

Routegebaseerde VPN configureren met statische route op FTD beheerd door FDM

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configuratiestappen op FDM](#)

[Verifiëren](#)

[Gerelateerde informatie](#)

Inleiding

In dit document wordt beschreven hoe u een statische route-gebaseerde site naar site VPN-tunnel configureert op een FTD die wordt beheerd door FDM.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Een goed begrip van hoe een VPN tunnel werkt.
- Voorkennis van het navigeren door de Firepower Device Manager (FDM).

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende softwareversies:

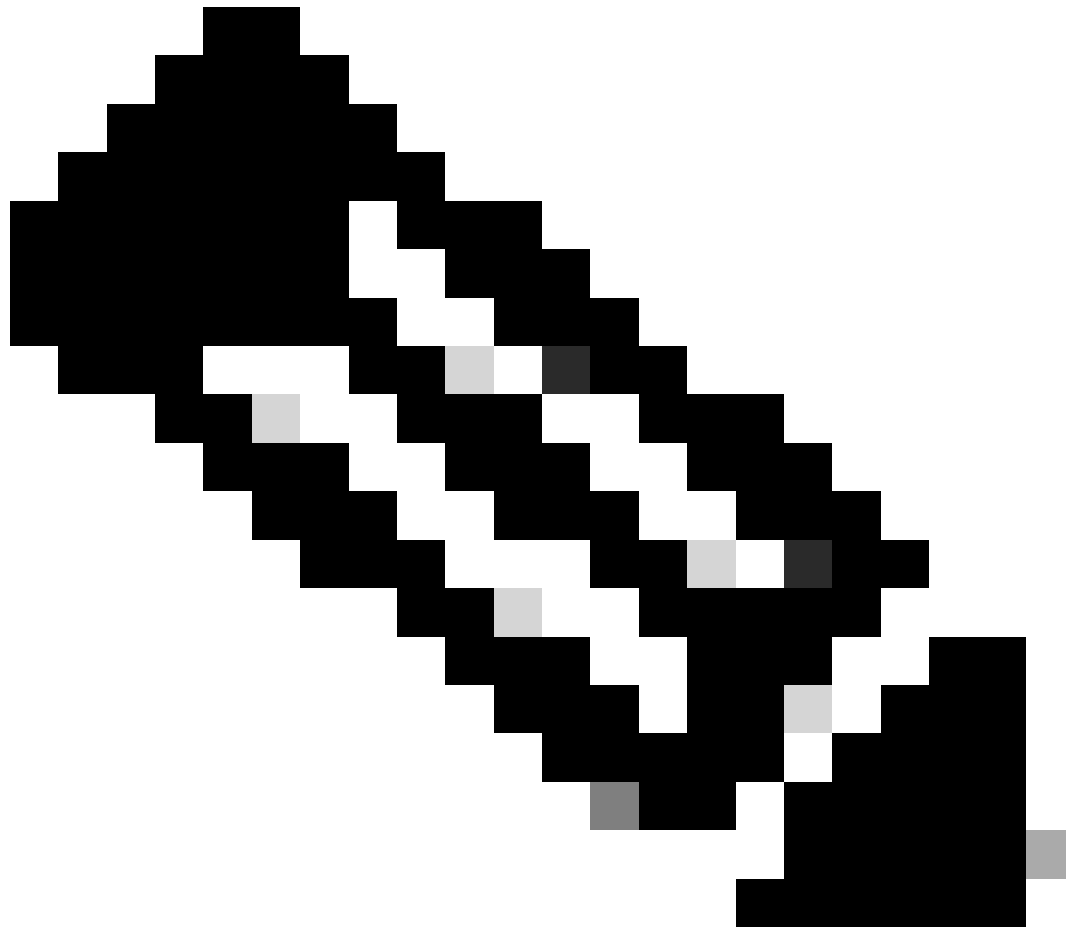
- Cisco Firepower Threat Defense (FTD) versie 7.0 wordt beheerd door Firepower Device Manager (FDM).

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

Met routegebaseerde VPN kan interessant verkeer worden gecodeerd of via een VPN-tunnel worden verzonden en verkeersrouting worden gebruikt in plaats van een beleid / toegangslijst zoals in een op beleid gebaseerde of op Crypto-map gebaseerde VPN. Het encryptiedomein is ingesteld om elk verkeer toe te staan dat de IPsec-tunnel binnenkomt. IPsec De lokale en externe verkeersselectors zijn ingesteld op 0.0.0.0/0.0.0.0. Dit betekent dat elk verkeer dat naar de IPsec-tunnel wordt geleid, wordt gecodeerd, ongeacht het bron- / bestemmingssubnet.

