Configuration d'un accès sécurisé avec Secure Firewall avec HA

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
  - Diagramme du réseau
- Configurer
- Configurer le VPN sur un accès sécurisé
- 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 un accès sécurisé avec un pare-feu sécurisé avec haute disponibilité (HA).

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

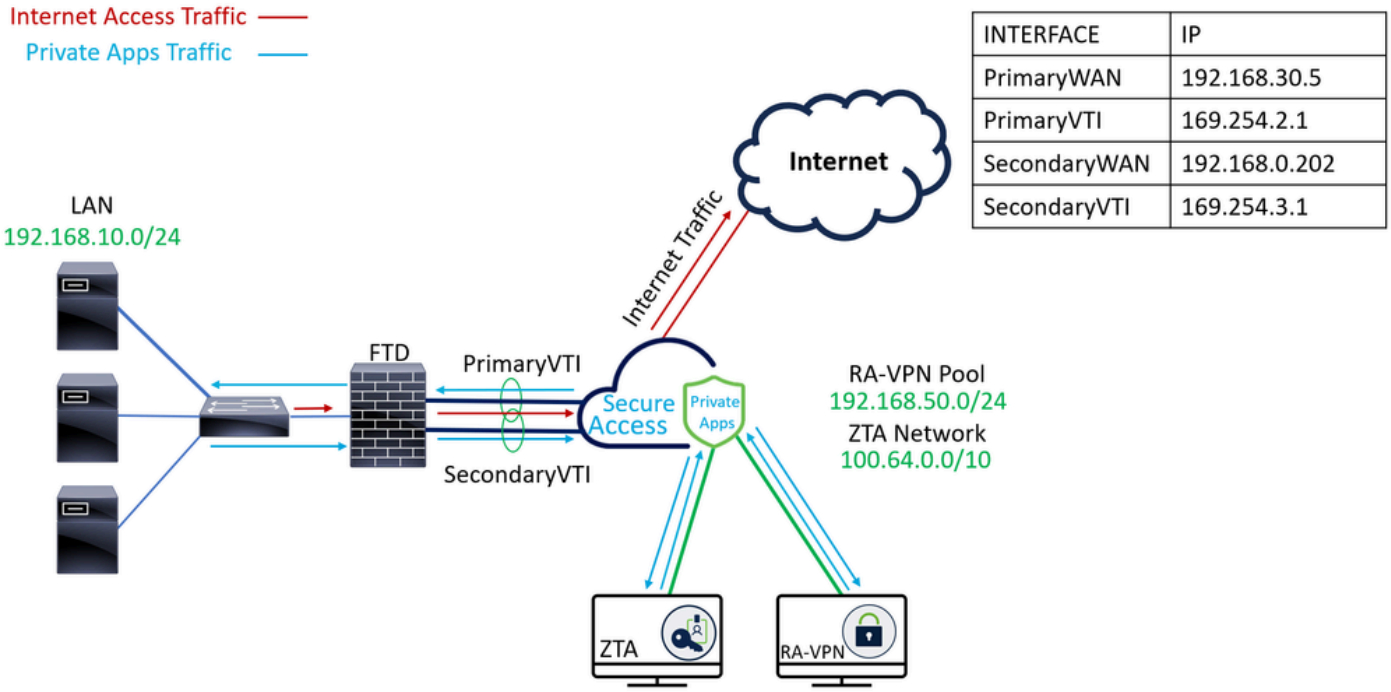
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales



Cisco 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



INTERFACE	IP
PrimaryWAN	192.168.30.5
PrimaryVTI	169.254.2.1
SecondaryWAN	192.168.0.202
SecondaryVTI	169.254.3.1

Configurer

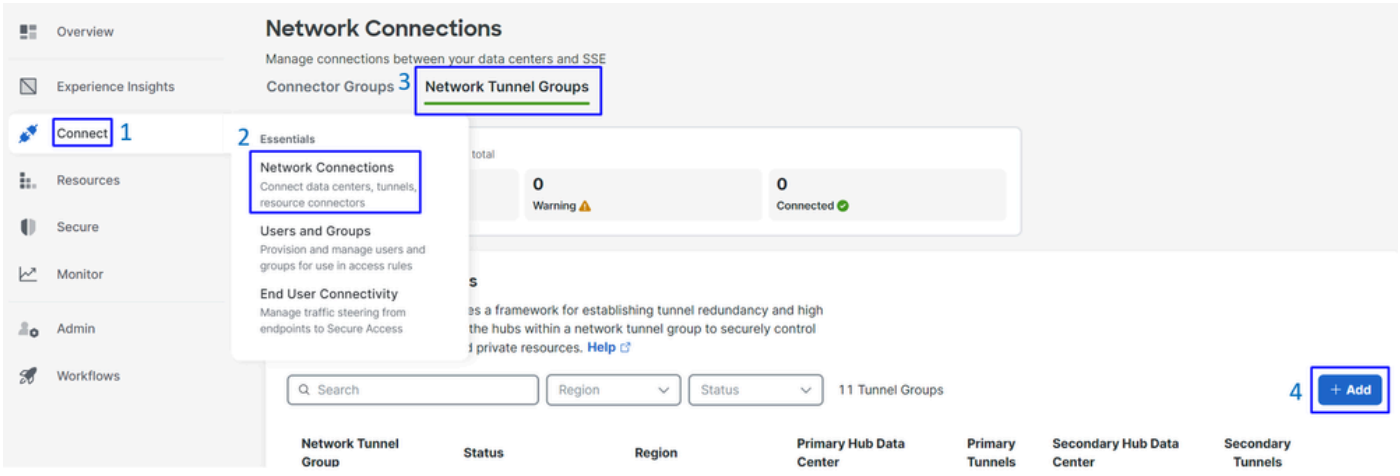
Configurer le VPN sur un accès sécurisé

Accédez au panneau d'administration de Secure Access.

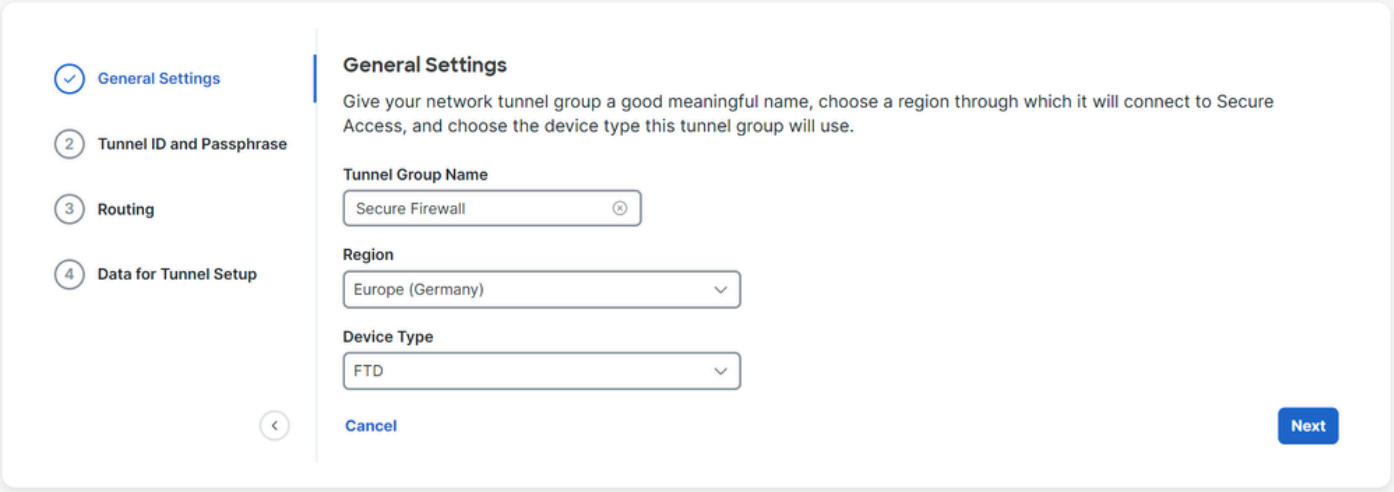


- Cliquez sur Connect>Network Connections.

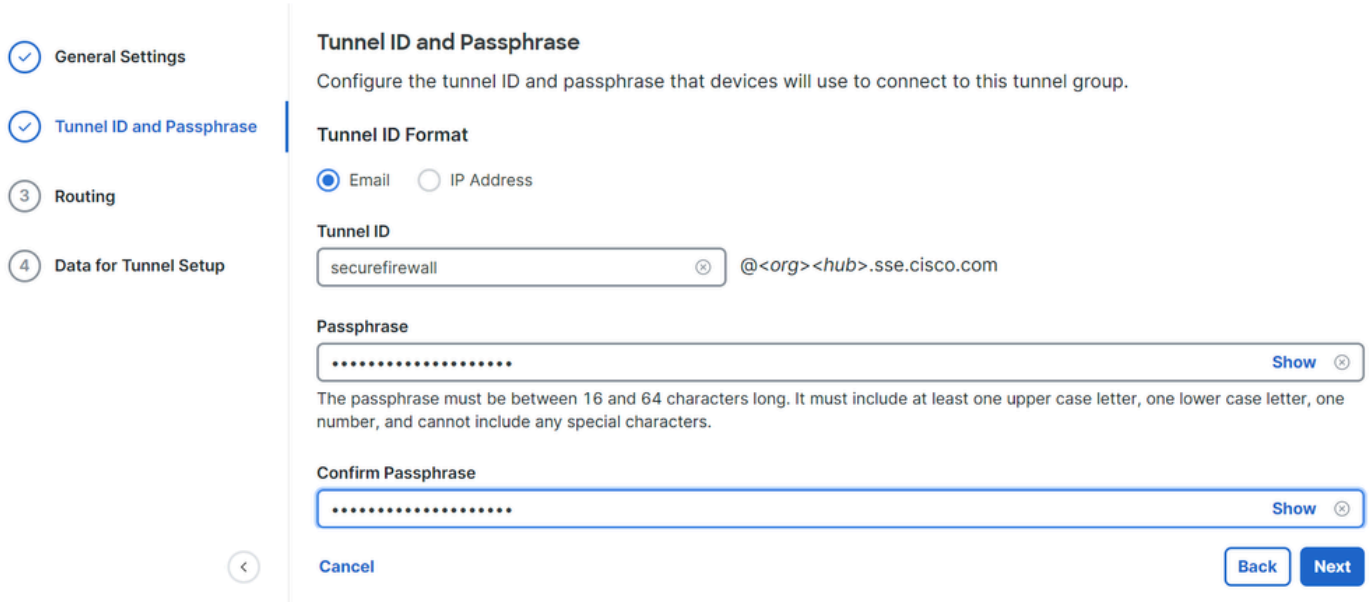
- Sous Network Tunnel Groups cliquez sur + Add.



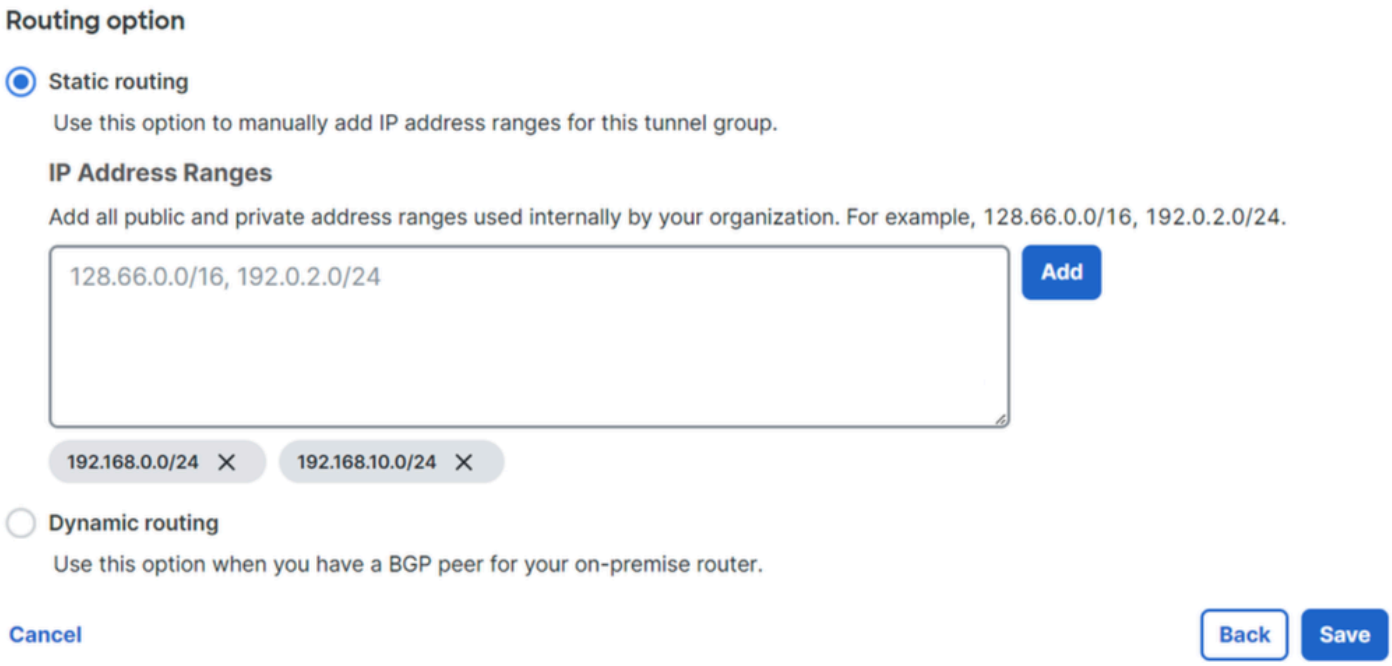
- Configurer Tunnel Group Name,Region etDevice Type.
- Cliquer **Next**.



- Configurez les Tunnel ID Format et **Passphrase**.
- Cliquer **Next**.

