

# Redundante data-interface implementeren in Azure FTD beheerd met CD-FMC

## Inhoud

---

---

## Inleiding

In dit document worden de stappen beschreven voor het configureren van een door het VCC beheerd virtueel FTD om gebruik te maken van de functie van de redundant beheerder access data interface.

## Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Secure Firewall Management Center
- Cisco Defense Orchestrator

### Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cloud-geleverd Firewallbeheercentrum
- Virtual Secure Firewall Threat Defence versie 7.3.1 gehost in Azure Cloud.

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.

### Verwante producten

Dit document kan ook worden gebruikt voor de volgende hardware- en softwareversies:

- Elk fysiek apparaat dat Firepower Threat Defence versie 7.3.0 of hoger kan uitvoeren.

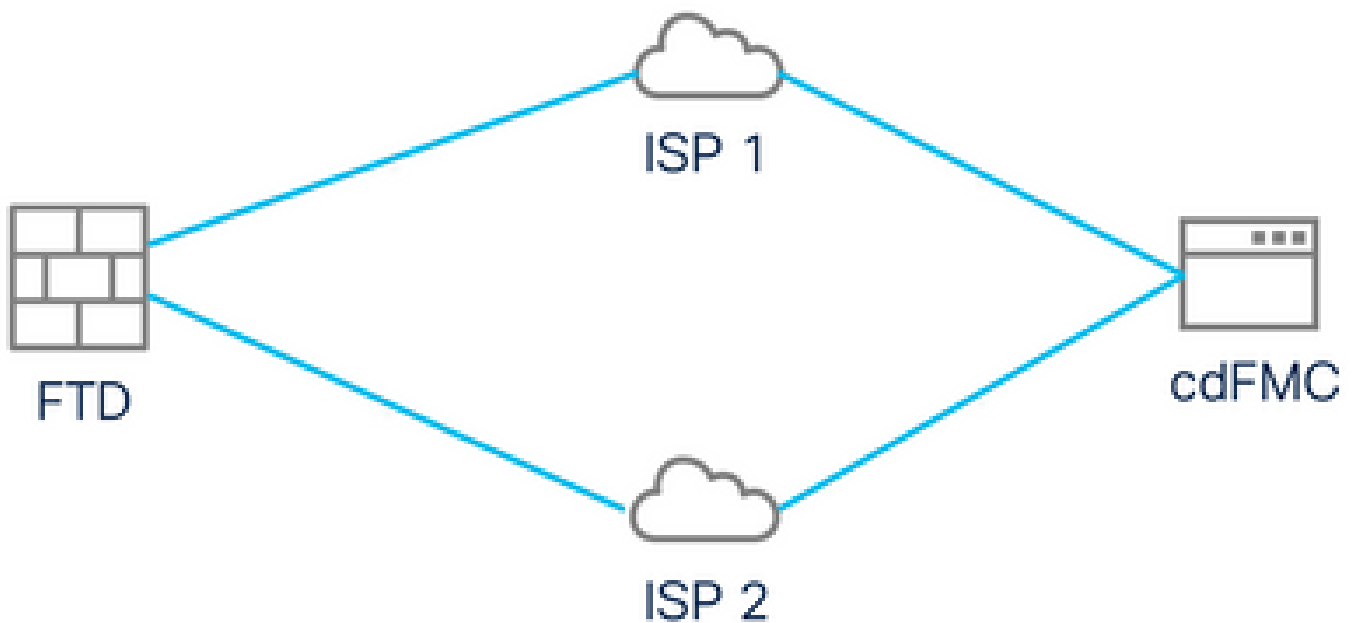
## Achtergrondinformatie

Dit document bevat de stappen voor het configureren en verifiëren van een vFTD die wordt beheerd door een CdFMC om twee gegevensinterfaces te gebruiken voor beheerdoeleinden. Deze functie is vaak handig wanneer klanten een tweede data-interface nodig hebben om hun FTD over het internet te beheren, met behulp van een tweede ISP. Standaard voert de FTD een round-robin taakverdeling uit voor het beheerverkeer tussen beide interfaces; dit kan worden gewijzigd in een Active/Backup-implementatie zoals in dit document wordt beschreven.

Redundant data-interface voor beheerfunctie werd geïntroduceerd in Secure Firewall Threat Defence versie 7.3.0. Er wordt aangenomen dat de vFTD bereikbaar is voor een naamserver die URL's voor CDO-toegang kan oplossen.

## Configuratie

### Netwerkdigram



Netwerkdigram

### Een gegevensinterface configureren voor beheertoegang

Log in op het apparaat via de console en configureer een van de gegevensinterfaces voor beheertoegang met de opdracht configureer netwerkbeheer-data-interface:

```
<#root>
```

```
>
```

```
configure network management-data-interface
```

Note: The Management default route will be changed to route through the data interfaces. If you are connected to the device via SSH, your connection may drop. You must reconnect using the console port.

Data interface to use for management:

GigabitEthernet0/0

Specify a name for the interface [outside]:

outside-1

IP address (manual / dhcp) [dhcp]:

manual

IPv4/IPv6 address:

10.6.2.4

Netmask/IPv6 Prefix:

255.255.255.0

Default Gateway:

