

Beveiligde toegang configureren met Secure FTD en ASA voor privétoegang met NAT

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Netwerkdigram](#)

[Configureren](#)

[Veilige toegang en veilige firewall Threat Defense - Dynamic \(BGP\) routegebaseerde VPN met PBR](#)

[FTD-beleidsgebaseerde routing](#)

[BGP configureren op FTD](#)

[Tunnelstatus controleren](#)

[Statische routegebaseerde IPsec VPN configureren op Adaptive Security Appliance \(ASA\) met PBR](#)

[VPN-configuratie voor beveiligde toegang](#)

[VPN-configuratie op ASA](#)

[op beleid gebaseerde routing](#)

[Verifiëren](#)

Inleiding

In dit document wordt beschreven hoe u de Secure Access Network Tunnel Group kunt configureren met Network Address Translation.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Firewall Management Center
- Cisco Secure Firewall Threat Defense
- Cisco Secure Access

- Cisco Adaptive Security Appliance
- netwerkadresvertaling
- op beleid gebaseerde routing
- Pakketvastlegging op firewall

Gebruikte componenten

De informatie in dit document is gebaseerd op:

- Cisco Firewall Management Center 7.10
- Cisco Secure Firewall Threat Defense 7.10
- Cisco Secure Access
- Cisco Adaptive Security Appliance 9.22
- Cisco-routers

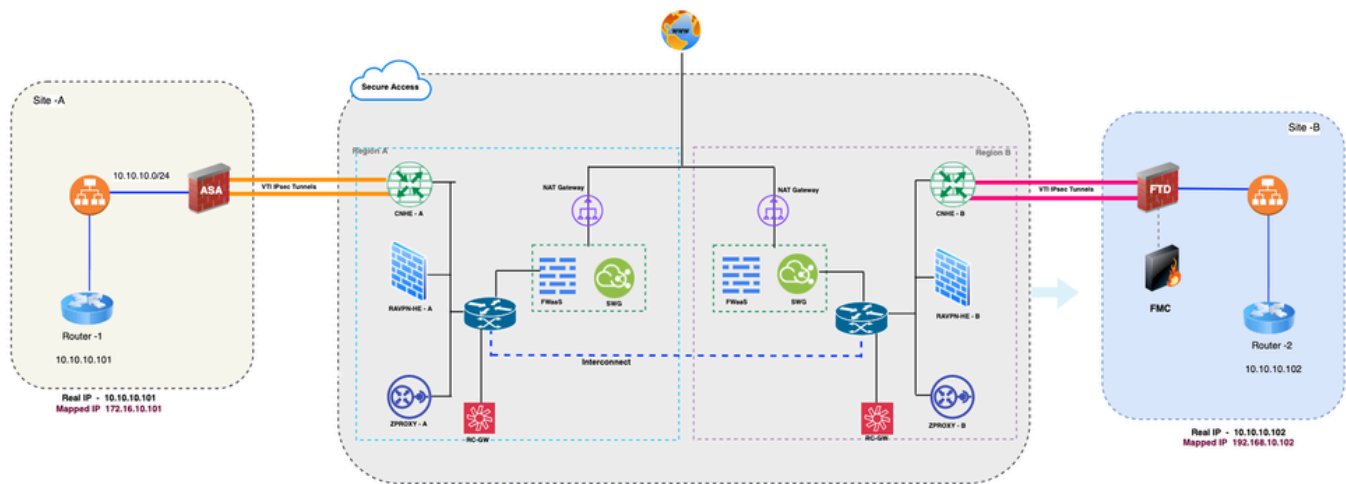
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Cisco Secure Access biedt cloud-native Secure Service Edge-mogelijkheden, waaronder Secure Internet Access (SIA) en Secure Private Access (SPA). Voor organisaties die de toegang tot privétoepassingen uitbreiden tot externe gebruikers zonder al het verkeer via een datacenter te backhalen, maakt Secure Access gebruik van IPsec Network Tunnel Groups (NTG's) om gecodeerde tunnels te maken tussen on-premises netwerkapparaten - zoals Cisco Firewall Threat Defense (FTD), Adaptive Security Appliance (ASA) en Cisco Secure Access cloud Points-of-Presence (PoP's).

In dit document wordt beschreven hoe een routegebaseerde IPsec-tunnel tot stand kan worden gebracht met behulp van IKEv2 tussen Cisco FTD, ASA en Cisco Secure Access, waardoor Network Address Translation (NAT) op Secure Access en Policy-Based Routing (PBR) op de FTD en ASA alleen privéverkeer naar de tunnel kan sturen.

Netwerkdigram



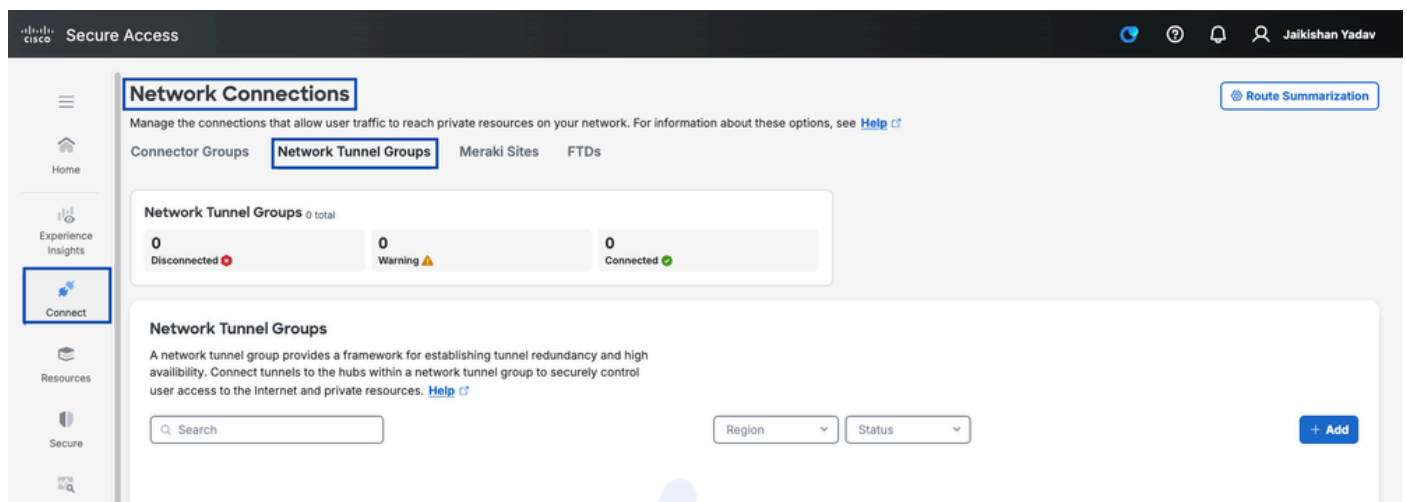
Netwerktopologie

Configureren

Veilige toegang en veilige firewall Thread Defense - Dynamic (BGP) routegebaseerde VPN met PBR

