手動方式によるセキュリティサービスエッジとSD-WAN間のプライベートアプリケーション相互接続の設定

内容

はじめに

このドキュメントでは、セキュアなプライベートアプリケーションアクセスに重点を置いて、Cisco Secure AccessとSD-WANルータを接続するための包括的なガイドについて説明します。

このガイドについて

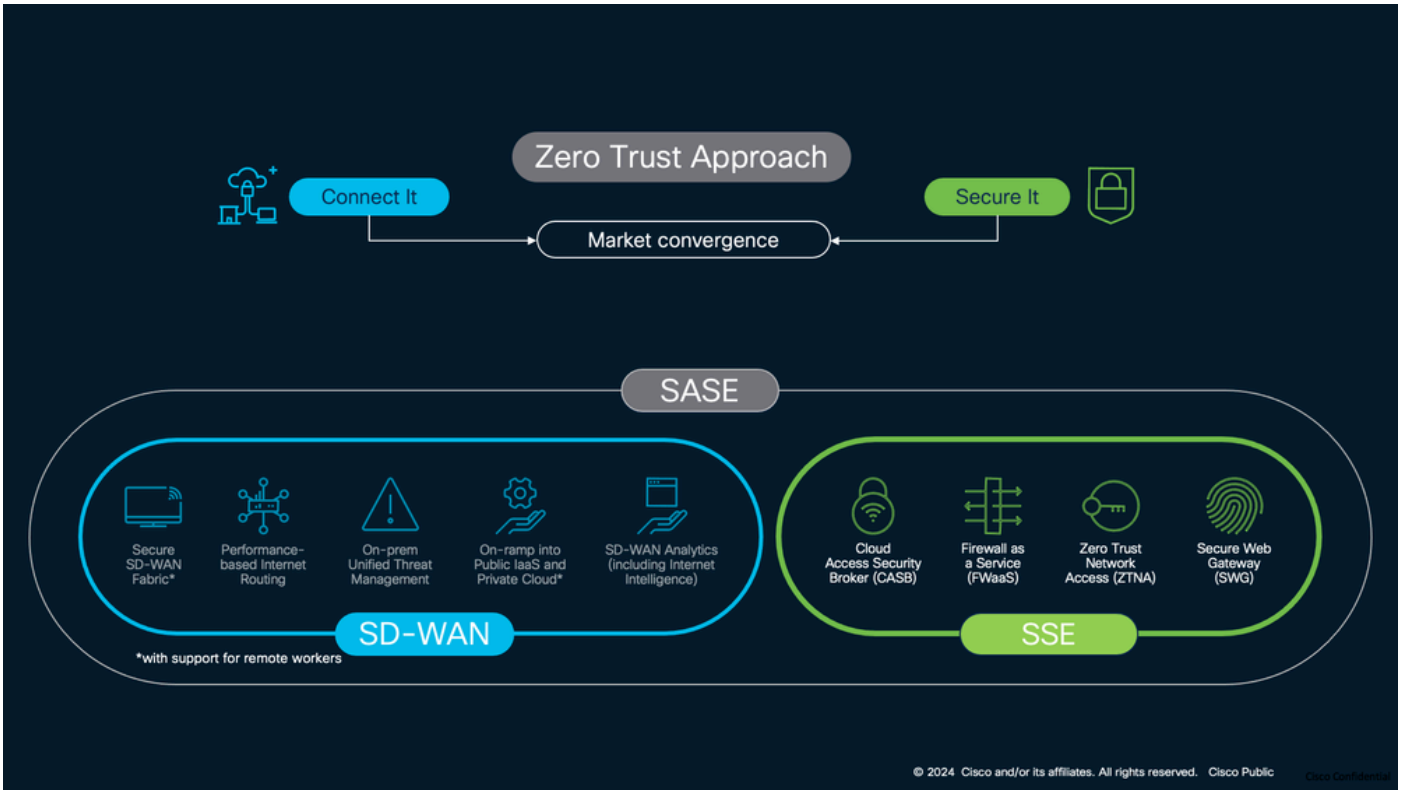
注：ここで示す設定は、SD-WANのバージョンUX1.0および17.9/20.9用に開発されています。

このガイドでは、次の重要なステップの構造化されたチュートリアルを提供します。

- ネットワークトンネルグループ(NTG)の定義
- IPSecトンネルの設定：Cisco SD-WANルータとCisco Secure Access NTGの間にセキュアなIPSecトンネルを設定するための詳細な手順。
- BGPネイバーシップ：IPSecトンネルを介してBGPネイバーシップを実行する手順をステップごとに説明し、ダイナミックルーティングとネットワーク復元力の向上を実現します。
- プライベートアプリケーションアクセス：確立されたトンネルを介したプライベートアプリ

ケーションへのアクセスの設定と保護に関するガイダンス。

図1:Cisco SD-WANおよびSSEのゼロトラストアプローチ



SSEとSD-WAN

このガイドでは、NTGインターコネクトの設計に関する考慮事項と導入のベストプラクティスを中心に説明します。このガイドでは、SD-WANコントローラはクラウドに導入され、WANエッジルータはデータセンターに導入され、少なくとも1つのインターネット回線に接続されます。

主な前提条件

- Cisco Secure Access Secure Service Edge(SSE):Cisco Secure Access SSEが組織にすでにプロビジョニングされていることを前提としています。
- Cisco SD-WAN WANエッジルータ：WANエッジルータはオーバーレイネットワークに統合されると想定されており、SD-WANインフラストラクチャ全体のユーザトラフィックを効率的に促進します。
- このガイドでは、主に設計と設定のSD-WANの側面に焦点を当てていますが、既存のネットワークアーキテクチャ内にCisco Secure Accessソリューションを統合するための全体的なアプローチを提供します。

このソリューションについて

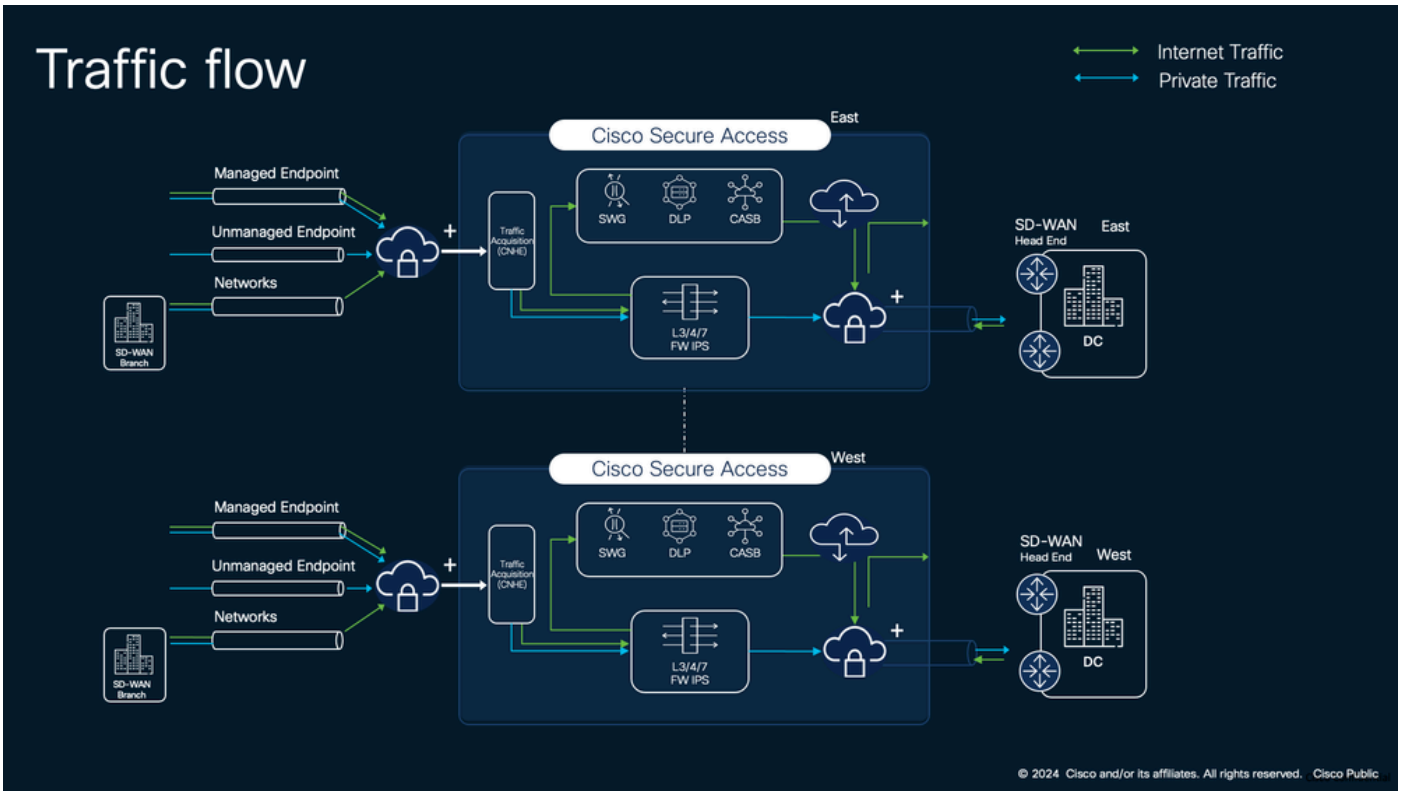
Cisco Secure Accessが提供するプライベートアプリトンネルは、Zero Trust Network Access(ZTNA)およびVPN as a Service(VPNaaS)を介して接続するユーザに、プライベートアプリケーションへの安全な接続を提供します。 これらのトンネルにより、組織はリモートユーザをデータセンターやプライベートクラウドでホストされるプライベートリソースに安全にリンクできます。

これらのトンネルグループは、IKEv2(Internet Key Exchange version 2)を使用して、Cisco Secure AccessとSD-WANルータ間にセキュアな双方向接続を確立します。同じグループ内の複数のトンネルによる高可用性をサポートし、スタティックルーティングとダイナミックルーティング(BGP)の両方による柔軟なトラフィック管理を提供します。
IPsecトンネルは、次のようなさまざまなソースからのトラフィックを伝送できます。

- リモートアクセスVPNユーザ
- ブラウザベースまたはクライアントベースのZTNA接続
- Cisco Secure Accessに接続されているその他のネットワークロケーション

