

セキュアファイアウォールとハイアベイラビリティ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](#)

[背景説明](#)

[ネットワーク図](#)

[設定](#)

[セキュアアクセスでのVPNの設定](#)

[トンネルセットアップのデータ](#)

[セキュアファイアウォールでのトンネルの設定](#)

[トンネルインターフェイスの設定](#)

[セカンダリインターフェイスのスタティックルートを設定する](#)

[VTIモードでアクセスを保護するためのVPNの設定](#)

[エンドポイントの設定](#)

[IKEの設定](#)

[IPSecの設定](#)

[高度な設定](#)

[アクセスポリシーの設定シナリオ](#)

[インターネットアクセスのシナリオ](#)

[RA-VPNシナリオ](#)

[CLAP-BAP ZTNAエスシナリオ](#)

[ポリシーベースルーティングの設定](#)

[セキュアアクセスでのインターネットアクセスポリシーの設定](#)

[ZTNAおよびRA-VPNのプライベートリソースアクセスの設定](#)

[トラブルシューティング](#)

[フェーズ1\(IKEv2\)の確認](#)

[フェーズ2\(IPSEC\)の確認](#)

[ハイアベイラビリティ機能](#)

[セキュアなアクセスへのトラフィックルーティングの確認](#)

[関連情報](#)

はじめに

このドキュメントでは、ハイアベイラビリティを備えたセキュアファイアウォール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。

前提条件

- [ユーザプロビジョニングの設定](#)
- [ZTNA SSO認証設定](#)
- [リモートアクセスVPNセキュアアクセスの設定](#)

要件

次の項目に関する知識があることが推奨されます。

- Firepower Management Center 7.2
- Firepower Threat Defense(FTD)7.2
- セキュアなアクセス
- Cisco Secure Client:VPN (トンネルモード)
- Cisco Secureクライアント – ZTNA
- クライアントレスZTNA

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。

- Firepower Management Center 7.2
- Firepower Threat Defense(FTD)7.2
- セキュアなアクセス
- Cisco Secure Client:VPN (トンネルモード)
- Cisco Secureクライアント – ZTNA

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。

背景説明



CISCO

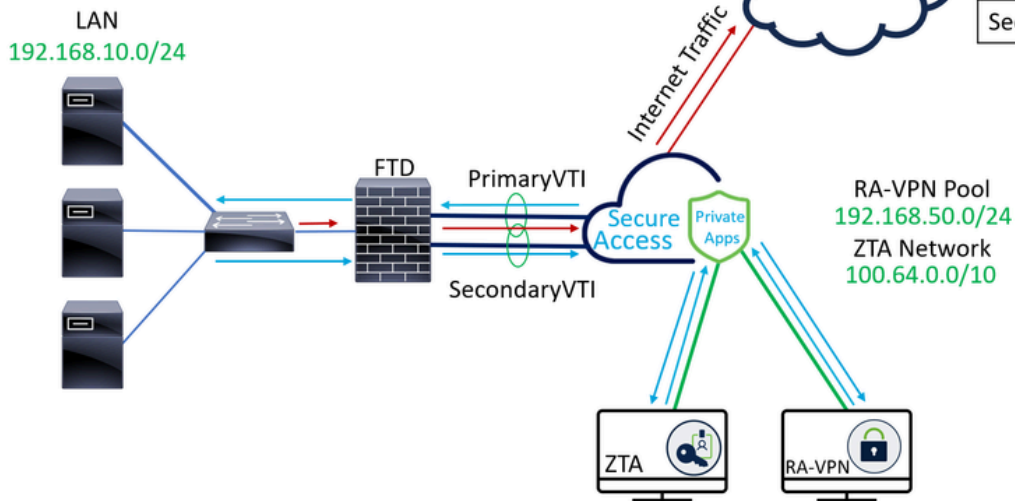
Secure Access Secure Firewall FTD

シスコは、プライベートアプリケーション（オンプレミスとクラウドベースの両方）を保護し、アクセスを提供するセキュアなアクセスを設計しました。また、ネットワークからインターネットへの接続も保護します。これは、複数のセキュリティ方式とレイヤの実装によって実現されます。すべての目的は、クラウド経由でアクセスする情報を保持することです。

ネットワーク図

Internet Access Traffic — (red line)
 Private Apps Traffic — (blue line)

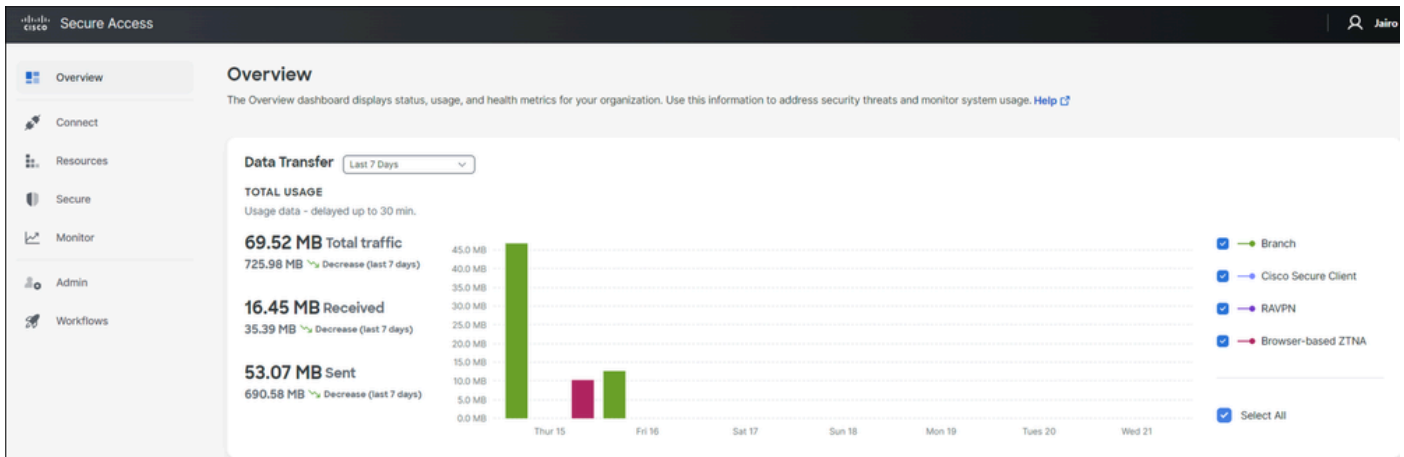
INTERFACE	IP
PrimaryWAN	192.168.30.5
PrimaryVTI	169.254.2.1
SecondaryWAN	192.168.0.202
SecondaryVTI	169.254.3.1



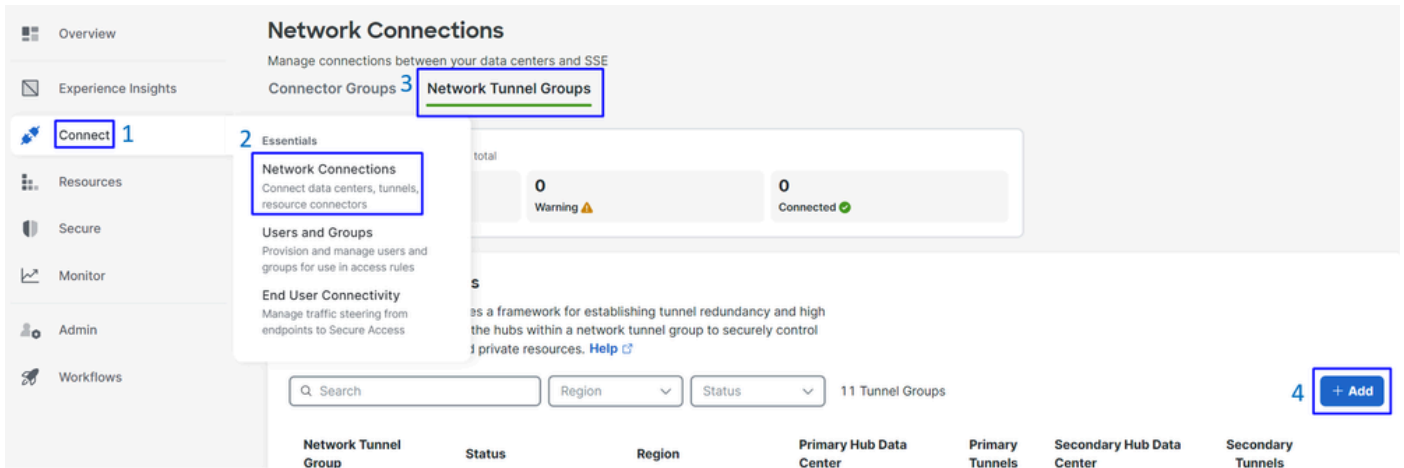
設定

セキュアアクセスでのVPNの設定

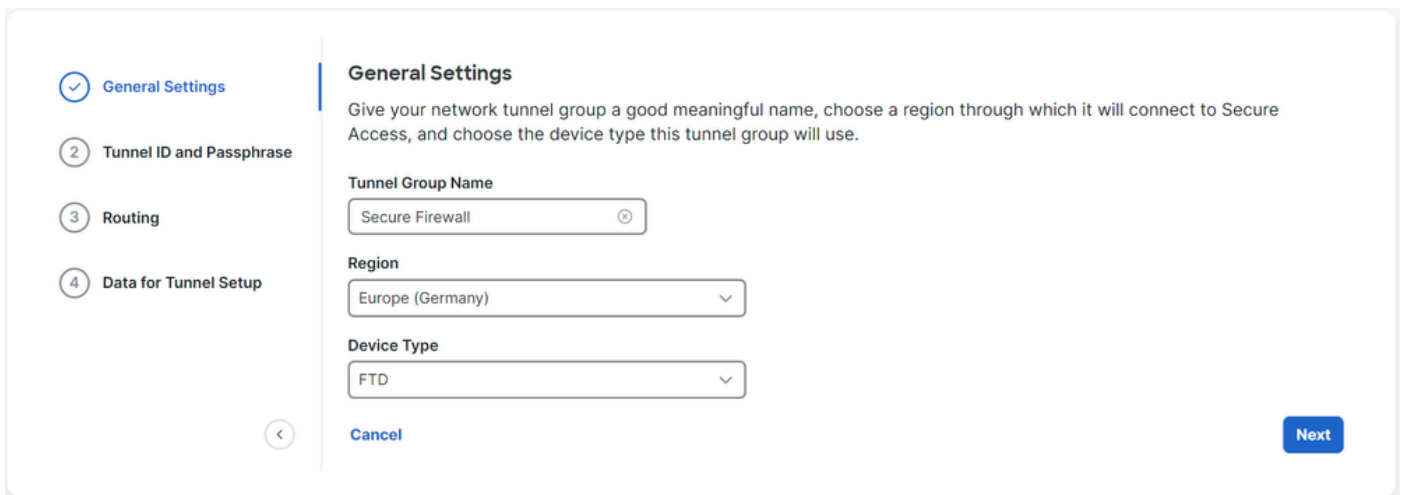
の管理パネルに移動します。 [セキュアなアクセス](#).



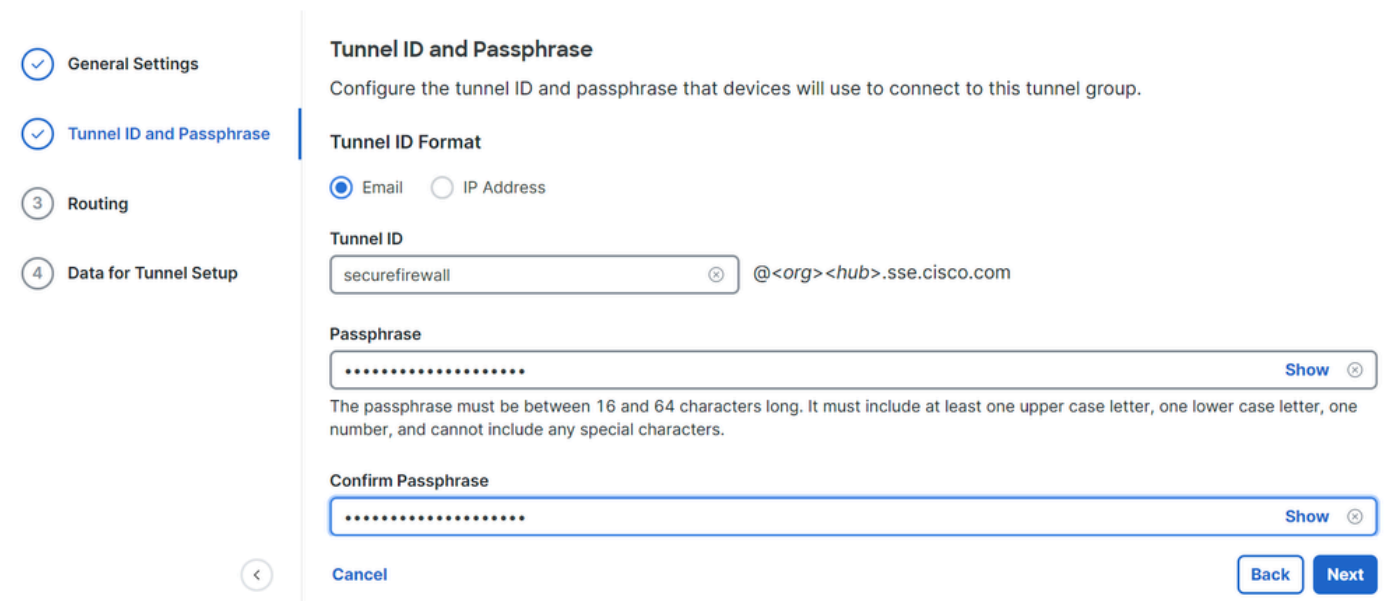
- クリック Connect > Network Connections
- 「Network Tunnel Groups」で、 + Add



- Tunnel Group Name、Regionの設定
- [保存 (Next



- Tunnel ID Formatコマンドと Passphrase
- [保存 (Next



- ネットワーク上で設定したIPアドレス範囲またはホストを設定し、トラフィックをセキュア

アクセス経由で通過させる

- [保存 (Save

Routing option

Static routing

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

IP Address Ranges

Add all public and private address ranges used internally by your organization. For example, 128.66.0.0/16, 192.0.2.0/24.

