

Beveiligde toegang configureren met Secure Firewall Threat Defense voor privétoegang met op beleid gebaseerde routing

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Beveiligde toegangsconfiguratie](#)

[Configuratie netwerktunnelgroep](#)

[beveiligde toegangsrouting](#)

[op beleid gebaseerde routing](#)

[Configuratie netwerktunnelgroep opslaan](#)

[Een privé-bron maken](#)

[Een regel voor toegangsbeleid maken](#)

[Beveiligde Firewall Threat Defense \(FTD\)-configuratie](#)

[Configuratie van virtuele tunnelinterfaces](#)

[IPsec-tunnelconfiguratie](#)

[FTD-routeringsconfiguratie](#)

[op beleid gebaseerde routing](#)

[Configuratie toegangsbeleid](#)

[Verifiëren](#)

[Controleren in FTD](#)

[De tunnelstatus in FTD](#)

[Verifiëren bij beveiligde toegang](#)

[Tunnel Status in Veilige Toegang](#)

[Evenementen in Secure Access](#)

[Gerelateerde informatie](#)

Inleiding

In dit document wordt beschreven hoe u Veilige toegang met FTD via IPsec configureert voor Veilige privétoegang met beleidsgebaseerde routing.

Voorwaarden

Vereisten

- Cisco Secure Access-kennis
- Cisco Secure Access-dashboard/tenant
- Kennis van het Secure Firewall Threat Defense and Firewall Management Center
- IPsec-kennis
- Beleidsgebaseerde routeringskennis

Gebruikte componenten

- Secure Firewall Running 7.7.10 code
- Het door de cloud geleverde Firewall Management Center. Configuratie is ook van toepassing voor de typische virtuele FMC
- Cisco Secure Access-dashboard

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

Netwerktunnels in Secure Access kunnen worden gebruikt voor twee primaire doeleinden: Secure Internet Access en Secure Private Access.

Voor Secure Private Access kunnen organisaties gebruikmaken van Zero Trust Access (ZTA) en/of VPN as a Service (VPNaaS) om gebruikers te verbinden met privébronnen zoals interne toepassingen of datacenters. IPsec-tunnels spelen een belangrijke rol in deze architectuur door het netwerkverkeer tussen gebruikers en privébronnen veilig te coderen en ervoor te zorgen dat gevoelige gegevens beschermd blijven terwijl ze door niet-vertrouwde netwerken gaan. Door IPsec-tunnels te integreren met ZTA of VPNaaS kunnen organisaties naadloze en veilige toegang bieden tot interne bronnen met behoud van robuuste beveiligingscontroles en zichtbaarheid.

In dit document wordt beschreven hoe u Secure Access configureert met Secure Firewall Threat Defense (FTD) via IPsec voor Secure Private Access.

Daarnaast bevat deze handleiding stappen voor het configureren van op beleid gebaseerde routing.

Hoewel dit document betrekking heeft op de configuratie van IPsec-tunnels voor beveiligde privétoegang, valt de installatie van Zero Trust Access (ZTA) of VPN as a Service (VPNaaS) voor toegang tot privétoepassingen buiten het toepassingsgebied van deze handleiding.

Configureren

Beveiligde toegangsconfiguratie

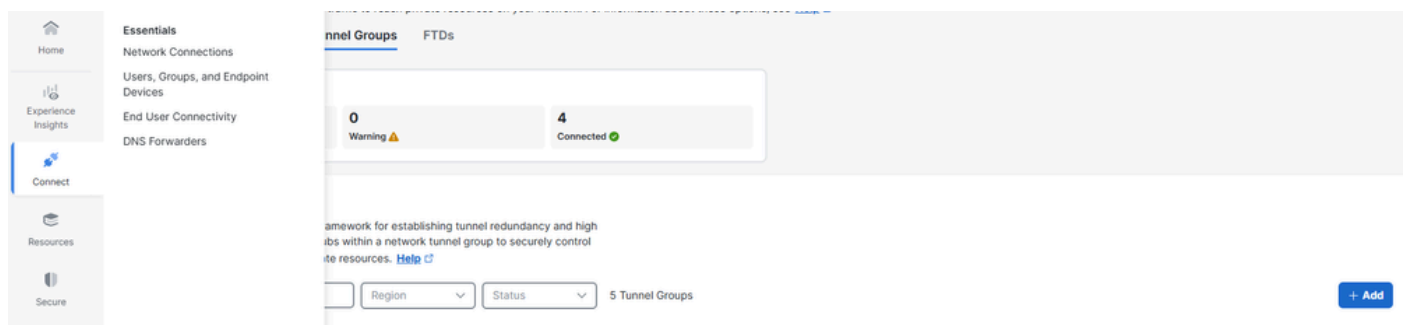
Configuratie netwerktunnelgroep

1. Navigeer naar het beheerderspaneel van [Secure Access](#).



2. Voeg een netwerktunnelgroep toe.

- Klik op **Connect** > **Network Connections**
 - Klik onder **Network Tunnel Groups** op > **Add**



3. General Settings Configuratie.

- Configureer de Tunnel Group Name en Region de Device Type
 - Klik op de knop **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 the type this tunnel group will use.