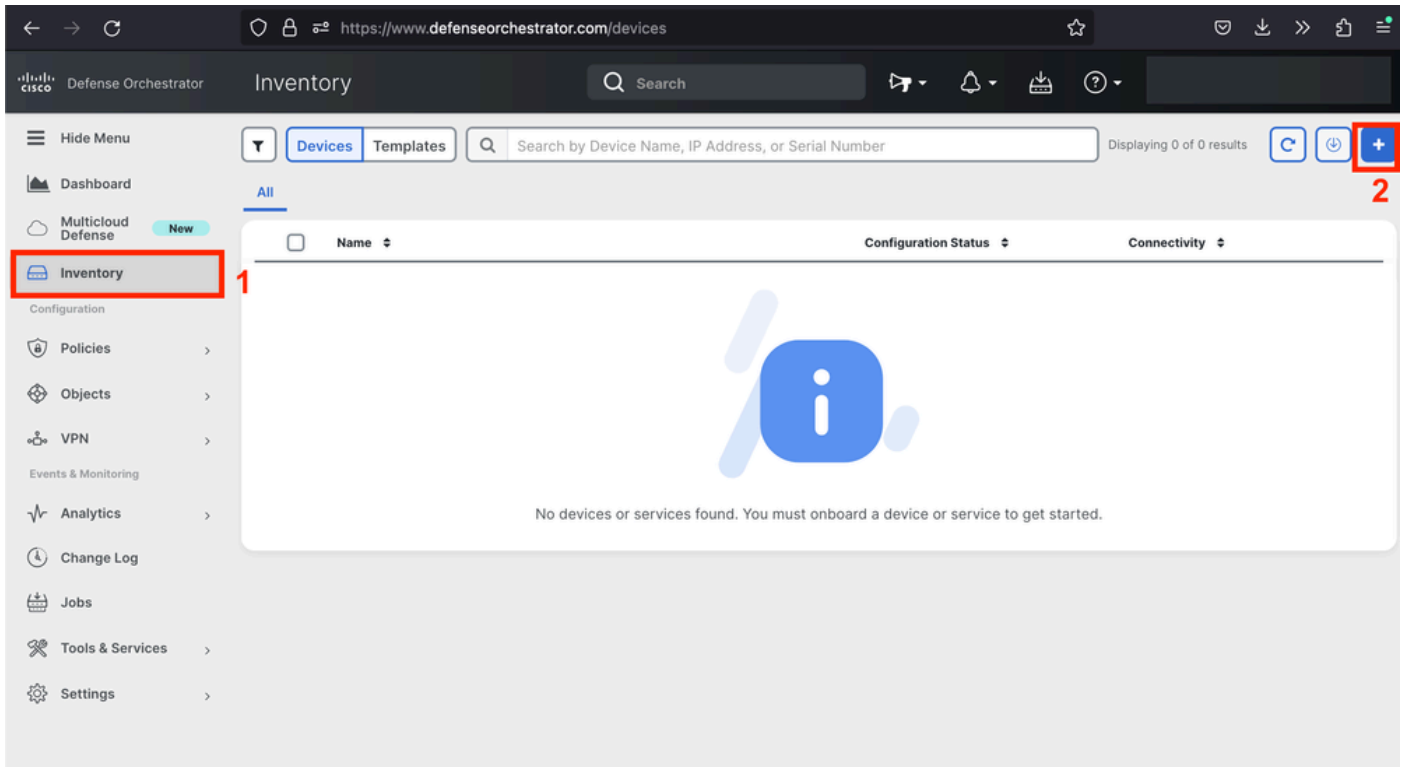
10.6.2.1

Houd in gedachten dat de oorspronkelijke beheerinterface niet kan worden geconfigureerd om DHCP te gebruiken. U kunt het bevel gebruiken toont netwerk om dit te verifiëren.

## Aan boord van de FTD met CDO

Dit proces maakt deel uit van het Azure FTD met CDO, zodat het kan worden beheerd door een FMC dat in de cloud wordt geleverd. Het proces gebruikt een CLI registratiesleutel, die voordelig is als uw apparaat een IP adres heeft dat via DHCP wordt toegewezen. Andere onboarding methodes zoals log-touch levering en serienummer worden alleen ondersteund op Firepower 1000, Firepower 2100 of Secure Firewall 3100 platforms.

Stap 1. Navigeer in de CDO portal naar Inventaris en klik vervolgens op Aan boord optie:



Voorraadpagina

Stap 2. Klik in de FTD-tegel:

## Select a Device or Service Type

No Secure Device Connector found to communicate with some types of devices. [Set up a Secure Device Connector](#)



### ASA

Adaptive Security Appliance  
(8.4+)



### Multiple ASAs

Adaptive Security Appliance  
(8.4+)



### FTD

Cisco Secure  
Firewall Threat Defense

Meraki

### Meraki

Meraki Security Appliance



### Integrations

Enable basic CDO functionality for  
integrations



### AWS VPC

Amazon Virtual Private Cloud



### Duo Admin

Duo Admin Panel

Umbrella

### Umbrella Organization

View Umbrella Organization Policies  
from CDO



### Import

Import configuration for offline  
management

Het aan boord gaan van de FTD

Stap 3. Kies de optie CLI-registratiesleutel gebruiken:



Firewall Threat Defense

**Important:** After onboarding your FTD, it will be managed by Firewall Management Center in CDO. Note that use of the firewall device manager will not be available after onboarding, and all existing policy configurations will be reset. You will need to reconfigure policies from CDO after onboarding. [Learn more](#)



#### Use CLI Registration Key

Onboard a device using a registration key generated from CDO and applied on the device using the Command Line Interface.  
(FTD 7.0.3+ & 7.2+)



#### Use Serial Number

Use this method for low-touch provisioning or for onboarding configured devices using their serial number.  
(FTD 7.2+)



#### Deploy an FTD to a cloud environment

Deploy an FTD to a supported cloud environment; AWS, GCP and Azure

Gebruik de CLI-registratiesleutel

Stap 4. Kopieert de CLI Key vanaf de opdracht Configure Manager:

1 Device Name **FTDv-Azure**

2 Policy Assignment **Access Control Policy: Default Access Control Policy**

3 Subscription License **Performance Tier: FTDv, License: Threat, Malware, URL License**

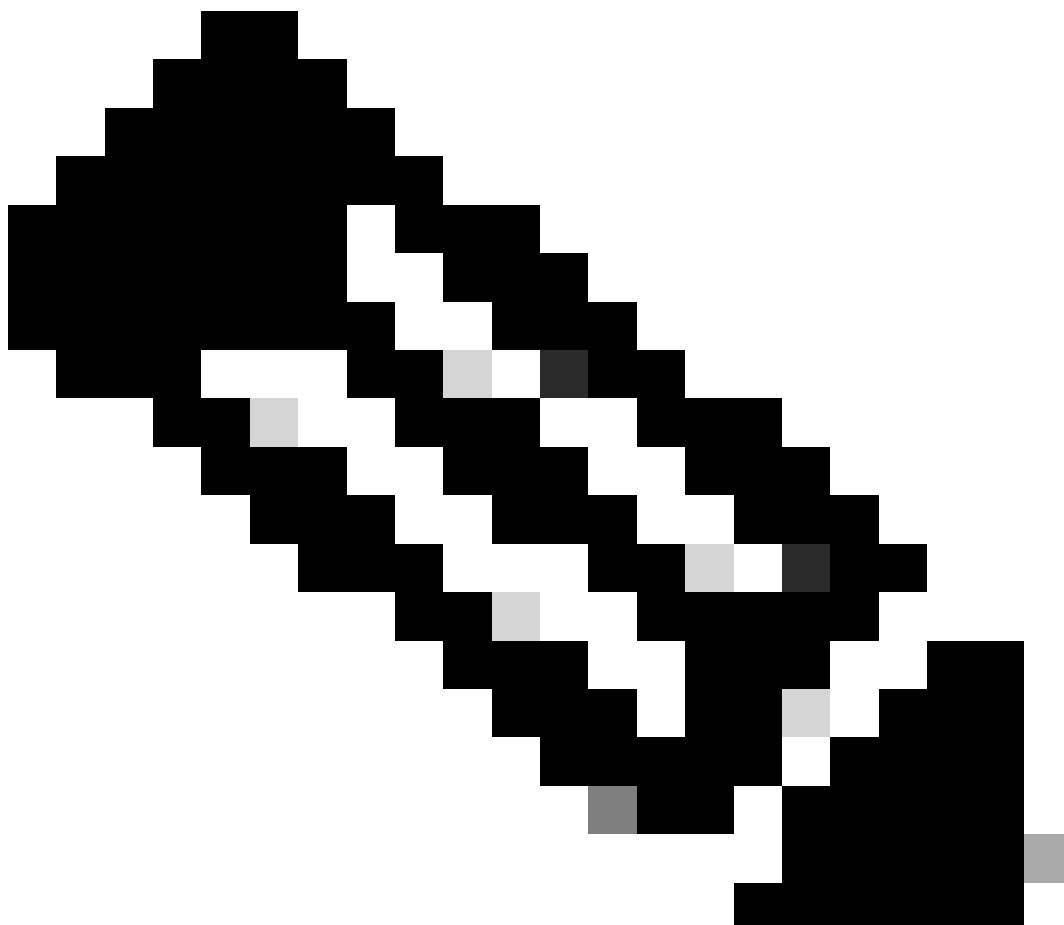
4 CLI Registration Key

- 1 Ensure the device's initial configuration is complete before trying to apply the registration key. [Learn more](#)
- 2 Copy the CLI Key below and paste it into the CLI of the FTD

```
configure manager add cisco-cisco-systems--s1kaau.app.us.cdo.cisco.com  
t67mPqC8cAW6GH2NhhhTUD4poWARdRr7 YJqFWzmpnfbJ6WANBeHTAhXnod9E7c1e cisco-cisco-  
systems--s1kaau.app.us.cdo.cisco.com
```

[Next](#)

Opdracht Configuratiebeheer kopiëren



Opmerking: de CLI-toets komt overeen met het formaat dat wordt gebruikt in registraties

van FTD's met on-prem FMC's, waar u een NAT-ID kunt configureren om registratie toe te staan wanneer uw beheerde apparaat zich achter een NAT-apparaat bevindt: configureer `manager add <fmc-hostname-or-ipv4> <registratiesleutel> <nat-id>`

Stap 5. Plakt de opdracht in de FTD CLI. U moet dit bericht ontvangen als de communicatie succesvol was:

```
Manager cisco-cisco-systems--s1kaau.app.us.cdo.cisco.com successfully configured.  
Please make note of reg_key as this will be required while adding Device in FMC.
```

Stap 6. Ga terug naar de CDO en klik in Volgende:

**3** Subscription License **Performance Tier: FTDv, Licen...**

**4** CLI Registration Key

- 1 Ensure the device's initial
- 2 Copy the CLI Key below a

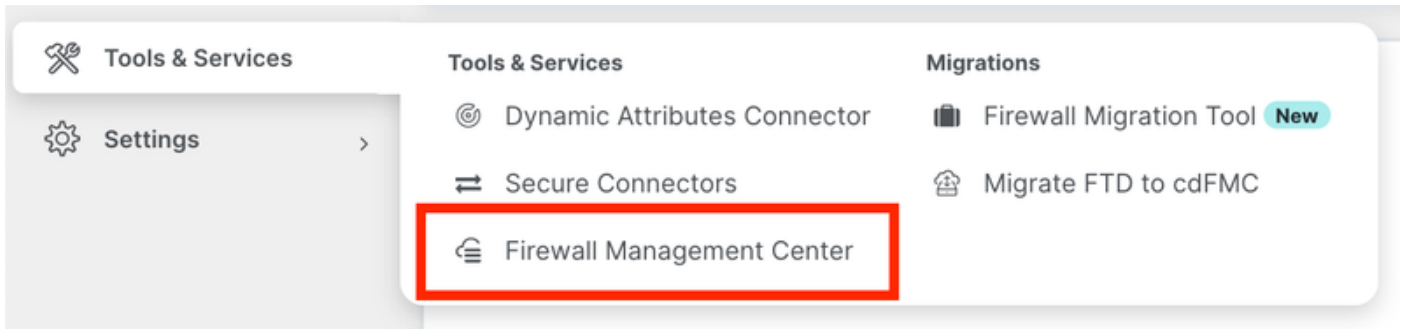
```
configure manager add  
t67mPqC8cAW6GH2NhhhTL  
systems--s1kaau.app.u
```