128.66.0.0/16, 192.0.2.0/24

Add

192.168.0.0/24 X

192.168.10.0/24 X

Dynamic routing

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

Cancel

Back

Save

トンネルに関する情報が表示されるSaveをクリックした後、次の手順のためにその情報を保存してください。 **Configure the tunnel on Secure Firewall.**

トンネルセットアップのデータ

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: securefirewall@[redacted]-sse.cisco.com

Primary Data Center IP Address: 18.156.145.74

Secondary Tunnel ID: securefirewall@[redacted]-sse.cisco.com

Secondary Data Center IP Address: 3.120.45.23

Passphrase: [redacted]

Download CSV

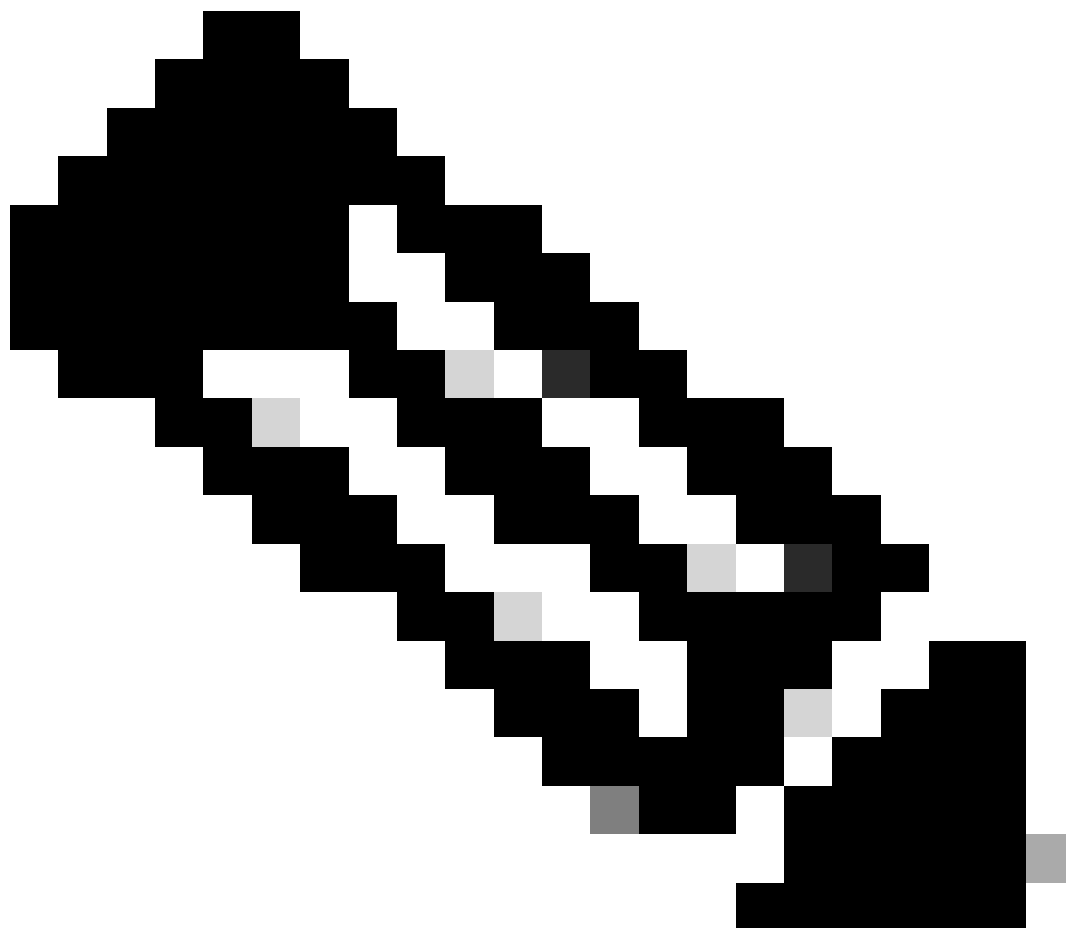
Done

セキュアファイアウォールでのトンネルの設定

トンネルインターフェイスの設定

このシナリオでは、この目標を達成するために、セキュアファイアウォールで仮想トンネルインターフェイス(VTI)設定を使用します。この例では、ISPが2つ存在し、いずれかのISPで障害が発生した場合にHAが必要です。

インターフェイス	役割
プライマリWAN	プリンシパルインターネットWAN
セカンダリWAN	セカンダリインターネットWAN
プライマリVTI	Principal Internet WANを介してトラフィックをセキュアアクセスに送信するようにリンクされます。
セカンダリVTI	Secondary Internet WANを介してトラフィックをセキュアアクセスに送信するようにリンクされます。



注：1.両方のトンネルを起動できるようにするには Primary or Secondary Datacenter IP、にスタティックルートを追加または割り当てる必要があります。

注:2. インターフェイス間でECMPを設定している場合、Primary or Secondary Datacenter IPへのスタティックルートを作成して両方のトンネルを有効にする必要はありません。

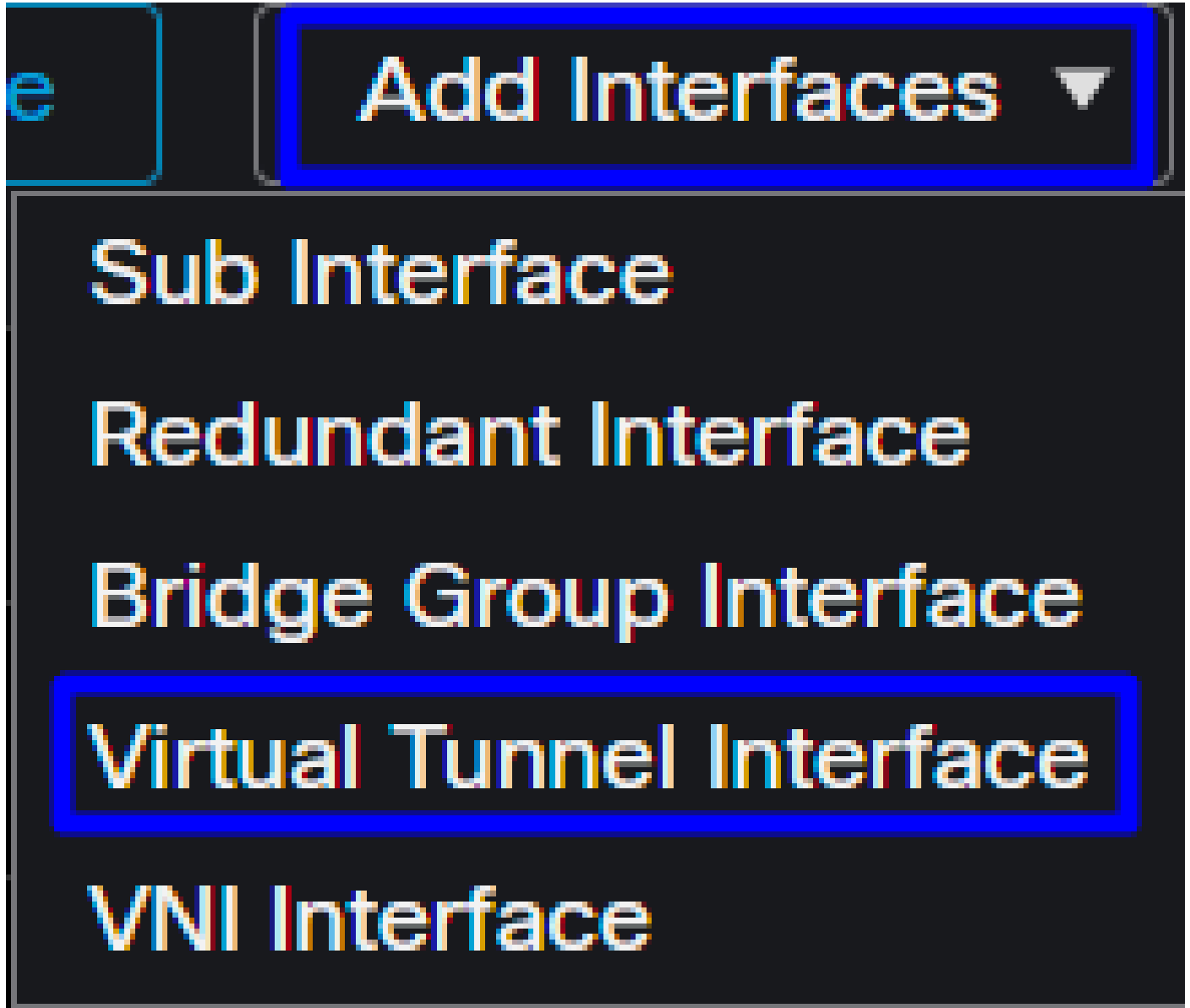
シナリオに基づいて、PrimaryWANとSecondaryWANを使用します。これらは、VTIインターフェイスを作成するために使用する必要があります。

Firepower Management Center > Devicesに移動します。

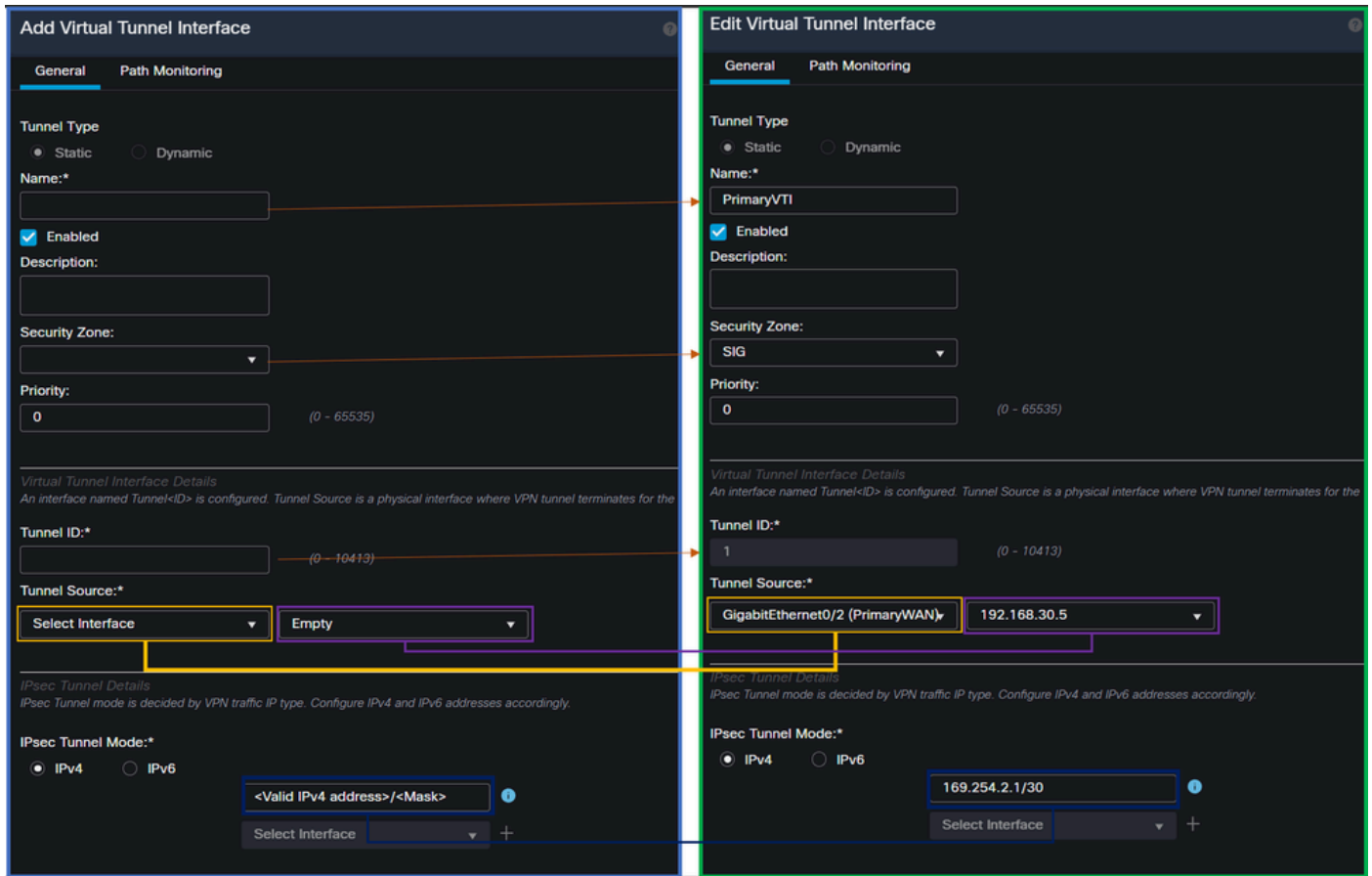
- FTDを選択します
- 選択 Interfaces

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address
Diagnostic0/0	diagnostic	Physical			
GigabitEthernet0/0	SecondaryWAN	Physical	SecondaryWAN		192.168.0.202/24(Static)
GigabitEthernet0/1	LAN	Physical	LAN		192.168.10.1/24(Static)
GigabitEthernet0/2	PrimaryWAN	Physical	PrimaryWAN		192.168.30.5/24(Static)

