FMC에서 관리하는 FTD 디바이스의 EIGRP 문제 해결

목차

소개

이 문서에서는 FMC에서 관리하는 FTD에서 EIGRP 컨피그레이션을 확인하고 문제를 해결하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- EIGRP(Enhanced Interior Gateway Routing Protocol)
- Cisco FMC(Secure Firewall Management Center)
- Cisco FTD(Secure Firewall Threat Defense)

사용되는 구성 요소

- 버전 7.4.2의 FTDv
- 버전 7.4.2의 FMCv

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.

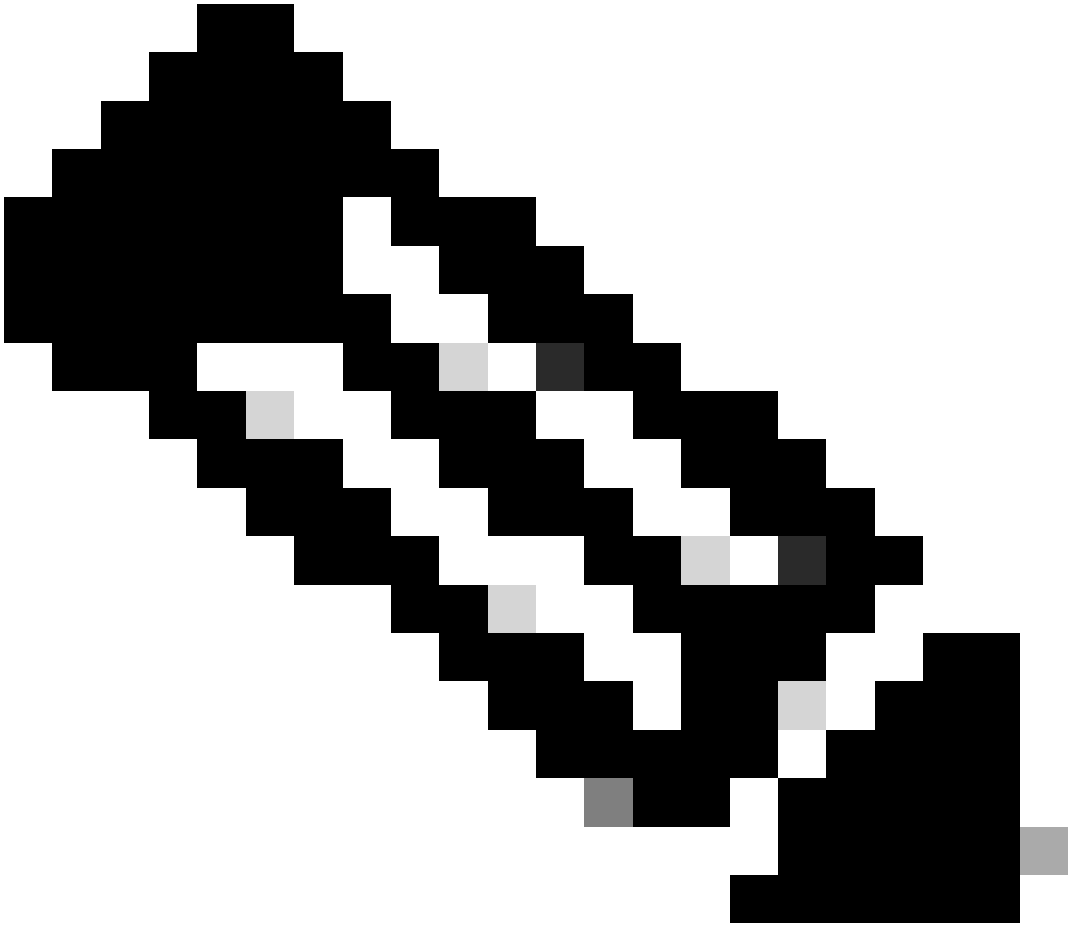
배경 정보

EIGRP는 거리 벡터 및 링크 상태 프로토콜의 기능을 결합하는 고급 거리 벡터 라우팅 프로토콜입니다. 네이버에서 라우팅 정보를 유지 관리하여 빠른 컨버전스를 제공하여 대체 경로에 빠르게 적응할 수 있습니다. EIGRP는 정기적인 전체 업데이트 대신 경로 또는 메트릭 변경에 대해 부분 트리거된 업데이트를 사용하여 효율적입니다.
통신을 위해 EIGRP는 IP 레이어(Protocol 88)에서 직접 작동하며 보장되고 순서가 지정된 패킷 전달을 위해 RTP(Reliable Transport Protocol)를 사용합니다. 특히 멀티캐스트 주소 224.0.0.10 또는 FF02::A를 사용하는 hello 메시지와 함께 멀티캐스트와 유니캐스트를 모두 지원합니다.
EIGRP 작업은 기본적으로 세 가지 테이블에 저장된 정보를 기반으로 합니다.