このアプローチにより、組織はあらゆるタイプのプライベートアプリケーショントラフィックを統合された暗号化チャネル経由で安全にルーティングでき、セキュリティと運用効率の両方を強化できます。
Cisco Secure Accessは、Cisco Security Service Edge(SSE)ソリューションの一部として、単一のクラウド管理コンソール、統合クライアント、一元化されたポリシー作成、および集約されたレポートにより、IT運用を簡素化します。ZTNA、Secure Web Gateway(SWG)、Cloud Access Security Broker(CASB)、Firewall as a Service(FWaaS)、DNSセキュリティ、Remote Browser Isolation(RBI)など、複数のセキュリティモジュールが1つのクラウド提供ソリューションに組み込まれています。この包括的なアプローチは、ゼロトラスト原則を適用し、きめ細かなセキュリティポリシーを適用することで、セキュリティリスクを軽減します

図2:Cisco Secure Accessとプライベートアプリケーション間のトラフィックフロー



SSEプライベートアプリケーショントラフィックフロー

このガイドで説明するソリューションは、データセンターのSD-WANルータとセキュリティサービスエッジ(SSE)側のネットワークトンネルグループ(NTG)の両方を含む、冗長性に関する包括的な考慮事項に対応しています。このガイドでは、アクティブ/アクティブ SD-WANハブの導入モ

デルに焦点を合わせています。このモデルは、中断のないトラフィックフローを維持し、高可用性を確保するのに役立ちます。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco SD-WANの設定と管理
- IKEv2およびIPSecプロトコルの基礎知識
- Cisco Secure Accessポータルでのネットワークトンネルグループの設定
- BGPとECMPに関する知識

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- 20.9.5a上のCisco SD-WANコントローラ
- 17.9.5a上のCisco SD-WAN Wanエッジルータ
- Cisco Secure Accessポータル

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設計

このガイドでは、SD-WANヘッドエンドルータのアクティブ/アクティブ設計モデルを使用したソリューションについて説明します。SD-WANヘッドエンドルータに関するアクティブ/アクティブ設計モデルでは、図3に示すように、データセンター内の2台のルータがどちらもセキュリティサービスエッジ(SSE)ネットワークトンネルグループ(NTG)に接続されていると想定しています。このシナリオでは、データセンター内の両方のSD-WANルータ（DC1-HE1とDC1-HE2）がアクティブにトラフィックフローを処理します。これを実現するには、内部DCネイバーに同じASパス長(ASPL)を送信します。その結果、DC内からのトラフィックは2つのヘッドエンド間でロードバランシングを行います。

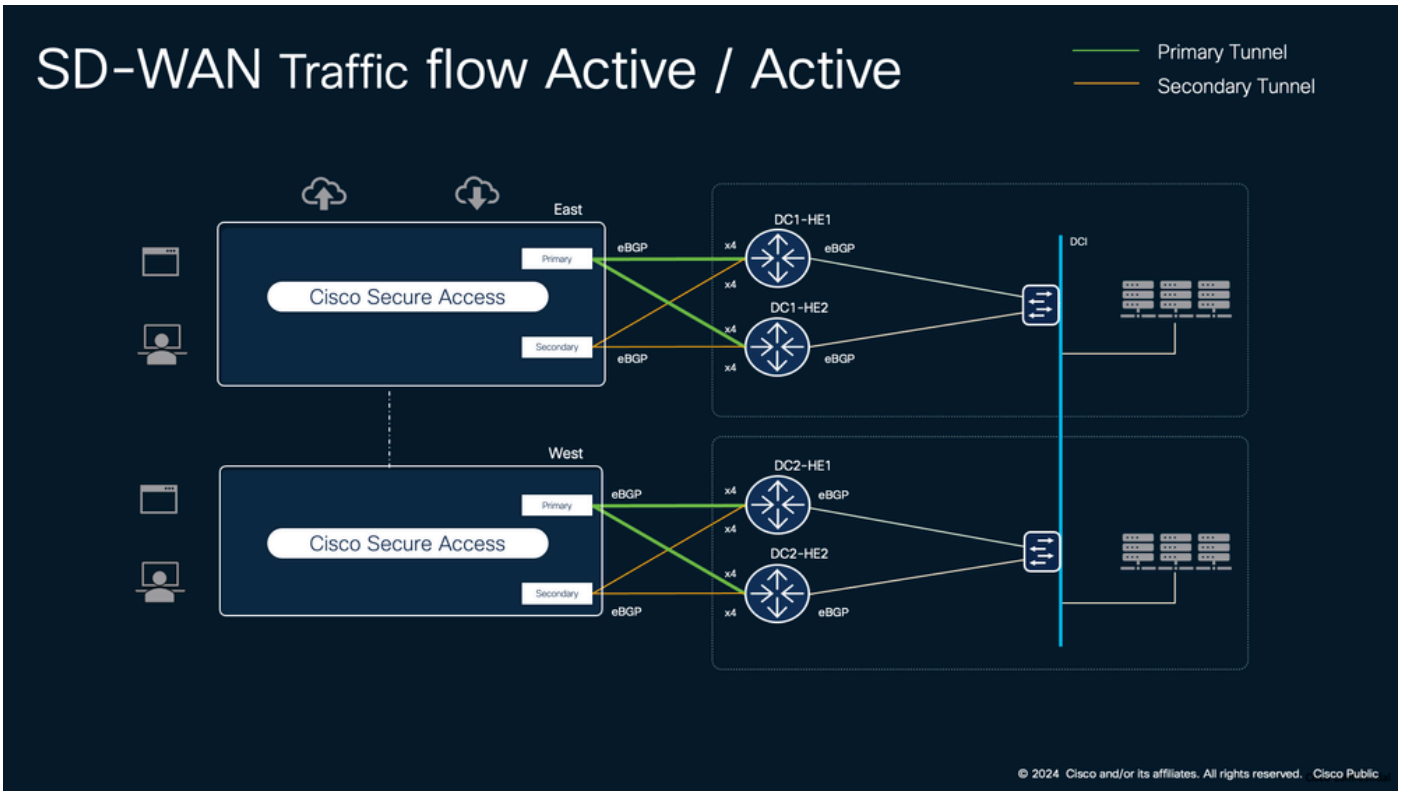
各ヘッドエンドルータは、SSEアクセスポイント(POP)への複数のトンネルを確立できます。 トンネルの数は、要件とSD-WANデバイスモデルによって異なります。この設計では、次のことを行います。

- 各ルータには、プライマリSSEハブへのトンネルが4つと、セカンダリSSEハブへのトンネルが4つあります。
- 各SSEハブでサポートされるトンネルの最大数は異なる場合があります。最新の情報につい

ては、次の公式ドキュメントを参照してください。https://docs.sse.cisco.com/sse-user-guide/docs/secure-access-network-tunnels

これらのヘッドエンドルータは、SSEに向かうトンネル上でBGPネイバーシップを形成します。これらのネイバーシップを通じて、ヘッドエンドはプライベートアプリケーションプレフィックスをSSEネイバーにアドバタイズし、プライベートリソースへのトラフィックの安全で効率的なルーティングを可能にします。

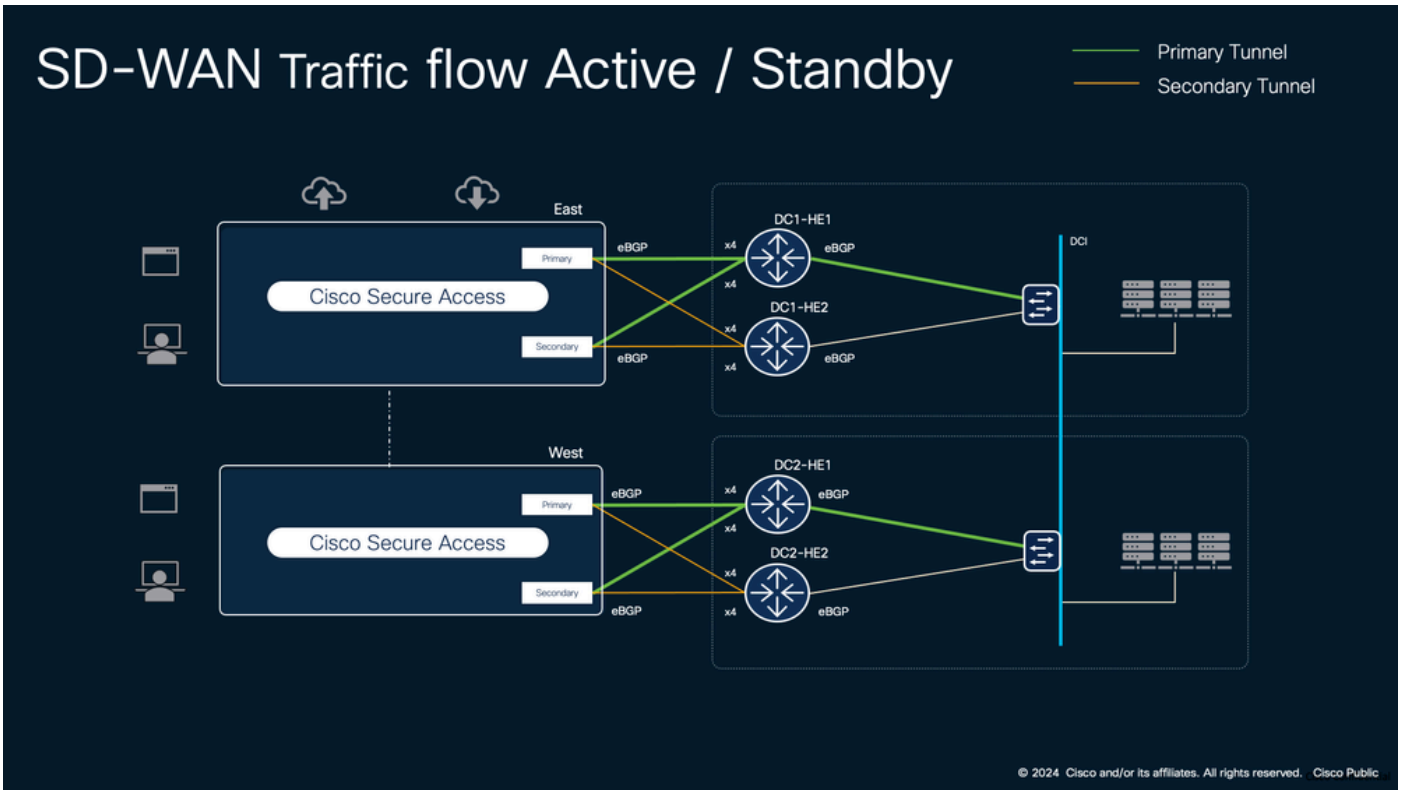
図3:SD-WANからSSEへのアクティブ/アクティブ導入モデル



SD-WANからSSEへのアクティブ/アクティブ導入モデル

アクティブ/スタンバイ設計では、1台のルータ(DC1-HE1)を常にアクティブとして指定し、セカンダリルータ(DC1-HE2)はスタンバイ状態を維持します。トラフィックは、完全に障害が発生しない限り、常にアクティブなヘッドエンド(DC1-HE1)を通過します。この導入モデルには欠点があります。SSEへのプライマリトンネルがダウンした場合、トラフィックはDC1-HE2のみを経由するセカンダリSSEトンネルに切り替わり、ステートフルトラフィックがリセットされます。
アクティブ/スタンバイモデルでは、BGP AS-Path Lengthを使用して、DC内とSSEへのトラフィックの舵取りが行われます。DC1-HE1はASPL 2でSSE BGPネイバーにプレフィクスアップデートを送信し、DC1-HE2はASPL 3でアップデートを送信します。DC1-HE1の内部DCネイバーが、DC1-HE2よりも短いASパス長のプレフィックスをアドバタイズするため、DC1-HE1のトラフィックの優先順位が保証されます（ユーザは他の属性やプロトコルを選択してトラフィックの優先順位に影響を与えることができます）。
お客様は、固有の要件に基づいて、アクティブ/アクティブまたはアクティブ/スタンバイのいずれかの導入モデルを選択できます。