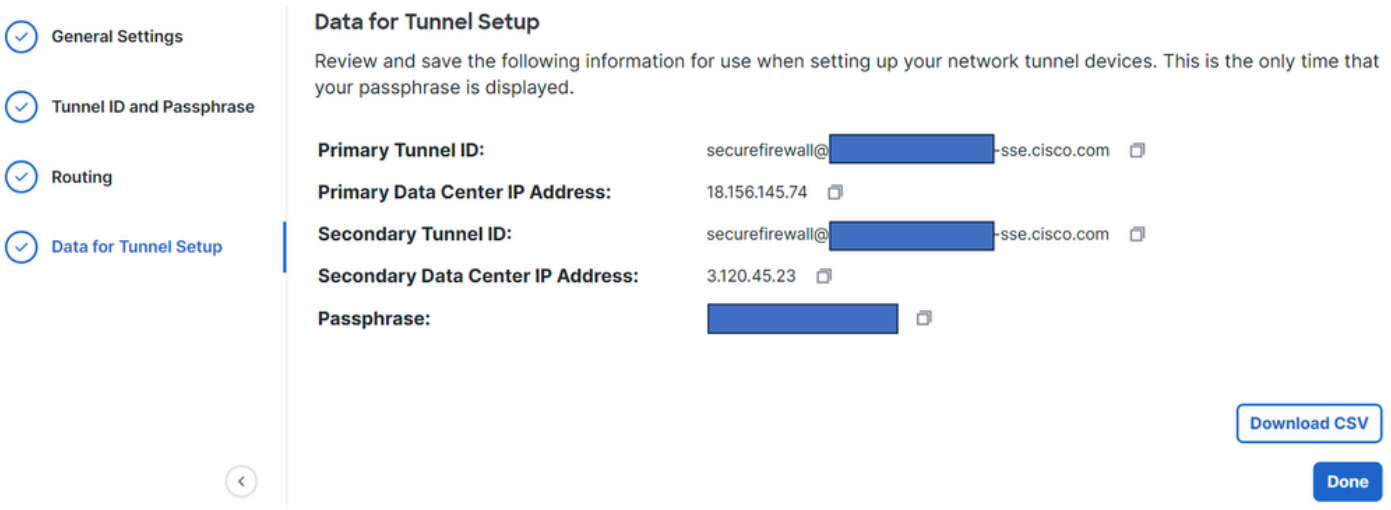


- Configurez les plages d'adresses IP ou les hôtes que vous avez configurés sur votre réseau et souhaitez faire passer le trafic via l'accès sécurisé.
- Cliquer**Save**.



Après avoir cliqué sur Save, les informations sur le tunnel s'affichent. Veuillez enregistrer ces informations pour l'étape suivante ; Configurez le tunnel sur Secure Firewall.

Données pour la configuration du tunnel



Configurer le tunnel sur Secure Firewall

Configuration de l'interface du tunnel

Pour ce scénario, vous devez utiliser la configuration VTI (Virtual Tunnel Interface) sur le pare-feu sécurisé pour atteindre cet objectif ; n'oubliez pas que dans ce cas, vous disposez d'un FAI double et que vous souhaitez bénéficier de la haute disponibilité (HA) si l'un de vos FAI tombe en panne.

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 affecter une route statique à l' **Primary or Secondary Datacenter IP** pour que les deux tunnels soient actifs.

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 actifs.

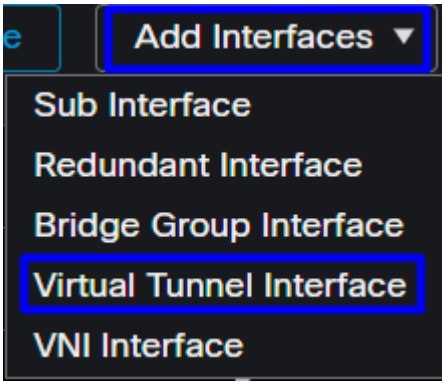
En fonction de ce scénario, vous disposez des **PrimaryWAN** et **SecondaryWAN**, que vous devez utiliser pour créer les interfaces VTI.

Accédez à votre Firepower Management Center > Devices.

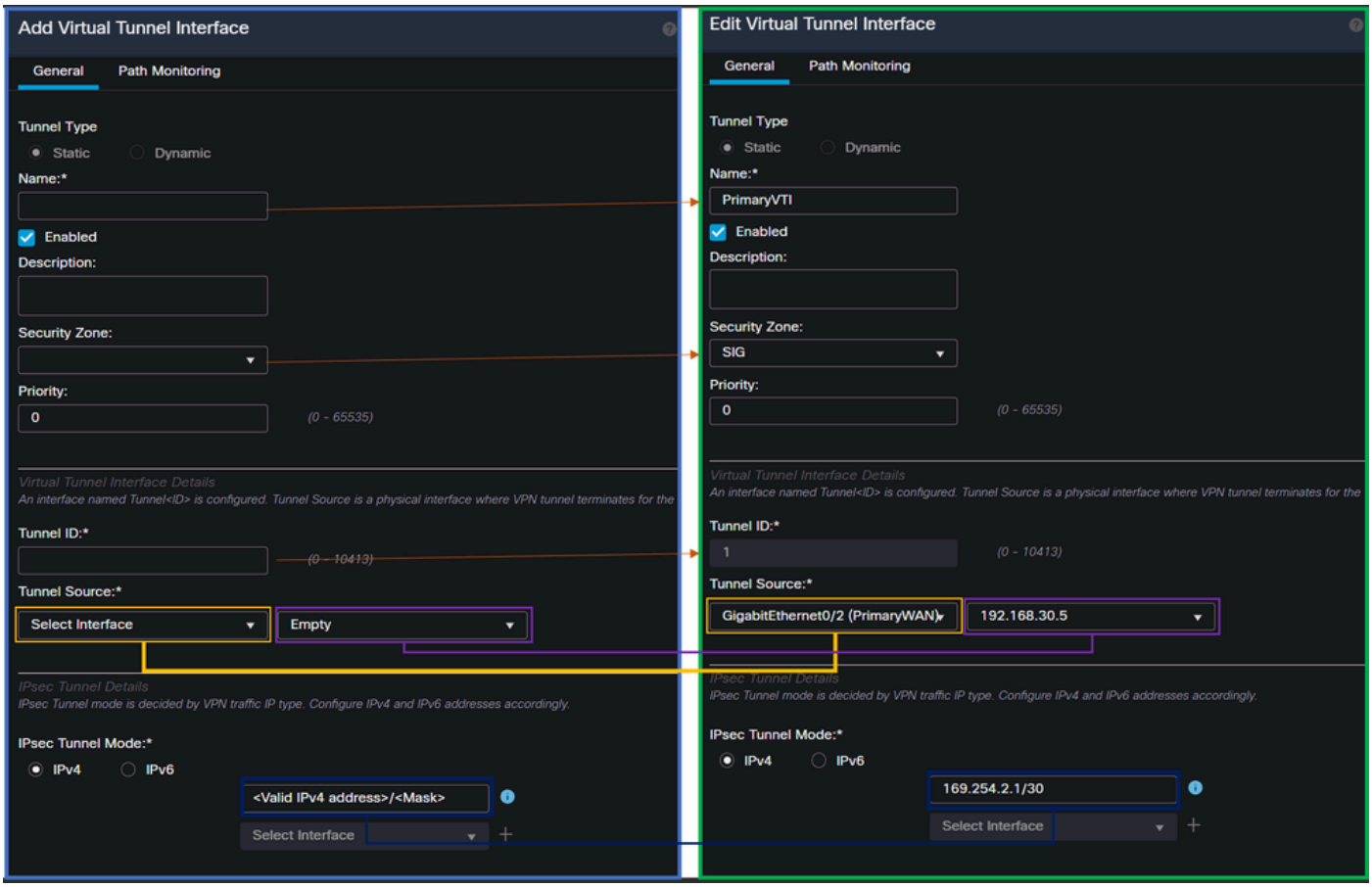
- Choisissez votre FTD
- Choisir **Interfaces**

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	PimaryWAN		192.168.30.5/24(Static)

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



- Configurez l'interface Add Virtual Tunnel.



- **Name**: Configurez un nom qui fait référence à la **PrimaryWAN interface**.
- **Security Zone**: Vous pouvez en réutiliser une autre **Security Zone**, mais il est préférable d'en créer une nouvelle pour le trafic d'accès sécurisé.
- **Tunnel ID**: Ajoutez un numéro pour l'ID de tunnel.
- **Tunnel Source**: Choisissez votre **PrimaryWAN interface** et sélectionnez une adresse IP privée ou publique pour 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 PrimaryVTI et 169.254.3.1/30 pour SecondaryVTI.

Après cela, vous devez faire la même chose pour le **SecondaryWAN interface**. Maintenant, votre VTI High Available est configuré, en conséquence votre interface affiche :



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	PimaryWAN		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

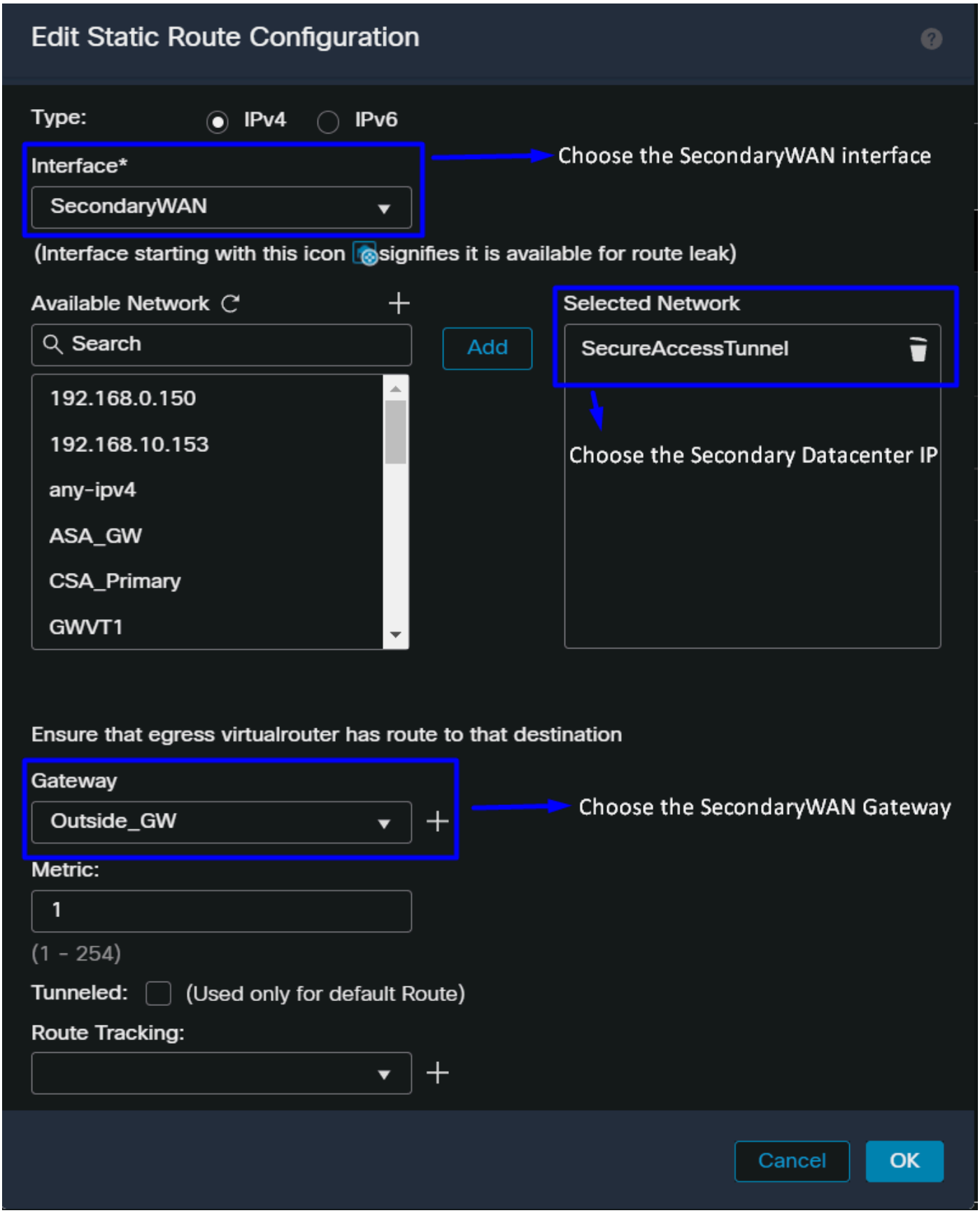
Configuration de la route statique pour l'interface secondaire

Pour permettre au trafic du **SecondaryWAN interface** d'atteindre le Secondary Datacenter IP Address , vous devez configurer une route statique vers l'adresse IP du data center. 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.

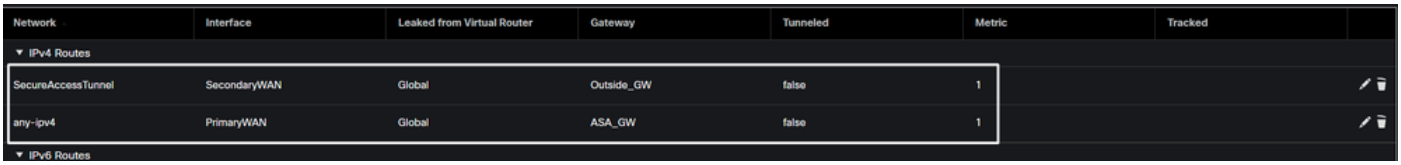
Mise en garde : Cela n'est nécessaire que si vous n'avez pas configuré un ECMP entre les canaux WAN ; si un ECMP est configuré, vous pouvez passer à l'étape suivante.

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

- Cliquez sur votre périphérique FTD
- Cliquez sur **Routing**
- Choisir **Static Route** > **+ Add Route**



- Interface: Sélectionnez l'interface WAN secondaire
- **Gateway**: Sélectionnez la passerelle WAN secondaire
- Selected Network: Si vous ajoutez l'adresse IP du data center secondaire en tant qu'hôte, vous pouvez trouver les informations lorsque vous configurez le tunnel à l'étape Secure Access, Data for Tunnel Setup
- **Metric**: Utiliser un (1)
- OKCliquez sur et **Save**, puis déployez.



