

Configuration d'un accès sécurisé avec pare-feu sécurisé haute disponibilité

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Diagramme du réseau](#)

[Configurer](#)

[Configurer le VPN sur un accès sécurisé](#)

[Données pour la configuration du tunnel](#)

[Configurer le tunnel sur Secure Firewall](#)

[Configuration de l'interface du tunnel](#)

[Configuration de la route statique pour l'interface secondaire](#)

[Configurer le VPN pour un accès sécurisé en mode VTI](#)

[Configuration des terminaux](#)

[Configuration IKE](#)

[Configuration IPSEC](#)

[Configuration avancée](#)

[Scénarios de configuration des politiques d'accès](#)

[Scénario d'accès Internet](#)

[Escenario RA-VPN](#)

[Escenario ZTNA CLAP-BAP](#)

[Configurer le routage de base de stratégie](#)

[Configurer la stratégie d'accès Internet sur l'accès sécurisé](#)

[Configuration de l'accès aux ressources privées pour ZTNA et RA-VPN](#)

[Dépannage](#)

[Vérification de Phase 1 \(IKEv2\)](#)

[Vérification de Phase2 \(IPSEC\)](#)

[Fonction de haute disponibilité](#)

[Vérification du routage du trafic pour un accès sécurisé](#)

[Informations connexes](#)

Introduction

Ce document décrit comment configurer l'accès sécurisé avec le pare-feu sécurisé à haute disponibilité.

Conditions préalables

- [Configurer le provisionnement utilisateur](#)
- [Configuration de l'authentification ZTNA SSO](#)
- [Configuration de l'accès sécurisé VPN à distance](#)

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Firepower Management Center 7.2
- Défense contre les menaces Firepower 7.2
- Accès sécurisé
- Client sécurisé Cisco - VPN
- Client sécurisé Cisco - ZTNA
- ZTNA sans client

Composants utilisés

Les informations contenues dans ce document sont basées sur :

- Firepower Management Center 7.2
- Défense contre les menaces Firepower 7.2
- Accès sécurisé
- Client sécurisé Cisco - VPN
- Client sécurisé Cisco - ZTNA

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales



CISCO

Secure

Access

Secure Firewall

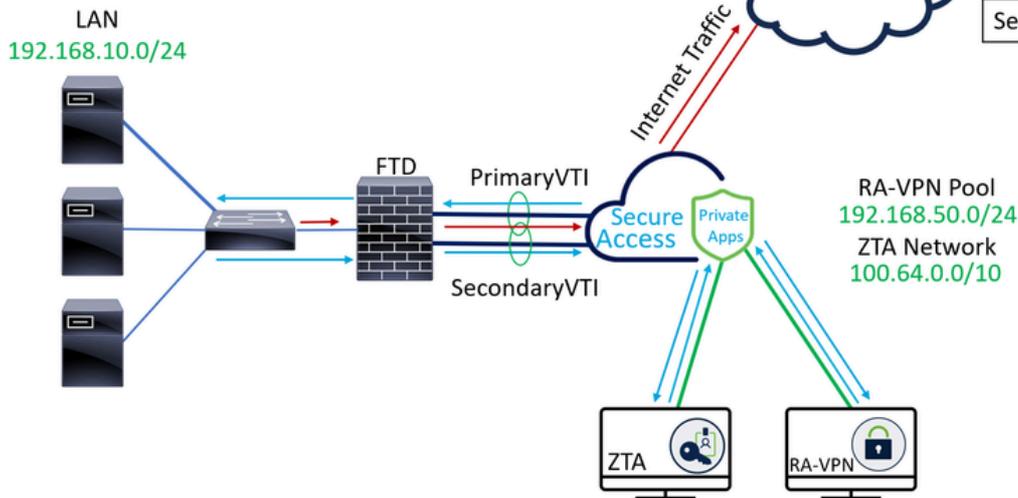
FTD

Cisco a conçu Secure Access pour protéger et fournir un accès aux applications privées, sur site et dans le cloud. Il protège également la connexion du réseau à Internet. Pour ce faire, plusieurs méthodes et couches de sécurité sont mises en oeuvre, toutes visant à préserver les informations lorsqu'elles y accèdent via le cloud.

Diagramme du réseau

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

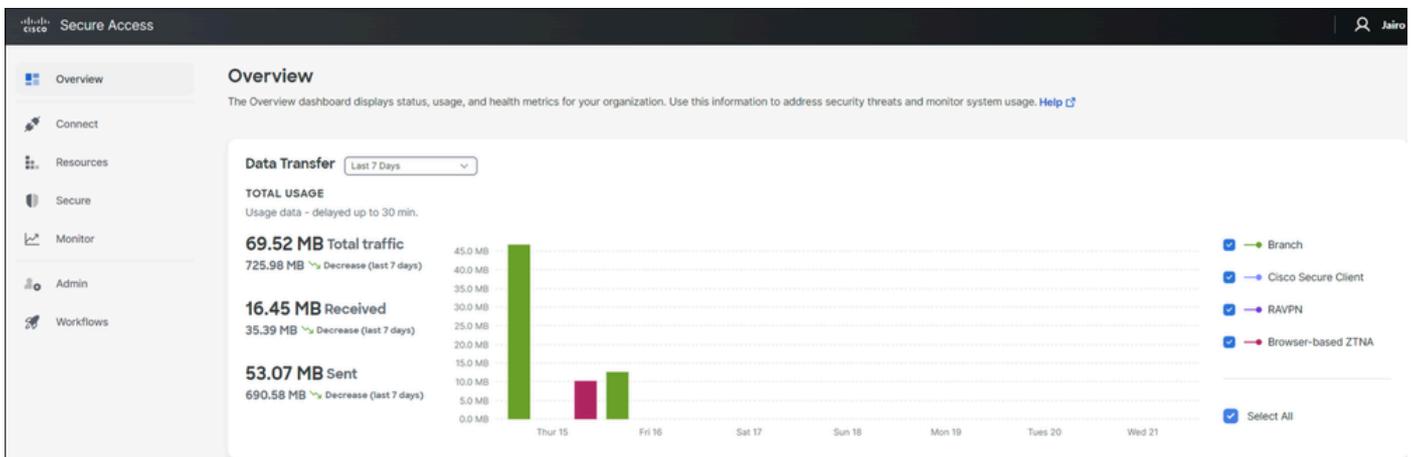
| INTERFACE | IP |
|--------------|---------------|
| PrimaryWAN | 192.168.30.5 |
| PrimaryVTI | 169.254.2.1 |
| SecondaryWAN | 192.168.0.202 |
| SecondaryVTI | 169.254.3.1 |



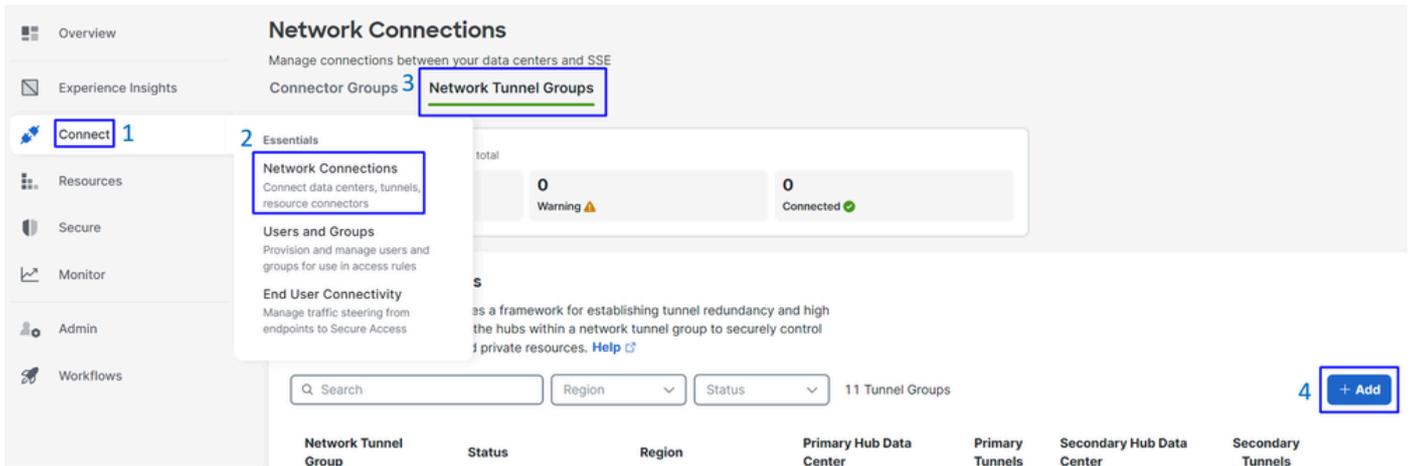
Configurer

Configurer le VPN sur un accès sécurisé

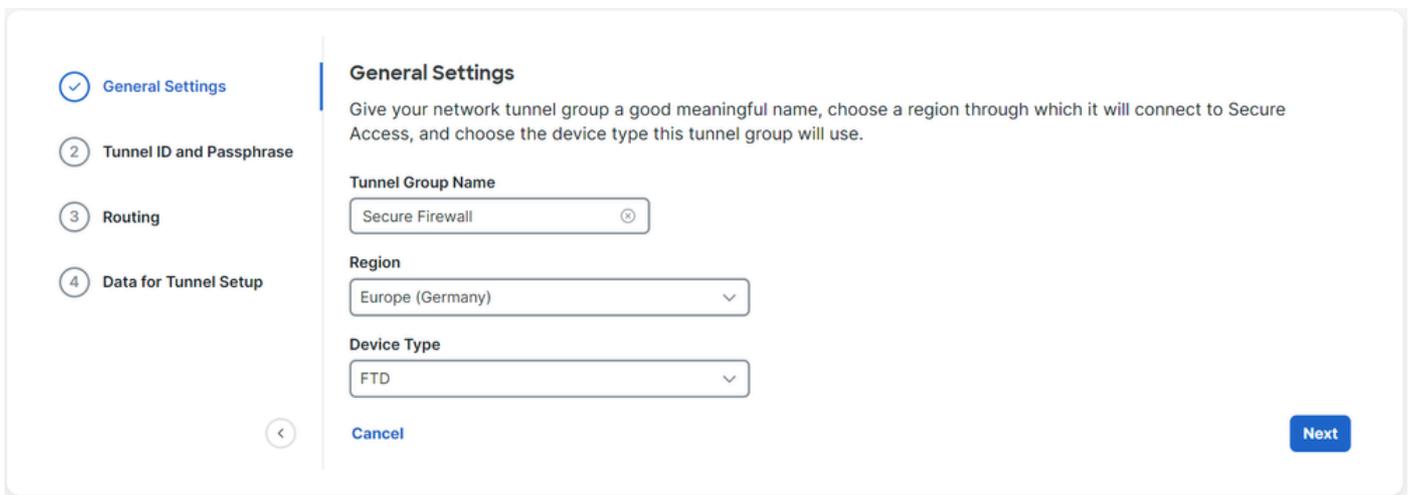
Accédez au panneau d'administration de [Accès sécurisé](#).



