Cisco Secure Management Center と AWS VPC 間でのルートベースサイト間 VPN の設定

改訂：2024 年 11 月 6 日

Cisco Secure Management Center と AWS VPC 間でのルートベースサイト間 VPN の設定

はじめに

Cisco Secure Firewall Management Center（Management Center）は、管理対象 Threat Defense デバイスでのサイト間 VPN の設定を合理化するように設計された直感的な VPN ウィザードを備えています。

これらのウィザードを使用すると、Threat Defense デバイスとエクストラネットデバイス間のルートベースサイト間 VPN のセットアップも容易になります。Management Center の直接管理下にないエクストラネットデバイスは、パブリック クラウド インフラストラクチャ内に配置されたゲートウェイで構成されている場合があります。ルートベース VPN は、仮想トンネルインターフェイス（VTI）を使用します。これは、VPN トンネルの基盤を形成するルーティング可能な論理インターフェイスです。

対象読者

このガイドは、Management Center を使用して、本社にある Threat Defense デバイスと AWS 仮想プライベートクラウド（VPC）の間にサイト間 VPN を確立するネットワーク管理者を対象としています。

シナリオ

中規模企業が複数の分散拠点を運用しており、各拠点に AWS でホストされている一連のインスタンスがあるとします。この組織は、すべての拠点間の安全かつシームレスな通信を促進するために、堅牢なネットワーク インフラストラクチャを確立する必要があります。その解決策には、各拠点の AWS VPC を、組織の本社にある Threat Defense デバイスに接続するサイト間 VPN の構成が含まれます。デフォルトでは、AWS VPC インスタンスは外部ネットワークから分離されているため、この接続は非常に重要です。この VPN の導入により、各拠点を企業のネットワークに統合できるようになり、アクセスとデータセキュリティの一元化が確保されます。

システム要件

次の表に、この機能のプラットフォームを示します。

製品	バージョン	このマニュアルで使用するバージョン
Cisco Secure Firewall Threat Defense（旧称 Firepower Threat Defense/FTD）	6.7 以降	7.4.1

製品	バージョン	このマニュアルで使用するバージョン
Cisco Secure Firewall Management Center（旧称 Firepower Management Center/FMC）	6.7 以降	7.4.1
AWS Account	-	-

利点

提案されているソリューションには、次のような大きな利点があります。

- セットアップの合理化：VTI は、従来のクリプトマップとアクセスリストの複雑さを排除して、VPN 設定へのシンプルなアプローチを実現します。
- 適応型ルーティング：VTI は、BGP、EIGRP、OSPF などのダイナミック ルーティング プロトコルに対応し、ネットワークの状態の変化に応じた VPN エンドポイント間のルートの自動更新を容易にします。
- ISP の復元力：VTI はセカンダリ バックアップ トンネルの作成を可能にし、接続の信頼性を高めます。
- ロードバランシング：VTI により、 ECMP ルーティングを介して VPN トラフィックを均等に配分できます。

前提条件

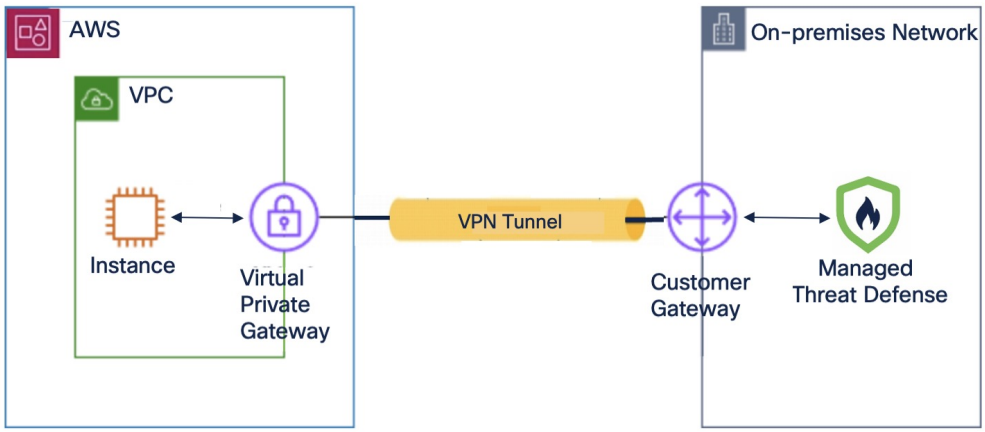
- ライセンス：Management Center Essentials（旧 Base）ライセンスで、輸出規制対象機能が許可されている必要があります。Management Center でこの機能を確認するには、[システム（System）] > [ライセンス（Licenses）] > [スマートライセンス（Smart Licenses）] の順に選択します。
- Threat Defense デバイスに対して、インターネットでルーティング可能なパブリック IP アドレスを設定します。
- Threat Defense デバイスのインターフェイスに、適切な論理名とIPアドレスを割り当てます。
- AWS アカウントを用意します。

Management Center と AWS 間のサイト間 VPN のコンポーネント

Management Center と AWS 間のサイト間 VPN は、次のコンポーネントで構成されます。

- 仮想プライベートゲートウェイ
- カスタマー ゲートウェイ デバイス（管理対象 Threat Defense）
- カスタマーゲートウェイ

図 *1 : AWS VPC* とオンプレミスネットワーク間のサイト間 *VPN*



仮想プライベートゲートウェイ

仮想プライベートゲートウェイは、サイト間 VPN 接続の AWS 側の VPN コンセントレータです。仮想プライベートゲートウェイを作成し、仮想プライベートクラウド（VPC）に接続します。

カスタマーゲートウェイ

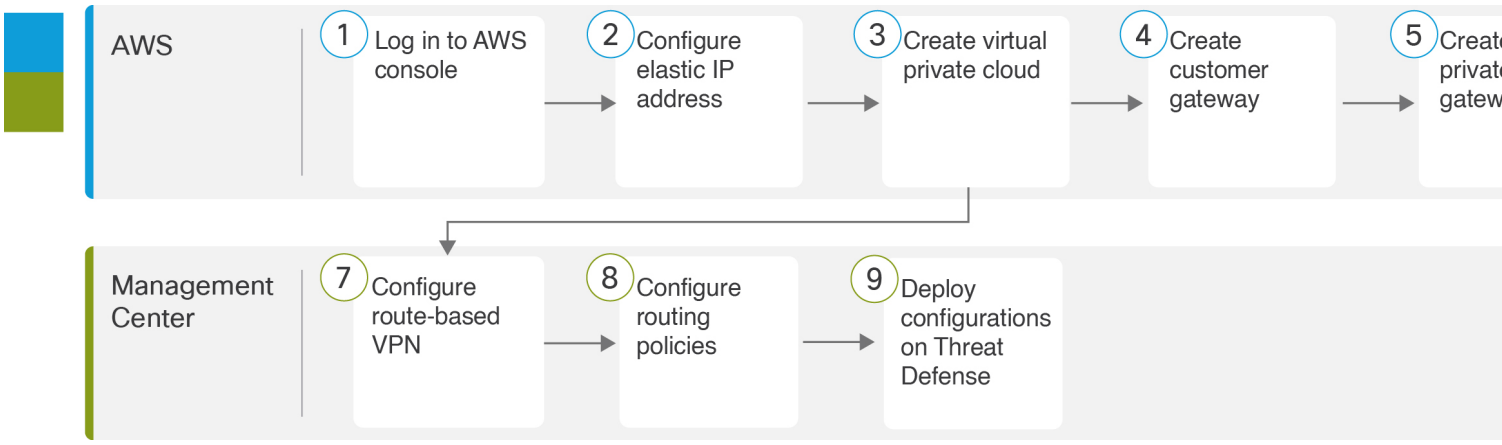
カスタマーゲートウェイは、お客様が AWS で作成するリソースであり、オンプレミスネットワークのカスタマーゲートウェイ デバイスのことです。カスタマーゲートウェイを作成する場合は、デバイスに関する情報を AWS に提供します。

カスタマー ゲートウェイ デバイス（管理対象 Threat Defense）

カスタマー ゲートウェイ デバイスは、本社のオンプレミスネットワーク内の Threat Defense デバイスです。AWS サイト間 VPN 接続で動作するようにデバイスを設定します。

Management Center と AWS VPC 間でのルートベース VPN 設定のエンドツーエンドの手順

次のフローチャートは、Management Center と AWS VPC 間でルートベース VPN を設定するためのワークフローを示しています。



1 AWS での Elastic IP アドレスの設定 （6 ページ）
2 Management Center でのルーティングポリシーの設定 （20 ページ）
3 AWS での仮想プライベートクラウドの作成 （6 ページ）
4 AWS でのカスタマーゲートウェイの作成 （9 ページ）
5 AWS での仮想プライベートゲートウェイの作成 （11 ページ）
6 AWS での VPN 接続の作成 （13 ページ）
7 Management Center でのルートベース VPN の設定 （16 ページ）

