Configuración del acceso seguro con Secure Firewall Threat Defence para el acceso privado con routing basado en políticas

Contenido

Introducción

Este documento describe cómo configurar Secure Access con FTD vía IPsec para Secure Private Access con Policy Based Routing.

Prerequisites

Requirements

- Conocimientos sobre Cisco Secure Access
- Panel/arrendatario de Cisco Secure Access
- Conocimiento de Secure Firewall Threat Defence y Firewall Management Center
- conocimiento de IPsec
- Conocimiento del routing basado en políticas

Componentes Utilizados

- Secure Firewall con código 7.7.10
- Centro de gestión de firewalls en la nube. La configuración también se aplica al FMC virtual típico
- Panel de Cisco Secure Access

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

Los túneles de red de Secure Access se pueden utilizar para dos fines principales: Acceso seguro a Internet y acceso privado seguro.

En el caso del acceso privado seguro, las organizaciones pueden aprovechar el acceso de confianza cero (ZTA) o VPN como servicio (VPNaaS) para conectar a los usuarios con recursos privados, como aplicaciones internas o Data Centers. Los túneles IPsec desempeñan un papel clave en esta arquitectura, ya que cifran de forma segura el tráfico de red entre los usuarios y los recursos privados, lo que garantiza que los datos confidenciales permanezcan protegidos mientras atraviesan redes no fiables. Al integrar túneles IPsec con ZTA o VPNaaS, las organizaciones pueden proporcionar un acceso seguro y sin problemas a los recursos internos, a la vez que mantienen unos sólidos controles de seguridad y visibilidad.

Este documento describe cómo configurar Secure Access con Secure Firewall Threat Defence (FTD) a través de IPsec para Secure Private Access.
Además, esta guía proporciona los pasos para configurar el ruteo basado en políticas.

Aunque este documento trata sobre la configuración de túneles IPsec para el acceso privado seguro, la configuración de Zero Trust Access (ZTA) o VPN as a Service (VPNaaS) para acceder a aplicaciones privadas está fuera del alcance de esta guía.

Configurar

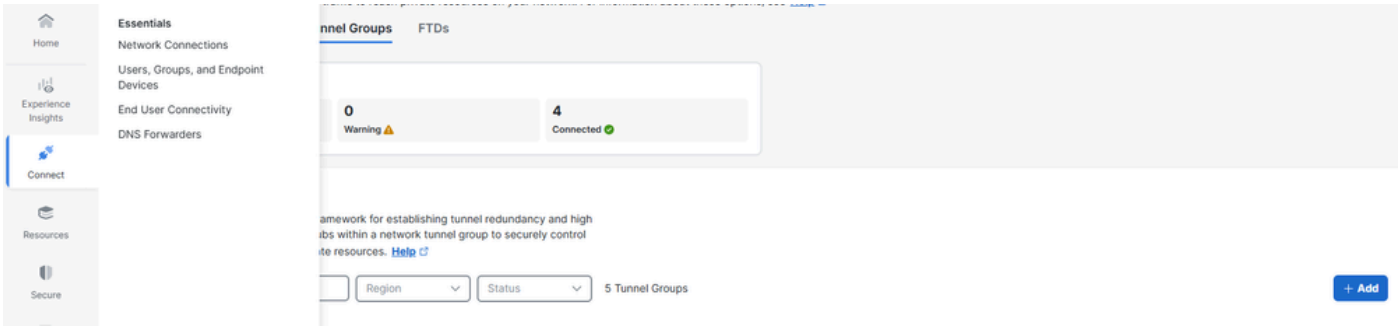
Configuración de Secure Access

Configuración del Grupo de Túnel de Red

1. Acceda al panel de administración de Acceso seguro.

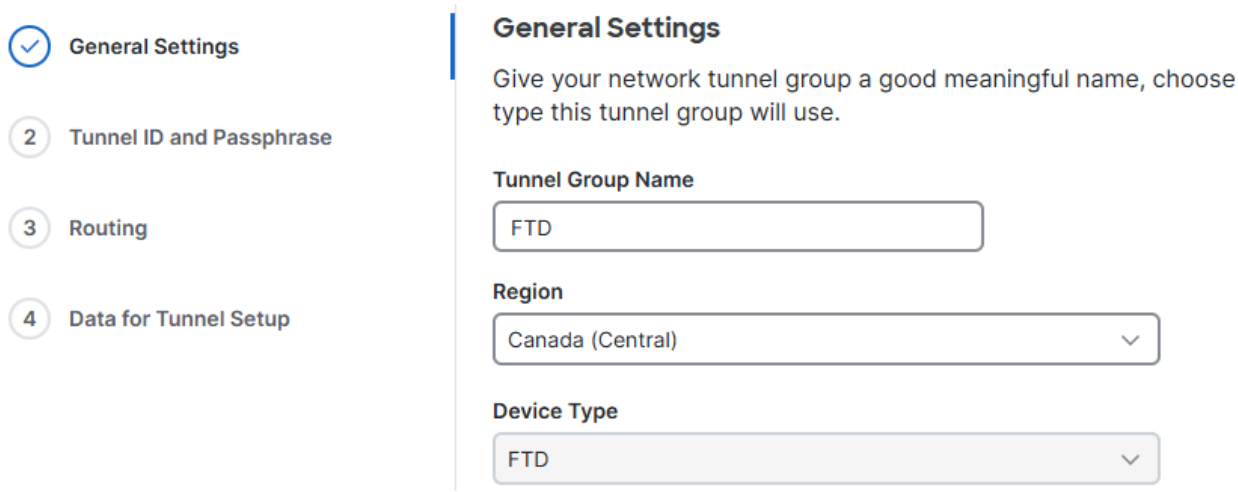
2. Agregue un grupo de túnel de red.

- Haga clic enConnect> Network Connections
  - En Network Tunnel Groups haga clic en > Add



3. General Settings Configuración.

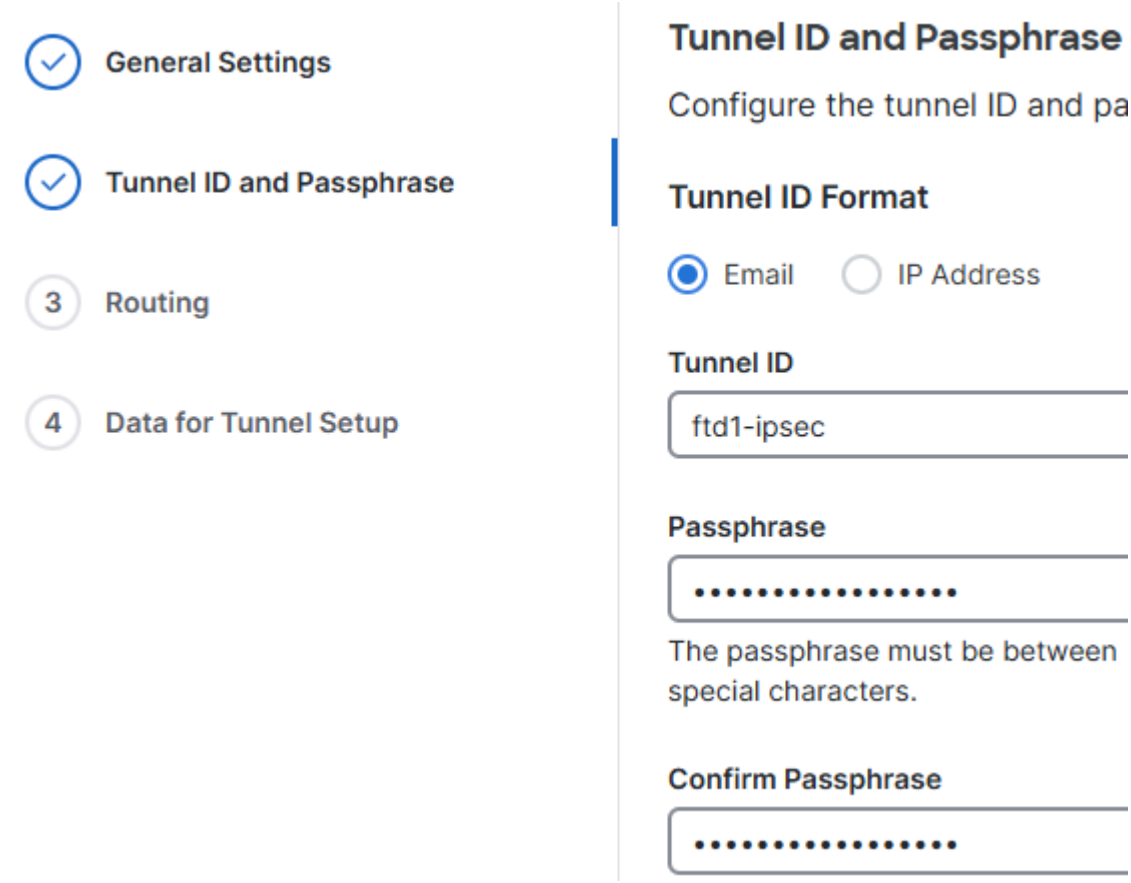
- Configure el Tunnel Group Name, **Region** y Device Type
  - Haga clic en Next



Configuración general

4. Configure Tunnel ID y Passphrase.

- Configure el **Tunnel ID**y Passphrase. Este ID es importante, ya que es necesario para la configuración de FTD
- Haga clic en Next



ID y PSK

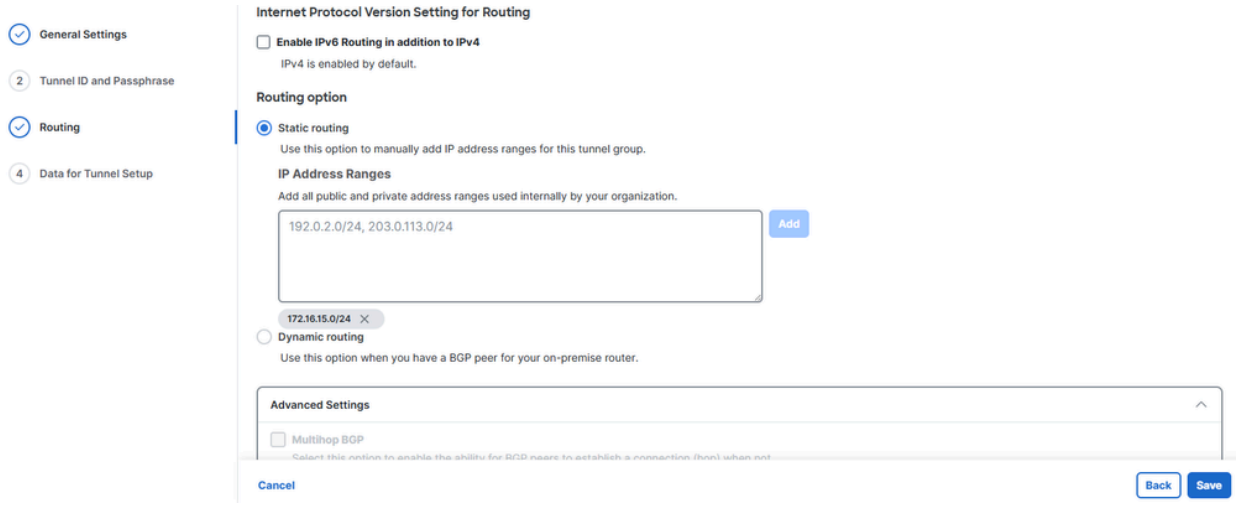
5. Configure el enrutamiento estático.

Routing de acceso seguro

Routing basado en políticas

Agregue las redes protegidas por el FTD a las que desea que accedan los usuarios remotos a través de ZTA o VPNaaS y haga clic en Save (Guardar).

