

Configureer dubbele ISP-failover voor FTD die door FMC wordt beheerd

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Statische routetracering - Overzicht](#)

[Configureren](#)

[Netwerkdigram](#)

[Configuraties](#)

[Verifiëren](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u DUBBELE ISP-failover kunt configureren met PBR en IP SLA™s op een FTD die wordt beheerd door FMC.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Op beleid gebaseerde routing (PBR)
- Internet Protocol-overeenkomst voor serviceniveau (IP SLA)
- Firepower Management Center (FMC)
- Firepower Threat Defense (FTD)

Gebruikte componenten

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

- VCCv 7.3.0
- FTDv 7.3.0

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

Statische routetracering - Overzicht

Met de functie Static Route Tracking kan de FTD een verbinding met een secundaire ISP gebruiken in het geval dat de primaire huurlijn niet beschikbaar wordt. Om deze redundantie te bereiken, associeert de FTD een statische route met een controledoel dat u definieert. De SSLA-handeling bewaakt het doel met periodieke ICMP-echoverzoeken.

Als een echoantwoord niet wordt ontvangen, dan wordt het voorwerp overwogen neer, en de bijbehorende route wordt verwijderd uit de verpletterende lijst. Een eerder ingestelde back-uproute wordt gebruikt in plaats van de route die wordt verwijderd. Tijdens het gebruik van de back-uproute gaat de SLA-monitorbewerking door met pogingen om het monitoringdoel te bereiken.

Zodra het doel opnieuw beschikbaar is, wordt de eerste route vervangen in de routingstabel, en de reserveroute wordt verwijderd.

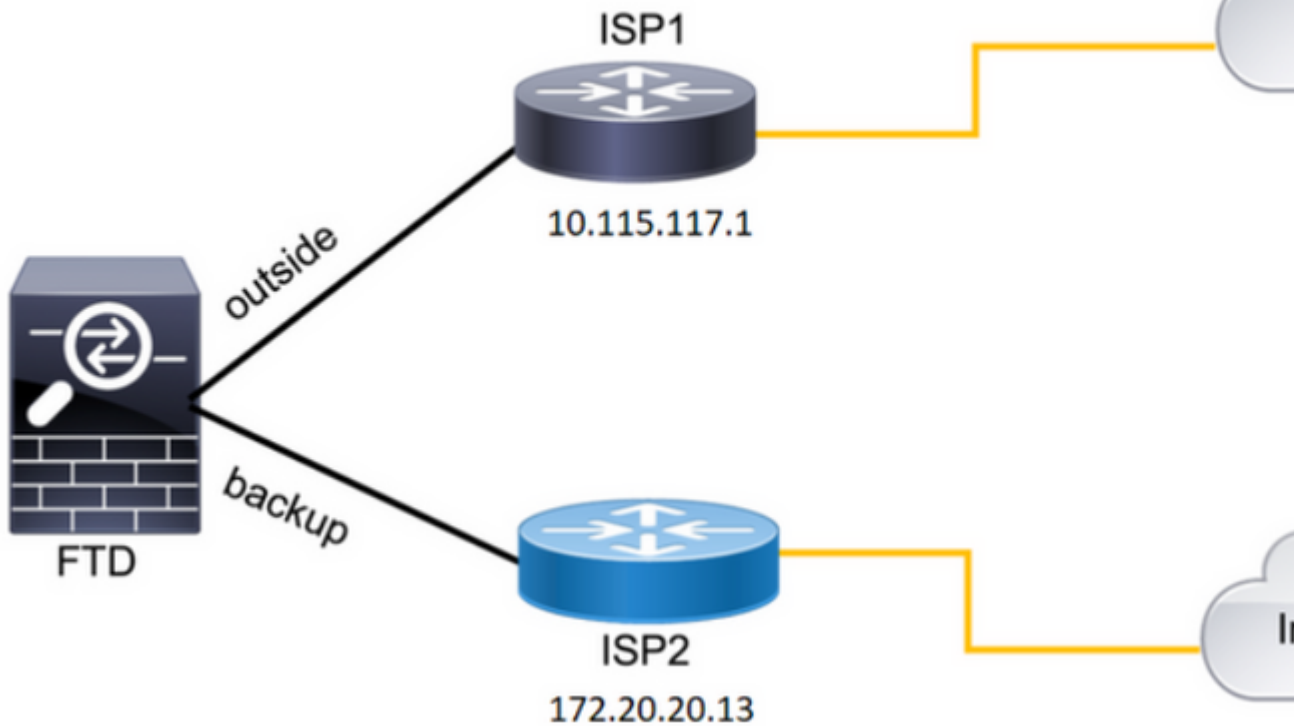
U kunt nu meerdere next-hop en op beleid gebaseerde routing doorsturen acties tegelijkertijd configureren. Wanneer het verkeer aan de criteria voor de route voldoet, probeert het systeem verkeer naar de IP-adressen in de door u opgegeven volgorde door te sturen, totdat het slaagt.

