Configuración de un acceso seguro con firewall seguro y alta disponibilidad

Contenido

Introducción

Este documento describe cómo configurar Secure Access con Secure Firewall con High Availability.

Prerequisites

- Configurar aprovisionamiento de usuarios
- Configuración de Autenticación SSO de ZTNA
- Configurar acceso seguro VPN de acceso remoto

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Firepower Management Center 7.2
- Firepower Threat Defense 7.2
- Acceso seguro
- Cisco Secure Client - VPN
- Cisco Secure Client: ZTNA
- ZTNA sin cliente

Componentes Utilizados

La información de este documento se basa en:

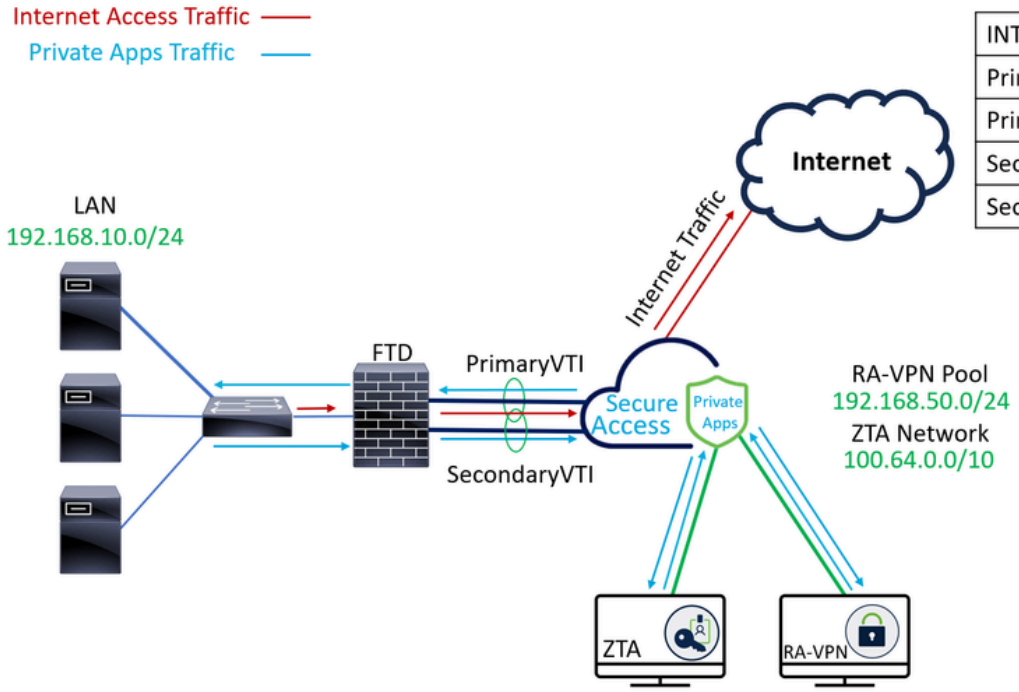
- Firepower Management Center 7.2
- Firepower Threat Defense 7.2
- Acceso seguro
- Cisco Secure Client - VPN
- Cisco Secure Client: ZTNA

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Cisco ha diseñado Secure Access para proteger y proporcionar acceso a aplicaciones privadas, tanto in situ como basadas en la nube. También protege la conexión de la red a Internet. Esto se consigue mediante la implementación de varios métodos y capas de seguridad, todo ello con el objetivo de preservar la información a medida que acceden a ella a través de la nube.

Diagrama de la red



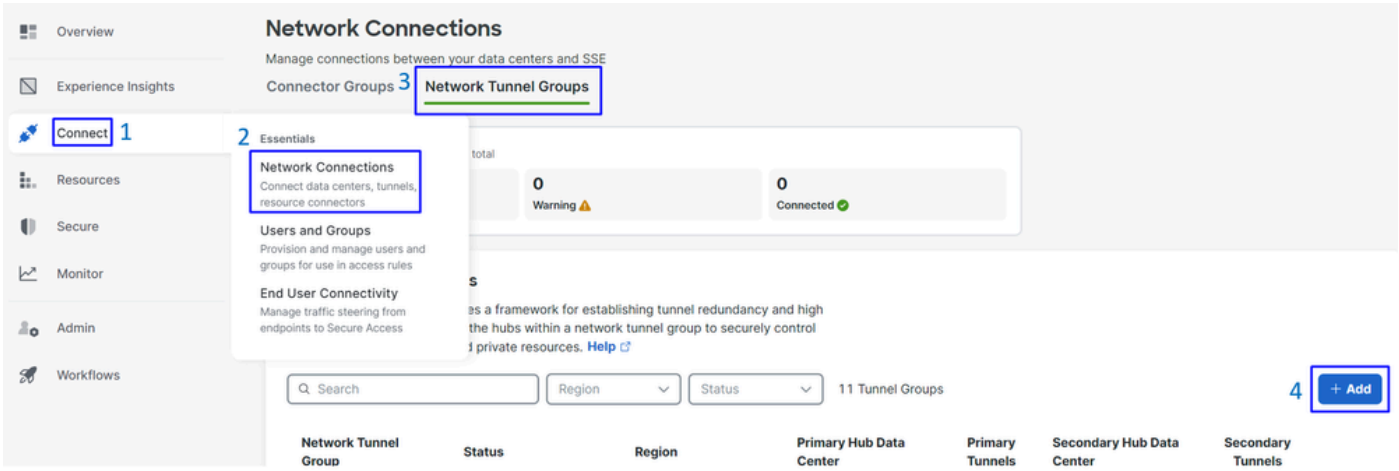
INTERFACE	IP
PrimaryWAN	192.168.30.5
PrimaryVTI	169.254.2.1
SecondaryWAN	192.168.0.202
SecondaryVTI	169.254.3.1

Configurar

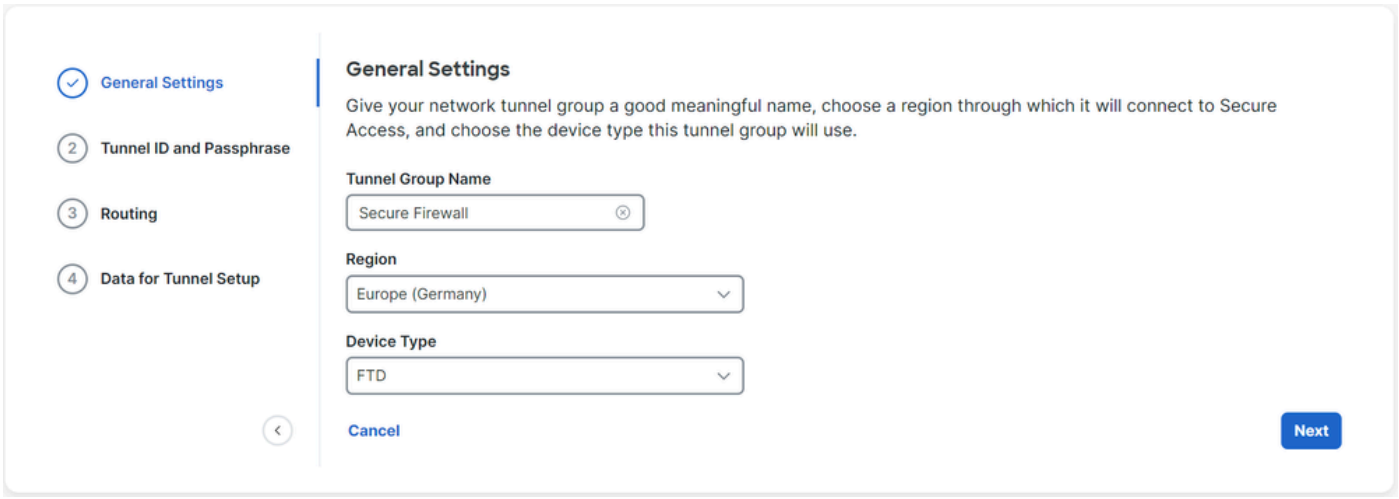
Configuración de la VPN en Secure Access

Vaya al panel de administración de Acceso seguro.

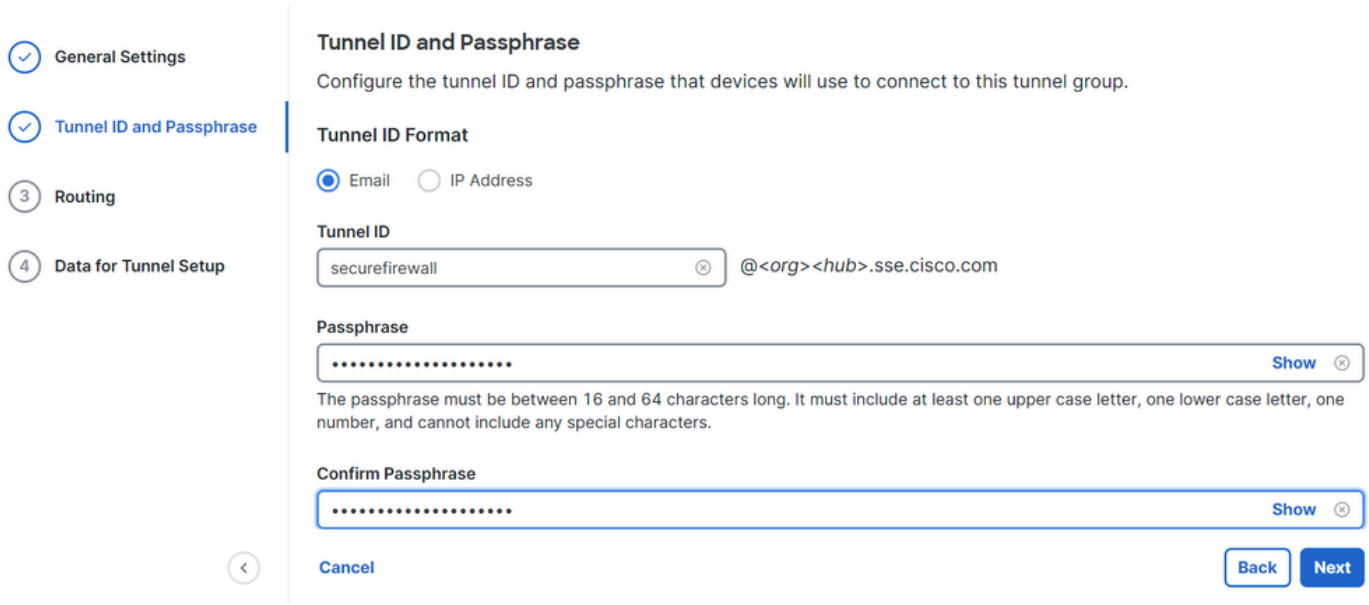
- Haga clic en Connect > Network Connections
- EnNetwork Tunnel Groupshaga clic en + Add



- ConfigurarTunnel Group Name, RegionyDevice Type
- Haga clic en **Next**



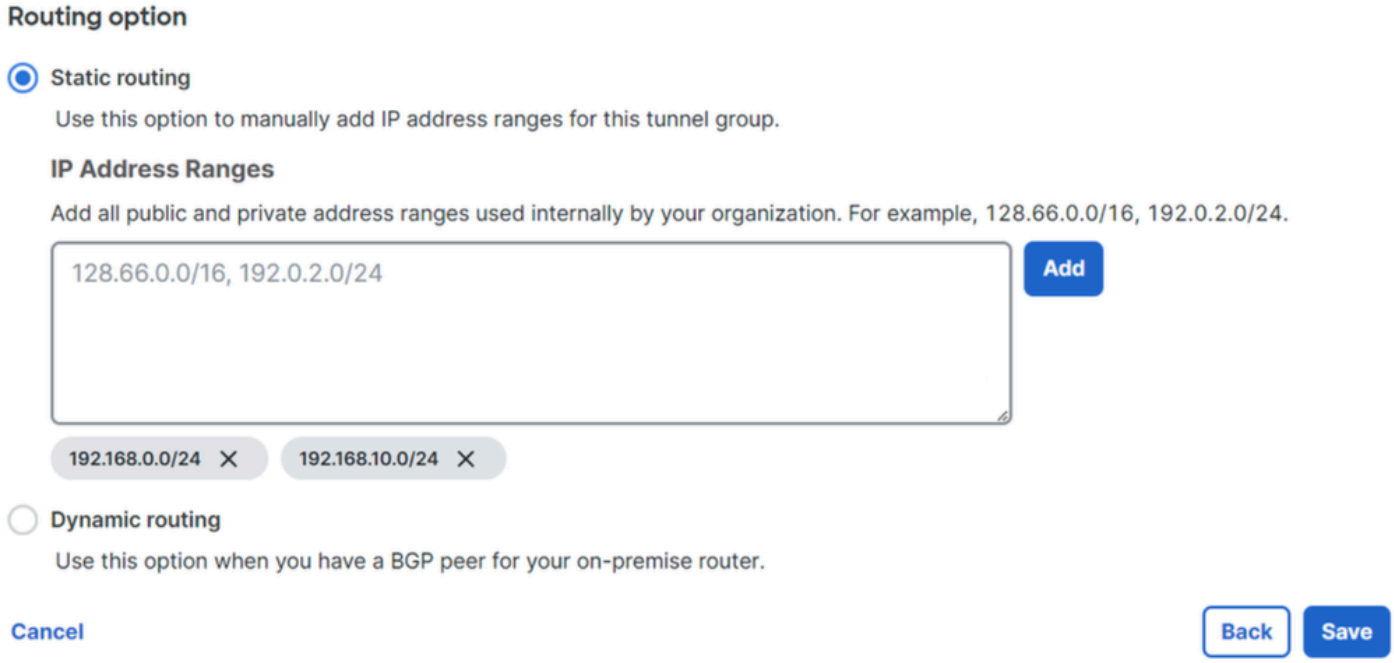
- Configure elTunnel ID Formaty Passphrase
- Haga clic enNext



- Configure los rangos de direcciones IP o los hosts que ha configurado en la red y que desea

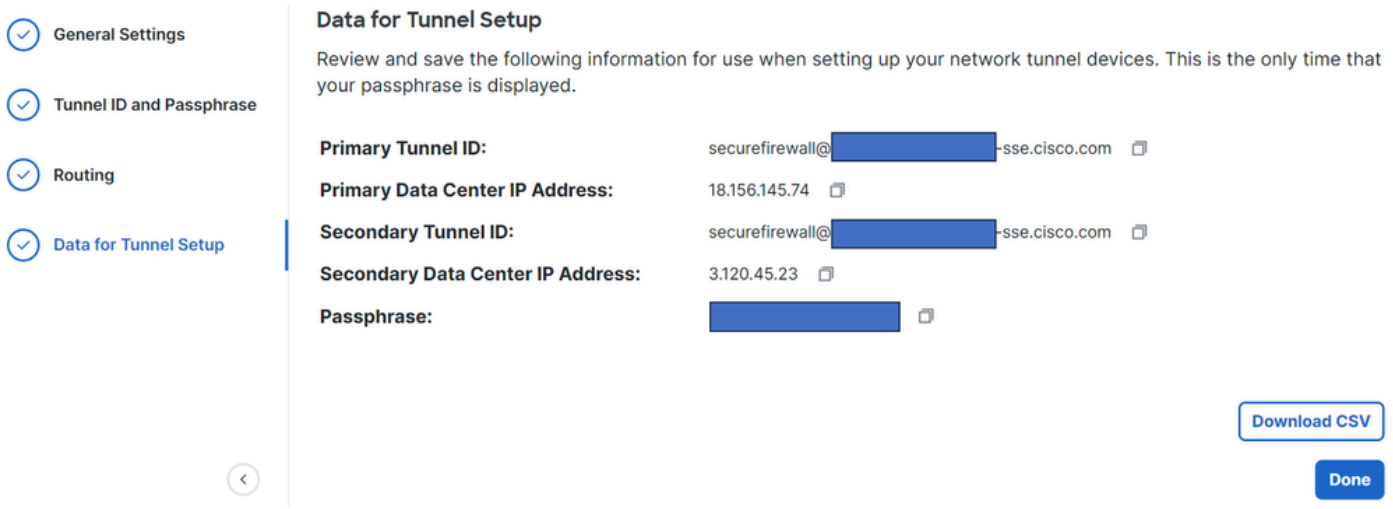
que el tráfico pase a través de Secure Access

- Haga clic en**Save**



Después de hacer clic en **Save** la información sobre el túnel se muestra, por favor, guarde esa información para el siguiente paso, **Configure the tunnel on Secure Firewall.**

Datos para la configuración del túnel

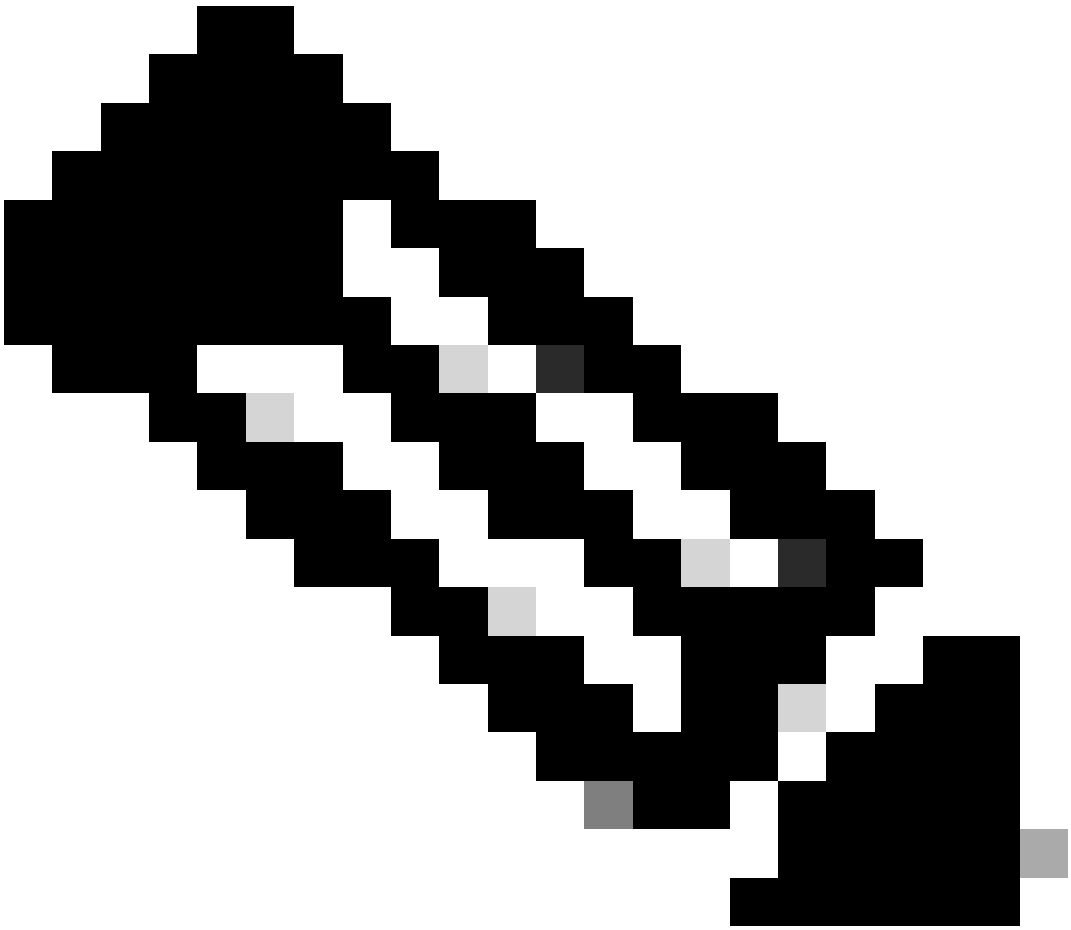


Configuración del túnel en Secure Firewall

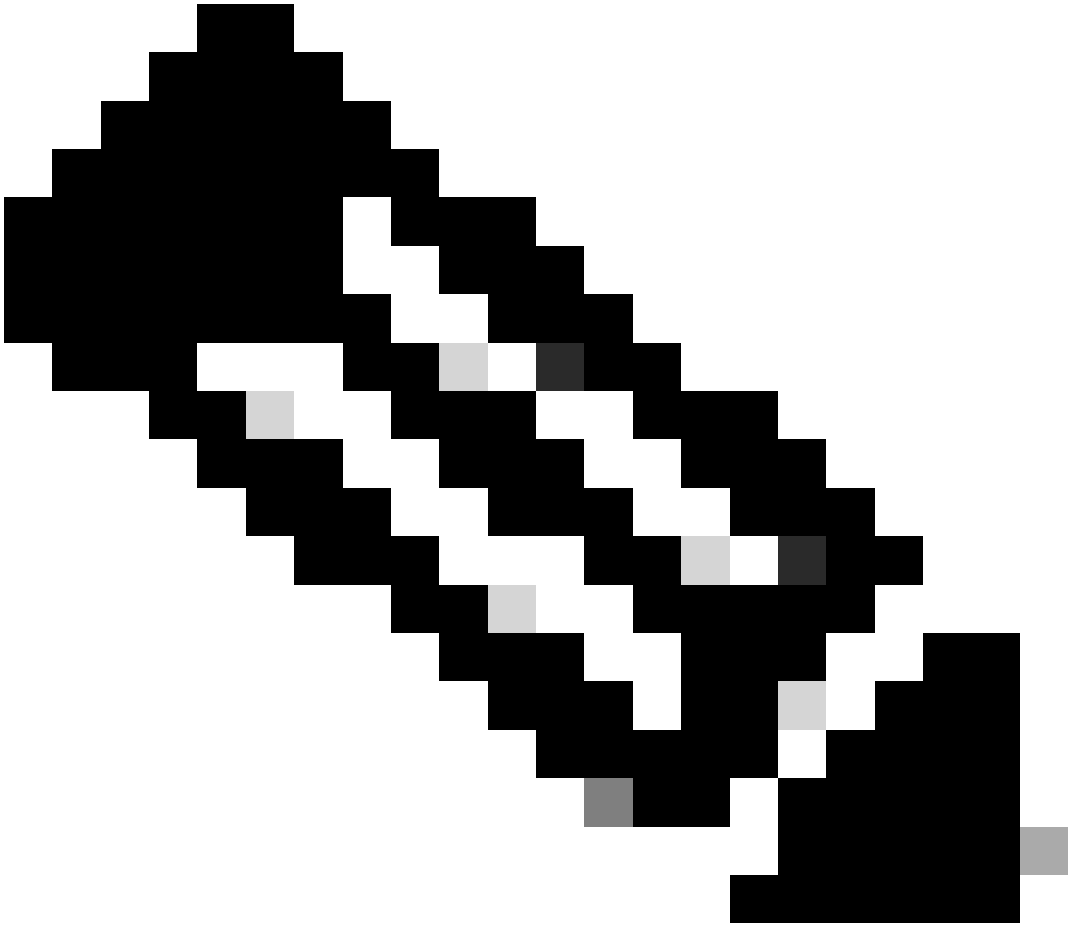
Configuración de la interfaz de túnel

Para este escenario, se utiliza la configuración de la interfaz de túnel virtual (VTI) en Secure Firewall para lograr este objetivo; recuerde, en este caso, tiene un ISP doble y queremos tener HA si uno de sus ISP falla.

