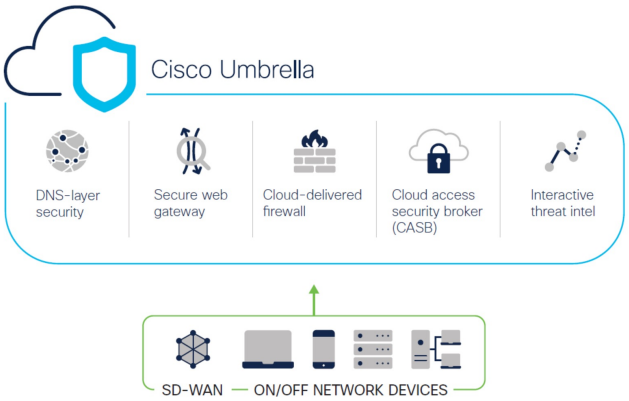
Cisco Umbrella 自動トンネルを使用したセキュアなインターネットトラフィック

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 *1 : 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 ブローカー（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。

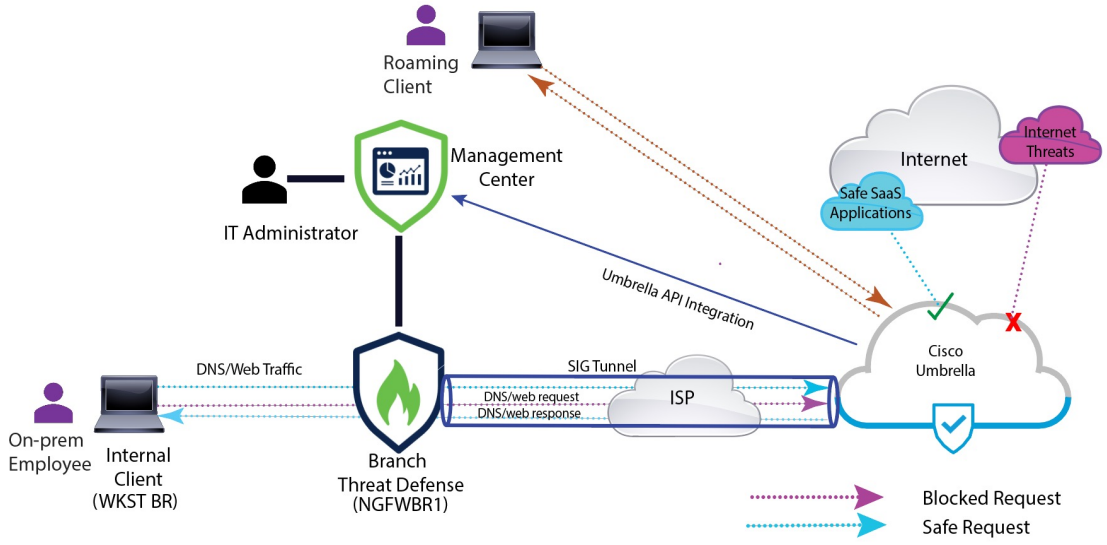
Sally は、一部の Web サイトがファイアウォールと Cisco Umbrella によってブロックされるようになったことに気が付きました。

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 *2 : 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

