

ダイナミックルーティングを使用したプライベートアクセスに対するセキュアファイアウォール脅威対策による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](#)

[設定](#)

[セキュアアクセスの設定](#)

[ネットワークトンネルグループの設定](#)

[セキュアアクセスルーティング](#)

[ダイナミックルーティング\(BGP\)](#)

[ネットワークトンネルグループ設定の保存](#)

[プライベートリソースの作成](#)

[アクセスポリシールールの作成](#)

[セキュアファイアウォール脅威対策\(FTD\)の設定](#)

[仮想トンネルインターフェイスの設定](#)

[IPSecトンネルの設定](#)

[FTDルーティングの設定](#)

[ダイナミックルーティング\(BGP\)](#)

[アクセスポリシーの設定](#)

[確認](#)

[FTDでの確認](#)

[FTDのトンネルステータス](#)

[セキュアアクセスのトンネルステータス](#)

[セキュアアクセスのイベント](#)

[関連情報](#)

はじめに

このドキュメントでは、ダイナミックルーティングを使用したセキュアプライベートアクセスのために、IPsec経由でFTDを使用したセキュアアクセスを設定する方法について説明します。

前提条件

要件

- Cisco Secure Accessの知識
- Cisco Secure Accessダッシュボード/テナント
- Secure Firewall Threat DefenseおよびFirewall Management Centerの知識
- IPSecに関する知識
- ダイナミックルーティングの知識

使用するコンポーネント

- 7.7.10コードを実行するセキュアファイアウォール
- クラウド提供のファイアウォール管理センター。設定は一般的な仮想FMCにも適用されません
- Cisco Secure Accessダッシュボード

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

Secure Accessのネットワークトンネルは、主にSecure Internet AccessとSecure Private Accessの2つの目的に使用できます。

セキュアなプライベートアクセスでは、ゼロトラストアクセス(ZTA)やVPN as a Service(VPNaaS)を活用して、ユーザを内部アプリケーションやデータセンターなどのプライベートリソースに接続できます。IPSecトンネルは、ユーザとプライベートリソース間のネットワークトラフィックを安全に暗号化することで、このアーキテクチャで重要な役割を果たします。これにより、機密データが信頼できないネットワークを通過する際も、機密データが保護された状態で維持されます。IPSecトンネルをZTAまたはVPNaaSと統合することで、組織は堅牢なセキュリティ制御と可視性を維持しながら、内部リソースへのシームレスで安全なアクセスを提供できます。

このドキュメントでは、セキュアプライベートアクセス用にIPsec経由でセキュアファイアウォール脅威対策(FTD)を使用してセキュアアクセスを設定する方法について説明します。また、このガイドでは、BGPを使用したダイナミックルーティングの設定手順についても説明します。

このドキュメントでは、セキュアプライベートアクセスのためのIPSecトンネルの設定について説明しますが、プライベートアプリケーションにアクセスするためのZero Trust Access(ZTA)またはVPN as a Service(VPNaaS)のセットアップについては、このガイドでは取り上げていません。

設定

セキュアアクセスの設定

ネットワークトンネルグループの設定

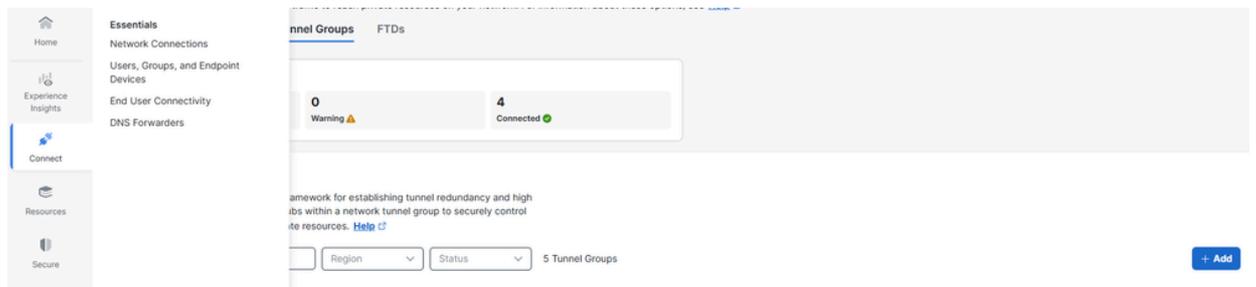
1. [Secure Access](#)の管理パネルに移動します。



CSAダッシュボード

2. ネットワークトンネルグループを追加します。

- Connect > Network Connectionsの順にクリックします。
 - Network Tunnel Groupsの下で、Addをクリックします。



NTGの確認

3. 一般設定の設定。

- トンネルグループ名、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。

- 1 General Settings
- 2 Tunnel ID and Passphrase
- 3 Routing
- 4 Data for Tunnel Setup

一般設定

General Settings

Give your network tunnel group a good meaningful name, choose type this tunnel group will use.

Tunnel Group Name

FTD

Region

Canada (Central)

Device Type

FTD

4. トンネル IDとパスフレーズを設定します。このIDはFTDの設定に必要なため、重要です

- Nextをクリックします。

- 1 General Settings
- 2 Tunnel ID and Passphrase
- 3 Routing
- 4 Data for Tunnel Setup

IDおよびPSK

Tunnel ID and Passphrase

Configure the tunnel ID and pa

Tunnel ID Format

Email IP Address

Tunnel ID

ftd1-ipsec

Passphrase

.....

The passphrase must be between special characters.

Confirm Passphrase

.....