INTERFACES	PAPEL
WAN principal	WAN de Internet principal
WAN secundaria	WAN de Internet secundaria
VTI primaria	Vinculado para enviar el tráfico a través del **Principal Internet WAN** a Secure Access
VTIsecundaria	Vinculado para enviar el tráfico a través del **Secondary Internet WAN** a Secure Access



Nota: 1. Debe agregar o asignar una ruta estática a los **Primary or Secondary Datacenter IP** túneles para poder tener ambos túneles activos.



Nota: 2. Si tiene ECMP configurado entre las interfaces, no necesita crear ninguna ruta estática al **Primary or Secondary Datacenter IP** para poder tener ambos túneles activos.

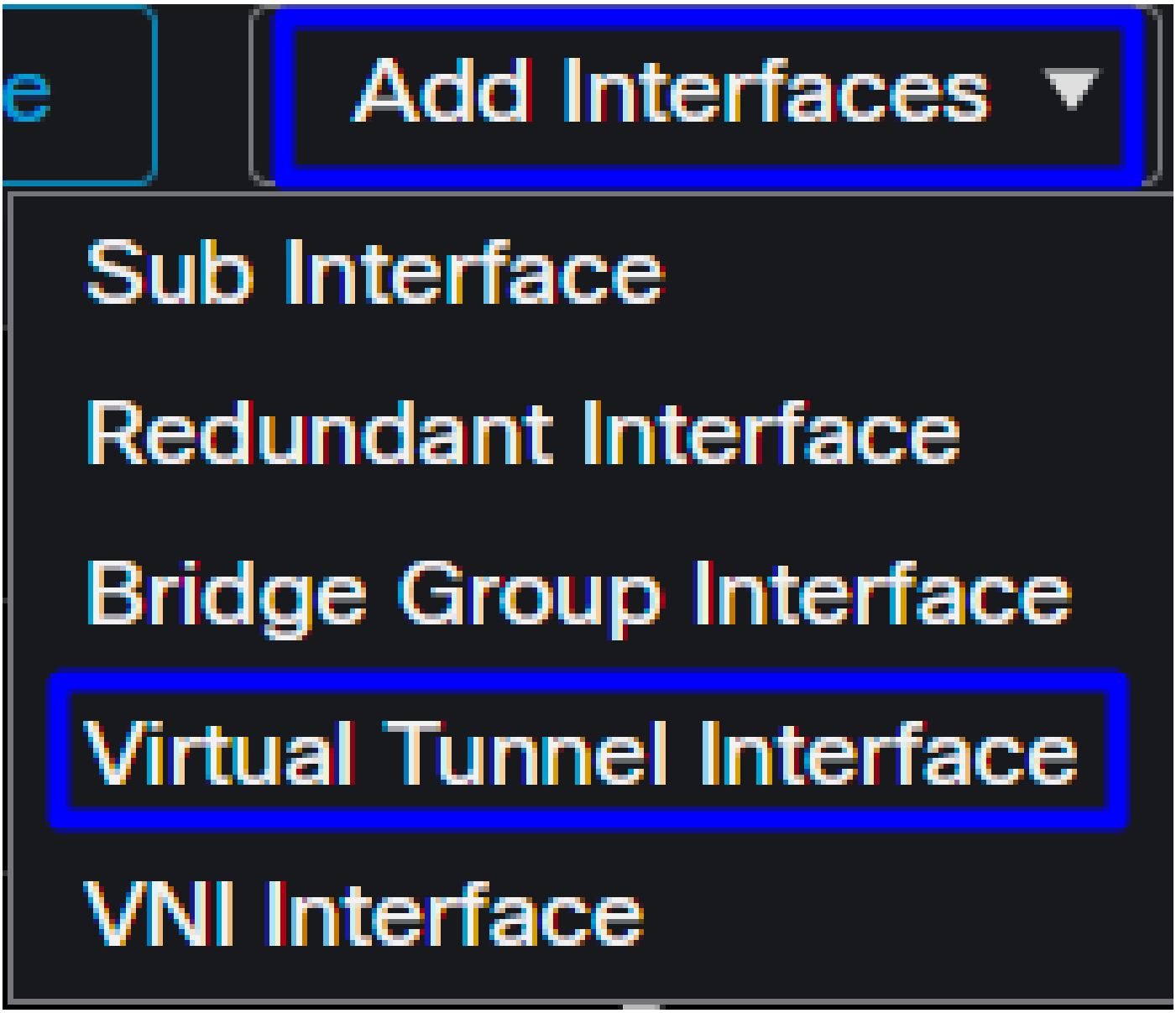
En función del escenario, tenemos **PrimaryWAN** y **SecondaryWAN**, que debemos utilizar para crear las interfaces VTI.

Desplácese hasta elFirepower Management Center > Devices.

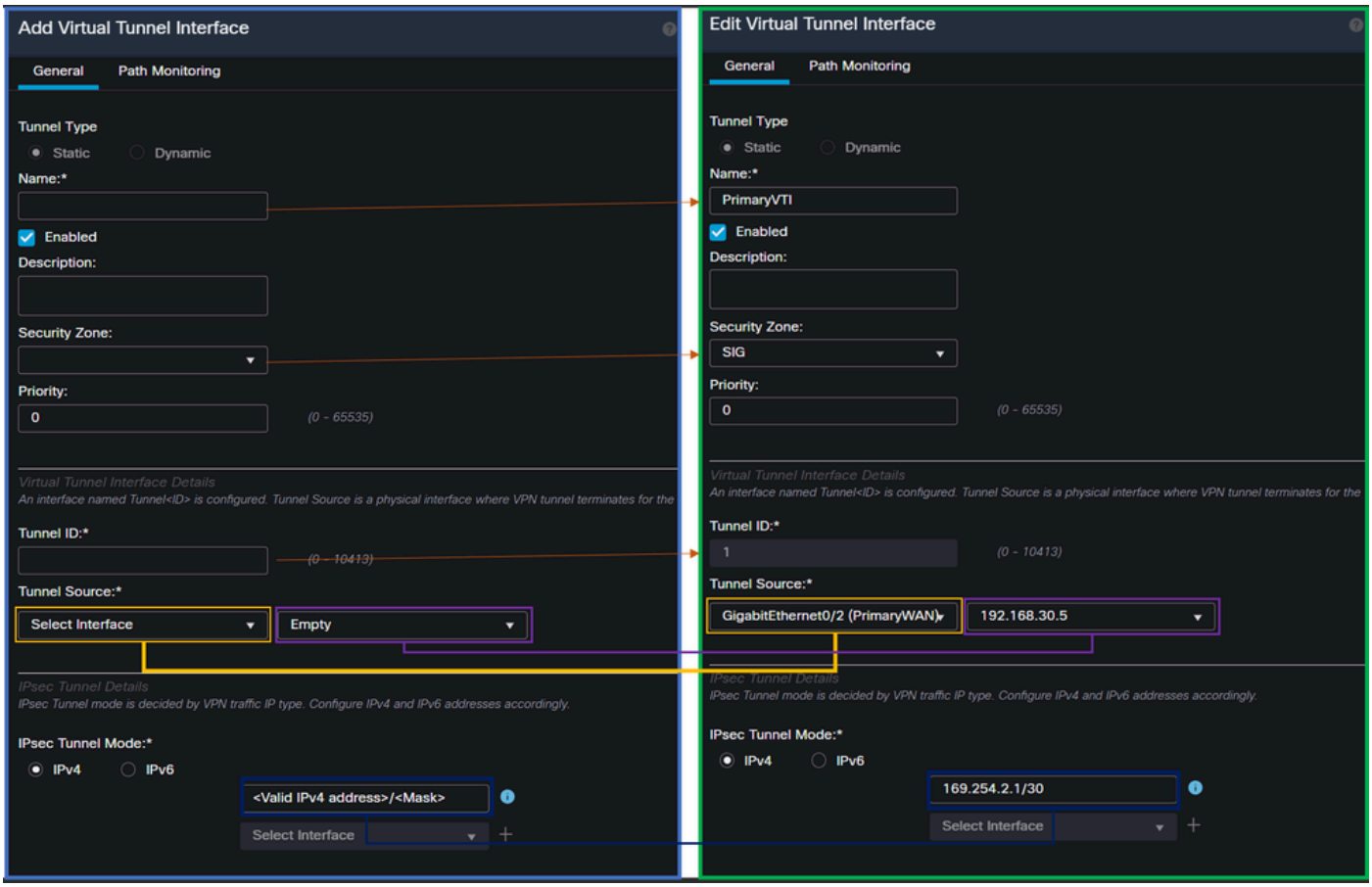
- Elija su FTD
- Elegir **Interfaces**

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)

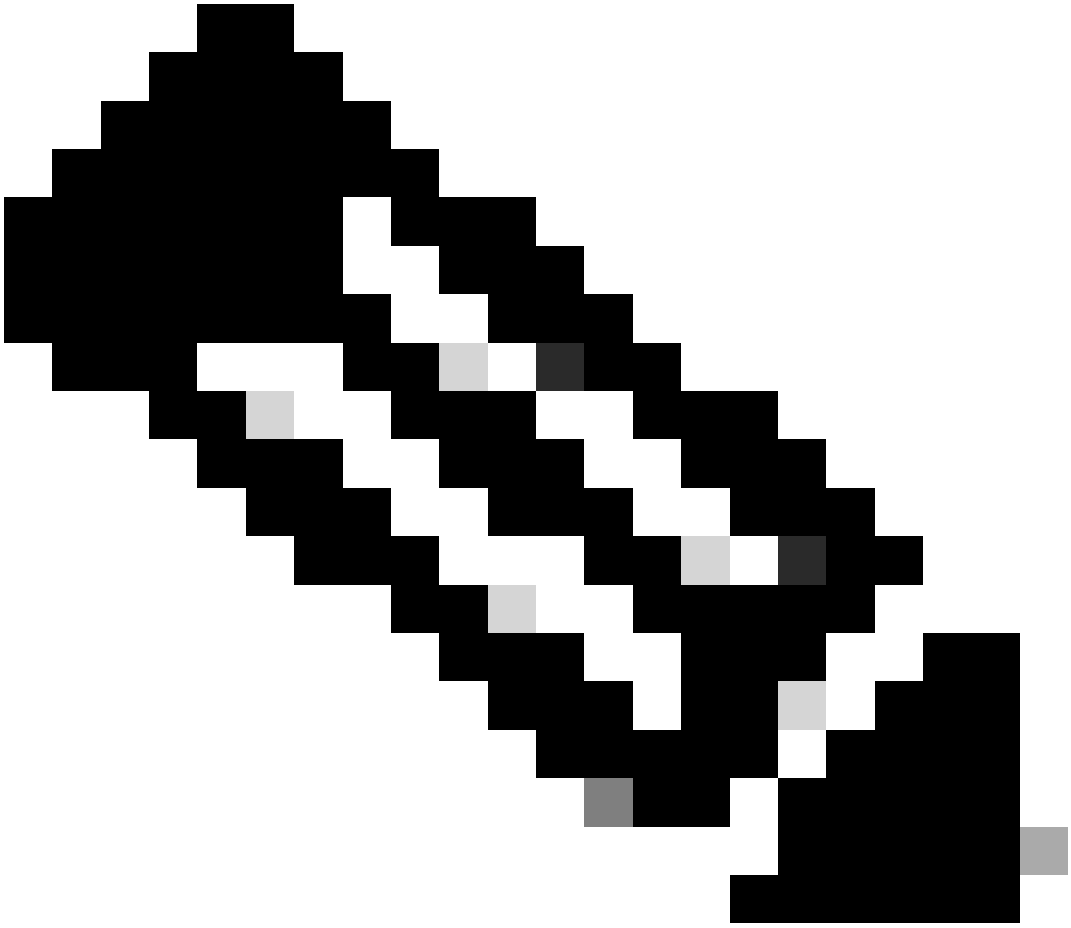
- Haga clic en **Add Interfaces** > **Virtual Tunnel Interface**



- Configurar la interfaz en función de la siguiente información



- **Name** : Configure un nombre que haga referencia al **PrimaryWAN interface**
- **Security Zone** : Puede reutilizar otro **Security Zone**, pero es mejor crear uno nuevo para el tráfico de acceso seguro
- **Tunnel ID** : Agregue un número para la ID de túnel
- **Tunnel Source** : Elija su **PrimaryWAN interface** y elija la IP privada o pública de su interfaz
- IPsec Tunnel Mode : Elija **IPv4** y configure una IP no enrutable en su red con la máscara 30



Nota: Para la interfaz VTI, debe utilizar una IP no enrutable; por ejemplo, si tiene dos interfaces VTI, puede utilizar 169.254.2.1/30 para el **PrimaryVTI** y 169.254.3.1/30 para el **SecondaryVTI.**

Después de eso, debe hacer lo mismo con el **SecondaryWAN interface**, y tiene todo configurado para la alta disponibilidad de VTI, y como resultado, tiene el siguiente resultado:

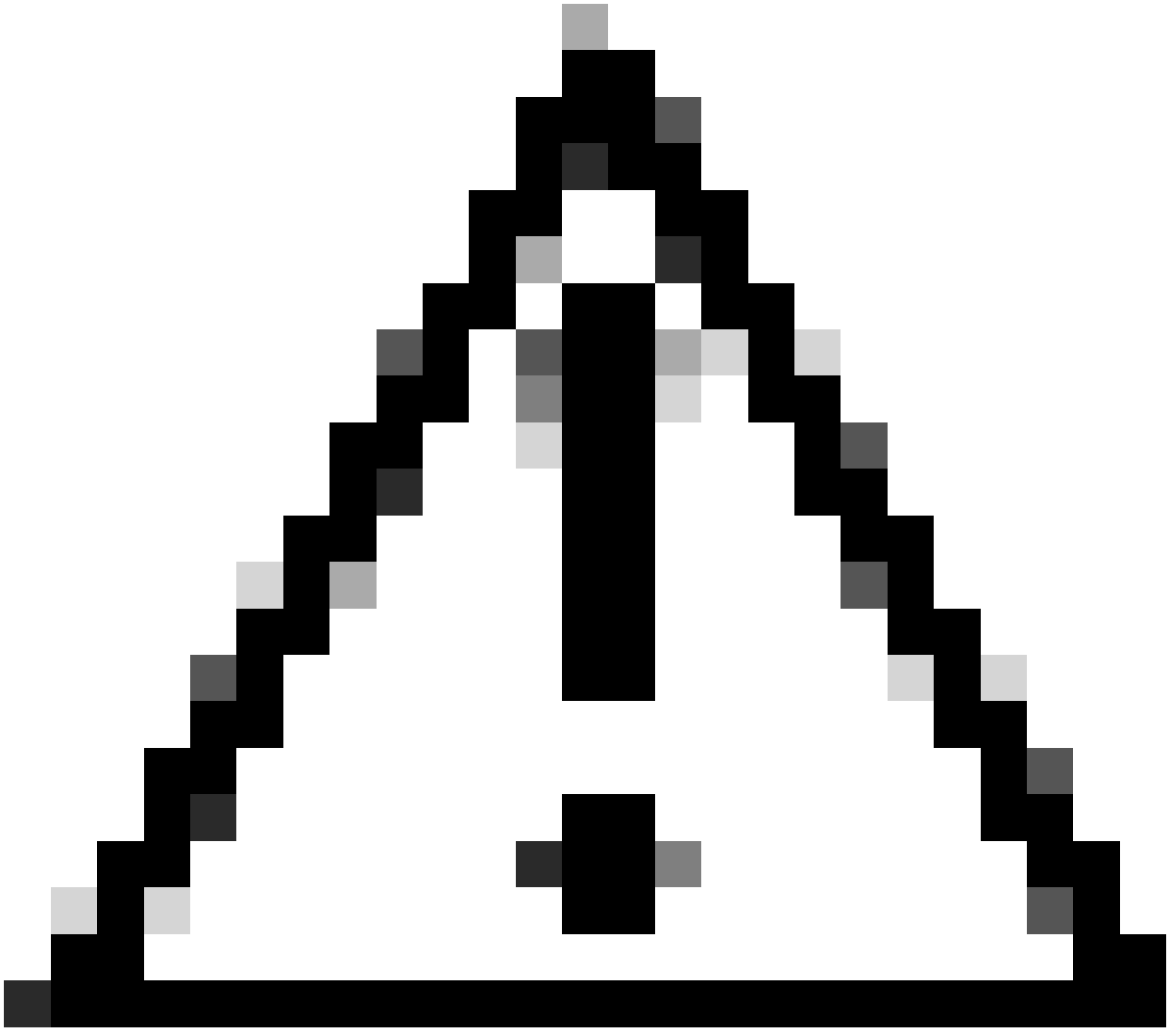
Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address
Diagnostic0/0	diagnostic	Physical			
GigabitEthernet0/0	SecondaryWAN	Physical	SecondaryWAN		192.168.0.202/24(Static)
Tunnel2	SecondaryVTI	VTI	SIG		169.254.3.1/30(Static)
GigabitEthernet0/1	LAN	Physical	LAN		192.168.10.1/24(Static)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

Para este escenario, las IP utilizadas son:

Configuración de IP de VTI		
Nombre lógico	IP	Rango
VTI primaria	169.254.2.1/30	169.254.2.1-169.254.2.2
VTIsecundaria	169.254.3.1/30	169.254.3.1-169.254.3.2

Configuración de la ruta estática para la interfaz secundaria

Para permitir que el tráfico de **SecondaryWAN interface** llegue a la redSecondary Datacenter IP Address, debe configurar una ruta estática a la IP del Data Center. Puede configurarlo con una métrica de uno (1) para colocarlo encima de la tabla de ruteo; también, especifique la IP como host.

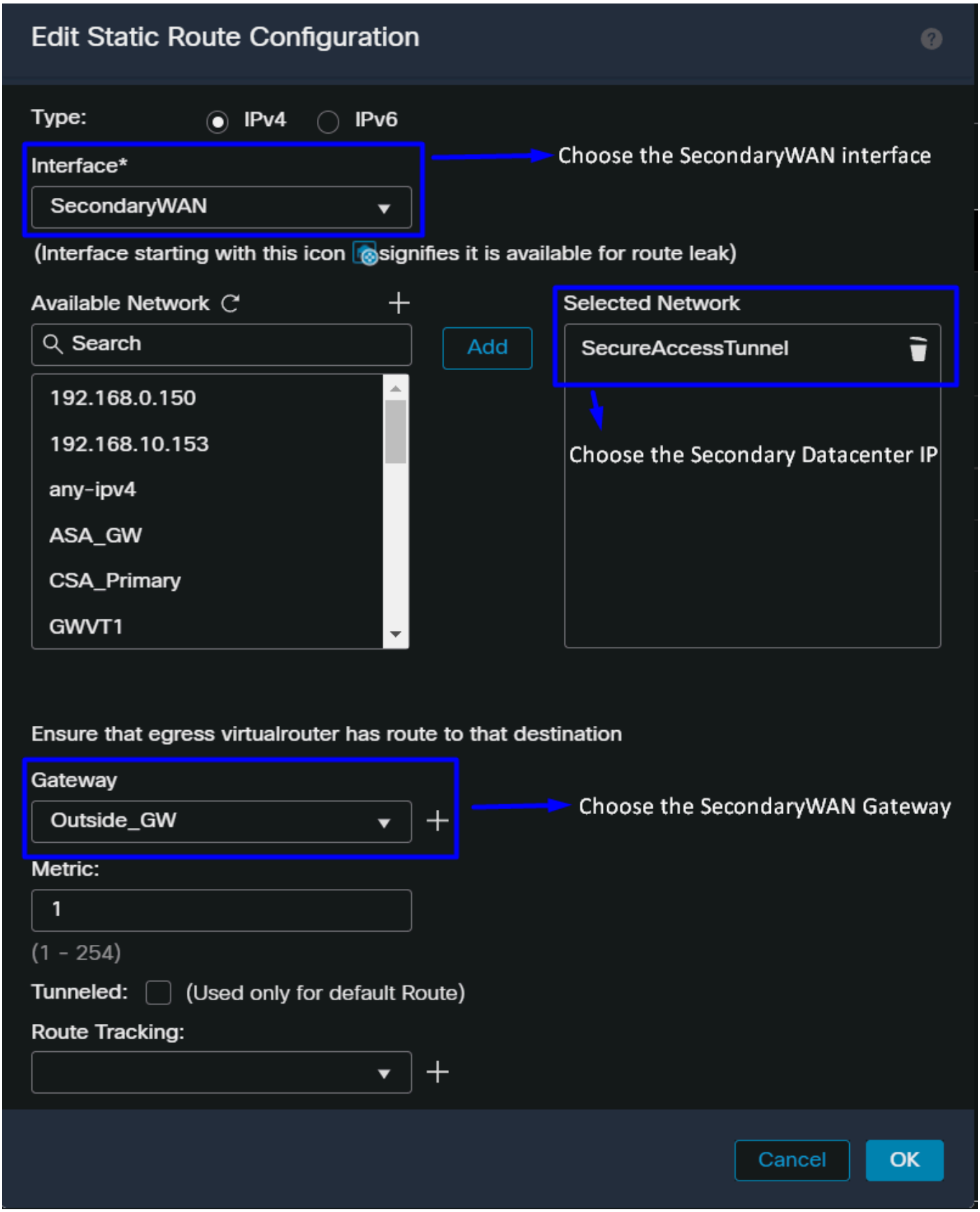


Precaución: Esto solo es necesario si no tiene una configuración ECMP entre los canales

WAN; si tiene ECMP configurado, puede saltar al paso siguiente.

