

FMC에서 HTTP Path Monitor를 사용하여 PBR 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[구성](#)

[네트워크 다이어그램](#)

[HTTP 경로 모니터링을 위한 PBR 구성](#)

[ECMP\(Equal-cost-multi-path\) 구성](#)

[보안 FTD를 위한 신뢰할 수 있는 DNS 구성](#)

[경로 모니터링 사용](#)

[모니터링 대시보드 추가](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[관련 정보](#)

소개

이 문서에서는 Cisco FMC(Secure Firewall Management Center)에서 PBR(Policy-Based Routing)과 HTTP 경로 모니터링을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- PBR 기본 지식
- 기본 Cisco Secure Management Center 환경
- 기본 Cisco FTD(Secure Firewall Threat Defense)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 7.4 릴리스를 실행하는 Cisco FMCv(Secure Firewall Management Center Virtual) VMware
- 7.4 릴리스를 실행하는 Cisco FTDv(Secure Firewall Threat Defense Virtual Appliance)

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

기존 라우팅에서는 패킷이 대상 IP 주소를 기반으로 라우팅되지만, 대상 기반 라우팅 시스템에서 트래픽을 지정하는 라우팅을 변경하는 것은 어렵습니다. PBR은 라우팅 프로토콜에서 제공하는 기존 메커니즘을 확장 및 보완하여 라우팅을 보다 효과적으로 제어할 수 있도록 합니다.

PBR에서는 IP 우선 순위를 설정할 수 있습니다. 또한 특정 트래픽에 대한 경로를 지정할 수 있습니다(예: 고비용 링크의 우선순위 트래픽). PBR의 경우 라우팅은 소스 포트, 대상 주소, 대상 포트, 프로토콜 애플리케이션 또는 이러한 객체의 조합과 같은 대상 네트워크 이외의 기준을 기반으로 합니다. PBR은 애플리케이션, 사용자 이름, 그룹 멤버십 및 보안 그룹 연결을 기반으로 네트워크 트래픽을 분류하는 데 사용할 수 있습니다. 이 라우팅 방법은 대규모 네트워크 구축에서 수많은 디바이스가 애플리케이션 및 데이터에 액세스하는 경우에 적용됩니다. 전통적으로 대규모 구축에는 라우팅 기반 VPN에서 모든 네트워크 트래픽을 암호화된 트래픽으로 허브에 백홀하는 토폴로지가 있습니다. 이러한 토폴로지는 종종 패킷 레이턴시, 대역폭 감소, 패킷 삭제 등의 문제를 초래합니다.

PBR은 라우팅된 방화벽 모드에서만 지원되며 원시 연결에는 적용되지 않습니다. HTTP 기반 애플리케이션은 물리적, 포트 채널, 하위 인터페이스 및 상태 터널 인터페이스에서 지원됩니다. 클러스터 디바이스에서는 지원되지 않습니다.

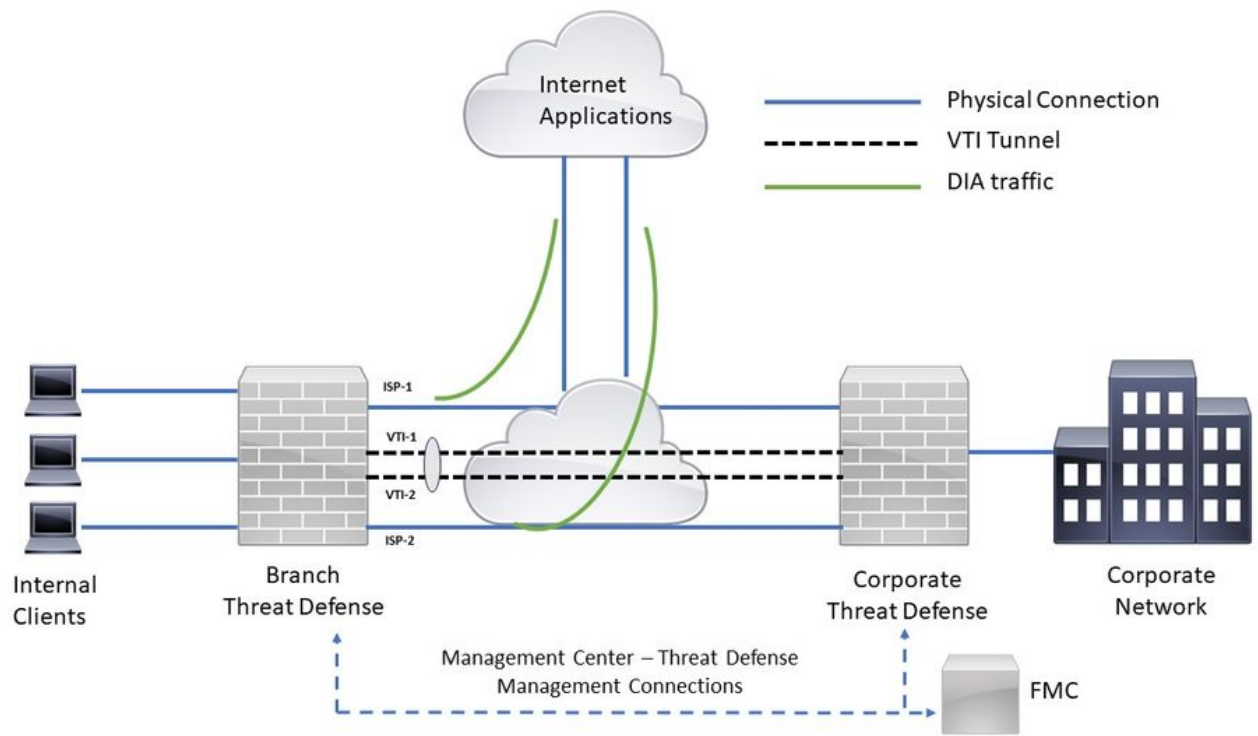
구성된 인터페이스에서 RTT(왕복 시간), 지터, MOS(평균 의견 점수) 및 인터페이스당 패킷 손실과 같은 메트릭을 파생시킬 경우 PBR 트래픽을 라우팅하기 위한 최적의 경로를 결정하는 데 사용됩니다. Path Monitoring(경로 모니터링)은 인터페이스당 여러 원격 피어에 대한 유연한 메트릭을 계산합니다. 브랜치 방화벽의 정책을 통해 여러 애플리케이션의 최적 경로를 모니터링하고 결정하기 위해 다음과 같은 이유로 ICMP보다 HTTP를 선호합니다.

- HTTP-ping은 애플리케이션이 호스팅되는 서버의 애플리케이션 레이어까지 경로의 성능 메트릭을 도출할 수 있습니다.
- 애플리케이션 서버 IP 주소가 변경될 때마다 방화벽 컨피그레이션을 변경해야 하는 이유는 IP 주소 대신 애플리케이션 도메인이 추적되기 때문입니다.

구성

네트워크 다이어그램

모든 브랜치 네트워크 트래픽이 기업 네트워크의 경로 기반 VPN을 통해 전송되고 필요할 때 엑스트라넷으로 분기되는 일반적인 기업 네트워크 시나리오를 가정해보겠습니다. 다음 토폴로지는 경로 기반 VPN을 통해 기업 네트워크에 연결된 브랜치 네트워크를 보여줍니다. 일반적으로 기업 위협 방어는 브랜치의 내부 및 외부 트래픽을 모두 처리하도록 구성됩니다. PBR 정책을 사용하면 가상 터널 대신 특정 트래픽을 WAN 네트워크로 라우팅하는 정책으로 브랜치 위협 방어가 구성됩니다. 나머지 트래픽은 평소처럼 경로 기반 VPN을 통해 흐릅니다.



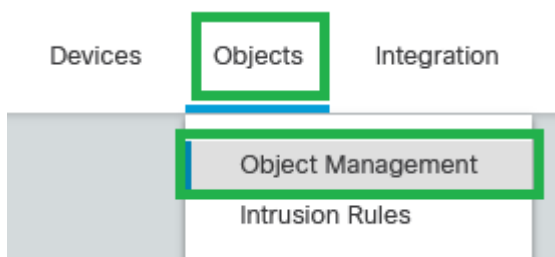
네트워크 토폴로지

컨피그레이션 섹션에서는 ISP 및 VTI 인터페이스가 Secure FMC의 브랜치 위협 방어에 대해 이미 구성되어 있다고 가정합니다.