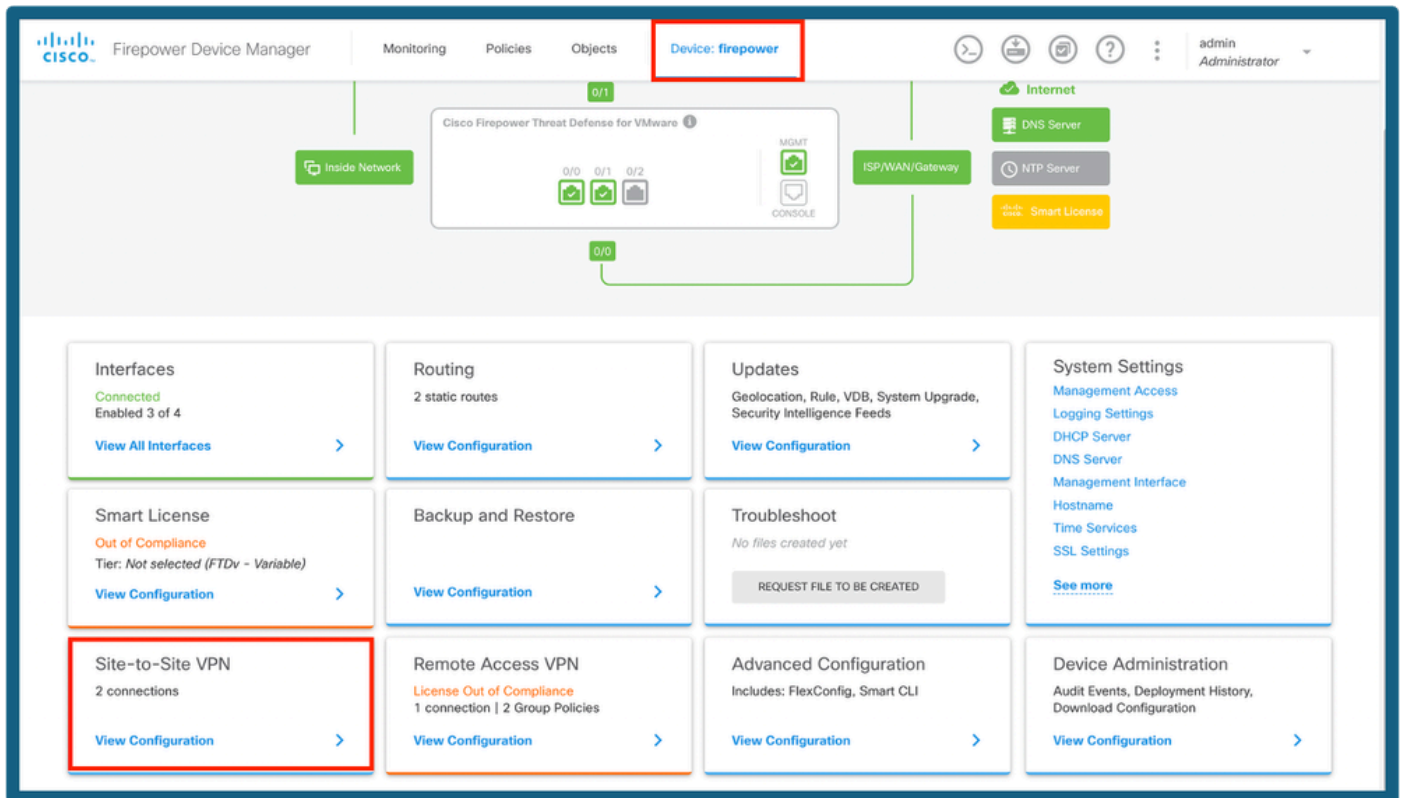
Dit document richt zich op de configuratie van de statische Virtual Tunnel Interface (SVTI).



Opmerking: er is geen extra licentie nodig, Route Based VPN kan worden geconfigureerd in zowel Licensed als Evaluation Modes. Zonder crypto-compliance (Export Controlled Features Enabled) kan alleen DES worden gebruikt als een coderingsalgoritme.

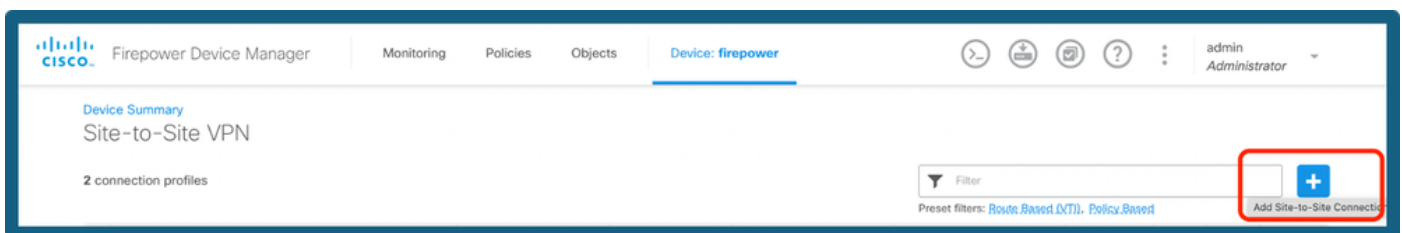
Configuratiestappen op FDM

Stap 1. Navigeer naar Apparaat > Site-to-site.



FDM-dashboard

Stap 2. Klik op het + pictogram om een nieuwe site aan de siteverbinding toe te voegen.



S2S-verbinding toevoegen

Stap 3: Geef een topologienaam op en selecteer het type VPN als Route Based (VTI).

Klik op Local VPN Access Interface en klik vervolgens op Create new Virtual Tunnel Interface of selecteer een van de bestaande lijsten.

Firepower Device Manager | Monitoring | Policies | Objects | Device: firepower | admin Administrator

Local Network --- FIREPOWER --- VPN TUNNEL --- INTERNET --- OUTSIDE INTERFACE --- PEER ENDPOINT --- Remote Network

Define Endpoints

Identify the interface on this device, and the remote peer's interface IP address, that form the point-to-point VPN connection. Then, identify the local and remote networks that can use the connection. Traffic between these networks is protected using IPsec encryption.