5. ダイナミックルーティングを設定します。

セキュアアクセスルーティング

ダイナミックルーティング(BGP)

- セキュアアクセスでBGPピアを設定するときに、FTDのBGP自律システム(AS)番号を指定します。
- Routing > Dynamic routingの順にクリックします。
 - Device AS Numberをクリックして、FTDのBGP ASNを追加します。
 - Block default route advertisement チェックボックスにチェックマークを付けます
 - [Save] をクリックします。

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

Device AS Number

64513

Advanced Settings

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

Multi-region backhaul
Use Secure Access as the network backbone and prioritize regions based on origin.

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

CSA BGPの設定



注：セキュアアクセスによってアドバタイズされたルートは、元のASパスを付加して、プライマリトンネルに1を、セカンダリトンネルに2を含めます。マルチリージョンバックホールシナリオがサポートされています。詳細については、[こちら](#)をクリックしてください。

ネットワークトンネルグループ設定の保存

FTDの設定に必要なトンネルセットアップデータをダウンロードして保存します。

- Download CSVをクリックします。
- Doneをクリックします。

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: ftd1-ipsec@
 Primary Data Center IP Address: [input]
 Secondary Tunnel ID: ftd1-ipsec@
 Secondary Data Center IP Address: [input]
 Passphrase: [input]

[Download CSV](#)
[Done](#)

NTGデータ

Summary

✖ Disconnected

Region	Canada (Central)	Routing Type	Dynamic Routing (BGP)
Device Type	FTD	Device BGP AS	64513
Last Status Update	Feb 18, 2026 3:58 PM	Peer (Secure Access) BGP AS	64512
		BGP Peer (Secure Access) IP Addresses	169.254.0.9, 169.254.0.5, 2a04:e4c4:b:c723::b67:0000/120
		Multihop BGP Addresses	—
		Multihop TTL	—

BGPの設定



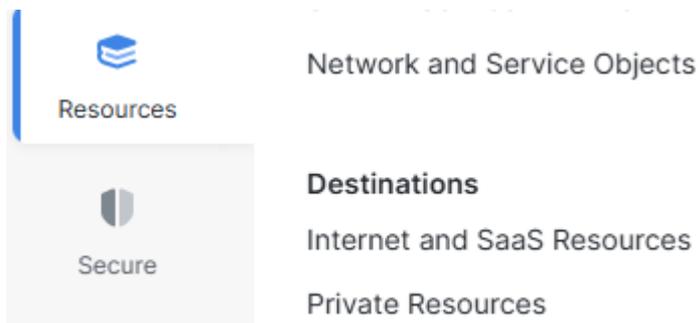
注: Network Tunnel Groupをクリックすると、BGP AS番号とBGPピアのIPアドレスが表示されます。これらは後でFTD側に設定されます。

プライベートリソースの作成

プライベートリソースは、データセンターまたはプライベートクラウド環境でホストされる内部アプリケーション、ネットワーク、またはサブネットです。これらのリソースは一般に公開されておらず、組織のインフラストラクチャの背後で保護されています。

Secure Accessでプライベートリソースとして定義することにより、ゼロトラストアクセス (ZTA)やVPN as a Service (VPNaaS)などのソリューションを通じてアクセス制御を実現できます。これにより、ユーザは、リソースをインターネットに直接公開することなく、ID、デバイスポスチャ、およびアクセスポリシーに基づいて内部システムに安全に接続できます。

Resources > Private Resourcesの順に選択し、Addをクリックします。



PR

- プライベートリソース名、内部到達可能アドレス、プロトコル、ポート/範囲を指定します。ポートとプロトコルを指定し、必要に応じてプライベートリソースを追加する
- 必要に応じて、接続方法（ゼロトラスト接続やVPN接続など）を選択します
- [Save] をクリックします。

Private Resource Name

Description (optional)

Private resource address

Define how the private resource will connect to applications through Secure Access.

Internally reachable address (FQDN, Wildcard FQDN, IPv4, IPv6, CIDR) ⓘ	Protocol	Port / Ranges
<input type="text" value="172.16.15.55"/>	<input type="text" value="TCP - (HTTP/H..."/>	<input type="text" value="8080"/>

