

PBR configureren met HTTP-padmonitor op FMC

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Netwerkdigram](#)

[PBR configureren voor HTTP Path Monitoring](#)

[Equal-cost-multi-path \(ECMP\) configureren](#)

[Vertrouwde DNS configureren voor beveiligde FTD](#)

[Padbewaking inschakelen](#)

[Bewakingsdashboard toevoegen](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

Inleiding

In dit document wordt beschreven hoe u Policy-Based Routing (PBR) configureert met HTTP Path Monitoring in het Cisco Secure Firewall Management Center (FMC).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- PBR basiskennis
- Basiservaring met Cisco Secure Management Center
- Cisco Secure Firewall Threat Defense (FTD)

Gebruikte componenten

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

- Cisco Secure Firewall Management Center Virtual (FMCv) VMware met versie 7.4
- Cisco Secure Firewall Threat Defense Virtual Appliance (FTDv) VMware met versie 7.4

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

Bij traditionele routing worden pakketten gerouteerd op basis van het IP-adres van de bestemming, maar het is moeilijk om de routing van het opgegeven verkeer in een bestemmingsgebaseerd routingssysteem te wijzigen. PBR geeft u meer controle over routing door de bestaande mechanismen van routingsprotocollen uit te breiden en aan te vullen.

Met PBR kan de IP-prioriteit worden ingesteld. Het maakt het ook mogelijk om een pad voor bepaald verkeer te specificeren, zoals prioritair verkeer over een dure verbinding. Met PBR is routing gebaseerd op andere criteria dan het bestemmingsnetwerk, zoals bronpoort, bestemmingsadres, bestemmingspoort, protocoltoepassingen of een combinatie van deze objecten. PBR kan worden gebruikt om het netwerkverkeer te classificeren op basis van toepassing, gebruikersnaam, groepslidmaatschap en associatie met beveiligingsgroepen. Deze routingsmethode is van toepassing in situaties waarin tal van apparaten toegang hebben tot toepassingen en gegevens in een grote netwerkimplementatie. Traditioneel hebben grote implementaties topologieën die al het netwerkverkeer naar een hub terugvoeren als gecodeerd verkeer in een routeerde VPN. Deze topologieën resulteren vaak in problemen zoals pakketlatentie, verminderde bandbreedte en pakketval.

PBR wordt alleen ondersteund in de gerouteerde firewallmodus en wordt niet toegepast voor embryonale verbindingen. HTTP-gebaseerde applicatie wordt ondersteund op fysieke, poortkanaal, subinterfaces en status tunnel interfaces. Het wordt niet ondersteund op clusterapparaten.

Wanneer geconfigureerde interfaces metrics afleiden zoals retourtijd (RTT), jitter, gemiddelde opiniesscore (MOS) en pakketverlies per interface, worden ze gebruikt om het beste pad te bepalen voor het routeren van PBR-verkeer. Path Monitoring berekent flexibele metrics voor meerdere externe peers per interface. Om het beste pad voor meerdere toepassingen te bewaken en te bepalen via een beleid voor een filiaalfirewall, heeft HTTP om deze redenen de voorkeur boven ICMP:

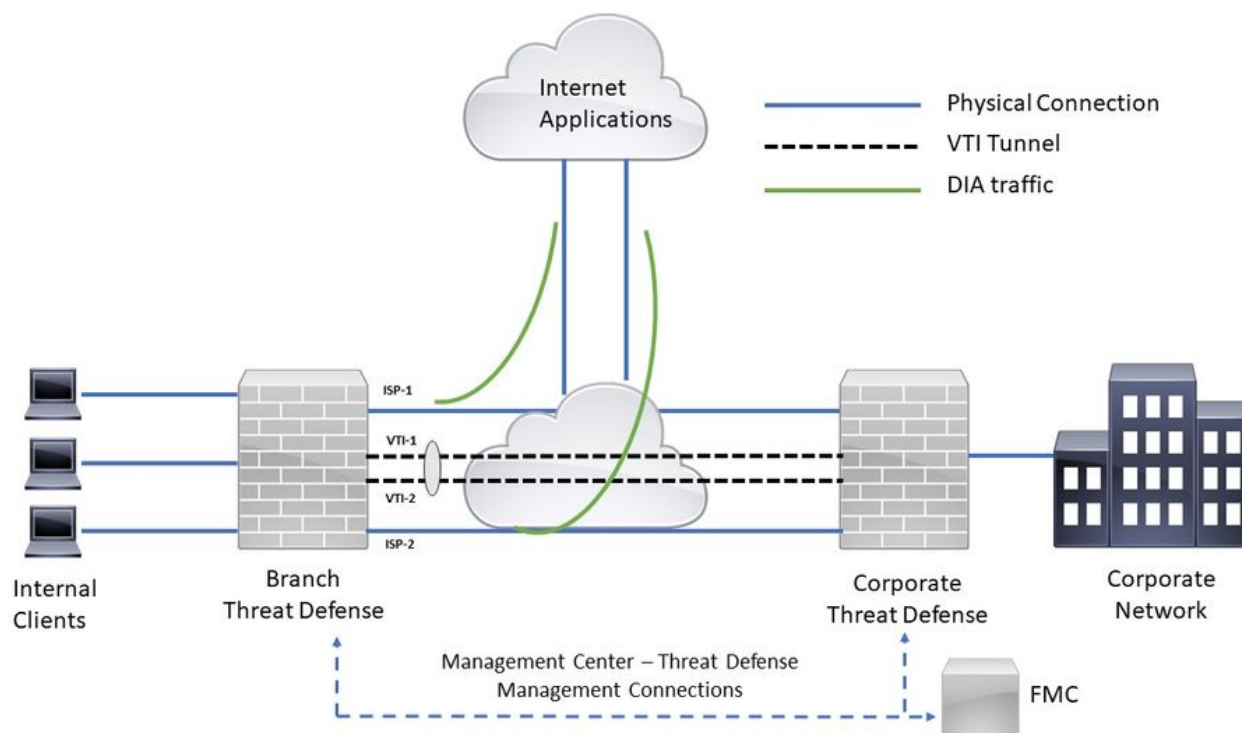
- HTTP-ping kan de prestatiemetingen van het pad afleiden naar de applicatielaag van de server, waar de applicatie wordt gehost.
- De noodzaak om de firewallconfiguratie te wijzigen wanneer het IP-adres van de toepassingsserver wordt gewijzigd, wordt verwijderd omdat het toepassingsdomein wordt gevolgd in plaats van het IP-adres.

Configureren

Netwerkdigram

Overweeg een typisch bedrijfsnetwerkscenario waarbij al het filiaalnetwerkverkeer wordt

verzonden via een routegebaseerde VPN van het bedrijfsnetwerk en afwijkt van het extranet wanneer dit nodig is. De volgende topologie toont een filiaalnetwerk dat is verbonden met het bedrijfsnetwerk via een routegebaseerde VPN. Traditioneel is de corporate threat defense geconfigureerd om zowel het interne als externe verkeer van het filiaal af te handelen. Met het PBR-beleid is de beveiliging tegen branchebedreigingen geconfigureerd met een beleid dat specifiek verkeer naar het WAN-netwerk in plaats van de virtuele tunnels leidt. De rest van het verkeer stroomt zoals gebruikelijk via de routegebaseerde VPN.



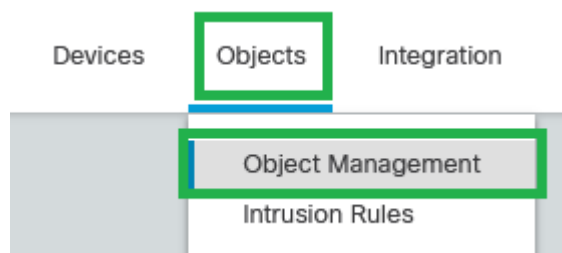
Netwerktopologie

In het gedeelte Configureren wordt ervan uitgegaan dat de ISP- en VTI-interfaces al zijn geconfigureerd voor de beveiliging van de branch threat in de Secure FMC.