HTTP 경로 모니터링을 위한 PBR 구성

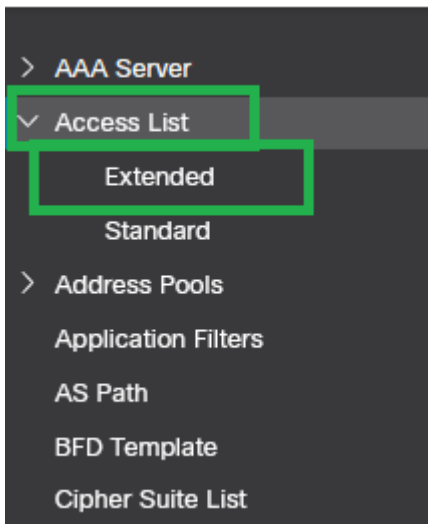
이 컨피그레이션 섹션에서는 ISP-1 및 ISP-2 인터페이스의 경로 모니터링 컨피그레이션을 보여줍니다.

1단계. 모니터링된 애플리케이션에 대한 확장 액세스 목록을 생성합니다. [로 이동합니다](#). Objects > Object Management



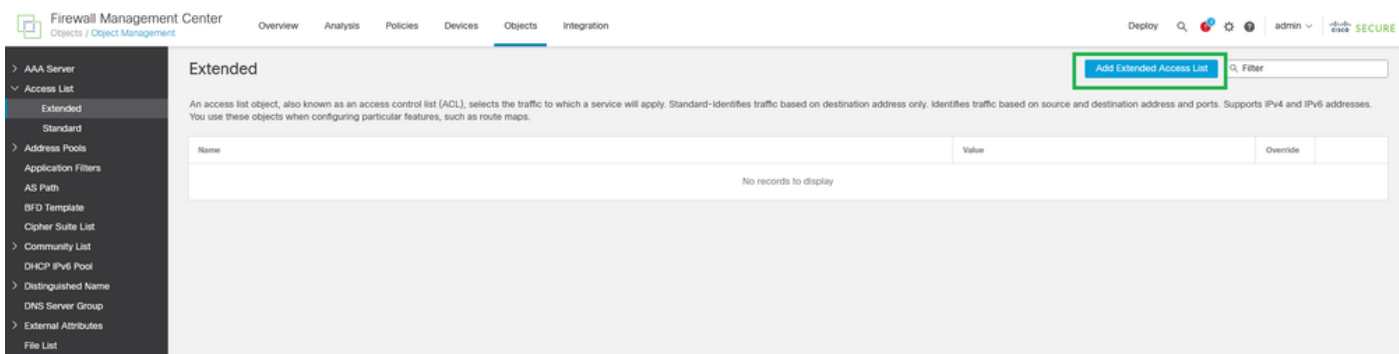
객체 - 객체 관리

2단계. 왼쪽 메뉴 [Access-list > Extended](#)로 이동합니다.



액세스 목록 - 확장

3단계. 을 클릭합니다Add Extended Access List.



확장 액세스 목록 추가

4단계. 확장 액세스 목록에 이름을 설정하고 을 클릭합니다Add.

New Extended Access List Object

Name

Applications

Entries (0)

Add

Sequence	Action	Source	Source Port	Destination	Destination Port	Application	Users	SGT
No records to display								

☐ Allow Overrides

Cancel Save

새 확장 액세스 목록 개체

5단계. 을 클릭하고 Application 원하는 애플리케이션(이 예에서는 일부 Cisco 애플리케이션이 선택됨)을 선택합니다. 그런 다음 을 클릭합니다Add.

Add Extended Access List Entry



Action:

Allow

Logging:

Default

Log Level:

Informational

Log Interval:

300 Sec.

Network Port Application Users Security Group Tag

Application Filters

Clear All Filters

Available Applications (4)

Search by name

Search cisco

Risks (Any Selected)

- ☐ Very Low 730
- ☐ Low 622
- ☐ Medium 734
- ☐ High 1556
- ☐ Very High 577

Business Relevance (Any Selected)

- ☐ Very Low 885

Cisco
Cisco Jabber
Cisco Secure Endpoint
Cisco Webex Assistant
Cisco Webex Assistant

Add to Rule

Selected Applications and Filters (6)

Applications
Cisco Jabber
Cisco Secure Endpoint
Cisco Webex Assistant
WebEx
WebEx Connect
Webex Teams

Cancel

Add

확장 액세스 목록 항목 추가



참고: 원하는 애플리케이션에 대한 특정 트래픽을 매칭하기 위해 Extended Access List(확장 액세스 목록)를 Source/Destination IPs(소스/대상 IP) 및 Ports(포트)로 구성할 수 있습니다. PBR 컨피그레이션에 적용하기 위해 여러 확장 액세스 제어 목록을 생성할 수 있습니다.

6단계. 확장 액세스 목록 컨피그레이션을 검증하고 을 클릭합니다Save.

New Extended Access List Object



Name

Applications

Entries (1)

Add

Sequence	Action	Source	Source Port	Destination	Destination Port	Application	Users	SGT	
1	Allow	Any	Any	Any	Any	Cisco Jabber Cisco Secure Endpoint Cisco Webex Assistant WebEx (2 more...)	Any		

