup VTI）] リンクをクリックして、セカンダリ VTI トンネルを追加します。このリンクをクリックすると、[バックアップVTI（Backup VTI）] セクションが表示されます。



ステップ 4 [仮想トンネルインターフェイス（Virtual Tunnel Interface）] ドロップダウンリストの横にある [+] をクリックして新しい VTI を追加します。

[仮想トンネルインターフェイスの追加（Add Virtual Tunnel Interface）] ダイアログボックスが表示され、次の事前入力されたデフォルト設定が示されます。

- [トンネルタイプ（Tunnel Type）] には [スタティック（Static）] が自動的に入力されます。
- [名前（Name）] は <*tunnel_source interface logical name*>+ static_vti +<*tunnel ID*> として自動入力されます。たとえば、**outside_static_vti_2** となります。
- [有効（Enabled）] チェックボックスはデフォルトでオンになります。
- [セキュリティゾーン（Security Zone）] ドロップダウンリストから [Tunnel_Zone] を選択します。
- [トンネルID（Tunnel ID）] には、2 の値が自動入力されます。
- [トンネルの送信元（Tunnel Source）] ドロップダウンリストから [GigabitEthernet0/3（outside2）（GigabitEthernet0/3 (outside2)）] を選択します。その横にあるドロップダウンリストから、outside3 インターフェイスの IP アドレスとして [198.19.40.4] を選択します。
- [IPsecトンネルモード（IPsec Tunnel Mode）] は、デフォルトでは IPv4 に設定されます。
- [IPアドレス（IP address）] は、スタティック IP アドレスまたは借用 IP のいずれかです。ループバック インターフェイスから静的インターフェイスの借用 IP を設定することをお勧めします。ループバック インターフェイスを追加するには、ドロップダウンリストから [ループバック1（Spoke_Tunnel_IP）（Loopback 1(Spoke_Tunnel_IP)）] を選択します。

[OK] をクリックして、VTI を保存します。VTI が正常に作成されたことを確認するメッセージが表示されます。[OK] をクリック

バックアップ VTI インターフェイスが [outside_static_vti_2（169.254.20.1）（outside_static_vti_2(169.254.20.1)）] に設定されます。

ステップ 5 [OK] をクリックして、スポーク設定を保存します。

ステップ 6 [保存（Save）] をクリックして、VPN トポロジを保存します。

プライマリおよびセカンダリ VTI インターフェイスの ECMP ゾーンの設定

リンクの冗長性と VPN トラフィックのロードバランシングのために、ブランチノードのプライマリおよびセカンダリのスタティック VTI インターフェイスで ECMP ゾーンを設定します。

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** を選択し、Threat Defense デバイス（**NGFWBR1**）を編集します。

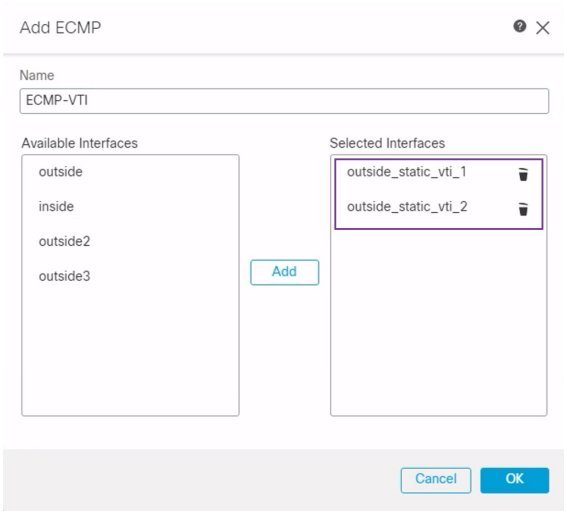
ステップ 2 NGFWBR1 のインターフェイスビューで [ルーティング（Routing）] タブをクリックします。

ステップ 3 [ECMP] をクリックします。

ステップ 4 [Add] をクリックします。

ステップ 5 [ECMPの追加（Add ECMP）] ボックスで、ECMP ゾーンの名前に **ECMP-VTI** と入力します。

ステップ 6 インターフェイスを関連付けるには、[使用可能なインターフェイス（Available Interfaces）] ボックスで [outside_static_vti_1] と [outside_static_vti_2] のインターフェイスを選択し、[追加（Add）] をクリックします。



ステップ 7 [OK] をクリック

[ECMP] ページに、新しく作成された ECMP ゾーンが表示されます。

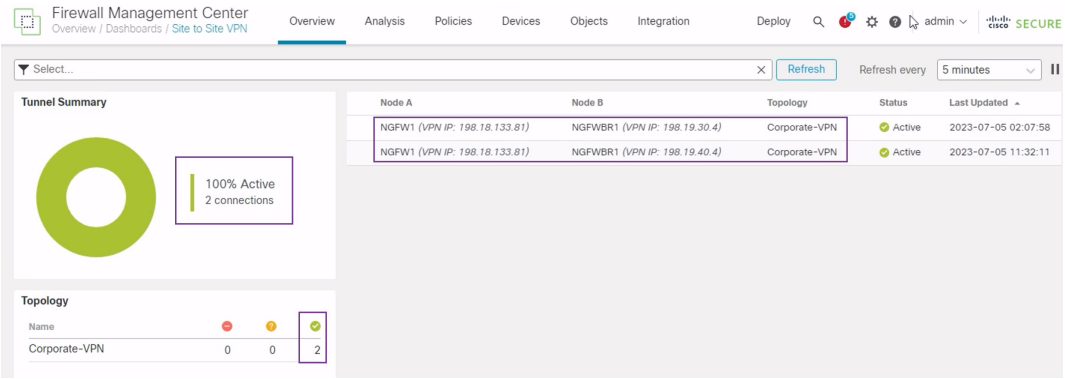
ステップ 8 [保存（Save）] をクリックします。

プライマリトンネルとセカンダリトンネルの確認

ブランチノードとハブノードの間のプライマリ VTI トンネルとセカンダリ VTI トンネルの両方が設定され、稼働していて、アクティブであることを確認します。

- **[サイト間VPN（Site-to-site VPN）] ダッシュボードでのトンネルステータスの確認**

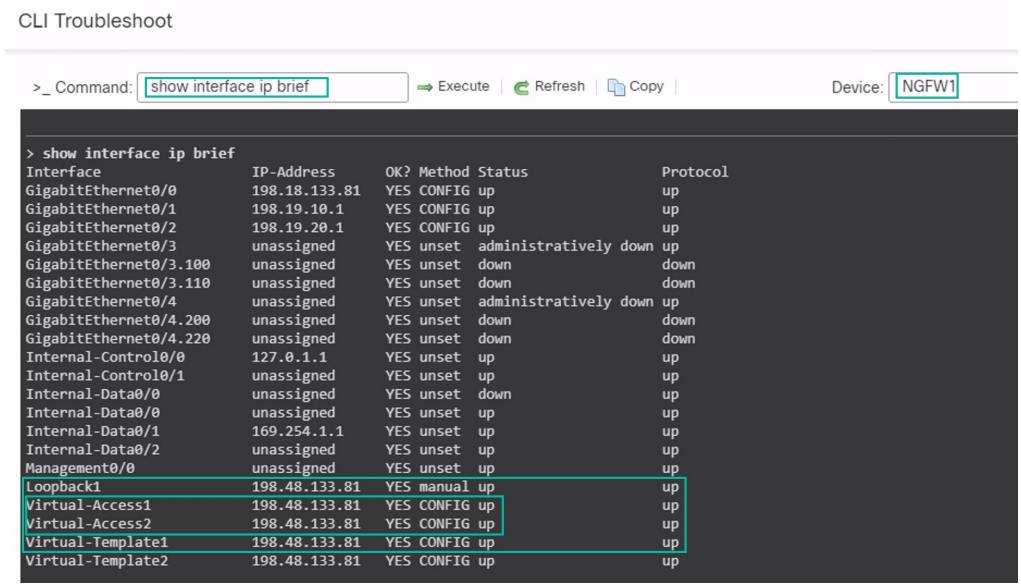
  VPN トンネルが稼働していて緑であることを確認するために、[概要（Overview）]>[ダッシュボード（Dashboards）]>[サイト間VPN（Site-to-site VPN）] を選択します。



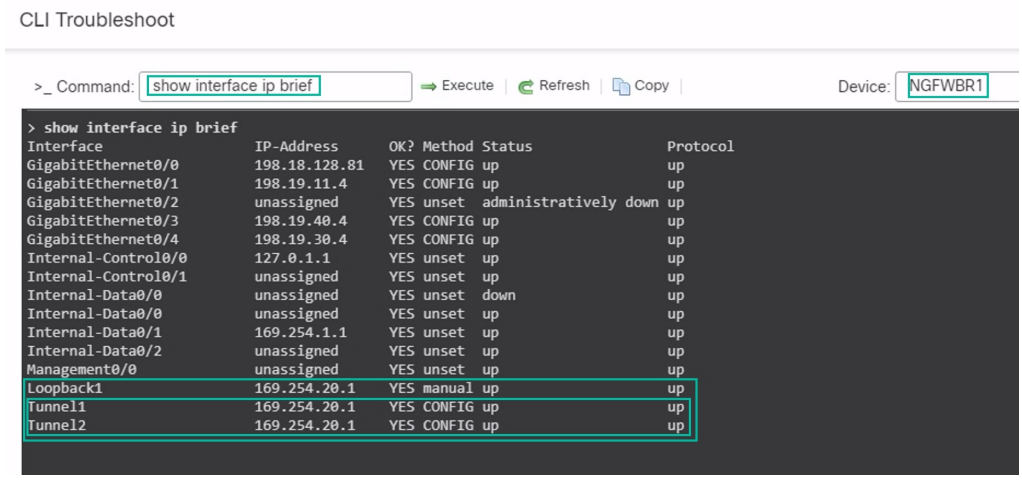
- **ハブノードとブランチノードでのルーティングの確認**

  1. [デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。
  2. NGFW1 を編集するために、[編集（Edit）] アイコンをクリックします。
  3. [デバイス（Device）] タブをクリックします。
  4. [全般（General）] カードの [CLI] ボタンをクリックします。[CLIのトラブルシュート（CLI Troubleshoot）] ウィンドウが表示されます
  5. [コマンド（Command）] フィールドに **show interface ip brief** と入力し、[実行（Execute）] をクリックして、ハブの DVTI から作成されたダイナミック仮想アクセスインターフェイスを表示します。

（注） **NGFWBR1** がセカンダリ VTI 接続を介して NGFW1 に接続するときに、同じ DVTI から Virtual-Access2 インターフェイスが生成されます。



6. NGFWBR1 ノードに対してステップ 2 ～ 5 を繰り返して、次の図に示すように、スタティック VTI インターフェイスの **Tunnel1** および **Tunnel2** を表示します。



7. [コマンド（Command）] フィールドに **show route** と入力し、[実行（Execute）] をクリックして、セカンダリ VTI トンネルの追加後のルートを表示します。

CLI Troubleshoot

>_ Command: show route | Execute | Refresh | Copy | Device: NGFWBR1

```
> show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is 198.19.40.64 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [1/0] via 198.19.40.64, outside2
                         [1/0] via 198.19.30.63, outside3
C        169.254.20.1 255.255.255.255 is directly connected, Spoke_tunnel_IP
C        198.18.128.0 255.255.192.0 is directly connected, outside
L        198.18.128.81 255.255.255.255 is directly connected, outside
O        198.19.10.0 255.255.255.0
           [110/1572] via 198.48.133.81, 00:12:13, outside_static_vti_2
           [110/1572] via 198.48.133.81, 00:12:33, outside_static_vti_1
S        198.19.10.100 255.255.255.255 [1/0] via 198.19.40.64, outside2
                                       [1/0] via 198.19.30.63, outside3
C        198.19.11.0 255.255.255.0 is directly connected, inside
L        198.19.11.4 255.255.255.255 is directly connected, inside
C        198.19.30.0 255.255.255.0 is directly connected, outside3
L        198.19.30.4 255.255.255.255 is directly connected, outside3
C        198.19.40.0 255.255.255.0 is directly connected, outside2
L        198.19.40.4 255.255.255.255 is directly connected, outside2
O        198.48.133.81 255.255.255.255
           [110/1563] via 198.48.133.81, 00:12:13, outside_static_vti_2
           [110/1563] via 198.48.133.81, 00:12:33, outside_static_vti_1
```

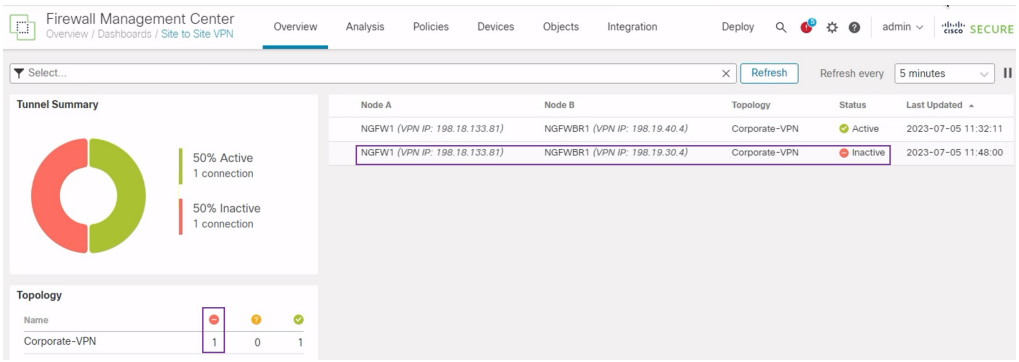
- プライマリ（**outside_static_vti_1**）とセカンダリ（**outside_static_vti_2**）の両方のVTI で、OSPF を介して **Corporate_LAN**（198.19.10.0/24）が学習されていることに注意してください。
- プライマリ VTI とセカンダリ VTI の両方で、OSPF を介して DVTI トンネル IP（198.48.133.81）も学習されていることに注意してください。

- **プライマリトンネルがダウンした場合のセカンダリトンネルへのフェールオーバーの確認**

1. この例では、セカンダリトンネルへのフェールオーバーを検証するために、アップストリームデバイスのアクセス制御リストを通じて、または、Management Center から Threat Defense の outside3 インターフェイスをシャットダウンして、outside3 インターフェイスから送信されてインターネットに向かうアウトバウンドトラフィックを制限することで、パケット損失を引き起こすことができます。

（注） インターフェイスをシャットダウンするとネットワークに影響が出る可能性があるため、実稼働ネットワークで試してはなりません。

2. [サイト間VPN（Site-to-site VPN）] ダッシュボードでは、次の図に示すように、プライマリトンネルがダウンしています。



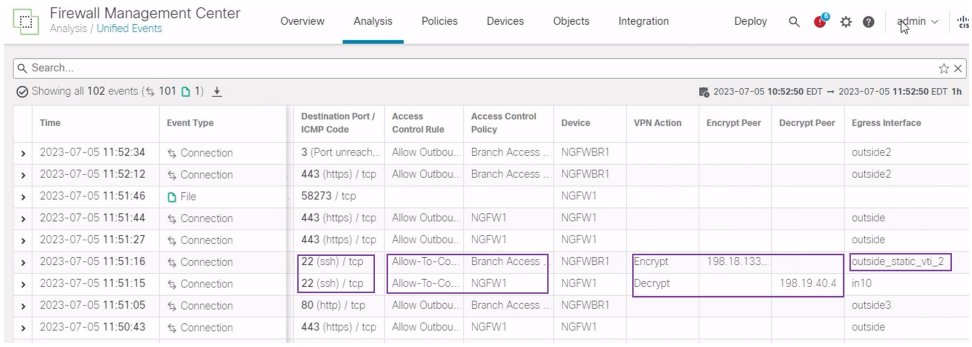
3. ブランチからハブへのトラフィックを開始します。WKST BR ワークステーションにログインし、NGFW1 の背後にあるホストに SSH 接続します。ホストに正常に SSH 接続できることを確認します。

4. 統合イベントビューアを使用して、トラフィックの出力パスを確認します。

   1. [分析（Analysis）] > [統合イベント（Unified Events）] を選択します。

   2. 列ピッカーを使用して、[VPNアクション（VPN Action）]、[ピアの暗号化（Encrypt Peer）]、[ピアの復号（Decrypt Peer）]、および [出力インターフェイス（Egress Interface）] の列を追加します。

   3. 次の図に示すように、新しい列と、[宛先ポート/ICMPコード（Destination Port/ICMP Code）]、[アクセスコントロールルール（Access Control Rule）]、[アクセスコントロールポリシー（Access Control Policy）]、および [デバイス（Device）] の列を並べ替えてサイズ変更します。



SSH の **NGFWBR1** での出力インターフェイス（ポート 22）がセカンダリインターフェイス（**outside_static_vti_2**）として表示されるようになったことに注意してください。

ルートベースのVPNトンネルのトラブルシューティング

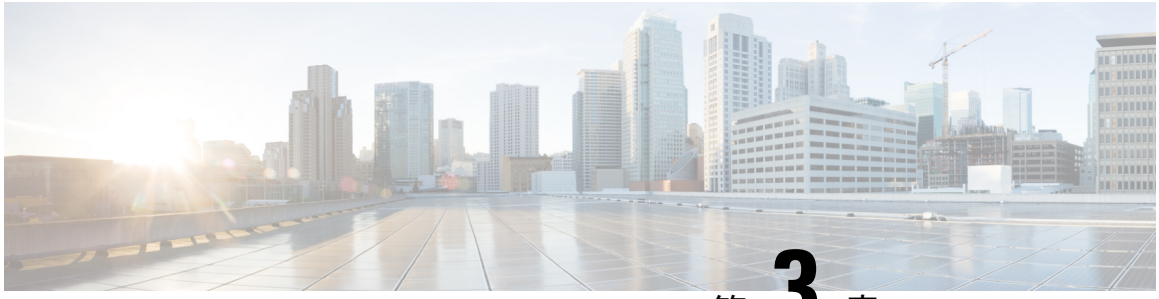
展開後に、次の CLI を使用して、Cisco Secure Firewall Threat Defense でのルートベースの VPN トンネルに関連する問題をデバッグします。

（注） 実稼働環境の Threat Defense デバイスで debug コマンドを実行する場合は、注意して進めてください。デバイスでさまざまなデバッグレベルを設定できるため、詳細な出力が行われる可能性があります。

操作	CLI コマンド
特定のピアの条件付きデバッグを有効にする	**debug crypto condition peer <peer-IP>**
仮想トンネルインターフェイス情報をデバッグする	**debug vti 255**
IKEv2 プロトコル関連のトランザクションをデバッグする	**debug crypto ikev2 protocol 255**
IKEv2プラットフォーム関連のトランザクションをデバッグする	**debug crypto ikev2 platform 255**
一般的なIKE関連のトランザクションをデバッグする	**debug crypto ike-common 255**
IPSec関連のトランザクションをデバッグする	**debug crypto ipsec 255**