Deze functie is beschikbaar op FTD-apparaten met versie 7.1 en wordt later beheerd door een FMC versie 7.3 en hoger.

Configureren

Netwerkdigram

Dit beeld verstrekt een voorbeeld van een netwerkdigram.



Afbeelding 1. Voorbeeld diagram.

ISP1 = 10.115.117.1

ISP2 = 172.20.20.13

Configuraties

Stap 1. Configureer de objecten SLA Monitor.

Navigeer in het VCC naar Object > Object Management > SLA Monitor > Add SLA Monitor en voeg een SLA Monitor object toe voor de IP-adressen van de ISP.

SLA-monitor voor de primaire standaardgateway (ISP1).

The screenshot shows the 'Edit SLA Monitor Object' configuration window. The 'Name' field is highlighted with a red box and contains the text 'SAL1'. The other fields are as follows:

Name:	Description:
SAL1	
Frequency (seconds):	SLA Monitor ID*:
60 (1-604800)	1
Threshold (milliseconds):	Timeout (milliseconds):
5000 (0-60000)	5000 (0-604800000)
Data Size (bytes):	ToS:
28 (0-16384)	0
Number of Packets:	Monitor Address*:
1	10.115.117.1

```
route-map FMC_GENERATED_PBR_1679065711925
, permit, sequence 5
Match clauses:
ip address (access-lists): internal_networks

Set clauses:
ip next-hop verify-availability 10.115.117.1 1
track 1 [up]

ip next-hop 10.115.117.234
route-map FMC_GENERATED_PBR_1679065711925, permit, sequence 10
Match clauses:
ip address (access-lists): all_ipv4_for_pbr

Set clauses:
ip next-hop verify-availability 172.20.20.13 2
track 2 [up]

ip next-hop 172.20.20.77
firepower#
```

- show running-config sla monitor: Deze opdracht geeft de SLA-configuratie weer.

```
<#root>
firepower#
show running-config sla monitor

sla monitor 1

type echo protocol ipIcmpEcho 10.115.117.1 interface outside
sla monitor schedule 1 life forever start-time now

sla monitor 2

type echo protocol ipIcmpEcho 172.20.20.13 interface backup
sla monitor schedule 2 life forever start-time now
firepower#
```

- show sla monitor configuration: Deze opdracht geeft de SLA-configuratiewaarden weer.

```
<#root>
firepower#
show sla monitor configuration
```

SA Agent, Infrastructure Engine-II
Entry number:

1

Owner:
Tag:
Type of operation to perform: echo
Target address: 10.115.117.1

Interface: outside
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: 172.20.20.13

Interface: backup
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:

- show sla monitor operational-state: Dit bevel toont de operationele staat van de verrichting van SLA.

<#root>

firepower#

show sla monitor operational-state

Entry number: 1

Modification time: 15:48:04.332 UTC Fri Mar 17 2023
Number of Octets Used by this Entry: 2056
Number of operations attempted: 74
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: 17:01:04.334 UTC Fri Mar 17 2023
Latest operation return code: OK
RTT Values:
RTTAvg: 1 RTTMin: 1 RTTMax: 1
NumOfRTT: 1 RTTSum: 1 RTTSum2: 1

Entry number: 2

Modification time: 15:48:04.335 UTC Fri Mar 17 2023
Number of Octets Used by this Entry: 2056
Number of operations attempted: 74
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: 17:01:04.337 UTC Fri Mar 17 2023
Latest operation return code: OK
RTT Values:
RTTAvg: 1 RTTMin: 1 RTTMax: 1
NumOfRTT: 1 RTTSum: 1 RTTSum2: 1

- show track: Deze opdracht geeft de informatie weer over objecten die worden bijgehouden door het SLA Track-proces.