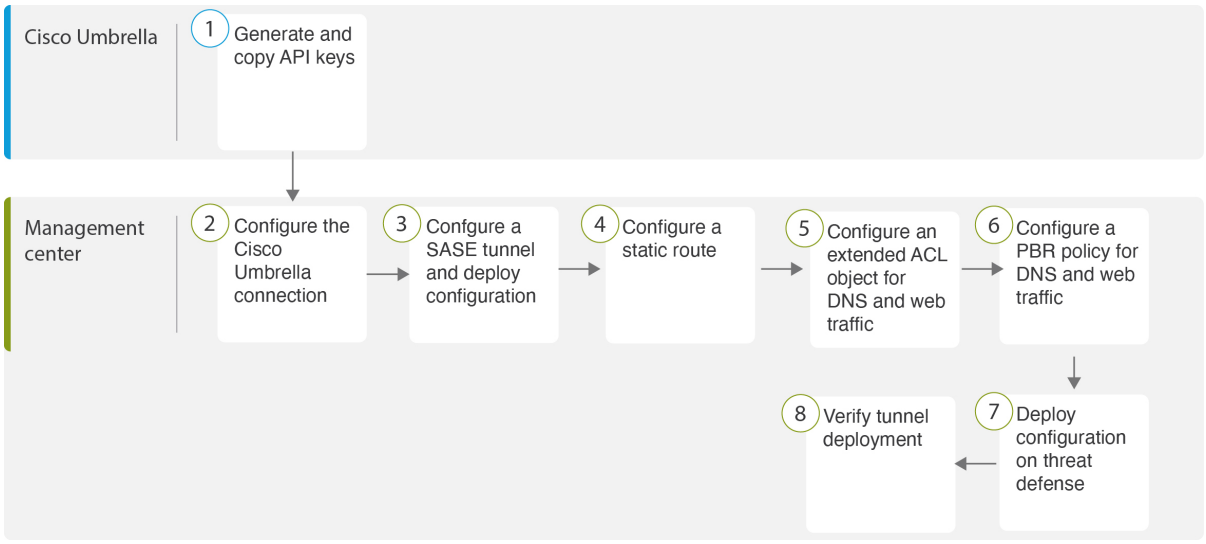
- Cisco Umbrella Secure Internet Gateway（SIG）Essentials サブスクリプションまたは無料の SIG トライアルバージョンが必要です。
- Management Center から Cisco Umbrella にトンネルを展開するには、輸出規制機能を使用してスマート ライセンス アカウントを有効にする必要があります。
- http://login.umbrella.com で Cisco Umbrella にログインし、Cisco Umbrella への接続を確立するために必要な情報を取得します。Management Center が management.api.umbrella.com 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 （9 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 （12 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 （13 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 （14 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 （15 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 （5 ページ）およびSASE Cisco Umbrella トンネルのベストプラクティス （5 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 （12 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。

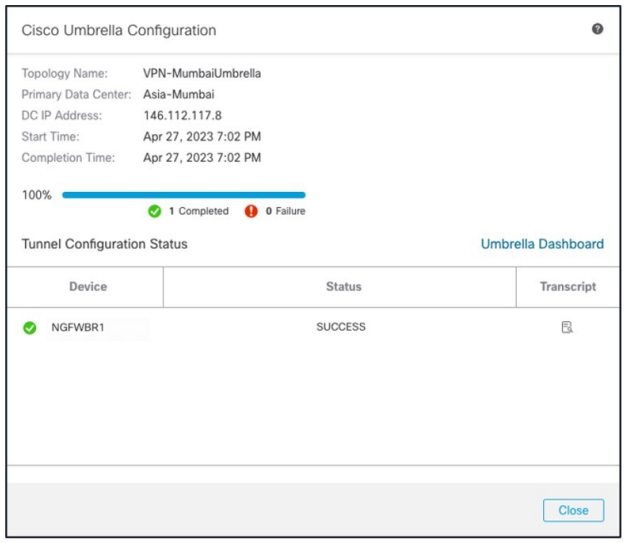
ステップ 9 [保存（Save）] をクリックします。

このアクションは、次のように動作します。

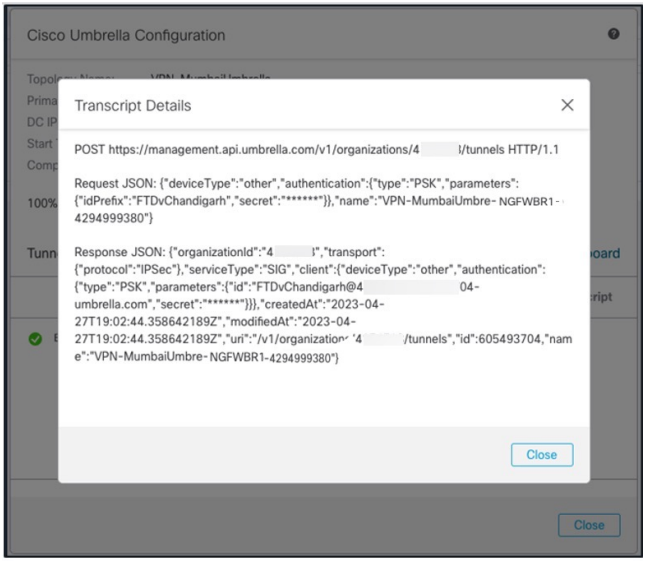
1. SASE トポロジを Management Center に保存します。
2. Cisco Umbrella への各 Threat Defense エンドポイントのネットワークトンネルの展開をトリガーします。

