

为由FMC管理的FTD配置双ISP故障切换

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[静态路由跟踪功能概述](#)

[配置](#)

[网络图](#)

[配置](#)

[验证](#)

[相关信息](#)

简介

本文档介绍如何在由FMC管理的FTD上使用PBR和IP SLA配置DUAL ISP故障切换。

先决条件

要求

Cisco 建议您了解以下主题：

- 策略型路由 (PBR)
- Internet协议服务级别协议(IP SLA)
- Firepower Management Center (FMC)
- Firepower Threat Defense (FTD)

使用的组件

本文档中的信息基于以下软件和硬件版本：

- FMCv 7.3.0
- FTDv 7.3.0

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

静态路由跟踪功能概述

静态路由跟踪功能允许FTD在主租用线路不可用时使用与辅助ISP的连接。为了实现此冗余，FTD将静态路由与您定义的监控目标相关联。SSLA操作使用定期ICMP回应请求监控目标。

如果未收到应答，则认为对象已关闭，并且将从路由表中删除关联的路由。并用以前配置的备份路由代替所删除的路由。当备份路由正在使用时，SLA监控操作会继续尝试访问监控目标。

目标再次可用后，将替换路由表中的第一个路由，并删除备份路由。

现在，您可以同时配置多个下一跳和基于策略的路由转发操作。当流量与路由标准匹配时，系统会尝试按照您指定的顺序将流量转发到IP地址，直到成功为止。

此功能在运行版本7.1及更高版本的FTD设备上可用，由FMC版本7.3及更高版本管理。

配置

网络图

下图为网络图示例。

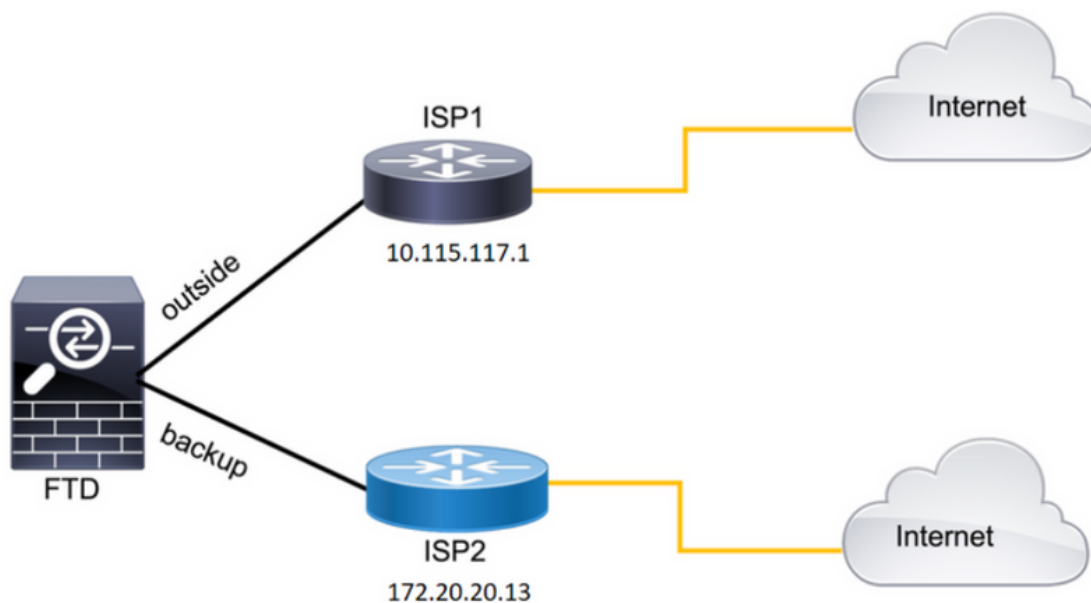


图 1.图示例。

ISP1 = 10.115.117.1

ISP2 = 172.20.20.13

配置

步骤1:配置SLA监控器对象。

在FMC上，导航到Object > Object Management > SLA Monitor > Add SLA Monitor，然后为ISP IP地址添加SLA监控器对象。

主默认网关(ISPI)的SLA监控器。

Edit SLA Monitor Object ?

