Dual-ISP-Failover für von FMC verwaltetes FTD konfigurieren

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie DUAL ISP Failover mit PBR und IP SLAs auf einem FTD konfiguriert wird, das vom FMC verwaltet wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Richtlinienbasiertes Routing
- Internet Protocol Service Level Agreement (IP SLA)
- Firepower Management Center (FMC)
- Firepower Threat Defense (FTD)

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- FMCv 7.3.0
- FTDv 7.3.0

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Übersicht über die Funktionen der statischen Routenverfolgung

Dank der Funktion zur statischen Routenverfolgung kann die FTD eine Verbindung zu einem sekundären ISP verwenden, wenn die primäre Mietleitung nicht mehr verfügbar ist. Um diese Redundanz zu erreichen, ordnet die FTD einem von Ihnen definierten Überwachungsziel eine statische Route zu. Beim SSLA-Vorgang wird das Ziel mit periodischen ICMP-Echo-Anforderungen überwacht.

Wenn keine Echo-Antwort empfangen wird, gilt das Objekt als ausgefallen, und die zugehörige Route wird aus der Routing-Tabelle entfernt. Anstelle der entfernten Route wird eine zuvor konfigurierte Backup-Route verwendet. Während der Backup-Route wird der SLA-Überwachungsvorgang fortgesetzt, um das Überwachungsziel zu erreichen.

Sobald das Ziel wieder verfügbar ist, wird die erste Route in der Routing-Tabelle ersetzt, und die Backup-Route wird entfernt.

Sie können jetzt mehrere Next-Hops und richtlinienbasierte Weiterleitungsaktionen gleichzeitig konfigurieren. Wenn der Datenverkehr die Kriterien für die Route erfüllt, versucht das System, den Datenverkehr an die von Ihnen angegebenen IP-Adressen weiterzuleiten, bis er erfolgreich ist.

Diese Funktion steht auf FTD-Geräten mit Version 7.1 und höher zur Verfügung, die von einem FMC mit Version 7.3 und höher verwaltet werden.

Konfigurieren

Netzwerkdiagramm

Dieses Bild zeigt ein Beispiel eines Netzwerkdiagramms.

