SASE および SSE ソリューションと Cisco Secure Firewall Threat Defense の統合

2025 年 9 月

SASE および SSE ソリューションと Threat Defense の統合

Secure Access Service Edge（SASE）は、クラウドを使用して、ネットワークおよびセキュリティサービスとユーザーおよびデバイスの距離を近付けます。
ネットワーク全体を変更することなくセキュリティを向上させるには、セキュリティサービスエッジ（SSE）を使用します。これにより、重要なセキュリティ機能がクラウドから提供され、セキュリティがシンプルになり、ユーザー体験が向上します。

Cisco SASE ソリューション：Cisco Umbrella および Threat Defense を使用したセキュアなインターネットトラフィック

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。インターネットの脅威に対する防御を複数のレベルで提供します。DNS レイヤセキュリティ、SWG、クラウド提供型ファイアウォール、DLP、CASB、および脅威インテリジェンスを統合して、すべてのブランチに拡張性の高いセキュリティを提供します。リモートまたはオンプレミスユーザーからインターネットに向かうトラフィックは、ブランチから最も近い Cisco Umbrella ポイントに自動的にルーティングされ、検査を受けた後、アクセスが許可または拒否されます。

シスコ ファイアウォールは、次の 2 つの方法で Cisco Umbrella と統合できます。

- 一貫した DNS ポリシーにより、すべてのブランチのインターネットトラフィックを保護。
- Cisco Umbrella 自動トンネルを使用してすべてのブランチのインターネットトラフィックを保護。

Cisco Umbrella SASE 自動トンネルを設定するためのワークフロー

Cisco Umbrella セキュア アクセス サービス エッジ（SASE）トンネルを設定するための前提条件

- Management Center はバージョン 7.3 以降である必要があります。
- Threat Defense デバイスはバージョン 7.1 以降である必要があります。
- 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必要があります。
- 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。

設定手順：

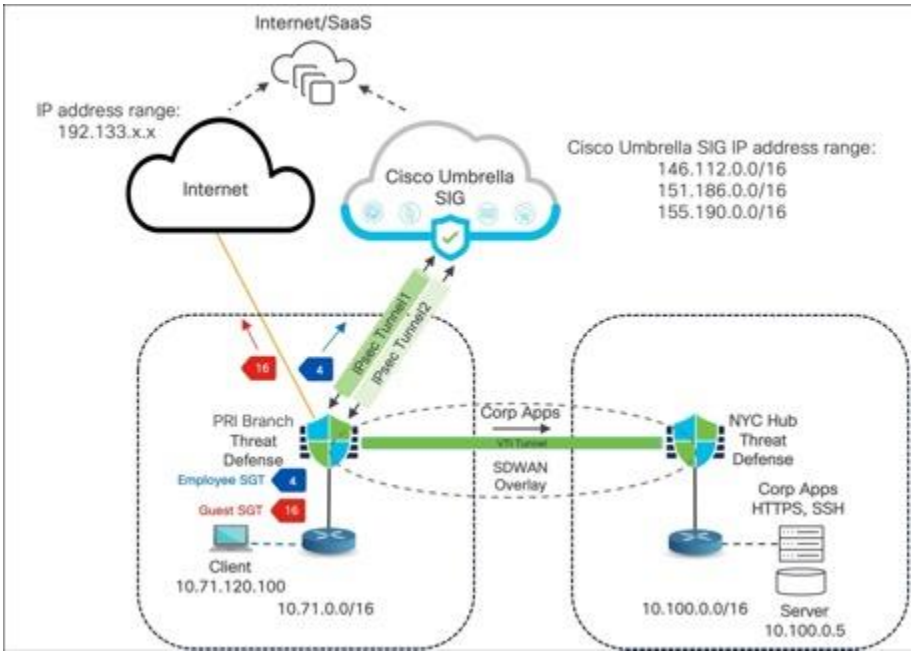
- http://login.umbrella.com で Cisco Umbrella にログインし、Cisco Umbrella への接続を確立するために必要な情報（組織 ID、キーとシークレット、API キー）を取得します。この設定については、このガイドの後半で説明します。
- Threat Defense デバイスから Cisco Umbrella データセンターと通信できる必要があります。「Cisco Umbrella データセンターに関連付けられている IP」を参照してください。

Cisco Umbrella SASE 自動トンネルのネットワークトポロジ

この例では、SASE 統合に Firepower 1010 を使用したプロビデンス、RI（PRI-FW-01）ブランチを使用します。

理解しやすいように、この例ではニューヨーク市、NY（NYC）のハブデバイスのみを使用しています。

図 1.　　Cisco Umbrella SASE 自動トンネルのネットワークトポロジ



- PRI-FW-01 には、NYC ハブデバイスとの SD-WAN 接続があります。
- PRI-FW-01 には、インターネットに接続されたインターフェイスがあります。
- Management Center で Cisco Umbrella SASE 自動トンネルウィザードを使用して、PRI-FW-01 から Cisco Umbrella への 2 つのトンネルを設定します。
- IPSec Tunnel1 は、Cisco Umbrella へのプライマリトンネルです。
- IPSec Tunnel2 は、Cisco Umbrella へのセカンダリトンネルです。
- 従業員には SGT 4 が割り当てられ、ゲストには SGT 16 が割り当てられます。

> **注：**　この SD-WAN アーキテクチャは、Cisco ISE と統合されていません。SGT は Management Center でローカルに割り当てられます。Cisco ISE を使用している場合は、ここで SGT を定義します。

- この例の PBR ポリシーは以下のとおりです。
  - SGT 4 を使用する 10.74.0.0/16 から 10.0.0.0/8 へのトラフィックをブロックします。これにより、すべての従業員オーバーレイトラフィックがデフォルトで通常のルーティングに設定されます。
  - SGT 4 を使用する従業員の DNS/HTTP/HTTPS トラフィックを、検査およびフィルタリングのために Cisco Umbrella SIG サービスにルーティングするよう許可します。
  - SGT 16 を使用するすべてのゲストトラフィックをインターネットに直接ルーティングするよう許可します。
  - SGT 以外のすべてのトラフィックは、自動的に通常のルーティングを使用します。
- PRI-FW-01 インターフェイスの詳細は以下のとおりです。
  - Ethernet1/1（outside1）はアンダーレイ インターフェイスです。
  - トンネル 1（outside1_static_vti_1）およびトンネル 2（outside1_static_vti_2）は、Ethernet1/1 配下のスタティック VTI インターフェイスです。

Management Center の Cisco Umbrella パラメータと Cisco Umbrella API キーのマッピング

Cisco Umbrella を Management Center に登録し、Management Center で Umbrella パラメータを設定する必要があります。

ステップ 1. Cisco Umbrella にログインします。

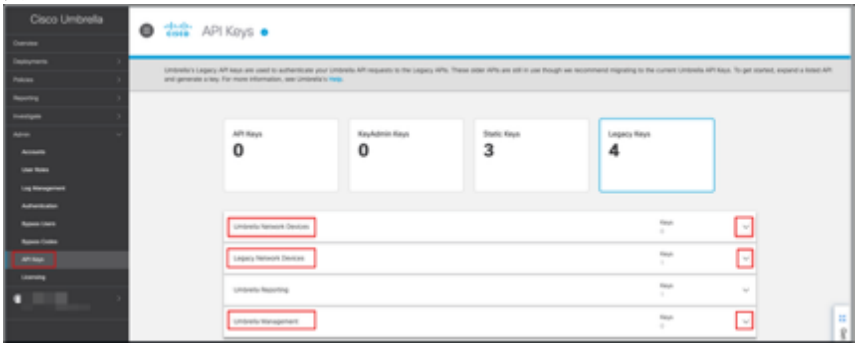
ステップ 2. URL から**組織 ID** をコピーします。

この例の URL は **https://dashboard.umbrella.com/o/abcde/#/overview** です。**abcde** は組織 ID です。

ステップ 3. **[管理（Admin）] > [APIキー（API Keys）] > [レガシーキー（Legacy Keys）] を選択します。**

ステップ 4. 各 API に対応する矢印を展開し、必要な API キーを生成してコピーします。

図 2.　Cisco Umbrella の API キー



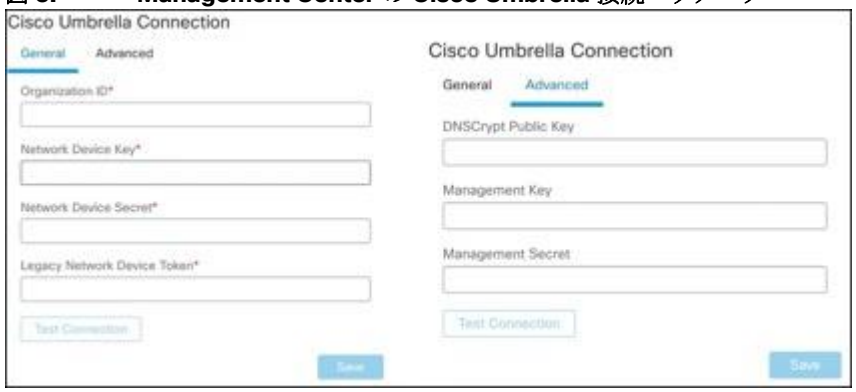
ステップ 5. Management Center にログインします。

ステップ 6. [統合（Integration）] > [その他の統合（Other Integrations）] > [クラウドサービス（Other Integrations）] > [Cisco Umbrella接続（Cisco Umbrella Connection）] を選択して、API キーを使用して Cisco Umbrella 接続パラメータを設定します。

表 1.　Management Center の Cisco Umbrella パラメータと Cisco Umbrella API キーのマッピング

Management Center のパラメータ	Cisco Umbrella の API キー
ネットワークデバイスキー ネットワーク デバイス シークレット	Umbrella ネットワークデバイス
レガシー ネットワーク デバイス トークン	レガシー ネットワーク デバイス
管理キー Management Secret	Umbrella 管理

図 3.　　Management Center の Cisco Umbrella 接続パラメータ



注：　DNSCrypt 公開キーはオプションのパラメータです。

ステップ 7.　組織 ID、トークン、およびキーを追加したら、[テスト接続（Test Connection）] をクリックして Cisco Umbrella との API 統合を確認します。

正常に接続されたら、[接続に成功しました（Connection Successful）] とのメッセージが表示されます。

Cisco Umbrella 用の SASE トポロジの設定

異なる Cisco Umbrella データセンターを使用して高可用性を実現できます。

ステップ 1.　Management Center にログインします。

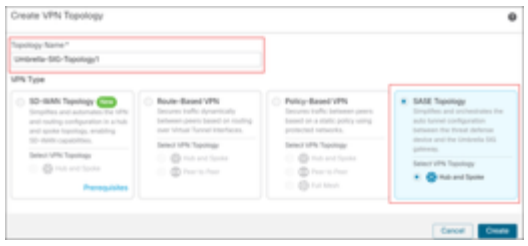
ステップ 2.　[デバイス（Devices）] > [VPN] > [サイト間（Site To Site）] を選択します。

ステップ 3.　[追加（Add）] をクリックします。

ステップ 4.　[SASEトポロジ（SASE Topology）] ラジオボタンをクリックして、**[SASEトポロジ（SASE Topology）]** ウィザードを開きます。

ステップ 5.　[トポロジ名（Topology Name）] フィールドに一意のトポロジ名を入力します。

この例では、名前は **Umbrella-SIG-Topology1** です。

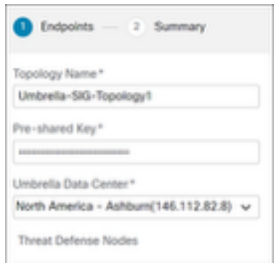


ステップ 6.　[作成（Create）] をクリックします。

ステップ 7.　[事前共有キー（Pre-shared Key）] フィールドには、**Umbrella PSK** 要件に従って自動生成されたキーがウィザードによって入力されます。

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 8.　**Cisco Umbrella データ**センター 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。



ステップ 9. [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 デバイスを追加します。

ステップ 10. [エンドポイントの追加（Add Endpoint）] ダイアログボックスで、次のパラメータを設定します。

i. [デバイス（Device）] ドロップダウンリストから Threat Defense デバイス（**PRI-FW-01**）を選択します。

ii. [VPNインターフェイス（VPN Interface）] ドロップダウンリストから [+] をクリックし、新しいスタティック VTI インターフェイスを作成します。

iii. [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に、事前入力されたデフォルト設定が示されます。次の手順で説明するように、いくつかのパラメータを設定する必要があります。

iv. [名前（Name）] フィールドに、スタティック VTI の名前を入力します。この例では、**Umbrella_SIG_Pri_svti_3** です。

v. [セキュリティゾーン（Security Zone）] ドロップダウンリストからセキュリティゾーンを選択します。この例では、**tunnel-zone** です。

vi. [トンネル送信元（Tunnel Source）] ドロップダウンリストから、インターフェイスを選択します。この例では、アンダーレイインターフェイスの **Ethernet1/1（outside1）** が選択され、値が **Dynamic** に設定されます。

vii. [IPアドレス（IP Address）] エリアで、**[IPの設定（Configure IP）]** オプションボタンを選択し、スタティック VTI インターフェイスの IP を入力します。この例では、**169.254.2.5/30** です。

viii. [OK] をクリックします。

ステップ 11.　[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。この例では、**PRI-FW-01-Pri** です。