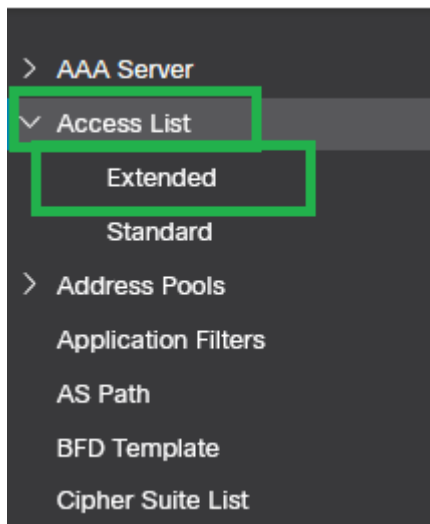
PBR configureren voor HTTP Path Monitoring

In deze configuratiesectie wordt de configuratie voor padbewaking weergegeven op ISP-1- en ISP-2-interfaces.

Stap 1. Maak een uitgebreide toegangslijst voor bewaakte toepassingen. Navigeer naar **Objects > Object Management**.

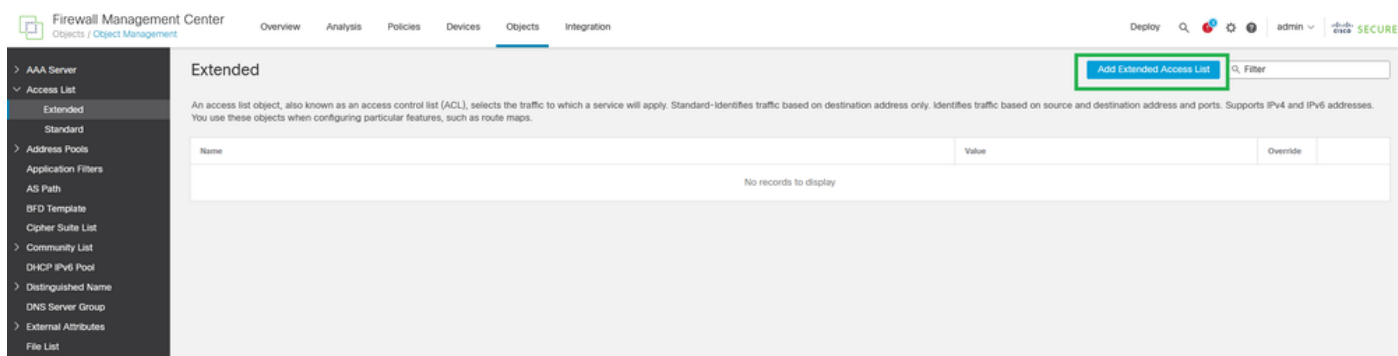


Stap 2. Navigeer naar Access-list > Extended in het linkermenu.



Toegangslijst - Uitgebreid

Stap 3. Klik op de knop . Add Extended Access List



Lijst met uitgebreide toegang toevoegen

Stap 4. Stel een naam in de lijst met uitgebreide toegang in en klik op Add.

New Extended Access List Object

Name
Applications

Entries (0)

Add

Sequence	Action	Source	Source Port	Destination	Destination Port	Application	Users	SGT
No records to display								

☐ Allow Overrides

Cancel Save

Nieuw object met uitgebreide toegangslijst

Stap 5. Klik op Application en kies de gewenste toepassingen (voor dit voorbeeld zijn enkele Cisco-

toepassingen gekozen). Klik vervolgens op **Add**.

Add Extended Access List Entry

?

Action:

Allow

Logging:

Default

Log Level:

Informational

Log Interval:

300

Sec.

Network

Port

Application

Users

Security Group Tag

Application Filters

Clear All Filters

Search by name

Risks (Any Selected)

Very Low

730

Low

622

Medium

734

High

1556

Very High

577

Business Relevance (Any Selected)

Very Low

885

Available Applications (4)

Search cisco

Cisco

Cisco Jabber

Cisco Secure Endpoint

Cisco Webex Assistant

Add to Rule

Selected Applications and Filters (6)

Applications

Cisco Jabber

Cisco Secure Endpoint

Cisco Webex Assistant

WebEx

WebEx Connect

Webex Teams

Cancel

Add

Toevoeging uitgebreide toegangslijst



Opmerking: de uitgebreide toegangslijst kan worden geconfigureerd met IP-adressen en poorten van de bron/bestemming om het specifieke verkeer af te stemmen op de gewenste toepassingen. U kunt meerdere uitgebreide toegangscontrolelijsten maken om toe te passen op de PBR-configuratie.

Stap 6. Valideer de configuratie van de uitgebreide toegangslijst en klik op **Save**.

New Extended Access List Object

?

Name

Applications

Entries (1)

Add

Sequence	Action	Source	Source Port	Destination	Destination Port	Application	Users	SGT	
1	Allow	Any	Any	Any	Any	Cisco Jabber Cisco Secure Endpoint Cisco Webex Assistant WebEx (2 more...)	Any		

