Firepower Intrusion Inspection에서 EIGRP, OSPF 및 BGP 메시지 제외

목차

[소개](#)
[사전 요구 사항](#)
[사용되는 구성 요소](#)
[네트워크 다이어그램](#)
[구성](#)
[EIGRP 예](#)
[OSPF 예](#)
[BGP 예](#)
[확인](#)
[EIGRP](#)
[OSPF](#)
[BGP](#)
[문제 해결](#)

소개

라우팅 프로토콜은 hello 메시지와 keepalive를 전송하여 라우팅 정보를 교환하고 인접 디바이스가 여전히 연결 가능한지 확인합니다.과부하 상태에서 Cisco Firepower 어플라이언스는 라우터가 인접 디바이스를 중단한다고 선언하기에 충분한 시간 동안 keepalive 메시지를 삭제하지 않고 지연할 수 있습니다.이 문서에서는 라우팅 프로토콜의 keepalive 및 제어 평면 트래픽을 제외하는 신뢰 규칙을 생성하는 단계를 제공합니다.Firepower 어플라이언스 또는 서비스는 검사 지연 없이 인그레스(ingress)에서 이그레스(egress) 인터페이스로 패킷을 전환할 수 있습니다.

사전 요구 사항

사용되는 구성 요소

이 문서의 액세스 제어 정책 변경 사항은 다음 하드웨어 플랫폼을 사용합니다.

- FMC(FireSIGHT Management Center)
- Firepower 어플라이언스:7000 시리즈, 8000 시리즈 모델

참고:이 문서의 정보는 특정 랩 환경의 디바이스에서 생성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

네트워크 다이어그램

- 라우터 A와 라우터 B는 레이어 2에 인접하며 인라인 Firepower 어플라이언스(ips로 표시됨)를 인식하지 못합니다.

- 라우터 A - 10.0.0.1/24
- 라우터 B - 10.0.0.2/24

- 테스트된 각 Interior Gateway Protocol(EIGRP 및 OSPF)에 대해 라우팅 프로토콜은 10.0.0.0/24 네트워크에서 활성화되었습니다.
- BGP를 테스트할 때 e-BGP가 사용되었으며 직접 연결된 물리적 인터페이스를 피어링의 업데이트 소스로 사용했습니다.

구성

EIGRP 예

라우터

라우터 A:

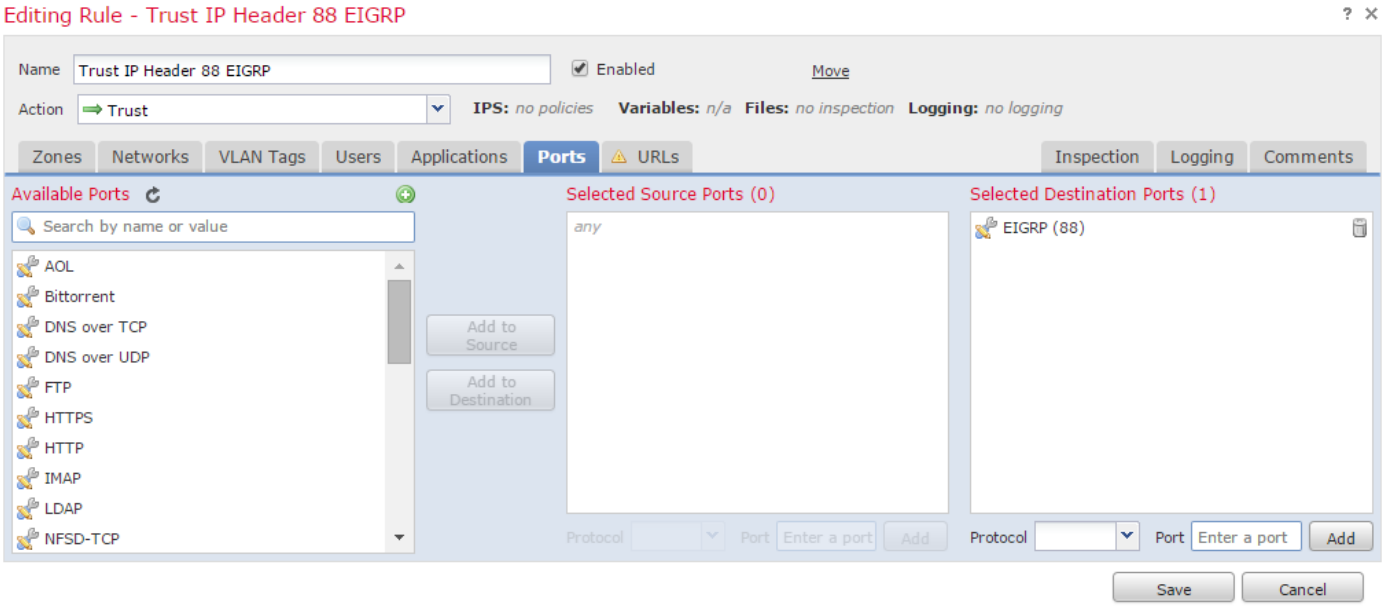
```
router eigrp 1
network 10.0.0.0 0.0.0.255
```