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。その後、Management Center 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。

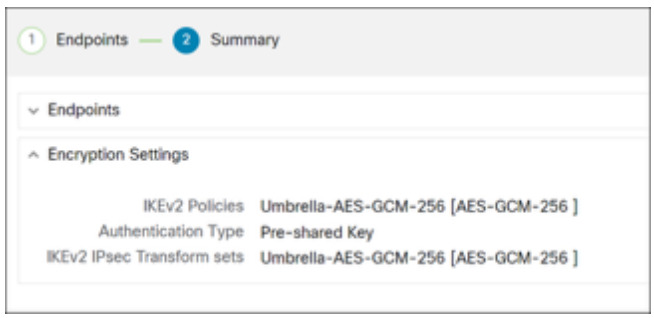
ステップ 12.　[保存（Save）] をクリックします。

ステップ 13.　画面の情報を確認します。

ステップ 14.　[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。

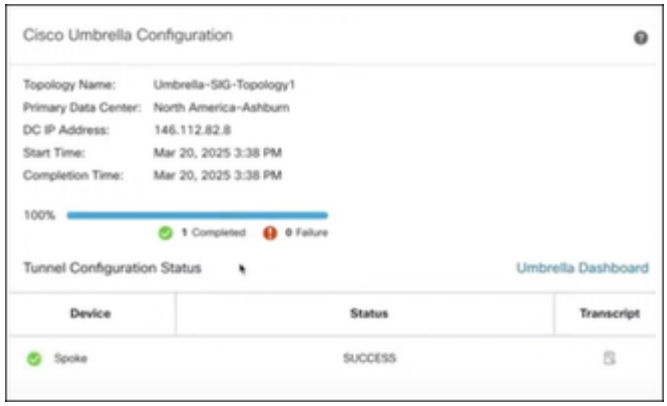


ステップ 15. [Threat Defenseノードに構成を展開する（Deploy configuration on threat defense nodes）] チェックボックスをオンにすると、Threat Defense デバイスへのネットワークトンネルの展開がトリガーされます。

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 16. [保存（Save）] をクリックして、次のアクションを実行します。

- SASE トポロジを Management Center に保存します。
- Threat Defense デバイスのネットワークトンネルの Cisco Umbrella への展開をトリガーします。
- オプションが有効になっている場合は、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設定とポリシー（非 VPN ポリシーを含む）が展開されます。
- [Cisco Umbrella設定（Cisco Umbrella Configuration）] ダイアログボックスを開き、Cisco Umbrella でのトンネル展開のステータスを表示します。



ステップ 17. [Cisco Umbrellaダッシュボード（Umbrella Dashboard）] をクリックして、Cisco Umbrella のネットワークトンネルを表示します。

ステップ 18. [トランスクリプト（Transcript）] アイコンをクリックして、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、トランスクリプトの詳細を表示します。

ステップ 19. 手順 3 ～ 18 を繰り返して、Cisco Umbrella へのセカンダリトンネル（**Umbrella-SIG-Topology2**）を設定します。

ステップ 20. セカンダリトンネルの設定時は、次のガイドラインに従います。

- このトンネルには別の Cisco Umbrella データセンターを選択します。

- 新しいスタティック VTI インターフェイス（**Umbrella_SIG_Sec_svti_4**）を作成します。
- [トンネル送信元（Tunnel Source）] で **Ethernet1/1 (outside1)** を選択します。
- 新しい**ローカルトンネル ID（PRI-FW-01-Sec）**を設定します。

セキュリティグループタグの設定

セキュリティ グループ タグ（SGT）オブジェクトは、単一の SGT 値を指定します。ルールで SGT オブジェクトを使用して、Cisco ISE で割り当てられたものではない SGT 属性を持つトラフィックを制御できます。

注： アイデンティティソースとして Cisco ISE を使用している場合、カスタム SGT オブジェクトを作成することはできません。

ステップ 1. [オブジェクト（Objects）] **>** [オブジェクト管理（Object Management）] を選択します。

ステップ 2. 左側のペインで、[外部属性（External Attributes）] > [セキュリティグループタグ（Security Group Tag）] をクリックします。

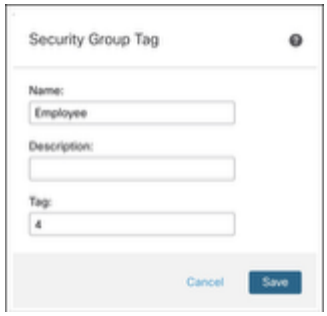
ステップ 3. [セキュリティ グループ タグの追加（Add Security Group Tag）] をクリックします。

ステップ 4. **[名前（Name）]** フィールドに、名前を入力します。この例では、**Employee** を使用します。

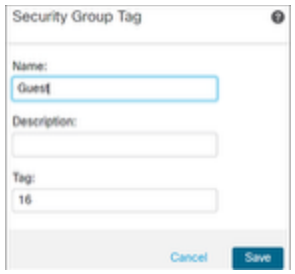
ステップ 5. （任意）[説明（Description）] フィールドに説明を入力します。

ステップ 6. [タグ（Tag）] フィールドに、単一の SGT を入力します。

ステップ 7. [保存（Save）] をクリックします。タグ値が **4** で名前が **Employee** の SGT が作成されます。



ステップ 8. 手順 3 から手順 7 を繰り返して、値 **16** の **Guest** SGT を作成します。



拡張 ACL オブジェクトの設定

アプリケーションの拡張 ACL を設定して、PBR を使用してさまざまな出力インターフェイスを介してアプリケーション トラフィックをインターネットに誘導する必要があります。

この例では、次のルールを使用して ACL を作成します。

- SGT 4 を使用する 10.71.0.0/16 から 10.0.0.0/8 へのトラフィックをブロックします。これにより、すべての従業員オーバーレイトラフィックが通常のルーティングを使用します。

- SGT 4 を使用する従業員の DNS/HTTP/HTTPS トラフィックを、検査およびフィルタリングのために Cisco Umbrella SIG サービスにルーティングするよう許可します。
- SGT 16 を使用するすべてのゲストトラフィックをインターネットに直接ルーティングするよう許可します。

ステップ 1. [オブジェクト（Objects）] **>** [オブジェクト管理（Object Management）] を選択します。

ステップ 2. 左側のペインで、**[アクセスリスト（Access Lists）] > [拡張（Extended）]** をクリックします。

ステップ 3. [拡張アクセスリストを追加（Add Extended Access List）] をクリックします。

ステップ 4. [新規拡張ACLオブジェクト（New Extended ACL Object）] ダイアログボックスで、次のパラメータを設定します。

i. [名前（Name）] フィールドにオブジェクトの名前（**Umbrella-SIG-employee-sgt4-acl**）を入力します。

ii. [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。

iii. [アクション（Actions）] ドロップダウンリストから、[ブロック（Block）] を選択します。

iv. [Network] タブをクリックします。

v. **PRI-inside-10.71.0.0-16** を検索し、[送信元に追加（Add to Source）] をクリックします。

vi. **IPv4-Private- 10.0.0.0-8** を検索し、[接続先に追加（Add to Destination）] をクリックします。

vii. [セキュリティグループタグ（Security Group Tag）] タブをクリックします。

viii. **Employee** を検索し、**[追加（Add）]** をクリックします。

ix. [保存（Save）] をクリックします。

x. [追加（Add）] をクリックして、次の拡張アクセスリストを追加します。

xi. [アクション（Action）] ドロップダウンリストから、[許可（Allow）] を選択します。

xii. [Network] タブをクリックします。

xiii. **PRI-inside-10.71.0.0-16** を検索し、[送信元に追加（Add to Source）] をクリックします。

xiv. **any** を検索し、[接続先に追加（Add to Destination）] をクリックします。

xv. [セキュリティグループタグ（Security Group Tag）] タブをクリックします。

xvi. **Employee** を検索し、**[追加（Add）]** をクリックします。

xvii. [保存（Save）] をクリックします。

ステップ 5. [保存（Save）] をクリックします。拡張 ACL が **[拡張ACL（Extended ACL）]** ページに表示されます。

ステップ 6. 送信元ネットワークを **PRI-inside-10.71.0.0-16**、SGT を **Guest** とする拡張アクセスリスト（**Umbrella-SIG-guest-sgt16-acl**）を作成します。

スタティック ルートの設定

スタティック VTI トンネル **169.254.2.x** のもう一方の端にネクストホップ IP アドレス使用する、Cisco Umbrella のデフォルト 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）] を選択し、Threat Defense デバイスを編集します。この例では、**PRI-FW-01** を使用します。

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. 左側のペインで、[スタティックルート（Static Route）] をクリックします。

ステップ 4. [ルートを追加（Add Route）] をクリックします。

ステップ 5. [スタティックルート設定の追加（Add Static Route Configuration）] ダイアログボックスで、次のパラメータを設定します。

i. [IPv4] オプションボタンをクリックします。

ii. [インターフェイス（Interface）] ドロップダウンリストから、**Umbrella_SIG_Pri_svti_3** を選択します。

iii. [ネットワーク（Network）] として **any-ipv4** を選択します。

iv. [ゲートウェイ（Gateway）] フィールドに、**169.254.2.2** と入力します。この IP アドレスは、「Cisco Umbrella 用の SASE トポロジの設定」セクションで定義されたトンネル IP アドレスサブネットから導かれます。

v. アンダーレイネットワークに 1 が使用されているため、[メトリック（Metric）] フィールドには 1 より大きい値を入力します。この例では、**10** を指定します。

vi. [OK] をクリックします。

ステップ 6. Cisco Umbrella へのセカンダリトンネルに別のスタティックルートを設定します。

i. [インターフェイス（Interface）] ドロップダウンリストから、**Umbrella_SIG_Sec_svti_4** を選択します。

ii. [ネットワーク（Network）] として **any-ipv4** を選択します。

iii. [ゲートウェイ（Gateway）] フィールドに、**169.254.2.6** と入力します。

iv. [メトリック（Metric）] フィールドに、値 **11** を入力します。

v. [OK] をクリックします。

ステップ 7. [保存（Save）] をクリックします。

ポリシー ベース ルーティング ポリシーの設定

ステップ 1. [デバイス（Devices）] **>** [デバイス管理（Device Management）] を選択します。

ステップ 2. デバイス（**PRI-FW-01**）の横にある [編集（Edit）] アイコンをクリックします。

ステップ 3. [ルーティング（Routing）] タブをクリックします。

ステップ 4. 左側のペインで、[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 5. [追加（Add）] をクリックします。

ステップ 6. [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インターフェイスを選択します。

> **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。

この例では、入力インターフェイスは **inside-employee** です。

ステップ 7. [追加（Add）] をクリックして、ポリシーの一致基準と転送アクションを指定します。

ステップ 8. [転送アクションの追加（Add Forwarding Actions）] ダイアログボックスで、以下のパラメータを設定します。

i. [ACLの照合（Match ACL）] ドロップダウンリストから、拡張 ACL（**Umbrella-SIG-employee-sgt4-acl**）を選択します。

ii. [宛先（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。

iii. [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。

iv. [使用可能なインターフェイス（Available Interfaces）] ボックスで、インターフェイスの横にある [+] 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。この例では、**Umbrella_SIG_Pri_svti_3** および **Umbrella_SIG_Sec_svti_4** を選択します。

v. [保存（Save）] をクリックします。

ステップ 9. [追加（Add）] をクリックして、ゲストトラフィックの転送アクションを設定します。

ステップ 10. [転送アクションの追加（Add Forwarding Actions）] ダイアログボックスで、以下のパラメータを設定します。

i. [ACLの照合（Match ACL）] ドロップダウンリストから、拡張 ACL（**Umbrella-SIG-guest-sgt16-acl**）を選択します。

ii. [宛先（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。

iii. [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 [インターフェイス プライオリティ（Interface Priority）] を選択します。

iv. [使用可能なインターフェイス（Available Interfaces）] ボックスで、インターフェイスの横にある [+] 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。この例では、**outside1** を選択します。