- 네이버 테이블: 이 테이블에서는 인접성이 성공적으로 설정된 직접 연결된 EIGRP 디바이스의 레코드를 유지 관리합니다.
- 토폴로지 테이블: 이 테이블은 네이버가 광고하는 모든 학습된 경로를 저장하며, 여기에는 특정 목적지에 대한 모든 가능한 경로와 관련 메트릭이 포함되며, 이를 통해 품질 및 사용 가능한 경로 수를 평가할 수 있습니다.
- 라우팅 테이블: 이 표에는 'Successor'라고 하는 각 대상에 대한 최상의 경로가 포함되어 있습니다. 이 Successor 경로는 트래픽 전달에 활발하게 사용되는 경로이며 이후에 다른 EIGRP 네이버에 광고됩니다.

EIGRP는 라우팅 및 메트릭 계산에서 K 값이라고 하는 메트릭 가중치를 사용하여 대상에 대한 최적의 경로를 결정합니다. 이 측정 단위 값은 매개변수를 사용하는 공식에서 파생됩니다.

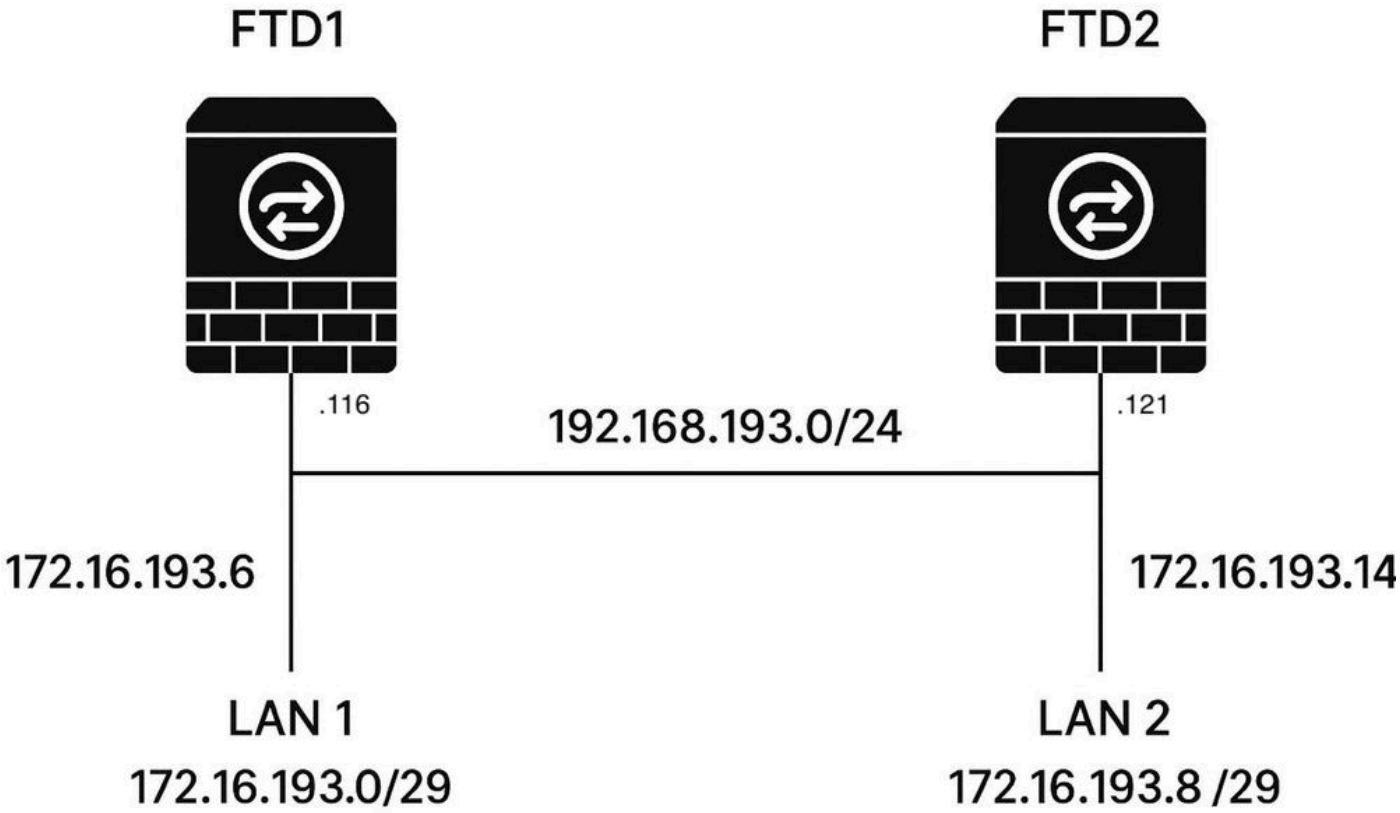
- Bandwidth
- 지연 시간
- Reliability
- 로드 중
- MTU



참고: 여러 경로 간의 메트릭 연결이 있는 경우 MTU(Maximum Transmission Unit)가 타이 브레이커로 사용되며, 더 높은 MTU 값이 선호됩니다.