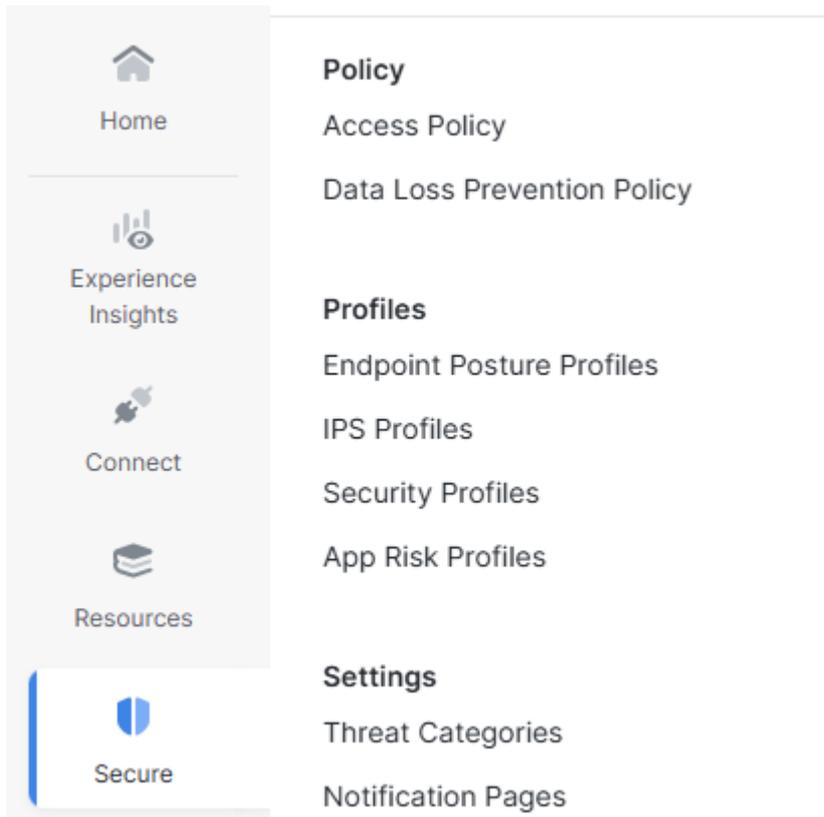
プライベートリソース

アクセスポリシーの作成

プライベートアクセスルールは、一般にアクセスできない内部リソースおよびアプリケーションにユーザが安全に接続する方法を定義します。

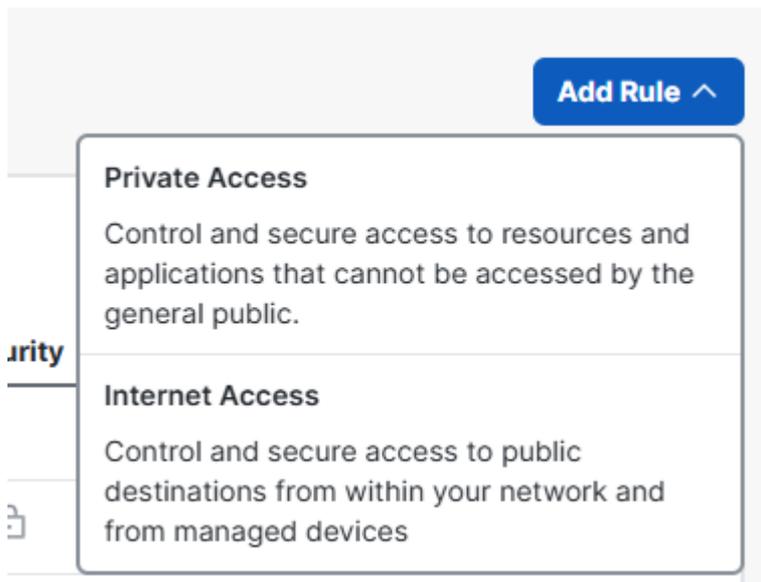
これらのルールは、ユーザID、グループメンバーシップ、デバイスのポスチャ、場所、その他のポリシー条件などの要因に基づいて、特定のプライベートリソースに誰がアクセスできるかを制御することで、セキュリティを強化します。これにより、機密性の高い内部システムを一般のパブリックアクセスから保護しながら、ZTAまたはVPNaaSを介して許可されたユーザが安全に利用できます。

移動先： セキュア>アクセスポリシー



ACP

- Add Rule をクリックします。
 - Private Access をクリックします。



ACPの追加

- Rule Name をクリックして、名前を指定します
- Action をクリックし、Allow to permit this traffic を選択します。
- onFrom from をクリックして、権限を付与されるユーザを指定します
- To をクリックし、ユーザがこのルールに基づいて持つアクセスを指定します

- Nextをクリックし、次のページでSaveをクリックします。

Rule name [ⓘ] Rule order

1 Specify Access
Specify which users and endpoints can access which resources. [Help](#) [ⓘ]

Action

Allow
Allow specified traffic if security requirements are met.

Block
Block specified traffic.

From Specify one or more sources

To Specify one or more destinations

+ AND

Endpoint Requirements

For VPN connections:
 End-user endpoint devices that are connected to the network using VPN may be able to access destinations specified in this rule. [ⓘ]
Endpoint requirements are configured in the VPN posture profile. Requirements are evaluated at the time the endpoint device connects to the network. [VPN Posture Profiles](#) [ⓘ]

For Branch connections:
 Endpoint device posture is not evaluated for endpoints connecting to these resources from a branch network.