注： インターネットトラフィック用のアクセスポリシーと NAT ポリシーがあることを確認します。

ステップ 11. [保存（Save）] をクリックします。

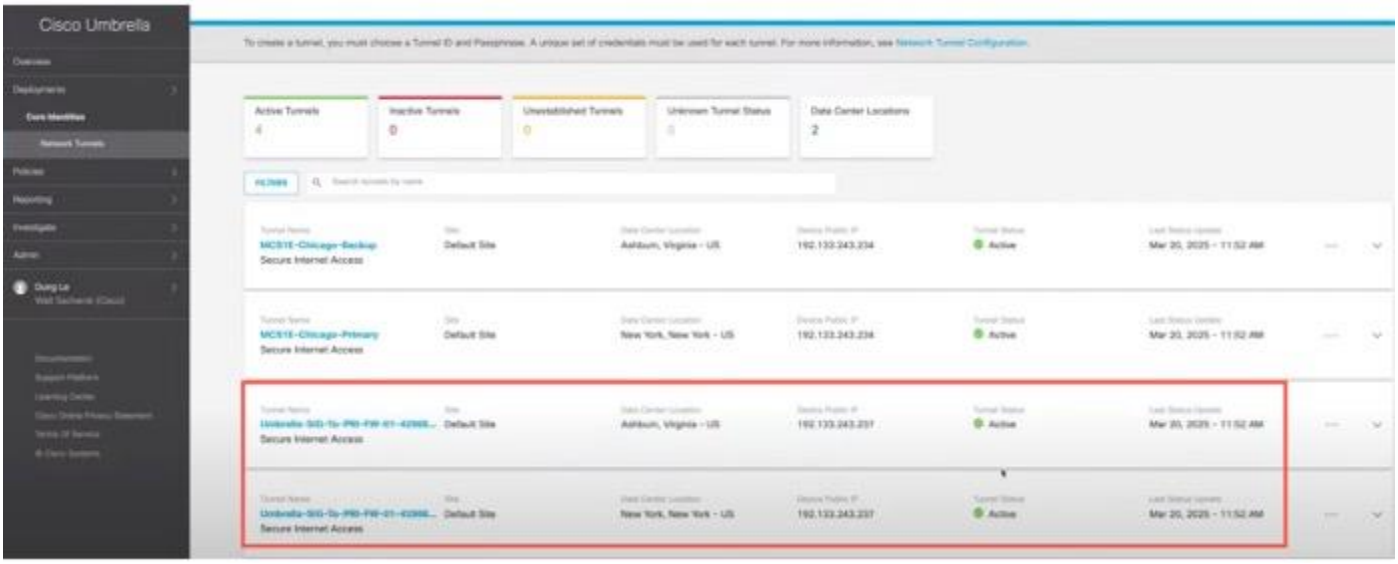
設定例を次に示します。

ステップ 12. デバイスに PBR ポリシーを展開します。

SASE Cisco Umbrella トンネルの展開の確認

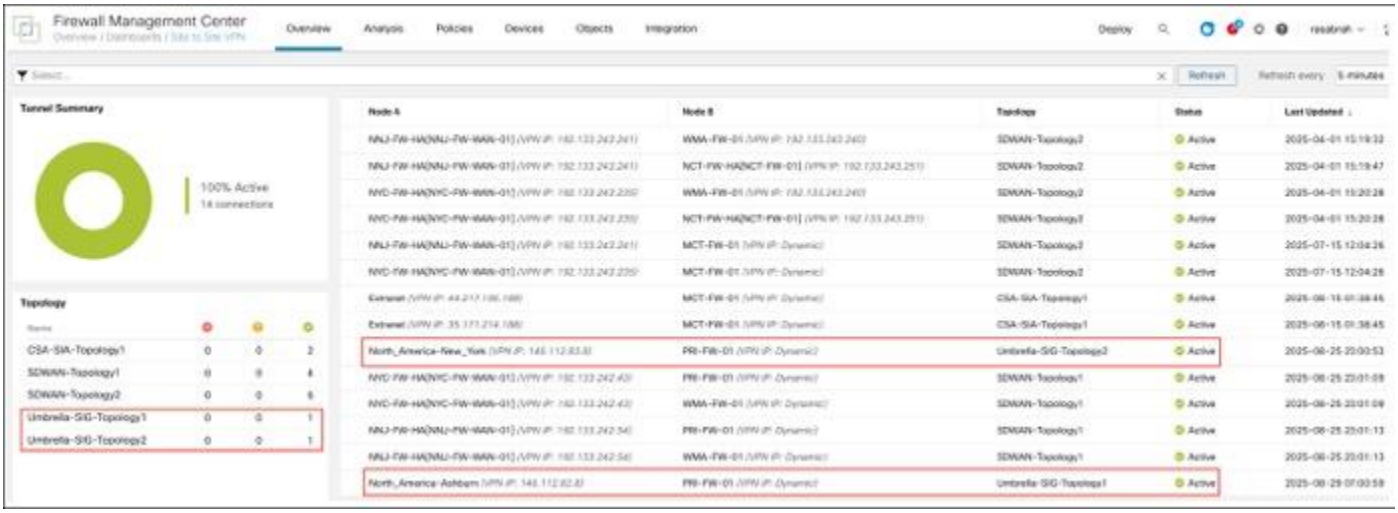
Cisco Umbrella での SASE トンネルの表示

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）] を選択します。Threat Defense デバイスから Cisco Umbrella へのネットワークトンネルが表示されます。



Management Center での SASE トンネルの表示

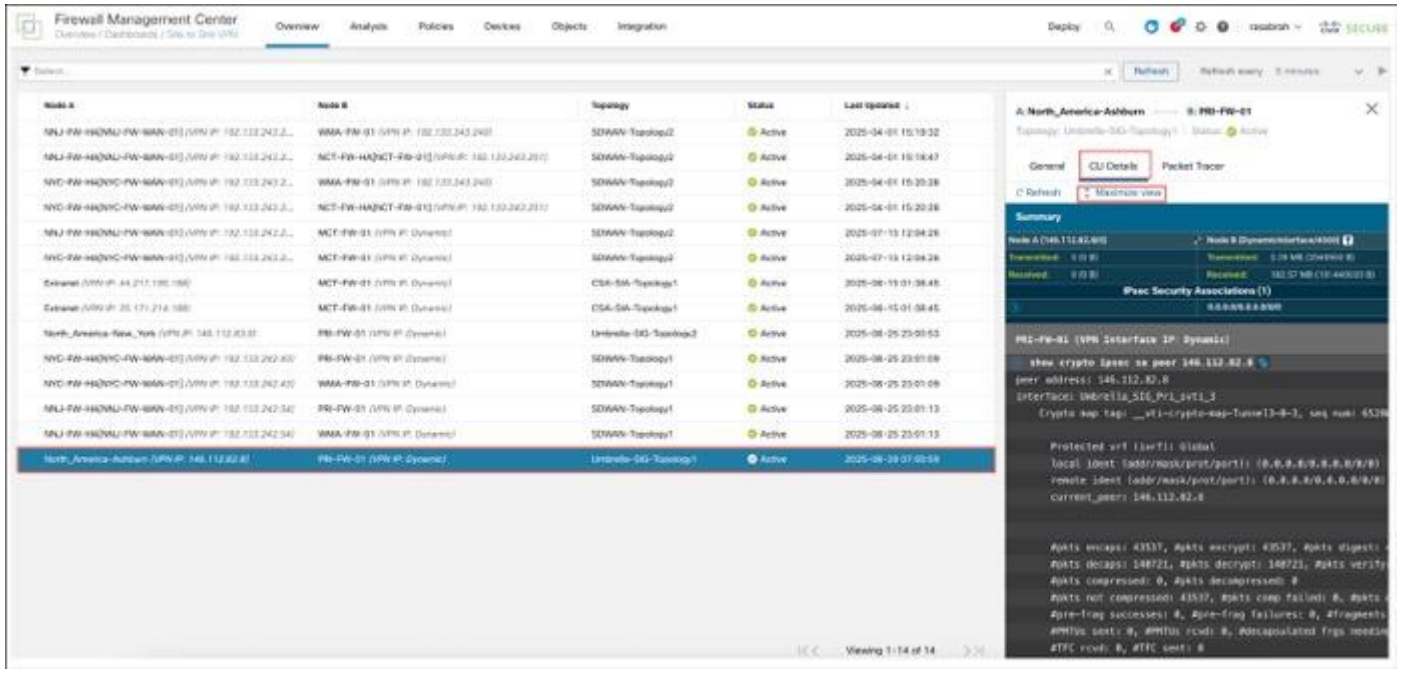
Management Center の [サイト間VPN（Site to Site VPN）] ダッシュボードで SASE トンネルを表示するには、[概要（Overview）] > [ダッシュボード（Dashboard）] > [サイト間VPN（Site to Site VPN）] を選択します。



各トンネルの詳細を表示するには、次の手順を実行します。

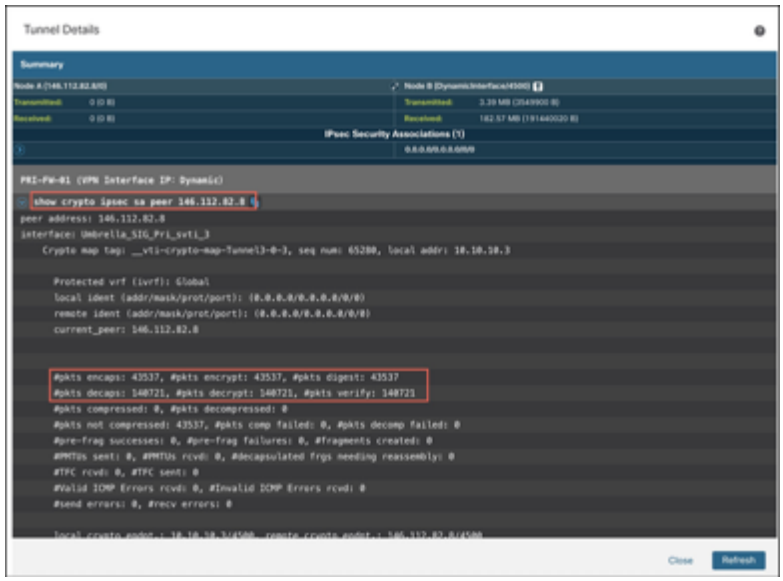
ステップ 1. 各トンネルで、トポロジの上にカーソルを置き、[表示（View）]（）アイコンをクリックします。

ステップ 2. [CLIの詳細（CLI Details）] タブをクリックします。

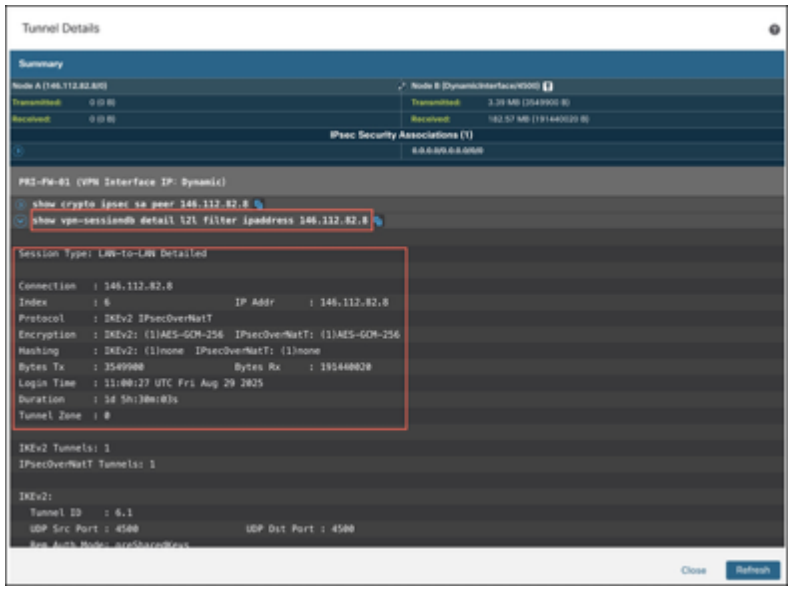


ステップ 3.　[ビューの最大化（Maximize View）] をクリックします。以下のコマンドの出力を表示できます。

- **show crypto ipsec sa peer**：トンネルを介して送信されたパケットの数を表示します。この例では、指定されたピア IP は **146.112.82.8** であり、含まれるトンネルが複数あるため、SASE の正確なトンネル統計を表示できます。



- **show vpn-sessiondb detail l2l filter ipaddress**：VPN 接続のより詳細なデータを表示します。



Cisco Umbrella へのトラフィックの確認

IP アドレスが **10.71.120.100** のクライアント（詳細については図 1. を参照）から、SGT 4 を使用して従業員としてログインすると、インターネットを参照できます。賭博サイトといったブロックされているサイトにアクセスしようとすると、Cisco Umbrella がこれらのサイトをブロックします。

クライアントの IP アドレスを確認すると、割り当てられている IP アドレスは **155.190.18.5** であり、これは Cisco Umbrella SIG IP アドレス範囲 **155.190.0.0/16** 内にあります。この場合、従業員は Cisco Umbrella SIG IP 範囲を使用してインターネットにアクセスできます。