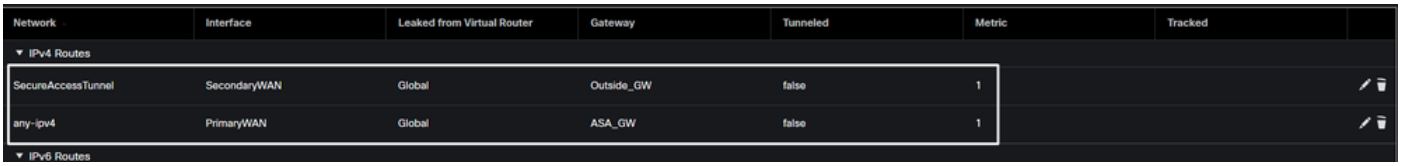
Vaya a **Device** > **Device Management**

- Haga clic en el dispositivo FTD
- Haga clic en **Routing**
- Elegir **Static Route** > **+ Add Route**



- Interface: Elija la interfaz WAN secundaria
- **Gateway**: Elija el gateway WAN secundario
- Selected Network: Agregue la IP del Data Center secundario como host; puede encontrar la información en la información proporcionada cuando configura el túnel en el paso Secure Access, Datos para la Configuración del Túnel

- **Metric**: Utilice una (1)
- OKHaga clic en **Save** y para guardar la información y, a continuación, realice la implementación.



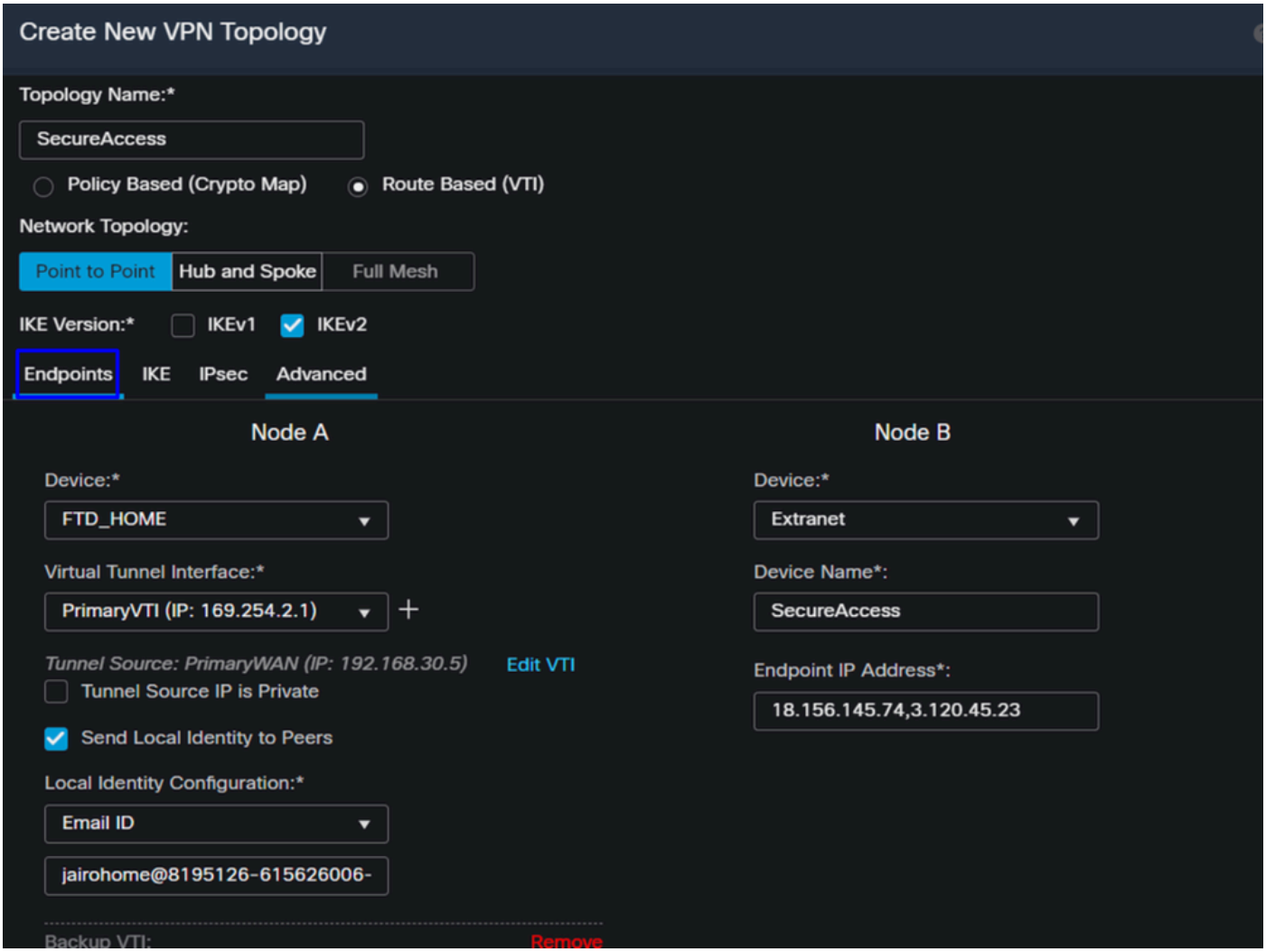
Configuración de VPN para Secure Access en modo VTI

Para configurar la VPN, navegue hasta el firewall:

- Haga clic en **Devices** > **Site to Site**
- Haga clic en + Site to Site VPN

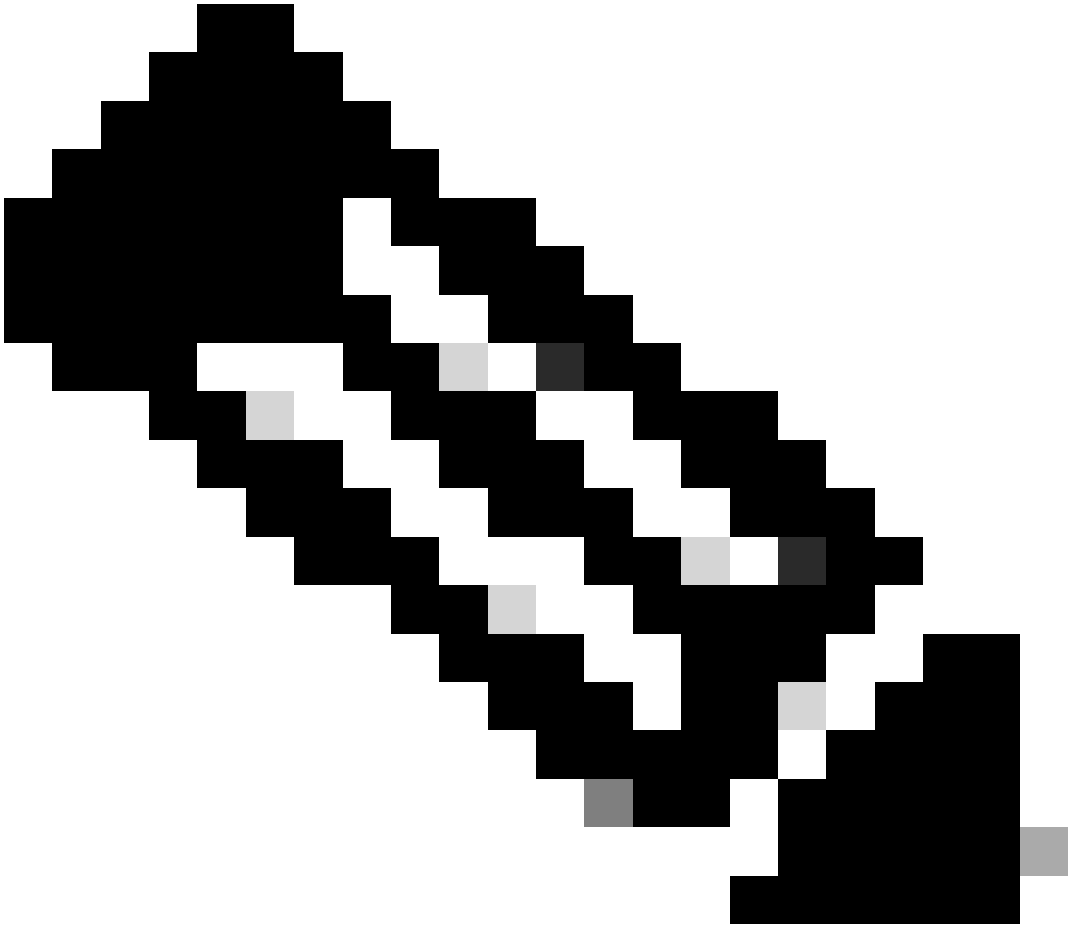
Configuración de terminales

Para configurar el paso Terminales, debe utilizar la información proporcionada en el paso Data for Tunnel Setup.



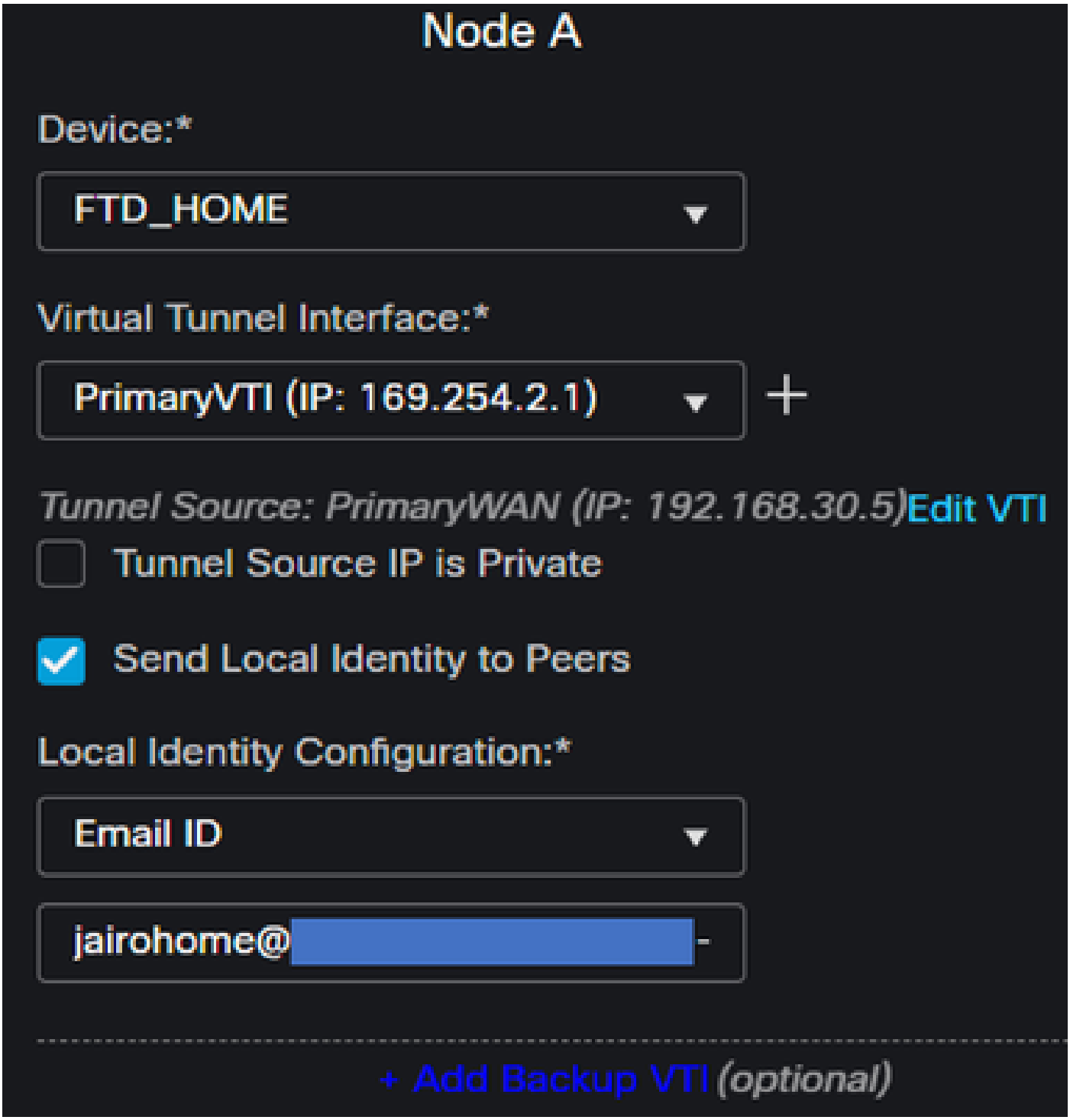
- Nombre de topología: Cree un nombre relacionado con la integración de Secure Access

- Elegir **Routed Based (VTI)**
- Elegir **Point to Point**
- IKE Version: Elija IKEv2



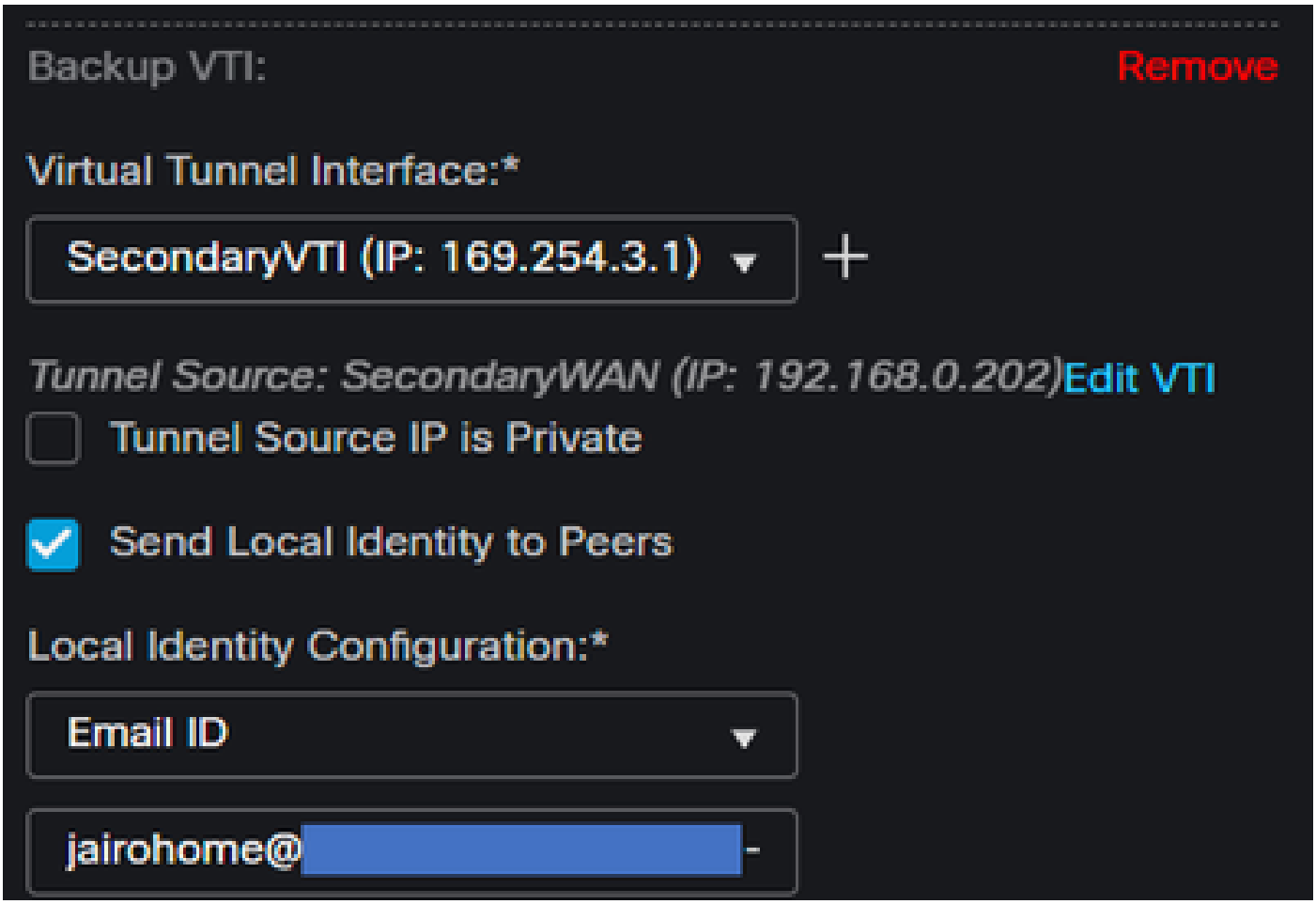
Nota: No se admite IKEv1 para la integración con Secure Access.