ステップ	説明
1	AWS コンソールにログインします。
2	Elastic IP アドレスを設定します。AWS での Elastic IP アドレスの設定 （6 ページ）を参照してください。
3	仮想プライベートクラウドを作成します。AWS での仮想プライベートクラウドの作成 （6 ページ）を参照してください。
4	カスタマーゲートウェイを作成します。AWS でのカスタマーゲートウェイの作成 （9 ページ）を参照してください。
5	仮想プライベートゲートウェイを作成します。AWS での仮想プライベートゲートウェイの作成 （11 ページ）を参照してください。
6	AWS VPN 接続を作成します。AWS での VPN 接続の作成 （13 ページ）を参照してください。
7	ルートベース VPN を設定します。Management Center でのルートベース VPN の設定 （16 ページ）を参照してください。
8	ルーティングポリシーを設定します。Management Center でのルーティングポリシーの設定 （20 ページ）を参照してください。
9	設定を Threat Defense に展開します。

AWS での Elastic IP アドレスの設定

Elastic IP アドレスは、AWS アカウントに割り当てられるスタティックパブリック IPv4 アドレスです。

手順

ステップ 1 [サービス（Services）] > [ネットワークとコンテンツ配信（Networking & Content Delivery）] > [VPC] を選択します。

ステップ 2 左側のペインで [Elastic IP（Elastic IPs）] をクリックします。

ステップ 3 [Elastic IPアドレスの割り当て（Allocate Elastic IP address）] をクリックします。

ステップ 4 [Elastic IPアドレスの割り当て（Allocate Elastic IP address）] ダイアログボックスで、次のパラメータを設定します。

a) [ネットワークボーダーグループ（Network Border Group）] には、デフォルト値を使用します。

b) [AmazonのIPv4アドレスのプール（Amazon's pool of IPv4 addresses）] オプションボタンをクリックします。

c) [割り当て（Allocate）] をクリックします。

AWS での仮想プライベートクラウドの作成

VPC は、AWS アカウント専用の仮想ネットワークです。これは、AWS クラウド内の他の仮想ネットワークから論理的に分離されています。VPC を作成すると、AWS は IPアドレス、サブネット、ルートテーブル、ネットワークゲートウェイ、およびセキュリティ設定を設定します。

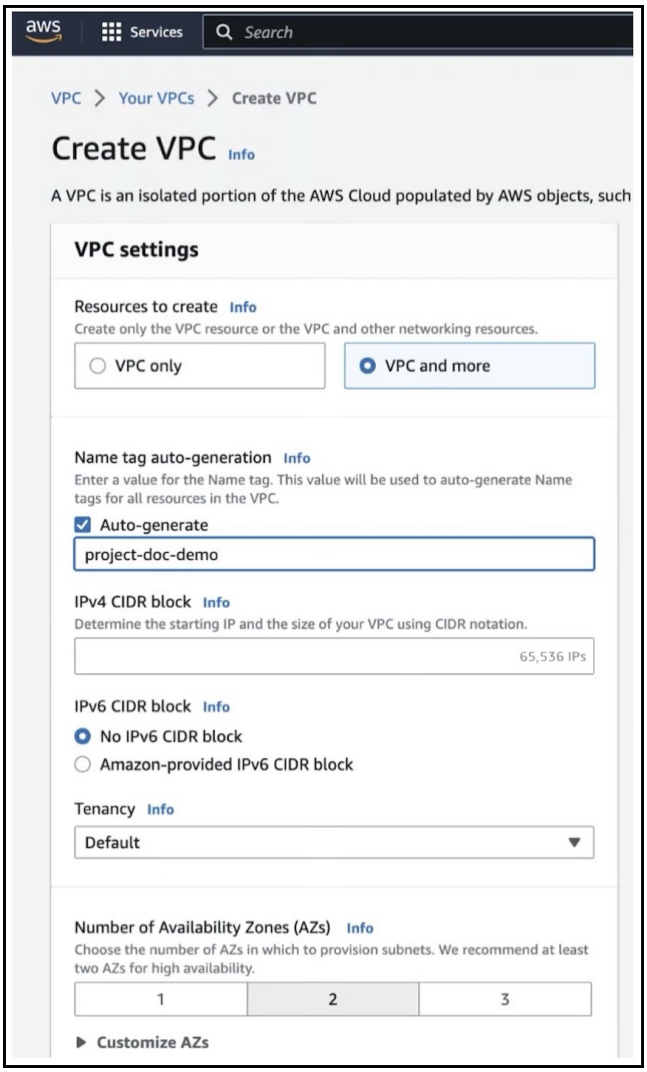
手順

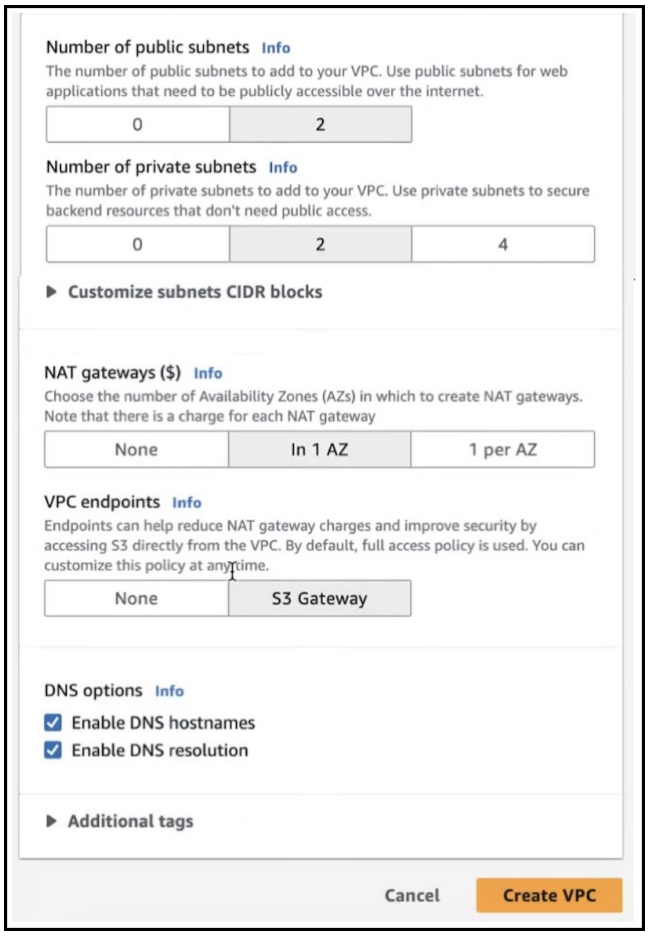
ステップ 1 [サービス（Services）] > [ネットワークとコンテンツ配信（Networking & Content Delivery）] > [VPC] を選択します。

ステップ 2 左側のペインで、[VPCダッシュボード（VPC dashboard）] をクリックします。

ステップ 3 [VPCの作成（Create VPC）] をクリックします。

ステップ 4 [VPCの作成（Create VPC）] ダイアログボックスで、次のパラメータを設定します。


aws
Services
Search
VPC > Your VPCs > Create VPC
Create VPC Info
A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such
VPC settings
Resources to create Info
Create only the VPC resource or the VPC and other networking resources.
VPC only
VPC and more
Name tag auto-generation Info
Enter a value for the Name tag. This value will be used to auto-generate Name tags for all resources in the VPC.
Auto-generate
project-doc-demo
IPv4 CIDR block Info
Determine the starting IP and the size of your VPC using CIDR notation.
65,536 IPs
IPv6 CIDR block Info
No IPv6 CIDR block
Amazon-provided IPv6 CIDR block
Tenancy Info
Default
Number of Availability Zones (AZs) Info
Choose the number of AZs in which to provision subnets. We recommend at least two AZs for high availability.
1
2
3
Customize AZs



a) [VPCとその他（VPC and more）] オプションボタンをクリックします。

b) [名前タグ（Name tag）] フィールドに、VPC を識別する名前を入力します。

c) [IPv4 CIDRブロック（IPv4 CIDR block）] フィールドに、IP アドレスを入力します。

CIDR ブロックサイズは /16 ～ /28 である必要があります。

d) [テナント（Tenancy）] ドロップダウンリストから、[デフォルト（Default）] を選択します。

このオプションでは、VPCに対して起動するインスタンスを、他のAWSアカウントと共有されているハードウェアで実行するか、または自分専用のハードウェアで実行するかを定義します。

e) 少なくとも2つの可用性ゾーンにサブネットをプロビジョニングするには、[可用性ゾーン（AZ）の数（Number of Availability Zones (AZs)）] として [2] を選択します。

f) [パブリックサブネットの数（Number of public subnets）] と [プライベートサブネットの数（Number of private subnets）] の値を選択して、サブネットを設定します。

g) [サブネットCIDRブロックのカスタマイズ（Customize subnets CIDR blocks）] を展開して、サブネットの IP アドレス範囲を選択します。AWS に選択させることもできます。

h) （オプション）[NATゲートウェイ（NAT gateways）] では、プライベートサブネット内のリソースが IPv4 経由でパブリックインターネットにアクセスする必要がある場合に、NAT ゲートウェイを作成する AZ の数を選択します。

i) [VPCエンドポイント（VPC endpoints）] では、[なし（None）] または [S3ゲートウェイ（S3 Gateway）] を選択します。

j) （オプション）[Domain Name System（DNS）オプション（Domain Name System (DNS) options）] では、両方のオプションがデフォルトで有効になっています。