Netwerktunnelgroep configureren voor beveiligde toegang

1. Meld u aan bij het dashboard voor beveiligde toegang [Veilige toegang](#)
2. Navigeer naar Verbinden > Netwerkverbindingen > Netwerktunnelgroepen en klik op +Toevoegen om de Netwerktunnelgroep te configureren



Veilige toegang - Netwerktunnelgroepen

3. Network Tunnel Group configureren - Algemene instellingen

- Naam, regio en apparaattype van tunnelgroep configureren
- Klik op Volgende

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.

Veilige toegang - Algemene instellingen voor netwerktunnelgroepen

4. Configureer Tunnel ID en wachtwoordgroep.

- Configureer de tunnel-ID en wachtwoordgroep.
- Klik op Volgende

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 has a placeholder '@<org><hub>.sse.cisco.com'. The 'Passphrase' field is a text input with 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 another text input with a 'Show' button. At the bottom left is a back arrow, and at the bottom right are 'Back' and 'Next' buttons.

5. Routing configureren

- AS-nummer van apparaat configureren
- Klik op Opslaan

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' and includes the following sections:

- Enable IPv6 Routing in addition to IPv4:** A checkbox that is currently unchecked. Below it, a note states 'IPv4 is enabled by default.'
- Routing option:** Two radio buttons are present. 'Static routing' is unselected, and 'Dynamic routing' is selected. Below 'Dynamic routing', a note states 'Use this option when you have a BGP peer for your on - premise router.'
- Device AS Number:** A text input field containing the value '65010'.
- Advanced Settings:** A section with three checkboxes, all of which are unchecked:
 - Multihop BGP:** Select this option to enable the ability for BGP peers to establish a connection (hop) when not directly connected.
 - Override BGP route summarization:** By default, advertised routes are summarized using the configured summary subnets in the Route Summarization page. Select this option to override route summarization.
 - Block default route advertisement:** Select to block the advertisement of the default route.

At the bottom of the page, there is a 'Cancel' button on the left and 'Back' and 'Save' buttons on the right.

6. Configuratie van netwerktunnelgroep opslaan

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

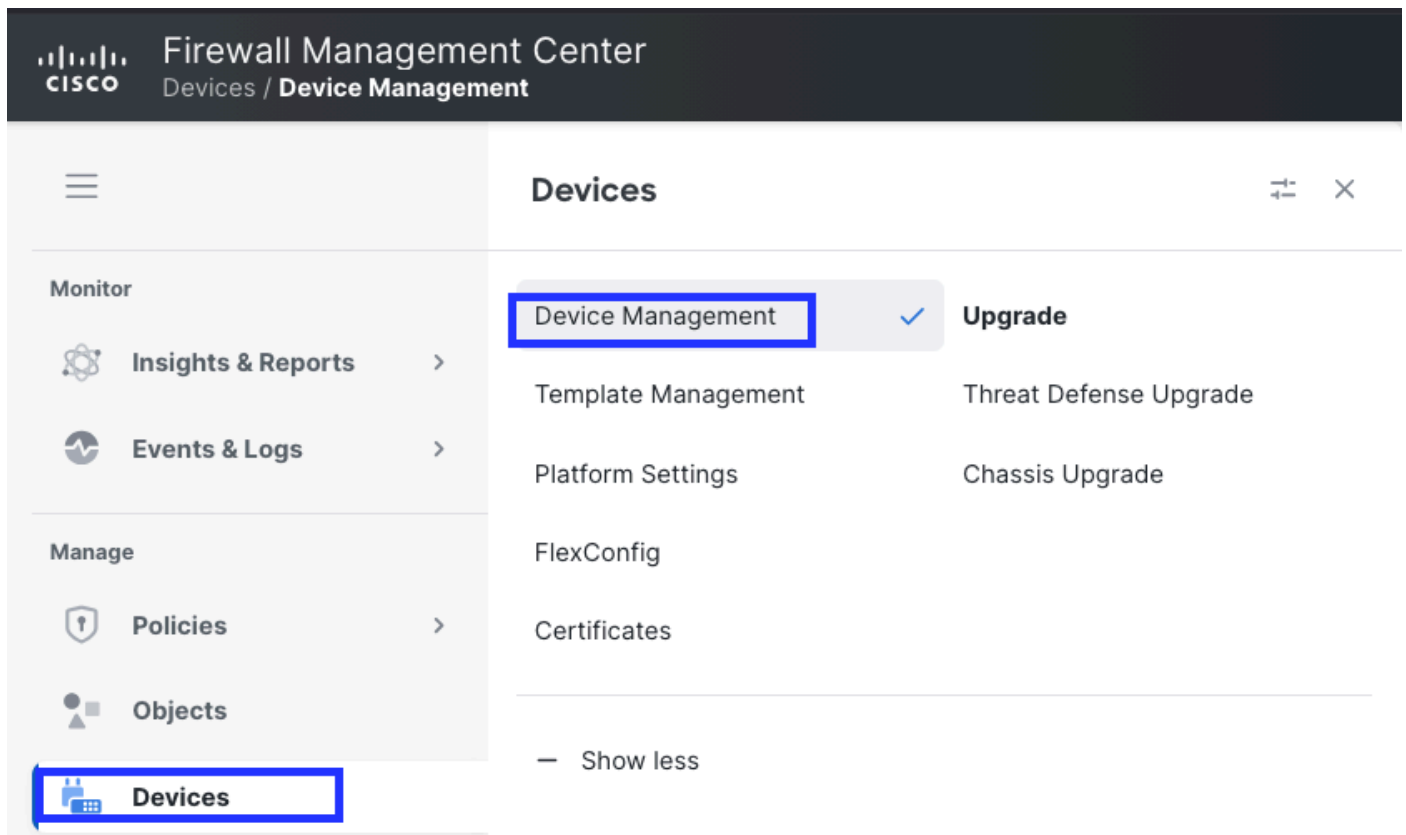
Veilige toegang - Netwerktunnelgroepen

Dynamic Route-based IPsec VPN configureren op Secure Firewall Threat Defense (FTD) met PBR