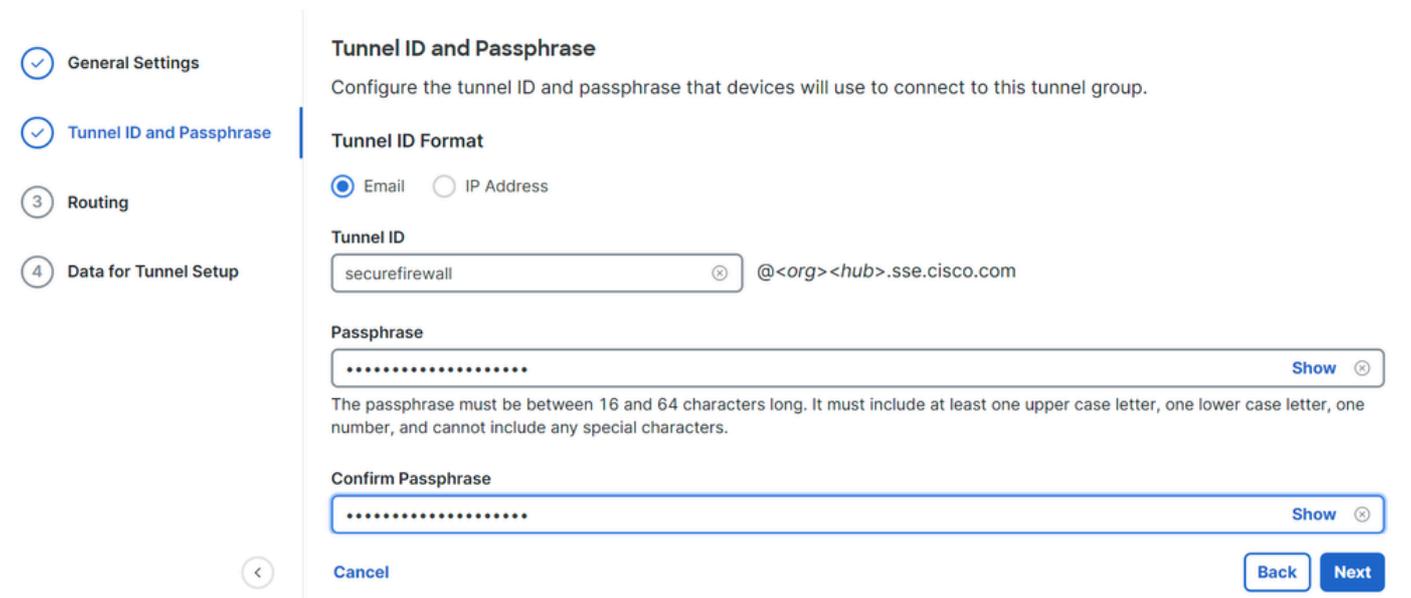
- Cliquez sur Connect > Network Connections
- Sous Network Tunnel Groups Cliquez sur + Add



- Configurer Tunnel Group Name, Region et Device Type
- Cliquer Next



- Configurez les Tunnel ID Format et Passphrase
- Cliquer Next



- Configurez les plages d'adresses IP ou les hôtes que vous avez configurés sur votre réseau

et souhaitez faire passer le trafic par un accès sécurisé

- Cliquer **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](#)

Après avoir cliqué sur **save** les informations sur le tunnel s'affiche, veuillez enregistrer ces informations pour l'étape suivante, **Configure the tunnel on Secure Firewall**.

Données pour la configuration du tunnel

- 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 <input type="checkbox"/> |
| Primary Data Center IP Address: | 18.156.145.74 <input type="checkbox"/> |
| Secondary Tunnel ID: | securefirewall@[redacted]-sse.cisco.com <input type="checkbox"/> |
| Secondary Data Center IP Address: | 3.120.45.23 <input type="checkbox"/> |
| Passphrase: | [redacted] <input type="checkbox"/> |

[Download CSV](#)

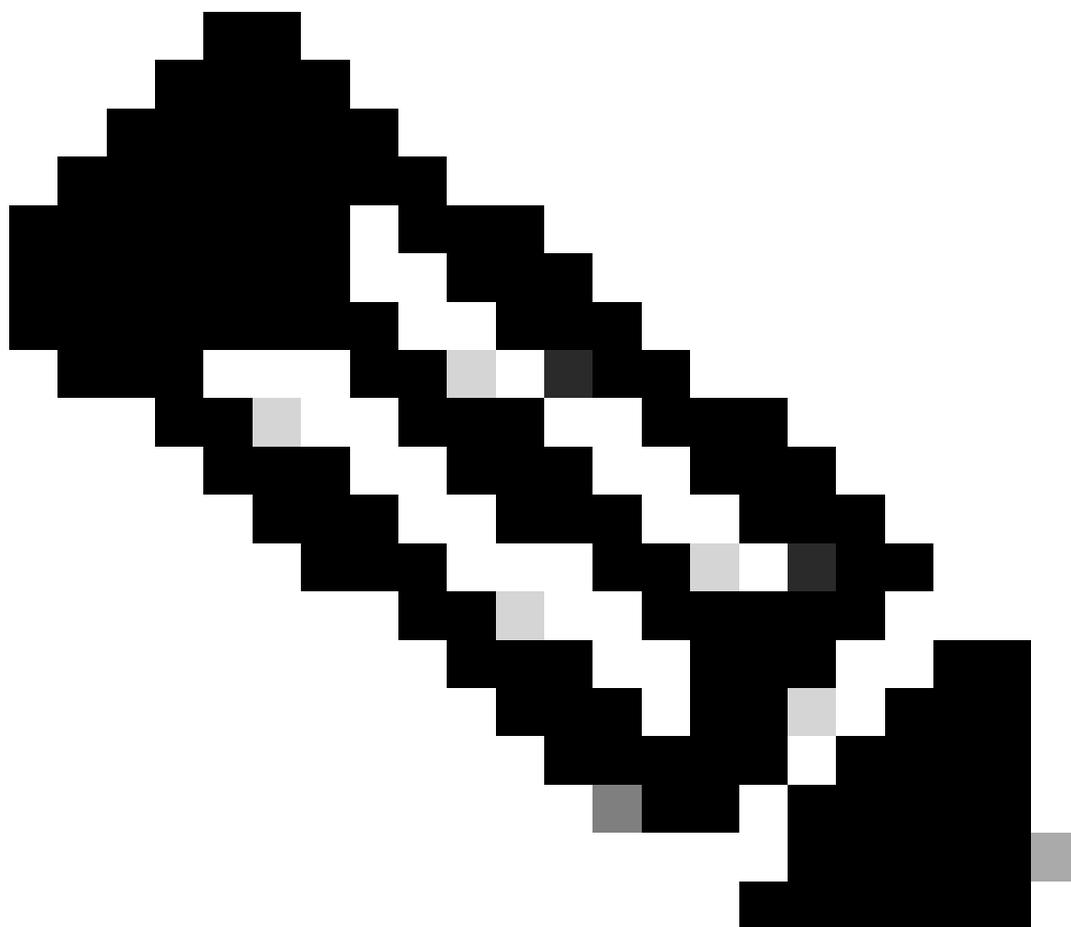
[Done](#)

Configurer le tunnel sur Secure Firewall

Configuration de l'interface du tunnel

Pour ce scénario, vous utilisez la configuration de l'interface de tunnel virtuel (VTI) sur le pare-feu sécurisé pour atteindre cet objectif ; n'oubliez pas que, dans ce cas, vous disposez d'un FAI double et que nous voulons disposer d'une haute disponibilité en cas de défaillance de l'un de vos FAI.

| INTERFACES | RÔLE |
|----------------|--|
| WAN principal | WAN Internet principal |
| WAN secondaire | WAN Internet secondaire |
| VTI principal | Lié pour envoyer le trafic via l' Principal Internet WAN accès sécurisé |
| VTI secondaire | Lié pour envoyer le trafic via l' Secondary Internet WAN accès sécurisé |



Remarque : 1. Vous devez ajouter ou attribuer une route statique à l' **Primary or Secondary Datacenter IP** pour pouvoir activer les deux tunnels.



Remarque : 2. Si vous avez configuré le protocole ECMP entre les interfaces, vous n'avez pas besoin de créer de route statique vers le **Primary or Secondary Datacenter IP** pour que les deux tunnels soient opérationnels.