Tunnel Group Name

FTD

Region

Canada (Central)

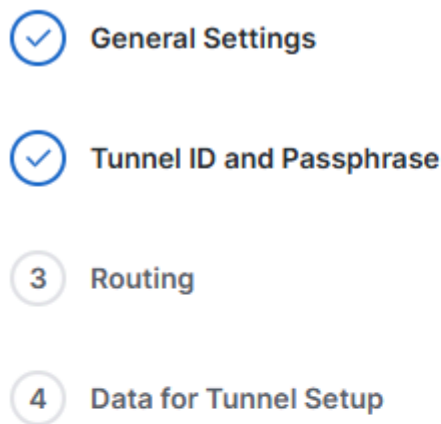
Device Type

FTD

Algemene instellingen

4. Configureren Tunnel ID en Passphrase instellen.

- Configureer de Tunnel ID en Passphrase. Deze ID is belangrijk, omdat deze vereist is voor de FTD-configuratie
- Klik op 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 en PSK

5. Statische routing configureren.

beveiligde toegangsroutering

op beleid gebaseerde routing

Voeg het netwerk (de netwerken) toe dat wordt beveiligd door de FTD en waartoe u externe gebruikers toegang wilt geven via ZTA en/of VPNaaS en klik op Opslaan.

- Klik op Routing > Static routing
 - Voeg de IP-adresbereiken of hosts toe die u in uw netwerk hebt geconfigureerd en die het verkeer via Secure Access willen doorgeven, en klik op Add
 - Klik op Save

statische CSA-routing

Configuratie netwerktunnelgroep opslaan

Download en sla de tunnelinstallatiegegevens op, zoals deze nodig zijn voor de FTD-configuratie.

- Klik op **Download CSV**
- Klik op **Done**

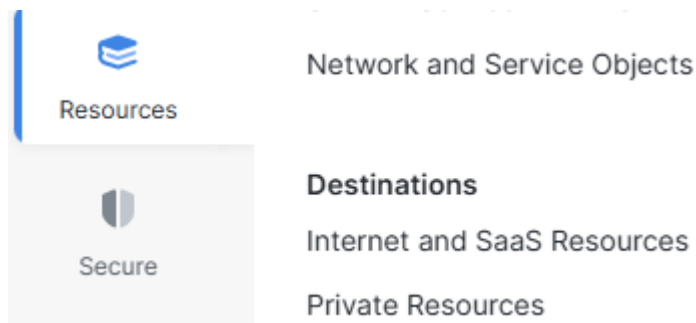
NTG-gegevens

Een privé-bron maken

Privébronnen zijn interne toepassingen, netwerken of subnetten die worden gehost in uw datacenter- of privécloudomgeving. Deze bronnen zijn niet openbaar toegankelijk en worden beschermd achter de infrastructuur van uw organisatie.

Door ze te definiëren als Private Resources in Secure Access, kunt u gecontroleerde toegang inschakelen via oplossingen zoals Zero Trust Access (ZTA) of VPN as a Service (VPNaaS). Dit zorgt ervoor dat gebruikers veilig verbinding kunnen maken met interne systemen op basis van identiteit, apparaathouding en toegangsbeleid, zonder de bronnen rechtstreeks aan het internet bloot te stellen.

Navigeer naar **Resources > Private Resources** > klik op **Add**.



PR

- Specificeer de **Private Resource Name**, Internally reachable address, Protocol, Port/Ranges. Geef poorten en protocollen op en voeg indien nodig extra privébronnen toe
- Selecteer de gewenste verbinding **Connection Method** op basis van uw behoefte, bijvoorbeeld Zero-trust-verbindingen en/of VPN-verbindingen, volgens uw vereisten
- Klik op **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