En la **Node A**, debe configurar los siguientes parámetros:



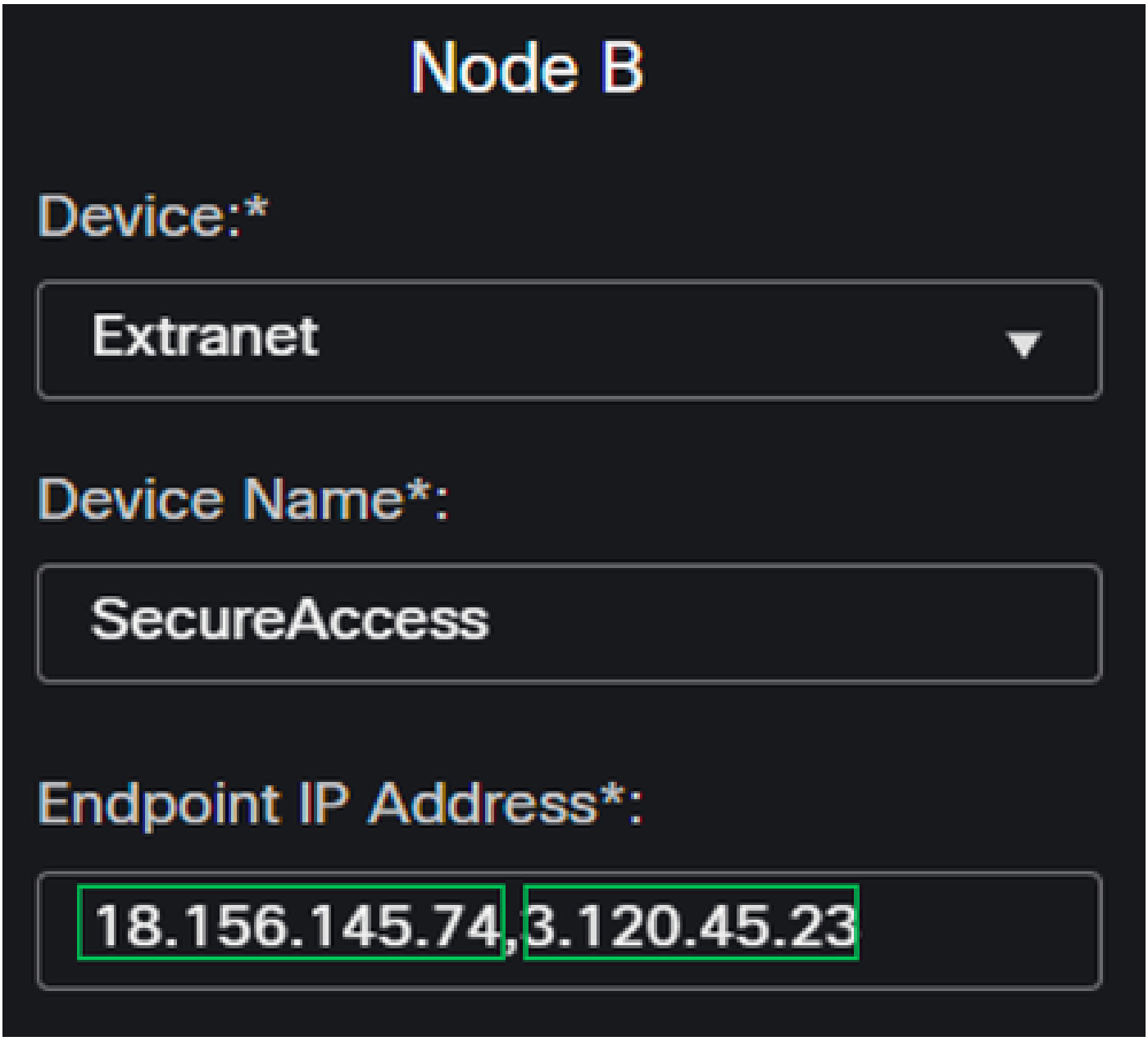
- **Device**: Elija su dispositivo FTD
- **Virtual Tunnel Interface**: Elija el VTI relacionado con el **PrimaryWAN Interface**.
- Marque la casilla de verificación de **Send Local Identity to Peers**
- Local Identity Configuration: Elija Email ID (ID de correo electrónico) y rellene la información en función de la información **Primary Tunnel ID** proporcionada en la configuración del paso Data for Tunnel Setup (Datos para la configuración del túnel)

Después de configurar la información en el **PrimaryVTI** haga clic en **+ Add Backup VTI**:



- **Virtual Tunnel Interface**: Elija el VTI relacionado con el **PrimaryWAN Interface**.
- Marque la casilla de verificación de **Send Local Identity to Peers**
- Local Identity Configuration: Elija Email ID (ID de correo electrónico) y rellene la información en función de la información **Secondary Tunnel ID** proporcionada en la configuración del paso Data for Tunnel Setup (Datos para la configuración del túnel)

En la **Node B**, debe configurar los siguientes parámetros:



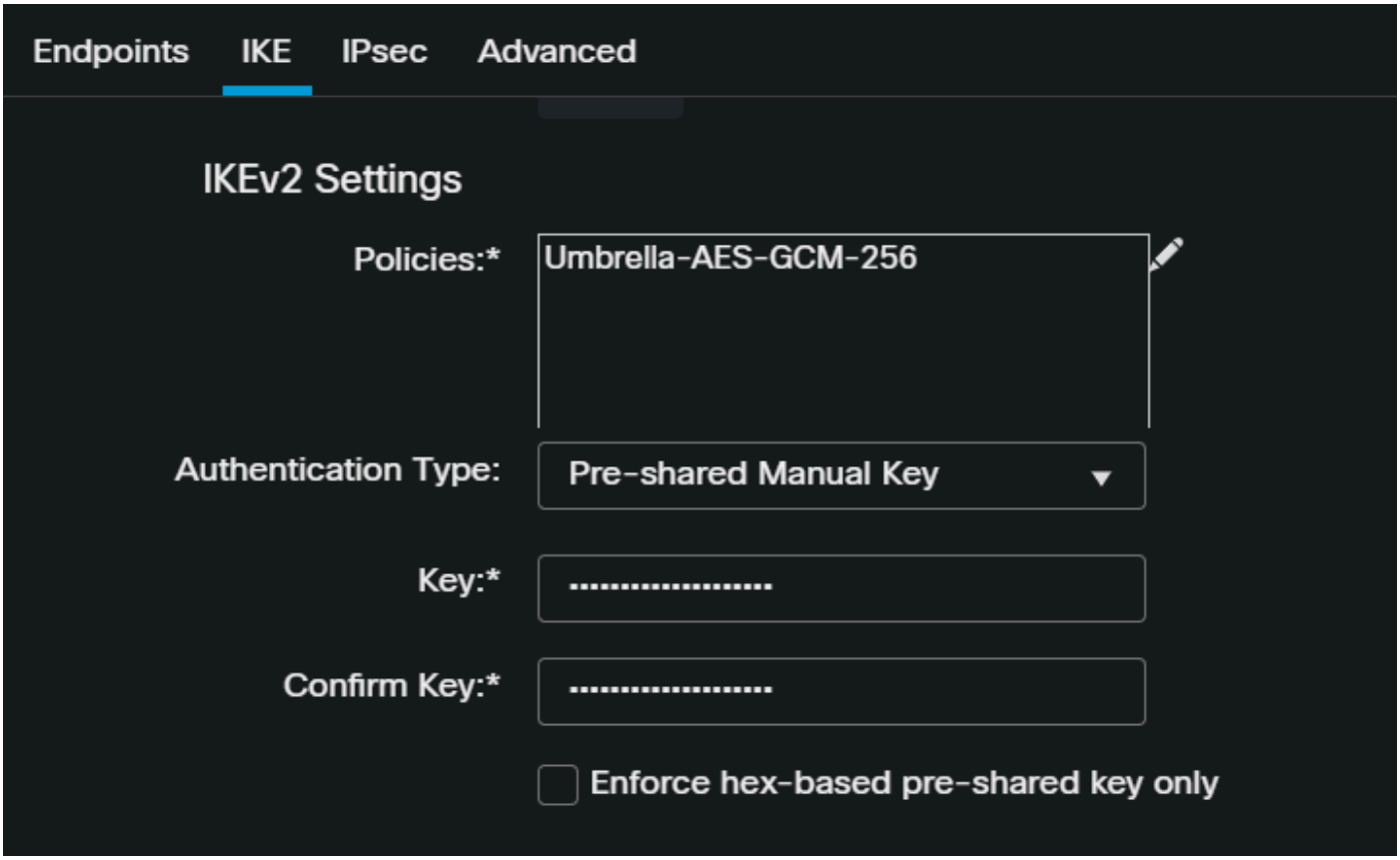
- **Device**: Extranet
- **Device Name**: Elija un nombre para reconocer el acceso seguro como destino.
- Endpoint IP Address: La configuración para primaria y secundaria debe ser Primaria **Datacenter IP,Secondary Datacenter IP**; puede encontrar esa información en el paso Data for Tunnel Setup (Datos para la configuración del túnel)

Después de esto, la configuración para **Endpoints** se ha completado y ahora puede ir al paso, Configuración IKE.

Configuración IKE

Para configurar los parámetros IKE, haga clic en **IKE**.

En **IKE**, debe configurar los siguientes parámetros:



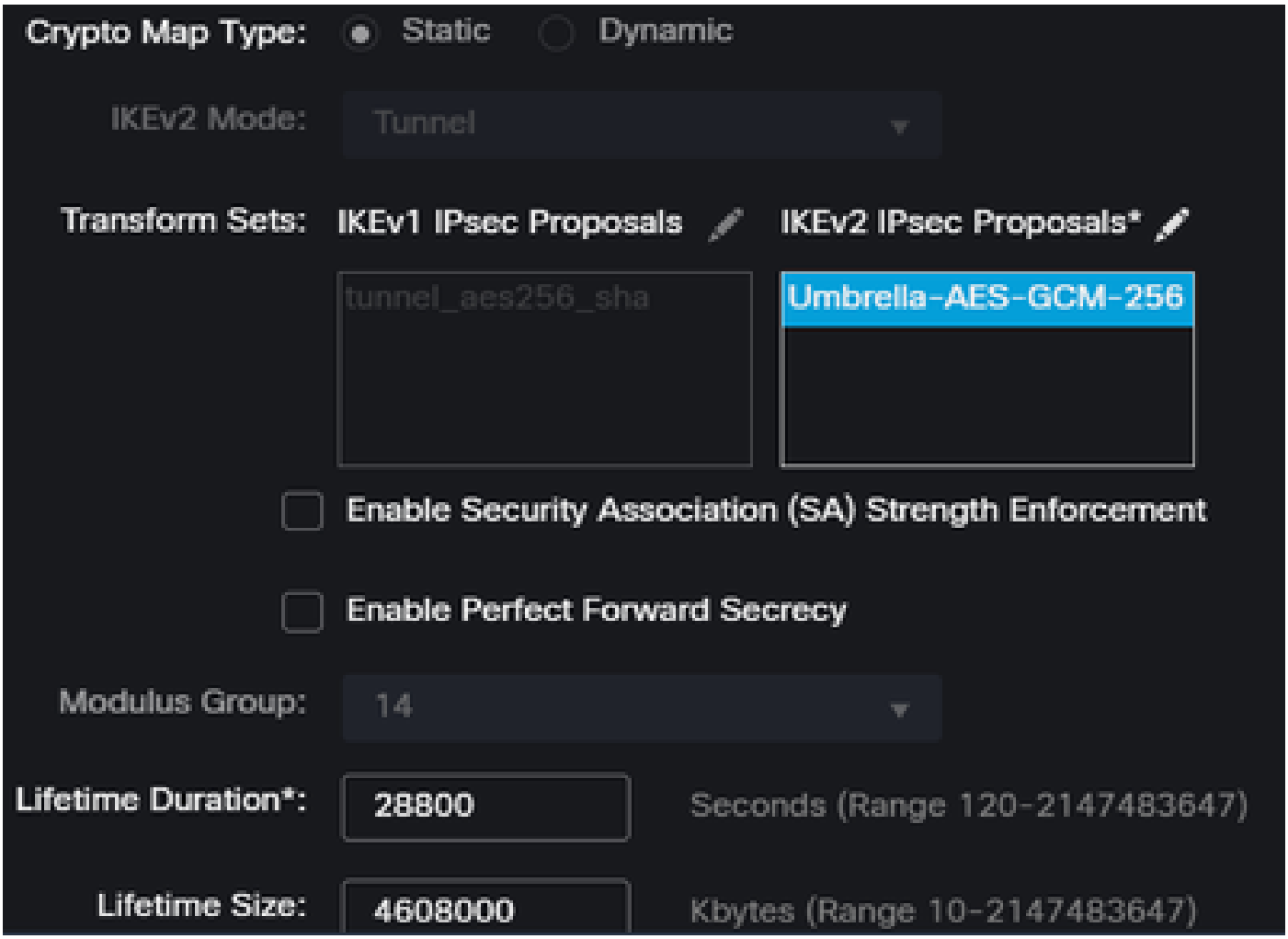
- Policies: Puede utilizar la configuración predeterminada de Umbrella **Umbrella-AES-GCM-256** o configurar parámetros diferentes en función de la Supported IKEv2 and IPSEC Parameters
- **Authentication Type**: Clave manual precompartida
- Keyy:**Confirm Key** Puede encontrar la **Passphrase** información en el paso, Datos para la Configuración del Túnel

Después de esto, su configuración para **IKE** se completa, y ahora puede ir al paso, Configuración IPSEC.

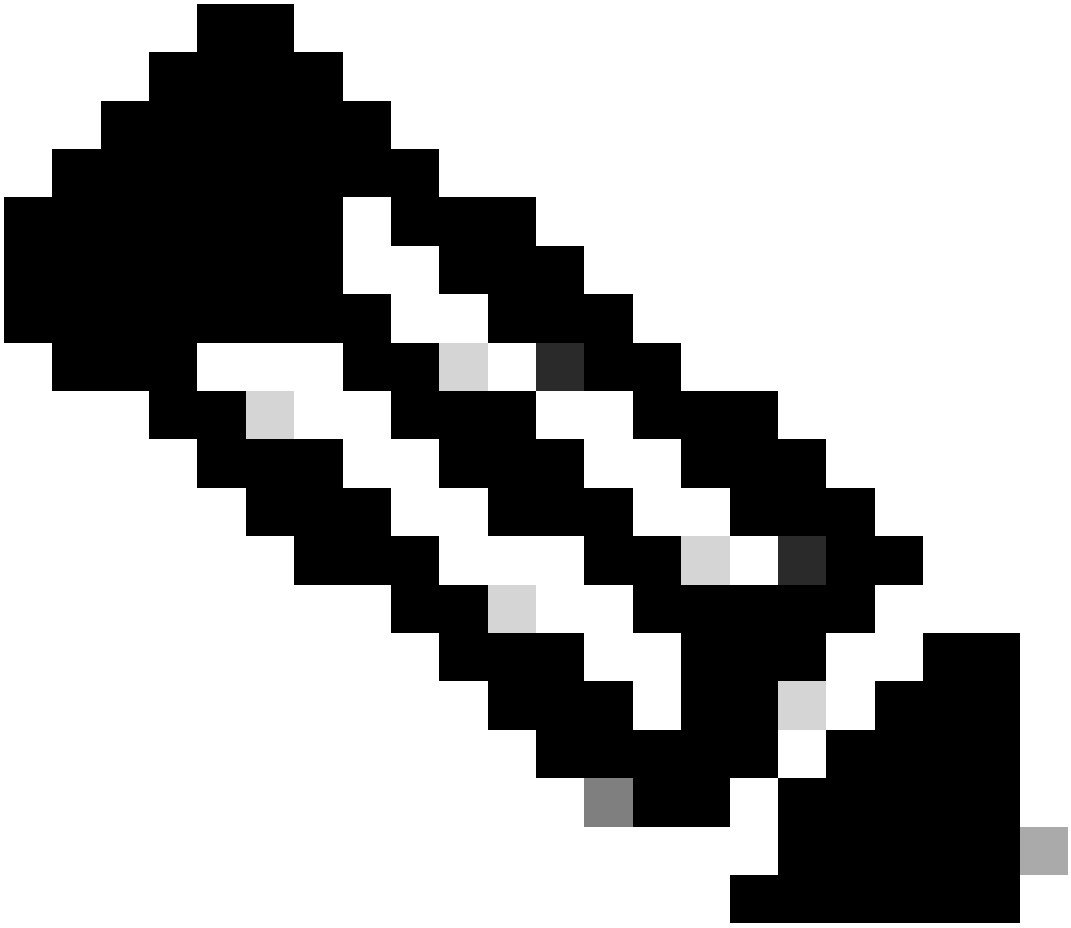
Configuración de IPSEC

Para configurar los parámetros IPSEC, haga clic en IPSEC.

En IPSEC, debe configurar los siguientes parámetros:



- Policies: Puede utilizar la configuración predeterminada de Umbrella **Umbrella-AES-GCM-256** o configurar parámetros diferentes en función de la Supported IKEv2 and IPSEC Parameters

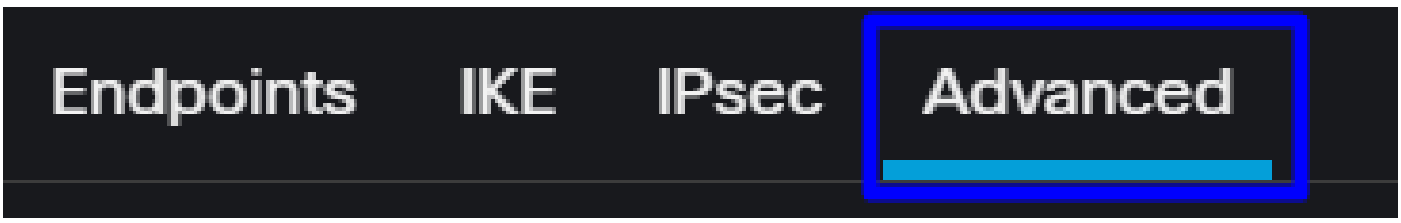


Nota: No se requiere nada más en IPSEC.

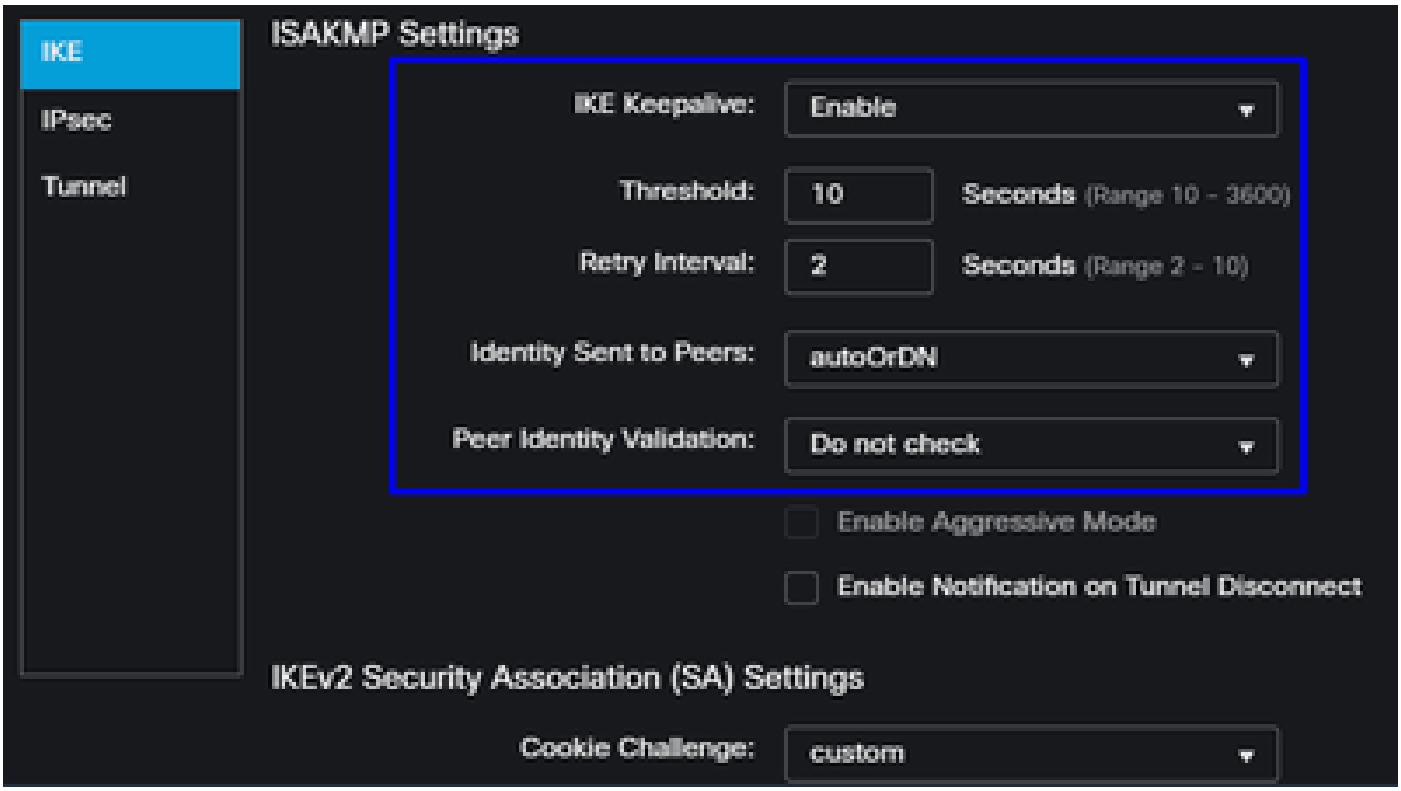
Después de esto, la configuración de **IPSEC** se ha completado y ahora puede ir al paso, Configuración avanzada.

Configuración avanzada

Para configurar los parámetros avanzados, haga clic en Advanced (Avanzado).