2 Configure Security
Configure security requirements that must be met before traffic is allowed. [Help](#) [ⓘ]

Cancel

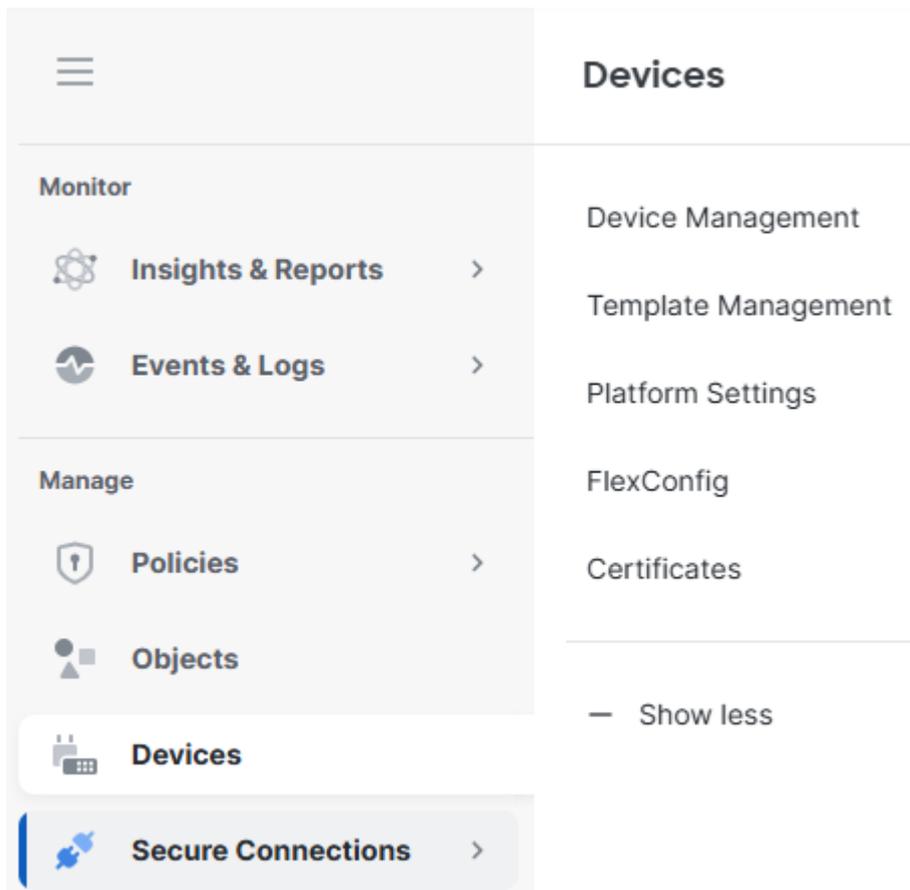
ACPの設定

セキュアファイアウォール脅威対策(FTD)の設定

仮想トンネルインターフェイスの設定

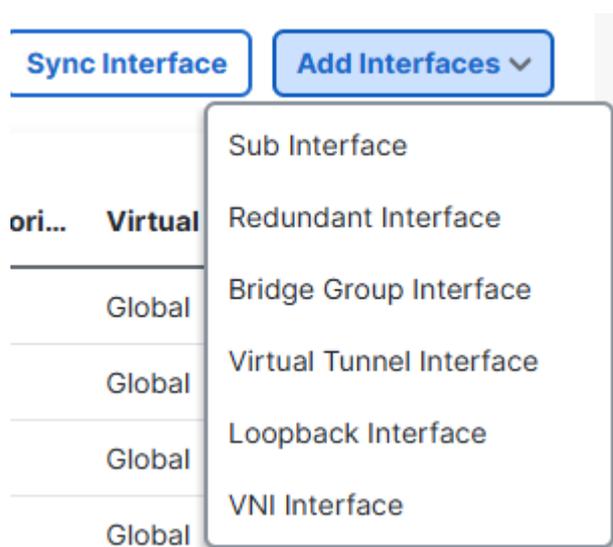
FTDの仮想トンネルインターフェイス(VTI)は、ルートベースのIPsec VPNトンネルの設定に使用される論理レイヤ3インターフェイスです。

1. Devices > Device Managementの順に移動します。



FTDデバイス

- FTDデバイスのInterfacesをクリックします。
 - Add Interfacesをクリックします。
 - Virtual Tunnel Interfaceをクリックします。
 - 2つの仮想トンネルインターフェイスの作成 (1つはプライマリセキュアアクセスハブ用、もう1つはセカンダリセキュアアクセスハブ用)



VTIの追加

仮想トンネルインターフェイス1:

- 名前を入力し、Enableをクリックします。
- セキュリティゾーンを選択または作成する
- Tunnel IDをクリックして、値を指定します。
- Tunnel Sourceをクリックし、トンネルを確立するWANインターフェイスを指定します
- IPSec Tunnel Modeをクリックし、selectIPv4
- IP Addressをクリックして、VTIのIPアドレスを設定します

OKをクリックします。

Tunnel Type

Static Dynamic

Name:*

VTI-1

Enabled

Description:

Security Zone:

zone_vti

Priority:

0

(0 - 65535)

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)

192.168.0.20

VTI1.1

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

169.254.0.1/30



VTI1.2

仮想トンネルインターフェイス2:

- 名前を入力し、Enableをクリックします。
- セキュリティゾーンを選択または作成する
- Tunnel IDをクリックして、値を指定します
- Tunnel Sourceをクリックし、トンネルを確立するWANインターフェイスを指定します
- IPsec Tunnel Modeをクリックし、selectIPv4
- IP Addressをクリックして、VTIのIPアドレスを設定します
- OKをクリックします。

Tunnel Type

Static Dynamic

Name:*

VTI-2

Enabled

Description:

Security Zone:

zone_vti

Priority:

0

(0 - 65535)

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:*

2

(0 - 10413)

Tunnel Source:*

GigabitEthernet0/0 (outside)