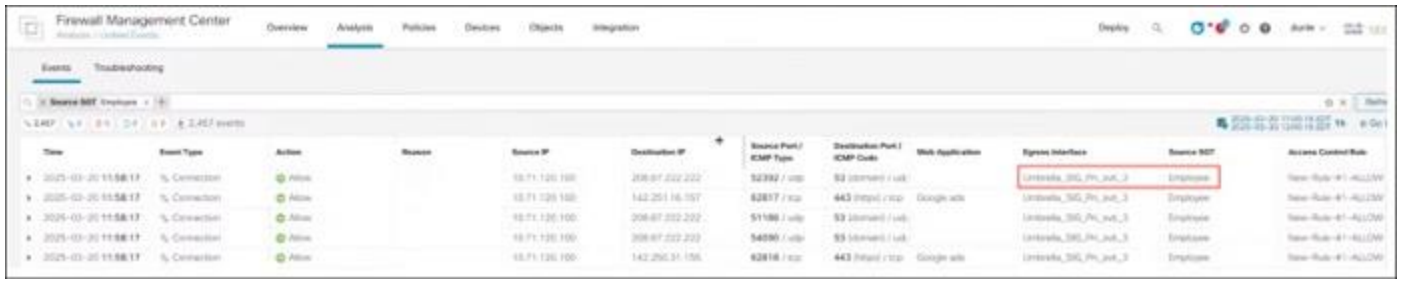
IP アドレス **10.71.120.100** のクライアントから、SGT 16 を使用してゲストとしてログインすると、内部ネットワークにアクセスできないことが確認できます。ただし、インターネットやブロックされたサイトにアクセスすることはできます。ゲストは、Cisco Umbrella を経由せずに直接インターネットにアクセスできます。

Management Center でのトラフィックフローの確認

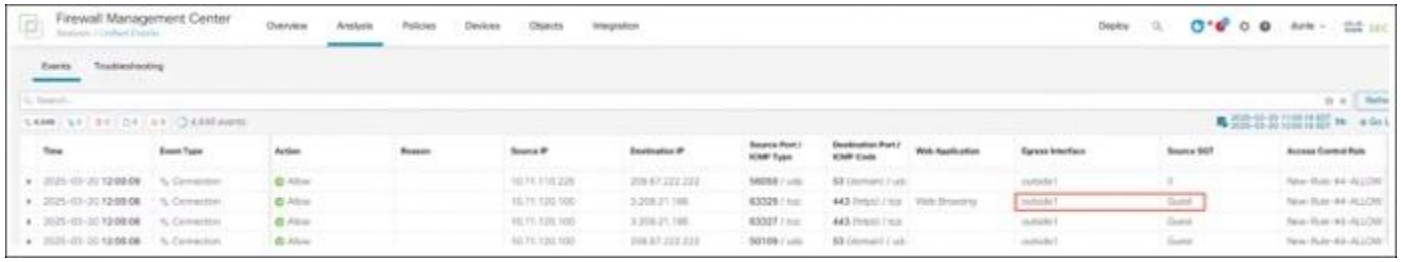
ステップ 1. [分析（Analysis）] > [統合イベント（Unified Events）] を選択します。

ステップ 2. [送信元SGT（Source SGT）] フィルタ内に、**Employee** と入力します。

送信元 **SGT 4** を持つトラフィックは、**Umbrella_SIG_Pri_svti_3 インターフェイス**を通過します。



送信元 **SGT 16** を持つトラフィックは、**outside1** インターフェイスを通過します。



Cisco Umbrella でのトラフィックフローの確認

アクティビティ検索レポートには、Cisco Umbrella によって許可またはブロックされたファイアウォールからのトラフィックに関する詳細が含まれます。

[レポート（Reporting）] > [コアレポート（Core Reports）] > [アクティビティ検索（Activity Search）] を選択します。

図 4.　　許可されたトラフィック

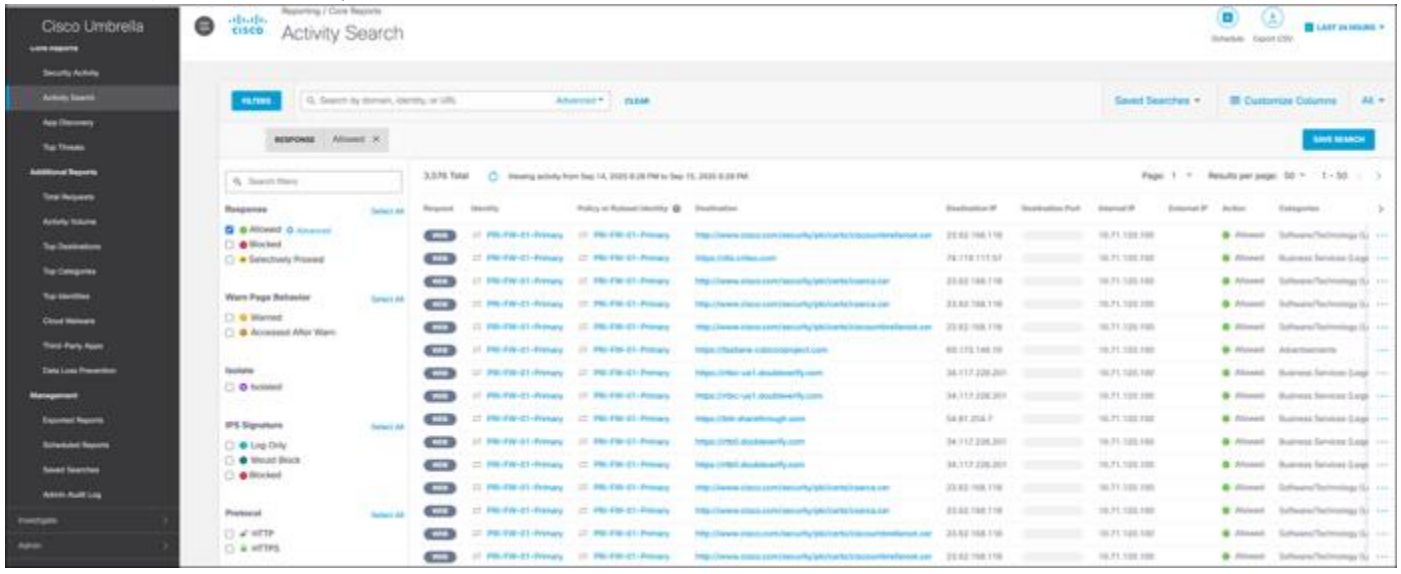
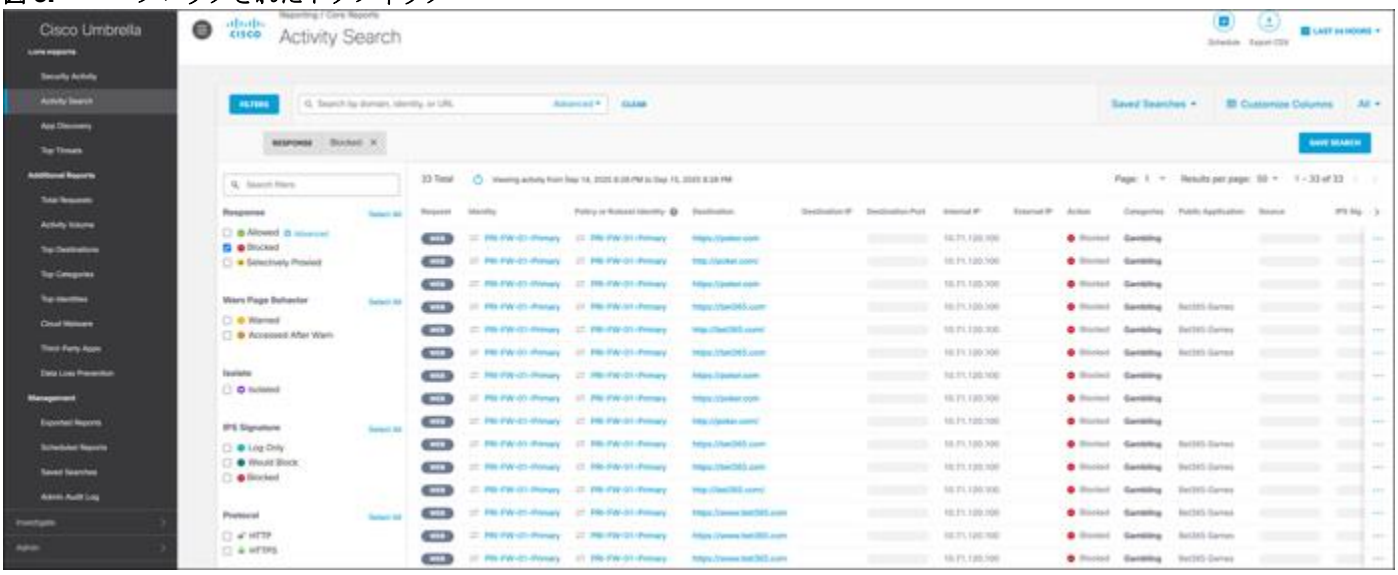


図 5.　　ブロックされたトラフィック



Cisco SSE ソリューション：Cisco Secure Access および Threat Defense を使用したセキュアなブランチ

Cisco Secure Access は、インターネットベースの脅威に対して複数レベルの防御を提供するシスコのクラウドベースのプラットフォームです。組織のネットワークから接続する場合でも、ネットワークからローミングする場合でも、インターネット、SaaS アプリケーションとの統合、およびプライベート デジタル リソースに安全に接続できます。

Cisco Secure Firewall は、主に以下のさまざまなユースケースで Secure Access とシームレスに統合します。

- **リモートユーザーの可視性と制御の強化**：Secure Access は、物理的なブランチ境界を越えてセキュリティポリシーを拡張し、場所に関係なくユーザーを保護します。これにより、オンプレミスと同等レベルの脅威保護とアクセス制御が提供され、一貫したセキュリティ施行が実現されます。
- **簡素化されたセキュリティアーキテクチャ**：Secure Access は Threat Defense デバイスと統合して、セキュア Web ゲートウェイ（SWG）、CASB、DLP、クラウドファイアウォールなどの複数のセキュリティ機能を統合します。この統合により、ブランチ展開とクラウド提供型セキュリティサービス全体のポリシーを一括管理できます。

Secure Access と Threat Defense を統合するためのワークフロー

このセクションでは、Cisco Secure Access 統合の設定プロセスの概要について説明します。この統合には、主に Threat Defense プラットフォームから Cisco Secure Access への手動トンネルの設定が含まれます。

1. Cisco Secure Access ダッシュボードでネットワーク トンネル グループを作成します。

   この最初のステップでは、トンネルグループを作成し、Cisco Secure Access ダッシュボードから必要な設定情報を収集します。

2. Management Center でルートベース VPN ウィザードを使用して、トンネルを設定します。

Cisco Secure Access でネットワーク トンネル グループを作成した後、Management Center に進み、Cisco Secure Access に接続するルートベース VPN トポロジを確立します。

3. 拡張アクセス制御リスト（ACL）を作成します。

   この ACL は、トンネル経由で Cisco Secure Access にルーティングする特定の DNS および Web トラフィックを定義します。このアプローチは、Cisco Umbrella の統合と連携します。

4. ポリシーベースルーティング（PBR）ポリシーの作成

   ポリシーベースルーティング内で以前に作成された ACL を使用して、定義済みの DNS および Web トラフィックをトンネル経由で Cisco Secure Access に送信し、セキュリティ検査を行います。

5. 検証および障害対応

   Cisco Umbrella の統合と同様に、検証および障害対応コマンドが使用できます。主な違いは、Cisco Secure Access ダッシュボードにログインして、トンネルステータスを確認したり、追加の統計を表示したりできることです。

Cisco Secure Access の統合は、Management Center バージョン 7.1 以降でサポートされています。また、Cisco Secure Access 用のトンネルを手動で作成することもできます。

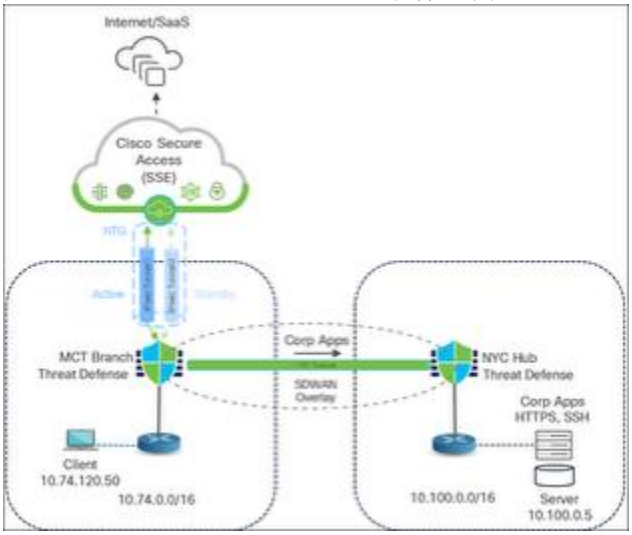
Secure Access と Threat Defense を統合するための前提条件