- 후속 경로: 이는 특정 대상에 대한 최상의 경로로 정의됩니다. 라우팅 테이블에 궁극적으로 설치되는 경로입니다.
- 실행 가능 거리(FD): 이는 로컬 라우터 관점에서 특정 서브넷에 도달하기 위해 가장 잘 계산된 메트릭을 나타냅니다.
- 보고된 거리(RD)/알려진 거리(AD): 네이버에서 보고한 특정 서브넷까지의 거리(메트릭)입니다. 경로가 실행 가능한 successor로 간주되려면 인접 디바이스의 보고된 거리가 동일한 대상에 대한 로컬 라우터의 실행 가능한 거리보다 작아야 합니다.
- 가능한 Successor(FS): 이는 기본 Successor 경로가 실패할 경우 대체 경로를 제공하는 대상에 대한 백업 경로입니다. 경로의 보고된 거리(광고 인접 라우터로부터의)가 동일한 목적지까지의 현재 Successor 경로의 실현가능한 거리보다 엄격하게 작으면 경로가 실현가능한 Successor가 됩니다.

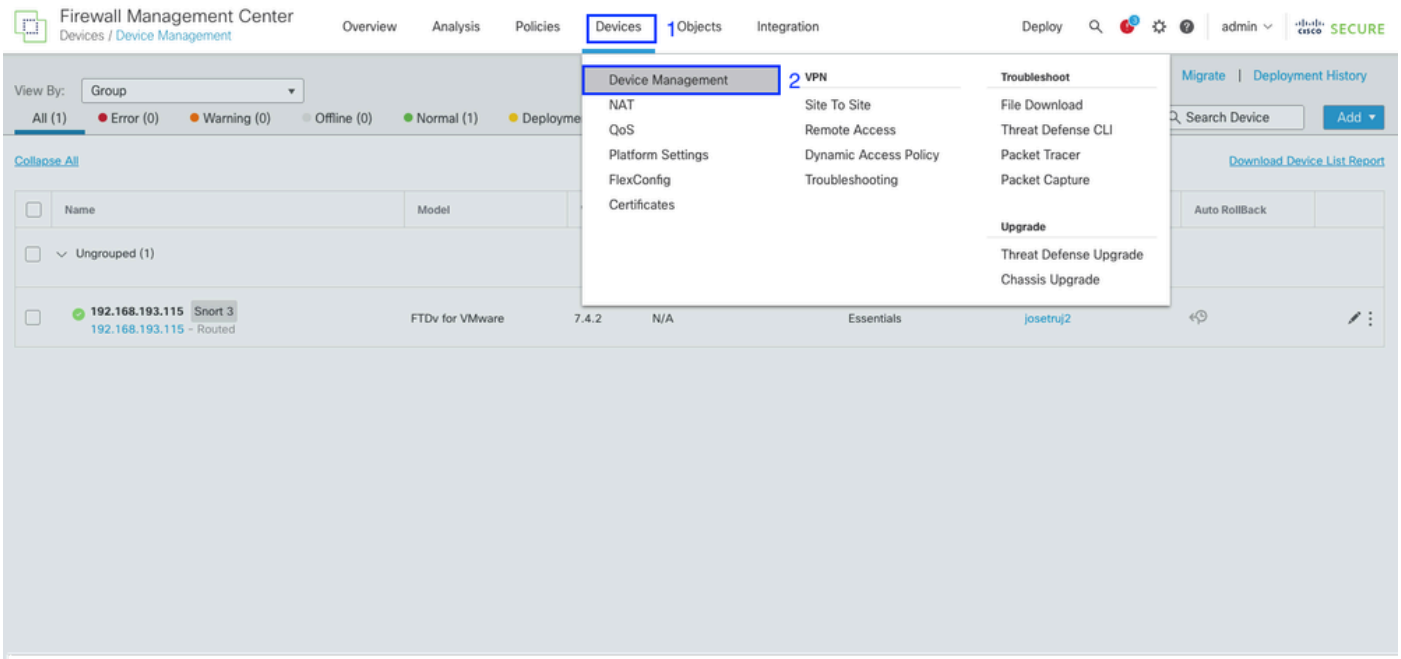
네트워크 다이어그램



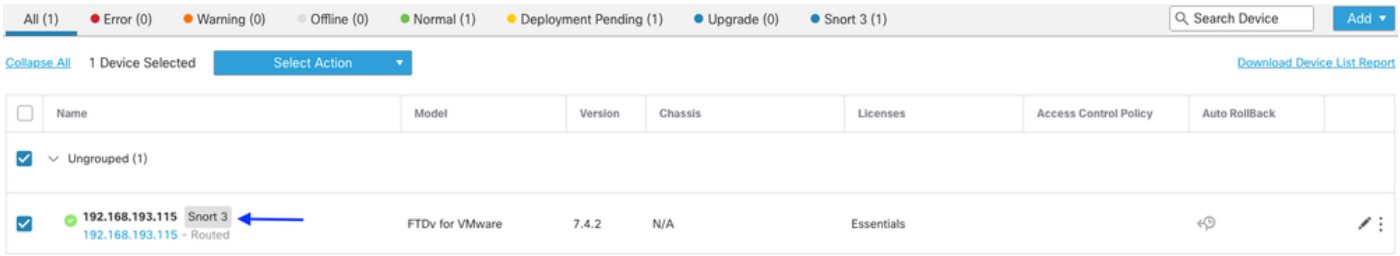
네트워크 다이어그램

기본 설정

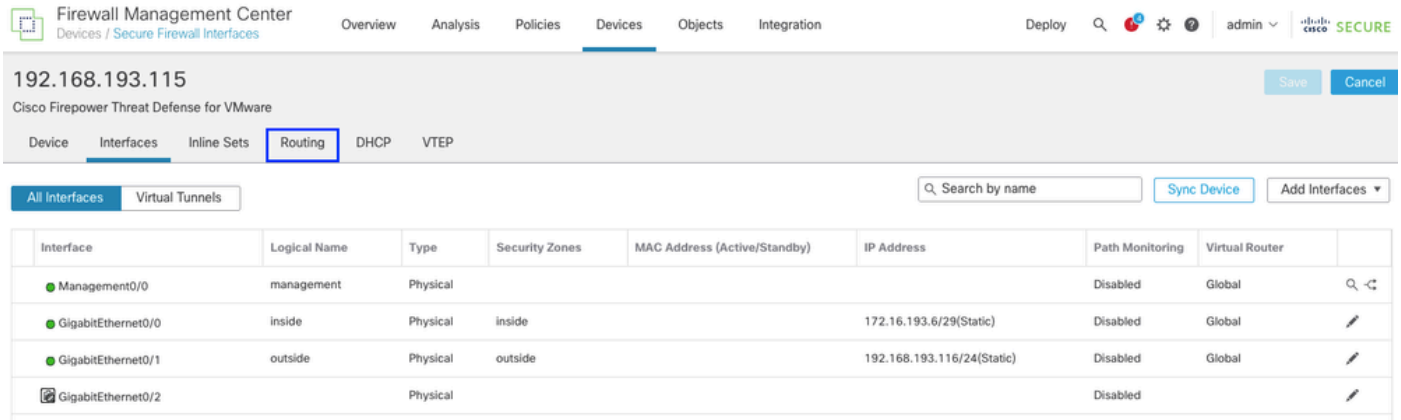
Devices(디바이스) **> Device Management(디바이스 관리)로 이동합니다**.



장치 **선택**:



라우팅 탭을 클릭합니다.



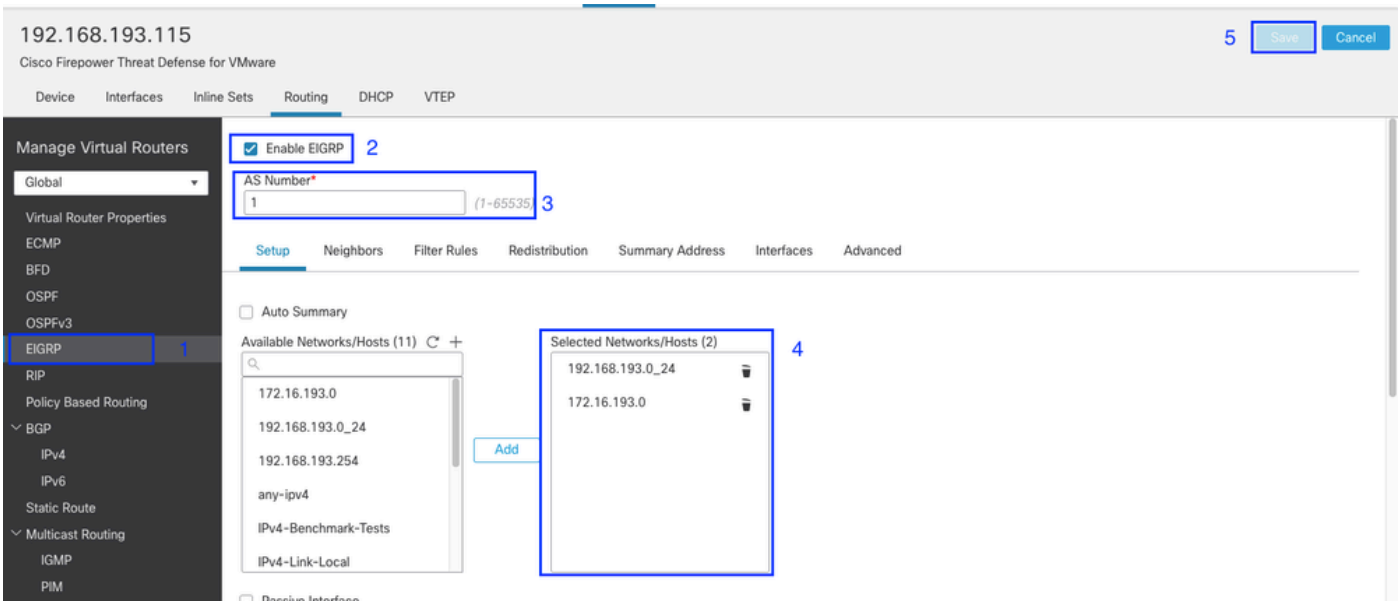
왼쪽 **메뉴**에서 EIGRP를 클릭합니다.