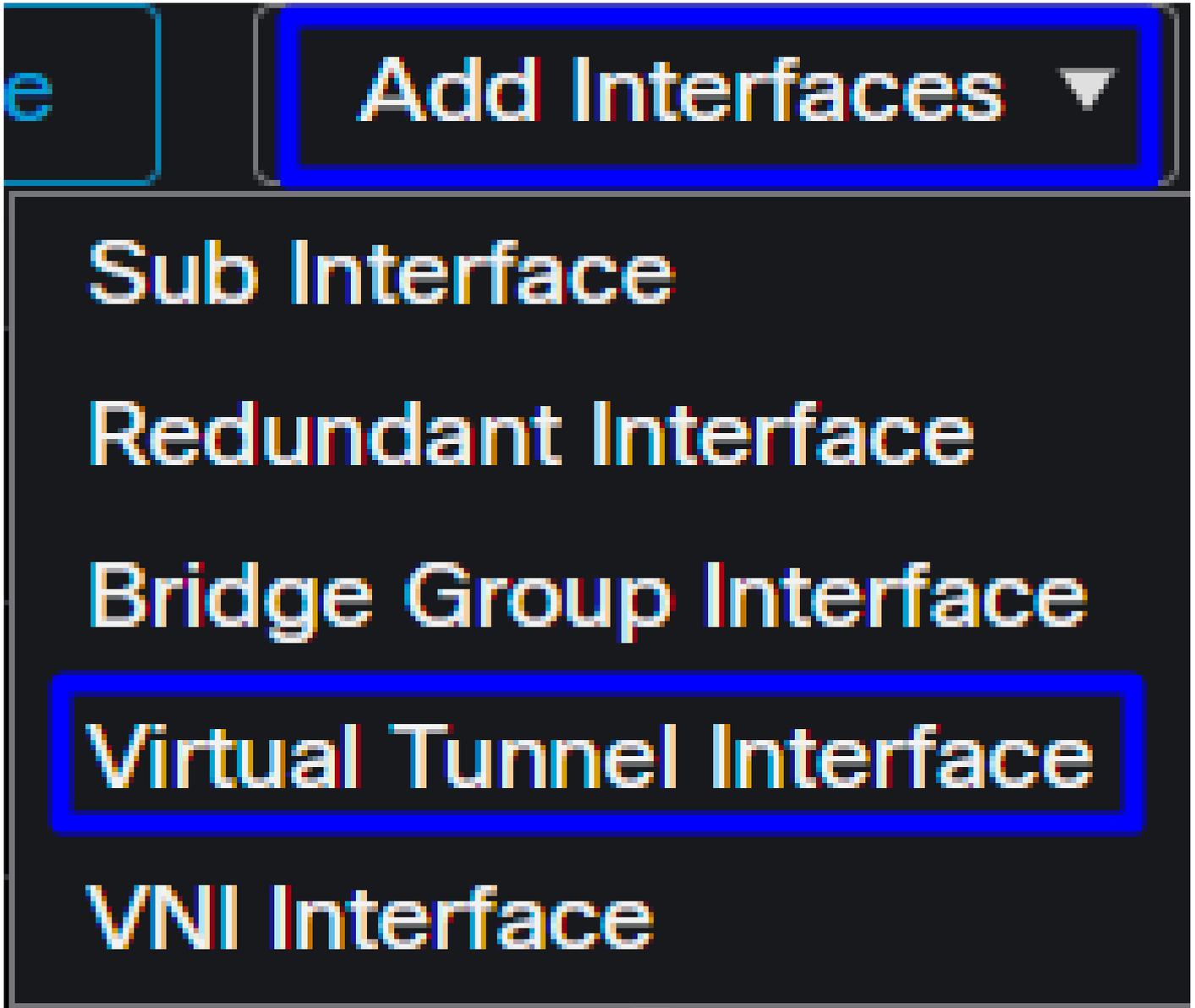
En fonction du scénario, nous avons **PrimaryWAN** et **SecondaryWAN**, que nous devons utiliser pour créer les interfaces VTI.

Accédez à votre **Firepower Management Center** > **Devices**.

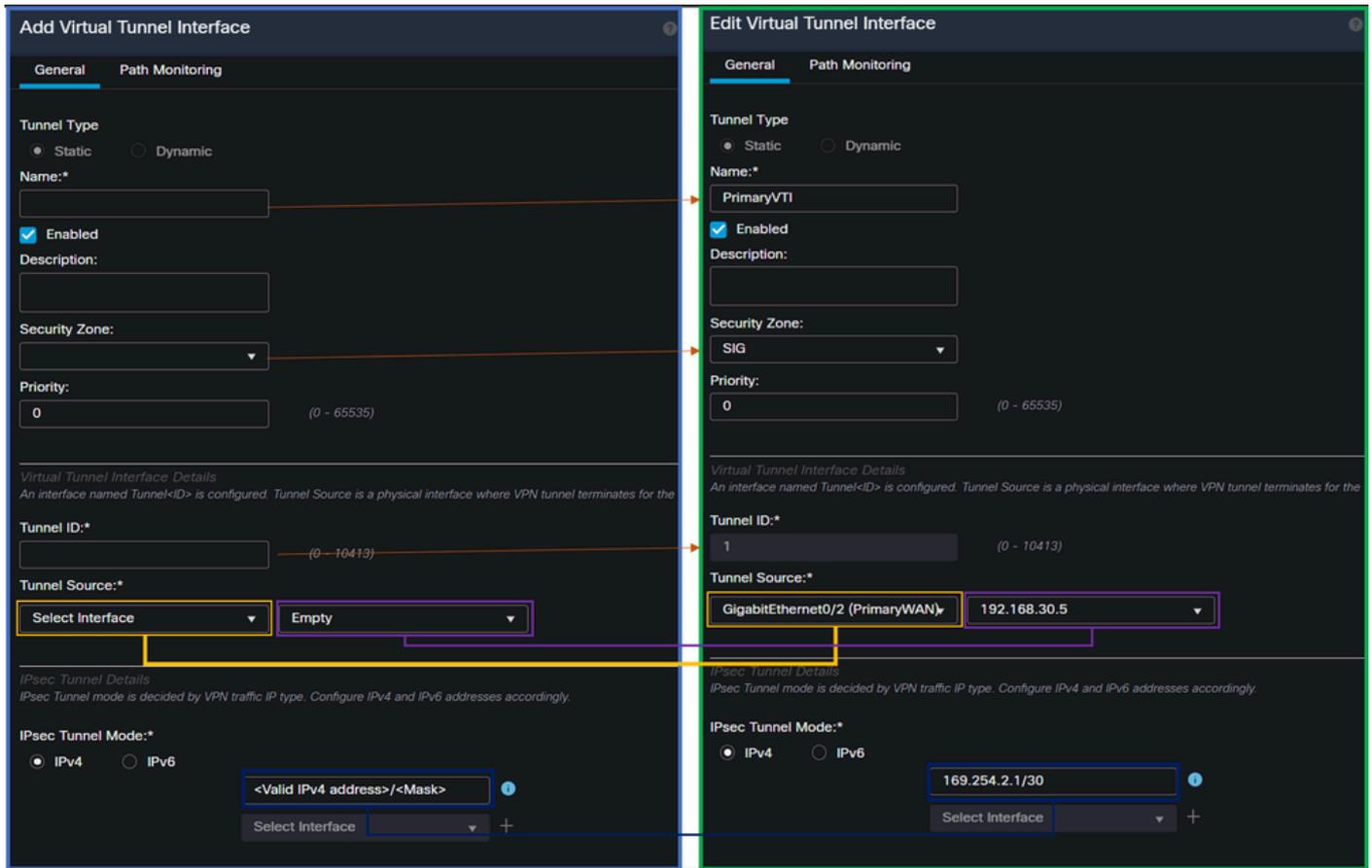
- Choisissez votre FTD
- Choisir **Interfaces**

| 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) |

- Cliquez sur **Add Interfaces > Virtual Tunnel Interface**



- Configurez l'interface en fonction des informations suivantes



- **Name** : Configurez un nom qui fait référence à la **PrimaryWAN** interface
- **Security Zone** : Vous pouvez en réutiliser un autre **Security Zone**, mais en créer un nouveau pour le trafic d'accès sécurisé est préférable
- **Tunnel ID** : Ajouter un numéro pour l'ID de tunnel
- **Tunnel Source** : Choisissez votre **PrimaryWAN** interface et choisissez l'adresse IP privée ou publique de votre interface
- **IPsec Tunnel Mode** : Choisissez **IPv4** et configurez une adresse IP non routable dans votre réseau avec le masque 30



Remarque : Pour l'interface VTI, vous devez utiliser une adresse IP non routable ; par exemple, si vous disposez de deux interfaces VTI, vous pouvez utiliser 169.254.2.1/30 pour le **PrimaryVTI** et 169.254.3.1/30 pour le **SecondaryVTI**.

Après cela, vous devez faire la même chose pour le **SecondaryWAN** interface, et vous avez tout configuré pour la haute disponibilité VTI, et par conséquent, vous avez le résultat suivant :

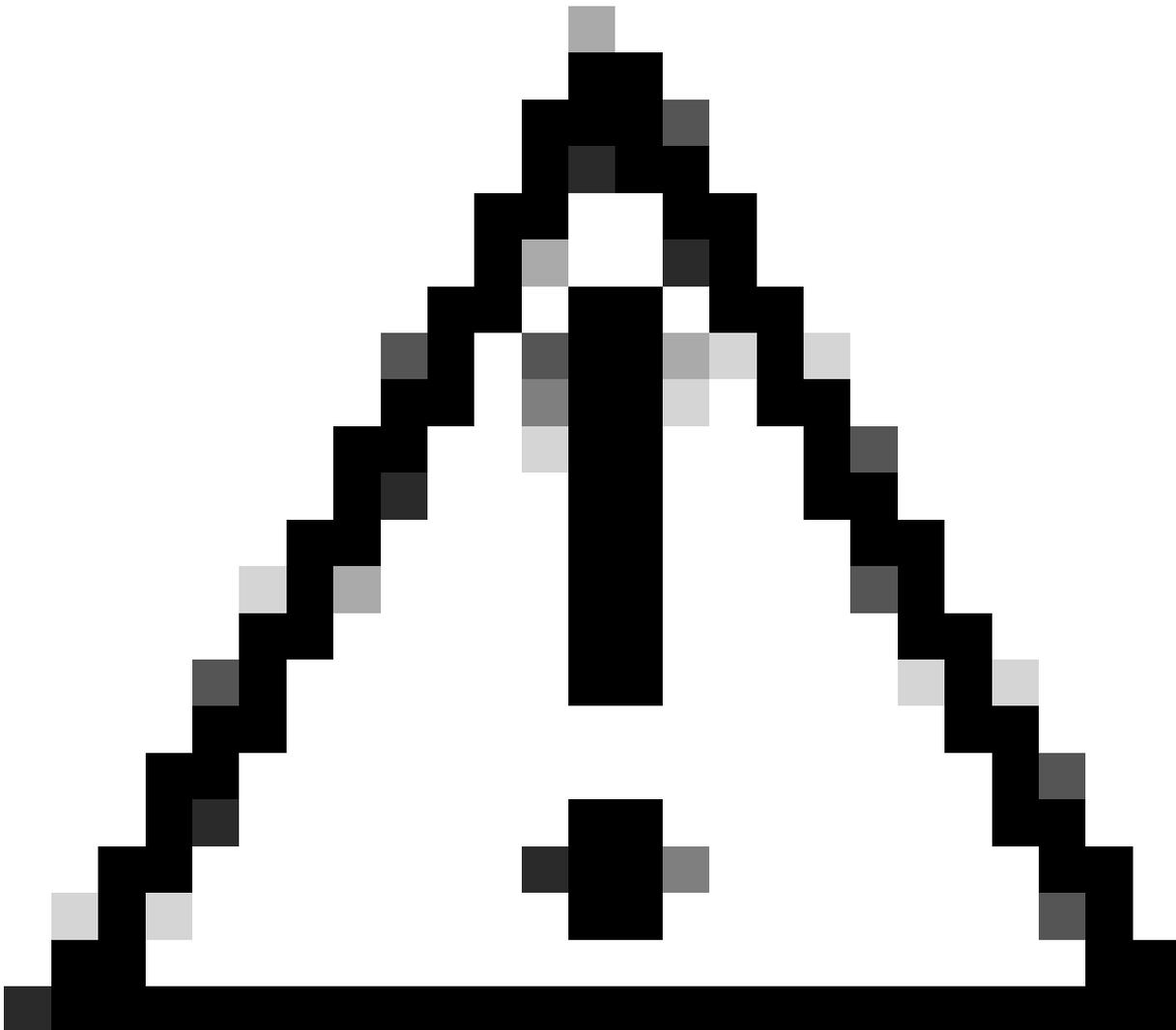
| Interface | Logical Name | Type | Security Zones | MAC Address (Active/Standby) | IP Address |
|--------------------|--------------|----------|----------------|------------------------------|--------------------------|
| Diagnostic0/0 | diagnostic | Physical | | | |
| GigabitEthernet0/0 | SecondaryWAN | 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) |