- クリック Add Interfaces > Virtual Tunnel Interface



- 次の情報に基づいてインターフェイスを設定します



- Name : インターフェイスを参照する名前を PrimaryWAN interface
- Security Zone : 別のSecurity Zoneを再利用できますが、Secure Accessトラフィック用に新しく作成の方が適切です
- Tunnel ID : トンネルIDの番号を追加します
- Tunnel Source : PrimaryWAN interfaceを選択し、インターフェイスのプライベートまたはパブリックIPを選択します
- IPsec Tunnel Mode : IPv4を選択し、ネットワーク内のルーティング不能IPをマスク30で設定します
-

注:VTIインターフェイスには、ルーティング不可能なIPを使用する必要があります。たとえば、2つのVTIインターフェイスがある場合、PrimaryVTIには169.254.2.1/30を、SecondaryVTIには169.254.3.1/30を使用できます。

その後、SecondaryWAN interfaceについても同じことを行う必要があります、VTIハイアベイラビリティ用にすべてが設定されているため、次の結果が得られます。

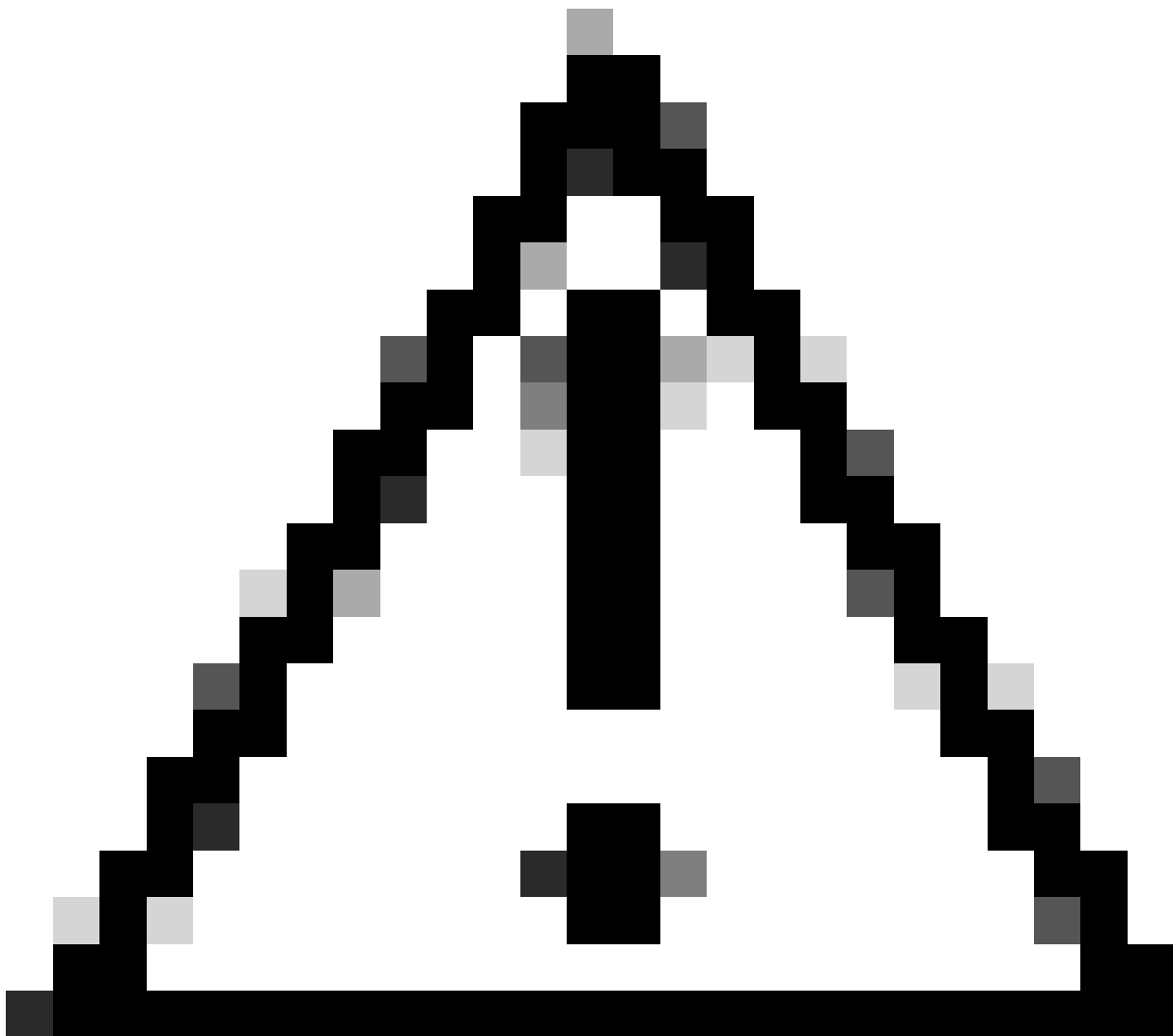
Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address
Diagnostic0/0	diagnostic	Physical			
GigabitEthernet0/0	SecondaryWAN	Physical	SecondaryWAN		192.168.0.202/24(Static)
Tunnel2	SecondaryVTI	VTI	SIG		169.254.3.1/30(Static)
GigabitEthernet0/1	LAN	Physical	LAN		192.168.10.1/24(Static)
GigabitEthernet0/2	PrimaryWAN	Physical	PrimaryWAN		192.168.30.5/24(Static)
Tunnel1	PrimaryVTI	VTI	SIG		169.254.2.1/30(Static)

このシナリオでは、次のIPが使用されます。

VTI IPの設定		
論理名	IP	範囲
プライマリVTI	169.254.2.1/30	169.254.2.1-169.254.2.2
セカンダリVTI	169.254.3.1/30	169.254.3.1-169.254.3.2

セカンダリインターフェイスのスタティックルートを設定する

SecondaryWAN interface のトラフィックが Secondary Datacenter IP Address に到達できるようにするには、データセンターIPへのスタティックルートを設定する必要があります。ルーティングテーブルの先頭に追加するには、メトリック1で設定します。また、ホストとしてIPを指定します。



注意：これは、WANチャンネル間にECMPを設定していない場合にのみ必要です。

ECMPを設定している場合は、次のステップに進むことができます。

移動先： **Device > Device Management**

- FTDデバイスをクリックします。
- クリック **Routing**
- 選択 **Static Route > + Add Route**

Edit Static Route Configuration




Type: IPv4 IPv6

Interface*

SecondaryWAN

Choose the SecondaryWAN interface


(Interface starting with this icon  signifies it is available for route leak)

Available Network  +

Search

Add

Selected Network

SecureAccessTunnel 

Choose the Secondary Datacenter IP

192.168.0.150

192.168.10.153

any-ipv4

ASA_GW

CSA_Primary

GWWT1

Ensure that egress virtualrouter has route to that destination

Gateway

Outside_GW

Choose the SecondaryWAN Gateway

Metric:

1

(1 - 254)

Tunneled: (Used only for default Route)

Route Tracking:

Cancel

OK

- Interface : セカンダリWANインターフェイスの選択
- Gateway : セカンダリWANゲートウェイを選択します。
- Selected Network : セカンダリデータセンターIPをホストとして追加します。この情報は、セキュアアクセスステップ「[トンネルセットアップのデータ](#)」でトンネルを設定するときに表示される情報から確認できます。

- Metric: 1を使用
- SaveOKをクリックして情報を保存し、展開します。

Network	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric	Tracked
▼ IPv4 Routes						
SecureAccessTunnel	SecondaryWAN	Global	Outside_GW	false	1	
any-ipv4	PrimaryWAN	Global	ASA_GW	false	1	
▼ IPv6 Routes						

VTIモードでアクセスを保護するためのVPNの設定

VPNを設定するには、ファイアウォールに移動します。

- クリック **Devices > Site to Site**
- クリック **+ Site to Site VPN**

エンドポイントの設定

エンドポイントの手順を設定するには、手順「[トンネルセットアップのデータ](#)」で提供される情報を使用する必要があります。

Create New VPN Topology

Topology Name:*

Policy Based (Crypto Map) Route Based (VTI)

Network Topology:

IKE Version:* IKEv1 IKEv2

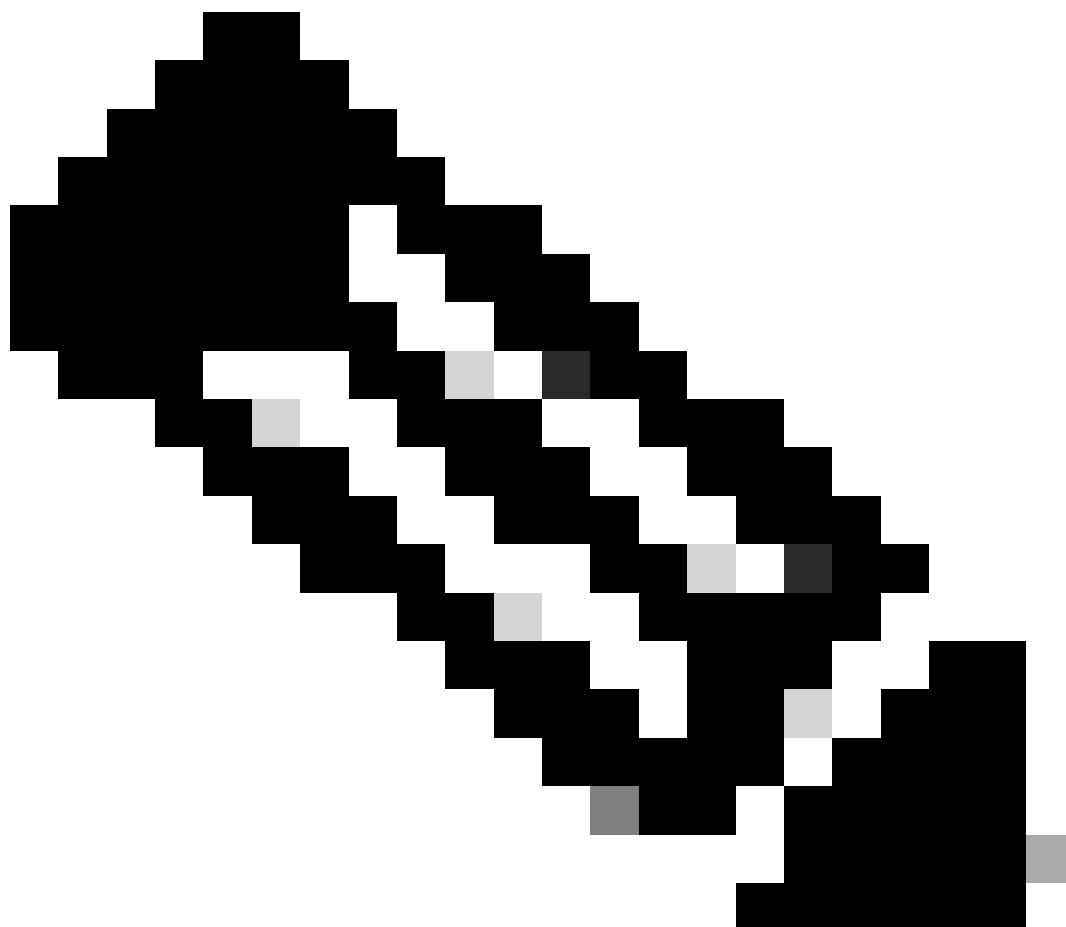
Endpoints

Node A	Node B
Device:* <input type="text" value="FTD_HOME"/>	Device:* <input type="text" value="Extranet"/>
Virtual Tunnel Interface:* <input type="text" value="PrimaryVTI (IP: 169.254.2.1)"/>	Device Name*: <input type="text" value="SecureAccess"/>
Tunnel Source: PrimaryWAN (IP: 192.168.30.5) Edit VTI <input type="checkbox"/> Tunnel Source IP is Private <input checked="" type="checkbox"/> Send Local Identity to Peers	Endpoint IP Address*: <input type="text" value="18.156.145.74,3.120.45.23"/>
Local Identity Configuration:* <input type="text" value="Email ID"/> <input type="text" value="jairohome@8195126-615626006-"/>	