**Next**

Klik op Volgende

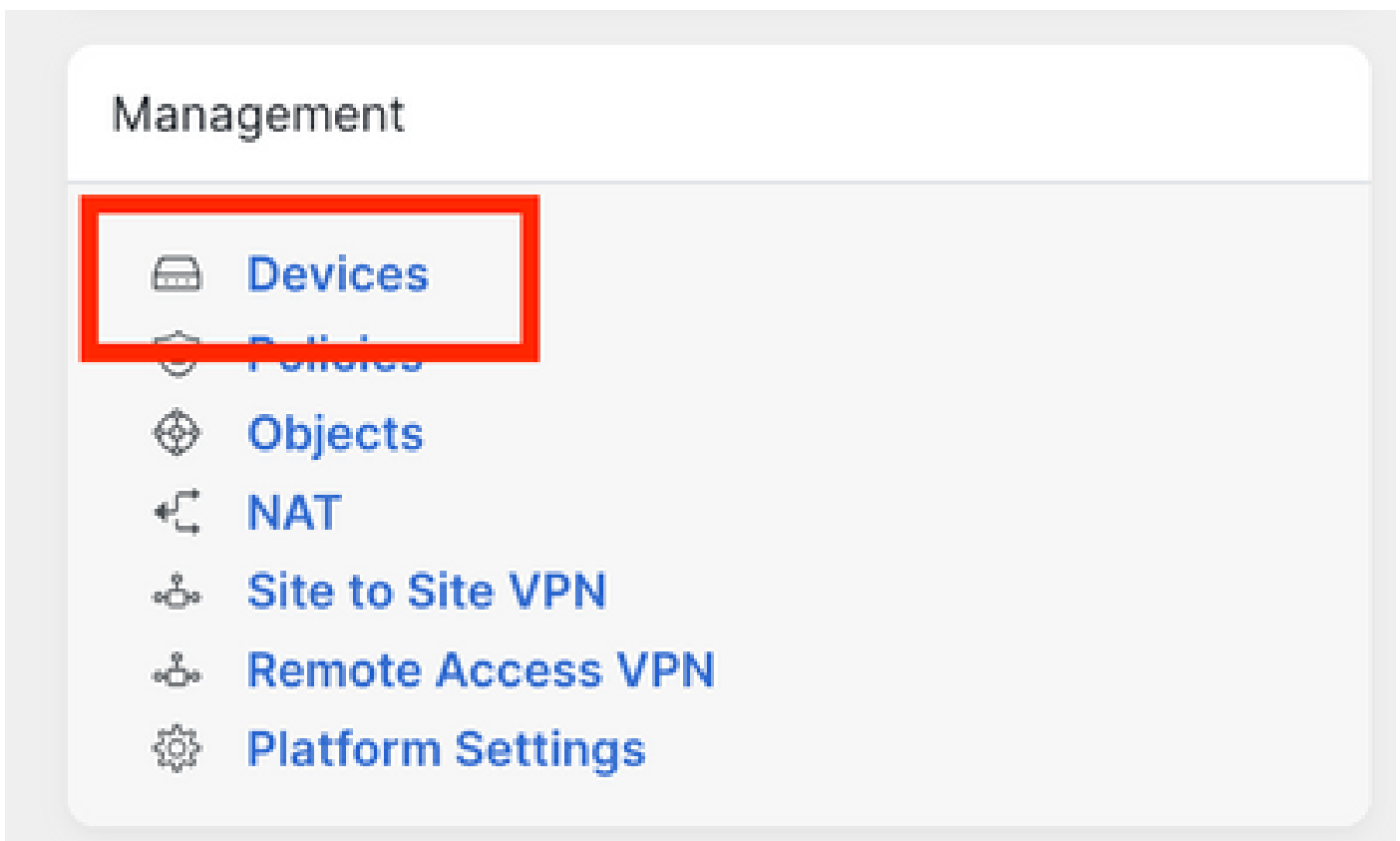
CDO zet het inschrijvingsproces voort en er wordt een bericht weergegeven waarin wordt aangegeven dat het lang zal duren voordat het proces is voltooid. U kunt de status van het inschrijvingsproces controleren door op de koppeling Apparaten op de pagina Services te klikken.

Stap 7. Ga naar uw VCC via de pagina Tools & Services.



Toegang tot het CVMC

Klik op de link Apparaten.



Klik op apparaten

Uw FTD is nu opgenomen in CDO en kan worden beheerd door het FMC dat in de cloud wordt geleverd. In de volgende afbeelding wordt gemeld dat er een NO-IP wordt vermeld onder de apparaatnaam. Dit wordt verwacht in een onboarding proces met behulp van CLI-registratiesleutel.



Defense Orchestrator  
FMC / Devices / Device Management

Analysis Policies **Devices** Objects Integration [Return Home](#) Deploy 🔍 🌐 ⚙️

View By: Group Deployment History

All (1) ● Error (0) ● Warning (0) ● Offline (0) ● Normal (1) ● Deployment Pending (0) ● Upgrade (0) ● Snort 3 (1) 🔍 Search Device Add ▾

[Collapse All](#)

<input type="checkbox"/>	Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	
<input type="checkbox"/>	▼ Ungrouped (1)							
<input type="checkbox"/>	FTDv-Azure NO-IP - Routed	FTDv for Azure	7.3.1	N/A	Essentials, IPS (2 more...)	Default Access Control Policy	🔊	✎ ⋮

Beheerde FTD

## Een redundante data-interface configureren voor beheertoegang

Dit proces wijst een tweede gegevensinterface toe voor beheertoegang.

Stap 1. Klik op het tabblad Apparaten in het potloodpictogram voor toegang tot de FTD-bewerkingsmodus:

Defense Orchestrator  
FMC / Devices / Device Management

Analysis Policies **Devices** Objects Integration [Return Home](#) Deploy 🔍 🌐 ⚙️

View By: Group Deployment History

All (1) ● Error (0) ● Warning (0) ● Offline (0) ● Normal (1) ● Deployment Pending (0) ● Upgrade (0) ● Snort 3 (1) 🔍 Search Device Add ▾

[Collapse All](#)

<input type="checkbox"/>	Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	
<input type="checkbox"/>	▼ Ungrouped (1)							
<input type="checkbox"/>	FTDv-Azure NO-IP - Routed	FTDv for Azure	7.3.1	N/A	Essentials, IPS (2 more...)	Default Access Control Policy	🔊	✎ ⋮

Het FTD bewerken

Stap 2. Bewerk vanuit het tabblad Interface de interface die zal worden toegewezen als de redundante beheerinterface. Als dit nog niet eerder is gedaan, configureer dan een interfacenaam en een IP-adres.

Stap 3. In het tabblad Manager Access schakelt u het aanvinkvakje Beheer op deze interface inschakelen in voor de beheerder:

## Edit Physical Interface



General

IPv4

IPv6

Path Monitoring

Hardware Configuration

Manager Access

Advanced

Enable management on this interface for the Manager

Available Networks



Search

any-ipv4  
any-ipv6  
IPv4-Benchmark-Tests  
IPv4-Link-Local  
IPv4-Multicast  
IPv4-Private-10.0.0.0-8

Add

Allowed Management Networks

any

Cancel

OK

Manager-toegang inschakelen

Stap 4. Zorg er in het tabblad Algemeen voor dat de interface is toegewezen aan een beveiligingszone en klik vervolgens op OK:

## Edit Physical Interface



General

IPv4

IPv6

Path Monitoring

Hardware Configuration

Manager Access

Advanced

Name:

outside-2

Enabled

Management Only

Description:

Mode:

None

Security Zone:

outside2-sz

Security Zone voor redundante data-interface

Stap 5. Bericht dat nu beide interfaces de markering van de Toegang van de Manager hebben. Bovendien, zorg ervoor dat de primaire data-interface a is toegewezen aan een andere Security Zone:

FTDv-Azure  
Cisco Firepower Threat Defense for Azure

Device Routing **Interfaces** Inline Sets DHCP VTEP

Search by name Sync Device Add Interfaces

Interface	Logical N...	Typ	Security Z...	MAC Address (Active/Standby)	IP Address	Path...	Virtual Ro...
Diagnostic0/0	diagnostic	Phy				Disa...	Global
GigabitEthernet0/0 (Manager Access)	outside-1	Phy	outside1-sz		10.6.2.4/255.255.255.0(Static)	Disa...	Global
GigabitEthernet0/1 (Manager Access)	outside-2	Phy	outside2-sz		10.6.3.4/255.255.255.0(Static)	Disa...	Global

Beoordeling van interfaceconfiguratie

In de volgende sectie, zijn de stappen 6 tot 10 bedoeld om twee gelijke kosten standaardroutes te vormen om CDO te bereiken, elk die door een onafhankelijk SLA het volgen proces wordt gecontroleerd. De SLA-tracering zorgt ervoor dat er een functioneel pad is om met de cdFMC te communiceren via de gecontroleerde interface.

