

NATを使用したプライベートアクセスのための、セキュアなFTDおよびASAを使用したセキュアアクセスの設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[バックグラウンド情報](#)

[ネットワーク図](#)

[設定](#)

[セキュアアクセスおよびセキュアファイアウォールスレッド防御：PBRを使用したダイナミック\(BGP\)ルートベースVPN](#)

[FTDポリシーベースルーティング](#)

[FTDでのBGPの設定](#)

[トンネルステータスの確認](#)

[PBRを使用した適応型セキュリティアプライアンス\(ASA\)でのスタティックルートベースIPsec VPNの設定](#)

[セキュアアクセスでのVPN設定](#)

[ASAでのVPNの設定](#)

[ポリシーベースルーティング](#)

[確認](#)

はじめに

このドキュメントでは、ネットワークアドレス変換(NAT)を使用してセキュアアクセスネットワークトンネルグループを設定する方法について説明します。

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ファイアウォール管理センター

- Cisco Secure Firewall脅威対策
- シスコセキュアアクセス
- Cisco Adaptive Security Appliance
- ネットワークアドレス変換
- ポリシーベースルーティング
- ファイアウォールでのパケットキャプチャ

使用するコンポーネント

このドキュメントの情報は、次のハードウェアに基づくものです。

- Ciscoファイアウォール管理センター7.10
- Cisco Secure Firewall Threat Defense 7.10
- シスコセキュアアクセス
- Cisco適応型セキュリティアプライアンス9.22
- Cisco ルータ

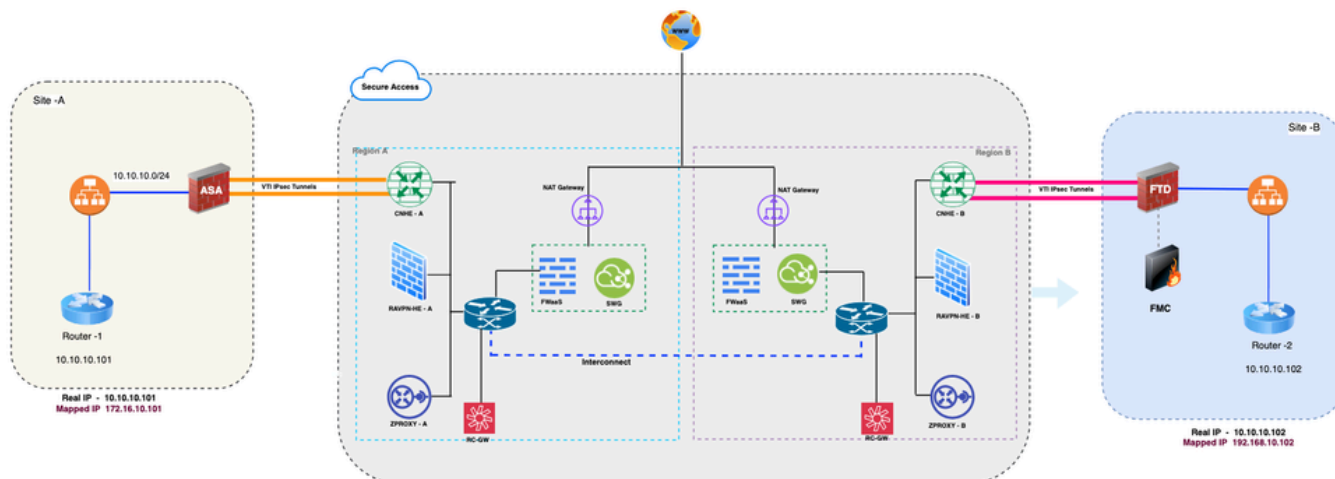
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

バックグラウンド情報

Cisco Secure Accessは、Secure Internet Access(SIA)やSecure Private Access(SPA)など、クラウドネイティブのセキュアサービスエッジ機能を提供します。データセンターを経由するすべてのトラフィックをバックホールすることなく、リモートユーザへのプライベートアプリケーションアクセスを拡張する組織では、Secure AccessはIPsecネットワークトンネルグループ(NTG)を使用して、Cisco Firewall Threat Defense(FTD)、Adaptive Security Appliance(ASA)、Cisco Secure Access Cloud Points-of-Presence(PoP)などのオンプレミスネットワークデバイス間に暗号化トンネルを作成します。

このドキュメントでは、Cisco FTD(FTD)、ASA、およびCisco Secure Accessの間でIKEv2を使用してルートベースのIPsecトンネルを確立し、セキュアアクセス上でネットワークアドレス変換(NAT)を有効にし、FTDおよびASA上でポリシーベースルーティング(PBR)を有効にして、プライベートアクセスバウンドのトラフィックだけをトンネルに誘導する方法について説明します。

ネットワーク図



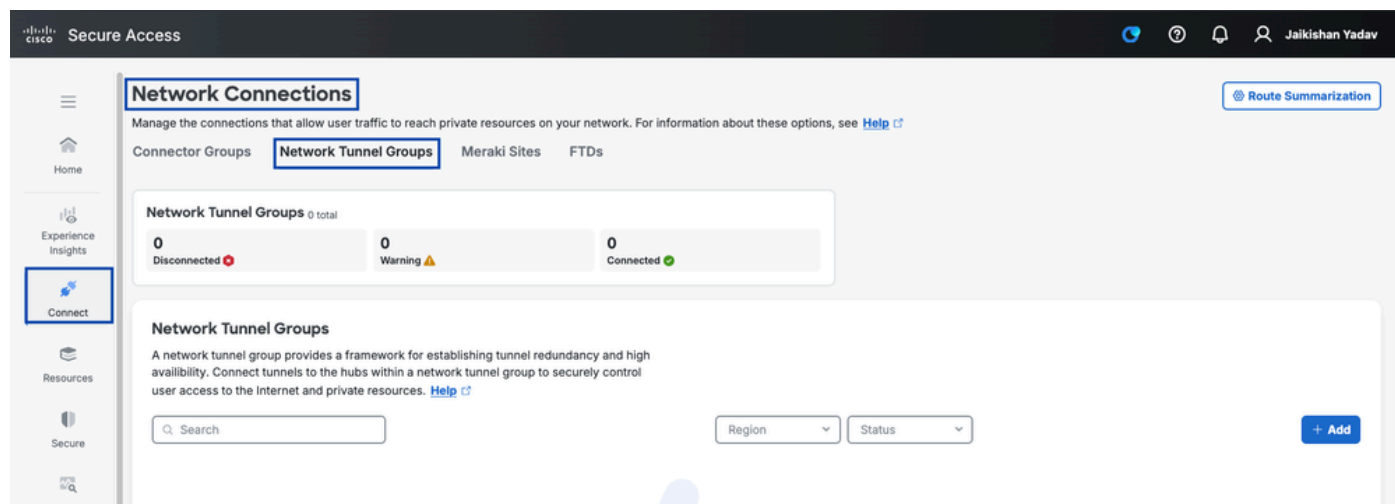
Network Topology

設定

セキュアアクセスおよびセキュアファイアウォールスレッド防御：PBRを使用したダイナミック(BGP)ルートベースVPN

セキュアアクセスでのネットワークトンネルグループの設定

1. セキュアアクセスダッシュボードへのログイン [セキュアアクセス](#)
2. Connect > Network Connections > Network Tunnel Groupsの順に移動し、+Addをクリックしてネットワークトンネルグループを設定します



セキュアアクセス – ネットワークトンネルグループ

3. ネットワークトンネルグループの構成 – 一般設定

- トンネルグループの名前、リージョン、およびデバイスタイプの設定
- [Next] をクリックします。

The screenshot shows the 'Add a Network Tunnel Group' configuration page. The left sidebar has four steps: 1. General Settings (selected), 2. Tunnel ID and Passphrase, 3. Routing, and 4. Data for Tunnel Setup. The main content area is titled 'General Settings' and includes instructions: 'Give your network tunnel group a good meaningful name, choose a region through which it will connect to Secure Access, and choose the device type this tunnel group will use.' There are three input fields: 'Tunnel Group Name' with the value 'FTD-BGP', 'Region' with a dropdown menu showing 'US (Pacific Northwest)', and 'Device Type' with a dropdown menu showing 'FTD'. At the bottom, there is a 'Cancel' button and a 'Next' button.

セキュアアクセス – ネットワークトンネルグループの一般設定

4. トンネルIDとパスフレーズを設定します。

- トンネルIDとパスフレーズを設定します。
- Nextをクリックします。

The screenshot shows the 'Add a Network Tunnel Group' configuration page, specifically the 'Tunnel ID and Passphrase' tab. The left sidebar has four steps: 1. General Settings, 2. Tunnel ID and Passphrase (selected), 3. Routing, and 4. Data for Tunnel Setup. The main content area is titled 'Tunnel ID and Passphrase' and includes instructions: 'Configure the tunnel ID and passphrase that devices will use to connect to this tunnel group.' There are two radio buttons for 'Tunnel ID Format': 'Email' (selected) and 'IP Address'. Below this is a 'Tunnel ID' input field with the value 'ftdbgpvpn' and a placeholder '@<org><hub>.sse.cisco.com'. There is a 'Passphrase' input field with a 'Show' button. Below the passphrase field is a note: 'The passphrase must be between 16 and 64 characters long. It must include at least one upper case letter, one lower case letter, one number, and cannot include any special characters.' There is a 'Confirm Passphrase' input field with a 'Show' button. At the bottom, there is a 'Cancel' button, a 'Back' button, and a 'Next' button.

5. ルーティングの設定

- デバイスAS番号の設定
- [Save] をクリックします。

The screenshot displays the 'Routing' configuration page. On the left, a sidebar shows three steps: 'Tunnel ID and Passphrase', 'Routing' (selected), and 'Data for Tunnel Setup'. The main content area is titled 'Internet Protocol Version Setting for Routing' and includes a checkbox for 'Enable IPv6 Routing in addition to IPv4'. Below this, the 'Routing option' section has two radio buttons: 'Static routing' and 'Dynamic routing' (selected). The 'Device AS Number' field is a text input containing '65010'. An 'Advanced Settings' section is expanded, showing three checkboxes: 'Multihop BGP', 'Override BGP route summarization', and 'Block default route advertisement'. At the bottom, there are 'Back' and 'Save' buttons.

