

Configuración de Secure Access con FTD y ASA seguros para acceso privado con NAT

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Diagrama de la red](#)

[Configurar](#)

[Secure Access y Secure Firewall Threat Defense - VPN dinámica \(BGP\) basada en ruta con PBR](#)

[Routing basado en políticas FTD](#)

[Configuración de BGP en FTD](#)

[Verificar el estado del túnel](#)

[Configuración de VPN IPsec basada en ruta estática en el dispositivo de seguridad adaptable \(ASA\) con PBR](#)

[Configuración de VPN en Secure Access](#)

[Configuración de VPN en ASA](#)

[Routing basado en políticas](#)

[Verificación](#)

Introducción

Este documento describe cómo configurar Secure Access Network Tunnel Group con Network Address Translation .

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Centro de gestión de firewall de Cisco
- Cisco Secure Firewall Threat Defence
- Acceso seguro de Cisco

- Cisco Adaptive Security Appliance
- Traducción de direcciones de red
- Routing basado en políticas
- Capturas de paquetes en firewall

Componentes Utilizados

La información de este documento se basa en:

- Cisco Firewall Management Center 7.10
- Cisco Secure Firewall Threat Defence 7.10
- Acceso seguro de Cisco
- Cisco Adaptive Security Appliance 9.22
- Routers de Cisco

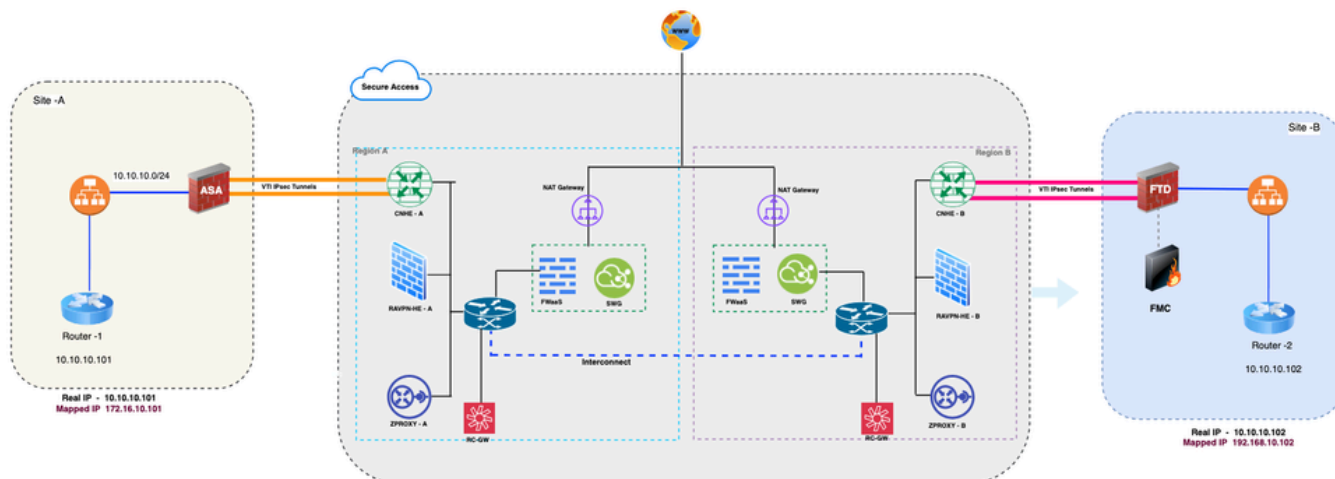
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender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

Antecedentes

Cisco Secure Access ofrece funciones Secure Service Edge nativas de la nube, como Secure Internet Access (SIA) y Secure Private Access (SPA). Para las organizaciones que amplían el acceso de aplicaciones privadas a usuarios remotos sin redirigir todo el tráfico a través de un Data Center, Secure Access utiliza los grupos de túnel de red (NTG) IPsec para crear túneles cifrados entre los dispositivos de red en las instalaciones, como Cisco Firewall Threat Defense (FTD), Adaptive Security Appliance (ASA) y los puntos de presencia (PoP) en la nube de Cisco Secure Access.

Este documento detalla cómo establecer un túnel IPsec basado en rutas usando IKEv2 entre Cisco FTD, ASA y Cisco Secure Access, permitiendo que la Traducción de direcciones de red (NAT) en Secure Access y el Ruteo basado en políticas (PBR) en el FTD y ASA dirija solamente el tráfico de acceso privado hacia el túnel.

Diagrama de la red



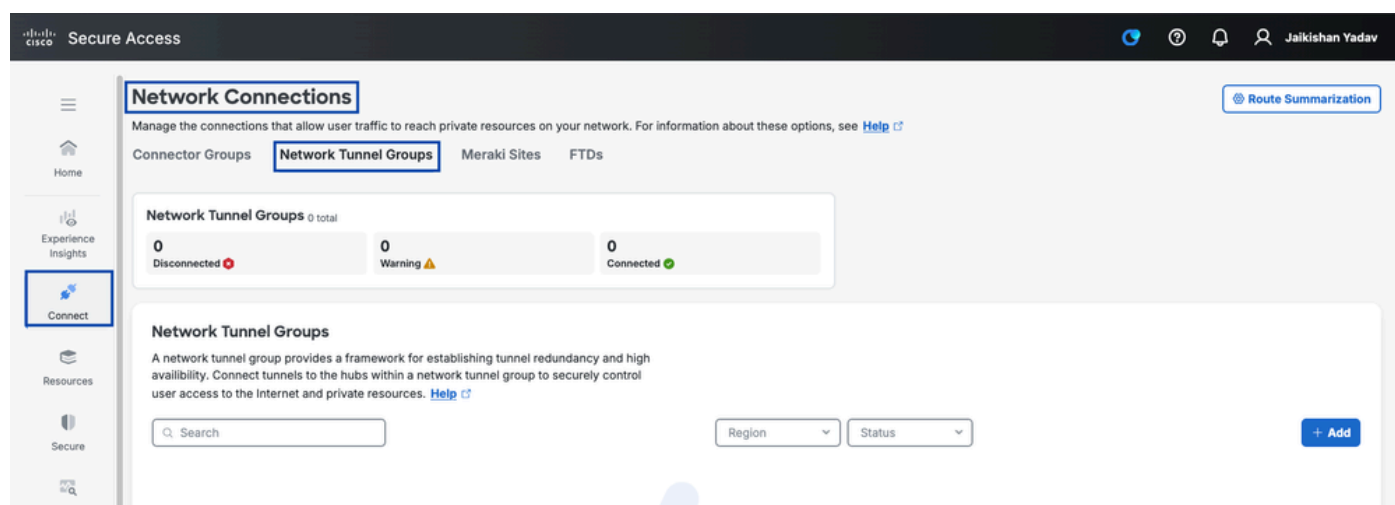
Topología de red

Configurar

Secure Access y Secure Firewall Threat Defense - VPN dinámica (BGP) basada en ruta con PBR

Configuración del Grupo de Túnel de Red en Acceso Seguro

1. Inicie sesión en el panel de acceso seguro [Acceso seguro](#)
2. Navegue hasta Connect > Network Connections > Network Tunnel Groups y haga clic en +Add para configurar el Network Tunnel Group



Acceso seguro - Grupos de túnel de red

3. Configure el Grupo de Túnel de Red: Parámetros Generales

- Configurar el nombre del grupo de túnel, la región y el tipo de dispositivo
- Haga clic en Next (Siguiente)

The screenshot shows the 'Add a Network Tunnel Group' configuration page. On the left, a sidebar lists four steps: 1. General Settings (selected with a checkmark), 2. Tunnel ID and Passphrase, 3. Routing, and 4. Data for Tunnel Setup. The main content area is titled 'General Settings' and includes instructions: 'Give your network tunnel group a good meaningful name, choose a region through which it will connect to Secure Access, and choose the device type this tunnel group will use.' Below this, there are three input fields: 'Tunnel Group Name' with the value 'FTD-BGP', 'Region' with a dropdown menu showing 'US (Pacific Northwest)', and 'Device Type' with a dropdown menu showing 'FTD'. At the bottom left is a back arrow, and at the bottom right is a 'Next' button.

Acceso seguro - Configuración general de los grupos de túnel de red

4. Configure la ID de túnel y la frase de paso.

- Configure el ID de túnel y la frase de paso.
- Haga clic en Siguiente

The screenshot shows the 'Add a Network Tunnel Group' configuration page, now on the 'Tunnel ID and Passphrase' tab. The sidebar shows the first two steps: 1. General Settings and 2. Tunnel ID and Passphrase (selected with a checkmark). The main content area is titled 'Tunnel ID and Passphrase' and includes instructions: 'Configure the tunnel ID and passphrase that devices will use to connect to this tunnel group.' Below this, there are two radio buttons for 'Tunnel ID Format': 'Email' (selected) and 'IP Address'. The 'Tunnel ID' field contains 'ftdbgpvpn' and a placeholder '@<org><hub>.sse.cisco.com'. The 'Passphrase' field is masked with dots and has a 'Show' button. Below it, a note states: 'The passphrase must be between 16 and 64 characters long. It must include at least one upper case letter, one lower case letter, one number, and cannot include any special characters.' The 'Confirm Passphrase' field is also masked with dots and has a 'Show' button. At the bottom left is a back arrow, and at the bottom right are 'Back' and 'Next' buttons.

