

Beveiligde toegang configureren met Secure Firewall Threat Defense voor privétoegang met dynamische routing

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Beveiligde toegangsconfiguratie](#)

[Configuratie netwerktunnelgroep](#)

[beveiligde toegangsroutering](#)

[Dynamische routing \(BGP\)](#)

[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](#)

[Dynamische routing \(BGP\)](#)

[Configuratie toegangsbeleid](#)

[Verifiëren](#)

[Controleren in FTD](#)

[De tunnelstatus in FTD](#)

[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 dynamische 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
- Kennis van dynamische routing

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 dynamische routing met BGP.

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 netwerk tunnelgroep

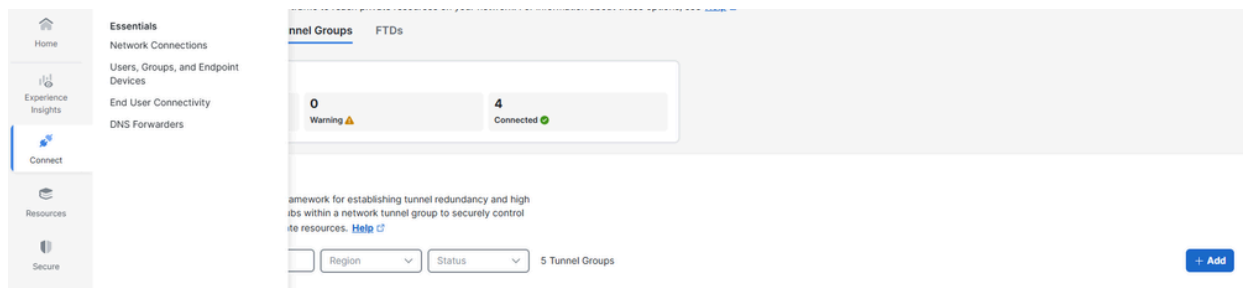
1. Navigeer naar het beheerderspaneel van [Secure Access](#).



CSA-dashboard

2. Voeg een netwerk tunnelgroep toe.

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



NTG controleren

3. General Settings Configuratie.

- Configureer de Tunnel Group Name en Region de Device Type
 - Klik op de knop **Next**

- ✓ General Settings
- 2 Tunnel ID and Passphrase
- 3 Routing
- 4 Data for Tunnel Setup

Algemene instellingen

General Settings

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

Tunnel Group Name

FTD

Region

Canada (Central)

Device Type

FTD

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

- Klik op Next

- ✓ General Settings
- ✓ Tunnel ID and Passphrase
- 3 Routing
- 4 Data for Tunnel Setup

ID en PSK

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

.....

5. Dynamische routing configureren.

beveiligde toegangsroutering

Dynamische routing (BGP)

- Geef het BGP Autonomous System (AS)-nummer van de FTD op bij het configureren van de BGP-peer in Secure Access.
- Klik op **Routing** > **Dynamic routing**
 - Klik op **Device AS Number** en voeg de FTD's BGP ASN toe
 - Vink het **Block default route advertisement** selectievakje aan
 - Klik op **Save**

☒ **Dynamic routing**
Use this option when you have a BGP peer for your on-premise router.

Device AS Number

64513

Advanced Settings

☐ **Multihop BGP**
Select this option to enable the ability for BGP peers to establish a connection (hop) when not directly connected.

☐ **Multi-region backhaul**
Use Secure Access as the network backbone and prioritize regions based on origin.

☒ **Block default route advertisement**
Select to block the advertisement of the default route.

CSA BGP Config



Opmerking: Routes die door Secure Access worden geadverteerd, vormen een aanvulling op het oorspronkelijke AS-pad en omvatten: 1 voor primaire tunnels en 2 voor secundaire tunnels. Back-upscenario's voor meerdere regio's worden ondersteund. Voor meer informatie klik op.