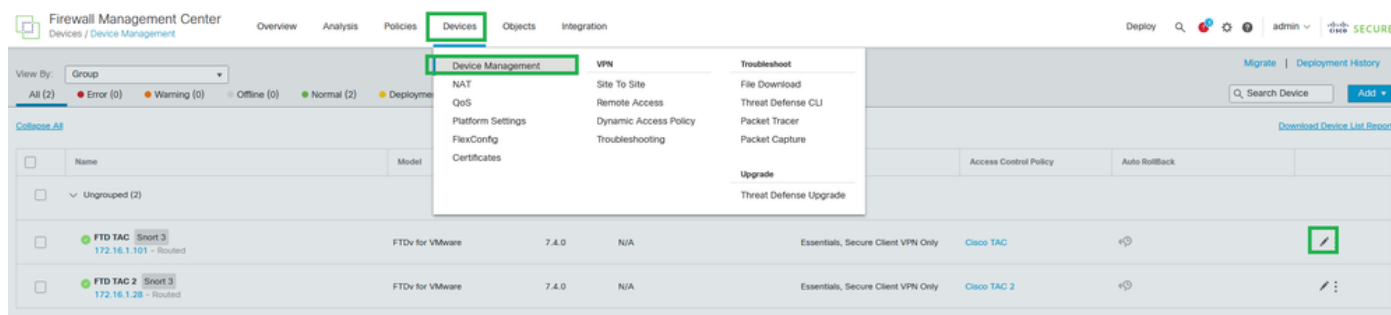
Allow Overrides

Cancel

Save

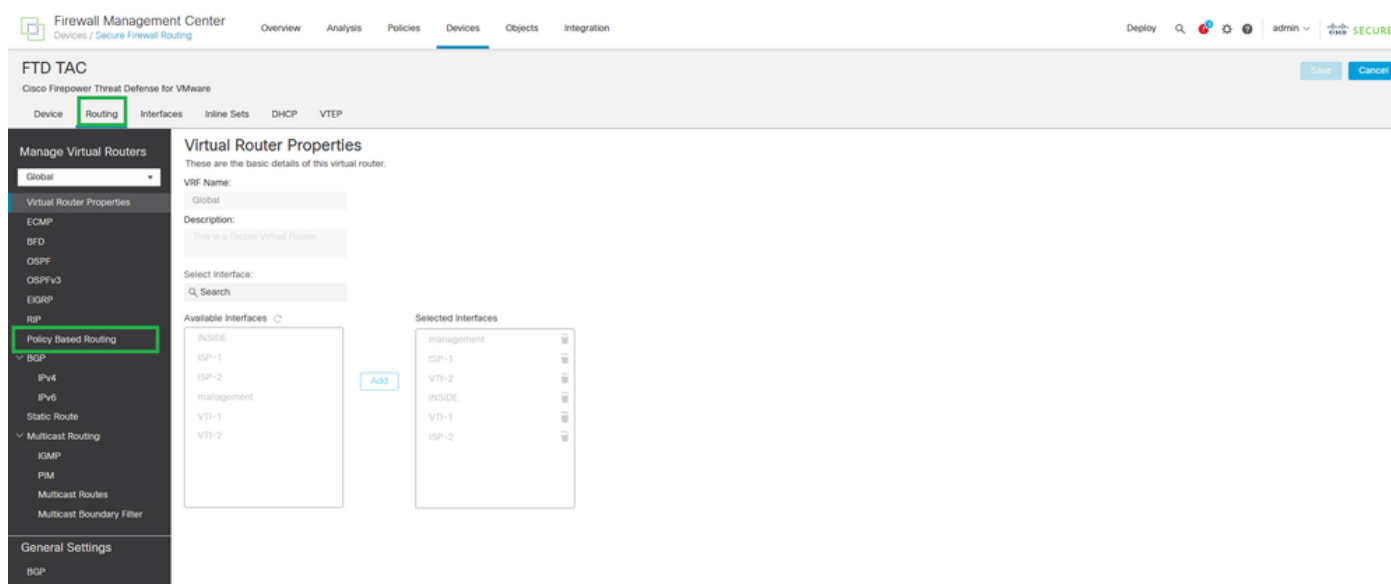
Object uitgebreide toegangslijst opslaan

Stap 7. Navigeer naar Devices > Device Management en bewerk de verdediging van de dreiging.



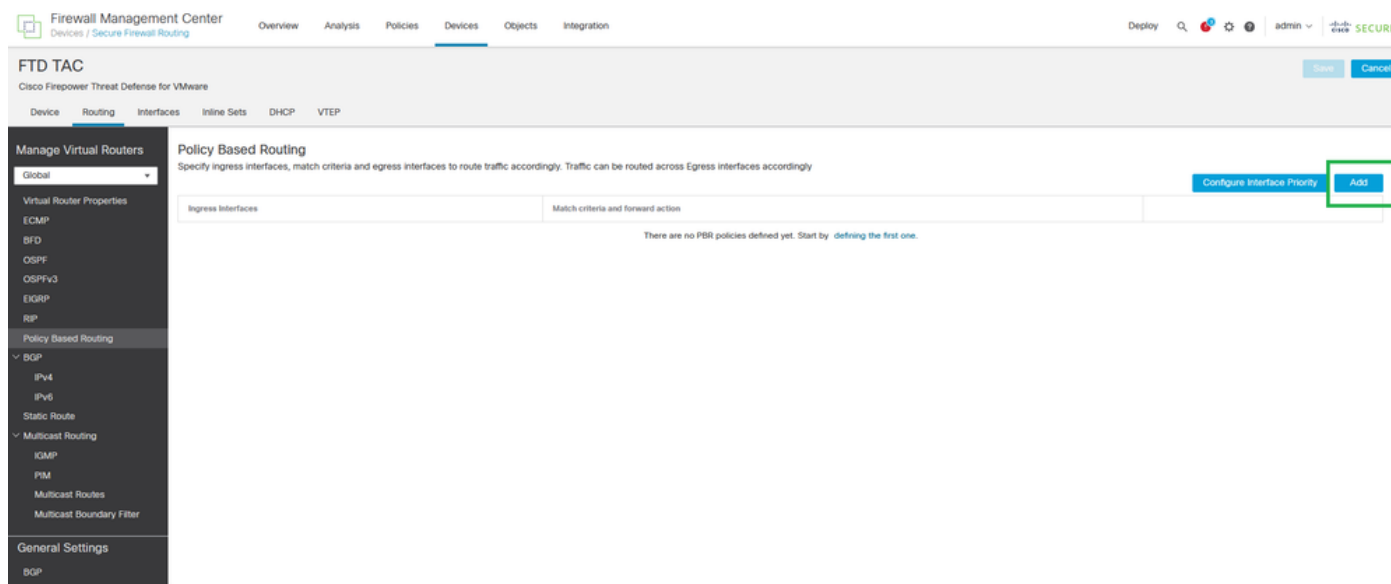
Apparaat - Apparaatbeheer

Stap 8. Navigeer naar Routing > Policy-Based Routing.



Routing - Beleidsgebaseerde routing

Stap 9. Klik op de knop . Add



Stap 10. Voeg de interface voor PBR-configuratie (INSIDE in dit voorbeeld) toe en klik vervolgens 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*

Select...

INSIDE

ISP-1

ISP-2

Add

There are no forward-actions defined yet. Start by [defining the first one](#).

Cancel

Save

Stap 11. Definieer matchcriteria (met de uitgebreide toegangslijst die in de eerdere stappen is gemaakt), Egress-interfaces en interfacebestelling.

Add Forwarding Actions



Match ACL:*	Applications	+
Send To:*	Egress Interfaces	
Interface Ordering:*	Minimal Jitter	i

Available Interfaces



Interface	
INSIDE	+
ISP-1	+
ISP-2	+
VTI-1	+
VTI-2	+

Selected Egress Interfaces*

No interfaces selected

Cancel

Save

Doorstuuracties toevoegen



Opmerking: voor deze configuratiehandleiding zijn Egress Interfaces en Minimal Jitter gekozen. Bekijk de [officiële PBR-documentatie](#) om meer te weten te komen over de andere opties.

Stap 12. Kies de Egress-interfaces (ISP-1 en ISP-2 voor dit voorbeeld) en klik vervolgens op **Save**.

Add Forwarding Actions



Match ACL:* Applications +

Send To:* Egress Interfaces v

Interface Ordering:* Minimal Jitter v

Available Interfaces

Search by interface name



Interface	
INSIDE	+
VTI-1	+
VTI-2	+

Selected Egress Interfaces*

Interface

ISP-1



ISP-2



Cancel

Save

Geselecteerde EGRESSE-interfaces

Stap 13. Valideer de PBR-configuratie en klik op Save.

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*

INSIDE x



Match Criteria and Egress Interface

Specify forward action for chosen match criteria.

Add

Match ACL

Forwarding Action

Applications

Send through minimum jitter interface



ISP-1



ISP-2



Cancel

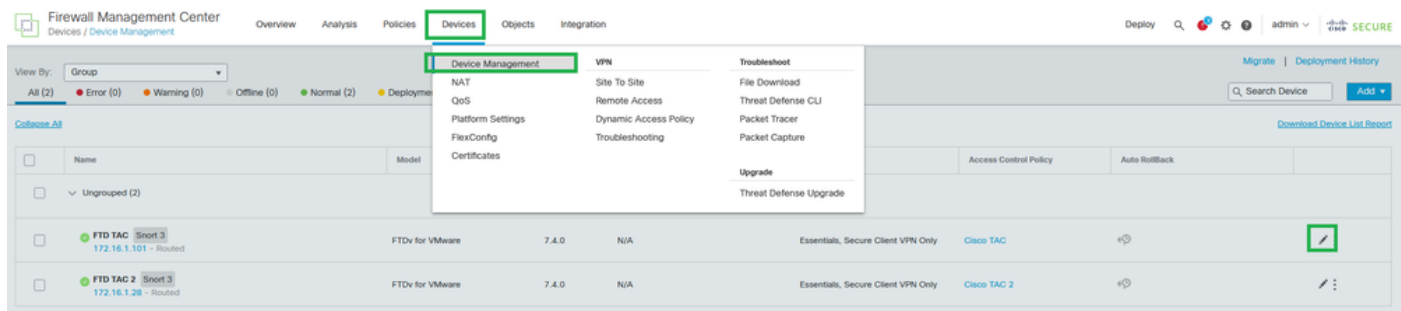
Save

Stap 14. (Optioneel) Herhaal stap 9, 10, 11, 12 en 13 als er meer uitgebreide toegangscontrolelijsten zijn gemaakt of als er meer broninterfaces zijn waarop de PBR-configuratie moet worden toegepast.