5. Configuración del enrutamiento

- Configurar número AS del dispositivo
- Haga clic en Save (Guardar).

The screenshot displays the 'Routing' configuration page. On the left, a sidebar shows three steps: 'Tunnel ID and Passphrase', 'Routing' (selected), and 'Data for Tunnel Setup'. The main content area is titled 'Internet Protocol Version Setting for Routing'. It includes a checkbox for 'Enable IPv6 Routing in addition to IPv4', which is currently unchecked, with a note that 'IPv4 is enabled by default.' Below this is the 'Routing option' section, where 'Dynamic routing' is selected with a radio button. A description for dynamic routing states: 'Use this option when you have a BGP peer for your on-premise router.' Underneath, the 'Device AS Number' is entered as '65010' in a text field. An 'Advanced Settings' section is expanded, showing three options: 'Multihop BGP' (unchecked), 'Override BGP route summarization' (unchecked), and 'Block default route advertisement' (unchecked). At the bottom of the page, there are 'Back' and 'Save' buttons, and a 'Cancel' button is located near the bottom left.

6. Guarde la configuración del grupo de túnel de red

← Network Tunnel Groups

Add a Network Tunnel Group

Add a network tunnel group to Secure Access and enable secure network connections to the internet and private resources. Select one of your organization's available network devices to establish this network tunnel group connection. [Help](#)

✓ General Settings

✓ Tunnel ID and Passphrase

✓ Routing

✓ Data for Tunnel Setup

Data for Tunnel Setup

Review and save the following information for use when setting up your network tunnel devices. This is the only time that your passphrase is displayed.

Primary Tunnel ID:

ftdbgpvpn@

Primary Data Center IP Address:

44.228.138.150 2603:5004:13:20e::110:1

Secondary Tunnel ID:

ftdbgpvpn@

Secondary Data Center IP Address:

52.35.201.56 2603:5004:13:20c::110:1

Passphrase:

Download CSV

Done

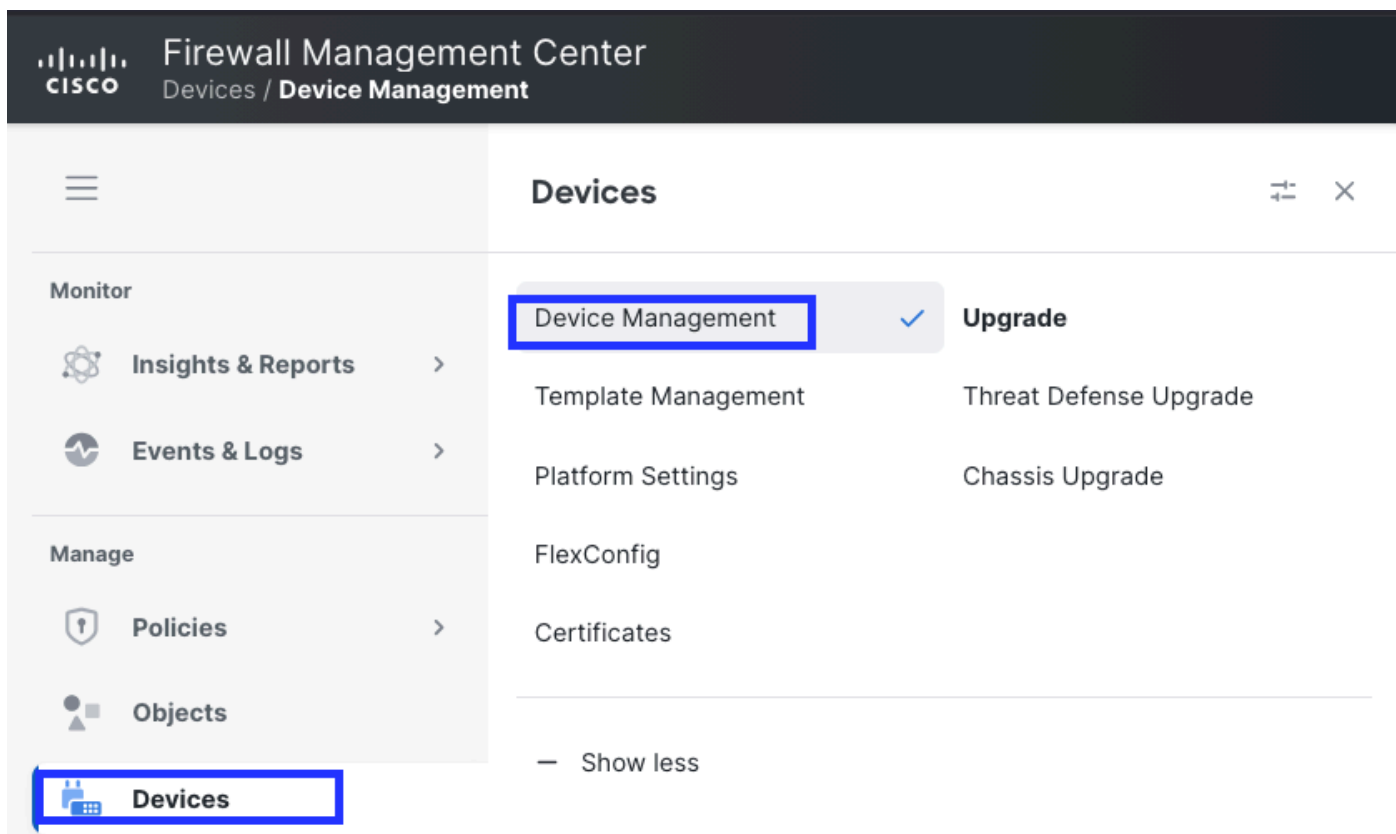
Acceso seguro - Grupos de túnel de red

Configuración de VPN IPsec basada en ruta dinámica en Secure Firewall Threat Defence (FTD) con PBR

1. Inicie sesión en Firewall Management Center (FMC)

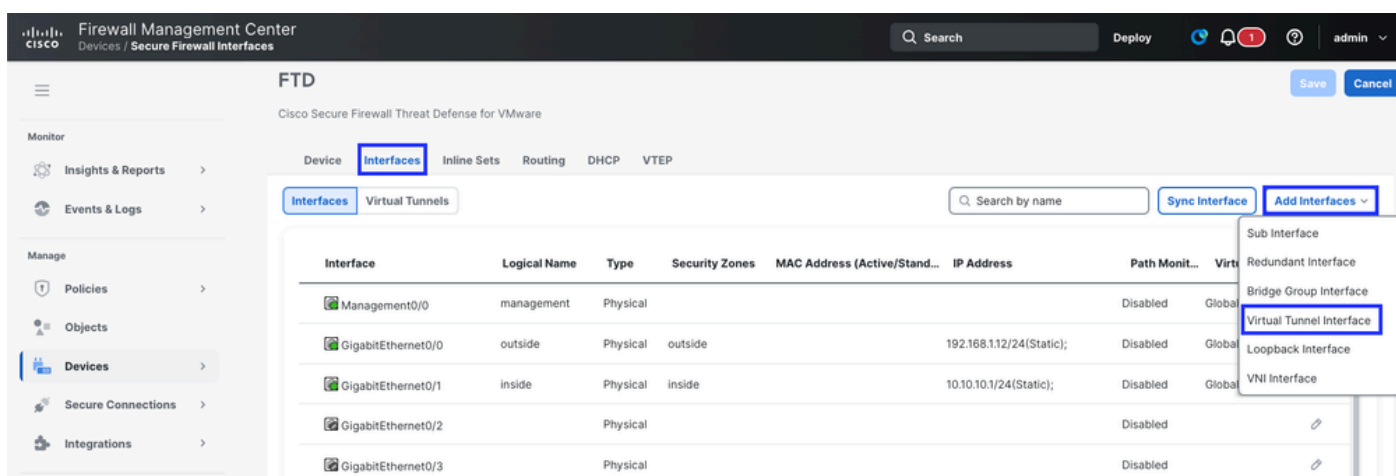
2. Configure Virtual Tunnel Interface [VTI](#)

- Vaya a Devices > Device Management .