関連リソース

リソース（Resource）	URL
Cisco Secure Firewall Threat Defense リリースノート	https://www.cisco.com/go/firewall-release-notes
すべての新機能と廃止された機能	http://www.cisco.com/go/whatsnew-fmc
Cisco.com の Cisco Secure Firewall	http://www.cisco.com/go/firewall
Cisco.com のマニュアル	http://www.cisco.com/go/firewall-docs
YouTube 上の Cisco Secure Firewall	https://www.youtube.com/cisco-netsec
Cisco Secure Firewall Essentials	https://secure.cisco.com/secure-firewall



第 3 章

ダイレクト インターネット アクセス（DIA）を使用したブランチからインターネットへのアプリケーション トラフィックのルーティング

この章では、2つの使用例を使用して、ダイレクトインターネットアクセス（DIA）の実践的な応用について詳しく説明します。各使用例では、シナリオ、ネットワークトポロジ、ベストプラクティス、および前提条件について詳しく説明します。また、シームレスな導入のための包括的なエンドツーエンドの手順も提供します。

ダイレクト インターネット アクセス

デジタルイノベーションにより、ビジネスの運営、コミュニケーション、お客様とのやり取りの方法が変革されています。コラボレーションとカスタマーエクスペリエンスを向上させるための新しいアプリケーションとテクノロジーが作成され、高帯域幅の低遅延な接続が必要になっています。

従来のネットワークの課題

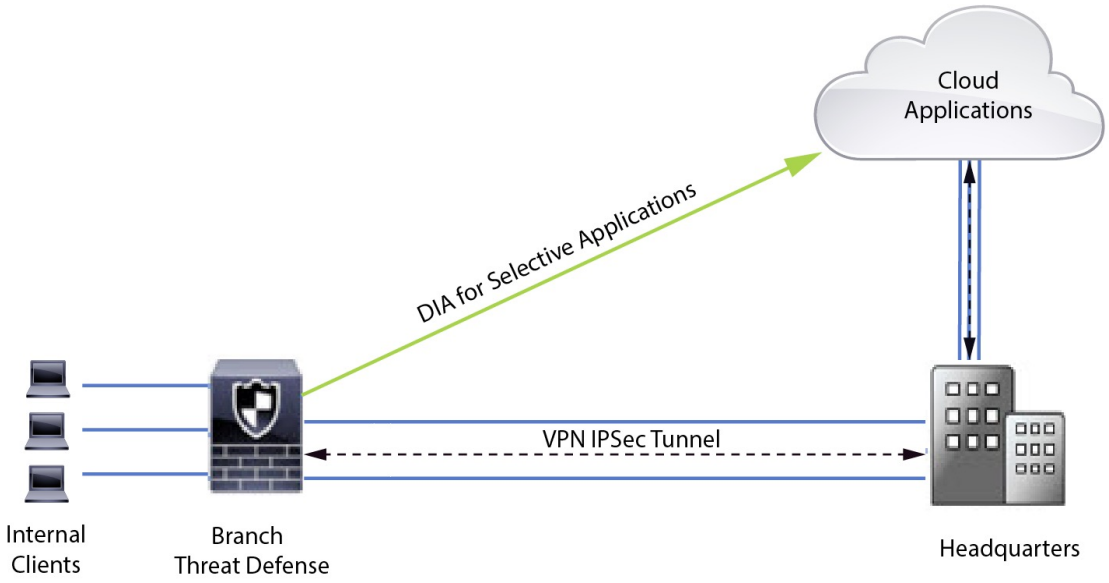
従来のネットワーク展開では、中央サイトの境界ファイアウォールを利用して、ローカルユーザーとブランチユーザーにセキュアなアクセスを提供しています。このアーキテクチャでは必要な接続が提供されますが、すべてのインターネットトラフィックが暗号化されたトラフィックとして VPN トンネル経由で中央サイトに転送されるため、パケットの遅延、ドロップ、およびジッターが発生します。さらに、このネットワークは、展開と複雑なネットワーク管理に関連する高いコストと帯域幅の使用率という課題に常に直面しています。

解決方法

これらの課題を克服する方法の 1 つは、ダイレクト インターネット アクセス（DIA）を使用することです。DIA は、Cisco Secure Firewall のブランチの簡素化機能のコンポーネントです。DIA では、ポリシーベースルーティング（PBR）が使用されます。DIA は、アプリケーション認識型ルーティングとも呼ばれます。

DIA トポロジでは、分散拠点からのアプリケーション トラフィックがインターネットに直接ルーティングされるため、本社へのインターネット宛トラフィックのトンネリングの遅延を回避できます。ブランチの Cisco Secure Firewall Threat Defense は、インターネット イグジット ポイントを使用して設定されます。入力インターフェイスで PBR ポリシーが適用され、拡張アクセスコントロールリストで定義されたアプリケーションに基づいてトラフィックが識別されます。それに応じて、トラフィックは出力インターフェイスを介して直接インターネットに転送されます。

図 *1*：特定の出力インターフェイスを介したダイレクト インターネット アクセス



ポリシーベースルーティングを使用する理由

PBR を使用して、指定したアプリケーションのトラフィックを分類し、安全にブレークアウトすることができます。また、特定のトラフィックのパスを指定することもできます。Cisco Secure Firewall Management Center ユーザーインターフェイスで PBR ポリシーを設定して、アプリケーションに直接アクセスできるようにすることができます。

PBR とパスモニタリング

通常、PBR では、トラフィックは、出力インターフェイスに設定された優先順位値（インターフェイスコスト）に基づいて、出力インターフェイスを介して転送されます。Cisco Secure Firewall Management Center 7.2 以降のバージョンでは、PBR はパスモニタリングを使用して、出力インターフェイスのパフォーマンスメトリック（RTT、ジッター、パケット損失、MOS）を収集します。PBR はこれらのメトリックを使用して、トラフィックを転送するための最適なパス（出力インターフェイス）を決定します。パスモニタリングは、メトリックが変更された場合にモニタリング対象インターフェイスを PBR に定期的に通知します。PBR は、モニタリング対象インターフェイスの最新のメトリック値をパス モニタリング データベースから取得し、データパスを更新します。

インターフェイスのパスモニタリングを有効にし、出力インターフェイスのモニタリングタイプを設定し、メトリック値を使用するパスモニタリングを活用するようにアプリケーション トラフィックを設定する必要があります。

パスモニタリングについては、シナリオ2：パスモニタリングを使用したダイレクトインターネット アクセス （43 ページ）を参照してください。

利点

DIA を使用する利点は次のとおりです

- インターネットの速度と分散拠点のユーザー体験が向上します。
- 複雑さが軽減され、ネットワーク管理が簡単かつ低コストになります。
- 帯域幅の使用量が削減され、高価なハードウェアが不要になるため、コスト効率が高くなります。
- リアルタイムメトリックを使用した動的なパス選択。
- 手動介入なしで保証される最適な出力パス。
- リンクの正常性とネットワーク状態の継続的なモニタリング。
- 俊敏性の向上により、組織は変化するビジネスニーズに迅速に適応できます。

この使用例の対象者

この使用例の対象者は、ブランチからの直接のインターネット宛トラフィックのローカルブレークアウトを許可するために、各リモートサイト内にダイレクト インターネット アクセスを導入することを希望するネットワーク設計エンジニア、ネットワーク運用担当者、およびセキュリティ運用担当者です。

ダイレクト インターネット アクセスのコンポーネント

ブランチファイアウォールが DIA に使用する重要なコンポーネントの一部を次に示します。

- **信頼された DNS サーバー**：DIA 機能のアプリケーション検出は、DNS スヌーピングを使用してアプリケーションまたはアプリケーションのグループを解決します。DNS リクエストが不正な DNS サーバーによって解決されず、実際に目的の DNS サーバーにロックされていることを確認するために、Management Center では、Threat Defense の信頼された DNS サーバーを設定できます。
- **インターフェイスの優先順位**：Cisco Secure Firewall は、インターフェイスの優先順位を使用して最適なインターネットパスを決定します。優先順位は小さいほど高く、インターネットにトラフィックを送信するときの特定の ISP の優先順位を決定します。Management Center では、Threat Defense のインターフェイスの優先順位を設定できます。
- **ネットワークサービス**：ポリシーベースルーティング内で使用される、特定のアプリケーションに関連付けられたオブジェクト。このオブジェクトは自動的に作成されます。
- **ネットワーク サービス グループ（NSG）**：ネットワーク サービス グループは、ファイアウォールが設定に基づいてパスを決定するために使用するアプリケーションのグループで

す。複数のネットワーク サービス オブジェクトを単一の NSG に含めることができます。Management Center は、ポリシーベースルーティング用に設定された拡張アクセスリストに基づいて NSG を自動生成します。

ベストプラクティス

- Cisco Secure Firewall Threat Defense はバージョン 7.1 以降を実行する必要があります。
- アプリケーション トラフィック フローをサポートするために、信頼された DNS サーバーを介して DNS スヌーピングが実行されるように、信頼された DNS サーバーを設定する必要があります。
- Threat Defense を通過する DNS リクエストはクリアテキスト形式である必要があり、DNS スヌーピングが PBR フローを支援できるように、暗号化されていない必要があります。
- アプリケーション トラフィックのアクティブ/アクティブ ロードバランシング用に、ECMP ゾーンを設定する必要があります。
- ECMP はルーテッド ファイアウォール モードでのみサポートされ、デバイスは最大で 256 の ECMP ゾーンを持つことができます。
- ルーテッドインターフェイスのみを使用する必要があります。各インターフェイスは、単一の ECMP ゾーンにのみ属する必要があります。
- インターフェイスが、ECMP が設定されている仮想ルータに属していることを確認してください。
- ECMP ゾーン設定で使用されるインターフェイスには、インターフェイス設定内で論理名が定義されている必要があります。
- Cisco Secure Firewall Threat Defense で PBR に設定されているインターフェイスが、ECMP ゾーンごとに 8 つ以下であることを確認します。
- PBR はこのモードではサポートされていないため、Cisco Secure Firewall Threat Defense はクラスタに展開しないでください。
- PBR は、ユーザー定義の仮想ルータではサポートされていないため、グローバル仮想ルータ用に設定する必要があります。
- PBR 内の入力および出力インターフェイスで使用されるインターフェイスが、ルーテッドインターフェイスまたは管理専用以外のインターフェイスのいずれかであり、グローバル仮想ルータに属していることを確認します。

前提条件

- Device Manager を使用した Threat Defense の初期設定の完了

- デバイスへのライセンスの割り当て
- インターネットアクセスのルートの追加。「スタティックルートの追加」を参照してください
- 脅威に対する防御のための NAT の設定
- 基本的なアクセス コントロール ポリシーの作成

シナリオ 1：パスモニタリングを使用しないダイレクト インターネット アクセス

Bob はアカウントマネージャで、Ann はヘルプデスクスペシャリストです。どちらも大企業の分散拠点で働いています。最近、Webex などの Web 会議ツールや YouTube などのストリーミング プラットフォームを使用しているときに、遅延の問題が発生しています。

リスクがあるもの

ネットワーク遅延とネットワーク輻輳により、Web会議およびストリーミングセッションのパフォーマンスとユーザー体験が低下します。これは、分散拠点の従業員の生産性と効率に影響を与え、事業運営全体に悪影響を及ぼす可能性があります。

PBR を使用した DIA による問題の解決方法

IT 管理者の Alice は、ポリシーベースのルーティングを DIA と組み合わせて使用し、ネットワークの遅延を低減します。

ダイレクト インターネット アクセスにより、分散拠点はセントラルサイトまたはデータセンターを介してトラフィックをルーティングすることなく、インターネットに直接アクセスできるようになりました。これにより、より直接的で最適化されたインターネット接続がブランチユーザーに提供されるため、遅延が低減されました。

ポリシーベースのルーティングにより、Webex と YouTube のトラフィックが異なる出力インターフェイスに分離されました。これにより、トラフィックが異なるパスを介して送信されるようになり、単一インターフェイスでの負荷が軽減され、アプリケーションのパフォーマンスが向上しました。

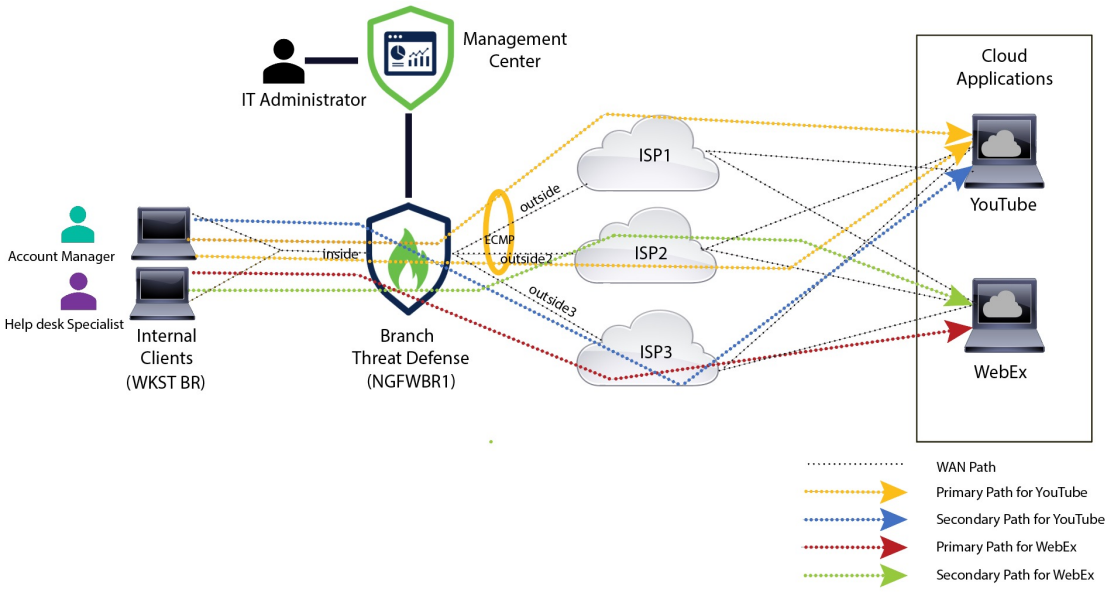
ネットワークトポロジ：パスモニタリングを使用しない DIA

このトポロジでは、Threat Defense デバイスが 3 つの出力インターフェイスを持つブランチロケーションに展開されます。デバイスは、PBR を使用した DIA 用に設定されています。

次の図では、内部クライアントまたはブランチワークステーションには**WKST BR** というラベルが付けられ、ブランチの Threat Defense には **NGFWBR1** というラベルが付けられています。**NGFWBR1** の入力インターフェイスには **inside** という名前が付けられ、出力インターフェイスにはそれぞれ **outside**、**outside2**、および **outside3** という名前が付けられています。

outside と **outside2** のインターフェイス間のロードバランシングは、ECMP ゾーンとスタティック ルートを設定することで実現されています。

図 *2:* ダイレクト インターネット アクセスのトポロジ（パスモニタリングなし）

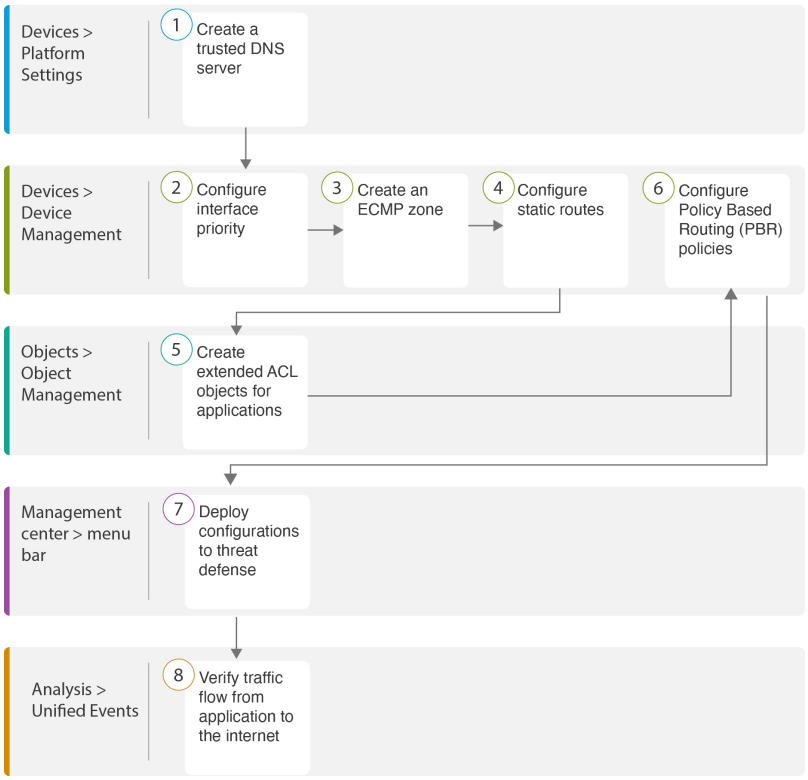


DIA を使用すると、ブランチファイアウォールの背後にあるユーザーは次へのアクセスが許可されます。

1. ソーシャル メディア アプリケーションのトラフィック（**YouTube** など）。2 つの出力インターフェイス（**outside** と **outside2**）を使用してロードバランシングされます。両方のインターフェイスに障害が発生した場合、トラフィックは 3 番目の出力インターフェイス（**outside3**）にフォールバックします。
2. コラボレーション アプリケーションのトラフィック（**Webex** など）。**outside3** インターフェイスを介して転送され、このリンクに障害が発生した場合、トラフィックは **outside2** インターフェイスを介して転送されます。

パスモニタリングを使用しない DIA の設定のエンドツーエンドの手順

次のフローチャートは、Cisco Secure Firewall Management Center でパスモニタリングを使用せずに DIA を設定するためのワークフローを示しています。



ステップ	説明
1	（前提条件）信頼されたDNSサーバーを設定します。信頼されたDNSサーバーの設定 （46 ページ）を参照してください。
2	（前提条件）インターフェイスの優先順位を設定します。インターフェイスの優先順位の設定 （47 ページ）を参照してください。
3	（前提条件）ECMP ゾーンを作成します。ECMP ゾーンの作成 （48 ページ）を参照してください。
4	（前提条件）スタティックルートを設定します。等コストスタティックルートの設定 （48 ページ）を参照してください。
5	アプリケーションの拡張 ACL オブジェクトを設定します。参照先 • YouTube の拡張 ACL オブジェクトの設定 （49 ページ） • Webex の拡張 ACL オブジェクトの設定 （50 ページ）
6	アプリケーションの PBR ポリシーを設定します。参照先 • YouTube の拡張 ACL オブジェクトの設定 （49 ページ） • YouTube のポリシー ベース ルーティング ポリシーの設定 （51 ページ）

ステップ	説明
7	設定を Threat Defense に展開します。設定の展開 （54 ページ）を参照してください。
8	YouTube および Webex のトラフィックフローを確認します。アプリケーション トラフィック フローの確認 （55 ページ） を参照してください。