- Management Center がバージョン 7.1 以降である必要があります。
- Threat Defense デバイスがバージョン 7.1 以降である必要があります。
- 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必要があります。
- Cisco Secure Access Essentials サブスクリプション ライセンスが使用可能である必要があります。

ブランチ ネットワーク セキュリティのための Cisco Secure Access と Threat Defense の統合

この例では、ブランチのネットワークセキュリティのために、Secure Access 統合に次のトポロジを使用します。

図 6.　　Cisco Secure Access 統合のネットワークトポロジ



- MCT ブランチのセットアップ：MCT ブランチでは、SD-WAN オーバーレイトンネルがすでに確立されている単一の Threat Defense デバイスを使用します。このトンネルは、企業のアプリケーションが存在するニューヨーク市（NYC）ハブサイト（10.100.0.0/16）の内部リソースへの接続を提供します。

- Cisco Secure Access へのトンネル：セキュアなインターネットアクセスとクラウドセキュリティの施行のために、MCT ブランチ Threat Defense から Cisco Secure Access への 2 つの IPSec トンネルが設定されます。一方のトンネルはアクティブとして指定される一方、他方のトンネルは冗長性のためにスタンバイとして動作し、プライマリ接続障害時での高い可用性が確保されます。
- ポリシーベースルーティング（PBR）：この統合の核心は、デバイス上のポリシーベースルーティング（PBR）設定にあり、さまざまなタイプのトラフィックの処理方法を以下のように明示的に指示します。
  - 内部トラフィック（オーバーレイトラフィック）：PBR ルールは、MCT ブランチの 10.74.0.0/16 IP ブロックから発信され、内部ネットワーク（10.0.0.0/8 で表され、NYC ハブの企業アプリケーション サブネット 10.100.0.0/16 を含む）に送信されるトラフィックをブロックするように設定されます。この明示的なブロックにより、すべての内部トラフィックまたは「オーバーレイトラフィック」が PBR ポリシーをバイパスし、通常のルーティングへと戻ります。その後、このトラフィックは、既存の SD-WAN オーバーレイトンネルを利用して、企業内部のアプリケーションおよびサービスにアクセスします。
  - インターネットトラフィック（SSE サービス）：逆に、セカンダリ PBR ルールは、他のすべてのトラフィックを許可するように設定されます。これにより、企業の内部ネットワーク宛てではないトラフィック（インターネット宛てのトラフィック）が、確立された IPSec トンネルを介して Cisco Secure Access に明示的にルーティングされます。セキュリティサービスエッジ（SSE）ソリューションとして機能する Cisco Secure Access は、検査、フィルタリング、DNS セキュリティ、レイヤ 3 またはレイヤ 4 ファイアウォール、および Secure Web ゲートウェイサービスなどの包括的なクラウド ベース セキュリティ機能を提供します。この主な目的は、ブランチから発信されるすべてのインターネット宛てトラフィックをクラウド セキュリティ プラットフォームで保護し、完全に検査することです。

ネットワーク トンネル グループの設定

ステップ 1. Cisco Security Cloud Sign On ポータルから Secure Access にサインインします。

ステップ 2. Security Cloud Sign On で、Secure Access 組織に参加するための招待を受信した電子メールアドレスを入力し、[サインイン（SIGN IN）] をクリックします。

Secure Access アカウントと Security Cloud Sign On アカウントには、同じ電子メールアドレスを使用する必要があります。

ステップ 3. [接続（Connect）] > [ネットワーク接続（Network Connections）] > [ネットワーク トンネル グループ（Network Tunnel Groups）] を選択します。

ステップ 4. [追加（Add）] をクリックします。

ステップ 5. トンネルグループの **全般設定**を入力します。

- **[トンネルグループ名（Tunnel Group Name）]**：名前を入力します。この例では、**MCT-FW-01** を使用します。
- **[地域（Region）]**：この例では、**[US（バージニア）（US (Virginia)）]** を選択します。
- **[デバイスタイプ（Device Type）]**：この例では、**[FTD]** を選択します。

ステップ 6. [次へ（Next）] をクリックします。

ステップ 7. [トンネルIDおよびパスフレーズ（Tunnel ID and Passphrase）] エリアでは、このトンネルグループへの接続に使用する **MCT-FW-01** デバイスのトンネル ID とパスフレーズを設定します。

- **[トンネルIDフォーマット（Tunnel ID Format）]**：この例では、手順 2 でトンネルグループに指定した名前を使用します（**MCT-FW-01**）。フォーマットは **<tunnel name>@<org><hub>.sse.cisco.com** です。

- **[パスフレーズ（Passphrase）]**：トンネルのパスフレーズを 16 ～ 64 文字で入力します。パスフレーズには、少なくとも 1 つの大文字、1 つの小文字、および 1 つの数字を使用する必要があります。パスフレーズに特殊文字を使用することはできません。
- 確認のためにパスフレーズを再入力します。

ステップ 8. [次へ（Next）] をクリックして続行します。

ステップ 9. [ルーティング（Routing）] エリアで、次の設定を行います。

ブランチのセキュアなインターネットアクセス用に Cisco Secure Access（SSE）を設定する場合には、[NAT/アウトバウンドのみ有効化（Enable NAT/Outbound Only）]、[スタティックルーティング（Static routing）]、および [ダイナミックルーティング（Dynamic routing）] の 3 つのプライマリ ルーティング オプションがあります。

この例では、[NAT/アウトバウンドのみ有効化（Enable NAT/Outbound Only）] チェックボックスをオンにします。MCT-FW-01 Threat Defense デバイスの背後にあるユーザーにセキュアなインターネットアクセスを提供する場合は、このオプションを使用します。

ダイナミック ルーティング メソッドは特に、セキュアなプライベート アプリケーション アクセスを処理する場合に使用されます。

ステップ 10. [保存（Save）] をクリックします。

ステップ 11. [トンネル設定のデータ（Data for Tunnel Setup）] エリアで、ネットワーク トンネル デバイスの設定時に使用する情報を確認し、保存します。

注： パスフレーズが表示されるのはこのときだけです。

ステップ 12. [CSVのダウンロード（Download CSV）] をクリックして、トンネル設定情報を保存します。この情報を使用して、Management Center から Threat Defense デバイスにトンネルを設定および展開できます。

ステップ 13. [完了（Done）] をクリックします。

トンネルグループが、[ネットワークトンネル（Network Tunnels）] エリアのトンネルなしで作成されます。

Threat Defense での VPN トンネルの作成

ステップ 1. Management Center で、[デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。

ステップ 2. [MCT-FW-01] をクリックします。

この例では、**NYC-FW-HA** および **NNJ-FW-HA** に向かう SDWAN オーバーレイ用に 2 つのオーバーレイトンネルがすでに作成されています。

Cisco Secure Access 用にトンネルを 2 つ追加作成します。

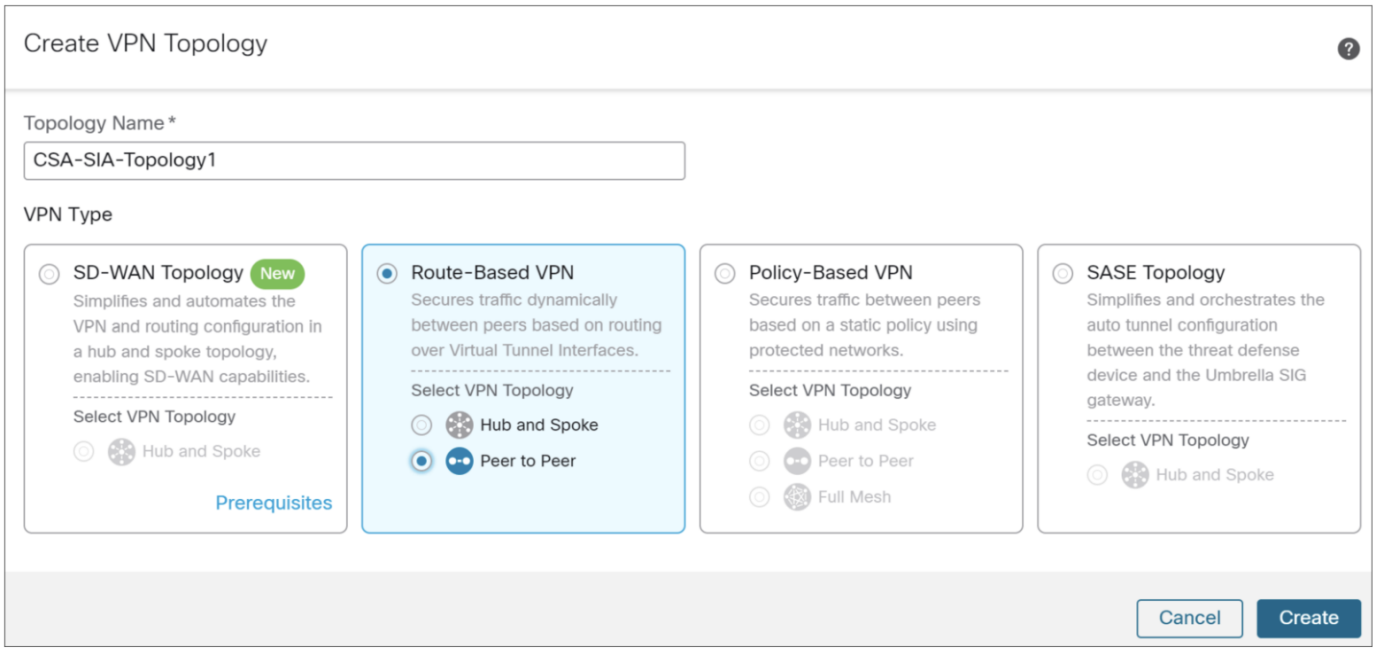
ステップ 3. [デバイス（Devices）] > [サイト間（Site To Site）] を選択します。

ステップ 4. [追加（Add）] をクリックします。

ステップ 5. [トポロジ名（Topology Name）] フィールドに名前を入力します。この例では、名前は **CSA-SIA-Topology1** です。

ステップ 6. [ルートベースVPN（Route-Based VPN）] をクリックし、[ピアツーピア（Peer to Peer）] を選択します。通常、このトポロジでのデフォルトの選択はハブアンドスポークですが、この例では別のアプローチが使用されています。2 台のデバイスを使用するピアツーピア接続を選択します。

図 7. ルートベース **VPN**



ステップ 7. [作成（Create）] をクリックします。

この VPN 設定では IKEv2 のみがサポートされており、これがデフォルトで選択されています。

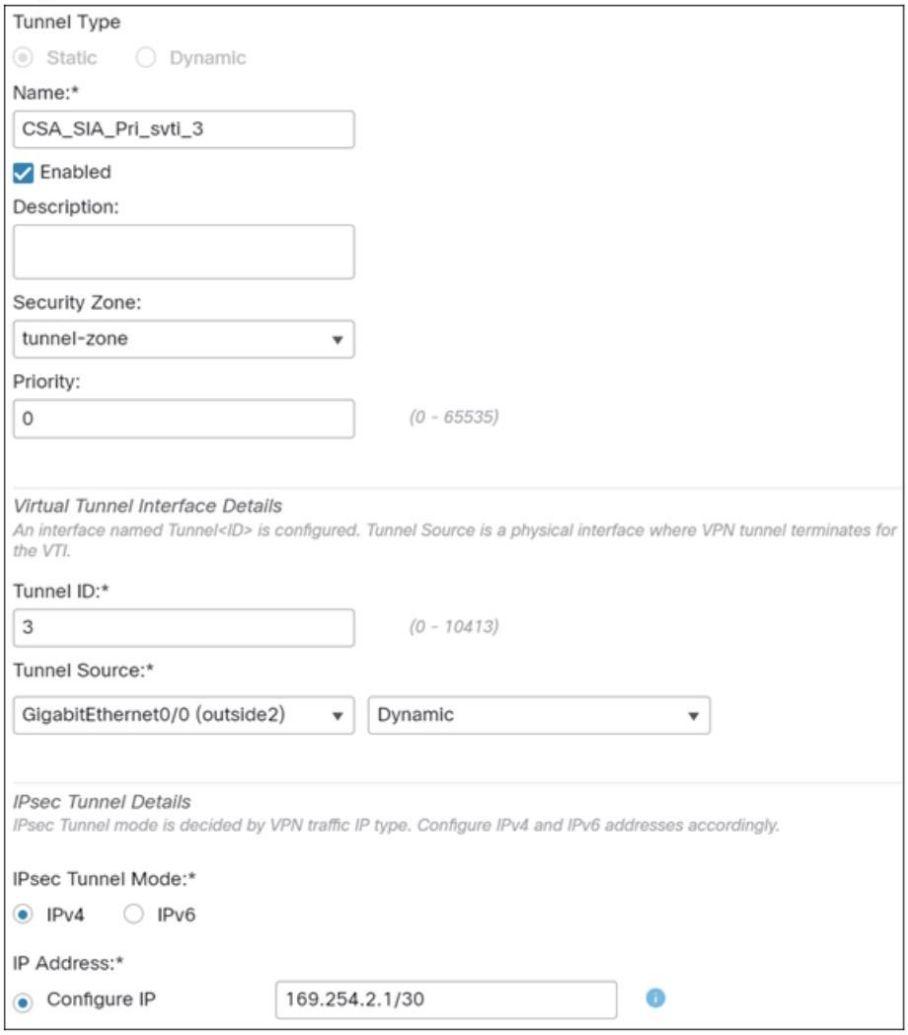
エンドポイントの設定

ステップ 1. [ポイントツーポイント（Point to Point）] タブで、**MCT-FW-01** デバイスを選択します。

ステップ 2. [+] 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ます。

図 8._　　仮想トンネルインターフェイスの追加



i. **[名前（Name）]** フィールドに、名前を入力します。この例では、インターフェイス名は **CSA_SIA_Pri_svti_3** です。

ii. Cisco Secure Access 統合のスタティック仮想トンネルインターフェイス（VTI）を設定する場合、このプロセスでは、[セキュリティゾーン（Security Zone）] に [トンネルゾーン（tunnel zone）] を選択し、優先順位とトンネル ID にデフォルト設定を使用する必要があります。[セキュリティゾーン（Security Zone）] ドロップダウンリストから [トンネルゾーン（tunnel-zone）] を選択します。

iii. [トンネル送信元（Tunnel Source）] ドロップダウンリストから、トンネル送信元インターフェイスを選択します。この例では、**GigabitEhternet0/0 (outside2)** を選択します。IP アドレスの割り当てには DHCP を使用するため、[ダイナミック（Dynamic）] が設定されています。

iv. [IPsecトンネルモード（IPsec Tunnel Mode）] では、 [IPv4] を選択し、[IPの設定（Configure IP）] フィールドでは、指定された **IP アドレス**を使用します。