Stap 15. Wijzigingen opslaan en implementeren vanuit FMC.

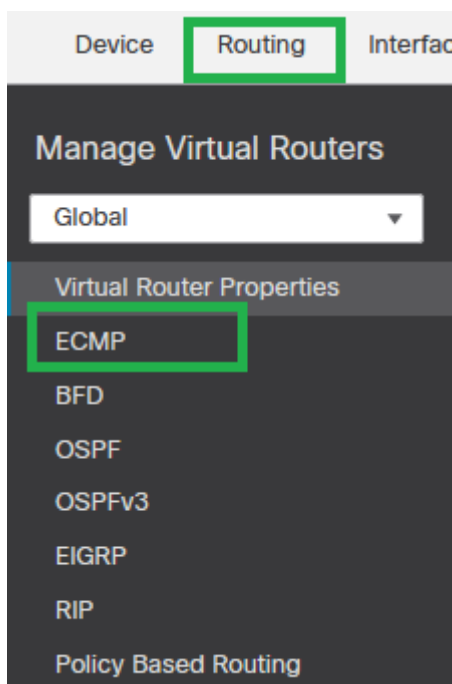
Equal-cost-multi-path (ECMP) configureren

Stap 1. Navigeer naar **Devices > Device Management** en bewerk de dreigingsverdediging.



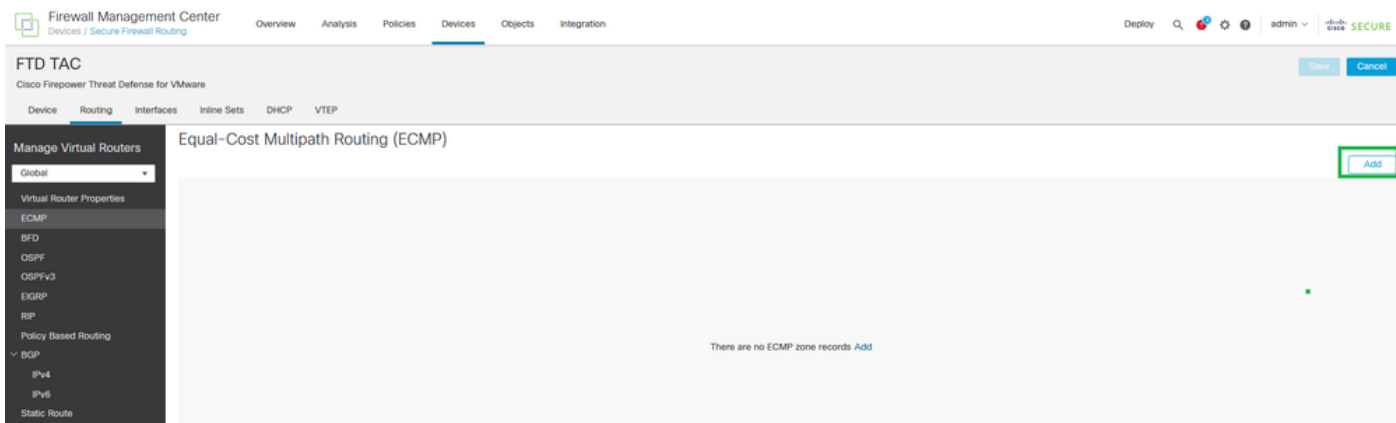
Apparaat - Apparaatbeheer

Stap 2. Navigeer naar **Routing > ECMP**.



Routing - ECMP

Stap 3. Klik op **Add** om een ECMP te maken tussen de VTI's en WAN-interfaces (ISP-1 en ISP-2 voor deze configuratiehandleiding).



Equal-Cost Multipath Routing (ECMP)

Stap 4. Stel de ECMP-naam in en kies alle VTI-interfaces en klik vervolgens op Add.

Add ECMP
? ×

Name

VTI-ECMP

Available Interfaces

INSIDE
ISP-1
ISP-2

Selected Interfaces

VTI-1
VTI-2

Add

Cancel

OK

ECMP voor VTI's

Stap 5. Herhaal stap 3 en 4 om ECMP te maken tussen WAN-interfaces (ISP-1 en ISP-2 voor deze configuratiehandleiding).

Add ECMP? ✕

Name

ISP-ECMP

Available Interfaces

INSIDE
VTI-1
VTI-2

Add

Selected Interfaces

ISP-2
ISP-1

Cancel

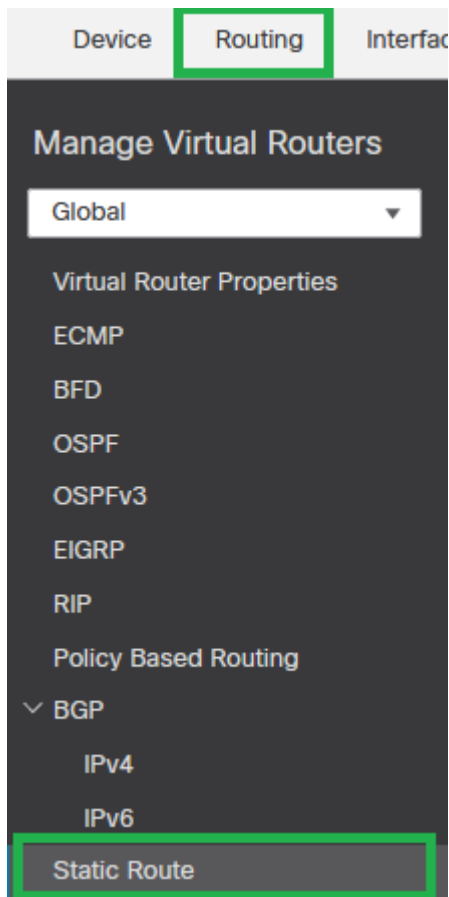
OK

ECMP voor ISP-interfaces

Stap 6. De ECMP-configuratie opslaan.

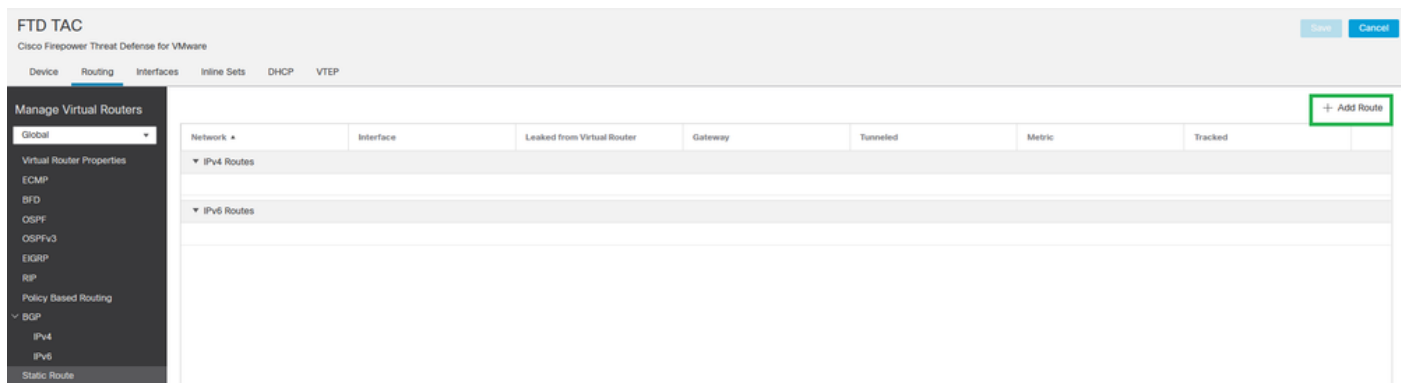
Stap 7. Configureer de statische routes voor de zone-interfaces om de lastbalans te bepalen.