Tunnel ID and Passphrase

Routing

4 Data for Tunnel Setup

Internet Protocol Version Setting for Routing

☐ Enable IPv6 Routing in addition to IPv4
IPv4 is enabled by default.

Routing option

☐ Static routing
Use this option to manually add IP address ranges for this tunnel group.

☒ Dynamic routing
Use this option when you have a BGP peer for your on-premise router.

Device AS Number

65010

Advanced Settings

☐ Multihop BGP
Select this option to enable the ability for BGP peers to establish a connection (hop) when not directly connected.

☐ Override BGP route summarization
By default, advertised routes are summarized using the configured summary subnets in the Route Summarization page. Select this option to override route summarization.

☐ Block default route advertisement
Select to block the advertisement of the default route.

Cancel

Back Save

6. ネットワークトンネルグループ設定の保存

← Network Tunnel Groups

Add a Network Tunnel Group

Add a network tunnel group to Secure Access and enable secure network connections to the internet and private resources. Select one of your organization's available network devices to establish this network tunnel group connection. [Help](#)

✓ General Settings

✓ Tunnel ID and Passphrase

✓ Routing

✓ Data for Tunnel Setup

Data for Tunnel Setup

Review and save the following information for use when setting up your network tunnel devices. This is the only time that your passphrase is displayed.

Primary Tunnel ID:	ftdbgpvpn@		
Primary Data Center IP Address:	44.228.138.150		2603:5004:13:20e::110:1
Secondary Tunnel ID:	ftdbgpvpn@		
Secondary Data Center IP Address:	52.35.201.56		2603:5004:13:20c::110:1
Passphrase:			

Download CSV

Done

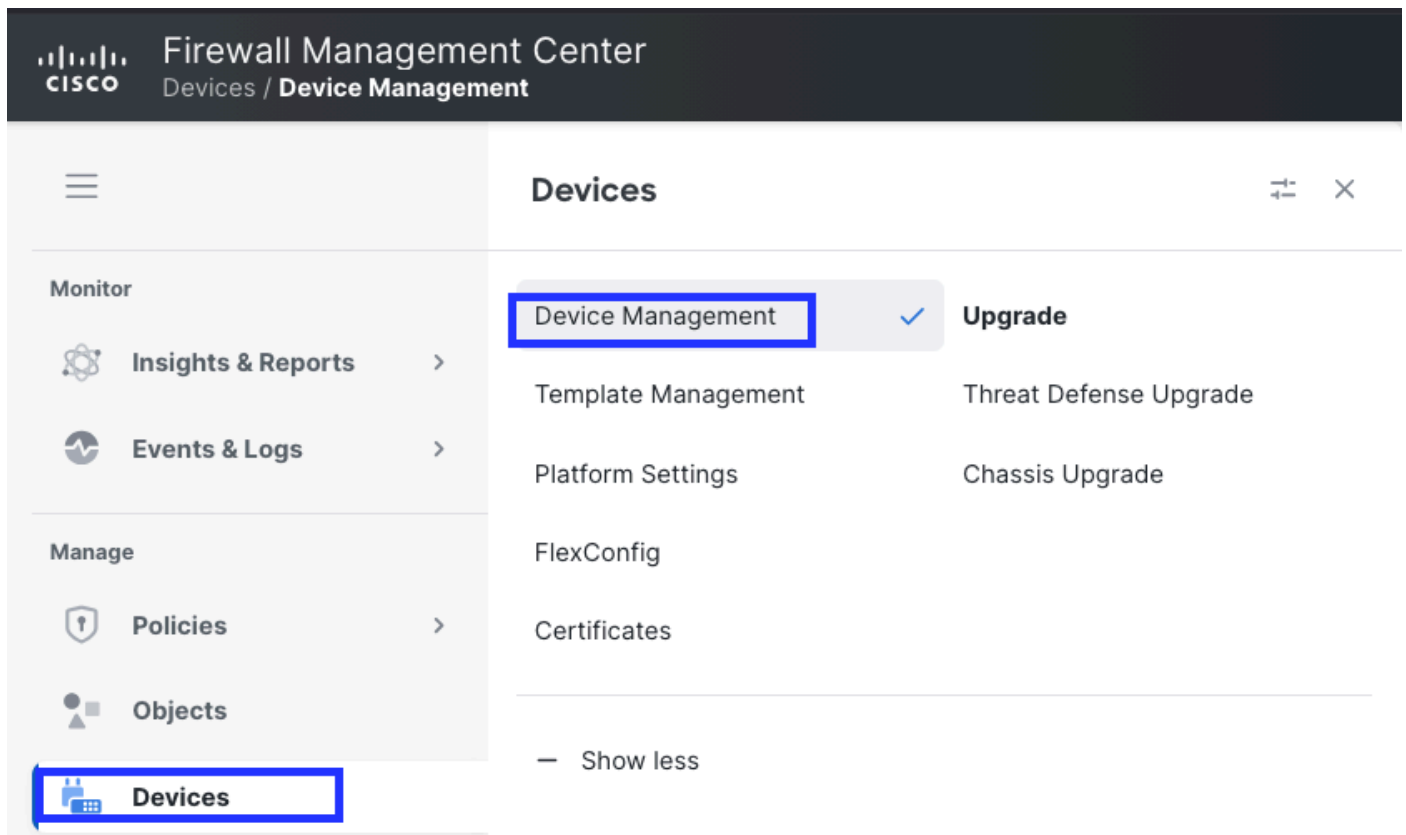
セキュアアクセス – ネットワークトンネルグループ

PBRを使用したSecure Firewall Threat Defense(FTD)でのダイナミックルートベースIPsec VPNの設定

1. ファイアウォール管理センター(FMC)へのログイン

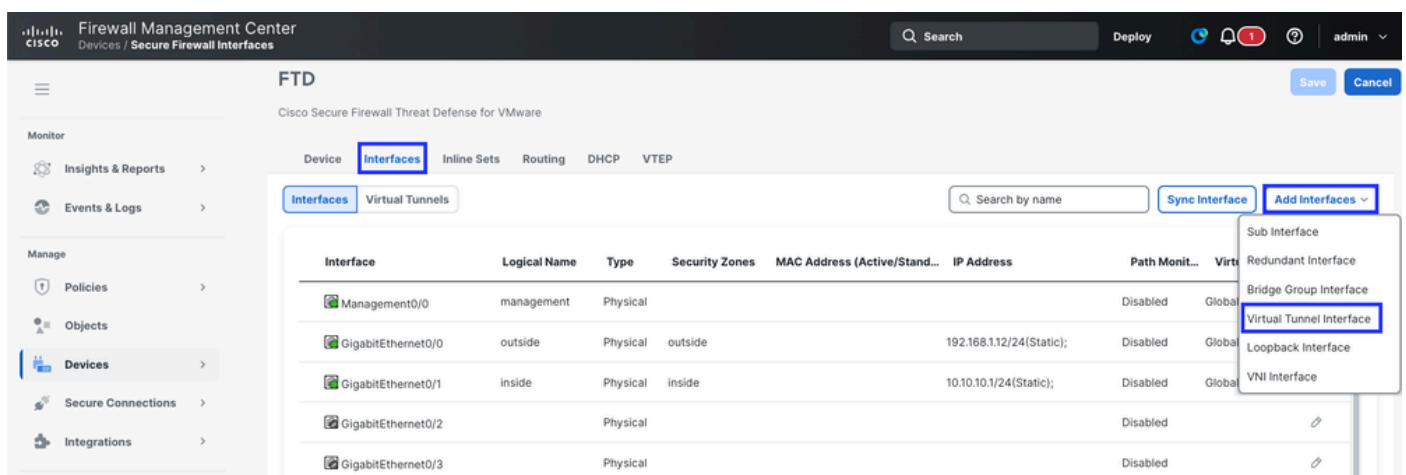
2. 仮想トンネルインターフェイスVTIの設定

- Devices > Device Managementに移動します



セキュアファイアウォール管理 – ダッシュボード

- デバイスの横にある鉛筆アイコンをクリックし、インターフェイスセクションに移動します。
- Add interfacesをクリックして、Virtual Tunnel Interfaceを選択します。



セキュアファイアウォール管理 : FTD VTIの設定

- VTIの設定

Add Virtual Tunnel Interface



General

Path Monitoring

Tunnel Type

☒ Static ☐ Dynamic

Name:*

VTI-1

☒ Enabled

Description:

Virtual Tunnel interface for
Primary VTI VPN

Security Zone:

vti

Priority:

0

(0 - 65535)

Propagate Security Group Tag: ☒

Virtual Tunnel Interface Details

An interface named Tunnel<ID> is configured. Tunnel Source is a physical interface where VPN tunnel terminates for the VTI.

Tunnel ID:*

1

(0 - 10413)

Virtual Tunnel Interface Details

An interface named Tunnel<ID> is configured. Tunnel Source is a physical interface where VPN tunnel terminates for the VTI.

Tunnel ID:*

1 (0 - 10413)

Tunnel Source:*

GigabitEthernet0/0 (outside) 192.168.1.12

IPsec Tunnel Details

IPsec Tunnel mode is decided by VPN traffic IP type. Configure IPv4 and IPv6 addresses accordingly.