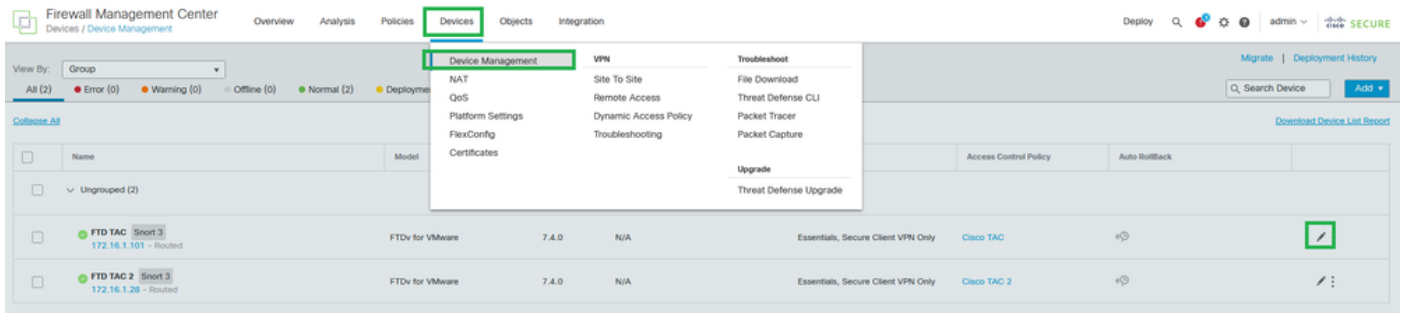
☐ Allow Overrides

Cancel

Save

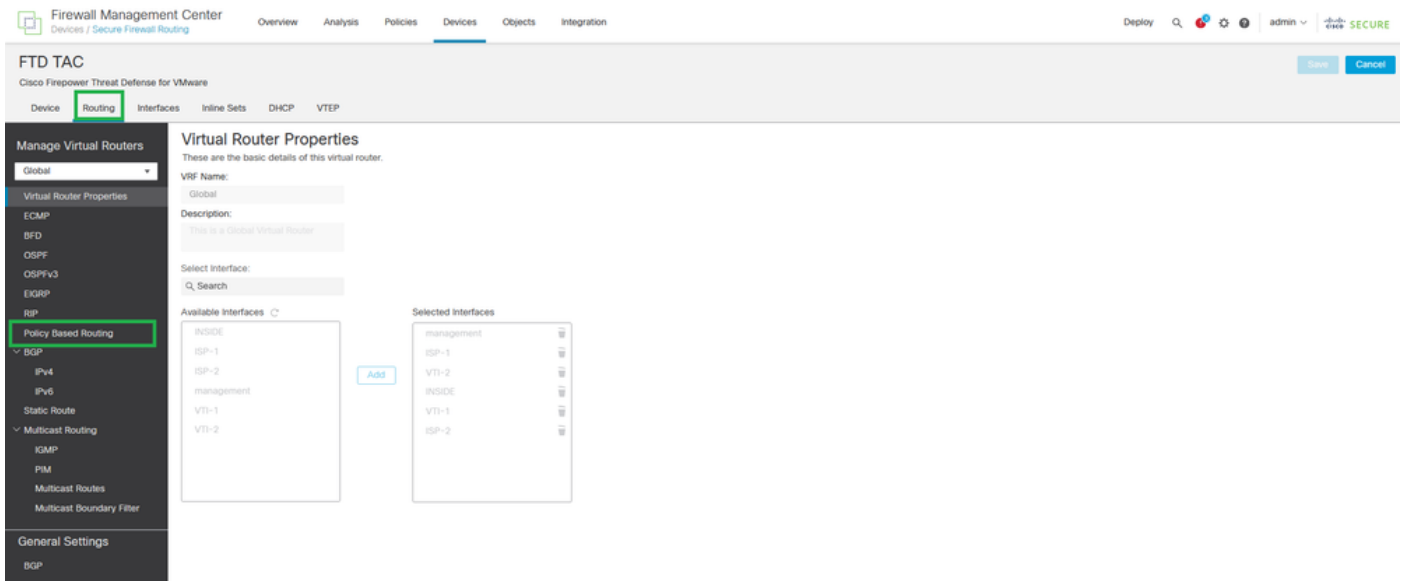
확장 액세스 목록 개체 저장

7단계. 위협 방어Devices > Device Management로 이동하여 수정합니다.



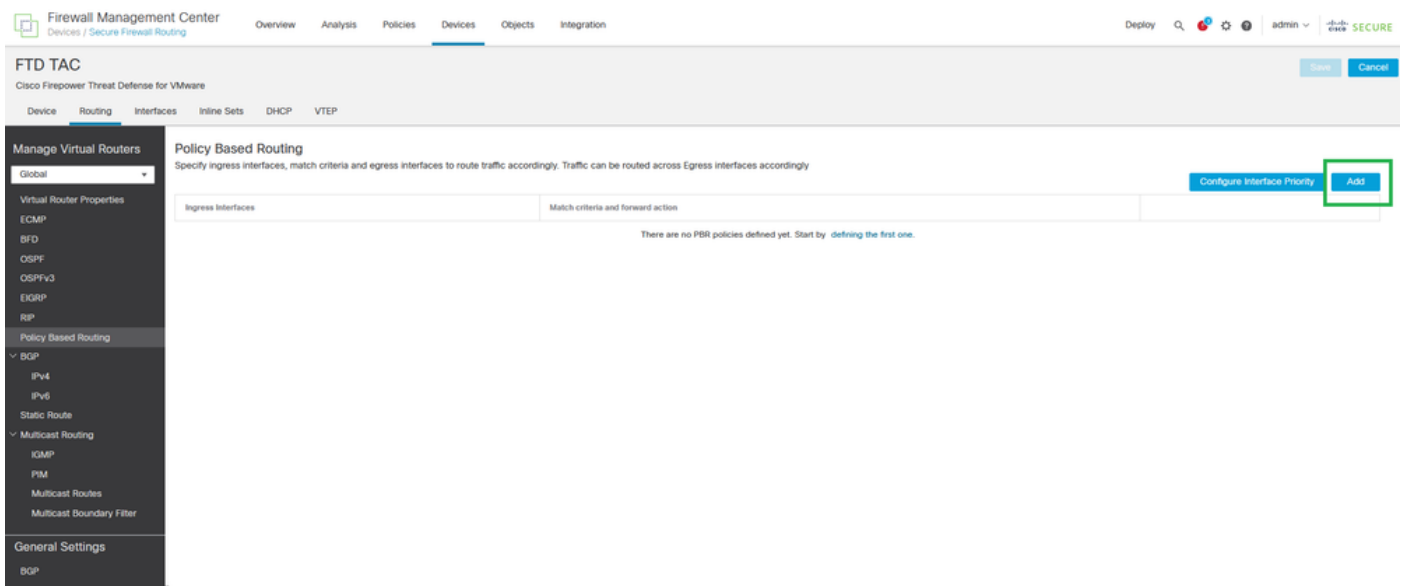
장치 - 장치 관리

8단계. 로 Routing > Policy-Based Routing이동합니다.



라우팅 - 정책 기반 라우팅

9단계. 을 클릭합니다Add.



정책 기반 라우팅 추가

10단계. PBR 컨피그레이션에 대한 인그레스 인터페이스(이 예에서는 INSIDE)를 추가한 다음 Add를 클릭합니다.

Add Policy Based Route

A policy based route consists of ingress interface list and a set of match criteria associated to egress interfaces

Ingress Interface*

Select...

INSIDE

ISP-1

ISP-2

Add

There are no forward-actions defined yet. Start by [defining the first one.](#)

Cancel

Save

정책 기반 경로 추가

11단계. 일치 기준(이전 단계에서 생성한 확장 액세스 목록과 함께), 이그레스 인터페이스 및 인터페이스 순서를 정의합니다.

Add Forwarding Actions



Match ACL:* Applications +

Send To:* Egress Interfaces

Interface Ordering:* Minimal Jitter ⓘ

Available Interfaces

Search by interface name 🔍

Interface	
INSIDE	+
ISP-1	+
ISP-2	+
VTI-1	+
VTI-2	+

Selected Egress Interfaces*

No interfaces selected

Cancel

Save

전달 작업 추가



참고: Egress Interfaces 및 Minimal Jitter 이 컨피그레이션 가이드로 선택되었습니다. 다른 옵션에 대해 자세히 알아보려면 [공식](#) PBR 문서를 확인하십시오.

12단계. 이그레스 인터페이스(이 예에서는 ISP-1 및 ISP-2)를 선택한 다음 을 클릭합니다 Save.

Add Forwarding Actions



Match ACL:* Applications

Send To:* Egress Interfaces

Interface Ordering:* Minimal Jitter

Available Interfaces

Search by interface name



Interface	
INSIDE	+
VTI-1	+
VTI-2	+

Selected Egress Interfaces*

Interface

ISP-1



ISP-2



Cancel

Save

선택한 이그레스 인터페이스

13단계. PBR 컨피그레이션을 검증하고 을 클릭합니다Save.

Add Policy Based Route



A policy based route consists of ingress interface list and a set of match criteria associated to egress interfaces

Ingress Interface*

INSIDE x



Match Criteria and Egress Interface

Specify forward action for chosen match criteria.

Add

Match ACL

Forwarding Action

Applications

Send through minimum jitter interface



ISP-1



ISP-2



Cancel

Save

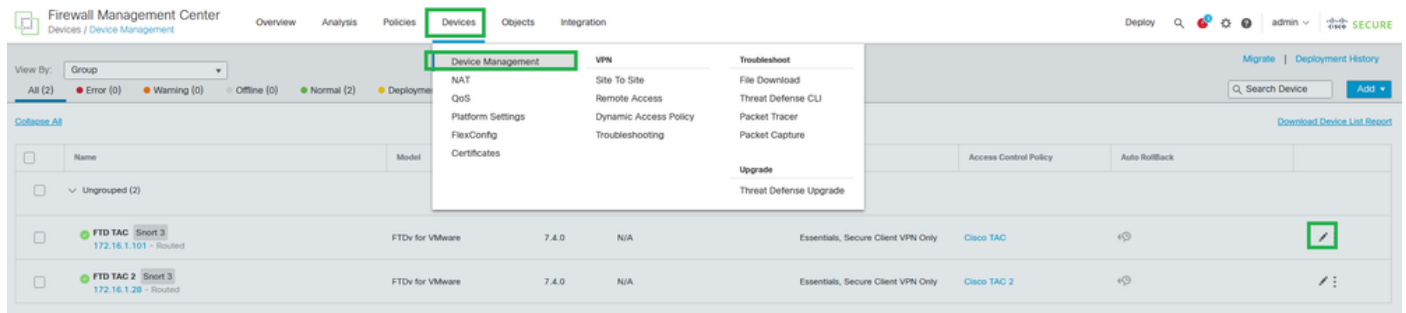
정책 기반 라우팅 검증

14단계. (선택 사항) 더 많은 Extended Access Control List가 생성되었거나 PBR 컨피그레이션을 적용해야 하는 소스 인터페이스가 더 많은 경우 9, 10, 11, 12, 13단계를 반복합니다.