Configuratie netwerktunnelgroep opslaan

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

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

✓ 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:

ftd1-ipsec@

Primary Data Center IP Address:

ftd1-ipsec@

Secondary Tunnel ID:

ftd1-ipsec@

Secondary Data Center IP Address:

Passphrase:

Download CSV

Done

NTG-gegevens

Summary

✖ Disconnected

Region	Canada (Central)	Routing Type	Dynamic Routing (BGP)
Device Type	FTD	Device BGP AS	64513
Last Status Update	Feb 18, 2026 3:58 PM	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	—

BGP-instellingen



Opmerking: Klik op de Netwerktunnelgroep om het BGP AS-nummer en de BGP peer IP-adressen te bekijken, die later aan de FTD-zijde worden geconfigureerd.

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**.


Resources


Secure

Network and Service Objects

Destinations

Internet and SaaS Resources

Private Resources

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

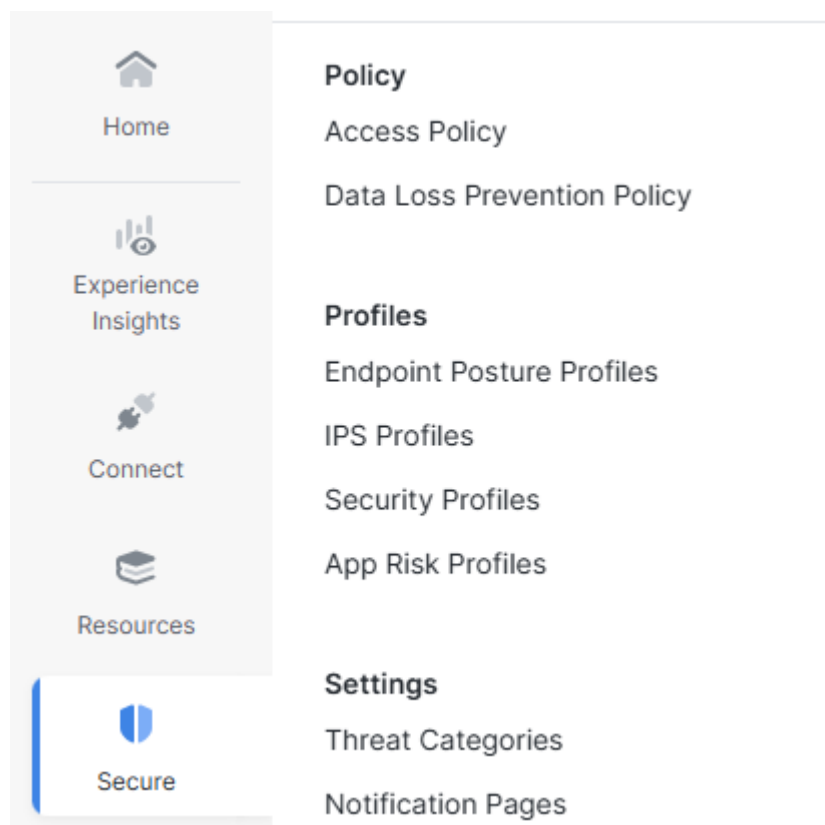
particuliere hulpbron

Een regel voor toegangsbeleid maken

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

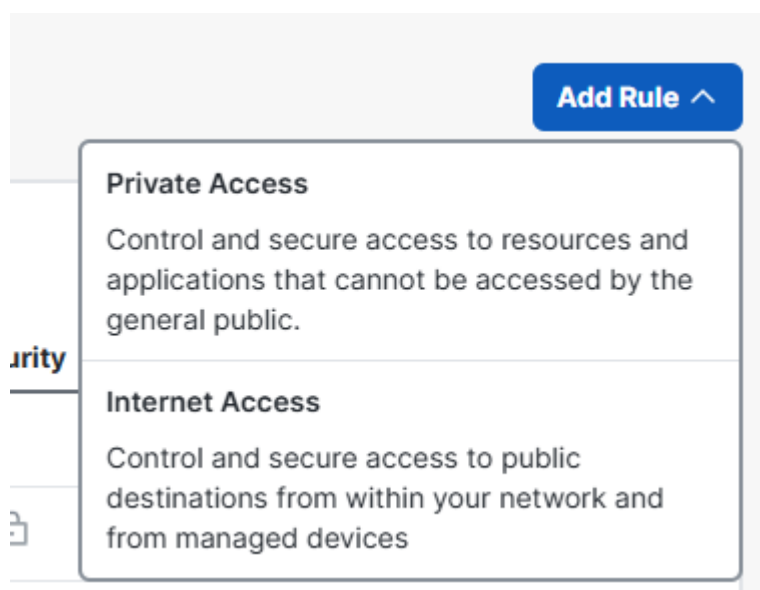
Deze regels handhaven de beveiliging door te bepalen wie toegang heeft tot specifieke privébronnen op basis van factoren zoals gebruikersidentiteit, groepslidmaatschap, apparaathouding, locatie of andere beleidsvoorwaarden. Dit zorgt ervoor dat gevoelige interne systemen beschermd blijven tegen algemene 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 **Action** en selecteer **Allow** om dit verkeer toe te staan
- Klik **From** op en geef de gebruikers op die toestemming hebben gekregen