- Haga clic en Routing> **Static routing**
  - Agregue los intervalos de direcciones IP o los hosts que ha configurado en la red y que desea que el tráfico pase a través de Secure Access y haga clic enAdd
  - Haga clic enSave

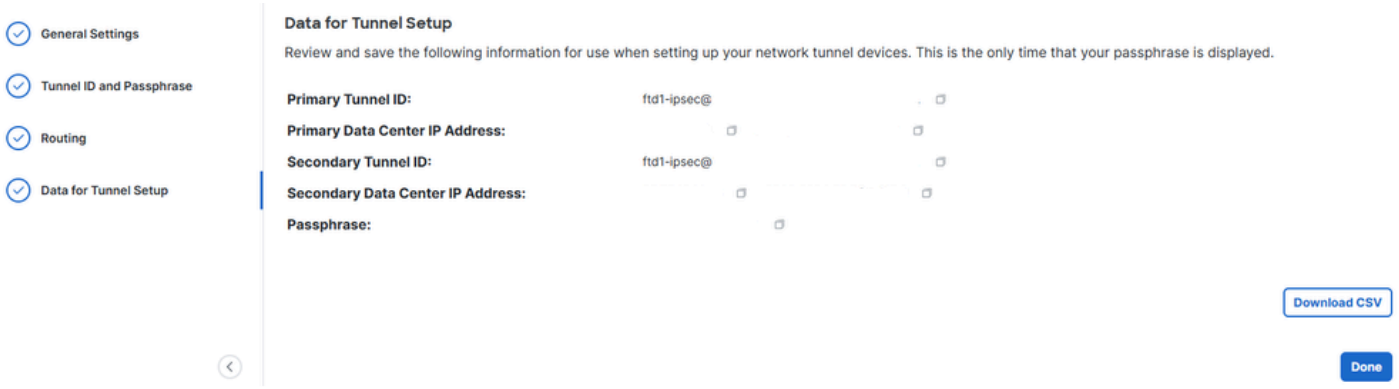


Enrutamiento estático de CSA

Guardar configuración de grupo de túnel de red

Descargue y guarde los datos de configuración del túnel, ya que son necesarios para la configuración del FTD.

- Haga clic en Download CSV
- Haga clic en Done



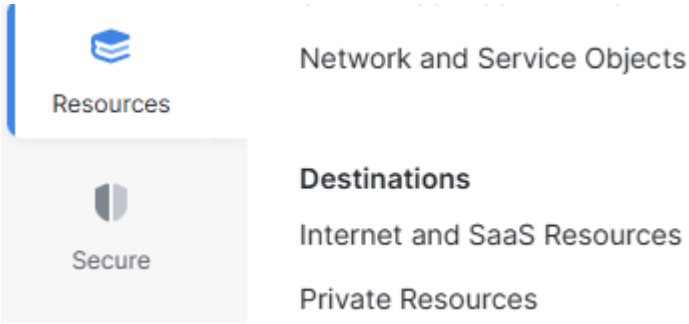
Datos NTG

Crear un recurso privado

Los recursos privados son aplicaciones internas, redes o subredes alojadas en su Data Center o entorno de nube privada. Estos recursos no son de acceso público y están protegidos detrás de la infraestructura de su organización.

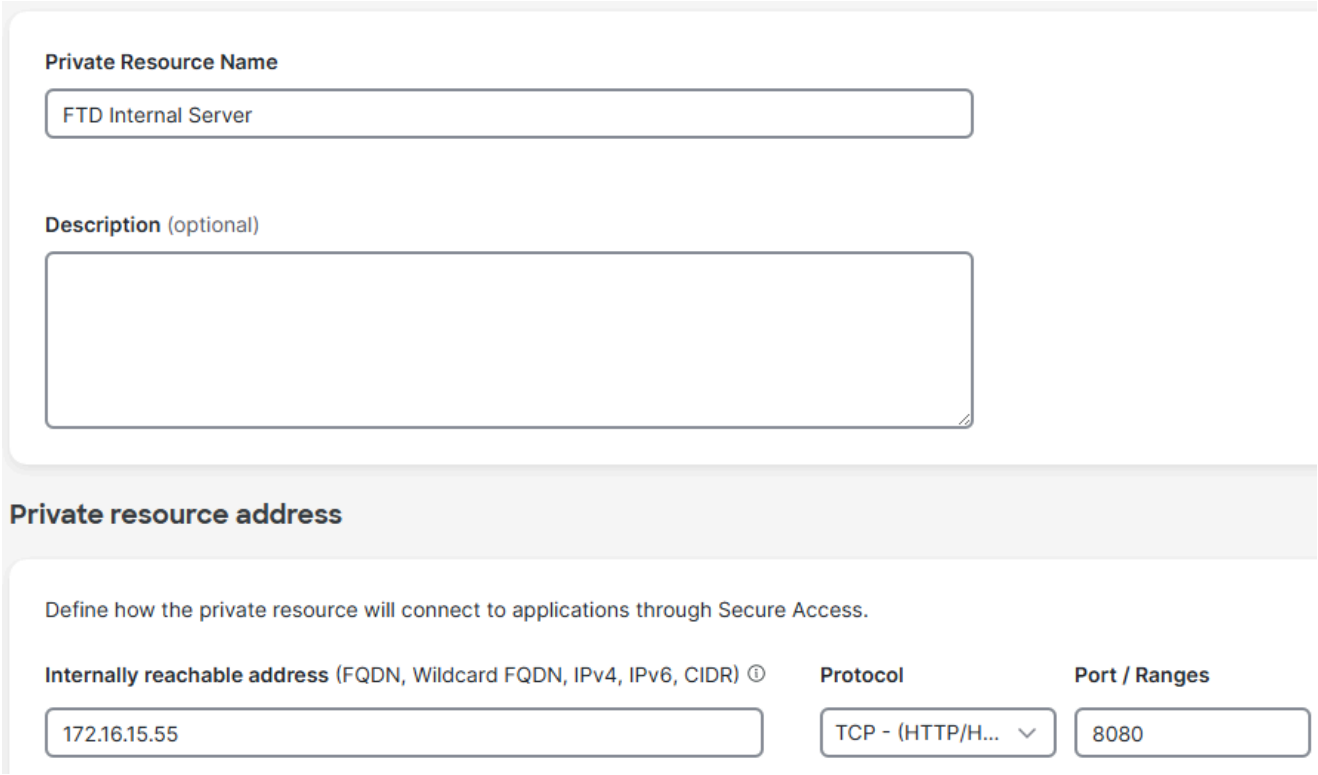
Al definirlos como recursos privados en Secure Access, puede habilitar el acceso controlado a través de soluciones como Zero Trust Access (ZTA) o VPN as a Service (VPNaaS). Esto garantiza que los usuarios puedan conectarse de forma segura a los sistemas internos en función de la identidad, el estado del dispositivo y las políticas de acceso, sin exponer los recursos directamente a Internet.

Vaya a **Resources** > **Private Resources**> haga clic enAdd.



PR

- Especifique el **Private Resource Name**, Internally reachable address, Protocol, Port/Ranges. Especifique puertos y protocolos y agregue recursos privados adicionales según sea necesario
- Seleccione la opción deseada Connection Method en función de sus necesidades, por ejemplo, conexiones de confianza cero o conexiones VPN, según sus requisitos
- Haga clic en Save



Recurso privado

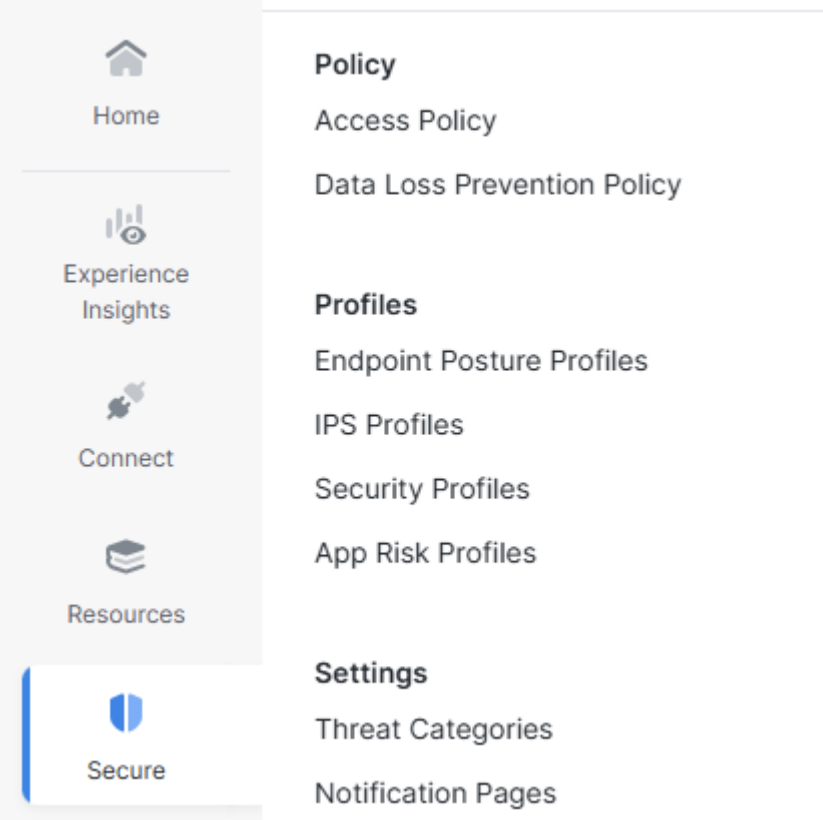
Crear una regla de directiva de acceso

Las reglas de acceso privado definen cómo los usuarios pueden conectarse de forma segura a recursos internos y aplicaciones que no son de acceso público.

Estas reglas aplican la seguridad al controlar quién puede acceder a recursos privados específicos en función de factores como la identidad del usuario, la pertenencia a un grupo, el

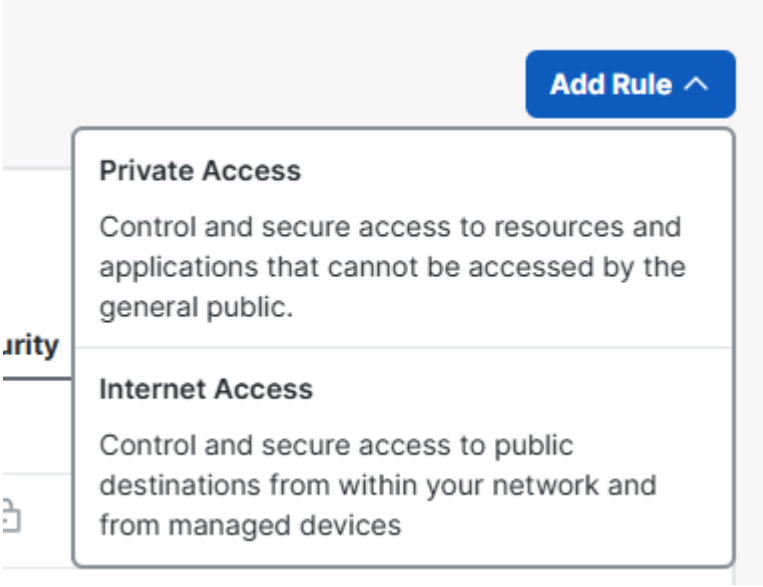
estado del dispositivo, la ubicación u otras condiciones de la directiva. Esto garantiza que los sistemas internos confidenciales permanezcan protegidos frente al acceso público general, al tiempo que se encuentran disponibles de forma segura para los usuarios autorizados a través de ZTA o VPNaaS.