192.168.0.20

VTI2.1

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:*

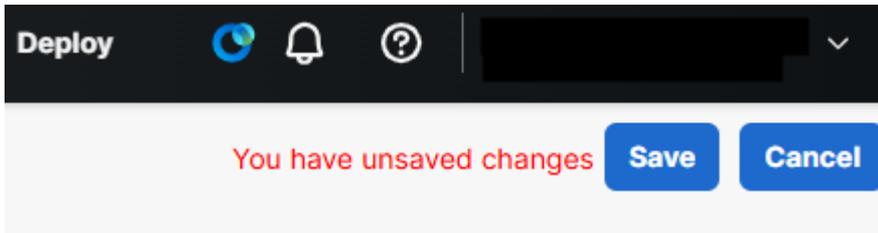
Configure IP

169.254.0.5/30



VTI2.2

[Save] をクリックします。

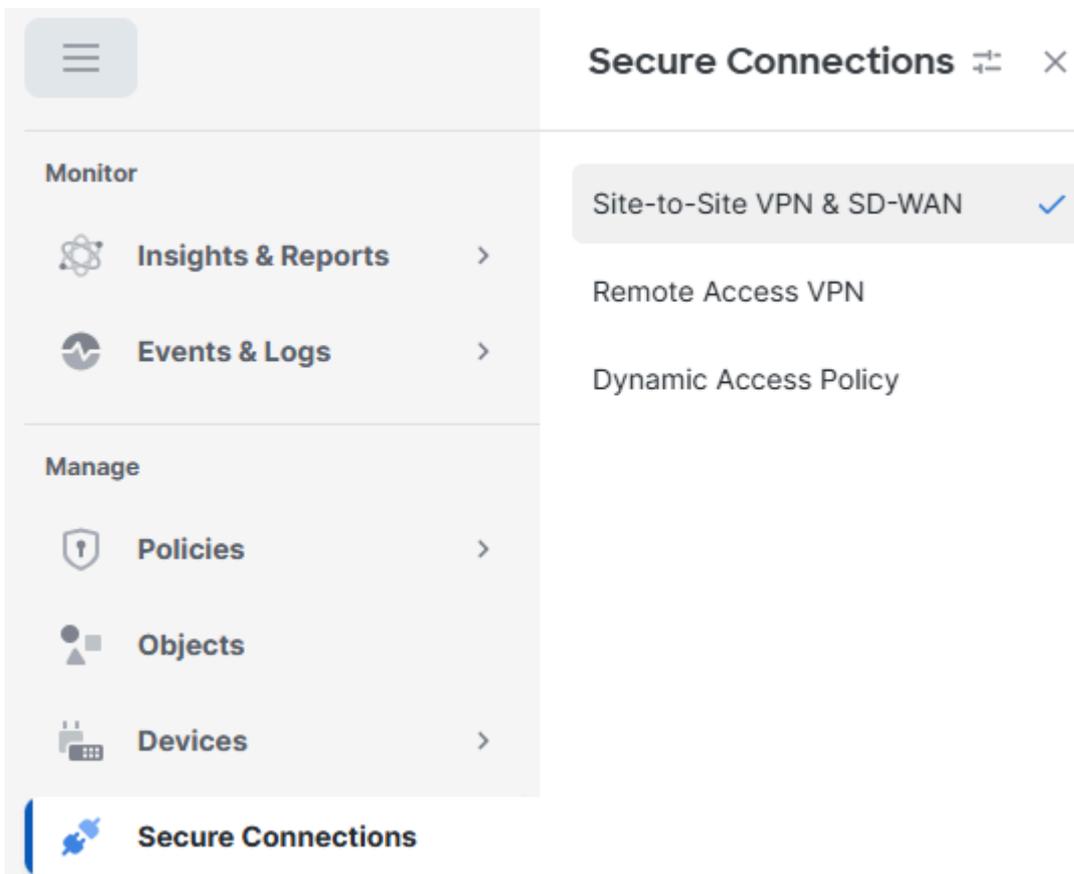


VTIの変更の保存

IPSecトンネルの設定

cdFMCダッシュボードに移動します。

- **Secure Connection** をクリックします > サイト間VPNおよびSD-WAN



S2S

- **onAdd** をクリックします。
 - **Route-Based VPN** をクリックします。
 - **ピアツーピア** をクリックします。

Last Updated: 12:56 PM Refresh NAT Exemptions Add

Create VPN Topology

Topology name *

VPN Type

SD-WAN Topology New

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

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

VPNの追加

- セキュアアクセス設定のステップ5から、プライマリ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
- onEndpoints をクリックします。
 - Node A の下で、onDevice をクリックして、Extranet を選択します。
 - Device Name をクリックして、名前を指定します
 - 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」 の下の 「Save Network Tunnel Group Configuration」 から)
 コンフィギュレーション)
 - ノードBでデバイスをクリックし、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、(Secure Access Configuration の下の 「Save Network Tunnel Group Configuration」 にある) プライマリトンネルIDを入力します。
 - Add Backup VTI をクリックします。
 - Virtual Tunnel Interface をクリックし、前のステップで作成した2番目のVTIインターフェイスを選択します
 - Send Local Identity to Peers option をクリックし、Email ID を選択し、(Secure Access Configuration の下の 「Save Network Tunnel Group Configuration」 にある) セカンダリトンネルIDを入力します。
 - [Save] をクリックします。

Network Topology:

Point to Point Hub and Spoke Full Mesh

IKE Version:* IKEv1 IKEv2

Endpoints IKE IPsec Advanced

Node A	Node B
Device:* <input type="text" value="Extranet"/>	Device:* <input type="text" value="cdFTD-1"/>
Device Name*: <input type="text" value="CSA"/>	Virtual Tunnel Interface:* <input type="text" value="VTI-1 (IP: 169.254.0.1)"/> +
Endpoint IP Address*: <input type="text" value="Primary-IP,Secondary-IP"/>	<i>Tunnel Source: outside (IP: 192.168.0.20)</i> Edit VTI <input type="checkbox"/> Tunnel Source IP is Private <input checked="" type="checkbox"/> Send Local Identity to Peers
	Local Identity Configuration*: <input type="text" value="Email ID"/> <input type="text" value="ftd1-ipsec@"/>
	----- Backup VTI: Remove
	Virtual Tunnel Interface:* <input type="text" value="VTI-2 (IP: 169.254.0.5)"/> +
	<i>Tunnel Source: outside (IP: 192.168.0.20)</i> Edit VTI <input type="checkbox"/> Tunnel Source IP is Private <input checked="" type="checkbox"/> Send Local Identity to Peers
	Local Identity Configuration*: <input type="text" value="Email ID"/> <input type="text" value="ftd1-ipsec@"/>

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

FTD VTIの設定

- IKEをクリックします
 - IKEv2 Settings > Policiesの順にクリックします。
 - Umbrella-AES-GCM-256オプションを選択します

OKをクリックします。

IKEv2 Policy



Available IKEv2 Policy

Search

- AES-GCM-NUL-**SHA**
- AES-GCM-NUL-**SHA-LA...**
- AES-**SHA**-**SHA**
- AES-**SHA**-**SHA-LATEST**
- DES-**SHA**-**SHA**
- DES-**SHA**-**SHA-LATEST**
- Umbrella-AES-GCM-256

Add

Selected IKEv2 Policy

Umbrella-AES-GCM-256

Cancel **OK**

IKEv2ポリシー

- Authentication Type をクリックして Pre Shared Manual Key を選択し、Secure Access (パスフレーズ) で設定したPSKを入力します

Endpoints **IKE** IPsec **Advanced**

Pre-shared Key Length:* Characters (Range 1-127)

IKEv2 Settings

Policies:*

Authentication Type:

Key:*

Confirm Key:*

Enforce hex-based pre-shared key only

IKE

- IPSEC

- IKEv2 Proposals
- Umbrella-AES-GCM-256を選択します。
- OKをクリックします。

Endpoints IKE **IPsec** Advanced

Crypto Map Type: Static Dynamic

IKEv2 Mode: Tunnel

Transform Sets: IKEv1 IPsec Proposals IKEv2 IPsec Proposals*

tunnel_aes256_sha Umbrella-AES-GCM-...