Connection Profile Name: **vdi-ipsec** | Type: **Route Based (VTI)** | Policy Based

Sites Configuration

LOCAL SITE

Local VPN Access Interface: Please select

Filter: Nothing found

REMOTE SITE

Remote IP Address:

[Create new Virtual Tunnel Interface](#)

NEXT

Tunnel-interface toevoegen

Stap 4. Definieer de parameters van de nieuwe virtuele tunnelinterface. Klik op OK.

Create Virtual Tunnel Interface

Name

tunnel10

Status

Most features work with named interfaces only, although some require unnamed interfaces.

Description

Tunnel ID

10

Tunnel Source

outside (GigabitEthernet0/0)

0 - 10413

IP Address and Subnet Mask

192.168.1.1

/

255.255.255.252

e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0

CANCEL

OK

VTI-configuratie

Stap 5. Kies de nieuw gemaakte VTI of een VTI die bestaat onder Virtual Tunnel Interface. Geef het externe IP-adres op.

New Site-to-site VPN

1 Endpoints 2 Configuration 3 Summary

Local Network FIREPOWER VPN TUNNEL INTERNET OUTSIDE INTERFACE PEER ENDPOINT Remote Network

Define Endpoints

Identify the interface on this device, and the remote peer's interface IP address, that form the point-to-point VPN connection. Then, identify the local and remote networks that can use the connection. Traffic between these networks is protected using IPsec encryption.

Connection Profile Name: Type: ☒ Route Based (VTI) ☐ Policy Based

Sites Configuration

LOCAL SITE

Local VPN Access Interface:

REMOTE SITE

Remote IP Address:

Peer IP toevoegen

Stap 6. Kies de IKE-versie en kies de knop Bewerken om de IKE- en IPsec-parameters in te stellen zoals weergegeven in de afbeelding.

IKE Policy

i IKE policies are global, you cannot configure different policies per VPN. Any enabled IKE Policies are available to all VPN connections.