Dans ce scénario, les adresses IP utilisées sont les suivantes :

| Configuration IP VTI | | |
|----------------------|----------------|-------------------------|
| Nom logique | IP | Plage |
| VTI principal | 169.254.2.1/30 | 169.254.2.1-169.254.2.2 |
| VTI secondaire | 169.254.3.1/30 | 169.254.3.1-169.254.3.2 |

Configuration de la route statique pour l'interface secondaire

Pour permettre au trafic du **Secondary WAN interface** d'atteindre le **Secondary Datacenter IP Address**, vous devez configurer une route statique vers l'adresse IP du centre de données. Vous pouvez le configurer avec une métrique de un (1) pour le placer au-dessus de la table de routage ; spécifiez également l'adresse IP en tant qu'hôte.



Mise en garde : Cela n'est nécessaire que si vous n'avez pas de configuration ECMP entre les canaux WAN ; si vous avez configuré ECMP, vous pouvez passer à l'étape suivante.

Naviguez jusqu'à **Device > Device Management**

- Cliquez sur votre périphérique FTD
- Cliquez sur **Routing**
- Choisir **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

GWT1

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: Sélectionnez l'interface WAN secondaire
- Gateway: Sélectionnez la passerelle WAN secondaire
- Selected Network: Ajouter l'adresse IP du data center secondaire en tant qu'hôte ; vous pouvez trouver les informations sur les informations données quand vous configurez le tunnel sur l'étape d'accès sécurisé, [Données pour la configuration du tunnel](#)

- **Metric:** Utiliser un (1)
- Cliquez sur **Save** et pour enregistrer les informations, puis procédez au déploiement.

| 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 | | | | | | |

Configurer le VPN pour un accès sécurisé en mode VTI

Pour configurer le VPN, accédez à votre pare-feu :

- Cliquez sur **Devices > Site to Site**
- Cliquez sur **+ Site to Site VPN**

Configuration des terminaux

Pour configurer l'étape Endpoints, vous devez utiliser les informations fournies sous l'étape, [Data for Tunnel Setup](#).

Create New VPN Topology

Topology Name:*

Policy Based (Crypto Map) **Route Based (VTI)**

Network Topology:

IKE Version:* IKEv1 **IKEv2**

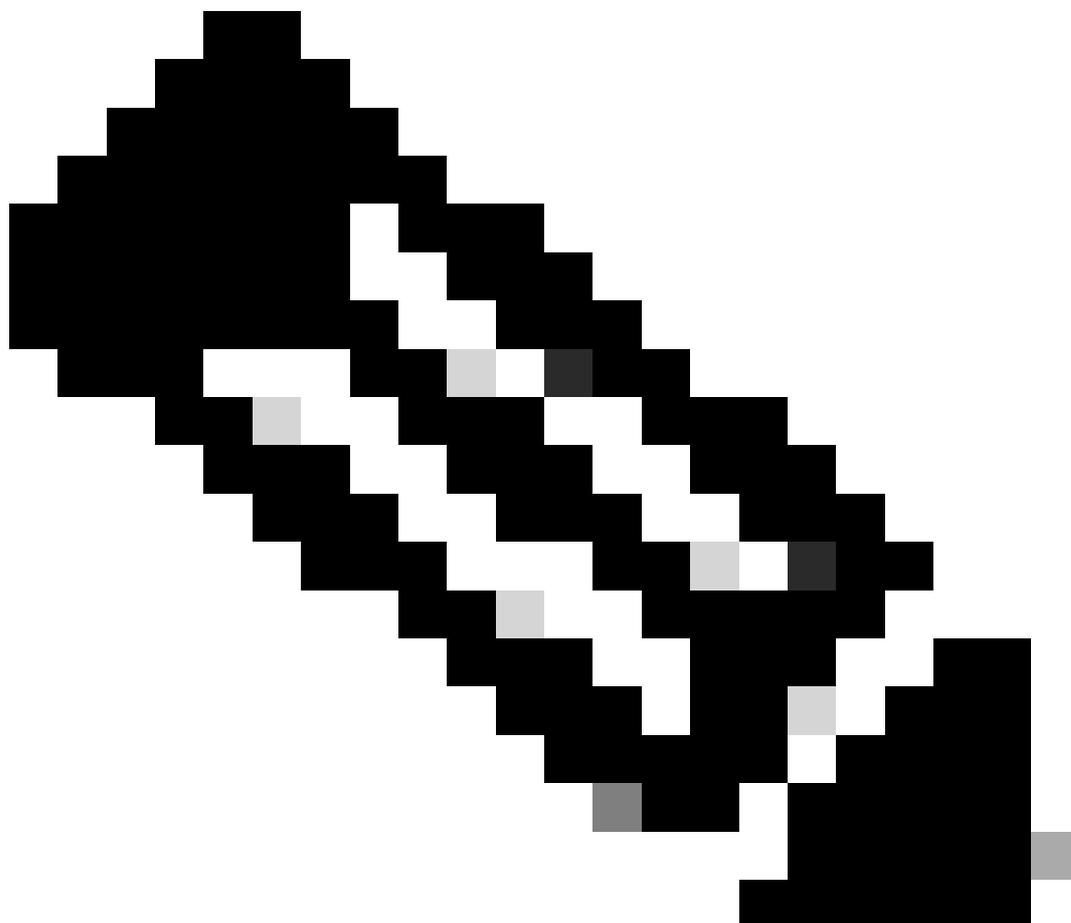
Endpoints | IKE | IPsec | Advanced

| | |
|--|---|
| 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](#)

- Nom de topologie : Créez un nom lié à l'intégration Secure Access
- Choisir **Routed Based (VTI)**

- Choisir **Point to Point**
 - IKE Version: Choisir **IKEv2**
-



Remarque : IKEv1 n'est pas pris en charge pour l'intégration avec Secure Access.

Sous la **Node A**, vous devez configurer les paramètres suivants :

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@

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

- **Device:** Choisissez votre périphérique FTD
- **Virtual Tunnel Interface:** Sélectionnez la VTI associée à la PrimaryWAN Interface.
- Cochez la case correspondant à **Send Local Identity to Peers**
- **Local Identity Configuration:** Choisissez Email ID, et remplissez les informations en fonction des **Primary Tunnel ID** données fournies dans votre configuration à l'étape [Data for Tunnel Setup](#)

Après avoir configuré les informations sur le, PrimaryVTI cliquez sur + Add Backup VTI:

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:** Sélectionnez la VTI associée à la PrimaryWAN Interface.
- Cochez la case correspondant à **Send Local Identity to Peers**
- **Local Identity Configuration:** Choisissez Email ID, et remplissez les informations en fonction des **Secondary Tunnel ID** données fournies dans votre configuration à l'étape [Data for Tunnel Setup](#)

Sous la **Node B**, vous devez configurer les paramètres suivants :

Node B

Device:*

Extranet

Device Name*:

SecureAccess

Endpoint IP Address*:

18.156.145.74, 3.120.45.23

- Device: Extranet
- Device Name: Choisissez un nom pour reconnaître l'accès sécurisé comme destination.
- Endpoint IP Address: La configuration pour le principal et le secondaire doit être Primaire **Datacenter IP**, **Secondary Datacenter IP**, vous pouvez trouver ces informations dans l'étape, [Données pour la configuration du tunnel](#)

Après cela, votre configuration pour **Endpoints** est terminée et vous pouvez maintenant passer à l'étape Configuration IKE.

Configuration IKE

Pour configurer les paramètres IKE, cliquez sur **IKE**.

Endpoints

IKE

IPsec

Advanced

Sous IKE, vous devez configurer les paramètres suivants :

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:** Vous pouvez utiliser la configuration Umbrella par défaut, Umbrella-AES-GCM-256 ou configurer un autre paramètre en fonction de la [Supported IKEv2 and IPSEC Parameters](#)
- **Authentication Type:** Clé manuelle pré-partagée
- **Key et Confirm Key** Vous pouvez trouver les **Passphrase** informations dans l'étape, [Données pour la configuration du tunnel](#)

Après cela, votre configuration pour IKE est terminée et vous pouvez maintenant passer à l'étape Configuration IPSEC.

Configuration IPSEC

Pour configurer les paramètres IPSEC, cliquez sur IPSEC.