シナリオ 2：パスモニタリングを使用したダイレクト インターネット アクセス

Ann はヘルプデスクスペシャリストであり、大企業の分散拠点で働いています。Ann は、Webex の使用中に接続の切断と遅延を経験しています。

リスクがあるもの

Webex Meetings は、会議のホストと参加者の間のリアルタイムのデータ伝送（音声とビデオのストリームを含む）に依存しています。このリアルタイムデータは、ネットワーク遅延とパケット損失の影響を受けます。ネットワークで大量のパケット損失が発生すると、フリーズ、遅れ、遅延などの音声とビデオの品質の問題が発生し、会議の体験に悪影響を与える可能性があります。

パスモニタリングを使用した PBR による問題の解決方法

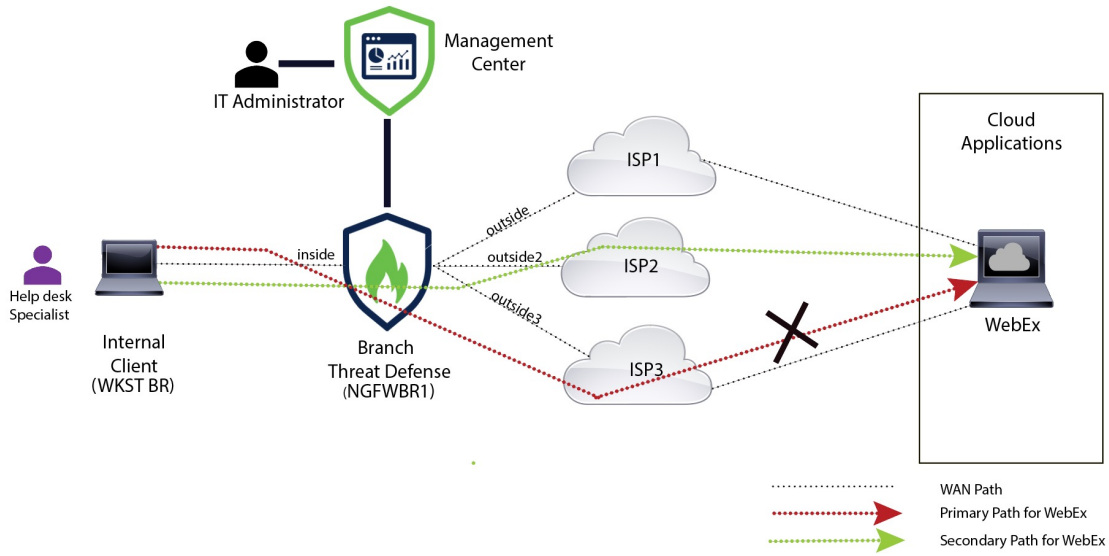
IT 管理者の Alice は、パスモニタリングを使用したポリシーベースルーティングを使用して、パケット損失を最小限に抑えながら Webex のアプリケーション トラフィックを出力インターフェイスを介してインターネットに誘導し、参加者に可能な限り優れた会議の体験を提供しました。

ネットワークトポロジ：パスモニタリングを使用した DIA

このトポロジでは、Threat Defense デバイスが 3 つの出力インターフェイスを持つブランチロケーションに展開されます。デバイスは、ポリシーベースルーティングを使用したダイレクト インターネット アクセス用に設定されています。

次の図では、内部クライアントまたはブランチワークステーションには **WKST BR** というラベルが付けられ、ブランチの Threat Defense には **NGFWBR1** というラベルが付けられています。**NGFWBR1** の入力インターフェイスには **inside** という名前が付けられ、出力インターフェイスにはそれぞれ **outside**、**outside2**、および **outside3** という名前が付けられています。

図 *3:* ダイレクト インターネット アクセスのトポロジ（パスモニタリングあり）



outside2 および **outside3** 出力インターフェイスが、パスモニタリングで有効になっています。Webex の PBR ポリシーは、パケット損失を最小限に抑えてトラフィックが出力インターフェイスにルーティングされるように設定されています。

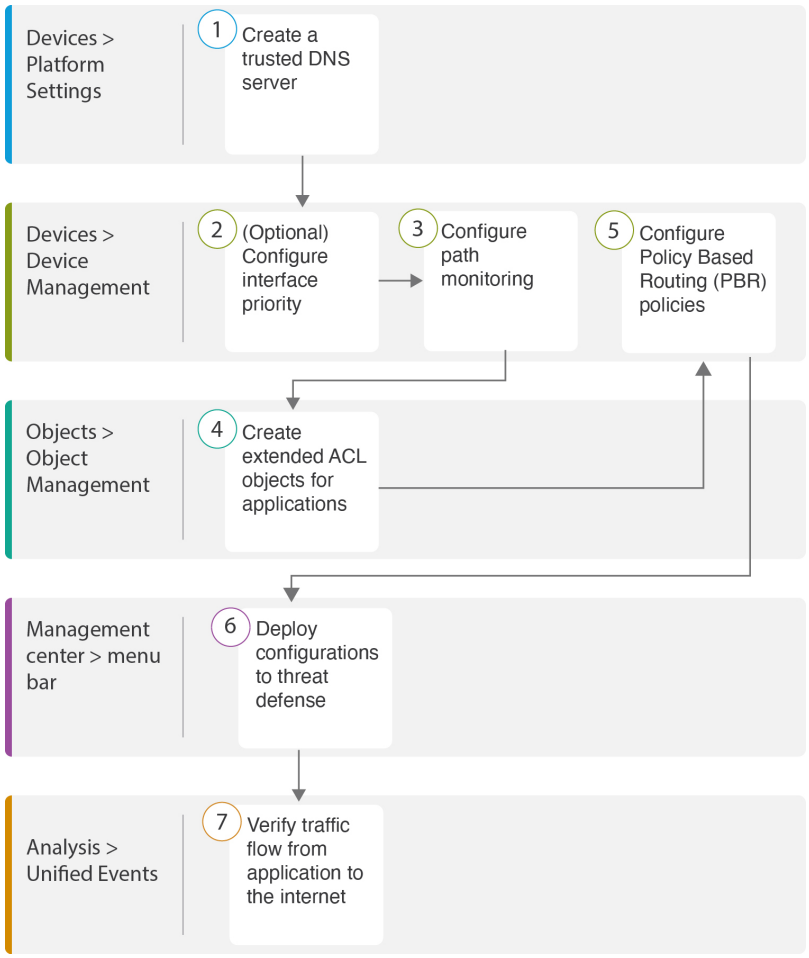
このシナリオでは、パスモニタリングを検証するために、アップストリームデバイスのアクセス制御リストを通じて、または、Firewall Management Center から Cisco Secure Firewall Threat Defense の **outside3** インターフェイスをシャットダウンして、**outside3** インターフェイスから送信されてインターネットに向かうアウトバウンドトラフィックを制限することで、パケット損失を引き起こすことができます。

（注） インターフェイスをシャットダウンするとネットワークに影響が出る可能性があるため、実稼働ネットワークで試してはなりません。

パケット損失の結果として、**outside3** インターフェイスに関連付けられているリンクがダウンします。コラボレーションアプリケーションのトラフィックは、**outside3** インターフェイスの代わりに、**outside2** インターフェイスを介して転送されます。

パスモニタリングを使用した DIA の設定のエンドツーエンドの手順

次のフローチャートは、Cisco Secure Firewall Management Center でパスモニタリングを使用して DIA を設定するためのワークフローを示しています。



ステップ	説明
1	（前提条件）信頼された DNS サーバーを設定します。信頼された DNS サーバーの設定 （46 ページ）を参照してください。
2	[前提条件（オプション）] インターフェイスの優先順位を設定します。インターフェイスの優先順位の設定 （47 ページ）を参照してください。
3	パスモニタリングを設定します。パスモニタリングの設定 （49 ページ）を参照してください。
4	アプリケーションの拡張 ACL オブジェクトを設定します。Webex の拡張 ACL オブジェクトの設定 （50 ページ）を参照してください。
5	アプリケーションの PBR ポリシーを設定します。Webex のパスモニタリングを使用したポリシー ベース ルーティング ポリシーの設定 （53 ページ）を参照してください。
6	設定を Threat Defense に展開します。設定の展開 （54 ページ）を参照してください。

ステップ	説明
7	Webex トラフィックフローを確認します。アプリケーション トラフィック フローの確認 （55 ページ） を参照してください。

信頼された DNS サーバーの設定

ダイレクト インターネット アクセス機能でのアプリケーション検出は、アプリケーションまたはアプリケーションのグループを検出するために、DNS スヌーピングを使用してアプリケーションドメインを IP にマッピングします。DNS リクエストが不正な DNS サーバーによって解決されず、実際に目的の DNS サーバーにロックされていることを確認するために、Cisco Secure Firewall Management Center では、Cisco Secure Firewall Threat Defense の信頼された DNS サーバーを設定できます。そのため、ファイアウォールは、信頼された DNS サーバーに向かうトラフィックのみをスヌーピングします。信頼された DNS サーバーの設定とは別に、設定済みのサーバーを、DNS サーバーグループ、DHCP プール、DHCP リレー、および DHCP クライアントに、信頼された DNS サーバーとして含めることができます。

[信頼されたDNSサーバー（Trusted DNS Servers）] タブを使用して、DNS スヌーピング用の信頼された DNS サービスを構成できます。

（注） アプリケーションベースの PBR の場合、信頼された DNS サーバーを構成する必要があります。また、ドメインを解決してアプリケーションを検出できるように、DNS トラフィックがクリアテキスト形式で Threat Defense を通過するようにする必要があります（暗号化された DNS はサポートされていません）。

始める前に

- 1 つ以上の DNS サーバーグループを作成していることを確認します。詳細については、DNS サーバー グループ オブジェクトの作成を参照してください。
- DNS サーバーに接続するためのインターフェイス オブジェクトが作成されていることを確認します。
- 管理対象デバイスに、DNS サーバーにアクセスするための適切なスタティックルートまたはダイナミックルートがあることを確認します。

ステップ 1 **[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]** を選択し、Threat Defense ポリシーを編集します。

ステップ 2 [編集（Edit）]（✎）アイコンをクリックします。

ステップ 3 [DNS] をクリックします。

ステップ 4 信頼された DNS サーバーを構成するには、[信頼されたDNSサーバー（Trusted DNS Servers）] タブをクリックします。

ステップ 5 既存のホストオブジェクトから **DNS_Server** を選択するには、[使用可能なホストオブジェクト（Available Host Objects）] で検索フィールドを使用してそのサーバーを検索し、[追加（Add）] をクリックして [選択済みDNSサーバー（Selected DNS Servers）] リストに追加します。

（注） **DNS_Server** は、この例で設定された DNS サーバーです。

ステップ 6 [保存（Save）] をクリックします。追加された DNS サーバーは、[信頼されたDNSサーバー（Trusted DNS Servers）] ページに表示されます。

ステップ 7 [ポリシー割り当て（Policy Assignments）] をクリックして、**NGFWBR1** が [選択されたデバイス（Selected Devices）] リストにすでにあることを確認します。

ステップ 8 [OK] をクリックして、変更内容を確定します。

ステップ 9 [保存（Save）] をクリックして、プラットフォーム設定の変更を書き込みます。

インターフェイスの優先順位の設定

Cisco Secure Firewall Threat Defense は、インターフェイスの優先順位を使用して最適なインターネットパスを決定します。優先順位の範囲は 0 ～ 65535 で、インターネットにトラフィックを送信するときの特定の ISP の優先順位を決定します。トラフィックは、インターフェイスの優先順位に基づいて転送されます。トラフィックは、優先度が最も低いインターフェイスに最初にルーティングされます。インターフェイスが使用できない場合、トラフィックは次に優先順位値が低いインターフェイスに転送されます。たとえば、outside2 と outside3 の優先順位値がそれぞれ 10 と 20 に設定されているとします。トラフィックは outside2 に転送されます。outside2 が使用できなくなった場合、トラフィックは outside3 に転送されます。

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** を選択し、Threat Defense デバイス（**NGFWBR1**）を編集します。

ステップ 2 NGFWBR1 のインターフェイスビューで [ルーティング（Routing）] タブをクリックします。

ステップ 3 [ポリシーベースルーティング（Policy Based Routing）] をクリックします。

ステップ 4 [インターフェイスの優先順位の設定（Configure Interface Priority）] をクリックします。

ステップ 5 ダイアログボックスで、インターフェイスに対して優先順位番号を指定します。

すべてのインターフェイスで優先度値が同じである場合、トラフィックはインターフェイス間で分散されます。

ステップ 6 [保存（Save）] をクリックします。

ECMP ゾーンの作成

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** を選択し、Threat Defense デバイス（**NGFWBR1**）を編集します。

ステップ 2 NGFWBR1 のインターフェイスビューで [ルーティング（Routing）] タブをクリックします。

ステップ 3 [ECMP] をクリックします。

ステップ 4 [Add] をクリックします。

ステップ 5 [ECMPの追加（Add ECMP）] ボックスで、ECMP ゾーンの名前に **ECMP-WAN** と入力します。

ステップ 6 インターフェイスを関連付けるには、[使用可能なインターフェイス（Available Interfaces）] ボックスでインターフェイスを選択し、[追加（Add）] をクリックします。

ステップ 7 [OK] をクリック

[ECMP] ページに、新しく作成された ECMP ゾーンが表示されます。

ステップ 8 [保存（Save）] をクリックします。

等コストスタティックルートの設定

グローバル仮想ルータとユーザー定義仮想ルータのどちらも、そのインターフェイスをデバイスの ECMP ゾーンに割り当てることができます。

始める前に

- インターフェイスの等コストスタティックルートを設定する場合は、必ず、それを ECMP ゾーンに関連付けてください。ECMP ゾーンの作成 （48 ページ） を参照してください。
- インターフェイスを ECMP ゾーンに関連付けずに、同じ宛先とメトリックでインターフェイスのスタティックルートを定義することはできません。

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** ページから、Threat Defense デバイス（**NGFWBR1**）を編集します。

ステップ 2 [ルーティング（Routing）] タブをクリックします。

ステップ 3 ドロップダウンリストから、インターフェイスが ECMP ゾーンに関連付けられている仮想ルータを選択します。

ステップ 4 インターフェイスの等コストスタティックルートを設定するには、[スタティックルート（Static Route）] をクリックします。

ステップ 5 [ルートを追加（Add Route）] をクリックして新しいルートを追加するか、既存のルートの場合は [編集（Edit）]（✎） をクリックします。

ステップ 6 [インターフェイス（Interface）] ドロップダウンから、仮想ルータと ECMP ゾーンに属するインターフェイスを選択します。

ステップ 7 [使用可能なネットワーク（Available Networks）] ボックスから宛先ネットワークを選択し、[追加（Add）] をクリックします。

ステップ 8 ネットワークのゲートウェイを入力します。

ステップ 9 メトリック値を入力します。1 ～ 254 の数値を指定できます。

ステップ 10 設定を保存するには、[Save] をクリックします。

ステップ 11 等コストスタティックルーティングを設定するには、手順を繰り返して、同じ ECMP ゾーンに含まれる別のインターフェイスのスタティックルートを、同じ宛先ネットワークとメトリック値で設定します。必ず、別のゲートウェイを指定してください。

パスモニタリングの設定

PBR ポリシーは、往復時間（RTT）、ジッター、平均オピニオン評点（MOS）、インターフェイスのパケット損失などの柔軟なメトリックを使用して、そのトラフィックに最適なルーティングパスを識別します。パスモニタリングは、指定されたインターフェイスでこれらのメトリックを収集します。[インターフェイス（Interface）] ページで、パスモニタリングの設定を使用してインターフェイスを設定し、メトリック収集のためにプローブを送信できます。

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、Threat Defense デバイス（**NGFWBR1**）の [編集（Edit）]（✎） をクリックします。

ステップ 2 編集するインターフェイス（**outside**）の [編集（Edit）]（✎） をクリックします。

ステップ 3 [パスモニタリング（Path Monitoring）] タブをクリックします。

ステップ 4 [IPベースのパスモニタリングの有効化（Enable IP based Path Monitoring）] チェックボックスをオンにします。

ステップ 5 [モニタリングタイプ（Monitoring Type）] ドロップダウンリストから、該当するオプションを選択します。この例では、デフォルト値の [インターフェイス外のデフォルトルートのネクストホップ（自動）（Next-hop of default route out of interface (Auto)）] を使用します。

ステップ 6 [OK] をクリックします。

ステップ 7 **outside2** および **outside3** インターフェイスに対してステップ 2 ～ 8 を繰り返します。

ステップ 8 [保存（Save）] をクリックします。

YouTube の拡張 ACL オブジェクトの設定

ポリシーベースルーティングを利用して、YouTube トラフィックがさまざまな出力インターフェイスからインターネットに向けて誘導されるように、アクセスリストが設定されます。

ステップ 1 **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]** を選択し、コンテンツテーブルから **[アクセスリスト（Access Lists）] > [拡張（Extended）]** を選択します。

ステップ 2 ソーシャル メディア トラフィック用の拡張アクセスリストを作成するには、[拡張アクセスリストの追加（Add Extended Access List）] をクリックします。

ステップ 3 [拡張ACLオブジェクト（Extended ACL Object）] ダイアログボックスで、オブジェクトの名前（**DIA_SocialMedia**）を入力します。

ステップ 4 [追加（Add）] をクリックして、新しい拡張アクセスリストを作成します。

ステップ 5 次のアクセス制御のプロパティを設定します。

1. トラフィック基準を許可（一致）するように [アクション（Action）] を選択します。
2. [アプリケーション（Application）] タブをクリックし、[使用可能なアプリケーション（Available Applications）] リストで **YouTube** を検索します。
3. [YouTube] を選択し、[ルールに追加（Add to Rule）] をクリックします。
4. [追加（Add）] をクリックして、エントリをオブジェクトに追加します。
5. [保存（Save）] をクリックします。

Webex の拡張 ACL オブジェクトの設定

ポリシーベースルーティングを利用して、Webex トラフィックがさまざまな出力インターフェイスからインターネットに向けて誘導されるように、アクセスリストが設定されます。

ステップ 1 **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]** を選択し、コンテンツテーブルから **[アクセスリスト（Access Lists）] > [拡張（Extended）]** を選択します。

ステップ 2 コラボレーショントラフィック用の拡張アクセスリストを作成するには、[拡張アクセスリストの追加（Add Extended Access List）] をクリックします。

ステップ 3 [拡張ACLオブジェクト（Extended ACL Object）] ダイアログボックスで、オブジェクトの名前（**DIA_Collaboration**）を入力します。

ステップ 4 [追加（Add）] をクリックして、新しい拡張アクセスリストを作成します。

ステップ 5 次のアクセス制御のプロパティを設定します。

1. トラフィック基準を許可（一致）するように [アクション（Action）] を選択します。
2. [アプリケーション（Application）] タブをクリックし、[使用可能なアプリケーション（Available Applications）] リストで **Webex** を検索します。
3. [Webex] を選択し、[ルールに追加（Add to Rule）] をクリックします。
4. [追加（Add）] をクリックして、エントリをオブジェクトに追加します。