15단계. FMC에서 변경 사항을 저장하고 구축합니다.

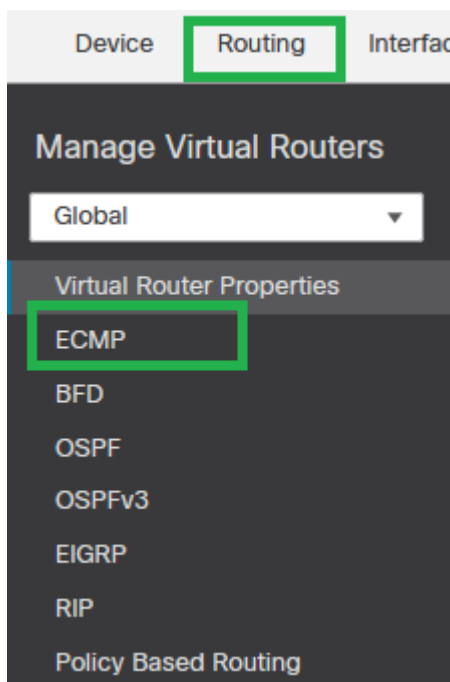
ECMP(Equal-cost-multi-path) 구성

1단계. 위협 방어로 Devices > Device Management 이동하여 수정합니다.



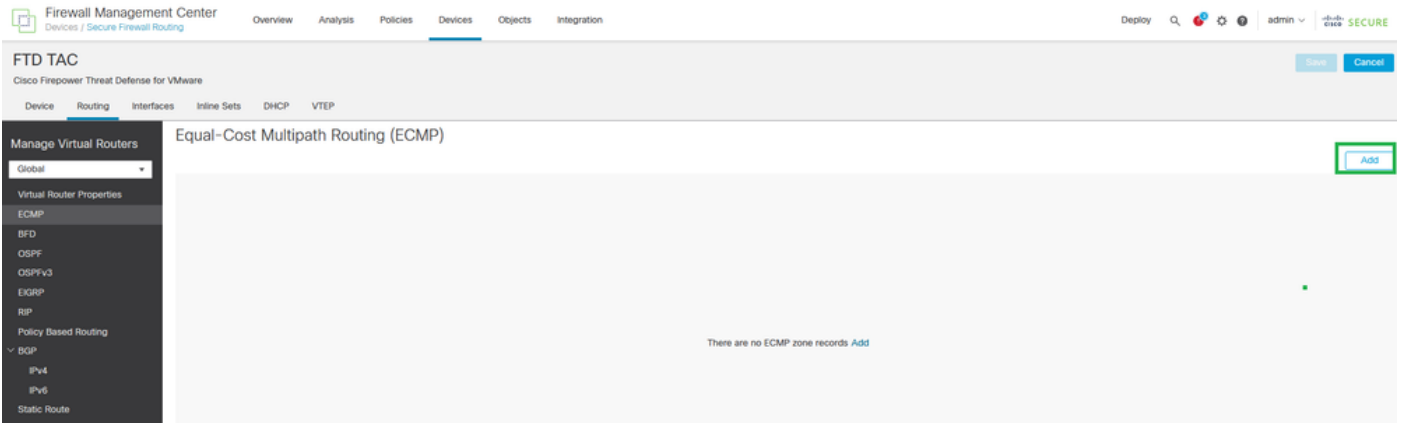
장치 - 장치 관리

2단계. 로 Routing > ECMP 이동합니다.



라우팅 - ECMP

3단계. VTI와 WAN 인터페이스(이 컨피그레이션 가이드의 경우 ISP-1 및 ISP-2) 간에 ECMP를 생성하려면 클릭합니다 Add.



ECMP(Equal-Cost Multipath Routing)

4단계. ECMP 이름을 설정하고 모든 VTI 인터페이스를 선택한 다음 을 클릭합니다Add.

Add ECMP
? ×

Name

VTI-ECMP

Available Interfaces

INSIDE
ISP-1
ISP-2

Selected Interfaces

VTI-1
VTI-2

Add

Cancel

OK

VTI용 ECMP

5단계. 3단계와 4단계를 반복하여 WAN 인터페이스 간에 ECMP를 생성합니다(이 컨피그레이션 가이드의 경우 ISP-1과 ISP-2).

Add ECMP? ×

Name

ISP-ECMP

Available Interfaces

INSIDE

VTI-1

VTI-2

Add

Selected Interfaces

ISP-2

ISP-1

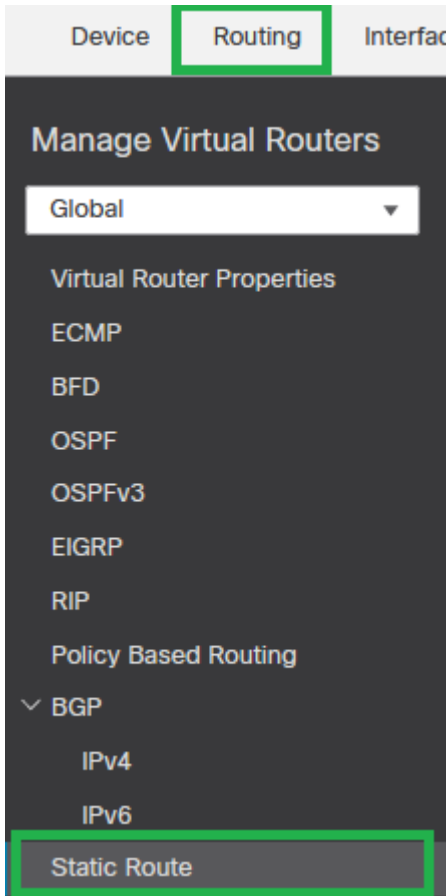
Cancel

OK

ISP 인터페이스용 ECMP

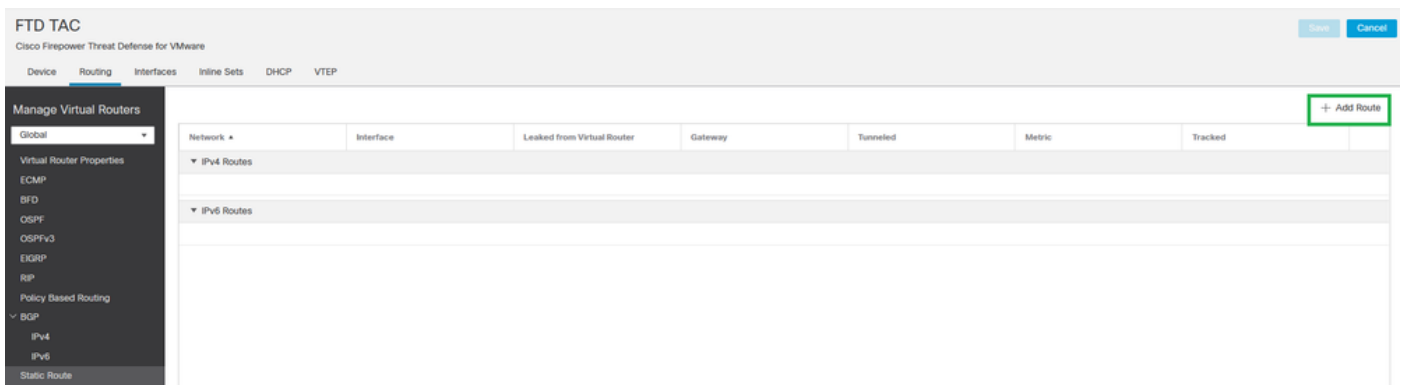
6단계. ECMP 구성을 저장합니다.