IPSec

Cancel **OK**

IKEv2プロポーザルの保存

FTDルーティングの設定

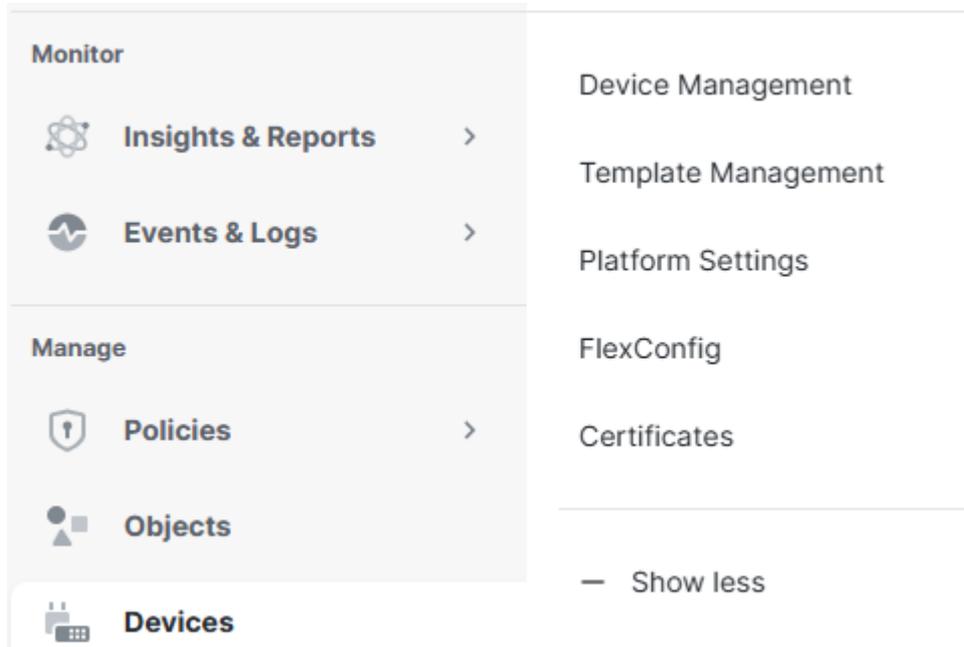
ダイナミックルーティング(BGP)

ボーダーゲートウェイプロトコル(BGP)は、自律システム(AS)間のルーティング情報の交換を自動化するダイナミックルーティングプロトコルです。スタティックルートに依存するのではなく、属性とポリシーに基づいてデータトラフィックに使用できるベストパスを決定する。

BGPは、ルートを動的に学習および更新することで、拡張性を向上させ、パス選択を最適化し、リンクまたはネットワークの変更時に自動フェールオーバーを提供します。

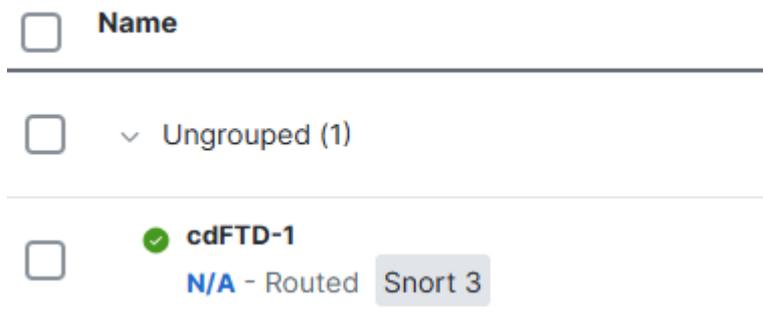
cdFMCダッシュボードに移動します。

- Devices > Device Managementの順にクリックします。



デバイス

- FTDをクリック



FTDデバイス

- Routing > BGP > IPv4 > Enable IPv4の順にクリックします
- Neighborをクリックして、セキュアアクセスのためのBGP自律システム(AS)番号を、ネイバーのIPアドレスとともに指定します
このプロセスに関連するすべての設定の詳細が記載されている「セキュアアクセスの設定」の下の注を参照してください。
- onSaveをクリックします

cdFTD-1 You have unsaved changes [Save](#) [Cancel](#)

Cisco Secure Firewall Threat Defense for VMware

Device Interfaces Inline Sets **Routing** DHCP VTEP

Enable IPv4: AS Number 64513

General **Neighbor** Add Aggregate Address Filtering Networks Redistribution Route Injection

Manage Virtual Routers: Global

Virtual Router Properties: ECMP, BFD, OSPF, OSPFv3, EIGRP, RIP, Policy Based Routing, BGP, **IPv4**

Address	Remote AS Number	Address Family	Remote Private AS Number	Description
169.254.0.2	64512	Enabled		Edit Delete
169.254.0.6	64512	Enabled		Edit Delete

BGPネイバー



注:2025年11月以降、新しく作成されたすべてのセキュアアクセス組織は、デフォルトでネットワークトンネルグループのBGPピアリングにパブリックASN 32644を使用します。2025年11月より前に設立された既存の組織は、以前はSecure Access BGPピア用に予約されていたプライベートASN 64512を引き続き使用します。

- **Networks** をクリックし、アドバタイズするネットワークをSecure Accessに追加します
- **[Save]** をクリックします。

cdFTD-1 You have unsaved changes [Save](#) [Cancel](#)