図4:SD-WANからSSEへのアクティブ/スタンバイ導入モデル



SD-WANからSSEへのアクティブ/スタンバイ導入モデル

設定

このセクションでは、この手順について説明します。

1. Cisco Secure Accessポータルでネットワークトンネルグループをプロビジョニングするための前提条件を確認します。
2. IPSec手動方式を使用して、SD-WAN相互接続をCisco Secure Access Network Tunnel Group(NTG)で設定します。
3. BGPネイバーシップの設定

注：この設定は、アクティブ/アクティブ展開モデルに基づいています

手順 1.Cisco Secure Access Portalでのネットワークトンネルグループ設定の確認

ネットワークトンネルグループの設定方法については、このガイドでは説明していません。このリファレンスを確認してください。

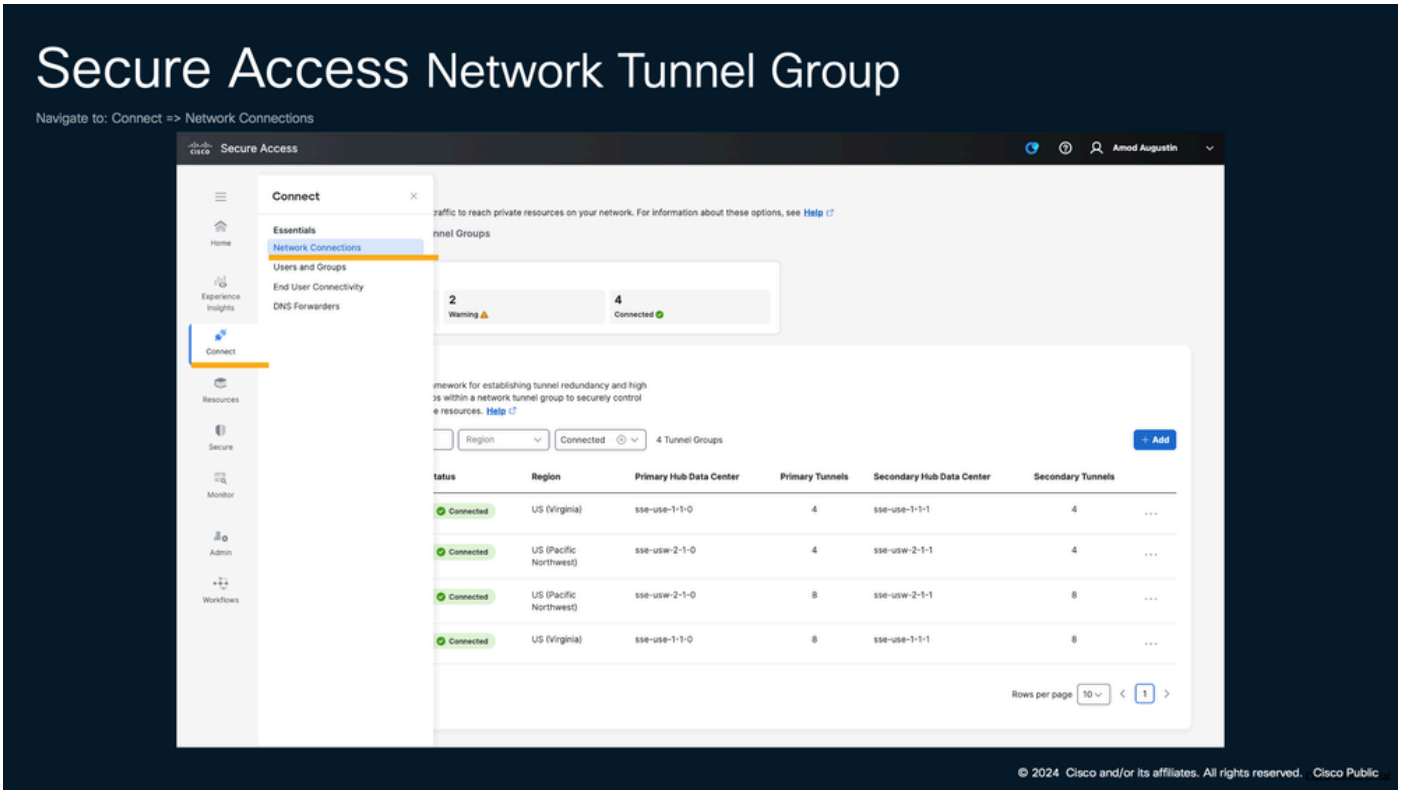
- ネットワークトンネルグループの追加：SSEのドキュメント
- BGPでECMPを使用したCisco Secure AccessとCisco IOS XEルータ間のネットワークトンネルの設定

Cisco Secure Accessに移動し、ネットワークトンネルグループ(NTG)がプロビジョニングされていることを確認します。現在の設計では、2つの異なるPoint of Presence(POP)でNTGをプロビジョニングする必要があります。 このガイドでは、US（バージニア）POPおよびUS（太平洋北西

部）POPでNTGを使用します。

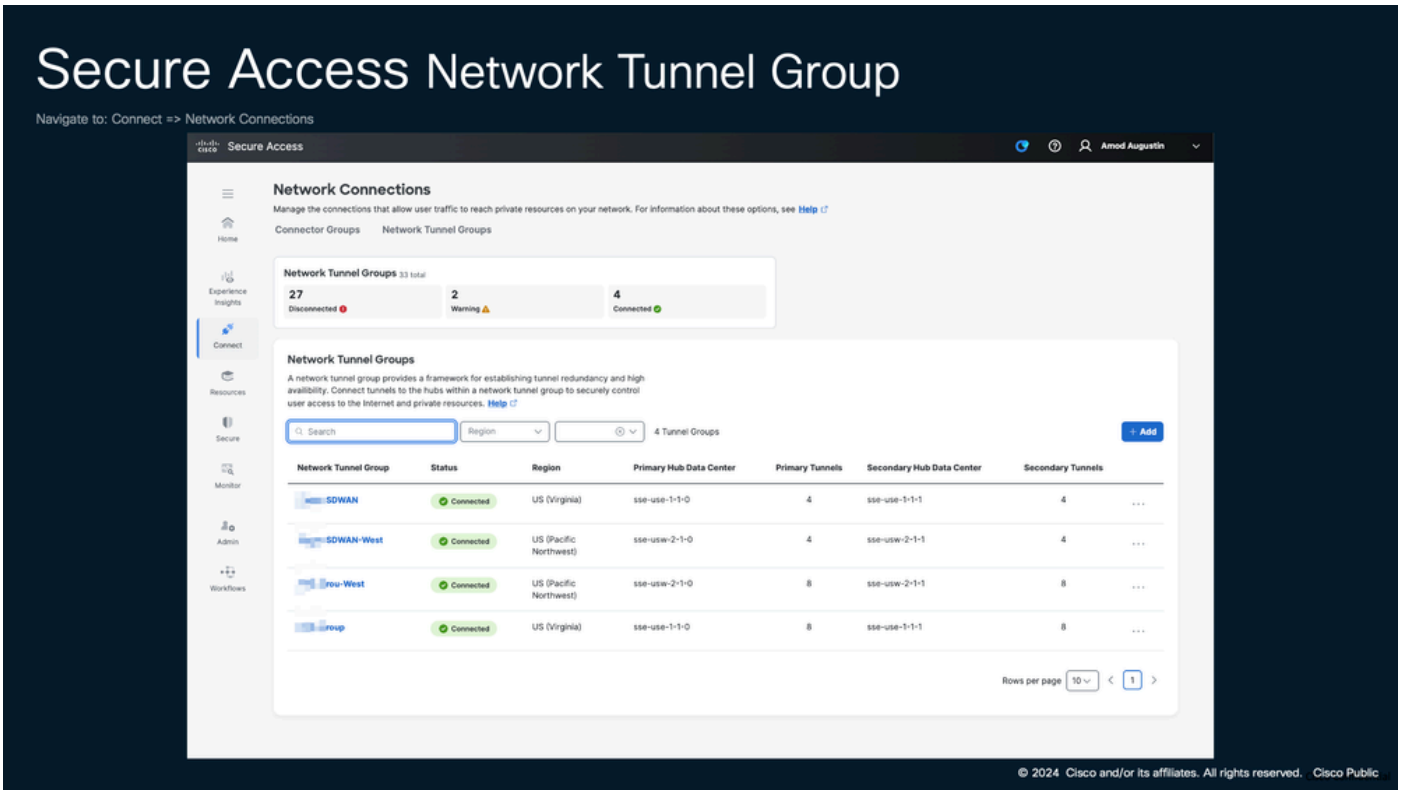
注:POPの名前と場所は異なる場合がありますが、重要な概念は、データセンターに地理的に近い場所で複数のNTGをプロビジョニングすることです。このアプローチは、ネットワークパフォーマンスの最適化に役立ち、冗長性を提供します。