7단계. 로드 밸런싱을 위해 영역 인터페이스에 대한 고정 경로를 구성합니다. 로 이동합니다 [Routing > Static Route](#).



라우팅 - 고정 경로

8단계. 을 클릭합니다+ Add Route.



+ 경로 추가

9단계. 메트릭 값으로 1을 사용하여 VTI 인터페이스(이 컨피그레이션 가이드의 경우 VTI-1)에 대한 기본 고정 경로를 생성한 다음 을 클릭합니다OK.

Add Static Route Configuration



Type:



IPv4



IPv6

Interface*

VTI-1



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

Available Network 



any



Add

any-ipv4

IPv6-to-IPv4-Relay-Anycast

Selected Network

any-ipv4



Gateway*

VTI-Tunnel1-FPR2



Metric:

1

(1 - 254)

Tunneled: ☐ (Used only for default Route)

Route Tracking:



Cancel

OK

VTI-1의 기본 고정 경로

10단계. 8단계를 반복합니다. 구성된 VTI 인터페이스가 더 많은 경우.



참고: 구성된 각 VTI 인터페이스에 대한 기본 경로를 생성합니다.

11단계. VTI보다 큰 메트릭 값을 사용하여 WAN/ISP 인터페이스(이 컨피그레이션 가이드의 경우 ISP-1)에 대한 기본 고정 경로를 생성한 다음 을 클릭합니다OK.

Add Static Route Configuration



Type: ☒ IPv4 ☐ IPv6

Interface*

ISP-1

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

Available Network



any-



Add

any-ipv4

Selected Network

any-ipv4



Gateway*

172.16.1.254GW-24



Metric:

10

(1 - 254)

Tunneled: ☐ (Used only for default Route)

Route Tracking:



Cancel

OK

ISP-1의 기본 고정 경로

12단계. 10단계를 반복합니다. 구성된 WAN/ISP 인터페이스가 더 많은 경우.



참고: 구성된 각 WAN/ISP 인터페이스에 대한 기본 경로를 생성합니다.

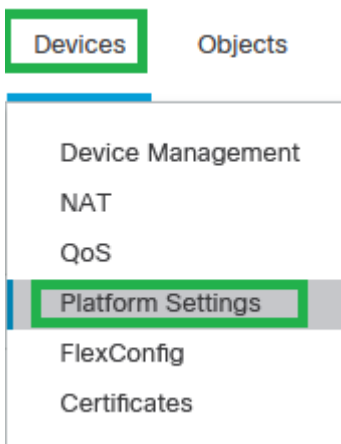
13단계. 기본 경로 컨피그레이션을 검증하고 **OK**를 클릭합니다.

FTD TAC							
Cisco Firepower Threat Defense for VMware							
Device Routing Interfaces Inline Sets DHCP VTEP							
Manage Virtual Routers Global Virtual Router Properties ECMP BFD OSPF OSPFv3 EIGRP RIP Policy Based Routing BGP							
Network Interface Leaked from Virtual Router Gateway Tunneled Metric Tracked							
▼ IPv4 Routes any-ipv4 ISP-2 Global 172.16.11.254-GW-24 false 10							
any-ipv4 ISP-1 Global 172.16.1.254GW-24 false 10							
any-ipv4 VTI-2 Global VTI-Tunnel2-FPR2 false 1							
any-ipv4 VTI-1 Global VTI-Tunnel1-FPR2 false 1							
▼ IPv6 Routes							

고정 경로 컨피그레이션

보안 FTD를 위한 신뢰할 수 있는 DNS 구성

1단계. 로Devices > Platform Settings이동합니다.



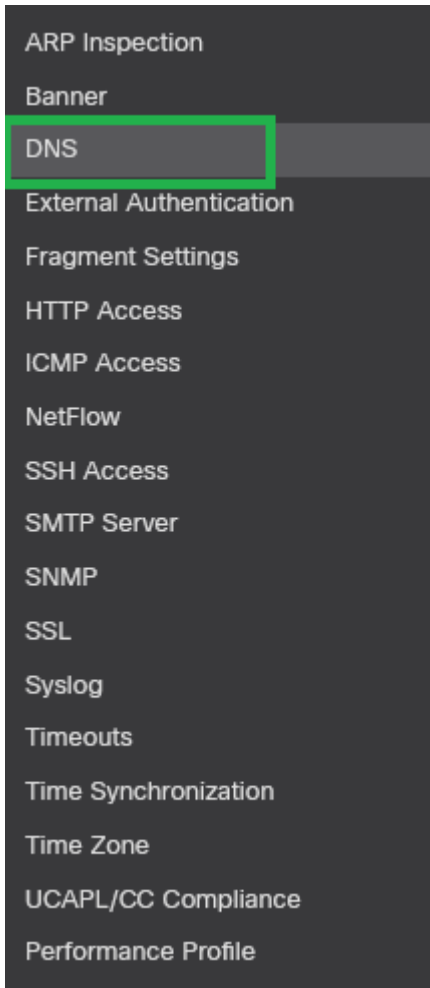
디바이스 - 플랫폼 설정

2단계. 기존 플랫폼 설정 정책을 만들거나 수정합니다.



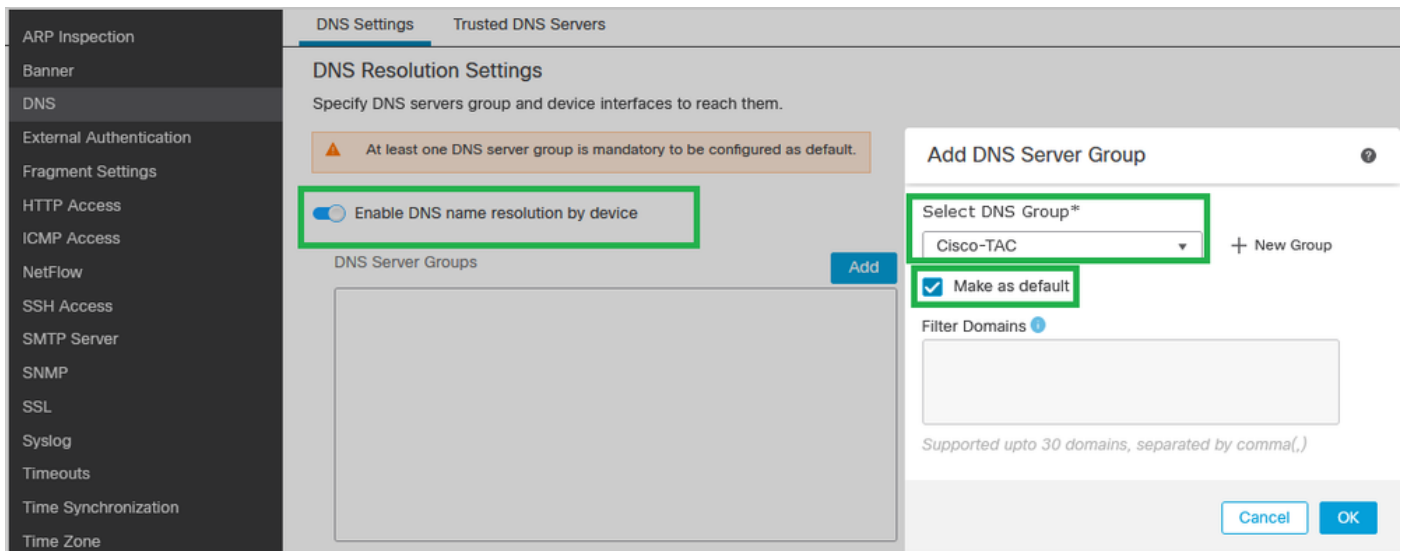
참고: 플랫폼 설정 정책이 Secure Threat Defense 디바이스에 적용되었는지 확인합니다.

3단계. 을 클릭합니다DNS.



