

FMC에서 관리하는 FTD에 대한 이중 ISP 장애 조치 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[고정 경로 추적 기능 개요](#)

[구성](#)

[네트워크 다이어그램](#)

[설정](#)

[다음을 확인합니다.](#)

[관련 정보](#)

소개

이 문서에서는 FMC에서 관리하는 FTD에서 PBR 및 IP SLA를 사용하여 이중 ISP 장애 조치를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

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

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- FMCv 7.3.0
- FTDv 7.3.0

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든

명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

고정 경로 추적 기능 개요

고정 경로 추적 기능을 사용하면 기본 임대 회선을 사용할 수 없는 경우 FTD에서 보조 ISP에 대한 연결을 사용할 수 있습니다. 이러한 이중화를 달성하기 위해 FTD는 고정 경로를 사용자가 정의하는 모니터링 대상과 연결합니다. SLA 작업은 주기적인 ICMP 에코 요청으로 대상을 모니터링합니다.

에코 응답이 수신되지 않으면 객체는 다운된 것으로 간주되며 연결된 경로가 라우팅 테이블에서 제거됩니다. 이전에 구성한 백업 경로가 제거된 경로 대신 사용됩니다. 백업 경로가 사용 중인 동안 SLA 모니터 작업은 모니터링 대상에 도달하기 위한 시도를 계속합니다.

대상을 다시 사용할 수 있게 되면 첫 번째 경로가 라우팅 테이블에서 대체되고 백업 경로가 제거됩니다.

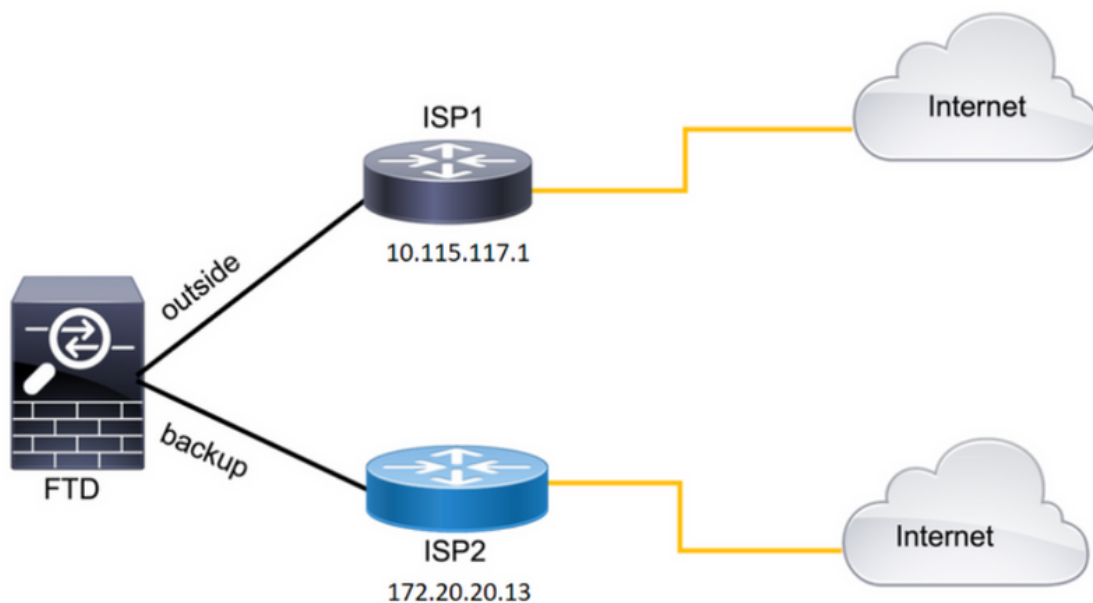
이제 여러 next-hop 및 정책 기반 라우팅 포워딩 작업을 동시에 구성할 수 있습니다. 트래픽이 경로 기준과 일치하면 시스템은 트래픽이 성공할 때까지 사용자가 지정한 순서대로 IP 주소로 트래픽을 전달하려고 시도합니다.

이 기능은 FMC 버전 7.3 이상에서 관리하는 버전 7.1 이상을 실행하는 FTD 디바이스에서 사용할 수 있습니다.

구성

네트워크 다이어그램

이 이미지는 네트워크 다이어그램의 예를 제공합니다.



이미지 1. 다이어그램 예

ISP1 = 10.115.117.1

ISP2 = 172.20.20.13

설정

1단계. SLA 모니터 객체를 구성합니다.