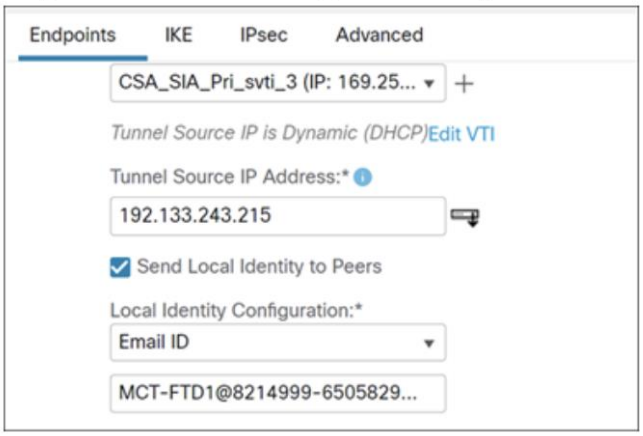
v. [OK] をクリックします。VTI トンネルが作成されます。[トンネル送信元IPアドレス（Tunnel Source IP Address）] フィールドに、外部インターフェイスの IP アドレスが取得されます。

ステップ 3.　[ピアへのローカルIDの送信（Send Local Identity to Peers）] チェックボックスをオンにします。

ステップ 4. [ローカルID設定（Local Identity Configuration）] フィールドで、[電子メール（Email）] を選択します。

ステップ 5. Secure Access からダウンロードした CSV ファイルに記載された**プライマリトンネル ID** アドレスを入力します。

図 9.　エンドポイントの設定



ステップ 6. [+] をクリックして、**バックアップ VTI** を追加します。

ステップ 7. **[名前（Name）]** フィールドに、名前を入力します。この例では、インターフェイス名は **CSA_SIA_Sec_svti_4** です。

i. Cisco Secure Access 統合のスタティック仮想トンネルインターフェイス（VTI）を設定する場合、このプロセスでは、トンネルゾーンを選択し、デフォルト設定の優先順位とトンネル ID の両方をそのまま使用します。[セキュリティゾーン（Security Zone）] ドロップダウンリストから [トンネルゾーン（tunnel-zone）] を選択します。

ii. [トンネル送信元（Tunnel Source）] ドロップダウンリストから、トンネル送信元インターフェイスを選択します。この例では、**GigabitEhternet0/0 (outside2)** を選択します。IP アドレスの割り当てには **DHCP** を使用するため、[ダイナミック（Dynamic）] が設定されています。

iii. [IPsecトンネルモード（IPsec Tunnel Mode）] では、 [IPv4] を選択し、[IPの設定（Configure IP）] フィールドでは、指定された IP アドレスを使用します。

iv. [OK] をクリックします。VTI トンネルが作成されます。[トンネル送信元IPアドレス（Tunnel Source IP Address）] フィールドに、外部インターフェイスの IP アドレスが取得されます。この例では、**169.254.3.1/30** です。

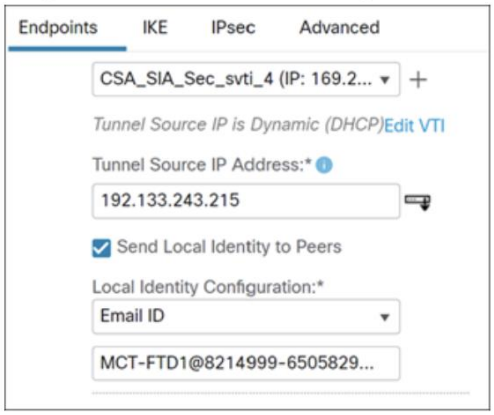
v. [OK] をクリックします。この IP アドレスは、後のルーティング設定で、特にトラフィックをトンネルのもう一方の端に転送する場合に重要です。

ステップ 8. [ピアへのローカルIDの送信（Send Local Identity to Peers）] チェックボックスをオンにします。

ステップ 9. [ローカルID設定（Local Identity Configuration）] フィールドで、[電子メール（Email）] を選択します。

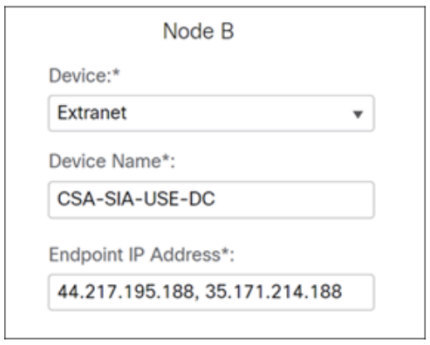
ステップ 10. Secure Access からダウンロードした CSV ファイルに記載された**セカンダリトンネル ID** アドレスを入力します。

図 10.　　セカンダリトンネル ID



ステップ 11.　[ノードB（Node B）] エリアで、[デバイス（Device）] ドロップダウンリストから、[エクストラネット（Extranet）] を選択します。

図 11.　　ノード B 設定



ステップ 12.　[デバイス名（Device Name）] フィールドに、名前を入力します。この例では、**CSA-USE-DC** を指定します。

ステップ 13.　[エンドポイントIPアドレス（Endpoint IP Address）] フィールドに、プライマリデータセンターの IP アドレスを入力し、その後にセカンダリデータセンターの IP アドレスをカンマ区切りで入力します。この情報は、「ネットワーク トンネル グループの追加」トピックの手順 12 で Secure Access からダウンロードした CSV ファイルに記載されています。

IKE の設定

ステップ 1.　[IKE] タブをクリックして、IKEv2 の事前共有キーを設定します。

ステップ 2.　[認証タイプ（Authentication Type）] ドロップダウンリストから [事前共有手動キー（Pre-shared Manual Key）] を選択します。

ステップ 3.　この VPN の事前共有キーを手動で割り当てます。[キー（Key）] を指定して、[キーの確認（Confirm Key）] に同じキーを再入力します。

入力したキーは表示されないため、必ず覚えておいてください。

注：　[詳細設定（Advanced）] タブの [ISAKMP設定（ISAKMP Settings）] で、[ピアアイデンティティ検証（Peer Identity Validation）] ドロップダウンリストから [チェックなし（Do not check）] を選択し、他の設定は変更しません。残りの設定にはデフォルト値が設定されている必要があります。

ステップ 4.　[保存（Save）] をクリックします。トポロジが作成されましたが、設定をプッシュしていないためトンネルはありません。

拡張アクセスリストの作成

ステップ 1. Management Center で、[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] を選択します。

ステップ 2. [アクセスリスト（Access List）] を展開し、[拡張（Extended）] をクリックします。

ステップ 3. [拡張アクセスリストを追加（Add Extended Access List）] をクリックします。

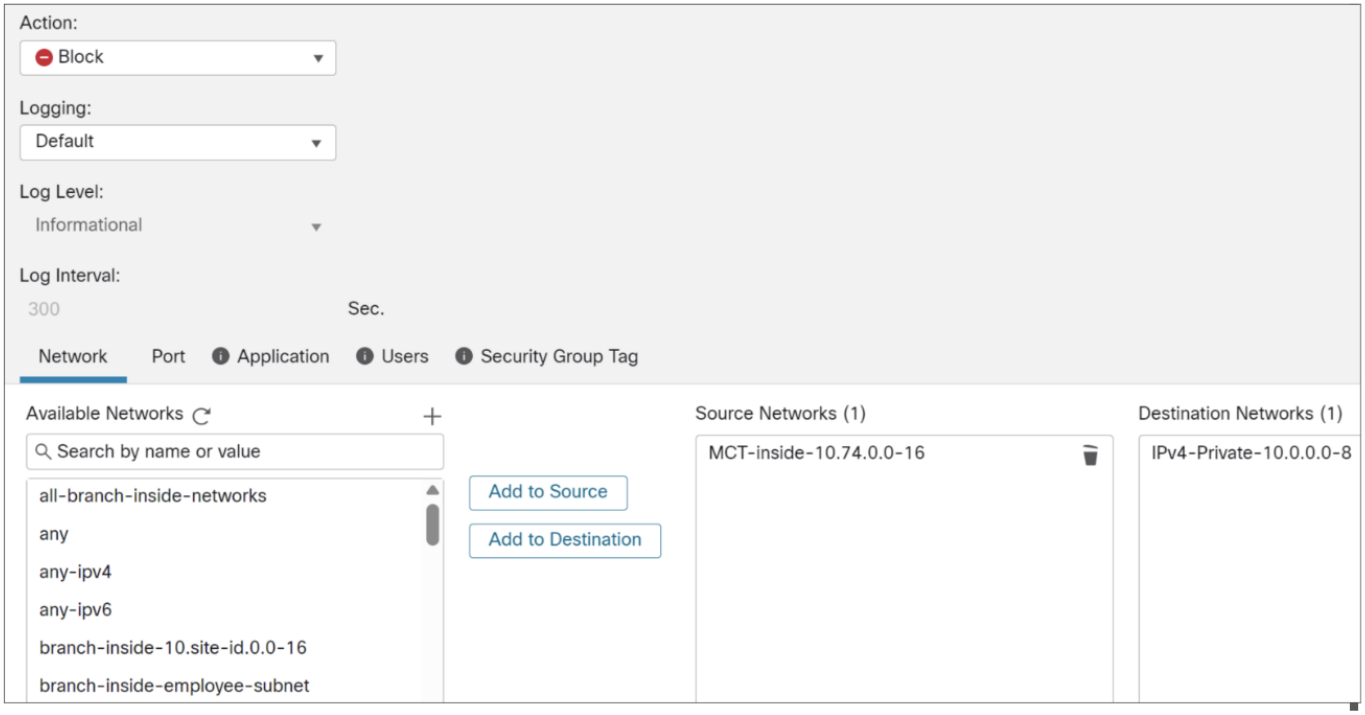
[新しい拡張アクセスリストオブジェクト（New Extended Access List Object）] ダイアログボックスが表示されます。

ステップ 4. [名前（Name）] フィールドにオブジェクトの名前を入力します。この例では、**CSA-SIA-acl** と入力します。

ステップ 5. [追加（Add）] をクリックしてルールを追加します。

最初のルールでは内部トラフィックを処理します。MCT ブランチに割り当てられている **10.74.0.0/16** IP ブロックから発信され、**10.0.0.0/8** 内部ネットワーク（企業のアプリケーションを表す）に送信されるトラフィックは、すべて「ポリシーからドロップされます」。これは、そのような内部トラフィックまたはオーバーレイトラフィックがこれらの PBR ルールから明示的に除外され、代わりにルーティング要件に既存の SD-WAN オーバーレイを利用して、「通常のルーティング」または「トポロジ駆動型ルーティング」でルーティングされることを意味します。