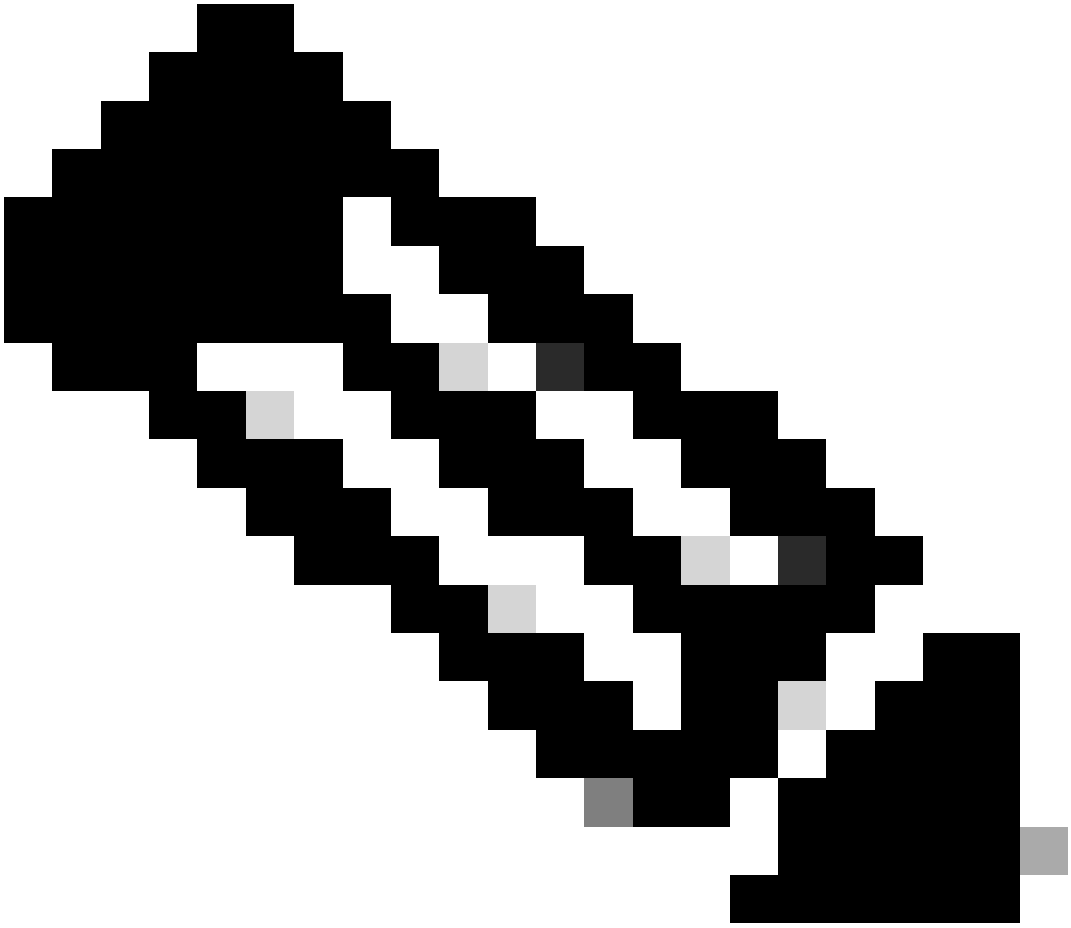


En **Advanced,** debe configurar los siguientes parámetros:

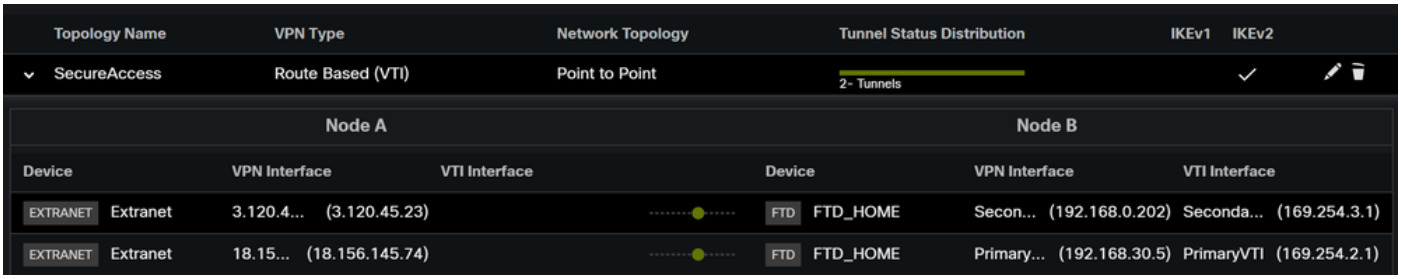


- **IKE Keepalive**: Habilitar
- **Threshold**: 10
- **Retry Interval**: 2
- **Identity Sent to Peers**: autoOrDN
- **Peer Identity Validation**: No comprobar

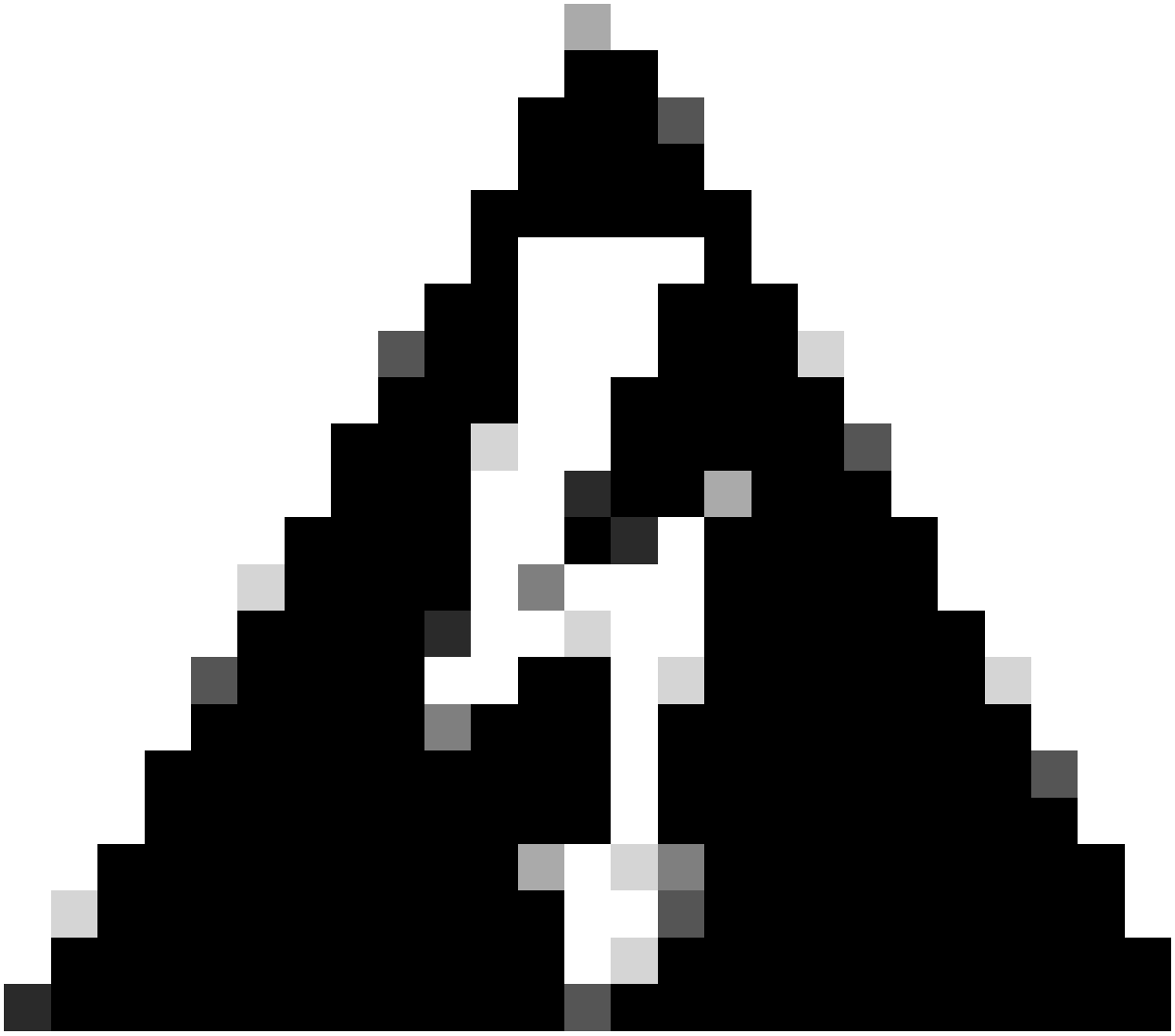
Después de eso, puede hacer clic enSavey **Deploy**.



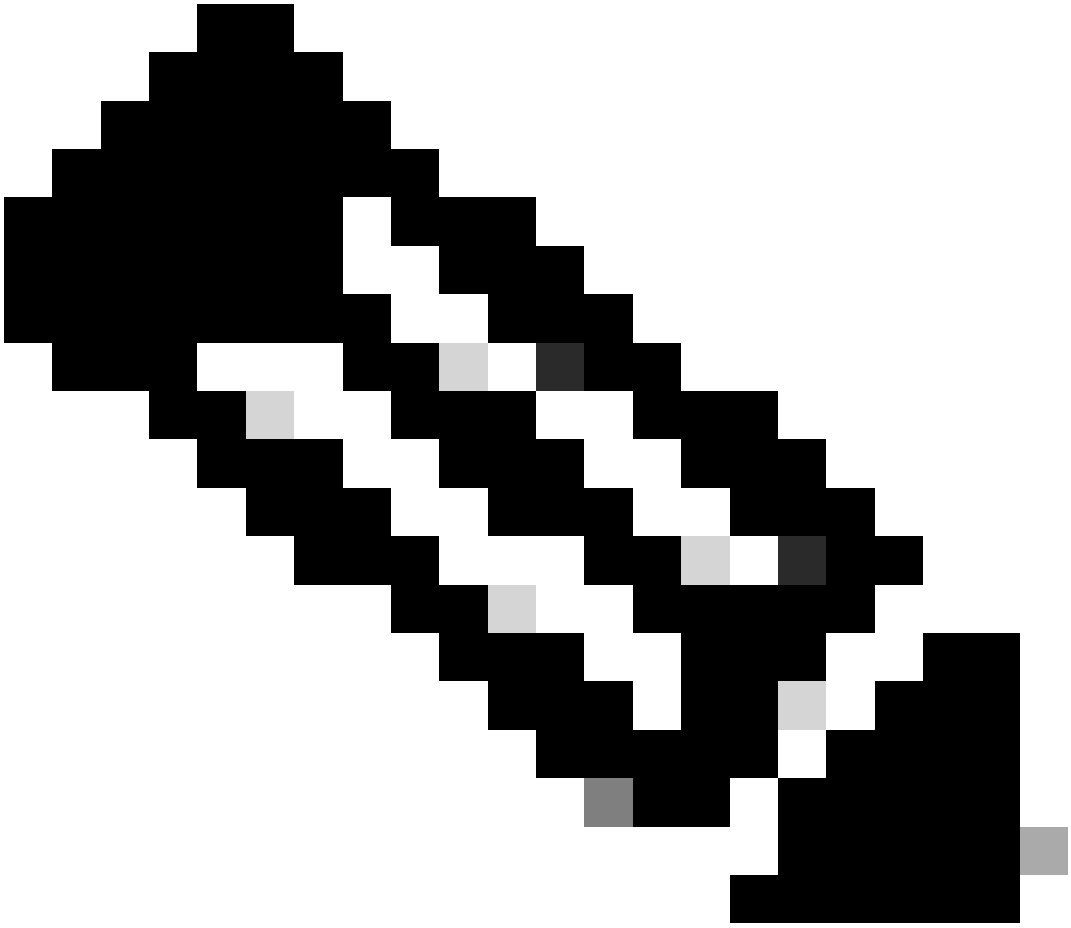
Nota: Después de unos minutos, verá la VPN establecida para ambos nodos.



Después de esto, se completa la configuración del **VPN to Secure Access in VTI Mode** y ahora puede ir al paso **Configure Policy Base Routing.**



Advertencia: El tráfico a Secure Access se reenvía solamente al túnel principal cuando ambos túneles están establecidos; si el primario se desactiva, Secure Access permite que el tráfico se reenvíe a través del túnel secundario.



Nota: La conmutación por error en el sitio de Secure Access se basa en los valores de DPD documentados en la guía del usuario para los valores de IPsec admitidos.

Escenarios de configuración de política de acceso

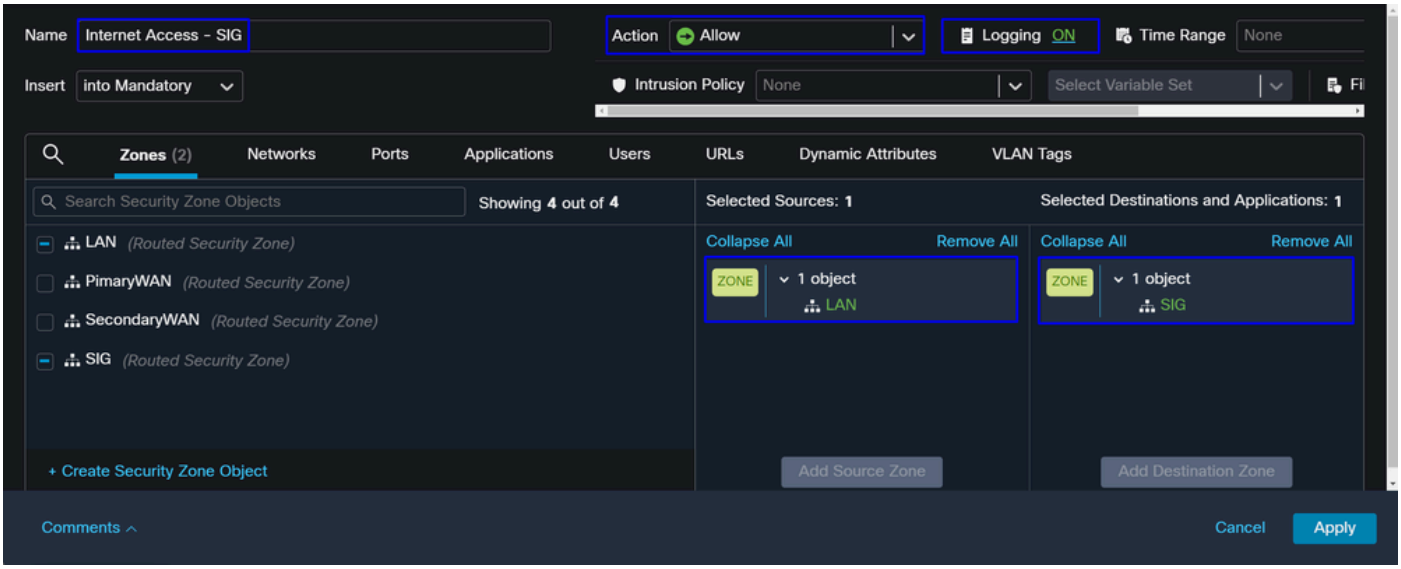
Las reglas de política de acceso definidas se basan en:

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)

Interfaz	Zone (Zona)
VTI primaria	SIG
VTIsecundaria	SIG
LAN	LAN

Escenario de acceso a Internet

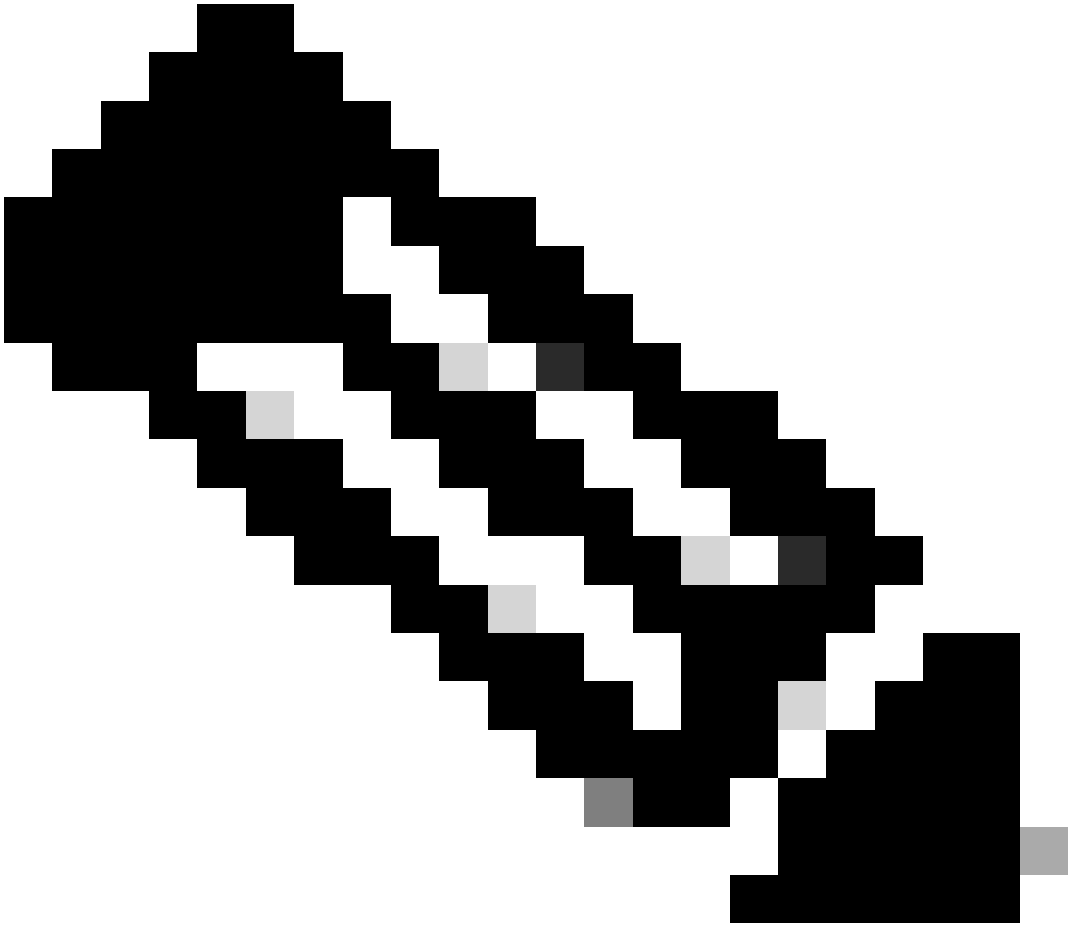
Para proporcionar acceso a Internet a todos los recursos que configure en Policy Base Routing, debe configurar algunas reglas de acceso y también algunas políticas en el acceso seguro, así que permítame explicarle cómo lograrlo en esta situación:



Esta regla proporciona acceso a Internet LAN y, en este caso, Internet está SIG.

Escenario de RA-VPN

Para proporcionar acceso desde los usuarios de RA-VPN, debe configurarlo en función del rango que asignó en el conjunto RA-VPN.



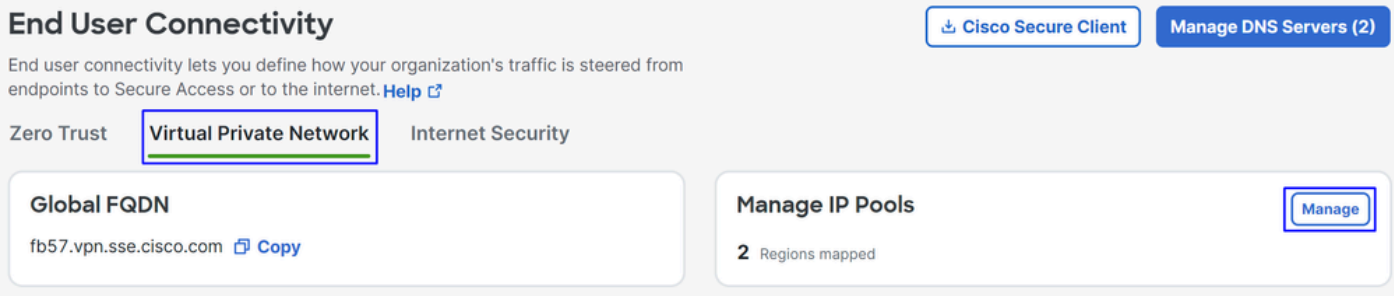
Nota: Para configurar su política RA-VPNaaS, puede ir a través de Administrar redes privadas virtuales

---

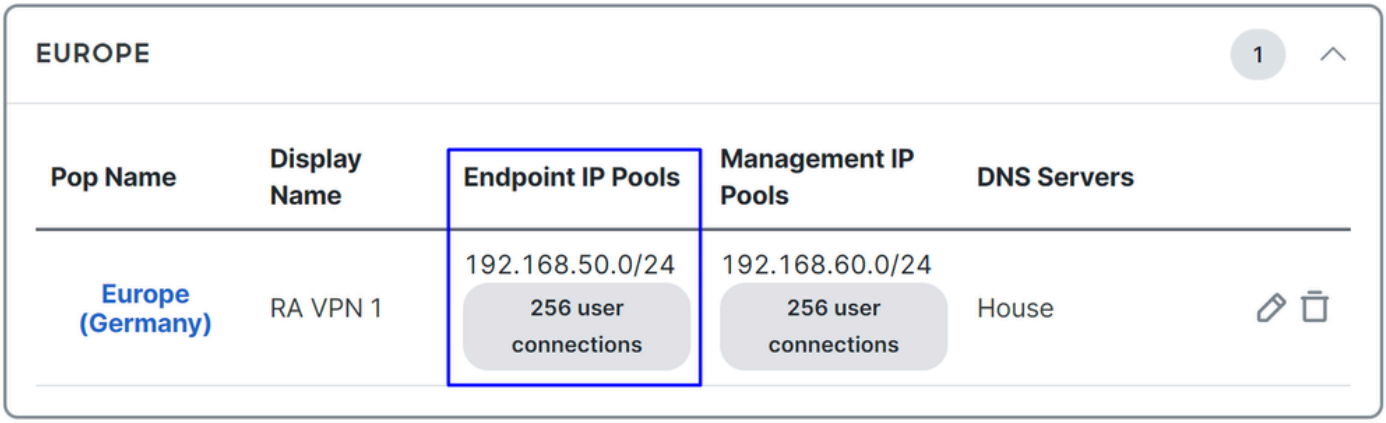
¿Cómo verifica el pool IP de su VPNaaS?

Desplácese hasta el panel de acceso seguro

- Haga clic en Connect > End User Connectivity
- Haga clic en **Virtual Private Network**
- En **Manage IP Pools**, haga clic en Manage



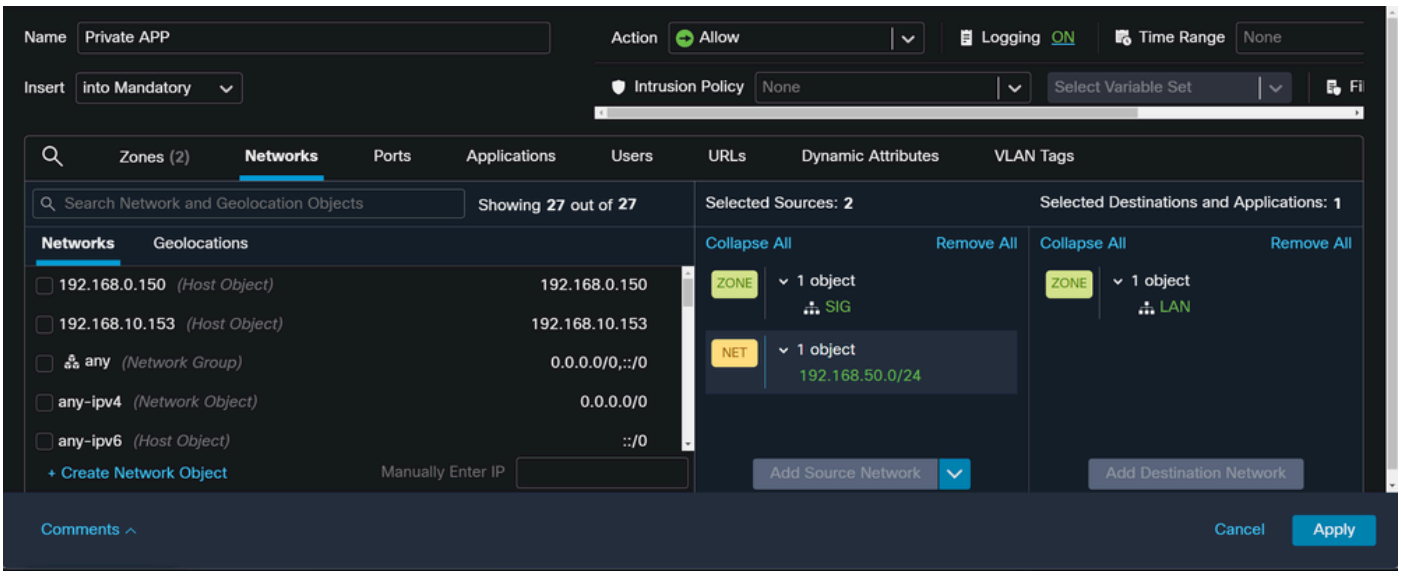
- Ves tu piscina debajo **Endpoint IP Pools**



- Debe permitir este rango bajo SIG, pero también debe agregarlo bajo la ACL que configure en su PBR.