1. Aanmelden bij Firewall Management Center (FMC)

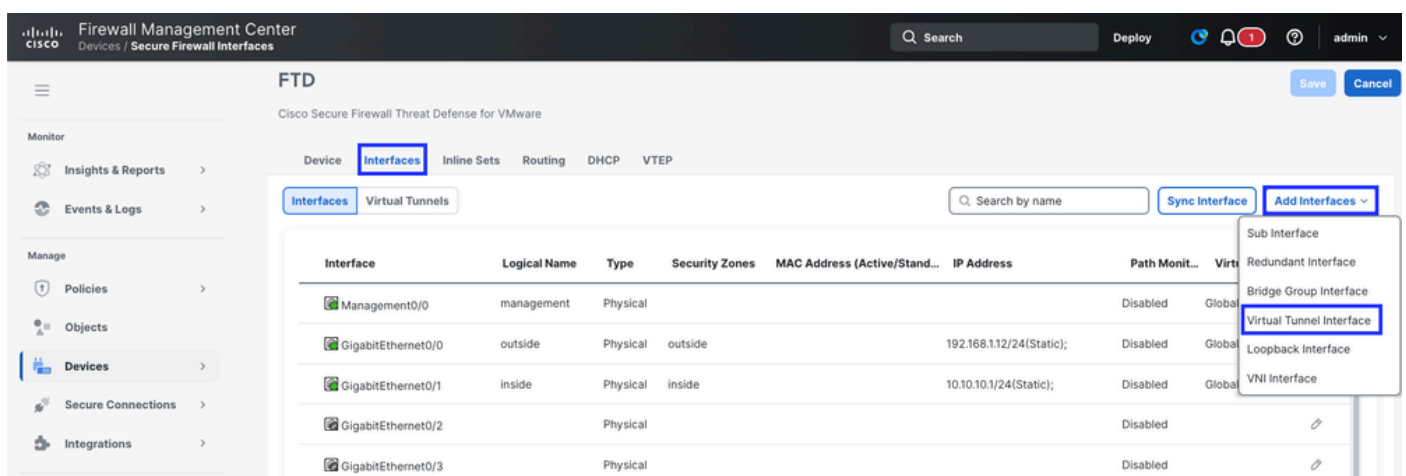
2. Virtual Tunnel Interface [VTI](#) configureren

- Navigeer naar Apparaten > Apparaatbeheer



Veilig firewallbeheer - Dashboard

- Klik op het potloodpictogram naast het apparaat en navigeer naar de sectie Interface
- Klik op Interfaces toevoegen en selecteer Virtual Tunnel Interface



Veilig firewallbeheer - FTD VTI-configuratie

- VTI configureren

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

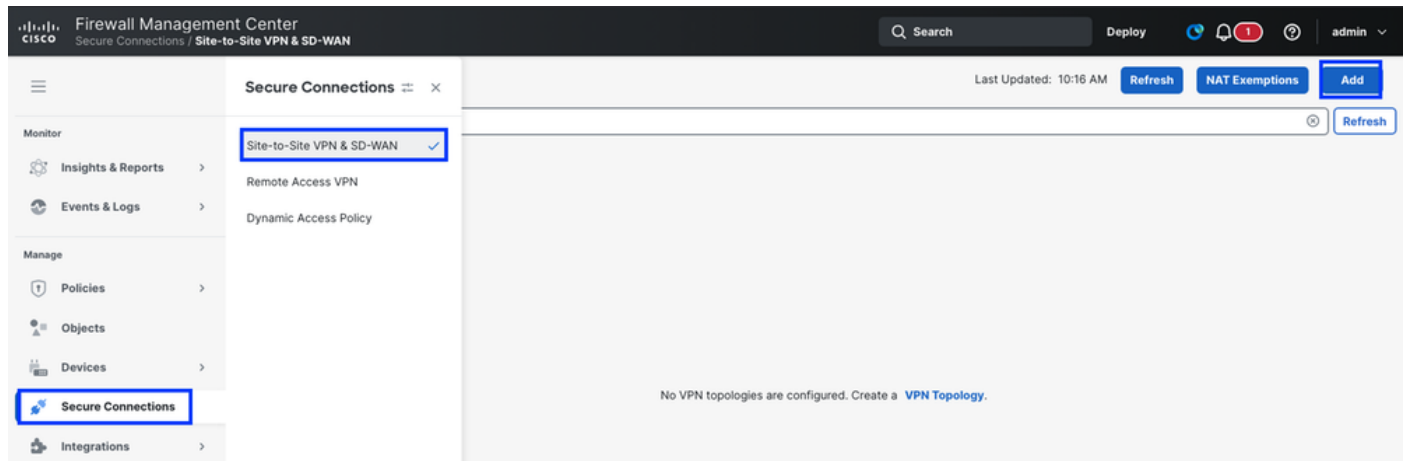
OK

Veilig firewallbeheer - FTD VTI-configuratie

- Configureer ook VTI-2 voor secundaire IPsec VPN met beveiligde toegang

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. Navigeer naar Beveiligde verbindingen > Site-to-Site VPN & SD-WAN en klik op Toevoegen om de VPN te configureren



- VPN-topologie maken

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

Warning: SASE Topology cannot be selected because Cisco Umbrella Connection is not configured.

Prerequisites

Refresh

Cancel Create

- Verkrijg vanaf stap 6 van de Configure Network Tunnel Group on Secure Access de tunnel-

ID's en IP-adressen voor de primaire en secundaire datacenters.