Cisco Secure Firewall Threat Defense for VMware

Device Interfaces Inline Sets **Routing** DHCP VTEP

Enable IPv4: AS Number 64513

General Neighbor Add Aggregate Address Filtering **Networks** Redistribution Route Injection

Manage Virtual Routers: Global

Virtual Router Properties: ECMP, BFD, OSPF, OSPFv3, EIGRP, RIP, Policy Based Routing, BGP, IPv4

Network	RouteMap
Subnet-172.16.15.0	

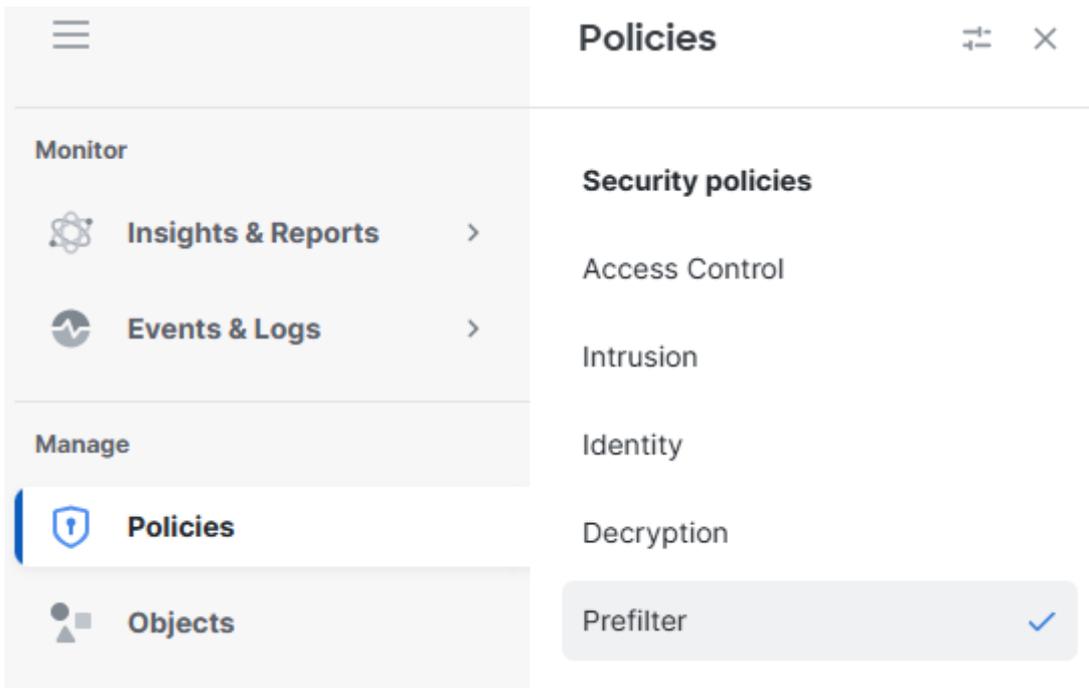
ネットワークの追加

アクセスポリシーの設定

Cisco Firepower Threat Defense(FTD)でトラフィックを許可し、プライベートリソースへのアクセスを有効にするには、トラフィックが最初にプレフィルタリングと呼ばれるアクセスコントロールの初期段階を通過する必要があります。

プレフィルタリングは、より深い検査が行われる前に処理され、シンプルで高速になるように設計されています。基本的な外部ヘッダー基準（送信元と宛先のIPアドレスとポートなど）を使用してトラフィックを評価し、トラフィックを迅速に許可、ブロック、またはバイパスします。この段階でトラフィックを許可すると、ディープパケットインスペクションや侵入ポリシーなど、よりリソースを大量に消費するインスペクションを省略できるため、セキュリティ制御を維持しながらパフォーマンスを向上させることができます。

Policies > Prefilter の順に移動します。



プレフィルタ

- アクセスポリシーで使用されているプレフィルタポリシーの編集をクリックします。



プレフィルタをクリックします。

- Add Tunnel Rule をクリックします。
 - VPNaaSネットワークやZTAサブネットからプライベートリソースへのトラフィックを追加し、許可します。
 - onSave をクリックします



ルールの保存

この時点で、FTDの設定が完了して確認されたら、展開を続行できます。導入後、IPsecトンネルとBGPネイバーセッションの両方が正常に起動し、接続とダイナミックルーティングが期待どおりに動作していることを確認します。

確認

FTDでの確認

FTDのトンネルステータス

トンネルの現在のステータス(アップ状態またはダウン状態を含む)を表示できます。これにより、IPSecトンネルが適切に確立されていることを確認できます。

- Secure Connectionsをクリックします。
- Site-to-Site VPN & SD-WANをクリックします。
- トポロジ名をクリックします。

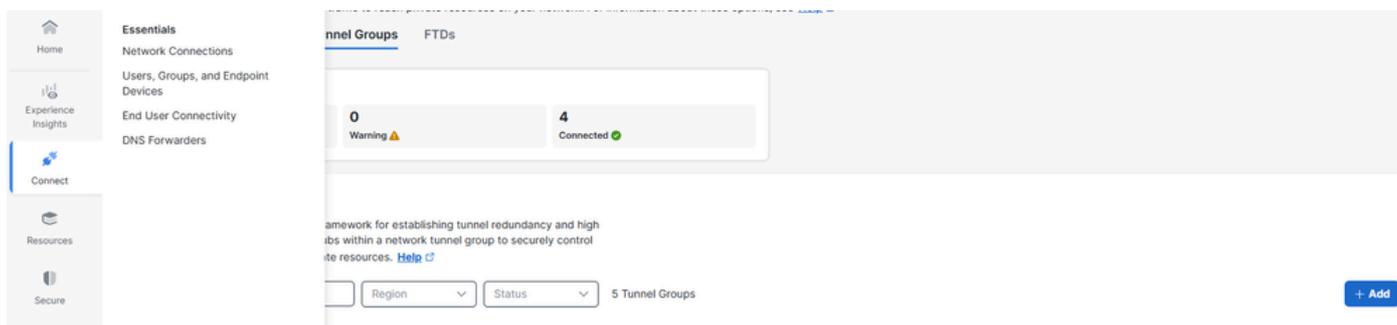
Topology name	VPN Type	Network Topology	Tunnel Status Distribution	IKEv1	IKEv2
CSA	Route Based (VTI)	Point-to-Point	2-Tunnels		✓
Node A					
Node B					
Device	VPN Interface	VTI Interface	Device	VPN Interface	VTI Interface
EXTRANET Extranet			FTD cdFTD-1	outside (192.168.0.20)	VTI-1 (169.254.0.1)
EXTRANET Extranet			FTD cdFTD-1	outside (192.168.0.20)	VTI-2 (169.254.0.5)