IKE VERSION 2 ☒ **IKE VERSION 1** ☐

IKE Policy

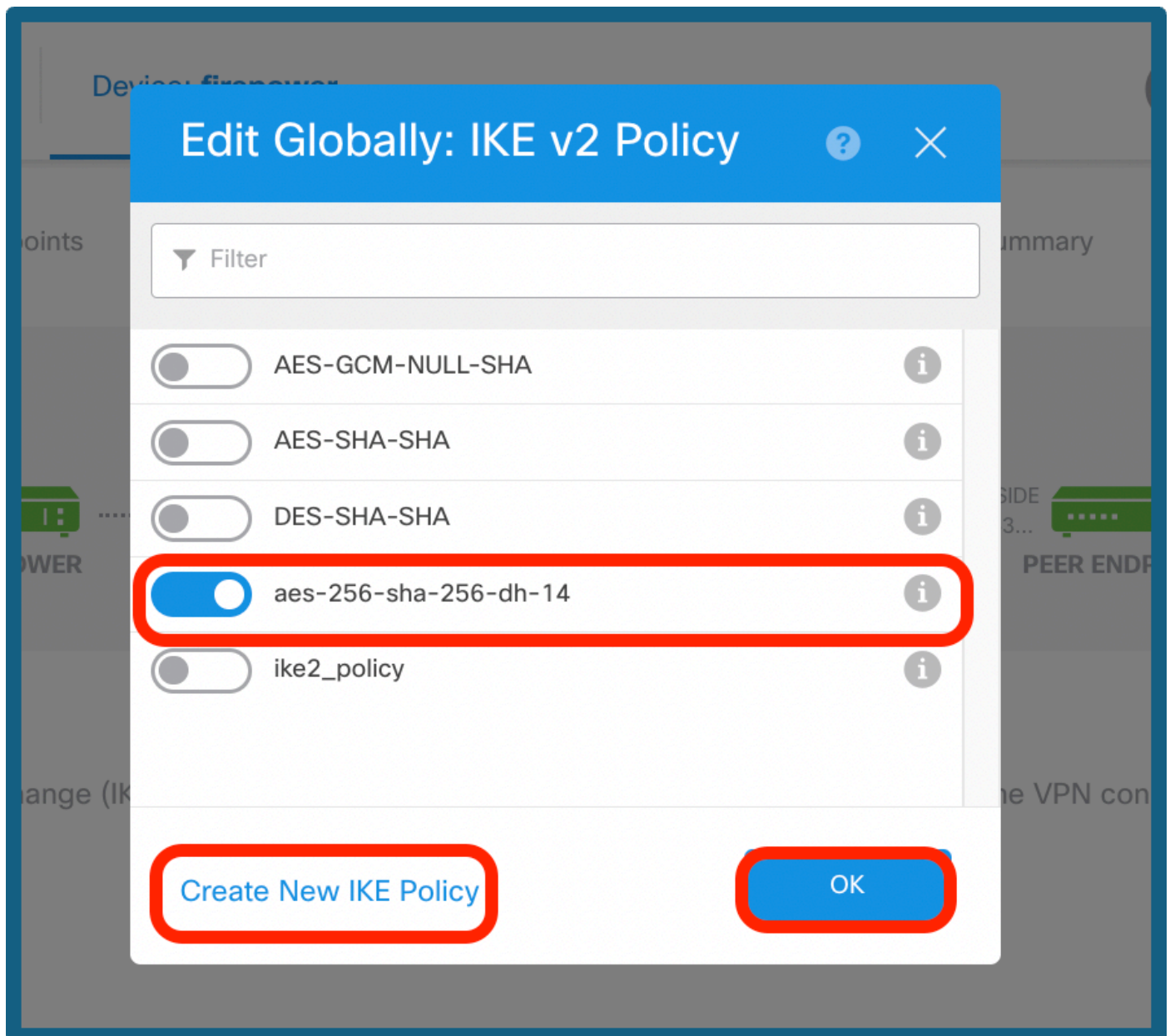
Globally applied

IPSec Proposal

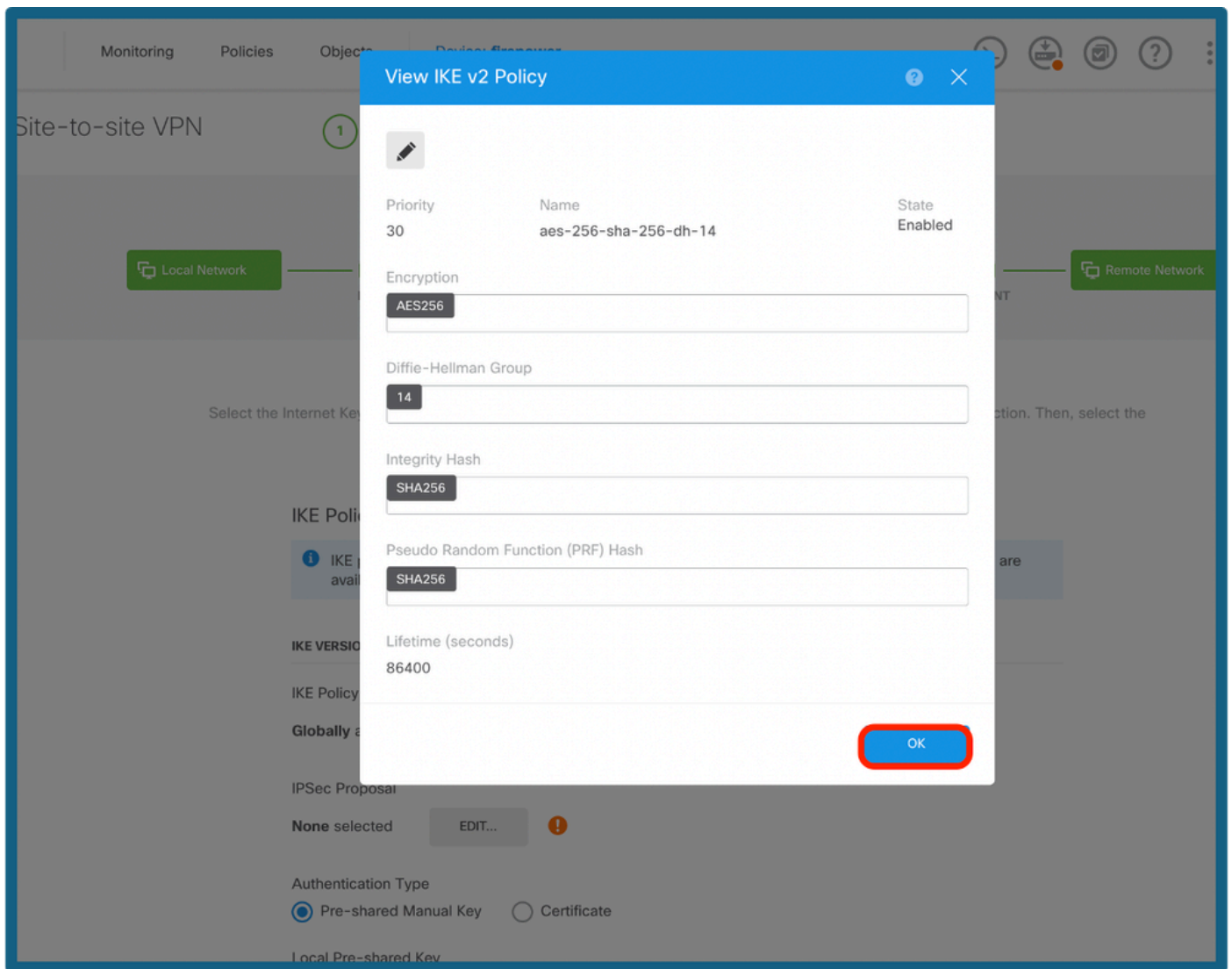
Custom set selected

IKE-versie configureren

Stap 7a. Kies de knop IKE-beleid zoals weergegeven in de afbeelding en klik op ok of Nieuwe IKE-beleid maken, als u een nieuw beleid wilt maken.