- Klik op Eindpunten
- Klik onder knooppunt A op Apparaat en selecteer uw FTD-apparaat
- Klik op Virtual Tunnel Interface en selecteer de eerste VTI-interface die in de vorige stap is gemaakt
- Klik op de optie Lokale identiteit naar collega's verzenden en selecteer E-mail-ID, voer de primaire tunnel-ID in (van "Configuratie netwerktunnelgroep opslaan" onder Netwerktunnelgroep configureren voor beveiligde toegang)
- Klik onder knooppunt B op Apparaat en selecteer Extranet
- Klik op Apparaatnaam en geef deze een naam
- Klik op IP-adressen van eindpunten en voer de primaire en secundaire IP-adressen voor beveiligde toegang in, gescheiden door een komma (van "Configuratie netwerktunnelgroep opslaan" onder Netwerktunnelgroep configureren voor beveiligde toegang)
- Klik op VTI voor back-up toevoegen
- Klik op Virtual Tunnel Interface en selecteer de tweede VTI-interface die in de vorige stap is gemaakt
- Klik op de optie Lokale identiteit naar collega's verzenden en selecteer E-mail-ID, voer de secundaire tunnel-ID in (van "Configuratie netwerktunnelgroep opslaan" onder Netwerktunnelgroep configureren voor beveiligde toegang)
- Klik op Opslaan

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

Veilige FTD - VPN-eindpuntconfiguratie

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

Veilige FTD - VPN-eindpuntconfiguratie

- IKEv2-instellingen configureren volgens [ondersteunde IPsec-parameters](#)
 - Selecteer Beleid als Paraplu-AES-GCM-256
 - Selecteer Verificatietype als vooraf gedeelde handmatige sleutel

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

Secure FTD - VPN IKE-instellingen

- IPsec-instellingen configureren
 - Selecteer IKEv2 IPsec-voorstellen als paraplu-AES-GCM-256
 - Inschakelen PFS als geselecteerde Modulus-groep als 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

Secure FTD - VPN IPsec-instellingen

- Geavanceerde instellingen
- Klik op Opslaan

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

Secure FTD - Geavanceerde VPN-instellingen

FTD-beleidsgebaseerde routing

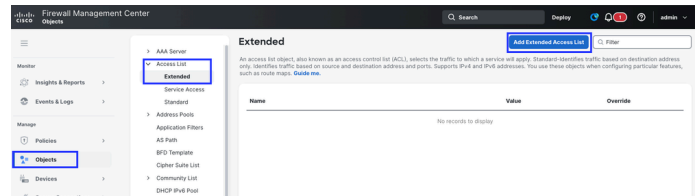
Bij traditionele routing worden pakketten gerouteerd op basis van het IP-adres van de bestemming. Het veranderen van de routing van specifiek verkeer in een op bestemming gebaseerd routingssysteem is moeilijk. Policy Based Routing (PBR) breidt de mechanismen die worden geboden door routingsprotocollen uit en vult deze aan, waardoor u meer controle hebt over routing.

Met PBR kunt u de IP-prioriteit instellen. Hiermee kunt u ook een pad opgeven voor bepaald verkeer, zoals prioriteitsverkeer via een dure link. Met PBR kunt u routing definiëren die is gebaseerd op andere criteria dan het bestemmingsnetwerk, zoals de bronpoort, het bestemmingsadres, de bestemmingspoort, het protocol, toepassingen of een combinatie van deze objecten. Raadpleeg [Beleidsgebaseerde routing voor](#) meer informatie

1. Toegangslijst configureren

- Navigeer naar Objecten > Toegangslijst > Uitgebreid

- Klik op Uitgebreide toegangslijst toevoegen



Veilige FTD - Uitgebreide toegangslijst

- Geef de naam van de toegangslijst op
- Definieer de actie
 - Toestaan. - Het gedefinieerde verkeer wordt naar de IPsec-tunnel gestuurd
 - Blokkering - Het verkeer wordt omzeild vanuit de IPsec-tunnel
 - Regel wordt gekoppeld op basis van volgnummer (van lager naar hoger)
 - Klik op Toevoegen
 - Klik op Opslaan

Add Extended Access List Entry

Action:

Logging:

Log Level:

Log Interval:
 Sec.

Network | Port | Application | Users | Security Group Tag

Available Networks

obj_10.10.10.0

Source Networks (1)

obj_10.10.10.0

Destination Networks (0)

any

Veilige FTD - Uitgebreide toegangslijst

New Extended Access List Object



Name

PBR

Entries (1)

Add

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 > > | C

☐ Allow Overrides

Cancel Save

Veilige FTD - Uitgebreide toegangslijst

2. Op beleid gebaseerde routing configureren

- Navigeer naar Apparaten > Apparaatbeheer > 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 (admin). The left sidebar contains a 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 active. Under 'Routing', there is a 'Manage Virtual Routers' section with a dropdown set to 'Global'. Below this is the 'Virtual Router Properties' section, which includes fields for 'VRF Name' (Global), 'Description' (This is a Global Virtual Router), and 'Select Interface' (Search). There 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 between the lists. The 'Policy Based Routing' option is highlighted in the left sidebar under the 'Routing' tab.

Veilige FTD - op beleid gebaseerde routing

- Klik op Toevoegen
- Selecteer Ingress Interface - Ingress-interface voor het subnet dat we in de toegangslijst hebben gedefinieerd

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

Veilige FTD - op beleid gebaseerde routing

- Overeenstemmingscriteria en uitgang-interface definiëren
 - Klik op Toevoegen
 - Selecteer de ACL-overeenkomst
 - Selecteer Verzenden naar als IP-adres
 - IP-adres voor volgende hop toevoegen. - IP-adressen van de VTI-interface worden verwijderd. 169.254.2.130 en. 169.254.2.5/30 . De volgende IP-adressen voor VTI-1 en VTI-2 zouden dus 169.254.2.2 en hoger zijn. 169 254 2,6
 - Klik op Opslaan