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。

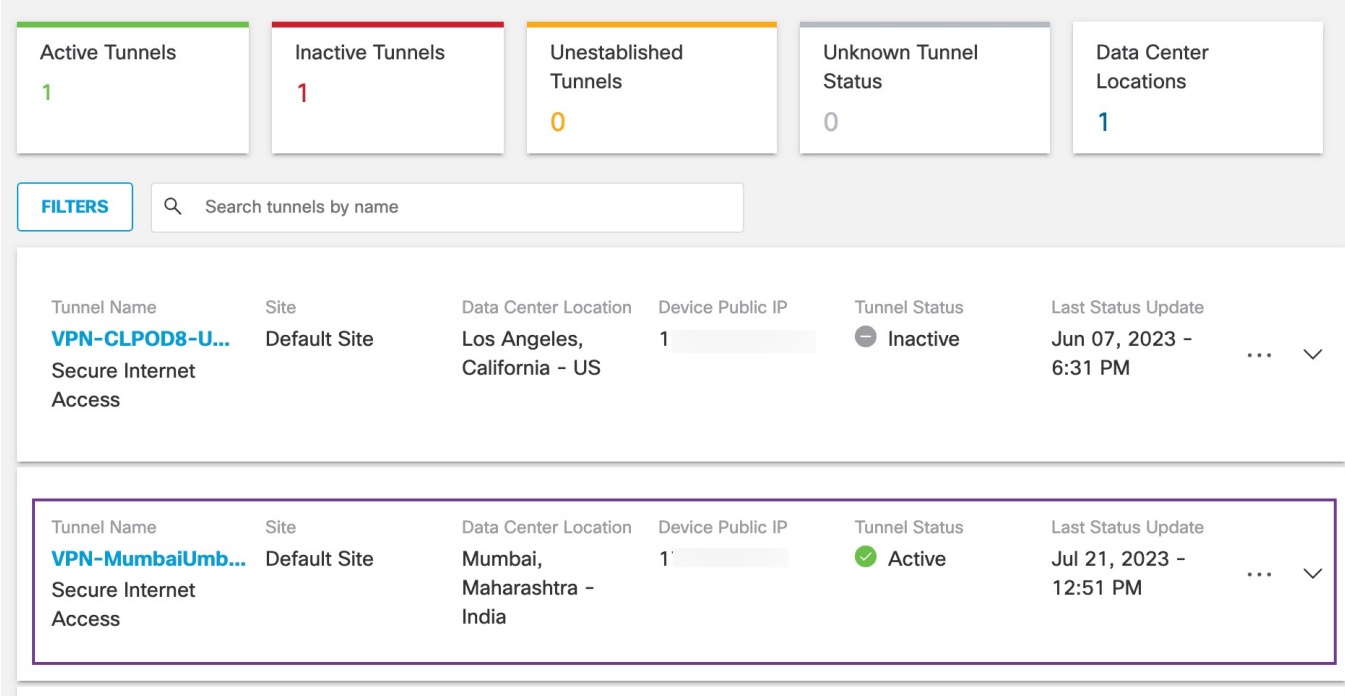
4. [Cisco Umbrella設定（Cisco Umbrella Configuration）] ウィンドウを開き、Cisco Umbrella でのトンネル展開のステータスを表示します。