Configuración de reglas de acceso

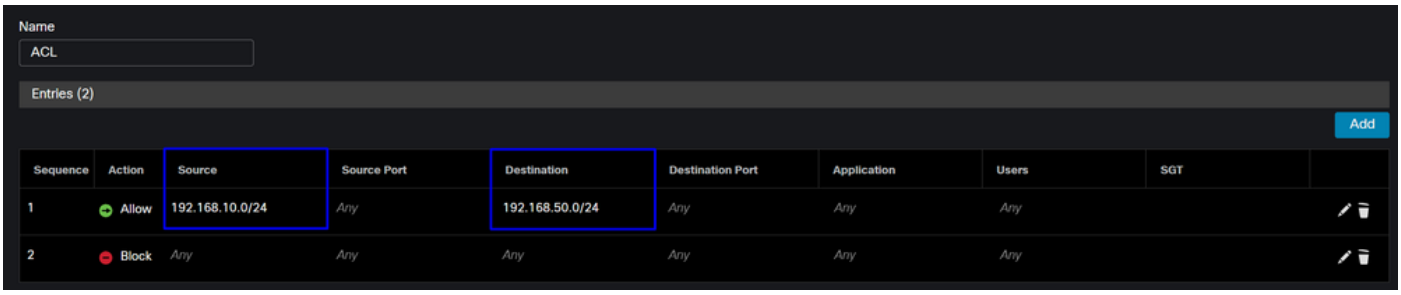
Si sólo va a configurar Secure Access para utilizarlo con las funciones para acceder a los recursos de las aplicaciones privadas, la regla de acceso tendrá el siguiente aspecto:



Esa regla permite el tráfico del conjunto RA-VPN 192.168.50.0/24 a su LAN; puede especificar más si es necesario.

Configuración de ACL

Para permitir el tráfico de ruteo de SIG a su LAN, debe agregarlo bajo la ACL para que funcione bajo el PBR.

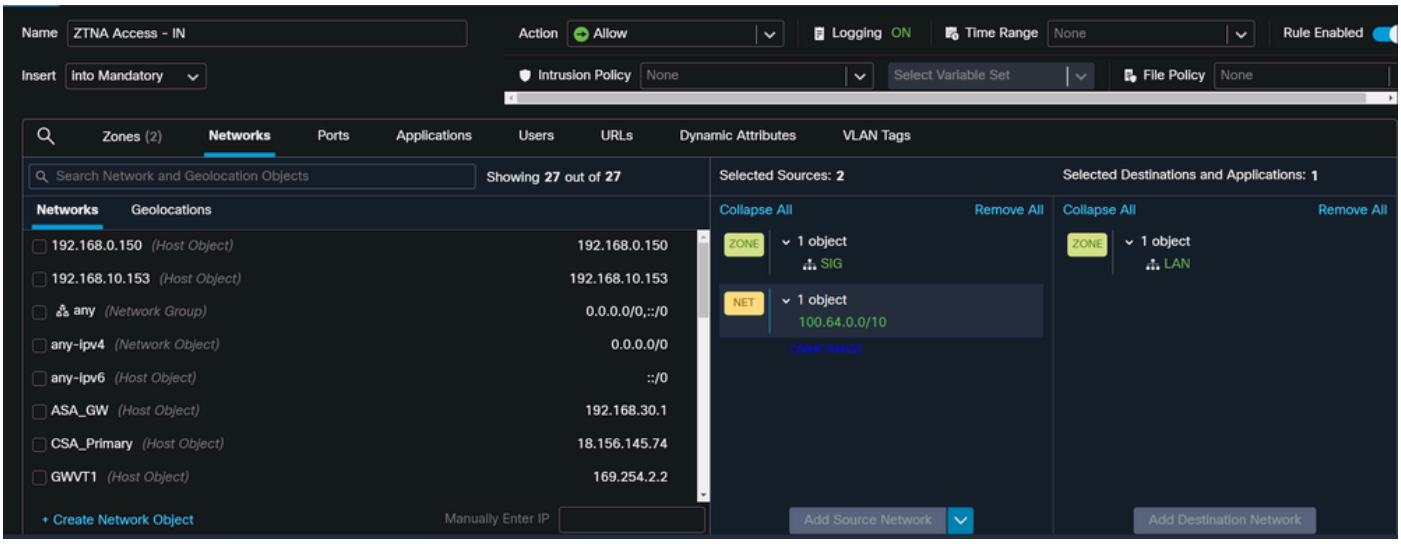


CLAP-BAP ZTNA Escenario

Debe configurar su red basada en el rango de CGNAT 100.64.0.0/10 para proporcionar acceso a su red desde los usuarios ZTA Client Base o Browser Base ZTA.

Configuración de reglas de acceso

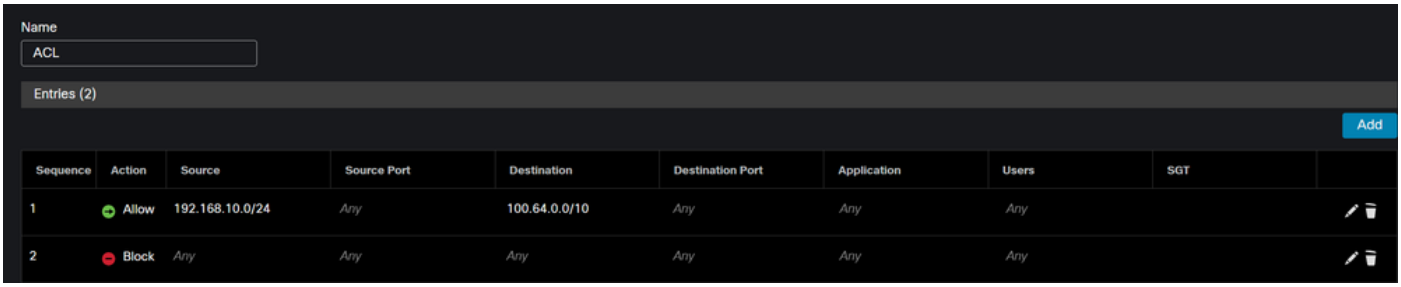
Si sólo va a configurar Secure Access para utilizarlo con las funciones para acceder a los recursos de las aplicaciones privadas, la regla de acceso tendrá el siguiente aspecto:



Esa regla permite el tráfico desde el rango CGNAT de ZTNA 100.64.0.0/10 a su LAN.

Configuración de ACL

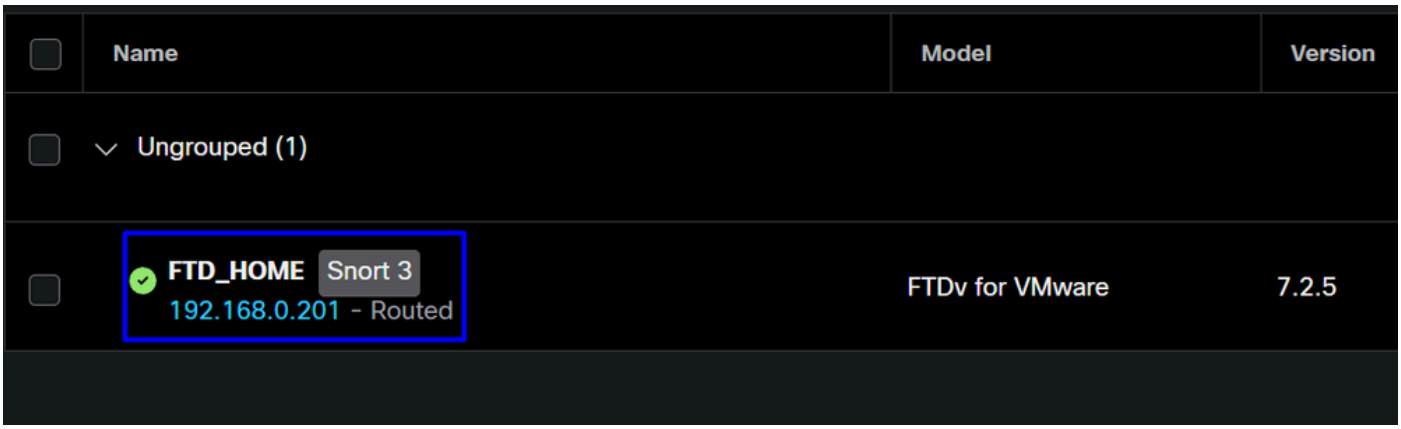
Para permitir el tráfico de ruteo desde SIG usando CGNAT a su LAN, debe agregarlo bajo la ACL para que funcione bajo el PBR.



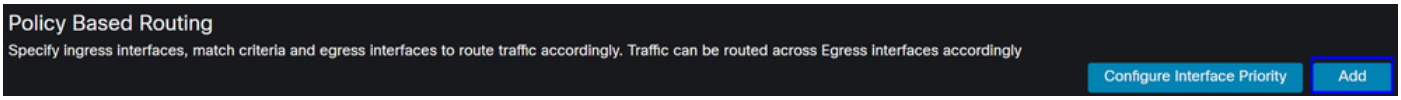
Configurar routing de base de políticas

Para proporcionar acceso a los recursos internos e Internet a través de Secure Access, debe crear rutas a través de Policy Base Routing (PBR) que faciliten el enrutamiento del tráfico desde el origen al destino.

- Vaya a **Devices > Device Management**
- Elija el dispositivo FTD en el que crea la ruta

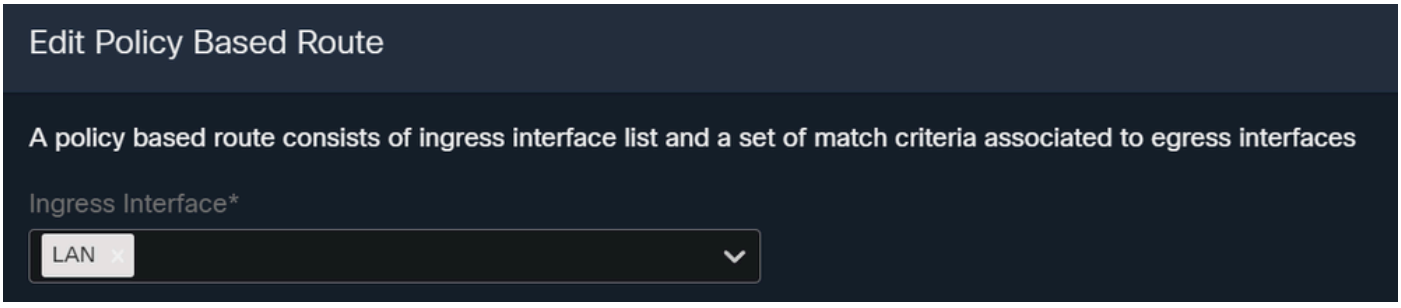


- Haga clic en **Routing**
- Elegir Policy Base Routing
- Haga clic en Add



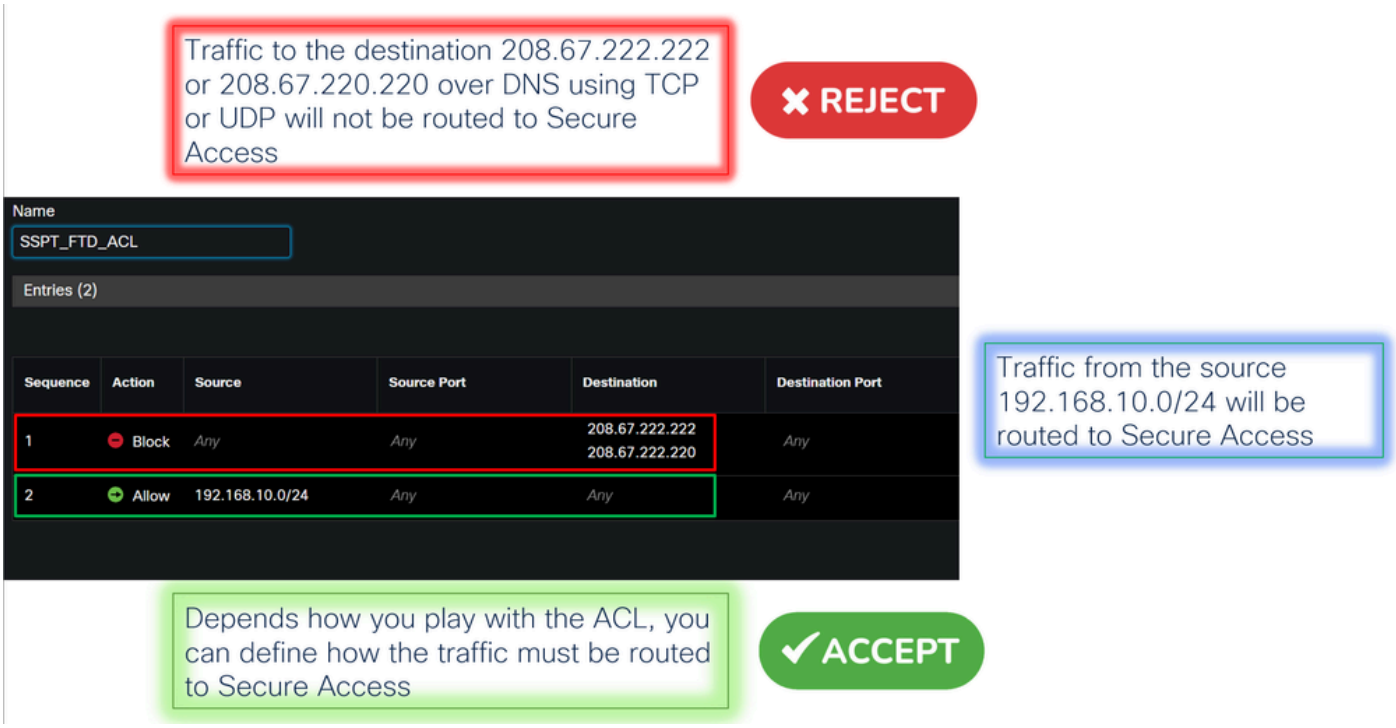
En este escenario, usted selecciona todas las interfaces que utiliza como origen para rutear el tráfico a Secure Access o para proporcionar autenticación de usuario a Secure Access usando RA-VPN o acceso ZTA basado en cliente o en navegador a los recursos internos de la Red:

- En Interfaz de entrada, seleccione todas las interfaces que envían tráfico a través de Secure Access:



- En Criterios de Coincidencia e Interfaz de Salida, defina los siguientes parámetros después de hacer clic enAdd:

- **Match ACL**: Para esta ACL, debe configurar todo lo que enruta a Secure Access:

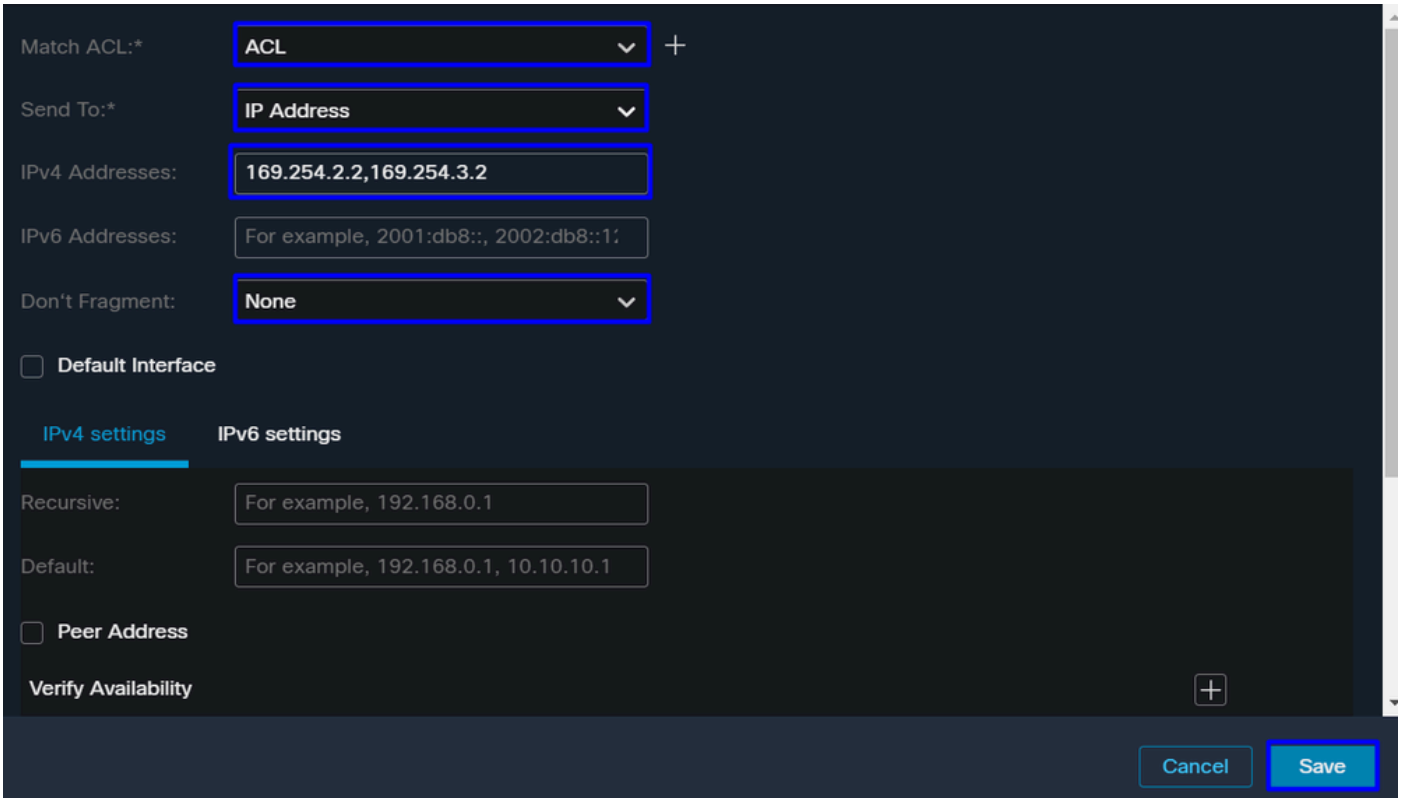


- **Send To**: Elegir dirección IP
- **IPv4 Addresses**: Debe utilizar la siguiente IP bajo la máscara 30 configurada en ambos VTI; puede verificar que en el paso, VTI Interface Config

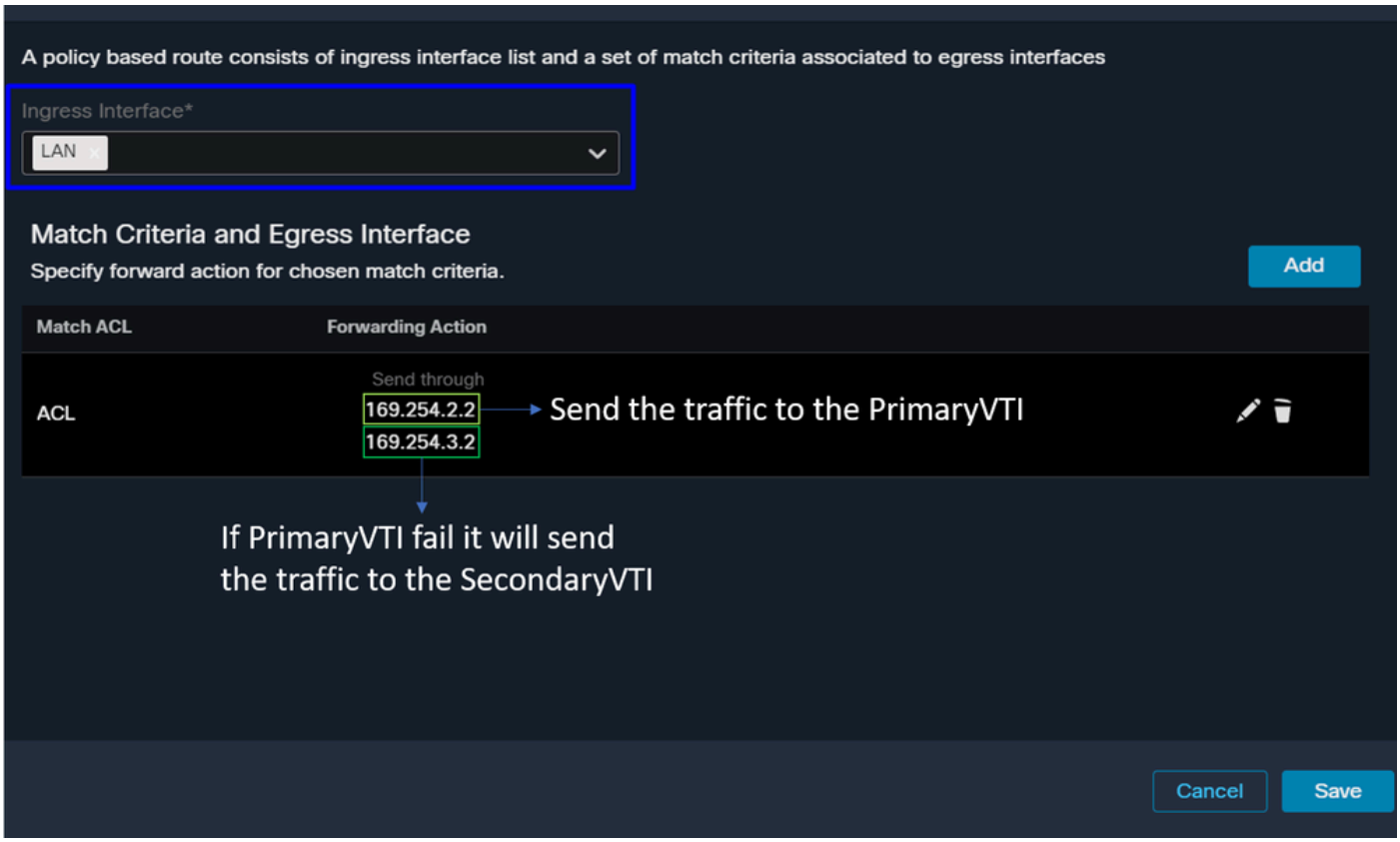
Interfaz	IP	GW
VTI primaria	169.254.2.1/30	169.254.2.2
VTIsecundaria	169.254.3.1/30	169.254.3.2