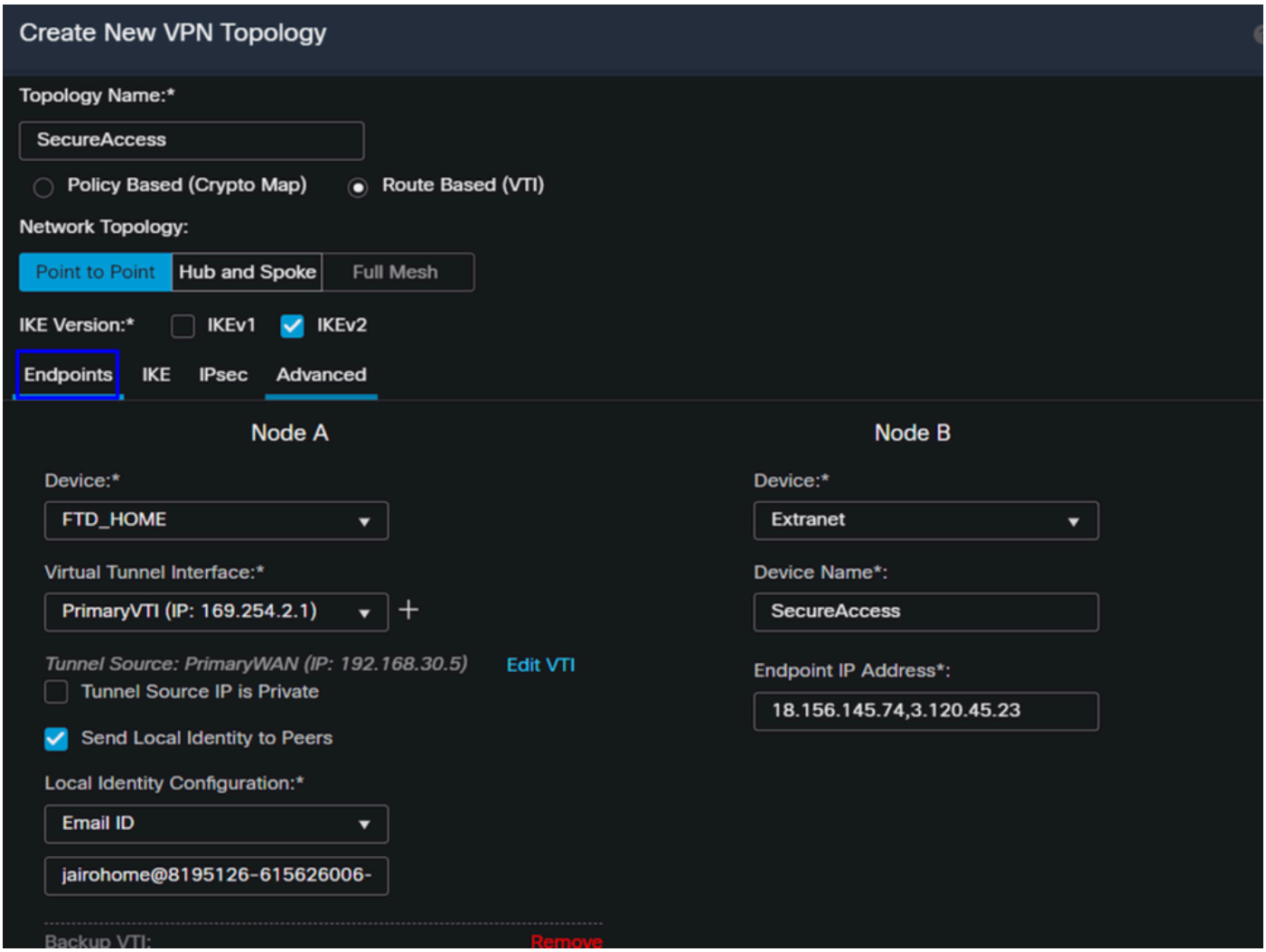
Configurer le VPN pour un accès sécurisé en mode VTI

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

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

Configuration des terminaux

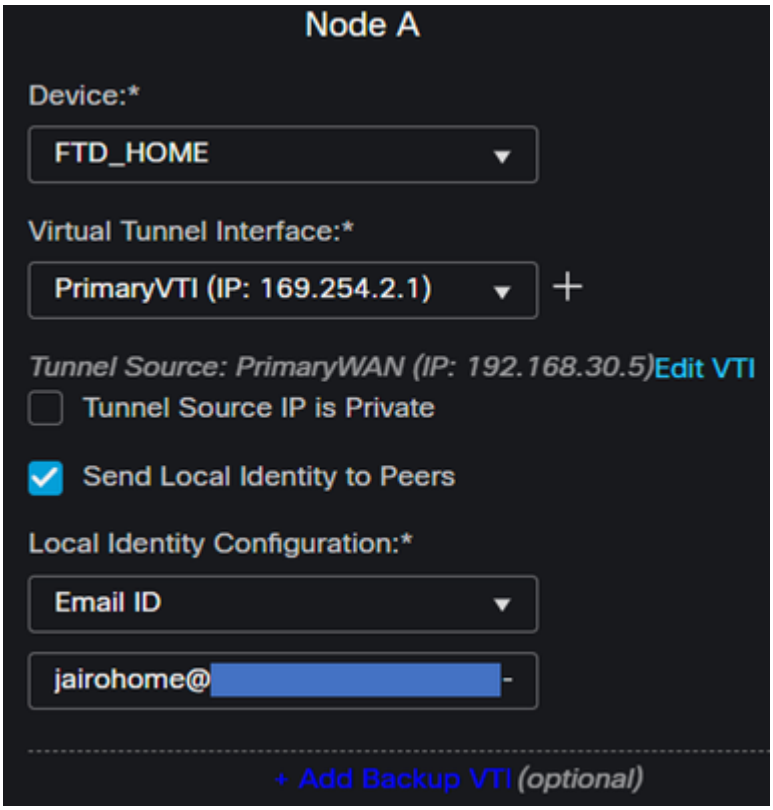
Pour configurer les points d'extrémité, vous devez utiliser les informations fournies dans l'étape, Données pour la configuration du tunnel.



- Nom de topologie : Créez un nom lié à l'intégration Secure Access
- Choisir **Routed Based (VTI)**
- Choisir **Point to Point**
- IKE Version: Choisir IKEv2

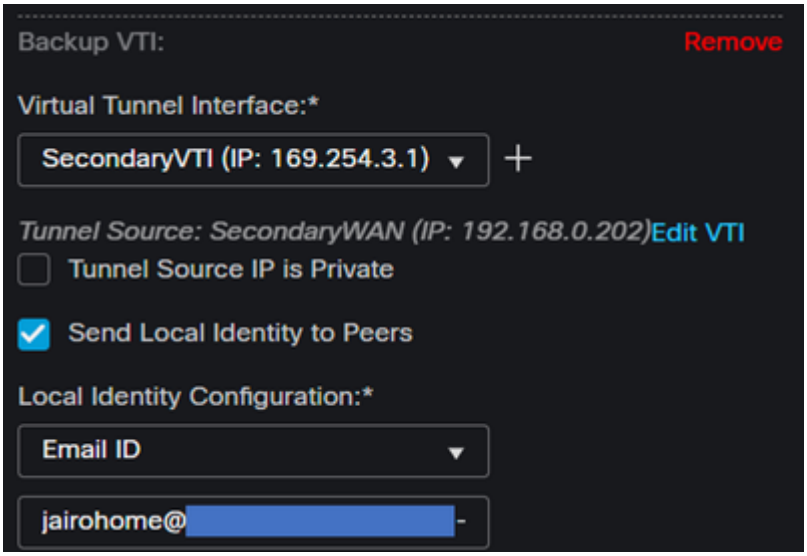
Remarque : IKEv1 n'est pas pris en charge pour l'intégration avec Secure Access.

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



- **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

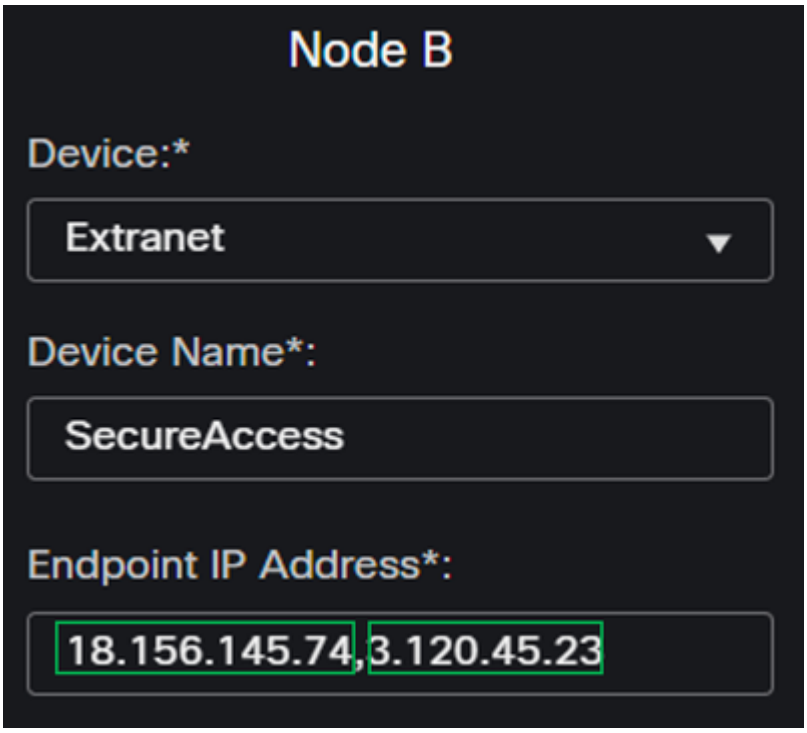
Après avoir configuré les informations sur le, **PrimaryVTI** cliquez sur **+ Add Backup VTI**:



- **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 :

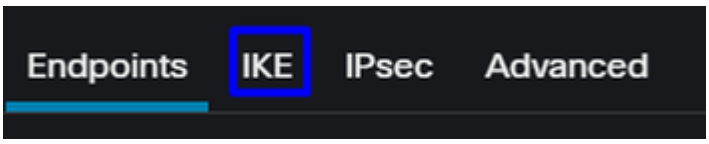


- **Device**: Extranet
- **Device Name**: Choisissez un nom pour reconnaître l'accès sécurisé comme destination
- Endpoint IP Address: La configuration pour le principal et le secondaire doit être Primaire **Datacenter IP,Secondary Datacenter IP**, vous pouvez trouver ces informations dans l'étape, Données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

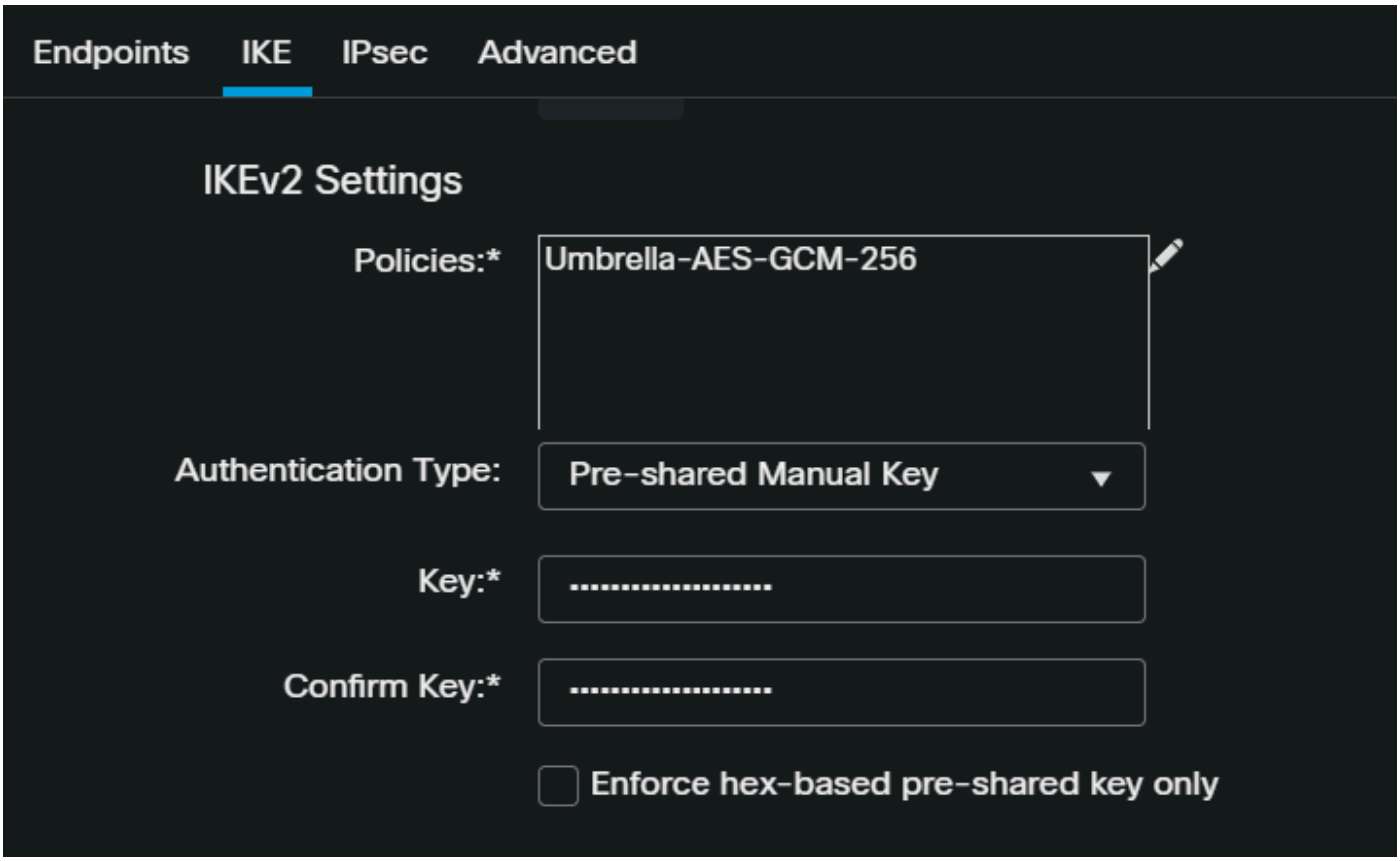
Après cela, votre configuration de **Endpoints** est terminée.

Configuration IKE

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



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



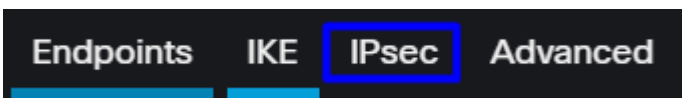
- Policies: Vous pouvez utiliser la configuration Umbrella par défaut, **Umbrella-AES-GCM-256** ou configurer différents paramètres en fonction de la Supported IKEv2 and IPSEC Parameters

- **Authentication Type**: Clé manuelle pré-partagée
- Keyet: **Confirm Key** Vous trouverez les **Passphrase** informations dans l'étape : Données pour la configuration du tunnel

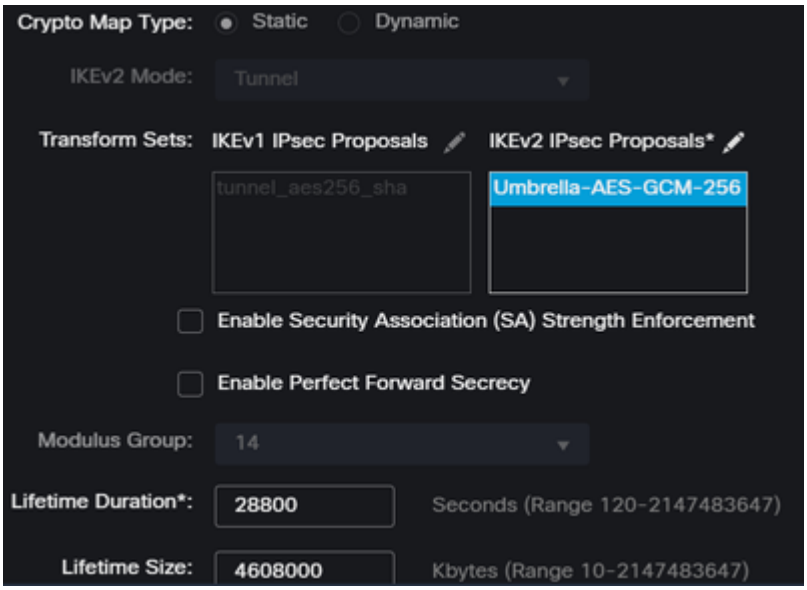
Après cela, votre configuration pour **IKE** est terminée et vous pouvez maintenant passer à l'étape Configuration IPSEC.