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。

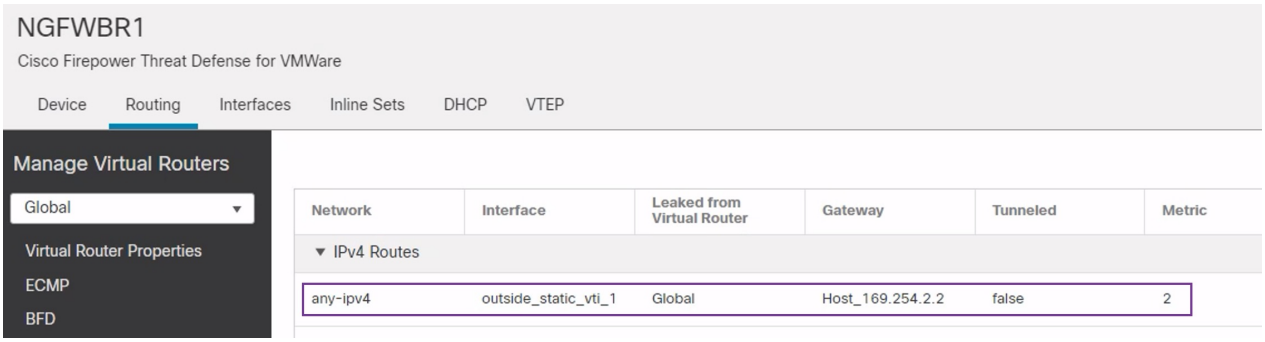
ステップ 6 [使用可能なネットワーク（Available Networks）] ボックスから宛先ネットワークとして [any-ipv4] を選択し、[追加（Add）] をクリックします。

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。

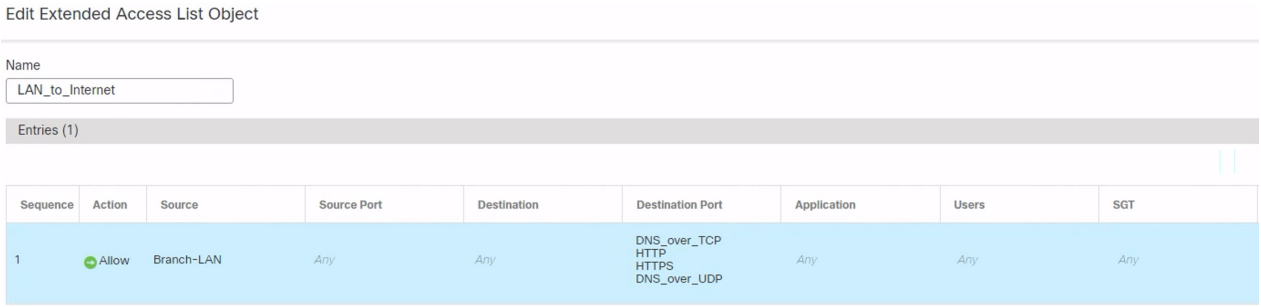
1. トラフィック基準を許可（一致）するように [アクション（Action）] を選択します。
2. [ポート（Port）] タブをクリックし、[利用可能なポート（Available Ports）] リストで **HTTP**、**HTTPS**、**DNS_over_UDP**、**DNS_over_TCP** を検索します。
3. ポートを選択し、[宛先に追加（Add to Destination）] をクリックします。
4. [ネットワーク（Network）] タブをクリックし、[利用可能なネットワーク（Available Networks）] リストでブランチ LAN を検索します。

   （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。

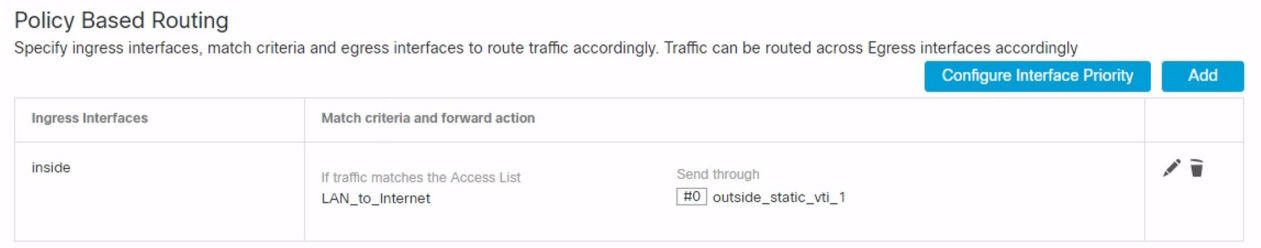
c) [使用可能なインターフェイス（Available Interfaces）] から、**Outside_static_vti_1** インターフェイスの横にある **Add (** ➕ **)** アイコンをクリックして、[選択した出力インターフェイス（Selected Egress Interfaces）] に移動します。