5. [保存（Save）] をクリックします。

YouTube のポリシー ベース ルーティング ポリシーの設定

[ポリシーベースルーティング（Policy Based Routing）]ページで、YouTube トラフィックをルーティングするための入力インターフェイス、一致基準（拡張アクセスコントロールリスト）および出力インターフェイスを指定することにより、PBR ポリシーを設定できます。

YouTube トラフィックは、**outside** および **outside2** のインターフェイス間でロードバランシングされ、両方のリンクに障害が発生した場合は **outside3** にフォールバックします。

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、Threat Defense デバイス（**NGFWBR1**）を編集します。

ステップ 2 NGFWBR1 のインターフェイスビューで [ルーティング（Routing）] タブをクリックします。

ステップ 3 [ポリシーベースルーティング（Policy Based Routing）] をクリックします。

[ポリシーベースルーティング（Policy Based Routing）]ページに、設定されたポリシーが表示されます。グリッドには、入力インターフェイスのリストと、ポリシーベースのルートアクセスリストと出力インターフェイスの組み合わせが表示されます。

ステップ 4 ポリシーを設定するには、[追加（Add）] をクリックします。

ステップ 5 [ポリシーベースルートの追加（Add Policy Based Route）] ダイアログボックスで、[入力インターフェイス（Ingress Interface）] ドロップダウンリストから [inside] を選択します。

（注） ドロップダウンには、論理名を持ち、グローバル仮想ルータに属するインターフェイスのみが表示されます。

ステップ 6 ポリシーで一致基準と転送アクションを指定するには、[追加（Add）] をクリックします。

ステップ 7 [転送アクションの追加（Add Forwarding Actions）] ダイアログボックスで、次の操作を実行します。

a) [ACLの照合（Match ACL）] ドロップダウンから、[DIA_SocialMedia] を選択します。

b) 設定されたインターフェイスを選択するには、[送信先（Send To）] ドロップダウンリストから [出力インターフェイス（Egress Interfaces）] を選択します。

c) [インターフェイスの順序付け（Interface Ordering）] ドロップダウンリストから [優先順位による（By Priority）] を選択します。

トラフィックは、優先度が最も低いインターフェイスに最初にルーティングされます。そのインターフェイスが使用できない場合、トラフィックは次に優先順位値が低いインターフェイスに転送されます。たとえば、outside2 と outside3 の優先順位値がそれぞれ 10 と 20 に設定されているとします。トラフィックは outside2 に転送されます。outside2 が使用できなくなった場合、トラフィックは outside3 に転送されます。

d) [使用可能なインターフェイス（Available Interfaces）] ボックスに、すべてのインターフェイスとその優先度の値が一覧表示されます。**Add** (+) アイコンをクリックして、選択した出力インターフェイスを追加します。

このシナリオでは、次の手順を実行します。

1. [使用可能なインターフェイス（Available Interfaces）] から、**outside** および **outside2** インターフェイスの横にある **Add** (+) アイコンをクリックして、[選択した出力インターフェイス（Selected Egress Interfaces）] に移動します。
2. 次に、**outside3** インターフェイスの横にある **Add** (+) アイコンをクリックして、[選択した出力インターフェイス（Selected Egress Interfaces）] に移動します。

e) [保存（Save）] をクリックして、一致基準の変更を書き込みます。
f) 設定を確認し、[保存（Save）] をクリックして、ポリシーベースルーティングのすべての設定変更を書き込みます。

ステップ 8 [保存（Save）] をクリックします。

Webex のポリシー ベース ルーティング ポリシーの設定

[ポリシーベースルーティング（Policy Based Routing）] ページで、Webex アプリケーション トラフィックをルーティングするための入力インターフェイス、一致基準（拡張アクセスコントロールリスト）および出力インターフェイスを指定することにより、PBR ポリシーを設定できます。

Webex アプリケーション トラフィックは **outside3** にルーティングされ、プライマリリンクに障害が発生した場合は **outside2** にフォールバックします。

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、Threat Defense デバイス（**NGFWBR1**）を編集します。

ステップ 2 NGFWBR1 のインターフェイスビューで [ルーティング（Routing）] タブをクリックします。

ステップ 3 [ポリシーベースルーティング（Policy Based Routing）] をクリックします。

[ポリシーベースルーティング（Policy Based Routing）] ページに、設定されたポリシーが表示されます。グリッドには、入力インターフェイスのリストと、ポリシーベースのルートアクセスリストと出力インターフェイスの組み合わせが表示されます。

ステップ 4 ポリシーを編集するには、[編集（Edit）]（✎） アイコンをクリックします。

ステップ 5 ポリシーで一致基準と転送アクションを指定するには、[追加（Add）] をクリックします。

ステップ 6 [転送アクションの追加（Add Forwarding Actions）] ダイアログボックスで、次の操作を実行します。

a) [ACLの照合（Match ACL）] ドロップダウンから、[DIA_Collaboration] を選択します。

b) 設定されたインターフェイスを選択するには、[送信先（Send To）] ドロップダウンリストから [出力インターフェイス（Egress Interfaces）] を選択します。
c) [インターフェイスの順序付け（Interface Ordering）] ドロップダウンリストから [順序（Order）] を選択します。

トラフィックは、ここで指定されたインターフェイスの順序に基づいて転送されます。

d) [使用可能なインターフェイス（Available Interfaces）] ボックスに、すべてのインターフェイスとその優先度の値が一覧表示されます。**Add** ( ) アイコンをクリックして、選択した出力インターフェイスを追加します。

このシナリオでは、次の手順を実行します。

1. [使用可能なインターフェイス（Available Interfaces）] から、**outside3** インターフェイスの横にある **Add** ( ) アイコンをクリックして、[選択した出力インターフェイス（Selected Egress Interfaces）] に移動します。
2. 次に、**outside2** インターフェイスの横にある **Add** ( ) アイコンをクリックして、[選択した出力インターフェイス（Selected Egress Interfaces）] に移動します。

e) [保存（Save）] をクリックして、一致基準の変更を書き込みます。
f) 設定を確認し、[保存（Save）]をクリックして、ポリシーベースルーティングのすべての設定変更を書き込みます。

ステップ 7 [保存（Save）] をクリックします。

Webex のパスモニタリングを使用したポリシー ベース ルーティング ポリシーの設定

[ポリシーベースルーティング（Policy Based Routing）] ページで、パスモニタリングを使用した PBR ポリシーを設定できます。この例では、Webex のアプリケーション トラフィックが、トラフィック損失が最も少ないインターフェイスに転送されます。

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、Threat Defense デバイス（**NGFWBR1**）を編集します。

ステップ 2 NGFWBR1 のインターフェイスビューで [ルーティング（Routing）] タブをクリックします。

ステップ 3 [ポリシーベースルーティング（Policy Based Routing）] をクリックします。

[ポリシーベースルーティング（Policy Based Routing）]ページに、設定されたポリシーが表示されます。グリッドには、入力インターフェイスのリストと、ポリシーベースのルートアクセスリストと出力インターフェイスの組み合わせが表示されます。

ステップ 4 ポリシーを設定するには、[追加（Add）] をクリックします。

ステップ 5 [ポリシーベースルートの追加（Add Policy Based Route）] ダイアログボックスで、[入力インターフェイス（Ingress Interface）] ドロップダウンリストから [inside] を選択します。

（注） ドロップダウンには、論理名を持ち、グローバル仮想ルータに属するインターフェイスのみが表示されます。

ステップ 6 ポリシーで一致基準と転送アクションを指定するには、[追加（Add）] をクリックします。

ステップ 7 [転送アクションの追加（Add Forwarding Actions）] ダイアログボックスで、次の操作を実行します。

a) [ACLの照合（Match ACL）] ドロップダウンから、[DIA_Collaboration] を選択します。

b) 設定されたインターフェイスを選択するには、[送信先（Send To）] ドロップダウンリストから [出力インターフェイス（Egress Interfaces）] を選択します。

c) [インターフェイスの順序付け（Interface Ordering）] ドロップダウンリストから [最小パケット損失（Minimal Packet Loss）] を選択します。

トラフィックは、パケット損失が最小のインターフェイスに転送されます。

d) [使用可能なインターフェイス（Available Interfaces）] ボックスに、すべてのインターフェイスが一覧表示されます。インターフェイスのリストから、**Add (**) アイコンをクリックして、選択した出力インターフェイスを追加します。

このシナリオでは、次の手順を実行します。

1. [使用可能なインターフェイス（Available Interfaces）] から、**outside3** インターフェイスの横にある **Add (**) アイコンをクリックして、[選択した出力インターフェイス（Selected Egress Interfaces）] に移動します。

2. 次に、**outside2** インターフェイスの横にある **Add (**) アイコンをクリックして、[選択した出力インターフェイス（Selected Egress Interfaces）] に移動します。

e) [保存（Save）] をクリックして、一致基準の変更を書き込みます。

f) 設定を確認し、[保存（Save）]をクリックして、ポリシーベースルーティングのすべての設定変更を書き込みます。

ステップ 8 [保存（Save）] をクリックします。

設定の展開

すべての設定が完了したら、管理対象デバイスに設定を展開します。

ステップ 1 Management Center メニューバーで、[展開（Deploy）] をクリックします。

ステップ 2 設定の変更を展開する NGFWBR1 の横にあるチェックボックスをオンにします。

ステップ 3 [展開（Deploy）] をクリックします。

ステップ 4 展開する変更に関するエラーや警告がシステムによって識別された場合は、[検証エラー（Validation Errors）] または [検証の警告（Validation Warnings）] ウィンドウにその内容が表示されます。完全な詳細を表示するには、[検証エラー（Validation Errors）] または [検証の警告（Validation Warnings）] リンクをクリックします。

次の選択肢があります。

- [展開の続行（Proceed with Deploy）]：警告状態を解決せずに展開を続行します。システムがエラーを確認した場合は続行できません。
- [閉じる（Close）]：展開せずに終了します。エラーおよび警告状態を解決し、設定の再展開を試行します。

アプリケーション トラフィック フローの確認

ステップ 1 Management Center のインターフェイスで、[分析（Analysis）] > [統合イベント（Unified Events）] を選択します。

ステップ 2 [Webアプリケーション（Web Application）] と [出力インターフェイス（Egress Interface）] を選択し、[適用（Apply）] をクリックすることで、列ピッカーを使用して列をカスタマイズします。

ステップ 3 確認しやすいように列の順序を変更します。

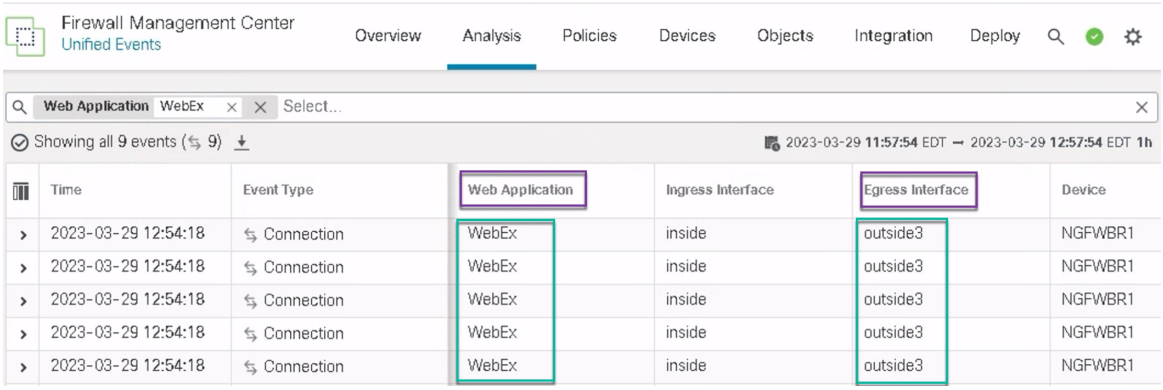
ステップ 4 [Webアプリケーション（Web Application）] フィルタ内で、**Webex** という名前を入力し、[適用（Apply）] をクリックします。

ステップ 5 [Webアプリケーション（Web Application）] フィルタ内で、**YouTube** という名前を入力し、[適用（Apply）] をクリックします。

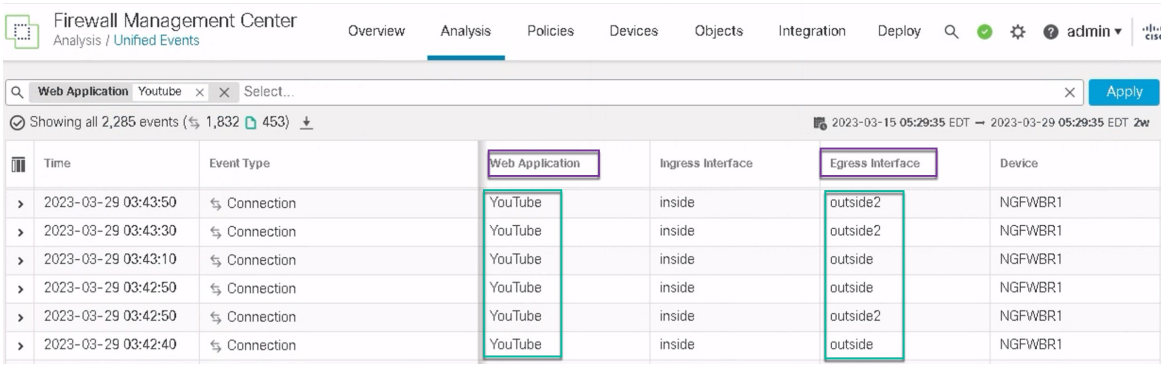
ステップ 6 Cisco Secure Firewall の背後にあるホストで **YouTube** および **Webex** アプリケーションのトラフィックを開始します。このシナリオでは、ブランチワークステーション **WKST BR1** で Google Chrome ブラウザを起動し、異なるタブで https://youtube.com と https://webex.com に移動します。

ステップ 7 Management Center で、両方のアプリケーションのトラフィックフローを確認します。

1. パスモニタリングを使用しない DIA の場合：
   - **Webex** アプリケーション トラフィックは、次の図に示すように、設定に従って **outside3** インターフェイスを介して送信されます。

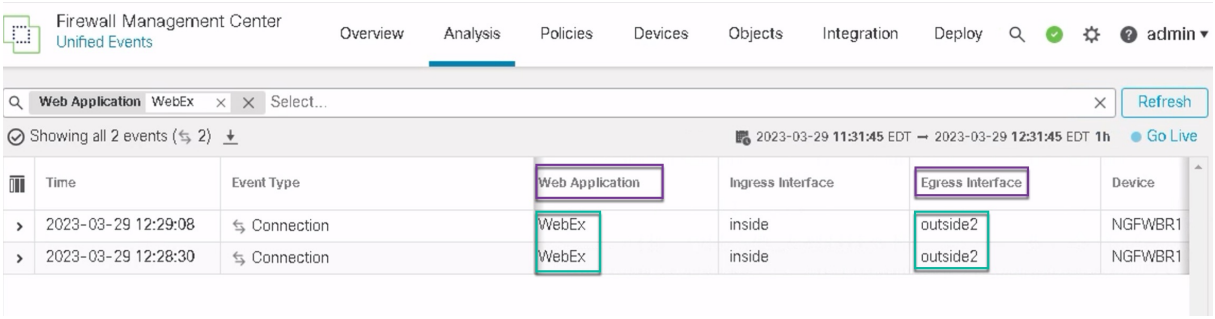


- **YouTube** アプリケーション トラフィックは、次の図に示すように、設定に従って **outside** および **outside2** インターフェイスの間でロードバランシングされます。



2. パスモニタリングを使用する DIA の場合：

   Webex アプリケーション トラフィックは、次の図に示すように、**outside3** インターフェイスでパケット損失があるため、**outside2** インターフェイスを介して送信されます。



ポリシーベースルーティングのモニターとトラブルシューティング

展開後に、次の CLI を使用して、Cisco Secure Firewall Threat Defense でのポリシーベースルーティングに関連する問題をモニターおよびトラブルシューティングします。

操作	CLI コマンド
Cisco Secure Firewall Threat Defense の Lina CLI にログインする	**system support diagnostic-cli**
展開中に Management Center から Threat Defense にプッシュされる事前定義されたネットワーク サービス オブジェクトを表示する	• **show object network-service** • **show object network-service detail**
設定されたアプリケーションに関連する特定のネットワーク サービス オブジェクト（NSG）を表示する	• **show object id YouTube** • **show object id WebEx**
Cisco Secure Firewall にプッシュされるネットワーク サービス グループ（NSG）を確認する	**show run object-group network-service**
ポリシーベースルーティングに関連付けられたルートマップを表示する	**show run route-map**
インターフェイス名やインターフェイスの優先順位などのインターフェイス設定の詳細を確認する	**show run interface**
信頼された DNS サーバーの設定を確認する	**show dns**
トラフィックが通過したパスを特定する	**debug policy-route** **重要** debug コマンドではトラフィックに基づいた詳細な出力が行われる可能性があるため、特に実稼働環境では注意して実行してください。
ルートのデバッグを停止する	**undebug all**

事前定義されたネットワーク サービス オブジェクトを表示するには、次のコマンドを使用します。

```
ngfwbr1# show object network-service
object network-service "ADrive" dynamic
 description Online file storage and backup.
 app-id 17
```

```
 domain adrive.com (bid=0) ip (hitcnt=0)
object network-service "Amazon" dynamic
 description Online retailer of books and most other goods.
 app-id 24
 domain amazon.com (bid=0) ip (hitcnt=0)
 domain amazon.jobs (bid=0) ip (hitcnt=0)
 domain amazon.in (bid=0) ip (hitcnt=0)
.
.
.
output snipped
.
.
.
object network-service "Logitech" dynamic
 description Company develops Computer peripherals and accessories.
 app-id 4671
 domain logitech.com (bid=0) ip (hitcnt=0)
object network-service "Lenovo" dynamic
 description Company manufactures/markets computers, software and related services.
 app-id 4672
 domain lenovo.com (bid=0) ip (hitcnt=0)
 domain lenovo.com.cn (bid=0) ip (hitcnt=0)
 domain lenovomm.com (bid=0) ip (hitcnt=0)
ngfwbr1#
```

YouTube や Webex などの特定のネットワーク サービス オブジェクトを表示するには、次のコマンドを使用します。

```
ngfwbr1# show object id YouTube
object network-service "YouTube" dynamic
 description A video-sharing website on which users can upload, share, and view videos.
 app-id 929
 domain youtubei.googleapis.com (bid=592729) ip (hitcnt=0)
 domain yt3.ggpht.com (bid=709809) ip (hitcnt=102)
 domain youtube.com (bid=830871) ip (hitcnt=101)
 domain ytimg.com (bid=1035543) ip (hitcnt=93)
 domain googlevideo.com (bid=1148165) ip (hitcnt=466)
 domain youtu.be (bid=1247981) ip (hitcnt=0)
ngfwbr1# show object id WebEx
object network-service "WebEx" dynamic
 description Cisco's online meeting and web conferencing application.
 app-id 905
 domain files-prod-us-east-2.webexcontent.com (bid=182837) ip (hitcnt=0)
 domain webex.com (bid=290507) ip (hitcnt=30)
 domain avatar-prod-us-east-2.webexcontent.com (bid=452667) ip (hitcnt=0)
ngfwbr1#
```