Backup VTI: [Remove](#)

- トポロジ名：セキュアアクセス統合に関連する名前を作成します。
- 選択 **Routed Based (VTI)**

- 選択 Point to Point
 - IKE Version: IKEv2を選択します。
-



注:IKEv1は、セキュアアクセスとの統合ではサポートされていません。

Node Aの下で、次のパラメータを設定する必要があります。

Node A

Device:*

FTD_HOME ▼

Virtual Tunnel Interface:*

PrimaryVTI (IP: 169.254.2.1) ▼



Tunnel Source: PrimaryWAN (IP: 192.168.30.5) [Edit VTI](#)

Tunnel Source IP is Private

Send Local Identity to Peers

Local Identity Configuration:*

Email ID ▼

jairohome@ [redacted]

[+ Add Backup VTI \(optional\)](#)

- Device:FTDデバイスを選択します
- Virtual Tunnel Interface:PrimaryWAN Interfaceに関連するVTIを選択します。
- チェックボックスをオンにする Send Local Identity to Peers
- Local Identity Configuration : 電子メールIDを選択し、手順「[トンネルのセットアップに関するデータ](#)」の設定で指定したPrimary Tunnel IDに基づいて情報を入力します。

PrimaryVTIで情報を設定したら、+ Add Backup VTIをクリックします。

Backup VTI:

Remove

Virtual Tunnel Interface:*

SecondaryVTI (IP: 169.254.3.1) ▼

+

Tunnel Source: SecondaryWAN (IP: 192.168.0.202) Edit VTI

Tunnel Source IP is Private

Send Local Identity to Peers

Local Identity Configuration:*

Email ID ▼

jairohome@

- Virtual Tunnel Interface:PrimaryWAN Interfaceに関連するVTIを選択します。
- チェックボックスをオンにする Send Local Identity to Peers
- Local Identity Configuration : 電子メールIDを選択し、手順「[トンネルのセットアップに関するデータ](#)」の設定で指定したSecondary Tunnel IDに基づいて情報を入力します。

Node Bの下で、次のパラメータを設定する必要があります。

Node B

Device:*

Extranet



Device Name*:

SecureAccess

Endpoint IP Address*:

18.156.145.74, 3.120.45.23

- Device:エクストラネット
- Device Name : セキュアアクセスを宛先として認識するための名前を選択します。
- Endpoint IP Address : プライマリとセカンダリの設定はプライマリDatacenter IP,Secondary Datacenter IPにする必要があります。この情報は、ステップ「[トンネルセットアップのデータ](#)」で確認できます。

その後、Endpointsの設定が完了したので、ステップ「IKEの設定」に進むことができます。

IKE の設定。

IKEパラメータを設定するには、IKEをクリックします。

Endpoints

IKE

IPsec

Advanced

次IKE, のパラメータを設定する必要があります。

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

- Policies : デフォルトのUmbrella設定Umbrella-AES-GCM-256を使用することも、 [Supported IKEv2 and IPSEC Parameters](#)
- Authentication Type : 事前共有手動キー
- KeyConfirm Key:Passphraseの情報は、ステップ「[トンネル設定に関するデータ](#)」にあります。

その後、IKEの設定が完了したので、ステップ「IPSECの設定」に進むことができます。

IPSec の設定

IPSECパラメータを設定するには、IPSECをクリックします。

Endpoints

IKE



IPsec

Advanced

次IPSEC,のパラメータを設定する必要があります。

Crypto Map Type: Static Dynamic

IKEv2 Mode: Tunnel

Transform Sets: IKEv1 IPsec Proposals  IKEv2 IPsec Proposals* 

tunnel_aes256_sha	Umbrella-AES-GCM-256
-------------------	-----------------------------

Enable Security Association (SA) Strength Enforcement

Enable Perfect Forward Secrecy

Modulus Group: 14

Lifetime Duration*: 28800 Seconds (Range 120-2147483647)

Lifetime Size: 4608000 Kbytes (Range 10-2147483647)

- Policies : デフォルトのUmbrella設定Umbrella-AES-GCM-256を使用することも、 [Supported IKEv2 and IPSEC Parameters](#)

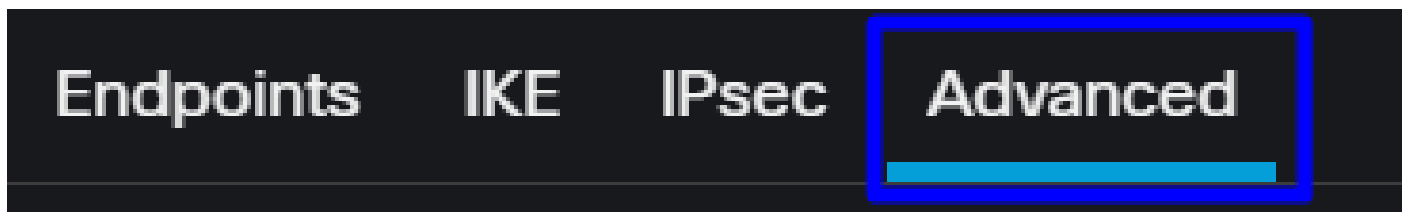


注:IPSECでは、これ以外は必要ありません。

その後、IPSECの設定が完了したので、高度な設定のステップに進むことができます。

高度な設定

詳細パラメータを設定するには、[詳細]をクリックします。



次Advanced,のパラメータを設定する必要があります。

ISAKMP Settings

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

Enable Aggressive Mode

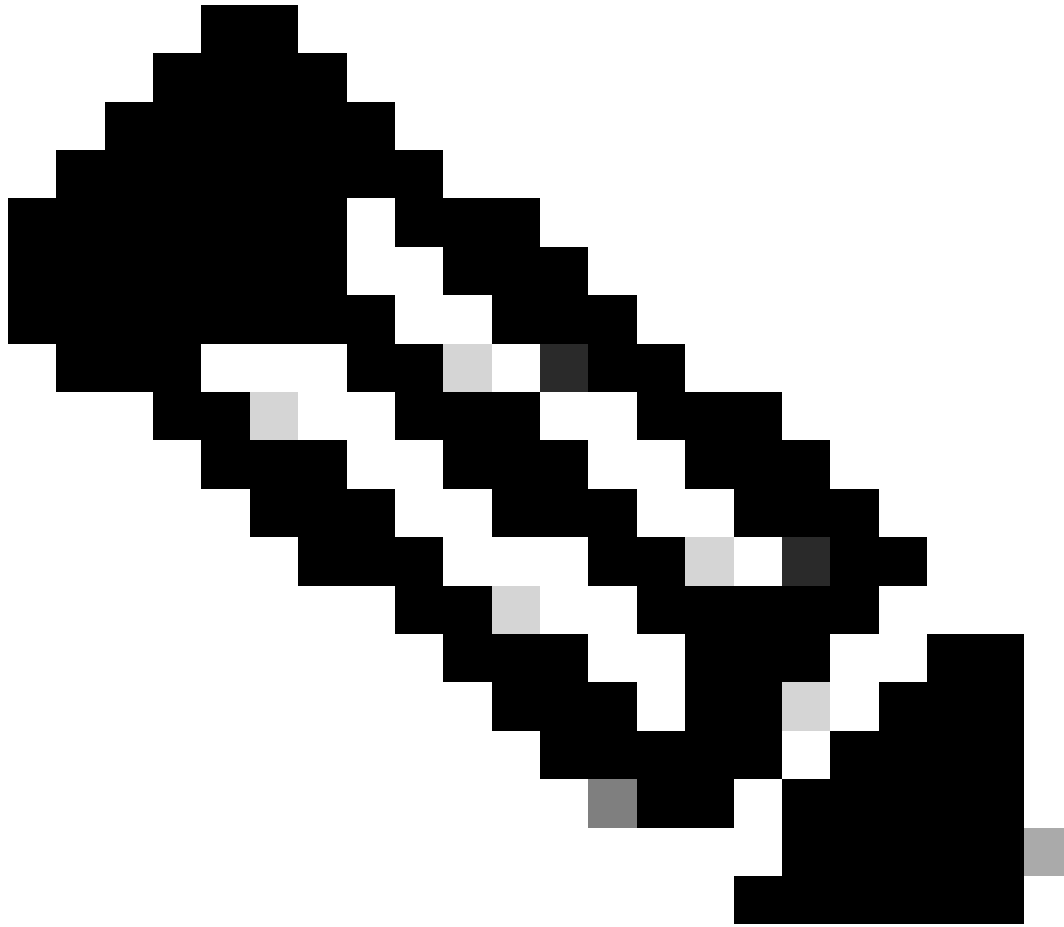
Enable Notification on Tunnel Disconnect

IKEv2 Security Association (SA) Settings

Cookie Challenge: custom

- IKE Keepalive:Enable
- Threshold:10
- Retry Interval:2
- Identity Sent to Peers: autoOrDN
- Peer Identity Validation : チェックしない

その後、SaveおよびDeployをクリックできます。



注：数分後に、両方のノードに対してVPNが確立されたことが表示されます。

Topology Name	VPN Type	Network Topology	Tunnel Status Distribution	IKEv1	IKEv2
SecureAccess	Route Based (VTI)	Point to Point	2 - Tunnels	✓	✖
Node A			Node B		
Device	VPN Interface	VTI Interface	Device	VPN Interface	VTI Interface
EXTRANET	Extranet	3.120.4... (3.120.45.23)	FTD	FTD_HOME	Secon... (192.168.0.202) Seconda... (169.254.3.1)
EXTRANET	Extranet	18.15... (18.156.145.74)	FTD	FTD_HOME	Primary... (192.168.30.5) PrimaryVTI (169.254.2.1)

その後、VPN to Secure Access in VTI Modeの設定が完了したので、ステップ Configure Policy Base Routingに進みます。



警告：セキュアアクセスへのトラフィックは、両方のトンネルが確立されている場合にプライマリトンネルにのみ転送されます。プライマリがダウンした場合は、セキュアアクセスによりトラフィックをセカンダリトンネル経由で転送できます。

注：セキュアアクセスサイトのフェールオーバーは、サポートされているIPSec値の『[ユ](#)
[ーザガイド](#)』に記載されているDPD値に基づいています。

アクセスポリシーの設定シナリオ

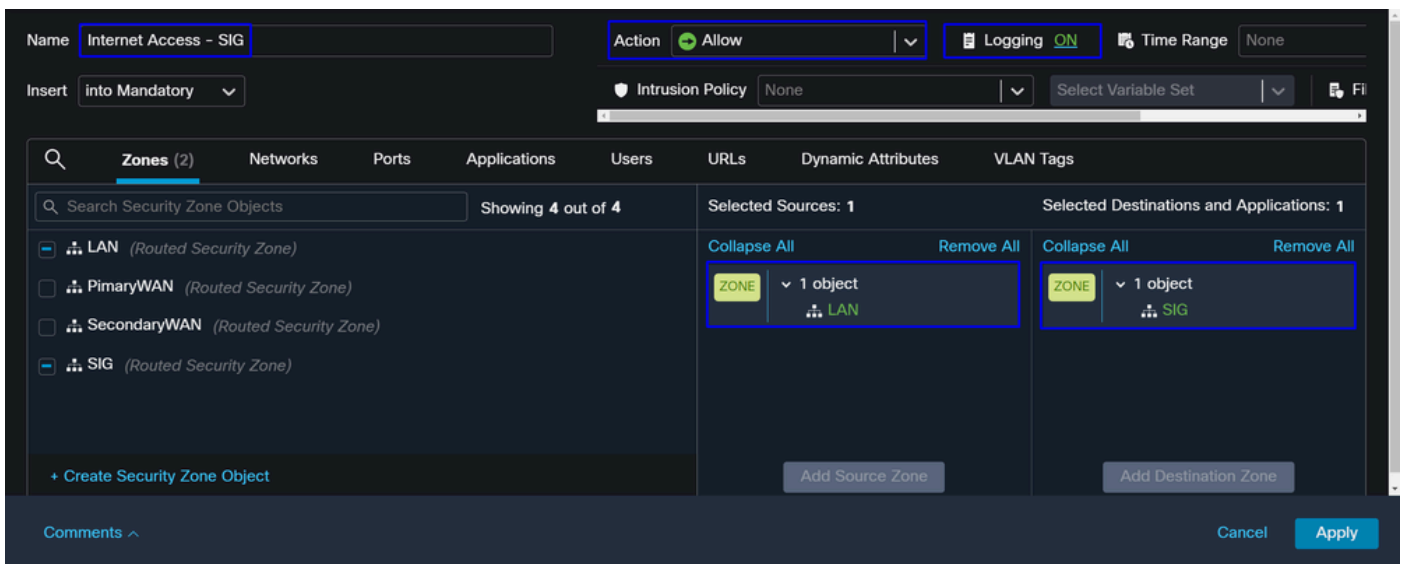
定義されるアクセスポリシールールは、次の条件に基づいています。

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address
● GigabitEthernet0/0	SecondaryWAN	Physical	SecondaryWAN		192.168.0.202/24(Static)
● Tunnel2	SecondaryVTI	VTI	SIG		169.254.3.1/30(Static)
● GigabitEthernet0/1	LAN	Physical	LAN		192.168.10.1/24(Static)
● GigabitEthernet0/2	PrimaryWAN	Physical	PrimaryWAN		192.168.30.5/24(Static)
● Tunnel1	PrimaryVTI	VTI	SIG		169.254.2.1/30(Static)