Enable EIGRP(**EIGRP 활성화)를 클릭합니다**.

AS 번호(1-65535)를 할당합니다.

네트워크/호스트 하나를 **선택합니다**. 'Available Network/Host' 목록에서 이전에 생성한 객체를 선택하거나 플러스(+) 버튼을 클릭하여 새 객체를 생성할 수 있습니다.

저장을 클릭합니다.



검증

다음은 EIGRP 네이버 인접성에 대한 최소 요구 사항입니다.

- AS 번호가 일치해야 합니다.
- 인터페이스는 활성 상태이고 연결 가능해야 합니다.
- 모범 사례로서, Hello 및 Hold 타이머가 일치해야 합니다.
- K-값은 일치해야 합니다.
- EIGRP 트래픽을 차단하는 액세스 목록이 없어야 합니다.

CLI를 사용한 검증

- show run router eigrp
- eigrp 네이버 표시
- eigrp 토폴로지 표시
- show eigrp interfaces
- 경로 eigrp 표시
- eigrp 트래픽 표시
- 디버그 ip eigrp 네이버
- eigrp 패킷 디버그

firepower 번호 show run router eigrp

라우터 eigrp 1

에 기본 정보 없음

기본 정보 출력 없음

eigrp log-neighbor-warnings 없음

eigrp log-neighbor-change 없음

네트워크 192.168.193.0 255.255.255.0

네트워크 172.16.193.8 255.255.255.248

firepower 번호

firepower# show eigrp neighbors

AS(1)용 EIGRP-IPv4 인접 디바이스

H 주소 인터페이스 보류 가동 시간 SRTT RTO 대기열

(초) (ms) Cnt 번호

0 14 외부 192.168.193.121 21 21:45:04 40 240 0 30

firepower# show eigrp topology

AS(1)/ID(192.168.193.121)용 EIGRP-IPv4 토폴로지 테이블

코드: P - 수동, A - 활성, U - 업데이트, Q - 쿼리, R - 회신,

r - 회신 상태, s - sia 상태

P 192.168.193.0 255.255.255.0, 1명의 후임자, FD는 512명

외부, 연결된 연결

P 172.16.193.0 255.255.255.248, 1명의 후임자, FD: 768

192.168.193.116(768/512)을 통해 외부

P 172.16.193.8 255.255.255.248, 1명의 후임자, FD 512

연결, 내부

firepower# show eigrp interface

AS(1)용 EIGRP-IPv4 인터페이스

Xmit 대기열 평균 속도 멀티캐스트 보류 중

인터페이스 피어 Un/Reliable SRTT Un/Reliable Flow Timer 경로

외부 1 0/0 10 0/1 50 0

내부 0 0/0 0 0/1 0 0 0

firepower 번호

firepower 번호 show route eigrp

코드: L - 로컬, C - 연결됨, S - 정적, R - RIP, M - 모바일, B - BGP

D - EIGRP, EX - EIGRP 외부, O - OSPF, IA - OSPF 영역 간

N1 - OSPF NSSA 외부 유형 1, N2 - OSPF NSSA 외부 유형 2

E1 - OSPF 외부 유형 1, E2 - OSPF 외부 유형 2, V - VPN

i - IS-IS, su - IS-IS 요약, L1 - IS-IS 레벨 1, L2 - IS-IS 레벨 2

ia - IS-IS inter area, * - 후보 기본값, U - 사용자별 고정 경로

o - ODR, P - 정기적으로 다운로드되는 고정 경로, + - 복제된 경로

SI - 정적 InterVRF, BI - BGP InterVRF

최종 목적지의 게이트웨이는 192.168.193.254에서 네트워크 0.0.0.0으로

D 172.16.193.0 255.255.255.248

[90/768] - 192.168.193.116, 02:32:58, 외부

firepower# show route

코드: L - 로컬, C - 연결됨, S - 정적, R - RIP, M - 모바일, B - BGP

D - EIGRP, EX - EIGRP 외부, O - OSPF, IA - OSPF 영역 간

N1 - OSPF NSSA 외부 유형 1, N2 - OSPF NSSA 외부 유형 2