Después de configurarlo de esta manera, obtendrá el siguiente resultado y podrá continuar

haciendo clic en Save:



Después de eso, necesita volver a Save hacerlo, y lo tiene configurado de la siguiente manera:



Después de eso, puede implementar y verá el tráfico de las máquinas configuradas en la ACL que rutea el tráfico a Secure Access:

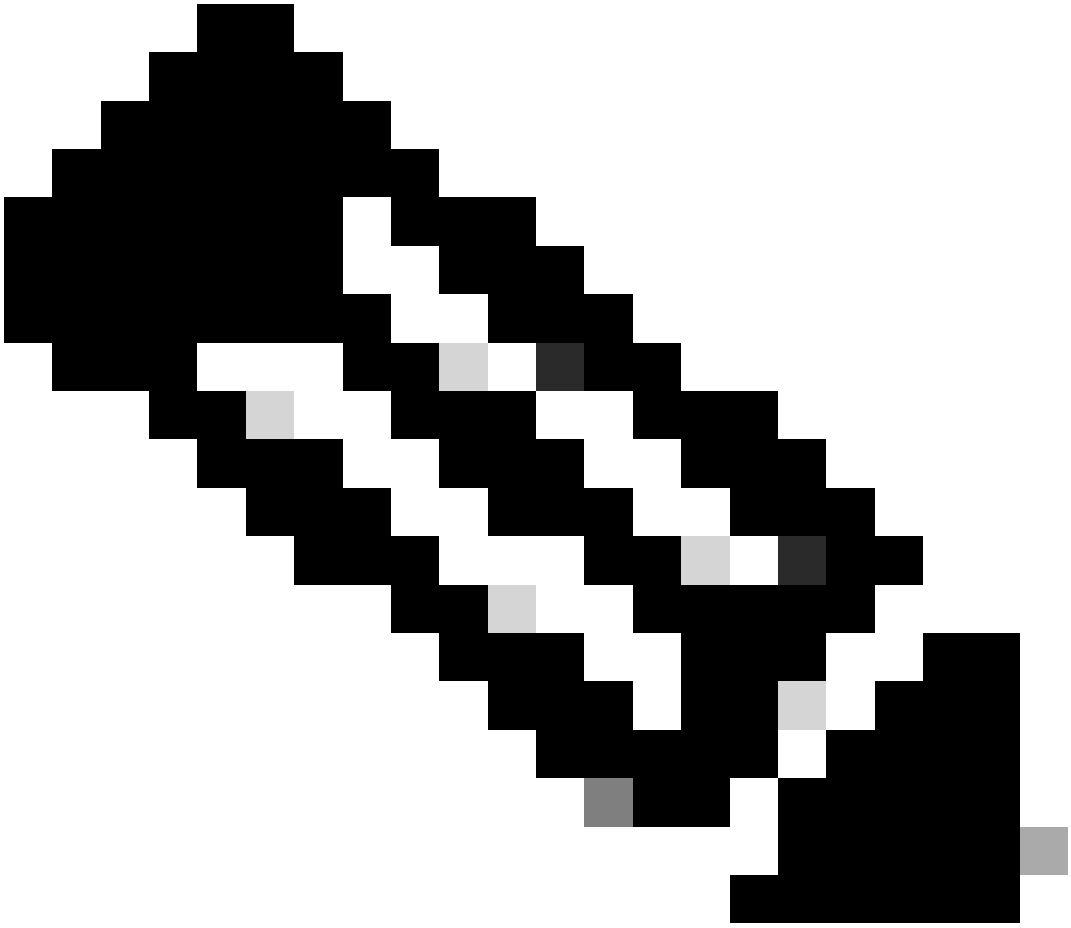
A partir del **Conexion Events** en el CSP:

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

Desde el **Activity Search** en Acceso seguro:

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	

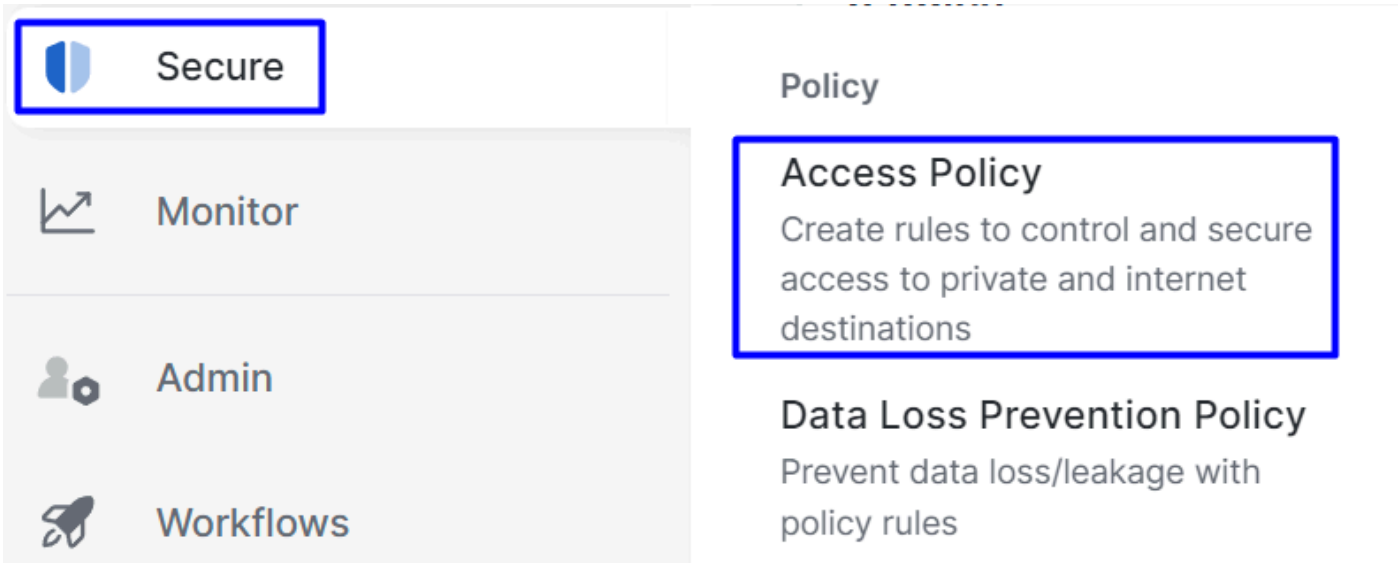


Nota: De forma predeterminada, la política de acceso seguro permite el tráfico a Internet. Para proporcionar acceso a aplicaciones privadas, debe crear recursos privados y agregarlos a la directiva de acceso para el acceso a recursos privados.

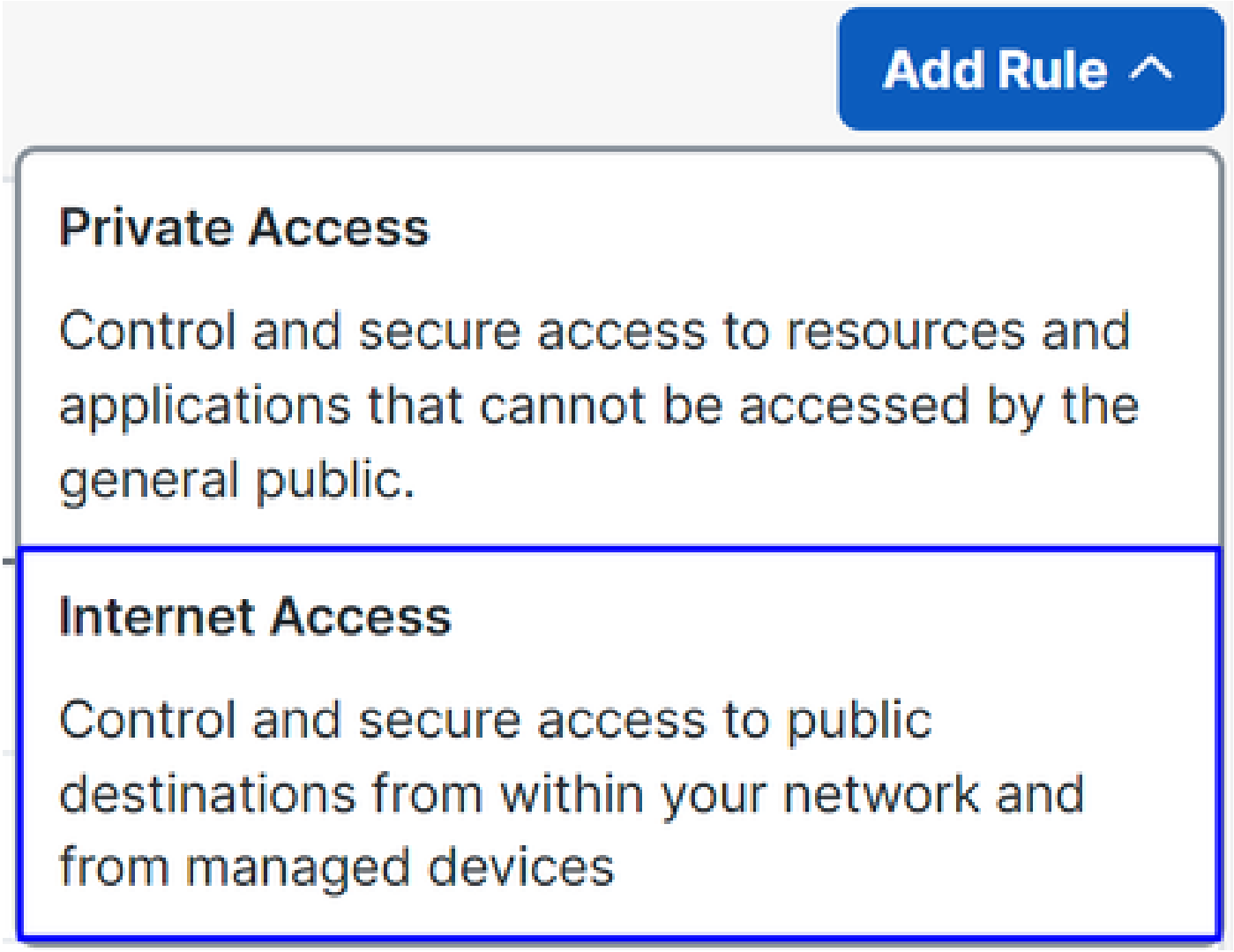
Configurar la directiva de acceso a Internet en el acceso seguro

Para configurar el acceso para el acceso a Internet, debe crear la política en el panel de acceso seguro:

- Haga clic en **Secure > Access Policy**



- Haga clic en Add Rule > Internet Access

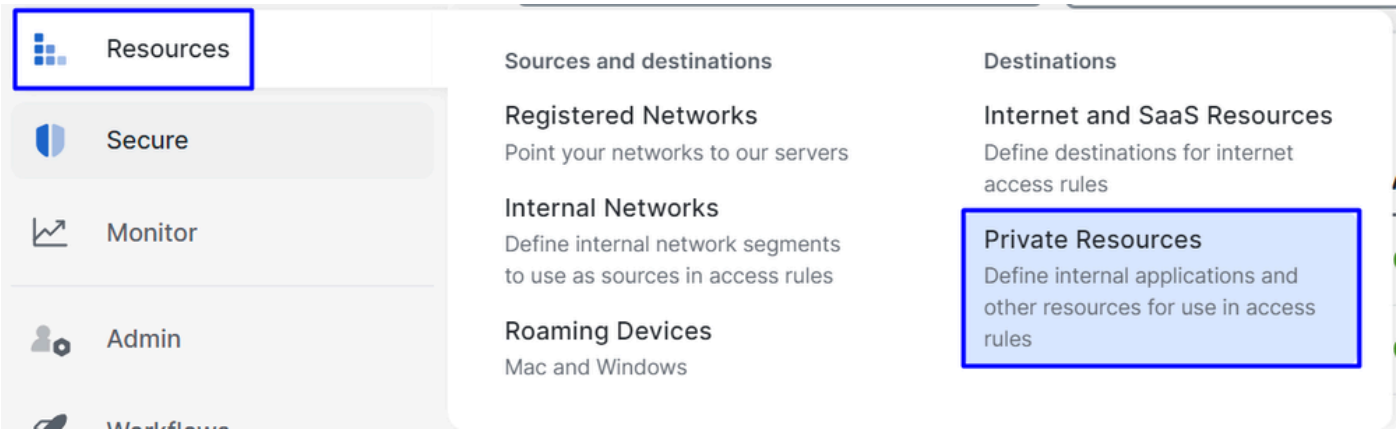


Allí, puede especificar el origen como el túnel, y hacia el destino, puede elegir cualquiera, dependiendo de lo que desee configurar en la política. Consulte la guía del usuario de Secure Access.

Configuración del Acceso a Recursos Privados para ZTNA y RA-VPN

Para configurar el acceso para los recursos privados, primero debe crear los recursos en el Panel de acceso seguro:

Haga clic en **Resources** > **Private Resources**



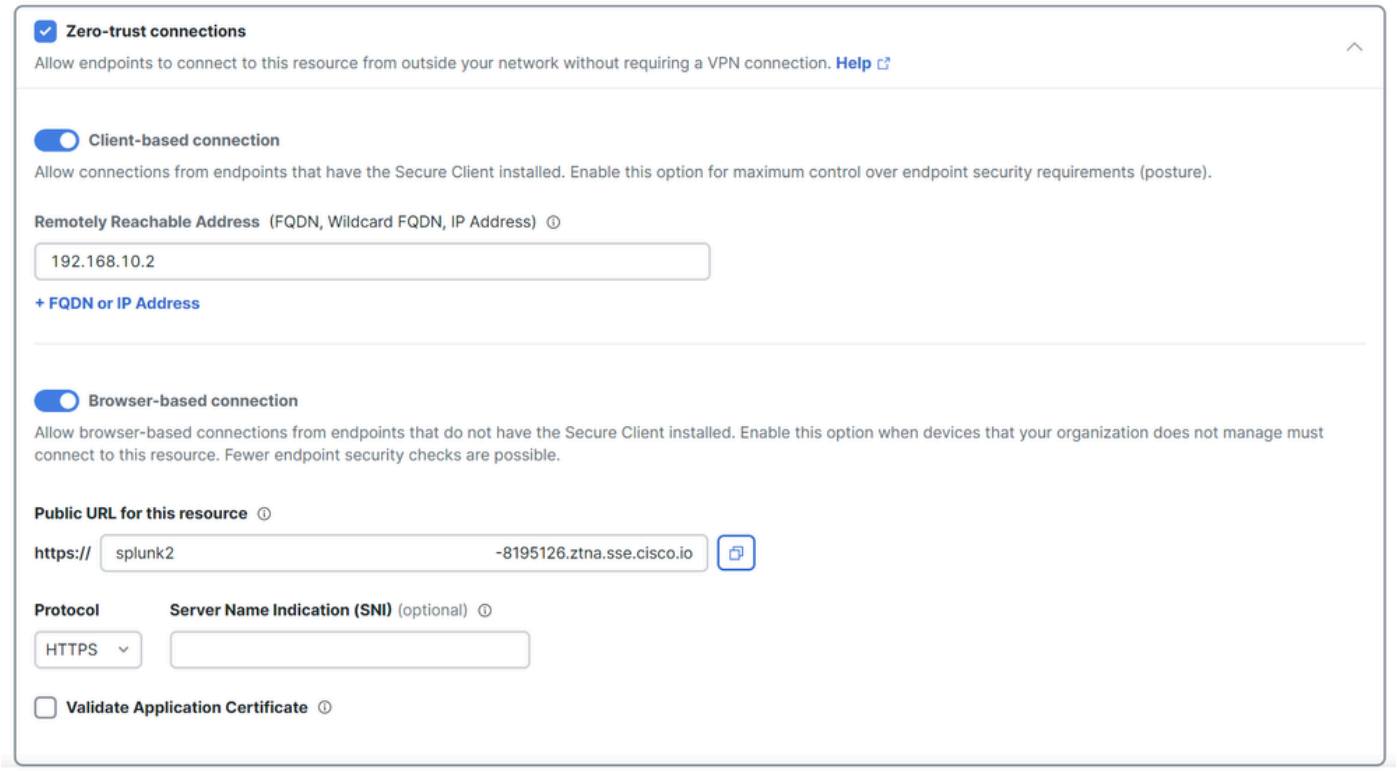
- Haga clic en **ADD**

En la sección de configuración encontrará las siguientes secciones para configurar:
General, Communication with Secure Access Cloud and Endpoint Connection Methods.

General

- Private Resource Name : Cree un nombre para el recurso al que proporciona acceso a través de Acceso seguro a la red

Métodos de conexión de terminales



- **Zero Trust Connections**: Marque la casilla.
- **Client-based connection**: Si lo habilita, puede utilizar el Secure Client - Zero Trust Module para habilitar el acceso a través del modo basado en cliente.
- **Remote Reachable Address (FQDN, Wildcard FQDN, IP Address)** : Configure la IP o FQDN de los recursos; si configura el FQDN, debe agregar el DNS para resolver el nombre.
- **Browser-based connection**: si lo activa, puede acceder a sus recursos a través del navegador (añada recursos solo con comunicación HTTP o HTTPS)
- **Public URL for this resource**: Configure la URL pública que utiliza a través del navegador; Secure Access protege este recurso.
- **Protocol**: Seleccione el protocolo (HTTP o HTTPS)

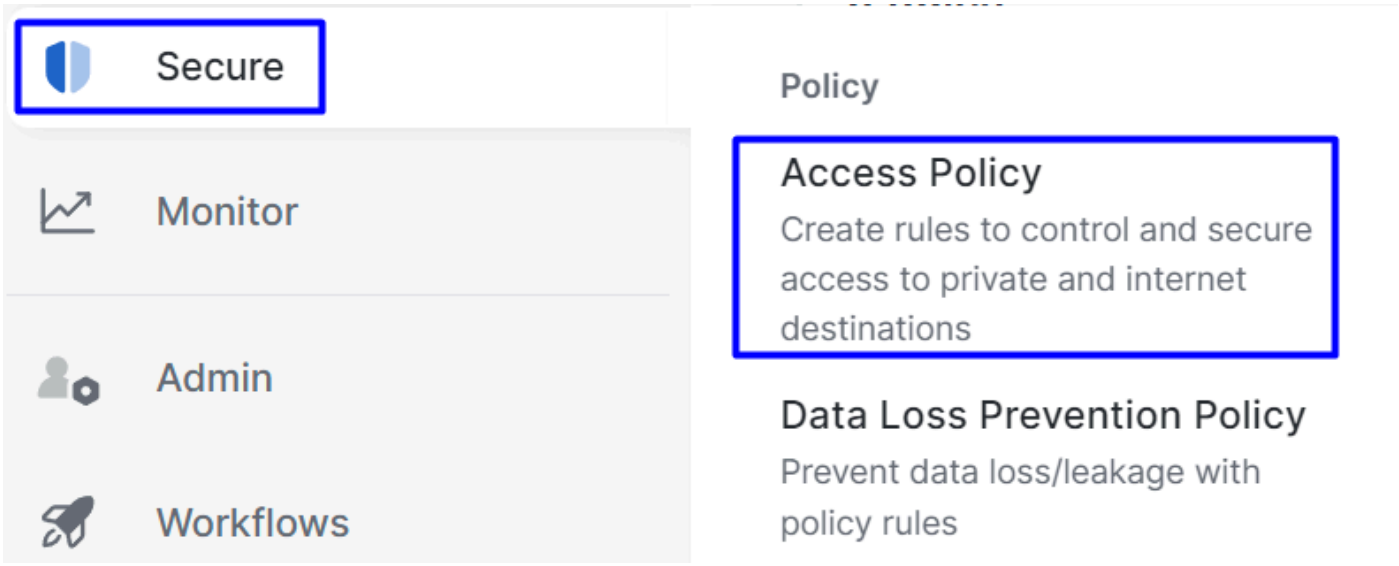
VPN Connection: Marque la casilla de verificación para habilitar el acceso mediante RA-VPNaaS.