Administración segura de firewall - Panel

- Haga clic en el icono Lápiz junto al dispositivo y navegue hasta la sección Interfaz
- Haga clic en Add interfaces y seleccione Virtual Tunnel Interface



Gestión segura de firewall - Configuración de FTD VTI

- Configuración de VTI

Add Virtual Tunnel Interface



General

Path Monitoring

Tunnel Type

☒ Static ☐ Dynamic

Name:*

VTI-1

☒ Enabled

Description:

Virtual Tunnel interface for
Primary VTI VPN

Security Zone:

vti

Priority:

0 (0 - 65535)

Propagate Security Group Tag: ☒

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)

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) 192.168.1.12

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 169.254.2.1/30
 ☐ Borrow IP (IP unnumbered) Select Interface +

Cancel

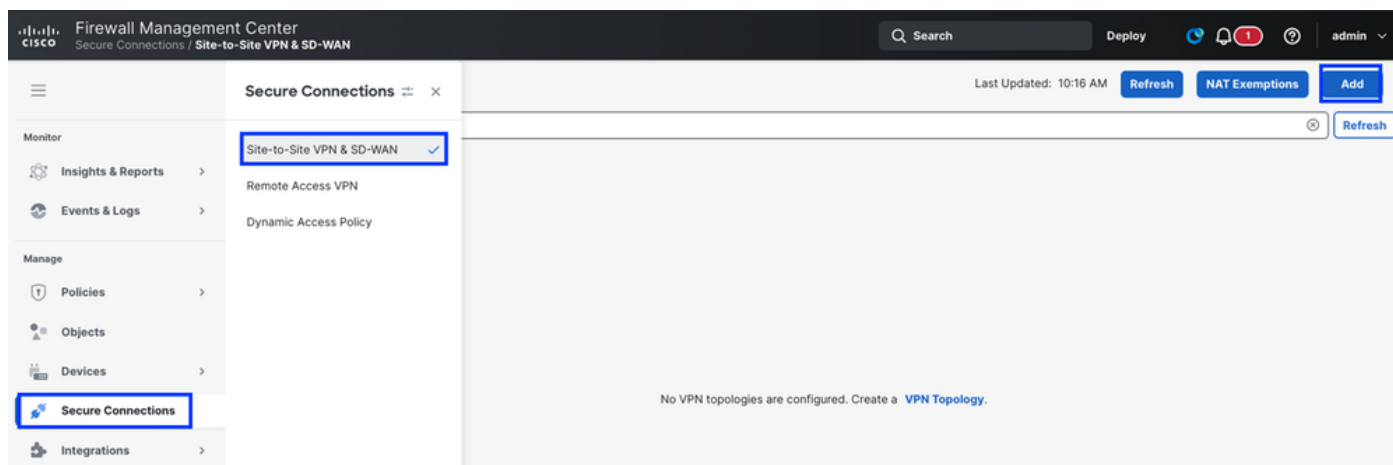
OK

Gestión segura de firewall - Configuración de FTD VTI

- Configure también VTI-2 para VPN IPsec secundaria con acceso seguro

FTD							
Cisco Secure Firewall Threat Defense for VMware							
Device Interfaces Inline Sets Routing DHCP VTEP							
Interfaces Virtual Tunnels Search by name Sync Interface Add interfaces							
Interface	Logical Name	Type	Security Zones	MAC Address (Active/Stand...	IP Address	Path Monit...	Virtual Router
Management0/0	management	Physical				Disabled	Global
GigabitEthernet0/0	outside	Physical	outside		192.168.1.12(Static);	Disabled	Global
Tunnel1	VTI-1	VTI	vti		169.254.2.1/30(Static);	Disabled	Global
Tunnel2	VTI-2	VTI	vti		169.254.2.5/30(Static);	Disabled	Global
GigabitEthernet0/1	inside	Physical	inside		10.10.10.1/24(Static);	Disabled	Global

3. Navegue hasta Conexiones seguras > VPN de sitio a sitio y SD-WAN y haga clic en Agregar para configurar la VPN



Gestión de firewall seguro - Configuración de VPN FTD

- Crear topología de VPN

Create VPN Topology ?

Topology Name *

SecureAccess-VPN-Primary

VPN Type

☐ **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](#)

Gestión de firewall seguro - Configuración de VPN FTD

- En el paso 6 de Configure Network Tunnel Group on Secure Access, obtenga los ID de túnel

y las direcciones IP para los Data Centers primarios y secundarios.

- Haga clic en Terminales
- En Nodo A, haga clic en Dispositivo y seleccione el dispositivo FTD
- Haga clic en Virtual Tunnel Interface (Interfaz de túnel virtual) y seleccione la primera interfaz VTI creada en el paso anterior
- Haga clic en la opción Send Local Identity to Peers (Enviar identidad local a pares) y seleccione Email ID (ID de correo electrónico). Introduzca el ID de túnel principal (de "Save Network Tunnel Group Configuration" (Guardar configuración de grupo de túnel de red) en Configure Network Tunnel Group on Secure Access)
- En Nodo B, haga clic en Dispositivo y seleccione Extranet
- Haga clic en Device Name (Nombre de dispositivo) y asígnele un nombre
- Haga clic en Endpoint IP Addresses (Direcciones IP de terminal) e introduzca las direcciones IP primaria y secundaria de acceso seguro separadas por una coma (en "Save Network Tunnel Group Configuration" [Guardar la configuración del grupo de túnel de red] en Configure Network Tunnel Group on Secure Access)
- Haga clic en Agregar VTI de respaldo
- Haga clic en Virtual Tunnel Interface (Interfaz de túnel virtual) y seleccione la segunda interfaz VTI creada en el paso anterior
- Haga clic en la opción Send Local Identity to Peers (Enviar identidad local a pares) y seleccione Email ID (ID de correo electrónico). Introduzca el ID de túnel secundario (de "Save Network Tunnel Group Configuration" (Guardar configuración de grupo de túnel de red) en Configure Network Tunnel Group on Secure Access)
- Haga clic en Guardar

Edit VPN Topology



Topology Name:*

SecureAccess-VPN-Primary

☐ Policy Based (Crypto Map)

☒ Route Based (VTI)

Network Topology:

Point to Point

Hub and Spoke

Full Mesh

IKE Version:*



IKEv1



IKEv2

Endpoints

IKE

IPsec

Advanced

Node A

Device:*

FTD

Virtual Tunnel Interface:*

VTI-1 (IP: 169.254.2.1)



Tunnel Source: outside (IP: 192.168.1.12) [Edit VTI](#)



Tunnel Source IP is Private



Send Local Identity to Peers

Local Identity Configuration:*

Email ID

ftdbgpvpn(

Node B

Device:*

Extranet

Device Name:*

Secure Access

Endpoint IP Address:*

44.228.138.150,52.35.201.56

Cancel

Save

FTD seguro - Configuración de terminales VPN

Edit VPN Topology



Topology Name:*

SecureAccess-VPN-Primary

☐ Policy Based (Crypto Map)

☒ Route Based (VTI)

Network Topology:

Point to Point

Hub and Spoke

Full Mesh

IKE Version:*

☐ IKEv1

☒ IKEv2

Endpoints

IKE

IPsec

Advanced

Backup VTI:

[Remove](#)

Virtual Tunnel Interface:*

VTI-2 (IP: 169.254.2.5)



Tunnel Source: outside (IP: 192.168.1.12) [Edit VTI](#)

☐ Tunnel Source IP is Private

☒ Send Local Identity to Peers

Local Identity Configuration:*

Email ID

tdbgpvpn@

22-

Additional
Configuration



Route traffic to the VTI : [Routing Policy](#)

Permit VPN traffic : [AC Policy](#)

Cancel

Save

FTD seguro - Configuración de terminales VPN

- Configure los Valores de IKEv2 según los [Parámetros IPsec Soportados](#)
 - Seleccionar políticas como Umbrella-AES-GCM-256
 - Seleccione el tipo de autenticación como clave manual precompartida

Edit VPN Topology



Topology Name:*

SecureAccess-VPN-Primary

☐ Policy Based (Crypto Map) ☒ Route Based (VTI)

Network Topology:

Point to Point

Hub and Spoke

Full Mesh

IKE Version:* ☐ IKEv1 ☒ IKEv2

Endpoints

IKE

IPsec

Advanced

IKEv2 Settings

Policies:*

Umbrella-AES-GCM-256

Authentication Type:

Pre-shared Manual Key

Key:*

.....

Confirm Key:*

.....

☐ Enforce hex-based pre-shared key only

Cancel

Save

FTD seguro: configuración IKE de VPN

- Configurar IPsec
 - Seleccione Propuestas IKEv2 IPsec como Umbrella-AES-GCM-256
 - Active PFS como select Modulus Group as 20

Edit VPN Topology



Topology Name:*

SecureAccess-VPN-Primary

☐ Policy Based (Crypto Map) ☒ Route Based (VTI)

Network Topology:

Point to Point

Hub and Spoke

Full Mesh

IKE Version:*

☐ IKEv1

☒ IKEv2

Endpoints

IKE

IPsec

Advanced

Transform Sets: IKEv1 IPsec Proposals IKEv2 IPsec Proposals*

tunnel_aes256_sha

Umbrella-AES-GCM-...

☐ Enable Security Association (SA) Strength Enforcement

☒ Enable Perfect Forward Secrecy

Modulus Group:

20

Cancel

Save

FTD seguro: configuración de VPN IPsec

- Configuración avanzada
- Haga clic en Save (Guardar).