Stap 6. Navigeer naar het tabblad Routing en creëer in het ECMP-menu een nieuwe ECMP-zone met beide interfaces erin:

FTDv-Azure  
Cisco Firepower Threat Defense for Azure

Device **Routing** Interfaces Inline Sets DHCP VTEP

Manage Virtual Routers

Global

Virtual Router Properties

**ECMP**

BFD

OSPF

OSPFv3

EIGRP

RIP

Policy Based Routing

BGP

IPv4

IPv6

Static Route

Multicast Routing

IGMP

PIM

Multicast Routes

Multicast Boundary Filter

General Settings

BGP

Equal-Cost Multipath Routing (ECMP)

Add

Add ECMP

Name

outside-ecmp

Available Interfaces

Selected Interfaces

outside-1

outside-2

Add

Cancel OK

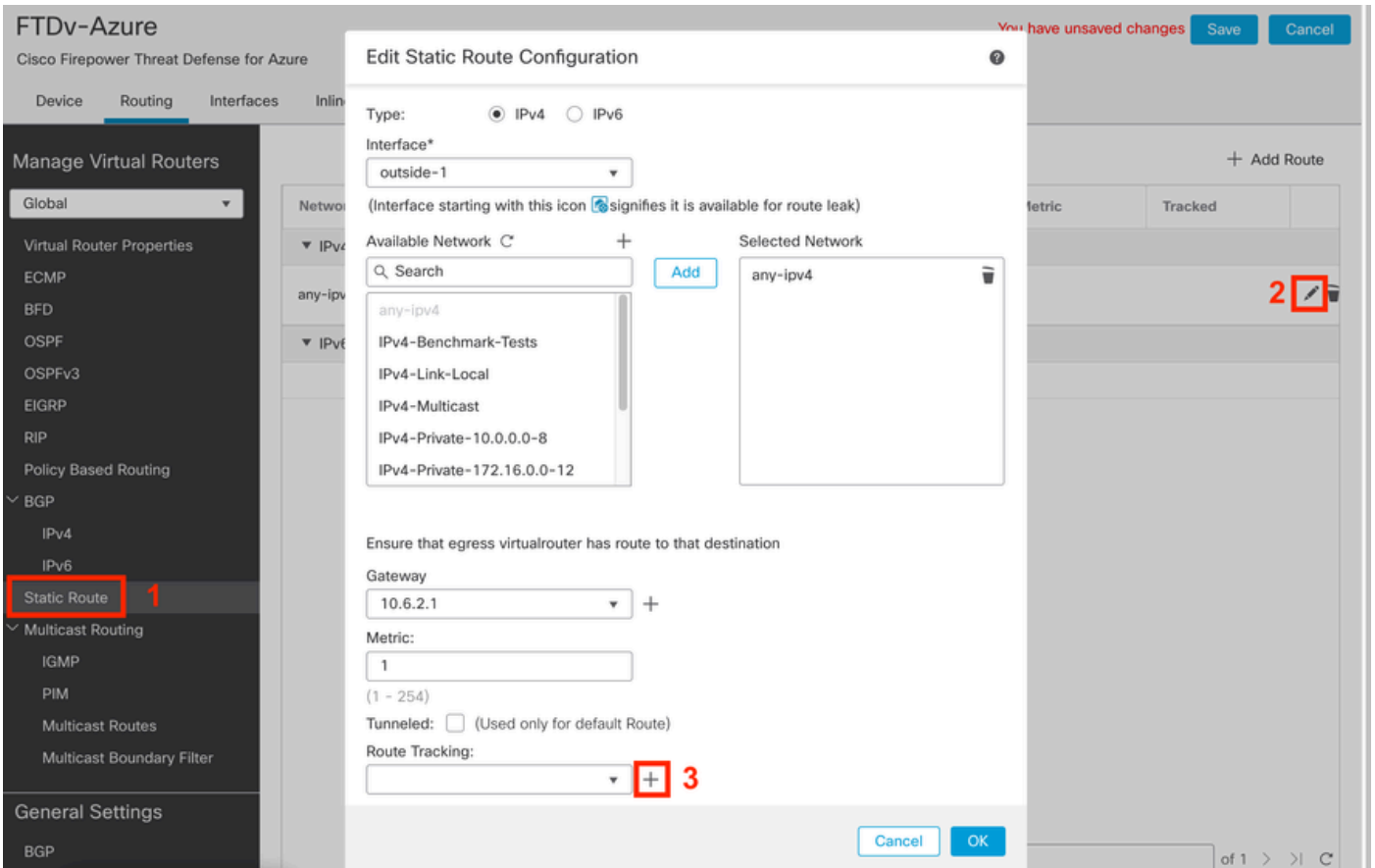
Een ECMP-zone configureren

Klik op OK en Sla op.

Stap 7. Van het tabblad Routing navigeer je naar Statische routers.

Klik in het potloodpictogram om uw primaire route te bewerken. Klik vervolgens op het plusteken

om een nieuw SLA-trackingobject toe te voegen:



Primaire route bewerken om SLA-tracering toe te voegen

Stap 8. De vereiste parameters voor een functionele SLA-tracering worden in de volgende afbeelding gemarkeerd. Optioneel kunt u andere instellingen afstemmen zoals Aantal pakketten, Time-out en frequentie.

