

ECMP configureren met IP SLA op FTD beheerd door FMC

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Netwerkdigram](#)

[Configuraties](#)

[Stap 0. Interfaces/netwerkobjecten vooraf configureren](#)

[Stap 1. ECMP-zone configureren](#)

[Stap 2. IP SLA-objecten configureren](#)

[Stap 3. Configureer statische routes met routespoor](#)

[Verifiëren](#)

[Taakverdeling](#)

[Verloren route](#)

[Problemen oplossen](#)

Inleiding

In dit document wordt beschreven hoe u de ECMP en IP SLA kunt configureren op een FTD die wordt beheerd door het VCC.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- ECMP-configuratie op Cisco Secure Firewall Threat Defence (FTD)
- IP SLA-configuratie op Cisco Secure Firewall Threat Defence (FTD)
- Cisco Secure Firewall Management Center (FMC)

Gebruikte componenten

De informatie in dit document is gebaseerd op deze software- en hardwareversie:

- Cisco FTD versie 7.4.1

- Cisco FMC versie 7.4.1

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

In dit document wordt beschreven hoe u Equal-Cost Multi-Path (ECMP) kunt configureren in combinatie met een Internet Protocol Service Level Agreement (IP SLA) op een Cisco FTD die wordt beheerd door Cisco FMC. Met het ECMP kunt u interfaces groeperen op FTD-verkeer en taakverdeling over meerdere interfaces. IP SLA is een mechanisme dat end-to-end connectiviteit bewaakt door de uitwisseling van reguliere pakketten. Samen met ECMP kan IP SLA worden geïmplementeerd om de beschikbaarheid van de volgende hop te garanderen. In dit voorbeeld wordt ECMP gebruikt om pakketten gelijkelijk te verdelen over twee internetserviceproviders (ISP's). Tegelijkertijd houdt een IP SLA de connectiviteit bij, waardoor een naadloze overgang naar beschikbare circuits in het geval van een storing wordt gegarandeerd.

Specifieke eisen voor dit document zijn onder meer:

- Toegang tot de apparaten met een gebruikersaccount met beheerdersrechten
- Cisco Secure Firewall Threat Defense versie 7.1 of hoger
- Cisco Secure Firewall Management Center versie 7.1 of hoger

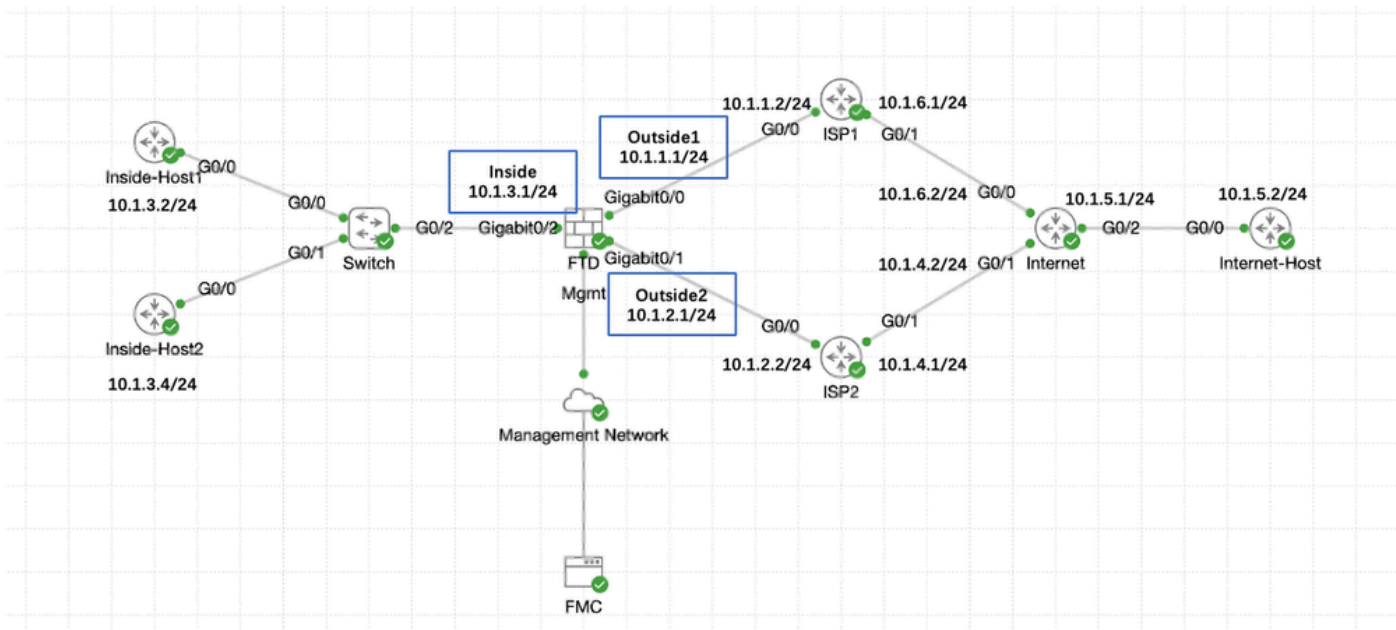
Configureren

Netwerkdigram

In dit voorbeeld heeft Cisco FTD twee buiteninterfaces: buitenkant1 en buitenkant2 . Elke verbinding met een ISP-gateway, buitenkant1 en buitenkant2 behoren tot dezelfde ECMP-zone die buiten is genoemd.