FMC에서 Object > Object Management > SLA Monitor > Add SLA Monitor ISP IP 주소에 대한 SLA Monitor 개체를 추가합니다.

기본 기본 게이트웨이(ISP1)에 대한 SLA 모니터입니다.

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
- Backup
- new
- Outside
- VLAN2816

Add

Selected Zones/Interfaces

- Outside

Cancel

Save

이미지 2. SLA1 모니터 구성 창

보조 기본 게이트웨이(ISP2)에 대한 SLA 모니터입니다.

Edit SLA Monitor Object ?

Name: <input type="text" value="SLA2"/>	Description: <input type="text"/>
Frequency (seconds): <input type="text" value="60"/> <small>(1-604800)</small>	SLA Monitor ID*: <input type="text" value="2"/>
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="172.20.20.13"/>
Available Zones ↻ <input type="text" value="Search"/>	Selected Zones/Interfaces
<ul style="list-style-type: none">BackboneBackupnewOutsideVLAN2816	<ul style="list-style-type: none">Backup 🗑

이미지 3. SLA2 모니터 구성 창

2단계. 경로 추적을 사용하여 고정 경로를 구성합니다.

FMC에서 Device > Device Management > Edit the desired FTD > Routing > Static Routes 올바른 SLA 모니터로 통계 경로를 추가합니다.

SLA 모니터는 기본 게이트웨이를 모니터링하는 것이어야 합니다.

기본 기본 게이트웨이의 고정 경로:

Edit Static Route Configuration



Type: IPv4 IPv6

Interface*

outside

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

Available Network  +

Search

Add

Selected Network

any-ipv4 

10.10.10.1

10.117.0.250

10.34.24.91

172.16.0.20

172.20.20.13

192.168.1.20

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 +


이미지 4. 외부 인터페이스에 대한 고정 경로 컨피그레이션 창

보조 기본 게이트웨이의 고정 경로입니다.

Edit Static Route Configuration ?

Type: IPv4 IPv6

Interface*

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

Available 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

Add

Selected Network

any-ipv4 🗑

Ensure that egress virtualrouter has route to that destination

Gateway
 +

Metric:

(1 - 254)

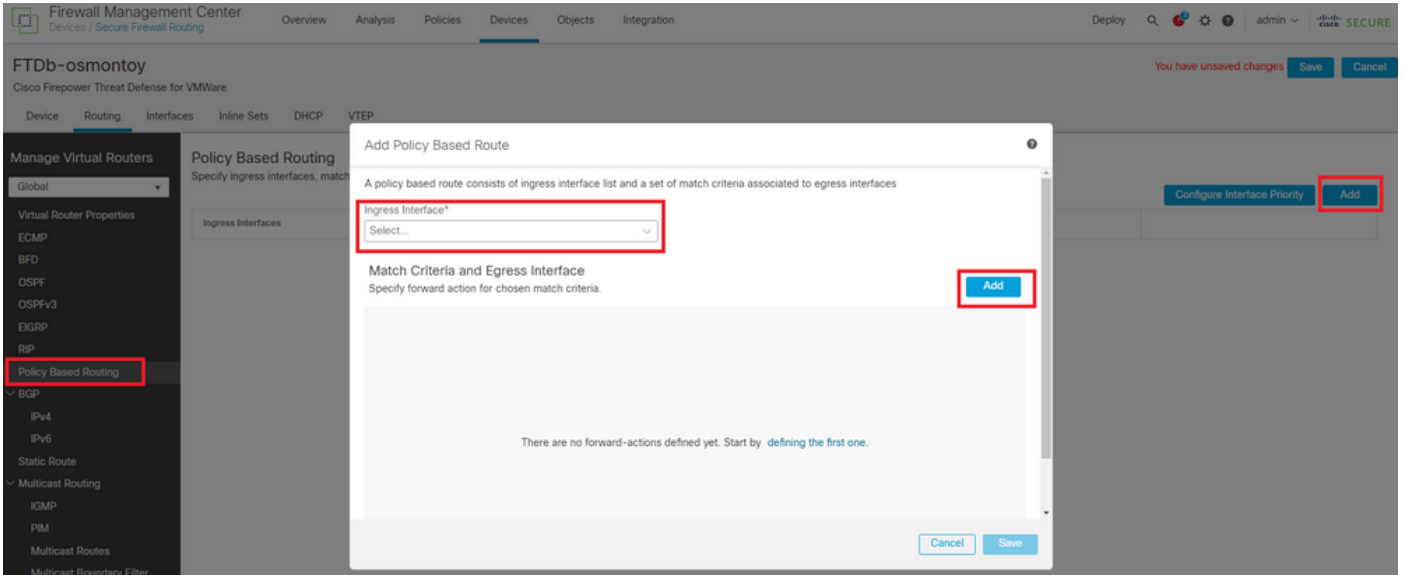
Tunneled: (Used only for default Route)

Route Tracking:
 +

이미지 5. 백업 인터페이스에 대한 고정 경로 컨피그레이션 창

3단계. 정책 기반 경로를 구성합니다.