k) [VPCの作成（Create VPC）] をクリックします。

AWS でのサブネットとルートテーブルの関連付け

VPC の各サブネットを VPC のルートテーブルに関連付ける必要があります。

始める前に

AWS で VPC を作成します。

手順

ステップ 1 左側のペインで [ルートテーブル（Route tables）] をクリックします。

ステップ 2 VPC に割り当てられたルートテーブルを選択します。

ステップ 3 [サブネットの関連付け（Subnet Associations）] タブをクリックします。

ステップ 4 [サブネットの関連付けの編集（Edit subnet associations）] をクリックします。

ステップ 5 プライベートサブネットとパブリックサブネットのチェックボックスをオンにします。

ステップ 6 [関連付けの保存（Save associations）] をクリックします。

AWS でのカスタマーゲートウェイの作成

カスタマーゲートウェイを作成して、デバイスに関する情報を AWS に提供します。

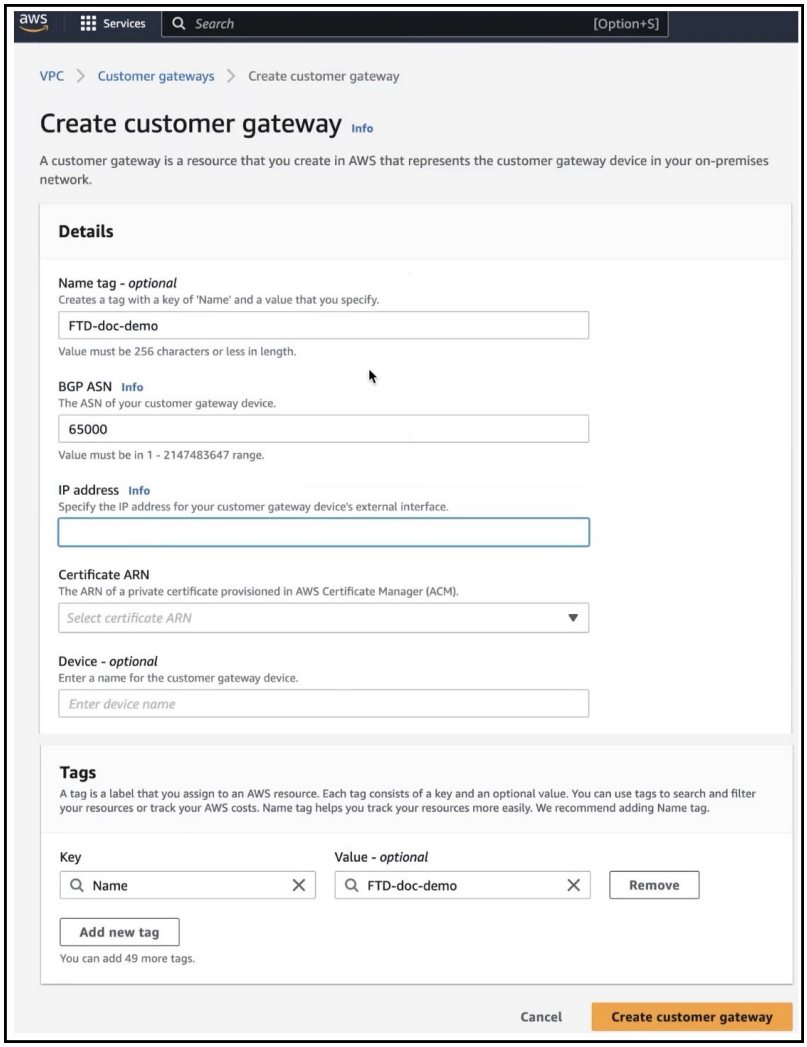
手順

ステップ 1 左側のペインで、[仮想プライベートネットワーク（VPN）（Virtual Private network (VPN)）] を展開します。

ステップ 2 [カスタマーゲートウェイ（Customer Gateway）] をクリックします。

ステップ 3 [カスタマーゲートウェイの作成（Create Customer Gateway）] をクリックします。

ステップ 4 [カスタマーゲートウェイの作成（Create Customer Gateway）] ダイアログボックスで、次のパラメータを設定します。



a) [名前タグ（Name tag）] フィールドに、カスタマーゲートウェイを識別する名前を入力します。

b) [BGP ASN] フィールドに、Threat Defense デバイスの BGP 自律システム番号（ASN）を入力します。

有効な範囲は 1 ～ 2,147,483,647 です。この例では、ASN は 65000 です。この ASN は、Management Center で BGP ルーティングを設定するときに必要です。

c) [IPアドレス（IP address）] フィールドに、Threat Defense デバイスの外部インターフェイスの IP アドレスを入力します。

IP アドレスは静的である必要があります。カスタマー ゲートウェイ デバイスが NAT デバイスの背後にある場合は、NAT デバイスの IP アドレスを使用します。

d) （オプション）[証明書ARN（Certificate ARN）] フィールドに、Threat Defense デバイスの AWS Certificate Manager（ACM）プライベート証明書の Amazon リソース名（ARN）を入力して、証明書ベースの認証を有効にします。

e) （オプション）[デバイス（Device）] フィールドに、Threat Defense デバイスの名前を入力します。

f) [カスタマーゲートウェイの作成（Create Customer Gateway）] をクリックします。

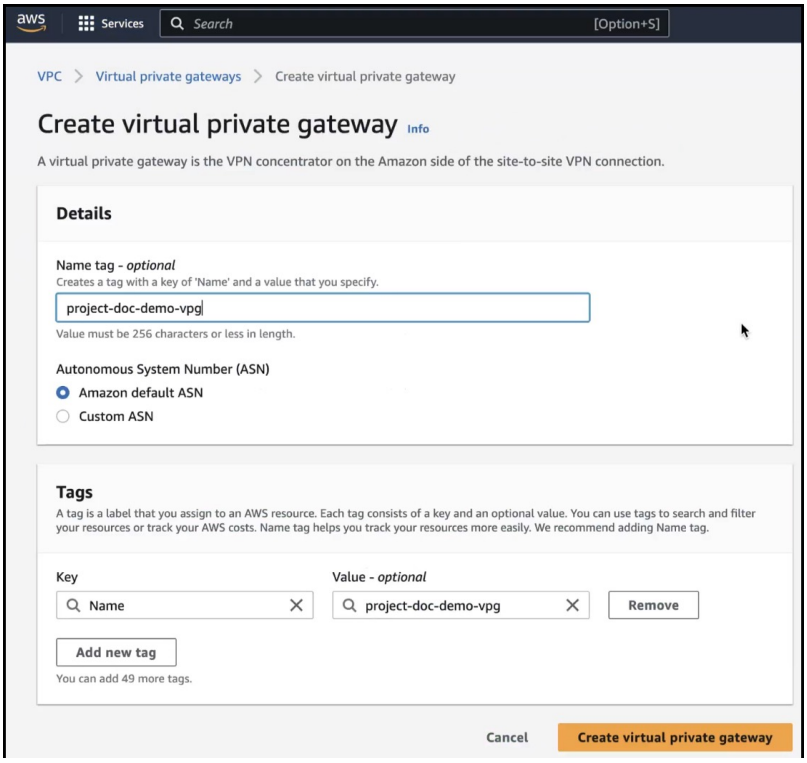
AWS での仮想プライベートゲートウェイの作成

手順

ステップ 1 左側のペインで、[仮想プライベートネットワーク（VPN）（Virtual private network (VPN)）] を展開します。

ステップ 2 [仮想プライベートゲートウェイの作成（Create virtual private gateway）] をクリックします。

ステップ 3 [仮想プライベートゲートウェイの作成（Create virtual private gateway）] ダイアログボックスで、次のパラメータを設定します。



a) [名前タグ（Name tag）] フィールドに、仮想プライベートゲートウェイの名前を入力します。

b) [AmazonデフォルトASN（Amazon default ASN）] オプションボタンと [カスタムASN（Custom ASN）] オプションボタンのいずれかをクリックします。

Amazon ASN は 64512 であることに注意してください。

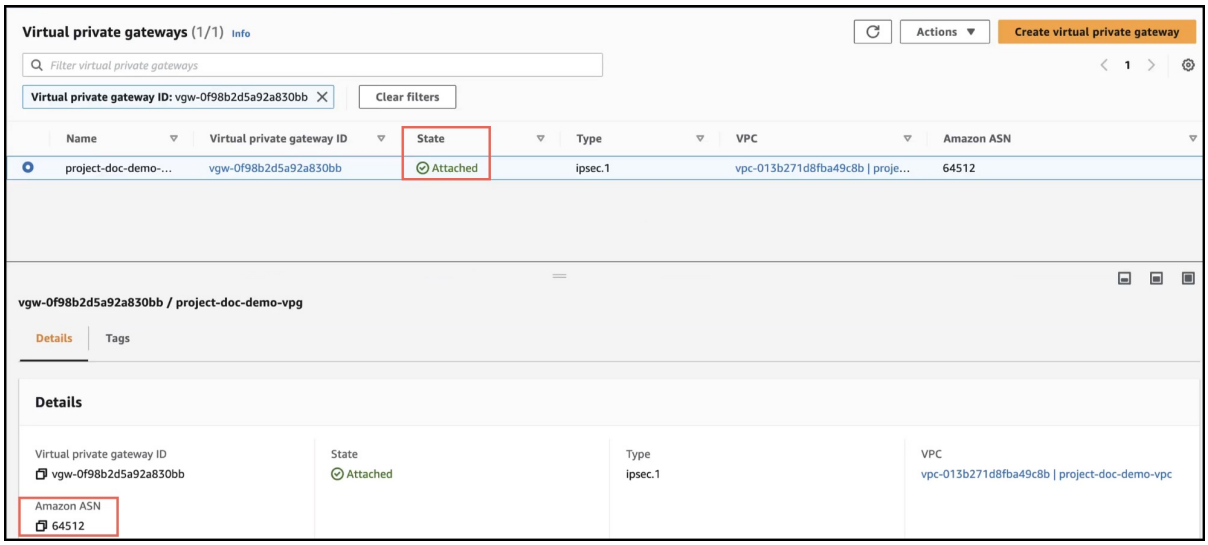
c) [タグ（Tags）] については、デフォルトでは名前がタグと見なされます。
d) [仮想プライベートゲートウェイの作成（Create virtual private gateway）] をクリックします。