インターフェイス	ゾーン
プライマリVTI	SIG (シグニチャ)
セカンダリVTI	SIG (シグニチャ)
LAN	LAN

インターネットアクセスのシナリオ

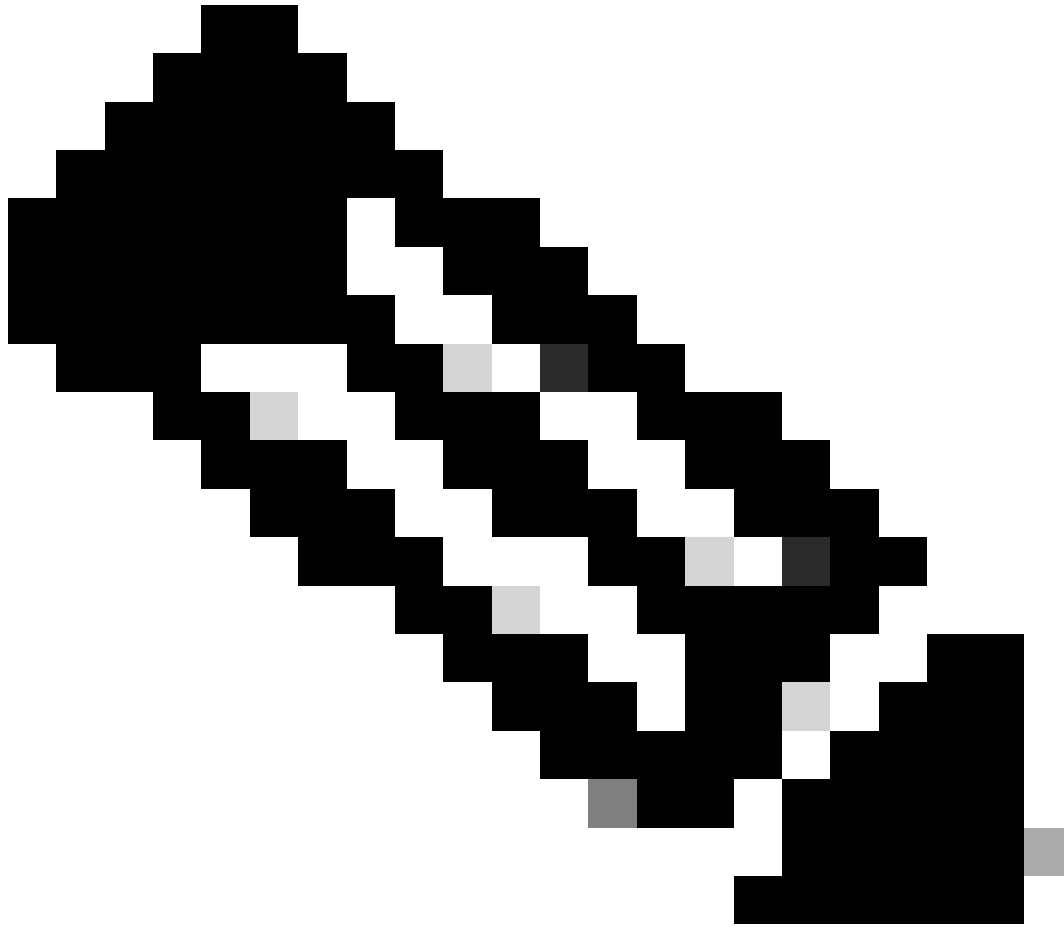
ポリシーベースルーティングで設定するすべてのリソースにインターネットへのアクセスを提供するには、アクセスルールとセキュアアクセスのポリシーを設定する必要があります。このシナリオで実行する方法について説明します。



このルールは、インターネットへの「LAN」へのアクセスを提供し、この場合はインターネットが「SIG」になります。

RA-VPNシナリオ

RA-VPNユーザからのアクセスを提供するには、RA-VPNプールで割り当てた範囲に基づいてアクセスを設定する必要があります。



注:RA-VPNaaSポリシーを設定するには、[Manage Virtual Private Networks](#)を使用します。

VPNaaSのIPプールを確認するには、どうすればよいですか。

[セキュアアクセスダッシュボード](#)に移動します

- クリック **Connect** > End User Connectivity
- クリック **Virtual Private Network**
- **Manage IP Pools**の下にある **Manage**

End User Connectivity

[Cisco Secure Client](#)[Manage DNS Servers \(2\)](#)

End user connectivity lets you define how your organization's traffic is steered from endpoints to Secure Access or to the internet. [Help](#)

Zero Trust **Virtual Private Network** Internet Security

Global FQDN

fb57.vpn.sse.cisco.com [Copy](#)

Manage IP Pools

[Manage](#)

2 Regions mapped

- 下にプールがあります Endpoint IP Pools

Pop Name	Display Name	Endpoint IP Pools	Management IP Pools	DNS Servers
Europe (Germany)	RA VPN 1	192.168.50.0/24 256 user connections	192.168.60.0/24 256 user connections	House

- SIGでこの範囲を許可する必要がありますが、PBRで設定するACLでも範囲を追加する必要があります。

アクセスルールの設定

プライベートアプリケーションリソースにアクセスする機能でセキュアアクセスを使用するように設定しているだけの場合、アクセスルールは次のようになります。

The screenshot shows the configuration of an Access Rule named 'Private APP'. The rule is set to 'Allow' with 'Logging ON' and 'Time Range None'. The 'Networks' tab is active, showing a list of source networks. Two source networks are selected: 'ZONE' (SIG) and 'NET' (192.168.50.0/24). The destination is set to 'LAN'.

このルールは、RA-VPNプール192.168.50.0/24からLANへのトラフィックを許可します。必要に応じて、さらに多くのトラフィックを指定できます。

ACLの設定

SIGからLANへのルーティングトラフィックを許可するには、トラフィックをACLの下に追加して、PBRの下で機能させる必要があります。

Sequence	Action	Source	Source Port	Destination	Destination Port	Application	Users	SGT
1	Allow	192.168.10.0/24	Any	192.168.50.0/24	Any	Any	Any	
2	Block	Any	Any	Any	Any	Any	Any	

CLAP-BAP ZTNAエスシナリオ

クライアントベースのZTAユーザまたはブラウザベースのZTAユーザからネットワークにアクセスできるように、CGNAT範囲100.64.0.0/10に基づいてネットワークを設定する必要があります。

。

アクセスルールの設定

プライベートアプリケーションリソースにアクセスする機能でセキュアアクセスを使用するように設定しているだけの場合、アクセスルールは次のようになります。

Name: ZTNA Access - IN Action: Allow Logging: ON Time Range: None Rule Enabled: ON

Insert: into Mandatory Intrusion Policy: None Select Variable Set: File Policy: None

Search Network and Geolocation Objects Showing 27 out of 27

Networks	Geolocations
<input type="checkbox"/> 192.168.0.150 (Host Object)	192.168.0.150
<input type="checkbox"/> 192.168.10.153 (Host Object)	192.168.10.153
<input type="checkbox"/> any (Network Group)	0.0.0.0/0::/0
<input type="checkbox"/> any-ipv4 (Network Object)	0.0.0.0/0
<input type="checkbox"/> any-ipv6 (Host Object)	::/0
<input type="checkbox"/> ASA_GW (Host Object)	192.168.30.1
<input type="checkbox"/> CSA_Primary (Host Object)	18.156.145.74
<input type="checkbox"/> GWT1 (Host Object)	169.254.2.2

+ Create Network Object Manually Enter IP: Add Source Network: Add Destination Network:

Selected Sources: 2 Selected Destinations and Applications: 1

Collapse All Remove All Collapse All Remove All

- ZONE (1 object): SIG
- NET (1 object): 100.64.0.0/10 (CGNAT RANGE)
- ZONE (1 object): LAN

このルールは、ZTNA CGNAT範囲100.64.0.0/10からLANへのトラフィックを許可します。

ACLの設定

CGNATを使用するSIGからLANへのルーティングトラフィックを許可するには、ACLの下に追加して、PBRで機能するようにする必要があります。

Sequence	Action	Source	Source Port	Destination	Destination Port	Application	Users	SGT
1	Allow	192.168.10.0/24	Any	100.64.0.0/10	Any	Any	Any	
2	Block	Any	Any	Any	Any	Any	Any	

ポリシーベースルーティングの設定

セキュアアクセスを通じて内部リソースとインターネットへのアクセスを提供するには、ポリシーベースルーティング(PBR)を介して、送信元から宛先へのトラフィックのルーティングを容易にするルートを作成する必要があります。

- 移動先： Devices > Device Management
- ルートを作成するFTDデバイスを選択します

Name	Model	Version
<input type="checkbox"/> Ungrouped (1)		
<input checked="" type="checkbox"/> FTD_HOME Snort 3 192.168.0.201 - Routed	FTDv for VMware	7.2.5

- クリック **Routing**
- 選択 Policy Base Routing
- [保存 (Add

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

このシナリオでは、トラフィックをセキュアアクセスにルーティングする送信元として、またはRA-VPNを使用したセキュアアクセスへのユーザ認証を提供する送信元として、またはネットワーク内部リソースへのクライアントベースまたはブラウザベースのZTAアクセスを提供する送信元として使用するすべてのインターフェイスを選択します。

- Ingress Interfaceの下で、Secure Access経由でトラフィックを送信するすべてのインターフェイスを選択します。

Edit Policy Based Route

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

Ingress Interface*

LAN

- Match Criteria and Egress Interfaceで次のパラメータを定義するには、Add:

Match Criteria and Egress Interface

Specify forward action for chosen match criteria.

Add

Add Forwarding Actions

Match ACL:* Select... +

Send To:* IP Address

IPv4 Addresses: For example, 192.168.0.1, 10.10.1.2

IPv6 Addresses: For example, 2001:db8::, 2002:db8::1

Don't Fragment: None

Internal Sources

Match ACL:* ACL

Send To:* IP Address

IPv4 Addresses: 169.254.2.2, 169.254.3.2

IPv6 Addresses: For example, 2001:db8::, 2002:db8::1

Don't Fragment: None

- Match ACL : このACLでは、セキュアアクセスにルーティングするすべてのものを設定します。

Traffic to the destination 208.67.222.222 or 208.67.220.220 over DNS using TCP or UDP will not be routed to Secure Access

✗ REJECT

Name: SSPT_FTD_ACL

Entries (2)

Sequence	Action	Source	Source Port	Destination	Destination Port
1	Block	Any	Any	208.67.222.222 208.67.220.220	Any
2	Allow	192.168.10.0/24	Any	Any	Any

Traffic from the source 192.168.10.0/24 will be routed to Secure Access

Depends how you play with the ACL, you can define how the traffic must be routed to Secure Access