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

Veilige FTD - op beleid gebaseerde routing

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

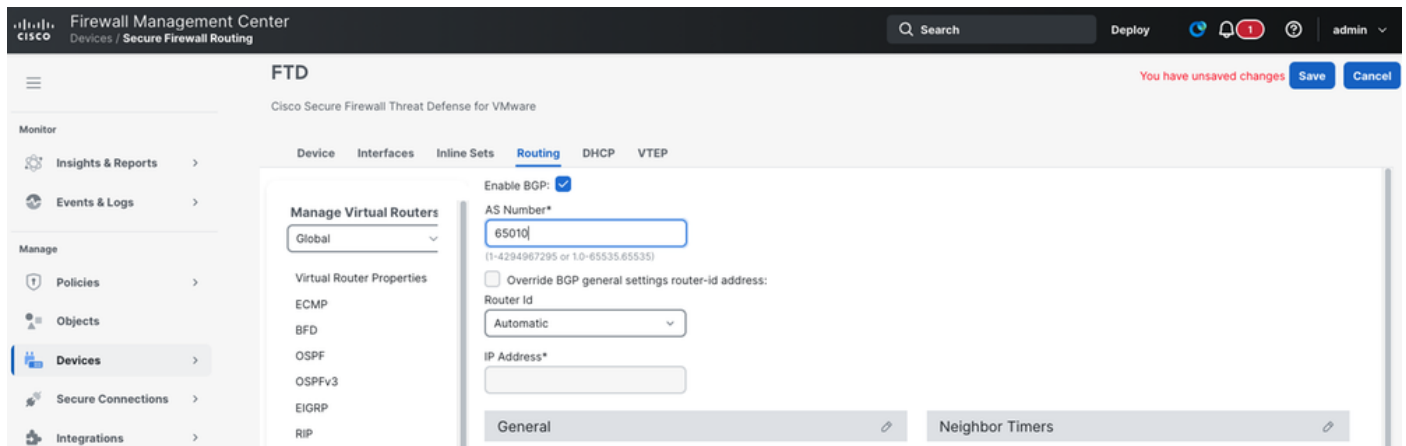
Ingress Interfaces	Match criteria and forward action	
inside	If traffic matches the Access List PBR Send through 169.254.2.2 169.254.2.6	

Veilige FTD - op beleid gebaseerde routing

BGP configureren op FTD

1. BGP inschakelen

- Navigeer naar Apparaten > Apparaatbeheer > FTD > Routing > Algemene instellingen > BGP
- BGP inschakelen en het AS-nummer toevoegen (FTD lokaal AS-nummer)
- Klik op Opslaan



Veilige FTD - BGP-routing

- Navigeer naar BGP > IPv4

2. Voeg BGP Neighbor - Secure Access BGP-peers toe: 169.254.0.5 en. 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

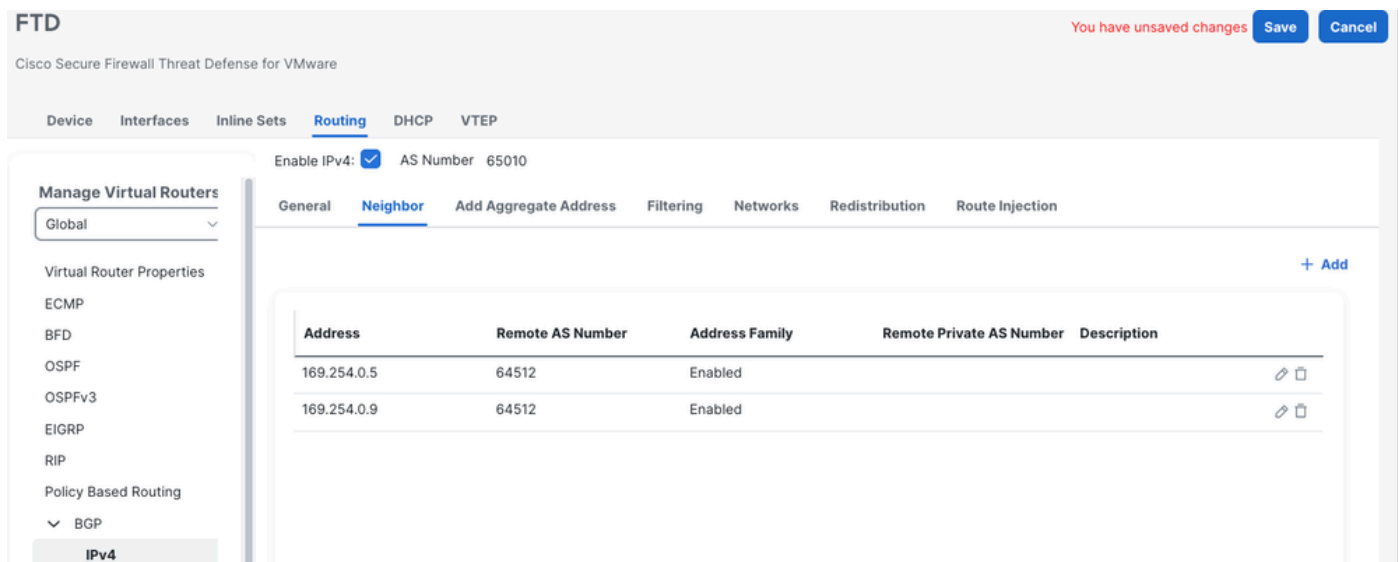
(1-254)