Endpoints

IKE

IPsec

Advanced

Sous IPSEC, vous devez configurer les paramètres suivants :

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

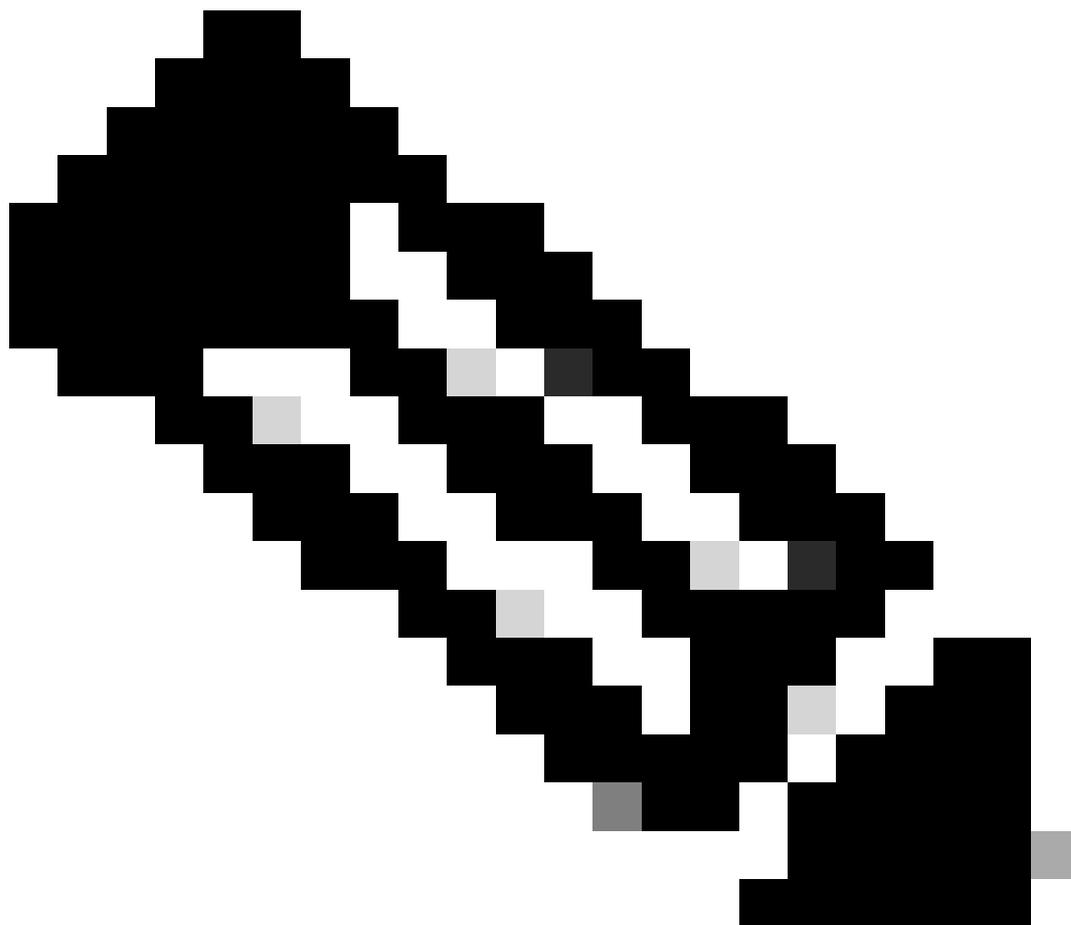
Enable Perfect Forward Secrecy

Modulus Group: 14

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

Lifetime Size: 4608000 Kbytes (Range 10-2147483647)

- Policies: Vous pouvez utiliser la configuration Umbrella par défaut, Umbrella-AES-GCM-256 ou configurer un autre paramètre en fonction de la [Supported IKEv2 and IPSEC Parameters](#)



Remarque : Rien d'autre n'est requis sur IPSEC.

Après cela, votre configuration pour IPSEC est terminée et vous pouvez maintenant passer à l'étape Configuration avancée.

Configuration avancée

Pour configurer les paramètres avancés, cliquez sur Advanced (Avancé).

Endpoints

IKE

IPsec

Advanced

Sous **Advanced**, vous devez configurer les paramètres suivants :

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

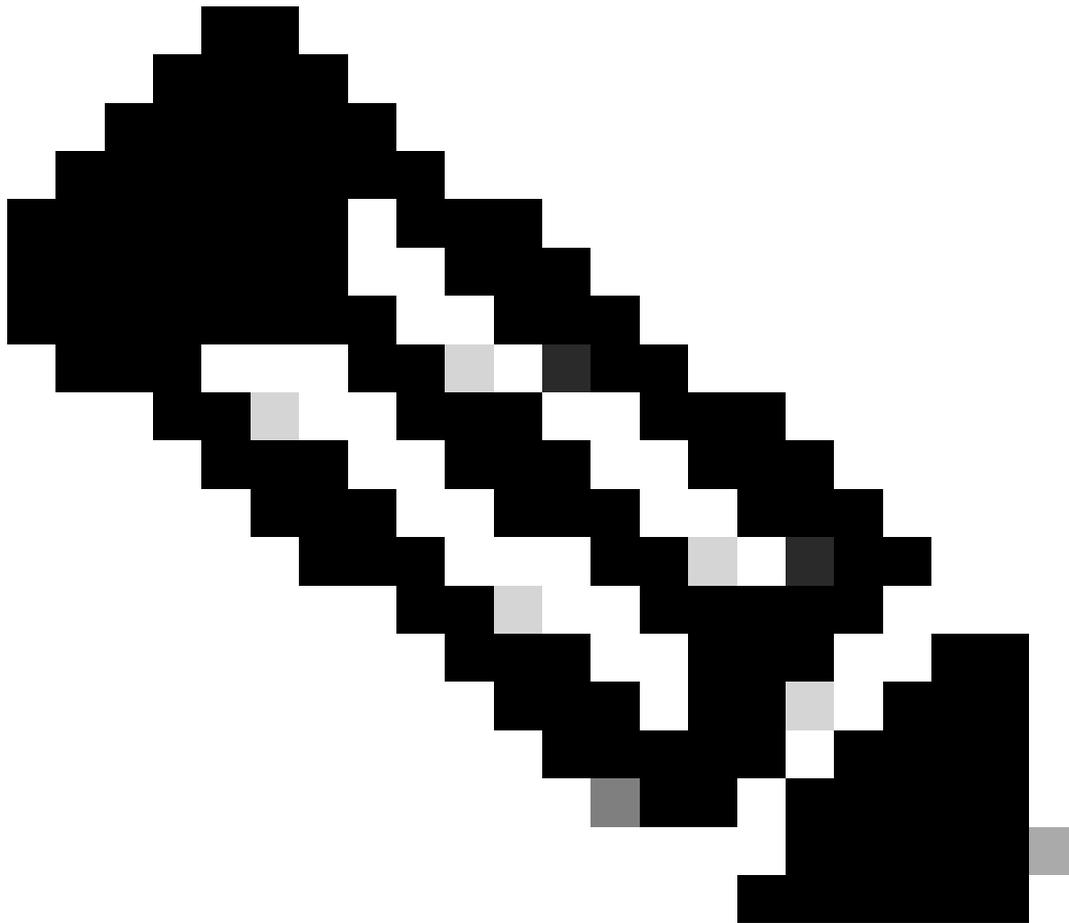
Enable Notification on Tunnel Disconnect

IKEv2 Security Association (SA) Settings

Cookie Challenge: custom

- IKE Keepalive: Activer
- Threshold: 10
- Retry Interval: 2
- Identity Sent to Peers: AutoOuDN
- Peer Identity Validation: Ne pas vérifier

Après cela, vous pouvez cliquer sur **Save** et **Deploy**.



Remarque : Après quelques minutes, vous voyez le VPN établi pour les deux noeuds.

| 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) |

Après cela, votre configuration pour le VPN to Secure Access in VTI Mode est terminée et vous pouvez maintenant passer à l'étape, **Configure Policy Base Routing**.



Avertissement : Le trafic vers l'accès sécurisé est transféré uniquement vers le tunnel principal lorsque les deux tunnels sont établis ; si le principal est désactivé, l'accès sécurisé autorise le transfert du trafic via le tunnel secondaire.

Remarque : le basculement sur le site d'accès sécurisé est basé sur les valeurs DPD documentées dans le [guide de l'utilisateur](#) pour les valeurs IPsec prises en charge.

Scénarios de configuration des politiques d'accès

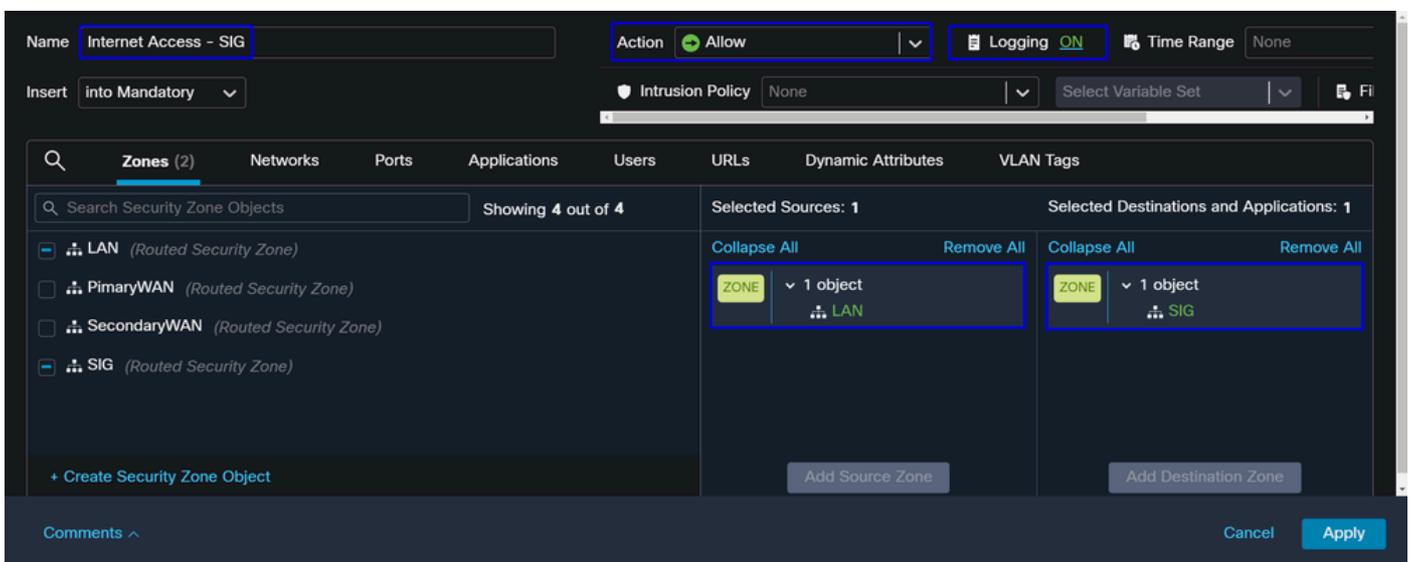
Les règles de stratégie d'accès définies sont basées sur :

| 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) |

| Interface | Zone |
|----------------|------|
| VTI principal | SIG |
| VTI secondaire | SIG |
| LAN | LAN |