図5:Cisco Secure Access Networkトンネルグループ



Cisco Secure Access Networkトンネルグループ

図6:Cisco Secure Access Networkトンネルグループリスト



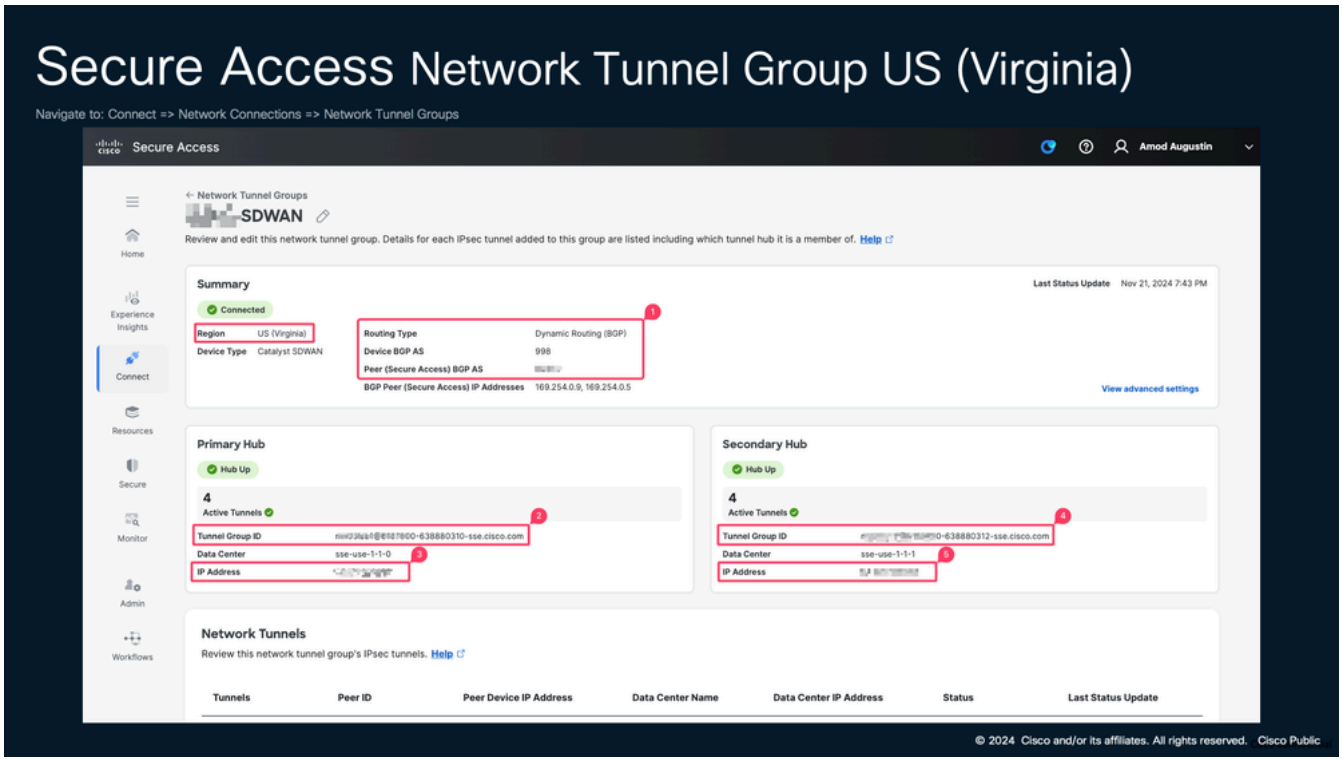
セキュアアクセスネットワークのトンネルグループリスト

トンネルパスフレーズ（トンネルの作成中に1回だけ表示される）をメモしていることを確認します。

注:「ネットワークトンネルグループの追加」のステップ6

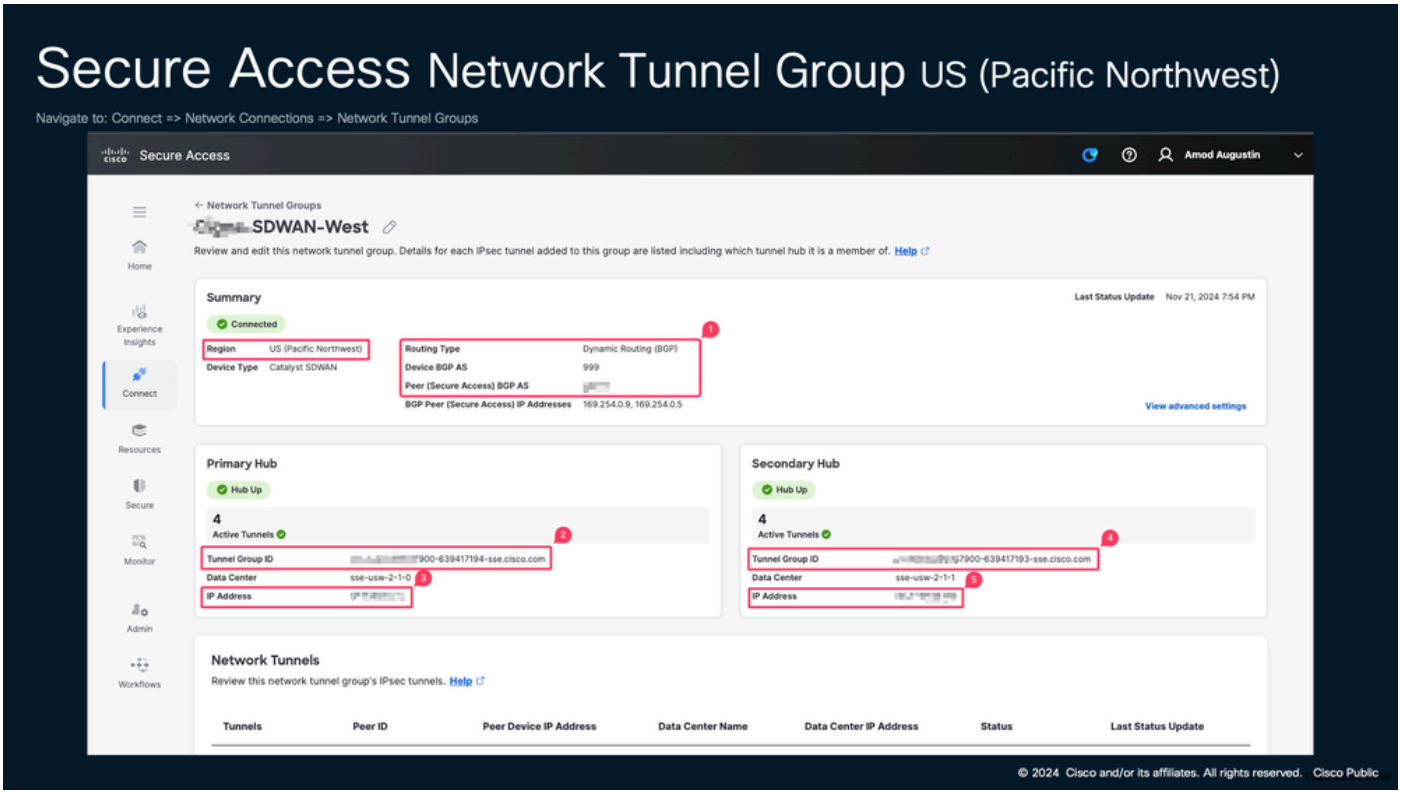
また、IPSecの設定時に使用するトンネルグループ属性をメモしておきます。スクリーンショット（図6）は、設計または使用の推奨事項に従って実稼働シナリオでNTGグループを作成するラボ環境から取得したものです。

図7：セキュアアクセスネットワークトンネルグループUS（バージニア）



Secure Access Network Tunnel Group US（バージニア州）

図8:Secure Access Network Tunnel Group US(Pacific Northwest)



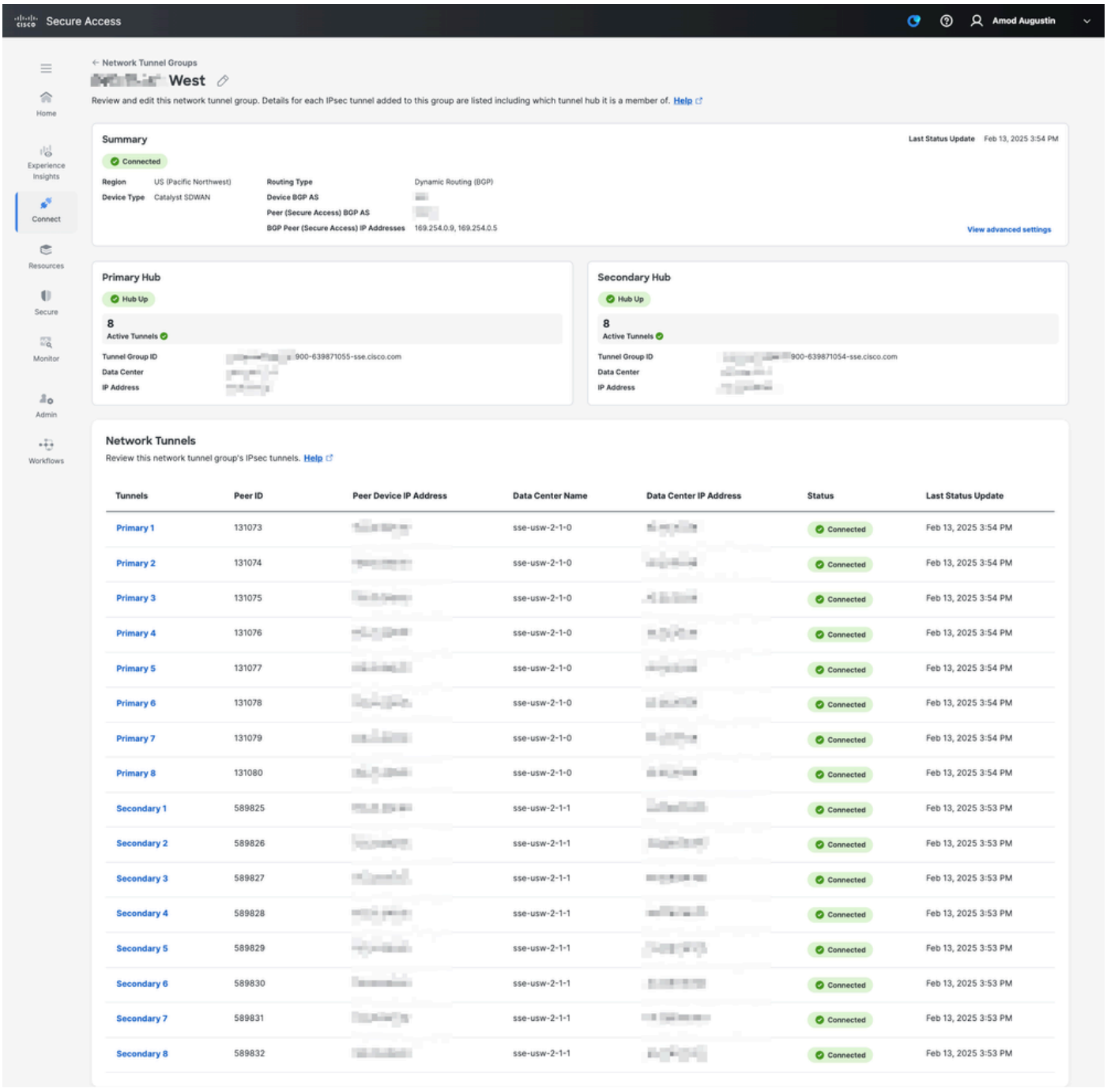
Secure Access Network Tunnel Group US（米国太平洋北西部）