IPsec Tunnel Mode:*

☒ IPv4 ☐ IPv6

IP Address:*

☒ Configure IP 169.254.2.1/30 ⓘ

☐ Borrow IP (IP unnumbered) Select Interface +

Cancel

OK

セキュアファイアウォール管理 : FTD VTIの設定

- セキュアアクセスを使用したセカンダリIPsec VPNに対してもVTI-2を設定します。

FTD Cisco Secure Firewall Threat Defense for VMware

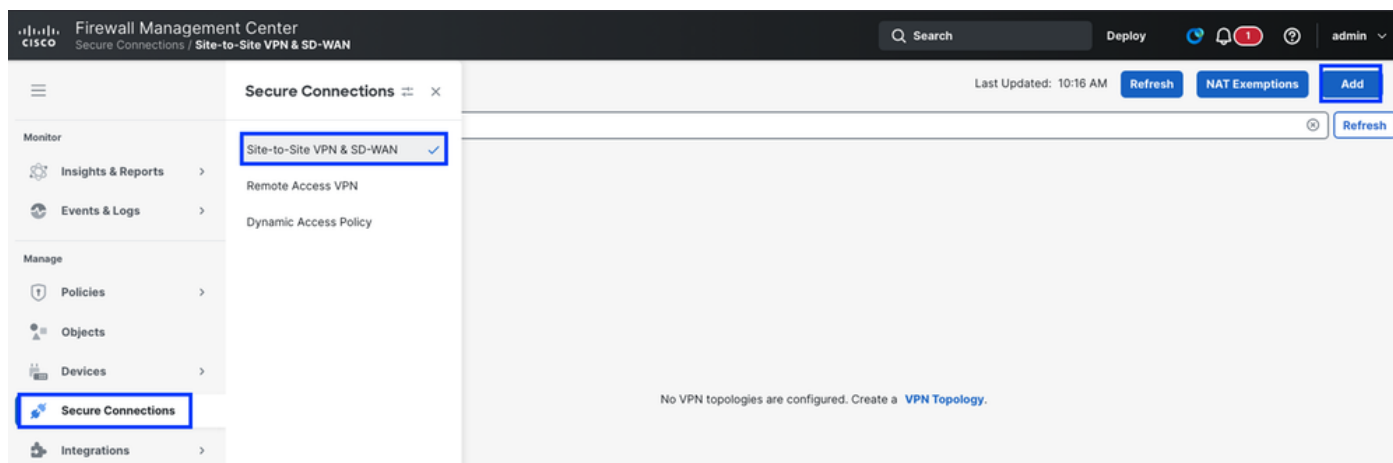
Device Interfaces Inline Sets Routing DHCP VTEP

Interfaces Virtual Tunnels

Search by name Sync Interface Add interfaces

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Stand...	IP Address	Path Monit...	Virtual Router
Management0/0	management	Physical				Disabled	Global
GigabitEthernet0/0	outside	Physical	outside		192.168.1.12(Static);	Disabled	Global
Tunnel1	VTI-1	VTI	vti		169.254.2.1/30(Static);	Disabled	Global
Tunnel2	VTI-2	VTI	vti		169.254.2.5/30(Static);	Disabled	Global
GigabitEthernet0/1	inside	Physical	inside		10.10.10.1/24(Static);	Disabled	Global

3. Secure Connections > Site-to-Site VPN & SD-WANの順に移動し、AddをクリックしてVPNを設定します



- VPNトポロジの作成

Create VPN Topology ?

Topology Name *

SecureAccess-VPN-Primary

VPN Type

☐ SD-WAN Topology

Simplifies and automates the VPN and routing configuration in a hub and spoke topology, enabling SD-WAN capabilities.

Select VPN Topology

☐ ☒ Hub and Spoke

Prerequisites

New

☒ Route-Based VPN

Secures traffic dynamically between peers based on routing over Virtual Tunnel Interfaces.

Select VPN Topology

☐ ☒ Hub and Spoke

☐ ☒ Peer to Peer

☐ Policy-Based VPN

Secures traffic between peers based on a static policy using protected networks.

Select VPN Topology

☐ ☒ Hub and Spoke

☐ ☒ Peer to Peer

☐ Full Mesh

☐ SASE Topology

! SASE Topology cannot be selected because Cisco Umbrella Connection is not configured.

Prerequisites

Refresh

Cancel Create

- 「セキュアアクセスでのネットワークトンネルグループの設定」のステップ6で、プライマ

りおよびセカンダリデータセンターのトンネルIDとIPアドレスを取得します。

- エンドポイントをクリック
- ノードAでDeviceをクリックし、FTDデバイスを選択します
- Virtual Tunnel Interfaceをクリックし、前の手順で作成した最初のVTIインターフェイスを選択します
- Send Local Identity to Peersオプションをクリックして、Email IDを選択し、プライマリトンネルIDを入力します (Secure AccessのConfigure Network Tunnel Groupの下の「Save Network Tunnel Group Configuration」のセクションを参照)。
- ノードBでDeviceをクリックし、Extranetを選択します
- Device Nameをクリックして、名前を付けます
- Endpoint IP Addressesをクリックし、Secure AccessのプライマリIPアドレスとセカンダリIPアドレスをカンマで区切って入力します (Secure AccessのConfigure Network Tunnel Groupの下のSave Network Tunnel Group Configurationから)
- Add Backup VTIをクリックします。
- Virtual Tunnel Interfaceをクリックし、前の手順で作成した2番目のVTIインターフェイスを選択します
- Send Local Identity to Peersオプションをクリックして、Email IDを選択し、セカンダリトンネルIDを入力します (「Configure Network Tunnel Group on Secure Access」の「Save Network Tunnel Group Configuration」の下)
- [Save] をクリックします。

Edit VPN Topology



Topology Name:*

SecureAccess-VPN-Primary

☐ Policy Based (Crypto Map)

☒ Route Based (VTI)

Network Topology:

Point to Point

Hub and Spoke

Full Mesh

IKE Version:*

☐

IKEv1

☒

IKEv2

Endpoints

IKE

IPsec

Advanced

Node A

Device:*

FTD

Virtual Tunnel Interface:*

VTI-1 (IP: 169.254.2.1)



Tunnel Source: outside (IP: 192.168.1.12) [Edit VTI](#)

☐ Tunnel Source IP is Private

☒ Send Local Identity to Peers

Local Identity Configuration:*

Email ID

ftdbgpvpn(

Node B

Device:*

Extranet

Device Name:*

Secure Access

Endpoint IP Address:*

44.228.138.150,52.35.201.56

Cancel

Save

セキュアFTD:VPNエンドポイントの設定

Edit VPN Topology



Topology Name:*

SecureAccess-VPN-Primary

☐ Policy Based (Crypto Map)

☒ Route Based (VTI)

Network Topology:

Point to Point

Hub and Spoke

Full Mesh

IKE Version:*

☐ IKEv1

☒ IKEv2

Endpoints

IKE

IPsec

Advanced

Backup VTI:

[Remove](#)

Virtual Tunnel Interface:*

VTI-2 (IP: 169.254.2.5)



Tunnel Source: outside (IP: 192.168.1.12) [Edit VTI](#)

☐ Tunnel Source IP is Private

☒ Send Local Identity to Peers

Local Identity Configuration:*

Email ID

tdbgpvpn@

22-

Additional
Configuration



Route traffic to the VTI : [Routing Policy](#)

Permit VPN traffic : [AC Policy](#)

Cancel

Save

セキュアFTD:VPNエンドポイントの設定

- [サポートされているIPsecパラメータ](#)に従ったIKEv2設定
 - ポリシーとしてUmbrella-AES-GCM-256を選択します。
 - 認証タイプとしてPre-Shared Manual Keyを選択します。

Edit VPN Topology



Topology Name:*

SecureAccess-VPN-Primary

☐ Policy Based (Crypto Map) ☒ Route Based (VTI)

Network Topology:

Point to Point

Hub and Spoke

Full Mesh

IKE Version:*



IKEv1



IKEv2

Endpoints

IKE

IPsec

Advanced

IKEv2 Settings

Policies:*

Umbrella-AES-GCM-256

Authentication Type:

Pre-shared Manual Key

Key:*

.....

Confirm Key:*

.....

☐ Enforce hex-based pre-shared key only

Cancel

Save

セキュアFTD:VPN IKEの設定

- IPSecの設定
 - IKEv2 IPsec Proposals as Umbrella-AES-GCM-256を選択します
 - select Modulus GroupとしてPFSを20に有効化

Edit VPN Topology



Topology Name:*

SecureAccess-VPN-Primary

☐ Policy Based (Crypto Map)

☒ Route Based (VTI)

Network Topology:

Point to Point

Hub and Spoke

Full Mesh

IKE Version:*

☐ IKEv1

☒ IKEv2

Endpoints

IKE

IPsec

Advanced

Transform Sets: IKEv1 IPsec Proposals IKEv2 IPsec Proposals*

tunnel_aes256_sha

Umbrella-AES-GCM-...