Scénario d'accès Internet

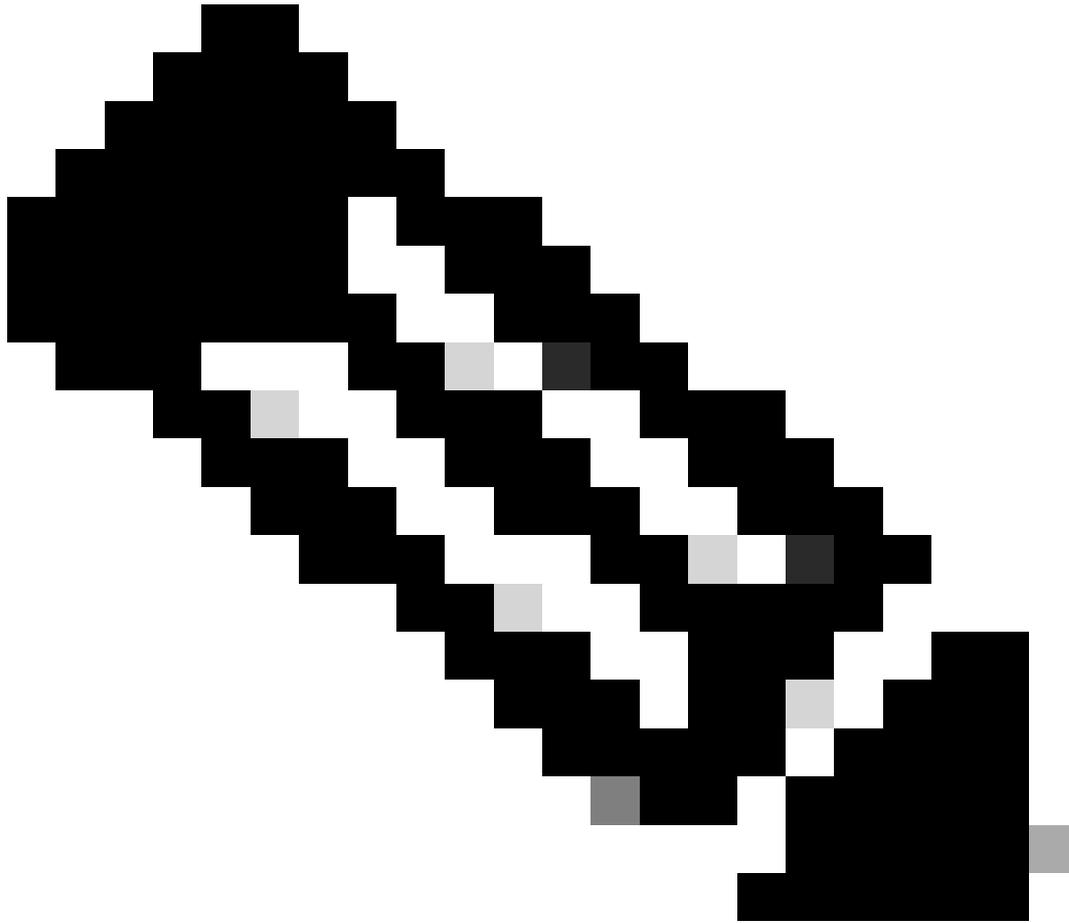
Pour fournir l'accès à Internet à toutes les ressources que vous configurez sur le routage de base de stratégie, vous devez configurer certaines règles d'accès ainsi que certaines stratégies d'accès sécurisé. Permettez-moi donc d'expliquer comment y parvenir dans ce scénario :



Cette règle permet d'accéder LAN à Internet et, dans ce cas, Internet est SIG.

Escenario RA-VPN

Pour fournir un accès à partir des utilisateurs RA-VPN, vous devez le configurer en fonction de la plage que vous avez attribuée sur le pool RA-VPN.



Remarque : Pour configurer votre stratégie RA-VPNaaS, vous pouvez passer par [Manage Virtual Private Networks](#)

Comment vérifiez-vous le pool d'adresses IP de votre VPNaaS ?

Accédez à votre tableau de [bord Secure Access](#)

- Cliquez sur **Connect > End User Connectivity**
- Cliquez sur **Virtual Private Network**
- Sous **Manage IP Pools**, cliquez sur **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

2 Regions mapped

Manage

- Vous voyez votre piscine en dessous **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 |

- Vous devez autoriser cette plage sous SIG, mais vous devez également l'ajouter sous la liste de contrôle d'accès que vous configurez dans votre PBR.

Configuration des règles d'accès

Si vous ne configurez l'accès sécurisé que pour l'utiliser avec les capacités d'accès aux ressources d'applications privées, votre règle d'accès peut ressembler à ceci :

The screenshot shows the configuration of an Access Control List (ACL) rule. The rule is named "Private APP" and is set to "Allow" with logging enabled. The source is configured with two selected networks: "192.168.10.153" and "192.168.50.0/24". The destination is configured with one selected network: "LAN". The interface shows a list of available networks and geolocations on the left, and a summary of selected sources and destinations on the right.

Cette règle autorise le trafic du pool RA-VPN 192.168.50.0/24 vers votre LAN ; vous pouvez en spécifier davantage si nécessaire.

Configuration ACL

Pour autoriser le trafic de routage de SIG vers votre LAN, vous devez l'ajouter sous la liste de contrôle d'accès pour qu'il fonctionne sous le PBR.

| 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 | |

Escenario ZTNA CLAP-BAP

Vous devez configurer votre réseau sur la base de la plage CGNAT 100.64.0.0/10 pour fournir un accès à votre réseau à partir des utilisateurs Client Base ZTA ou Browser Base ZTA.

Configuration des règles d'accès

Si vous ne configurez l'accès sécurisé que pour l'utiliser avec les capacités d'accès aux ressources d'applications privées, votre règle d'accès peut ressembler à ceci :

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

Showing 27 out of 27

Selected Sources: 2

- ZONE SIG
- NET 100.64.0.0/10 (CGNAT RANGE)

Selected Destinations and Applications: 1

- ZONE LAN

Cette règle autorise le trafic de la plage ZTNA CGNAT 100.64.0.0/10 vers votre réseau local.

Configuration ACL

Pour autoriser le trafic de routage de SIG à votre LAN à l'aide de CGNAT, vous devez l'ajouter sous la liste de contrôle d'accès pour qu'il fonctionne sous le PBR.

| 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 | |

Configurer le routage de base de stratégie

Pour fournir un accès aux ressources internes et à Internet via l'accès sécurisé, vous devez créer des routes via le routage PBR (Policy Base Routing) qui facilitent le routage du trafic de la source à la destination.

- Naviguez jusqu'à **Devices > Device Management**
- Choisissez le périphérique FTD où vous créez la route

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

- Cliquez sur **Routing**
- Choisir **Policy Base Routing**
- Cliquer **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](#)

Dans ce scénario, vous sélectionnez toutes les interfaces que vous utilisez comme source pour acheminer le trafic vers l'accès sécurisé ou pour fournir une authentification utilisateur vers l'accès sécurisé à l'aide de RA-VPN ou d'un accès ZTA basé sur le client ou le navigateur aux ressources internes du réseau :

- Sous **Ingress Interface**, sélectionnez toutes les interfaces qui envoient le trafic via **Secure Access** :

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

- Sous **Critères de correspondance** et **Interface de sortie**, vous définissez les paramètres suivants après avoir cliqué sur **Add**:

Match Criteria and Egress Interface

Specify forward action for chosen match criteria.

Add

Add Forwarding Actions

Match ACL:* +

Send To:*

IPv4 Addresses:

IPv6 Addresses:

Don't Fragment:

Internal Sources

Match ACL:*

Send To:*

IPv4 Addresses:

IPv6 Addresses:

Don't Fragment:

- **Match ACL:** Pour cette liste de contrôle d'accès, vous configurez tout ce que vous routez vers l'accès sécurisé :

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:

Entries (2)

| Sequence | Action | Source | Source Port | Destination | Destination Port |
|----------|--------|-----------------|-------------|----------------------------------|------------------|
| 1 | Block | Any | Any | 208.67.222.222 208.67.222.220 | 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:** Choisir une adresse IP
- **IPv4 Addresses:** Vous devez utiliser l'adresse IP suivante sous le masque 30 configuré sur les deux VTI ; vous pouvez vérifier que dans l'étape, [VTI Interface Config](#)

| Interface | IP | GW |
|----------------|----------------|-------------|
| VTI principal | 169.254.2.1/30 | 169.254.2.2 |
| VTI secondaire | 169.254.3.1/30 | 169.254.3.2 |



Après l'avoir configuré comme cela, vous obtenez le résultat suivant et vous pouvez continuer en cliquant sur **Save**:

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**

Default Interface

IPv4 settings IPv6 settings

Recursive: For example, 192.168.0.1

Default: For example, 192.168.0.1, 10.10.10.1

Peer Address

Verify Availability +

Cancel **Save**

Après cela, vous devez le **Save** reconfigurer, et vous l'avez configuré de la manière suivante :

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 **Add**

Specify forward action for chosen match criteria.

| Match ACL | Forwarding Action |
|------------|--|
| ACL | Send through 169.254.2.2 169.254.3.2 → Send the traffic to the PrimaryVTI |

If PrimaryVTI fail it will send the traffic to the SecondaryVTI

Cancel **Save**

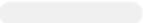
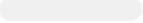
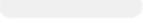
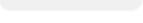
Après cela, vous pouvez déployer et vous voyez le trafic des machines configurées sur la liste de contrôle d'accès acheminer le trafic vers l'accès sécurisé :