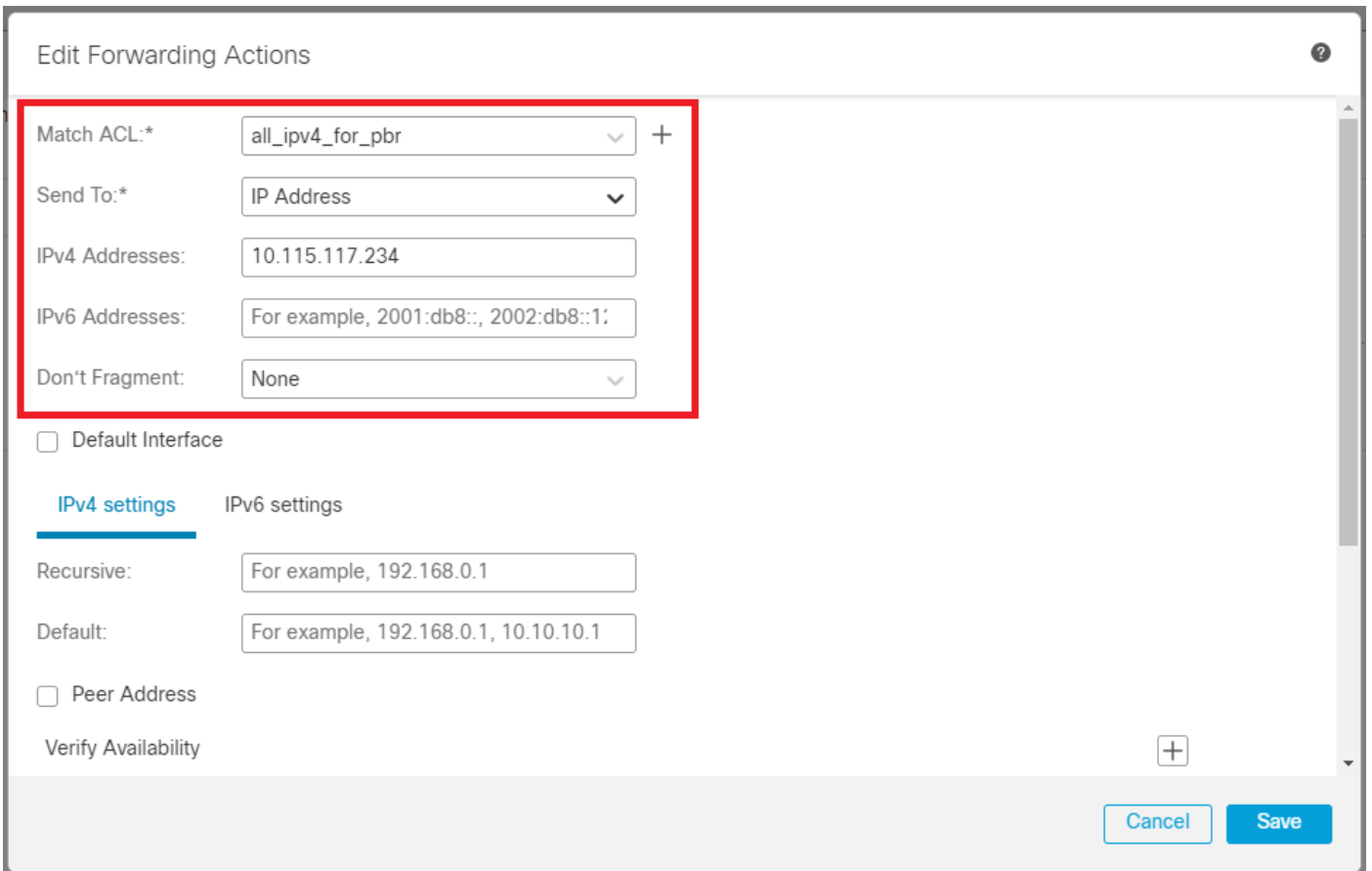
탐색 Device > Device Management > Edit the desired FTD > Routing > Policy Based Routing, pbr을 추가하고 인그레스 인터페이스를 선택합니다.