NSG が Threat Defense にプッシュされていることを確認するには、次のコマンドを使用します。

```
ngfwbr1# show run object-group network-service
object-group network-service FMC_NSG_292057776181
 network-service-member "WebEx"
object-group network-service FMC_NSG_292057776200
 network-service-member "YouTube"
ngfwbr1#
```

PBR に関連付けられたルートマップを確認するには、次のコマンドを使用します。

```
ngfwbr1# show run route-map
!
route-map FMC_GENERATED_PBR_1678091359817 permit 5
 match ip address DIA_Collaboration
```

```
 set interface outside3 outside2

!
route-map FMC_GENERATED_PBR_1678091359817 permit 10
 match ip address DIA_SocialMedia
 set adaptive-interface cost outside outside2 outside3
!
ngfwbr1#
```

インターフェイス設定とインターフェイスの優先順位の詳細を確認するには、次のコマンドを使用します。

```
ngfwbr1# show run interface
!
interface GigabitEthernet0/0
 nameif outside
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
 security-level 0
  zone-member ECMP-WAN
 ip address 198.18.128.81 255.255.192.0
 policy-route cost 10
!
interface GigabitEthernet0/1
 nameif inside
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
 security-level 0
 ip address 198.19.11.4 255.255.255.0
 policy-route route-map FMC_GENERATED_PBR_1678091359817
!
interface GigabitEthernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/3
 nameif outside2
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
 security-level 0
 zone-member ECMP-WAN
 ip address 198.19.40.4 255.255.255.0
 policy-route cost 10
!
interface GigabitEthernet0/4
 nameif outside3
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
 security-level 0
 ip address 198.19.30.4 255.255.255.0
 policy-route cost 20
!
interface Management0/0
 management-only
 nameif diagnostic
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
```

```
 security-level 0
 no ip address
ngfwbr1#
```

信頼された DNS 設定を確認するには、次のコマンドを使用します。

```
ngfwbr1# show dns

DNS Trusted Source enabled for DHCP Server Configured
DNS Trusted Source enabled for DHCP Client Learned
DNS Trusted Source enabled for DHCP Relay Learned
DNS Trusted Source enabled for DNS Server Configured
DNS Trusted Source not enabled for Trust-any
DNS Trusted Source: Type: IPs : Interface : Idle/Timeout (sec)
    DNS Server Configured: 198.19.10.100: <ifc-not-specified> : N/A
Trusted Source Configured: 198.19.10.100: <ifc-not-specified> : N/A
DNS snooping IP cache: 0 in use, 37 most used
Address                              Idle(sec) Timeout(sec) Hit-count          Branch(es)
ngfwbr1#
```

ポリシールートをデバッグするには、次のコマンドを使用します。

```
ngfwbr1# debug policy-route
debug policy-route  enabled at level 1
ngfwbr1# pbr: policy based route lookup called for 198.19.11.225/58119 to 198.19.10.100/53
 proto 17 sub_proto 0 received on interface inside, NSGs, nsg_id=none
pbr: no route policy found; skip to normal route lookup
.
output-snipped
.
pbr: policy based route lookup called for 198.19.11.225/61482 to 63.140.48.151/443 proto
 6 sub_proto 0 received on interface inside
                                                                , NSGs, nsg_id=1
pbr: First matching rule from ACL(2)
pbr: route map FMC_GENERATED_PBR_1678091359817, sequence 5, permit; proceed with policy
 routing
pbr: evaluating interface outside3
pbr: policy based routing applied; egress_ifc = outside3 : next_hop = 198.19.30.63

ngfwbr1#
```

上記のデバッグ例は、Webex のトラフィック用です。PBR によりルートパスが outside2 インターフェイスに変更される前は、トラフィックが outside3 インターフェイスを介してルーティングされることに注意してください。

デバッグプロセスを停止するには、次のコマンドを使用します。

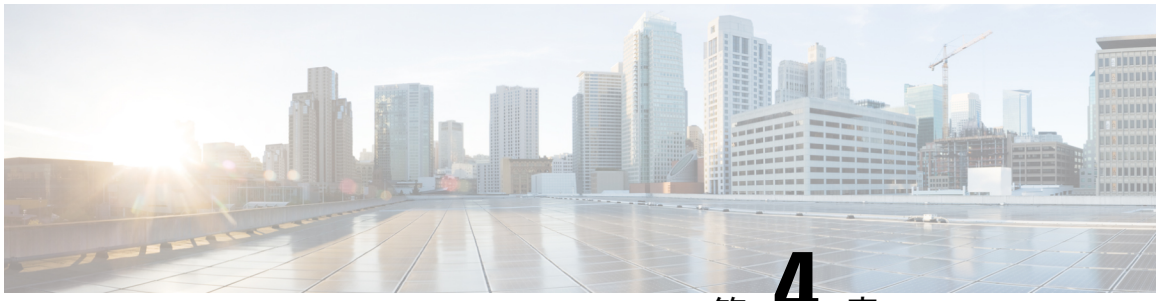
```
ngfwbr1# undebug all
```

関連リソース

リソース（Resource）	URL
Cisco Secure Firewall Threat Defense リリースノート	https://www.cisco.com/go/firewall-release-notes
すべての新機能と廃止された機能	http://www.cisco.com/go/whatsnew-fmc
Cisco.com の Cisco Secure Firewall	http://www.cisco.com/go/firewall

リソース（Resource）	URL
Cisco.com のマニュアル	http://www.cisco.com/go/firewall-docs
YouTube 上の Cisco Secure Firewall	https://www.youtube.com/cisco-netsec
Cisco Secure Firewall Essentials	https://secure.cisco.com/secure-firewall

関連リソース



第 4 章

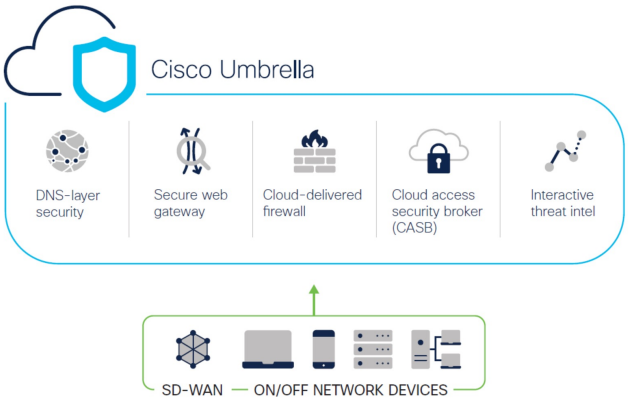
Cisco Umbrella 自動トンネルを使用したセキュアなインターネットトラフィック

この章では、Cisco Umbrella 自動トンネルの実践的な応用について詳しく説明します。この使用例では、シナリオ、ネットワークトポロジ、ベストプラクティス、および前提条件について詳しく説明します。また、シームレスな導入のための包括的なエンドツーエンドの手順も提供します。

Cisco Umbrella 自動トンネル

ドメインネームシステム（DNS）は、攻撃でよく使用されるインターネットプロトコルです。マルウェアの 90% が DNS を使用しています（出典：Cisco Security Research Report）。しかし、多くの組織は、DNS をモニターせず、DNS に焦点を当てたセキュリティを使用していません。

図 *4 : Cisco Umbrella*



Cisco Umbrella は、クラウドベースのセキュア インターネット ゲートウェイ プラットフォームです。インターネットベースの脅威に対する防御を複数のレベルで提供します。Cisco Umbrella は、DNS 層のセキュリティ、クラウド アクセス セキュリティ ボーダー（CASB）機能、クラウド提供型ファイアウォール、およびセキュア Web ゲートウェイを統合して、ブランチのリソースに関係なく、拡張性の高いセキュリティを提供します。インターネット宛トラフィックを、インターネットへのアクセスが許可または拒否される前に、検査のために、ブランチから最も近い Cisco Umbrella アクセスポイントにセキュアに自動的に送信することができます。

リリース 7.3 以降、Cisco Secure Firewall Management Center は Cisco Umbrella セキュア インターネット ゲートウェイ（SIG）統合の自動トンネル設定をサポートしています。これにより、ネットワークデバイスは DNS および Web トラフィックを Cisco Umbrella SIG に転送して、SIG トンネルを介した検査とフィルタリングを行うことができます。

Cisco Umbrella 内で定義された DNS および Web ポリシーは、Cisco Secure Firewall を介して接続に適用できます。これにより、ドメイン名に基づいてリクエストを適用および検証することができます。

Management Center では、このトンネルを構築するための、新しい簡素化された直感的なウィザードベースのインターフェイスが提供されるため、Firewall Threat Defense と Cisco Umbrella での設定手順を最小限に抑えることができます。

Management Center は、Cisco Umbrella API を使用して、Cisco Umbrella の接続設定のパラメータを使用してネットワークトンネルを設定します。次に、Management Center は Cisco Umbrella データセンターのリストを取得し、SASE トポロジのハブとして選択できるようにユーザーインターフェイスに表示します。ネットワークトンネルが Threat Defense デバイスで展開され、Management Center での展開が完了した後に Cisco Umbrella で自動的に作成されます。これは、オンプレミスユーザーとローミングユーザーに統一された DNS ポリシーと Web ポリシーを適用するために役立ちます。

利点

Cisco Umbrella を使用したインターネットトラフィックの保護には、次のような利点があります。

- 接続が確立される前に DNS 層でユーザーとアプリケーションを保護することで、結果として生じるパケット処理を減らし、より迅速な保護を実現します。
- ハイブリッドユーザー（オンプレミスユーザーとローミングユーザー）に、統一された DNS 制御ポリシーが適用されます。
- Cisco Umbrella は、接続が確立される前でも、Web リクエストだけでなく、マルウェア、ランサムウェア、フィッシング攻撃、およびボットネットに対するリクエストもブロックするため、ネットワークまたはエンドポイントに到達する前に脅威を阻止できます。これにより、修復が必要な感染とアラートの数が大幅に減少します。
- URL フィルタリングや TLS 復号などの高度なファイアウォール機能が不要になります。
- 自動トンネルセットアップには、Management Center での最小限の設定が必要です。
- Cisco Umbrella ダッシュボードでの自動ネットワークトンネル設定。

この使用例の対象者

Cisco Umbrella SASE 自動トンネル設定の対象者は、組織のネットワーク インフラストラクチャの管理と保護を担当する IT チーム、ネットワーク管理者、およびセキュリティ プロフェッショナルです。これらのユーザーは、セキュアなリモートアクセスのための高度なソリューションの検討と、セキュアなトンネルの設定と管理の簡素化に関心があります。Cisco Umbrella SASE 自動トンネル設定の説明は、ネットワークセキュリティの強化、リモート接続の合理化、および組織のリモートワークフォースの全体的なユーザー体験の向上を求めるユーザーにとって魅力的です。

シナリオ

IT 管理者である Alice は、組織の IT インフラストラクチャを管理し、セキュリティを確保する責任を負っています。Alice はサイバースペースでの脅威の増加を認識していて、マルウェア、ランサムウェア、フィッシングなどの潜在的なサイバー攻撃を防ぐために、堅牢なセキュリティ対策を導入したいと考えています。

Sally は分散拠点で働き、仕事関連のアクティビティのために組織のネットワークを使用してインターネットにアクセスする従業員です。

リスクがあるもの

適切なセキュリティ対策を講じていない場合、従業員が知らないうちに悪意のある Web サイトにアクセスし、有害なソフトウェアをダウンロードする可能性があります。これにより、組織のネットワークセキュリティとデータプライバシーが侵害される可能性があります。

SIG 統合によって問題がどのように解決されるか

Alice は、ブランチファイアウォールと Cisco Umbrella を使用して 2 層のセキュリティアプローチを導入しました。このファイアウォールは、Web ベースおよび非 Web ベースの攻撃に対す

るネットワークのインバウンドセキュリティを提供しました。Cisco Umbrella は、DNS 層および Web 層で悪意のあるドメイン、IP、および URL をブロックすることで、アウトバウンドセキュリティを提供しました。

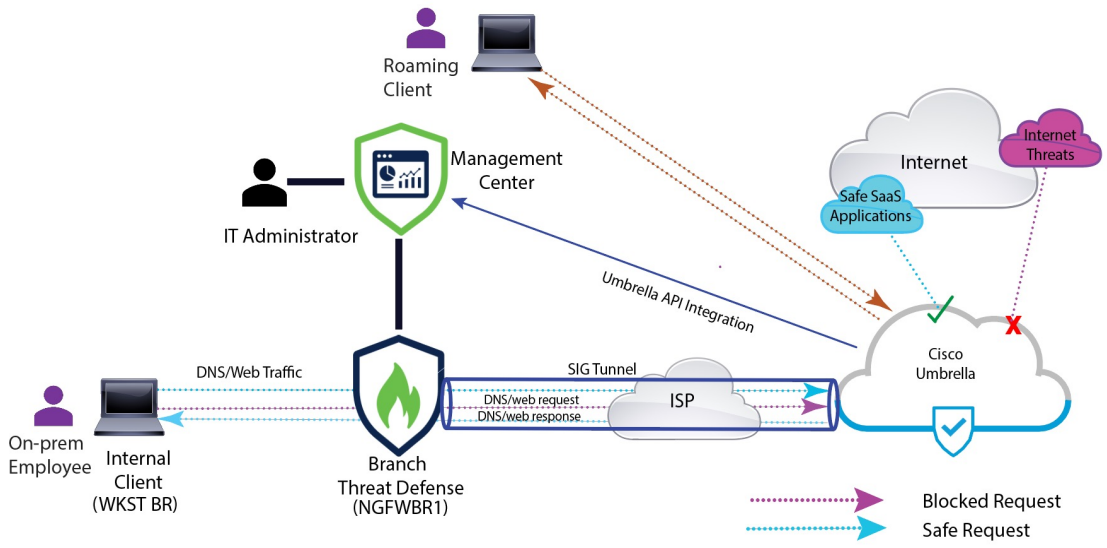
Sally は、一部の Web サイトがファイアウォールと Cisco Umbrella によってブロックされるようになったことに気が付きました。

オンプレミスユーザーとリモートユーザーの両方が、Cisco Umbrella ダッシュボード内で定義された同じ DNS ポリシーと Web ポリシーの対象となります。この導入の結果、組織のネットワークはより安全になり、潜在的なサイバー攻撃から保護されます。

ネットワーク トポロジ

このトポロジでは、Threat Defense デバイスがブランチロケーションに展開されます。次の図では、内部クライアントまたはブランチワークステーションには WKST BR というラベルが付けられ、ブランチの Threat Defense には NGFWBR1 というラベルが付けられています。NGFWBR1 と Cisco Umbrella の間に SIG 自動トンネルが設定されています。

図 *5 : Cisco Umbrella* 自動トンネル設定のネットワークトポロジ



すべての DNS および Web トラフィックは、SIG トンネルを介して Cisco Umbrella に送信され、Cisco Umbrella の DNS および Web ポリシーに基づいて検証され、許可またはブロックされます。これにより、2 つの保護層が提供されます。1 つは Cisco Secure Threat Defense によってローカルに適用され、もう 1 つは Cisco Umbrella によってクラウドで提供されます。

DNS トラフィックの場合：

1. Cisco Umbrella は、分類されていないドメインの DNS リクエストを検出すると、ドメインのレピュテーションをクエリします。
2. ドメインが悪意のあるものとして分類された場合、DNS リクエストはブロックされ、エンドユーザーは Web サイトにアクセスできなくなります。

3. ドメインが安全なものとして分類された場合、DNS リクエストは解決され、エンドユーザーは Web サイトにアクセスできます。

SASE Cisco Umbrella トンネルのベストプラクティス

- Management Center で、輸出規制機能のある基本ライセンスが有効になっていることを確認します。
- インターネットに面する Threat Defense インターフェイスには、**outside** という名前またはプレフィックスを付けることを推奨します。
- Cisco Umbrella への展開がそのトポロジで実行されている場合は、SASE トポロジを編集または削除しないでください。
- バックアップ Cisco Umbrella DC を設定するには、バックアップ Cisco Umbrella DC を使用して、同じ Threat Defense エンドポイントを持つ同じトポロジを複製します。
- Threat Defense エンドポイントでバックアップ インターフェイスを設定するには、バックアップ インターフェイスで VTI を使用して、同じ Threat Defense エンドポイントを持つ同じ Cisco Umbrella DC を持つ同じトポロジを複製します。

Cisco Umbrella SASE トンネルを設定するための前提条件

- Device Manager を使用した Threat Defense の初期設定の完了
- デバイスへのライセンスの割り当て
- インターネットアクセスのルートの追加。「スタティックルートの追加」を参照してください。
- 脅威に対する防御のための NAT の設定
- 基本的なアクセス コントロール ポリシーの作成
- Cisco Umbrella Secure Internet Gateway（SIG）Essentials サブスクリプションまたは無料の SIG トライアルバージョンが必要です。
- Management Center から Cisco Umbrella にトンネルを展開するには、輸出規制機能を使用してスマート ライセンス アカウントを有効にする必要があります。
- http://login.umbrella.com で Cisco Umbrella にログインし、Cisco Umbrella への接続を確立するために必要な情報を取得します。Management Center が management.api.umbrella.com に到達できることを確認します。
- 自分の Cisco Umbrella の組織を Management Center に登録し、Cisco Umbrella の接続の詳細設定で管理キーと管理シークレットを設定する必要があります。これにより、Cisco Umbrella クラウドからデータセンターの詳細が取得されます。Cisco Umbrella の接続の全般設定で、[組織ID（Organization ID）]、[ネットワークデバイスキー（Network Device Key）]、[ネッ

トワークデバイスシークレット（Network Device Secret）]、および[レガシーネットワークデバイストークン（Legacy Network Device Token）] も設定する必要があります。

詳細については、以下を参照してください。

- Cisco Umbrella の接続設定の設定
- Management Center の Cisco Umbrella パラメータと Cisco Umbrella API キーのマッピング

- Threat Defense から Cisco Umbrella データセンターに到達できることを確認します。
- Threat Defense がローカルトンネル ID をサポートするルートベース VPN（バージョン 7.1.0 以降）をサポートしていることを確認します。Management Center バージョン 7.3.0 以降では、ローカルトンネル ID をサポートする SASE トンネルを展開できます。