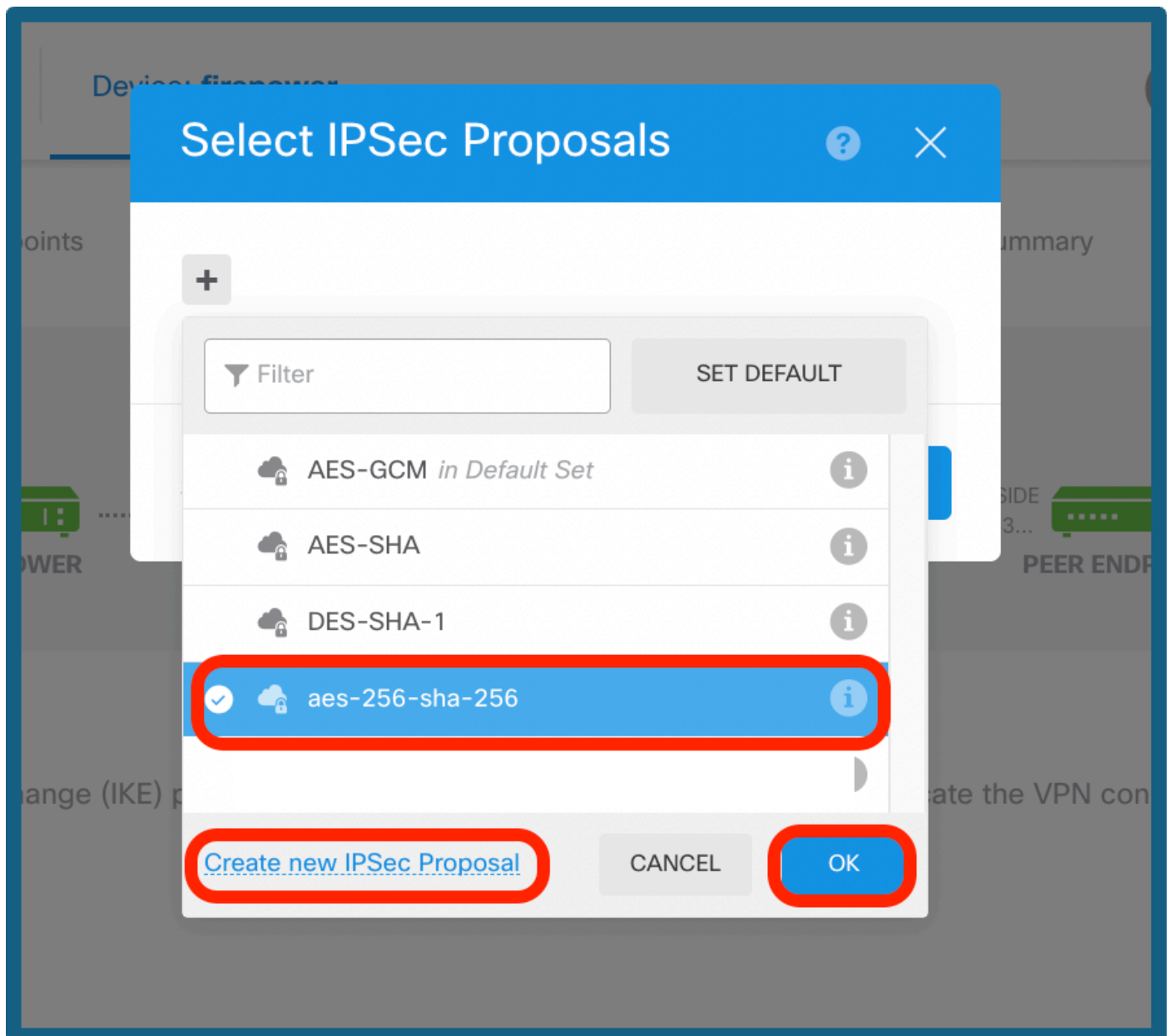


Kies IKE-beleid

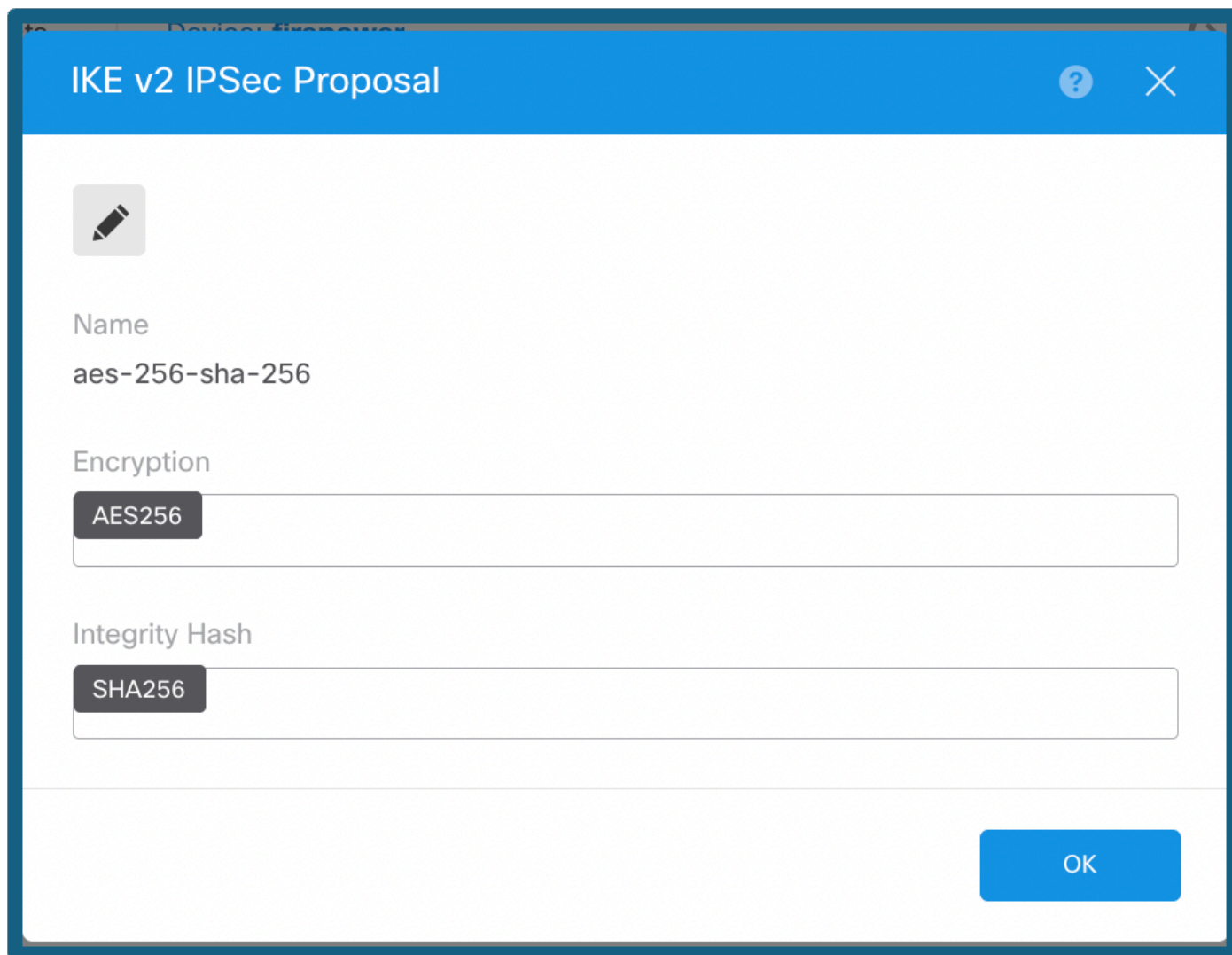


Config van het IKE-beleid

Stap 7b. Kies de knop IPsec-beleid zoals weergegeven in de afbeelding en klik op de knop ok of Maak een nieuw IPsec-voorstel, als u een nieuw voorstel wilt maken.



IPsec-voorstel selecteren



IKE v2 IPSec Proposal

Name
aes-256-sha-256

Encryption
AES256

Integrity Hash
SHA256

OK

Config van het IPsec-voorstel

Stap 8a. Selecteer het verificatietype. Als een vooraf gedeelde handmatige sleutel wordt gebruikt, geeft u de lokale en externe vooraf gedeelde sleutel op.

Stap 8b. (Optioneel) Kies de instellingen voor Perfect Forward Secrecy. Configureer de IPsec Lifetime Duration en Lifetime Size en klik vervolgens op Next.

IKE VERSION 2 ☒

IKE VERSION 1 ☐

IKE Policy

Globally applied

EDIT...

IPSec Proposal

Custom set selected

EDIT...

Authentication Type

☒ Pre-shared Manual Key ☐ Certificate

Local Pre-shared Key

••••••••

Remote Peer Pre-shared Key

••••••••|

IPSEC SETTINGS

Lifetime Duration

28800

seconds

120 - 2147483647; (Default: 28800)

Lifetime Size

4608000

kilobytes

10 - 2147483647; (Default: 4608000).