Het verkeer van het interne netwerk wordt via FTD gerouteerd en wordt via de twee ISP's gebalanceerd met de lading op internet.

Tegelijkertijd maakt FTD gebruik van IP SLA's om de connectiviteit met elke ISP-gateway te bewaken. In het geval van een storing op een van de ISP-circuits, FTD-failovers naar de andere ISP-gateway om de bedrijfscontinuïteit te handhaven.



Netwerkdigram

Configuraties

Stap 0. Interfaces/netwerkobjecten vooraf configureren

Log in de FMC web GUI, selecteer Apparaten>Apparaatbeheer en klik op de knop Bewerken voor uw bedreigingsverdediging apparaat. De pagina Interfaces is standaard geselecteerd. Klik op de knop Bewerken voor de interface die u wilt bewerken, in dit voorbeeld Gigabit Ethernet0/0.

Firewall Management Center
Devices / Secure Firewall Interfaces

Overview Analysis Policies **Devices** Objects Integration

Deploy Search Settings Help admin **SECURE**

10.106.32.250 Save Cancel

Cisco Firepower Threat Defense for KVM

Device Routing **Interfaces** Inline Sets DHCP VTEP

All Interfaces Virtual Tunnels

Search by name Sync Device Add Interfaces

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring	Virtual Router	
Management0/0	management	Physical				Disabled	Global	
GigabitEthernet0/0		Physical				Disabled		
GigabitEthernet0/1		Physical				Disabled		
GigabitEthernet0/2		Physical				Disabled		
GigabitEthernet0/3		Physical				Disabled		
GigabitEthernet0/4		Physical				Disabled		
GigabitEthernet0/5		Physical				Disabled		
GigabitEthernet0/6		Physical				Disabled		
GigabitEthernet0/7		Physical				Disabled		

Displaying 1-9 of 9 interfaces | Page 1 of 1

Interface Gi0/0 bewerken

In het venster Fysieke interface bewerken, onder het tabblad Algemeen:

1. Stel de naam in, in dit geval Buiten1.
2. Schakel de interface in door het aanvinkvakje Ingeschakeld in te schakelen.
3. Selecteer in de vervolgkeuzelijst Security Zone een bestaande Security Zone of maak een nieuwe Security Zone, in dit voorbeeld Outside1_Zone.

Edit Physical Interface



General IPv4 IPv6 Path Monitoring Hardware Configuration Manager Access Advanced

Name:
Outside1

Enabled
 Management Only

Description:

Mode:
None

Security Zone:
Outside1_Zone

Interface ID:
GigabitEthernet0/0

MTU:
1500
(64 - 9000)

Priority:
0 (0 - 65535)

Propagate Security Group Tag:

NVE Only:

Cancel OK

Algemene interface Gi0/0

Onder het tabblad IPv4:

1. Kies een van de opties uit de vervolgkeuzelijst IP-type in dit voorbeeld Statische IP gebruiken.
2. Stel het IP-adres in dit voorbeeld in 10.1.1.1/24.
3. Klik op OK.

Edit Physical Interface



General **IPv4** IPv6 Path Monitoring Hardware Configuration Manager Access Advanced

IP Type:
Use Static IP

IP Address:
10.1.1.1/24
eg. 192.0.2.1/255.255.255.128 or 192.0.2.1/25

Cancel OK

Interface Gi0/20 IPv4

Herhaal dezelfde stap om de interface Gigabit Ethernet0/1 te configureren in het venster Fysieke interface bewerken, onder het tabblad Algemeen:

1. Stel de naam in, in dit geval Outside2.
2. Schakel de interface in door het aanvinkvakje Ingeschakeld in te schakelen.
3. Selecteer in de vervolgkeuzelijst Security Zone een bestaande Security Zone of maak een nieuwe Security Zone, in dit voorbeeld Outside2_Zone.

Edit Physical Interface



General IPv4 IPv6 Path Monitoring Hardware Configuration Manager Access Advanced

Name:
Outside2

Enabled
 Management Only

Description:

Mode:
None

Security Zone:
Outside2_Zone

Interface ID:
GigabitEthernet0/1

MTU:
1500
(64 - 9000)

Priority:
0 (0 - 65535)

Propagate Security Group Tag:

NVE Only:

Cancel OK

Interface Gi0/1 algemeen

Onder het tabblad IPv4:

1. Kies een van de opties uit de vervolgkeuzelijst IP-type in dit voorbeeld Statische IP gebruiken.
2. Stel het IP-adres in dit voorbeeld in 10.1.2.1/24.
3. Klik op OK.

Edit Physical Interface

General IPv4 IPv6 Path Monitoring Hardware Configuration Manager Access Advanced

IP Type:
Use Static IP

IP Address:
10.1.2.1/24

eg. 192.0.2.1/24, 2001:db8:2:1::1/64, 192.0.2.1/24

Cancel OK

Interface Gi0/1 IPv4

Herhaal dezelfde stap om de interface Gigabit Ethernet0/2 te configureren in het venster Fysieke interface bewerken, onder het tabblad Algemeen:

1. Stel de naam in, in dit geval Inside.
2. Schakel de interface in door het aanvinkvakje Ingeschakeld in te schakelen.
3. Selecteer in de vervolgkeuzelijst Security Zone een bestaande Security Zone of maak een nieuwe Security Zone, in dit voorbeeld Inside_Zone.