☐ Use TCP path MTU discovery

TCP Transport Mode

Cancel

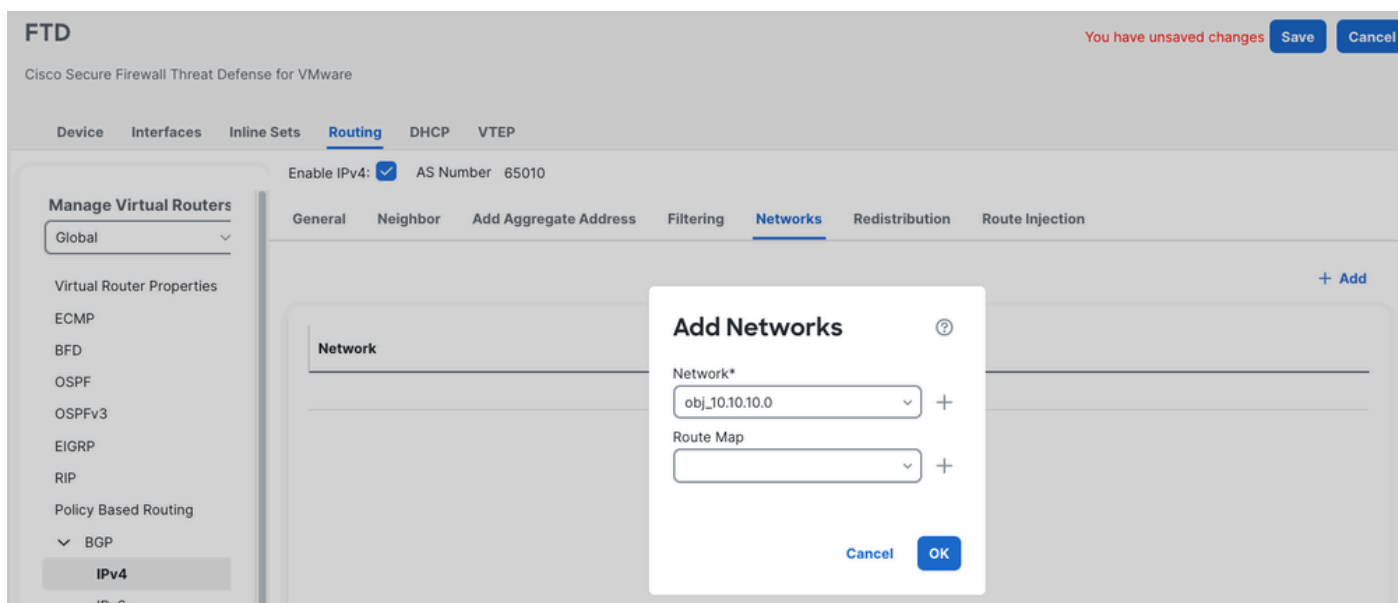
OK



Veilige FTD - BGP-routering

3. Voeg de netwerken toe - Netwerken waarvoor moet worden geadverteerd voor beveiligde toegang

- Klik op OK



Veilige FTD - BGP-routering

- De wijzigingen opslaan en implementeren

Tunnelstatus controleren

over beveiligde toegang

The screenshot shows the Cisco Secure Access interface. The main section is titled "FTD-BGP" and includes a "Summary" card with the following details:

- Region:** US (Pacific Northwest)
- Device Type:** FTD
- Last Status Update:** Jun 08, 2026 3:53 AM
- Routing Type:** Dynamic Routing (BGP)
- Device BGP AS:** 65010
- 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:** —

Below the summary, there are two sections for tunnel hubs:

- Primary Tunnel Hub:** Shows 1 Active Tunnel. Tunnel Group ID: ftdbgvpn@, Data Center: sse-usw-2-1-1, IP Address: 44.228.138.150 2603:5004:13:20e::110:1.
- Secondary Tunnel Hub:** Shows 1 Active Tunnel. Tunnel Group ID: ftdbgvpn@, Data Center: sse-usw-2-1-0, IP Address: 52.35.201.56 2603:5004:13:20c::110:1.

Veilige FTD - IPsec-tunnelstatus

Over FMC

The screenshot shows the Cisco Firewall Management Center (FMC) interface. The main section is titled "SecureAccess-VPN" and displays a table of VPN configurations:

Topology Name	VPN Type	Network Topology	Tunnel Status Distribution	IKEv1	IKEv2
SecureAccess-VPN	Route Based (VTI)	Point-to-Point	2 Tunnels	✓	

Below the table, there are two sections for Node A and Node B, each showing a table of VPN interfaces:

Device	VPN Interface	VTI Interface
EXTRANET	Extranet	44.228.138.150 (44.228.138.150)
EXTRANET	Extranet	52.35.201.56 (52.35.201.56)

Node B shows similar information for the second node.

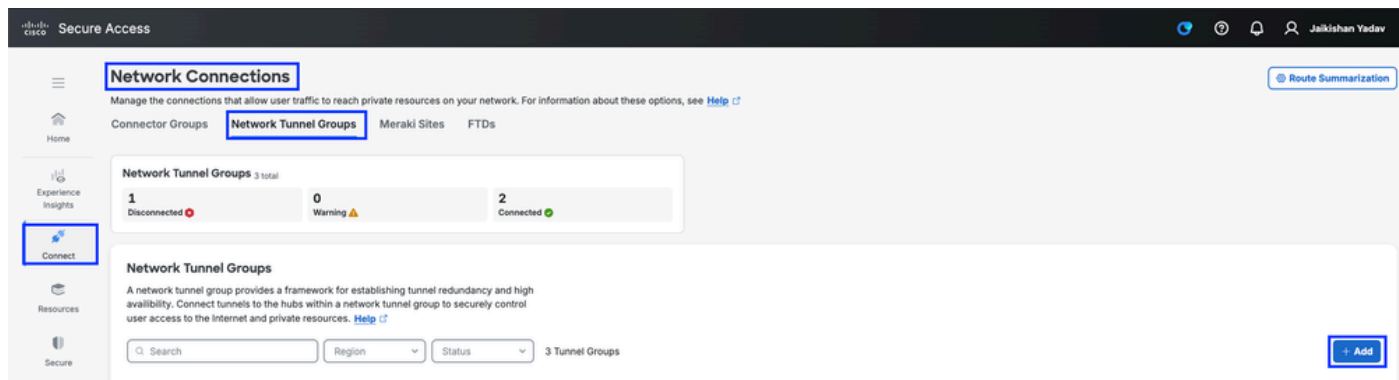
Veilige FMC - IPsec-tunnelstatus

Statische routegebaseerde IPsec VPN configureren op Adaptive Security Appliance (ASA) met PBR

VPN-configuratie voor beveiligde toegang

1. Meld u aan bij het dashboard voor beveiligde toegang [Veilige toegang](#)
2. Navigeer naar Verbinden > Netwerkverbindingen > Netwerktunnelgroepen en klik op