- Klik op **Toen** 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

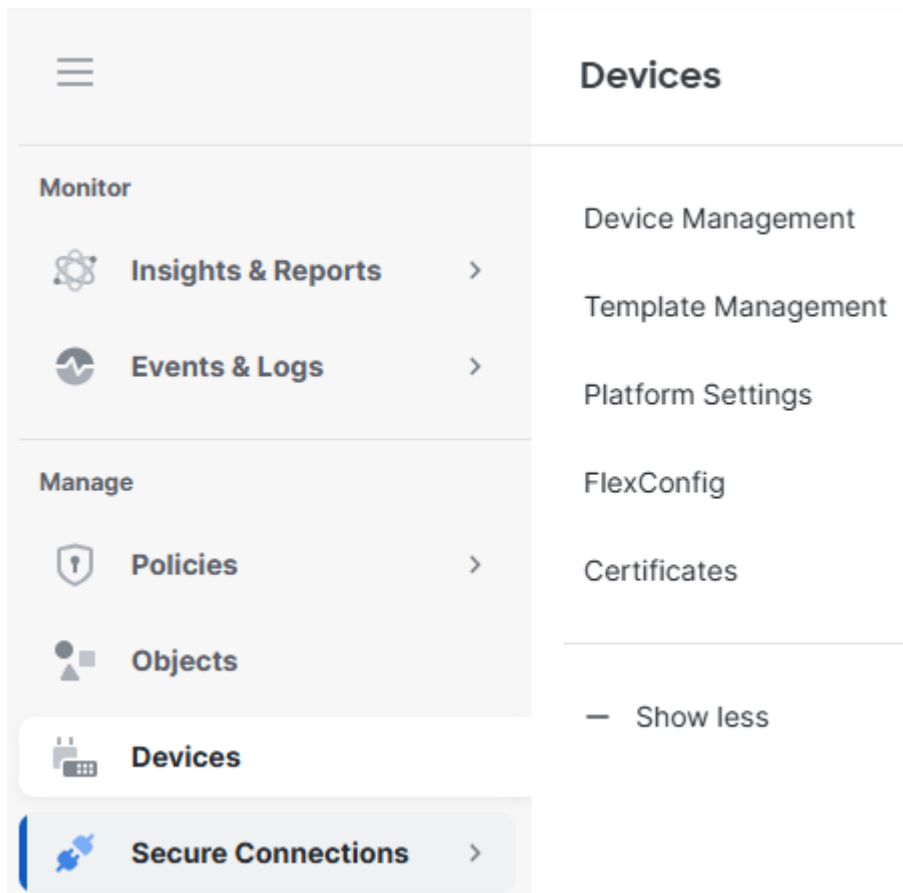
ACS-configuratie

Beveiligde Firewall Threat Defense (FTD)-configuratie

Configuratie van virtuele tunnelinterfaces

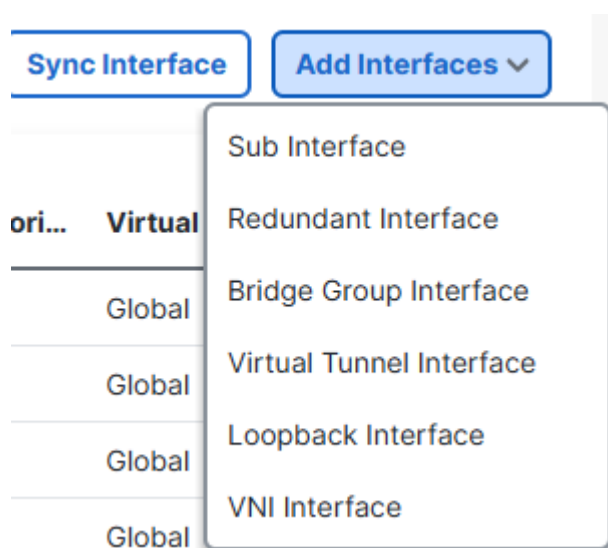
Een Virtual Tunnel Interface (VTI) op FTD is een logische Layer 3-interface die wordt gebruikt om routegebaseerde IPsec VPN-tunnels te configureren.