Vaya a Secure>Access Policy



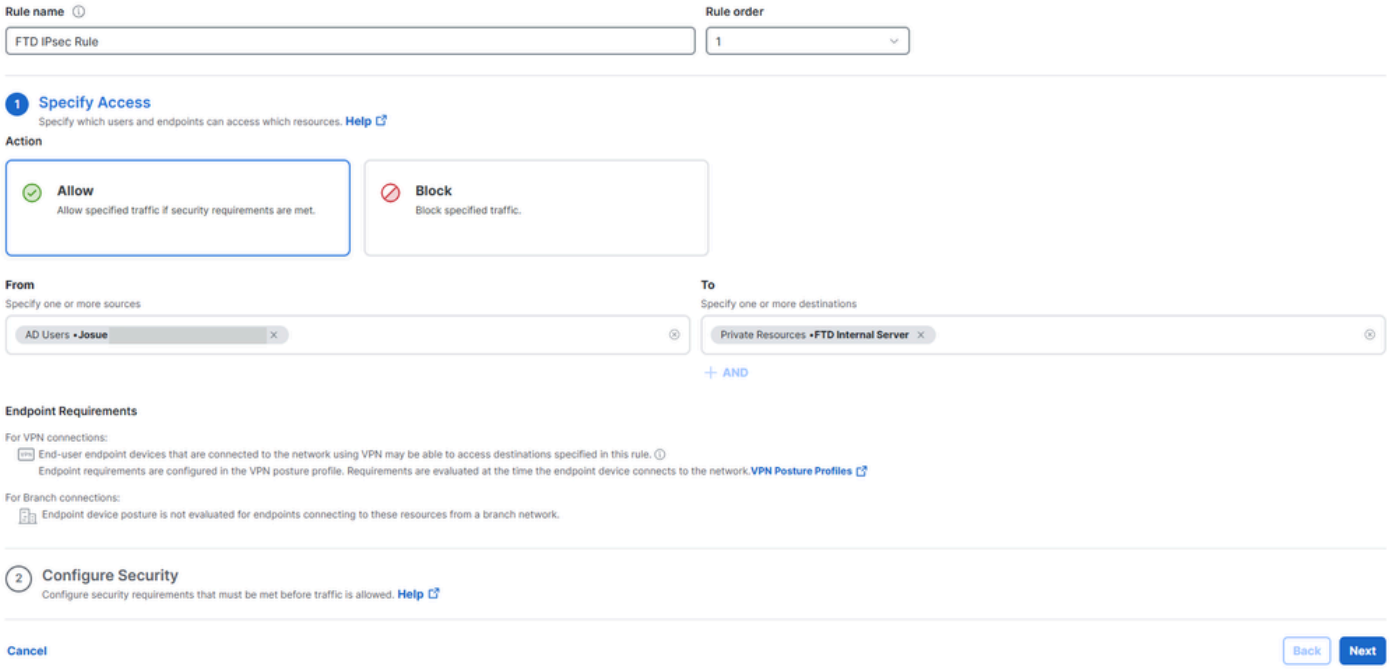
ACP

- Haga clic en Add Rule
  - Haga clic en Private Access



Agregar ACP

- Haga clic en Rule Name y asigne un nombre
- Haga clic enAction, seleccione Allowpara permitir este tráfico
- Haga clicFromen y especifique los usuarios a los que se concede permiso
- Haga clic en Toy especifique el acceso que tienen esos usuarios según esta regla
- Haga clic enNexty Saveen la página siguiente



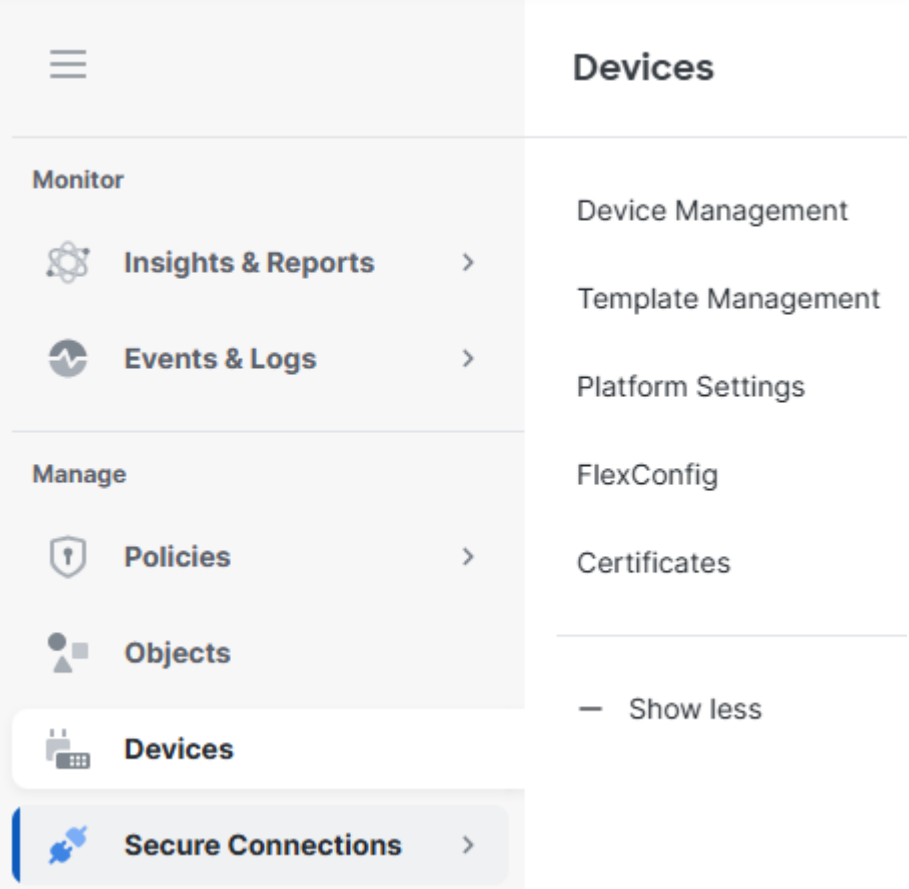
configuración de ACP

Configuración de Secure Firewall Threat Defence (FTD)

Configuración de Interfaces de Túnel Virtual

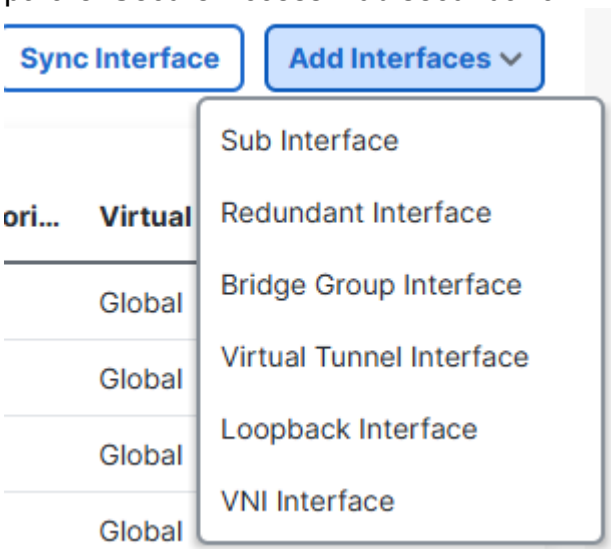
Una interfaz de túnel virtual (VTI) en FTD es una interfaz de capa 3 lógica que se utiliza para configurar túneles VPN IPsec basados en ruta.

1. Acceda a Devices> Device Management.



Dispositivos FTD

- Haga clic en el dispositivo FTD, Interfaces
  - Haga clic en Add Interfaces
  - Haga clic en Virtual Tunnel Interface
  - Cree dos interfaces de túnel virtuales, una para el Secure Access Hub principal y otra para el Secure Access Hub secundario

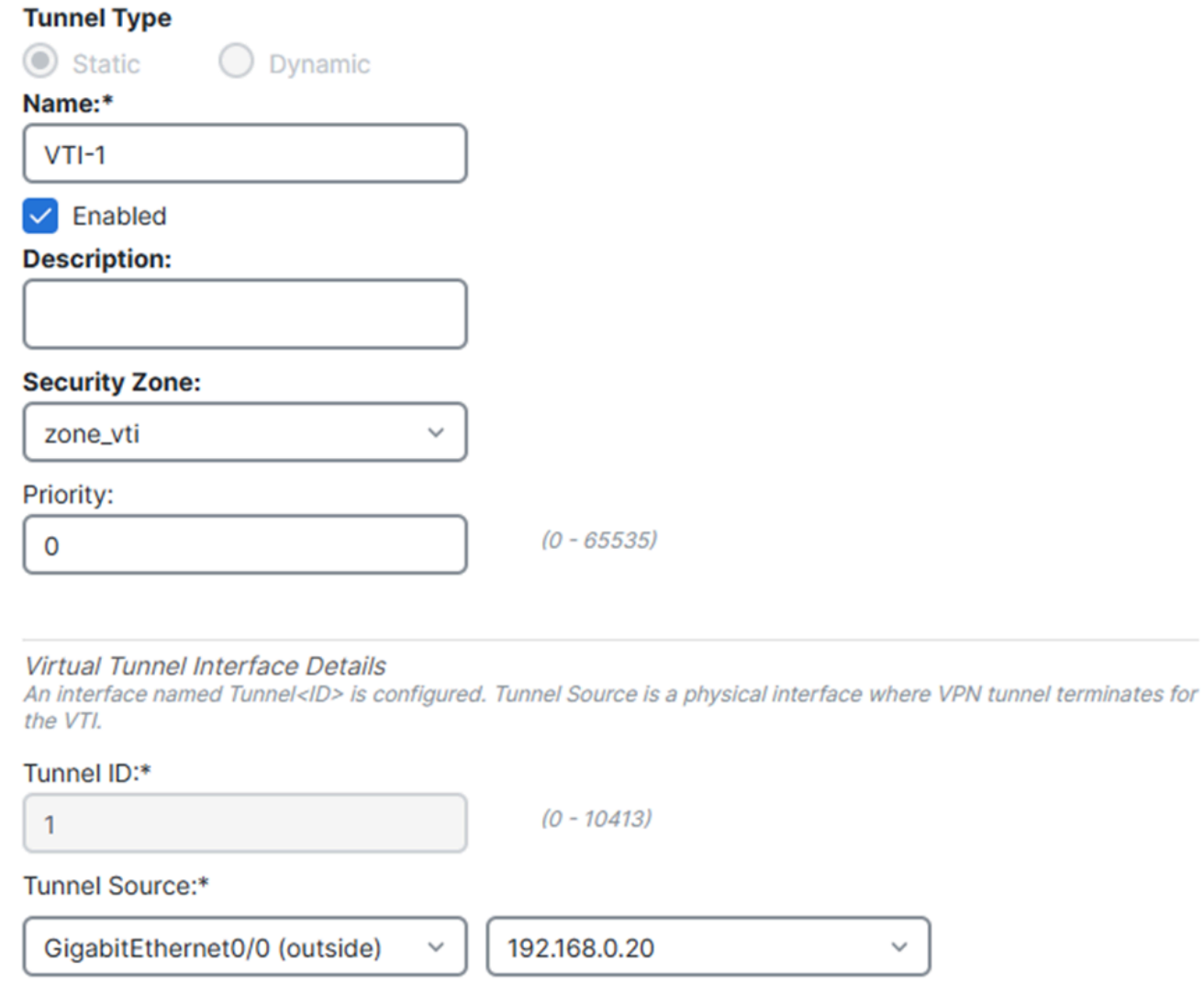


Agregar VTI

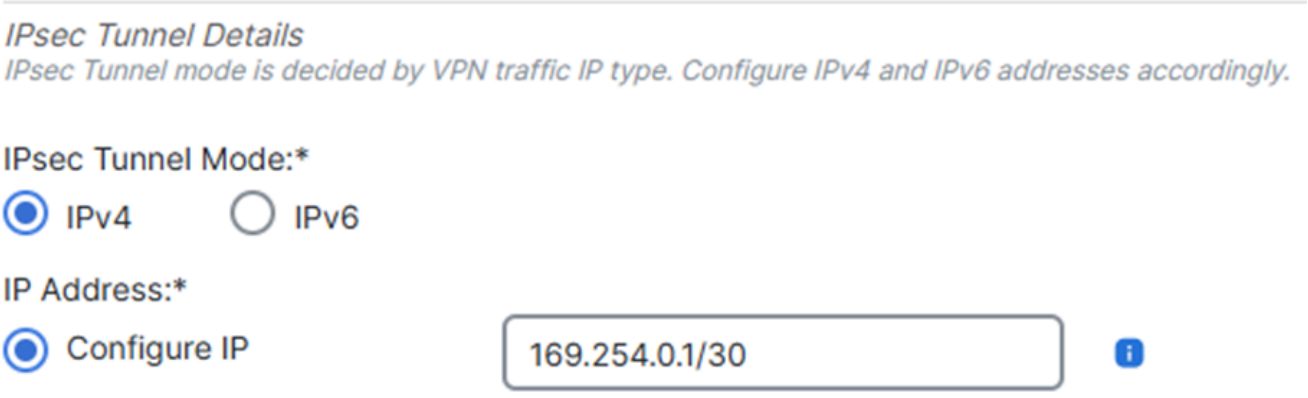
Interfaz de túnel virtual 1:

- Dé un nombre, haga clic en Enable

- Seleccione o cree un Security Zone
- Haga clic en Tunnel ID y asigne un valor.
- Haga clic en Tunnel Source y especifique la interfaz WAN desde la que se establecerá el túnel
- Haga clic en IPsec Tunnel Mode, seleccioneIPv4
- Haga clic en IP Address y configure la dirección IP para el VTI
- Haga clic enOK



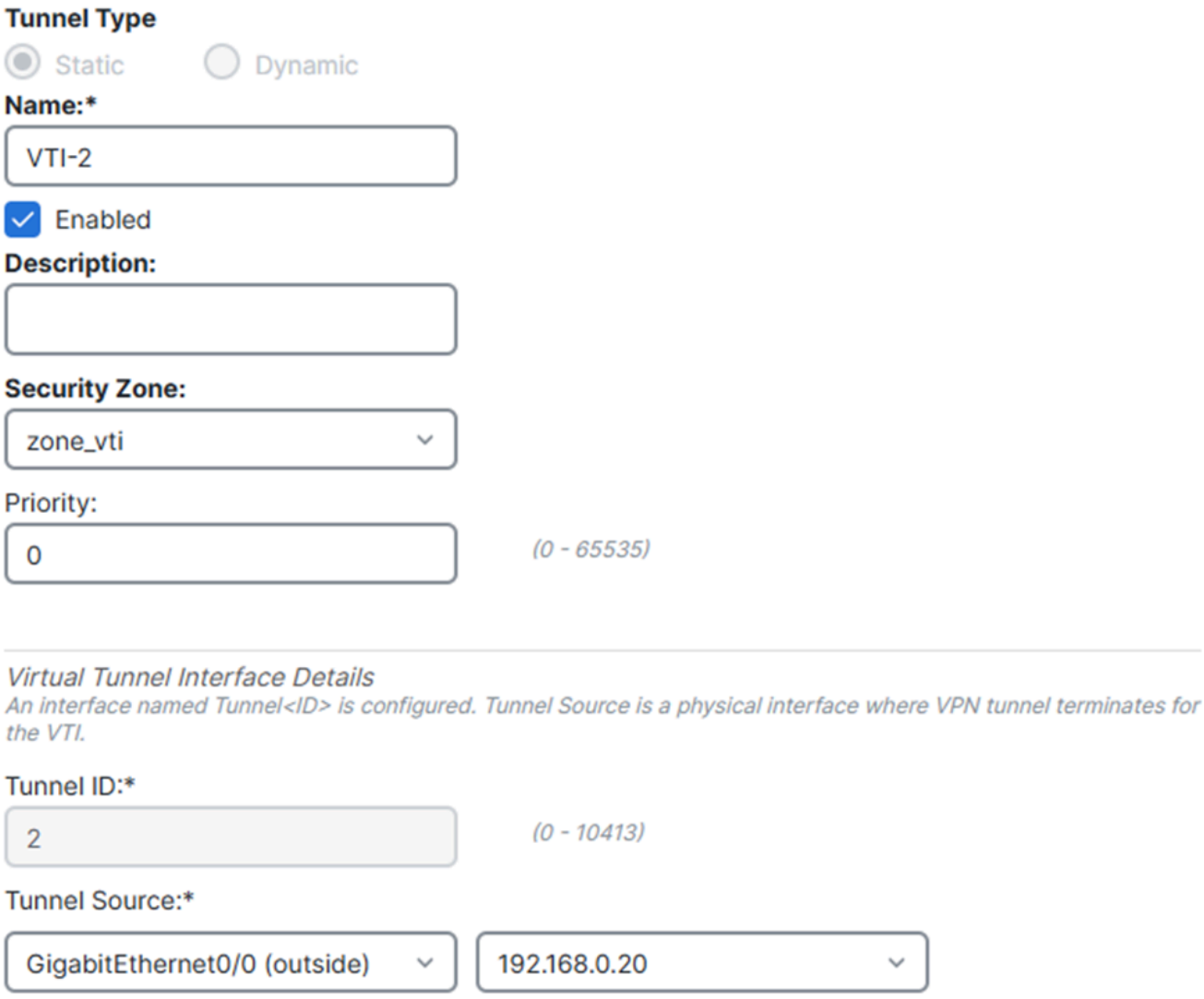
VTI1.1



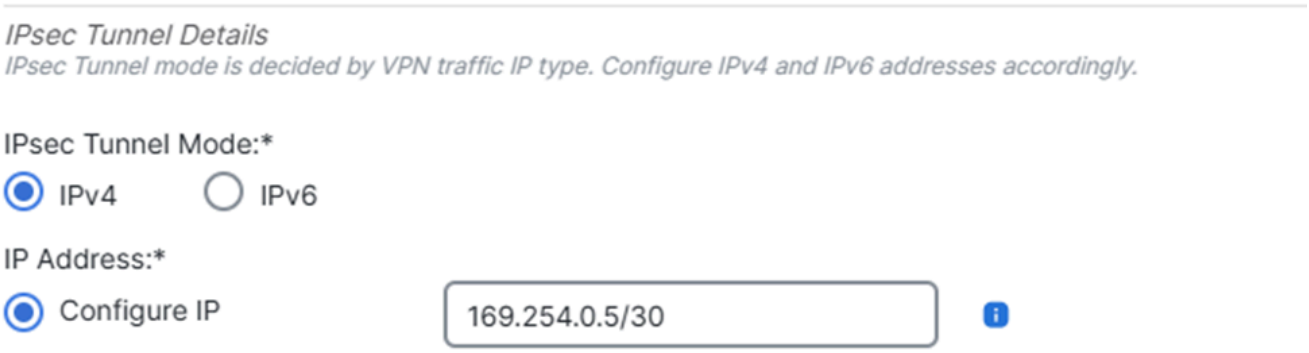
VTI1.2

Interfaz de túnel virtual 2:

- Dé un nombre, haga clic en Enable
- Seleccione o cree un Security Zone
- Haga clic en Tunnel ID y asígnele un valor
- Haga clic en Tunnel Source y especifique la interfaz WAN desde la que se establecerá el túnel
- Haga clic en IPsec Tunnel Mode, seleccioneIPv4
- Haga clic en IP Address y configure la dirección IP para el VTI
- Haga clic enOK

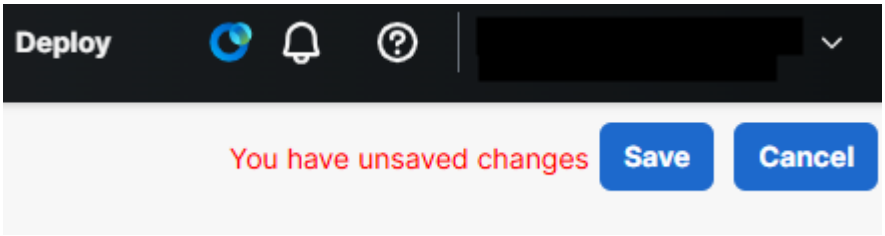


VTI2.1



VTI2.2

- Haga clic en Guardar.

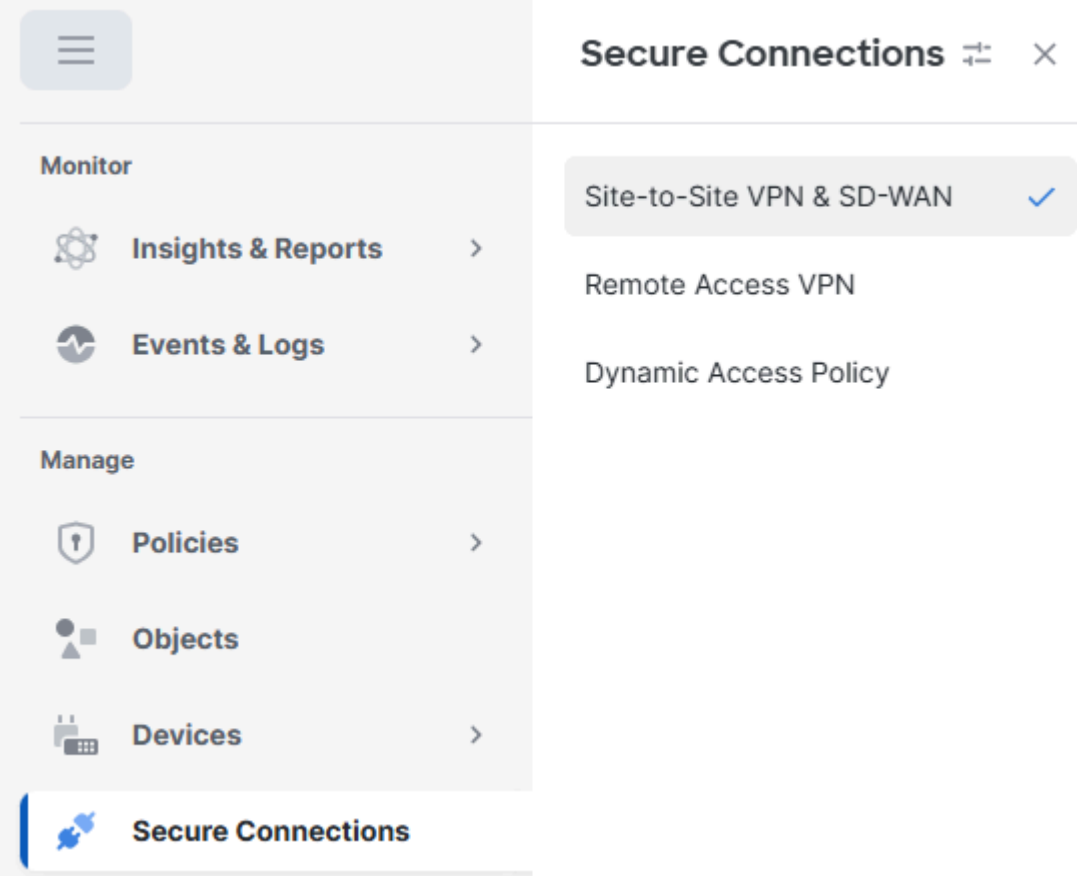


Guardar cambios VTI

Configuración del túnel IPsec

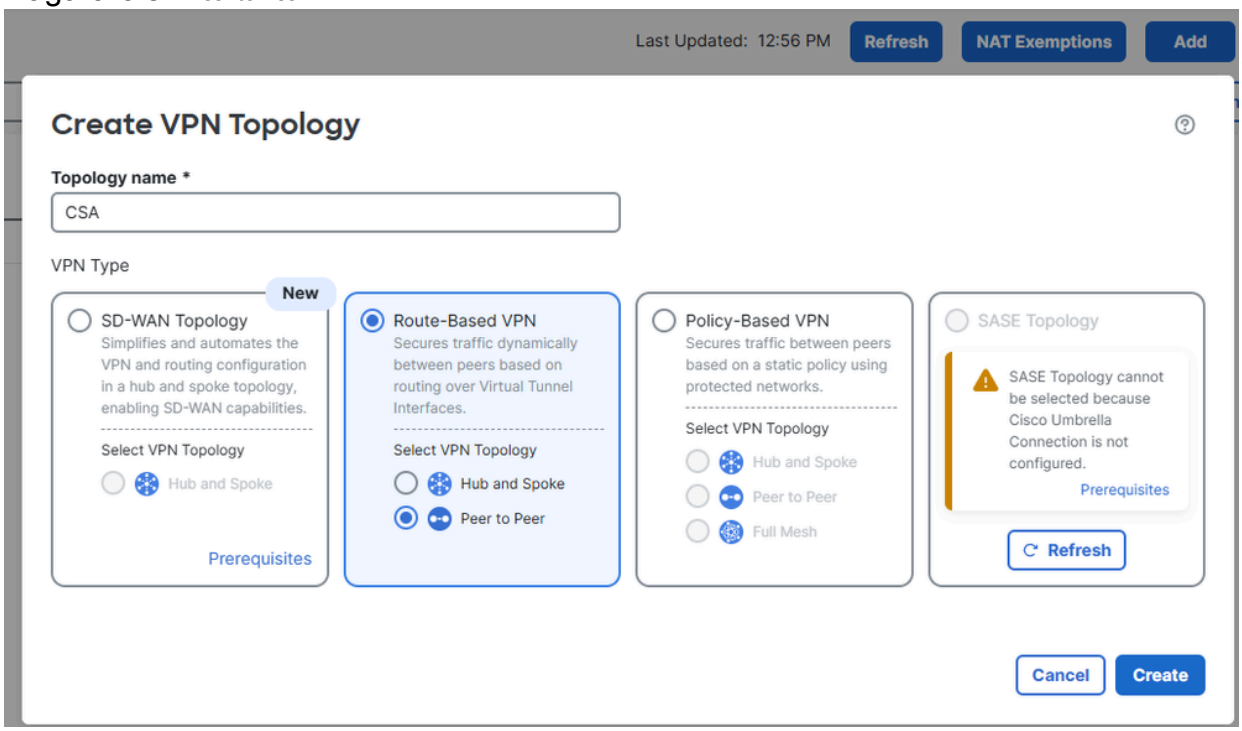
Vaya al panel de cdFMC.