이미지 6. PBR 컨피그레이션 창

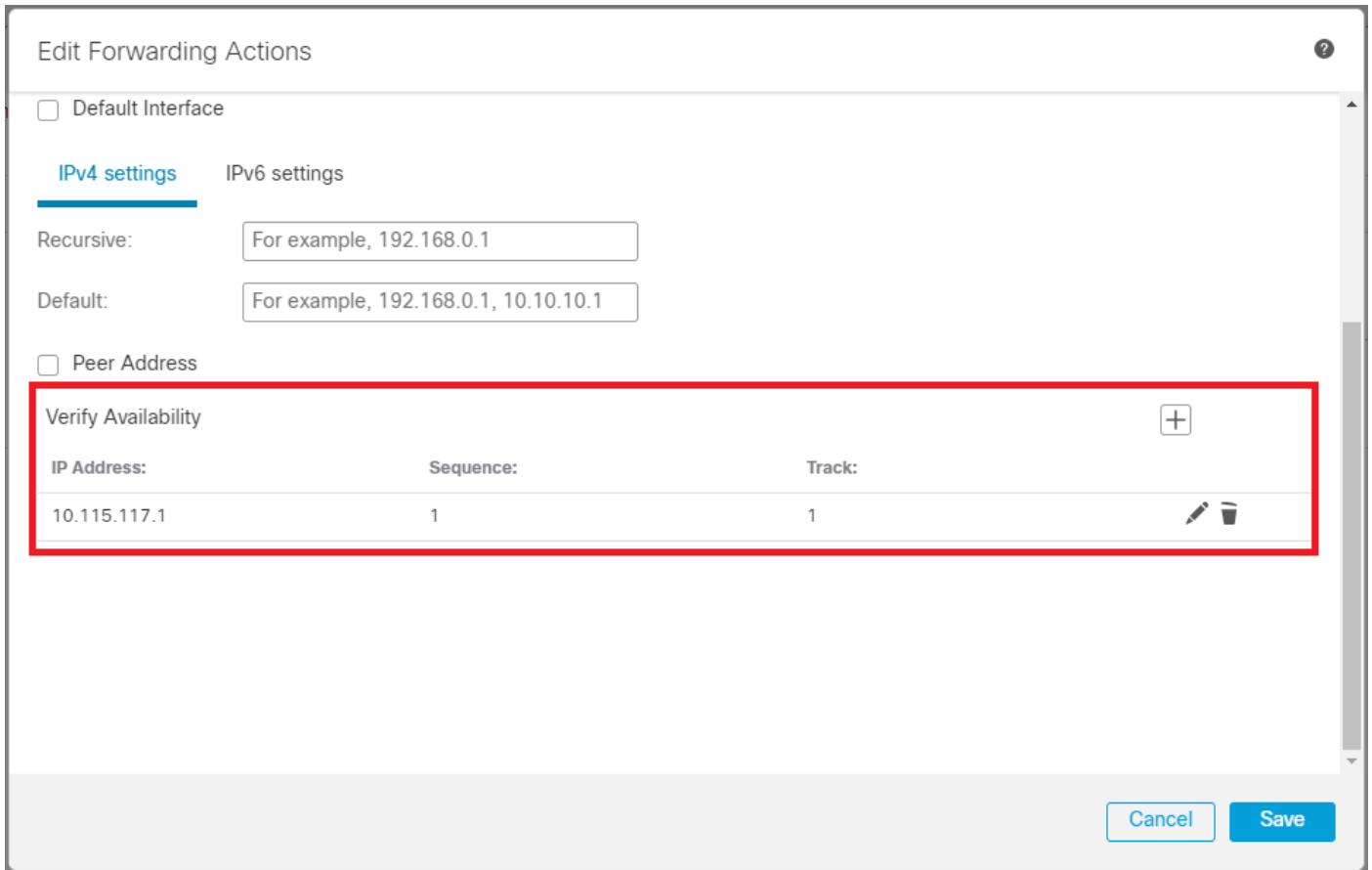
전달 작업을 구성합니다.