☐ Enable Security Association (SA) Strength Enforcement

☒ Enable Perfect Forward Secrecy

Modulus Group:

20

Cancel

Save

セキュアFTD:VPN IPsecの設定

- 高度な設定
- [Save] をクリックします。

Edit VPN Topology



Topology Name:*

SecureAccess-VPN-Primary

☐ Policy Based (Crypto Map) ☒ Route Based (VTI)

Network Topology:

Point to Point

Hub and Spoke

Full Mesh

IKE Version:*



IKEv1



IKEv2

Endpoints

IKE

IPsec

Advanced

IPsec

Tunnel

IKE Keepalive:

Enable

Threshold:

10

Seconds

(Range 10 - 3600)

Retry Interval:

2

Seconds

(Range 2 - 10)

Identity Sent to Peers:

autoOrDN

Peer Identity Validation:

Do not check

Cancel

Save

セキュアFTD:VPNの詳細設定

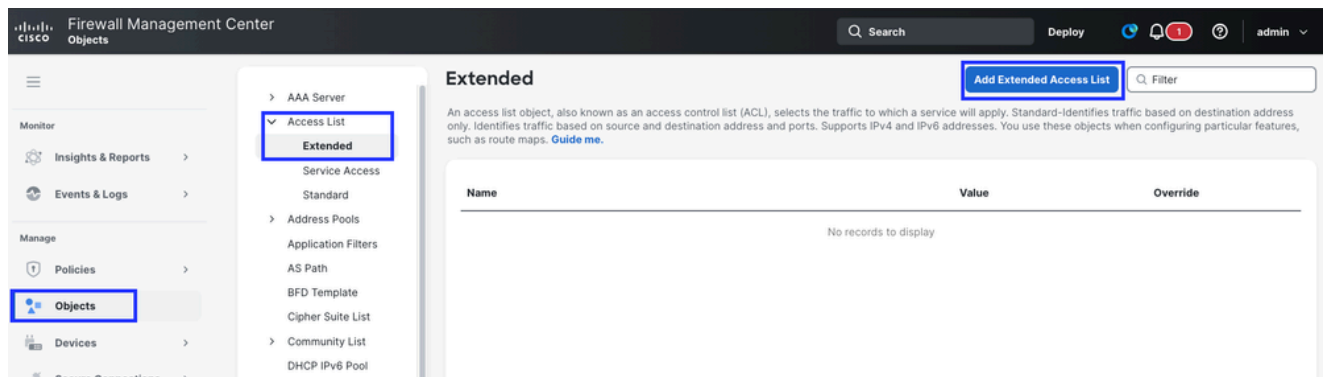
FTDポリシーベースルーティング

従来のルーティングでは、パケットは宛先IPアドレスに基づいてルーティングされます。宛先ベースのルーティングシステムで特定のトラフィックのルーティングを変更することは困難です。ポリシーベースルーティング(PBR)は、ルーティングプロトコルによって提供されるメカニズムを拡張および補完し、ルーティングをより詳細に制御できるようにします。

PBRでは、IP優先順位を設定できます。また、高コストリンク上のプライオリティトラフィックなど、特定のトラフィックのパスを指定することもできます。PBRを使用すると、送信元ポート、宛先アドレス、宛先ポート、プロトコル、アプリケーション、またはこれらのオブジェクトの組み合わせなど、宛先ネットワーク以外の基準に基づいてルーティングを定義できます。詳細については、『[ポリシーベースルーティング\(PBR\)](#)』を参照してください。

1. アクセスリストの設定

- Objects > Access List > Extendedの順に移動します。
- Add Extended Access Listをクリックします。



セキュアFTD：拡張アクセスリスト

- アクセスリスト名の指定
- アクションの定義
 - allow です。 – 定義されたトラフィックはIPSecトンネルに送信されます
 - ブロック：トラフィックはIPSecトンネルからバイパスされる
 - ルールはシーケンス番号に基づいて照合される（下位から上位）
 - Addをクリックします。
 - [Save] をクリックします。

Add Extended Access List Entry

Action: Allow
 Logging: Default
 Log Level: Informational
 Log Interval: 300 Sec.

Network Port Application Users Security Group Tag

Available Networks +
 10.10.10.
 obj_10.10.10.0

Add to Source
 Add to Destination

Source Networks (1)
 obj_10.10.10.0

Destination Networks (0)
 any

Cancel Add

セキュアFTD：拡張アクセスリスト

New Extended Access List Object

Name
PBR

Entries (1)

Sequence	Action	Source	Source Port	Destination	Destination Port	Application	Users	SGT
1	Allow	obj_10.10.10.0	Any	Any	Any	Any	Any	

Displaying 1 - 1 of 1 rows < < Page 1 of 1 > >

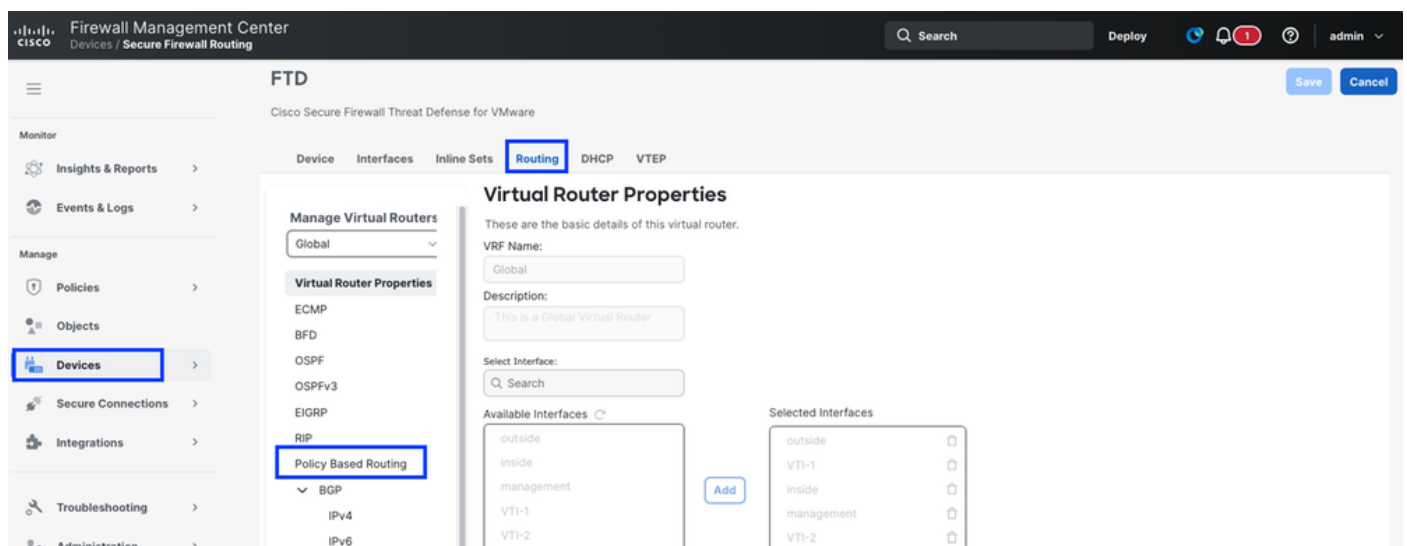
☐ Allow Overrides

Cancel Save

セキュアFTD：拡張アクセスリスト

2. ポリシーベースルーティングの設定

- Devices > Device Management > FTD > Routingの順に移動します。



セキュアなFTD：ポリシーベースルーティング

- Addをクリックします。
- Ingress Interfaceの選択：アクセスリストで定義したサブネットの入カインターフェイス

Add Policy Based Route



A policy based route consists of ingress interface list and a set of match criteria associated to egress interfaces

Ingress Interface *

Match Criteria and Egress Interface

Specify forward action for chosen match criteria.

Add

There are no forward-actions defined yet. Start by [defining the first one](#).

Cancel

Save

セキュアなFTD：ポリシーベースルーティング

- 一致基準と出カインターフェイスの定義
 - Addをクリックします。
 - Match ACLを選択します。
 - IPアドレスとしてSend toを選択します。
 - ネクストホップIPアドレスを追加します。 - VTIインターフェイスのIPアドレスはです。 169.254.2.130および169.254.2.5/30.したがって、VTI-1とVTI-2のネクストホップIPアドレスは169.254.2.2であり、それぞれ169.254.2.6
 - [Save] をクリックします。

Add Forwarding Actions

Match ACL: * +

Send To: *

IPv4 Addresses:

IPv6 Addresses:

Don't Fragment:

☐ Default Interface

IPv4 settings

IPv6 settings

Recursive:

Default:

☐ Peer Address

Cancel

Save

セキュアなFTD：ポリシーベースルーティング

FTD

You have unsaved changes

SaveCancel

Cisco Secure Firewall Threat Defense for VMware

DeviceInterfacesInline SetsRoutingDHCPVTEP

Manage Virtual Routers

Global

Virtual Router Properties

ECMP

BFD

OSPF

OSPFv3

EIGRP

RIP

Policy Based Routing

BGP

Policy Based Routing

Specify ingress interfaces, match criteria and egress interfaces to route traffic accordingly. Traffic can be routed across Egress interfaces accordingly

Configure Interface Priority

Add

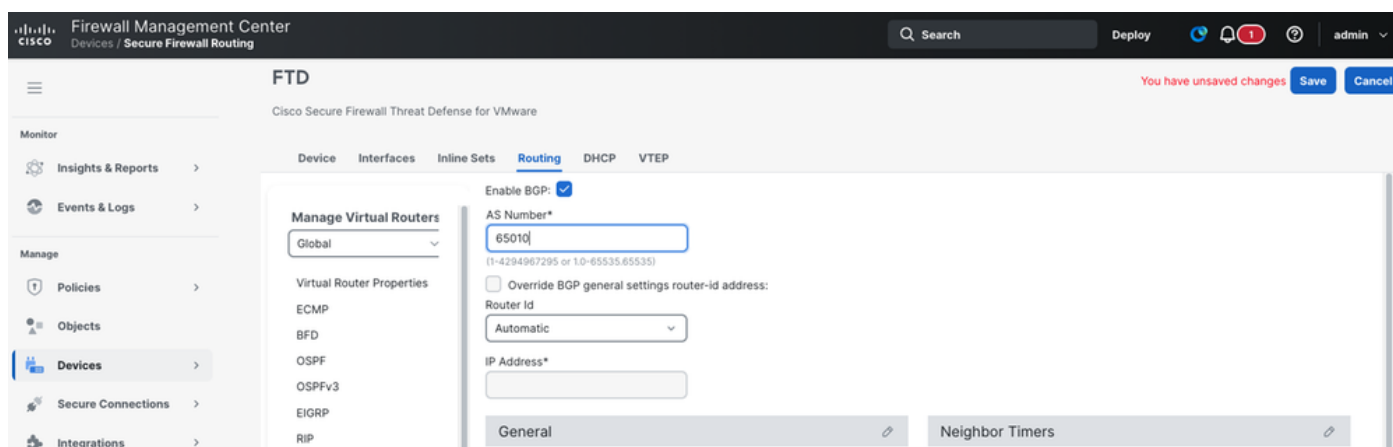
Ingress Interfaces	Match criteria and forward action	
inside	If traffic matches the Access List PBR Send through 169.254.2.2 169.254.2.6	