Edit VPN Topology



Topology Name:*

SecureAccess-VPN-Primary

☐ Policy Based (Crypto Map) ☒ Route Based (VTI)

Network Topology:

Point to Point

Hub and Spoke

Full Mesh

IKE Version:*



IKEv1



IKEv2

Endpoints

IKE

IPsec

Advanced

IPsec

Tunnel

IKE Keepalive:

Enable

Threshold:

10

Seconds

(Range 10 - 3600)

Retry Interval:

2

Seconds

(Range 2 - 10)

Identity Sent to Peers:

autoOrDN

Peer Identity Validation:

Do not check

Cancel

Save

FTD seguro: configuración avanzada de VPN

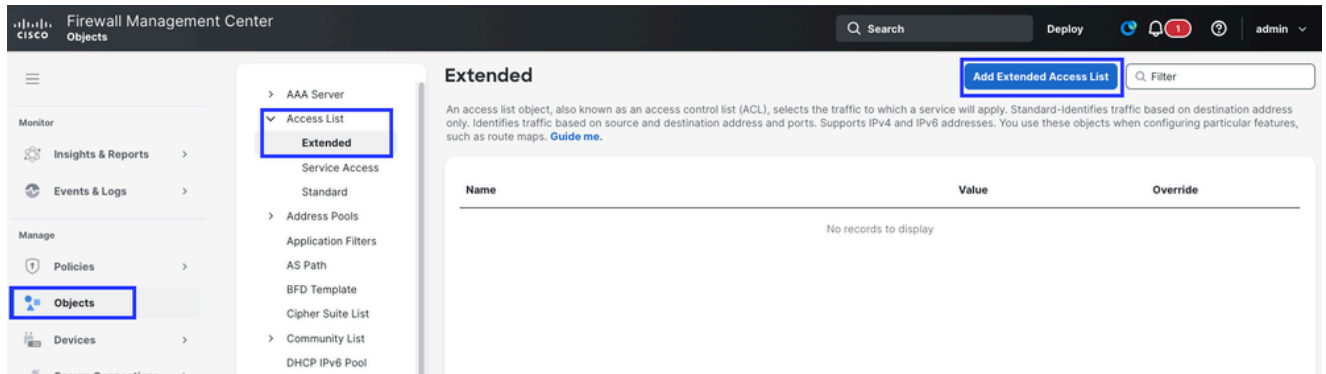
Routing basado en políticas FTD

En el ruteo tradicional, los paquetes se rutean según la dirección IP de destino. Cambiar el ruteo de tráfico específico en un sistema de ruteo basado en el destino es difícil. El routing basado en políticas (PBR) amplía y complementa los mecanismos proporcionados por los protocolos de routing, lo que le proporciona un mayor control sobre el routing.

PBR le permite establecer la precedencia IP. También le permite especificar una trayectoria para cierto tráfico, como el tráfico prioritario sobre un link de alto costo. Con PBR, puede definir el ruteo basado en criterios distintos de la red de destino, como el puerto de origen, la dirección de destino, el puerto de destino, el protocolo, las aplicaciones o una combinación de estos objetos. Para obtener más información, consulte [Ruteo Basado en Políticas](#)

1. Configurar lista de acceso

- Vaya a Objetos > Lista de acceso > Extendido
- Haga clic en Add Extended Access List .



FTD seguro: lista de acceso ampliada

- Dé el nombre de la lista de acceso
- Definir la acción
 - Permiso. - El tráfico definido se enviará al túnel IPsec
 - Bloquear: el tráfico se omitirá del túnel IPsec
 - La regla coincidirá según el número de secuencia (de menor a mayor)
 - Haga clic en Agregar
 - Haga clic en Save (Guardar).

Add Extended Access List Entry

Action: Allow

Logging: Default

Log Level: Informational

Log Interval: 300 Sec.

Network | Port | Application | Users | Security Group Tag

Available Networks +

10.10.10.0

obj_10.10.10.0

Add to Source

Add to Destination

Source Networks (1)

obj_10.10.10.0

Destination Networks (0)

any

Cancel Add

FTD seguro: lista de acceso ampliada

New Extended Access List Object

Name
PBR

Entries (1)

Sequence	Action	Source	Source Port	Destination	Destination Port	Application	Users	SGT
1	Allow	obj_10.10.10.0	Any	Any	Any	Any	Any	

Displaying 1 - 1 of 1 rows < < Page 1 of 1 > >

☐ Allow Overrides

Cancel Save

FTD seguro: lista de acceso ampliada

2. Configuración del routing basado en políticas

- Vaya a Devices > Device Management > FTD > Routing .

The screenshot shows the Cisco Firewall Management Center (FMC) interface. The top navigation bar includes the Cisco logo, 'Firewall Management Center', 'Devices / Secure Firewall Routing', a search bar, and user information. The left sidebar shows a navigation menu with 'Monitor' (Insights & Reports, Events & Logs) and 'Manage' (Policies, Objects, Devices, Secure Connections, Integrations, Troubleshooting, Administration). The 'Devices' menu item is highlighted. The main content area is titled 'FTD' and 'Cisco Secure Firewall Threat Defense for VMware'. It has tabs for 'Device', 'Interfaces', 'Inline Sets', 'Routing', 'DHCP', and 'VTEP'. The 'Routing' tab is selected. Under 'Routing', there is a 'Manage Virtual Routers' section with a dropdown menu set to 'Global'. Below this is the 'Virtual Router Properties' section. It includes fields for 'VRF Name' (Global) and 'Description' (This is a Global Virtual Router). There is a 'Select Interface' search bar. Below that are two lists: 'Available Interfaces' (outside, inside, management, VTI-1, VTI-2) and 'Selected Interfaces' (outside, VTI-1, inside, management, VTI-2). An 'Add' button is located between these two lists.

FTD seguro: routing basado en políticas

- Haga clic en Agregar
- Seleccione Interfaz de ingreso - Interfaz de ingreso para la subred que definimos en la Lista de acceso

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

There are no forward-actions defined yet. Start by [defining the first one](#).

Cancel

Save

FTD seguro: routing basado en políticas

- Definición de Criterios de Coincidencia e Interfaz de Salida
 - Haga clic en Agregar
 - Seleccione la ACL de coincidencia
 - Seleccione Enviar a como dirección IP
 - Agregue la dirección IP de próximo salto. - Las direcciones IP de la interfaz VTI son. 169.254.2.130 y 169.254.2.5/30. Por lo tanto, las direcciones IP de salto siguiente para VTI -1 y VTI-2 serían 169.254.2.2 y 169.254.2.2. 169.254.2.6, respectivamente
 - Haga clic en Guardar

Add Forwarding Actions

Match ACL: * +

Send To: *

IPv4 Addresses:

IPv6 Addresses:

Don't Fragment:

☐ Default Interface

IPv4 settings **IPv6 settings**

Recursive:

Default:

☐ Peer Address

Cancel

Save

FTD seguro: routing basado en políticas

FTD

You have unsaved changes

Save

Cancel

Cisco Secure Firewall Threat Defense for VMware

Device

Interfaces

Inline Sets

Routing

DHCP

VTEP

Manage Virtual Routers

Global

Virtual Router Properties

ECMP

BFD

OSPF

OSPFv3

EIGRP

RIP

Policy Based Routing

BGP

Policy Based Routing

Specify ingress interfaces, match criteria and egress interfaces to route traffic accordingly. Traffic can be routed across Egress interfaces accordingly

Configure Interface Priority

Add

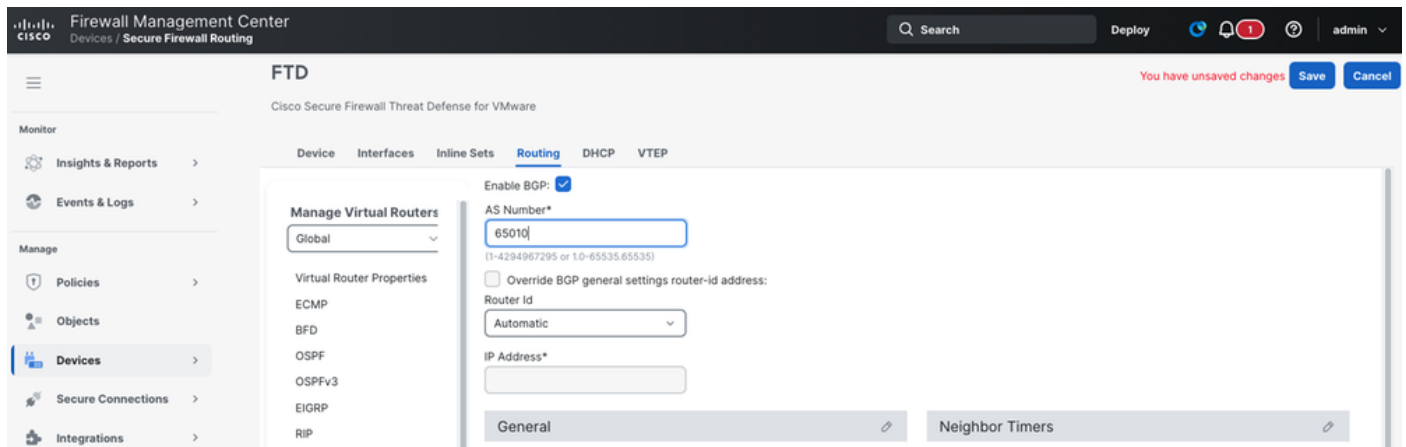
Ingress Interfaces	Match criteria and forward action	
inside	If traffic matches the Access List PBR Send through 169.254.2.2 169.254.2.6	

FTD seguro: routing basado en políticas

Configuración de BGP en FTD

1. Activar BGP

- Vaya a Devices > Device Management > FTD > Routing > General Settings > BGP
- Habilite BGP y agregue el número AS (número AS local de FTD)
- Haga clic en Save (Guardar).