Name: <input type="text" value="SAL1"/>	Description: <input type="text"/>
Frequency (seconds): <input type="text" value="60"/> <small>(1-604800)</small>	SLA Monitor ID*: <input type="text" value="1"/>
Threshold (milliseconds): <input type="text" value="5000"/> <small>(0-60000)</small>	Timeout (milliseconds): <input type="text" value="5000"/> <small>(0-604800000)</small>
Data Size (bytes): <input type="text" value="28"/> <small>(0-16384)</small>	ToS: <input type="text" value="0"/>
Number of Packets: <input type="text" value="1"/>	Monitor Address*: <input type="text" value="10.115.117.1"/>
Available Zones ↻ <input type="text" value="Search"/> Backbone Backup new Outside VLAN2816	Selected Zones/Interfaces <input type="text" value="Outside"/>

图 2.SLA1 monitor configuration窗口。

辅助默认网关(ISP2)的SLA监控器。

Edit SLA Monitor Object



Name:

Description:

Frequency (seconds):

(1-604800)

SLA Monitor ID*:

Threshold (milliseconds):

(0-60000)

Timeout (milliseconds):

(0-604800000)

Data Size (bytes):

(0-16384)

ToS:

Number of Packets:

Monitor Address*:

Available Zones

Backbone

Add

Selected Zones/Interfaces

Backup

Backup

new

Outside

VLAN2816

Cancel

Save

图 3.SLA2监控配置窗口。

第二步：使用路由跟踪配置静态路由。

在FMC上，导航到Device > Device Management > Edit the desired FTD > Routing > Static Routes，并使用正确的SLA监控器添加static路由。


SLA监控器必须是监控默认网关的监控器。


主默认网关的静态路由：

Edit Static Route Configuration

Type: IPv4 IPv6

Interface*
outside

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


Available Network  +

Selected Network

Search

10.10.10.1
10.117.0.250
10.34.24.91
172.16.0.20
172.20.20.13
192.168.1.20

Add

any-ipv4 

Ensure that egress virtualrouter has route to that destination

Gateway
10.115.117.1 +

Metric:
1
(1 - 254)

Tunneled: (Used only for default Route)

Route Tracking:
SAL1 +

图 4.外部接口的静态路由配置窗口。

辅助默认网关的静态路由。

Edit Static Route Configuration

Type: IPv4 IPv6

Interface*
backup

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

Available Network +

Selected Network

10.10.10.1
10.117.0.250
10.34.24.91
172.16.0.20
172.20.20.13
192.168.1.20

any-ipv4

Ensure that egress virtualrouter has route to that destination

Gateway
172.20.20.13 +

Metric:
254
(1 - 254)

Tunneled: (Used only for default Route)

Route Tracking:
SLA2 +

图 5.备份接口的静态路由配置窗口。

第三步：配置策略基本路由。

导航至添Device > Device Management > Edit the desired FTD > Routing > Policy Based Routing, 加PBR , 然后选择入口接口。