セキュアなFTD：ポリシーベースルーティング

FTDでのBGPの設定

1. BGPの有効化

- Devices > Device Management > FTD > Routing > General Settings > BGPの順に移動します。
- BGPを有効にし、AS番号 (FTDローカルAS番号) を追加します。
- [Save] をクリックします。



セキュアFTD:BGPルーティング

- BGP > IPv4の順に移動します。

2. BGP ネイバーを追加します。セキュアアクセスBGPピアは169.254.0.5およびです。
169.254.0.9

Add Neighbor



IP Address*

169.254.0.5

Remote AS*

64512

(1-4294967295 or 1.0-65535.65535)

☒ Enabled address

☐ AS Override

☐ Shutdown administratively

☐ Configure graceful restart (failover/spanned mode)

☐ Enable graceful restart

BFD Fallover

none

Description

Update Source:

Filtering Routes

Routes

Timers

Advanced

Migration

☐ Enable Authentication

Enable Encryption

0

Password

Confirm Password

☐ Send Community attribute to this neighbor

☐ Use itself as next hop for this neighbor

☐ Disable Connection Verification

☐ Allow connections with neighbor that is not directly connected

☒ Limited number of TTL hops to neighbor

TTL Hops

254

(1-254)

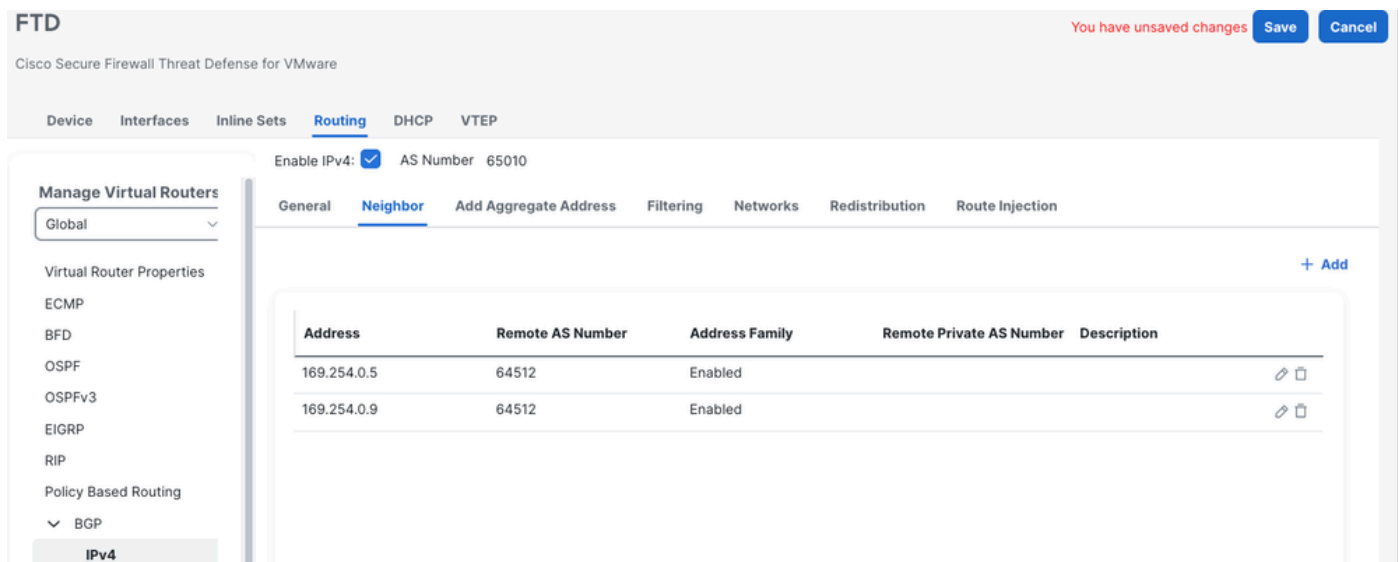
☐ Use TCP path MTU discovery

TCP Transport Mode

Cancel

OK

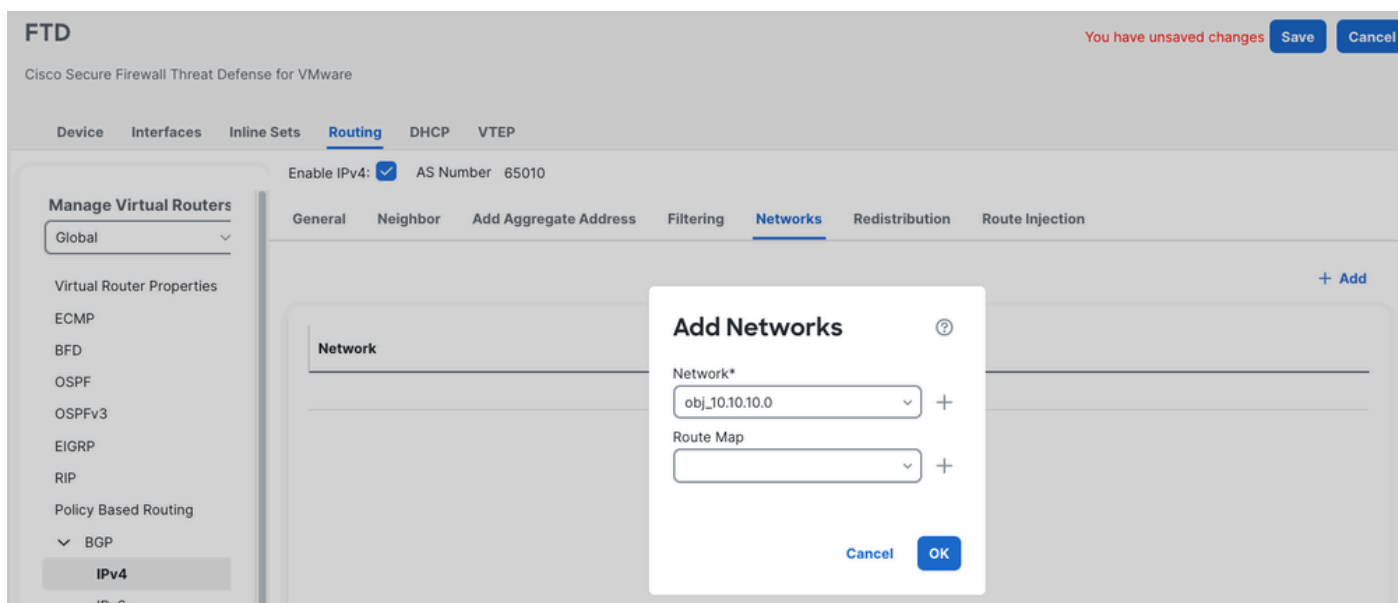
セキュアFTD:BGPルーティング



セキュアFTD:BGPルーティング

3. ネットワークを追加する – アクセスを保護するためにアドバタイズする必要があるネットワーク

- [OK] をクリックします。

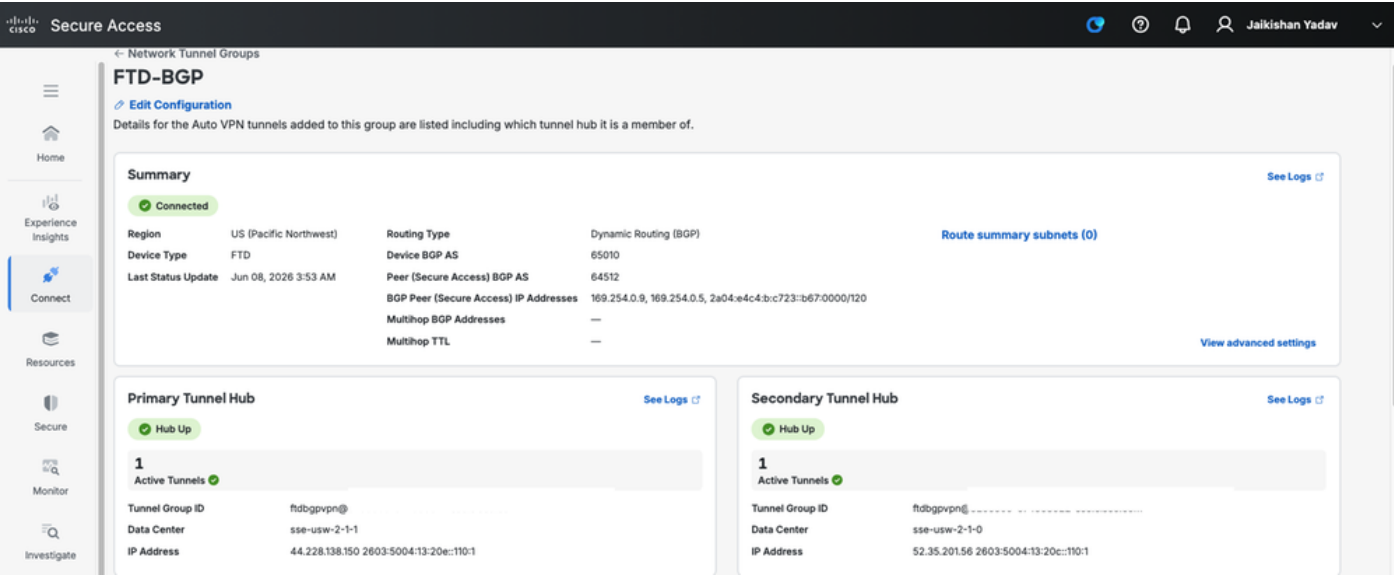


セキュアFTD:BGPルーティング

- 変更を保存して展開する

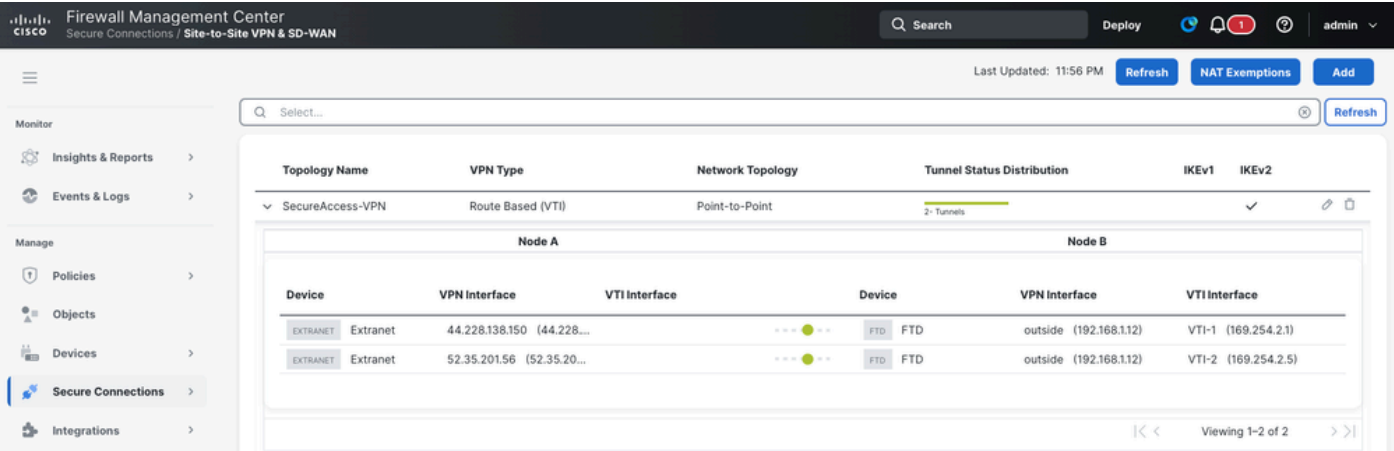
トンネルステータスの確認

セキュアアクセス



セキュアFTD:IPsecトンネルステータス

FMC上



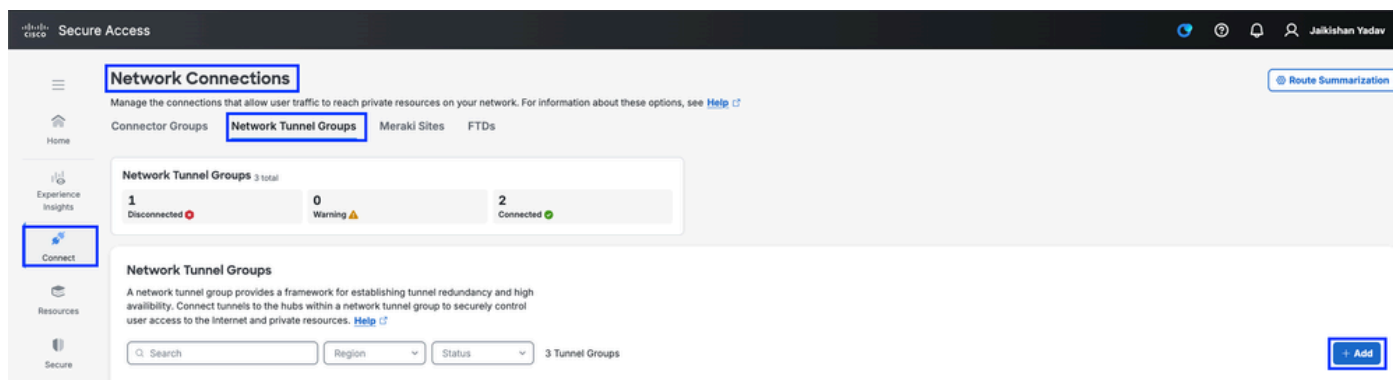
セキュアFMC:IPsecトンネルステータス

PBRを使用した適応型セキュリティアプライアンス(ASA)でのスタティックルータベースIPsec VPNの設定

セキュアアクセスでのVPN設定

- 1.セキュアアクセスダッシュボードへのログイン[セキュアアクセス](#)
2. Connect > Network Connections > Network Tunnel Groupsの順に移動し、+Addをクリックして

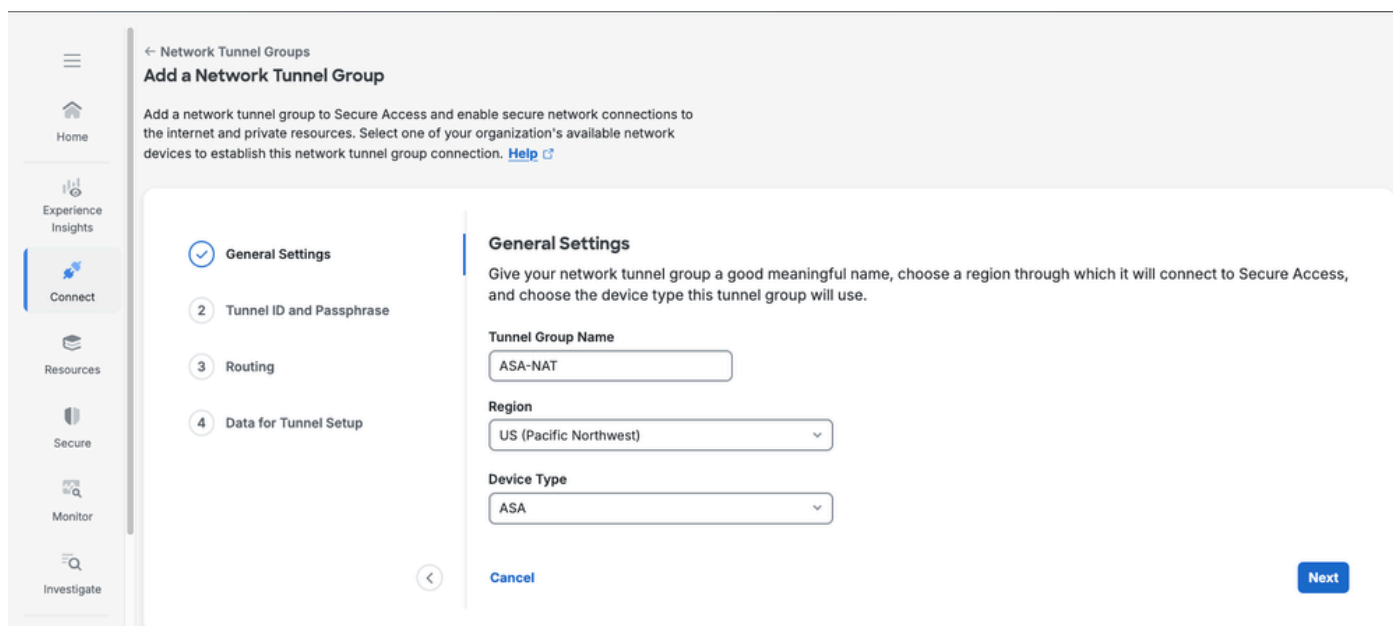
ネットワークトンネルグループを設定します



セキュアアクセス – ネットワークトンネルグループ

3. ネットワークトンネルグループの構成 – 一般設定

- トンネルグループの名前、リージョン、およびデバイスタイプの設定
- [Next] をクリックします。



セキュアアクセス – ネットワークトンネルグループの一般設定

4. トンネルIDとパスフレーズを設定します。

- トンネルIDとパスフレーズを設定します。
- Nextをクリックします。

← Network Tunnel Groups

Add a Network Tunnel Group

Add a network tunnel group to Secure Access and enable secure network connections to the internet and private resources. Select one of your organization's available network devices to establish this network tunnel group connection. [Help](#)

General Settings

Tunnel ID and Passphrase

Routing

Data for Tunnel Setup

Tunnel ID and Passphrase

Configure the tunnel ID and passphrase that devices will use to connect to this tunnel group.