E1 - OSPF 외부 유형 1, E2 - OSPF 외부 유형 2, V - VPN

i - IS-IS, su - IS-IS 요약, L1 - IS-IS 레벨 1, L2 - IS-IS 레벨 2

ia - IS-IS inter area, * - 후보 기본값, U - 사용자별 고정 경로

o - ODR, P - 정기적으로 다운로드되는 고정 경로, + - 복제된 경로

SI - 정적 InterVRF, BI - BGP InterVRF

최종 목적지의 게이트웨이는 192.168.193.254에서 네트워크 0.0.0.0으로

S* 0.0.0.0 0.0.0 [1/0] - 192.168.193.254, 외부

D 172.16.193.0 255.255.255.248

[90/768] - 192.168.193.116, 02:33:41, 외부

C 172.16.193.8 255.255.255.248은 내부에 직접 연결되어 있습니다.

L 172.16.193.14 255.255.255.255는 내부에서 직접 연결됩니다

C 192.168.193.0 255.255.255.0은 외부에 직접 연결되어 있습니다.

L 192.168.193.121 255.255.255.255는 외부에서 직접 연결됩니다

firepower 번호

firepower 번호 show eigrp traffic

AS(1)에 대한 EIGRP-IPv4 트래픽 통계

  Hello 보내기/받기: 4006/4001

  보내기/받은 업데이트: 4/4

  전송/수신된 쿼리: 0/0

  보내기/받은 회신: 0/0

  전송/수신된 Ack: 3/2

  SIA 쿼리 전송/수신: 0/0

  SIA-Replies 보내기/받기: 0/0

  안녕하세요 프로세스 ID: 2503149568

  PDM 프로세스 ID: 2503150496

  소켓 큐:

  입력 대기열: 0/2000/2/0(현재/최대/최고/삭제)

firepower 번호

문제 해결

시나리오 1 - 디버그 IP EIGRP 네이버

Debug 명령은 네이버 상태의 변경 사항을 관찰하는 데 사용할 수 있습니다.

firepower# 디버그 ip eigrp 네이버

firepower 번호

EIGRP: 보류 시간 만료

아래로 이동: 피어 192.168.193.121 total=0 stub 0, iidb-stub=0 iid-all=0

EIGRP: 할당 취소 실패 처리 [0]

EIGRP: 네이버 192.168.193.121이 바깥으로 다운되었습니다.

show eigrp neighbors 명령을 실행하여 FTD 간의 네이버 상태를 확인합니다.

firepower# show eigrp neighbors

AS(1)용 EIGRP-IPv4 인접 디바이스

show interface ip brief 명령을 사용하여 인터페이스의 상태를 확인합니다. GigabitEthernet0/1 인터페이스가 관리상 다운된 것을 확인할 수 있습니다.

firepower# show interface ip brief

인터페이스 IP 주소 정상 여부 메서드 상태 프로토콜

GigabitEthernet0/0 172.16.193.14 YES CONFIG up

GigabitEthernet0/1 192.168.193.121 YES CONFIG administratively down up

GigabitEthernet0/2 192.168.194.24 YES manual up

Internal-Control0/0 127.0.1.1 예 설정 해제

Internal-Control0/1 unassigned YES unset up

Internal-Data0/0 unassigned YES unset down up

Internal-Data0/0 unassigned 예 설정 해제

Internal-Data0/1 169.254.1.1 예 설정 해제

Internal-Data0/2 unassigned YES unset up

Management0/0 203.0.113.130 예 설정 해제

시나리오 2 - 인증

FTD는 EIGRP 패킷을 인증하는 MD5 해시 알고리즘을 지원합니다. 기본적으로 이 인증은 비활성화되어 있습니다.

MD5 해시 알고리즘을 활성화하려면 'MD5 Authentication'(MD5 인증) 확인란을 선택합니다. 인증 설정이 두 디바이스 모두에서 일치해야 합니다. 한 디바이스에서는 활성화되지만 다른 디바이스에서는 활성화되지 않는 경우 네이버 인접성이 둘 사이에 형성될 수 없습니다.