라우터 B:

```
router eigrp 1
network 10.0.0.0 0.0.0.255
```

FireSIGHT Management Center에서

1. Firepower 어플라이언스에 적용된 액세스 제어 정책을 선택합니다.
2. Trust 작업으로 액세스 제어 규칙을 **생성합니다.**
3. Ports(포트) 탭에서 프로토콜 88에서 EIGRP를 선택합니다.
4. Add(**추가**)를 클릭하여 목적지 포트에 포트를 추가합니다.
5. 액세스 제어 규칙을 저장합니다.



OSPF 예

라우터

라우터 A:

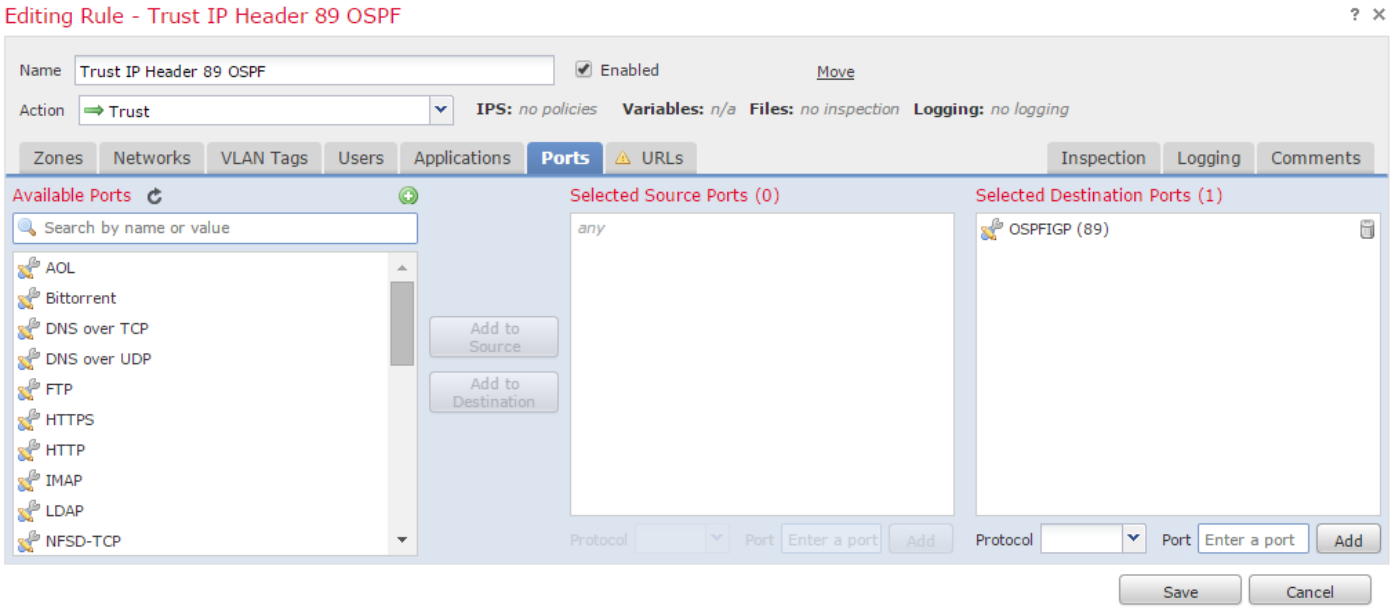
```
router ospf 1
network 10.0.0.0 0.0.0.255 area 0
```

라우터 B:

```
router ospf 1
network 10.0.0.0 0.0.0.255 area 0
```

FireSIGHT Management Center에서

1. Firepower 어플라이언스에 적용된 액세스 제어 정책을 선택합니다.
2. Trust 작업으로 액세스 제어 규칙을 **생성합니다.**
3. Ports(포트) 탭에서 프로토콜 89에서 OSPF를 선택합니다.
4. Add(**추가**)를 클릭하여 목적지 포트에 포트를 추가합니다.
5. 액세스 제어 규칙을 저장합니다.