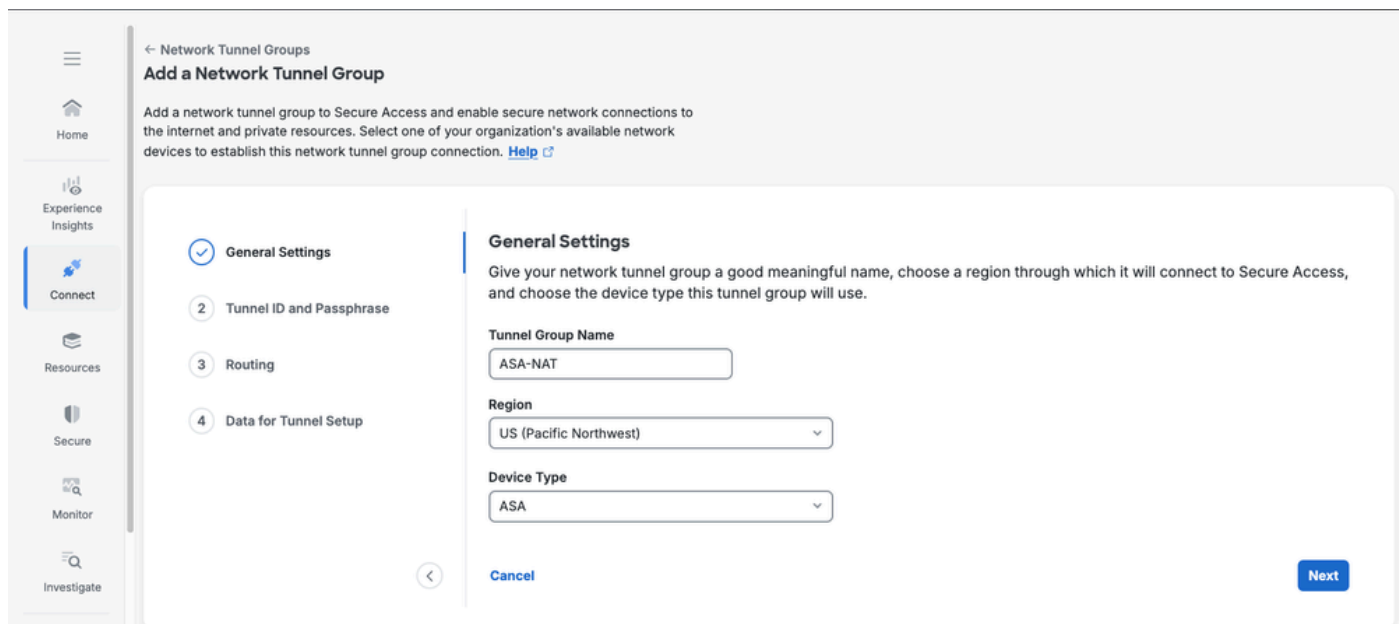
+Toevoegen om de Netwerktunnelgroep te configureren



Veilige toegang - Netwerktunnelgroepen

3. Network Tunnel Group configureren - Algemene instellingen

- Naam, regio en apparaattype van tunnelgroep configureren
- Klik op Volgende



Veilige toegang - Algemene instellingen voor netwerktunnelgroepen

4. Configureer Tunnel ID en wachtwoordgroep.

- Configureer de tunnel-ID en wachtwoordgroep.
- Klik op Volgende

← 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

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](#)

Veilige toegang - Netwerktunnelgroepen

5. Network Address Translation (NAT) inschakelen

← 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 ⓘ

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	...
Configure full bi-directional granular control over destination IP address translation. + Add Mappings				

Internet Protocol Version Setting for Routing

☐ Enable IPv6 Routing in addition to IPv4

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

Veilige toegang - NAT-instellingen voor netwerktunnelgroepen

6. Toevoeging van NAT-toewijzing van bestemming toevoegen

Flow 1 - Router 1 naar Router 2 (Site to Secure Access)

Flow 2 - Router 2 naar Router 1 (beveiligde toegang tot de site)

The screenshot shows the 'Add a Network Tunnel Group' configuration page. The left sidebar contains navigation links: Home, Experience Insights, Connect, Resources, Secure, Monitor, Investigate, Admin, Workflows, and Return to Meraki. The main content area is titled 'Routing options and network overlaps' and includes a section for 'Network Address Translation (NAT)'. Under 'Source Mappings', there are two boxes: 'Site → Secure Access' and 'Secure Access → Site'. The 'Site → Secure Access' box shows a source NAT rule with a range of 100.96.0.0/16 and a checkbox to 'Translate to Secure Access NAT subnet'. The 'Secure Access → Site' box has a message to 'Add a destination mapping to enable this rule'. Below these is a table for 'Destination NAT Mappings' with columns for Name, Direction, Original CIDR, and Translated CIDR. The table contains one entry: 'ASA-To-FTD' with direction 'Site → Secure Access', original CIDR '10.10.10.102/32', and translated CIDR '192.168.10.102/32'. At the bottom, there is a section for 'Internet Protocol Version Setting for Routing' with a checkbox to 'Enable IPv6 Routing in addition to IPv4'.

← 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
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
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

Veilige toegang - NAT-instellingen voor netwerktunnelgroepen



Let op: Wanneer NAT is ingeschakeld, is BGP niet mogelijk. Configureer ook statische VPN op Customer Edge-apparaten



Tip: vergeet nooit een vertaalde IP te pingen.
Vertaalde IP gaat in Vertaalde CIDR en echte IP gaat in Originele CIDR.

← 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

Veilige toegang - NAT-instellingen voor netwerktunnelgroepen

Klik op opslaan



Tip: Voor verkeer dat van 'Site A' naar 'Site B' gaat, is vanuit CNHE-1-oogpunt de richting 'Site-> SecureAccess'

Voor verkeer dat van 'site B' naar 'site A' gaat, is vanuit het oogpunt van CNHE-1 de richting 'SecureAccess -> Site'

VPN-configuratie op ASA

1. Meld u aan bij ASA CLI, voer de activeringsmodus in en controleer de basis-IP-connectiviteit met internet

ASA# schip

Systeem-IP-adressen:

Interface Naam IP adres Subnet masker Methode

Gigabit Ethernet0/0 buiten 192.168.1.40 255.255.255.0 handleiding

Gigabit Ethernet0/1 inside 10.10.10.1 255.255.255.0 handleiding

Huidige IP-adressen:

Interface Naam IP adres Subnet masker Methode

Gigabit Ethernet0/0 buiten 192.168.1.40 255.255.255.0 handleiding

Gigabit Ethernet0/1 inside 10.10.10.1 255.255.255.0 handleiding

ASA# ping 8.8.8.8

Typ escape sequence om af te breken.

De time-out is 2 seconden bij het verzenden van 5, 100-byte ICMP Echo's naar 8.8.8.8:

Ja!!!!