디버그 eigrp 패킷을 사용하여 이 컨피그레이션을 확인합니다.

firepower 번호 디버그 eigrp 패킷

(업데이트, 요청, 쿼리, 응답, HELLO, IPXSAP, PROBE, ACK, STUB, SIAQUERY, SIAREPLY)EIGRP 패킷 디버깅이 켜져 있음

firepower 번호

EIGRP: 외부: 192.168.193.121에서 무시된 패킷, opcode = 5(인증 해제 또는 키 체인 누락)

EIGRP: 외부 nbr 172.16.193.14에서 HELLO 수신

AS 1, 플래그 0x0:(NULL), 시퀀스 0/0 인터페이스Q 0/0

EIGRP: 외부에서 HELLO 보내기

AS 1, 플래그 0x0:(NULL), Seq 0/0 interfaceQ 0/0 iidbQ un/rely 0/0

EIGRP: 내부에서 HELLO 보내기

AS 1, 플래그 0x0:(NULL), Seq 0/0 interfaceQ 0/0 iidbQ un/rely 0/0

EIGRP: 외부: 192.168.193.121에서 무시된 패킷, opcode = 5(인증 해제 또는 키 체인 누락)

EIGRP: 외부 nbr 172.16.193.14에서 HELLO 수신

AS 1, 플래그 0x0:(NULL), 시퀀스 0/0 인터페이스Q 0/0

EIGRP: 내부에서 HELLO 보내기

AS 1, 플래그 0x0:(NULL), Seq 0/0 interfaceQ 0/0 iidbQ un/rely 0/0

EIGRP: 외부에서 HELLO 보내기

AS 1, 플래그 0x0:(NULL), Seq 0/0 interfaceQ 0/0 iidbQ un/rely 0/0

EIGRP: 외부: 192.168.193.121에서 무시된 패킷, opcode = 5(인증 해제 또는 키 체인 누락).

인증이 꺼져 있거나 키 체인이 없음을 나타내는 메시지를 관찰할 수 있습니다. 이 시나리오에서는 일반적으로 인증이 한 피어에서 활성화되지만 다른 피어에서는 활성화되지 않을 때 발생합니다.

EIGRP: 외부: 192.168.193.121에서 무시된 패킷, opcode = 5(인증 해제 또는 키 체인 누락).

show run interface <EIGRP interface>를 사용하여 확인합니다.

Firepower1# show run interface GigabitEthernet0/1

!

인터페이스 GigabitEthernet0/1

nameif 외부

보안 수준 0

ip 주소 192.168.193.121 255.255.255.0

인증 키 eigrp 1 ***** key-id 10

인증 모드 eigrp 1 md5

Firepower2# show run interface GigabitEthernet0/1

!

인터페이스 GigabitEthernet0/1

nameif 외부

보안 수준 0

ip 주소 192.168.193.116 255.255.255.0

시나리오 3 - 패시브 인터페이스

EIGRP가 구성된 경우 EIGRP hello 패킷은 일반적으로 네트워크가 활성화된 인터페이스에서 송수신됩니다.

그러나 인터페이스가 패시브로 구성된 경우 EIGRP는 해당 인터페이스의 두 라우터 간에 hello 패킷이 교환되는 것을 억제하여 인접 디바이스 인접성이 손실됩니다. 따라서 이 작업은 라우터가 라우팅 업데이트를 해당 인터페이스에서 알리지 못하게 할 뿐 아니라 해당 인터페이스에서 라우팅 업데이트를 수신하지 못하게 합니다.

show eigrp neighbors 명령을 실행하여 FTD 간의 네이버 상태를 확인합니다.

firepower# show eigrp neighbors

AS(1)용 EIGRP-IPv4 인접 디바이스

debug eigrp packets 명령을 사용하여 전송 중인 EIGRP 패킷과 이러한 패킷을 통해 전송되는 인터페이스를 확인할 수 있습니다.

FTD 1

Firepower1#

(업데이트, 요청, 쿼리, 응답, HELLO, IPXSAP, PROBE, ACK, STUB, SIAQUERY, SIAREPLY)EIGRP 패킷 디버깅이 켜져 있음

firepower 번호

EIGRP: 외부에서 HELLO 보내기

AS 1, 플래그 0x0:(NULL), Seq 0/0 interfaceQ 0/0 iidbQ un/rely 0/0

EIGRP: 내부에서 HELLO 보내기

AS 1, 플래그 0x0:(NULL), Seq 0/0 interfaceQ 0/0 iidbQ un/rely 0/0

EIGRP: 외부에서 HELLO 보내기

AS 1, 플래그 0x0:(NULL), Seq 0/0 interfaceQ 0/0 iidbQ un/rely 0/0

EIGRP: 내부에서 HELLO 보내기

AS 1, 플래그 0x0:(NULL), Seq 0/0 interfaceQ 0/0 iidbQ un/rely 0/0

EIGRP: 외부에서 HELLO 보내기

FTD 2

Firepower2# eigrp 패킷 디버그

(업데이트, 요청, 쿼리, 응답, HELLO, IPXSAP, PROBE, ACK, STUB, SIAQUERY, SIAREPLY)EIGRP 패킷 디버깅이 켜져 있음