✓ ACCEPT

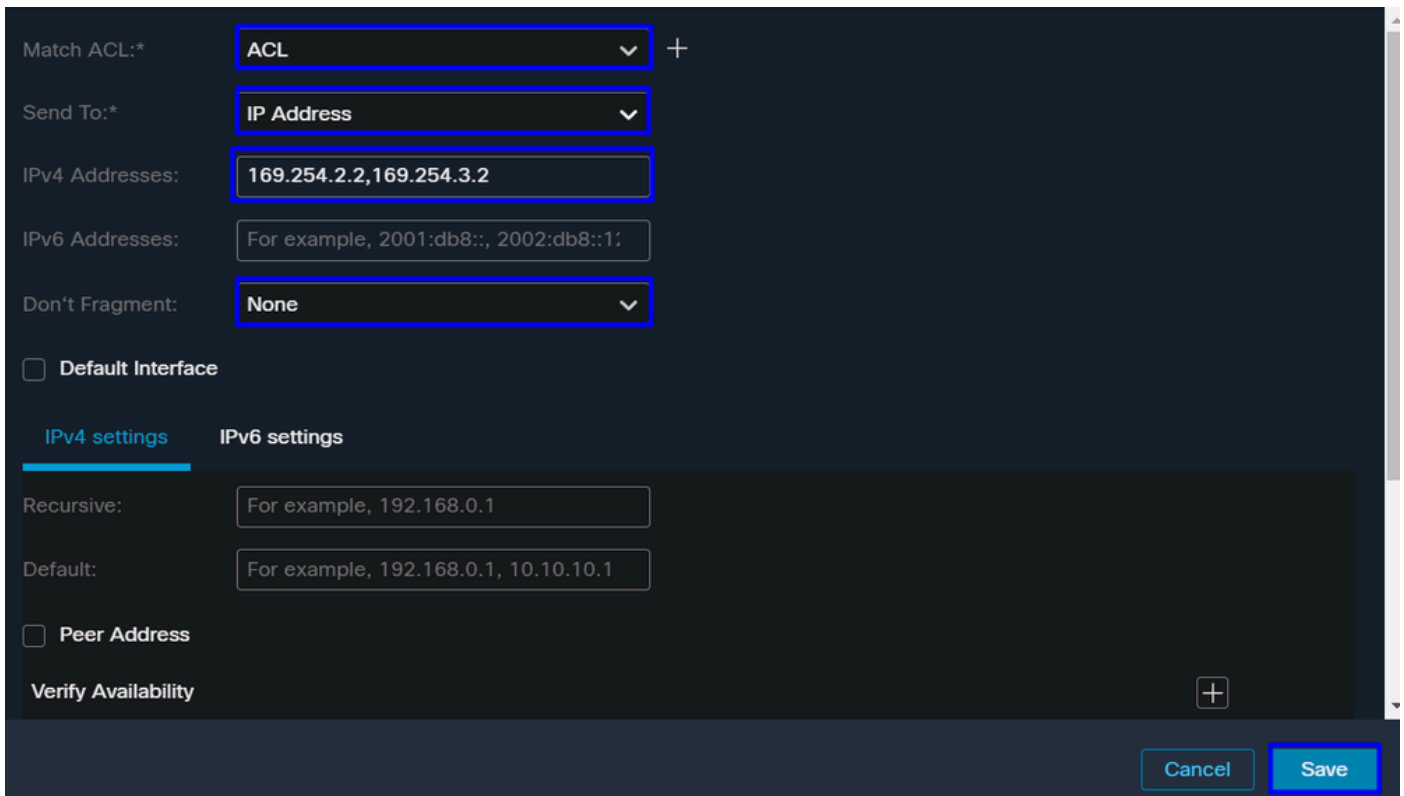
- Send To: IPアドレスの選択
- IPv4 Addresses : 両方のVTIで設定されているマスク30の下で、次のIPを使用する必要があります

す。このステップの「[VTI Interface Config](#)

インターフェイス	IP	GW
プライマリVTI	169.254.2.1/30	169.254.2.2
セカンダリVTI	169.254.3.1/30	169.254.3.2



このように設定すると、次の結果が得られ、「Save」のクリックに進むことができます。



その後、再度設定する必要があるSaveあり、次の方法で設定します。

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

Match ACL	Forwarding Action
ACL	Send through 169.254.2.2 → Send the traffic to the PrimaryVTI 169.254.3.2 If PrimaryVTI fail it will send the traffic to the SecondaryVTI

Cancel Save

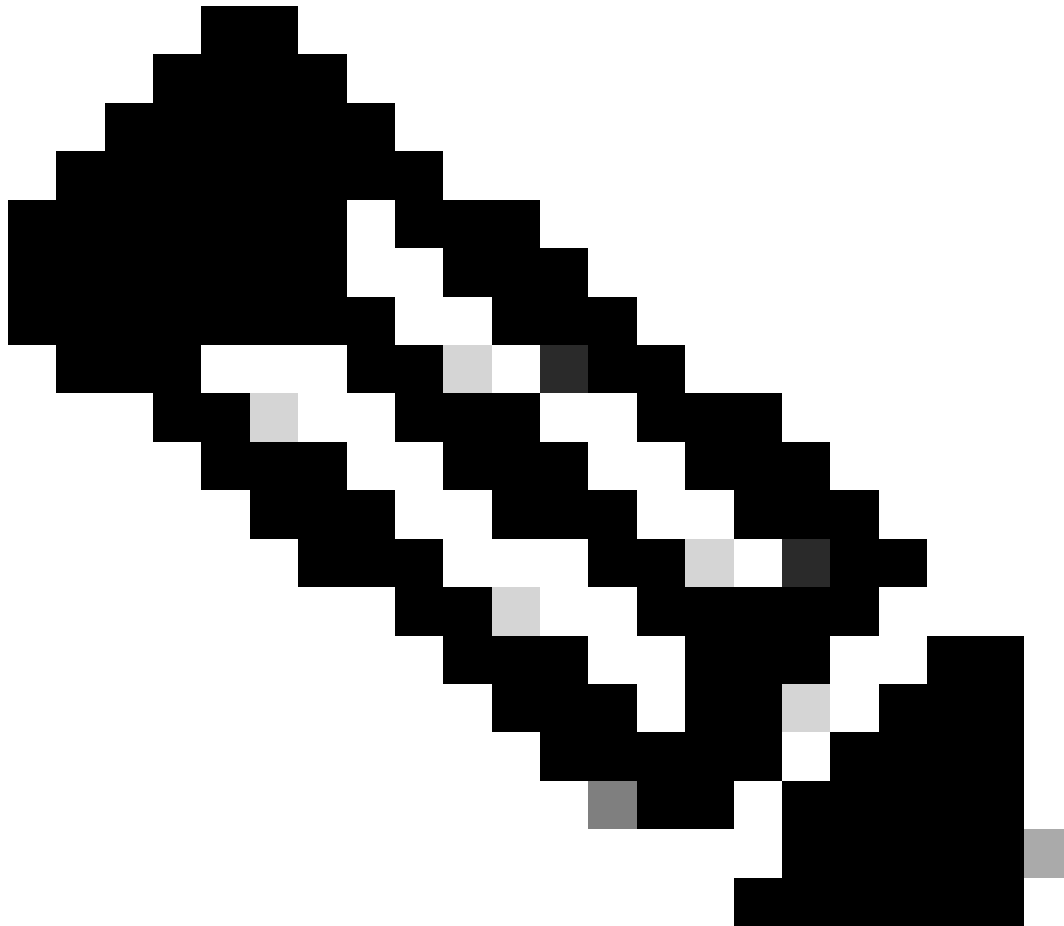
その後、展開すると、ACLで設定されたマシンのトラフィックがセキュアアクセスにルーティングされていることがわかります。

FMCの「Conexion Events」から：

<input type="checkbox"/>	Action ×	Initiator IP ×	Responder IP ×	↓ Application Risk ×	Access Control Policy ×	Ingress Interface ×	Egress Interface ×
▼ <input type="checkbox"/>	Allow	192.168.10.40	8.8.8.8	Medium	HOUSE	LAN	PrimaryVTI
▼ <input type="checkbox"/>	Allow	192.168.10.40	8.8.8.8	Medium	HOUSE	LAN	PrimaryVTI
▼ <input type="checkbox"/>	Allow	192.168.10.40	8.8.8.8	Medium	HOUSE	LAN	PrimaryVTI
▼ <input type="checkbox"/>	Allow	192.168.10.40	8.8.8.8	Medium	HOUSE	LAN	PrimaryVTI
▼ <input type="checkbox"/>	Allow	192.168.10.40	8.8.8.8	Medium	HOUSE	LAN	PrimaryVTI
▼ <input type="checkbox"/>	Allow	192.168.10.40	8.8.8.8	Medium	HOUSE	LAN	PrimaryVTI

セキュアアクセスの「Activity Search」から：

Request	Source	Rule Identity	Destination	Destination IP	Internal IP	External IP	Action	Categories	Res
FW	⇒ HomeFTD	⇒ HomeFTD		8.8.8.8	192.168.10.40		✓ Allowed	Uncategorized	
FW	⇒ HomeFTD	⇒ HomeFTD		8.8.8.8	192.168.10.40		✓ Allowed	Uncategorized	
FW	⇒ HomeFTD	⇒ HomeFTD		8.8.8.8	192.168.10.40		✓ Allowed	Uncategorized	
FW	⇒ HomeFTD	⇒ HomeFTD		8.8.8.8	192.168.10.40		✓ Allowed	Uncategorized	
FW	⇒ HomeFTD	⇒ HomeFTD		8.8.8.8	192.168.10.40		✓ Allowed	Uncategorized	
FW	⇒ HomeFTD	⇒ HomeFTD		8.8.8.8	192.168.10.40		✓ Allowed	Uncategorized	
FW	⇒ HomeFTD	⇒ HomeFTD		8.8.8.8	192.168.10.40		✓ Allowed	Uncategorized	

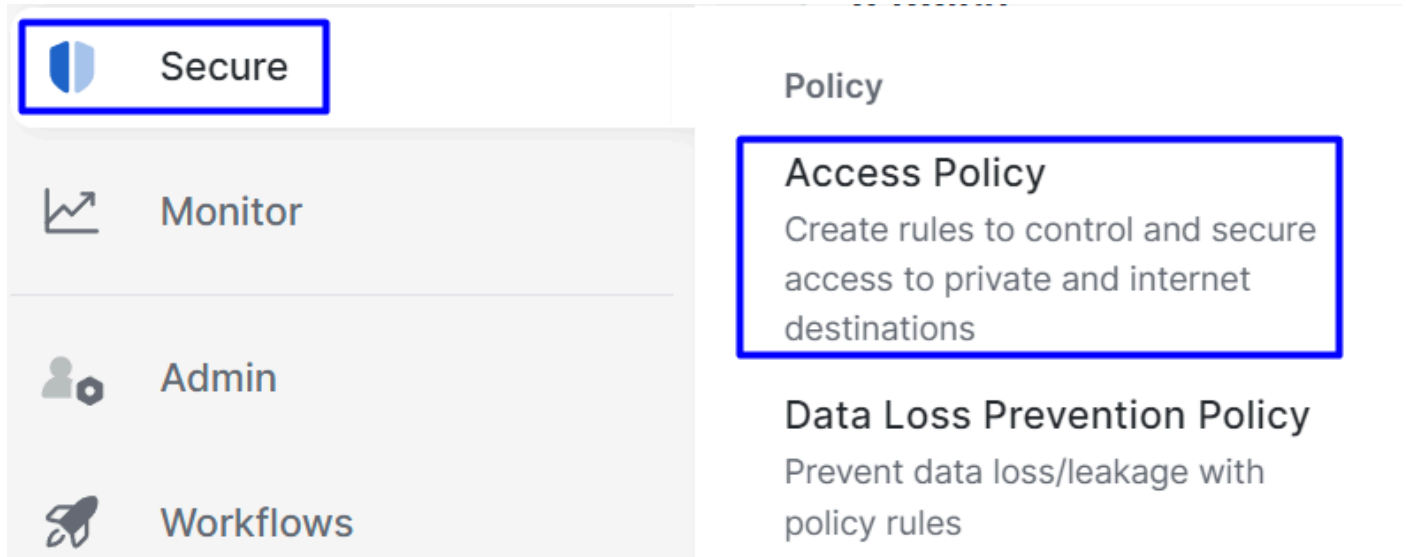


注：デフォルトでは、デフォルトのセキュアアクセスポリシーでインターネットへのトラフィックが許可されます。プライベートアプリケーションへのアクセスを提供するには、プライベートリソースを作成し、それらをプライベートリソースアクセス用のアクセスポリシーに追加する必要があります。

セキュアアクセスでのインターネットアクセスポリシーの設定

インターネットアクセスのアクセスを設定するには、[セキュアアクセスダッシュボード](#)でポリシーを作成する必要があります。

- クリック Secure > Access Policy



- クリック Add Rule > Internet Access

Add Rule ^

Private Access

Control and secure access to resources and applications that cannot be accessed by the general public.

Internet Access

Control and secure access to public destinations from within your network and from managed devices

トンネルの送信元として送信元を指定でき、宛先には、ポリシーで設定する内容に応じて任意のものを選択できます。『[Secure Access User Guide](#)』を確認してください。

ZTNAおよびRA-VPNのプライベートリソースアクセスの設定

プライベートリソースへのアクセスを設定するには、最初に[Secure Access Dashboard](#)でリソースを作成する必要があります。

クリック **Resources > Private Resources**

The screenshot shows the dashboard interface with a left-hand navigation menu and a main content area. The 'Resources' menu item is highlighted with a blue box. The main content area is divided into two columns: 'Sources and destinations' and 'Destinations'. Under 'Sources and destinations', there are three items: 'Registered Networks', 'Internal Networks', and 'Roaming Devices'. Under 'Destinations', there are two items: 'Internet and SaaS Resources' and 'Private Resources'. The 'Private Resources' item is highlighted with a blue box.