FTD seguro: routing BGP

- Vaya a BGP > IPv4

2. Add BGP Neighbor - Los peers BGP Secure Access son 169.254.0.5 y 169.254.0.5.
169.254.0.9

Add Neighbor



IP Address*

169.254.0.5

Remote AS*

64512

(1-4294967295 or 1.0-65535.65535)

☒ Enabled address

☐ AS Override

☐ Shutdown administratively

☐ Configure graceful restart (failover/spanned mode)

☐ Enable graceful restart

BFD Fallover

none

Description

Update Source:

Filtering Routes

Routes

Timers

Advanced

Migration

☐ Enable Authentication

Enable Encryption

0

Password

Confirm Password

☐ Send Community attribute to this neighbor

☐ Use itself as next hop for this neighbor

☐ Disable Connection Verification

☐ Allow connections with neighbor that is not directly connected

☒ Limited number of TTL hops to neighbor

TTL Hops

254

(1-254)

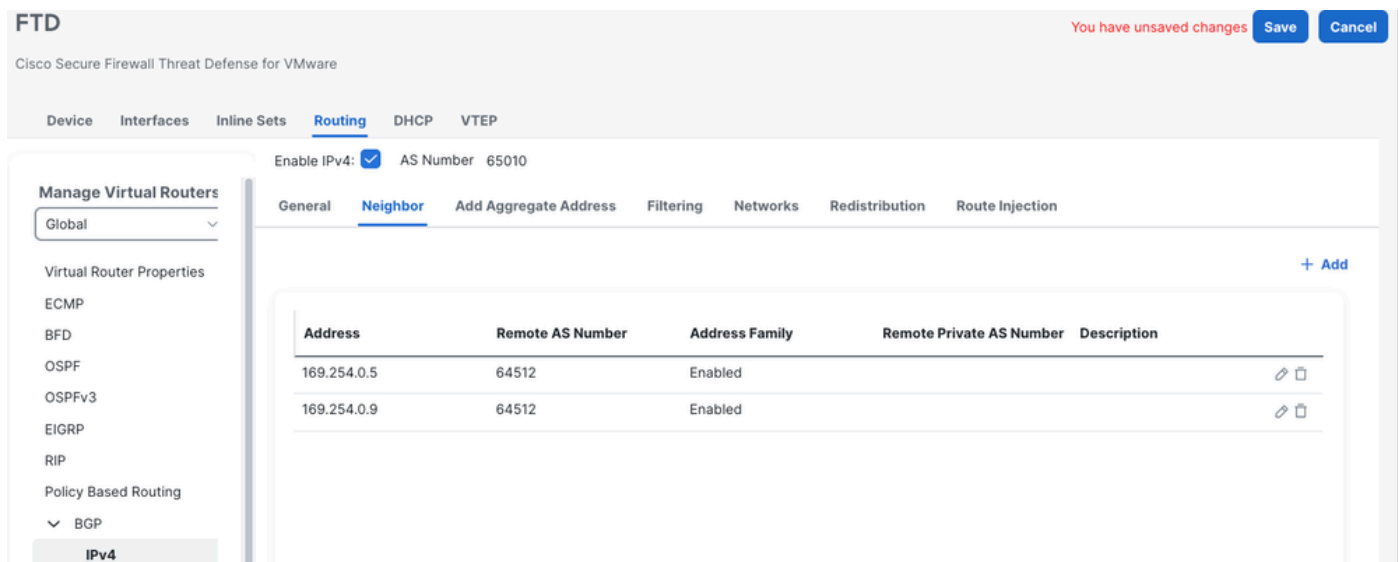
☐ Use TCP path MTU discovery

TCP Transport Mode

Cancel

OK

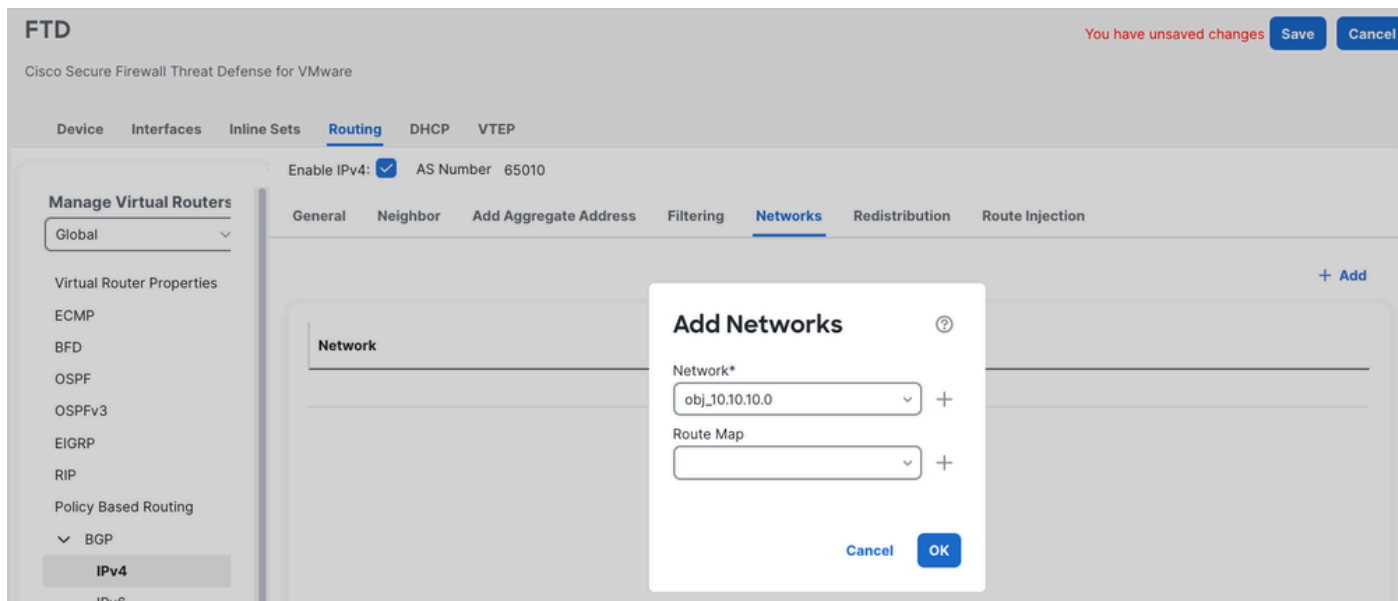
FTD seguro: routing BGP



FTD seguro: routing BGP

3. Agregue Redes: Redes que deben anunciarse a Acceso seguro.

- Haga clic en OK (Aceptar).



FTD seguro: routing BGP

- Guardar e implementar los cambios

Verificar el estado del túnel

En Secure Access

Secure Access

Network Tunnel Groups

FTD-BGP

Edit Configuration

Details for the Auto VPN tunnels added to this group are listed including which tunnel hub it is a member of.

Summary

Connected

Region

US (Pacific Northwest)

Routing Type

Dynamic Routing (BGP)

Device Type

FTD

Device BGP AS

65010

Last Status Update

Jun 08, 2026 3:53 AM

Peer (Secure Access) BGP AS

64512

BGP Peer (Secure Access) IP Addresses

169.254.0.9, 169.254.0.5, 2a04:e4c4:b:c723:b67:0000/120

Multihop BGP Addresses

—

Multihop TTL

—

Route summary subnets (0)

View advanced settings

Primary Tunnel Hub

Hub Up

1 Active Tunnels

Tunnel Group ID

ftdbgpvpn@

Data Center

sse-usw-2-1-1

IP Address

44.228.138.150 2603:5004:13:20c::110:1

Secondary Tunnel Hub

Hub Up

1 Active Tunnels

Tunnel Group ID

ftdbgpvpn@

Data Center

sse-usw-2-1-0

IP Address

52.35.201.56 2603:5004:13:20c::110:1

FTD seguro - Estado del túnel IPsec

En FMC

Firewall Management Center

Secure Connections / Site-to-Site VPN & SD-WAN

Search

Deploy

1

admin

Monitor

Insights & Reports

Events & Logs

Manage

Policies

Objects

Devices

Secure Connections

Integrations

SecureAccess-VPN

Route Based (VTI)

Point-to-Point

2 Tunnels

✓

Node A

Node B

Device	VPN Interface	VTI Interface	Device	VPN Interface	VTI Interface
EXTRANET	Extranet	44.228.138.150 (44.228...	FTD	outside (192.168.1.12)	VTI-1 (169.254.2.1)
EXTRANET	Extranet	52.35.201.56 (52.35.20...	FTD	outside (192.168.1.12)	VTI-2 (169.254.2.5)