Edit Physical Interface



General IPv4 IPv6 Path Monitoring Hardware Configuration Manager Access Advanced

Name:
Inside

Enabled
 Management Only

Description:

Mode:
None

Security Zone:
Inside_Zone

Interface ID:
GigabitEthernet0/2

MTU:
1500
(64 - 9000)

Priority:
0 (0 - 65535)

Propagate Security Group Tag:

NVE Only:

Cancel OK

Interface Gi0/2 algemeen

Onder het tabblad IPv4:

1. Kies een van de opties uit de vervolgkeuzelijst IP-type in dit voorbeeld Statische IP gebruiken.
2. Stel het IP-adres in dit voorbeeld in 10.1.3.1/24.
3. Klik op OK.

Edit Physical Interface

General **IPv4** IPv6 Path Monitoring Hardware Configuration Manager Access Advanced

IP Type:
Use Static IP

IP Address:
10.1.3.1/24

Cancel OK

Interface Gi0/2 IPv4

Klik op Opslaan en de configuratie implementeren.

Navigeer naar objecten > Objectbeheer, kies Network uit de lijst met objecttypes, kies Object toevoegen uit het vervolgkeuzemenu Network toevoegen om een object te maken voor de eerste ISP-gateway.

Firewall Management Center
Objects / Object Management

Overview Analysis Policies Devices **Objects** Integration

Deploy Filter admin **SECURE**

Network

A network object represents one or more IP addresses. Network objects are used in various places, including access control policies, network variables, intrusion rules, identity rules, network event searches, reports, and so on.

Add Network Add Object Import Object Add Group

Name	Value	Type	Override
any	0.0.0.0/0 :::0	Group	
any-ipv4	0.0.0.0/0	Network	
any-ipv6	:::0	Host	
IPv4-Benchmark-Tests	198.18.0.0/15	Network	
IPv4-Link-Local	169.254.0.0/16	Network	
IPv4-Multicast	224.0.0.0/4	Network	
IPv4-Private-10.0.0.0-8	10.0.0.0/8	Network	
IPv4-Private-172.16.0.0-12	172.16.0.0/12	Network	
IPv4-Private-192.168.0.0-16	192.168.0.0/16	Network	
IPv4-Private-All-RFC1918	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	Group	
IPv6-IPv4-Mapped	:::ffff:0.0.0.0/96	Network	
IPv6-Link-Local	fe80::/10	Network	
IPv6-Private-Unique-Local-Addresses	fc00::/7	Network	
IPv6-to-IPv4-Relay-Anycast	192.88.99.0/24	Network	

Displaying 1 - 14 of 14 rows Page 1 of 1

Netwerkoject

In het venster Nieuwe netwerkojecten:

1. Stel de naam in dit voorbeeld gw-outdoor1 in.
2. Selecteer in het veld Network de gewenste optie en voer een juiste waarde in, in dit voorbeeld Host en 10.1.1.2.

3. Klik op Save (Opslaan).

New Network Object

Name
gw-outside1

Description

Network
 Host Range Network FQDN
10.1.1.2

Allow Overrides

Cancel Save

Voorwerp GW-buiten1

Herhaal vergelijkbare stappen om een ander object voor een tweede ISP-gateway te maken. In het venster Nieuwe netwerkobjecten:

1. Stel de naam in dit voorbeeld gw-outdoor2 in.
2. Selecteer in het veld Network de gewenste optie en voer een juiste waarde in, in dit voorbeeld Host en 10.1.2.2.
3. Klik op Save (Opslaan).

New Network Object



Name

gw-outside2

Description

Network

Host

Range

Network

FQDN

10.1.2.2

Allow Overrides

Cancel

Save

Object Gw-buitenkant2

Stap 1. ECMP-zone configureren

Navigeer naar Apparaten > Apparaatbeheer en bewerk het bedreigingsbeschermingsapparaat, klik op Routing. Selecteer in de vervolgkeuzelijst virtuele router de virtuele router waarin u de ECMP-zone wilt aanmaken. U kunt ECMP-zones maken in wereldwijde virtuele routers en door de gebruiker gedefinieerde virtuele routers. Kies in dit voorbeeld Global.

Klik op ECMP en vervolgens op Add.

Firewall Management Center
Devices / Secure Firewall Routing

Overview Analysis Policies **Devices** Objects Integration

10.106.32.250

Cisco Firepower Threat Defense for KVM

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

Equal-Cost Multipath Routing (ECMP)

There are no ECMP zone records [Add](#)

Save Cancel

ECMP-zone configureren

In het venster Add ECMP:

1. Stel Naam in voor ECMP zone, in dit voorbeeld Buiten.
2. Om interfaces te associëren selecteert u de interface onder het vak Beschikbare interfaces en vervolgens klikt u op Toevoegen. In dit voorbeeld Outside1 en Outside2.
3. Klik op OK.