- Haga clic en Secure Connection> Site-to-Site VPN & SD-WAN



S2S

- Haga clic enAdd
  - Haga clic en Route-Based VPN
  - Haga clic en Peer to Peer

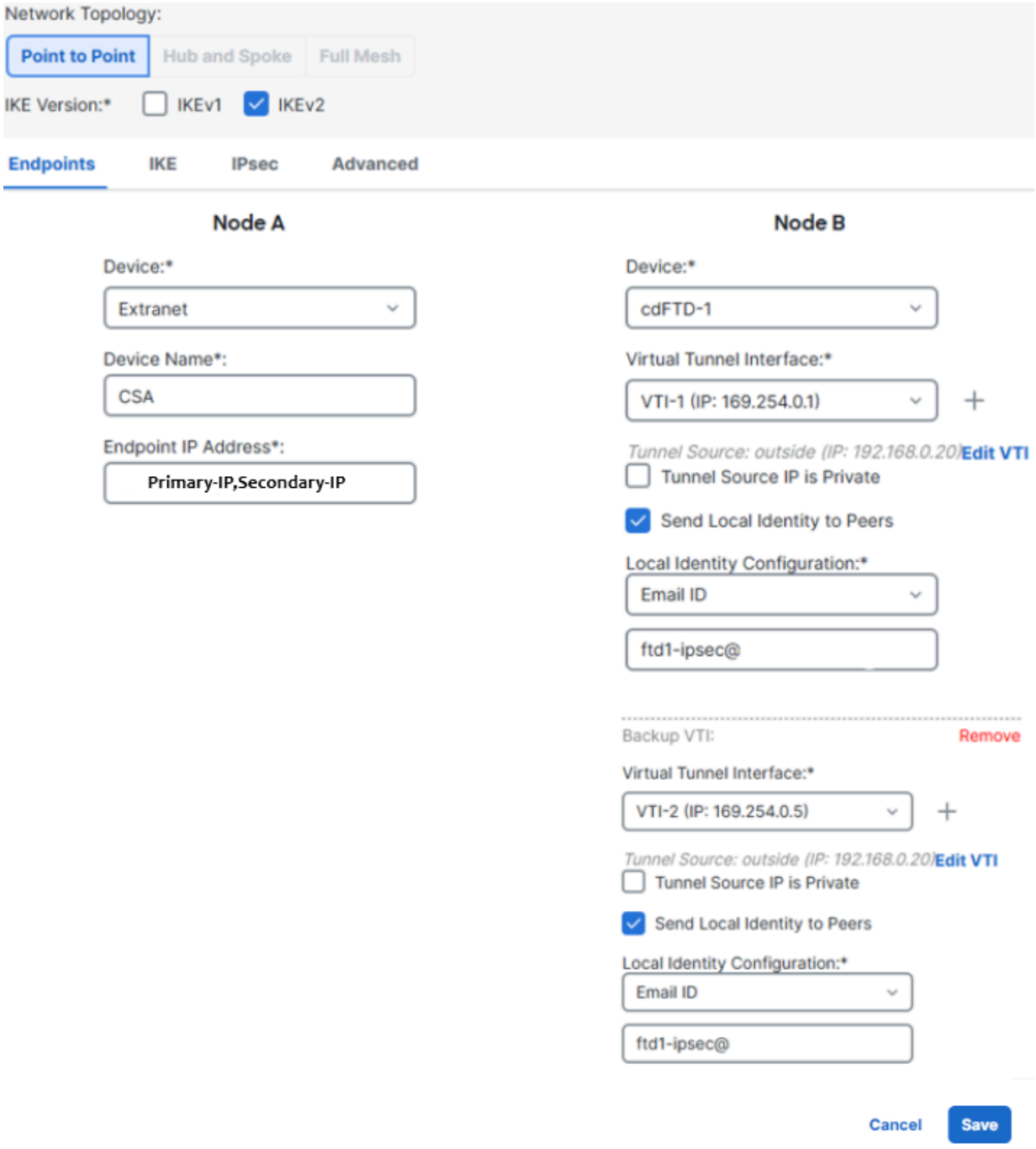


Agregar VPN

- En el paso 5 de la configuración de Secure Access, obtenga los ID de túnel y las direcciones

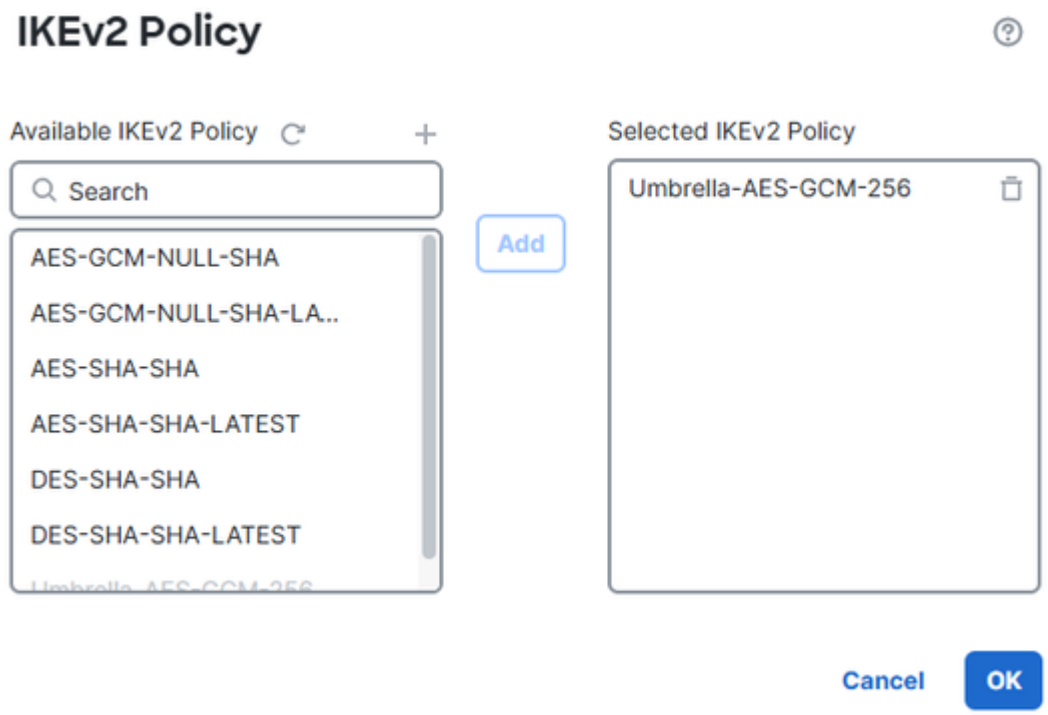
IP de los Data Centers principales y secundarios

- Haga clic enEndpoints
  - EnNode A, haga clic enDevicey seleccione Extranet
  - Haga clic en Device Namey asigne un nombre
  - Haga clic en Enpoint IP Addresses e introduzca las direcciones IP primaria y secundaria de Secure Access separadas por una coma (en "Save Network Tunnel Group Configuration" [Guardar configuración de grupo de túnel de red]) en Secure Access Configuración)
  - En Node B, haga clic enDevicey seleccione el dispositivo FTD
  - Haga clic en Virtual Tunnel Interface y seleccione la primera interfaz VTI creada en el paso anterior
  - Haga clic en Send Local Identity to Peers option (opción) y seleccione Email ID, ingrese el ID de túnel principal (de "Save Network Tunnel Group Configuration" (Guardar configuración de grupo de túnel de red) bajo la configuración de acceso seguro)
  - Haga clic en Add Backup VTI
  - Haga clic en Virtual Tunnel Interface y seleccione la segunda interfaz VTI creada en el paso anterior
  - Haga clic enSend Local Identity to Peersonoption y seleccione Email ID, ingrese el ID del túnel secundario (de "Save Network Tunnel Group Configuration" en Secure Access Configuration)
  - Haga clic en Guardar



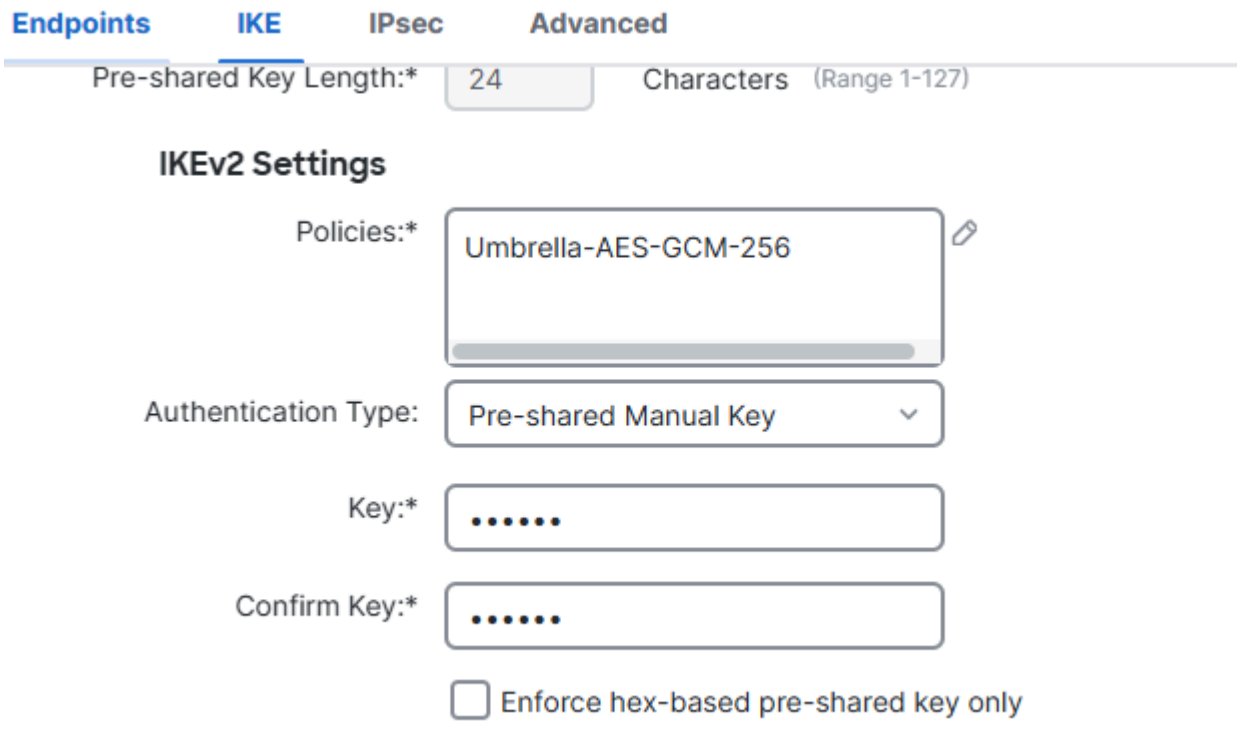
configuración de FTD VTI

- Haga clic enIKE
  - Haga clic en **IKEv2 Settings >** Policies
  - Seleccione laUmbrella-AES-GCM-256opción
  - Haga clic en OK