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



VTI1,2

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

VTI2,1

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:*

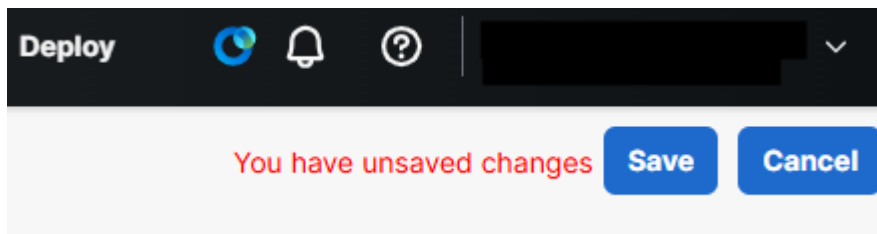
☒ Configure IP

169.254.0.5/30



VTI2,2

Klik op Opslaan.

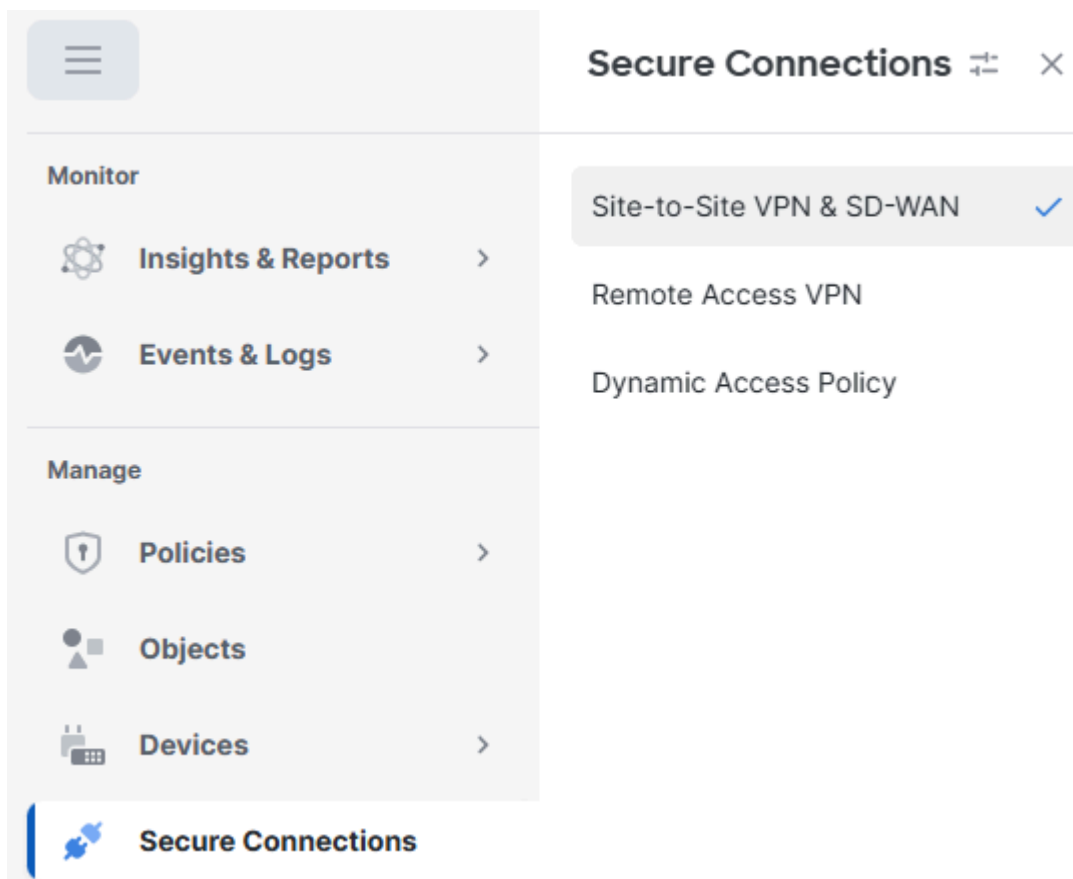


VTI-wijzigingen opslaan

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 *

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](#)