particuliere hulpbron

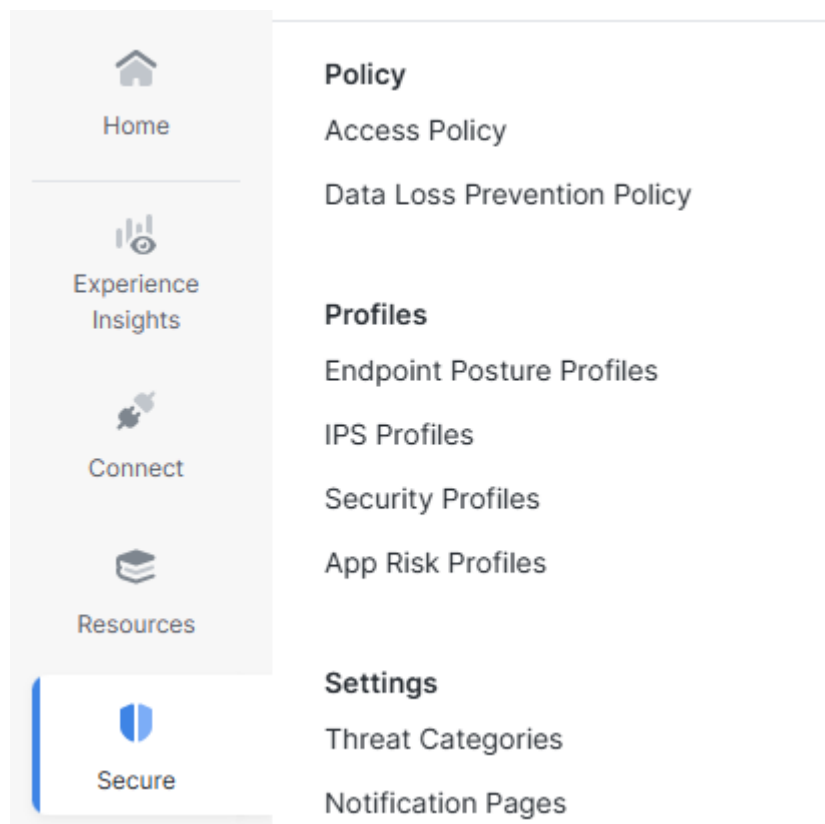
Een regel voor toegangsbeleid maken

Privé-toegangsregels bepalen hoe gebruikers veilig verbinding kunnen maken met interne bronnen en toepassingen die niet openbaar toegankelijk zijn.

Deze regels handhaven de beveiliging door te bepalen wie toegang heeft tot specifieke privébronnen op basis van factoren zoals gebruikersidentiteit, groepslidmaatschap, apparaathouding, locatie of andere beleidsvoorwaarden. Dit zorgt ervoor dat gevoelige interne systemen beschermd blijven tegen algemene publieke toegang, terwijl ze nog steeds veilig

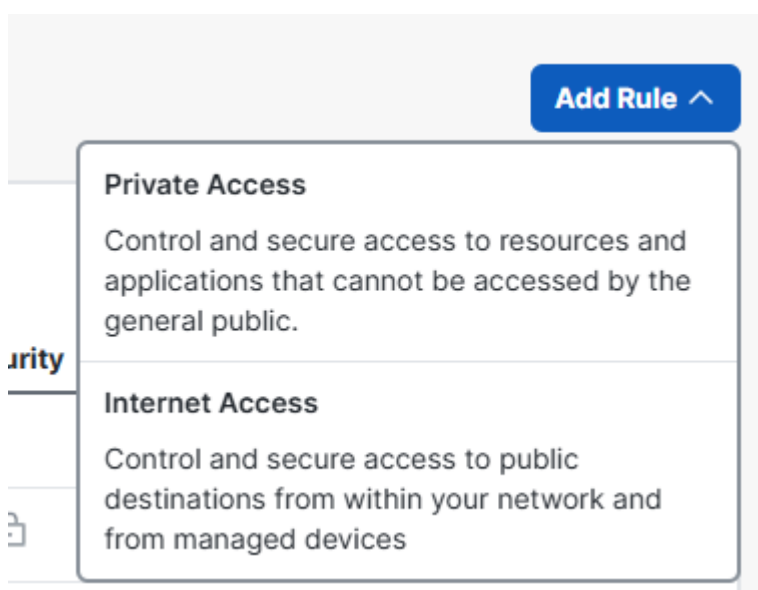
beschikbaar zijn voor geautoriseerde gebruikers via ZTA of VPNaaS.

Navigeer naar [Secure](#)>[Access Policy](#)



ACS

- Klik op [Add Rule](#)
 - Klik op [Private Access](#)



ACP toevoegen

- Klik erop [Rule Name](#) en geef het een naam

- Klik op **Actionen** selecteer **Allow** om dit verkeer toe te staan
- Klik **From** op en geef de gebruikers op die toestemming hebben gekregen
- Klik op **To** en geef de toegang op die gebruikers hebben op basis van deze regel
- Klik op **Next** en dan **Save** op de volgende pagina