# Edit SLA Monitor Object



Name:

outside1-sla

Description:

Frequency (seconds):

60

(1-604800)

SLA Monitor ID\*:

1

Threshold (milliseconds):

5000

(0-60000)

Timeout (milliseconds):

5000

(0-604800000)

Data Size (bytes):

28

(0-16384)

ToS:

0

Number of Packets:

1

Monitor Address\*:

Available Zones

Search

outside1-sz

outside2-sz

Selected Zones/Interfaces

Add

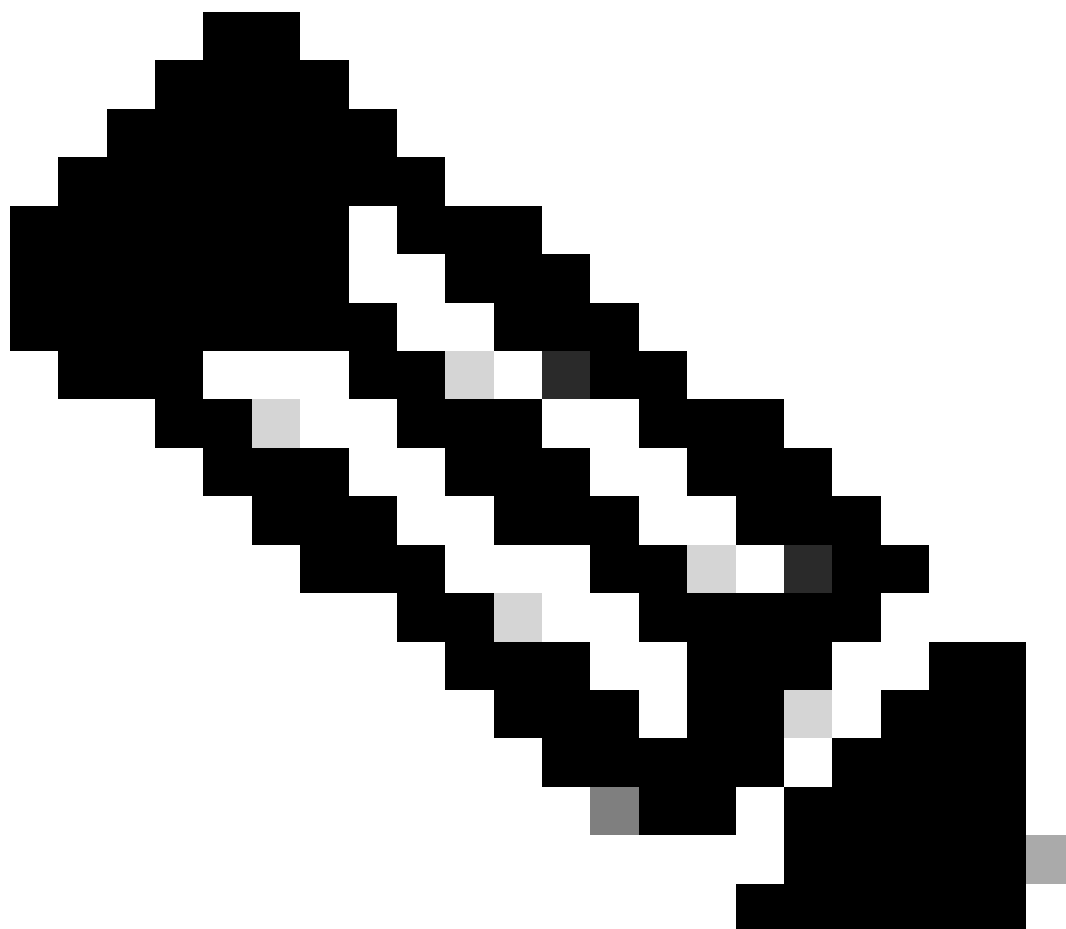
outside1-sz

Cancel

Save

In dit voorbeeld werd Google DNS IP gebruikt om FTD-mogelijkheden te monitoren om internet (en CDO) te bereiken via de buitenkant1-interface. Klik op OK wanneer u klaar bent.

---



Opmerking: Zorg ervoor dat u een IP volgt die al is geverifieerd als bereikbaar via uw FTD buiteninterface. Het configureren van een track met een onbereikbare IP kan de standaardroute in dit FTD omlaag brengen en vervolgens voorkomen dat deze kan communiceren met CDO.

---

Stap 9. Klik op Opslaan en zorg ervoor dat de nieuwe SLA-tracering is toegewezen aan de route die naar de primaire interface wijst:

## Route Tracking:



Buiten 1 SLA-tracering

Zodra u op OK klikt, wordt een pop-up weergegeven met het volgende WAARSCHUWING-bericht:

## Warning about Static Route

**This Static route is defined on the Defense Orchestrator Access Interface. Ensure the change is not affecting connectivity to the device**

OK

Waarschuwing voor configuratie

Stap 10. Klik op Add Route optie om een nieuwe route toe te voegen voor de redundante data-interface. Bericht van het volgende beeld dat de Metrische waarde voor de route het zelfde is; bovendien, heeft het volgen SLA een verschillende ID:

# Add Static Route Configuration



Type:  IPv4  IPv6

Interface\*

outside-2

(Interface starting with this icon signifies it is available for route leak)

Available Network



Search

Add

any-ipv4

IPv4-Benchmark-Tests

IPv4-Link-Local

IPv4-Multicast

IPv4-Private-10.0.0.0-8

IPv4-Private-172.16.0.0-12

Selected Network

any-ipv4

Gateway\*

10.6.3.1



Metric:

1

(1 - 254)

Tunneled:  (Used only for default Route)

Route Tracking:

outside2-sla



Cancel

OK

Redundante statische route configureren



# Edit SLA Monitor Object



Name:

outside2-sla

Description:

Frequency (seconds):

60

(1-604800)

SLA Monitor ID\*:

2

Threshold (milliseconds):

5000

(0-60000)

Timeout (milliseconds):

5000

(0-604800000)

Data Size (bytes):

28

(0-16384)

ToS:

0

Number of Packets:

1

Monitor Address\*

Available Zones

outside1-sz

outside2-sz

Add

Selected Zones/Interfaces

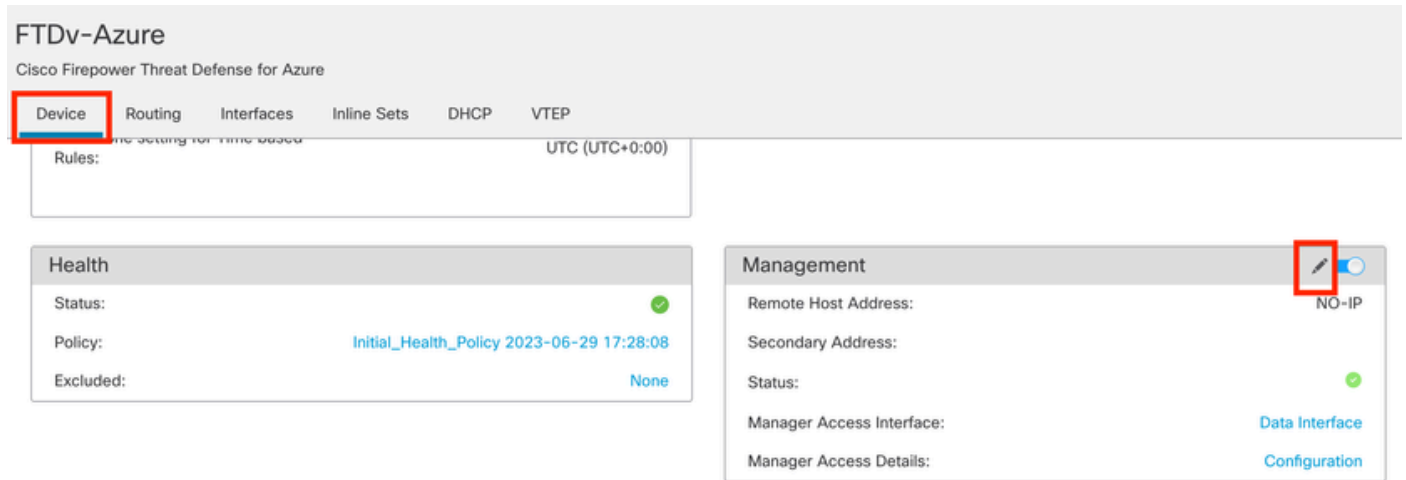
outside2-sz

Cancel

Save

Klik op Save (Opslaan).

Stap 11. U kunt desgewenst de secundaire gegevensinterface IP opgeven onder Apparaat > Beheer. Ondanks dat is dit niet nodig, gezien het feit dat de huidige onboarding methode het CLI-registratiesleutelproces gebruikte:



(Optioneel) Specificeer een IP voor redundante data-interface in het veld Beheer

Stap 12. Breng de veranderingen aan.

(Optioneel) Stel een interfaceprijs in voor een Active/Backup-interfacemodus:

Standaard wordt bij redundant beheer via data-interface round robin gebruikt om het beheerverkeer tussen beide interfaces te distribueren. Als een WAN-link een grotere bandbreedte heeft dan de andere en u wilt dat dit de primaire beheerlink is terwijl de andere als back-up blijft, kunt u de primaire link een kostprijs van 1 geven en de back-uplink een kostprijs van 2 geven. In het volgende voorbeeld wordt de interface Gigabit Ethernet0/0 behouden als de primaire WAN-link, terwijl Gigabit Ethernet0/1 fungeert als de back-upbeheerlink:

1. Navigeer naar Apparaten > FlexConfig-link en maak een flexConfig-beleid. Als er al een flexConfig-beleid is geconfigureerd en toegewezen aan uw FTD, bewerk het:

Device Management	VPN	Troubleshoot
Device Upgrade	Site To Site	File Download
NAT	Remote Access	Threat Defense CLI
QoS	Dynamic Access Policy	Packet Tracer
Platform Settings	Troubleshooting	Packet Capture
<b>FlexConfig</b>	Site to Site Monitoring	
Certificates		

Het menu FlexConfig gebruiken

## 2. Een nieuw FlexConfig-object maken:

- Geef een naam aan het object FlexConfig.
- Kies Everytime en voeg toe in de secties Implementatie en Type.
- Stel de kosten voor de interfaces in met de volgende opdrachten zoals weergegeven in afbeelding 2.
- Klik op Save (Opslaan).

```
<#root>
```

```
interface GigabitEthernet0/0
```

```
    policy-route cost 1
```

<=== A cost of 1 means this will be the primary interface for management communication with CDO tenant.

```
interface GigabitEthernet0/1
```

```
    policy-route cost 2
```

<=== Cost 2 sets this interface as a backup interface.

Defense Orchestrator  
FMC / Devices / Flexconfig Policy Editor

Analysis Policies Devices Objects Integration

MyFlexconfig  
Enter Description

Available FlexConfig

FlexConfig Object

User Defined

System Defined

- Default\_DNS\_Configure
- Default\_Inspection\_Protocol\_Disable
- Default\_Inspection\_Protocol\_Enable
- DHCPv6\_Prefix\_Delegation\_Configure
- DHCPv6\_Prefix\_Delegation\_UnConfigure
- DNS\_Configure
- DNS\_UnConfigure
- Eigrp\_Configure
- Eigrp\_Interface\_Configure
- Eigrp\_UnConfigure
- Eigrp\_Unconfigure\_All
- Inspect\_IPv6\_Configure
- Inspect\_IPv6\_UnConfigure
- ISIS\_Configure
- ISIS\_Interface\_Configuration
- ISIS\_Unconfigure
- ISIS\_Unconfigure\_All
- Netflow\_Add\_Destination
- Netflow\_Clear\_Parameters

Add FlexConfig Object

Name: InterfaceCost

Description:

Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.

Insert Deployment: Everytime Type: Append

```
interface GigabitEthernet0/0
policy-route cost 1
interface GigabitEthernet0/1
policy-route cost 2
```

Variables

Name	Dimension	Default Value	Property (Type:Name)	Override	Description
No records to display					

Cancel Save

Een Flexconfig-object toevoegen

3. Kies het recent gemaakte object en voeg het toe aan de geselecteerde sectie FlexConfigurs toevoegen zoals in de afbeelding. Sla de wijzigingen op en implementeer uw configuratie.

Defense Orchestrator  
Flexconfig Policy Editor

Analysis Policies Devices Objects Integration [Return Home](#) **Deploy** 5 ✓ ⚙️ ?