Leave empty for Unlimited.

Additional Options

Diffie-Hellman Group for Perfect Forward Secrecy

No Perfect Forward Secrecy (turned off)

BACK

NEXT

PSK en Lifetime Config

Stap 9. Controleer de configuratie en klik op Voltooien.

Summary

Review your configuration. Click Finish to save the connection, or Back to edit settings. When you click Finish, this information will be copied to the clipboard so that you can save it and use it to configure the remote endpoint.

Vti-Ipsec Connection Profile

 Peer endpoint needs to be configured according to specified below configuration.

**VPN Access
Interface IP**  tunnel10 (1.1.1.1)



Peer IP Address 10.106.63.23

IKE V2

IKE Policy aes-256-sha256-sha256-14

IPSec Proposal aes-256-sha-256

**Authentication
Type** Pre-shared Manual Key

IKE V1: DISABLED

IPSEC SETTINGS

**Lifetime
Duration** 28800 seconds

Lifetime Size 4608000 kilobytes

ADDITIONAL OPTIONS

**Diffie-Hellman
Group** Null (not selected)

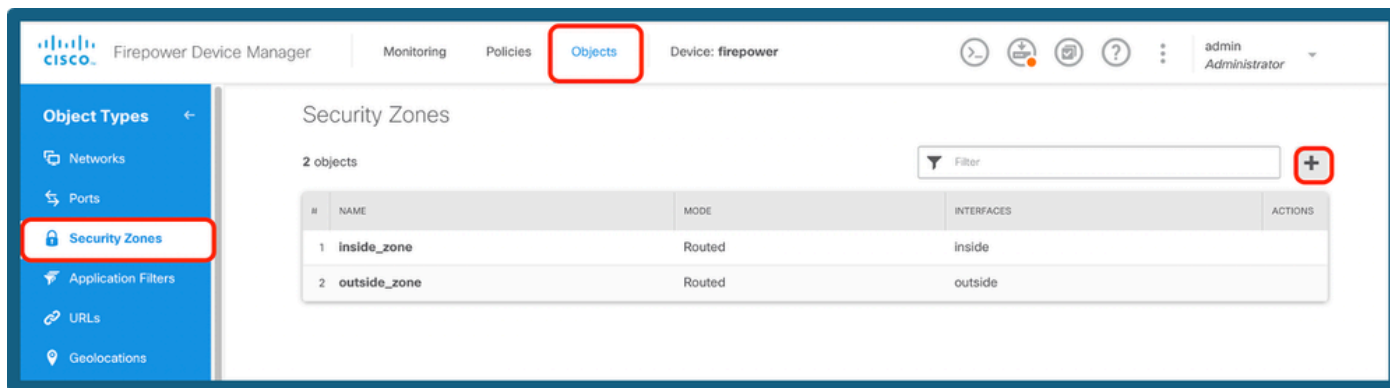
 Information is copied to the clipboard when you click Finish. You must allow the browser to access your clipboard for the copy to be successful.