SASE Cisco Umbrella トンネルのベストプラクティス

- Management Center で、輸出規制機能のある基本ライセンスが有効になっていることを確認します。
- インターネットに面する Threat Defense インターフェイスには、**outside** という名前またはプレフィックスを付けることを推奨します。
- Cisco Umbrella への展開がそのトポロジで実行されている場合は、SASE トポロジを編集または削除しないでください。
- バックアップ Cisco Umbrella DC を設定するには、バックアップ Cisco Umbrella DC を使用して、同じ Threat Defense エンドポイントを持つ同じトポロジを複製します。
- Threat Defense エンドポイントでバックアップ インターフェイスを設定するには、バックアップ インターフェイスで VTI を使用して、同じ Threat Defense エンドポイントを持つ同じ Cisco Umbrella DC を持つ同じトポロジを複製します。

Cisco Umbrella SASE トンネルを設定するための前提条件

- Device Manager を使用した Threat Defense の初期設定の完了
- デバイスへのライセンスの割り当て
- インターネットアクセスのルートの追加。「スタティックルートの追加」を参照してください。
- 脅威に対する防御のための NAT の設定
- 基本的なアクセス コントロール ポリシーの作成

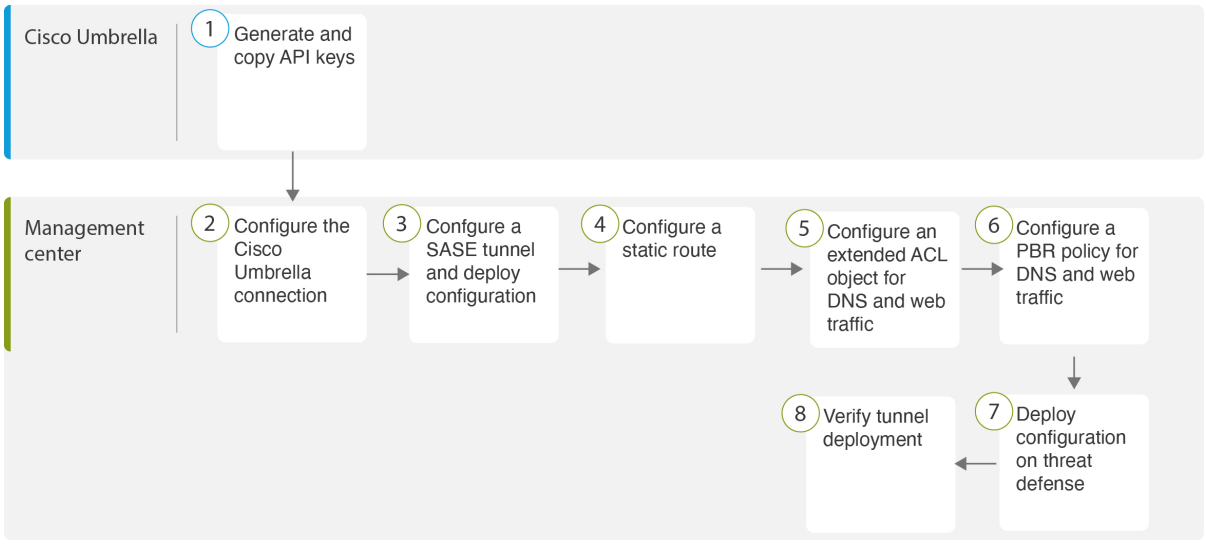
- Cisco Umbrella Secure Internet Gateway（SIG）Essentials サブスクリプションまたは無料の SIG トライアルバージョンが必要です。
- Management Center から Cisco Umbrella にトンネルを展開するには、輸出規制機能を使用してスマート ライセンス アカウントを有効にする必要があります。
- http://login.umbrella.com で Cisco Umbrella にログインし、Cisco Umbrella への接続を確立するために必要な情報を取得します。Management Center が management.api.umbrella.com に到達できることを確認します。
- 自分の Cisco Umbrella の組織を Management Center に登録し、Cisco Umbrella の接続の詳細設定で管理キーと管理シークレットを設定する必要があります。これにより、Cisco Umbrella クラウドからデータセンターの詳細が取得されます。Cisco Umbrella の接続の全般設定で、[組織ID（Organization ID）]、[ネットワークデバイスキー（Network Device Key）]、[ネットワークデバイスシークレット（Network Device Secret）]、および[レガシーネットワークデバイストークン（Legacy Network Device Token）] も設定する必要があります。

  詳細については、以下を参照してください。

  - Cisco Umbrella の接続設定の設定
  - Management Center の Cisco Umbrella パラメータと Cisco Umbrella API キーのマッピング
- Threat Defense から Cisco Umbrella データセンターに到達できることを確認します。
- Threat Defense がローカルトンネル ID をサポートするルートベース VPN（バージョン 7.1.0 以降）をサポートしていることを確認します。Management Center バージョン 7.3.0 以降では、ローカルトンネル ID をサポートする SASE トンネルを展開できます。

Cisco Umbrella 自動トンネルを設定するためのエンドツーエンドの手順

次のフローチャートは、Cisco Secure Firewall Management Center で SASE トンネルを設定するためのワークフローを示しています。



ステップ	説明
1	（前提条件）Cisco Umbrella で API キーを生成してコピーします。「Management Center の Cisco Umbrella パラメータと Cisco Umbrella API キーのマッピング」を参照してください。
2	（前提条件）Cisco Umbrella の接続を設定します。「Cisco Umbrella の接続設定の設定」を参照してください。
3	SASE トンネルを作成し、設定を Threat Defense に展開します。Cisco Umbrella 用の SASE トンネルの設定 （71 ページ）を参照してください。
4	静的ルートを設定します。スタティック ルートの設定 （74 ページ）を参照してください。
5	DNS および Web トラフィックの拡張 ACL オブジェクトを設定します。DNS および Web トラフィックの拡張 ACL の設定 （75 ページ）を参照してください。
6	DNS および Web トラフィックの PBR ポリシーを設定します。DNS および Web トラフィックの PBR ポリシーの設定 （76 ページ）を参照してください。
7	設定を Threat Defense に展開します。設定の展開 （23 ページ）を参照してください。
8	トンネルの展開を確認します。SASE Cisco Umbrella トンネルの展開の確認 （77 ページ） を参照してください。

Cisco Umbrella 用の SASE トンネルの設定

始める前に

必ずCisco Umbrella SASE トンネルを設定するための前提条件 （67 ページ）およびSASE Cisco Umbrella トンネルのベストプラクティス （67 ページ）を確認してください。

ステップ 1 Management Center にログインし、[デバイス（Devices）] > [VPN] > [サイト間（Site To Site）] を選択します。

ステップ 2 [+ SASEトポロジ（+ SASE Topology）] をクリックして、SASEトポロジウィザードを開きます。

ステップ 3 一意の [トポロジ名（Topology Name）] を入力します。この例では、**VPN-MumbaiUmbrella** と入力します。

ステップ 4 [事前共有キー（Pre-shared Key）]：このキーは、Umbrella PSK 要件に従って自動生成されます。

デバイスと Cisco Umbrella はこの秘密鍵を共有し、IKEv2 はそれを認証に使用します。自動生成されたキーは上書きできます。このキーを構成する場合は、長さが 16 ～ 64 文字で、少なくとも 1 つの大文字、1 つの小文字、1 つの数字を使用する必要があります。特殊文字は使用できません。各トポロジには、一意の事前共有キーが必要です。トポロジに複数のトンネルがある場合、すべてのトンネルの事前共有キーは同じです。

ステップ 5 [Cisco Umbrellaデータセンター（Umbrella Data center）] ドロップダウンリストからデータセンターを選択しますCisco Umbrella データセンターには、リージョンと IP アドレスが自動的に入力されます。

ステップ 6 [追加（Add）] をクリックして、SASE トポロジのエンドポイントとして Threat Defense ノードを追加します。

a) [デバイス（Device）] ドロップダウンリストから Threat Defense デバイス（**NGFWBR1**）を選択します。

b) [VPNインターフェイス（VPN Interface）] ドロップダウンリストからスタティック VTI インターフェイスを選択します。

新しいスタティック VTI インターフェイス（たとえば、**Outside_static_vti_1**）を作成するには、[+] をクリックします。[仮想トンネルインターフェイスの追加（Add Virtual Tunnel Interface）] ダイアログボックスが表示され、次の事前入力されたデフォルト設定が示されます。

- [トンネルタイプ（Tunnel Type）] は、デフォルトでは [スタティック（Static）] に設定されます。
- [名前（Name）] は <*tunnel_source interface logical name*>+ static_vti +<*tunnel ID*> です。たとえば、Outside_static_vti_1 となります。
- トンネルは、デフォルトでは [有効（Enabled）] になります。
- セキュリティゾーンは、デフォルトでは [外部（Outside）] として設定されます。
- [トンネルID（Tunnel ID）] には、一意の ID が自動入力されます。
- [トンネル ソース インターフェイス（Tunnel Source Interface）] には、「outside」プレフィックスを持つインターフェイスが自動的に入力されます。

（注） トンネルの送信元が **GigabitEthernet0/0** に設定されていることを確認します

（注） [トンネル送信元インターフェイス（Tunnel Source Interface）] を別のインターフェイスに設定することもできます。

- IPsec トンネルモードは、デフォルトでは IPv4 です。
- 169.254.x.x/30 プライベート IP アドレスの範囲から、未使用の IP アドレスが選択されます。この例では、**169.254.2.1/30** が選択されています。

（注） /30 サブネットを使用する場合、使用できる IP アドレスは 2 つだけです。最初の IP アドレスは自動トンネル VTI IP であり、2 番目の IP アドレスは Cisco Umbrella DC へのスタティックルートを設定するときにネクストホップ IP として使用されます。この例では、169.254.2.1 が VTI IP で、169.254.2.2 がスタティックルートに使用されます。スタティック ルートの設定 （74 ページ）を参照してください。

- [OK] をクリックします。

[VPNインターフェイス（VPN Interface）] ドロップダウンリストから [outside_static_vti_1] を選択します。

c) [ローカルトンネルID（Local Tunnel ID）] フィールドに、ローカルトンネル ID のプレフィックスを入力します。

プレフィックスは 8 文字以上で、100 文字を上限とします。Management Center で Cisco Umbrella にトンネルが展開された後、Cisco Umbrella によって完全なトンネル ID（<*prefix*>@<*umbrella-generated-ID*>-umbrella.com）が生成されます。次に、管理センターは完全なトンネル ID を取得して更新し、Threat Defense デバイスに展開します。各トンネルには、一意のローカルトンネル ID があります。

d) [保存（Save）] をクリックして、エンドポイントデバイスをトポロジに追加します。

ステップ 7 [次へ（Next）] をクリックして、Cisco Umbrella SASE トンネル設定の概要を確認します。

- [エンドポイント（Endpoints）] ペイン：設定された Threat Defense エンドポイントの概要が表示されます。
- [暗号化設定（Encryption Settings）] ペイン：SASE トンネルの暗号化設定が表示されます。

ステップ 8 [Threat Defense ノードに構成を展開する（Deploy configuration on threat defense nodes）] チェック ボックスをオンにすると、Threat Defense へのネットワークトンネルの展開がトリガーされます。この展開は、トンネルが Cisco Umbrella に展開された後にのみ行われます。Threat Defense の展開には、ローカルトンネル ID が必要です。

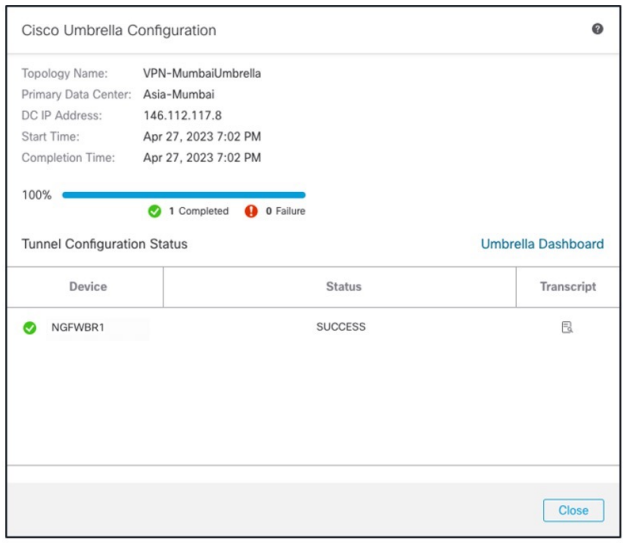
ステップ 9 [保存（Save）] をクリックします。

このアクションは、次のように動作します。

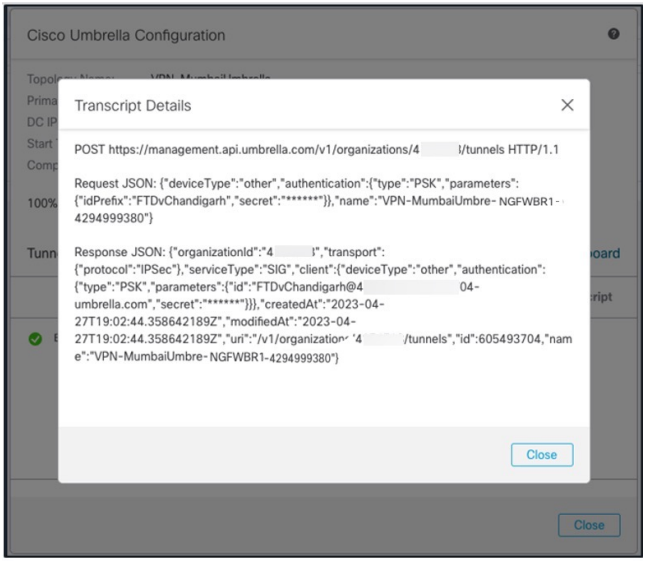
1. SASE トポロジを Management Center に保存します。
2. Cisco Umbrella への各 Threat Defense エンドポイントのネットワークトンネルの展開をトリガーします。

3. オプションが有効になっている場合、Threat Defense デバイスへのネットワークトンネルの展開をトリガーします。このアクションでは、デバイスでの最後の展開以降に更新されたすべての構成とポリシー（非 VPN ポリシーを含む）がコミットされて展開されます。

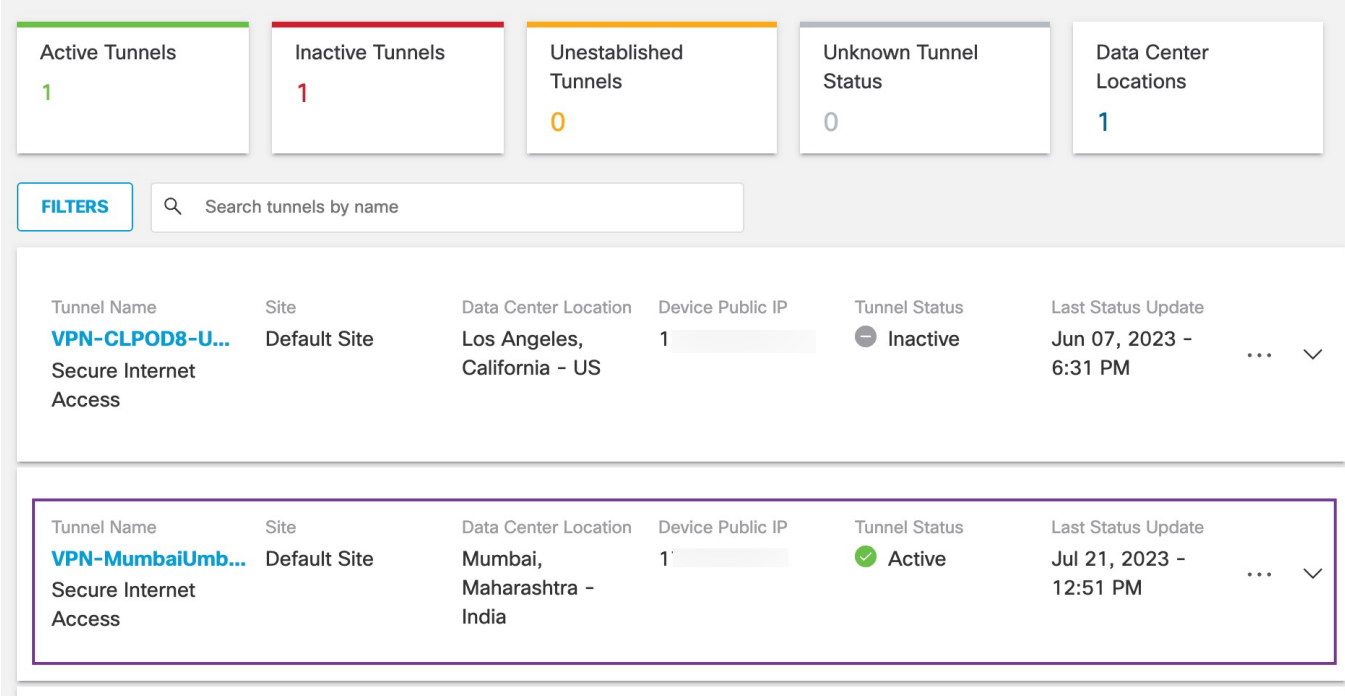
4. [Cisco Umbrella設定（Cisco Umbrella Configuration）] ウィンドウを開き、Cisco Umbrella でのトンネル展開のステータスを表示します。



展開の詳細を表示するには、[トランスクリプト（Transcript）]ボタンをクリックして、API、リクエストペイロード、Cisco Umbrella から受信したレスポンスなどの、トランスクリプトの詳細を表示します。



[Cisco Umbrellaダッシュボード（Umbrella Dashboard）] リンクをクリックして、Cisco Umbrella の [ネットワークトンネル（Network Tunnels）] ページを表示します。



次のタスク

SASE トンネルを通過するように意図されたトラフィックについては、特定の一致基準を使用して PBR ポリシーを設定し、VTI を介してトラフィックを送信します。

スタティック ルートの設定

自動トンネルから Cisco Umbrella DC へのスタティックルートを設定する必要があります。

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** ページから、Threat Defense デバイス（**NGFWBR1**）を編集します。

ステップ 2 [ルーティング（Routing）] タブをクリックします。

ステップ 3 [Static Route] をクリックします。

ステップ 4 [ルートを追加（Add Route）] をクリックして、新しいルートを追加します。

ステップ 5 [インターフェイス（Interface）] ドロップダウンリストから、インターフェイスとして [outside_static_vti_1] を選択します。