Configuration IPSEC

Pour configurer les paramètres IPSEC, cliquez sur IPSEC.



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



- 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

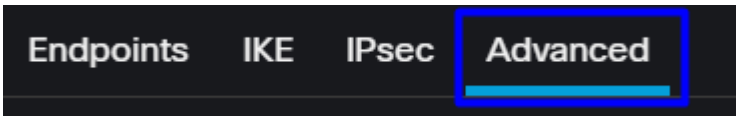
---

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

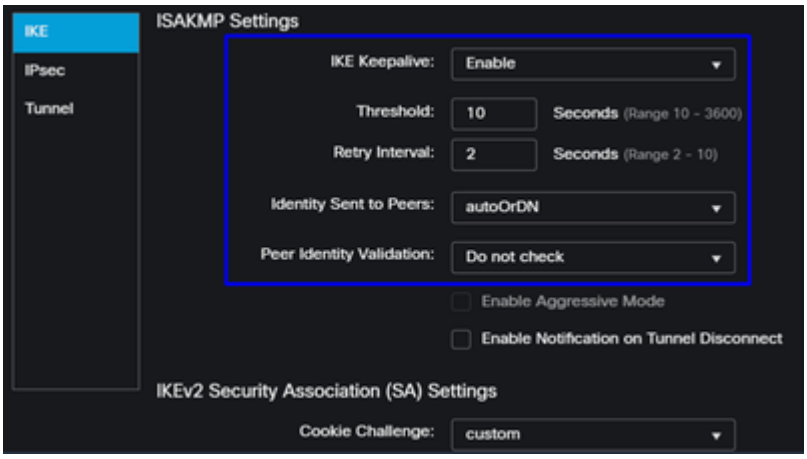
Votre configuration de **IPSEC** est maintenant terminée.

Configuration avancée

Pour configurer les paramètres avancés, cliquez sur Advanced.



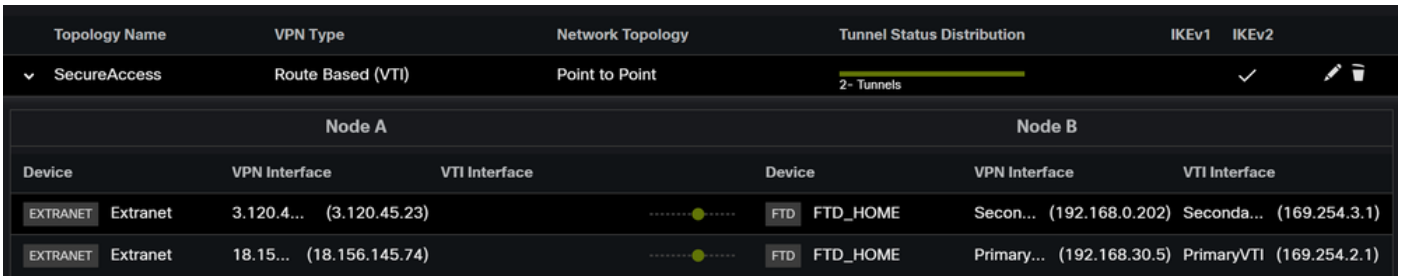
Sous **Advanced,** vous devez configurer les paramètres suivants :



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

Cliquez sur Save et **Deploy**.

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



La configuration du **VPN to Secure Access in VTI Mode** est terminée et vous pouvez passer à l'étape Configurer le routage de base de la stratégie.

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.

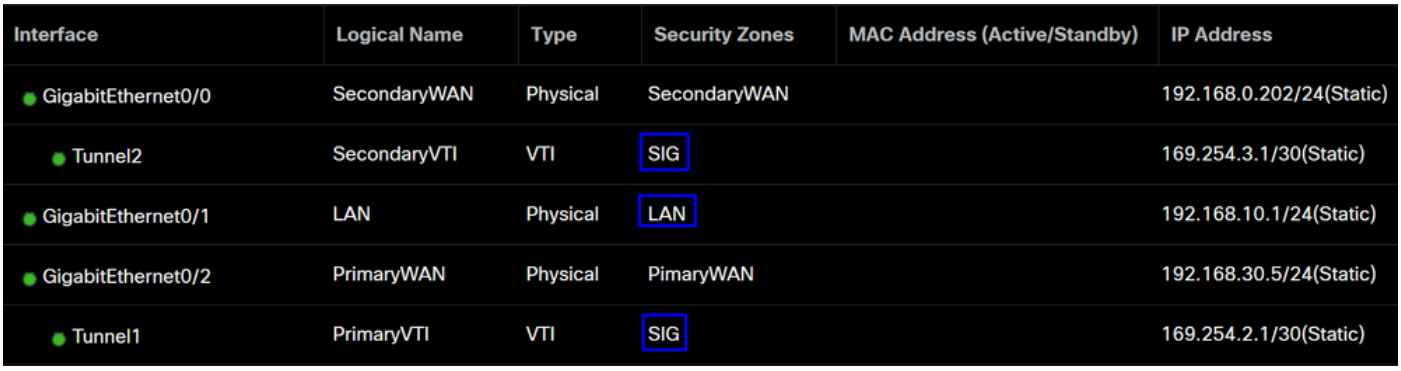
Remarque : Le basculement sur le site d'accès sécurisé est basé sur les valeurs DPD

---

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 :

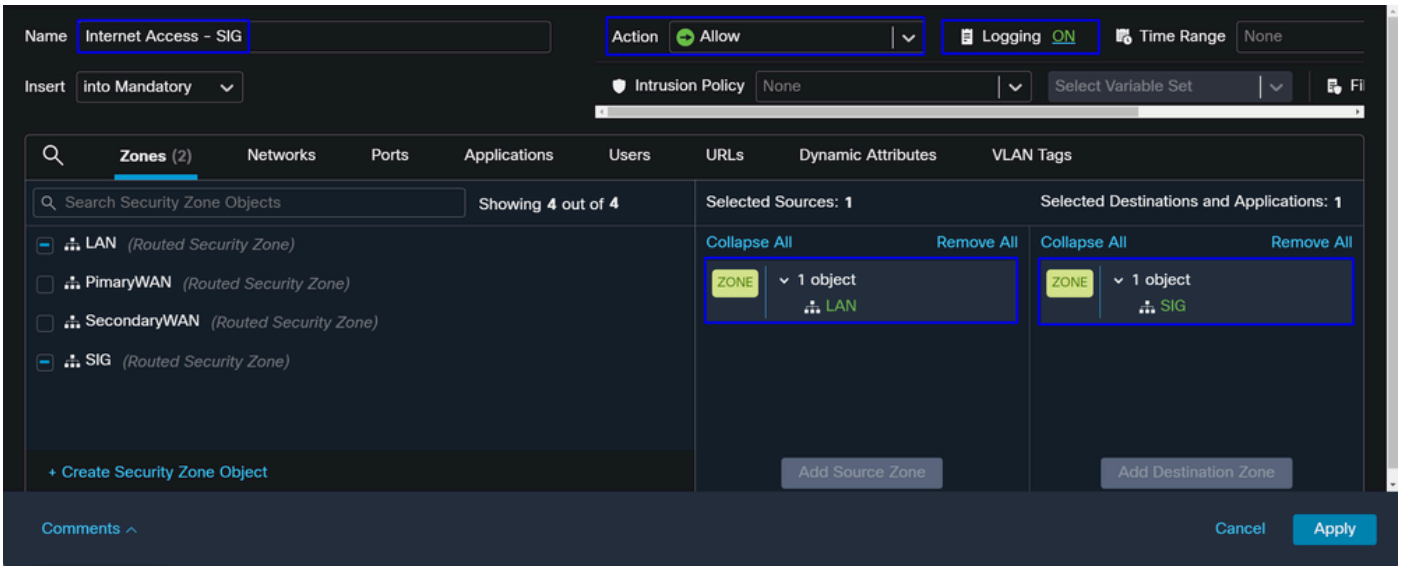


Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address
GigabitEthernet0/0	SecondaryWAN	Physical	SecondaryWAN		192.168.0.202/24(Static)
Tunnel2	SecondaryVTI	VTI	SIG		169.254.3.1/30(Static)
GigabitEthernet0/1	LAN	Physical	LAN		192.168.10.1/24(Static)
GigabitEthernet0/2	PrimaryWAN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

Fournir un accès à Internet sur toutes les ressources que vous configurez sur le routage de base de la politique. Vous devez configurer certaines règles d'accès et certaines stratégies d'accès sécurisé.



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

Escenario RA-VPN

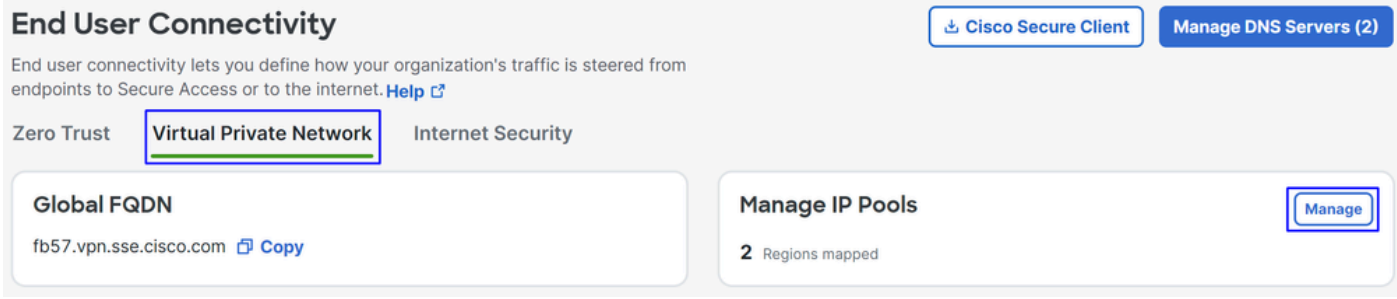
Pour fournir un accès à partir des utilisateurs RA-VPN, vous devez le configurer en fonction de la plage que vous avez attribuée sur le pool RA-VPN.

Remarque : Pour configurer votre stratégie RA-VPNaaS, vous pouvez passer par Manage Virtual Private Networks.

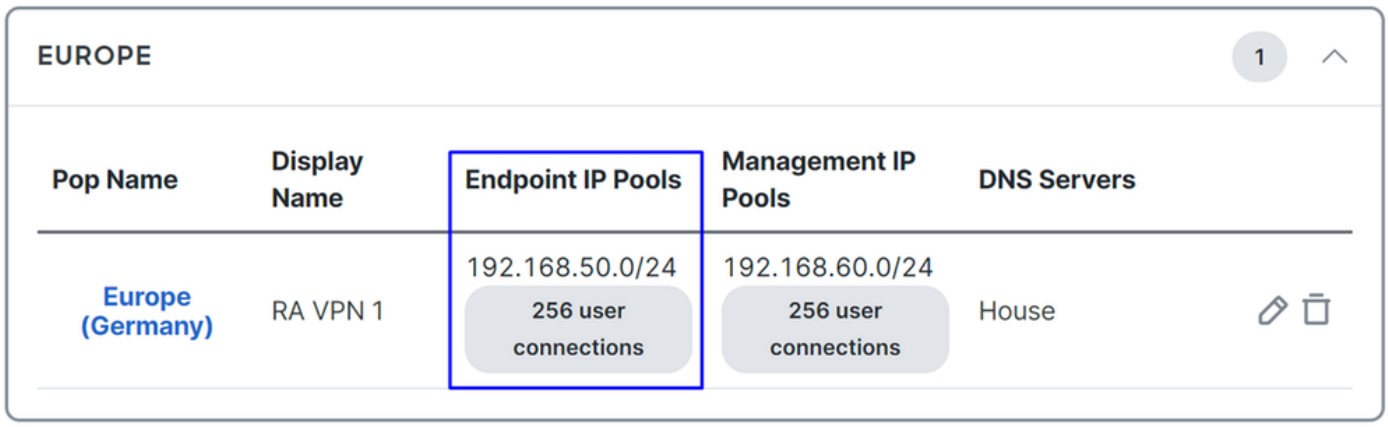
Comment vérifiez-vous le pool d'adresses IP de votre VPNaaS ?

Accédez à votre tableau de bord Secure Access

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



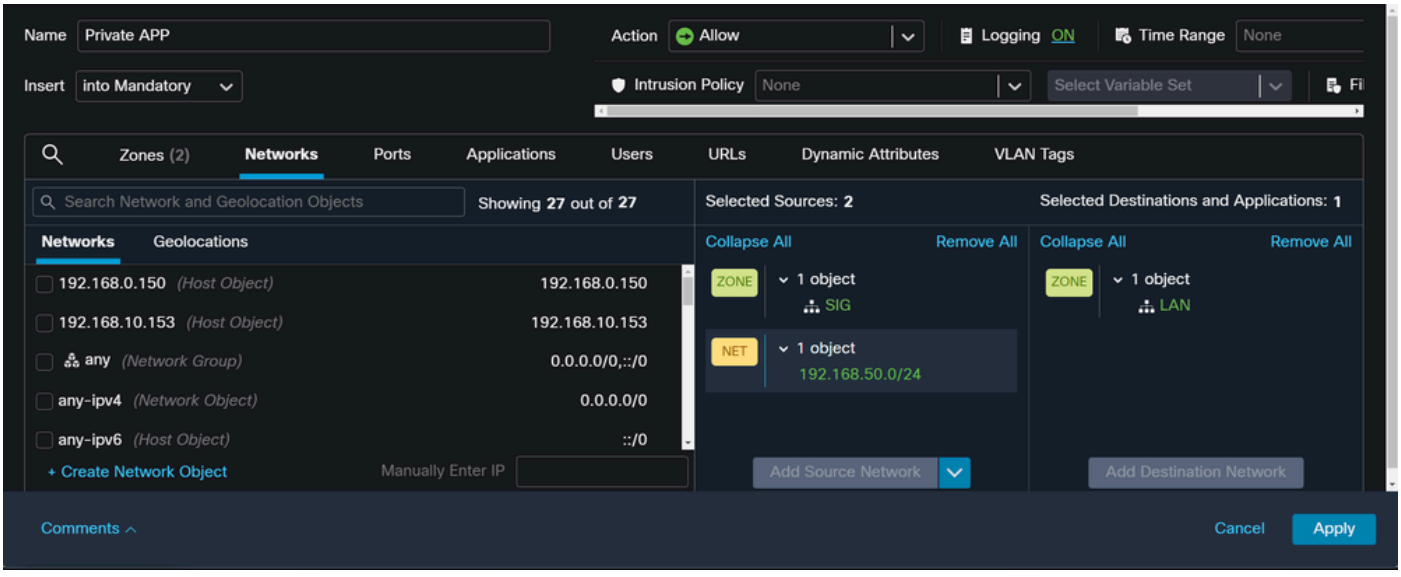
- Vous pouvez voir votre piscine sous **Endpoint IP Pools**.