Add ECMP



Name
Outside

Available Interfaces
Inside

Selected Interfaces
Outside1
Outside2

Add

Cancel OK

ECMP-zone buiten configureren

Klik op Opslaan en de configuratie implementeren.

Stap 2. IP SLA-objecten configureren

Navigeer naar objecten > Objectbeheer, kies SLA-monitor uit de lijst met objecttypes, klik op SLA-monitor toevoegen om een nieuwe SLA-monitor toe te voegen voor de eerste ISP-gateway.

Firewall Management Center
Objects / Object Management

Overview Analysis Policies Devices **Objects** Integration

Deploy 🔍 ⚙️ 👤 admin 🔒 SECURE

SLA Monitor

Add SLA Monitor 🔍 Filter

SLA monitor defines a connectivity policy to a monitored address and tracks the availability of a route to the address. The SLA Monitor object is used in the Route Tracking field of an IPv4 Static Route Policy. IPv6 routes do not have the option to use SLA monitor via route tracking.

Name	Value
No records to display	

AAA Server
Access List
Address Pools
Application Filters
AS Path
BFD Template
Cipher Suite List
Community List
DHCP IPv6 Pool
Distinguished Name
DNS Server Group
External Attributes
File List
FlexConfig
Geolocation
Interface
Key Chain
Network
PKI
Policy List
Port
Prefix List
Route Map
Security Intelligence
SLA Monitor
Time Range

SLA-monitor maken

In het venster Nieuwe SLA Monitor Object:

1. Stel de naam voor het SLA-monitorobject in, in dit geval sla-external1.
2. Voer het ID-nummer van de SLA-handeling in het veld SLA Monitor ID in. Waarden variëren van 1 tot 2147483647. U kunt maximaal 2000 SLA-bewerkingen op een apparaat maken. Elk ID-nummer moet uniek zijn voor het beleid en de apparaatconfiguratie. In dit voorbeeld 1.
3. Voer het IP-adres in dat voor beschikbaarheid wordt bewaakt door de SLA-handeling in het veld Gemonitord adres. In dit voorbeeld 10.1.1.2.
4. De lijst Beschikbare zones/interfaces geeft zowel zones als interfacegroepen weer. In de lijst met zones/interfaces kunt u de zones of interfacegroepen toevoegen die de interfaces bevatten waarmee het apparaat communiceert met het beheerstation. Om één enkele interface te specificeren, moet u een zone of de interfacegroepen voor de interface creëren. In dit voorbeeld Outside1_Zone.
5. Klik op Save (Opslaan).

New SLA Monitor Object



Name:

sla-outside1

Description:

Frequency (seconds):

60

{1-604800}

SLA Monitor ID*:

1

Threshold (milliseconds):

{0-60000}

Timeout (milliseconds):

5000

{0-604800000}

Data Size (bytes):

28

{0-16384}

ToS:

Number of Packets:

1

Monitor Address*:

10.1.1.2

Available Zones/interfaces



Q Search

Inside_Zone

Outside1_Zone

Outside2_Zone

Add

Selected Zones/interfaces

Outside1_Zone



Cancel

Save

SLA-object SLA-buitenkant1

Herhaal soortgelijke stappen om een andere SLA-monitor voor de tweede ISP-gateway te maken.

In het venster Nieuwe SLA Monitor Object:

1. Stel de naam voor het SLA-monitorobject in, in dit geval sla-external2.
2. Voer het ID-nummer van de SLA-handeling in het veld SLA Monitor ID in. Waarden variëren van 1 tot 2147483647. U kunt maximaal 2000 SLA-bewerkingen op een apparaat maken. Elk ID-nummer moet uniek zijn voor het beleid en de apparaatconfiguratie. In dit voorbeeld 2.
3. Voer het IP-adres in dat voor beschikbaarheid wordt bewaakt door de SLA-handeling in het veld Gemonitord adres. In dit voorbeeld 10.1.2.2.
4. De lijst Beschikbare zones/interfaces geeft zowel zones als interfacegroepen weer. In de lijst met zones/interfaces kunt u de zones of interfacegroepen toevoegen die de interfaces bevatten waarmee het apparaat communiceert met het beheerstation. Om één enkele interface te specificeren, moet u een zone of de interfacegroepen voor de interface creëren. In dit voorbeeld Outside2_Zone.
5. Klik op Save (Opslaan).

New SLA Monitor Object



Name:

sla-outside2

Description:

Frequency (seconds):

60

{1-604800}

SLA Monitor ID*:

2

Threshold (milliseconds):

{0-60000}

Timeout (milliseconds):

5000

{0-604800000}

Data Size (bytes):

20

{0-16384}

ToS:

Number of Packets:

1

Monitor Address*:

10.1.2.2

Available Zones/Interfaces

Q Search

Inside_Zone

Outside1_Zone

Outside2_Zone

Add

Selected Zones/Interfaces

Outside1_Zone

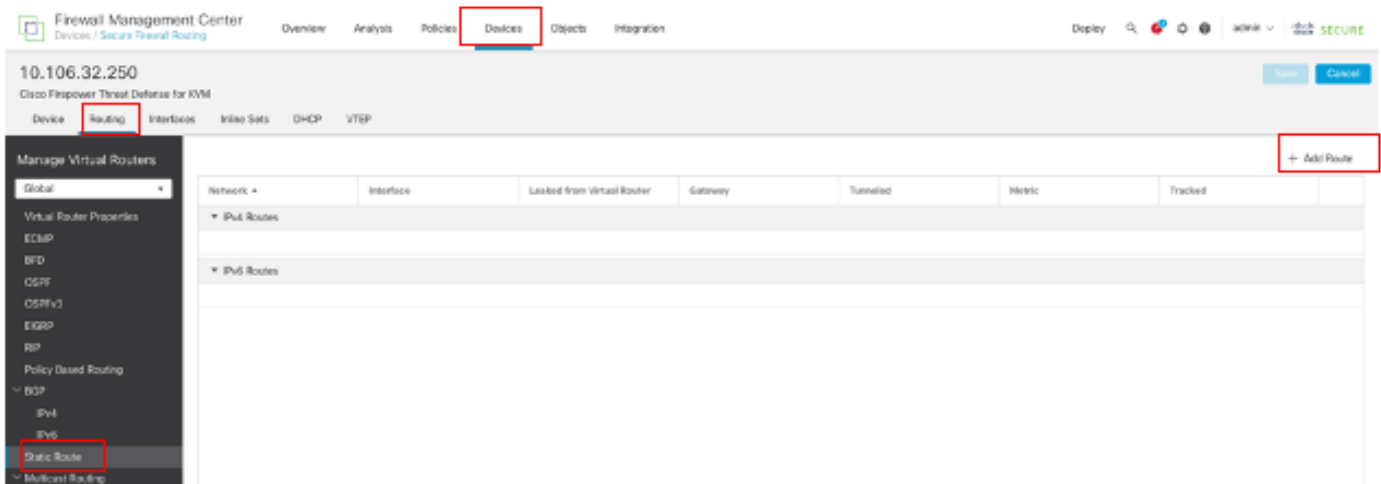
Cancel

Save

Stap 3. Configureer statische routes met routespoor

Navigeer naar Apparaten > Apparaatbeheer en bewerk het bedreigingsbeschermingsapparaat, klik op Routing, selecteer uit de vervolgkeuzelijst virtuele routers de virtuele router waarvoor u een statische route configureert. In dit voorbeeld Global.

Selecteer Statische Route, klik op Add Route om de standaardroute aan de eerste ISP-gateway toe te voegen.



Statische route configureren


In het venster Add Static Route Configuration:


1. Klik op IPv4 of IPv6 afhankelijk van het type statische route dat u toevoegt. In dit voorbeeld IPv4.
2. Kies de interface waarop deze statische route van toepassing is. In dit voorbeeld Outside1.
3. Kies in de lijst Beschikbare netwerken het doelnetwerk. In dit voorbeeld any-ipv4.
4. Voer in het veld Gateway of IPv6 Gateway de gatewayrouter in of kies deze die de volgende hop voor deze route is. U kunt een IP-adres of een Netwerken/Hosts-object opgeven. In dit voorbeeld gw-outdoor1.
5. Voer in het veld Metriek het aantal hop in naar het doelnetwerk. Geldige waarden variëren van 1 tot 255; de standaardwaarde is 1. In dit voorbeeld 1.
6. Om routebeschikbaarheid te controleren, voer of kies de naam van een SLA Monitor-object dat het monitoringbeleid definieert, in het veld Route Tracking. In dit voorbeeld sla-outside1.
7. Klik op OK.

Add Static Route Configuration

Type: IPv4 IPv6

Interface*
Outside1

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

Available Network  + Selected Network

Search

any-ipv4
gw-outside1
gw-outside2
IPv4-Benchmark-Tests
IPv4-Link-Local
IPv4-Multicast

Add

any-ipv4

Gateway*
gw-outside1 +

Metric:
1

(1 = 254)

Tunneled: (Used only for default Routes)

Route Tracking:
sla-outside1 +

Cancel OK

Voeg eerst statische route-ISP toe

Herhaal soortgelijke stappen om de standaardroute aan een tweede ISP-gateway toe te voegen. In het venster Add Static Route Configuration:

1. Klik op IPv4 of IPv6 afhankelijk van het type statische route dat u toevoegt. In dit voorbeeld IPv4.
2. Kies de interface waarop deze statische route van toepassing is. In dit voorbeeld Outside2.

3. Kies in de lijst Beschikbare netwerken het doelnetwerk. In dit voorbeeld any-ipv4.
4. Voer in het veld Gateway of IPv6 Gateway de gatewayrouter in of kies deze die de volgende hop voor deze route is. U kunt een IP-adres of een Netwerken/Hosts-object opgeven. In dit voorbeeld gw-outdoor2.
5. Voer in het veld Metriek het aantal hop in naar het doelnetwerk. Geldige waarden variëren van 1 tot 255; de standaardwaarde is 1. Zorg ervoor dat u dezelfde metriek opgeeft als de eerste route, in dit voorbeeld 1.
6. Om routebeschikbaarheid te controleren, voer of kies de naam van een SLA Monitor-object dat het monitoringbeleid definieert, in het veld Route Tracking. In dit voorbeeld sla-outdoor2.
7. Klik op OK.