Navigeer naar [Routing > Static Route](#).



Routing - statische route

Stap 8. Klik op de knop . + Add Route



+ Route toevoegen

Stap 9. Maak een standaard statische route voor de VTI-interface(s) (VTI-1 voor deze configuratiehandleiding) met 1 als metrische waarde en klik vervolgens op OK.

Add Static Route Configuration



Type:



IPv4



IPv6

Interface*

VTI-1



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

Available Network 



any



Add

any-ipv4

IPv6-to-IPv4-Relay-Anycast

Selected Network

any-ipv4



Gateway*

VTI-Tunnel1-FPR2



Metric:

1

(1 - 254)

Tunneled: ☐ (Used only for default Route)

Route Tracking:



Cancel

OK

Standaard statische route voor VTI-1

Stap 10. Herhaal stap 8. als er meer VTI-interfaces zijn geconfigureerd.



Opmerking: maak een standaardroute voor elke geconfigureerde VTI-interface.

Stap 11. Maak een standaard statische route voor de WAN/ISP-interface(s) (ISP-1 voor deze configuratiehandleiding) met een grotere metrische waarde dan VTI en klik vervolgens op OK.

Add Static Route Configuration



Type: ☒ IPv4 ☐ IPv6

Interface*

ISP-1

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

Available Network 



any-



Add

any-ipv4

Selected Network

any-ipv4



Gateway*

172.16.1.254GW-24



Metric:

10

(1 - 254)

Tunneled: ☐ (Used only for default Route)

Route Tracking:



Cancel

OK

Standaard statische route voor ISP-1

Stap 12. Herhaal stap 10. als er meer WAN/ISP-interfaces zijn geconfigureerd.



Opmerking: maak een standaardroute voor elke WAN/ISP-interface die is geconfigureerd.

Stap 13. Valideer de standaardrouteconfiguratie en klik op OK.

FTD TAC

Cisco Firepower Threat Defense for VMware

Device

Routing

Interfaces

Inline Sets

DHCP

VTEP

Manage Virtual Routers

Global

Virtual Router Properties

ECMP

BFD

OSPF

OSPFv3

EIGRP

RIP

Policy Based Routing

BGP

Network

Interface

Leaked from Virtual Router

Gateway

Tunneled

Metric

Tracked

+

Add Route

▼ IPv4 Routes

any-ipv4

ISP-2

Global

172.16.11.254-GW-24

false

10

any-ipv4

ISP-1

Global

172.16.1.254GW-24

false

10

any-ipv4

VTI-2

Global

VTI-Tunnel2-FPR2

false

1

any-ipv4

VTI-1

Global

VTI-Tunnel1-FPR2

false

1

▼ IPv6 Routes

You have unsaved changes

Save

Cancel

statische routeconfiguratie

Vertrouwde DNS configureren voor beveiligde FTD

Stap 1. Navigeer naarDevices > Platform Settings.

Devices

Objects

Device Management

NAT

QoS

Platform Settings

FlexConfig

Certificates

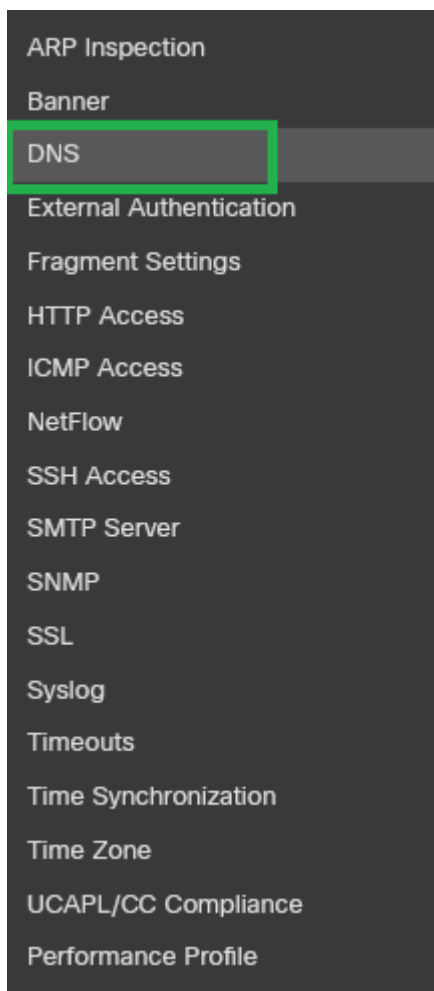
Apparaten - Platforminstellingen

Stap 2. Een bestand beleid voor platforminstellingen maken of bewerken.



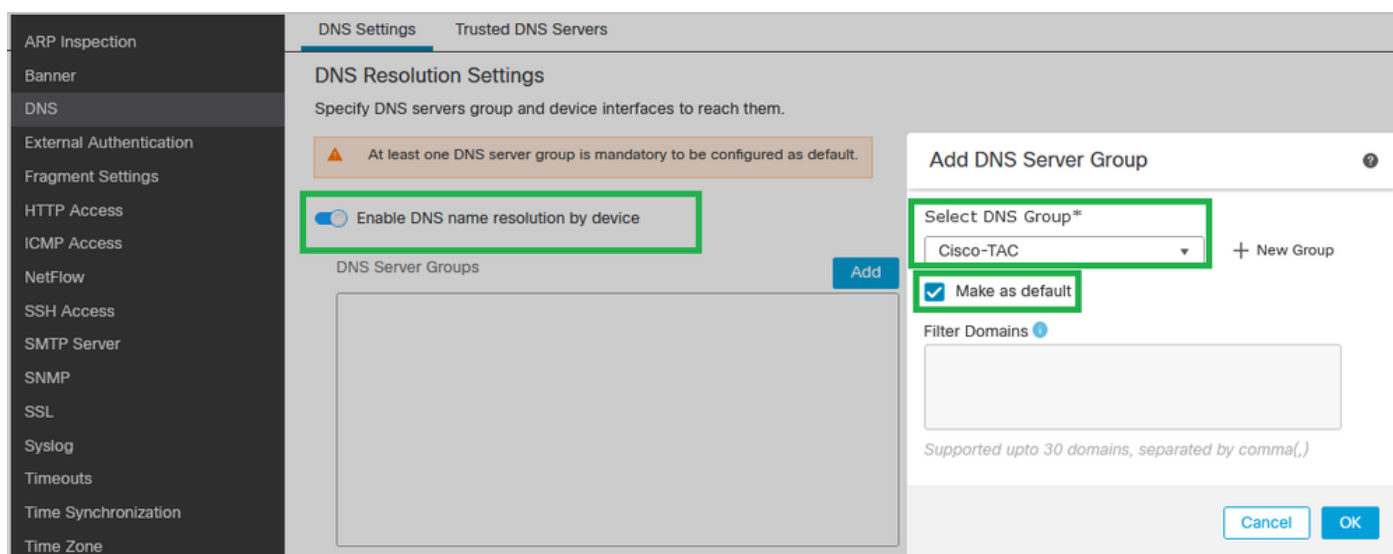
Opmerking: zorg ervoor dat het beleid voor platforminstellingen wordt toegepast op beveiligde dreigingsverdedigingsapparaten.

Stap 3. Klik op de knop . DNS



DNS-platforminstellingen

Stap 4. Schakel DNS name resolution by device **en klik op** Add **of kies een bestaande DNS-groep. Kies** Make as default **en klik op** OK.



DNS-servergroep toevoegen



Opmerking: als u meer wilt weten over de DNS-configuratie in het beleid voor

platforminstellingen, raadpleegt u de documentatie met [officiële platforminstellingen](#).

Stap 5. Kies de WAN/ISP-interfaces onder het Interface Objects gedeelte.