Resources	Sources and destinations	Destinations
Secure	Registered Networks Point your networks to our servers	Internet and SaaS Resources Define destinations for internet access rules
Monitor	Internal Networks Define internal network segments to use as sources in access rules	Private Resources Define internal applications and other resources for use in access rules
Admin	Roaming Devices Mac and Windows	
Workflows		

- 次に、ADD

設定の下に、次の設定セクションがあります。General, Communication with Secure Access Cloud and Endpoint Connection Methods。

一般

General

Private Resource Name

SplunkFTD

Description (optional)

- Private Resource Name : ネットワークへのセキュアアクセスを通じてアクセスを提供するリソースの名前を作成します。

エンドポイントの接続方法

Zero-trust connections
Allow endpoints to connect to this resource from outside your network without requiring a VPN connection. [Help](#)

Client-based connection
Allow connections from endpoints that have the Secure Client installed. Enable this option for maximum control over endpoint security requirements (posture).

Remotely Reachable Address (FQDN, Wildcard FQDN, IP Address) ⓘ

[+ FQDN or IP Address](#)

Browser-based connection
Allow browser-based connections from endpoints that do not have the Secure Client installed. Enable this option when devices that your organization does not manage must connect to this resource. Fewer endpoint security checks are possible.

Public URL for this resource ⓘ
 ⓘ

Protocol Server Name Indication (SNI) (optional) ⓘ

Validate Application Certificate ⓘ

- **Zero Trust Connections** : チェックボックスをオンにします。
- **Client-based connection** : これを有効にすると、Secure Client - Zero Trust Module(SGT)を使用して、クライアントベースモードによるアクセスを有効にすることができます。
- **Remote Reachable Address (FQDN, Wildcard FQDN, IP Address)** : リソースのIPまたはFQDNを設定します。FQDNを設定する場合、名前を解決するためにDNSを追加する必要があります。
- **Browser-based connection** : 有効にすると、ブラウザを介してリソースにアクセスできます (HTTPまたはHTTPS通信を使用してリソースを追加してください)
- **Public URL for this resource** : ブラウザから使用するパブリックURLを設定します。セキュアアクセスはこのリソースを保護します。
- **Protocol** : プロトコル (HTTPまたはHTTPS) を選択します。

VPN connections

Allow endpoints to connect to this resource when connected to the network using VPN.

VPN Connection : チェックボックスをオンにして、RA-VPNaaS経由のアクセスを有効にします。

その後、「Save」をクリックすると、そのリソースを「Access Policy」に追加できます。

アクセスポリシーの設定

リソースを作成するときは、次のいずれかのセキュアアクセスポリシーにリソースを割り当てる必要があります。

- クリック **Secure > Access Policy**

The screenshot shows the Azure portal navigation pane on the left with the 'Secure' menu item highlighted in a blue box. The main content area on the right shows the 'Policy' section with 'Access Policy' highlighted in a blue box. Below 'Access Policy' are two other policy options: 'Data Loss Prevention Policy' and 'Data Loss Prevention Policy'.

- [保存 (**Add > Private Resource**

Add Rule ^

Private Access

Control and secure access to resources and applications that cannot be accessed by the general public.

Internet Access

Control and secure access to public destinations from within your network and from managed devices

このプライベートアクセスルールでは、リソースへのアクセスを提供するデフォルト値を設定します。ポリシー設定の詳細については、『[ユーザガイド](#)』を参照してください。

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.

vpn user (vpnuser@ciscospt.es) ×

Information about sources, including selecting multiple sources. [Help](#)

To

Specify one or more destinations.

SplunkFTD ×

Information about destinations, including selecting multiple destinations. [Help](#)

- **Action** : リソースへのアクセスを許可するには、「許可」を選択します。
- **From** : リソースへのログインに使用できるユーザを指定します。
- **To** : セキュアアクセスを介してアクセスするリソースを選択します。

Endpoint Requirements

For zero-trust connections, if endpoints do not meet the specified requirements, this rule will not match the traffic. [Help](#)

Zero-Trust Client-based Posture Profile Rule Defaults

Requirements for end-user devices on which the Cisco Secure Client is installed.

System provided (Client-based)

Private Resources: **SplunkFTD**

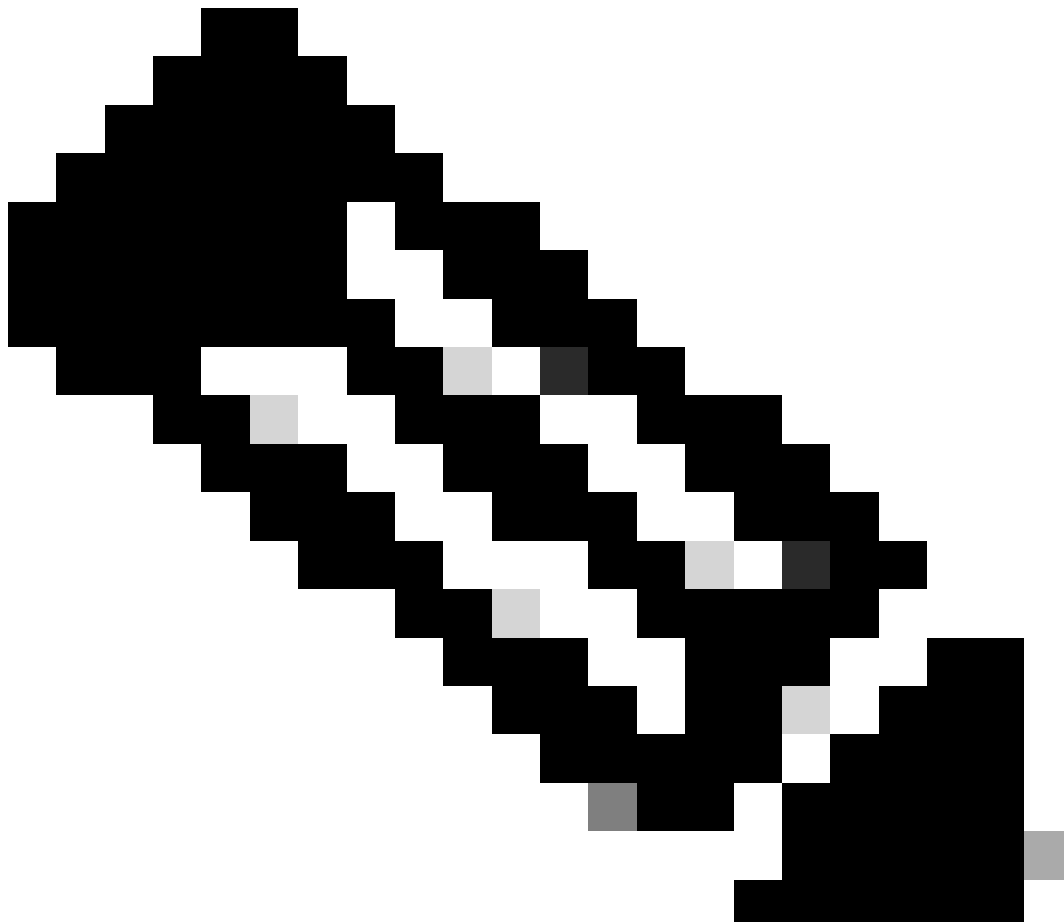
Zero Trust Browser-based Posture Profile Rule Defaults

Requirements for end-user devices on which the Cisco Secure Client is NOT installed.

System provided (Browser-based)

Private Resources: **SplunkFTD**

- **Zero-Trust Client-based Posture Profile** : クライアントベースアクセスのデフォルトプロファイルを選択します。
- **Zero-Trust Browser-based Posture Profile** : デフォルトのプロファイルブラウザのベースアクセスを選択します



注：ポスチャポリシーの詳細については、セキュアアクセスに関する『[ユーザガイド](#)』を参照してください。

その後、NextおよびSaveと設定をクリックすると、RA-VPNおよびクライアントベースZTNAまたはブラウザベースZTNAを介してリソースへのアクセスを試行できます。

トラブルシューティング

セキュアファイアウォールとセキュアアクセス間の通信に基づいてトラブルシューティングを行うには、デバイス間でPhase1(IKEv2)とPhase2(IPSEC)が問題なく確立されているかどうかを確認できます。

フェーズ1(IKEv2)の確認

Phase1を確認するには、FTDのCLIで次のコマンドを実行する必要があります。

```
show crypto isakmp sa
```

この場合、望ましい出力は、セキュアアクセスのデータセンターIPに対して確立された2つの「IKEv2 SAs」であり、望ましいステータスはREADYです。

```
There are no IKEv1 SAs
```

```
IKEv2 SAs:
```

```
Session-id:3, Status:UP-ACTIVE, IKE count:1, CHILD count:1
```

```
Tunnel-id Local Remote
52346451 192.168.0.202/4500 3.120.45.23/4500
Encr: AES-GCM, keysize: 256, Hash: N/A, DH Grp:20, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/4009 sec
Child sa: local selector 0.0.0.0/0 - 255.255.255.255/65535
remote selector 0.0.0.0/0 - 255.255.255.255/65535
ESP spi in/out: 0xfb34754c/0xc27fd2ba
```

```
IKEv2 SAs:
```

```
Session-id:2, Status:UP-ACTIVE, IKE count:1, CHILD count:1
```

```
Tunnel-id Local Remote
52442403 192.168.30.5/4500 18.156.145.74/4500
Encr: AES-GCM, keysize: 256, Hash: N/A, DH Grp:20, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/3891 sec
Child sa: local selector 0.0.0.0/0 - 255.255.255.255/65535
remote selector 0.0.0.0/0 - 255.255.255.255/65535
ESP spi in/out: 0x4af761fd/0xfbca3343
```

フェーズ2(IPSEC)の確認

Phase2を確認するには、FTDのCLIで次のコマンドを実行する必要があります。

```
interface: PrimaryVTI
  Crypto map tag: __vti-crypto-map-Tunnel1-0-1, seq num: 65280, local addr: 192.168.30.5

  Protected vrf (ivrf): Global
  local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  current_peer: 18.156.145.74

  #pkts encaps: 71965, #pkts encrypt: 71965, #pkts digest: 71965
  #pkts decaps: 91325, #pkts decrypt: 91325, #pkts verify: 91325
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 71965, #pkts comp failed: 0, #pkts decomp failed: 0
  #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
  #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
  #TFC rcvd: 0, #TFC sent: 0
  #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
  #send errors: 0, #recv errors: 0

  local crypto endpt.: 192.168.30.5/4500, remote crypto endpt.: 18.156.145.74/4500
  path mtu 1500, ipsec overhead 63(44), media mtu 1500
  PMTU time remaining (sec): 0, DF policy: copy-df
  ICMP error validation: disabled, TFC packets: disabled
  current outbound spi: FBCA3343
  current inbound spi : 4AF761FD

inbound esp sas:
  spi: 0x4AF761FD (1257726461)
  SA State: active
  transform: esp-aes-gcm-256 esp-null-hmac no compression
  in use settings ={L2L, Tunnel, NAT-T-Encaps, IKEv2, VTI, }
  slot: 0, conn_id: 2, crypto-map: __vti-crypto-map-Tunnel1-0-1
  sa timing: remaining key lifetime (kB/sec): (3916242/27571)
  IV size: 8 bytes
  replay detection support: Y
  Anti replay bitmap:
    0xFFFFFFFF 0xFFFFFFFF

outbound esp sas:
  spi: 0xFBCA3343 (4224332611)
  SA State: active
  transform: esp-aes-gcm-256 esp-null-hmac no compression
  in use settings ={L2L, Tunnel, NAT-T-Encaps, IKEv2, VTI, }
  slot: 0, conn_id: 2, crypto-map: __vti-crypto-map-Tunnel1-0-1
  sa timing: remaining key lifetime (kB/sec): (4239174/27571)
  IV size: 8 bytes
  replay detection support: Y
  Anti replay bitmap:
    0x00000000 0x00000001

interface: SecondaryVTI
  Crypto map tag: __vti-crypto-map-Tunnel2-0-2, seq num: 65280, local addr: 192.168.0.202

  Protected vrf (ivrf): Global
  local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
```

current_peer: 3.120.45.23

```
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#TFC rcvd: 0, #TFC sent: 0
#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
#send errors: 0, #recv errors: 0
```

```
local crypto endpt.: 192.168.0.202/4500, remote crypto endpt.: 3.120.45.23/4500
path mtu 1500, ipsec overhead 63(44), media mtu 1500
PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled
current outbound spi: C27FD2BA
current inbound spi : FB34754C
```

inbound esp sas:

```
spi: 0xFB34754C (4214519116)
SA State: active
transform: esp-aes-gcm-256 esp-null-hmac no compression
in use settings ={L2L, Tunnel, NAT-T-Encaps, IKEv2, VTI, }
slot: 0, conn_id: 20, crypto-map: __vti-crypto-map-Tunnel2-0-2
sa timing: remaining key lifetime (kB/sec): (4101120/27412)
IV size: 8 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001
```

outbound esp sas:

```
spi: 0xC27FD2BA (3263156922)
SA State: active
transform: esp-aes-gcm-256 esp-null-hmac no compression
in use settings ={L2L, Tunnel, NAT-T-Encaps, IKEv2, VTI, }
slot: 0, conn_id: 20, crypto-map: __vti-crypto-map-Tunnel2-0-2
sa timing: remaining key lifetime (kB/sec): (4239360/27412)
IV size: 8 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001
```

