

Configurazione del failover di due ISP per FTD gestito da FMC

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Panoramica della funzione Tracciamento route statica](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazioni](#)

[Verifica](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come configurare il failover di due ISP con PBR e SLA IP su un FTD gestito da FMC.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- PBR (Policy Based Routing)
- Contratto di servizio (SLA) per il protocollo Internet
- Firepower Management Center (FMC)
- Firepower Threat Defense (FTD)

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- FMCv 7.3.0
- FTDv 7.3.0

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Panoramica della funzione Tracciamento route statica

La funzione Static Route Tracking consente all'FTD di utilizzare una connessione a un ISP secondario in caso di indisponibilità della linea principale. Per ottenere questa ridondanza, l'FTD associa una route statica a un oggetto di monitoraggio definito dall'utente. L'operazione SSLA monitora la destinazione con richieste echo ICMP periodiche.

Se non si riceve una risposta echo, l'oggetto viene considerato inattivo e la route associata viene rimossa dalla tabella di routing. Al posto della route rimossa viene utilizzata una route di backup configurata in precedenza. Mentre il percorso di backup è in uso, l'operazione di monitoraggio SLA continua i tentativi di raggiungere la destinazione di monitoraggio.

Quando la destinazione è nuovamente disponibile, la prima route viene sostituita nella tabella di routing e la route di backup viene rimossa.

È ora possibile configurare contemporaneamente più hop successivi e più azioni di inoltro di routing basate su criteri. Quando il traffico soddisfa i criteri per la route, il sistema tenta di inoltrare il traffico agli indirizzi IP nell'ordine specificato, fino a quando non riesce.

La funzionalità è disponibile sui dispositivi FTD che eseguono la versione 7.1 e successive gestiti da un FMC versione 7.3 e successive.

Configurazione

Esempio di rete

L'immagine mostra un esempio di diagramma di rete.

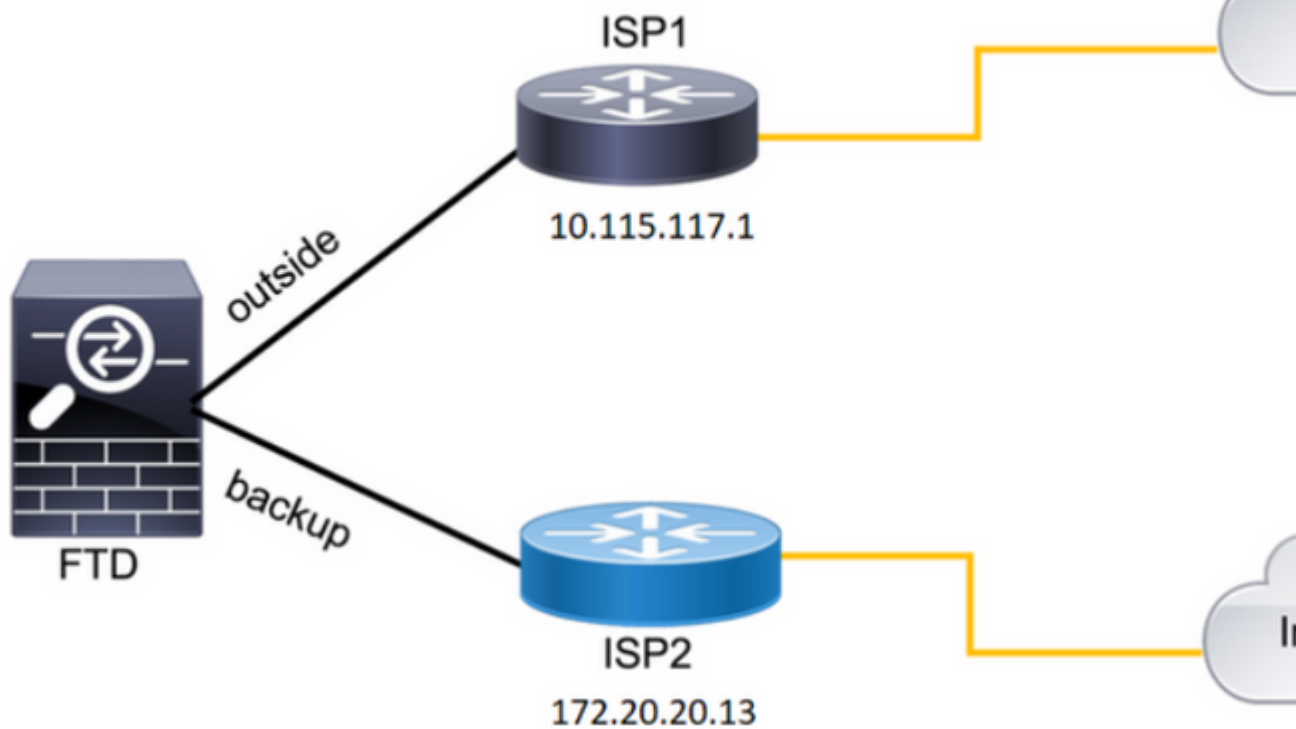


Immagine 1. Esempio di diagramma.

ISP1 = 10.115.117.1

ISP2 = 172.20.20.13

Configurazioni

Passaggio 1. Configurare gli oggetti di monitoraggio SLA.

Nel CCP passare a Object > Object Management > SLA Monitor > Add SLA Monitor e aggiungere un oggetto Monitor contratto di servizio per gli indirizzi IP dell'ISP.

Monitor SLA per il gateway predefinito primario (ISP1).

The screenshot shows the 'Edit SLA Monitor Object' configuration window. The fields are as follows:

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

- Scegli IP Address dal Send to opzione.
- Nell'esempio, 10.115.117.234 è l'indirizzo IP interno del FTD.

Edit Forwarding Actions

Match ACL:*	<input type="text" value="all_ipv4_for_pbr"/>	+
Send To:*	<input type="text" value="IP Address"/>	
IPv4 Addresses:	<input type="text" value="10.115.117.234"/>	
IPv6 Addresses:	<input type="text" value="For example, 2001:db8::, 2002:db8::1"/>	
Don't Fragment:	<input type="text" value="None"/>	

Default Interface

IPv4 settings

IPv6 settings

Recursive:

Default:

Peer Address

Verify Availability

Immagine 7. Finestra di configurazione Azioni di inoltra.

Scorrere verso il basso e aggiungere la **Verify Availability** valori per ISP1.

Edit Forwarding Actions

Default Interface

IPv4 settings

IPv6 settings

Recursive:

Default:

Peer Address

Verify Availability

IP Address:

Sequence:

Track:

```
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: questo comando visualizza la configurazione del contratto di servizio.

```
<#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: questo comando visualizza i valori di configurazione del contratto di servizio.

```
<#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: questo comando visualizza lo stato operativo dell'operazione 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`: questo comando visualizza le informazioni sugli oggetti tracciati dal processo di tracciamento del contratto di servizio.

```
<#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`: questo comando visualizza la configurazione corrente del percorso.

<#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`: questo comando visualizza la tabella di routing per le interfacce dati.

```
<#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
```

Quando il collegamento principale non riesce:

- show route-map: questo comando visualizza la configurazione route-map quando un collegamento non riesce.

```
<#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`: questo comando visualizza la nuova tabella di routing per interfaccia.

```
<#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
```

Informazioni correlate

- [Guida all'amministrazione di Cisco Secure Firewall Management Center, 7.3](#)
- [Documentazione e supporto tecnico "Cisco Systems"](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).