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。

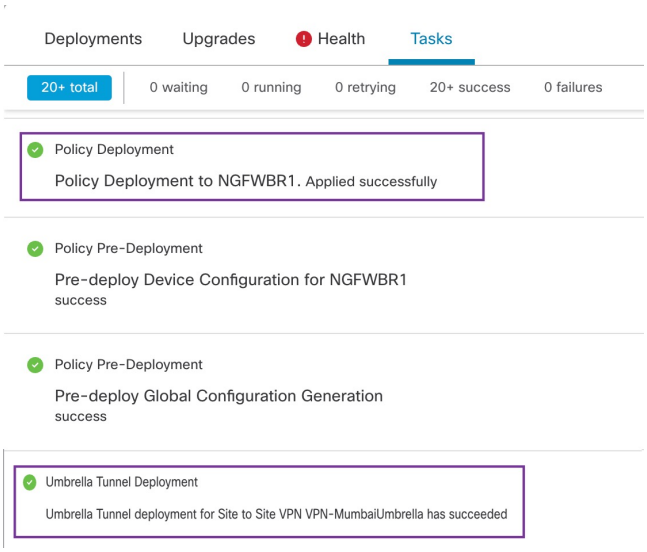
ステップ 4 展開する変更に関するエラーや警告がシステムによって識別された場合は、[検証エラー（Validation Errors）] または [検証の警告（Validation Warnings）] ウィンドウにその内容が表示されます。完全な詳細を表示するには、[検証エラー（Validation Errors）] または [検証の警告（Validation Warnings）] リンクをクリックします。

次の選択肢があります。

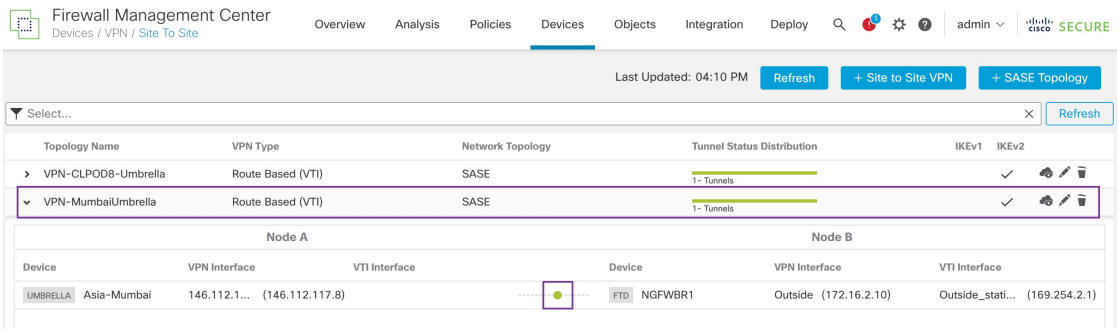
- [展開の続行（Proceed with Deploy）]：警告状態を解決せずに展開を続行します。システムがエラーを確認した場合は続行できません。
- [閉じる（Close）]：展開せずに終了します。エラーおよび警告状態を解決し、設定の再展開を試行します。

SASE Cisco Umbrella トンネルの展開の確認

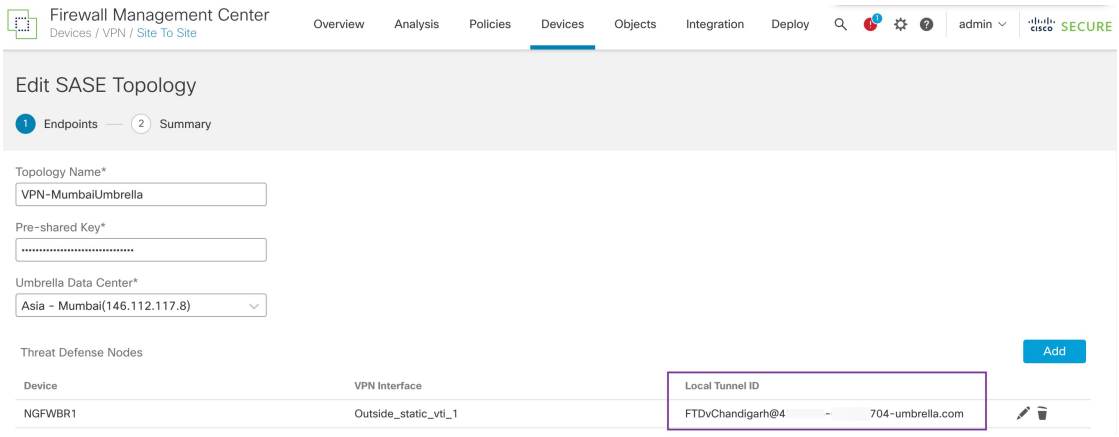
Management Center で、[通知（Notifications）] > [タスク（Tasks）] に移動し、Threat Defense デバイス（NGFWBR1）での Cisco Umbrella トンネルの展開とポリシーの展開のステータスを表示します。