最後の出力では、両方のトンネルが確立されたことが確認できます。望ましくない結果は、パケットencapsおよびdecapsの次の出力です。

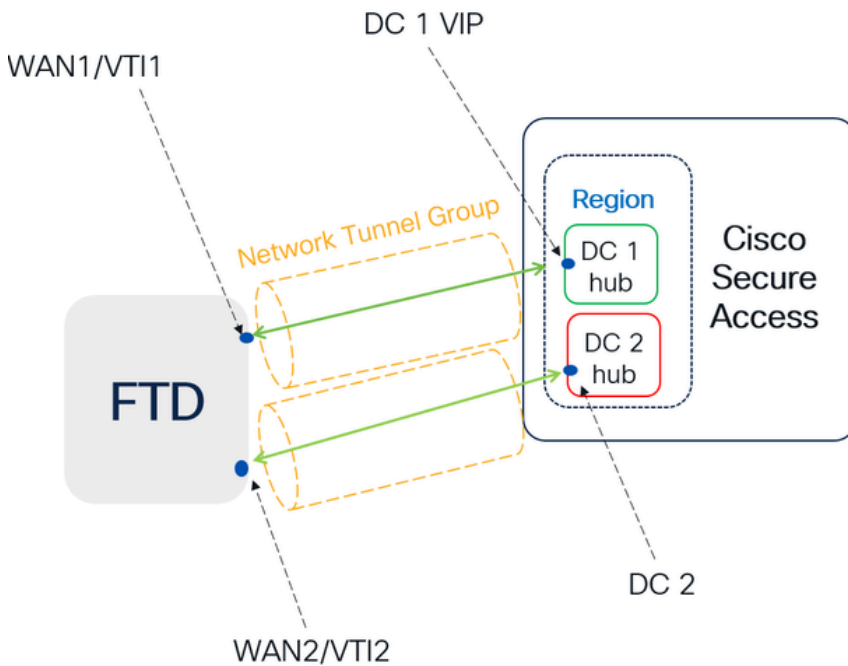
```
#pkts encaps: 71965, #pkts encrypt: 71965, #pkts digest: 71965 → Packets forwarded to Secure Access
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0 → No packets forwarded from Secure
#pkts compressed: 0, #pkts decompressed: 0 → Access to your firewall
#pkts not compressed: 71965, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#TFC rcvd: 0, #TFC sent: 0
#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
#send errors: 0, #recv errors: 0
```

このシナリオがある場合は、TACでケースをオープンします。

ハイアベイラビリティ機能

クラウド内のデータセンターと通信するセキュアアクセスを備えたトンネルの機能はアクティブ/パッシブです。つまり、DC 1のドアだけがトラフィックを受信するために開かれます。DC 2のドアは、トンネル番号1がダウンするまで閉じられます。

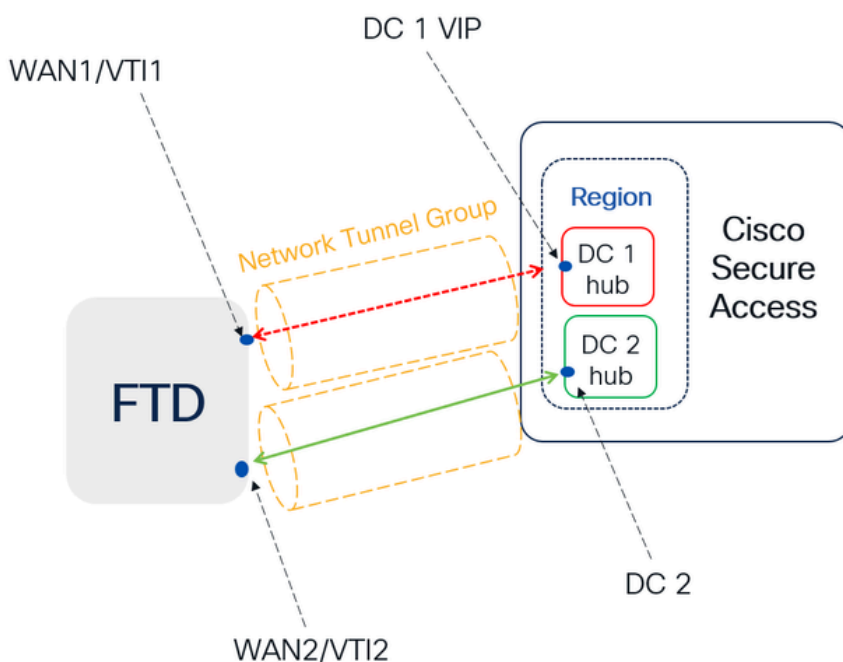
Normal Behavior



Secure Access default behavior

- DC2 is **passive** when DC1 is **active**
- Data Centers operating in High Availability (HA) mode ensure that only one tunnel receives traffic at a time. The other tunnel remains on standby and will drop any packets sent through it while in standby mode.

HA Behavior



Secure Access HA Behavior

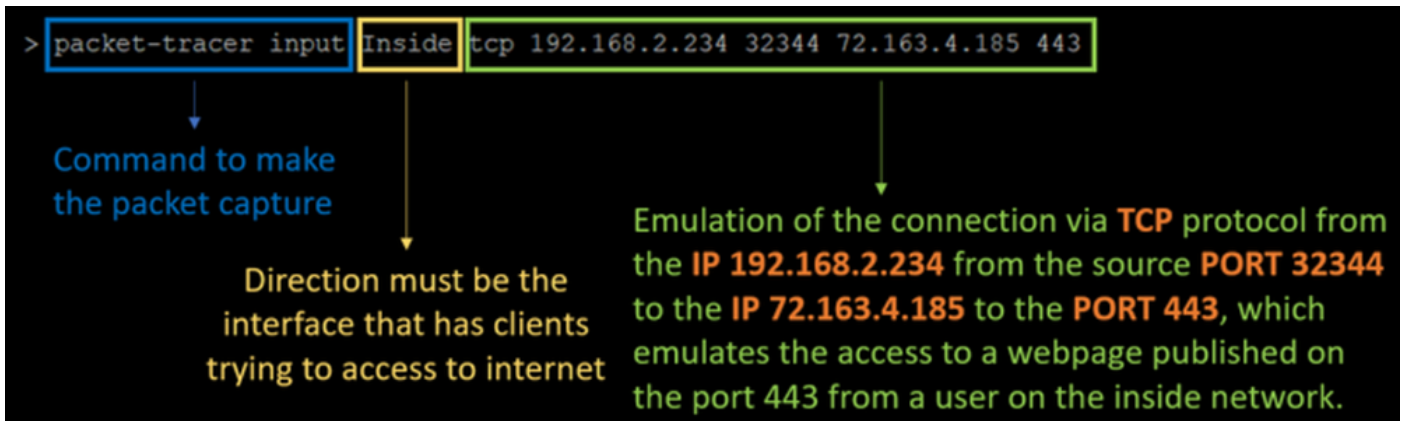
- DC2 is **Active** when DC1 or WAN1 peer is **Down**
- High availability is implemented to address failures in the WAN1 channel on the Firewall, ensuring operational continuity in the **region** and mitigating potential issues in DC1

セキュアなアクセスへのトラフィックルーティングの確認

この例では、送信元をファイアウォールネットワーク上のマシンとして使用します。

- Source:192.168.10.40
- 宛先 : 146.112.255.40 (セキュアアクセスモニタリングIP)

以下に例を挙げます。



コマンド :

```
packet-tracer input LAN tcp 192.168.10.40 3422 146.112.255.40 80
```

出力 :

```
Phase: 1
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Elapsed time: 14010 ns
Config:
Implicit Rule
Additional Information:
MAC Access list
```

```
Phase: 2
Type: PBR-LOOKUP
Subtype: policy-route
Result: ALLOW
Elapsed time: 21482 ns
Config:
route-map FMC_GENERATED_PBR_1707686032813 permit 5
  match ip address ACL
  set ip next-hop 169.254.2.2 169.254.3.2
Additional Information:
Matched route-map FMC_GENERATED_PBR_1707686032813, sequence 5, permit
Found next-hop 169.254.2.2 using egress ifc PrimaryVTI
```

Phase: 3
Type: OBJECT_GROUP_SEARCH
Subtype:
Result: ALLOW
Elapsed time: 0 ns
Config:
Additional Information:
Source Object Group Match Count: 0
Destination Object Group Match Count: 0
Object Group Search: 0

Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Elapsed time: 233 ns
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip any ifc PrimaryVTI any rule-id 268434435
access-list CSM_FW_ACL_ remark rule-id 268434435: ACCESS POLICY: HOUSE - Mandatory
access-list CSM_FW_ACL_ remark rule-id 268434435: L7 RULE: New-Rule-#3-ALLOW
Additional Information:
This packet will be sent to snort for additional processing where a verdict will be reached

Phase: 5
Type: CONN-SETTINGS
Subtype:
Result: ALLOW
Elapsed time: 233 ns
Config:
class-map class_map_Any
match access-list Any
policy-map policy_map_LAN
class class_map_Any
set connection decrement-ttl
service-policy policy_map_LAN interface LAN
Additional Information:

Phase: 6
Type: NAT
Subtype: per-session
Result: ALLOW
Elapsed time: 233 ns
Config:
Additional Information:

Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Elapsed time: 233 ns
Config:
Additional Information:

Phase: 8
Type: VPN
Subtype: encrypt
Result: ALLOW
Elapsed time: 18680 ns
Config:
Additional Information:

Phase: 9
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Elapsed time: 25218 ns
Config:
Additional Information:

Phase: 10
Type: NAT
Subtype: per-session
Result: ALLOW
Elapsed time: 14944 ns
Config:
Additional Information:

Phase: 11
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Elapsed time: 0 ns
Config:
Additional Information:

Phase: 12
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Elapsed time: 19614 ns
Config:
Additional Information:
New flow created with id 23811, packet dispatched to next module

Phase: 13
Type: EXTERNAL-INSPECT
Subtype:
Result: ALLOW
Elapsed time: 27086 ns
Config:
Additional Information:
Application: 'SNORT Inspect'

Phase: 14
Type: SNORT
Subtype: appid
Result: ALLOW
Elapsed time: 28820 ns
Config:
Additional Information:
service: (0), client: (0), payload: (0), misc: (0)

Phase: 15
Type: SNORT
Subtype: firewall
Result: ALLOW
Elapsed time: 450193 ns
Config:
Network 0, Inspection 0, Detection 0, Rule ID 268434435
Additional Information:
Starting rule matching, zone 1 -> 3, geo 0 -> 0, vlan 0, src sgt: 0, src sgt type: unknown, dst sgt: 0,
Matched rule ids 268434435 - Allow


```
Result:
input-interface: LAN(vrfid:0)
input-status: up
input-line-status: up
output-interface: PrimaryVTI(vrfid:0)
output-status: up
output-line-status: up
Action: allow
Time Taken: 620979 ns
```

ここでは、通信に関するコンテキストを提供し、PBR設定の下ですべてが正しく行われているかどうかを確認して、トラフィックをセキュアアクセスに正しくルーティングする方法について、多くの情報が提供されています。

```
Phase: 2
Type: PBR-LOOKUP
Subtype: policy-route
Result: ALLOW
Elapsed time: 21482 ns
Config:
route-map FMC_GENERATED_PBR_1707686032813 permit 5
  match ip address ACL
  set ip next-hop 169.254.2.2 169.254.3.2
Additional Information:
  Matched route-map FMC GENERATED PBR 1707686032813, sequence 5, permit
  Found next-hop 169.254.2.2 using egress ifc PrimaryVTI
```

フェーズ2は、トラフィックがPrimaryVTIインターフェイスに転送されていることを示します。このシナリオの設定に基づくと、インターネットトラフィックはVTIを介してセキュアアクセスに転送される必要があるため、これは正しいです。

Phase: 8

Type: VPN

Subtype: encrypt

Result: ALLOW

Elapsed time: 18680 ns

Config:

Additional Information:

Phase: 9

Type: VPN

Subtype: ipsec-tunnel-flow

Result: ALLOW

Elapsed time: 25218 ns

Config:

Additional Information:

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。