

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

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Configuración de Secure Access](#)

[Configuración del Grupo de Túnel de Red](#)

[Routing de acceso seguro](#)

[Routing basado en políticas](#)

[Guardar configuración de grupo de túnel de red](#)

[Crear un recurso privado](#)

[Crear una regla de directiva de acceso](#)

[Configuración de Secure Firewall Threat Defence \(FTD\)](#)

[Configuración de Interfaces de Túnel Virtual](#)

[Configuración del túnel IPsec](#)

[Configuración de enrutamiento de FTD](#)

[Policy-Based Routing](#)

[Configuración de política de acceso](#)

[Verificación](#)

[Verificar en FTD](#)

[Estado del túnel en FTD](#)

[Verificar en Secure Access](#)

[Estado del túnel en Secure Access](#)

[Eventos en Secure Access](#)

[Información Relacionada](#)

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

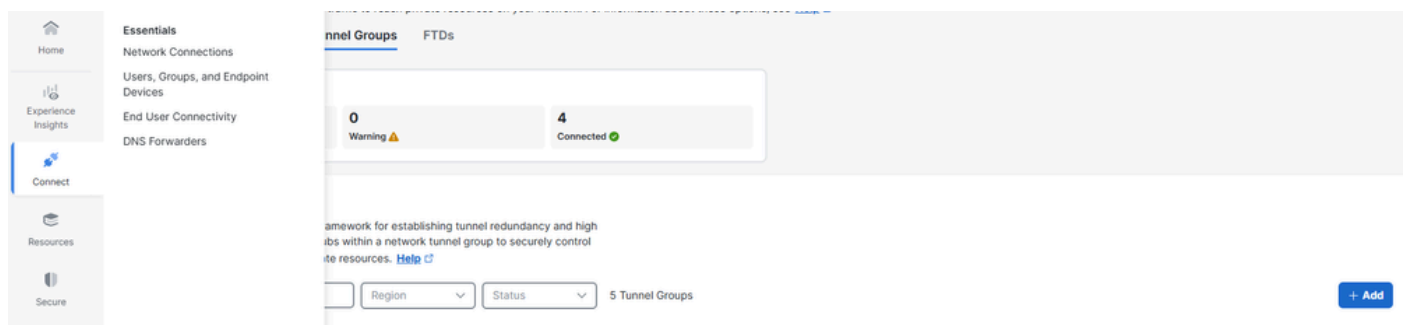
Configuración del Grupo de Túnel de Red

1. Acceda al panel de administración de [Acceso seguro](#).



2. Agregue un grupo de túnel de red.

- Haga clic en **Connect** > **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**

1 General Settings

2 Tunnel ID and Passphrase

3 Routing

4 Data for Tunnel Setup

General Settings

Give your network tunnel group a good meaningful name, choose type this tunnel group will use.

Tunnel Group Name

Region

Canada (Central) ▾

Device Type

FTD ▾

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

Tunnel ID and Passphrase

Configure the tunnel ID and pa

Tunnel ID Format

☒ Email ☐ IP Address

Tunnel ID

ftd1-ipsec

Passphrase

.....

The passphrase must be between special characters.

Confirm Passphrase

.....

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 en Add
 - Haga clic en Save

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**

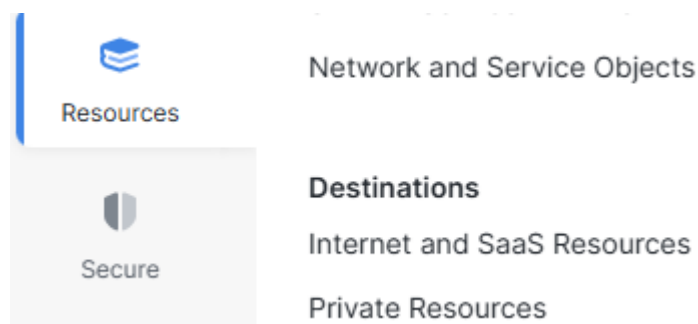
Datos NTG

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 en **Add**.



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**

Private Resource Name

Description (optional)

Private resource address

Define how the private resource will connect to applications through Secure Access.