Add Static Route Configuration



Type: IPv4 IPv6

Interface*

Outside2

[Interface starting with this icon  signifies it is available for route leak]

Available Network 



Selected Network

Search

Add

any-ipv4

any-ipv4

gw-outside1

gw-outside2

IPv4-Benchmark-Tests

IPv4-Link-Local

IPv4-Multicast

Gateway*

gw-outside2



Metric:

1

[1 - 254]

Tunneled: (Used only for default Route)

Route Tracking:

sla-outside2



Cancel

OK

Statische route tweede ISP toevoegen

Klik op Opslaan en de configuratie implementeren.

Verifiëren

Log in op de CLI van de FTD en voer de opdracht uit `show zone` om informatie over ECMP-verkeerszones te controleren, inclusief de interfaces die deel uitmaken van elke zone.

```
<#root>
```

```
> show zone  
Zone: Outside ecmp  
Security-level: 0
```

```
Zone member(s): 2
```

```
Outside2 GigabitEthernet0/1
```

```
Outside1 GigabitEthernet0/0
```

Stel het bevel in werking `show running-config route` om de lopende configuratie de routerconfiguratie te controleren, in dit geval zijn er twee statische routes met routesporen.

```
<#root>
```

```
> show running-config route
```

```
route Outside1 0.0.0.0 0.0.0.0 10.1.1.2 1 track 1
```

```
route Outside2 0.0.0.0 0.0.0.0 10.1.2.2 1 track 2
```

Stel het bevel in werking show route om de routingstabel te controleren, in dit geval zijn er twee standaardroutes via de interface buitenkant1 en buitenkant2 met gelijke kosten, kan het verkeer tussen twee ISP kringen worden verdeeld.

```
<#root>
```

```
> 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 10.1.2.2 to network 0.0.0.0
```

```
S* 0.0.0.0 0.0.0.0 [1/0] via 10.1.2.2, Outside2
```

```
[1/0] via 10.1.1.2, Outside1
```

```
C 10.1.1.0 255.255.255.0 is directly connected, Outside1  
L 10.1.1.1 255.255.255.255 is directly connected, Outside1  
C 10.1.2.0 255.255.255.0 is directly connected, Outside2  
L 10.1.2.1 255.255.255.255 is directly connected, Outside2  
C 10.1.3.0 255.255.255.0 is directly connected, Inside  
L 10.1.3.1 255.255.255.255 is directly connected, Inside
```

Voer de opdracht uit **show sla monitor configuration** om de configuratie van de SLA-monitor te controleren.

<#root>

```
> show sla monitor configuration
SA Agent, Infrastructure Engine-II
Entry number: 1
Owner:
Tag:
```

Type of operation to perform: echo

Target address: 10.1.1.2

Interface: Outside1

```
Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 60
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:
```

Entry number: 2

Owner:
Tag:

Type of operation to perform: echo

Target address: 10.1.2.2

Interface: Outside2

Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 60
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:

Voer de opdracht `show sla monitor operational-state` uit om de status van de SLA-monitor te bevestigen. In dit geval kunt u vinden "**Time-out voorkwam: FALSE**" in de opdrachtoutput, het geeft aan dat de ICMP-echo naar de gateway reageert, zodat de standaardroute door doelinterface actief is en geïnstalleerd in routingtabel.

<#root>

> show sla monitor operational-state

Entry number: 1
Modification time: 09:31:28.785 UTC Thu Feb 15 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 82
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE

Timeout occurred: FALSE

Over thresholds occurred: FALSE
Latest RTT (milliseconds): 1
Latest operation start time: 10:52:28.785 UTC Thu Feb 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 1 RTTMin: 1 RTTMax: 1
NumOfRTT: 1 RTTSum: 1 RTTSum2: 1

Entry number: 2
Modification time: 09:31:28.785 UTC Thu Feb 15 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 82
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE

Timeout occurred: FALSE

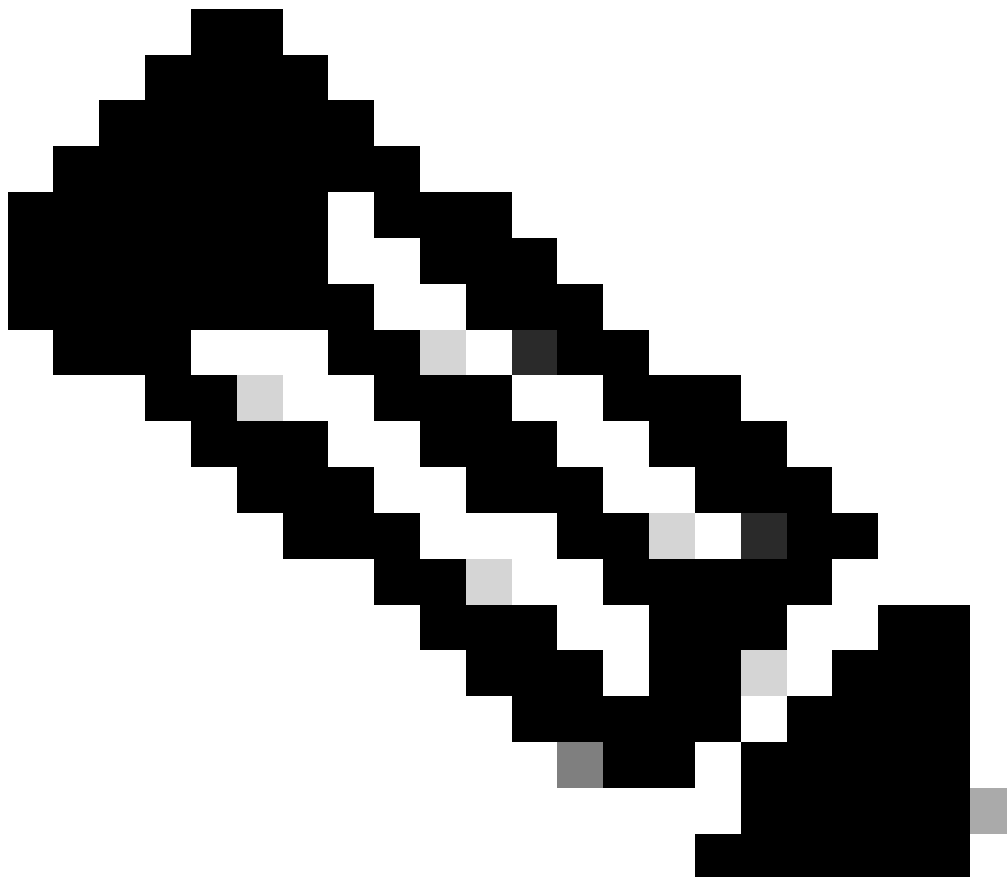
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 1
Latest operation start time: 10:52:28.785 UTC Thu Feb 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 1 RTTMin: 1 RTTMax: 1
NumOfRTT: 1 RTTSum: 1 RTTSum2: 1

Taakverdeling

Aanvankelijk verkeer via FTD om te controleren of de ECMP-werklastverdeling gelijk is aan het verkeer tussen de gateways in de ECMP-zone. In dit geval, initieer Telnet verbinding van Inside-Host1 (10.1.3.2) en Inside-Host2 (10.1.3.4) naar Internet-Host (10.1.5.2), voer het commando uit **show conn** om te bevestigen dat het verkeer taakverdeling tussen twee ISP-koppelingen heeft: Inside-Host1 (10.1.3.2) gaat door een interface buiten1, Inside-Host2 (10.1.3.4) gaat door een interface buiten2.

```
> show conn
2 in use, 3 most used
Inspect Snort:
preserve-connection: 2 enabled, 0 in effect, 2 most enabled, 0 most in effect

TCP Inside 10.1.3.2:46069 Outside1 10.1.5.2:23, idle 0:00:24, bytes 1329, flags UIO N1
TCP Inside 10.1.3.4:61915 Outside2 10.1.5.2:23, idle 0:00:04, bytes 1329, flags UIO N1
```



Opmerking: het verkeer is taakverdeling tussen de gespecificeerde gateways op basis van een algoritme dat de bron- en

bestemmingsIP-adressen, inkomende interface, protocol, bron- en bestemmingshavens blokkeert. Wanneer u de test uitvoert, kan het verkeer dat u simuleert naar dezelfde gateway worden gerouteerd vanwege het hashalgoritme, dit wordt verwacht, verandert elke waarde onder de 6 tuples (bron IP, bestemming IP, inkomende interface, protocol, bronpoort, bestemmingshaven) om het hashresultaat te wijzigen.

Verloren route

Als de verbinding met de eerste ISP Gateway is uitgeschakeld, moet u in dit geval de eerste te simuleren gatewayrouter uitschakelen. Als FTD geen echoantwoord van eerste ISP gateway binnen de drempeltijdopnemer ontvangt die in het voorwerp van de SLA Monitor wordt gespecificeerd, wordt de gastheer beschouwd als onbereikbaar en zoals neer gemarkeerd. De gevolgde route aan eerste gateway wordt ook verwijderd uit het verpletteren van lijst.

Voer de opdracht `show sla monitor operational-state` uit om de huidige status van de SLA-monitor te bevestigen. In dit geval kunt u "Time-out voorgekomen vinden: Waar" in de opdrachtoutput, het geeft aan dat de ICMP-echo naar de eerste ISP-gateway niet reageert.

```
<#root>
```

```
> show sla monitor operational-state
Entry number: 1
Modification time: 09:31:28.783 UTC Thu Feb 15 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 104
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
```

```
Timeout occurred: TRUE
```

```
Over thresholds occurred: FALSE
Latest RTT (milliseconds): NoConnection/Busy/Timeout
Latest operation start time: 11:14:28.813 UTC Thu Feb 15 2024
Latest operation return code: Timeout
RTT Values:
RTTAvg: 0 RTTMin: 0 RTTMax: 0
NumOfRTT: 0 RTTSum: 0 RTTSum2: 0
```

```
Entry number: 2
Modification time: 09:31:28.783 UTC Thu Feb 15 2024
```

Number of Octets Used by this Entry: 2056
Number of operations attempted: 104
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE

Timeout occurred: FALSE

Over thresholds occurred: FALSE
Latest RTT (milliseconds): 1
Latest operation start time: 11:14:28.813 UTC Thu Feb 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 1 RTTMin: 1 RTTMax: 1
NumOfRTT: 1 RTTSum: 1 RTTSum2: 1

Voer de opdracht uit **show route** om de huidige routingstabel te controleren, de route naar de eerste ISP-gateway via interface buitenkant1 wordt verwijderd, er is slechts één actieve standaardroute naar de tweede ISP-gateway via interface buitenkant2.

