CSF CLI에서 트래픽 문제 해결

목차

소개

이 문서에서는 Cisco Secure Firewall CLI를 사용하여 라우팅, 패킷 흐름 및 Snort 동작을 검증하여 트래픽 문제를 해결하는 방법에 대해 설명합니다.

사전 요구 사항

이 문서에 대한 특정 요건이 없습니다.

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- FMC(firepower 관리 센터) 정책 및 개체 컨피그레이션
- Cisco CSF(Secure Firewall) 라우팅 및 인터페이스 로직
- 패킷 검사 및 방화벽 트러블슈팅 개념

사용되는 구성 요소

이 문서는 CSF용 특정 소프트웨어 및 하드웨어 버전으로 제한되지 않습니다. 문서에 사용된 장치는 코드 7.6.5를 실행하고 있습니다.

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.

관련 제품

이 문서는 다음 하드웨어 및 소프트웨어 버전에서도 사용할 수 있습니다.

- FMC(Secure Firewall Management Center)
- Cisco CSF(Secure Firewall)
- Firepower Threat Defense CLI 툴

중요 정보

디바이스에 CPU, 메모리 또는 I/O 사용률이 높아지면 문제 해결 명령을 실행하면 성능 저하가 심화될 수 있습니다. 먼저 자원 고갈 상태를 조사하여 해결한 후 트래픽 문제 진단을 진행하는 것이 좋습니다. 진단 명령은 추가 시스템 리소스를 소비하므로 가용성이 더욱 저하되고 복구 시간이 길어질 수 있습니다.

배경 정보

CSF의 트래픽 문제 해결은 패킷이 방화벽을 통과해야 하는 논리적 경로를 확인하는 것으로 시작하는 경우가 많습니다. 경로 및 인터페이스 매핑이 파악되면 다음 단계는 예상 경로를 실제 패킷 흐름과 비교하는 것입니다. 이 작업은 경로 조회, 패킷 추적기 시뮬레이션, 패킷 캡처 및 Snort 엔진 추적을 사용하여 수행할 수 있습니다.

각 툴은 서로 다른 가시성 레이어를 제공합니다.

- show route는 패킷의 라우팅 경로 및 인터페이스 id를 확인합니다.
- packet-tracer는 트래픽 흐름을 시뮬레이션하고 ACL, NAT 및 인터페이스 결정을 식별합니다.
- 패킷 캡처는 방화벽을 통과하는 라이브 트래픽을 검사합니다.
- 시스템 지원 추적은 정책 관련 블록 또는 검사 이벤트에 대한 Snort 의사 결정을 표시합니다.

팁: 트래픽을 캡처하기 전에 라우팅 및 패킷 추적기 검증부터 시작하므로, 라이브 트래픽을 분석하기 전에 예상 경로 및 액세스 제어 결정이 올바른지 확인할 수 있습니다.

문제

트래픽 흐름이 예상대로 작동하지 않으므로 관리자는 패킷이 올바른 경로를 사용하는지, 방화벽이 연결을 허용하는지 거부하는지, Snort 또는 정책 검사가 트래픽을 차단하는지 확인해야 합니다.

1단계: 경로 찾기

라우팅 경로를 식별하고 소스 및 목적지 IP 주소와 연결된 논리적 인터페이스 이름을 결정합니다. 논리적 인터페이스 이름은 대부분의 트러블슈팅 명령에서 필요하므로 트러블슈팅 워크플로의 첫 번째 단계여야 합니다.