Internally reachable address (FQDN, Wildcard FQDN, IPv4, IPv6, CIDR) ⓘ	Protocol	Port / Ranges
172.16.15.55	TCP - (HTTP/H...	8080

Recurso privado

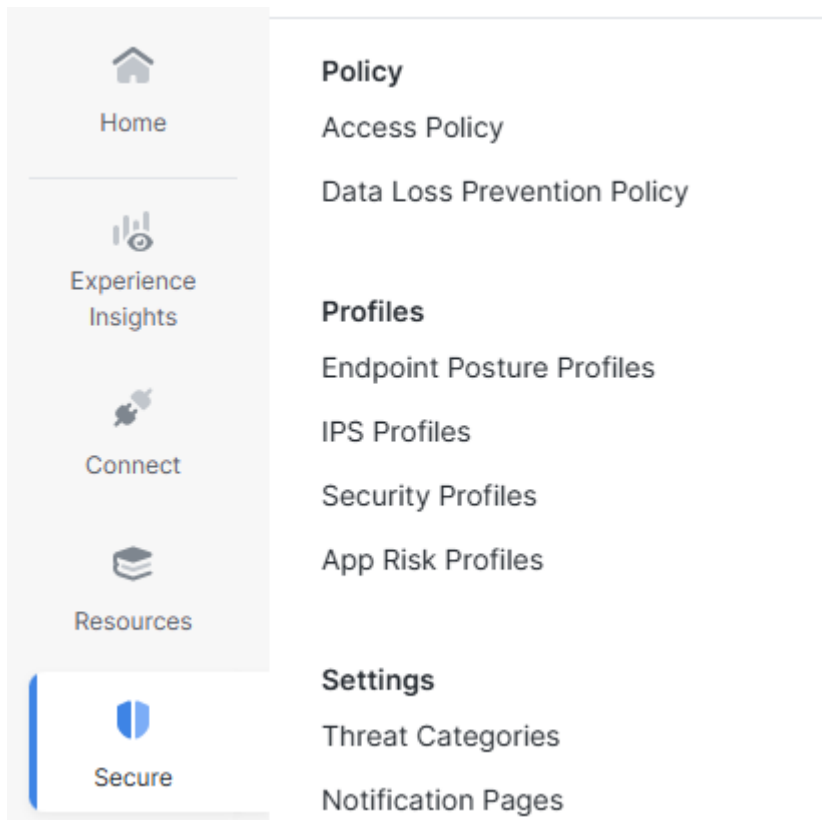
Crear una regla de directiva de acceso

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

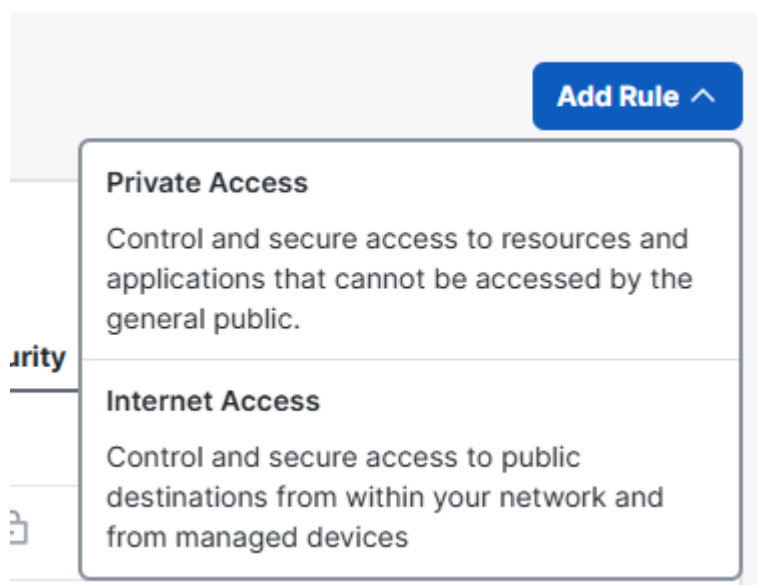
estado del dispositivo, la ubicación u otras condiciones de la directiva. Esto garantiza que los sistemas internos confidenciales permanezcan protegidos frente al acceso público general, al tiempo que se encuentran disponibles de forma segura para los usuarios autorizados a través de ZTA o VPNaaS.

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 en **Action**, seleccione **Allow** para permitir este tráfico
- Haga clic en **From** y especifique los usuarios a los que se concede permiso
- Haga clic en **To** y especifique el acceso que tienen esos usuarios según esta regla
- Haga clic en **Next** **Save** en la página siguiente

Rule name ⓘ Rule order

FTD IPsec Rule 1

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

Action

 **Allow**
Allow specified traffic if security requirements are met.

 **Block**
Block specified traffic.

From
Specify one or more sources

AD Users • Josue

To
Specify one or more destinations

Private Resources • FTD Internal Server

+ AND

Endpoint Requirements

For VPN connections:
 End-user endpoint devices that are connected to the network using VPN may be able to access destinations specified in this rule. ⓘ
Endpoint requirements are configured in the VPN posture profile. Requirements are evaluated at the time the endpoint device connects to the network. [VPN Posture Profiles](#)

For Branch connections:
 Endpoint device posture is not evaluated for endpoints connecting to these resources from a branch network.