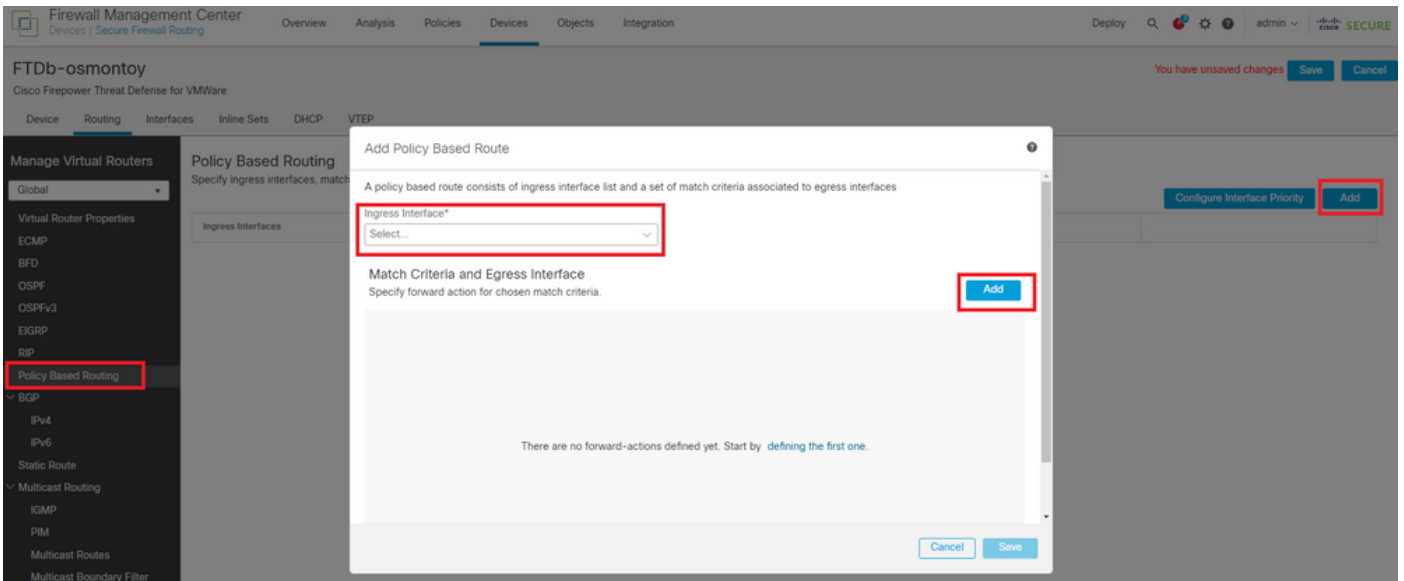


图 6.PBR配置窗口。

配置转发操作。

- 选择或添加要匹配的新访问控制列表。
- 从Send to选项中选择IP Address。
- 在本示例中，10.115.117.234是FTD外部IP地址。

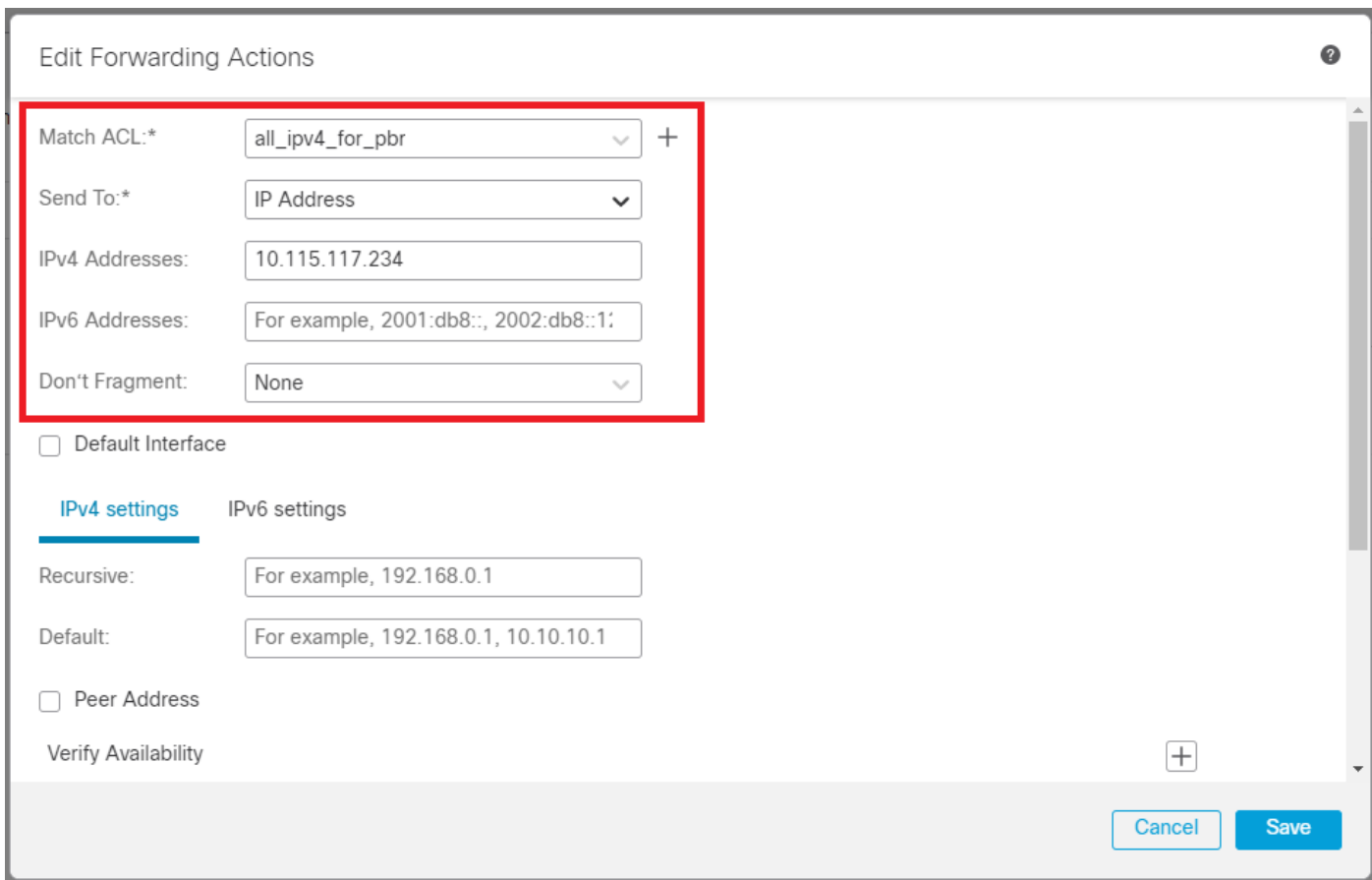


图 7. Forwarding Actions 配置窗口。

向下滚动并添加ISP1的Verify Availability 值。