図8は、プライマリハブとセカンダリハブの両方で4つのトンネルだけを示しています。ただし、コントローラ環境では最大8つのトンネルが正常にテストされています。最大トンネルサポートは、使用しているハードウェアデバイスと現在のSSEトンネルサポートによって異なります。最新情報については、公式ドキュメント(https://docs.sse.cisco.com/sse-user-guide/docs/secure-

access-network-tunnels)およびそれぞれのハードウェアデバイスのリリースノートを参照してください。

8トンネルセットアップの例を次に示します。

図8a：最大8つのNTGトンネル



SSE NTG最大8トンネル

手順 2.IPSecの手動方式を使用して、Cisco Secure Access Network Tunnel Group(NTG)とのSD-WAN相互接続を設定します。

この手順では、Cisco Catalyst SD-WAN Manager 20.9および17.9リリースを実行するCisco Catalystエッジルータで機能テンプレートを使用して、Network Tunnel Group（NTG；ネットワ

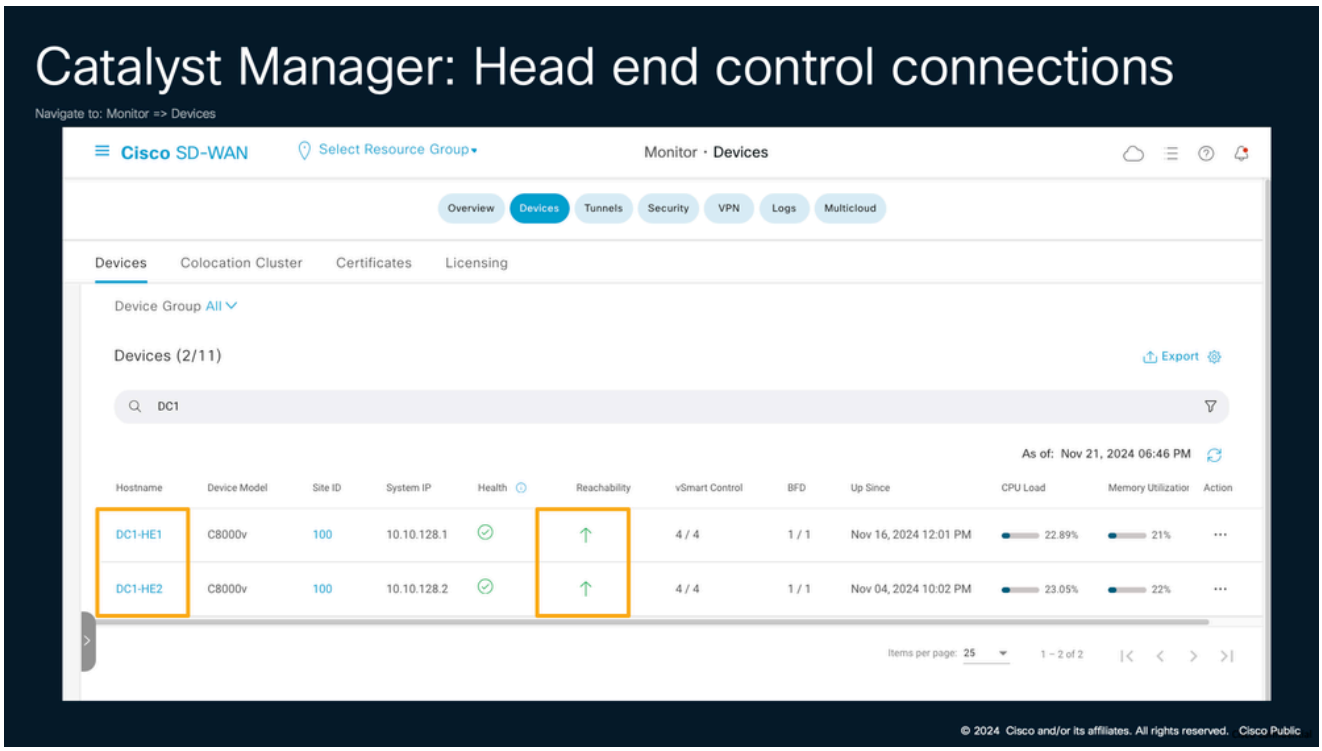
ークトンネルグループ）を接続する方法を示します。

> 注：このガイドでは、ハブアンドスポークまたはフルメッシュ型トポロジのいずれかでSD-WANオーバーレイが既に展開されていることを前提としています。ハブは、データセンターでホストされるプライベートアプリケーションのアクセスエントリポイントとして機能します。この手順は、ブランチまたはクラウドの導入にも適用できます。

次に進む前に、前提条件が満たされていることを確認します。

1. デバイス上でコントロール接続が有効になっており、Cisco Catalyst SD-WAN Managerからの必要な更新が可能です。

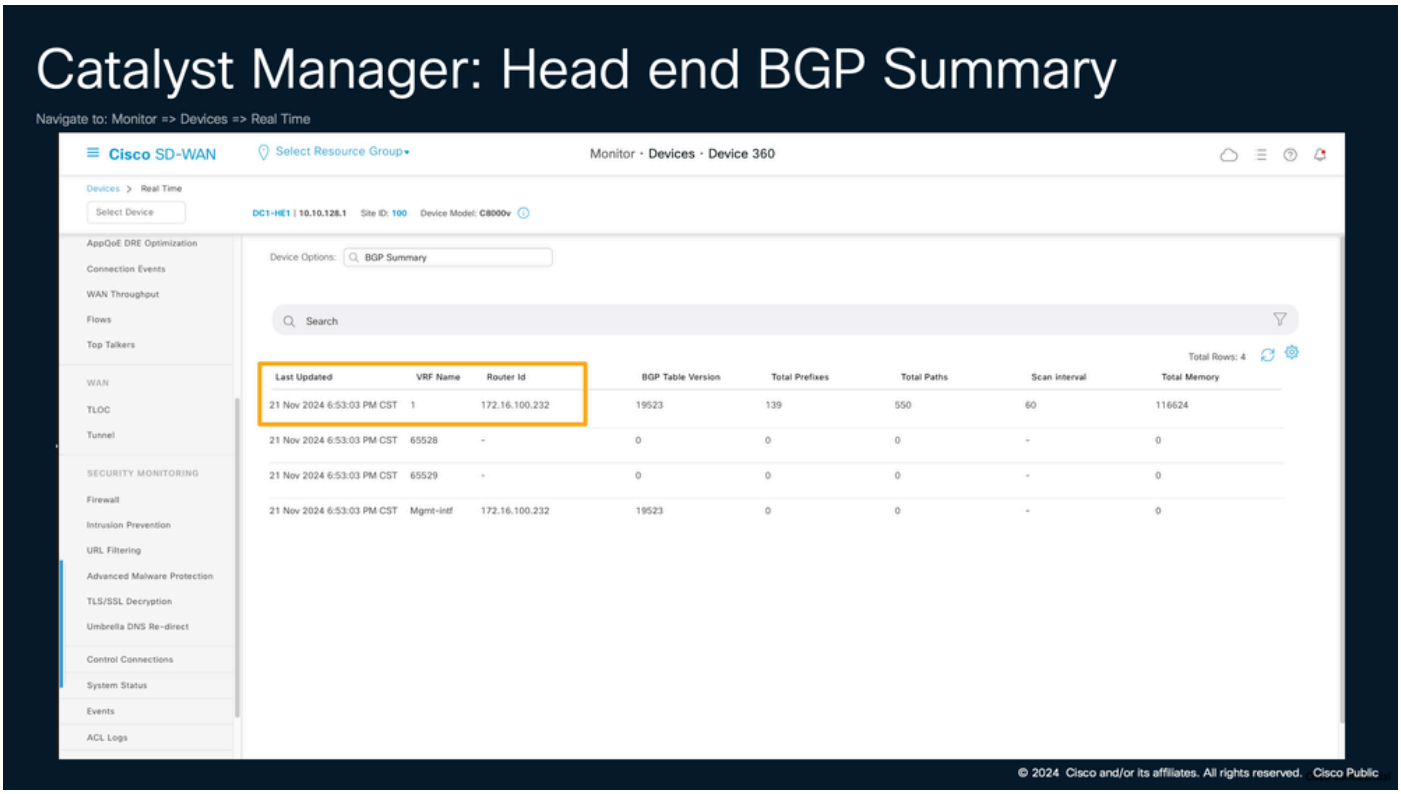
   図9: Cisco Catalyst SD-WAN Manager：ヘッドエンドコントロール接続



   Catalystマネージャ：ヘッドエンドコントロール接続

2. サービス側のVPNが設定され、プレフィクスをアドバタイズするためにルーティングプロトコルを使用します。このガイドでは、サービス側のルーティングプロトコルとしてBGPを使用します。