2 Configure Security
Configure security requirements that must be met before traffic is allowed. [Help](#)

Cancel Back Next

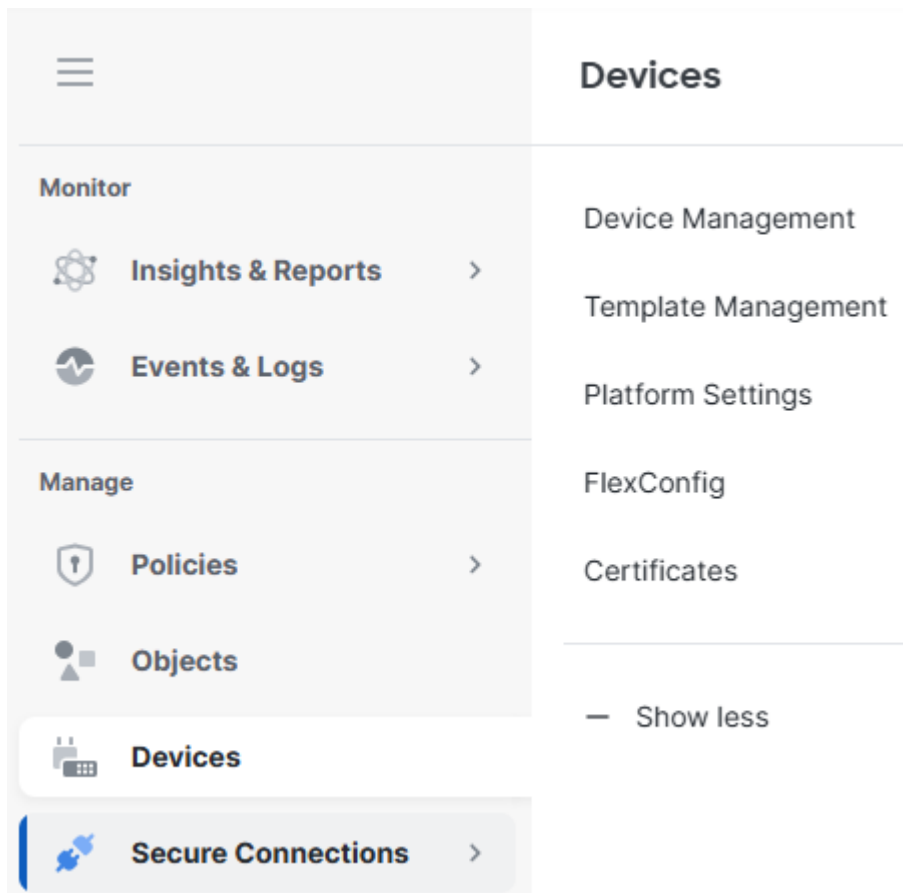
configuración de ACP

Configuración de Secure Firewall Threat Defence (FTD)

Configuración de Interfaces de Túnel Virtual

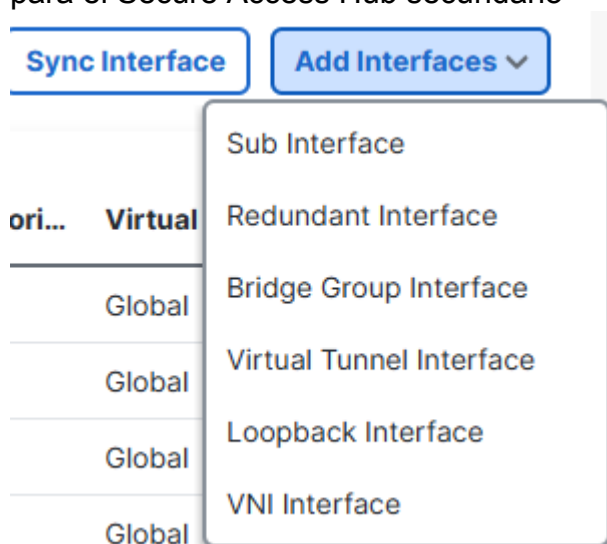
Una interfaz de túnel virtual (VTI) en FTD es una interfaz de capa 3 lógica que se utiliza para configurar túneles VPN IPsec basados en ruta.