소스 및 대상 IP 주소에 대한 명령을 실행합니다.

```
show route <IP>
```

기본 경로를 사용하는 인터넷으로 향하는 트래픽에는 논리적 이그레스(egress) 인터페이스를 식별해야 합니다. 논리적 인터페이스 이름은 다음 단계를 실행하여 결정할 수 있습니다.

```
show route 0.0.0.0
```

출력 예:

```
FTD1# show route 192.168.0.11

Routing entry for 192.168.0.0 255.255.255.0
Known via "connected", distance 0, metric 0 (connected, via interface)
Routing Descriptor Blocks:

    directly connected, via Inside
    Route metric is 0, traffic share count is 1
```

```
FTD1# show route 0.0.0.0

Routing entry for 0.0.0.0 0.0.0.0, supernet
Known via "static", distance 1, metric 0, candidate default path
Routing Descriptor Blocks:

    128.107.0.1, via Outside
    Route metric is 0, traffic share count is 1
```

이 예에서 논리적 인그레스 인터페이스는 Inside이고 이그레스 인터페이스는 Outside입니다.

주의: NAT(Network Address Translation)는 NAT 정책이 트래픽 흐름과 일치하는 경우 라우팅 테이블이 나타내는 것과 다른 인터페이스를 통해 트래픽을 리디렉션할 수 있습니다. 연결 문제를 해결할 때 NAT 컨피그레이션이 예상 트래픽 경로와 일치하는지 확인합니다.

팁: 논리적 인터페이스 이름은 CLI 트러블슈팅 명령에서 사용됩니다. 향후 참조를 위해 논리적 이름을 기록해 두십시오.

2단계: 패킷 추적기 실행

packet-tracer를 사용하여 방화벽이 특정 트래픽 흐름을 평가하는 방법을 시뮬레이션합니다. 이 툴은 어떤 인터페이스가 사용되는지, NAT 정책이 적용되는지, ACL이 트래픽을 허용하는지 또는 거부하는지 확인하는 데 도움이 됩니다.

다음 명령 구문을 사용합니다.

```
packet-tracer input <source interface> <protocol> <source IP> <source port> <destination IP> <destinati
```

명령 예:

```
FTD1# packet-tracer input Inside tcp 192.168.0.11 55555 72.163.4.161 443
```

출력을 검토하여 패킷이 예상 경로를 따르고 시뮬레이션 중에 허용되는지 확인합니다. 이 기능은 라이브 패킷 분석에 참여하기 전에 문제가 라우팅, NAT 또는 정책 일치와 관련이 있는지 확인해야 할 때 유용합니다.

packet-tracer의 transmit 키워드는 시뮬레이션된 패킷이 인그레스 인터페이스에 삽입되도록 하여

시뮬레이션으로 남아 있지 않고 모든 방화벽 처리 단계를 통과하도록 합니다.

명령 예:

```
FTD1# packet-tracer input Inside tcp 192.168.0.11 55555 72.163.4.161 443 transmit
```

3단계: 캡처 실행

방화벽을 통과할 때 패킷 캡처를 사용하여 라이브 트래픽을 검사합니다. 패킷 캡처는 실제 트래픽을 캡처하므로 캡처가 활성화된 시점에 방화벽을 통과하는 실제 흐름과 일치해야 하므로 패킷 추적기와 다릅니다. 패킷 캡처는 양방향이며, 연결의 양쪽을 문서화합니다.

대부분의 트래픽 문제 해결 시나리오에서 다음 캡처를 구성합니다.

- 인그레스 캡처 — 소스 측 인터페이스에 도착하는 트래픽을 캡처합니다.
- 이그레스 캡처 — 목적지 측 인터페이스에서 나가는 트래픽을 캡처합니다
- ASP Drop Capture — 방화벽에 의해 삭제된 패킷을 캡처하고 구성된 기준과 일치시킵니다

일반 캡처 구문:

```
capture <name> interface <interface name> trace match ip host <source IP> host <destination IP>
```

인그레스 캡처 예:

```
FTD1# capture in interface trace Inside match ip host 192.168.0.11 host 72.163.4.161
```

이그레스 캡처 예:

```
FTD1# capture out interface trace Outside match ip host 128.107.0.22 host 72.163.4.161
```

ASP 드롭 캡처 예:

```
FTD1# cap asp type asp-drop match ip host 192.168.0.11 host 72.163.4.161
```

패킷 캡처는 양방향입니다. 즉, 정의된 일치 기준에 따라 전달 트래픽과 반환 트래픽을 모두 캡처할 수 있습니다. 추적 기능을 사용하면 방화벽이 실제 트래픽에서 내리는 결정을 시각화할 수 있습니다.