- 일치시킬 새 액세스 제어 목록을 선택하거나 추가합니다.
- 선택IP Address 에서 Send to 옵션을 선택합니다.
- 이 예에서는 10.115.117.234가 FTD 내부 IP 주소입니다.



이미지 7. 전달 작업 구성 창

아래로 스크롤하여 Verify Availability ISP1의 값입니다.



이미지 8. 전달 작업 구성 창

백업 인터페이스에 대해 동일한 프로세스를 반복합니다. 그러나 다른 ACL(Access Control List) 객체를 사용해야 합니다.

Edit Forwarding Actions

Match ACL:* +

Send To:*

IPv4 Addresses:

IPv6 Addresses:

Don't Fragment:

Default Interface

IPv4 settings IPv6 settings

Recursive:

Default:

Peer Address

Verify Availability +

Cancel Save

이미지 9. Forwarding Actions 컨피그레이션 창

에 대해 동일한 프로세스를 반복합니다 Verify Availability ISP2에 대한 컨피그레이션입니다.

Edit Forwarding Actions

Default Interface

IPv4 settings IPv6 settings

Recursive:

Default:

Peer Address

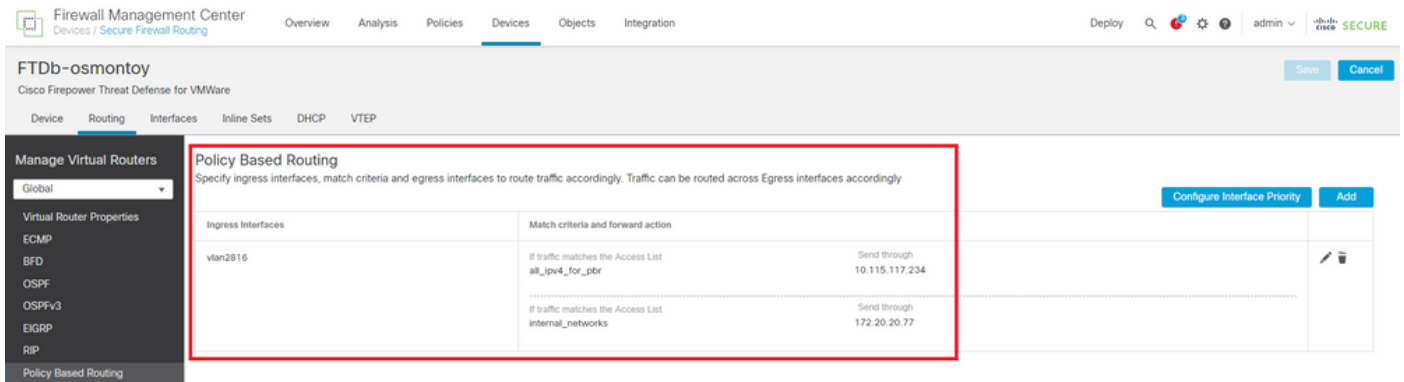
Verify Availability +

IP Address:	Sequence:	Track:	
172.20.20.13	2	2	✎ 🗑

Cancel Save

이미지 10.가용성 구성을 확인합니다.

컨피그레이션을 확인합니다.



이미지 11. PBR 컨피그레이션

다음을 확인합니다.

SSH(Secure Shell)를 통해 FTD에 액세스하고 명령을 사용합니다 system support disagnostic-cli 다음 명령을 실행합니다.

- show route-map: 이 명령은 route-map 컨피그레이션을 표시합니다.

```
<#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: 이 명령은 SLA 컨피그레이션을 표시합니다.

```
<#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: 이 명령은 SLA 컨피그레이션 값을 표시합니다.

```
<#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: 이 명령은 SLA 작업의 작업 상태를 표시합니다.

<#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: 이 명령은 SLA 추적 프로세스에 의해 추적되는 객체에 대한 정보를 표시합니다.

<#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`: 이 명령은 현재 경로 컨피그레이션을 표시합니다.

```
<#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`: 이 명령은 데이터 인터페이스의 라우팅 테이블을 표시합니다.

```
<#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
```

기본 링크에 장애가 발생하는 경우:

- `show route-map`: 이 명령은 링크가 실패할 경우 route-map 컨피그레이션을 표시합니다.

<#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`: 이 명령은 인터페이스당 새 라우팅 테이블을 표시합니다.

<#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
```

관련 정보

- [Cisco Secure Firewall Management Center 관리 가이드, 7.3](#)
- [기술 지원 및 문서 - Cisco Systems](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.