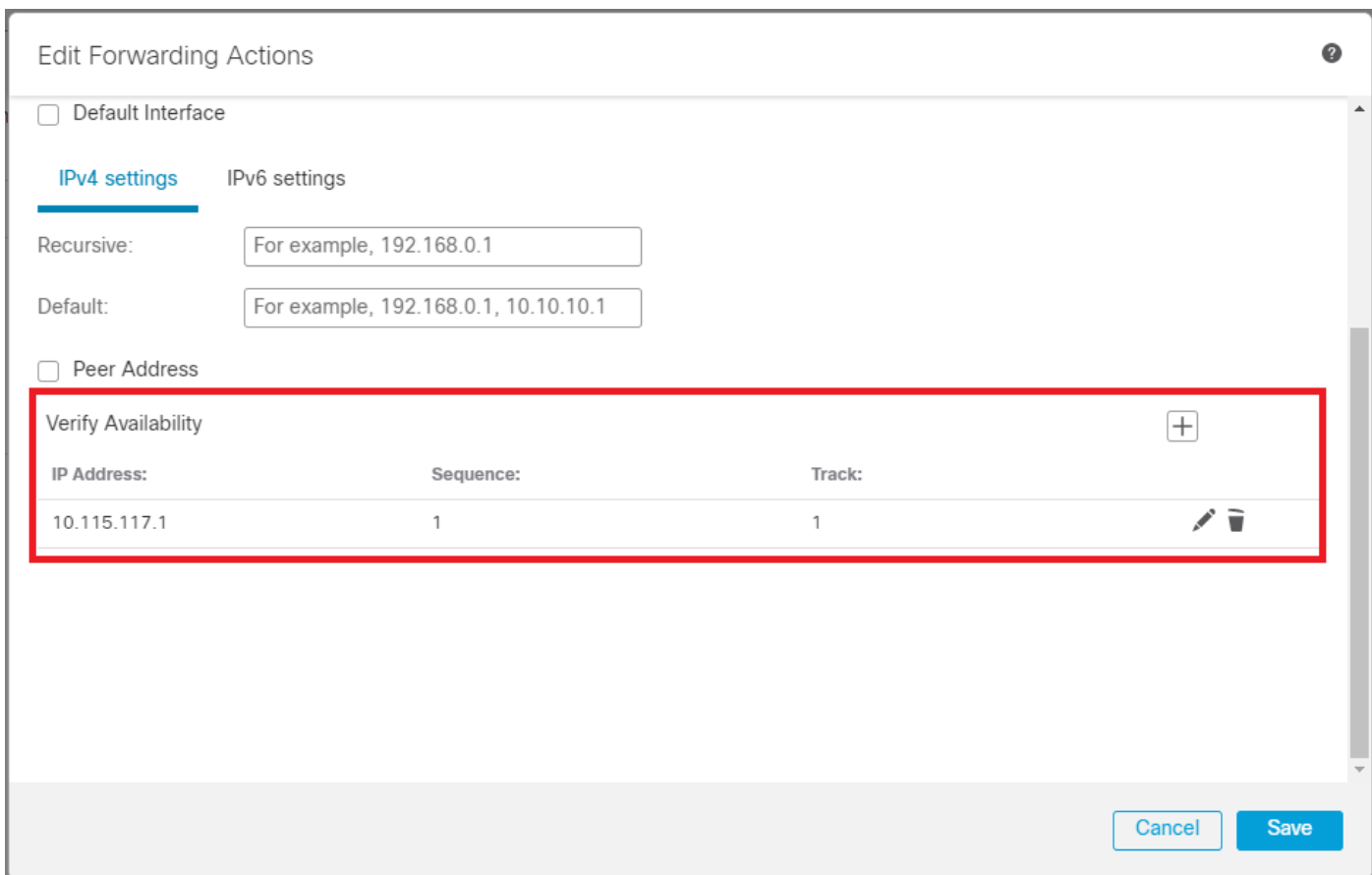


图 8. Forwarding Actions 配置窗口。

对备份接口重复相同的过程。但是，请确保使用其他访问控制列表对象。

The image shows a configuration window titled "Edit Forwarding Actions". A red rectangular box highlights the following fields:

- Match ACL:*: internal_networks