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, seleccione IPv4
- Haga clic en IP Address y configure la dirección IP para el VTI
- Haga clic en OK

Tunnel Type

☒ Static ☐ Dynamic

Name:*

VTI-1

☒ Enabled

Description:

Security Zone:

zone_vti

Priority:

0

(0 - 65535)

Virtual Tunnel Interface Details

An interface named Tunnel<ID> is configured. Tunnel Source is a physical interface where VPN tunnel terminates for the VTI.

Tunnel ID:*

1

(0 - 10413)

Tunnel Source:*

GigabitEthernet0/0 (outside)

192.168.0.20

VTI1.1

IPsec Tunnel Details

IPsec Tunnel mode is decided by VPN traffic IP type. Configure IPv4 and IPv6 addresses accordingly.

IPsec Tunnel Mode:*

☒ IPv4 ☐ IPv6

IP Address:*

☒ Configure IP

169.254.0.1/30



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**, seleccione **IPv4**
- Haga clic en **IP Address** y configure la dirección IP para el VTI
- Haga clic en **OK**

Tunnel Type

☒ Static ☐ Dynamic

Name:*

VTI-2

☒ Enabled

Description:**Security Zone:**

zone_vti

Priority:

0

(0 - 65535)

Virtual Tunnel Interface Details

An interface named Tunnel<ID> is configured. Tunnel Source is a physical interface where VPN tunnel terminates for the VTI.

Tunnel ID:*

2

(0 - 10413)

Tunnel Source:*

GigabitEthernet0/0 (outside)

192.168.0.20

IPsec Tunnel Details

IPsec Tunnel mode is decided by VPN traffic IP type. Configure IPv4 and IPv6 addresses accordingly.

IPsec Tunnel Mode:*

☒ IPv4 ☐ IPv6

IP Address:*

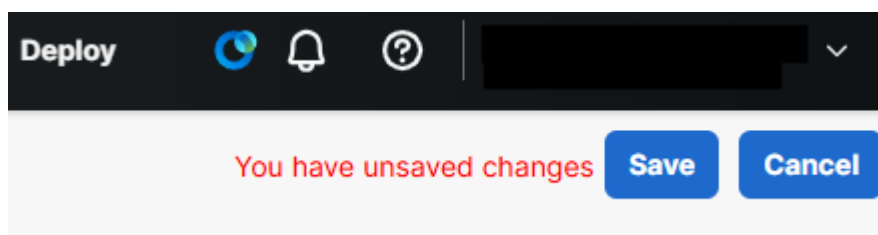
☒ Configure IP

169.254.0.5/30



VTI2.2

- Haga clic en Guardar.