주의: NAT가 수행되는 경우 이그레스 캡처는 원래 소스 IP가 아닌 변환된 소스 IP를 사용하여 사후 NAT 트래픽을 올바르게 캡처해야 합니다.

4단계: 시스템 지원 추적 실행

시스템 지원 추적을 사용하여 특정 트래픽 흐름에 대한 실시간 Snort 검사 프로세스를 확인합니다. 이는 트래픽이 ACL 허용 규칙과 일치하지만 정책 검사에 의해 차단된 경우 특히 유용합니다. 표준 패킷 캡처를 통해 패킷이 차단되었음을 알 수 있지만, 시스템 지원 추적을 통해 해당 패킷이 그렇게 처리된 이유를 파악할 수 있습니다. 시스템 지원 추적은 양방향입니다. 즉 양쪽에서 트래픽을 수신합니다. 즉, IP를 툴에 추가하는 순서는 중요하지 않습니다.

이 명령을 실행하고 프롬프트에 응답합니다.

```
> system support trace


Enable firewall-engine-debug too? [n]: y
Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.0.11
Please specify a client port:
Please specify a server IP address: 72.163.4.161
Please specify a server port: 443
```

이 툴은 환경에서 애플리케이션 또는 URL 규칙, ID 기반 규칙, 파일 정책 또는 침입 정책을 사용할 때 특히 유용합니다. 이러한 기능은 ACL 일치 이후에 평가되므로 패킷은 액세스 제어 정책에서 허용될 수 있지만 Snort 검사에 의해 차단될 수 있습니다.

참고: 정확한 소스 포트를 알 수 없는 경우 클라이언트 포트를 비워 둘 수 있습니다.

다음을 확인합니다.

경로 조회, 패킷 추적기 시뮬레이션, 패킷 캡처 및 시스템 지원 추적의 출력을 함께 사용하여 트래픽

흐름의 동작을 확인합니다. 목표는 심층 검사를 기반으로 패킷이 올바른 경로를 취하고 있는지, 방화벽이 이를 허용하거나 거부하고 있는지, 그리고 Snort가 이를 차단하고 있는지 확인하는 것입니다.

전체 트러블슈팅 흐름에서 일반적으로 확인하는 내용은 다음과 같습니다.

- 경로 조회는 논리적 인그레스 및 이그레스 인터페이스를 표시합니다.
- 패킷 추적기는 의도한 전달 경로 및 정책 평가를 확인합니다.
- 패킷 캡처는 트래픽이 예상대로 들어오고 나가는지 확인합니다.
- 시스템 지원 추적에서는 Snort 또는 정책 검사로 인해 차단되는지 확인합니다.

문제 해결

트래픽 문제가 지속되면 다음 영역을 검토하십시오.

- 경로 조회가 예상 소스 및 대상 인터페이스와 일치하는지 확인합니다.
- 패킷 추적기 출력에 ACL 또는 NAT 스테이지에서 거부되는 트래픽이 표시되는지 확인합니다.
- 인그레스 및 이그레스 패킷 캡처를 검토하여 트래픽이 방화벽에 도달하고 올바른 인터페이스에서 나가는지 확인합니다.
- ASP 삭제 캡처를 사용하여 방화벽에서 트래픽을 내부적으로 삭제하는지 여부를 확인합니다.
- 시스템 지원 추적을 사용하여 ACL 허용 결정 후 Snort가 트래픽을 차단하는지 여부를 확인합니다.

관련 정보

- firepower 방화벽 캡처를 분석하여 네트워크 문제 해결
- firepower Threat Defense 캡처 및 패킷 추적기 사용

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.