Tunnel ID Format

☒ Email ☐ IP Address

Tunnel ID

asahomevpn @<org><hub>.sse.cisco.com

Passphrase

..... [Show](#)

The passphrase must be between 16 and 64 characters long. It must include at least one upper case letter, one lower case letter, one number, and cannot include any special characters.

Confirm Passphrase

..... [Show](#)

[Cancel](#) [Back](#) [Next](#)

セキュアアクセス – ネットワークトンネルグループ

5. ネットワークアドレス変換(NAT)の有効化

← Network Tunnel Groups

Add a Network Tunnel Group

Add a network tunnel group to Secure Access and enable secure network connections to the internet and private resources. Select one of your organization's available network devices to establish this network tunnel group connection. [Help](#)

General Settings

Tunnel ID and Passphrase

Routing

Data for Tunnel Setup

Routing options and network overlaps

Configure routing options for this tunnel group.

☒ **Network Address Translation (NAT)**

Select to add NAT mapping configurations that resolve overlapping subnet IP address ranges, including networks with conflicting IP address spaces.

Source Mappings

Site → Secure Access ⓘ

Source NAT

All source IP addresses translate to range:

100.96.0.0/16

☐ Translate to Secure Access NAT subnet

Secure Access → Site ⓘ

Source NAT

Add a destination mapping to enable this rule

Destination NAT Mappings

Name	Direction ⓘ	Original CIDR	Translated CIDR	...
ⓘ Configure full bi-directional granular control over destination IP address translation. + Add Mappings				

Internet Protocol Version Setting for Routing

☐ Enable IPv6 Routing in addition to IPv4

[Cancel](#) [Back](#) [Save](#)

セキュアアクセス – ネットワークトンネルグループのNAT設定

6. 宛先NATマッピングの追加

フロー1： ルータ1からルータ2 (アクセスを保護するサイト)

フロー2 – ルータ2からルータ1 (サイトへのセキュアなアクセス)

Network Tunnel Groups

Add a Network Tunnel Group

Add a network tunnel group to Secure Access and enable secure network connections to the internet and private resources. Select one of your organization's available network devices to establish this network tunnel group connection. [Help](#)

- General Settings
- Tunnel ID and Passphrase
- Routing**
- Data for Tunnel Setup

Routing options and network overlaps

Configure routing options for this tunnel group.

☒ **Network Address Translation (NAT)**

Select to add NAT mapping configurations that resolve overlapping subnet IP address ranges, including networks with conflicting IP address spaces.