図10:Cisco Catalyst SD-WAN Manager：ヘッドエンドBGPの概要



手動IPSec方式を使用してネットワークトンネルグループ(NTG)でSD-WAN相互接続を設定するには、次の手順を実行します。

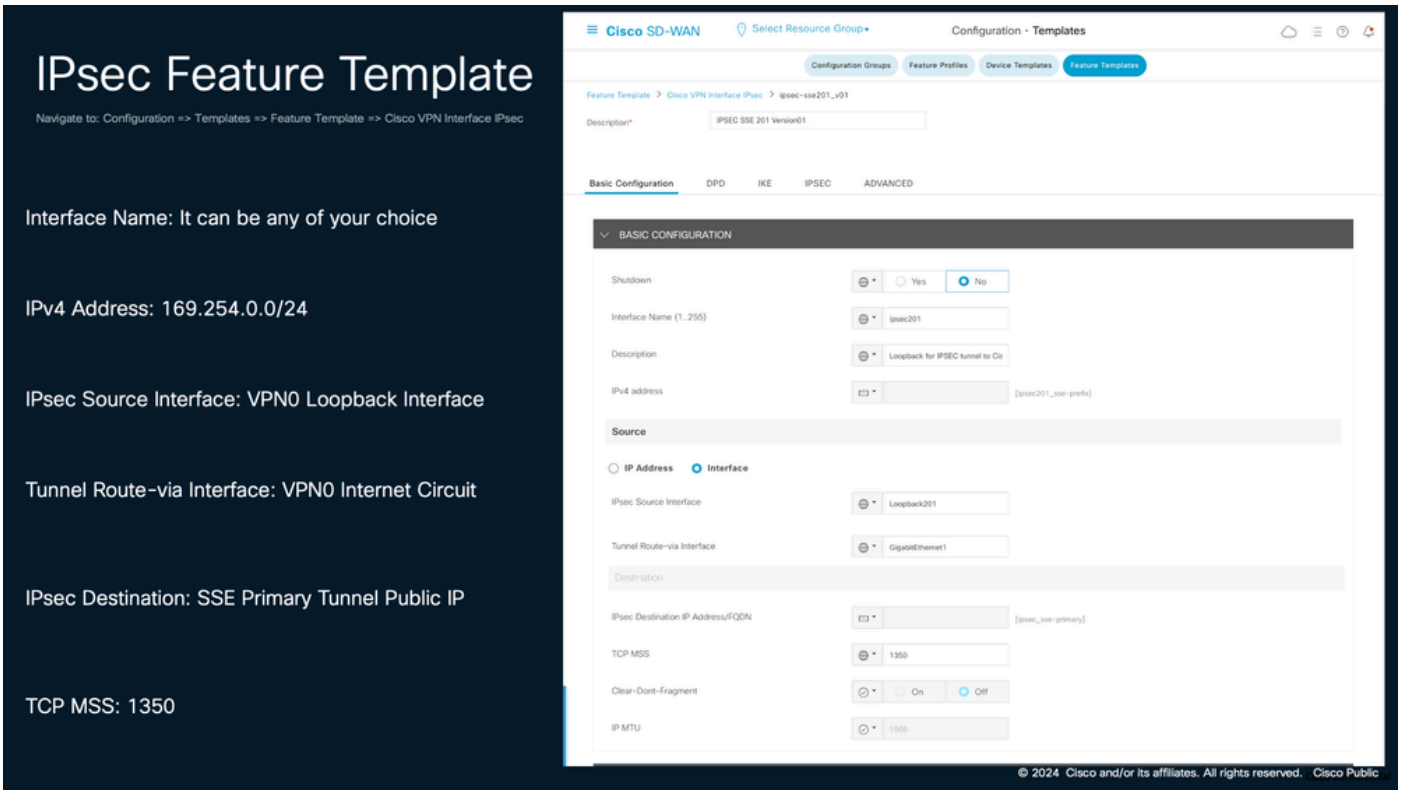
注:導入に必要な数のトンネルについて、この手順を繰り返します。

トンネルの制限については、次のURLにある公式のドキュメントを参照してください。
https://docs.sse.cisco.com/sse-user-guide/docs/secure-access-network-tunnels

これらの手順では、DC1-HE1(Data Center 1 Head-End 1)をSSE Virginia Primary Hubに接続するプロセスを詳しく説明します。この設定では、データセンターのSD-WANルータとバージニア州のアクセスポイント(POP)にあるCisco Secure Access Network Tunnel Group(NTG)の間にセキュアトンネルを確立します

ステップ1:IPSec機能テンプレートの作成
SD-WANヘッドエンドルータをNTGに接続するIPSecトンネルのパラメータを定義するためのIPSec機能テンプレートを作成します。

図11:IPsec機能テンプレート：基本設定



IPSec機能テンプレート：基本設定

インターフェイス名：任意の名前を選択できます
IPv4アドレス：SSEは、サブネットを任意のサブネットに分割するという要件に基づいて169.254.0.0/24をリッスンします。ベストプラクティスとして、/30を使用してください。このガイドでは、今後の使用のために最初のブロックを省略しています。

IPSec送信元インターフェイス：現在のIPSecインターフェイスに対して一意のVPN0ループバックインターフェイスを定義します。一貫性とトラブルシューティングのために、同じ番号を維持することをお勧めします。
トンネルRoute-viaインターフェイス：SSEに到達するためのアンダーレイとして使用できるインターフェイスを指定します（インターネットにアクセスできる必要があります）。

IPsec宛先：プライマリハブIPアドレス

図7:Secure Access Network TunnelグループUS（バージニア州）を参照してください。これは35.171.214.188です

TCP MSS:1350(参照：https://docs.sse.cisco.com/sse-user-guide/docs/supported-ipsec-parameters)

例：DC1-HE1からSSE Virginia Primary Hubへ

インターフェイス名：ipsec201

説明：シスコへのIPSECトンネルのループバック

IPv4アドレス：169.254.0.x/30

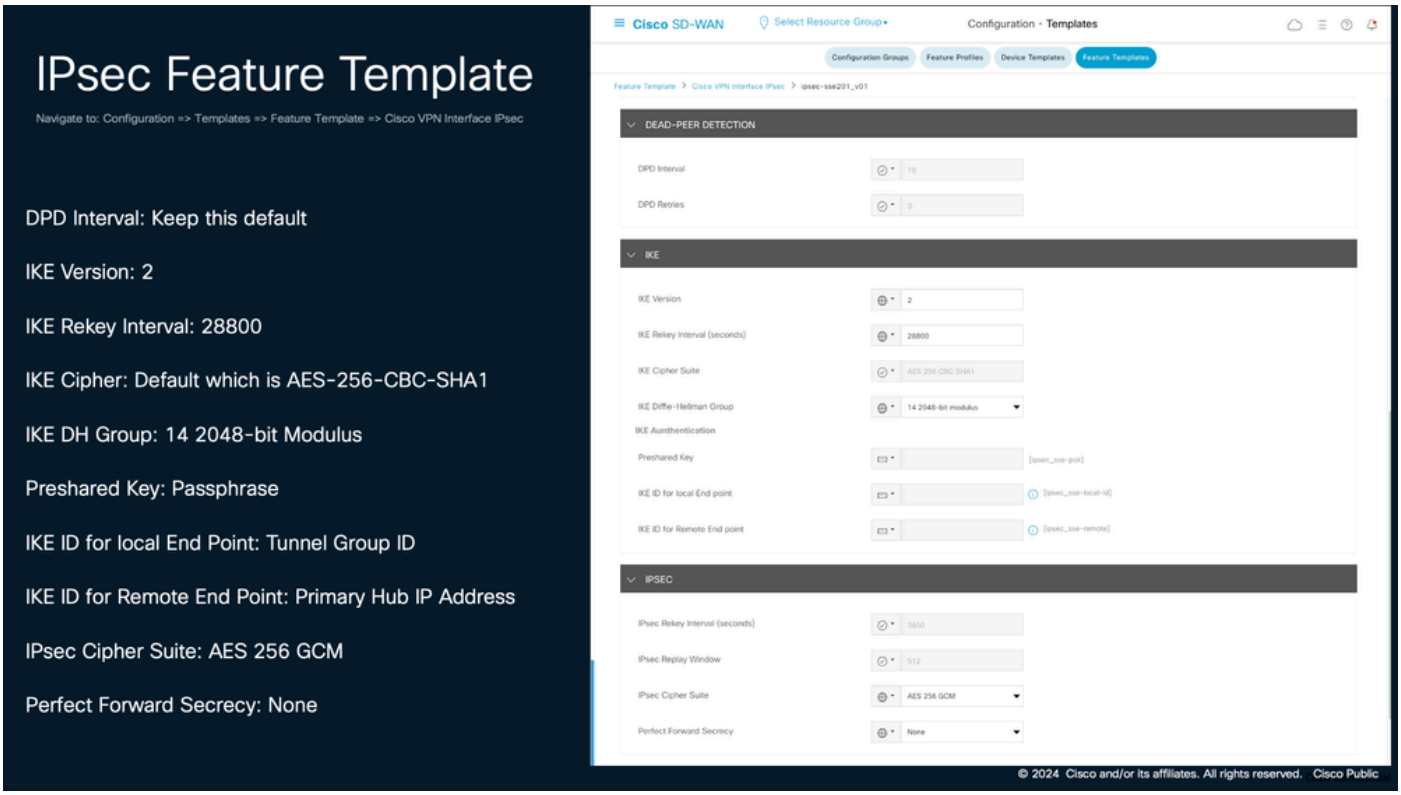
IPsec送信元インターフェイス：Loopback201

トンネルのRoute-viaインターフェイス：GigabitEthernet1

IPsec宛先IPアドレス/FQDN: 35.xxx.xxx.xxx

TCP MSS:1350

図12:IPsec機能テンプレート：IKE IPSEC



IPsec機能テンプレート：IKE IPSEC

DPD間隔：このデフォルトを保持
IKEバージョン：2
IKEキー再生成間隔：28800
IKE Cipher：デフォルトはAES-256-CBC-SHA1
IKE DHグループ：14 2048ビットモジュラス
事前共有キー：パスフレーズ
ローカルエンドポイントのIKE ID：トンネルグループID

図7:Secure Access Network Tunnel Group US（バージニア州）を参照してください。これは mn03lab1+201@8167900-638880310-sse.cisco.comです。

注:このためには、各トンネルに一意のエンドポイントが必要です。「+loopbackID」を使用してください。例：mn03lab1+202@8167900-638880310-sse.cisco.com、mn03lab1+203@8167900-638880310-sse.cisco.comなど。

リモートエンドポイントのIKE ID：プライマリハブIPアドレス
IPsec暗号スイート：AES 256 GCM

完全転送秘密：なし

参考：https://docs.sse.cisco.com/sse-user-guide/docs/configure-tunnels-with-catalyst-sdwan#define-the-feature-template

例：

IKEバージョン：2
IKEキー再生成間隔：28800
IKE暗号：AES-256-CBC-SHA1
IKE DHグループ：14 2048ビットモジュラス
事前共有キー：*****