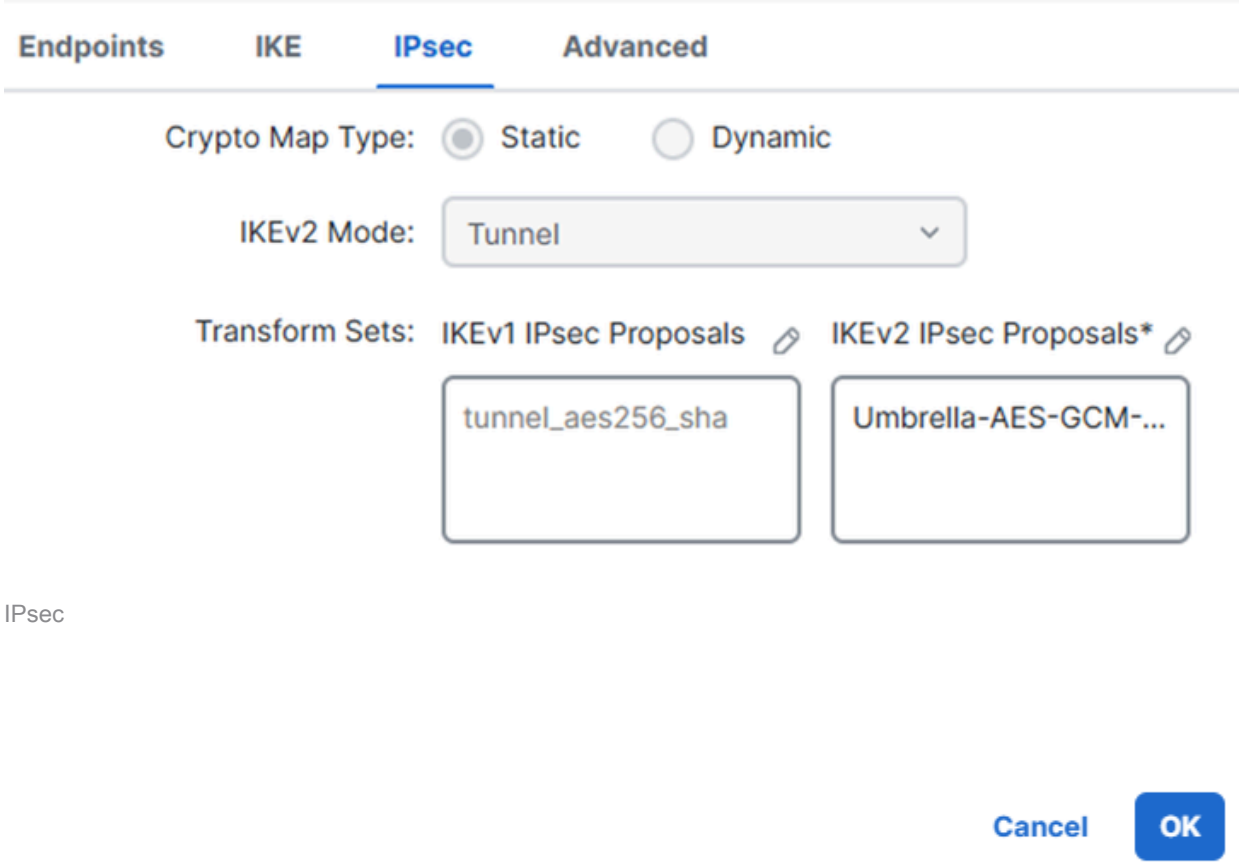
Política IKEv2

- Haga clic en Authentication Type y seleccionePre Shared Manual Keye introduzca la PSK configurada en Secure Access (frase de paso)



IKE

- Haga clic en IPSEC
  - Haga clic en IKEv2 Proposals
  - Seleccionar Umbrella-AES-GCM-256
  - Haga clic en OK



IPsec

Guardar las propuestas de IKEv2

Configuración de enrutamiento de FTD

El routing basado en políticas (PBR) permite controlar el reenvío de tráfico según criterios que van más allá de la dirección IP de destino. En lugar de depender únicamente de la tabla de ruteo, PBR puede rutear el tráfico basado en el origen, la aplicación, el protocolo, los puertos u otras políticas definidas.

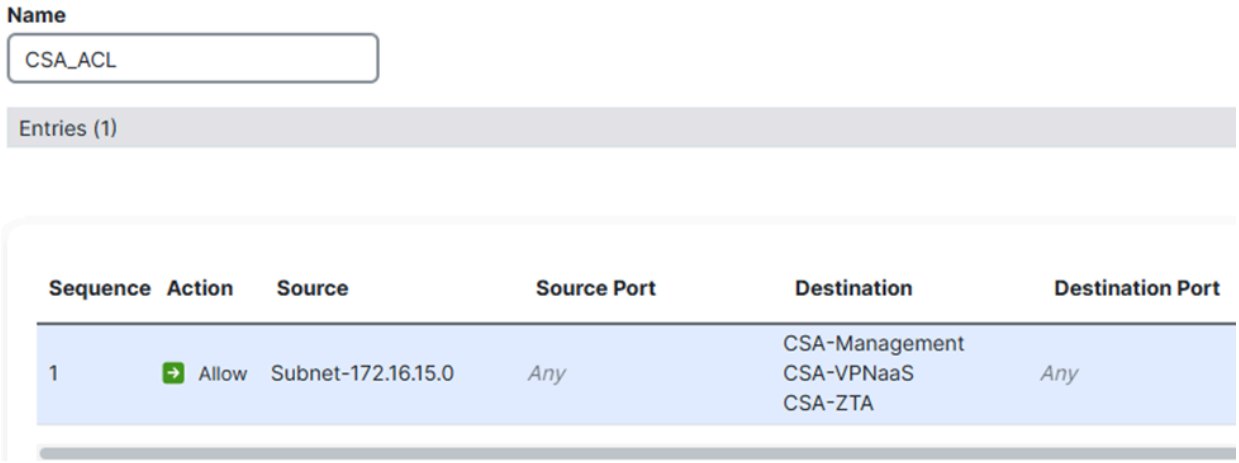
Esto permite a las organizaciones dirigir el tráfico específico o de alta prioridad sobre los enlaces preferidos (como un ancho de banda alto o un enlace directo a Internet), optimizar el rendimiento y desglosar de forma segura determinadas aplicaciones sin enviar todo el tráfico a través de un túnel VPN.

Policy-Based Routing

- Vaya a Objects
  - Haga clic en Access List
  - Haga clic en Extended
  - Haga clic enAdd Extended Access List

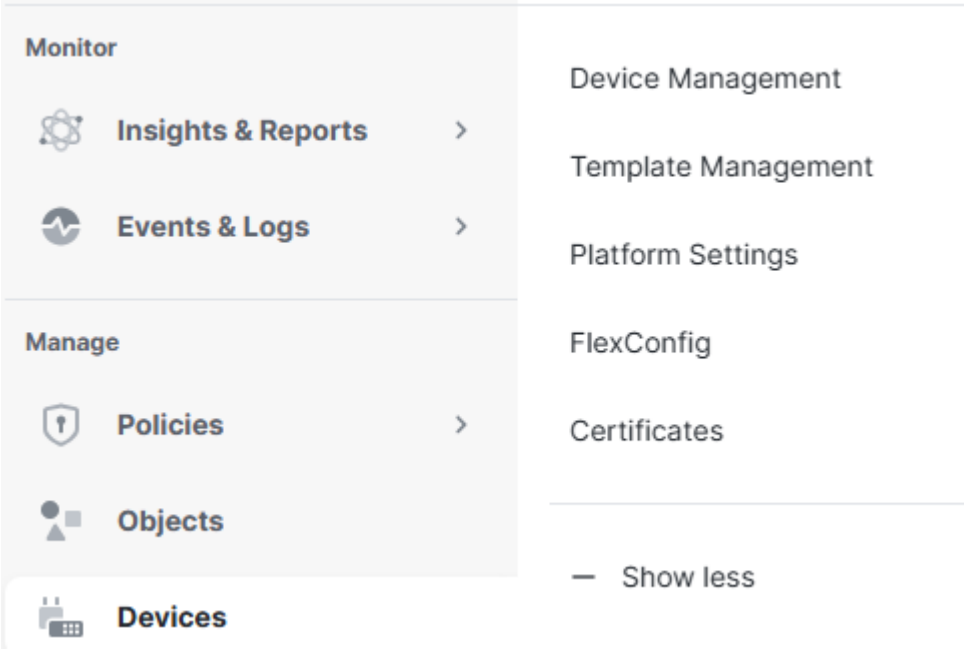
Agregar ACL

Cree una lista de control de acceso (ACL) ampliada que coincida con la red de origen protegida por el FTD (por ejemplo, 172.16.15.0/24) para enviarla a través del túnel. Para el destino, agregue las redes utilizadas por ZTA (rango CGNAT) y la red utilizada por su VPNaaS (verifique Virtual Private Network IP Pool).



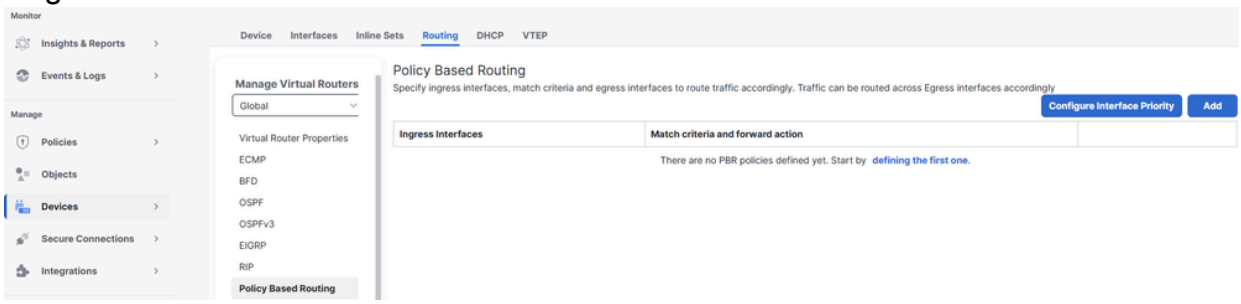
ACL

- Haga clic en Devices> Device Management



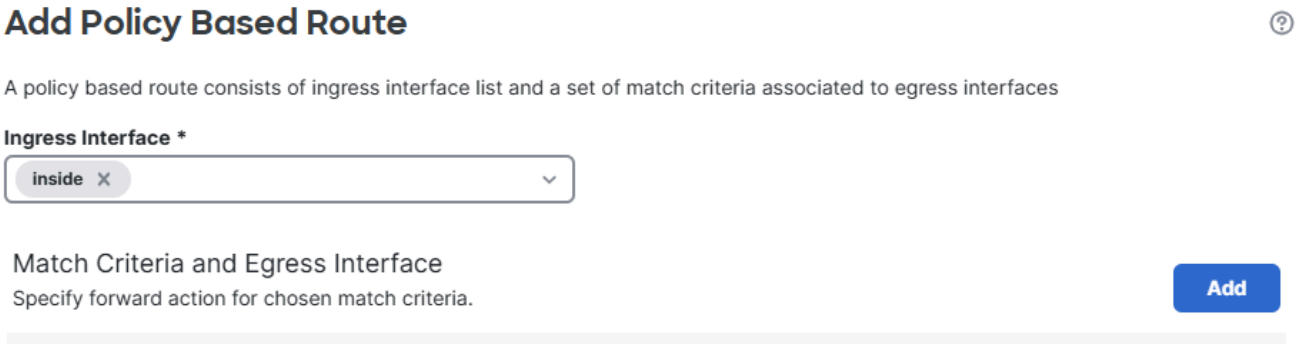
Dispositivo

- Haga clic en el FTD
  - Haga clic enRouting
  - Haga clic en Policy Based Routing
  - Haga clic en Add