Source Mappings

Site to Secure Access

Source NAT

All source IP addresses translate to range:

100.96.0.0/16

☒ Translate to Secure Access NAT subnet

Secure Access to Site

Source NAT

Add a destination mapping to enable this rule

Destination NAT Mappings

Name	Direction	Original CIDR	Translated CIDR	
ASA-To-FTD	Site to Secure Access	10.10.10.102/32	192.168.10.102/32	☒

[+ Add Mappings](#)

Internet Protocol Version Setting for Routing

☒ Enable IPv6 Routing in addition to IPv4

セキュアアクセス – ネットワークトンネルグループのNAT設定



注意:NATが有効な場合、BGPは使用できません (BGPが有効な場合)。また、カスタマーエッジデバイスでもスタティックVPNを設定します



ヒント：常に、変換されたIP (宛先IP) に対してpingを実行することを忘れないでください。

変換後のIPは変換後のCIDRに配置され、実際のIPは元のCIDRに配置されます。

← Network Tunnel Groups

Add a Network Tunnel Group

Add a network tunnel group to Secure Access and enable secure network connections to the internet and private resources. Select one of your organization's available network devices to establish this network tunnel group connection. [Help](#)

General Settings

Tunnel ID and Passphrase

Routing

4 Data for Tunnel Setup

Routing options and network overlaps

Configure routing options for this tunnel group.

☒ **Network Address Translation (NAT)**

Select to add NAT mapping configurations that resolve overlapping subnet IP address ranges, including networks with conflicting IP address spaces.

Source Mappings

Site → Secure Access ⓘ
Source NAT

All source IP addresses translate to range:

☐ Translate to Secure Access NAT subnet

Secure Access → Site ⓘ
Source NAT

All source IP addresses translate to range:

☐ Translate to Secure Access NAT subnet

Destination NAT Mappings

Name	Direction ⓘ	Original CIDR	Translated CIDR	
> ASA-To-FTD	Site → Secure Access	10.10.10.102/32	→ 192.168.10.102/32	ⓘ ⌵
> FTD-To-ASA	Secure Access → Site	10.10.10.101/32	→ 172.16.10.101/32	ⓘ ⌵

Rows per page

[+ Add Mappings](#)

Internet Protocol Version Setting for Routing

[Cancel](#) [Back](#) [Save](#)

セキュアアクセス－ネットワークトンネルグループのNAT設定

クリック 保存します。



ヒント: 「サイトA」から「サイトB」に送信されるトラフィックの場合、CNHE-1の観点から見た方向は「サイト→セキュアアクセス」です。

「サイトB」から「サイトA」に送信されるトラフィックの場合、CNHE-1の観点から見ると、方向は「SecureAccess→Site」です。

ASAでのVPNの設定

1. ASA CLIにログインし、イネーブルモードに入り、インターネットへの基本的なIP接続を確認します

ASA# sh ip

システムIPアドレス:

インターフェイス名IPアドレスサブネットマスク方式

GigabitEthernet0/0 outside 192.168.1.40 255.255.255.0 マニュアル

10.10.10.1 255.255.255.0 マニュアル内のGigabitEthernet0/1

現在のIPアドレス:

インターフェイス名IPアドレスサブネットマスク方式

GigabitEthernet0/0 outside 192.168.1.40 255.255.255.0 マニュアル

10.10.10.1 255.255.255.0 マニュアル内のGigabitEthernet0/1

ASA# ping 8.8.8.8

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 20/28/30 ms

ASA番号

2. IKEv2ポリシーを設定し、外部インターフェイスでIKEv2を有効にします

クリプトikev2ポリシー10

暗号化aes-gcm-256

整合性 NULL

group 19

ライフタイム秒数86400

crypto ikev2 enable outside

3. IPSecプロポーザルの設定

crypto ipsec ikev2 ipsec-proposal Ipsec-Proposal-primary

protocol esp encryption aes-gcm-256

4. IPsecプロファイルの設定

crypto ipsec profile csa-profile-primary (暗号化IPSecプロファイルのCSAプロファイルのプライマリ)

set ikev2 ipsec-proposal Ipsec-Proposal-primary

set ikev2 local-identity email-id <primary tunnel-id>

5. グループポリシーを設定し、attributeでIKEv2プロトコルを有効にします。

group-policy csa-policy-primary internalコマンド

group-policy csa-policy-primary属性

vpn-tunnel-protocol ikev2

6. トンネルグループを設定します。

tunnel-group 44.228.138.150 type ipsec-l2l

tunnel-group 44.228.138.150一般属性

デフォルト : グループポリシーcsa-policy-primary
tunnel-group 44.228.138.150 ipsec属性
ikev2 remote-authentication pre-shared-key <事前共有キー>
ikev2 local-authentication pre-shared-key <事前共有キー>

7. 仮想トンネルインターフェイス(VTI)の設定

- Nameifは任意の場合に使用できます
- VTIに割り当てられたIPアドレスがASAの他のインターフェイスと重複しないようにしてください
- Tunnel sourcemustbe : ファイアウォールのOutsideインターフェイス。
- トンネルの宛先は、データセンターのIPアドレスである必要があります

```
interface Tunnel1
nameif VTI-1
ip address 169.254.2.1 255.255.255.252
トンネル送信元インターフェイス外部
トンネルの宛先44.228.138.150
トンネルモードipsec ipv4
トンネル保護ipsecプロファイルcsa-profile-primary
```

8. マッピングされたIPアドレスまたはサブネットへのトラフィックがVTIインターフェイス内でルーティングされるようにルーティングを設定します。ネクストホップは、VTIの範囲内のIPを使用する必要があります。

```
route VTI-1 0.0.0.0 0.0.0.0 169.254.2.2 5.(インターネットベースの場合、RAVPNプールまたはCGNATトラフィック
```

または

```
ルートVTI-1 172.16.10.101 255.255.255.255 169.254.2.2 5
```

ポリシーベースルーティング

1. アクセスリスト

```
access-list PBR extended permit ip 10.10.10.0 255.255.255.0 any
```

2. ルートマップ

```

route-map RM-CSA permit 10
IPアドレスPBRの照合
set ip next-hop 169.254.2.2 169.254.2.6

```

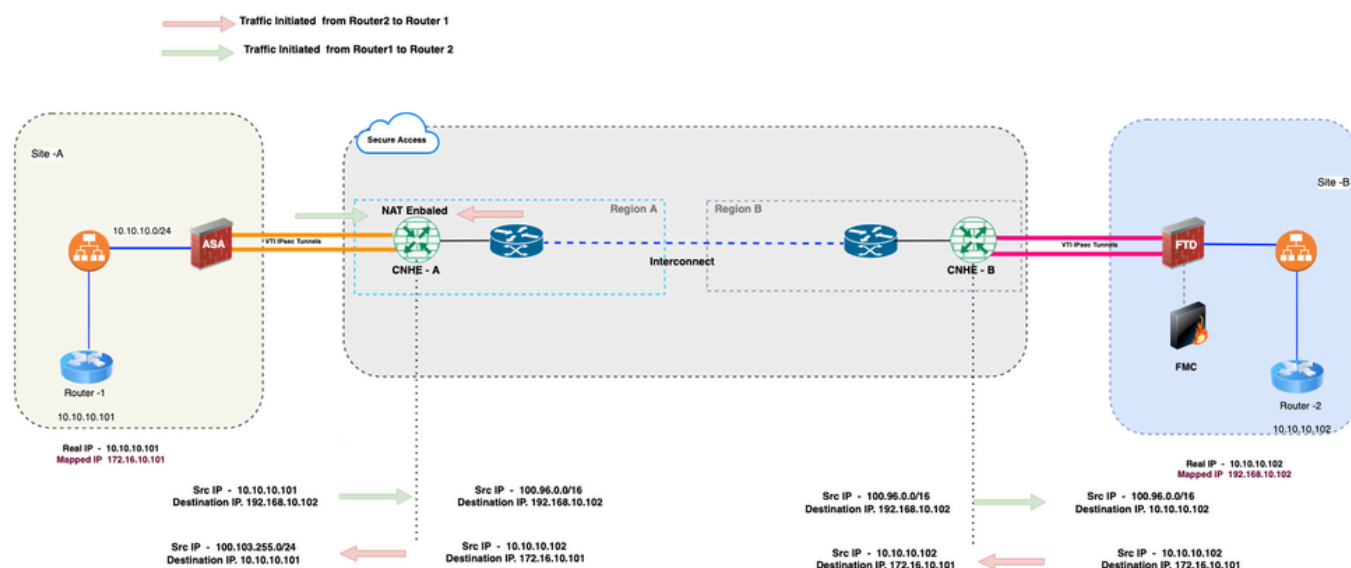
3. 入インターフェイスでルートマップを適用します。

```

interface GigabitEthernet0/1
nameif内部
セキュリティレベル100
ip address 10.10.10.1 255.255.255.0
policy-route route-map RM-CSA ( 使用可能な場合 )

```

確認



ルータインターフェイスおよびGW到達可能性ステータス

```

Router1#show ip interface brief
Interface          IP-Address      OK? Method Status      Protocol
GigabitEthernet1   192.168.1.101   YES NVRAM    down       down
GigabitEthernet2   10.10.10.101    YES NVRAM    up         up
GigabitEthernet3   unassigned      YES NVRAM    administratively down down
GigabitEthernet9   unassigned      YES unset   administratively down down
Router1#ping 10.10.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms

```

テスト1- Router2 → Router1。-ping テスト

```
Router1#ping 192.168.10.102
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.102, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 207/211/223 ms
Router1#
```