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 A** 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 netwerk tunnelgroep opslaan" onder de optie **Beveiligde toegang**)
 - Klik onder **Node B** 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  

Q Search

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

Endpoints
IKE
IPsec
Advanced

Crypto Map Type:
☒ Static
☐ Dynamic

IKEv2 Mode:
Tunnel

Transform Sets:
IKEv1 IPsec Proposals
IKEv2 IPsec Proposals*

tunnel_aes256_sha
Umbrella-AES-GCM-...

IPSEC

Cancel
OK

IKEv2-voorstellen opslaan

FTD-routeringsconfiguratie

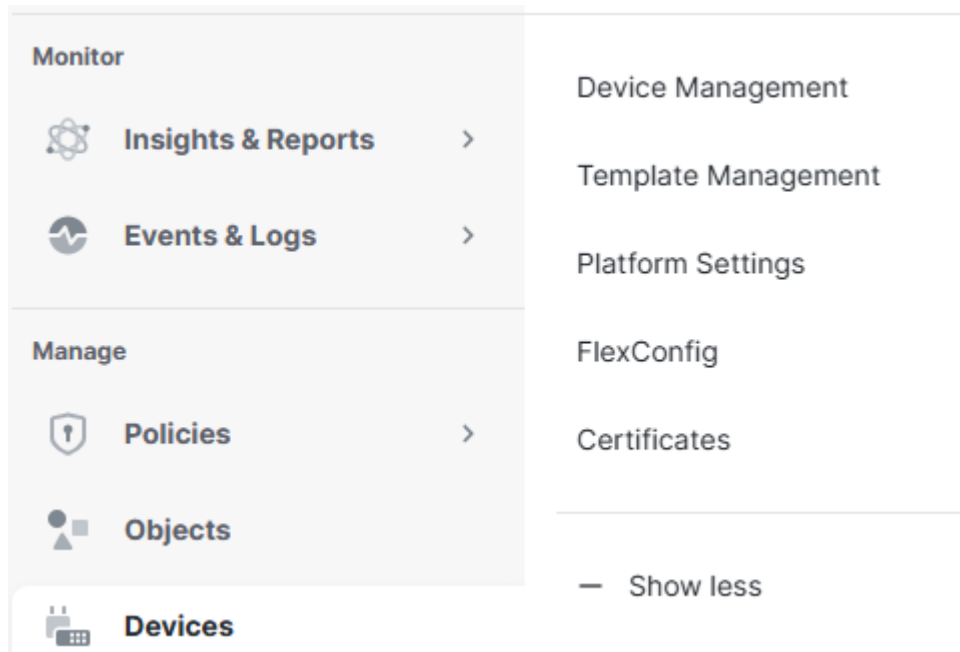
Dynamische routering (BGP)

Border Gateway Protocol (BGP) is een dynamisch routeringsprotocol dat de uitwisseling van routeringsinformatie tussen autonome systemen automatiseert. Het bepaalt het best beschikbare pad voor gegevensverkeer op basis van kenmerken en beleid, in plaats van te vertrouwen op statische routes.

Door dynamisch routes te leren en bij te werken, verbetert BGP de schaalbaarheid, optimaliseert het de padselectie en zorgt het voor automatische failover in het geval van link- of netwerkwijzigingen.