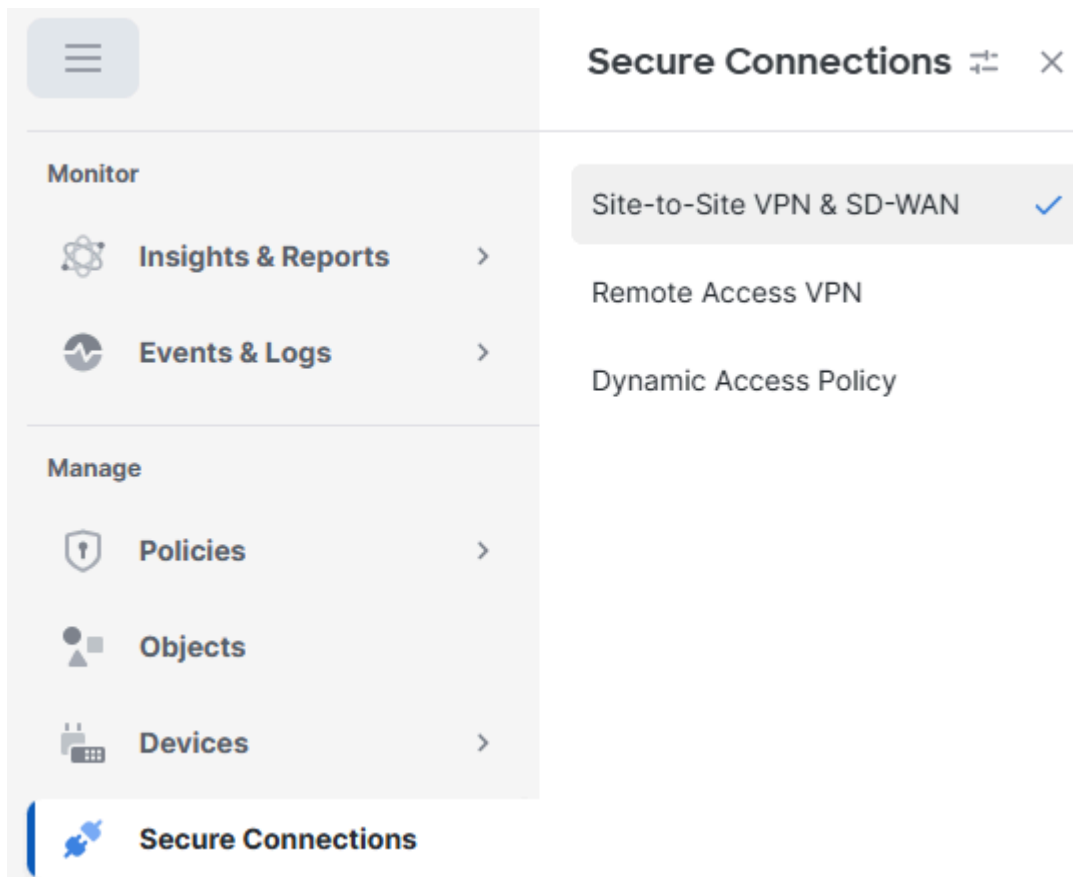


Guardar cambios VTI

Configuración del túnel IPsec

Vaya al panel de cdFMC.

- Haga clic en [Secure Connection](#) > [Site-to-Site VPN & SD-WAN](#)



S2S

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

Last Updated: 12:56 PM [Refresh](#) [NAT Exemptions](#) [Add](#)

Create VPN Topology

Topology name *
CSA

VPN Type

New

☐ SD-WAN Topology
Simplifies and automates the VPN and routing configuration in a hub and spoke topology, enabling SD-WAN capabilities.
Select VPN Topology
☐ ☒ Hub and Spoke
[Prerequisites](#)

☒ **Route-Based VPN**
Secures traffic dynamically between peers based on routing over Virtual Tunnel Interfaces.
Select VPN Topology
☐ ☒ Hub and Spoke
☒ ☐ Peer to Peer

☐ Policy-Based VPN
Secures traffic between peers based on a static policy using protected networks.
Select VPN Topology
☐ ☒ Hub and Spoke
☐ ☒ Peer to Peer
☐ ☒ Full Mesh

☐ SASE Topology
⚠ SASE Topology cannot be selected because Cisco Umbrella Connection is not configured.
[Prerequisites](#)
[Refresh](#)

[Cancel](#) [Create](#)

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 en Endpoints
 - En Node A, haga clic en Device y seleccione Extranet
 - Haga clic en Device Name y asigne un nombre
 - Haga clic en Endpoint 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 en Device y 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 en Send Local Identity to Peers option y seleccione Email ID, ingrese el ID del túnel secundario (de "Save Network Tunnel Group Configuration" en Secure Access Configuración)
 - Haga clic en Guardar

Network Topology:

IKE Version:* ☐ IKEv1 ☒ IKEv2

[Endpoints](#)
[IKE](#)
[IPsec](#)
[Advanced](#)

Node A

Device:*

Device Name*:

Endpoint IP Address*:

Node B

Device:*

Virtual Tunnel Interface:*
 +

Tunnel Source: outside (IP: 192.168.0.20) [Edit VTI](#)

☐ Tunnel Source IP is Private

☒ Send Local Identity to Peers

Local Identity Configuration*:

Backup VTI: [Remove](#)

Virtual Tunnel Interface:*
 +

Tunnel Source: outside (IP: 192.168.0.20) [Edit VTI](#)

☐ Tunnel Source IP is Private

☒ Send Local Identity to Peers

Local Identity Configuration*:

[Cancel](#)

configuración de FTD VTI

- Haga clic en **IKE**
 - Haga clic en **IKEv2 Settings** > Policies
 - Seleccione la **Umbrella-AES-GCM-256** opción
 - Haga clic en **OK**

IKEv2 Policy



Available IKEv2 Policy  +

AES-GCM-NUL-SHA

AES-GCM-NUL-SHA-LA...