仮想プライベートゲートウェイの仮想プライベートクラウドへの接続

仮想プライベートゲートウェイを作成したら、それを VPC に接続する必要があります。

手順

ステップ 1 作成した仮想プライベートゲートウェイを選択します。
ステップ 2 [アクション（Actions）] ドロップダウンリストから [VPCへの接続（Attach to VPC）] を選択します。
ステップ 3 [VPCへの接続（Attach to VPC）] ダイアログボックスで、[使用可能なVPC（Available VPCs）] ドロップダウンリストから VPC を選択します。
ステップ 4 [VPCへの接続（Attach to VPC）] をクリックします。
ステップ 5 仮想プライベートゲートウェイの [状態（State）] が [接続済み（Attached）] であることを確認します。



AWS での VPN 接続の作成

始める前に

VPC、カスタマーゲートウェイ、および仮想プライベートゲートウェイがあることを確認します。

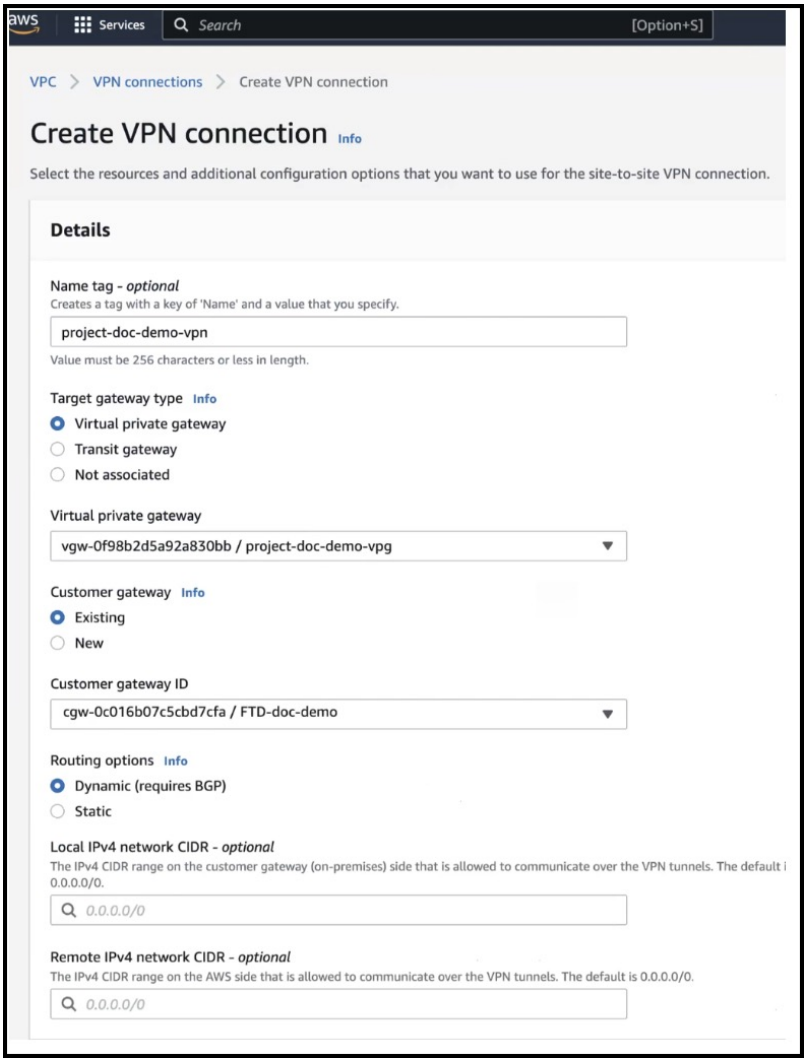
手順

ステップ 1 左側のペインで、[仮想プライベートネットワーク（VPN）（Virtual private network (VPN)）] を展開します。

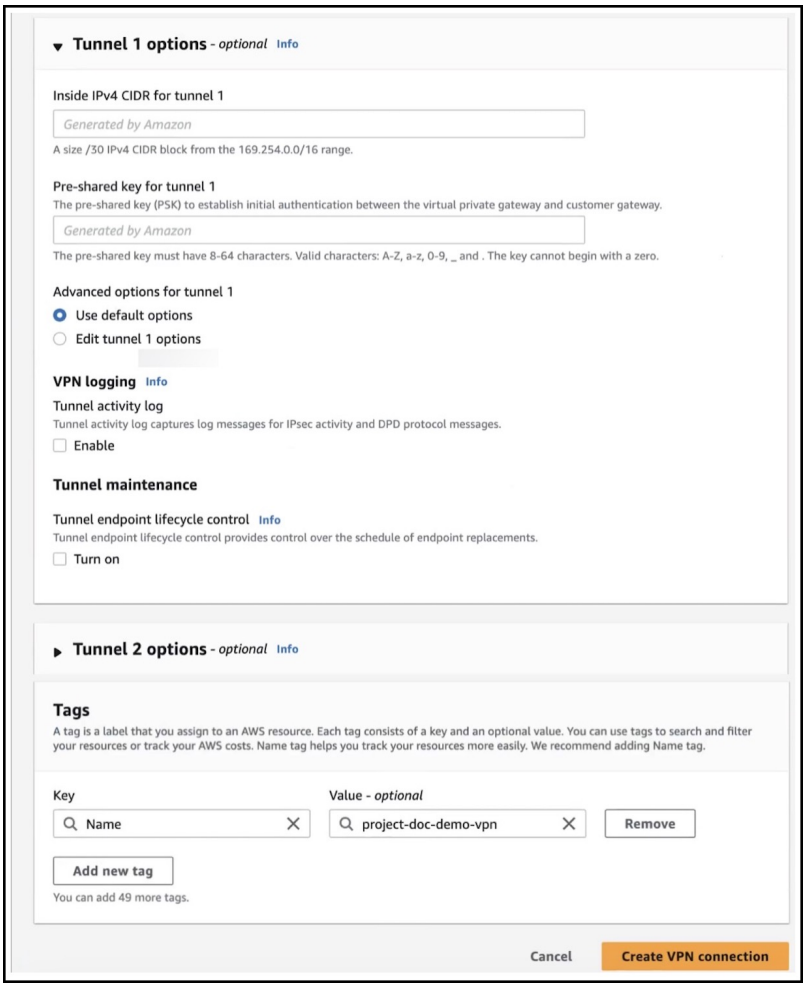
ステップ 2 [サイト間VPN接続（Site-to-Site VPN connections）] をクリックします。

ステップ 3 [VPN接続の作成（Create VPN Connection）] をクリックします。

ステップ 4 [VPN接続の作成（Create VPN Connection）] ダイアログボックスで、次の VPN パラメータを設定します。



a) [名前タグ（Name）] フィールドに VPN 接続の名前を入力します。
b) [ターゲットゲートウェイタイプ（Target gateway type）] で、[仮想プライベートゲートウェイ（Virtual private gateway）] オプションボタンをクリックます。
c) [仮想プライベートゲートウェイ（Virtual private gateway）] ドロップダウンリストから、仮想プライベートゲートウェイを選択します。
d) [カスタマーゲートウェイ（Customer gateway）] で、[既存（Existing）] オプションボタンをクリックし、[カスタマーゲートウェイID（Customer gateway ID）] ドロップダウンリストからカスタマーゲートウェイを選択します。
e) [ルーティングオプション（Routing options）] で、[ダイナミック（BGP が必要）（Dynamic (requires BGP)）] オプションボタンをクリックします。
f) （オプション）[ローカルIPv4ネットワークCIDR（Local IPv4 Network CIDR）] で、Threat Defense デバイスの保護対象ネットワークの IP アドレスを入力するか、デフォルト値 0.0.0.0/0 を使用します。
g) （オプション）[リモートIPv4ネットワークCIDR（Remote IPv4 Network CIDR）] で、AWS 側ネットワークの IP アドレスを入力するか、デフォルト値 0.0.0.0/0 を使用します。
h) [トンネル1オプション（Tunnel 1 options）] を展開して、VPN トンネルパラメータを設定します。



1. [トンネル1の内部IPv4 CIDR（Inside IPv4 CIDR for tunnel 1）] に対して、AWS は IPv4 アドレスを生成します。
2. [トンネル1の事前共有キー（Pre-shared key for tunnel 1）] フィールドに、仮想プライベートゲートウェイとカスタマーゲートウェイ間の認証用の事前共有キー（PSK）を入力します。PSK を指定しない場合、AWS は PSK を生成します。

   この PSK は、Management Center で VPN を設定するために必要です。
3. [トンネル1の詳細オプション（Advanced options for tunnel 1）] で、[デフォルトオプションを使用（Use default options）] オプションボタンをクリックします。