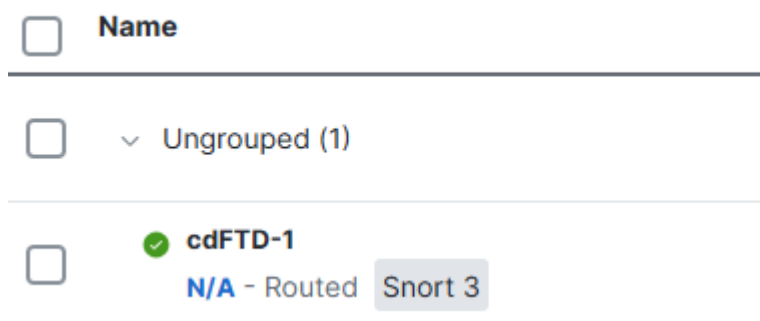
Navigeer naar uw cdFMC-dashboard.

- Klik op [Devices](#) > Device Management



Apparaat

- Klik op de FTD



FTD-apparaat

- Klik op **Routing > BGP > IPv4 > Enable IPv4**
- Klik op **Neighbor** en geef het BGP Autonomous System (AS)-nummer voor beveiligde toegang op, samen met de IP-adressen van de buren
Raadpleeg de opmerking onder de Configuratie beveiligde toegang, waar alle relevante configuratiedetails voor dit proces worden verstrekt.
- Klik op **Save**

cdFTD-1 You have unsaved changes [Save](#) [Cancel](#)

Cisco Secure Firewall Threat Defense for VMware

Device Interfaces Inline Sets **Routing** DHCP VTEP

Enable IPv4: ☒ AS Number 64513

General **Neighbor** Add Aggregate Address Filtering Networks Redistribution Route Injection

Manage Virtual Routers: Global

Virtual Router Properties

ECMP

BFD

OSPF

OSPFv3

EIGRP

RIP

Policy Based Routing

▼ BGP

IPv4

Address	Remote AS Number	Address Family	Remote Private AS Number	Description
169.254.0.2	64512	Enabled		
169.254.0.6	64512	Enabled		

+ Add

BGP-buur



Opmerking: vanaf november 2025 gebruiken alle nieuw opgerichte organisaties voor beveiligde toegang standaard de openbare ASN 32644 voor BGP-peering in netwerktunnelgroepen. Bestaande organisaties die vóór november 2025 zijn opgericht, blijven gebruikmaken van de private ASN 64512 die voorheen was gereserveerd voor Secure Access BGP-peers.

- Klik op **Networks** en voeg de netwerk(en) die u wilt adverteren toe aan Secure Access
- Klik op **Save**

cdFTD-1 You have unsaved changes [Save](#) [Cancel](#)

Cisco Secure Firewall Threat Defense for VMware

Device Interfaces Inline Sets **Routing** DHCP VTEP

Enable IPv4: ☒ AS Number 64513

General Neighbor Add Aggregate Address Filtering **Networks** Redistribution Route Injection