The screenshot displays the DNS configuration page. On the left is a dark sidebar with a list of settings: ARP Inspection, Banner, DNS (highlighted), External Authentication, Fragment Settings, HTTP Access, ICMP Access, NetFlow, SSH Access, SMTP Server, SNMP, SSL, Syslog, Timeouts, Time Synchronization, Time Zone, UCAPL/CC Compliance, and Performance Profile.

The main content area has a large empty box at the top. Below it are two timer settings: 'Expiry Entry Timer' with a value of 1 and a range of 1-65535 minutes, and 'Poll Timer' with a value of 240 and a range of 1-65535 minutes.

The 'Interface Objects' section is highlighted with a green box. It contains the text: 'Devices will use specified interface objects for connecting with DNS Servers.' Below this is a list of 'Available Interface Objects' with a search bar and a refresh icon. The list includes INSIDE, ISP-1, ISP-2 (highlighted in blue), VTI-1, VTI-11, and VTI-2. An 'Add' button is to the right of the list.

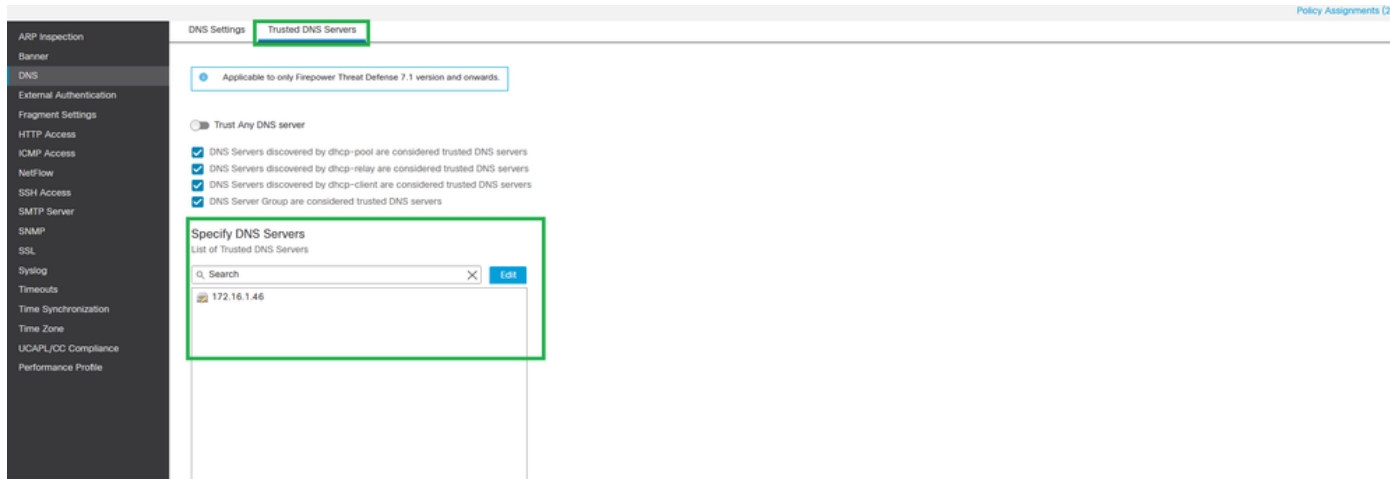
To the right of the available list is a 'Selected Interface Objects' box, also highlighted with a green box. It contains ISP-1 and ISP-2, each with a trash icon to its right.

At the bottom of the section is a checkbox labeled 'Enable DNS Lookup via diagnostic/Management interface also.', which is currently unchecked.

DNS-interfaceconfiguratie

Stap 6. Sla de wijzigingen op.

Stap 7. Navigeer naar de Trusted DNS Servers en geef de vertrouwde DNS-servers op.

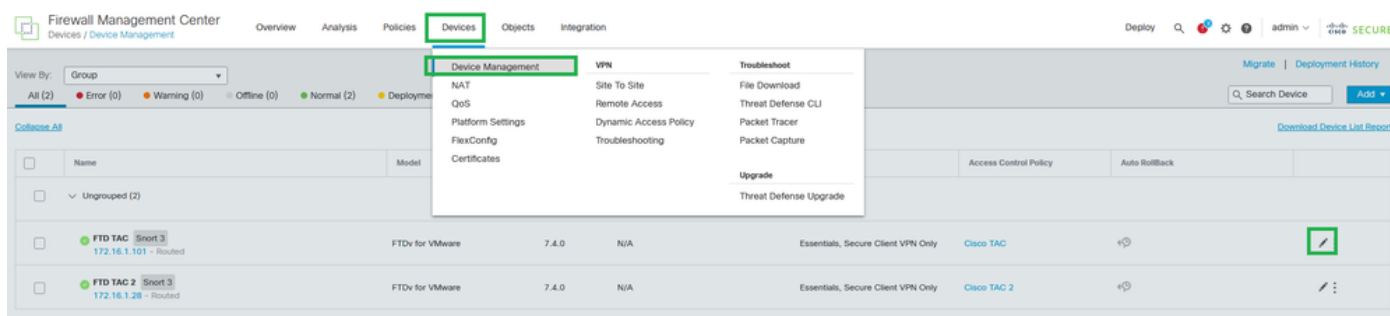


Vertrouwde DNS-servers

Stap 8. Klik op **Save** en implementeer de wijzigingen.

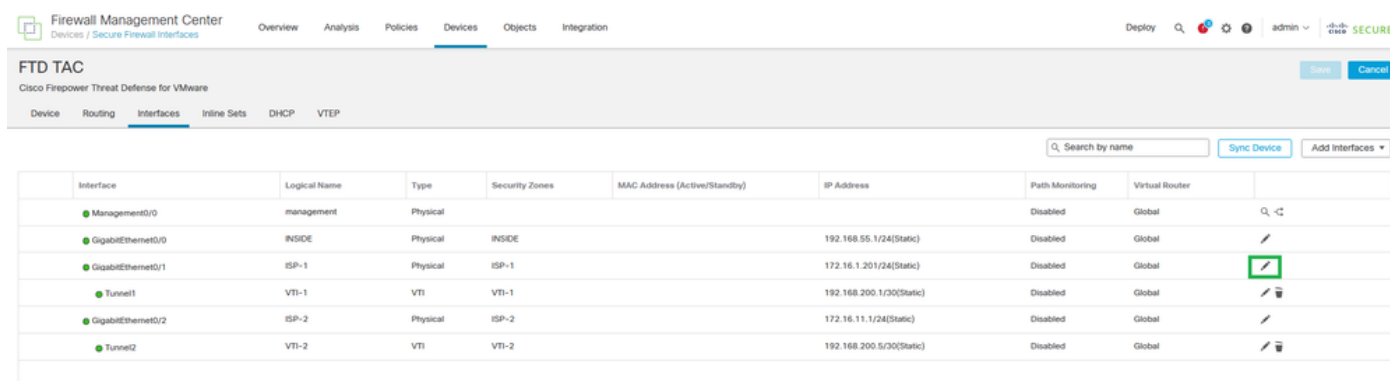
Padbewaking inschakelen

Stap 1. Navigeer naar **Devices > Device Management** en bewerk de dreigingsverdediging.



Apparaat - Apparaatbeheer

Stap 2. Bewerk onder het tabblad **Interfaces** de interface WAN/ISP-interfaces (ISP-1 en ISP-2 voor deze configuratiehandleiding).



Interface-configuratie

Stap 3. Klik op het tabblad **Path Monitoring**, kies de **Enable IP Monitoring** en schakel het **HTTP-based Application Monitoring** in. Klik vervolgens op **Save**.

Edit Physical Interface



General

IPv4

IPv6

Path Monitoring

Hardware Configuration

Manager Access

Advanced

☒ Enable IP based Monitoring

Select to monitor jitter, round trip time, packet-lost & mean opinion score of each interface.