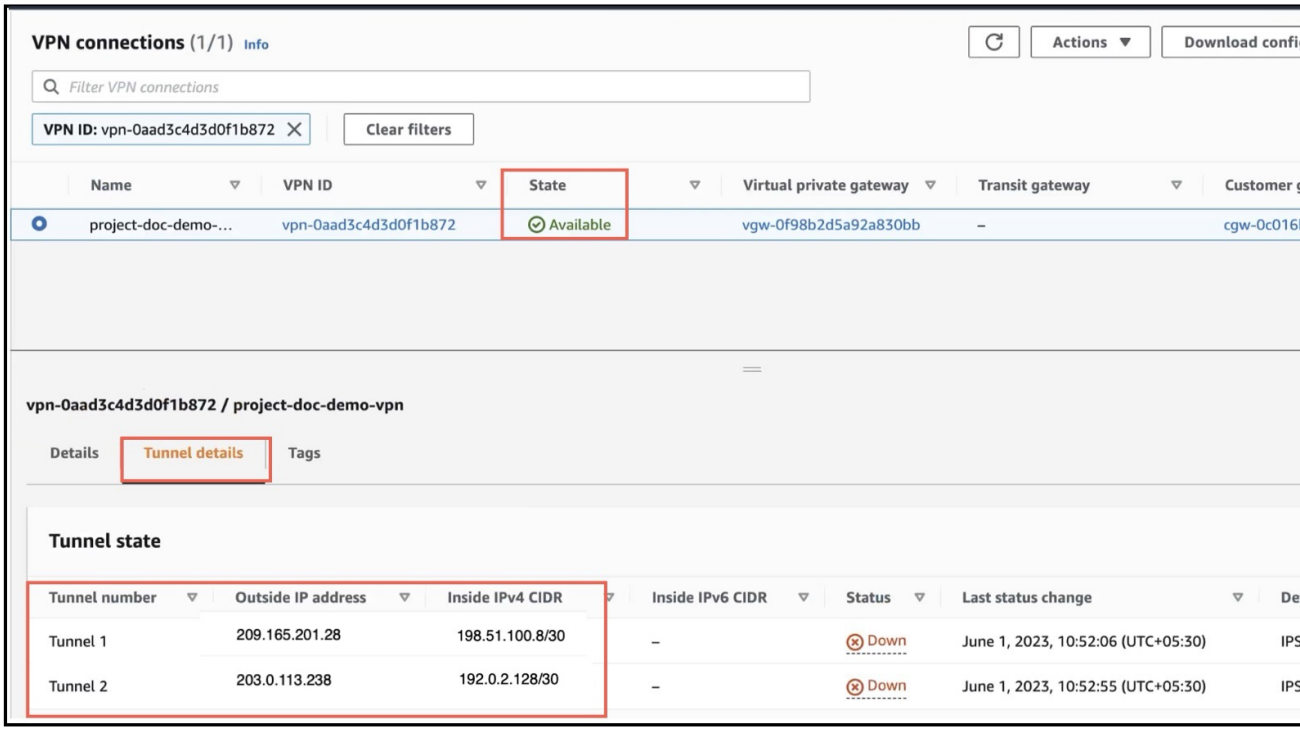
i) （オプション）[トンネル2オプション（Tunnel 2 options）] を展開して、バックアップ VPN トンネルパラメータを設定します。

（注） 両方のトンネルに同じ PSK を使用していることを確認します。

ステップ 5 [VPN接続の作成（Create VPN Connection）] をクリックします。

VPN 接続が作成されると、[状態（State）] が [保留中（Pending）] から [使用可能（Available）] に変わります。

a) 作成した VPN 接続を選択して、詳細を表示します。
b) [トンネルの詳細（Tunnel details）] タブをクリックします。



上記の例では、次の詳細に注意してください。

Tunnel	外部（エクストラネット）IP アドレス	AWS VTI IP アドレス	Threat Defense デバイス VTI IP アドレス
Tunnel 1	209.165.201.28	198.51.100.9/30	198.51.100.10/30
Tunnel 2	203.0.113.238	192.0.2.129/30	192.0.2.130/30

Management Center でルートベース VPN を設定する場合は、上記の詳細情報が必要です。

Management Center でのルートベース VPN の設定

始める前に

AWS の VPN トンネルの内部 IP アドレスと外部 IP アドレスをメモしておきます。

手順

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

ステップ 2 [+サイト間VPN（+ Site To Site VPN）] をクリックします。

ステップ 3 [トポロジ名（Topology Name）] フィールドに、VPN トポロジの名前を入力します。

ステップ 4 [ルートベース（VTI）（Route Based (VTI)）] オプションボタンをクリックします。

ステップ 5 [ポイントツーポイント（Point to Point）] タブをクリックします。

ステップ 6 [IKEv2] チェックボックスをオンにします。

ステップ 7 [エンドポイント（Endpoints）] タブをクリックします。

ステップ 8 [ノードA（Node A）] について、次のパラメータを設定します。

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

b) [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から Threat Defense デバイスのスタティック仮想トンネルインターフェイス（SVTI）を選択するか、[+] をクリックして SVTI を作成します。

SVTI の作成の詳細については、「Management Center での Threat Defense スタティック VTI の作成（19 ページ）」を参照してください。

c) （オプション）[+バックアップVTIの追加（+ Add Backup VTI）] をクリックしてバックアップ VTI を設定し、必要なパラメータを設定します。

[トンネル送信元（Tunnel Source）] は、両方の VTI トンネルで同じです。この例では、バックアップ VTI IP アドレスは 192.0.2.130/30 です。「AWS での VPN 接続の作成 （13 ページ）」の IP アドレステーブルを参照してください。

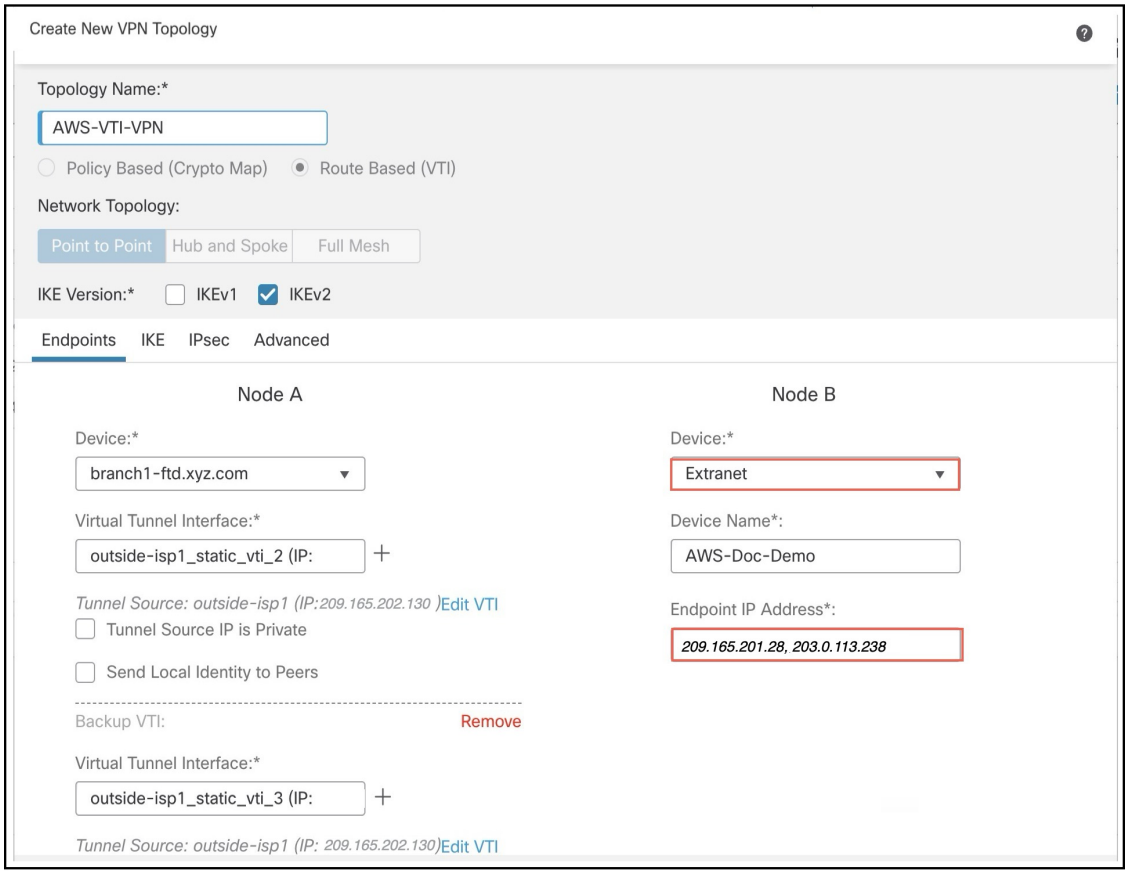
ステップ 9 [ノードB（Node B）] について、次のパラメータを設定します。