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

Configuration des règles d'accès

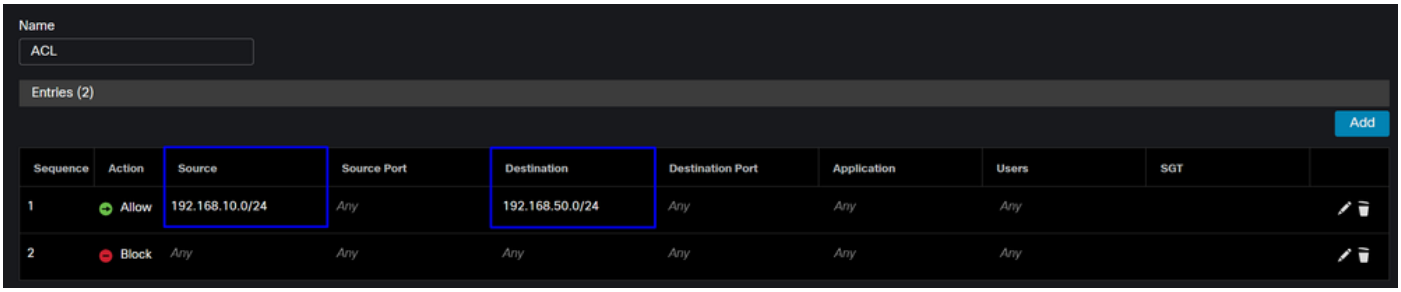
Si vous ne configurez l'accès sécurisé que pour l'utiliser avec les capacités d'accès aux ressources d'applications privées, votre règle d'accès peut ressembler à ceci :



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.

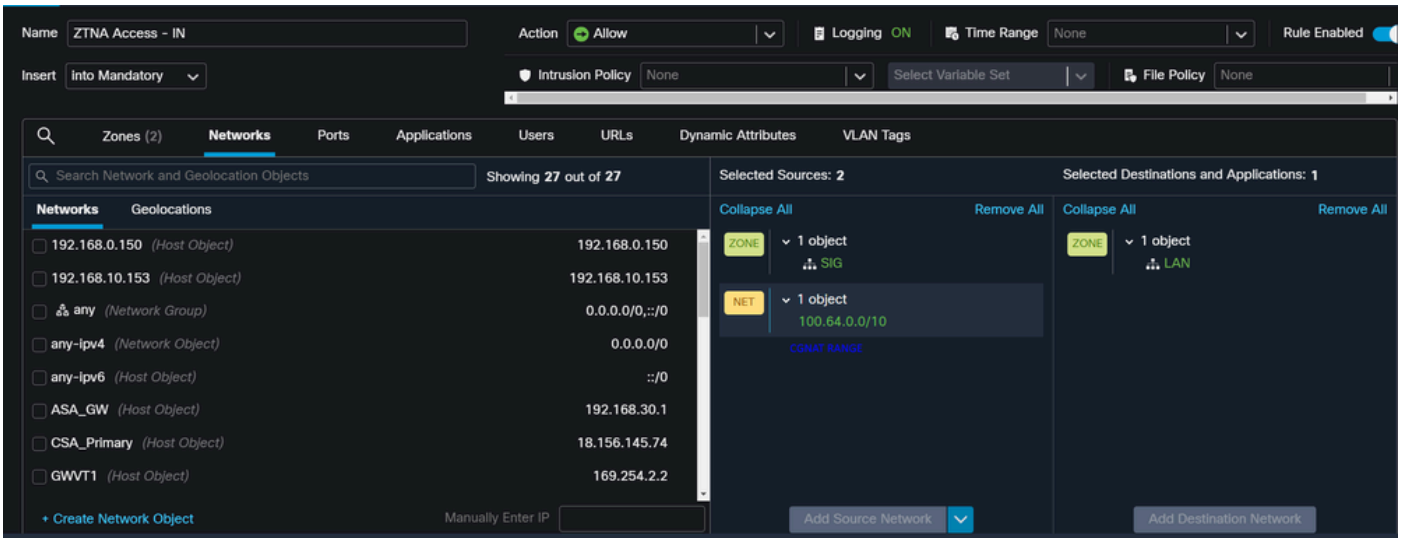


Escenario ZTNA CLAP-BAP

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

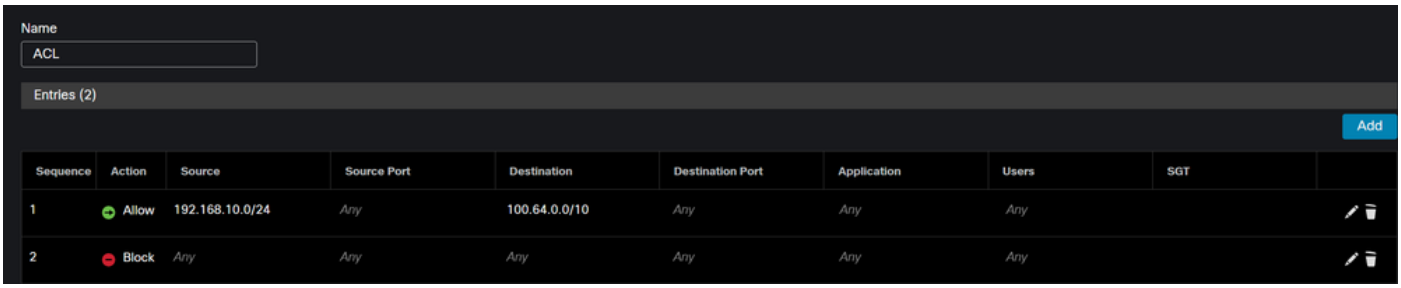
Si vous ne configurez l'accès sécurisé que pour l'utiliser avec les capacités d'accès aux ressources d'applications privées, votre règle d'accès peut ressembler à ceci :



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

Configuration ACL

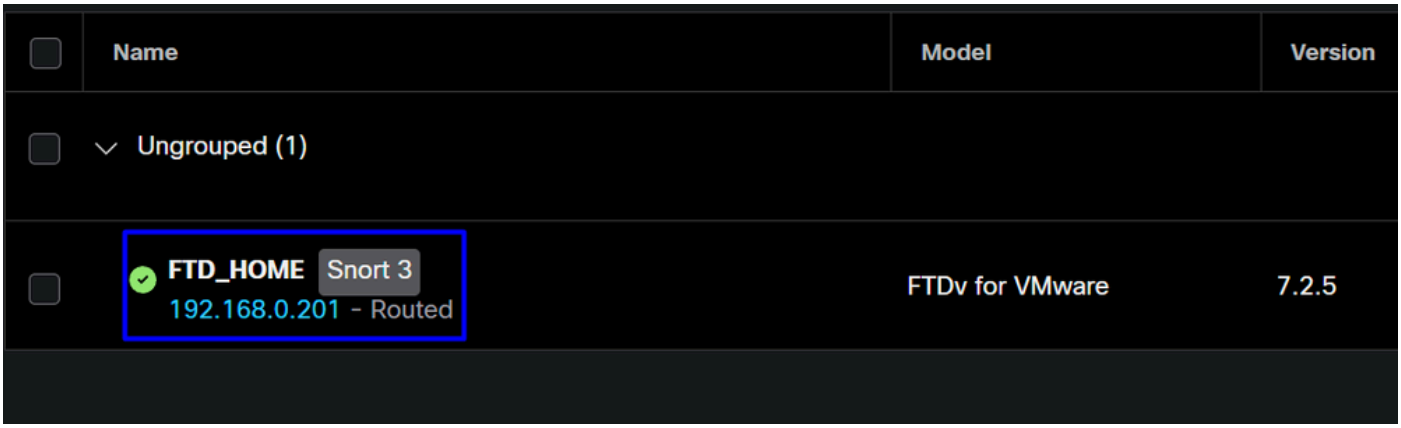
Pour autoriser le trafic de routage de SIG à votre LAN à l'aide de CGNAT, vous devez l'ajouter sous la liste de contrôle d'accès pour qu'il fonctionne sous le PBR.



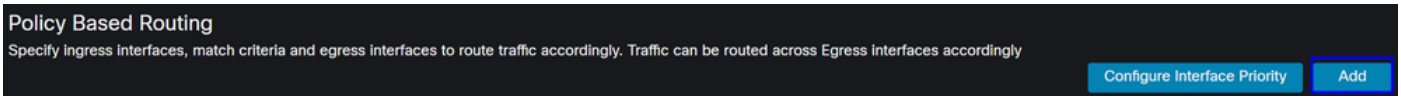
Configurer le routage de base de stratégie

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



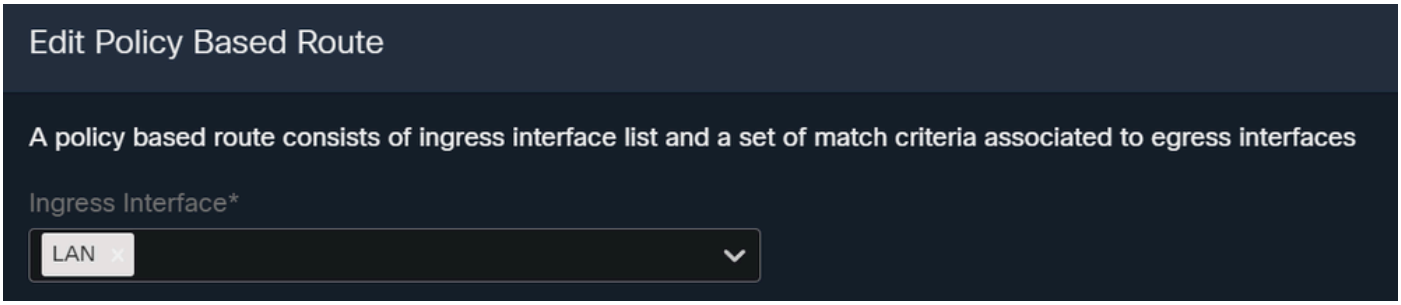
- Cliquez sur **Routing**
- Choisir Policy Base Routing
- Cliquer Add



Dans ce scénario, vous sélectionnez toutes les interfaces que vous utilisez comme source pour

acheminer le trafic vers l'accès sécurisé ou pour fournir l'authentification utilisateur à l'accès sécurisé à l'aide de RA-VPN. L'accès ZTA basé sur le client ou le navigateur aux ressources internes du réseau :

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

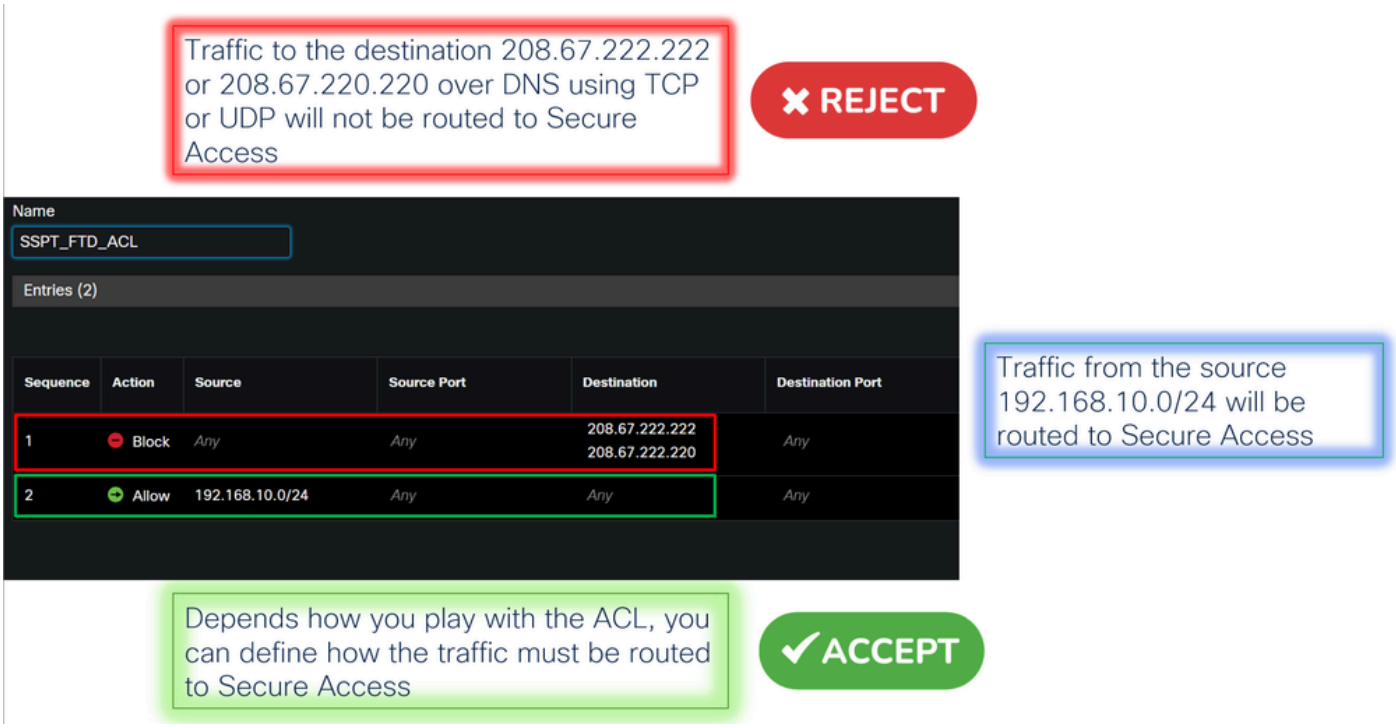


- Sous Critères de correspondance et Interface de sortie, vous définissez les paramètres suivants après avoir cliqué sur Add:





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

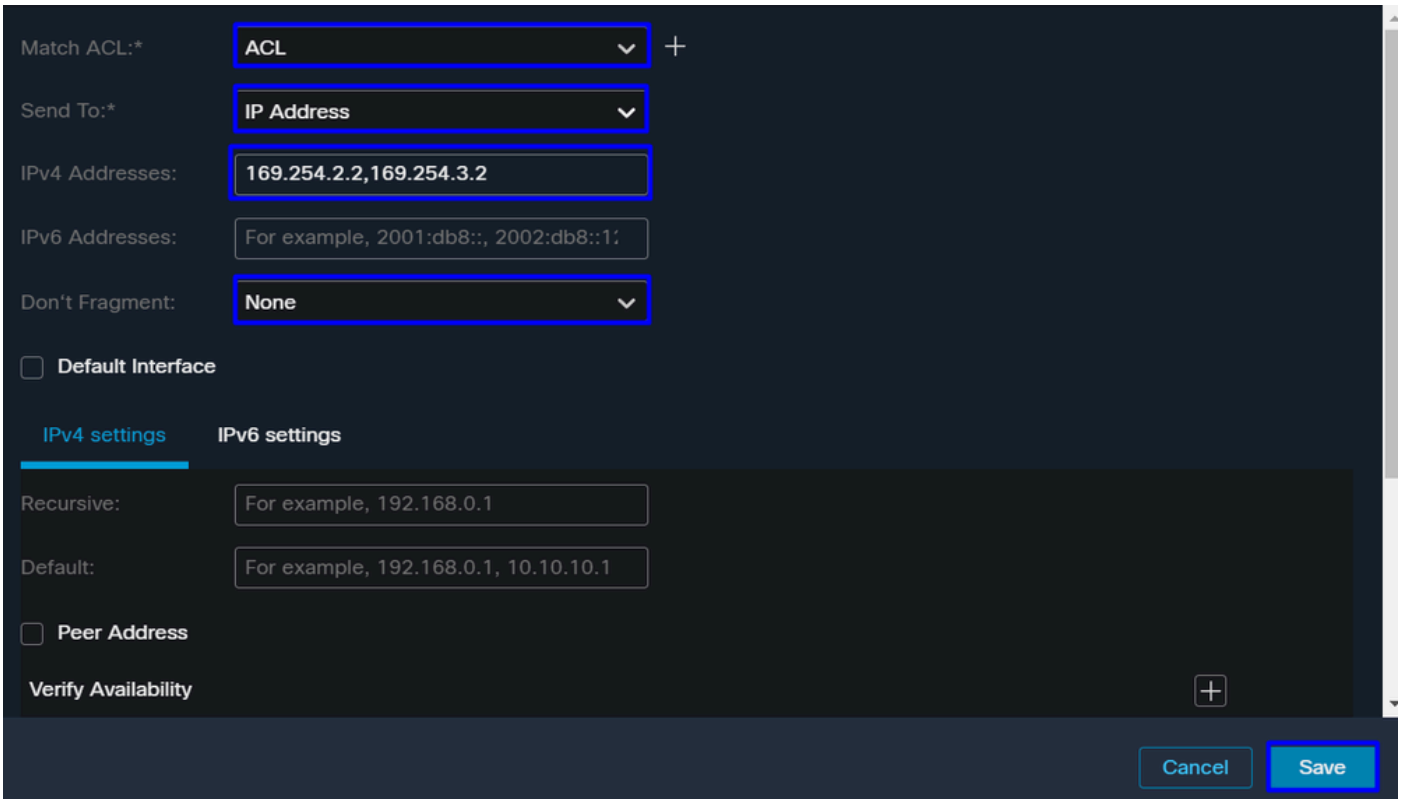


- **Send To**: Sélectionnez l'adresse IP
- **IPv4 Addresses**: Vous devez utiliser l'adresse IP suivante sous le masque 30 qui a été configuré sur les deux VTI ; vous pouvez vérifier que sous l'étape : VTI Interface Config

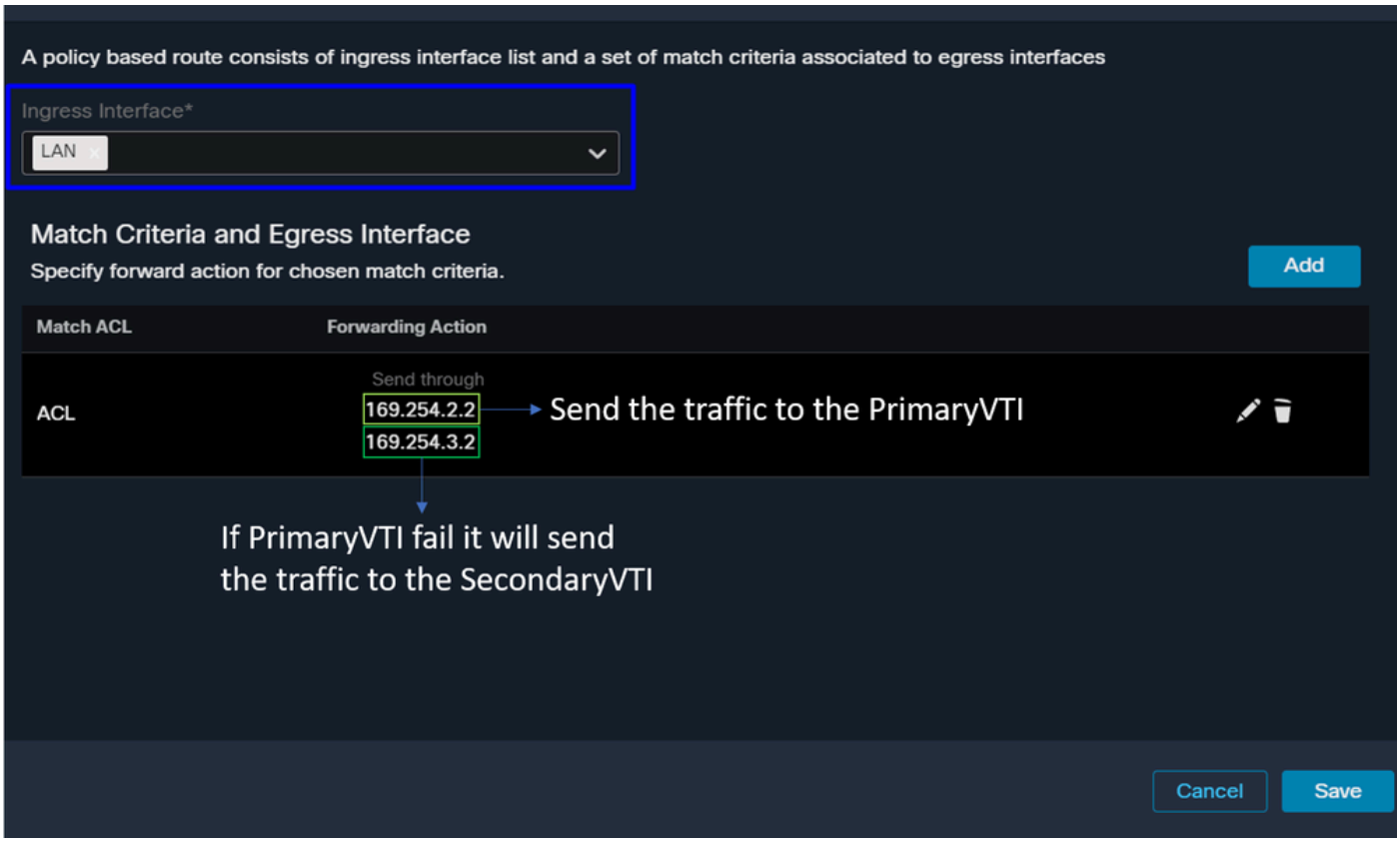
Interface	IP	GW
VTI principal	169.254.2.1/30	169.254.2.2
VTI secondaire	169.254.3.1/30	169.254.3.2



Une fois configuré, vous obtenez les résultats suivants, puis cliquez sur **Save**:



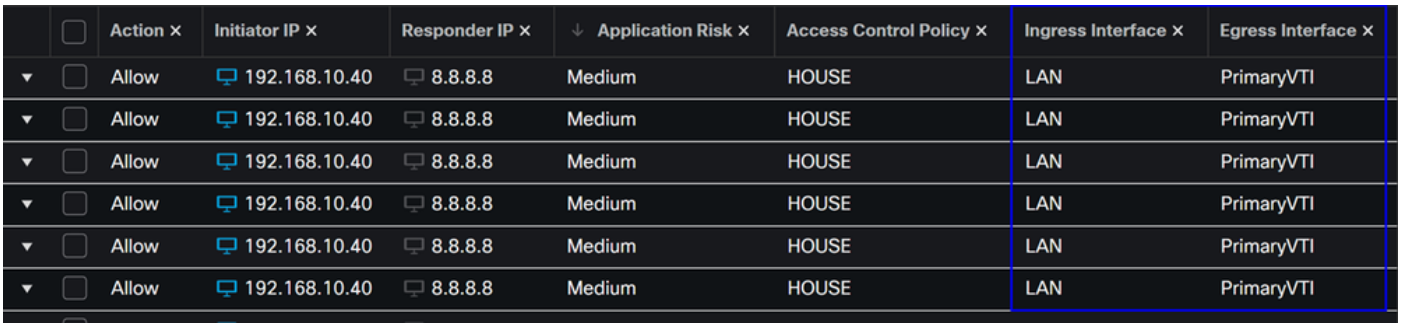
Après cela, vous devez le **Save** reconfigurer, et vous l'avez configuré de la manière suivante :



Vous pouvez déployer et vous pouvez voir le trafic des machines configurées sur la liste de

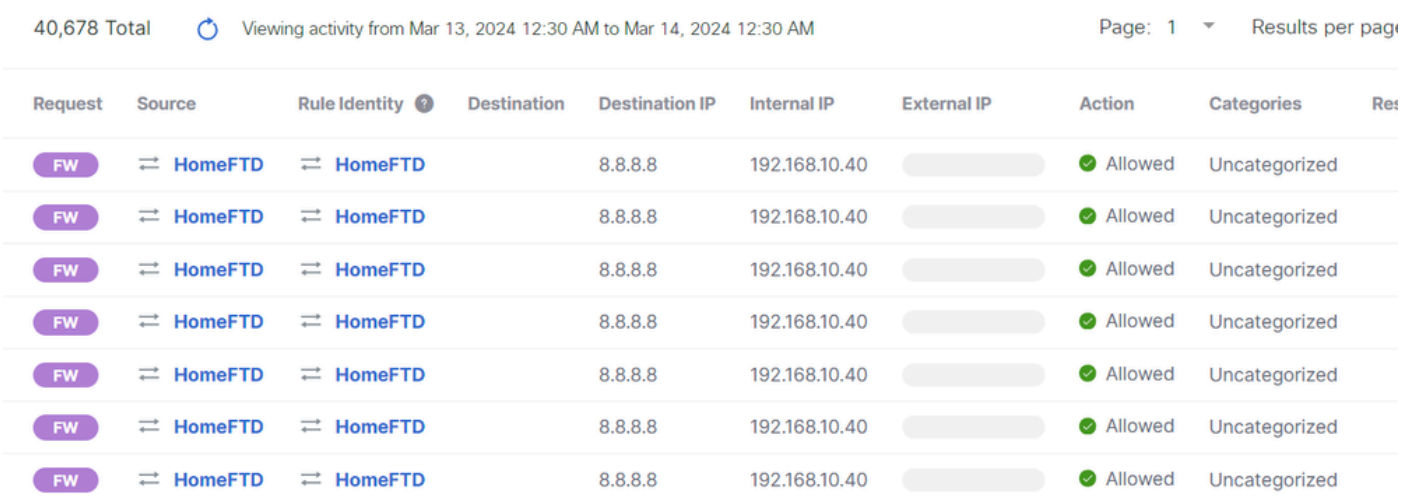
contrôle d'accès acheminer le trafic vers l'accès sécurisé :

À partir des événements Conexion dans le FMC :



Action	Initiator IP	Responder IP	Application Risk	Access Control Policy	Ingress Interface	Egress Interface
Allow	192.168.10.40	8.8.8.8	Medium	HOUSE	LAN	PrimaryVTI
Allow	192.168.10.40	8.8.8.8	Medium	HOUSE	LAN	PrimaryVTI
Allow	192.168.10.40	8.8.8.8	Medium	HOUSE	LAN	PrimaryVTI
Allow	192.168.10.40	8.8.8.8	Medium	HOUSE	LAN	PrimaryVTI
Allow	192.168.10.40	8.8.8.8	Medium	HOUSE	LAN	PrimaryVTI
Allow	192.168.10.40	8.8.8.8	Medium	HOUSE	LAN	PrimaryVTI

À partir de la recherche d'activité dans Secure Access :



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

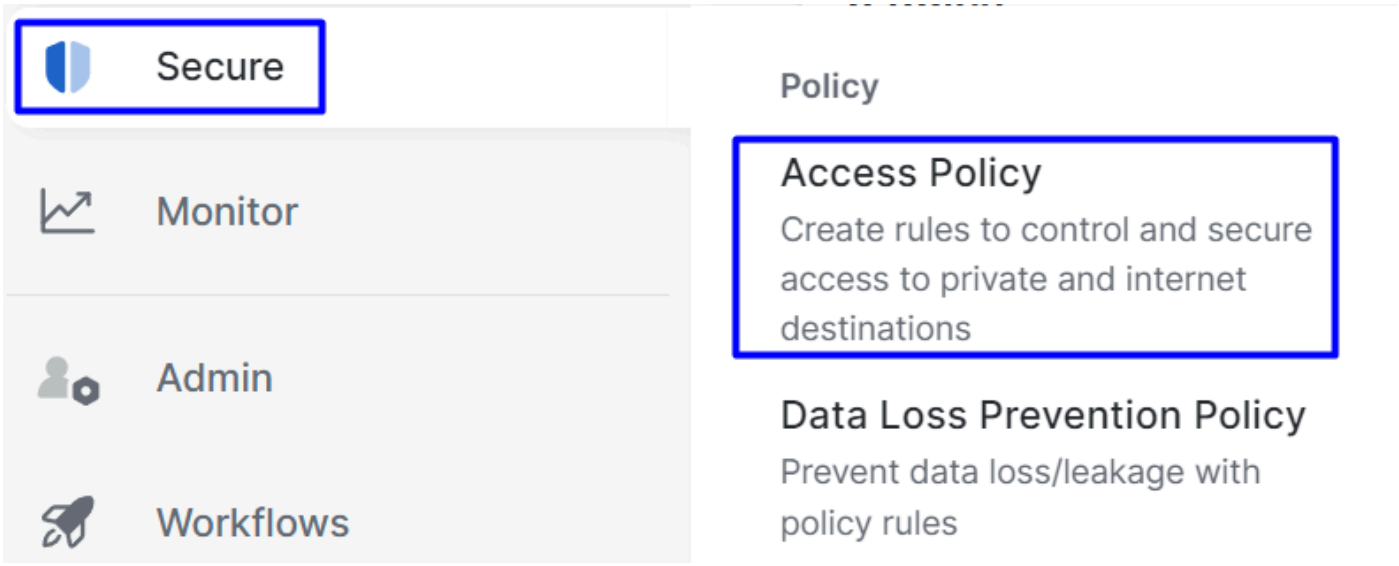
Request	Source	Rule Identity	Destination	Destination IP	Internal IP	External IP	Action	Categories	Res
FW	HomeFTD	HomeFTD		8.8.8.8	192.168.10.40		Allowed	Uncategorized	
FW	HomeFTD	HomeFTD		8.8.8.8	192.168.10.40		Allowed	Uncategorized	
FW	HomeFTD	HomeFTD		8.8.8.8	192.168.10.40		Allowed	Uncategorized	
FW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