Succespercentage is 100 procent (5/5), retourvlucht min/avg/max = 20/28/30 ms

ASA#

2. IKEv2-beleid configureren en IKEv2 inschakelen op de externe interface

Crypto IKEV2-beleid 10

Codering AES-GCM-256

integriteit null

Groep 19

Levensduur seconden 86400

Crypto IKEV2 inschakelen buiten

3. IPSec-voorstel configureren

crypto ipsec ikev2 ipsec-proposal Ipsec-Proposal-primary

Protocol ESP-codering AES-GCM-256

4. IPsec-profiel configureren

Crypto IPSEC-profiel CSA-profiel-primair

set ikev2 ipsec-proposal Ipsec-Proposal-primary

IKEV2 Local-Identity Email-ID <Primary Tunnel-ID> instellen

5. Configureer groepsbeleid en schakel het IKEv2-protocol in onder attribuut.

Groepsbeleid-CSA-beleid-Primair intern

Groepsbeleid-CSA-beleid-primaire kenmerken

VPN-tunnel-protocol IKEV2

6. Tunnelgroep configureren.

tunnelgroep 44.228.138.150 type IPSec-L2L

tunnelgroep 44.228.138.150 algemene kenmerken

default-group-policy-csa-policy-primary

Tunnel-Group 44.228.138.150 IPSec-attributen

IKEV2-verificatie op afstand, vooraf gedeelde sleutel <pre-shared-key>

IKEV2 Local-Authentication Pre-Shared-Key <Pre-Shared-Key>

7. Virtual Tunnel Interface (VTI) configureren

- Naamgeving kan zijn als uw keuze
- Het IP-adres dat aan VTI is toegewezen, mag niet overlappen met een andere interface op de ASA
- De tunnelbron moet de buiteninterface van de firewall zijn
- De bestemming van de tunnel moet het IP-adres van het datacenter zijn

Tunnel-interface1

naam VTI-1

IP-adres 169.254.2.1 255.255.255.252

tunnelbroninterface buiten

Tunnelbestemming 44.228.138.150

tunnelmodus ipsec ipv4

Tunnel Protection IPSec Profile CSA-Profile-Primary

8. Configureer de routing zodanig dat het verkeer naar het toegewezen IP-adres of subnet binnen de VTI-interface wordt gerouteerd. De volgende hop moet worden uitgevoerd via IP binnen het bereik van VTI.

route VTI-1 0.0.0.0.0.0.0.0 169.254.2.2 5. (voor internetgebaseerd, RAVPN-pool- of CGNAT-verkeer

of

Route VTI-1 172.16.10.101 255.255.255.255 169.254.2.2 5

op beleid gebaseerde routing

1. Toegangslijst

toegangslijst PBR verlengde vergunning ip 10.10.10.0 255.255.255.0 elke

2. Routekaart

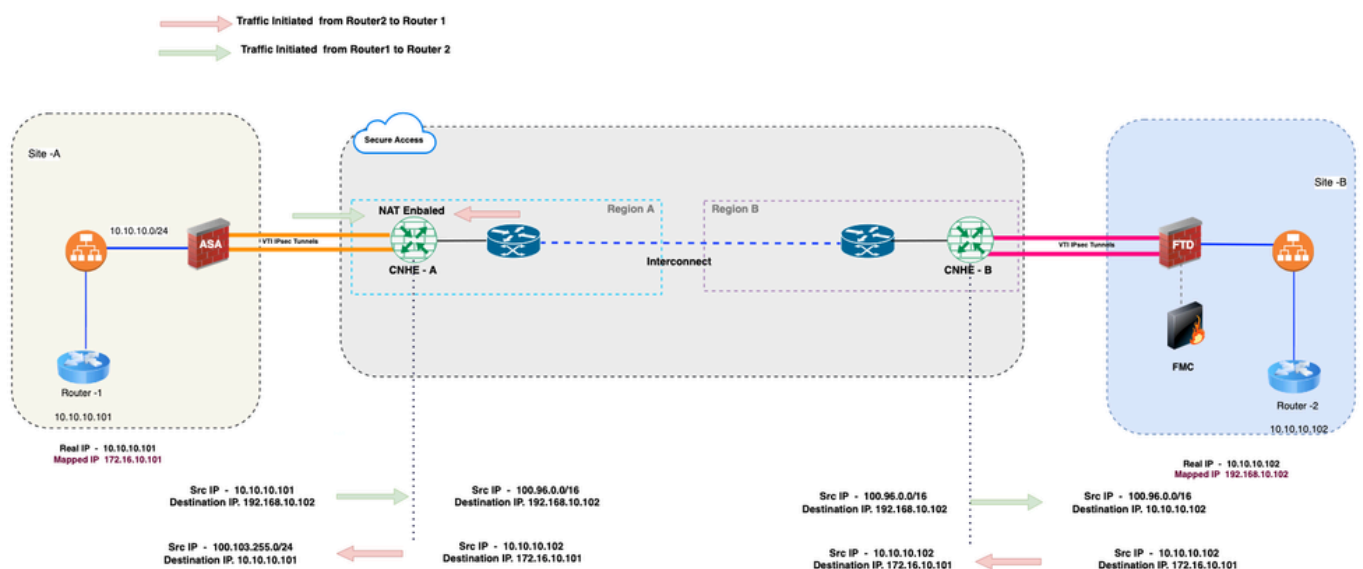
routekaart RM-CSA-vergunning 10

overeenkomend IP-adres PBR
SET IP NEXT-HOP 169.254.2.2 169.254.2.6

3. Routekaart toepassen op de ingangsinterface

Gigabit Ethernet-interface0/1
Naam binnen
veiligheidsniveau 100
IP-adres 10.10.10.1 255.255.255.0
policy-route-map RM-CSA

Verifiëren



Routerinterface en GW-bereikbaarheidsstatus

```
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
```

Test 1- Router2 --> Router1. - Ping-test

```

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#

```

Packet capture op ASA (lokaal FW)

```

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

```

Packet Capture op FTD (externe FW)


```

ftd# sh cap
ftd# sh capture
capture vti type raw-data trace interface VTI-1 include-decryptd [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

Test 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

```

FTD Packet Capture (lokaal FW)

```

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

```

ASA packet capture (Remote FW)

```

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

```

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.