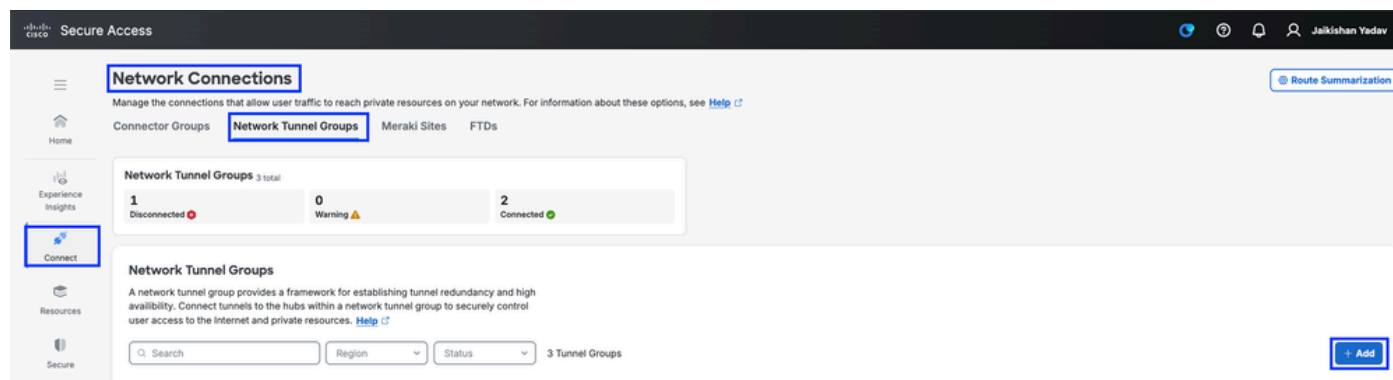
Secure FMC - Estado del túnel IPsec

Configuración de VPN IPsec basada en ruta estática en el dispositivo de seguridad adaptable (ASA) con PBR

Configuración de VPN en Secure Access

1. Inicie sesión en el panel de acceso seguro [Acceso seguro](#)
2. Navegue hasta Connect > Network Connections > Network Tunnel Groups y haga clic en +Add

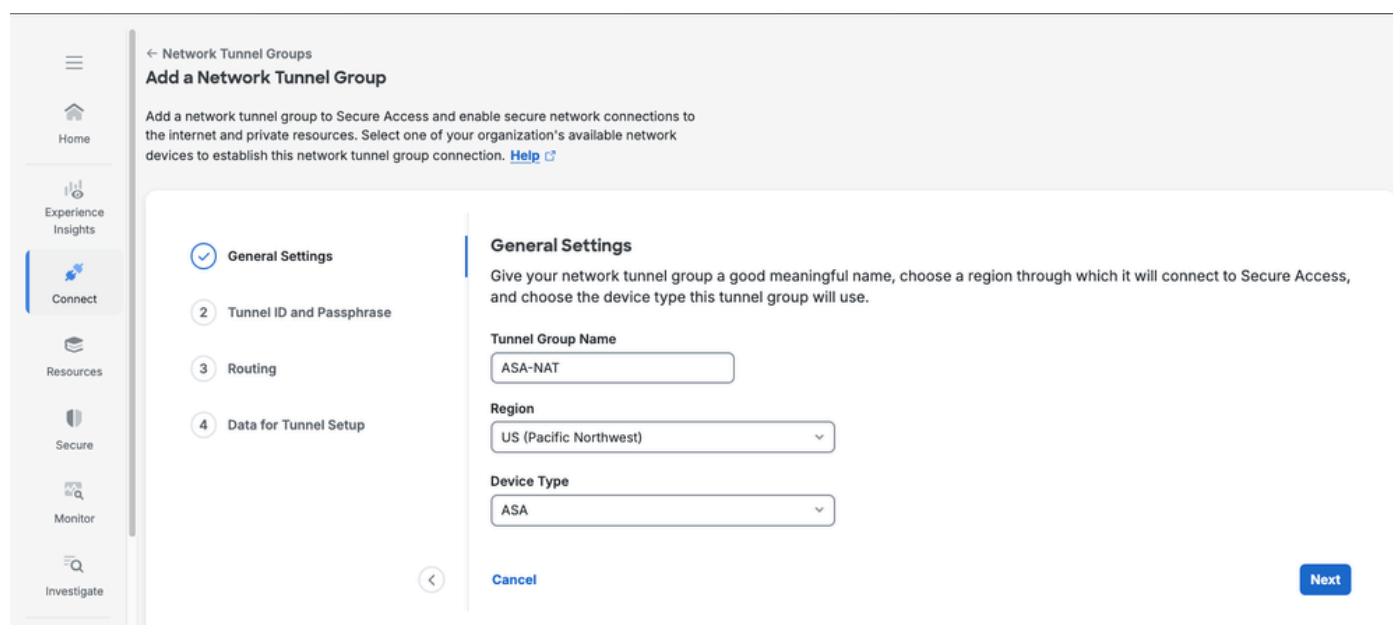
para configurar el Network Tunnel Group



Acceso seguro - Grupos de túnel de red

3. Configure el Grupo de Túnel de Red: Parámetros Generales

- Configurar el nombre del grupo de túnel, la región y el tipo de dispositivo
- Haga clic en Next (Siguiente)



Acceso seguro - Configuración general de los grupos de túnel de red

4. Configure la ID de túnel y la frase de paso.

- Configure el ID de túnel y la frase de paso.
- Haga clic en Siguiente

← Network Tunnel Groups

Add a Network Tunnel Group

Add a network tunnel group to Secure Access and enable secure network connections to the internet and private resources. Select one of your organization's available network devices to establish this network tunnel group connection. [Help](#)

Home

Experience Insights

Connect

Resources

Secure

Monitor

Investigate

Admin

General Settings

Tunnel ID and Passphrase

Routing

Data for Tunnel Setup

Tunnel ID and Passphrase

Configure the tunnel ID and passphrase that devices will use to connect to this tunnel group.

Tunnel ID Format

☒ Email ☐ IP Address

Tunnel ID

asahomevpn @<org><hub>.sse.cisco.com

Passphrase

..... [Show](#)

The passphrase must be between 16 and 64 characters long. It must include at least one upper case letter, one lower case letter, one number, and cannot include any special characters.

Confirm Passphrase

..... [Show](#)

[Cancel](#) [Back](#) [Next](#)

Acceso seguro - Grupos de túnel de red

5. Habilitar traducción de direcciones de red (NAT)

← Network Tunnel Groups

Add a Network Tunnel Group

Add a network tunnel group to Secure Access and enable secure network connections to the internet and private resources. Select one of your organization's available network devices to establish this network tunnel group connection. [Help](#)

Home

Experience Insights

Connect

Resources

Secure

Monitor

Investigate

Admin

Workflows

Return to Meraki

General Settings

Tunnel ID and Passphrase

Routing

Data for Tunnel Setup

Routing options and network overlaps

Configure routing options for this tunnel group.

☒ **Network Address Translation (NAT)**

Select to add NAT mapping configurations that resolve overlapping subnet IP address ranges, including networks with conflicting IP address spaces.

Source Mappings

Site → Secure Access

Source NAT

All source IP addresses translate to range:

100.96.0.0/16

☐ Translate to Secure Access NAT subnet

Secure Access → Site

Source NAT

Add a destination mapping to enable this rule

Destination NAT Mappings

Name	Direction	Original CIDR	Translated CIDR	...
+ Add Mappings Configure full bi-directional granular control over destination IP address translation.				

Internet Protocol Version Setting for Routing

☐ Enable IPv6 Routing in addition to IPv4

[Cancel](#) [Back](#) [Save](#)

Acceso seguro - Grupos de túnel de red Configuración de NAT

6. Agregar asignación NAT de destino

Flujo 1: del router 1 al router 2 (acceso seguro a sitios)

Flujo 2: del router 2 al router 1 (acceso seguro al sitio)

Network Tunnel Groups

Add a Network Tunnel Group

Add a network tunnel group to Secure Access and enable secure network connections to the internet and private resources. Select one of your organization's available network devices to establish this network tunnel group connection. [Help](#)

General Settings

Tunnel ID and Passphrase

Routing

Data for Tunnel Setup

Routing options and network overlaps

Configure routing options for this tunnel group.

Network Address Translation (NAT)

Select to add NAT mapping configurations that resolve overlapping subnet IP address ranges, including networks with conflicting IP address spaces.

Source Mappings

Site → Secure Access

All source IP addresses translate to range:

100.96.0.0/16

Translate to Secure Access NAT subnet

Secure Access → Site

Add a destination mapping to enable this rule

Destination NAT Mappings

Name	Direction	Original CIDR	Translated CIDR	
ASA-To-FTD	Site → Secure Access	10.10.10.102/32	192.168.10.102/32	☒

+ Add Mappings

Internet Protocol Version Setting for Routing

Enable IPv6 Routing in addition to IPv4

Acceso seguro - Grupos de túnel de red Configuración de NAT



Precaución: Cuando NAT está habilitado, BGP no es posible . Además, configure VPN estática en los dispositivos periféricos del cliente



Consejo: Recuerde siempre hacer ping a una IP traducida . La IP traducida va en el CIDR traducido y la IP real va en el CIDR original.

← Network Tunnel Groups

Add a Network Tunnel Group

Add a network tunnel group to Secure Access and enable secure network connections to the internet and private resources. Select one of your organization's available network devices to establish this network tunnel group connection. [Help](#)

General Settings

Tunnel ID and Passphrase

Routing

4 Data for Tunnel Setup

Routing options and network overlaps

Configure routing options for this tunnel group.

☒ Network Address Translation (NAT)

Select to add NAT mapping configurations that resolve overlapping subnet IP address ranges, including networks with conflicting IP address spaces.