Manage Virtual Routers: Global

Virtual Router Properties

ECMP

BFD

OSPF

OSPFv3

EIGRP

RIP

Policy Based Routing

▼ BGP

IPv4

Network	RouteMap
Subnet-172.16.15.0	

+ Add

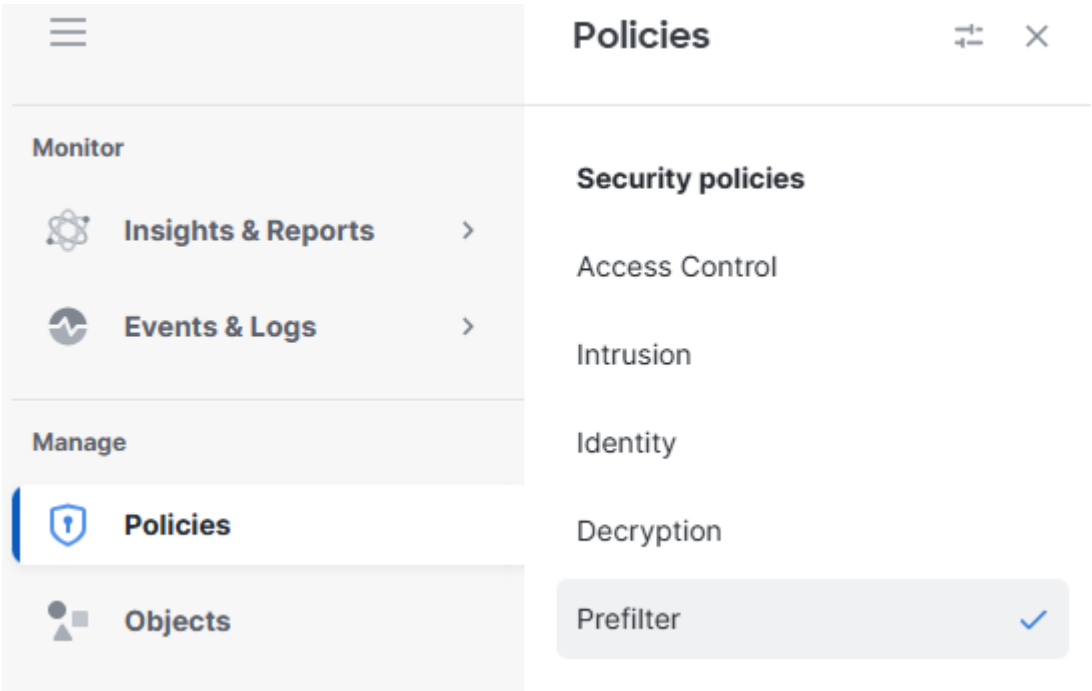
Netwerk toevoegen

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

New Policy

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

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

PreFilter - Josue											
Enter Description											
Rules											
#	Name	Rule Type	Source Interface Objects	Destination Interface Objects	Source Networks	Destination Networks	Source Port	Destination Port	VLAN Tag	Action	Tunnel Zone
1	CSA Rule	Prefilter	zone_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 zowel de IPsec-tunnels als de BGP-buursessies met succes naar voren, wat bevestigt dat connectiviteit en dynamische routing werken zoals

verwacht.

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 & SD-WAN
- Klik op de topologienaam

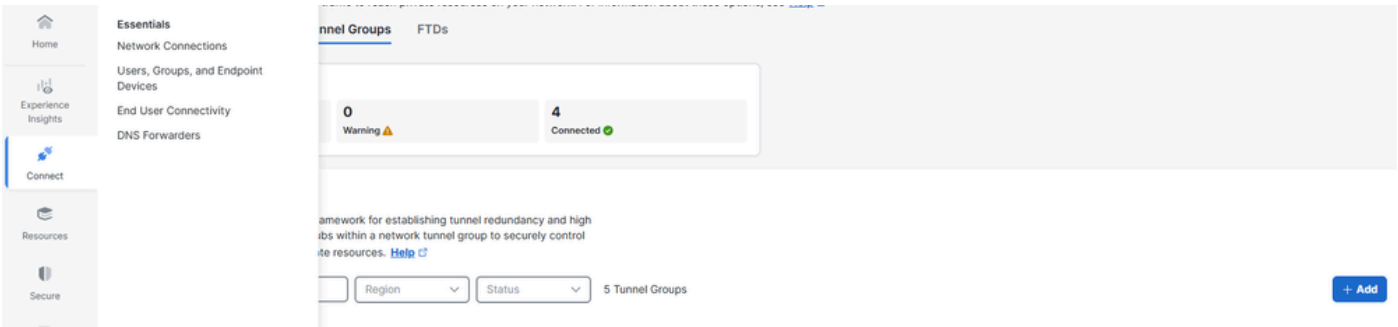
Topology name	VPN Type	Network Topology	Tunnel Status Distribution	IKEv1	IKEv2
CSA	Route Based (VTI)	Point-to-Point	2 Tunnels		✓
Node A		Node B			
Device	VPN Interface	VTI Interface	Device	VPN Interface	VTI Interface
EXTRANET Extranet			FTD cdFTD-1	outside (192.168.0.20)	VTI-1 (169.254.0.1)
EXTRANET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

FTD-tunnelstatus

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



NTG controleren

- Klik op de Netwerktunnelgroep

Summary

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

Primary Hub

See Logs

Hub Up

1

Active Tunnels

Tunnel Group ID ftd1-ipsec@

Secondary Hub

Hub Up

1

Active Tunnels

Tunnel Group ID

CSA-tunnelstatus

Evenementen in Secure Access

U kunt de gebeurtenissen Tunnel en BGP bekijken en bevestigen of de status van de IPsec-tunnels is ingesteld en stabiel is en of BGP-sessies zijn ingesteld.

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 X

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

NTG-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 View Full Details.

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

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.