- Send To:*: IP Address
- IPv4 Addresses: 172.20.20.77
- IPv6 Addresses: For example, 2001:db8::, 2002:db8::1:
- Don't Fragment: None

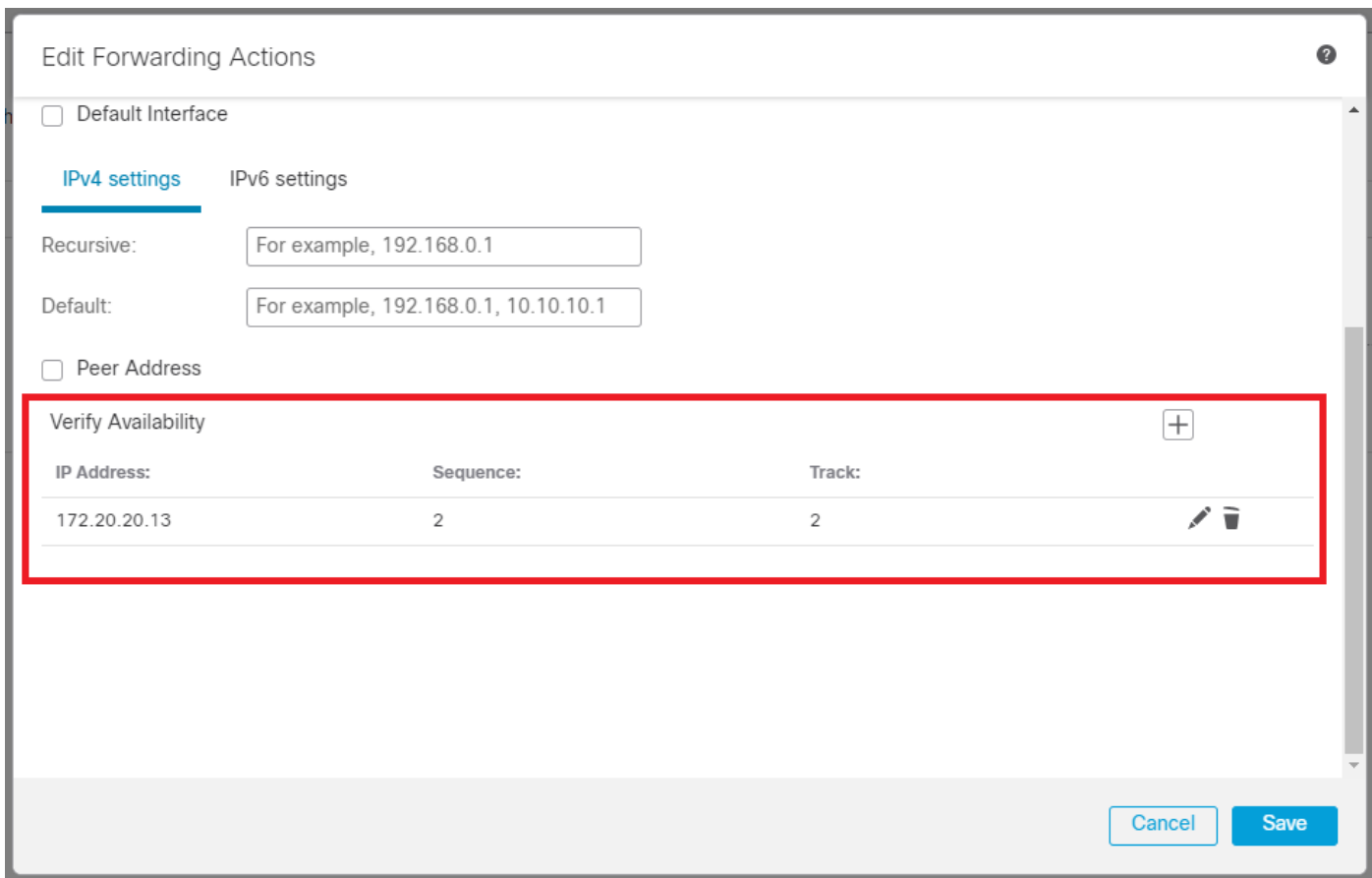
Below the highlighted section, there are several other options:

- Default Interface
- IPv4 settings (selected) | IPv6 settings
- Recursive: For example, 192.168.0.1
- Default: For example, 192.168.0.1, 10.10.10.1
- Peer Address
- Verify Availability

At the bottom right, there are "Cancel" and "Save" buttons, and a "+" icon for adding more actions.

图 9. Forwarding Actions 配置窗口

对ISP2重复相同Verify Availability的配置过程。



映像10.验证可用性配置。

验证您的配置。

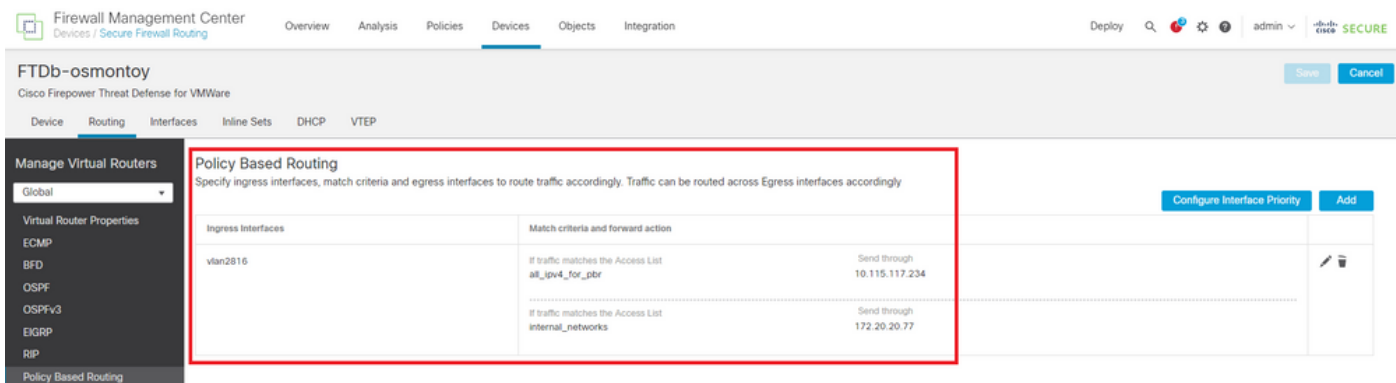


图 11.PBR配置。

验证

通过安全外壳(SSH)访问FTD并使用命令system support disagnotsic-cli , 然后运行以下命令 :

•

show route-map : 此命令显示路由映射配置。

<#root>

firepower#

show route-map

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 : 此命令显示SLA配置。

<#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 : 此命令显示SLA配置值。

<#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 : 此命令显示SLA操作的运行状态。

<#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 : 此命令显示SLA跟踪进程跟踪的对象的信息。

<#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 : 此命令显示当前路由配置。

<#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 v1an2816 10.42.0.37 255.255.255.255 10.43.0.1 254
firepower#

- show route : 此命令显示数据接口的路由表。

<#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

当主链路发生故障时：

- show route-map : 此命令在链路发生故障时显示路由映射配置。

<#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 : 此命令显示每个接口的新路由表。

```
<#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

相关信息

- [Cisco安全防火墙管理中心管理指南7.3](#)
- [技术支持和文档 - Cisco Systems](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。