Monitoring Type:

Next-hop of default route out of interface (Auto) ▼

System monitors the next hop of the interface. Tries IPv4 and then IPv6.
If the peer is unavailable, monitoring is not done.

☒ Enable HTTP based Application Monitoring

By enabling application monitoring you are allowing all the applications configured in Extended ACLs used in policy based routing with this interface as egress interface to be monitored automatically.

Applications

Cisco Jabber

Cisco Secure Endpoint

Cisco Webex Assistant

WebEx

WebEx Connect

Cancel

OK

Configuratie voor bewaking van interfacepaden



Waarschuwing: de toepassingen die in de sectie Eerdere configuratie zijn geconfigureerd, moeten worden vermeld.



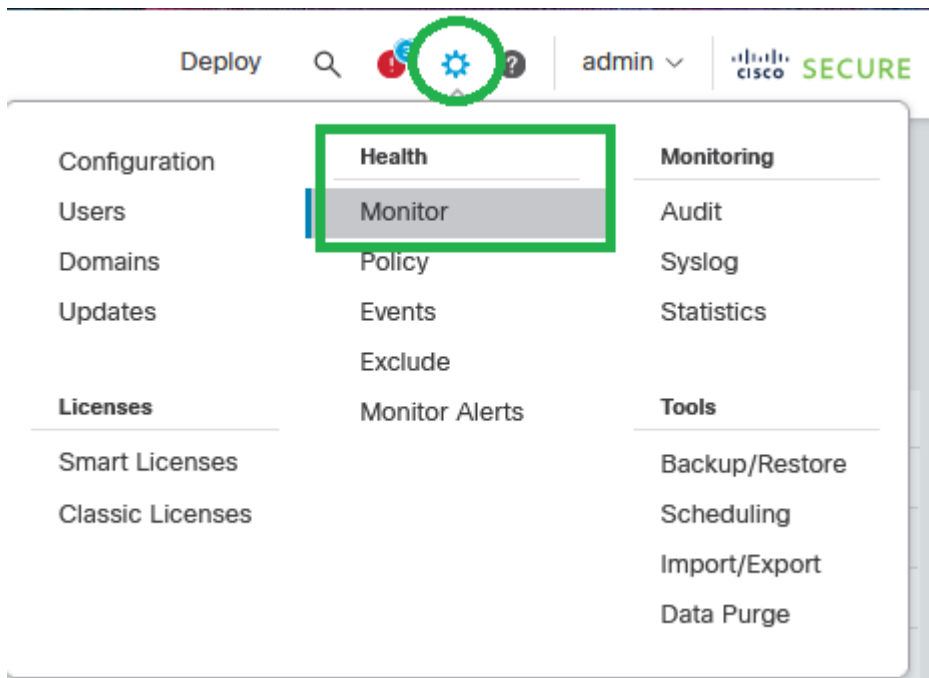
Opmerking: voor deze configuratiegids is 'Type bewaking' gekozen. Controleer de instellingen voor padbewaking in de [officiële configuratiehandleiding](#) voor meer informatie over andere opties.

Stap 4. Herhaal stap 2 en 3 voor alle geconfigureerde WAN/ISP-interfaces.

Stap 5. Klik op **Save** en implementeer de wijzigingen.

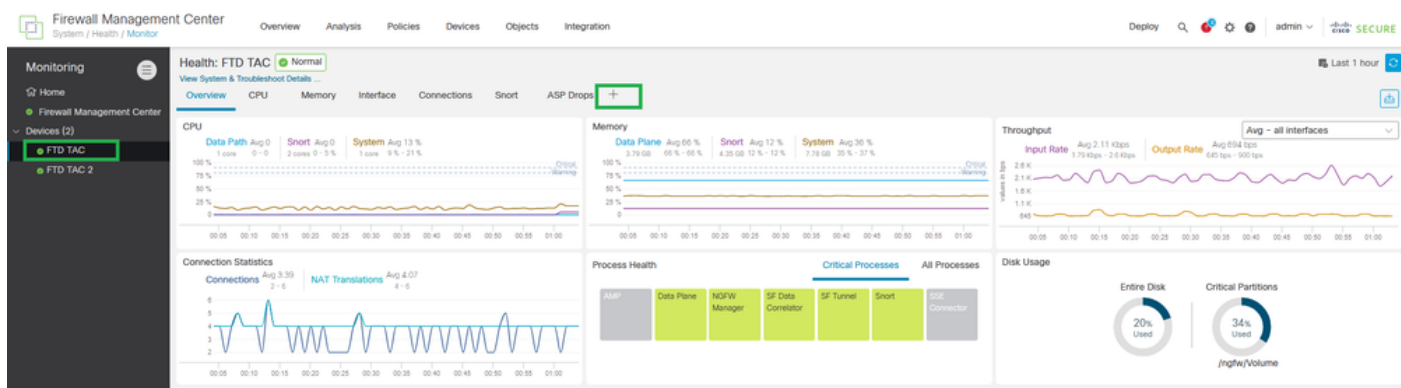
Bewakingsdashboard toevoegen

Stap 1. Navigeer naar **System > Health > Monitor**.



Systeem - Gezondheid - Monitor

Stap 2. Kies het Secure FTD-apparaat en klik op Add New Dashboard.



Nieuw dashboard toevoegen

Stap 3. Stel de naam van het dashboard in en kies in het Correlate Metrics dialoogvenster in de vervolgkeuzelijst Interface - Path Metrics. Klik vervolgens op Add Dashboard.

Add New Dashboard



Name*

FTD HTTP Path Monitoring

Metrics*

Metrics can be chosen from pre-defined correlation groups or/and metrics of your choice. Related metrics are grouped together, select a group and then the metrics.

Interface

Jitter x

x

v



Interface

Mean Opinion Score (MOS) x

x

v



Interface

Round Trip Time x

x

v



Interface

Packet Loss x

x

v



Add Metrics

Add from Predefined Correlations v

Clear All

Cancel

Add Dashboard

Nieuw dashboard toevoegen met padstatistieken

Verifiëren

In dit gedeelte wordt beschreven hoe u de zwevende statische routes, ECMP, objectgroep met toepassingen en PBR-configuraties kunt verifiëren.

Controleer de standaardroutes en de configuratie van zwevende statische routes:

```
firepower# show run route
route VTI-1 0.0.0.0 0.0.0.0 192.168.200.1 1
route VTI-2 0.0.0.0 0.0.0.0 192.168.200.5 1
route ISP-1 0.0.0.0 0.0.0.0 172.16.1.254 10
route ISP-2 0.0.0.0 0.0.0.0 172.16.11.254 10
```

Controleer de ECMP-configuratie:

```
firepower# sh run | i ecmp
zone ECMP-VTI ecmp
zone ECMP-ISP ecmp
```

Controleer of het verkeer wordt gebalanceerd door de ECMP, op de routingstabel. De routingstabel moet beide routes op de Secure FTD-routingstabel installeren.

```
firepower# show route static
```

```
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 172.16.11.254 to network 0.0.0.0

S* 0.0.0.0 0.0.0.0 [1/0] via 192.168.200.5, VTI-2
[1/0] via 192.168.200.1, VTI-1
```

Configuratie PBR-routekaart verifiëren:

```
firepower# show run route-map
!
route-map FMC_GENERATED_PBR_1694885402369 permit 5
match ip address Applications
set adaptive-interface cost ISP-1 ISP-2
!
```

Controleer de ACL die is toegewezen aan de PBR-configuratie (controleer de ACL-naam op de routekaartconfiguratie):

```
firepower# show run access-list | i Applications
access-list Applications extended permit ip any object-group-network-service FMC_NSQ_639950173988
```

Controleer de objectgroep met toepassingen die zijn toegewezen aan de toegangslijst (controleer de naam van de objectgroep in de ACL-configuratie):

```
firepower# show run object-group
object-group network-service FMC_NSQ_639950173988
network-service-member "Cisco Jabber"
network-service-member "Cisco Secure Endpoint"
network-service-member "Cisco Webex Assistant"
network-service-member "WebEx"
network-service-member "WebEx Connect"
network-service-member "Webex Teams"
```

Controleer de beleidsroute die is toegewezen aan de gegevensinterfaces die worden gebruikt in de PBR-configuratie:

```

interface GigabitEthernet0/0
nameif INSIDE
cts manual
propagate sgt preserve-untag
policy static sgt disabled trusted
security-level 0
ip address 172.16.35.1 255.255.255.0
policy-route route-map FMC_GENERATED_PBR_1694885402369
!
interface GigabitEthernet0/1
nameif ISP-1
cts manual
propagate sgt preserve-untag
policy static sgt disabled trusted
security-level 0
zone-member ECMP-ISP
ip address 172.16.1.202 255.255.255.0
policy-route path-monitoring auto
!
interface GigabitEthernet0/2
nameif ISP-2
security-level 0
zone-member ECMP-ISP
ip address 172.16.11.2 255.255.255.0
policy-route path-monitoring auto
!