ASAでのパケットキャプチャ (ローカルFW)

```
ASA# sh capture
capture capin type raw-data trace interface inside [Capturing - 1300 bytes]
  match icmp any any
capture tunnel type raw-data trace interface vti-1 [Capturing - 1300 bytes]
  match icmp any any
capture asp type asp-drop all [Capturing - 0 bytes]
  match icmp any any
ASA#
ASA#
ASA# ter pag 20
ASA# sh cap capin

10 packets captured

  1: 10:56:45.024244      10.10.10.101 > 192.168.10.102 icmp: echo request
  2: 10:56:45.231143      192.168.10.102 > 10.10.10.101 icmp: echo reply
  3: 10:56:45.232470      10.10.10.101 > 192.168.10.102 icmp: echo request
  4: 10:56:45.441856      192.168.10.102 > 10.10.10.101 icmp: echo reply
  5: 10:56:45.443122      10.10.10.101 > 192.168.10.102 icmp: echo request
  6: 10:56:45.652477      192.168.10.102 > 10.10.10.101 icmp: echo reply
  7: 10:56:45.653423      10.10.10.101 > 192.168.10.102 icmp: echo request
  8: 10:56:45.875397      192.168.10.102 > 10.10.10.101 icmp: echo reply
  9: 10:56:45.876450      10.10.10.101 > 192.168.10.102 icmp: echo request
 10: 10:56:46.082301      192.168.10.102 > 10.10.10.101 icmp: echo reply
10 packets shown
ASA# sh cap tunnel

10 packets captured

  1: 10:56:45.024458      10.10.10.101 > 192.168.10.102 icmp: echo request
  2: 10:56:45.230914      192.168.10.102 > 10.10.10.101 icmp: echo reply
  3: 10:56:45.232516      10.10.10.101 > 192.168.10.102 icmp: echo request
  4: 10:56:45.441795      192.168.10.102 > 10.10.10.101 icmp: echo reply
  5: 10:56:45.443153      10.10.10.101 > 192.168.10.102 icmp: echo request
  6: 10:56:45.652432      192.168.10.102 > 10.10.10.101 icmp: echo reply
  7: 10:56:45.653454      10.10.10.101 > 192.168.10.102 icmp: echo request
  8: 10:56:45.875351      192.168.10.102 > 10.10.10.101 icmp: echo reply
  9: 10:56:45.876480      10.10.10.101 > 192.168.10.102 icmp: echo request
 10: 10:56:46.082240      192.168.10.102 > 10.10.10.101 icmp: echo reply
10 packets shown
```

FTD (リモートFW) でのパケットキャプチャ


```

ftd# sh cap
ftd# sh capture
capture vti type raw-data trace interface VTI-1 include-decrypted [Capturing - 1300 bytes]
  match icmp any any
capture capin type raw-data interface inside [Capturing - 1300 bytes]
  match icmp any any
capture asp type asp-drop all [Capturing - 0 bytes]
  match icmp any any
ftd# sh cap vti

```

10 packets captured

```

 1: 16:06:41.122292      100.96.2.0 > 10.10.10.102 icmp: echo request
 2: 16:06:41.124856      10.10.10.102 > 100.96.2.0 icmp: echo reply
 3: 16:06:41.329557      100.96.2.0 > 10.10.10.102 icmp: echo request
 4: 16:06:41.330442      10.10.10.102 > 100.96.2.0 icmp: echo reply
 5: 16:06:41.546327      100.96.2.0 > 10.10.10.102 icmp: echo request
 6: 16:06:41.547106      10.10.10.102 > 100.96.2.0 icmp: echo reply
 7: 16:06:41.752036      100.96.2.0 > 10.10.10.102 icmp: echo request
 8: 16:06:41.752814      10.10.10.102 > 100.96.2.0 icmp: echo reply
 9: 16:06:41.967891      100.96.2.0 > 10.10.10.102 icmp: echo request
10: 16:06:41.968501      10.10.10.102 > 100.96.2.0 icmp: echo reply

```

10 packets shown

```
ftd# sh cap capin
```

10 packets captured

```

 1: 16:06:41.123299      100.96.2.0 > 10.10.10.102 icmp: echo request
 2: 16:06:41.124825      10.10.10.102 > 100.96.2.0 icmp: echo reply
 3: 16:06:41.330000      100.96.2.0 > 10.10.10.102 icmp: echo request
 4: 16:06:41.330396      10.10.10.102 > 100.96.2.0 icmp: echo reply
 5: 16:06:41.546800      100.96.2.0 > 10.10.10.102 icmp: echo request
 6: 16:06:41.547090      10.10.10.102 > 100.96.2.0 icmp: echo reply
 7: 16:06:41.752448      100.96.2.0 > 10.10.10.102 icmp: echo request
 8: 16:06:41.752783      10.10.10.102 > 100.96.2.0 icmp: echo reply
 9: 16:06:41.968242      100.96.2.0 > 10.10.10.102 icmp: echo request
10: 16:06:41.968486      10.10.10.102 > 100.96.2.0 icmp: echo reply

```

10 packets shown

テスト2. - ルータ2 → ルータ1 pingテスト

```

Router2#sh ip int br
Interface                IP-Address      OK? Method Status      Protocol
GigabitEthernet1         unassigned      YES NVRAM    administratively down down
GigabitEthernet2         10.10.10.102    YES NVRAM    up          up
GigabitEthernet3         unassigned      YES NVRAM    administratively down down
Router2#ping 10.10.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms

```

FTDパケットキャプチャ (ローカルFW)

```

ftd# sh capture
capture vti type raw-data trace interface VTI-1 include-decrypted [Capturing - 1300 bytes]
  match icmp any any
capture capin type raw-data interface inside [Capturing - 1300 bytes]
  match icmp any any
capture asp type asp-drop all [Capturing - 0 bytes]
  match icmp any any
ftd#
ftd#
ftd#
ftd# sh cap vti

10 packets captured

  1: 16:11:45.622450      10.10.10.102 > 172.16.10.101 icmp: echo request
  2: 16:11:45.823825      172.16.10.101 > 10.10.10.102 icmp: echo reply
  3: 16:11:45.825762      10.10.10.102 > 172.16.10.101 icmp: echo request
  4: 16:11:46.045667      172.16.10.101 > 10.10.10.102 icmp: echo reply
  5: 16:11:46.046857      10.10.10.102 > 172.16.10.101 icmp: echo request
  6: 16:11:46.252321      172.16.10.101 > 10.10.10.102 icmp: echo reply
  7: 16:11:46.253572      10.10.10.102 > 172.16.10.101 icmp: echo request
  8: 16:11:46.453803      172.16.10.101 > 10.10.10.102 icmp: echo reply
  9: 16:11:46.454764      10.10.10.102 > 172.16.10.101 icmp: echo request
 10: 16:11:46.664119      172.16.10.101 > 10.10.10.102 icmp: echo reply
10 packets shown
ftd# sh cap capin

10 packets captured

  1: 16:11:45.622083      10.10.10.102 > 172.16.10.101 icmp: echo request
  2: 16:11:45.823886      172.16.10.101 > 10.10.10.102 icmp: echo reply
  3: 16:11:45.825442      10.10.10.102 > 172.16.10.101 icmp: echo request
  4: 16:11:46.045697      172.16.10.101 > 10.10.10.102 icmp: echo reply
  5: 16:11:46.046582      10.10.10.102 > 172.16.10.101 icmp: echo request
  6: 16:11:46.252352      172.16.10.101 > 10.10.10.102 icmp: echo reply
  7: 16:11:46.253313      10.10.10.102 > 172.16.10.101 icmp: echo request
  8: 16:11:46.453849      172.16.10.101 > 10.10.10.102 icmp: echo reply
  9: 16:11:46.454596      10.10.10.102 > 172.16.10.101 icmp: echo request
 10: 16:11:46.664150      172.16.10.101 > 10.10.10.102 icmp: echo reply
10 packets shown

```

ASA/パケットキャプチャ (リモートFW)

```

ASA# sh capture
capture capin type raw-data trace interface inside [Capturing - 1300 bytes]
  match icmp any any
capture tunnel type raw-data trace interface vti-1 [Capturing - 1300 bytes]
  match icmp any any
capture asp type asp-drop all [Capturing - 0 bytes]
  match icmp any any
ASA# sh cap capin

10 packets captured

  1: 11:08:30.288391      100.103.255.195 > 10.10.10.101 icmp: echo request
  2: 11:08:30.289123      10.10.10.101 > 100.103.255.195 icmp: echo reply
  3: 11:08:30.504566      100.103.255.195 > 10.10.10.101 icmp: echo request
  4: 11:08:30.504963      10.10.10.101 > 100.103.255.195 icmp: echo reply
  5: 11:08:30.710992      100.103.255.195 > 10.10.10.101 icmp: echo request
  6: 11:08:30.711404      10.10.10.101 > 100.103.255.195 icmp: echo reply
  7: 11:08:30.917112      100.103.255.195 > 10.10.10.101 icmp: echo request
  8: 11:08:30.917402      10.10.10.101 > 100.103.255.195 icmp: echo reply
  9: 11:08:31.128243      100.103.255.195 > 10.10.10.101 icmp: echo request
 10: 11:08:31.128640      10.10.10.101 > 100.103.255.195 icmp: echo reply
10 packets shown
ASA# sh cap tunnel

10 packets captured

  1: 11:08:30.287964      100.103.255.195 > 10.10.10.101 icmp: echo request
  2: 11:08:30.289322      10.10.10.101 > 100.103.255.195 icmp: echo reply
  3: 11:08:30.504505      100.103.255.195 > 10.10.10.101 icmp: echo request
  4: 11:08:30.505009      10.10.10.101 > 100.103.255.195 icmp: echo reply
  5: 11:08:30.710961      100.103.255.195 > 10.10.10.101 icmp: echo request
  6: 11:08:30.711434      10.10.10.101 > 100.103.255.195 icmp: echo reply
  7: 11:08:30.917066      100.103.255.195 > 10.10.10.101 icmp: echo request
  8: 11:08:30.917417      10.10.10.101 > 100.103.255.195 icmp: echo reply
  9: 11:08:31.128197      100.103.255.195 > 10.10.10.101 icmp: echo request
 10: 11:08:31.128685      10.10.10.101 > 100.103.255.195 icmp: echo reply
10 packets shown

```

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。