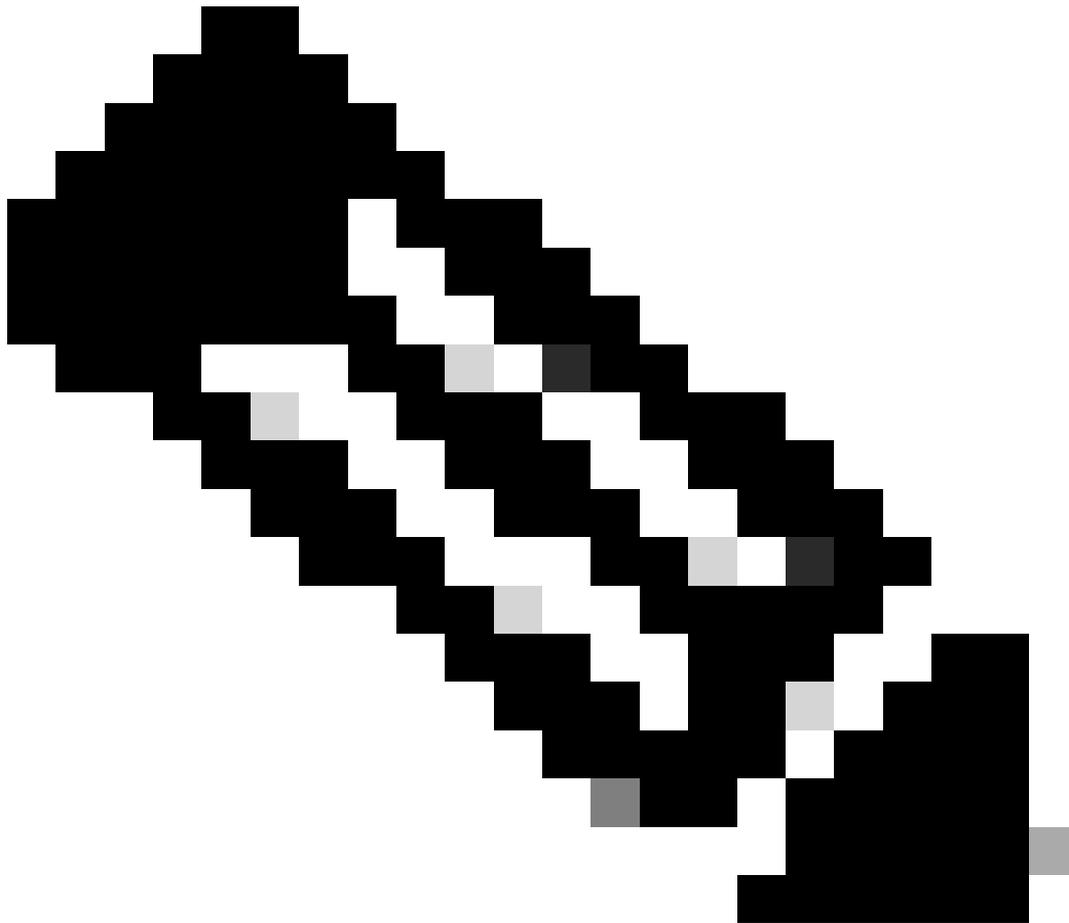
À partir de la **Conexion Events** dans le FMC :

| <input type="checkbox"/> | Action x | Initiator IP x | Responder IP x | ↓ Application Risk x | Access Control Policy x | Ingress Interface x | Egress Interface x |
|----------------------------|----------|----------------|----------------|----------------------|-------------------------|---------------------|--------------------|
| ▼ <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 |

À partir de la **Activity Search** dans Accès sécurisé :

40,678 Total  Viewing activity from Mar 13, 2024 12:30 AM to Mar 14, 2024 12:30 AM Page: 1  Results per page

| 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 | |



Remarque : Par défaut, la stratégie d'accès sécurisé par défaut autorise le trafic vers Internet. Pour fournir l'accès aux applications privées, vous devez créer des ressources privées et les ajouter à la stratégie d'accès pour l'accès aux ressources privées.

Configurer la stratégie d'accès Internet sur l'accès sécurisé

Pour configurer l'accès à Internet, vous devez créer la stratégie sur votre tableau de [bord d'accès sécurisé](#) :

- Cliquez sur **Secure > Access Policy**



Secure



Monitor



Admin



Workflows

Policy

Access Policy

Create rules to control and secure access to private and internet destinations

Data Loss Prevention Policy

Prevent data loss/leakage with policy rules

- Cliquez sur `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

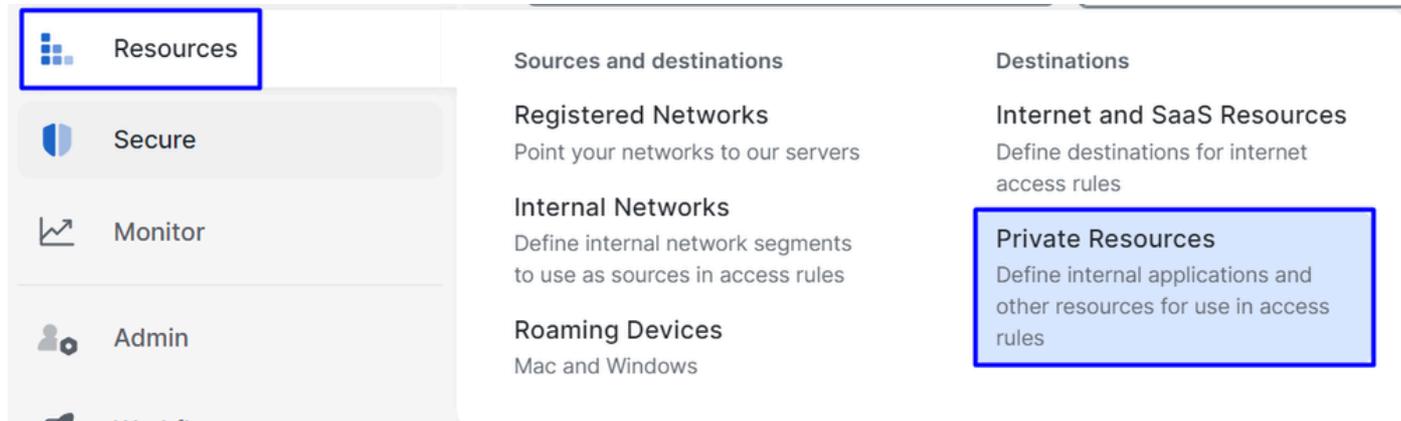
Control and secure access to public destinations from within your network and from managed devices

Là, vous pouvez spécifier la source comme tunnel, et vers la destination, vous pouvez choisir n'importe lequel, en fonction de ce que vous voulez configurer sur la politique. Consultez le [Guide de l'utilisateur Secure Access](#).

Configuration de l'accès aux ressources privées pour ZTNA et RA-VPN

Pour configurer l'accès pour les ressources privées, vous devez d'abord créer les ressources sous le tableau de [bord d'accès sécurisé](#) :

Cliquez sur **Resources > Private Resources**



- Cliquez ensuite sur **ADD**

Sous la configuration, vous trouverez les sections suivantes à configurer : **General, Communication with Secure Access Cloud and Endpoint Connection Methods.**

Généralités

General

Private Resource Name

Description (optional)

- Private Resource Name : Créez un nom pour la ressource à laquelle vous accordez un accès sécurisé à votre réseau

Méthodes de connexion Endpoint

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 ⓘ
 https:// ⓘ

Protocol Server Name Indication (SNI) (optional) ⓘ

Validate Application Certificate ⓘ

- **Zero Trust Connections:** Cochez la case.
- **Client-based connection:** Si vous l'activez, vous pouvez utiliser le module Secure Client - Zero Trust pour activer l'accès via le mode client-base.
- **Remote Reachable Address (FQDN, Wildcard FQDN, IP Address) :** Configurez les ressources IP ou FQDN ; si vous configurez le nom de domaine complet, vous devez ajouter le DNS pour résoudre le nom.
- **Browser-based connection:** si vous l'activez, vous pouvez accéder à vos ressources via un navigateur (veuillez ajouter uniquement des ressources avec une communication HTTP ou HTTPS)
- **Public URL for this resource:** Configurez l'URL publique que vous utilisez via le navigateur ; Secure Access protège cette ressource.
- **Protocol:** Sélectionnez le protocole (HTTP ou HTTPS)

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

VPN Connection: Cochez cette case pour activer l'accès via RA-VPNaaS.

Après cela, cliquez sur *Save* et vous pourrez ajouter cette ressource à la *Access Policy*.

Configurer la stratégie d'accès

Lorsque vous créez la ressource, vous devez l'affecter à l'une des stratégies d'accès sécurisé :

- Cliquez sur **Secure > Access Policy**



Secure



Monitor



Admin



Workflows

Policy

Access Policy

Create rules to control and secure access to private and internet destinations

Data Loss Prevention Policy

Prevent data loss/leakage with policy rules

- Cliquer **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

Pour cette règle d'accès privé, vous configurez les valeurs par défaut pour fournir l'accès à la ressource. Pour en savoir plus sur les configurations des stratégies, consultez le [Guide de l'utilisateur](#).

1 Specify Access

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

Action

| | |
|--|--|
| <input checked="" type="radio"/> Allow Allow specified traffic if security requirements are met. | <input type="radio"/> Block Block specified traffic. |
|--|--|

From

Specify one or more sources.

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

To

Specify one or more destinations.

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

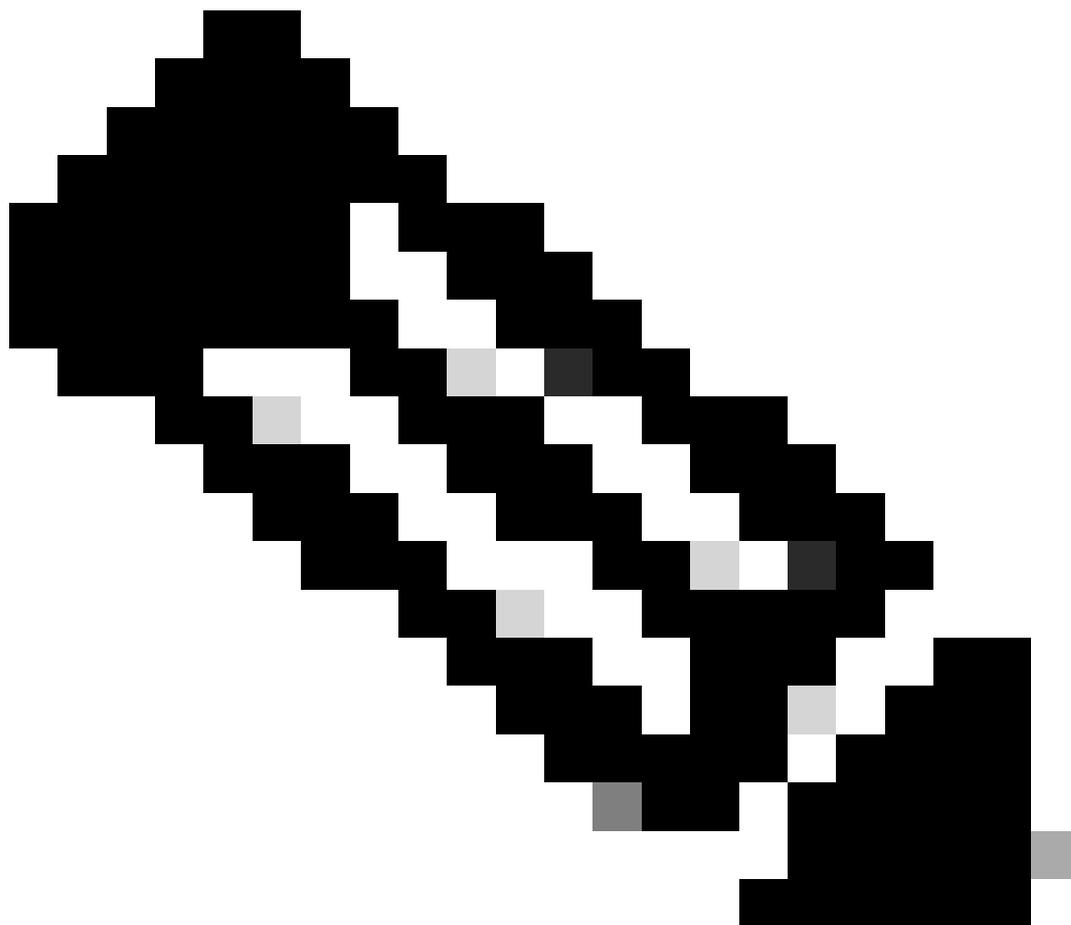
- **Action** : Sélectionnez Autoriser pour fournir l'accès à la ressource.
- **From** : Spécifiez l'utilisateur qui peut être utilisé pour se connecter à la ressource.
- **To** : Sélectionnez la ressource à laquelle vous souhaitez accéder via l'accès sécurisé.