DNS 플랫폼 설정

4단계. 활성화한 DNS name resolution by device 다음 클릭하거나 기존 DNS 그룹을 선택합니다 Add. 을 Make as default 선택하고 을 클릭합니다 OK.



DNS 서버 그룹 추가



참고: 플랫폼 설정 정책에서 DNS 컨피그레이션에 대해 자세히 알아보려면 [공식 플랫폼 설](#)

[정 설명서를](#) 확인하십시오.

5단계. 섹션 아래에서 WAN/ISP 인터페이스를 Interface Objects 선택합니다.

ARP Inspection

Banner

DNS

External Authentication

Fragment Settings

HTTP Access

ICMP Access

NetFlow

SSH Access

SMTP Server

SNMP

SSL

Syslog

Timeouts

Time Synchronization

Time Zone

UCAPL/CC Compliance

Performance Profile

Expiry Entry Timer:

1

Range: 1-65535 minutes

Poll Timer:

240

Range: 1-65535 minutes

Interface Objects

Devices will use specified interface objects for connecting with DNS Servers.

Available Interface Objects

Q Search

INSIDE

ISP-1

ISP-2

VTI-1

VTI-11

VTI-2

Add

Selected Interface Objects

ISP-1

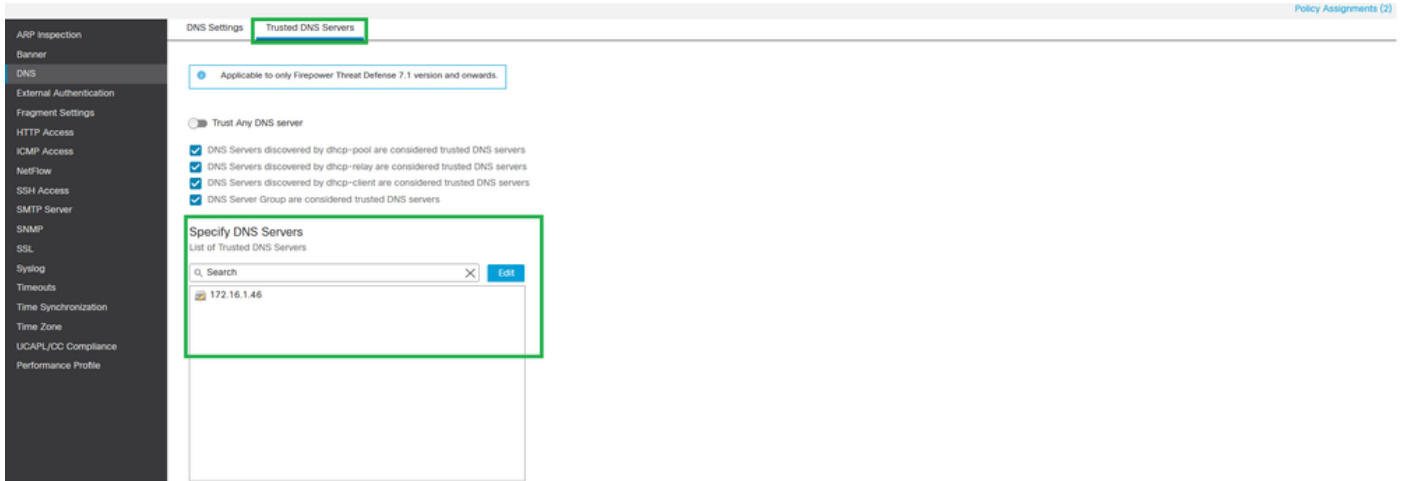
ISP-2

☐ Enable DNS Lookup via diagnostic/Management interface also.

DNS 인터페이스 컨피그레이션

6단계. 변경 사항을 저장합니다.

7단계. 로 이동하여 Trusted DNS Servers 신뢰할 수 있는 DNS 서버를 지정합니다.

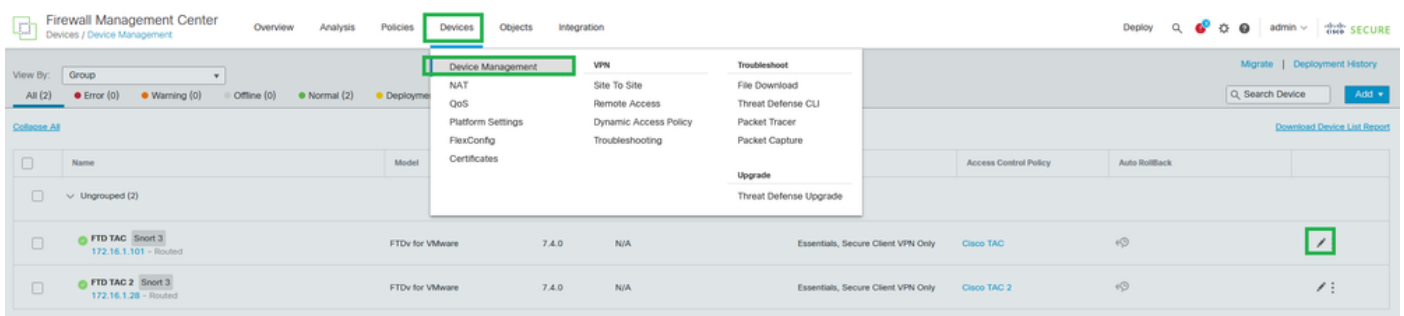


신뢰할 수 있는 DNS 서버

8단계. 을 누르고 변경 사항을 구축합니다Save.

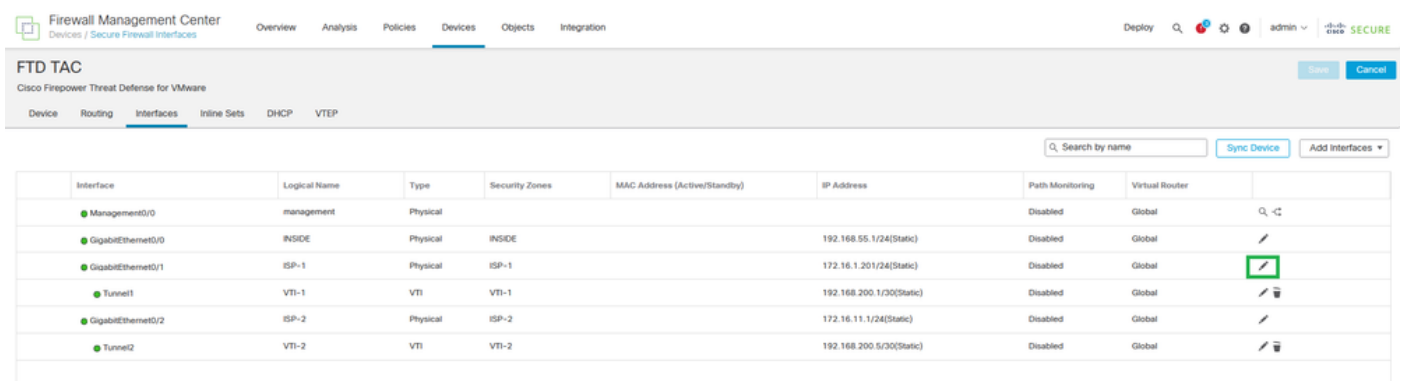
경로 모니터링 사용

1단계. 위협 방어로Devices > Device Management이동하여 수정합니다.



장치 - 장치 관리

2단계.Interfaces 탭 아래에서 인터페이스 WAN/ISP 인터페이스(이 컨피그레이션 가이드의 경우 ISP-1 및 ISP-2)를 편집합니다.



인터페이스 컨피그레이션

3단계. 탭을 Path Monitoring 클릭하고 확인란을 Enable IP Monitoring선택한 후 확인란을HTTP-based Application Monitoring활성화합니다. 그런 다음 을 클릭합니다Save.

Edit Physical Interface



General

IPv4

IPv6

Path Monitoring

Hardware Configuration

Manager Access

Advanced

☒ Enable IP based Monitoring

Select to monitor jitter, round trip time, packet-lost & mean opinion score of each interface.