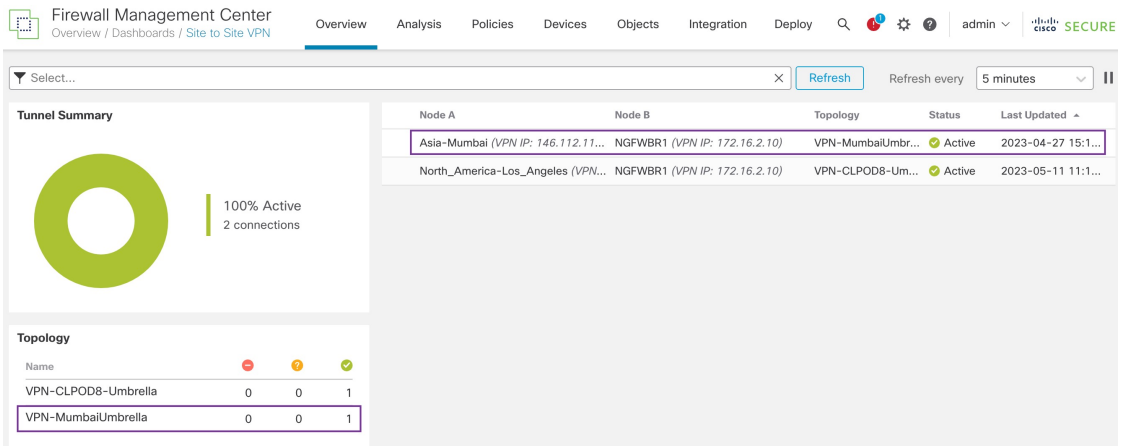
Management Center で SASE 自動トンネルのステータスを確認するには、[デバイス（Devices）] > [VPN] > [サイト間（Site To Site）] を選択します。