Source Mappings

Site → Secure Access ⓘ

Source NAT

All source IP addresses translate to range:

100.96.0.0/16

☐ Translate to Secure Access NAT subnet

Secure Access → Site ⓘ

Source NAT

All source IP addresses translate to range:

100.103.255.0/24

☐ Translate to Secure Access NAT subnet

Destination NAT Mappings

Name	Direction ⓘ	Original CIDR	Translated CIDR	...
> ASA-To-FTD	Site → Secure Access	10.10.10.102/32	→ 192.168.10.102/32	ⓘ ⌵
> FTD-To-ASA	Secure Access → Site	10.10.10.101/32	→ 172.16.10.101/32	ⓘ ⌵

Rows per page 30 < 1 >

[+ Add Mappings](#)

Internet Protocol Version Setting for Routing

Cancel

Back Save

Acceso seguro - Grupos de túnel de red Configuración de NAT

Haga clic en Guardar



Consejo: Para el tráfico que va de 'Sitio A' a 'Sitio B', desde el punto de vista de CNHE-1 la dirección es 'Sitio-> SecureAccess'

Para el tráfico que va desde el 'sitio B' al 'sitio A', desde el punto de vista de CNHE-1 la dirección es 'SecureAccess -> Sitio'

Configuración de VPN en ASA

1. Inicie sesión en ASA CLI, ingrese al modo enable y verifique la conectividad IP básica hacia Internet

ASA# sh ip

Direcciones IP del sistema:

Nombre de interfaz Dirección IP Método de máscara de subred

GigabitEthernet0/0 fuera 192.168.1.40 255.255.255.0 manual

GigabitEthernet0/1 inside 10.10.10.1 255.255.255.0 manual

Direcciones IP actuales:

Nombre de interfaz Dirección IP Método de máscara de subred

GigabitEthernet0/0 fuera 192.168.1.40 255.255.255.0 manual

GigabitEthernet0/1 inside 10.10.10.1 255.255.255.0 manual

ASA# ping 8.8.8.8

Ingrese escape sequence para abortar.

Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 20/28/30 ms

ASA#

2. Configure la política IKEv2 y habilite IKEv2 en la interfaz externa

```
crypto ikev2 policy 10
encryption aes-gcm-256
integridad nula
grupo 19
lifetime seconds 86400
crypto ikev2 enable outside
```

3. Configurar la propuesta de IPSec

```
crypto ipsec ikev2 ipsec-offer Ipsec-Propuesta-primary
protocol esp encryption aes-gcm-256
```

4. Configuración del perfil IPsec

```
crypto ipsec profile csa-profile-primary
set ikev2 ipsec-offer Ipsec-posed-primary
set ikev2 local-identity email-id <primary tunnel-id>
```

5. Configure la directiva de grupo y habilite el protocolo IKEv2 en el atributo.

```
group-policy csa-policy-primary internal
group-policy csa-policy-primary attributes
vpn-tunnel-protocol ikev2
```

6. Configure el Grupo de Túnel.

```
tunnel-group 44.228.138.150 type ipsec-l2l
tunnel-group 44.228.138.150 general-attributes
default-group-policy csa-policy-primary
```

```
tunnel-group 44.228.138.150 ipsec-attributes
ikev2 remote-authentication pre-shared-key <pre-shared-key>
ikev2 local-authentication pre-shared-key <pre-shared-key>
```

7. Configuración de la interfaz de túnel virtual (VTI)

- Nameif puede ser si su elección
- La dirección IP asignada a VTI no debe solaparse con ninguna otra interfaz en el ASA
- El origen del túnel debe ser la interfaz externa del firewall
- El destino del túnel debe ser la dirección IP del Data Center

```
interface Tunnel1
nameif VTI-1
ip address 169.254.2.1 255.255.255.252
tunnel source interface outside
tunnel destination 44.228.138.150
tunnel mode ipsec ipv4
tunnel protection ipsec profile csa-profile-primary
```

8. Configure el ruteo de manera que el tráfico a la dirección IP o subred asignada se rutee dentro de la interfaz VTI. El salto siguiente debe buscar IP dentro del alcance de VTI.

```
route VTI-1 0.0.0.0 0.0.0.0 169.254.2.2 5. (para tráfico CGNAT, conjunto RAVPN o basado en Internet)
```

or

```
route VTI-1 172.16.10.101 255.255.255.255 169.254.2.2 5
```

Routing basado en políticas

1. Lista de acceso

```
access-list PBR extended permit ip 10.10.10.0 255.255.255.0 any
```

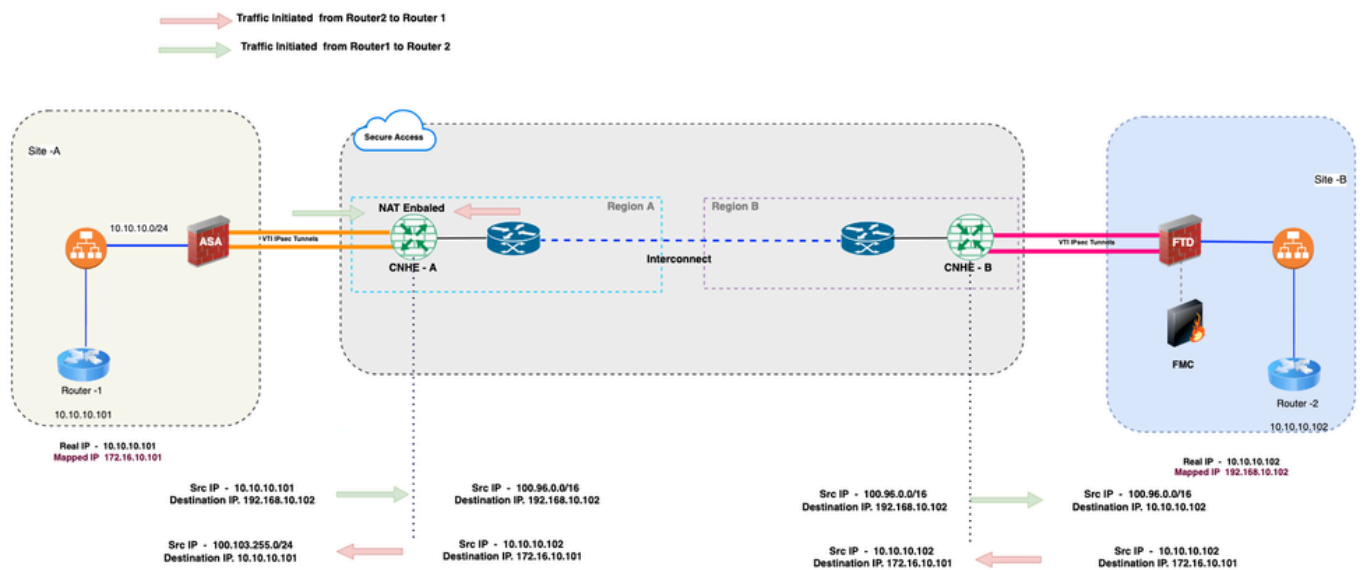
2. Mapa de ruta

```
route-map RM-CSA permit 10
match ip address PBR
set ip next-hop 169.254.2.2 169.254.2.6
```

3. Aplicar mapa de ruta en la interfaz de ingreso

```
interface GigabitEthernet0/1
nameif inside
security-level 100
IP address 10.10.10.1 255.255.255.0
policy-route route-map RM-CSA
```

Verificación



Estado de disponibilidad de GW e interfaz del router

```
Router1#show ip interface brief
Interface          IP-Address      OK? Method Status      Protocol
GigabitEthernet1   192.168.1.101   YES NVRAM    down        down
GigabitEthernet2   10.10.10.101    YES NVRAM    up          up
GigabitEthernet3   unassigned      YES NVRAM    administratively down down
GigabitEthernet9   unassigned      YES unset   administratively down down
Router1#ping 10.10.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
```

Prueba 1: Router2 —> Router1. - Prueba de ping

```

Router1#ping 192.168.10.102
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.102, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 207/211/223 ms
Router1#