図 12.　[ルールの追加（Add Rule）]



i. **アクション**：ブロック

ii. **ロギング**：デフォルト

iii. **送信元ネットワーク**：MCT-inside-10.74.0.0-16

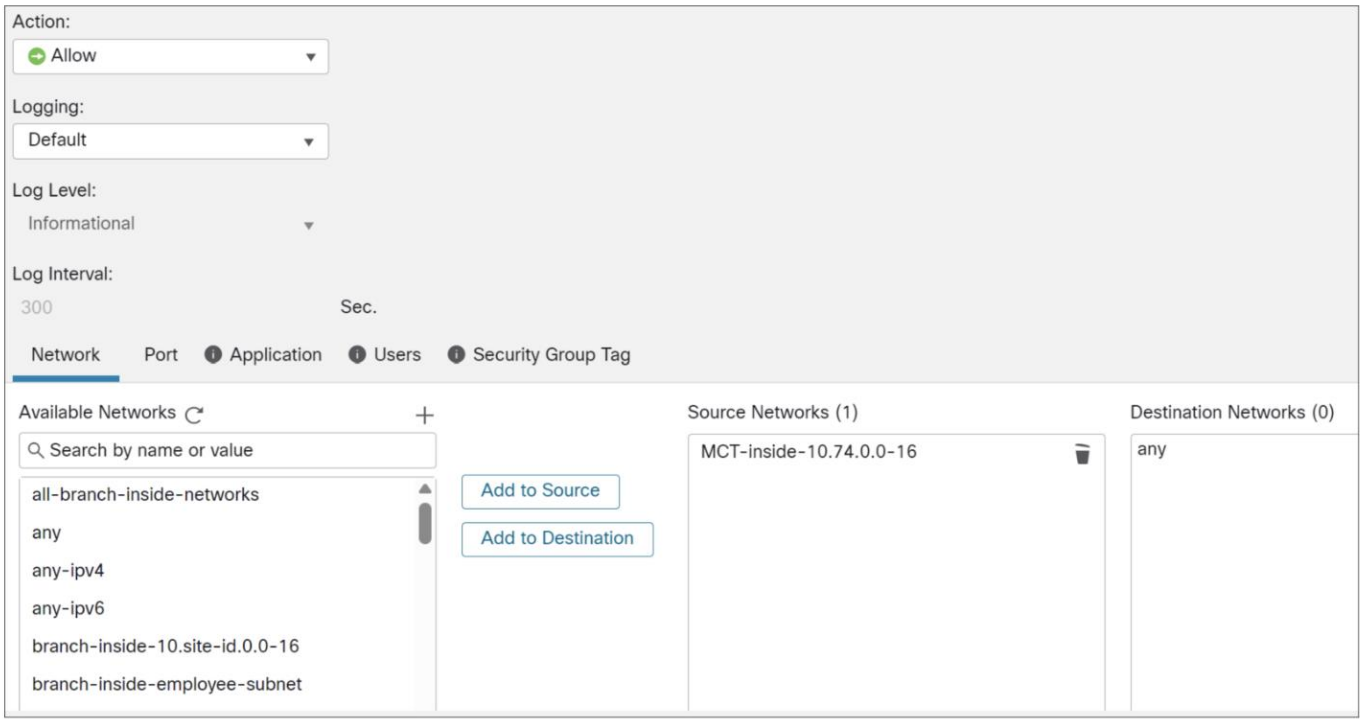
iv. **接続先ネットワーク**：IPv4-Private-10.0.0.0-8

v. [追加（Add）] をクリックします。

ステップ 6. [追加（Add）] をクリックして別のルールを追加します。

10.74.0.0/16 ブロックから発信されたトラフィックで、内部 10.0.0.0/8 ネットワークに送信されていないトラフィックは、インターネットトラフィックとして分類されます。その後、このインターネット宛てトラフィックは、Cisco Secure Access に直接ルーティングされます。これにより、MCT ブランチからのすべての外部トラフィックが、外部の接続先に進む前に、Cisco Secure Access によって提供される検査やフィルタリングなどの必須 SSE サービスの適用を受けるようになります。

図 13.　　ルールを追加



i. **アクション**：許可

ii. **ロギング**：デフォルト

iii. **送信元ネットワーク**：MCT-inside-10.74.0-16

iv. **送信先ネットワーク**：すべて

v. [追加（Add）] をクリックします。

ステップ 7.　[保存（Save）] をクリックします。

拡張 ACL が作成されます。

この例は、ポリシーベースルーティングの別の方法を示すことが目的であるため、スタティックルートは作成しません。スタティックルーティングも 1 つの選択肢ですが、ここでは別の方法を使用します。

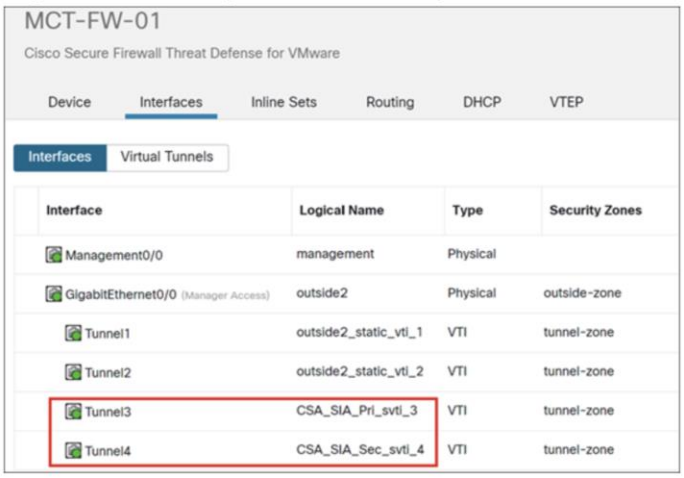
ポリシーベースルーティングの作成

ステップ 1.　Management Center で、[デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。

ステップ 2.　**MCT-FW-01** デバイスをクリックします。

2 つのトンネルが作成済みですが、まだ使用できません。

図 14.　MCT-FW-01 のトンネルインターフェイス

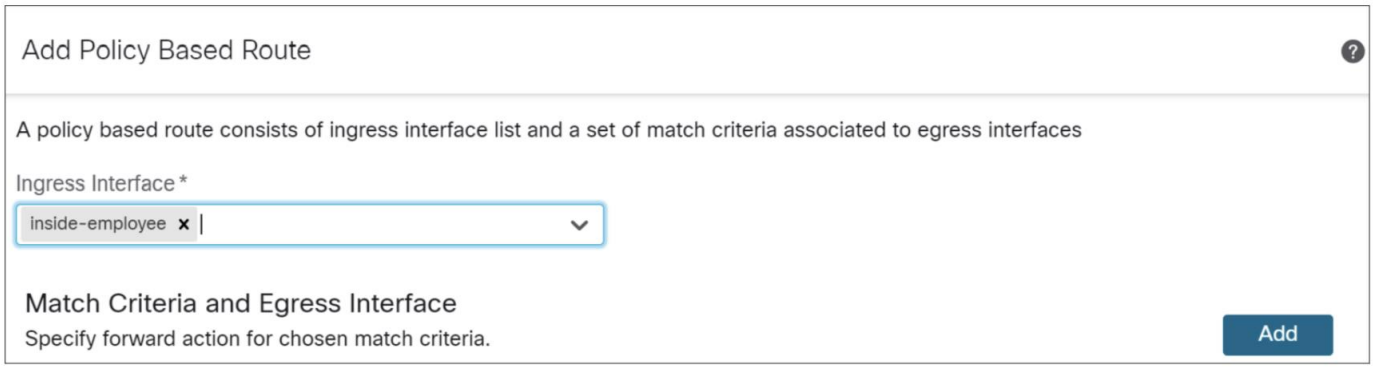


ステップ 3.　[ルーティング（Routing）] タブをクリックします。

ステップ 4.　**[ポリシーベースルーティング（Policy Based Routing）]** をクリックし、**[追加（Add）]** をクリックします。

[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が表示されます。

ステップ 5.　[入力インターフェイス（Ingress Interface）] ドロップダウンリストで入力インターフェイスを選択します。この例では、**inside-employee** を選択します。



注：　Threat Defense デバイスのポリシーベース ルーティング ルールは、デバイス上のインターフェイスに入力するときのトラフィックに適用されます。

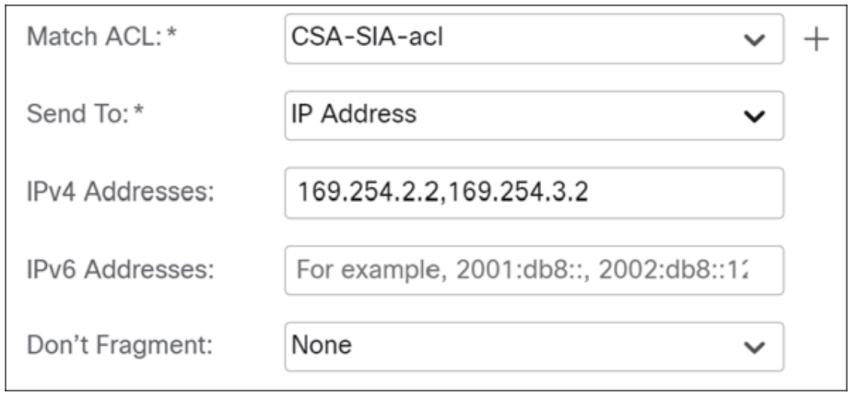
ステップ 6.　[追加（Add）] をクリックします。

ステップ 7.　[ACLの照合（Match ACL）] ドロップダウンリストから、ポリシーベースルーティングに使用するトラフィックを識別する拡張アクセス制御リストオブジェクトを選択します。ACL オブジェクトは、**「拡張リストオブジェクトの設定」**セクションで事前に定義されています。この例では、**CSA-SIA-acl** を選択します。

ステップ 8.　[送信先（Send To）] ドロップダウンリストから、[IPアドレス（IP Address）] を選択して、**IPv4** ネクストホップアドレスを指定します。

ステップ 9.　[IPv4アドレス（IP Address）] フィールドに、アドレスを指定します。ネクストホップは、Cisco Secure Access のトンネルの IP アドレスです。この例では、**169.254.2.2**, 169.254.3.2 と入力します。

図 15.　新しいホップ IP アドレスの追加



プライマリトンネルのネクストホップは **169.254.2.2** として設定されます。この設定は Cisco Secure Access 側となり、**169.254.2.1** がプライマリトンネルのファイアウォール側になります。プライマリトンネルがダウンすると、トラフィックは自動的にセカンダリトンネルにリダイレクトされます。このときのネクストホップは **169.254.3.2** であり、これも Cisco Secure Access 側となっています。

ステップ 10.　[保存（Save）] をクリックします。

デバイスへの変更の展開

ステップ 1.　[展開（Deploy）] をクリックします。

ステップ 2.　[MCT-FW-01] チェックボックスをオンにして、[すべて展開（Deploy All）] をクリックします。

Secure Access でのトンネルの検証

ステップ 1.　Cisco Security Cloud Sign On ポータルから Secure Access にサインインします。

ステップ 2.　Security Cloud Sign On で、Secure Access 組織に参加するための招待を受信した電子メールアドレスを入力し、[サインイン（SIGN IN）] をクリックします。

Secure Access アカウントと Security Cloud Sign On アカウントには、同じ電子メールアドレスを使用する必要があります。

ステップ 3.　[接続（Connect）] > [ネットワーク接続（Network Connections）] > [ネットワーク トンネル グループ（Network Tunnel Groups）] を選択します。

ステップ 4.　**MCT-FW-01** トンネルグループをクリックします。

ステップ 5.　[ネットワークトンネル（Network Tunnels）] エリアに、プライマリトンネルとセカンダリトンネルが表示されます。**Primary1** トンネルはブランチの outside2 インターフェイスから始まり、プライマリ Cisco Secure Access データセンターに向けられています。**Secondary1** トンネルもブランチの **outside2** インターフェイスから始まり、セカンダリデータセンターに接続されて、継続的な接続のためのスタンバイとして機能します。

Secure Access のアクセスポリシーの表示

注：　このドキュメントは設計ガイドとして提供されます。ここで参照するアクセスポリシーは、Cisco Secure Access 内で設定済みであることを前提としています。ポリシー作成の詳細な手順は、このガイドでは説明しません。

ステップ 1.　[接続（Connect）] > [ポリシー（Policy）] > [アクセスポリシー（Access Policy）] を選択します。

最初のルール **mct74-to-internet-block-web-categories** では、MCT サイト 74 から発信されたインターネット向けトラフィックがセキュリティ制御され、特にギャンブルサイトをブロックします。これは、Cisco Secure Access によって提供される URL フィルタリングまたはセキュア Web ゲートウェイ（SWG）サービスの機能です。目的は、ブランチからのインターネット宛てトラフィックに検査やフィルタリングなどのセキュリティポリシーを適用することです。