AES-SHA-SHA

AES-SHA-SHA-LATEST

DES-SHA-SHA

DES-SHA-SHA-LATEST

Umbrella-AES-GCM-256

Add

Selected IKEv2 Policy

Umbrella-AES-GCM-256 

Cancel

OK

Política IKEv2

- Haga clic en Authentication Type y seleccione Pre Shared Manual Key e introduzca la PSK configurada en Secure Access (frase de paso)

Endpoints

IKE

IPsec

Advanced

Pre-shared Key Length:*

24

Characters (Range 1-127)

IKEv2 Settings

Policies:*

Umbrella-AES-GCM-256 

Authentication Type:

Pre-shared Manual Key

▼

Key:*

.....

Confirm Key:*

.....

☐

 Enforce hex-based pre-shared key only

IKE

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

EndpointsIKEIPsecAdvanced

Crypto Map Type:

☒ Static☐ Dynamic

IKEv2 Mode:

Tunnel

Transform Sets:

IKEv1 IPsec ProposalsIKEv2 IPsec Proposals*

tunnel_aes256_sha

Umbrella-AES-GCM-...

IPsec

Cancel

OK

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).

Name

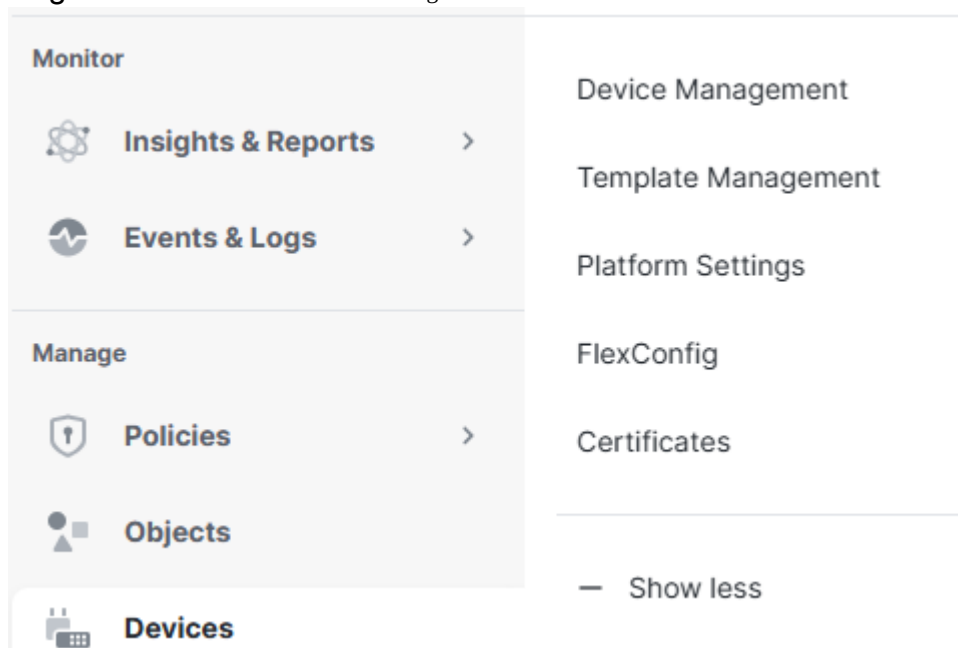
CSA_ACL

Entries (1)

Sequence	Action	Source	Source Port	Destination	Destination Port
1	 Allow	Subnet-172.16.15.0	Any	CSA-Management CSA-VPNaaS CSA-ZTA	Any

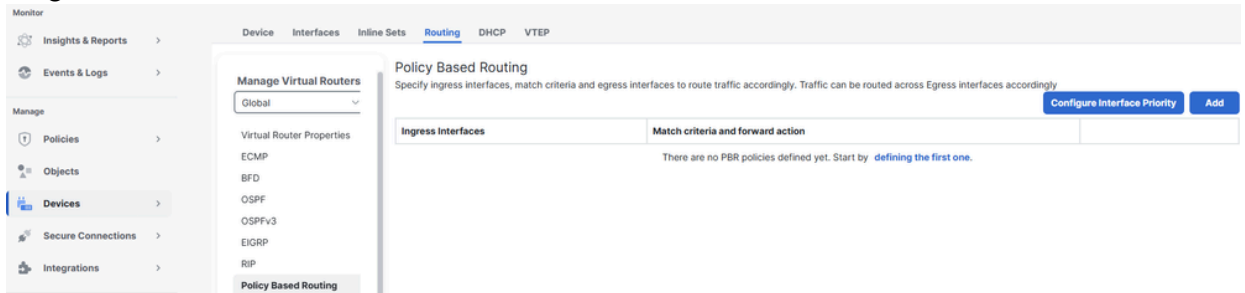
ACL

- Haga clic en **Devices** > **Device Management**



Dispositivo

- Haga clic en el FTD
 - Haga clic en Routing
 - 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

Add Policy Based Route



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

Ingress Interface *

Match Criteria and Egress Interface

Specify forward action for chosen match criteria.