Monitoring Type:

Next-hop of default route out of interface (Auto) ▼

System monitors the next hop of the interface. Tries IPv4 and then IPv6.
If the peer is unavailable, monitoring is not done.

☒ Enable HTTP based Application Monitoring

By enabling application monitoring you are allowing all the applications configured in Extended ACLs used in policy based routing with this interface as egress interface to be monitored automatically.

Applications

Cisco Jabber

Cisco Secure Endpoint

Cisco Webex Assistant

WebEx

WebEx Connect

Cancel

OK

인터페이스 경로 모니터링 컨피그레이션



주의: 이전 컨피그레이션 섹션에서 구성한 애플리케이션을 나열해야 합니다.



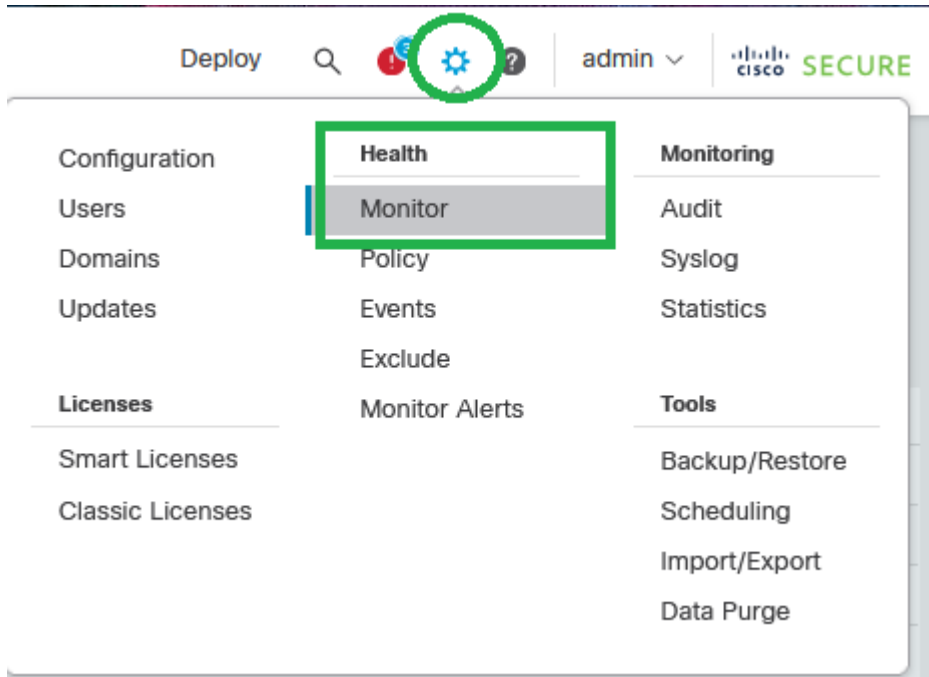
참고: 이 컨피그레이션 가이드에 대해 '모니터링 유형'이 선택되었습니다. 다른 옵션에 대해 자세히 알아보려면 [공식 컨피그레이션 가이드](#)에서 Path Monitoring Settings(경로 모니터링 설정)를 확인하십시오.

4단계. 구성된 모든 WAN/ISP 인터페이스에 대해 2단계와 3단계를 반복합니다.

5단계. 을 누르고 변경 사항을 구축합니다Save.

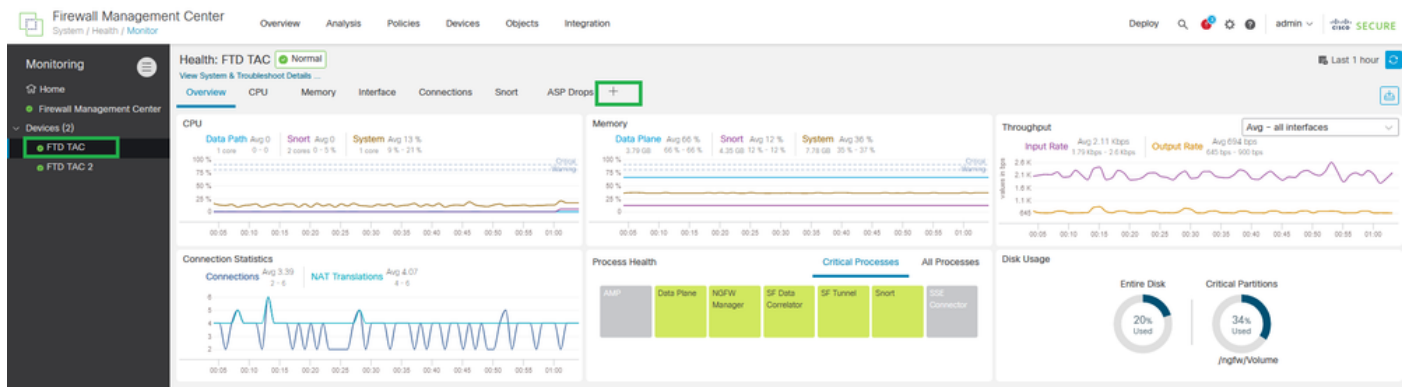
모니터링 대시보드 추가

1단계. 로System > Health > Monitor이동합니다.



시스템 - 상태 - 모니터

2단계. Secure FTD(보안 FTD) 디바이스를 선택하고 을 클릭합니다Add New Dashboard.



새 대시보드 추가

3단계. Dashboard Name(대시보드 이름)을 설정하고Correlate Metrics대화 상자의 드롭다운 목록에서 Interface - Path Metrics선택합니다. 그런 다음 을 클릭합니다Add Dashboard.

Add New Dashboard



Name*

FTD HTTP Path Monitoring

Metrics*

Metrics can be chosen from pre-defined correlation groups or/and metrics of your choice. Related metrics are grouped together, select a group and then the metrics.

Interface

Jitter x

x

v



Interface

Mean Opinion Score (MOS) x

x

v



Interface

Round Trip Time x

x

v



Interface

Packet Loss x

x

v



Add Metrics

Add from Predefined Correlations v

Clear All

Cancel

Add Dashboard

경로 메트릭이 있는 새 대시보드 추가

다음을 확인합니다.

이 섹션에서는 부동 고정 경로, ECMP, 애플리케이션이 있는 객체 그룹 및 PBR 컨피그레이션을 확인하는 방법에 대해 설명합니다.

기본 경로 및 부동 고정 경로 컨피그레이션을 확인합니다.

```
firepower# show run route
route VTI-1 0.0.0.0 0.0.0.0 192.168.200.1 1
route VTI-2 0.0.0.0 0.0.0.0 192.168.200.5 1
route ISP-1 0.0.0.0 0.0.0.0 172.16.1.254 10
route ISP-2 0.0.0.0 0.0.0.0 172.16.11.254 10
```

ECMP 컨피그레이션을 확인합니다.

```
firepower# sh run | i ecmp
zone ECMP-VTI ecmp
zone ECMP-ISP ecmp
```

라우팅 테이블에서 트래픽이 ECMP에 의해 밸런싱되는지 확인합니다. 라우팅 테이블은 Secure FTD 라우팅 테이블에 두 경로를 모두 설치해야 합니다.

```
firepower# show route static
```

```
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 172.16.11.254 to network 0.0.0.0
```

```
S* 0.0.0.0 0.0.0.0 [1/0] via 192.168.200.5, VTI-2
[1/0] via 192.168.200.1, VTI-1
```

PBR route-map 컨피그레이션을 확인합니다.

```
firepower# show run route-map
!
route-map FMC_GENERATED_PBR_1694885402369 permit 5
match ip address Applications
set adaptive-interface cost ISP-1 ISP-2
!
```

PBR 컨피그레이션에 할당된 ACL을 확인합니다(경로 맵 컨피그레이션의 ACL 이름 확인).

```
firepower# show run access-list | i Applications
access-list Applications extended permit ip any object-group-network-service FMC_NSNG_639950173988
```

액세스 목록에 할당된 애플리케이션이 있는 객체 그룹을 확인합니다(ACL 컨피그레이션에서 객체 그룹 이름 확인).

```
firepower# show run object-group
object-group network-service FMC_NSNG_639950173988
network-service-member "Cisco Jabber"
network-service-member "Cisco Secure Endpoint"
network-service-member "Cisco Webex Assistant"
network-service-member "WebEx"
network-service-member "WebEx Connect"
network-service-member "Webex Teams"
```

PBR 컨피그레이션에 사용된 데이터 인터페이스에 할당된 정책 경로를 확인합니다.

```

interface GigabitEthernet0/0
nameif INSIDE
cts manual
propagate sgt preserve-untag
policy static sgt disabled trusted
security-level 0
ip address 172.16.35.1 255.255.255.0
policy-route route-map FMC_GENERATED_PBR_1694885402369
!
interface GigabitEthernet0/1
nameif ISP-1
cts manual
propagate sgt preserve-untag
policy static sgt disabled trusted
security-level 0
zone-member ECMP-ISP
ip address 172.16.1.202 255.255.255.0
policy-route path-monitoring auto
!
interface GigabitEthernet0/2
nameif ISP-2
security-level 0
zone-member ECMP-ISP
ip address 172.16.11.2 255.255.255.0
policy-route path-monitoring auto
!