注:「ネットワークトンネルグループの追加」のステップ6

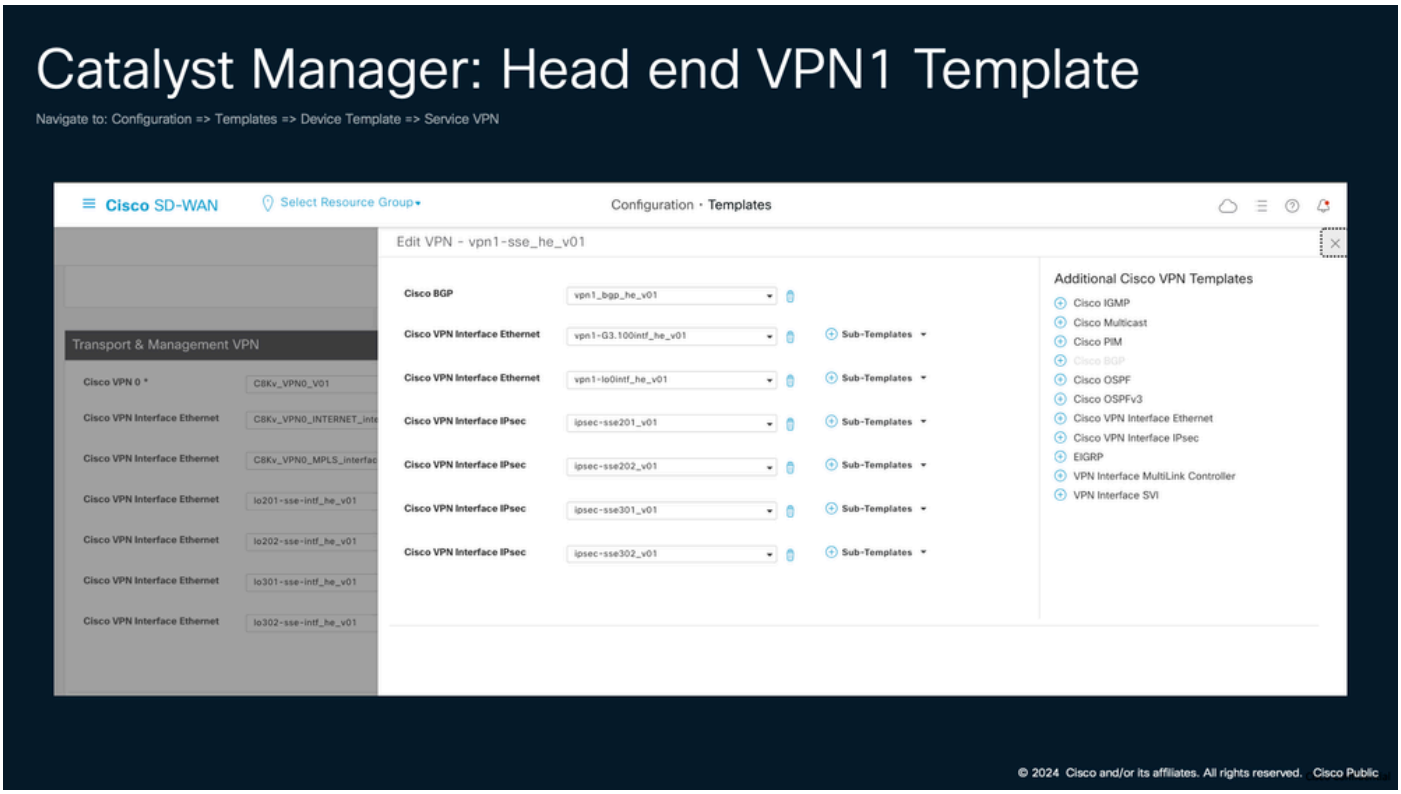
ローカルエンドポイントのIKE ID:mn03lab1@8167900-638880310-sse.cisco.com
リモートエンドポイントのIKE ID:35.171.xxx.xxx
IPsec暗号スイート：AES 256 GCM
完全転送秘密：なし

手順を繰り返して、プライマリとセカンダリの両方のセキュアアクセスハブに必要なトンネルを設定します。2x2の設定では、合計4つのトンネルを作成します。

- DC1-HE1からプライマリセキュアアクセスハブへの2つのトンネル
- DC1-HE1からセカンダリSecure Accessハブへの2つのトンネル

これでテンプレートが作成され、図13に示すサービス側のvrfでテンプレートが使用され、図14に示すグローバルvrfに定義されたループバックが使用されます。

図13:Catalyst SD-WAN Manager：ヘッドエンドVPN1テンプレート2x2



Catalyst Manager：ヘッドエンドVPN1テンプレート

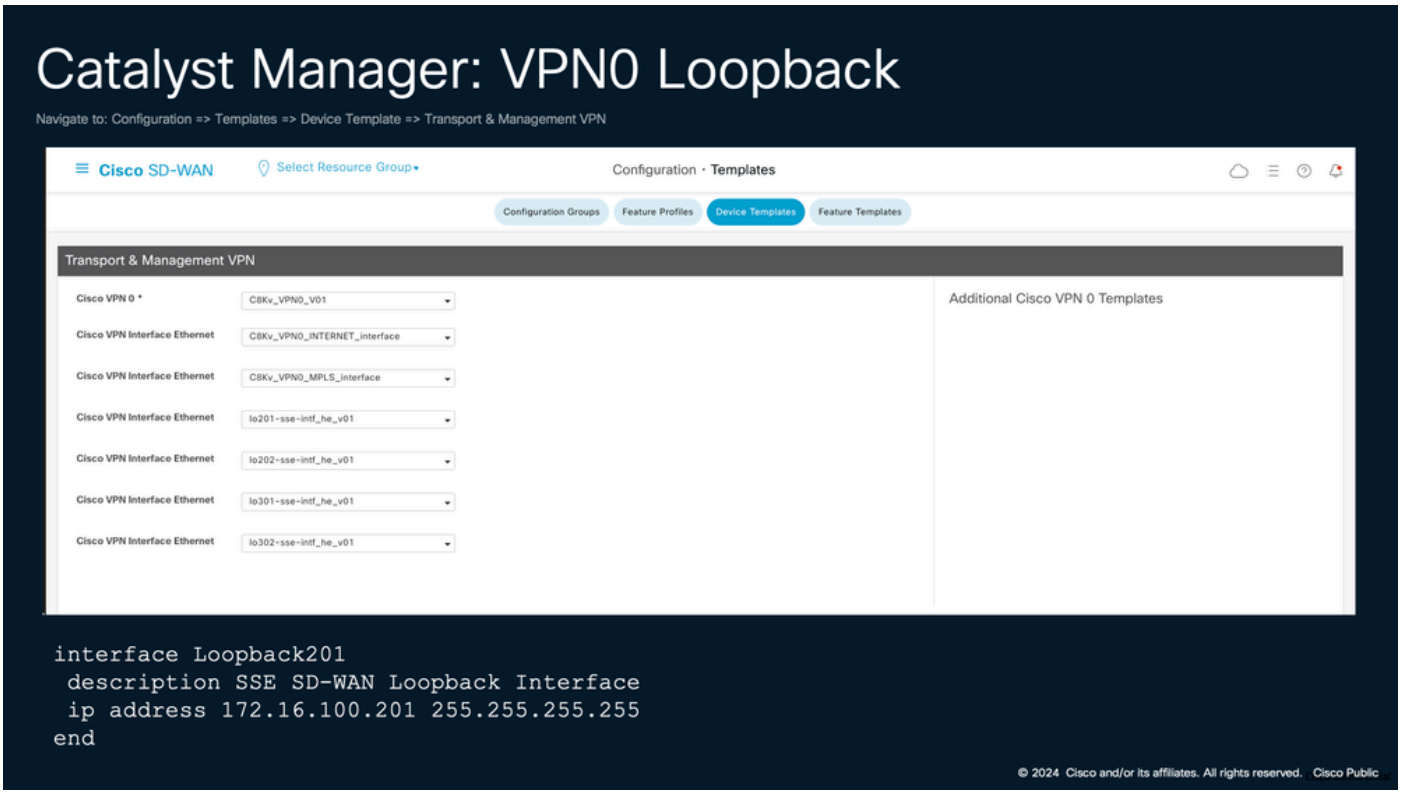
ステップ2：グローバルVRFでループバックを定義する

グローバルVRF(Virtual Routing and Forwarding)テーブルでループバックインターフェイスを設定します。このループバックは、ステップ1で作成したIPSecトンネルの送信元インターフェイスとして機能します。

ステップ1で参照されるすべてのループバックは、グローバルVRFで定義する必要があります。

IPアドレスは、任意のRFC1918範囲で定義できます。

図14:Catalyst SD-WAN Manager:VPN0ループバック

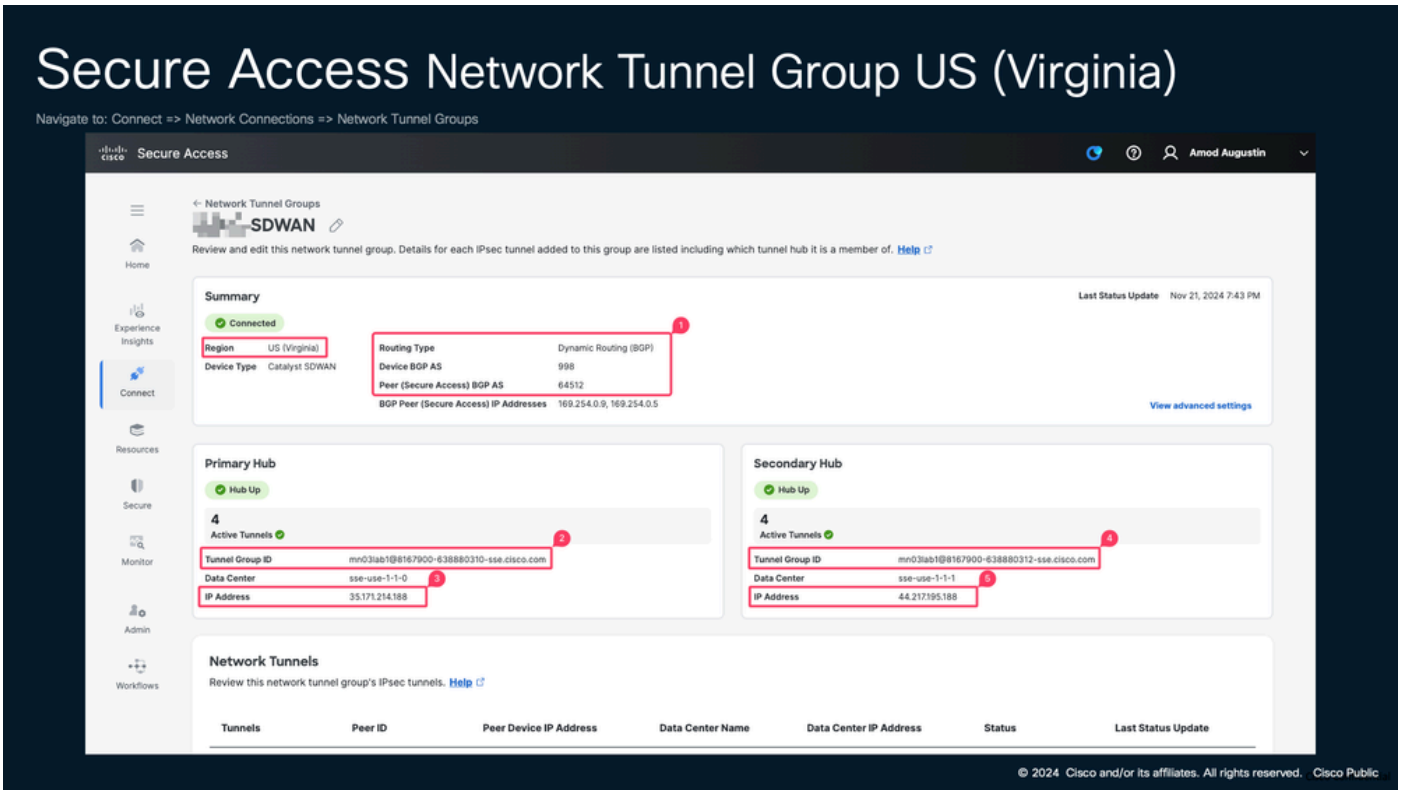


Catalyst Manager:VPN0ループバック

手順 3.BGPネイバーシップの設定

BGP機能テンプレートを使用して、すべてのトンネルインターフェイスのBGPネイバーシップを定義します。BGP値を設定するには、Cisco Secure Access Portalのそれぞれのネットワークトンネルグループ BGP設定を参照してください。