BACK

FINISH

Configuratieoverzicht

Stap 10a. Navigeer naar Objecten > Beveiligingszones en klik op het + pictogram.



Een beveiligingszone toevoegen

Stap 10b. Maak een zone en selecteer de VTI-interface zoals hieronder wordt weergegeven.

Add Security Zone

Name

vti-zone

Description

Mode

☒ Routed ☐ Passive

Interfaces

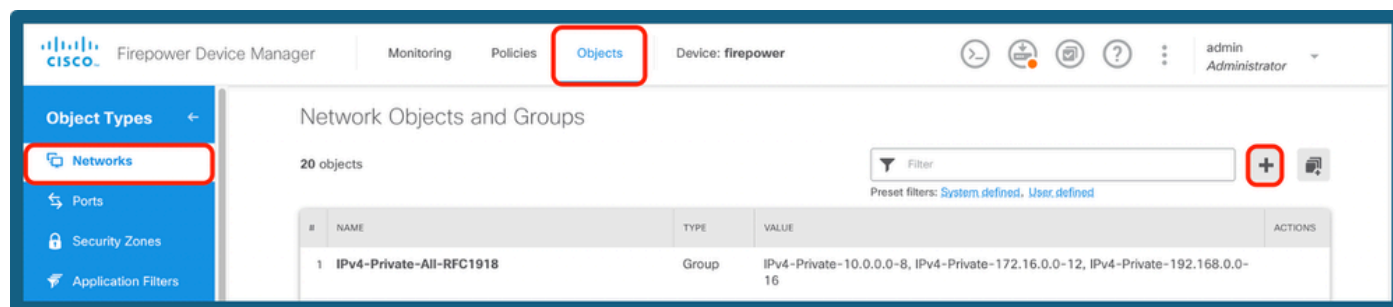
+

0 tunnel10 (Tunnel10)

CANCEL OK

Beveiligingszone configureren

Stap 11a. Navigeer naar Objecten > Netwerken, klik op + pictogram.



Netwerkbobjecten toevoegen

Stap 11b. Voeg een host-object toe en maak een gateway met een IP-tunnel van peer-end.

Edit Network Object

Name

vpn-gateway

Description

Type

☐ Network ☒ **Host** ☐ FQDN ☐ Range

Host

192.168.1.2

e.g. 192.168.2.1 or 2001:DB8::0DB8:800:200C:417A

CANCEL OK

VPN-gateway configureren

Stap 11c. Voeg het externe subnet en het lokale subnet toe.

Edit Network Object



Name

remote-vpn-network

Description

Type



Network



Host



FQDN



Range

Network

172.16.10.0/24

e.g. 192.168.2.0/24 or 2001:DB8:0:CD30::/60

CANCEL

OK

Edit Network Object

?

×

Name

inside-network

Description

Type

☒ Network

☐ Host

☐ FQDN

☐ Range

Network

10.10.10.0/24

e.g. 192.168.2.0/24 or 2001:DB8:0:CD30::/60

CANCEL

OK

Lokale IP-configuratie

Stap 12. Navigeer naar Apparaat > Beleid en configureer het beleid voor toegangscontrole.

Add Access Rule

Order: 1 | Title: vti-acl | Action: Allow

Source/Destination | Applications | URLs | Users | Intrusion Policy | File policy | Logging

SOURCE

Zones	Networks	Ports	SGT Groups
inside_zone	inside-network	ANY	ANY
vti-zone	remote-vpn-...		