Rule name ⓘ

FTD IPsec Rule

Rule order

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

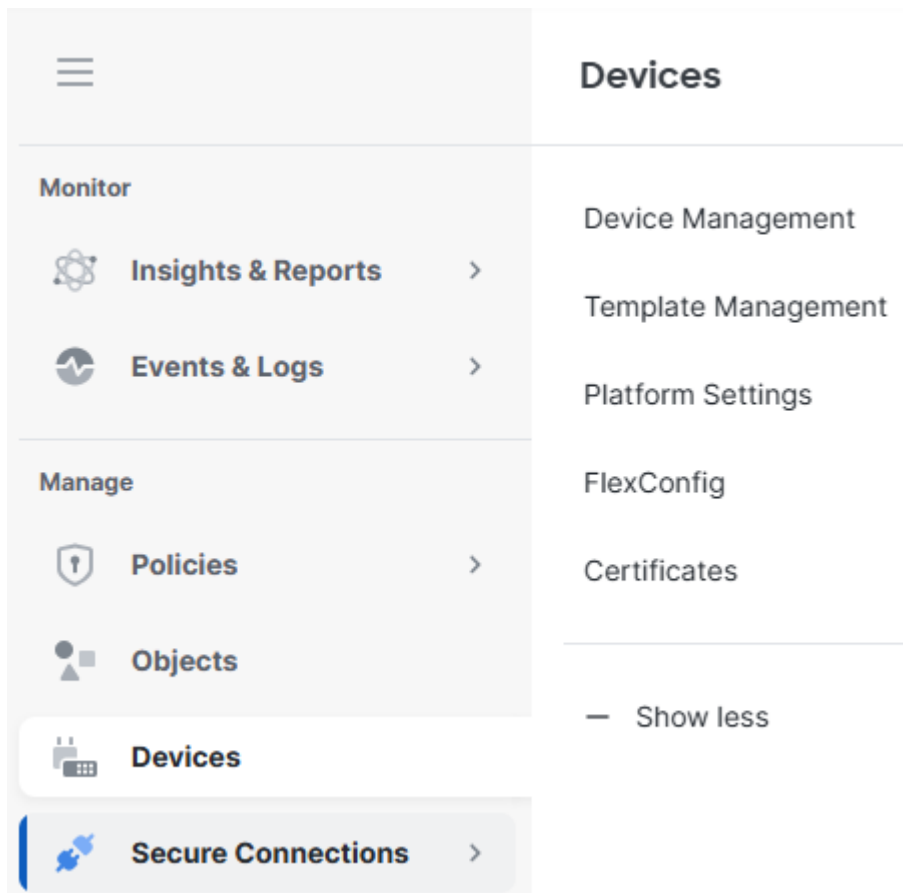
ACS-configuratie

Beveiligde Firewall Threat Defense (FTD)-configuratie

Configuratie van virtuele tunnelinterfaces

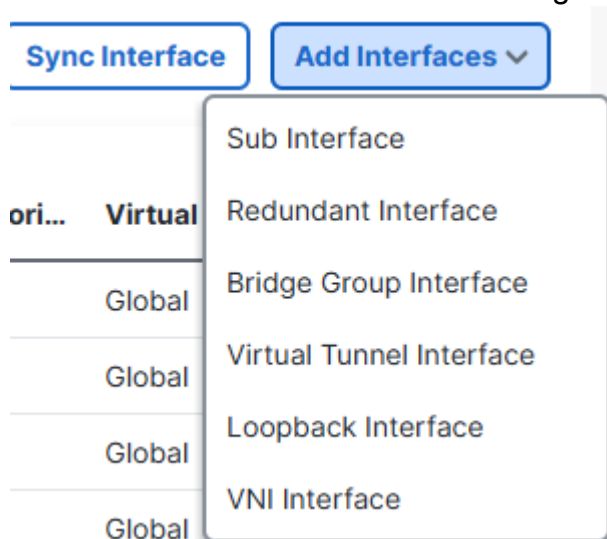
Een Virtual Tunnel Interface (VTI) op FTD is een logische Layer 3-interface die wordt gebruikt om routegebaseerde IPsec VPN-tunnels te configureren.

1. Navigeer naar **Devices** ➤ **Device Management**.



FTD-apparaten

- Klik op het FTD-apparaat, [Interfaces](#)
 - Klik op [Add Interfaces](#)
 - Klik op [Virtual Tunnel Interface](#)
 - Maak twee Virtual Tunnel Interfaces, één voor de primaire beveiligde toegangshub en een andere voor de secundaire beveiligde toegangshub



VTI's toevoegen

Virtual Tunnel Interface 1:

- Geef het een naam, klik op [Enable](#)

- Selecteer of maak een Security Zone
- Klik erop Tunnel ID en geef het een waarde.
- Klik op en specificeer Tunnel Source de WAN-interface van waaruit de tunnel wordt ingesteld
- Klik op IPsec Tunnel Mode en selecteer IPv4
- Klik op IP Address en configureer het IP-adres voor de VTI
- Klik op 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



Virtual Tunnel Interface 2:

- Geef het een naam, klik op **Enable**
- Selecteer of maak een **Security Zone**
- Klik erop **Tunnel ID** en geef het een waarde
- Klik op en specificeer **Tunnel Source** de WAN-interface van waaruit de tunnel wordt ingesteld
- Klik op **IPsec Tunnel Mode** en selecteer **IPv4**
- Klik op **IP Address** en configureer het IP-adres voor de VTI
- Klik op **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:*

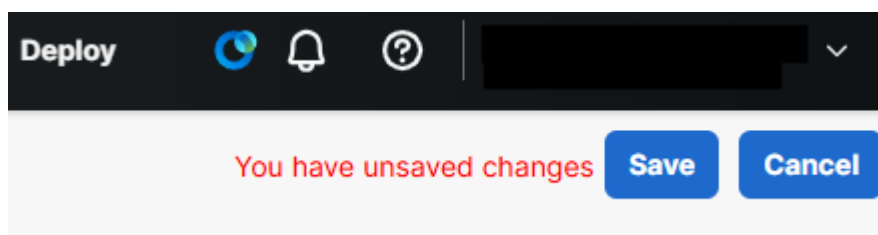
☒ Configure IP

169.254.0.5/30



VTI2,2

- Klik op Opslaan.

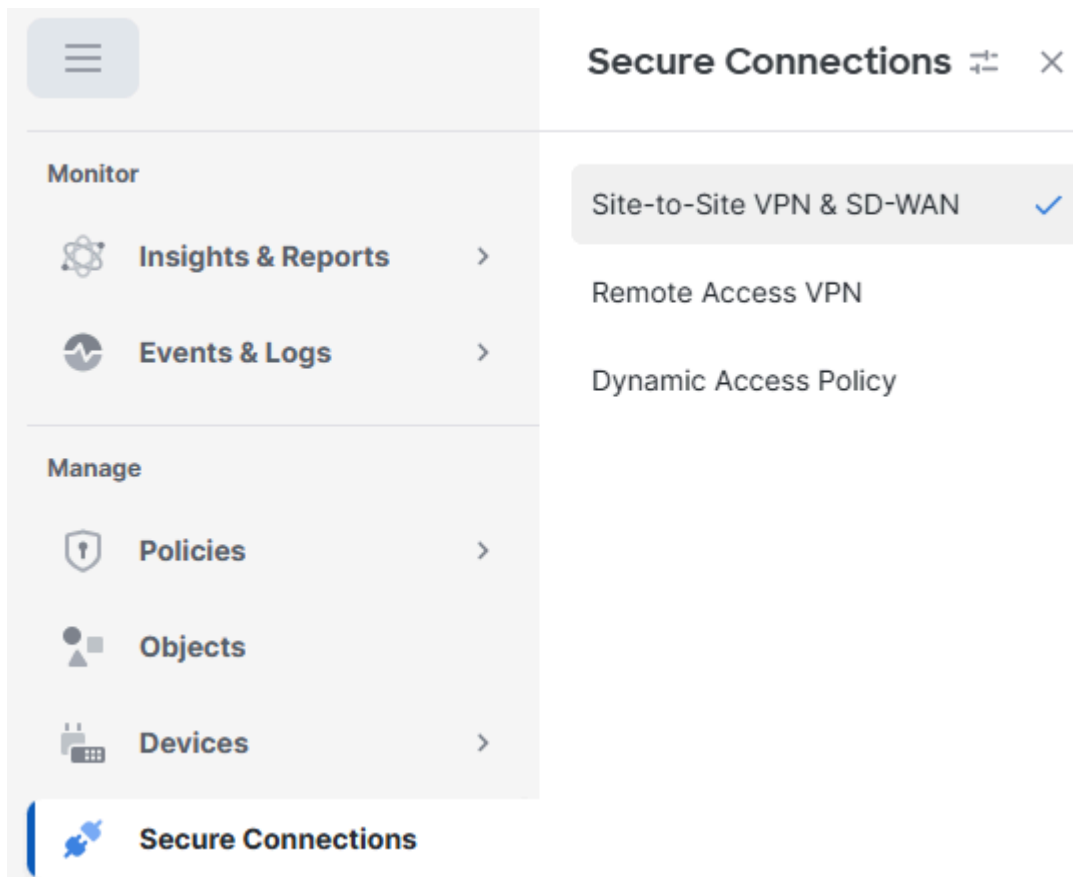


VTI-wijzigingen opslaan

IPsec-tunnelconfiguratie

Navigeer naar uw cdFMC-dashboard.