Add

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

Match ACL: * CSA_ACL +

Send To: * IP Address

IPv4 Addresses: 169.254.0.2,169.254.0.6

Configuración basada en políticas

Cancel

Save

Guardar PBR

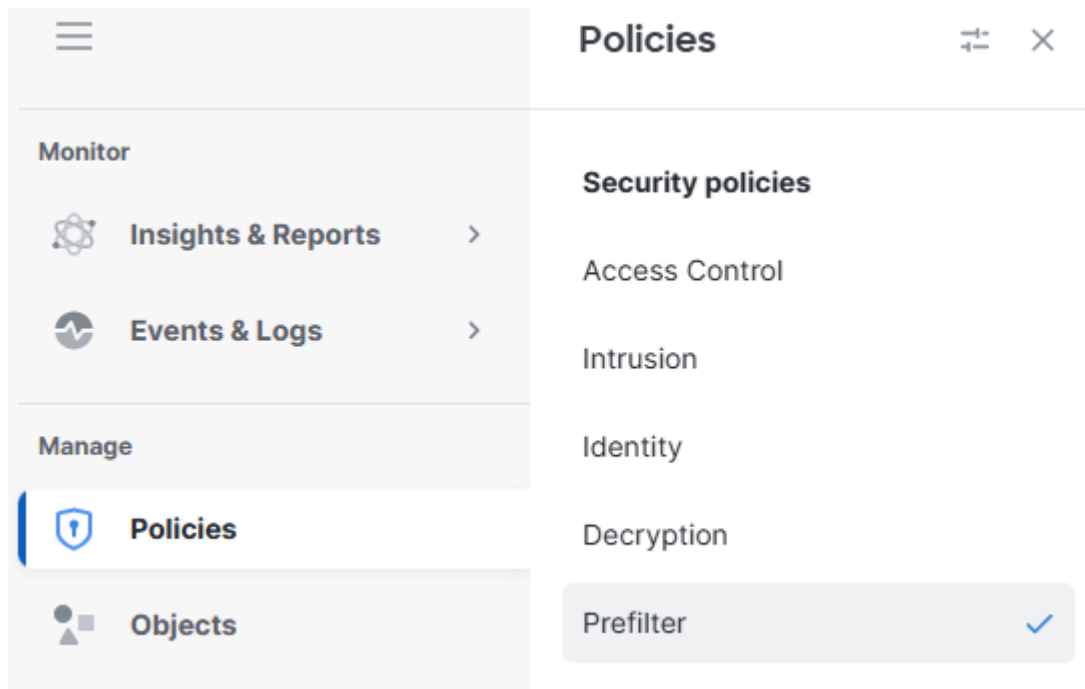
Asegúrese de seleccionar la opción **Send To > IP Address** , y no la **Egress Interface** opción.

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

Prefilter Policy				New Policy
Prefilter Policy	Domain	Last Modified		
Default Prefilter Policy Default Prefilter Policy with default action to allow all tunnels	Global	2025-07-24 08:27:51 Modified by "admin"		
PreFilter - Josue	Global	2026-02-18 15:26:37 Modified by		

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 en Save

PreFilter - Josue											
Enter Description											
Rules											
Add Tunnel Rule Add Prefilter Rule Search Rules											
#	Name	Rule Type	Source Interface Objects	Destination Interface Objects	Source Networks	Destination Networks	Source Port	Destination Port	VLAN Tag	Action	Tunnel Zone
1	CSA Rule	Prefilter	zone_vti (Routed)	zone_in (Routed)	CSA-Manager CSA-VPNaaS CSA-ZTA	Internal-Subnet Subnet-172.16.15	any	any	any	Fastpath	na

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.