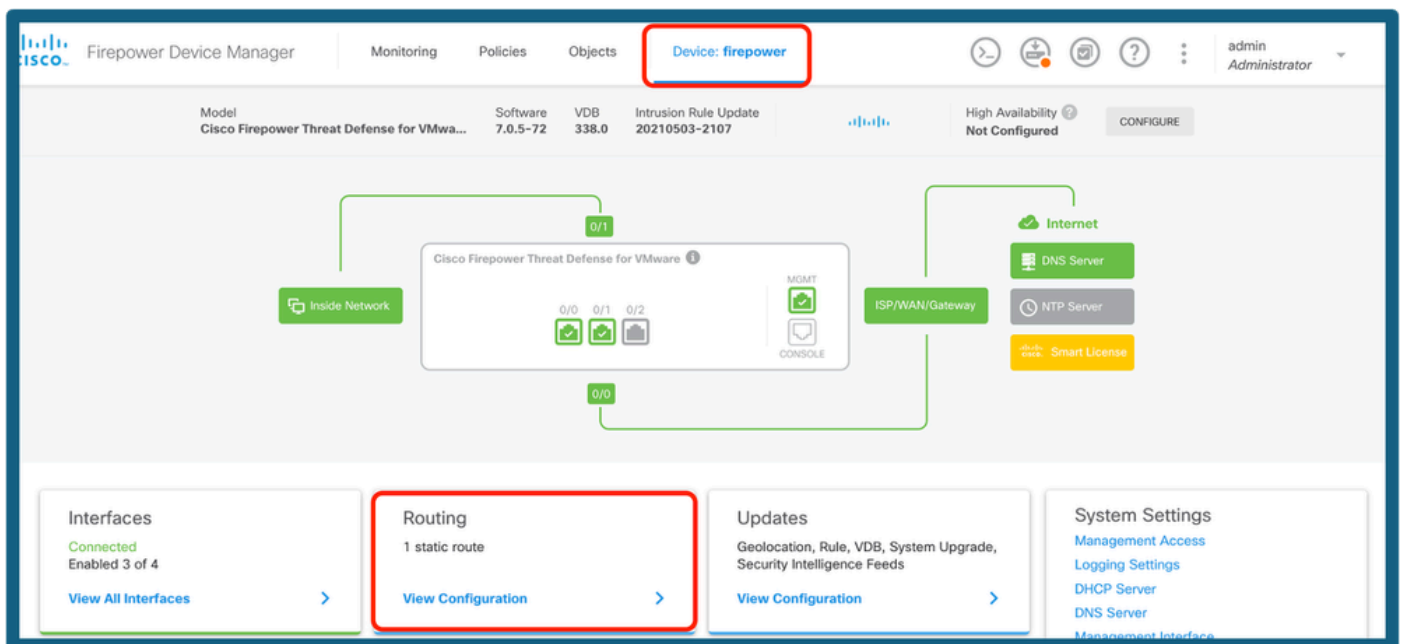
DESTINATION

Zones	Networks	Ports	SGT Groups
inside_zone	inside-network	ANY	ANY
vti-zone	remote-vpn-...		

Show Diagram: ☐ | CANCEL | OK

Toegangscontrolebeleid toevoegen

Stap 13a. Voeg de routing over de VTI-tunnel toe. Navigeer naar Apparaat > Routing.



Routing selecteren

Stap 13b. Navigeer naar Statische route onder het tabblad Routing. Klik op + pictogram.

Device Summary

Routing

Add Multiple Virtual Routers ▼ Commands BGP Global Settings

Static Routing BGP OSPF EIGRP ECMP Traffic Zones

1 route Filter +

#	NAME	INTERFACE	IP TYPE	NETWORKS	GATEWAY IP	SLA MONITOR	METRIC	ACTIONS
1	default	outside	IPv4	0.0.0.0/0	10.106.52.1		1	

Route toevoegen

Stap 13c. Geef de interface op, kies het netwerk, geef de gateway op. Klik op OK.

Add Static Route

Name

vti-route

Description

Interface

tunnel10 (Tunnel10)

Protocol

☒ IPv4

☐ IPv6

Networks

+

remote-vpn-network

Gateway

vpn-gateway

Metric

1

SLA Monitor

Applicable only for IPv4 Protocol type

Please select an SLA Monitor

CANCEL

OK

Statische route configureren

Stap 14. Navigeer naar Implementeren. Controleer de wijzigingen en klik op Nu implementeren.

Pending Changes

?

×

✓

Last Deployment Completed Successfully

26 Jun 2025 05:27 PM. [See Deployment History](#)

Deployed Version (26 Jun 2025 05:27 PM)

Pending Version

LEGEND

+

Static Route Added: *vti-route*

-	metricValue: 1
-	ipType: IPv4
-	name: vti-route
iface:	
-	tunnel10
gateway:	
-	vpn-gateway
networks:	
-	remote-vpn-network

+

Access Rule Added: *vti-acl*

-	logFiles: false
-	eventLogAction: LOG_NONE
-	ruleId: 268435458
-	name: vti-acl
sourceZones:	
-	vti-zone
-	inside_zone
destinationZones:	
-	vti-zone
-	inside_zone
sourceNetworks:	
-	remote-vpn-network
-	inside-network
destinationNetworks:	

MORE ACTIONS ▼

CANCEL

DEPLOY NOW ▼

Implementeer de configuratie

Verifiëren

Nadat de implementatie is voltooid, kunt u de tunnelstatus op de CLI controleren met behulp van de volgende opdrachten:

1. Crypto IKEV2 SA weergeven
2. Crypto IPSec SA <peer-IP> weergeven

```
> show crypto ikev2 sa
```

```
IKEv2 SAs:
```

```
Session-id:2, Status:UP-ACTIVE, IKE count:1, CHILD count:1
```

Tunnel-id	Local	Remote	Status	Role
3294213359	10.106.52.222/500	10.106.63.23/500	READY	INITIATOR
Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK				
Life/Active Time: 86400/141 sec				
Child sa:	local selector 0.0.0.0/0 - 255.255.255.255/65535			
	remote selector 0.0.0.0/0 - 255.255.255.255/65535			
	ESP spi in/out: 0x26a14554/0xd5db88bc			

```
> show crypto ipsec sa
```

```
interface: tunnel10
```

```
Crypto map tag: __vti-crypto-map-5-0-10, seq num: 65280, local addr: 10.106.52.222
```

```
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)  
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)  
current_peer: 10.106.63.23
```

Opdrachten weergeven

Gerelateerde informatie

Voor meer informatie over Site-to-Site VPN's op de FTD beheerd door FDM, kunt u de volledige configuratiehandleiding hier vinden:

[FTD beheerd door FDM Configuration Guide](#)

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.