MyFlexconfig Migrate Config Preview Config **Save** 4 Cancel

Enter Description Policy Assignments (1)

Available FlexConfig FlexConfig Object

- ✓ User Defined
  - InterfaceCost** 1
- System Defined
  - Default\_DNS\_Configure
  - Default\_Inspection\_Protocol\_Disable
  - Default\_Inspection\_Protocol\_Enable
  - DHCPv6\_Prefix\_Delegation\_Configure
  - DHCPv6\_Prefix\_Delegation\_UnConfigure
  - DNS\_Configure
  - DNS\_UnConfigure
  - Eigrp\_Configure
  - Eigrp\_Interface\_Configure
  - Eigrp\_UnConfigure
  - Eigrp\_Unconfigure\_All
  - Inspect\_IPv6\_Configure
  - Inspect\_IPv6\_UnConfigure
  - ISIS\_Configure
  - ISIS\_Interface\_Configuration
  - ISIS\_Unconfigure
  - ISIS\_Unconfigure\_All
  - Netflow\_Add\_Destination

Selected Prepend FlexConfigs

#	Name	Description

Selected Append FlexConfigs

#	Name	Description
1	InterfaceCost	

Het object toe wijzen aan het Flexconfiguratiebeleid

4. Breng de veranderingen aan.

## Verifiëren

1. Om te verifiëren, gebruik het bevel tonen netwerk. Er wordt een nieuw exemplaar voor de redundante beheerinterface gevormd:

```
> show network
```

```
<<----- output omitted for brevity ----->>
```

```
=====[ eth0 ]=====
State : Enabled
Link : Up
Channels : Management & Events
Mode : Non-Autonegotiation
MDI/MDIX : Auto/MDIX
MTU : 1500
MAC Address : 60:45:BD:D8:62:D7
-----[ IPv4 ]-----
Configuration : Manual
```

```

Address : 10.6.0.4
Netmask : 255.255.255.0
-----[ IPv6 ]-----
Configuration : Disabled

=====[ Proxy Information ]=====
State : Disabled
Authentication : Disabled
. . .

=====[ GigabitEthernet0/0 ]=====
State : Enabled
Link : Up
Name : outside-1
MTU : 1500
MAC Address : 60:45:BD:D8:6F:5C
-----[ IPv4 ]-----
Configuration : Manual
Address : 10.6.2.4
Netmask : 255.255.255.0
Gateway : 10.6.3.1
-----[ IPv6 ]-----
Configuration : Disabled

=====[ GigabitEthernet0/1 ]=====
State : Enabled
Link : Up
Name : outside-2
MTU : 1500
MAC Address : 60:45:BD:D8:67:CA
-----[ IPv4 ]-----
Configuration : Manual
Address : 10.6.3.4
Netmask : 255.255.255.0
Gateway : 10.6.3.1
-----[ IPv6 ]-----
Configuration : Disabled

```

2. De interface maakt nu deel uit van het sftunneldomein. U kunt dit bevestigen met de show sftunnelinterfaces en de show in werking stelt -in werking stellen -in werking stellen sftunnel opdrachten:

```
<#root>
```

```
>
```

```
show sftunnel interfaces
```

```
Physical Interface Name of the Interface
```

```
GigabitEthernet0/0 outside-1
```

```
GigabitEthernet0/1 outside-2
```

```
>
```

```
show running-config sftunnel
```

```
sftunnel interface outside-2
```

```
sftunnel interface outside-1
sftunnel port 8305
sftunnel route-map FMC_GEN_19283746_RBD_DUAL_WAN_RMAP_91827346
```

3. Er wordt automatisch een op beleid gebaseerde route aangegeven. Als u geen interfacekosten hebt opgegeven, stelt de optie adaptieve interface de verwerking van het robot in om het beheerverkeer tussen beide interfaces in evenwicht te brengen:

```
<#root>
```

```
>
```

```
show running-config route-map
```

```
!
```

```
route-map FMC_GEN_19283746_RBD_DUAL_WAN_RMAP_91827346 permit 5
 match ip address FMC_GEN_056473829_RBD_DUAL_WAN_ACL_165748392
 set adaptive-interface cost outside-1 outside-2
```

```
>
```

```
show access-list FMC_GEN_056473829_RBD_DUAL_WAN_ACL_165748392
```

```
access-list FMC_GEN_056473829_RBD_DUAL_WAN_ACL_165748392; 1 elements; name hash: 0x8e8cb508
access-list FMC_GEN_056473829_RBD_DUAL_WAN_ACL_165748392 line 1 extended permit tcp any any eq 8305 (hi
```

4. Gebruik de opdracht show in werking stellen-configuratieinterface <interface> om de interfacestanden te controleren:

```
<#root>
```

```
>
```

```
show running-config interface GigabitEthernet 0/0
```

```
!
```

```
interface GigabitEthernet0/0
 nameif outside-1
 security-level 0
 zone-member outside-ecmp
 ip address 10.6.2.4 255.255.255.0
 policy-route cost 1
```

```
>
```

```
show running-config interface GigabitEthernet 0/1
```

```
!
```

```
interface GigabitEthernet0/1
 nameif outside-2
 security-level 0
 zone-member outside-ecmp
```

```
ip address 10.6.3.4 255.255.255.0
policy-route cost 2
```

Sommige extra bevelen kunnen worden gebruikt om het volgen van de gevormde routes te controleren:

```
<#root>
```

```
>
```

```
show track
```

```
Track 1
```

```
Response Time Reporter 2 reachability
```

```
Reachability is Up
```

```
<===== Ensure reachability is up for the monitored interf
```

```
2 changes, last change 09:45:00
```

```
Latest operation return code: OK
```

```
Latest RTT (milliseconds) 10
```

```
Tracked by:
```

```
STATIC-IP-ROUTING 0
```

```
Track 2
```

```
Response Time Reporter 1 reachability
```

```
Reachability is Up
```

```
<===== Ensure reachability is up for the monitored interf
```

```
2 changes, last change 09:45:00
```

```
Latest operation return code: OK
```

```
Latest RTT (milliseconds) 1
```

```
Tracked by:
```

```
STATIC-IP-ROUTING 0
```

```
>
```

```
show route
```

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
```

```
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
```

```
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```

```
E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
```

```
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
```

```
ia - IS-IS inter area, * - candidate default, U - per-user static route
```

```
o - ODR, P - periodic downloaded static route, + - replicated route
```

```
SI - Static InterVRF, BI - BGP InterVRF
```

```
Gateway of last resort is 10.6.3.1 to network 0.0.0.0
```

```
S* 0.0.0.0 0.0.0.0 [1/0] via 10.6.3.1, outside-2
```

```
[1/0] via 10.6.2.1, outside-1
```

```
C 10.6.2.0 255.255.255.0 is directly connected, outside-1
```

```
L 10.6.2.4 255.255.255.255 is directly connected, outside-1
```

```
C 10.6.3.0 255.255.255.0 is directly connected, outside-2
```

```
L 10.6.3.4 255.255.255.255 is directly connected, outside-2
```

## Gerelateerde informatie



- [Cisco Technical Support en downloads](#)
- [Firewallbeveiliging tegen bedreigingen beheren met cloudbeheerd Firewallbeheercentrum in Cisco Defense Orchestrator](#)

## 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.