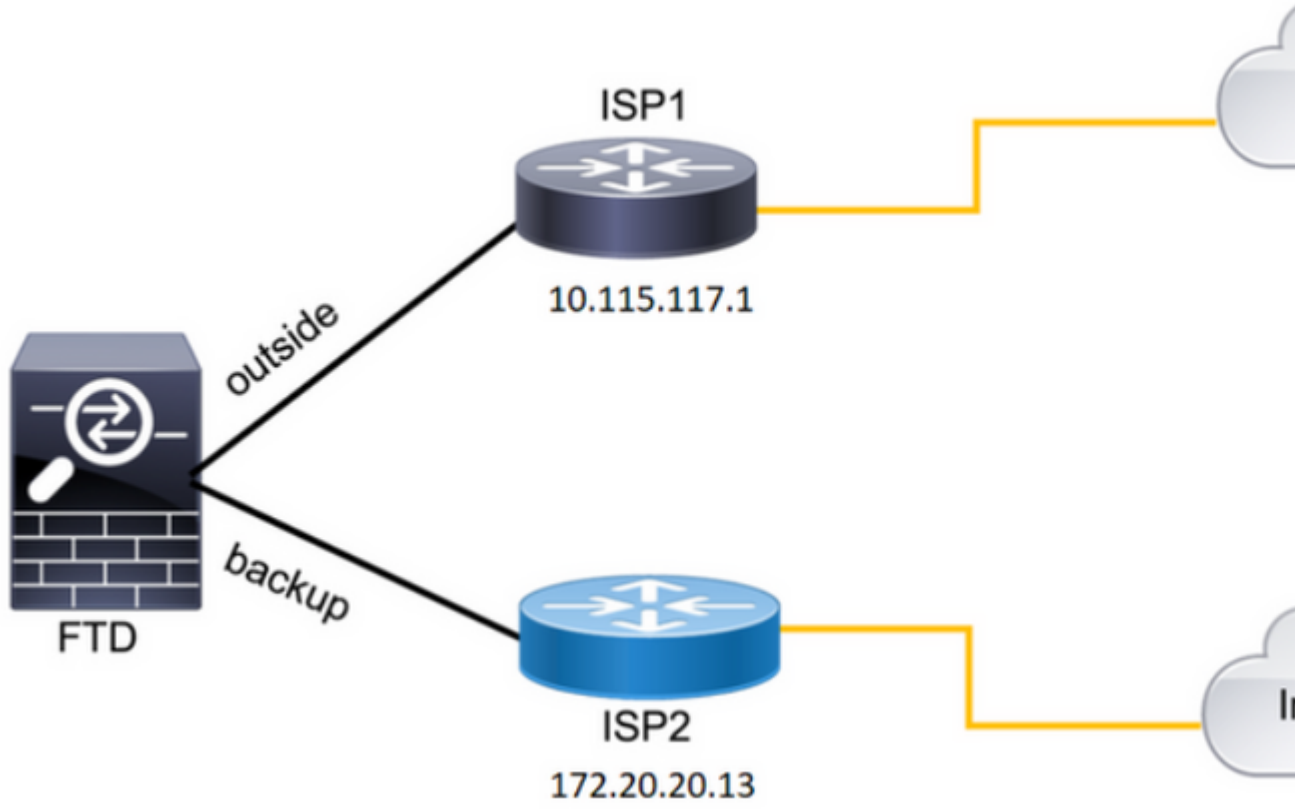


Bild 1. Beispiel: Diagramm

ISP1 = 10,115.117,1

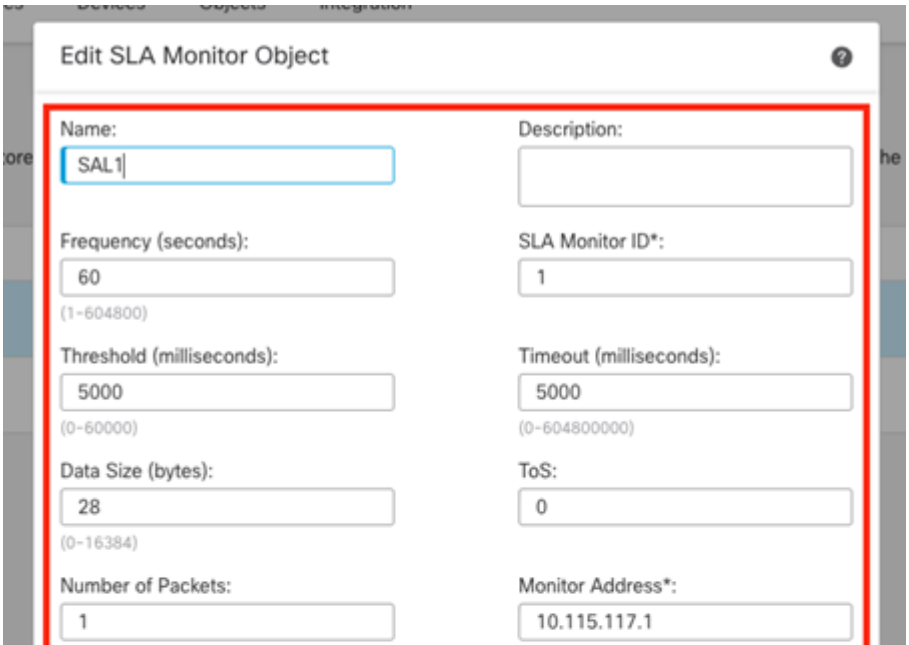
ISP2 = 172,20,20,13

Konfigurationen

Schritt 1: Konfigurieren Sie die SLA-Überwachungsobjekte.

Navigieren Sie auf dem FMC zu Object > Object Management > SLA Monitor > Add SLA Monitor und fügen Sie ein SLA-Überwachungsobjekt für die IP-Adressen des ISP hinzu.

SLA-Monitor für das primäre Standard-Gateway (ISP1).



```
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: Mit diesem Befehl wird die SLA-Konfiguration angezeigt.

<#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: Dieser Befehl zeigt die SLA-Konfigurationswerte an.

<#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: Dieser Befehl zeigt den Betriebsstatus des SLA-Vorgangs an.

<#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: Dieser Befehl zeigt Informationen zu Objekten an, die vom SLA Track-Prozess verfolgt werden.

<#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 (millisecs) 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 (millisecs) 1
Tracked by:
ROUTE-MAP 0
STATIC-IP-ROUTING 0
```

- show running-config route: Mit diesem Befehl wird die aktuelle Routenkonfiguration angezeigt.

<#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: Mit diesem Befehl wird die Routing-Tabelle für die Datenschnittstellen angezeigt.

<#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
```

Wenn die primäre Verbindung ausfällt:

- show route-map: Dieser Befehl zeigt die Routing-Map-Konfiguration an, wenn eine Verbindung fehlschlägt.

<#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: Mit diesem Befehl wird die neue Routing-Tabelle pro Schnittstelle angezeigt.

<#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
```

Zugehörige Informationen

- Cisco Secure Firewall Management Center - Administrationsleitfaden, 7.3
- Technischer Support und Dokumentation für Cisco Systeme