A continuación, haga clic en **Save** y podrá agregar el recurso a la **Access Policy**.

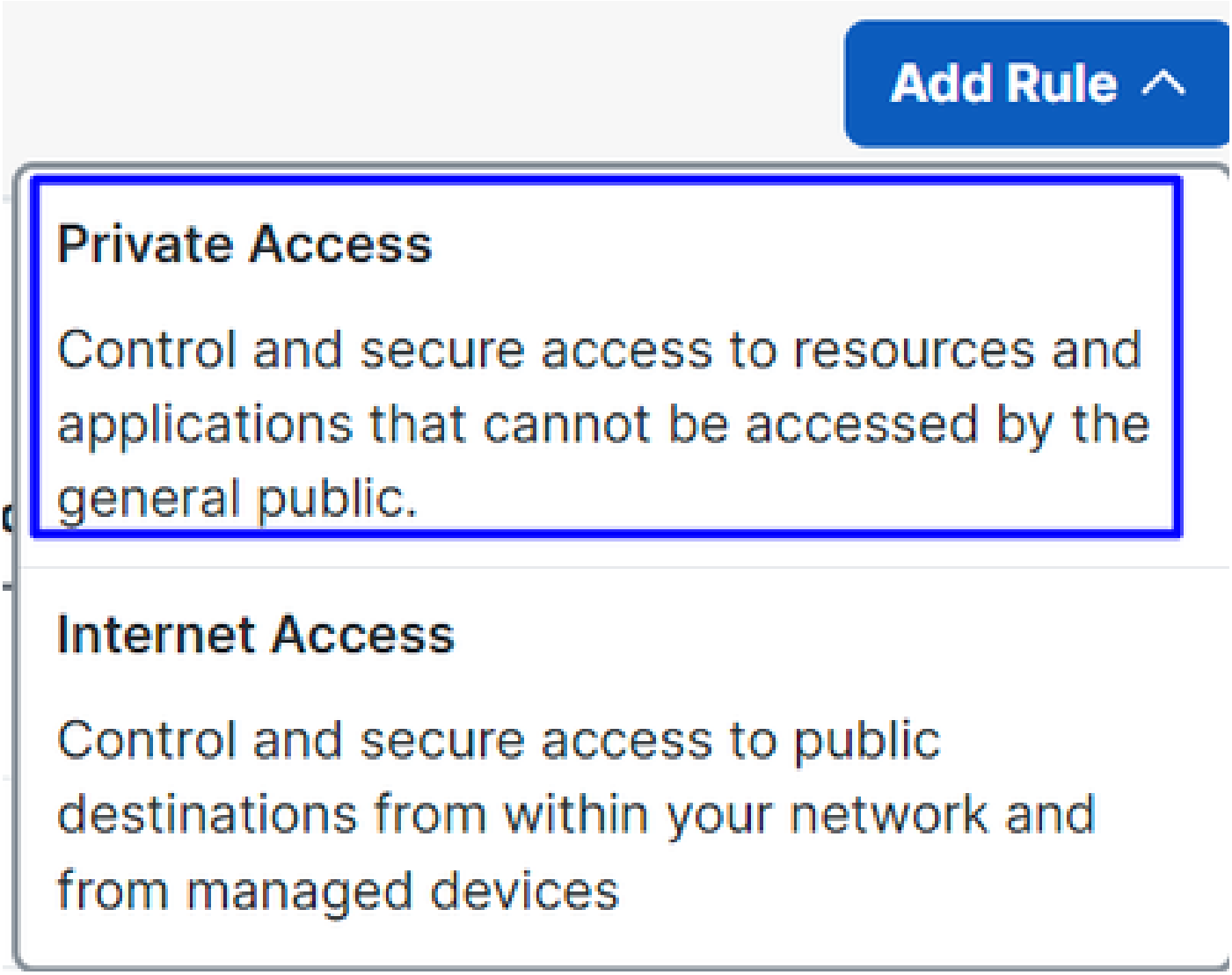
Configuración de la política de acceso

Al crear el recurso, debe asignarlo a una de las directivas de acceso seguro:

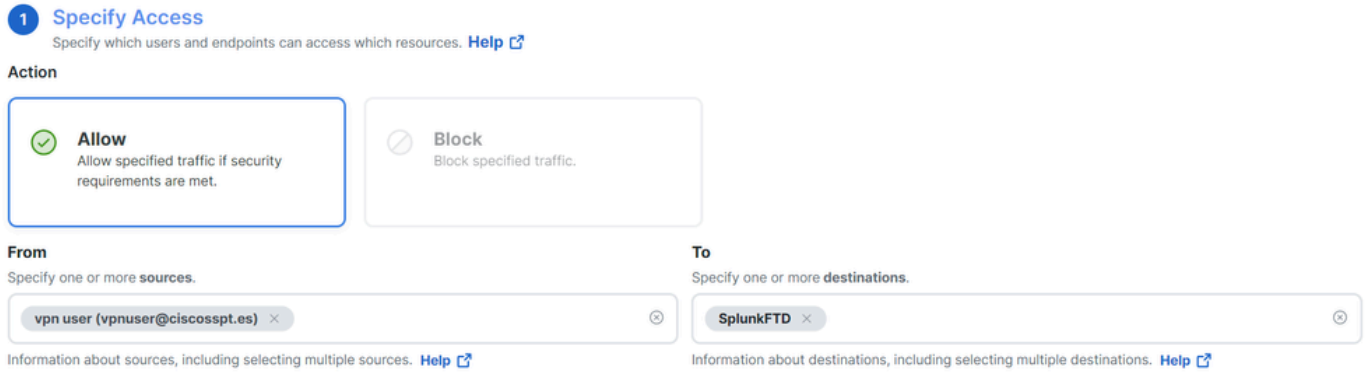
- Haga clic en **Secure** > **Access Policy**



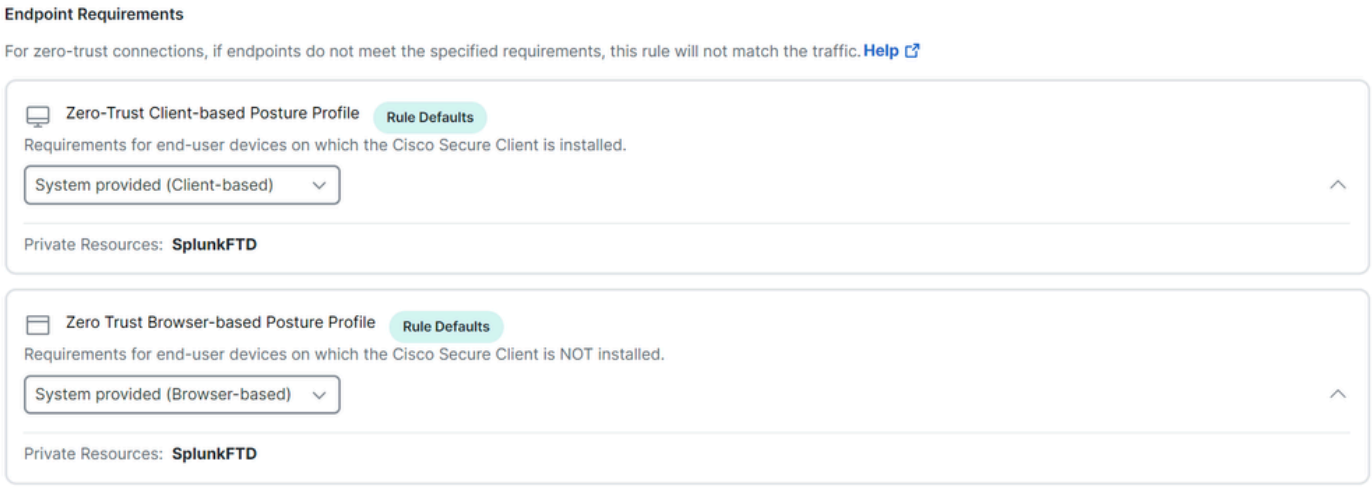
- Haga clic en **Add** > **Private Resource**



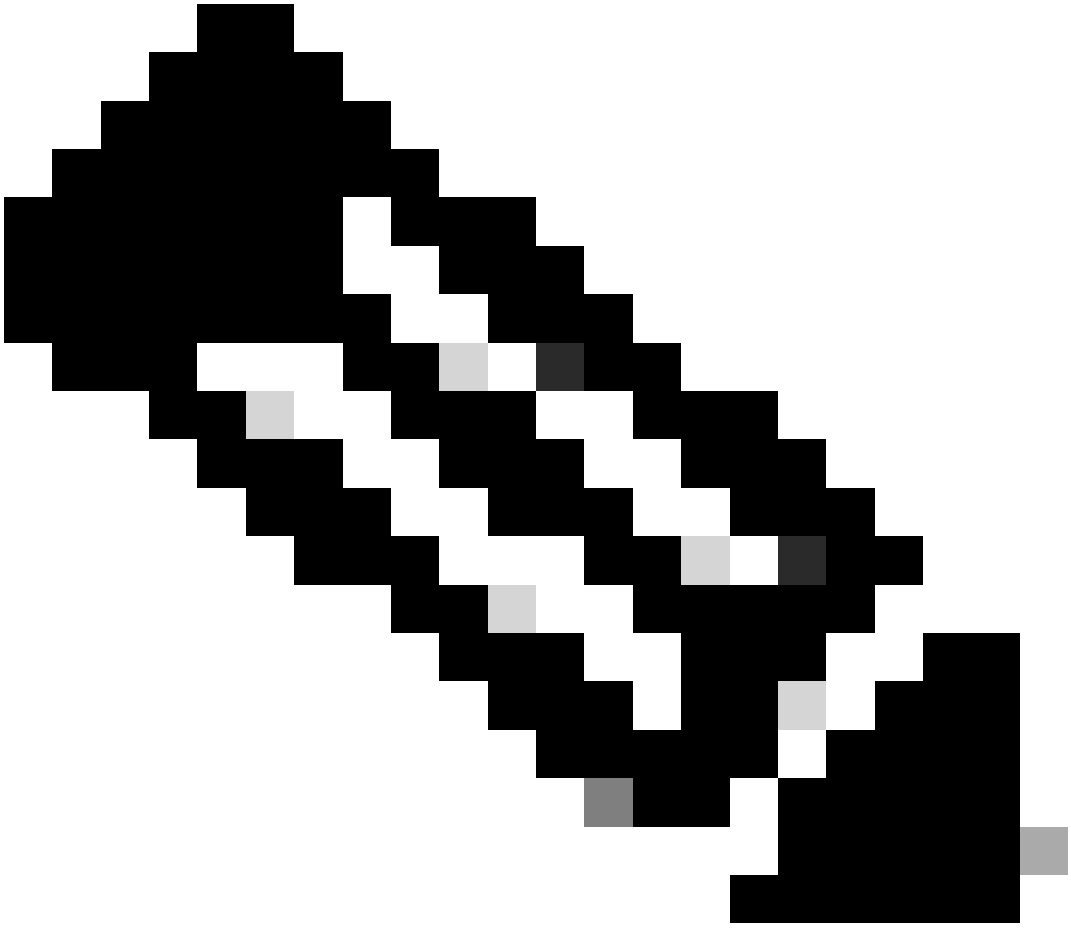
Para esta regla de acceso privado, debe configurar los valores predeterminados para proporcionar acceso al recurso. Para obtener más información sobre las configuraciones de directivas, consulte la guía del usuario.



- **Action** : Seleccione Permitir para proporcionar acceso al recurso.
- **From** : Especifique el usuario que se puede utilizar para iniciar sesión en el recurso.
- **To** : Elija el recurso al que desea acceder a través de Secure Access.



- **Zero-Trust Client-based Posture Profile**: Elija el perfil predeterminado para el acceso base de clientes
- **Zero-Trust Browser-based Posture Profile**: elija el acceso base del explorador de perfiles predeterminado



Nota: Para obtener más información sobre la política de estado, consulte la guía del usuario para obtener acceso seguro.

Después de eso, haga clic en **Next** y**Save** y en su configuración, y puede intentar acceder a sus recursos a través de RA-VPN y Client Base ZTNA o Browser Base ZTNA.

Troubleshoot

Para solucionar problemas basados en la comunicación entre Secure Firewall y Secure Access, puede comprobar si se han establecido la fase 1 (IKEv2) y la fase 2 (IPSEC) entre los dispositivos sin ningún problema.

Verificación de la fase 1 (IKEv2)

Para verificar la fase 1, debe ejecutar el siguiente comando en la CLI de su FTD:

```
show crypto isakmp sa
```

En este caso, el resultado deseado se establece en dos **IKEv2 SAs** direcciones IP de Data Center de acceso seguro y el estado deseado es **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
```

Verificación de la fase 2 (IPSEC)

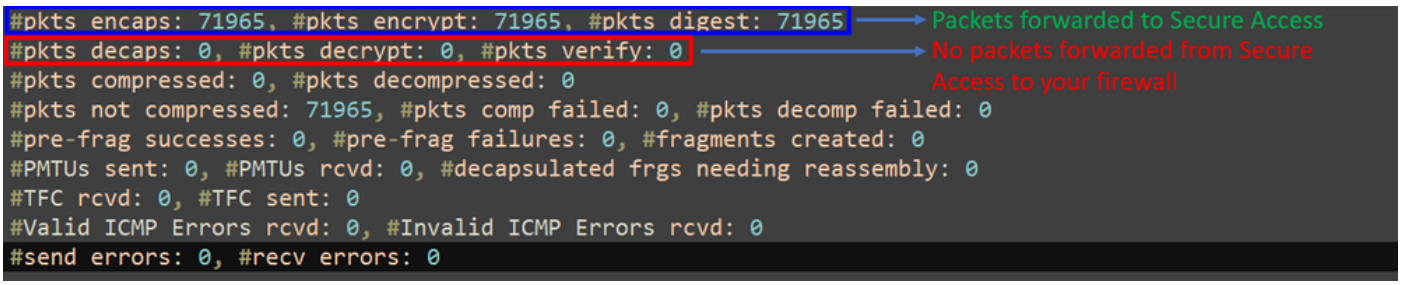
Para verificar la fase 2, debe ejecutar el siguiente comando en la CLI de su FTD:

```
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
```

En la última salida, puede ver ambos túneles establecidos; lo que no se desea es la siguiente salida bajo el paquete encaps y decaps.

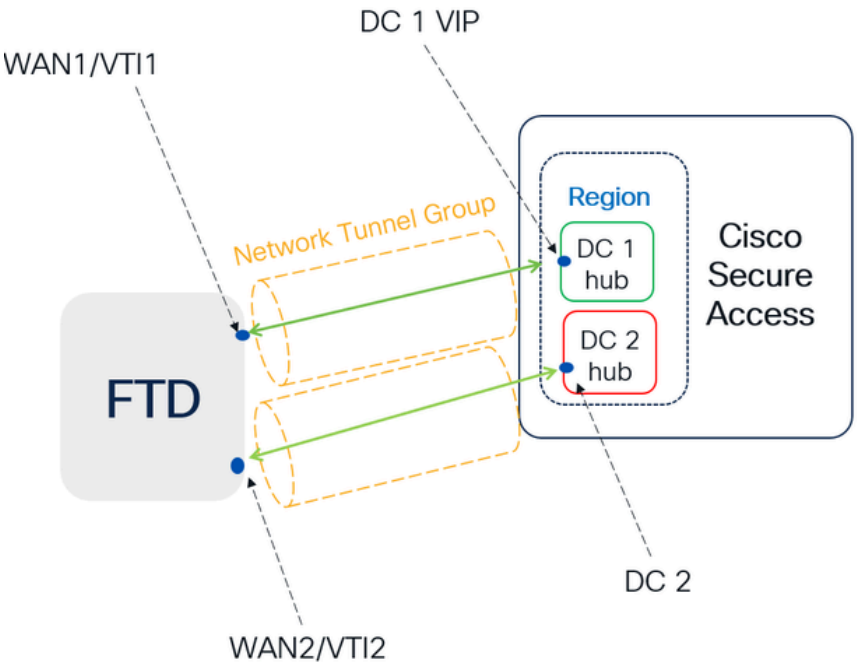


Si tiene este escenario, abra un caso con el TAC.

Función de alta disponibilidad

La función de los túneles con Secure Access que se comunican con el Data Center en la nube es activa/pasiva, lo que significa que solo la puerta del DC 1 estará abierta para recibir tráfico; la puerta DC 2 está cerrada hasta que el túnel número 1 se desactiva.

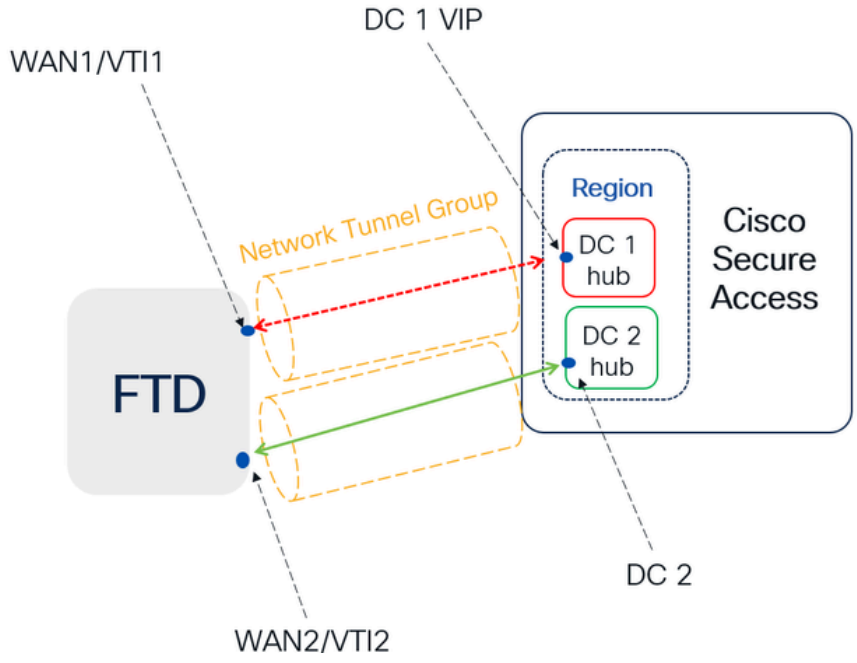
Normal Behavior



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

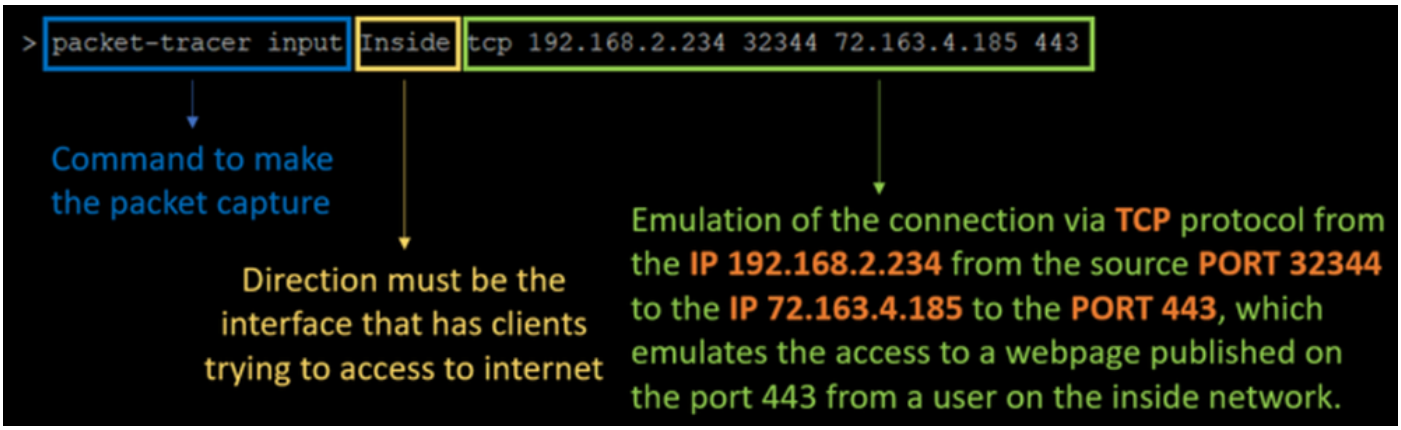
- DC2 is Active when DC1or WAN1 peer is Down
- High availability is implemented to address failures in the WAN1 channel on the Firewall, ensuring operational continuity in the region and mitigating potential issues in DC1

Verificación del enrutamiento del tráfico para proteger el acceso

En este ejemplo, utilizamos el origen como la máquina en la red de firewall:

- Fuente: 192.168.10.40
- Destino: 146.112.255.40 (IP de supervisión de acceso seguro)

Ejemplo:



Comando:

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

Salida:

```
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
```

Aquí, muchas cosas pueden darnos contexto sobre la comunicación y saber si todo está correctamente bajo la configuración PBR para rutear el tráfico correctamente a Secure Access:

```
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 fase 2 indica que el tráfico se está reenviando a la **PrimaryVTI** interfaz, lo cual es correcto porque, según las configuraciones en este escenario, el tráfico de Internet debe reenviarse a Secure Access a través de 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:
```

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).