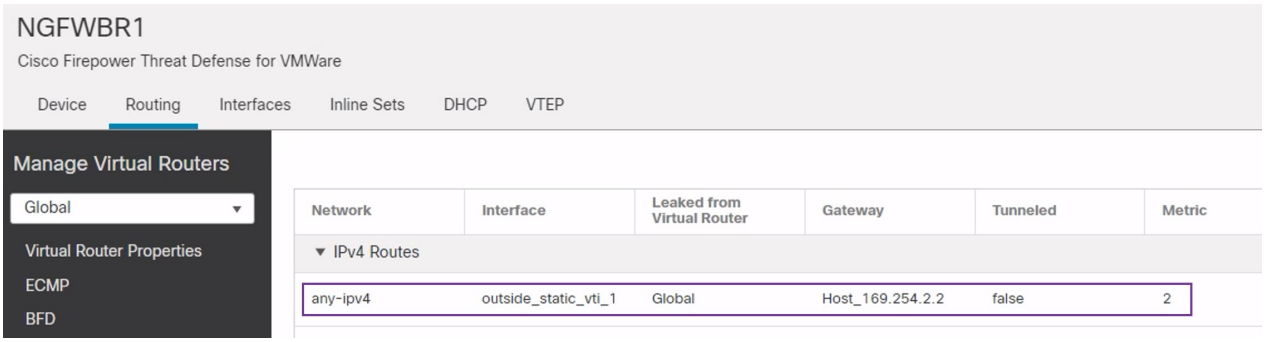
ステップ 6 [使用可能なネットワーク（Available Networks）] ボックスから宛先ネットワークとして [any-ipv4] を選択し、[追加（Add）] をクリックします。

ステップ 7 ネットワークのゲートウェイを入力します。この例では、**169.254.2.2** と入力します。

ステップ 8 メトリック値を入力します。1 ～ 254 の数値を指定できます。この例では、値として 2 を入力します。

ステップ 9 設定を保存するには、[Save] をクリックします。

次の図に示すように、スタティックルートが作成されます。



DNS および Web トラフィックの拡張 ACL の設定

ポリシーベースルーティングを利用して、DNS および Web トラフィックが出力インターフェイスからインターネットに向けて誘導されるように、アクセスリストが設定されます。

ステップ 1 **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]** を選択し、コンテンツテーブルから **[アクセスリスト（Access Lists）] > [拡張（Extended）]** を選択します。

ステップ 2 ソーシャル メディア トラフィック用の拡張アクセスリストを作成するには、[拡張アクセスリストの追加（Add Extended Access List）] をクリックします。

ステップ 3 [拡張ACLオブジェクト（Extended ACL Object）] ダイアログボックスで、オブジェクトの名前（**LAN_to_Internet**）を入力します。

ステップ 4 [追加（Add）] をクリックして、新しい拡張アクセスリストを作成します。

ステップ 5 次のアクセス制御のプロパティを設定します。

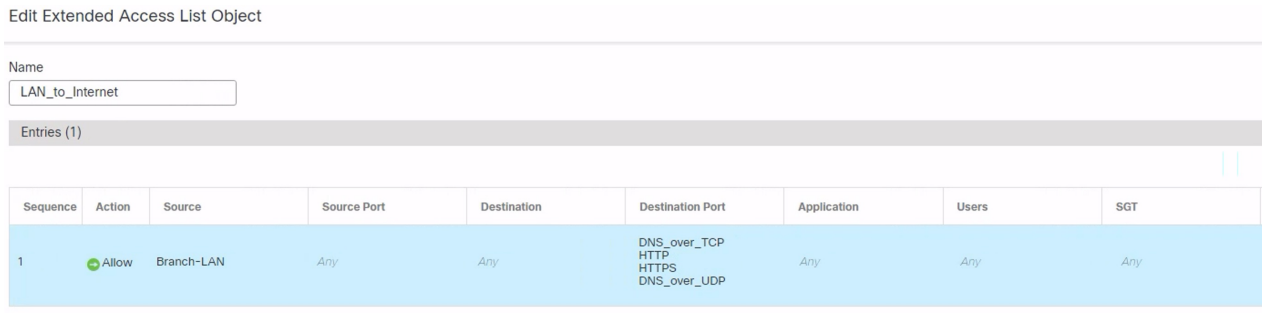
1. トラフィック基準を許可（一致）するように [アクション（Action）] を選択します。
2. [ポート（Port）] タブをクリックし、[利用可能なポート（Available Ports）] リストで **HTTP**、**HTTPS**、**DNS_over_UDP**、**DNS_over_TCP** を検索します。
3. ポートを選択し、[宛先に追加（Add to Destination）] をクリックします。
4. [ネットワーク（Network）] タブをクリックし、[利用可能なネットワーク（Available Networks）] リストでブランチ LAN を検索します。

   （注） この例では、ネットワークは **Branch-LAN** です。

5. [Branch-LAN] を選択し、[送信元に追加（Add to Source）] をクリックします。
6. [追加（Add）] をクリックして、エントリをオブジェクトに追加します。

7. [保存（Save）] をクリックします。

次の図に示すように、ACL オブジェクトが作成されます。



DNS および Web トラフィックの PBR ポリシーの設定

[ポリシーベースルーティング（Policy Based Routing）] ページで、DNS および Web トラフィックをルーティングするための入力インターフェイス、一致基準（拡張アクセスコントロールリスト）および出力インターフェイスを指定することにより、PBR ポリシーを設定できます。

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、Threat Defense デバイス（**NGFWBR1**）を編集します。

ステップ 2 NGFWBR1 のインターフェイスビューで [ルーティング（Routing）] タブをクリックします。

ステップ 3 [ポリシーベースルーティング（Policy Based Routing）] をクリックします。

ステップ 4 [ポリシーベースルートの追加（Add Policy Based Route）] ダイアログボックスで、ドロップダウンリストから [入力インターフェイス（Ingress Interface）] を選択します。

ステップ 5 ポリシーで一致基準と転送アクションを指定するには、[追加（Add）] をクリックします。

ステップ 6 [転送アクションの追加（Add Forwarding Actions）] ダイアログボックスで、次の操作を実行します。

a) [ACLの照合（Match ACL）] ドロップダウンから、[LAN_to_Internet] を選択します。

b) 設定されたインターフェイスを選択するには、[送信先（Send To）] ドロップダウンリストから [出力インターフェイス（Egress Interfaces）] を選択します。

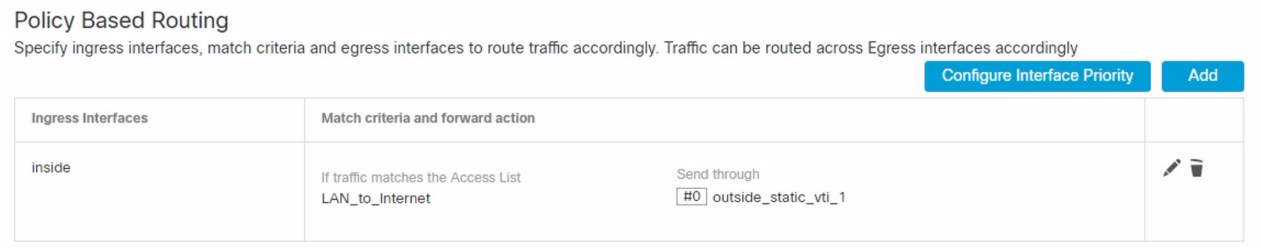
c) [使用可能なインターフェイス（Available Interfaces）] から、**Outside_static_vti_1** インターフェイスの横にある **Add (** ➕ **)** アイコンをクリックして、[選択した出力インターフェイス（Selected Egress Interfaces）] に移動します。

d) [保存（Save）] をクリックして、一致基準の変更を書き込みます。

e) 設定を確認し、[保存（Save）] をクリックして、ポリシーベースルーティングのすべての設定変更を書き込みます。

ステップ 7 [保存（Save）] をクリックします。

次の図に示すように、PBR ポリシーが作成されます。



設定の展開

すべての設定が完了したら、管理対象デバイスに設定を展開します。

ステップ 1 Management Center メニューバーで、[展開（Deploy）] をクリックします。展開準備が完了しているデバイスのリストが表示されます。

ステップ 2 設定の変更を展開する NGFWBR1 と NGFW1 の横にあるチェックボックスをオンにします。

ステップ 3 [展開（Deploy）] をクリックします。[展開（Deploy）] ダイアログボックスで展開が [完了（Completed）] とマークされるまで待ちます。

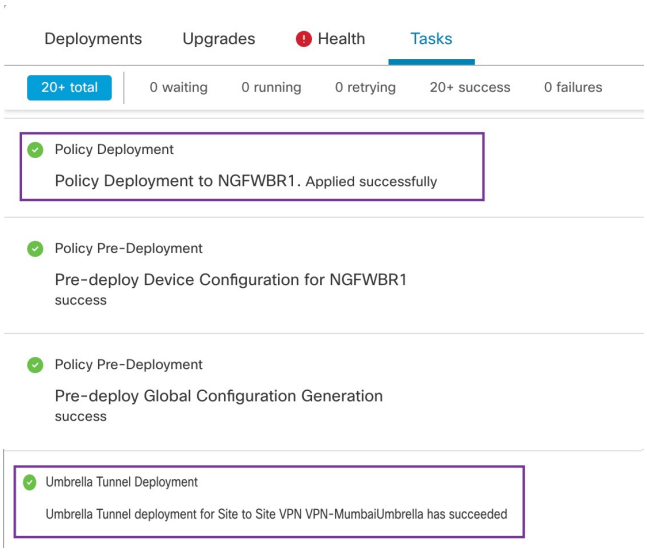
ステップ 4 展開する変更に関するエラーや警告がシステムによって識別された場合は、[検証エラー（Validation Errors）] または [検証の警告（Validation Warnings）] ウィンドウにその内容が表示されます。完全な詳細を表示するには、[検証エラー（Validation Errors）] または [検証の警告（Validation Warnings）] リンクをクリックします。

次の選択肢があります。

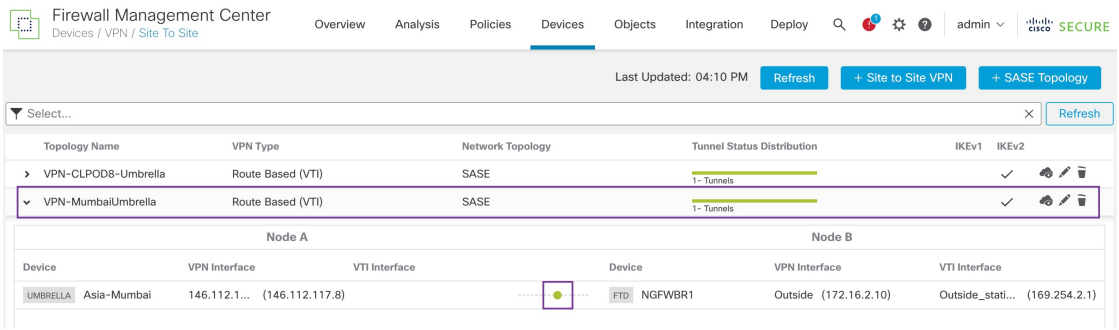
- [展開の続行（Proceed with Deploy）]：警告状態を解決せずに展開を続行します。システムがエラーを確認した場合は続行できません。
- [閉じる（Close）]：展開せずに終了します。エラーおよび警告状態を解決し、設定の再展開を試行します。

SASE Cisco Umbrella トンネルの展開の確認

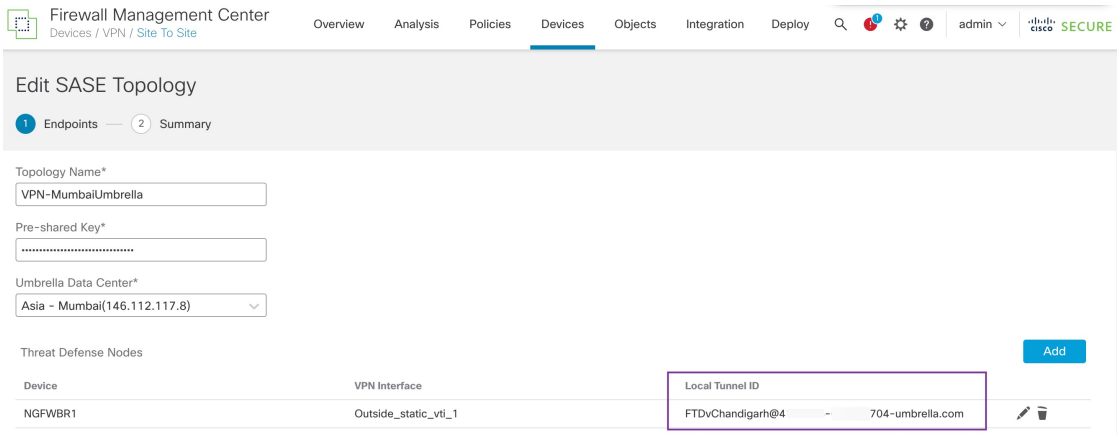
Management Center で、[通知（Notifications）] > [タスク（Tasks）] に移動し、Threat Defense デバイス（NGFWBR1）での Cisco Umbrella トンネルの展開とポリシーの展開のステータスを表示します。



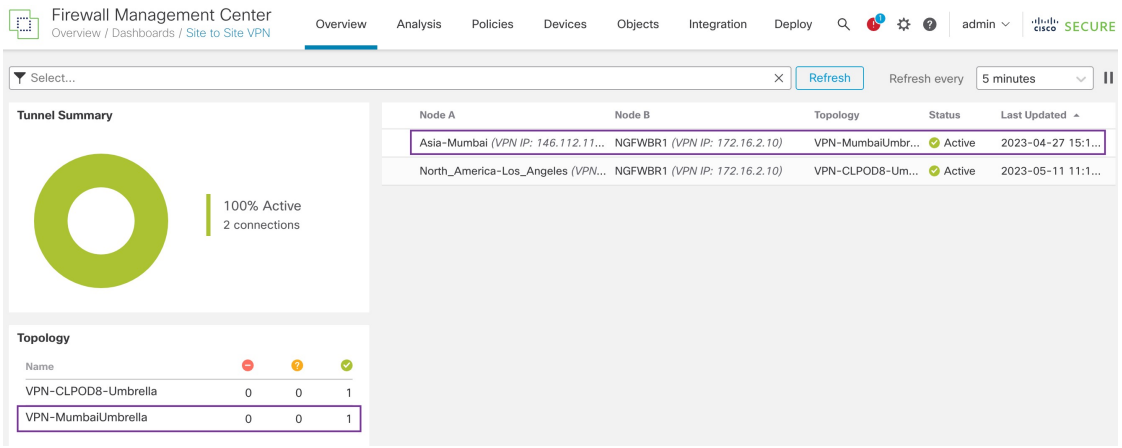
Management Center で SASE 自動トンネルのステータスを確認するには、[デバイス（Devices）] > [VPN] > [サイト間（Site To Site）] を選択します。



Management Center で更新された SASE トポロジを確認するには、[デバイス（Devices）]>[VPN] > [サイト間（Site To Site）] > [SASE トポロジの編集（Edit SASE Topology）] を選択します。ローカルトンネル ID は、Cisco Umbrella への展開後に更新されます。



Management Center で [サイト間VPN（Site to Site VPN）] ダッシュボードを表示するには、[概要（Overview）] > [ダッシュボード（Dashboard）] > [サイト間VPN（Site to Site VPN）] の順に選択します。



Threat Defense での SASE Cisco Umbrella トンネルを確認するには、次の CLI コマンドを使用します。

- SASE トンネルの詳細を確認するには、次のコマンドを使用します。

```
> show running-config interface tunnel 1
!
interface Tunnel1
 nameif Outside_static_vti_1
 ip address 169.254.2.1 255.255.255.252
 tunnel source interface Outside
 tunnel destination 146.112.117.8
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile FMC_IPSEC_PROFILE_1
```

- IPSec プロファイルおよび関連する提案を確認するには、次のコマンドを使用します。

```
> show running-config crypto ipsec
crypto ipsec ikev2 ipsec-proposal CSM_IP_1
 protocol esp encryption aes-gcm-256
 protocol esp integrity sha-256
crypto ipsec profile FMC_IPSEC_PROFILE_1
 set ikev2 ipsec-proposal CSM_IP_1
 set ikev2 local-identity email-id FTDvChandigarh@41xxxxx-xxxxxxxxx-umbrella.com
 set reverse-route
crypto ipsec security-association pmtu-aging infinite
```

- IKeV2 ポリシーセットを確認するには、次のコマンドを使用します。

```
> show running-config crypto ikev2
crypto ikev2 policy 15
 encryption aes-gcm-256
 integrity null
 group 20 19
 prf sha256
 lifetime seconds 86400
crypto ikev2 enable Outside
```

- Tx および Rx データを含むトンネルの統計を確認するには、次のコマンドを使用します。

```
> show vpn-sessiondb l2l
Session Type: LAN-to-LAN
Connection   : 146.112.117.8
Index        : 19                    IP Addr      : 146.112.117.8
Protocol     : IKEv2 IPsecOverNatT
Encryption   : IKEv2: (1)AES-GCM-256  IPsecOverNatT: (1)AES-GCM-256
Hashing      : IKEv2: (1)none  IPsecOverNatT: (1)none
Bytes Tx     : 234                     Bytes Rx     : 446
Login Time   : 19:14:51 UTC Thu Apr 27 2023
Duration     : 0h:55m:16s
Tunnel Zone  : 0
```

- トンネルのステータスを確認するには、次のコマンドを使用します。

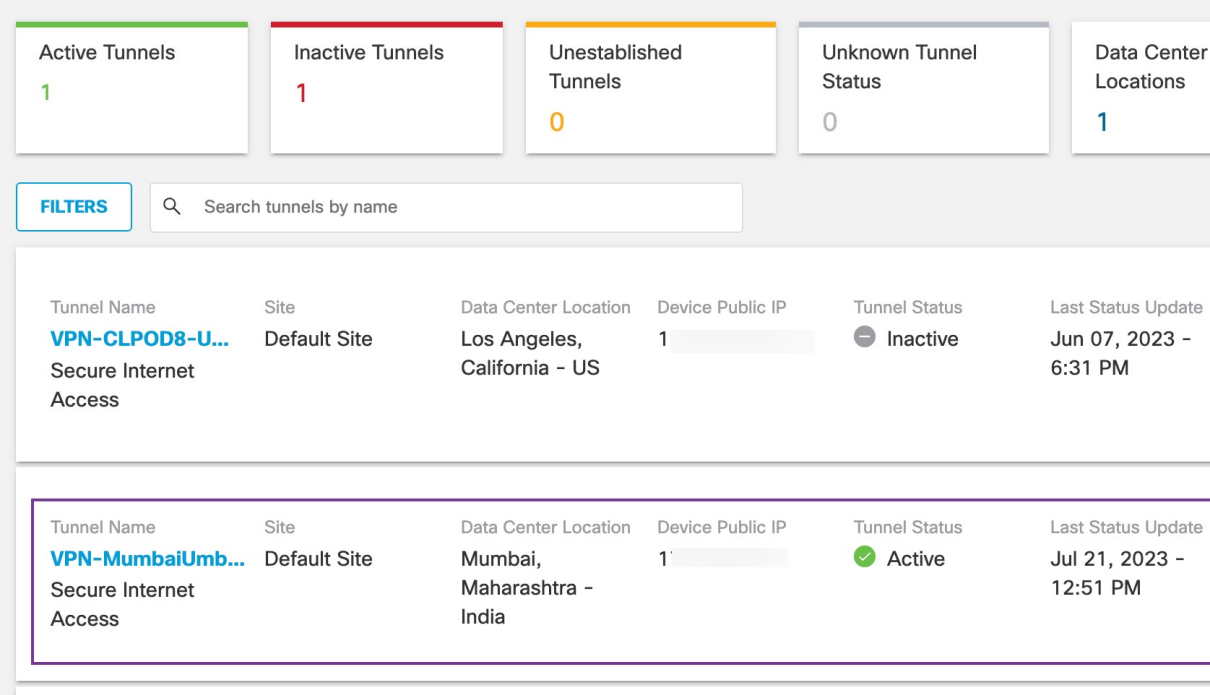
```
> show interface ip brief

Interface                  IP-Address      OK? Method Status                Protocol
Internal-Control0/0        127.0.1.1       YES unset  up                    up
Internal-Control0/1        unassigned      YES unset  up                    up
Internal-Data0/0           unassigned      YES unset  down                  up
Internal-Data0/0           unassigned      YES unset  up                    up
Internal-Data0/1           169.254.1.1     YES unset  up                    up
Internal-Data0/2           unassigned      YES unset  up                    up
Management0/0              203.0.113.130   YES unset  up                    up
TenGigabitEthernet0/0      172.16.2.10     YES manual up                    up
TenGigabitEthernet0/1      172.16.3.10     YES manual up                    up
TenGigabitEthernet0/2      unassigned      YES unset  administratively down up
Tunnel1                    169.254.2.1     YES manual up                    up
```