<#root>

> 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 10.1.2.2 to network 0.0.0.0

S* 0.0.0.0 0.0.0.0 [1/0] via 10.1.2.2, Outside2

C 10.1.1.0 255.255.255.0 is directly connected, Outside1

```
L 10.1.1.1 255.255.255.255 is directly connected, Outside1
C 10.1.2.0 255.255.255.0 is directly connected, Outside2
L 10.1.2.1 255.255.255.255 is directly connected, Outside2
C 10.1.3.0 255.255.255.0 is directly connected, Inside
L 10.1.3.1 255.255.255.255 is directly connected, Inside
```

Start de opdracht show conn , u kunt zien dat de twee verbindingen nog steeds actief zijn. Telnet-sessies zijn ook actief op Inside-Host1 (10.1.3.2) en Inside-Host2 (10.1.3.4) zonder enige onderbreking.

<#root>

```
> show conn
2 in use, 3 most used
Inspect Snort:
preserve-connection: 2 enabled, 0 in effect, 2 most enabled, 0 most in effect
```

```
TCP Inside 10.1.3.2:46069 Outside1 10.1.5.2:23, idle 0:00:22, bytes 1329, flags UIO N1
```

```
TCP Inside 10.1.3.4:61915 Outside2 10.1.5.2:23, idle 0:00:02, bytes 1329, flags UIO N1
```



Opmerking: in de uitvoer van show conn , telnet sessie van Inside-Host1 (10.1.3.2) is nog steeds via interface buitenkant1, hoewel de standaardroute door interface buitenkant1 is verwijderd uit de routingstabel. Dit wordt verwacht en door ontwerp, het werkelijke verkeer stroomt door interface buitenkant2. Als u nieuwe verbinding van Inside-Host1 (10.1.3.2) naar Internet-Host (10.1.5.2) start, kunt u al het verkeer vinden via de interface buitenkant2.

Problemen oplossen

Om de routingstabel te bevestigen verander, stel bevel in werking debug ip routing.

In dit voorbeeld, wanneer de verbinding met eerste ISP gateway neer is, wordt de route door interface outdoor1 verwijderd uit het verpletteren van lijst.

```
<#root>
```

```
> debug ip routing  
IP routing debugging is on
```

```
RT: ip_route_delete 0.0.0.0 0.0.0.0 via 10.1.1.2, Outside1
```

```
ha_cluster_synced 0 routetype 0
```

```
RT: del 0.0.0.0 via 10.1.1.2, static metric [1/0]NP-route: Delete-Output 0.0.0.0/0 hop_count:1 , via 0.0.0.0
```

```
RT(mgmt-only): NP-route: Update-Output 0.0.0.0/0 hop_count:1 , via 10.1.2.2, Outside2
```

```
NP-route: Update-Input 0.0.0.0/0 hop_count:1 Distance:1 Flags:0X0 , via 10.1.2.2, Outside2
```

Voer de opdracht show route uit om de huidige routertabel te bevestigen.

```
<#root>
```



```
> 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 10.1.2.2 to network 0.0.0.0
```

```
S* 0.0.0.0 0.0.0.0 [1/0] via 10.1.2.2, Outside2
```

```
C 10.1.1.0 255.255.255.0 is directly connected, Outside1  
L 10.1.1.1 255.255.255.255 is directly connected, Outside1  
C 10.1.2.0 255.255.255.0 is directly connected, Outside2  
L 10.1.2.1 255.255.255.255 is directly connected, Outside2  
C 10.1.3.0 255.255.255.0 is directly connected, Inside  
L 10.1.3.1 255.255.255.255 is directly connected, Inside
```

Wanneer de verbinding met de eerste ISP gateway omhoog opnieuw is, wordt de route door interface external1 toegevoegd terug naar routingstabel.

```
<#root>
```

```
> debug ip routing  
IP routing debugging is on
```

```
NP-route: Update-Output 0.0.0.0/0 hop_count:1 , via 10.1.2.2, Outside2
```

```
NP-route: Update-Output 0.0.0.0/0 hop_count:1 , via 10.1.1.2, Outside2
```

NP-route: Update-Input 0.0.0.0/0 hop_count:2 Distance:1 Flags:0X0 , via 10.1.2.2, Outside2

via 10.1.1.2, Outside1

Voer de opdracht show route uit om de huidige routertabel te bevestigen.

<#root>

> 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 10.1.2.2 to network 0.0.0.0

s* 0.0.0.0 0.0.0.0 [1/0] via 10.1.2.2, Outside2

[1/0] via 10.1.1.2, Outside1

C 10.1.1.0 255.255.255.0 is directly connected, Outside1
L 10.1.1.1 255.255.255.255 is directly connected, Outside1
C 10.1.2.0 255.255.255.0 is directly connected, Outside2
L 10.1.2.1 255.255.255.255 is directly connected, Outside2
C 10.1.3.0 255.255.255.0 is directly connected, Inside
L 10.1.3.1 255.255.255.255 is directly connected, Inside

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.