- Klik op [Secure Connection](#) > [Site-to-Site VPN & SD-WAN](#)



S2S

- Klik op **Add**
 - Klik op **Route-Based VPN**
 - Klik op **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](#)

VPN toevoegen

- Verzamel in stap 5 van de Secure Access-configuratie de tunnel-ID's en IP-adressen voor de

primaire en secundaire datacenters

- Klik op Endpoints
 - Klik onder Node Aan en Device selecteer Extranet
 - Klik op Device Name en geef het een naam
 - Klik op Endpoint IP Addresses en voer de primaire en secundaire IP-adressen voor beveiligde toegang in, gescheiden door een komma (van "Configuratie netwerktunnelgroep opslaan" onder de optie Beveiligde toegang Configuratie)
 - Klik onder Node Aan Device 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 Send Local Identity to Peers en selecteer Email ID, voer de primaire tunnel-ID in (van "Save Network Tunnel Group Configuration" onder de Secure Access Configuration)
 - Klik op Add Backup VTI
 - Klik op Virtual Tunnel Interface en selecteer de tweede VTI-interface die in de vorige stap is gemaakt
 - Klik Send Local Identity to Peers op optie en selecteer Email ID, voer de secundaire tunnel-ID in (van "Save Network Tunnel Group Configuration" onder de Secure Access Configuration)
 - Klik op Opslaan

Network Topology:

IKE Version:* ☐ IKEv1 ☒ IKEv2

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

Node A

Device:*

Extranet
▼

Device Name*:

CSA

Endpoint IP Address*:

Primary-IP,Secondary-IP

Node B

Device:*

cdFTD-1
▼

Virtual Tunnel Interface:*

VTI-1 (IP: 169.254.0.1)
▼
+

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

☐ Tunnel Source IP is Private

☒ Send Local Identity to Peers

Local Identity Configuration*

Email ID
▼

ftd1-ipsec@

Backup VTI: Remove

Virtual Tunnel Interface:*

VTI-2 (IP: 169.254.0.5)
▼
+

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

☐ Tunnel Source IP is Private

☒ Send Local Identity to Peers

Local Identity Configuration*

Email ID
▼

ftd1-ipsec@

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

FTD VTI-configuratie

- Klik op **IKE**
 - Klik op **IKEv2 Settings > Policies**
 - Selecteer de **Umbrella-AES-GCM-256** optie
 - Klik op **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

IKEv2-beleid

- Klik op **Authentication Type** en selecteer **Pre Shared Manual Key** de PSK die is geconfigureerd in **Secure Access** (wachtwoordgroep)

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

- Klik op **IPSEC**
 - Klik op **IKEv2 Proposals**
 - selecteren **Umbrella-AES-GCM-256**
 - Klik op **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

IKEv2-voorstellen opslaan

FTD-routeringsconfiguratie

Met Policy-Based Routing (PBR) kunt u het doorsturen van verkeer beheren op basis van criteria die verder gaan dan alleen het IP-adres van de bestemming. In plaats van alleen te vertrouwen op de routingstabel, kan PBR verkeer routeren op basis van bron, toepassing, protocol, poorten of ander gedefinieerd beleid.

Dit stelt organisaties in staat om specifiek of hoog prioritair verkeer via voorkeurslinks te sturen (zoals een hoge bandbreedte of directe internetlink), de prestaties te optimaliseren en geselecteerde applicaties veilig uit te breken zonder al het verkeer door een VPN-tunnel te sturen.

op beleid gebaseerde routing

- Navigeer naarObjects
 - Klik op Access List
 - Klik op Extended
 - Klik opAdd Extended Access List

Monitor

Insights & Reports

Events & Logs

Manage

Policies

Objects

AAA Server

Access List

Extended

Service Access

Standard

Address Pools

Application Filters

AS Path

BFD Template

Cipher Suite List

Extended

An access list object, also known as an access control list (ACL), selects the traffic to which a service will apply. Standard-identifies traffic based on destination on source and destination address and ports. Supports IPv4 and IPv6 addresses. You use these objects when configuring particular features, such as route map

Add Extended Access List

Name

Value

ACL toevoegen

Maak een uitgebreide toegangscontrolelijst (ACL) die overeenkomt met uw bronnetwerk dat wordt beschermd door de FTD (bijvoorbeeld 172.16.15.0/24) om door de tunnel te worden verzonden. Voeg voor de bestemming de netwerken toe die worden gebruikt door ZTA (CGNAT-bereik) en het netwerk dat wordt gebruikt door uw VPNaaS (controleer 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