- VTI トンネルに関連付けられている IPSec SA を確認するには、次のコマンドを使用します。

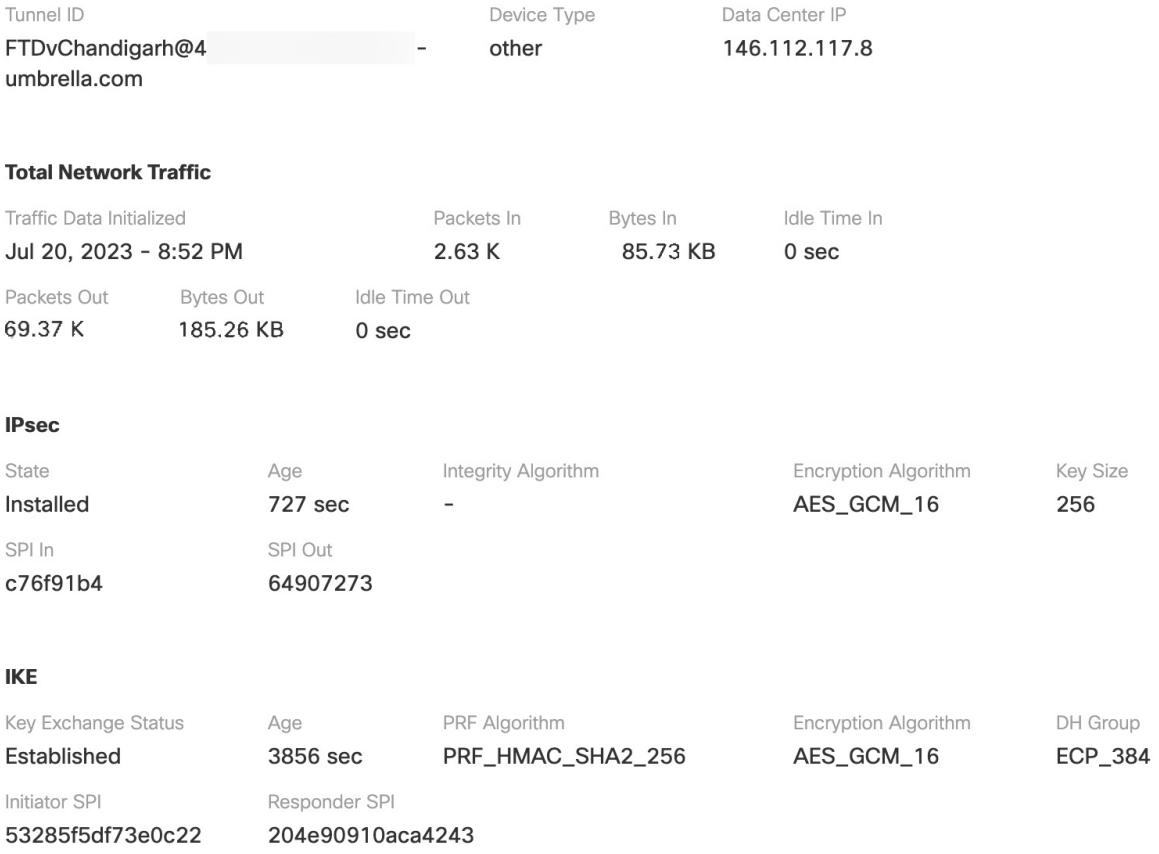
```
> show crypto ipsec sa
interface: outside_static_vti_1
    Crypto map tag: __vti-crypto-map-Tunnel1-0-1, seq num: 65280, local addr:
198.18.128.81

      Protected vrf (ivrf): Global
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      current_peer: 146.112.117.8


      #pkts encaps: 705, #pkts encrypt: 705, #pkts digest: 705
      #pkts decaps: 743, #pkts decrypt: 743, #pkts verify: 743
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 705, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 0

     local crypto endpt.: 198.18.128.81/4500, remote crypto endpt.: 146.112.117.8/4500

      path mtu 1500, ipsec overhead 63(44), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: C76F91B4
      current inbound spi : 64907273

    inbound esp sas:
      spi: 0x2BF92601 (737748481)
         SA State: active
```

```
      transform: esp-aes-gcm-256 esp-null-hmac no compression
      in use settings ={L2L, Tunnel,  NAT-T-Encaps, IKEv2, VTI, }
      slot: 0, conn_id: 32, crypto-map: __vti-crypto-map-Tunnel1-0-1
      sa timing: remaining key lifetime (kB/sec): (4331520/27987)
      IV size: 8 bytes
      replay detection support: Y
      Anti replay bitmap:
       0x00000000 0x00000001
outbound esp sas:
  spi: 0xCA2DC006 (3391995910)
      SA State: active
      transform: esp-aes-gcm-256 esp-null-hmac no compression
      in use settings ={L2L, Tunnel,  NAT-T-Encaps, IKEv2, VTI, }
      slot: 0, conn_id: 32, crypto-map: __vti-crypto-map-Tunnel1-0-1
      sa timing: remaining key lifetime (kB/sec): (4101072/27987)
      IV size: 8 bytes
      replay detection support: Y
      Anti replay bitmap:
       0x00000000 0x00000001
```

Cisco Umbrella で SASE トンネルを表示するには、Cisco Umbrella にログインし、[展開（Deployments）]>[コアアイデンティティ（Core Identities）]>[ネットワークトンネル（Network Tunnels）] に移動します。次の図に示すように、Threat Defense から Cisco Umbrella へのネットワークトンネルが表示されます。



トンネルの詳細を表示するには、セクションを展開します。



Cisco Umbrella 自動トンネルのトラブルシューティング

展開後に、次の CLI を使用して、Cisco Secure Firewall Threat Defense での Cisco Umbrella 自動トンネルに関連する問題をデバッグします。

（注） 実稼働環境の Threat Defense デバイスで debug コマンドを実行する場合は、注意して進めてください。デバイスでさまざまなデバッグレベルを設定できるため、詳細な出力が行われる可能性があります。

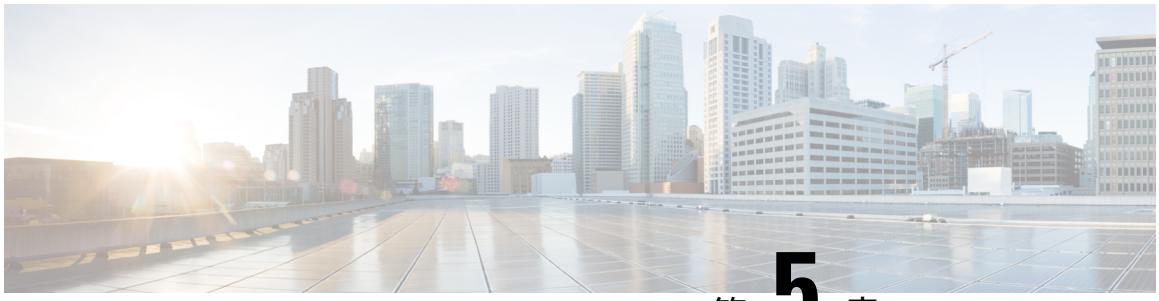
操作	CLI コマンド
特定のピアの条件付きデバッグを有効にする	**debug crypto condition peer <peer-IP>**
仮想トンネルインターフェイス情報をデバッグする	**debug vti 255**

操作	CLI コマンド
IKEv2 プロトコル関連のトランザクションをデバッグする	**debug crypto ikev2 protocol 255**
IKEv2プラットフォーム関連のトランザクションをデバッグする	**debug crypto ikev2 platform 255**
一般的なIKE関連のトランザクションをデバッグする	**debug crypto ike-common 255**
IPSec関連のトランザクションをデバッグする	**debug crypto ipsec 255**

関連リソース

リソース（**Resource**）	**URL**
Cisco Secure Firewall Threat Defense リリースノート	https://www.cisco.com/go/firewall-release-notes
すべての新機能と廃止された機能	http://www.cisco.com/go/whatsnew-fmc
Cisco.com の Cisco Secure Firewall	http://www.cisco.com/go/firewall
Cisco.com のマニュアル	http://www.cisco.com/go/firewall-docs
YouTube 上の Cisco Secure Firewall	https://www.youtube.com/cisco-netsec
Cisco Secure Firewall Essentials	https://secure.cisco.com/secure-firewall

関連リソース



第 5 章

リモートワーカーへのセキュアな接続の提供：DIA、Cisco Umbrella 自動トンネル、および DVTI の適用例

この章では、DIA、Cisco Umbrella 自動トンネル、および DVTI の使用の実践的な応用について詳しく説明します。この使用例では、シームレスな導入のためのシナリオ、ネットワークトポロジ、およびエンドツーエンドの手順について詳しく説明します。

DIA、Cisco Umbrella SASE 自動トンネル、および DVTI によるリモートワーカーの接続とセキュリティの強化

今日の相互接続されたリモートワーク環境では、組織は、分散型ワークフォースにシームレスな接続、セキュアなアクセス、および最適化されたパフォーマンスを提供するという課題に直面しています。この使用例では、ネットワーク接続の問題を解決し、コラボレーションを強化し、機密情報を保護し、リモートユーザーがどこからでも効率的に作業できるようにするための、DIA（ダイレクト インターネット アクセス）、Cisco Umbrella SASE 自動トンネル、および DVTI（ダイナミック仮想トンネルインターフェイス）テクノロジーの導入について説明します。

この使用例の対象者

この使用例の対象者は、ネットワーク インフラストラクチャの管理と保護を担当する IT プロフェッショナル、ネットワーク管理者、および意思決定者と、リモートワークフォースの接続とセキュリティの最適化を試みている組織です。DIA、Cisco Umbrella SASE 自動トンネル、およびDVTI テクノロジーの導入に関するインサイトを提供し、リモートワーカーが直面する課題に対処する際にもたらされる利点をハイライトします。

シナリオ

Sally は、リアルタイムのコラボレーションとデータアクセスに大きく依存するグローバル企業のリモート営業担当者として働いています。さまざまなクライアントの場所に頻繁に出張していますが、販売データへのアクセスや同僚とのコミュニケーションに課題があります。

リスクがあるもの

会社の既存のネットワーク インフラストラクチャでは、複数の場所にシームレスな接続性とセキュアなアクセスを提供できないため、遅延、データの不整合、および通信の中断が発生しています。

ハブアンドスポークトポロジの DIA、Cisco Umbrella 自動トンネル、および DVTI で構成されるソリューションによる問題の解決方法

Sallyのようなリモートワーカーが直面する課題に対処するために、彼女の会社は、DIA、Cisco Umbrella SASE 自動トンネル、およびDVTI を使用した包括的なソリューションを導入します。

1. **DIA**：DIA を使用することで、Sally は企業のネットワークを経由せずにインターネットに直接接続できます。これにより、より高速で信頼性の高いインターネットアクセスが提供され、クラウドベースのアプリケーションおよびサービスにすばやくアクセスできます。これにより、企業のネットワークからネットワークトラフィックがオフロードされ、輻輳が軽減され、パフォーマンスが最適化されます。

2. **Cisco Umbrella 自動トンネル**：Cisco Umbrella 自動トンネルの設定を活用することで、Sallyの会社は、Sallyがリモートで接続されているか、ブランチファイアウォールの背後にあるかに関係なく、統一されたセキュリティポリシーがトラフィックに適用されるようにします。これにより、VPN接続を手動で設定する必要がなくなり、従来のトンネル設定に関連する複雑さと潜在的なエラーが軽減されます。このテクノロジーは、Sally と組織内のその他のリモートワーカーに、シンプルさ、利便性、および強化されたセキュリティを提供します

3. **DVTI**：ハブアンドスポークトポロジの DVTI により、分散拠点と企業のネットワークの間にセキュアな IPsec トンネルを動的に作成できます。このトンネルではデータ伝送が暗号化され、リモートで作業する際に企業のリソースへのセキュアなアクセスが確保されます。また、DVTI は、最も効率的なパスを介してトラフィックをインテリジェントにルーティングし、接続が中断されないようにするための冗長性を提供することで、ネットワークパフォーマンスを最適化します。

DIA、Cisco Umbrella SASE 自動トンネル、および DVTI を組み合わせることで、Sally の会社は、彼女のリモートワーカーとしての接続性、セキュリティ、および生産性を向上させています。彼女はクラウドアプリケーションにすばやくアクセスし、同僚とシームレスにコラボレーションし、企業のリソースへのセキュアで信頼性の高い接続をどこからでも利用することができます。IT チームには、一元化されたセキュリティ管理、ネットワークの複雑さの軽減、リモートワーカーのアクティビティの可視性の向上などの利点があります。

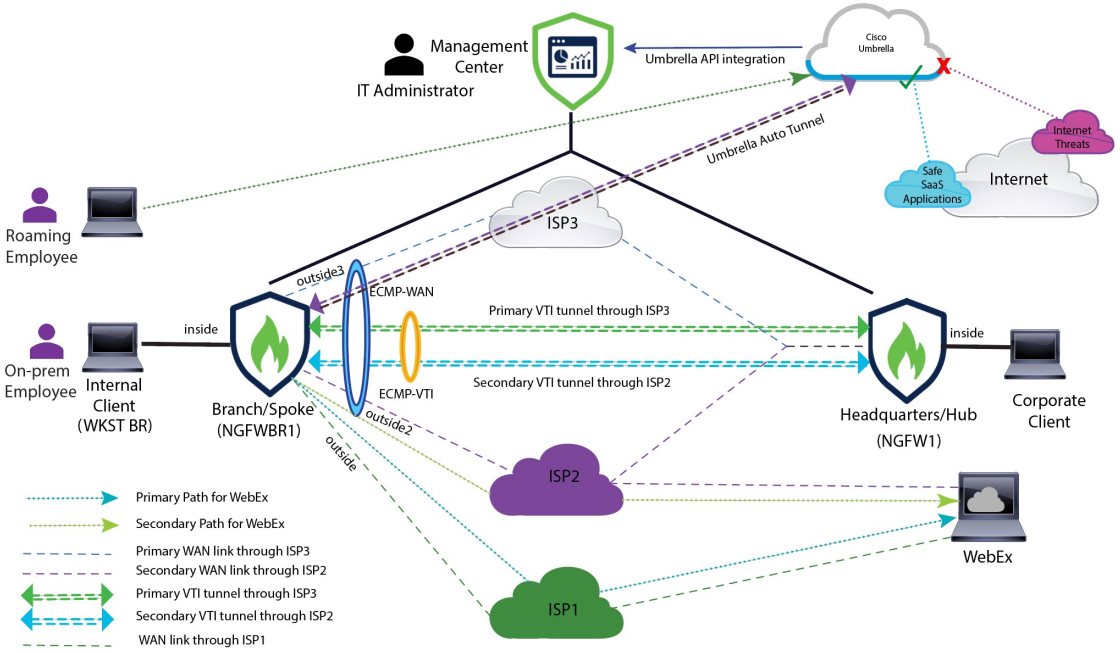
トポロジ

このトポロジでは、内部クライアントまたはブランチワークステーションが WKST BR としてラベル付けされ、NGFWBR1 としてラベル付けされたブランチの Threat Defense に接続されます。本社の Threat Defense には NGFW1 というラベルが付けられています。企業のネットワークは NGFW1 を介して到達可能です。NGFWBR1 の入力インターフェイスには inside という名前が付けられ、出力インターフェイスにはそれぞれ outside、outside2、および outside3 という名前が付けられています。

NGFWBR1 と Cisco Umbrella の間に Cisco Umbrella 自動トンネルが設定されています。

すべての DNS および Web トラフィックは、Cisco Umbrella 自動トンネルを介して Cisco Umbrella に送信され、Cisco Umbrella の DNS および Web ポリシーに基づいて許可またはブロックされます。これにより、2 つの保護層が提供されます。1 つは Cisco Secure Threat Defense によってローカルに適用され、もう 1 つは Cisco Umbrella によってクラウドで提供されます。

ハブスポーク設定の場合、VPN トンネルは NGFWBR1 と NGFW1 の間に設定されます。リンクの冗長性と VPN トラフィックのロードバランシングのために、ブランチノードのプライマリおよびセカンダリのスタティック VTI インターフェイスで ECMP ゾーンが設定されます。



DIA、Cisco Umbrella 自動トンネル、および DVTI を設定するためのエンドツーエンドの手順

DIA、Cisco Umbrella SASE 自動トンネル、および DVTI を使用したソリューションを設定するには、次の手順を実行します。

- **ダイレクト インターネット アクセスの設定**：パスモニタリングを使用した DIA の設定のエンドツーエンドの手順 （44 ページ）
- **Cisco Umbrella SIG 自動トンネルの設定**：Cisco Umbrella 自動トンネルを設定するためのエンドツーエンドの手順 （69 ページ）
- **DVTI ハブアンドスポークトポロジの設定**：ルートベース VPN（ハブアンドスポークトポロジ）を設定するためのエンドツーエンドの手順 （9 ページ）

関連リソース

リソース（Resource）	URL
Cisco Secure Firewall Threat Defense リリースノート	https://www.cisco.com/go/firewall-release-notes
すべての新機能と廃止された機能	http://www.cisco.com/go/whatsnew-fmc
Cisco.com の Cisco Secure Firewall	http://www.cisco.com/go/firewall
Cisco.com のマニュアル	http://www.cisco.com/go/firewall-docs
YouTube 上の Cisco Secure Firewall	https://www.youtube.com/cisco-netsec
Cisco Secure Firewall Essentials	https://secure.cisco.com/secure-firewall

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。