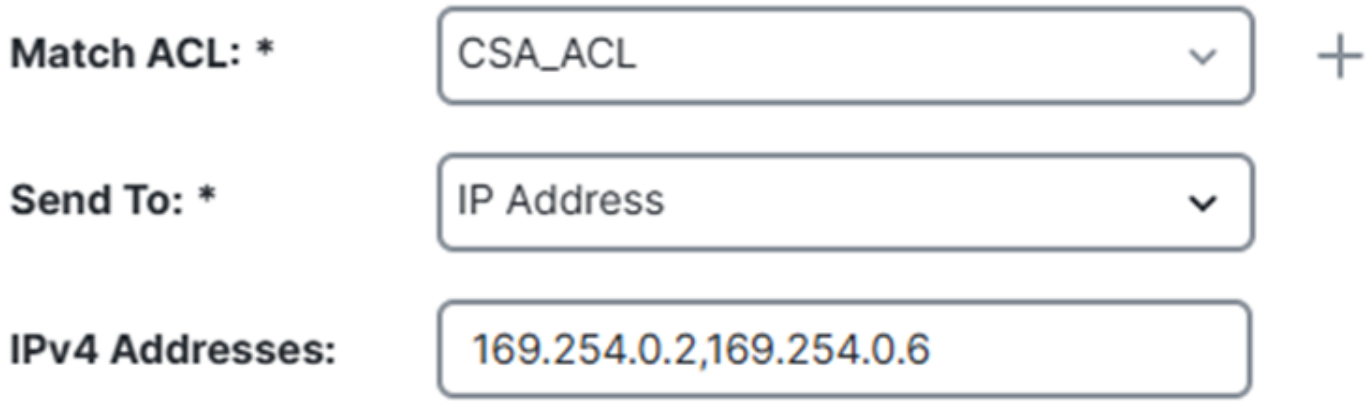
Agregar PBR

- Haga clic en Ingress Interface y seleccione la interfaz de entrada en la que entra el tráfico de las redes internas
- En Criterios de coincidencia e Interfaz de salida, haga clic en Add



Interfaz de entrada

- Haga clic en Match ACL y seleccione la lista de control de acceso ampliada creada anteriormente
- Haga clic en Send To and select IP Address
- Haga clic en IPv4 Addresses y establezca como saltos siguientes las direcciones IP dentro de las subredes de interfaz VTI configuradas anteriormente en el FTD (169.254.0.2 y 169.254.0.6)
- Haga clic en Save



Configuración basada en políticas

Guardar PBR

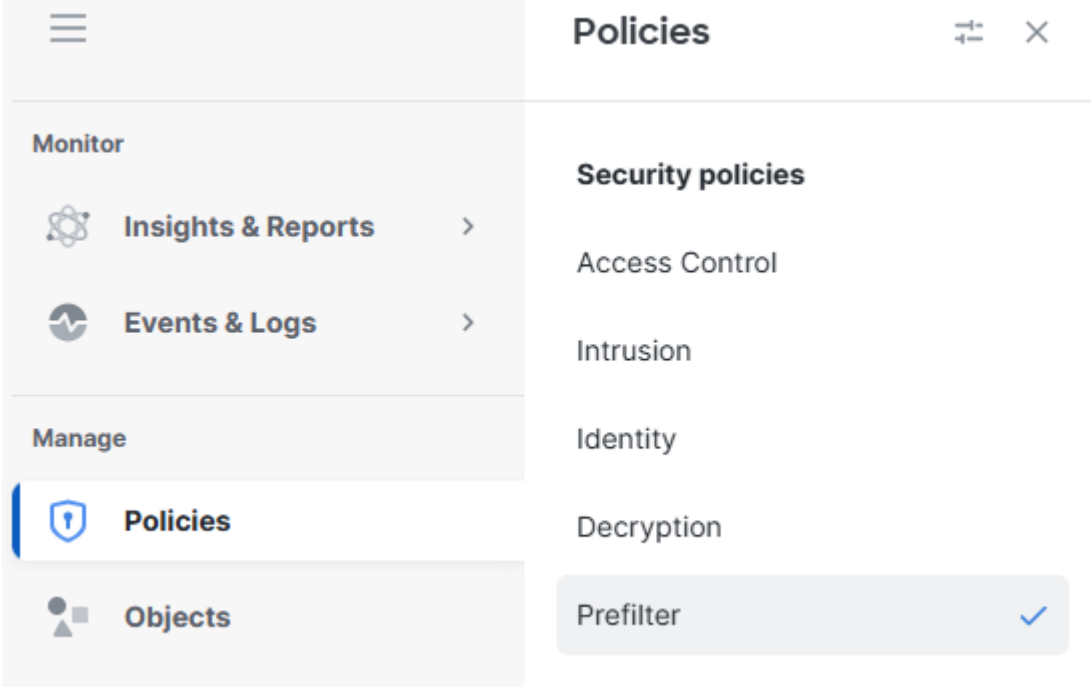
Asegúrese de seleccionar la opción Send To > IP Address , y no la Egress Interface opción.

Configuración de política de acceso

Para permitir el tráfico en un Cisco Firepower Threat Defence (FTD) y permitir el acceso a recursos privados, el tráfico debe pasar primero por la fase inicial del control de acceso conocida como filtrado previo.

El prefiltrado se procesa antes de que se produzca una inspección más profunda y está diseñado para ser sencillo y rápido. Evalúa el tráfico utilizando criterios básicos de encabezado externo (como direcciones IP y puertos de origen y destino) para permitir, bloquear o omitir el tráfico rápidamente. Cuando se permite el tráfico en esta etapa, puede omitir inspecciones que requieren más recursos, como la inspección profunda de paquetes o las políticas de intrusión, lo que mejora el rendimiento al tiempo que mantiene el control de seguridad.

- Vaya a Policies> Prefilter



Prefiltrar

- Haga clic en Editar la política de filtro previo que utiliza su política de acceso

haga clic en prefiltrar

- Haga clic en Add Tunnel Rule
  - Agregue y permita el tráfico de la red VPNaaS y/o la subred ZTA a sus recursos privados
  - Haga clic enSave

Guardar regla

Llegados a este punto, una vez completada y verificada la configuración del FTD, podrá continuar

con la implementación. Después de la implementación, los túneles IPsec se activan correctamente, lo que confirma que se ha establecido una conectividad segura con los recursos privados.

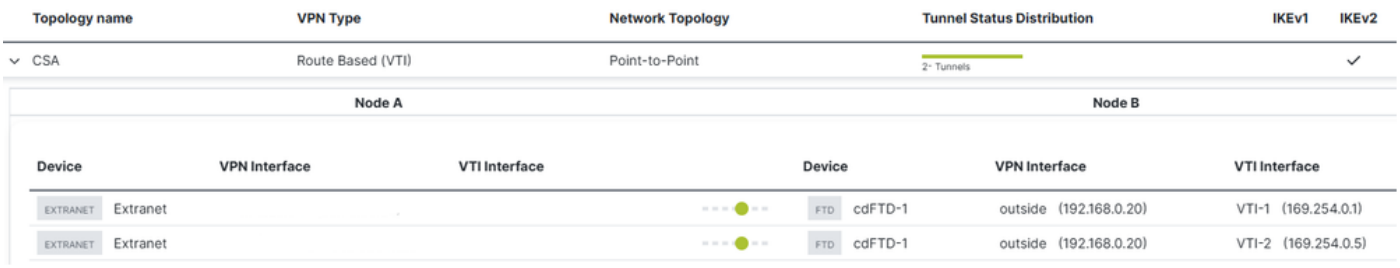
Verificación

Verificar en FTD

Estado del túnel en FTD

Puede ver el estado actual del túnel, incluso si está activo o inactivo. Esto ayuda a verificar que el túnel IPsec esté establecido correctamente.

- Haga clic en Conexiones seguras.
- Haga clic en VPN de sitio a sitio y SD-WAN.
- Haga clic en el nombre de topología.



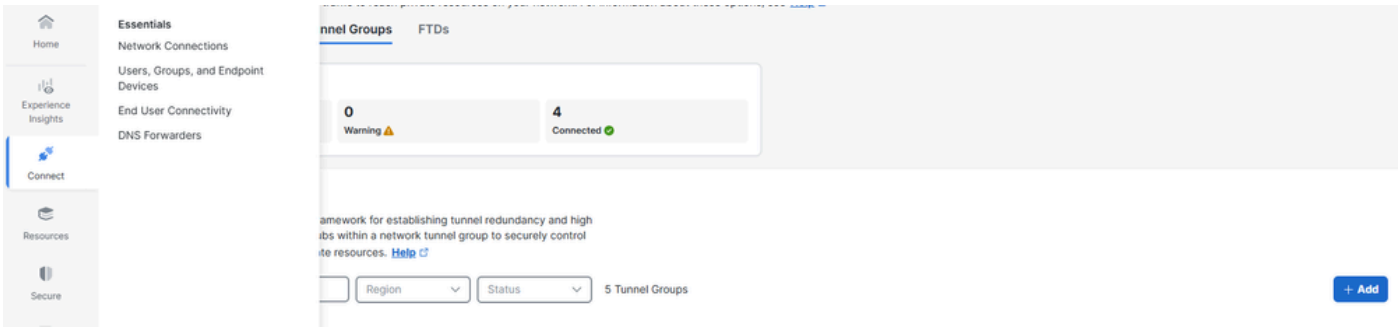
Estado del túnel FTD

Verificar en Secure Access

Estado del túnel en Secure Access

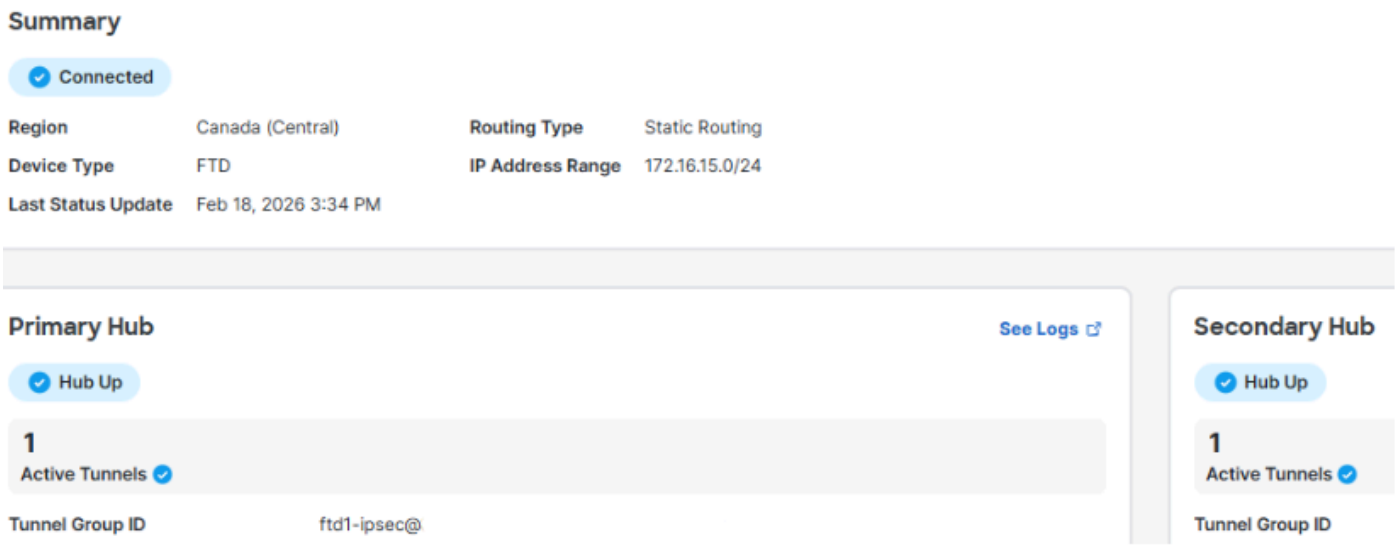
Puede ver el estado actual del túnel, incluido si está desconectado, con advertencia o conectado. Esto ayuda a verificar que el túnel IPsec esté establecido correctamente.