- Klik op **Devices** > **Device Management**

Monitor

Insights & Reports

Events & Logs

Manage

Policies

Objects

Devices

Device Management

Template Management

Platform Settings

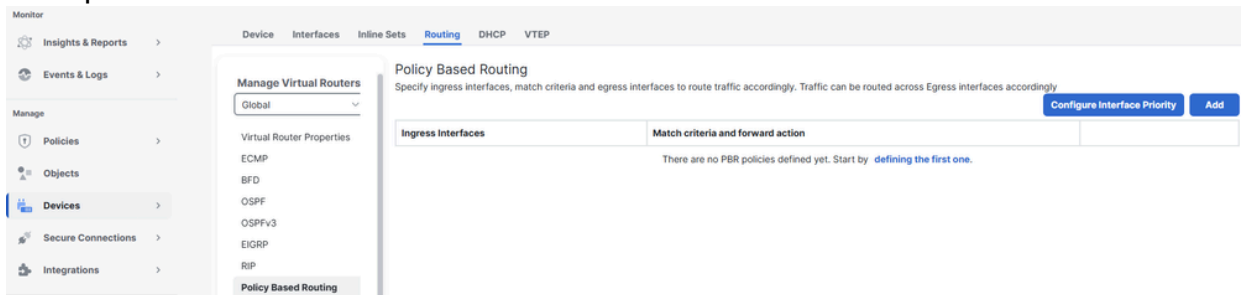
FlexConfig

Certificates

Show less

Apparaat

- Klik op de FTD
 - Klik op Routing
 - Klik op Policy Based Routing
 - Klik op Add



PBR toevoegen

- Klik op Ingress Interface en selecteer de ingangsinterface waar verkeer van interne netwerken binnenkomt
- Klik onder Overeenstemmingscriteria en Uitgangs-interface op 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

Ingress-interface

- Klik op Match ACL en selecteer de uitgebreide ACL die eerder is gemaakt
- Klik op Send To and select IP Address
- Klik op IPv4 Addresses en stel als volgende stappen de IP-adressen in de VTI-interfacesubnetten in die eerder in de FTD zijn geconfigureerd (169.254.0.2 en 169.254.0.6)
- Klik op Save

Match ACL: *

CSA_ACL



Send To: *

IP Address



IPv4 Addresses:

169.254.0.2,169.254.0.6

Cancel

Save

PBR opslaan

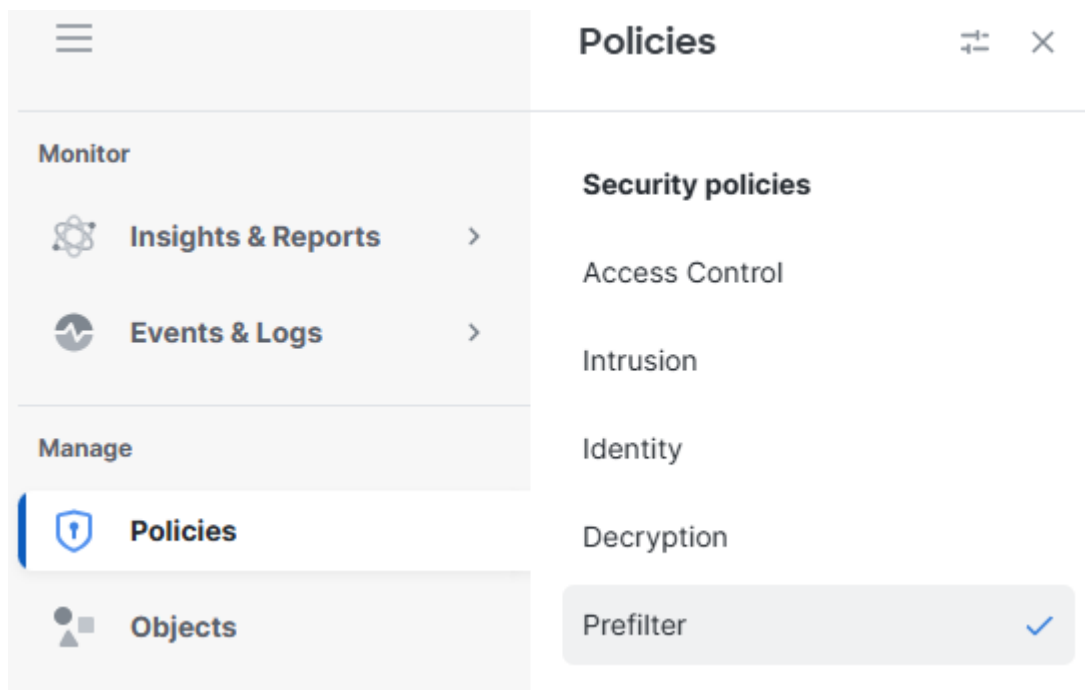
Selecteer de optie **Send To > IP Address** en niet de **Egress Interface** optie.

Configuratie toegangsbeleid

Om verkeer op een Cisco Firepower Threat Defense (FTD) mogelijk te maken en toegang tot privébronnen mogelijk te maken, moet het verkeer eerst door de eerste fase van toegangscontrole gaan die bekend staat als Prefiltering.