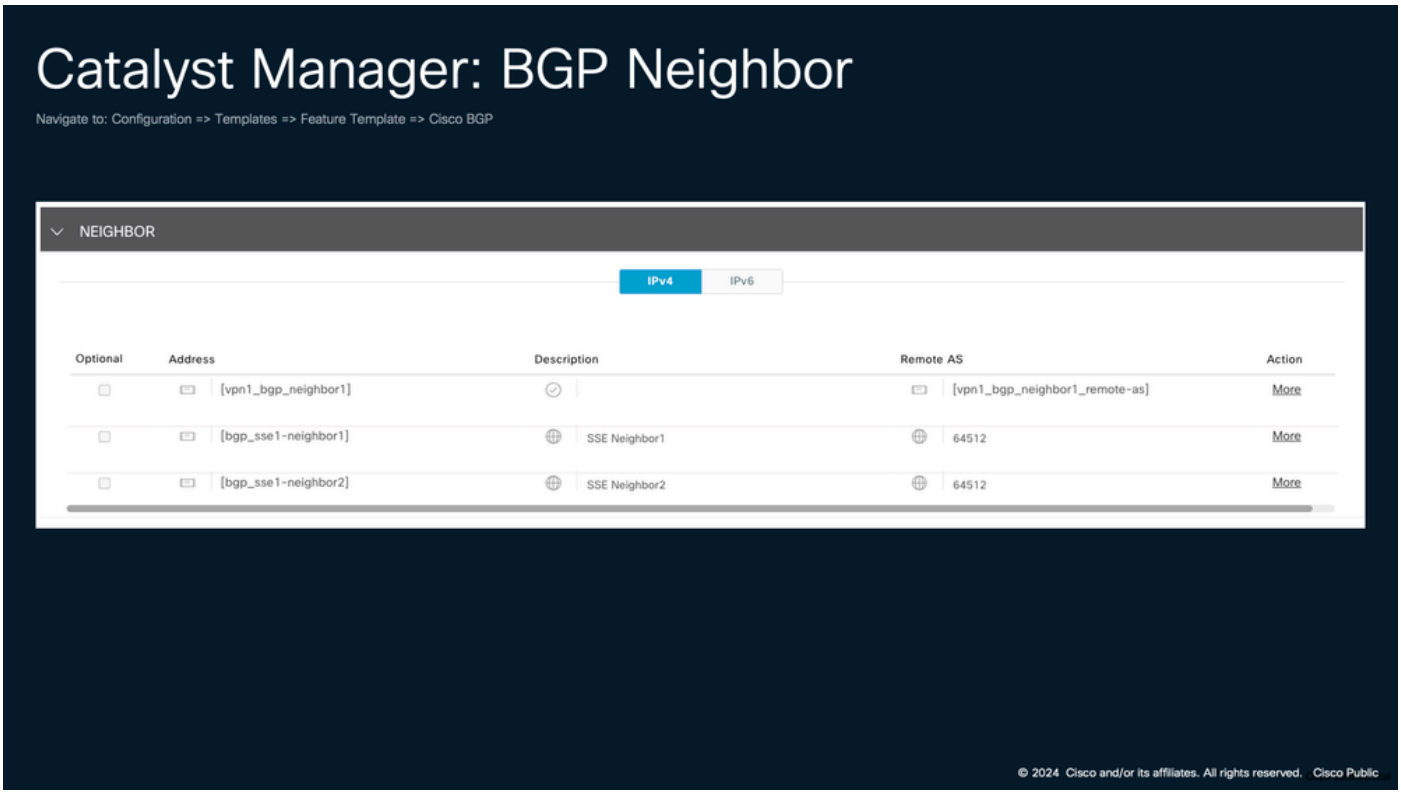
図15：セキュアアクセスネットワークトンネルグループUS（バージニア州）



Secure Access Network Tunnel Group US（バージニア州）

この例では、図15（ボックス1）の情報を使用して、機能テンプレートを使用してBGPを定義します。

図16:Catalyst SD-WAN Manager BGPネイバー



Catalyst SD-WAN Manager BGPネイバー

機能テンプレートを使用して生成された設定：

```
router bgp 998
 bgp log-neighbor-changes
 !
 address-family ipv4 vrf 1
  network 10.10.128.1 mask 255.255.255.255
  neighbor 169.254.0.5 remote-as 64512
  neighbor 169.254.0.5 description SSE Neighbor1
  neighbor 169.254.0.5 ebgp-multihop 5
  neighbor 169.254.0.5 activate
  neighbor 169.254.0.5 send-community both
  neighbor 169.254.0.5 next-hop-self
  neighbor 169.254.0.9 remote-as 64512
  neighbor 169.254.0.9 description SSE Neighbor2
  neighbor 169.254.0.9 ebgp-multihop 5
  neighbor 169.254.0.9 activate
  neighbor 169.254.0.9 send-community both
  neighbor 169.254.0.9 next-hop-self
  neighbor 169.254.0.105 remote-as 64512
  neighbor 169.254.0.105 description SSE Neighbor3
  neighbor 169.254.0.105 ebgp-multihop 5
  neighbor 169.254.0.105 activate
  neighbor 169.254.0.105 send-community both
  neighbor 169.254.0.105 next-hop-self
  neighbor 169.254.0.109 remote-as 64512
  neighbor 169.254.0.109 description SSE Neighbor4
  neighbor 169.254.0.109 ebgp-multihop 5
  neighbor 169.254.0.109 activate
  neighbor 169.254.0.109 send-community both
  neighbor 169.254.0.109 next-hop-self
  neighbor 172.16.128.2 remote-as 65510
  neighbor 172.16.128.2 activate
  neighbor 172.16.128.2 send-community both
  neighbor 172.16.128.2 route-map sse-routes-in in
  neighbor 172.16.128.2 route-map sse-routes-out out
  maximum-paths eibgp 4
  distance bgp 20 200 20
 exit-address-family
DC1-HE1#
```

検証

```
DC1-HE1#show ip route vrf 1 bgp | begin Gateway
Gateway of last resort is not set

35.0.0.0/32 is subnetted, 1 subnets
B 35.95.175.78 [20/0] via 169.254.0.9, 3d01h
[20/0] via 169.254.0.5, 3d01h
44.0.0.0/32 is subnetted, 1 subnets
B 44.240.251.165 [20/0] via 169.254.0.9, 3d01h
[20/0] via 169.254.0.5, 3d01h
100.0.0.0/8 is variably subnetted, 17 subnets, 2 masks
B 100.81.0.58/32 [20/0] via 169.254.0.9, 3d01h
```

```
[20/0] via 169.254.0.5, 3d01h
B 100.81.0.59/32 [20/0] via 169.254.0.9, 3d01h
[20/0] via 169.254.0.5, 3d01h
B 100.81.0.60/32 [20/0] via 169.254.0.9, 3d01h
[20/0] via 169.254.0.5, 3d01h
B 100.81.0.61/32 [20/0] via 169.254.0.9, 3d01h
[20/0] via 169.254.0.5, 3d01h
B 100.81.0.62/32 [20/0] via 169.254.0.9, 3d01h
[20/0] via 169.254.0.5, 3d01h
B 100.81.0.63/32 [20/0] via 169.254.0.9, 3d01h
[20/0] via 169.254.0.5, 3d01h
B 100.81.0.64/32 [20/0] via 169.254.0.9, 3d01h
[20/0] via 169.254.0.5, 3d01h
B 100.81.0.65/32 [20/0] via 169.254.0.9, 3d01h
[20/0] via 169.254.0.5, 3d01h

DC1-HE1#show ip bgp vpnv4 all summary
BGP router identifier 172.16.100.232, local AS number 998

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
169.254.0.5 4 64512 12787 13939 3891 0 0 4d10h 18
169.254.0.9 4 64512 66124 64564 3891 0 0 3d01h 18
169.254.0.13 4 64512 12786 13933 3891 0 0 4d10h 18
169.254.0.17 4 64512 12786 13927 3891 0 0 4d10h 18
172.16.128.2 4 65510 83956 84247 3891 0 0 7w3d 1

DC1-HE1#show ip interface brief | include Tunnnel
Tunnel1 192.168.128.202 YES TFTP up up
Tunnel4 198.18.128.11 YES TFTP up up
Tunnel100022 172.16.100.22 YES TFTP up up
Tunnel100023 172.16.100.23 YES TFTP up up
Tunnel100201 169.254.0.6 YES other up up
Tunnel100202 169.254.0.10 YES other up up
Tunnel100301 169.254.0.14 YES other up up
Tunnel100302 169.254.0.18 YES other up up
```

参考

アクティブ/アクティブ実装では、両方のSD-WANヘッドエンドに接続されているコアスイッチからのマルチパスが存在します。

図17:BGPネイバーのアクティブ/アクティブシナリオ

```
DC1-Core-Switch#show ip bgp
BGP table version is 62893, local router ID is 172.16.128.6
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
              t secondary path,

     Network          Next Hop            Metric LocPrf Weight Path
 *m   1.1.1.1/32       172.16.128.5           65535             0 998 ?
 *>                    172.16.128.1           65535             0 998 ?
 *m   3.[redacted]/32  172.16.128.5           65535             0 998 ?
 *>                    172.16.128.1           65535             0 998 ?
 *m   3.[redacted]/32  172.16.128.5           65535             0 998 ?
 *>                    172.16.128.1           65535             0 998 ?
<snip>
```

アクティブ/アクティブBGPネイバー

Active/Stanby実装では、ASPLプリペンド（ネイバーへのルートマップを使用して実行）により、コアスイッチからSD-WANヘッドエンドへのパスが1つアクティブになります。

図18:BGPネイバーのアクティブ/スタンバイシナリオ

```
DC1-Core-Switch#show ip bgp
BGP table version is 62893, local router ID is 172.16.128.6
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
              t secondary path,

     Network          Next Hop            Metric LocPrf Weight Path
 *    1.1.1.1/32       172.16.128.5           65535             0 998 998?
 *>                    172.16.128.1           65535             0 998 ?
 *    [redacted]32     172.16.128.5           65535             0 998 998?
 *>                    172.16.128.1           65535             0 998 ?
 *    [redacted]/32    172.16.128.5           65535             0 998 998?
 *>                    172.16.128.1           65535             0 998 ?
 <snip>
```

アクティブ/スタンバイBGPネイバー

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。