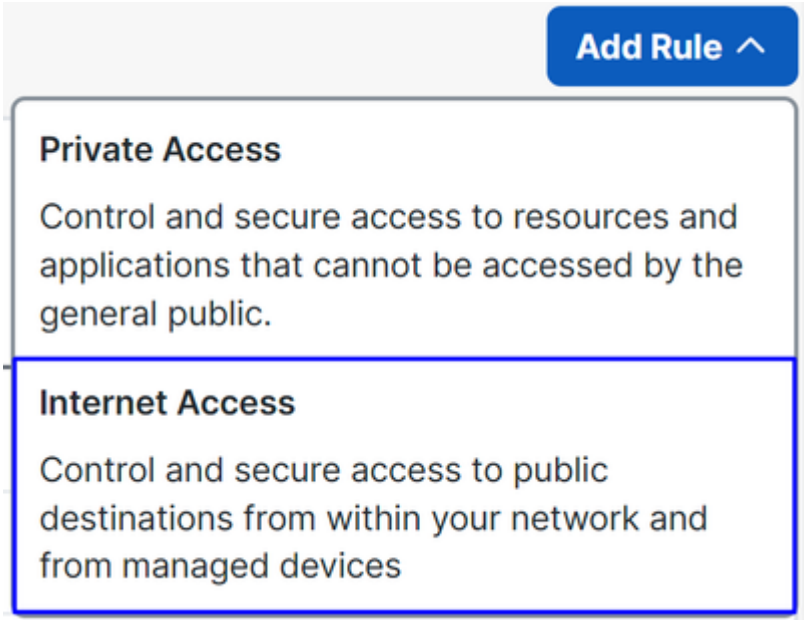
Configurer la stratégie d'accès Internet sur l'accès sécurisé

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

- Cliquez sur **Secure** > **Access Policy**



- Cliquez sur Add Rule > Internet Access

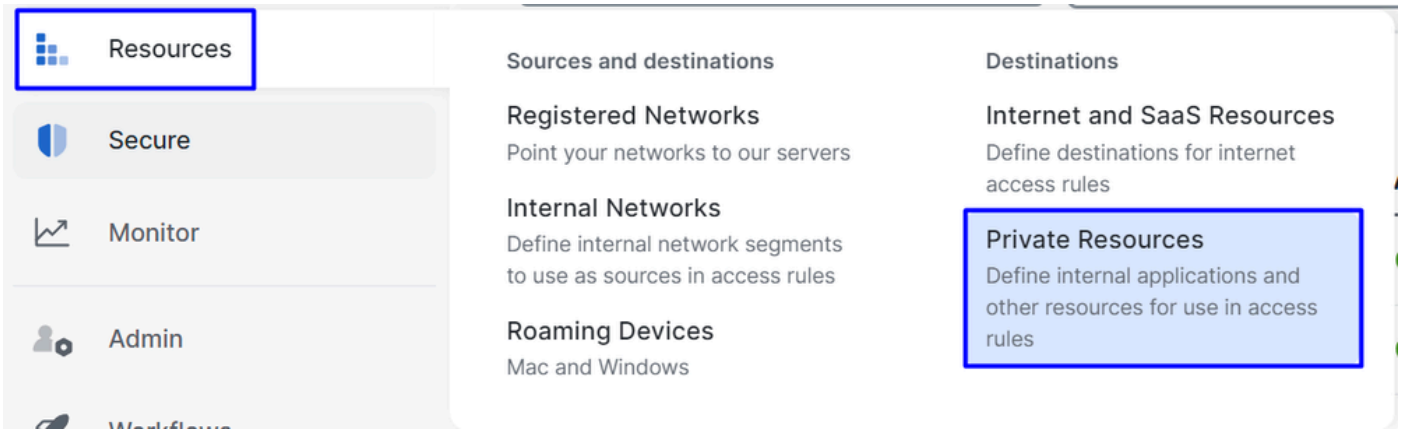


Vous pouvez alors spécifier la source comme tunnel et la destination. Vous pouvez choisir n'importe lequel, en fonction de ce que vous configurez sur la stratégie. Veuillez consulter le Guide de l'utilisateur Secure Access.

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

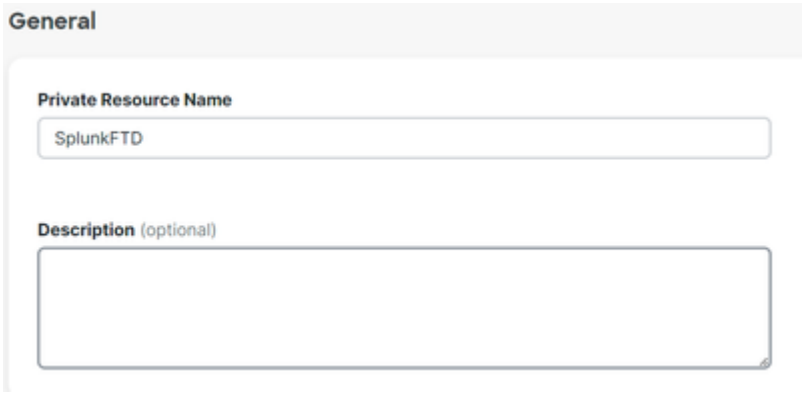
Pour configurer l'accès pour les ressources privées, vous devez d'abord créer les ressources sous le tableau de bord d'accès sécurisé :

- Cliquez sur **Resources** > **Private Resources**



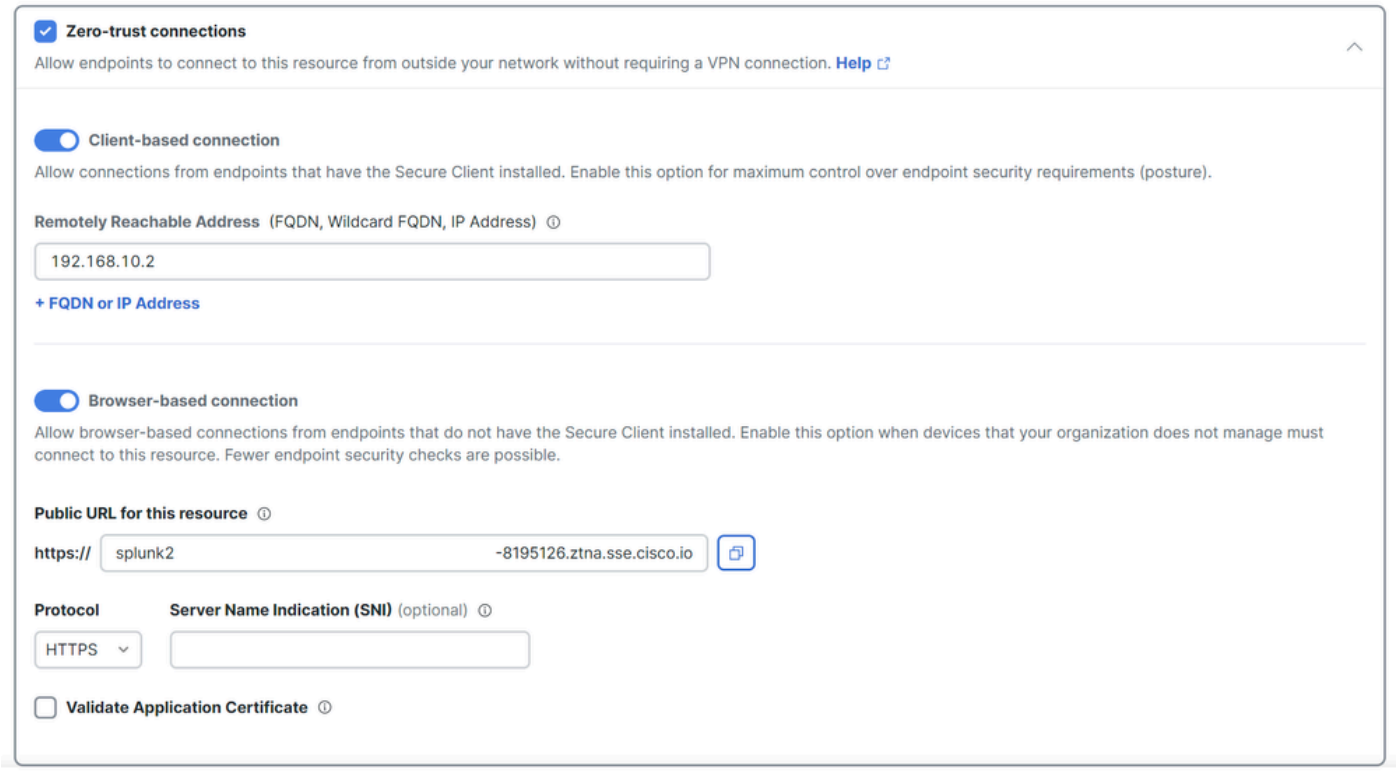
- Cliquez ensuite sur **Add**
- Sous la configuration, vous trouverez les sections suivantes à configurer : **General, Communication with Secure Access Cloud and Endpoint Connection Methods.**

Généralités



- Private Resource Name: Créez un nom pour la ressource à laquelle vous fournissez un accès via l'accès sécurisé à votre réseau.

Méthodes de connexion Endpoint



- **Zero Trust Connections**: Cochez la case.
- **Client-based connection**: Si vous activez cette option, 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 FQDN, vous devez ajouter DNS pour résoudre le nom.
- **Browser-based connection**: Si vous activez cette option, 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 votre navigateur (Secure Access protège cette ressource).
- **Protocol**: Sélectionnez le protocole (HTTP ou HTTPS).



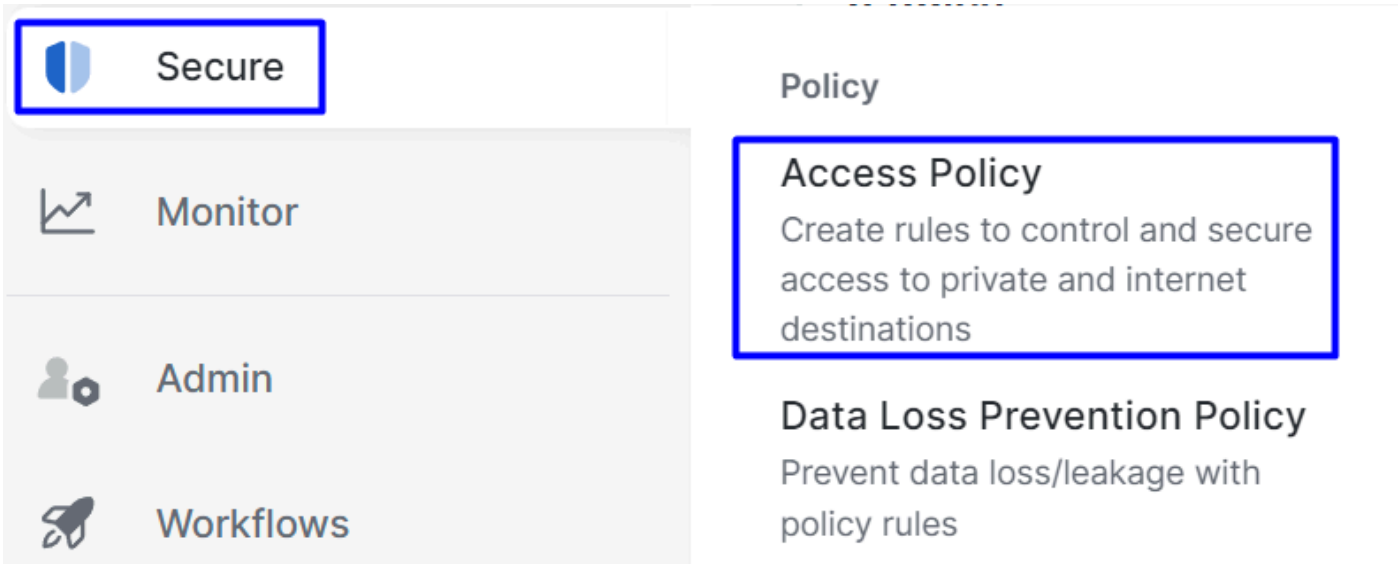
VPN Connection: Cochez cette case pour activer l'accès via RA-VPNaaS.

Cliquez sur **Save** et vous pouvez ajouter cette ressource à la **Access Policy**.