Endpoint Requirements

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

| |
|---|
| <input type="checkbox"/> Zero-Trust Client-based Posture Profile Rule Defaults Requirements for end-user devices on which the Cisco Secure Client is installed. <input type="text" value="System provided (Client-based)"/> |
| Private Resources: SplunkFTD |
| <input type="checkbox"/> Zero Trust Browser-based Posture Profile Rule Defaults Requirements for end-user devices on which the Cisco Secure Client is NOT installed. <input type="text" value="System provided (Browser-based)"/> |
| Private Resources: SplunkFTD |

- **Zero-Trust Client-based Posture Profile**: Choisir le profil par défaut pour l'accès client de base
- **Zero-Trust Browser-based Posture Profile**: sélectionnez l'accès de base par défaut du navigateur de profils



Remarque : Pour en savoir plus sur la politique de posture, consultez le [guide](#) de l'[utilisateur](#) pour l'accès sécurisé.

Après cela, cliquez sur **Next** et **Save** et votre configuration, et vous pouvez essayer d'accéder à vos ressources via RA-VPN et Client Base ZTNA ou Browser Base ZTNA.

Dépannage

Pour effectuer un dépannage en fonction de la communication entre le pare-feu sécurisé et l'accès sécurisé, vous pouvez vérifier si Phase1 (IKEv2) et Phase2 (IPSEC) sont établies entre les périphériques sans problème.

Vérification de Phase 1 (IKEv2)

Pour vérifier Phase1, vous devez exécuter la commande suivante sur l'interface de ligne de commande de votre FTD :

```
show crypto isakmp sa
```

Dans ce cas, le résultat souhaité est deux IKEv2 SAs adresses IP de centre de données d'accès sécurisé et l'état souhaité est **READY**:

```
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
```

Vérification de Phase2 (IPSEC)

Pour vérifier Phase2, vous devez exécuter la commande suivante sur l'interface de ligne de commande de votre FTD :

```
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

```

Dans la dernière sortie, vous pouvez voir les deux tunnels établis ; ce qui n'est pas souhaité, c'est la sortie suivante sous le paquetencaps etdecaps.

```

#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

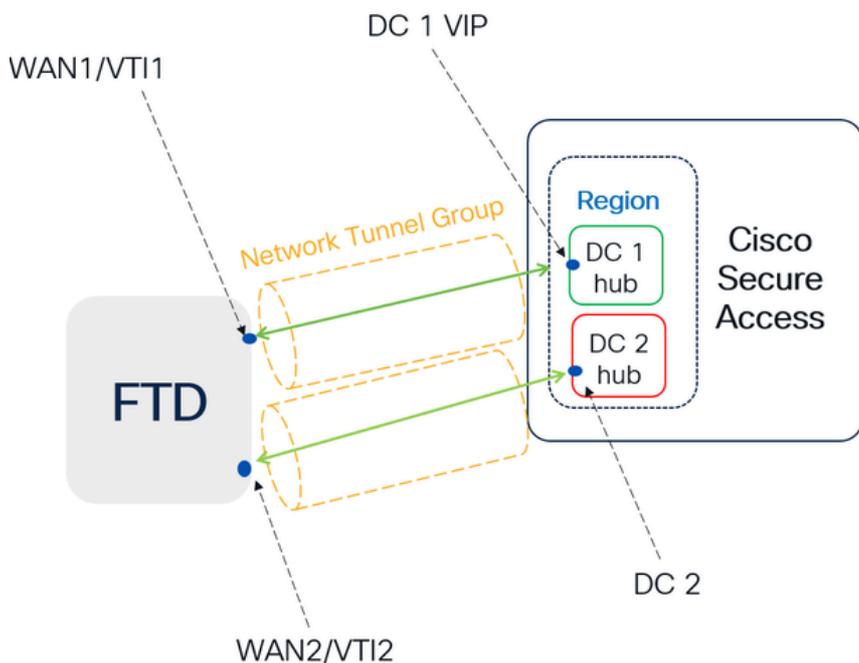
```

Si vous avez ce scénario, ouvrez un dossier auprès du TAC.

Fonction de haute disponibilité

La fonction des tunnels avec accès sécurisé communiquant avec le data center dans le cloud est active/passive, ce qui signifie que seule la porte pour DC 1 sera ouverte pour recevoir le trafic ; la porte du DC 2 est fermée jusqu'à ce que le tunnel numéro 1 tombe en panne.

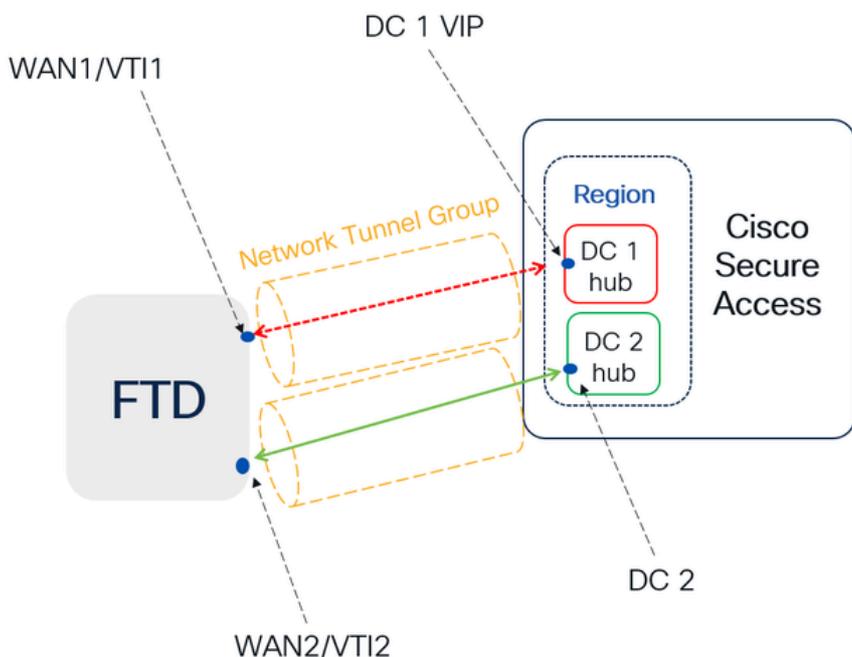
Normal Behavior



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

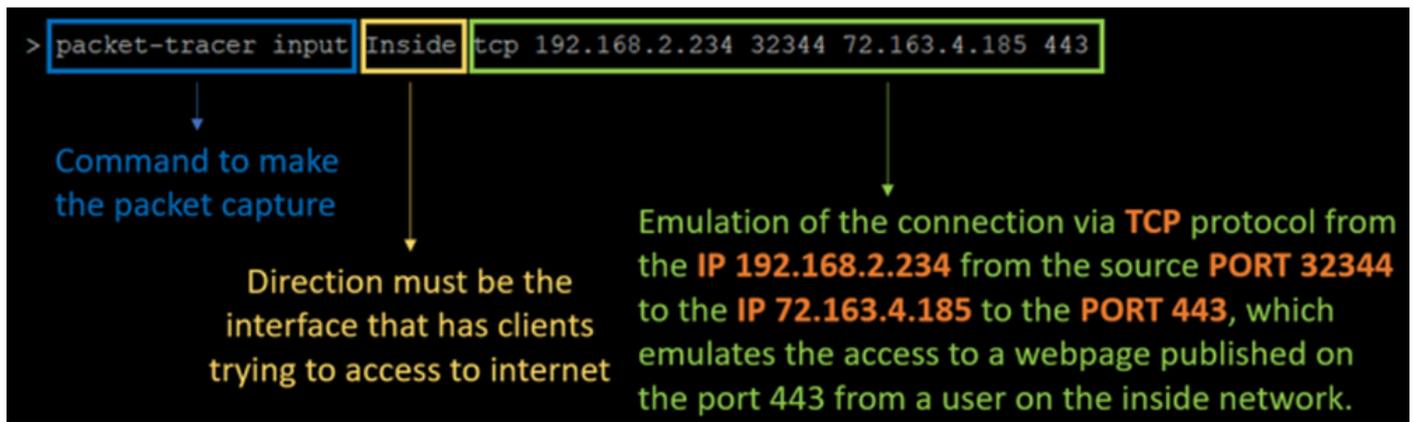
- DC2 is **Active** when DC1 or WAN1 peer is **Down**
- High availability is implemented to address failures in the WAN1 channel on the Firewall, ensuring operational continuity in the **region** and mitigating potential issues in DC1

Vérification du routage du trafic pour un accès sécurisé

Dans cet exemple, nous utilisons la source comme machine sur le réseau du pare-feu :

- Source : 192.168.10.40
- Destination : 146.112.255.40 (IP de surveillance d'accès sécurisé)

Exemple :



commande :

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

Sortie :

```
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

Ici, beaucoup de choses peuvent nous donner un contexte sur la communication et savoir si tout est correctement sous la configuration PBR pour acheminer correctement le trafic vers l'accès sécurisé :

```
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
```

La phase 2 indique que le trafic est transféré vers l'PrimaryVTI interface, ce qui est correct car, en fonction des configurations de ce scénario, le trafic Internet doit être transféré vers l'accès sécurisé via l'interface VTI.

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:

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.