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。

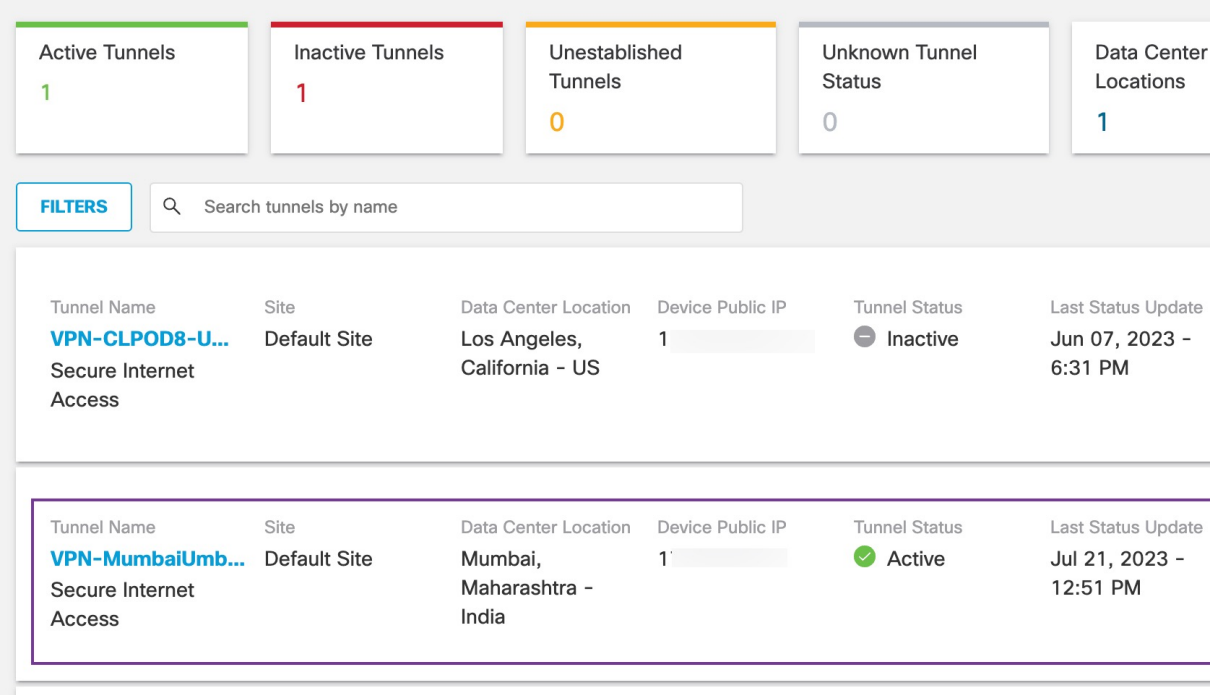
```
> show interface ip brief

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。

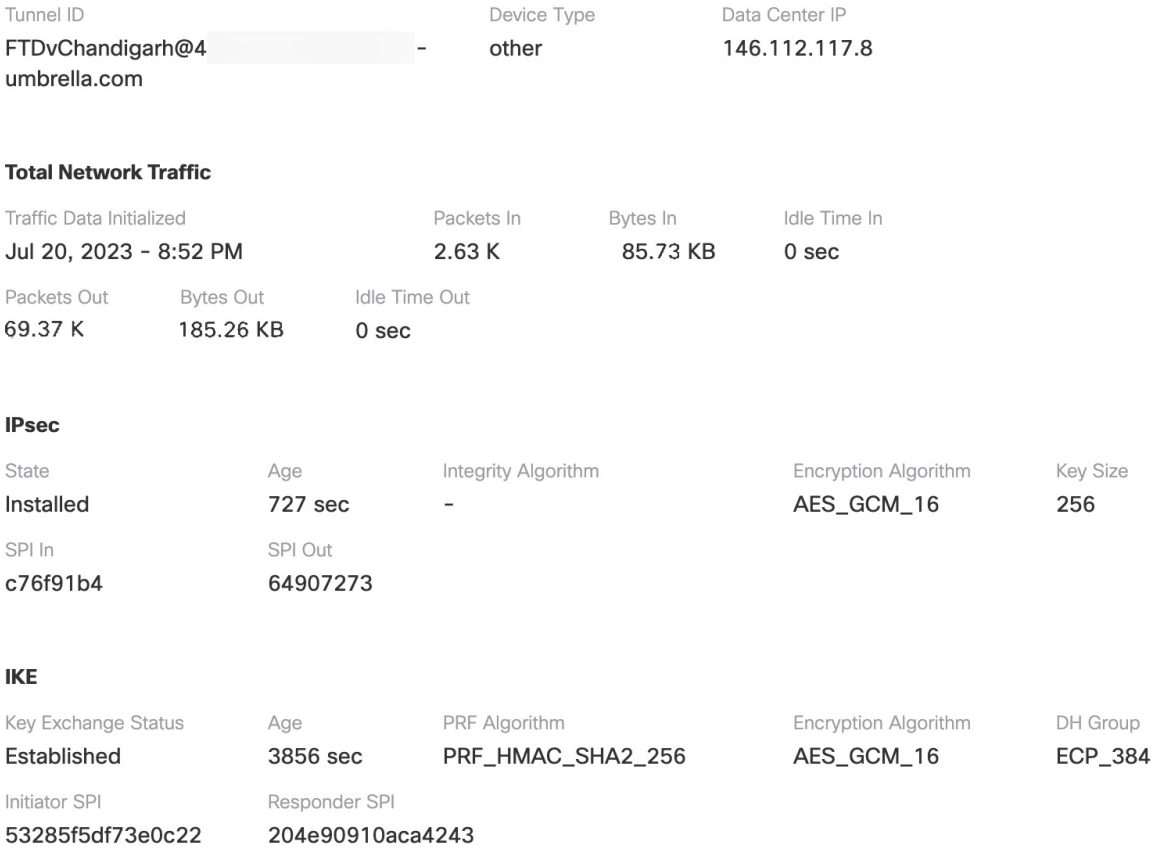
```
> show crypto ipsec sa
interface: outside_static_vti_1
    Crypto map tag: __vti-crypto-map-Tunnel1-0-1, seq num: 65280, local addr:
198.18.128.81

      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

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。