Topology name	VPN Type	Network Topology	Tunnel Status Distribution	IKEv1	IKEv2
CSA	Route Based (VTI)	Point-to-Point	2+ Tunnels		✓
Node ANode B					
Device	VPN Interface	VTI Interface	Device	VPN Interface	VTI Interface
EXTRANET Extranet			FTD cdFTD-1	outside (192.168.0.20)	VTI-1 (169.254.0.1)
EXTRANET Extranet			FTD cdFTD-1	outside (192.168.0.20)	VTI-2 (169.254.0.5)

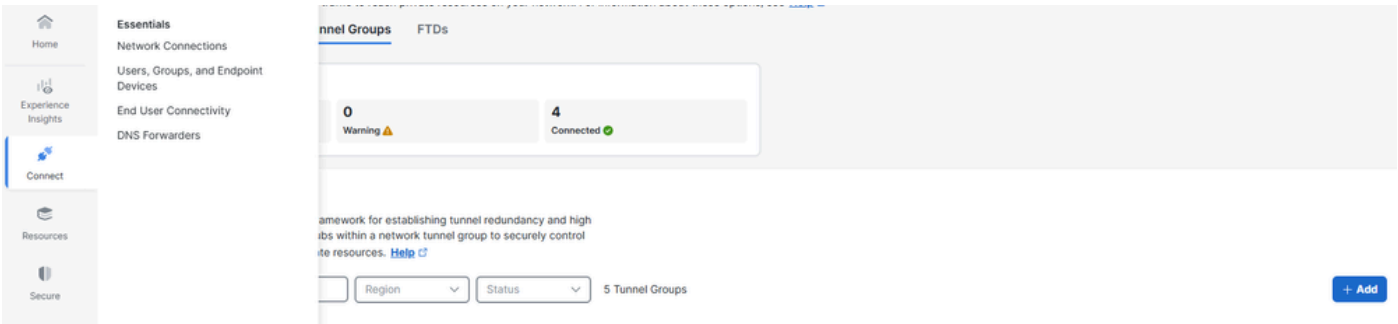
Estado del túnel FTD

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

Summary

✓ Connected

Region	Canada (Central)	Routing Type	Static Routing
Device Type	FTD	IP Address Range	172.16.15.0/24
Last Status Update	Feb 18, 2026 3:34 PM		

Primary Hub

[See Logs](#)

✓ Hub Up

1

Active Tunnels ✓

Tunnel Group ID ftd1-ipsec@

Secondary Hub

✓ Hub Up

1

Active Tunnels ✓

Tunnel Group ID

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.

Home

Experience Insights

Connect

Resources

Secure

Monitor

Monitor

Reports

Remote Access Logs

Activity Search

Connectivity Logs

Security Activity

Total Requests

Activity Volume

App Discovery

Private Resource Discovery

Top Destinations

Top Categories

Third-Party Apps

Cloud Malware

Data Loss Prevention

AI Supply Chain

Supervisar registros de conexión

FTD

All severity levels

All services

All regions

Last 24 hours

Refresh

120 results

Search Text: FTD

Reset All

Network tunnel group	Data center IP address	Hub type	Region	Alerts	Service	Device type	Details	Time (UTC)
FTD		Secondary	ca-central-1	Info	BGP	FTD	BGP peer up	Feb 18, 2026 4:07 PM
FTD		Secondary	ca-central-1	Info	IKE	FTD	Successful CHILD re...	Feb 18, 2026 4:07 PM
FTD		Primary	ca-central-1	Info	BGP	FTD	BGP peer up	Feb 18, 2026 4:06 PM
FTD		Primary	ca-central-1	Info	IKE	FTD	Successful CHILD re...	Feb 18, 2026 4:06 PM

Registros de conexión

Vaya a en Monitor > Activity Search.

Home

Experience Insights

Connect

Resources

Secure

Monitor

Monitor

×

Reports

Remote Access Logs

Activity Search

Connectivity Logs

Security Activity

Total Requests

Activity Volume

App Discovery

Private Resource Discovery

Top Destinations

Top Categories

Third-Party Apps

Cloud Malware

Data Loss Prevention

AI Supply Chain

Supervisar registros de conexión

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

13,606 Total

Page: 1 Results per page: 50 1 - 50 < >

Source	Rule Identity ⓘ	Destination	
Josue	Josue		View Full Details
Josue	Josue		Filter by Josue
Josue	Josue		Filter by
Josue	Josue		Filter by
Josue	Josue		View Rule
Josue	Josue		Edit Rule
Josue	Josue		

Detalles completos

Event Details

×

Action

Allowed

Time

Feb 18, 2026 3:30 PM

Rule Name

FTD IPsec Rule (2386307)

Enforced By

-

Source

 Josue

Source IP

-

Destination

http://172.16.15.55:8080/favicon.ico

Security Group Tag (SGT)

-

Destination IP

172.16.15.55

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).