a) [デバイス（Devices）] 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。

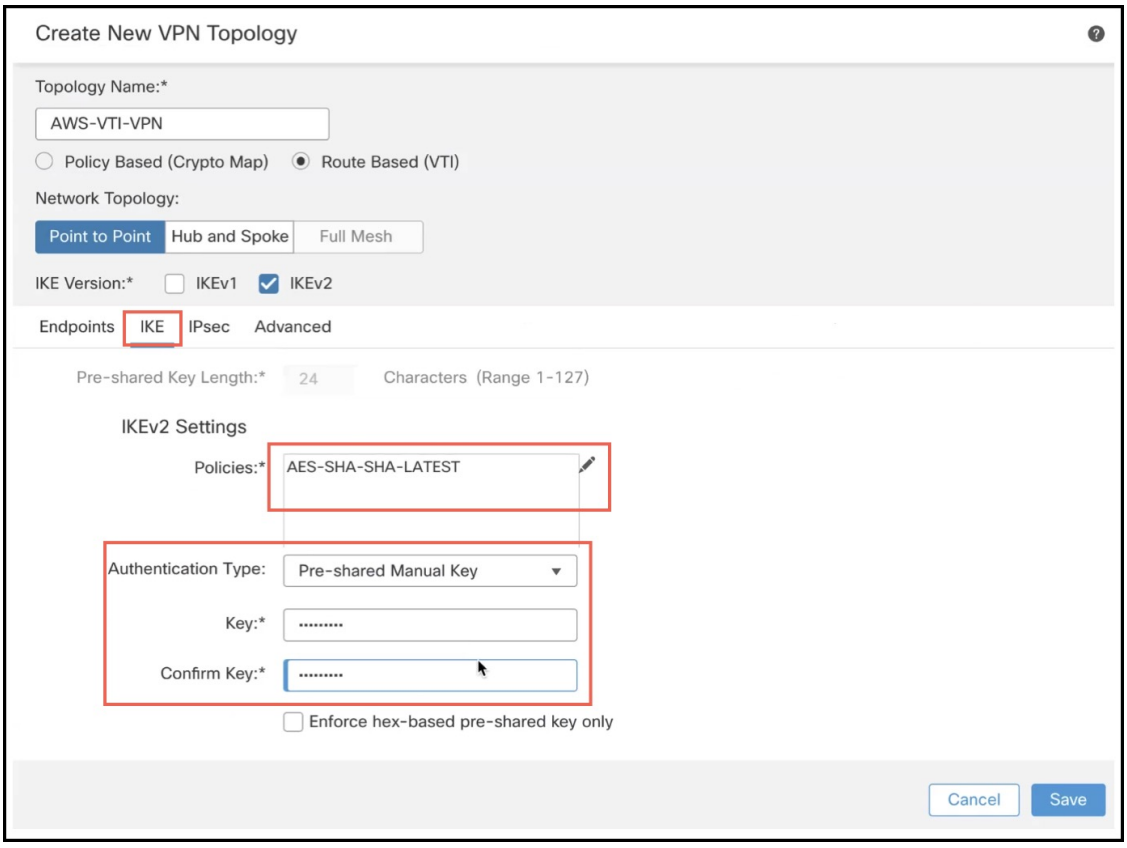
b) [デバイス名（Device Name）] フィールドに、エクストラネットデバイス名を入力します。

c) [エンドポイントIPアドレス（Endpoint IP Address）] フィールドに、AWS VPN の IP アドレスを入力します。

この例では、IP アドレスは 209.165.201.28 および 203.0.113.238 です。



ステップ 10 [IKE] をクリックして、次のパラメータを設定します。



a) [IKEv2設定（IKEv2 Settings）] で、[ポリシー（Policies）] に隣接する編集アイコンをクリックし、ドロップダウンリストから [AES-SHA-SHA-LATEST] を選択します。このプロトコルは、AWS VPN のデフォルトの IKE プロトコルです。

b) [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。

c) [キー（Key）] フィールドと [キーの確認（Confirm Key）] フィールドにキーを入力します。

この例では、AWS VPN で設定した PSK を使用します。

ステップ 11 [IPsec] と [詳細（Advanced）] の設定には、デフォルト値を使用します。

ステップ 12 [保存（Save）] をクリックします。

[サイト間VPN概要（Site-to-Site VPN Summary）] ページ（[デバイス（Devices）] > [サイト間VPN（Site To Site VPN）]）で、トポロジを表示できます。すべてのデバイスに設定を展開すると、このページですべてのトンネルのステータスを確認できます。

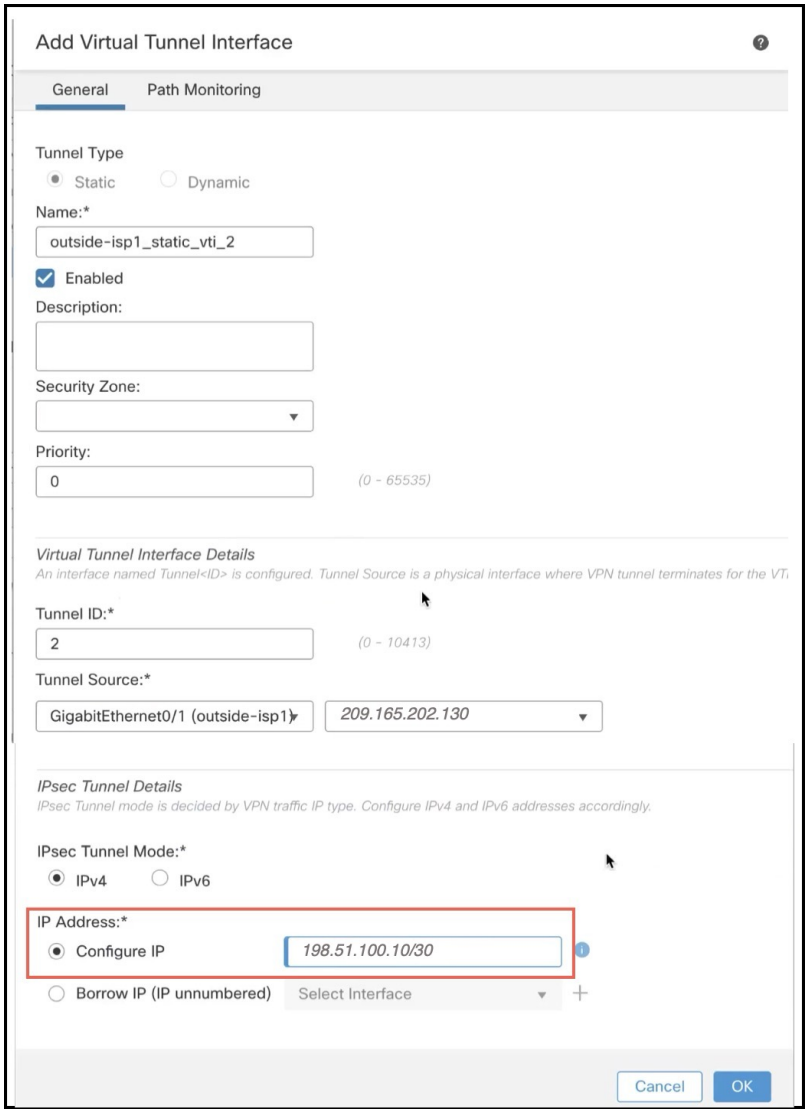
Management Center での Threat Defense スタティック VTI の作成

始める前に

「Management Center でのルートベース VPN の設定 （16 ページ）」の説明に従って、ルートベース VPN のポイントツーポイント トポロジの基本パラメータを設定し、[エンドポイント（Endpoints）] タブをクリックして、[デバイス（Device）] ドロップダウンリストから [ノードA（Node A）] として Threat Defense デバイスを選択します。

手順

[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で、次のパラメータを設定します。



a) [名前（Name）] フィールドに SVTI の名前を入力します。
b) [有効（Enabled）] チェックボックスをオンにします。

c) （オプション）[セキュリティゾーン（Security Zone）] ドロップダウンリストから、スタティック VTI のセキュリティゾーンを選択します。

d) [優先順位（Priority）] フィールドに、複数の VTI 間でトラフィックをロードバランシングする優先順位を入力します。

指定できる範囲は 0 ～ 65535 です。最も小さい番号が最も高い優先順位になります。

e) [トンネルID（Tunnel ID）] フィールドに、一意のトンネル ID を入力します。

範囲は 0 ～ 10413 です。

f) [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。

g) [IPSecトンネルモード（IPSec Tunnel Mode）] で、[IPv4] オプションボタンをクリックして、IPSec トンネルを通過するトラフィックのタイプを指定します。

h) [IPの設定（Configure IP）] フィールドに、SVTI の IP アドレスを入力します。

この例では、SVTI IPアドレスは 198.51.100.10/30 です。「AWS での VPN 接続の作成 （13 ページ）」の IP アドレステーブルを参照してください。

i) [OK] をクリックします。

Management Center でのルーティングポリシーの設定

Management Center でのアンダーレイ ルーティング ポリシーの設定

AWS との間のトラフィックを有効にするには、アンダーレイ ルーティング ポリシーを設定する必要があります。スタティックルートまたはダイナミック ルーティング プロトコルを設定できます。この例では、スタティックルートを使用します。

手順

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 編集するインターフェイスの横にある編集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、[スタティックルート（Static Route）] をクリックしてスタティックルートを設定します。