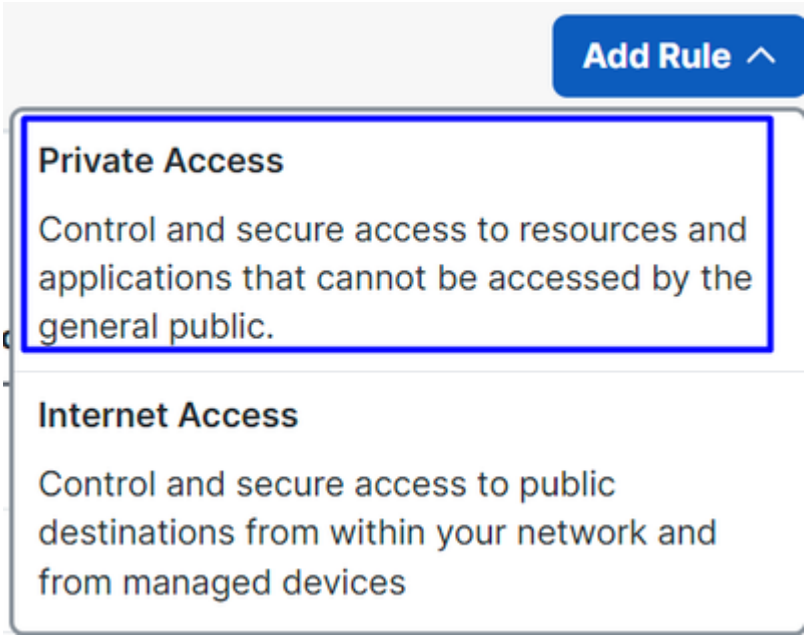
Configurer la stratégie d'accès

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

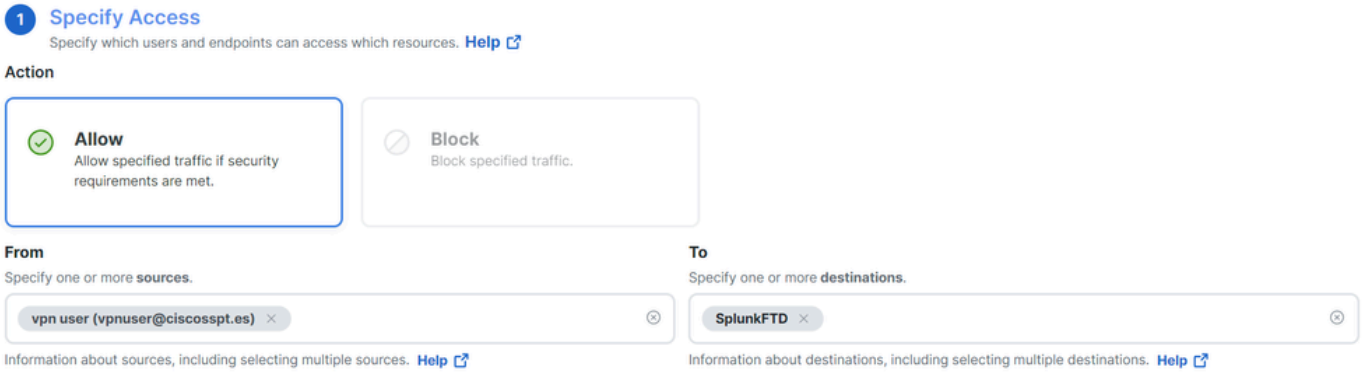
- Cliquez sur **Secure** > **Access Policy**



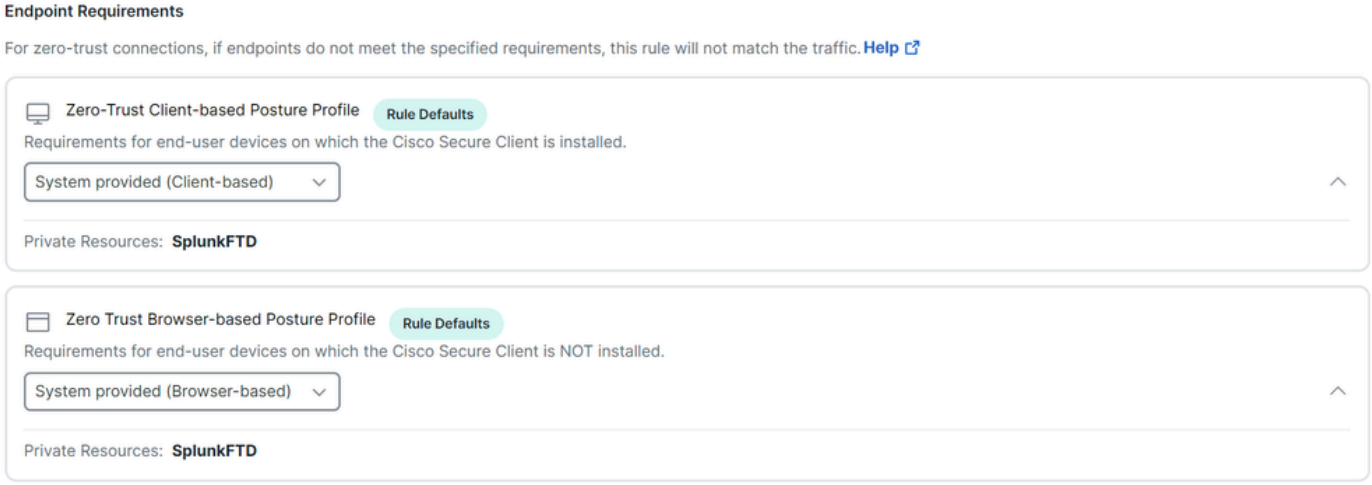
- Cliquer **Add** > **Private Resource**



Pour cette règle d'accès privé, vous devez configurer les valeurs par défaut pour fournir l'accès à la ressource. Pour plus d'informations sur les configurations des stratégies, consultez le Guide de l'utilisateur.



- **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.



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

---

Remarque : Pour plus d'informations sur la politique de posture, consultez le guide de l'utilisateur sur l'accès sécurisé.

- Cliquez **Next** et Save après vos configurations, et vous pouvez accéder à vos ressources via RA-VPN, Client Base ZTNA ou Browser Base ZTNA.

Dépannage

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

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                        G
      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                      G
      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

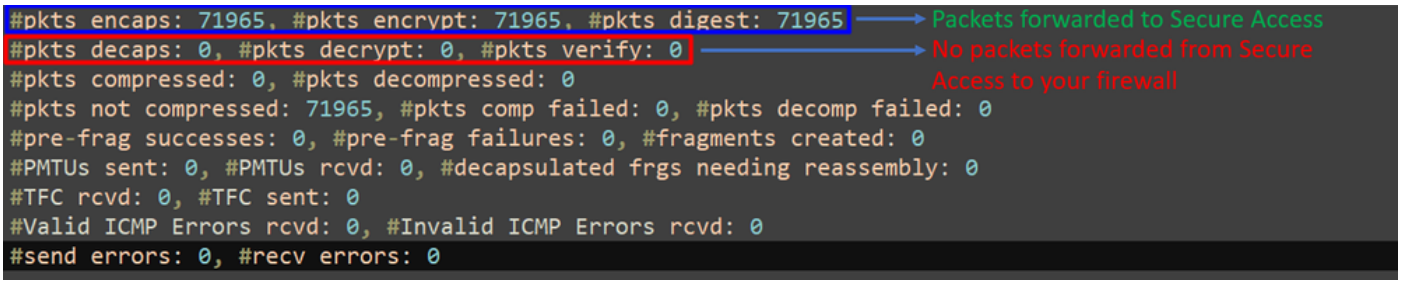

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
```

```
    #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 paquet encaps et decaps.



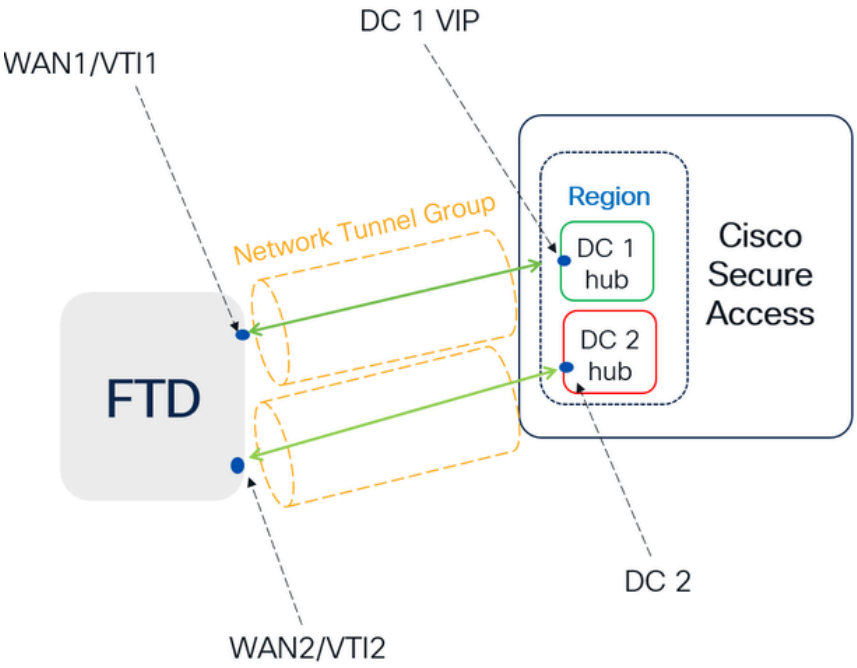
Si vous avez ce scénario, ouvrez un dossier auprès du TAC.

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 est ouverte pour recevoir le trafic ; la porte du DC 2 est fermée jusqu'à ce que le tunnel numéro 1 soit hors service.

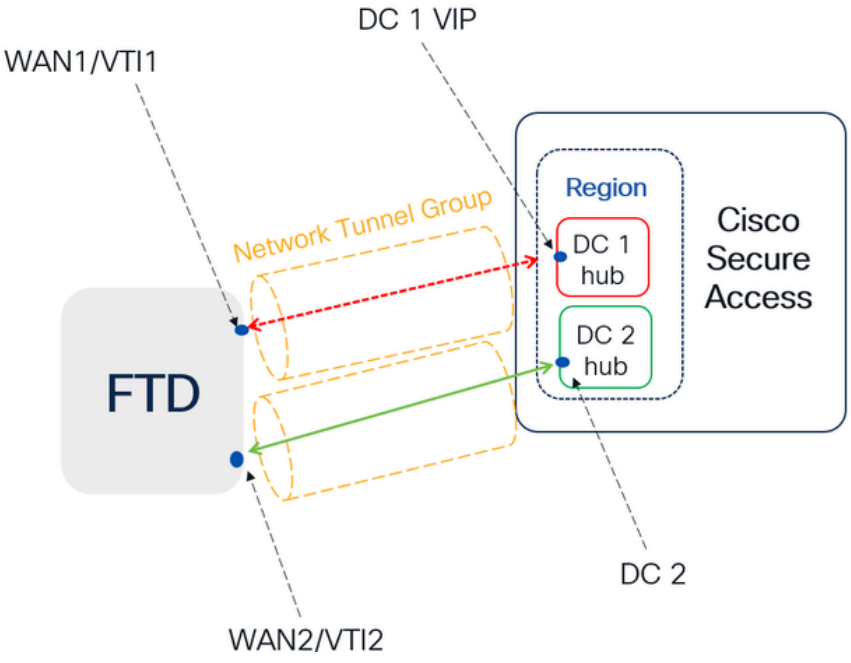
Normal Behavior



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

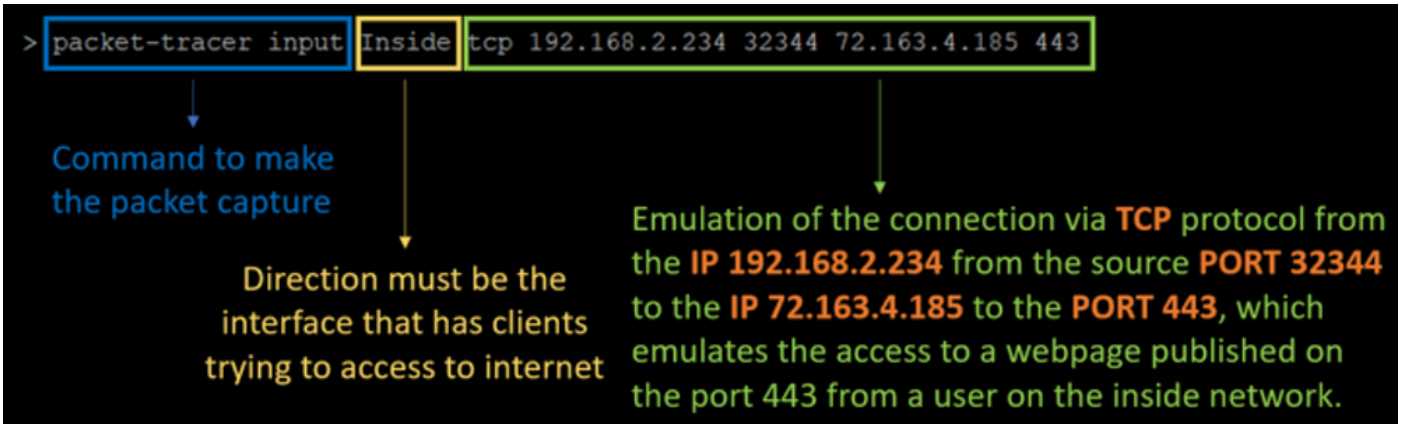
- DC2 is Active when DC1or WAN1 peer is Down
- High availability is implemented to address failures in the WAN1 channel on the Firewall, ensuring operational continuity in the region and mitigating potential issues in DC1

Vérification du routage du trafic pour un accès sécurisé

Dans cet exemple, la machine source sur le réseau de pare-feu utilisé est :

- 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'

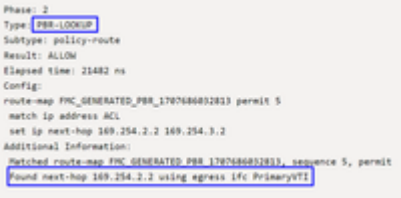
Phase: 14
Type: SNORT
Subtype: appid
Result: ALLOW
Elapsed time: 28820 ns
Config:
Additional Information:
service: (0), client: (0), payload: (0), misc: (0)

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
```

Il existe de nombreux scénarios qui peuvent fournir un contexte supplémentaire sur la configuration sous la configuration PBR pour garantir que le trafic est correctement acheminé vers l'accès sécurisé :



La phase 2 indique que le trafic est transféré vers l' **PrimaryVTI**interface, ce qui est correct en fonction des configurations de ce scénario, car 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:
```

La phase 8 correspond à l'étape de cryptage dans une connexion VPN, où le trafic est évalué et autorisé pour le cryptage, garantissant ainsi la transmission sécurisée des données. La phase 9 se concentre sur la gestion spécifique du flux de trafic dans le tunnel VPN IPSec, confirmant que le trafic chiffré est correctement routé et autorisé à passer par le tunnel établi.

```
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
```

Pour finaliser, à la fin du flux, vous pouvez voir le trafic de la LAN vers le trafic de **PrimaryVTI** transfert vers l'accès sécurisé. Cette action confirme que le trafic est routé sans problème.

Informations connexes

- Assistance technique de Cisco et téléchargements
- Centre d'aide Cisco Secure Access
- Présentation du module de plateforme sécurisée virtuelle
- Module d'accès Zero Trust
- Dépannez L'Erreur D'Accès Sécurisé « Le Service D'Inscription Ne Répond Pas. Contactez votre service d'assistance informatique"

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.