- Haga clic en Connect > Network Connections
- Haga clic en Network Tunnel Groups .



Comprobar NTG

- Haga clic en el grupo de túnel de red

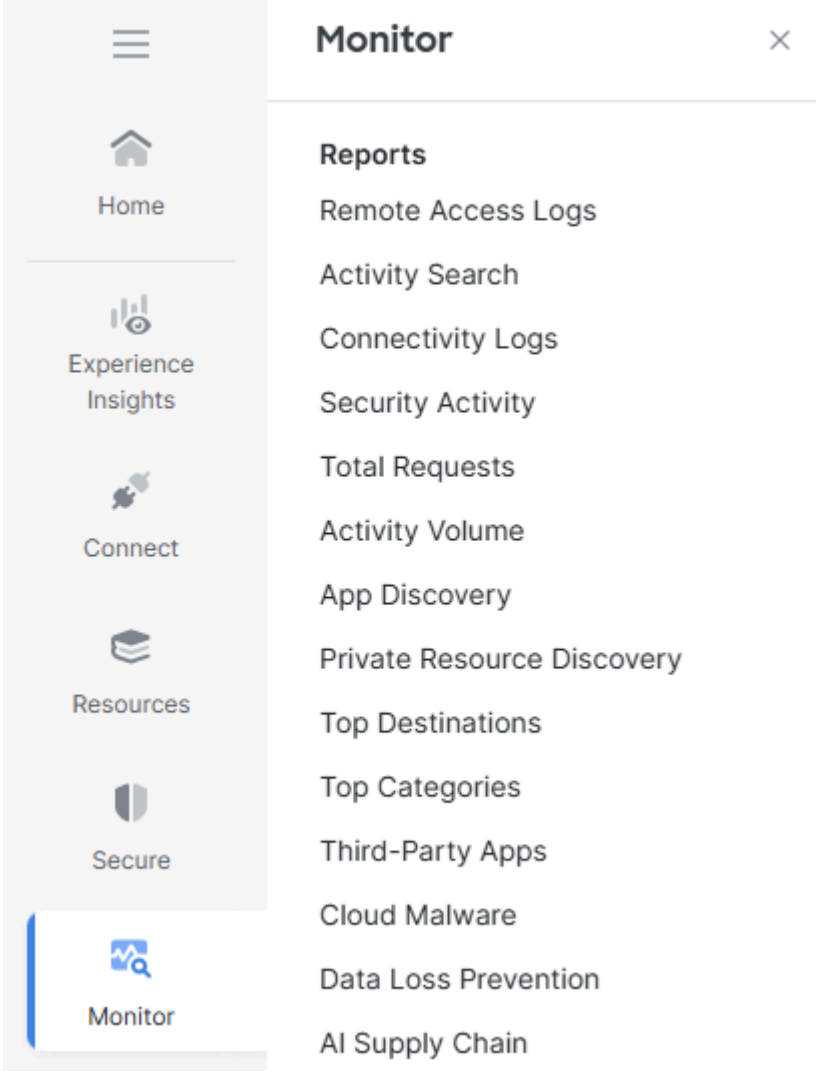


Estado del túnel CSA

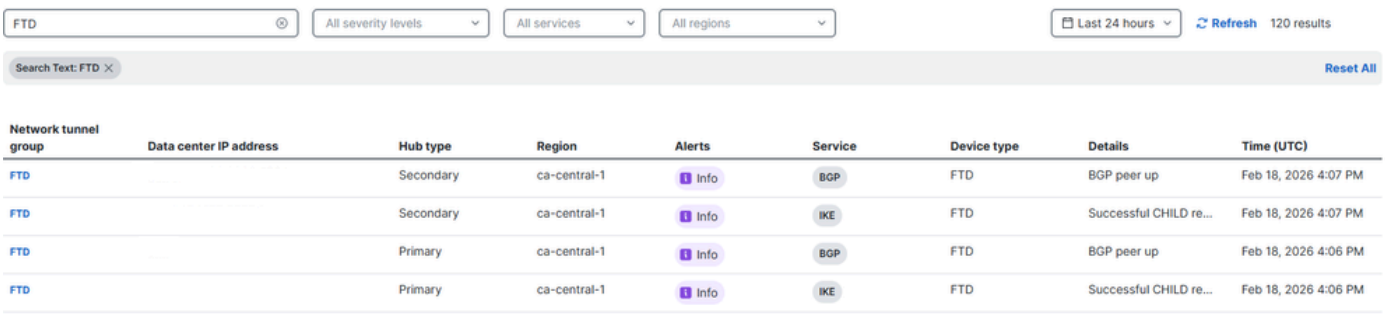
Eventos en Secure Access

Puede ver los eventos de túnel y confirmar si el estado de los túneles IPsec es activo y estable.

Haga clic en Monitor > Network Connectivity.

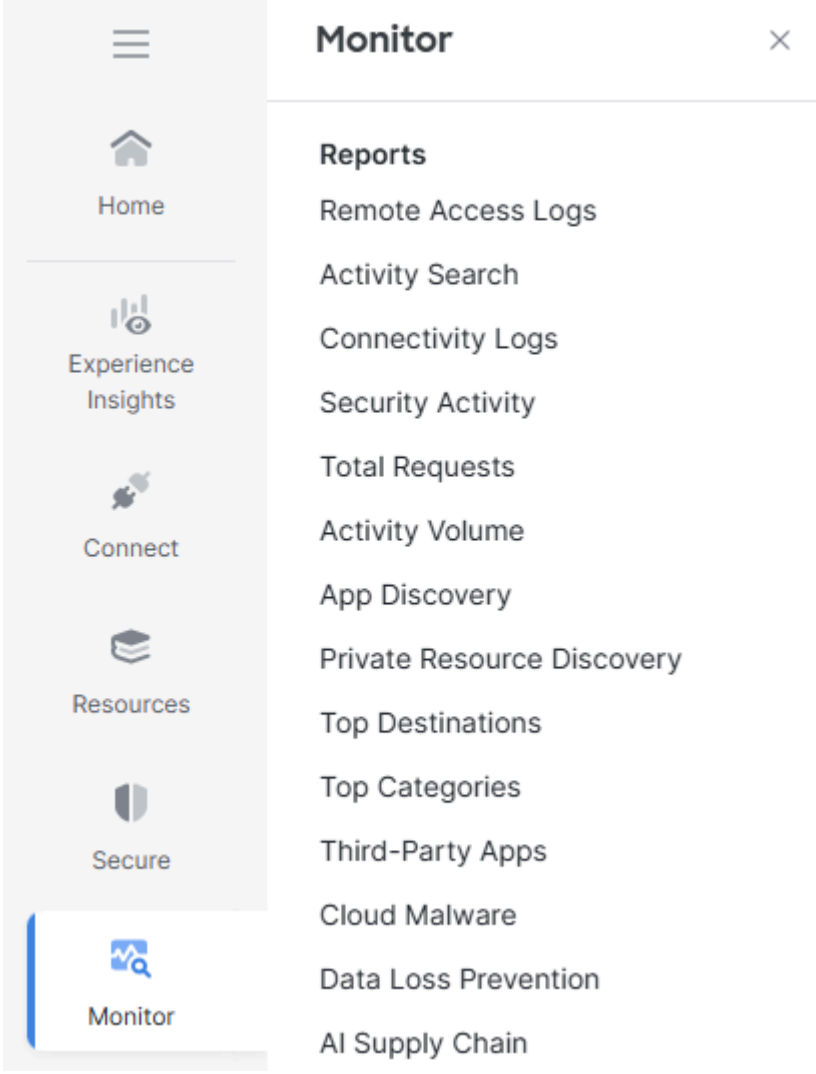


Supervisar registros de conexión



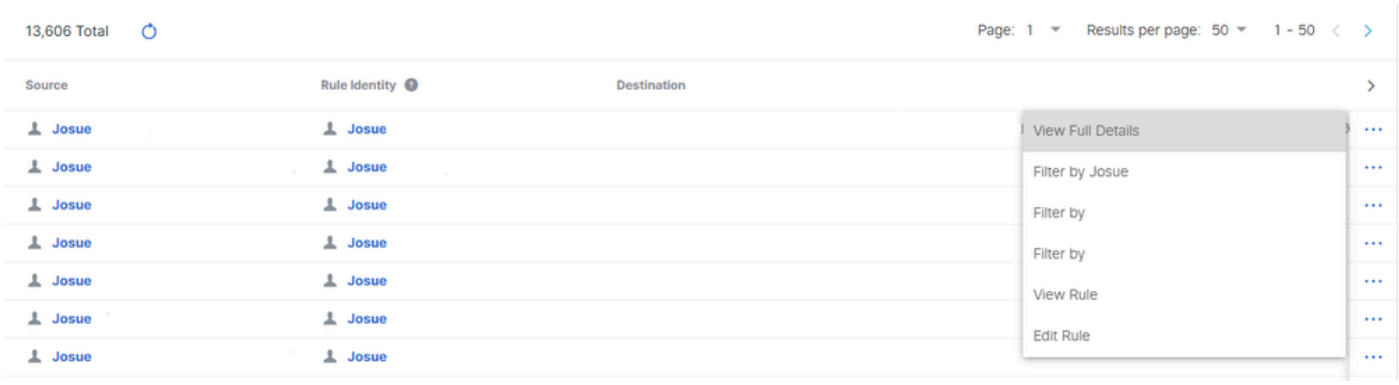
Registros de conexión

Vaya a en Monitor > Activity Search.

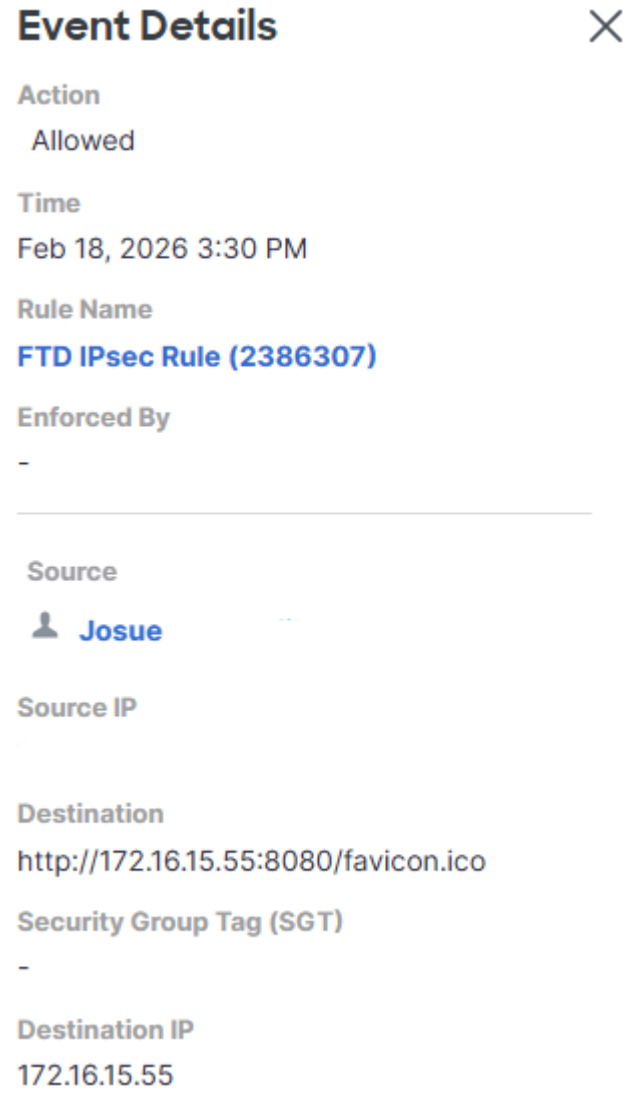


Supervisar registros de conexión

En cualquiera de los eventos relacionados, haga clic en Ver detalles completos.



Detalles completos



Búsqueda de actividad

Información Relacionada

- Soporte técnico y descargas de Cisco
- Guía de configuración de dispositivos de Cisco Secure Firewall Management Center, 7.7

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).