ステップ 5 [+ルートを追加（+Add Route）] をクリックします。

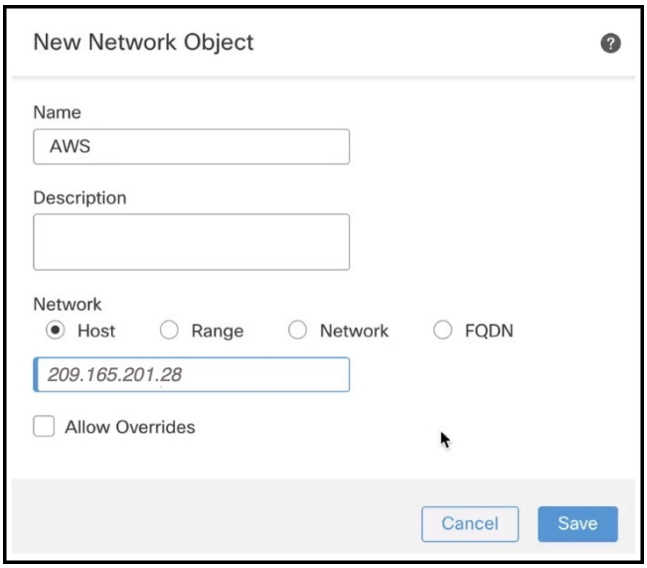
ステップ 6 [スタティックルート設定の追加（Add Static Route Configuration）] ダイアログボックスで、次のパラメータを設定します。

a) [IPv4] オプションボタンをクリックします。

b) [インターフェイス（Interface）] ドロップダウンリストから、Threat Defense デバイスの外部インターフェイスを選択します。

c) [使用可能なネットワーク（Available Network）] で [+] をクリックして、AWS ネットワークのネットワークオブジェクトを作成します。

d) [新規ネットワークオブジェクト（New Network Object）] ダイアログボックスで、次のパラメータを設定します。



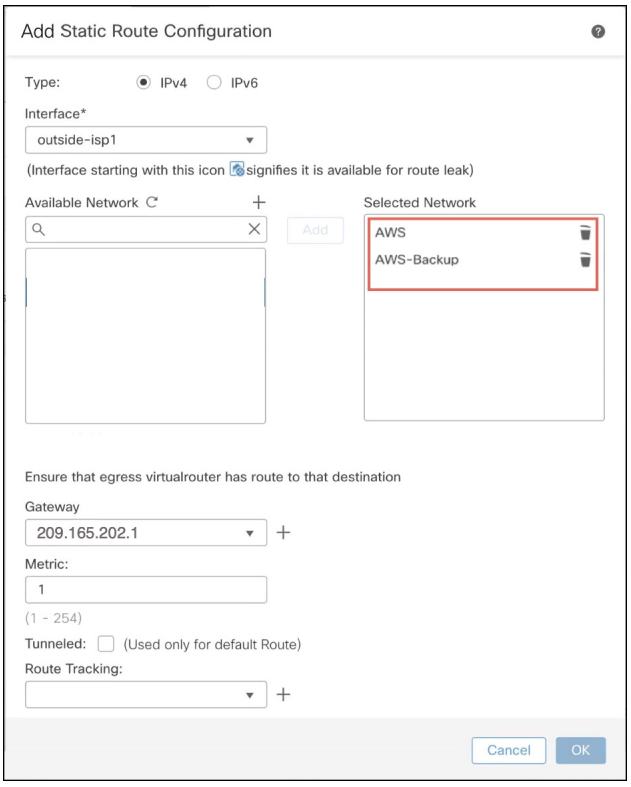
1. [名前（Name）] フィールドに AWS ネットワークの名前を入力します。
2. [ホスト（Host）] オプションボタンをクリックし、AWS ネットワークの IP アドレスを入力します。

   この例では、AWS ネットワークの IP アドレスは 209.165.201.28 です。
3. [保存（Save）] をクリックします。

e) ステップ 6c ～ 6d を繰り返して、バックアップ AWS ネットワーク用のネットワークオブジェクトを作成します。

この例では、バックアップ AWS ネットワークの IP アドレスは 203.0.113.238 です。

f) [使用可能なネットワーク（Available Network）] リストから AWS ネットワークとバックアップ AWS ネットワークを選択し、[追加（Add）] をクリックして [選択したネットワーク（Selected Network）] リストに移動させます。



g) [ゲートウェイ（Gateway）] フィールドに、Threat Defense デバイスのゲートウェイの IP アドレスを入力します。

h) [OK] をクリックします。

Management Center でのオーバーレイ ルーティング ポリシーの設定

VPN トラフィックのオーバーレイ ルーティング ポリシーを設定する必要があります。この例では、BGP ルーティング ポリシーを設定します。

手順

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 編集するインターフェイスの横にある編集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 左側のペインの [全般設定（General Settings）] で [BGP] をクリックします。

ステップ 5 [BGPの有効化（Enable BGP）] チェックボックスをオンにします。

ステップ 6 [AS番号（AS Number）] フィールドに、AWS カスタマーゲートウェイ用に設定した Threat Defense デバイスの AS 番号を入力します。

この例では、番号は 65000 です。

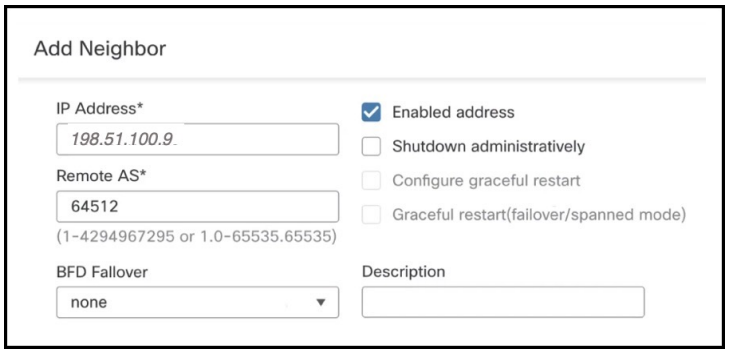
ステップ 7 [保存（Save）] をクリックします。

ステップ 8 左側のペインで、[BGP] > [IPv4] を選択します。

ステップ 9 [IPv4の有効化（Enable IPv4）] チェックボックスをオンにします。

ステップ 10 [ネイバー（Neighbor）] タブをクリックし、[+追加（+Add）] をクリックします。

ステップ 11 [ネイバーの追加（Add Neighbor）] ダイアログボックスで、次のパラメータを設定します。



a) [IPアドレス（IP Address）] フィールドに、AWS VPN 設定の AWS VTI IP アドレス（Tunnel1）を入力します。

この例では、AWS IPアドレスは 198.51.100.9 です。

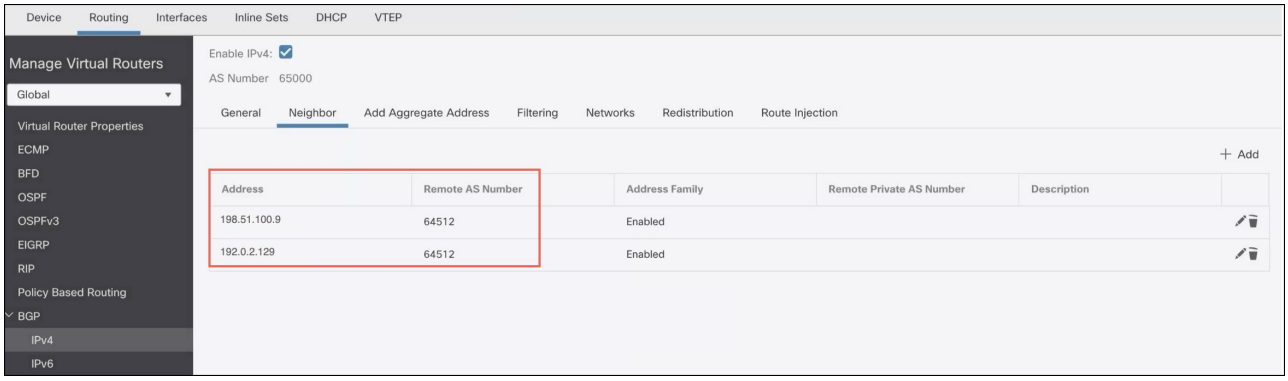
b) [リモートAS（Remote AS）] フィールドに、AWS VPN 設定の AWS AS 番号を入力します。