```

Captura de paquetes en ASA (FW local)

```

ASA# sh capture
capture capin type raw-data trace interface inside [Capturing - 1300 bytes]
  match icmp any any
capture tunnel type raw-data trace interface vti-1 [Capturing - 1300 bytes]
  match icmp any any
capture asp type asp-drop all [Capturing - 0 bytes]
  match icmp any any
ASA#
ASA#
ASA# ter pag 20
ASA# sh cap capin

10 packets captured

  1: 10:56:45.024244      10.10.10.101 > 192.168.10.102 icmp: echo request
  2: 10:56:45.231143      192.168.10.102 > 10.10.10.101 icmp: echo reply
  3: 10:56:45.232470      10.10.10.101 > 192.168.10.102 icmp: echo request
  4: 10:56:45.441856      192.168.10.102 > 10.10.10.101 icmp: echo reply
  5: 10:56:45.443122      10.10.10.101 > 192.168.10.102 icmp: echo request
  6: 10:56:45.652477      192.168.10.102 > 10.10.10.101 icmp: echo reply
  7: 10:56:45.653423      10.10.10.101 > 192.168.10.102 icmp: echo request
  8: 10:56:45.875397      192.168.10.102 > 10.10.10.101 icmp: echo reply
  9: 10:56:45.876450      10.10.10.101 > 192.168.10.102 icmp: echo request
 10: 10:56:46.082301      192.168.10.102 > 10.10.10.101 icmp: echo reply
10 packets shown
ASA# sh cap tunnel

10 packets captured

  1: 10:56:45.024458      10.10.10.101 > 192.168.10.102 icmp: echo request
  2: 10:56:45.230914      192.168.10.102 > 10.10.10.101 icmp: echo reply
  3: 10:56:45.232516      10.10.10.101 > 192.168.10.102 icmp: echo request
  4: 10:56:45.441795      192.168.10.102 > 10.10.10.101 icmp: echo reply
  5: 10:56:45.443153      10.10.10.101 > 192.168.10.102 icmp: echo request
  6: 10:56:45.652432      192.168.10.102 > 10.10.10.101 icmp: echo reply
  7: 10:56:45.653454      10.10.10.101 > 192.168.10.102 icmp: echo request
  8: 10:56:45.875351      192.168.10.102 > 10.10.10.101 icmp: echo reply
  9: 10:56:45.876480      10.10.10.101 > 192.168.10.102 icmp: echo request
 10: 10:56:46.082240      192.168.10.102 > 10.10.10.101 icmp: echo reply
10 packets shown

```

Captura de paquetes en FTD (FW remoto)


```

ftd# sh cap
ftd# sh capture
capture vti type raw-data trace interface VTI-1 include-decrypted [Capturing - 1300 bytes]
  match icmp any any
capture capin type raw-data interface inside [Capturing - 1300 bytes]
  match icmp any any
capture asp type asp-drop all [Capturing - 0 bytes]
  match icmp any any
ftd# sh cap vti

```

10 packets captured

```

 1: 16:06:41.122292      100.96.2.0 > 10.10.10.102 icmp: echo request
 2: 16:06:41.124856      10.10.10.102 > 100.96.2.0 icmp: echo reply
 3: 16:06:41.329557      100.96.2.0 > 10.10.10.102 icmp: echo request
 4: 16:06:41.330442      10.10.10.102 > 100.96.2.0 icmp: echo reply
 5: 16:06:41.546327      100.96.2.0 > 10.10.10.102 icmp: echo request
 6: 16:06:41.547106      10.10.10.102 > 100.96.2.0 icmp: echo reply
 7: 16:06:41.752036      100.96.2.0 > 10.10.10.102 icmp: echo request
 8: 16:06:41.752814      10.10.10.102 > 100.96.2.0 icmp: echo reply
 9: 16:06:41.967891      100.96.2.0 > 10.10.10.102 icmp: echo request
10: 16:06:41.968501      10.10.10.102 > 100.96.2.0 icmp: echo reply

```

10 packets shown

```
ftd# sh cap capin
```

10 packets captured

```

 1: 16:06:41.123299      100.96.2.0 > 10.10.10.102 icmp: echo request
 2: 16:06:41.124825      10.10.10.102 > 100.96.2.0 icmp: echo reply
 3: 16:06:41.330000      100.96.2.0 > 10.10.10.102 icmp: echo request
 4: 16:06:41.330396      10.10.10.102 > 100.96.2.0 icmp: echo reply
 5: 16:06:41.546800      100.96.2.0 > 10.10.10.102 icmp: echo request
 6: 16:06:41.547090      10.10.10.102 > 100.96.2.0 icmp: echo reply
 7: 16:06:41.752448      100.96.2.0 > 10.10.10.102 icmp: echo request
 8: 16:06:41.752783      10.10.10.102 > 100.96.2.0 icmp: echo reply
 9: 16:06:41.968242      100.96.2.0 > 10.10.10.102 icmp: echo request
10: 16:06:41.968486      10.10.10.102 > 100.96.2.0 icmp: echo reply

```

10 packets shown

Prueba 2. - Router 2 —> Router 1 ping test

```

Router2#sh ip int br
Interface                IP-Address      OK? Method Status      Protocol
GigabitEthernet1         unassigned      YES NVRAM    administratively down down
GigabitEthernet2         10.10.10.102    YES NVRAM    up          up
GigabitEthernet3         unassigned      YES NVRAM    administratively down down
Router2#ping 10.10.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms

```

Captura de paquetes FTD (FW local)

```

ftd# sh capture
capture vti type raw-data trace interface VTI-1 include-decrypted [Capturing - 1300 bytes]
  match icmp any any
capture capin type raw-data interface inside [Capturing - 1300 bytes]
  match icmp any any
capture asp type asp-drop all [Capturing - 0 bytes]
  match icmp any any
ftd#
ftd#
ftd#
ftd# sh cap vti

10 packets captured

  1: 16:11:45.622450      10.10.10.102 > 172.16.10.101 icmp: echo request
  2: 16:11:45.823825      172.16.10.101 > 10.10.10.102 icmp: echo reply
  3: 16:11:45.825762      10.10.10.102 > 172.16.10.101 icmp: echo request
  4: 16:11:46.045667      172.16.10.101 > 10.10.10.102 icmp: echo reply
  5: 16:11:46.046857      10.10.10.102 > 172.16.10.101 icmp: echo request
  6: 16:11:46.252321      172.16.10.101 > 10.10.10.102 icmp: echo reply
  7: 16:11:46.253572      10.10.10.102 > 172.16.10.101 icmp: echo request
  8: 16:11:46.453803      172.16.10.101 > 10.10.10.102 icmp: echo reply
  9: 16:11:46.454764      10.10.10.102 > 172.16.10.101 icmp: echo request
 10: 16:11:46.664119      172.16.10.101 > 10.10.10.102 icmp: echo reply
10 packets shown
ftd# sh cap capin

10 packets captured

  1: 16:11:45.622083      10.10.10.102 > 172.16.10.101 icmp: echo request
  2: 16:11:45.823886      172.16.10.101 > 10.10.10.102 icmp: echo reply
  3: 16:11:45.825442      10.10.10.102 > 172.16.10.101 icmp: echo request
  4: 16:11:46.045697      172.16.10.101 > 10.10.10.102 icmp: echo reply
  5: 16:11:46.046582      10.10.10.102 > 172.16.10.101 icmp: echo request
  6: 16:11:46.252352      172.16.10.101 > 10.10.10.102 icmp: echo reply
  7: 16:11:46.253313      10.10.10.102 > 172.16.10.101 icmp: echo request
  8: 16:11:46.453849      172.16.10.101 > 10.10.10.102 icmp: echo reply
  9: 16:11:46.454596      10.10.10.102 > 172.16.10.101 icmp: echo request
 10: 16:11:46.664150      172.16.10.101 > 10.10.10.102 icmp: echo reply
10 packets shown

```

Captura de paquetes ASA (FW remoto)

```

ASA# sh capture
capture capin type raw-data trace interface inside [Capturing - 1300 bytes]
  match icmp any any
capture tunnel type raw-data trace interface vti-1 [Capturing - 1300 bytes]
  match icmp any any
capture asp type asp-drop all [Capturing - 0 bytes]
  match icmp any any
ASA# sh cap capin

10 packets captured

  1: 11:08:30.288391      100.103.255.195 > 10.10.10.101 icmp: echo request
  2: 11:08:30.289123      10.10.10.101 > 100.103.255.195 icmp: echo reply
  3: 11:08:30.504566      100.103.255.195 > 10.10.10.101 icmp: echo request
  4: 11:08:30.504963      10.10.10.101 > 100.103.255.195 icmp: echo reply
  5: 11:08:30.710992      100.103.255.195 > 10.10.10.101 icmp: echo request
  6: 11:08:30.711404      10.10.10.101 > 100.103.255.195 icmp: echo reply
  7: 11:08:30.917112      100.103.255.195 > 10.10.10.101 icmp: echo request
  8: 11:08:30.917402      10.10.10.101 > 100.103.255.195 icmp: echo reply
  9: 11:08:31.128243      100.103.255.195 > 10.10.10.101 icmp: echo request
 10: 11:08:31.128640      10.10.10.101 > 100.103.255.195 icmp: echo reply
10 packets shown
ASA# sh cap tunnel

10 packets captured

  1: 11:08:30.287964      100.103.255.195 > 10.10.10.101 icmp: echo request
  2: 11:08:30.289322      10.10.10.101 > 100.103.255.195 icmp: echo reply
  3: 11:08:30.504505      100.103.255.195 > 10.10.10.101 icmp: echo request
  4: 11:08:30.505009      10.10.10.101 > 100.103.255.195 icmp: echo reply
  5: 11:08:30.710961      100.103.255.195 > 10.10.10.101 icmp: echo request
  6: 11:08:30.711434      10.10.10.101 > 100.103.255.195 icmp: echo reply
  7: 11:08:30.917066      100.103.255.195 > 10.10.10.101 icmp: echo request
  8: 11:08:30.917417      10.10.10.101 > 100.103.255.195 icmp: echo reply
  9: 11:08:31.128197      100.103.255.195 > 10.10.10.101 icmp: echo request
 10: 11:08:31.128685      10.10.10.101 > 100.103.255.195 icmp: echo reply
10 packets shown

```

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).