BGP 예

라우터

라우터 A:

```
router bgp 65001
neighbor 10.0.0.2 remote-as 65002
```

라우터 B:

```
router bgp 65002
neighbor 10.0.0.1 remote-as 65001
```

FireSIGHT Management Center에서

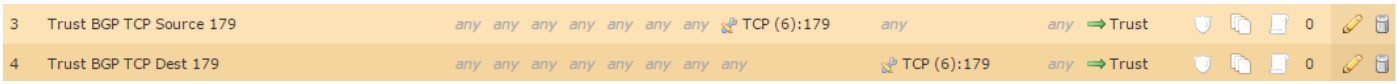
참고:두 개의 액세스 제어 항목을 생성해야 합니다. 포트 179는 어떤 BGP 스피커의 TCP SYN이 세션을 먼저 설정하는지에 따라 소스 또는 대상 포트일 수 있습니다.

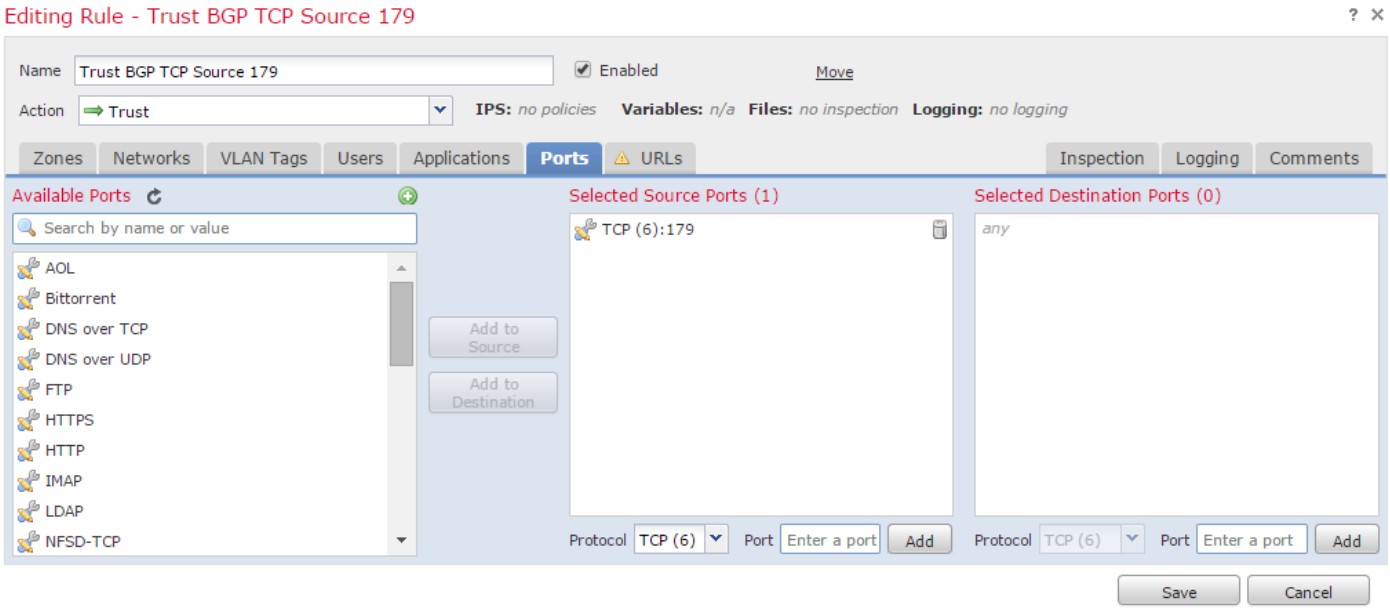
규칙 1:

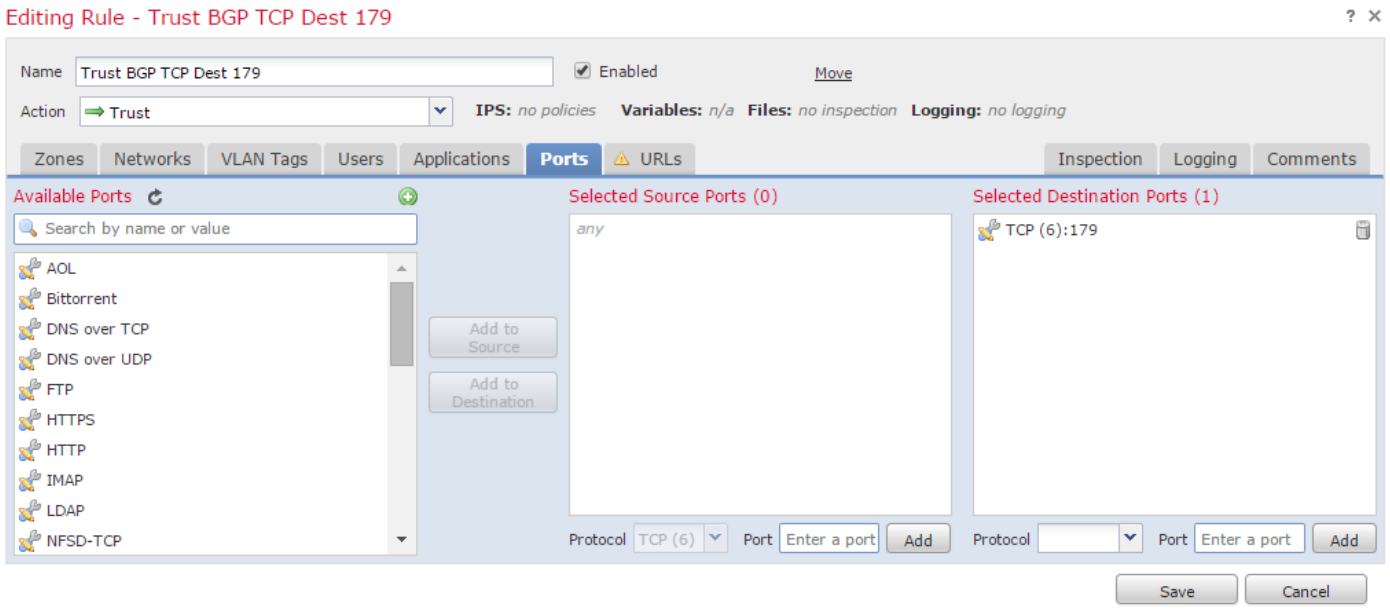
1. Firepower 어플라이언스에 적용된 액세스 제어 정책을 선택합니다.
2. **Trust 작업을 사용하여 액세스 제어 규칙을 생성합니다.**
3. Ports(**포트**) 탭에서 **TCP(6)를** 선택하고 **포트 179**를 **입력합니다**.
4. Add(**추가**)를 클릭하여 포트를 **소스 포트**에 추가합니다.
5. 액세스 제어 규칙을 저장합니다.

규칙 2:

1. Firepower 어플라이언스에 적용된 액세스 제어 정책을 선택합니다.
2. **Trust 작업을 사용하여 액세스 제어 규칙을 생성합니다.**
3. Ports(**포트**) 탭에서 **TCP(6)를 선택하고 포트 179**를 **입력합니다**.
4. Add(**추가**)를 클릭하여 포트를 **대상 포트**에 **추가합니다**.
5. 액세스 제어 규칙 저장







확인

신뢰 규칙이 예상대로 작동하는지 확인하려면 Firepower 어플라이언스에서 패킷을 캡처합니다.패킷 캡처에서 EIGRP, OSPF 또는 BGP 트래픽을 발견하면 트래픽이 예상대로 신뢰되지 않습니다.

> **팁**:FirePOWER 어플라이언스에서 트래픽을 캡처하는 방법에 대한 단계를 보려면 을/를 참조하십시오.

다음은 몇 가지 예입니다.

EIGRP

Trust 규칙이 예상대로 작동하는 경우 다음 트래픽이 표시되지 않아야 합니다.

```
16:46:51.568618 IP 10.0.0.1 > 224.0.0.10: EIGRP Hello, length: 40
16:46:51.964832 IP 10.0.0.2 > 224.0.0.10: EIGRP Hello, length: 40
```

OSPF

Trust 규칙이 예상대로 작동하는 경우 다음 트래픽이 표시되지 않아야 합니다.

```
16:46:52.316814 IP 10.0.0.2 > 224.0.0.5: OSPFv2, Hello, length 60
16:46:53.236611 IP 10.0.0.1 > 224.0.0.5: OSPFv2, Hello, length 60
```

BGP

Trust 규칙이 예상대로 작동하는 경우 다음 트래픽이 표시되지 않아야 합니다.

```
17:10:26.871858 IP 10.0.0.1.179 > 10.0.0.2.32158: Flags [S.], seq 1060979691, ack 3418042121,
win 16384, options [mss 1460], length 0
17:10:26.872584 IP 10.0.0.2.32158 > 10.0.0.1.179: Flags [.], ack 1, win 16384, length 0
```

> **참고:**TCP 및 keepalive를 기반으로 BGP 라이드가 IGP만큼 자주 발생하지 않습니다.업데이트 또는 철회할 접두사가 없다고 가정할 경우, 포트 TCP/179에서 트래픽이 표시되지 않음을 확인하기 위해 더 오랜 시간을 기다려야 할 수 있습니다.

문제 해결

라우팅 프로토콜 트래픽이 계속 표시되면 다음 작업을 수행하십시오.

1. 액세스 제어 정책이 FireSIGHT Management Center에서 Firepower 어플라이언스에 성공적으로 적용되었는지 확인합니다.이렇게 하려면 **System > Monitoring > Task Status** 페이지로 이동합니다.
2. 규칙 작업이 **Trust**이고 Allow가 **아닌지 확인합니다**.

3. **Trust** 규칙에서 로깅이 활성화되지 않았는지 확인합니다.