```

Verifieer en controleer Jitter, MOS, Round Trip Time en Packet Loss-statistieken op basis van de HTTP Path Monitoring Dashboard-informatie.



HTTP-padcontrole-dashboard verifiëren

Problemen oplossen

In het geval van een Path Monitoring-fout, waarbij IP-gebaseerde monitoring is ingeschakeld, worden WAN/ISP-interfaces geconfigureerd om ICMP-probe-pakketten naar de gateway te sturen

die op statische routes is geconfigureerd. Configureer ingress/egress-opnames op WAN/ISP-interfaces om te controleren of ICMP werkt.

Ingress en egress capture:

```
firepower# cap in interface ISP-1 trace match icmp any any
firepower# cap in2 interface isP-2 trace match icmp any any
```

Ingress capture:

```
firepower# show cap in
```

```
12 packets captured
1: 00:08:28.073604 172.16.1.202 > 172.16.1.254 icmp: echo request
2: 00:08:28.074672 172.16.1.254 > 172.16.1.202 icmp: echo reply
3: 00:08:29.150871 172.16.1.202 > 172.16.1.254 icmp: echo request
4: 00:08:29.151832 172.16.1.254 > 172.16.1.202 icmp: echo reply
5: 00:08:30.217701 172.16.1.202 > 172.16.1.254 icmp: echo request
6: 00:08:30.218876 172.16.1.254 > 172.16.1.202 icmp: echo reply
7: 00:08:31.247728 172.16.1.202 > 172.16.1.254 icmp: echo request
8: 00:08:31.248980 172.16.1.254 > 172.16.1.202 icmp: echo reply
9: 00:08:32.309005 172.16.1.202 > 172.16.1.254 icmp: echo request
10: 00:08:32.310317 172.16.1.254 > 172.16.1.202 icmp: echo reply
11: 00:08:33.386622 172.16.1.202 > 172.16.1.254 icmp: echo request
12: 00:08:33.387751 172.16.1.254 > 172.16.1.202 icmp: echo reply
12 packets shown
1: 00:08:28.073604 172.16.1.202 > 172.16.1.254 icmp: echo request
2: 00:08:28.074672 172.16.1.254 > 172.16.1.202 icmp: echo reply
3: 00:08:29.150871 172.16.1.202 > 172.16.1.254 icmp: echo request
4: 00:08:29.151832 172.16.1.254 > 172.16.1.202 icmp: echo reply
5: 00:08:30.217701 172.16.1.202 > 172.16.1.254 icmp: echo request
6: 00:08:30.218876 172.16.1.254 > 172.16.1.202 icmp: echo reply
7: 00:08:31.247728 172.16.1.202 > 172.16.1.254 icmp: echo request
8: 00:08:31.248980 172.16.1.254 > 172.16.1.202 icmp: echo reply
9: 00:08:32.309005 172.16.1.202 > 172.16.1.254 icmp: echo request
10: 00:08:32.310317 172.16.1.254 > 172.16.1.202 icmp: echo reply
11: 00:08:33.386622 172.16.1.202 > 172.16.1.254 icmp: echo request
12: 00:08:33.387751 172.16.1.254 > 172.16.1.202 icmp: echo reply
12 packets shown
```

Inname van uitgangen:

```
firepower# show cap in2
```

```
12 packets captured
1: 00:08:28.073543 172.16.11.2 > 172.16.11.254 icmp: echo request
2: 00:08:28.074764 172.16.11.254 > 172.16.11.2 icmp: echo reply
3: 00:08:29.150810 172.16.11.2 > 172.16.11.254 icmp: echo request
4: 00:08:29.151954 172.16.11.254 > 172.16.11.2 icmp: echo reply
```

```
5: 00:08:30.217640 172.16.11.2 > 172.16.11.254 icmp: echo request
6: 00:08:30.218799 172.16.11.254 > 172.16.11.2 icmp: echo reply
7: 00:08:31.247667 172.16.11.2 > 172.16.11.254 icmp: echo request
8: 00:08:31.248888 172.16.11.254 > 172.16.11.2 icmp: echo reply
9: 00:08:32.308913 172.16.11.2 > 172.16.11.254 icmp: echo request
10: 00:08:32.310012 172.16.11.254 > 172.16.11.2 icmp: echo reply
11: 00:08:33.386576 172.16.11.2 > 172.16.11.254 icmp: echo request
12: 00:08:33.387888 172.16.11.254 > 172.16.11.2 icmp: echo reply
12 packets captured
```



Let op: zorg ervoor dat u opnames configureert met IP-adressen van bron en bestemming, omdat opnames de prestaties op de doos aanzienlijk kunnen verhogen.



Tip: Als ping niet werkt, lost u de directe verbinding met de standaardgateway op, controleert u de ARP-tabel of neemt u contact op met Cisco TAC.

Om te controleren of PBR werkt, kunt u de pakkettracer-tool gebruiken om ervoor te zorgen dat toepassingsverkeer wordt gerouteerd met PBR.

```
firepower# packet-tracer input inside tcp 172.16.35.2 54352 'PUBLIC-IP-ADDRESS-FOR-WEBEX' $
---
[Output omitted]
---
Phase: 3
Type: PBR-LOOKUP
Subtype: policy-route
Result: ALLOW
Config:
route-map FMC_GENERATED_PBR_1694885402369 permit 5
match ip address Applications
set ip next-hop 172.16.1.254
Additional Information:
Matched route-map FMC_GENERATED_PBR_1694885402369, sequence 5, permit
Found next-hop 172.16.1.254 using egress ifc ISP-1
---
[Output omitted]
---
Result:
input-interface: INSIDE
input-status: up
input-line-status: up
output-interface: ISP-1
output-status: up
output-line-status: up
Action: allow
```



Opmerking: als u meer wilt weten over de IP-adressen van de toepassing voor de netwerkservice die is geconfigureerd voor objectgroepen, gebruikt u de `show object-group network-service detail`.

Gerelateerde informatie

Aanvullende documenten met betrekking tot PBR met HTTP Path Monitoring zijn hier te vinden:

- [Beleidsgebaseerde routeringsconfiguratie op de apparaatconfiguratiehandleiding van het Secure Firewall Management Center](#)
- [Padcontrole bij op beleid gebaseerde routeringsconfiguratie op de apparaatconfiguratiehandleiding van het Secure Firewall Management Center](#)
- [Beleidsgebaseerd routeringsbeleid configureren](#)
- [Configuratievoorbeeld voor beleidsgebaseerde routing](#)
- [Voorbeeld configureren voor PBR Path Monitoring](#)
- [Padmonitoring-dashboard toevoegen](#)
- [Configuratie van DNS-platforminstellingen op de apparaatconfiguratiehandleiding van het Secure Firewall Management Center](#)
- [Cisco Technical Support en downloads](#)

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.