FTDトンネルステータス

セキュアアクセスのトンネルステータス

トンネルの現在のステータスを表示できます。ステータスには、接続解除、警告、または接続の有無が含まれます。これにより、IPSecトンネルが適切に確立されていることを確認できます。

- Connect > Network Connectionsの順にクリックします
- Network Tunnel Groupsをクリックします。



NTGの確認

- Network Tunnel Groupをクリックします

Summary

Connected

Region Canada (Central) Routing Type Static Routing
Device Type FTD IP Address Range 172.16.15.0/24
Last Status Update Feb 18, 2026 3:34 PM

Primary Hub

See Logs

Hub Up

1

Active Tunnels

Tunnel Group ID ftd1-ipsec@

Secondary Hub

Hub Up

1

Active Tunnels

Tunnel Group ID

CSAトンネルステータス

セキュアアクセスのイベント

トンネルとBGPのイベントを表示して、IPSecトンネルのステータスがアップ状態で安定しているかどうか、およびBGPセッションが確立されているかどうかを確認できます。

Monitor > Network Connectivityの順にクリックします。

The screenshot shows a sidebar menu on the left with icons for Home, Experience Insights, Connect, Resources, Secure, and Monitor. The Monitor option is highlighted. The main content area is titled 'Monitor' and lists various reports and logs:

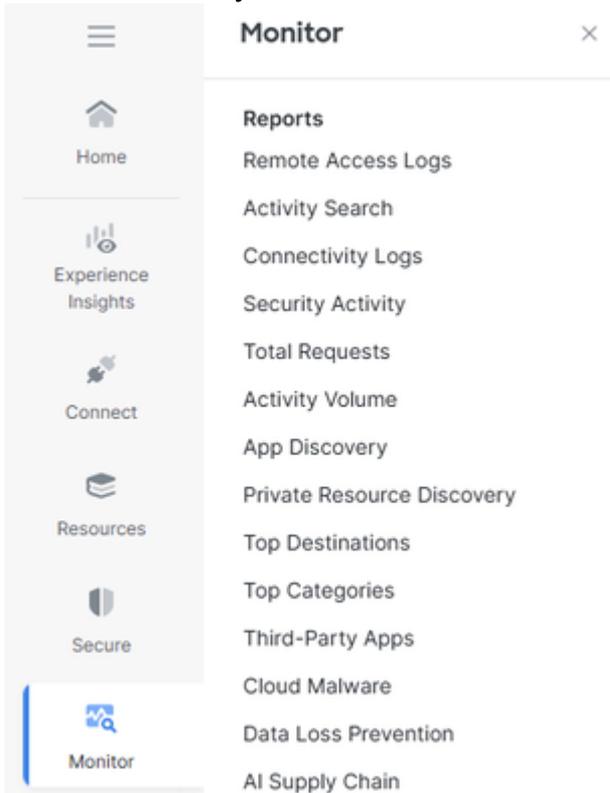
- Reports
- Remote Access Logs
- Activity Search
- Connectivity Logs
- Security Activity
- Total Requests
- Activity Volume
- App Discovery
- Private Resource Discovery
- Top Destinations
- Top Categories
- Third-Party Apps
- Cloud Malware
- Data Loss Prevention
- AI Supply Chain

接続ログの監視

Network tunnel group	Data center IP address	Hub type	Region	Alerts	Service	Device type	Details	Time (UTC)
FTD		Secondary	ca-central-1	Info	BGP	FTD	BGP peer up	Feb 18, 2026 4:07 PM
FTD		Secondary	ca-central-1	Info	IKE	FTD	Successful CHILD re...	Feb 18, 2026 4:07 PM
FTD		Primary	ca-central-1	Info	BGP	FTD	BGP peer up	Feb 18, 2026 4:06 PM
FTD		Primary	ca-central-1	Info	IKE	FTD	Successful CHILD re...	Feb 18, 2026 4:06 PM

NTGログ

Monitor > Activity Searchの順に移動します。



接続ログの監視

関連するイベントで、View Full Detailsをクリックします。

Source	Rule Identity	Destination	
Josue	Josue		View Full Details
Josue	Josue		Filter by Josue
Josue	Josue		Filter by
Josue	Josue		Filter by
Josue	Josue		View Rule
Josue	Josue		Edit Rule

詳細

Event Details



Action

Allowed

Time

Feb 18, 2026 3:30 PM

Rule Name

FTD IPsec Rule (2386307)

Enforced By

-

Source

 **Josue**

Source IP

Destination

http://172.16.15.55:8080/favicon.ico

Security Group Tag (SGT)

-

Destination IP

172.16.15.55

アクティビティ検索

関連情報

- [シスコのテクニカルサポートとダウンロード](#)
- [Cisco Secure Firewall Management Centerデバイス設定ガイド、7.7](#)

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。