Firepower2#

이 시나리오에서 FTD 2는 내부 및 외부 인터페이스가 패시브로 구성되어 있으므로 EIGRP hello 메시지를 보내지 않습니다. show run router eigrp 명령을 사용하여 이를 확인합니다.

Firepower2# show run router eigrp

라우터 eigrp 1

에 기본 정보 없음

기본 정보 출력 없음

eigrp log-neighbor-warnings 없음

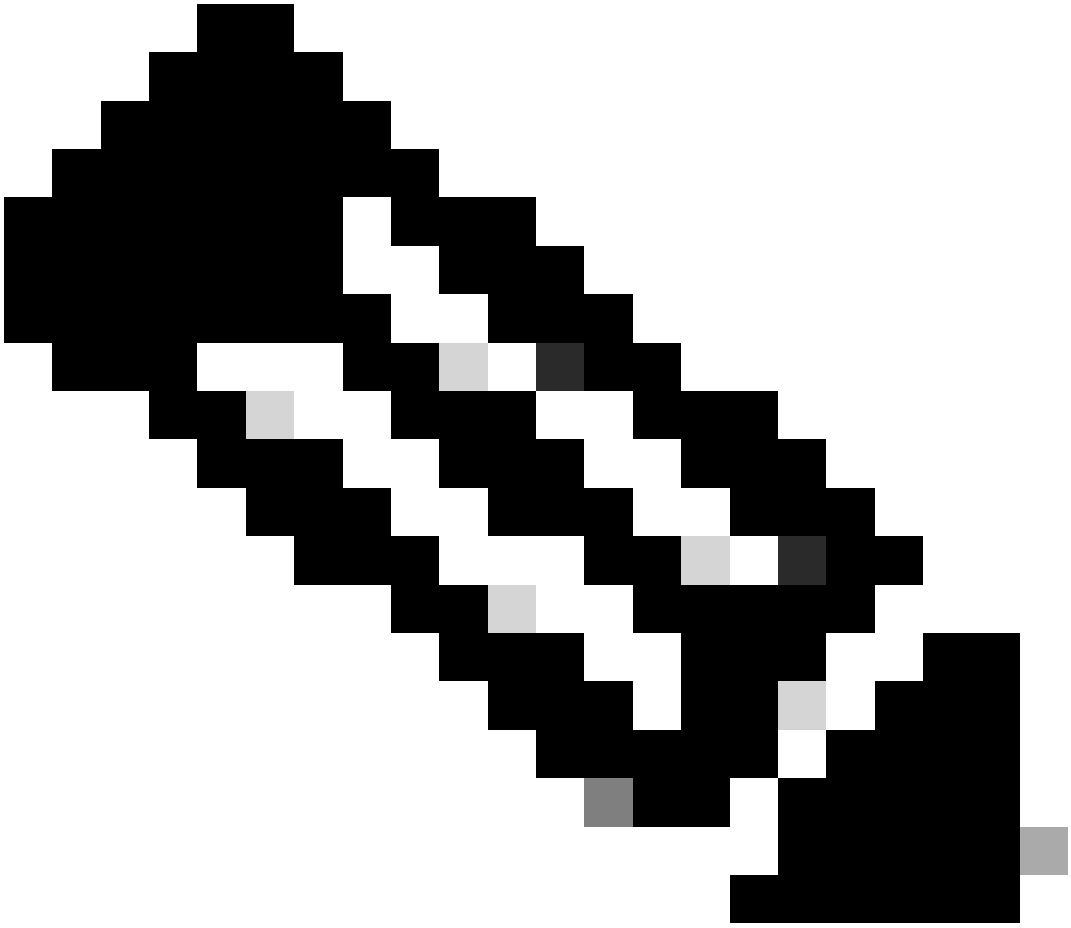
eigrp log-neighbor-change 없음

네트워크 192.168.193.0 255.255.255.0

네트워크 172.16.193.8 255.255.255.248

외부 패시브 인터페이스

내부 패시브 인터페이스



참고: 구성된 모든 디버그 프로세스를 중지하려면 undebug all 명령을 사용합니다.

관련 정보

- FTD 디바이스의 EIGRP
- FTD에서 EIGRP 구성
- EIGRP 복합 비용 메트릭

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.