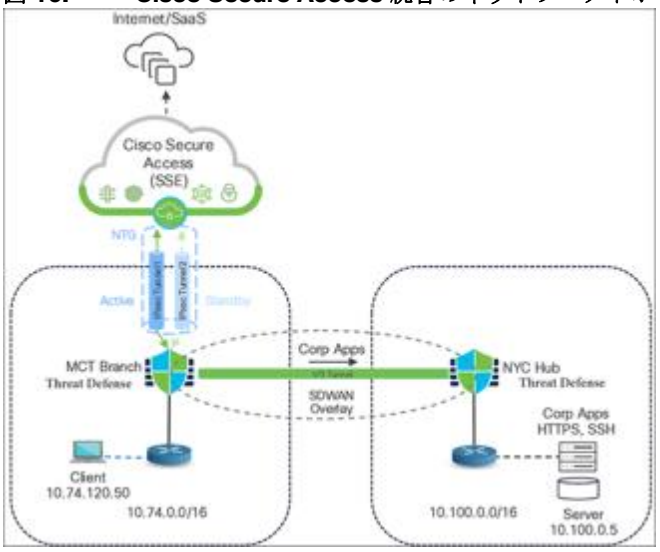
2 つ目のルール **mct74-to-internet-block-ping-8.8.8.8** では、MCT サイト 74 から IP アドレス 8.8.8.8 宛てのトラフィックをドロップします。

3 つ目のルール **mct74-to-internet-permit-all** では、前のルールで明示的にブロックまたはドロップされていない他のすべてのインターネットトラフィックが、さらなる SSE サービスのために Cisco Secure Access の通過を許可されます。

注： ユーザートラフィックは、まず MCT-FW-01 のアクセス制御ポリシーおよび検査の対象になります。これらのポリシーによって許可されたトラフィックのみが、さらなる検査のために Secure Access に転送されます。

CLI を使用した接続の確認

図 16.　Cisco Secure Access 統合のネットワークトポロジ図



テストの目的のために、（上図に従い）IP アドレス 10.74.120.50 のクライアントを使用します。最初のテストでは、ニューヨークのデータセンターの 10.100.0.5 にあるサーバーへのアクセスを試みて、トラフィックフローを確認しました。

```
C:\Users\user\>ipconfig
Ethernet adapter Main NIC:
Connection-specific DNS Suffix
IPv4 Address          : 10.74.120.50
Subnet Mask           : 255.255.255.0
Default Gateway       : 10.74.120.1

C:\Users\user> ping 10.100.0.5
Pinging 10.100.0.5 with 32 bytes of data:
Reply from 10.100.0.5: bytes=32 time=2ms TTL=252
```

```
Reply from 10.100.0.5: bytes=32 time=2ms TTL=252
Reply from 10.100.0.5: bytes=32 time=2ms TTL=252
Reply from 10.100.0.5: bytes=32 time=2ms TTL=252
Ping statistics for 10.100.0.5:
           Packets: Sent 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
           Minimum = 2ms, Maximum = 3ms, Average = 2ms
```

定義済みポリシーに従い、次のようになる必要があります。

- 8.8.8.8 への ping 要求はブロックされます。
- 8.8.4.4 への ping 要求は成功します。
- cisco.com への ping 要求は成功します。

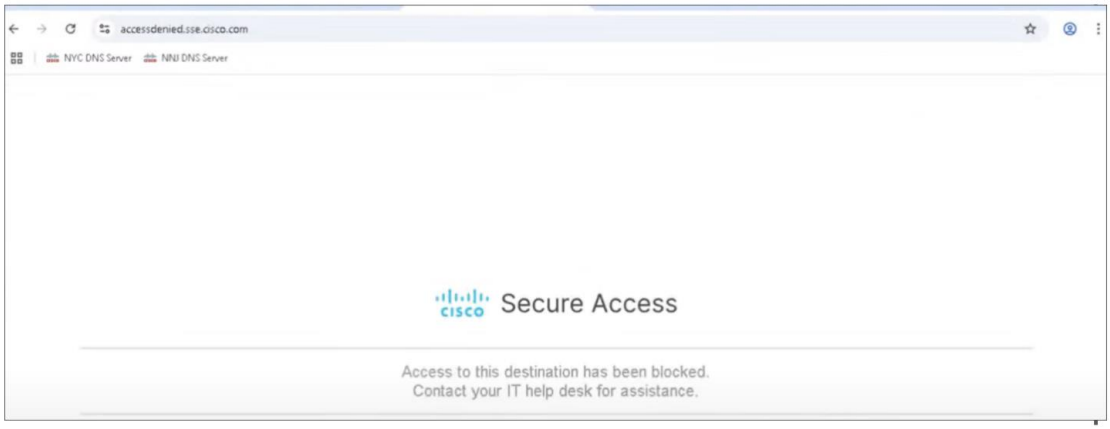
ポリシー評価を検証するため、上記の IP および URL に対してテストを実行します。

```
C:\Users\user>ping 8.8.8.
Pinging 8.8.8.8 with 32 bytes of data:
Request timed out.

C:\Users\user>ping 8.8.4.4
Pinging 8.8.4.4 with 32 bytes of data:
Reply from 8.8.4.4: bytes=32 time=2ms TTL=45
Reply from 8.8.4.4: bytes=32 time=2ms TTL=45
Reply from 8.8.4.4: bytes=32 time=2ms TTL=45
Reply from 8.8.4.4: bytes=32 time=2ms TTL=45
Ping statistics for 8.8.4.4:
           Packets: Sent 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
           Minimum = 13ms, Maximum = 14ms, Average = 13ms

C:\Users\user>ping cisco.com
Pinging cisco.com [72.163.4.185] with 32 bytes of data:
Reply from 72.163.4.185: bytes=32 time=2ms TTL=38
Reply from 72.163.4.185: bytes=32 time=2ms TTL=38
Reply from 72.163.4.185: bytes=32 time=2ms TTL=38
Reply from 72.163.4.185: bytes=32 time=2ms TTL=38
Ping statistics for 72.163.4.185:
           Packets: Sent 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
           Minimum = 48ms, Maximum = 49ms, Average = 48ms
```

Secure Access SWG ポリシーのテスト

セキュア Web ゲートウェイ（SWG）フィルタリング機能を確認するには、次のテストを実行します。

- **Web アクセスの許可**：e-コマース（ショッピング）Web サイト（www.amazon.com）および自動車購入サイト（www.ford.com）へのアクセスに成功しました。これは、トラフィックフローが SWG を介して許可されていることを示します。
- **Web アクセスのブロック**：ギャンブル Web サイト（www.bet365.com）へのアクセスがブロックされています。これにより、URL フィルタリングポリシーが効果的に適用されていることが確認されます。



Secure Access でのアクティビティ検索レポートの表示

アクティビティ検索レポートには、アクセスポリシールールによって許可またはブロックされたファイアウォール要求に関する完全な詳細情報が含まれます。

ステップ 1. Secure Access アプリケーションで、[モニター（Monitor）] > [アクティビティ検索（Activity Search）] を選択します。

MCT-FW-01 から発信されているトラフィックを確認できます。このアクティビティには、許可されたトラフィックとブロックされたトラフィックの両方が含まれます。

ステップ 2. [応答（Response）] フィルタで、[ブロック（Blocked）] チェックボックスをオンにして、ブロックされたアクティビティを表示します。

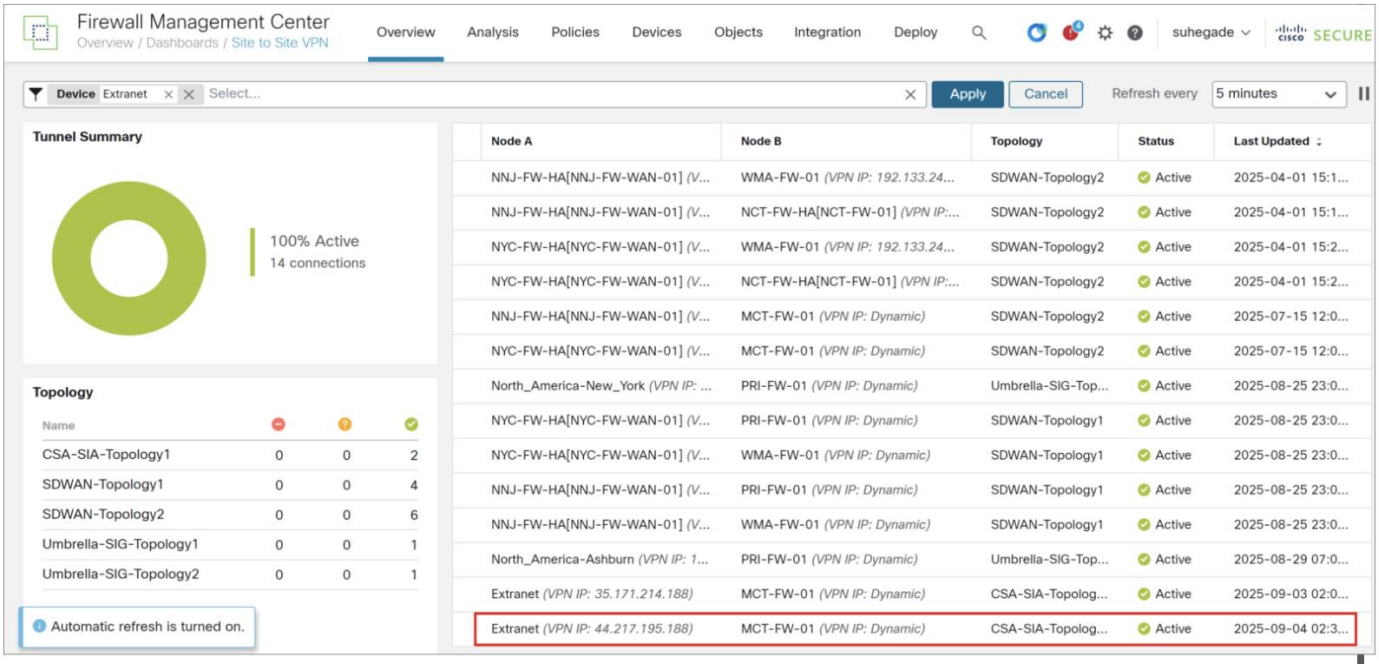
ギャンブルサイト（www.bet365.com）と 8.8.8.8 への ping がブロックされていることがわかります。

Management Center でのトンネルステータスの表示

ステップ 1. Management Center で、[概要（Overview）] > [ダッシュボード（Dashboard）] > [サイト間VPN（Site to Site VPN）] を選択します。

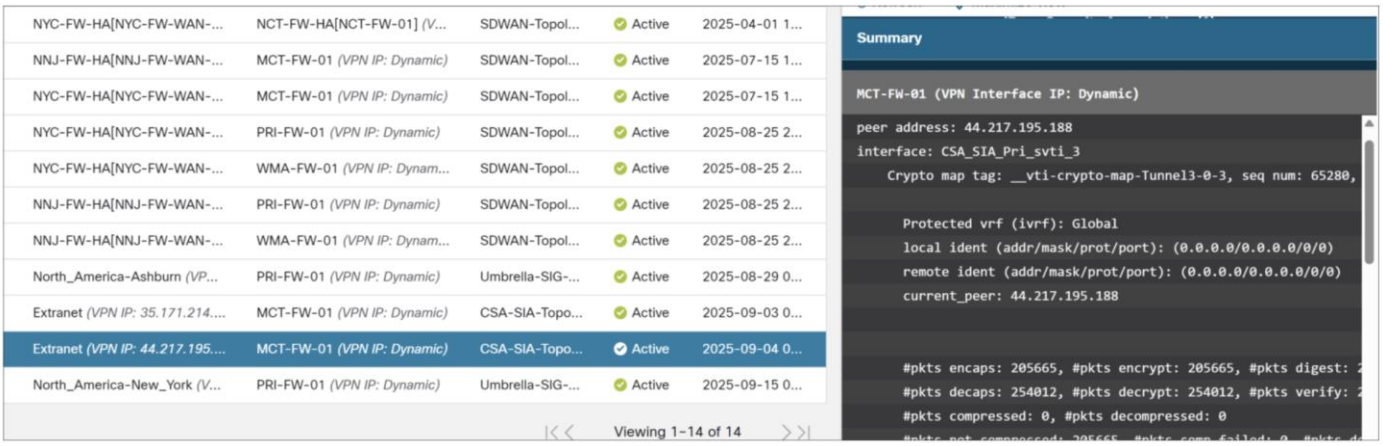
ステップ 2. Cisco Secure Access への**エクストラネット**トンネルの横にある [すべての情報を表示（View full information）]（）アイコンをクリックします。

図 17.　　サイト間 VPN ダッシュボード



ステップ 3.　　[CLIの詳細（CLI Details）] タブをクリックし、「**show crypto ipsec sa peer**」コマンドを展開します。

図 18.　　CLI の詳細



ステップ 4.　　トンネルが稼働しており、トラフィックが許可されていることの検証として、パケットの暗号化と復号を観察できます。

SD-WAN 設計およびその他のユースケースの詳細については、『Cisco Secure Firewall Threat Defense SD-WAN 設計および展開ガイド』を参照してください。

米国本社
カリフォルニア州サンノゼ

アジア太平洋本社
シンガポール

ヨーロッパ本社
アムステルダム（オランダ）

シスコは世界各国に約 400 のオフィスを開設しています。オフィスの住所、電話番号、FAX 番号は当社の Web サイト（www.cisco.com/jp/go/offices）をご覧ください。

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。