```

HTTP Path Monitoring Dashboard(HTTP 경로 모니터링 대시보드) 정보에서 Jitter(지터), MOS(MOS), Round Trip Time(왕복 시간) 및 Packet Loss(패킷 손실) 통계를 확인하고 확인합니다.



HTTP 경로 모니터링 대시보드 확인

문제 해결

경로 모니터링 실패 시 IP 기반 모니터링이 활성화된 상태에서 WAN/ISP 인터페이스는 ICMP 프로브 패킷을 정적 경로에 구성된 게이트웨이로 전송하도록 구성됩니다. ICMP가 작동하는지 확인하기 위해 WAN/ISP 인터페이스에서 인그레스/이그레스 캡처를 구성합니다.

인그레스 및 이그레스 캡처:

```
firepower# cap in interface ISP-1 trace match icmp any any
firepower# cap in2 interface isP-2 trace match icmp any any
```

인그레스 캡처:

```
firepower# show cap in
```

12 packets captured

```
1: 00:08:28.073604 172.16.1.202 > 172.16.1.254 icmp: echo request
2: 00:08:28.074672 172.16.1.254 > 172.16.1.202 icmp: echo reply
3: 00:08:29.150871 172.16.1.202 > 172.16.1.254 icmp: echo request
4: 00:08:29.151832 172.16.1.254 > 172.16.1.202 icmp: echo reply
5: 00:08:30.217701 172.16.1.202 > 172.16.1.254 icmp: echo request
6: 00:08:30.218876 172.16.1.254 > 172.16.1.202 icmp: echo reply
7: 00:08:31.247728 172.16.1.202 > 172.16.1.254 icmp: echo request
8: 00:08:31.248980 172.16.1.254 > 172.16.1.202 icmp: echo reply
9: 00:08:32.309005 172.16.1.202 > 172.16.1.254 icmp: echo request
10: 00:08:32.310317 172.16.1.254 > 172.16.1.202 icmp: echo reply
11: 00:08:33.386622 172.16.1.202 > 172.16.1.254 icmp: echo request
12: 00:08:33.387751 172.16.1.254 > 172.16.1.202 icmp: echo reply
```

12 packets shown

```
1: 00:08:28.073604 172.16.1.202 > 172.16.1.254 icmp: echo request
2: 00:08:28.074672 172.16.1.254 > 172.16.1.202 icmp: echo reply
3: 00:08:29.150871 172.16.1.202 > 172.16.1.254 icmp: echo request
4: 00:08:29.151832 172.16.1.254 > 172.16.1.202 icmp: echo reply
5: 00:08:30.217701 172.16.1.202 > 172.16.1.254 icmp: echo request
6: 00:08:30.218876 172.16.1.254 > 172.16.1.202 icmp: echo reply
7: 00:08:31.247728 172.16.1.202 > 172.16.1.254 icmp: echo request
8: 00:08:31.248980 172.16.1.254 > 172.16.1.202 icmp: echo reply
9: 00:08:32.309005 172.16.1.202 > 172.16.1.254 icmp: echo request
10: 00:08:32.310317 172.16.1.254 > 172.16.1.202 icmp: echo reply
11: 00:08:33.386622 172.16.1.202 > 172.16.1.254 icmp: echo request
12: 00:08:33.387751 172.16.1.254 > 172.16.1.202 icmp: echo reply
```

12 packets shown

이그레스 캡처:

```
firepower# show cap in2
```

12 packets captured

```
1: 00:08:28.073543 172.16.11.2 > 172.16.11.254 icmp: echo request
2: 00:08:28.074764 172.16.11.254 > 172.16.11.2 icmp: echo reply
3: 00:08:29.150810 172.16.11.2 > 172.16.11.254 icmp: echo request
4: 00:08:29.151954 172.16.11.254 > 172.16.11.2 icmp: echo reply
5: 00:08:30.217640 172.16.11.2 > 172.16.11.254 icmp: echo request
6: 00:08:30.218799 172.16.11.254 > 172.16.11.2 icmp: echo reply
7: 00:08:31.247667 172.16.11.2 > 172.16.11.254 icmp: echo request
8: 00:08:31.248888 172.16.11.254 > 172.16.11.2 icmp: echo reply
```

```
9: 00:08:32.308913 172.16.11.2 > 172.16.11.254 icmp: echo request
10: 00:08:32.310012 172.16.11.254 > 172.16.11.2 icmp: echo reply
11: 00:08:33.386576 172.16.11.2 > 172.16.11.254 icmp: echo request
12: 00:08:33.387888 172.16.11.254 > 172.16.11.2 icmp: echo reply
12 packets captured
```



주의: Source 및 Destination IP 주소로 캡처를 구성하십시오. 캡처를 사용하면 시스템 성능을 상당히 향상시킬 수 있기 때문입니다.



팁: ping이 작동하지 않을 경우 기본 게이트웨이와의 직접 연결 문제를 해결하거나 ARP 테이블을 확인하거나 Cisco TAC에 문의하십시오.

PBR이 작동하는지 확인하기 위해 패킷 추적기 도구를 사용하여 애플리케이션 트래픽이 PBR로 라우팅되는지 확인할 수 있습니다.

```
firepower# packet-tracer input inside tcp 172.16.35.2 54352 'PUBLIC-IP-ADDRESS-FOR-WEBEX' $
---
[Output omitted]
---
Phase: 3
Type: PBR-LOOKUP
Subtype: policy-route
Result: ALLOW
Config:
route-map FMC_GENERATED_PBR_1694885402369 permit 5
match ip address Applications
set ip next-hop 172.16.1.254
Additional Information:
Matched route-map FMC_GENERATED_PBR_1694885402369, sequence 5, permit
Found next-hop 172.16.1.254 using egress ifc ISP-1
---
[Output omitted]
---
Result:
input-interface: INSIDE
input-status: up
input-line-status: up
output-interface: ISP-1
output-status: up
output-line-status: up
Action: allow
```



참고: 객체 그룹에 구성된 네트워크 서비스의 애플리케이션 IP 주소에 대해 자세히 알아보려면 명령을 사용합니다 `show object-group network-service detail`.

관련 정보

HTTP 경로 모니터링이 포함된 PBR과 관련된 추가 문서는 여기에서 찾을 수 있습니다.

- [Secure Firewall Management Center Device Configuration Guide의 Policy-Based Routing Configuration](#)
- [Secure Firewall Management Center Device Configuration Guide의 Path Monitoring on Policy-Based Routing Configuration](#)
- [정책 기반 라우팅 정책 구성](#)
- [정책 기반 라우팅의 컨피그레이션 예](#)
- [PBR 경로 모니터링의 예 구성](#)
- [경로 모니터링 대시보드 추가](#)
- [SSM\(Secure Firewall Management Center\) 디바이스 컨피그레이션 가이드에서 DNS 플랫폼 설정 컨피그레이션](#)
- [Cisco 기술 지원 및 다운로드](#)

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.