この例では、AWS AS 番号は 64512 です。

c) [OK] をクリックします。

ステップ 12 ステップ 11a ～ 11c を繰り返して、バックアップ AWS IP アドレス（Tunnel2）をネイバーとして追加します。

この例では、IPアドレスは 192.0.2.129 で、AWS AS 番号は 64512 です。



ステップ 13 [保存（Save）] をクリックします。

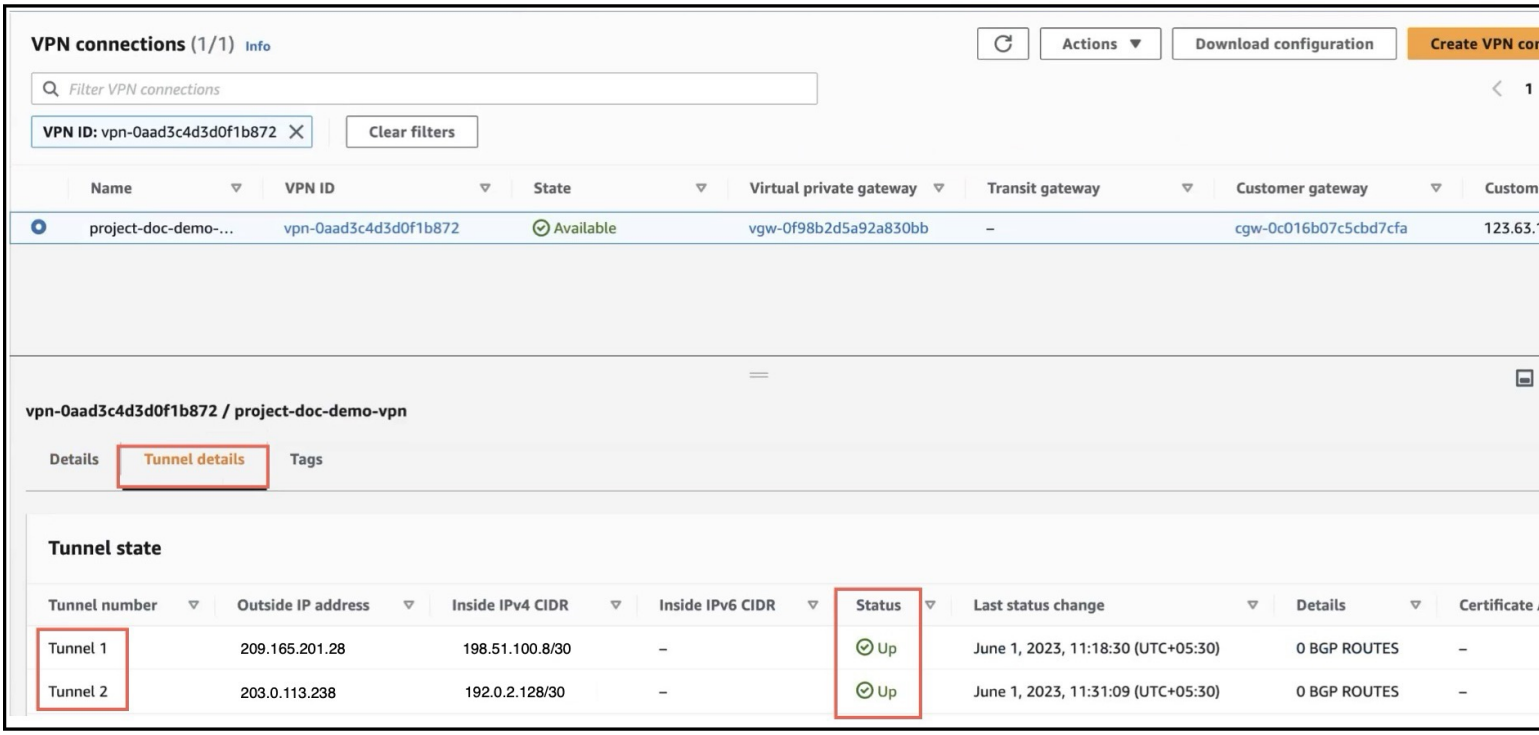
VTI トンネルのステータスと設定の確認

Threat Defense デバイスに設定を展開した後、デバイス、Management Center、および AWS で VTI トンネルの設定とステータスを確認できます。

AWS でのトンネルステータスの確認

AWS で VPN トンネルを確認するには、次の手順を実行します。

1. [仮想プライベートネットワーク（VPN）（Virtual private network (VPN)）] > [サイト間VPN接続（Site-to-Site VPN connections）] を選択します。
2. VPN に隣接するオプションボタンをクリックします。
3. [トンネルの詳細（Tunnel details）] タブをクリックします。トンネルの [ステータス（Status）] が [アップ（Up）] になっている必要があります。



Threat Defense デバイスでのトンネルとルーティングの設定の確認

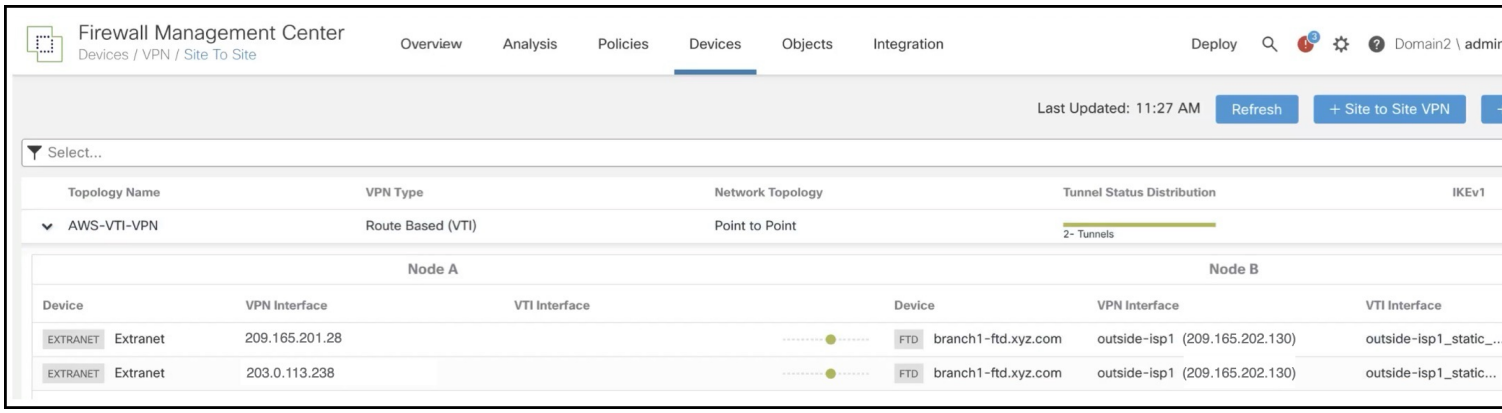
- Threat Defense デバイスでのインターフェイス設定を確認するには、**show running-config interface** コマンドを使用します。

```
interface Tunnel2
 nameif outside-isp1 static_vti_2
 ip address  198.51.100.10   255.255.255.252
 tunnel source interface outside-isp1
 tunnel destination 209.165.201.28
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile FMC_IPSEC_PROFILE_1
!
interface Tunnel3
 nameif outside-isp1_static_vti_3
 ip address   192.0.2.130     255.255.255.252
 tunnel source interface outside-isp1
 tunnel destination 203.0.113.238
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile FMC_IPSEC_PROFILE_1
```

- Threat Defense デバイスの BGP 設定を確認するには、**show bgp** コマンドを使用します。

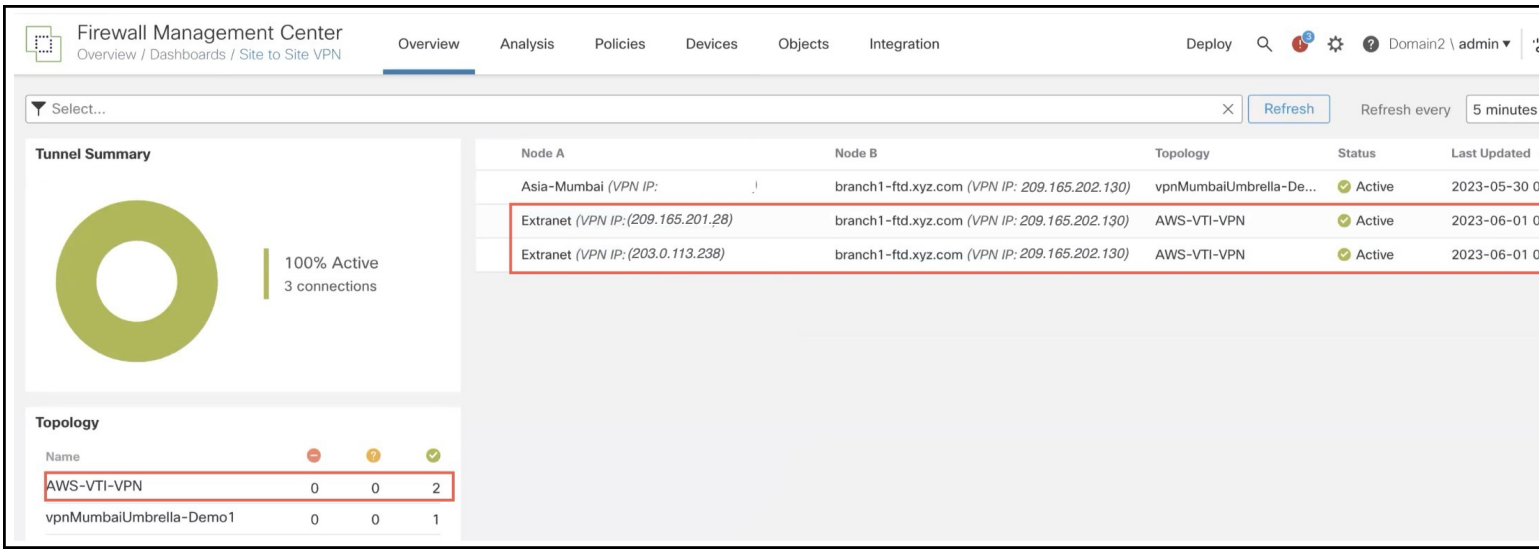
[サイト間VPN概要（Site-to-Site VPN Summary）] ページでのトンネルステータスの確認

VPN トンネルのステータスを確認するには、[デバイス（Device）] > [VPN] > [サイト間（Site To Site）] の順に選択します。



[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 トンネルの詳細を表示するには、[概要（Overview）]>[ダッシュボード（Dashboards）]>[サイト間VPN（Site-to-site VPN）] の順に選択します。



【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。

この資料の記載内容は2008年10月現在のものです。
この資料に記載された仕様は予告なく変更する場合があります。

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/

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。