<#root>

firepower#

show track

Track 1

Response Time Reporter 1 reachability

Reachability is Up

4 changes, last change 00:53:42
Latest operation return code: OK
Latest RTT (milliseconds) 1
Tracked by:
ROUTE-MAP 0
STATIC-IP-ROUTING 0

Track 2

Response Time Reporter 2 reachability

Reachability is Up

2 changes, last change 01:13:41
Latest operation return code: OK
Latest RTT (milliseconds) 1
Tracked by:
ROUTE-MAP 0
STATIC-IP-ROUTING 0

- show running-config route: Dit bevel toont de huidige routeconfiguratie.

```
<#root>
```

```
firepower#
```

```
show running-config route
```

```
route
```

```
outside
```

```
0.0.0.0 0.0.0.0 10.115.117.1 1
```

```
track 1
```

```
route
```

```
backup
```

```
0.0.0.0 0.0.0.0 172.20.20.13 254
```

```
track 2
```

```
route vlan2816 10.42.0.37 255.255.255.255 10.43.0.1 254
```

```
firepower#
```

- show route: Dit bevel toont de routingstabel voor de gegevensinterfaces.

```
<#root>
```

```
firepower#
```

```
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 10.115.117.1 to network 0.0.0.0
```

```
s* 0.0.0.0 0.0.0.0 [1/0] via 10.115.117.1, outside
```

```
S 10.0.0.0 255.0.0.0 [1/0] via 10.88.243.1, backbone  
C 10.88.243.0 255.255.255.0 is directly connected, backbone  
L 10.88.243.67 255.255.255.255 is directly connected, backbone  
C 10.115.117.0 255.255.255.0 is directly connected, outside  
L 10.115.117.234 255.255.255.255 is directly connected, outside  
C 10.42.0.0 255.255.255.0 is directly connected, vlan2816  
L 10.42.0.1 255.255.255.255 is directly connected, vlan2816  
S 10.42.0.37 255.255.255.255 [254/0] via 10.43.0.1, vlan2816  
C 172.20.20.0 255.255.255.0 is directly connected, backup  
L 172.20.20.77 255.255.255.255 is directly connected, backup
```

Wanneer de primaire link mislukt:

- show route-map: Dit bevel toont de route-kaart configuratie wanneer een verbinding ontbreekt.

```
<#root>
```

```
firepower#
```

```
show route-map FMC_GENERATED_PBR_1679065711925
```

```
route-map FMC_GENERATED_PBR_1679065711925, permit, sequence 5  
Match clauses:  
ip address (access-lists): internal_networks  
  
Set clauses:  
ip next-hop verify-availability 10.115.117.1 1  
  
track 1 [down]
```

```
ip next-hop 10.115.117.234
```



```
route-map FMC_GENERATED_PBR_1679065711925, permit, sequence 10
Match clauses:
ip address (access-lists): all_ipv4_for_pbr

Set clauses:
ip next-hop verify-availability 172.20.20.13 2

track 2 [up]
```

```
ip next-hop 172.20.20.77
firepower#
```

- show route: Dit bevel toont de nieuwe routingstabel per interface.

```
<#root>
```

```
firepower#
```

```
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 10.115.117.1 to network 0.0.0.0
```

```
S* 0.0.0.0 0.0.0.0 [1/0] via 172.20.20.13, backup
```

```
S 10.0.0.0 255.0.0.0 [1/0] via 10.88.243.1, backbone
C 10.88.243.0 255.255.255.0 is directly connected, backbone
L 10.88.243.67 255.255.255.255 is directly connected, backbone
C 10.115.117.0 255.255.255.0 is directly connected, outside
L 10.115.117.234 255.255.255.255 is directly connected, outside
C 10.42.0.0 255.255.255.0 is directly connected, vlan2816
L 10.42.0.1 255.255.255.255 is directly connected, vlan2816
S 10.42.0.37 255.255.255.255 [254/0] via 10.43.0.1, vlan2816
C 172.20.20.0 255.255.255.0 is directly connected, backup
L 172.20.20.77 255.255.255.255 is directly connected, backup
```

Gerelateerde informatie

- [Cisco Secure Firewall Management Center-beheershandleiding, 7.3](#)
- [Technische ondersteuning en documentatie â€™ Cisco Systems](#)

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.