Prefiltering wordt verwerkt voordat diepere inspectie plaatsvindt en is ontworpen om eenvoudig en snel te zijn. Het evalueert verkeer met behulp van basis-criteria voor de buitenste koptekst (zoals bron- en bestemmings-IP-adressen en -poorten) om snel verkeer toe te staan, te blokkeren of te omzeilen. Wanneer verkeer in dit stadium is toegestaan, kan het meer resource-intensieve inspecties zoals diepe pakketinspectie of inbraakbeleid overslaan, waardoor de prestaties worden verbeterd terwijl de beveiligingscontrole behouden blijft.

- Navigeer naar **Policies > Prefilter**



voorfilter

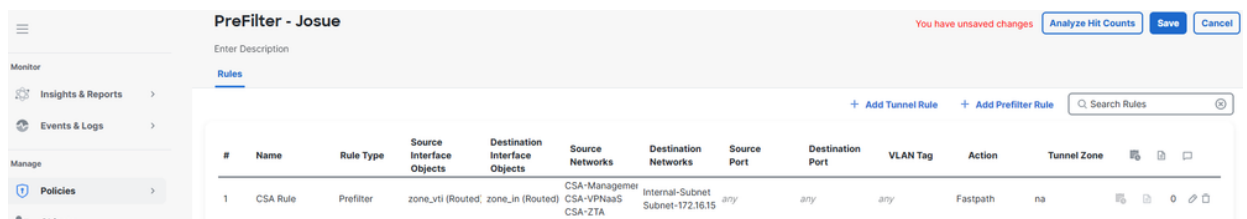
- Klik op het beleid Voorfilter bewerken dat wordt gebruikt in uw toegangsbeleid



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	 

Klik op Prefilter

- Klik op Add Tunnel Rule
 - Voeg het verkeer van het VPNaaS-netwerk en/of het ZTA-subnet toe aan uw privébronnen
 - Klik op Save



#	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_vrt (Routed)	zone_in (Routed)	CSA-Manager CSA-VPNaaS CSA-ZTA	Internal-Subnet Subnet-172.16.15	any	any	any	Fastpath	na	  

Regel opslaan

Zodra de configuratie op de FTD is voltooid en geverifieerd, kunt u doorgaan met de implementatie. Na de implementatie komen de IPsec-tunnels met succes tevoorschijn, wat bevestigt dat een veilige verbinding met de privébronnen tot stand is gebracht.

Verifiëren

Controleren in FTD

De tunnelstatus in FTD

U kunt de huidige status van de tunnel bekijken, inclusief of deze omhoog of omlaag is. Dit helpt om te controleren of de IPsec-tunnel correct is ingesteld.

- Klik op Beveiligde verbindingen.
- Klik op Site-to-Site VPN en SD-WAN.
- Klik op de naam van de topologie.

Topology name	VPN Type	Network Topology	Tunnel Status Distribution	IKEv1	IKEv2
CSA	Route Based (VTI)	Point-to-Point	2 Tunnels		✓
Node A			Node 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)

FTD-tunnelstatus

Verifiëren bij beveiligde toegang

Tunnel Status in Veilige Toegang

U kunt de huidige status van de tunnel bekijken, inclusief of de tunnel is losgekoppeld, gewaarschuwd of verbonden. Dit helpt om te controleren of de IPsec-tunnel correct is ingesteld.

- Klik op Verbinden > Netwerk verbindingen
- Klik op Network Tunnel Groups

Home

Experience Insights

Connect

Resources

Secure

Essentials

Network Connections

Users, Groups, and Endpoint Devices

End User Connectivity

DNS Forwarders

Tunnel Groups

FTDs

0 Warning

4 Connected

Framework for establishing tunnel redundancy and high availability within a network tunnel group to securely control its resources. [Help](#)

Region

Status

5 Tunnel Groups

+ Add

NTG controleren

- Klik op de Netwerktunnelgroep

Summary

Connected

RegionCanada (Central)

Routing TypeStatic Routing

Device TypeFTD

IP Address Range172.16.15.0/24

Last Status UpdateFeb 18, 2026 3:34 PM

Primary Hub

Hub Up

1 Active Tunnels

Tunnel Group IDftd1-ipsec@

See Logs

Secondary Hub

Hub Up

1 Active Tunnels

Tunnel Group ID

Evenementen in Secure Access

U kunt tunnelgebeurtenissen bekijken en bevestigen of de status van de IPsec-tunnels is ingesteld en stabiel is.

Klik op Monitor > Netwerk connectiviteit.

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

Conn-logboeken bewaken

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

Conn Logs

Navigeer naar Monitor > Activiteit zoeken.

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

Conn-logboeken bewaken

Klik op een van de gerelateerde gebeurtenissen op Volledige details bekijken.

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		

Volledige details

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

Activiteit zoeken

Gerelateerde informatie

- [Cisco Technical Support en downloads](#)
- [Apparaatconfiguratiehandleiding Cisco Secure Firewall Management Center, 7.7](#)

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.