FirePOWER Management Center에서 일부 TCP 연결 이벤트를 잘못된 방향으로 표시합니다.

목차

소개

이 문서에서는 Initiator IP가 TCP 연결의 서버 IP이고 Responder IP가 TCP 연결의 클라이언트 IP인 반대 방향으로 TCP 연결 이벤트를 표시하는 FirePOWER Management Center(FMC)의 이유와 완화 단계를 설명합니다.

> **참고:**이러한 이벤트가 발생하는 이유는 여러 가지가 있습니다.이 문서에서는 이 증상의 가장 일반적인 원인을 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- FirePOWER 기술
- ASA(Adaptive Security Appliance)에 대한 기본 지식
- TCP(Transmission Control Protocol) 타이밍 메커니즘의 이해

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 소프트웨어 버전 6.0.1 이상을 실행하는 ASA Firepower Threat Defense(5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X)
- 소프트웨어 버전 6.0.1 이상을 실행하는 ASA Firepower Threat Defense(5512-X,5515-X, ASA 5525-X, ASA 555-X, FP9300, FP4100)
- Firepower 모듈(5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X, 5515-X, ASA 5525-X, ASA 5545-X, ASA 555-5555 소프트웨어 버전 6.0.0 이상을 실행하는 X, ASA 5585-X)

- FMC(Firepower Management Center) 버전 6.0.0 이상

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 일반(기본) 구성으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경

TCP 연결에서 **클라이언트**는 초기 패킷을 전송하는 IP를 참조합니다.FirePOWER Management Center는 관리되는 디바이스(센서 또는 FTD)에서 연결의 초기 TCP 패킷을 볼 때 연결 이벤트를 생성합니다.

TCP 연결 상태를 추적하는 디바이스에는 엔드포인트에서 잘못 닫히지 않는 연결이 장기간 사용 가능한 메모리를 사용하지 않도록 **유휴 시간** 제한이 정의되어 있습니다.FirePOWER에서 설정된 TCP 연결의 기본 유휴 시간 제한은 **3분입니다**.3분 이상 유휴 상태로 유지된 TCP 연결은 FirePOWER IPS 센서에서 추적되지 않습니다.

시간 초과 이후의 후속 패킷은 새 TCP 흐름으로 처리되고 이 패킷과 일치하는 규칙에 따라 전달 결정이 수행됩니다.패킷이 서버에서 전송되면 서버의 IP가 이 새 흐름의 개시자로 기록됩니다.규칙에 대해 로깅을 활성화하면 FirePOWER Management Center에서 연결 이벤트가 생성됩니다.

> **참고:**구성된 정책에 따라 시간 초과 이후에 오는 패킷에 대한 전달 결정은 초기 TCP 패킷에 대한 결정과 다릅니다.구성된 기본 작업이 "Block"이면 패킷이 삭제됩니다.

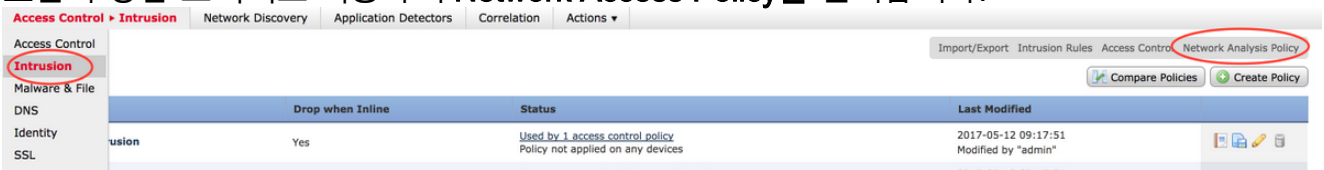
이 증상의 예는 아래 스크린샷과 같습니다.

First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code
2017-05-12 17:48:05		Block		10.32.38.30		192.168.38.30				443 (https) / tcp	44705 / tcp
2017-05-12 17:39:13		Allow		192.168.38.30		10.32.38.30				44705 / tcp	443 (https) / tcp

솔루션

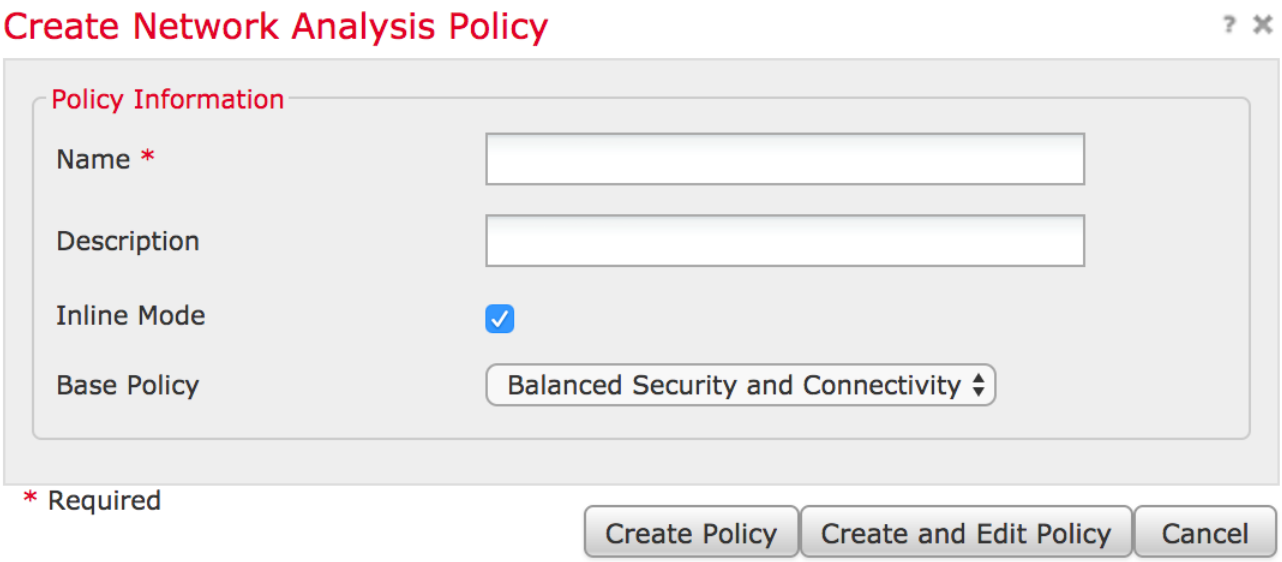
위에서 언급한 문제는 TCP 연결의 **시간 초과**를 늘려 완화됩니다.시간 제한을 변경하려면

1. Policies(정책) **> Access Control(액세스 제어) > Intrusion(침입)으로 이동합니다**.
2. 오른쪽 상단 모서리로 이동하여 **Network Access Policy를** 선택합니다.

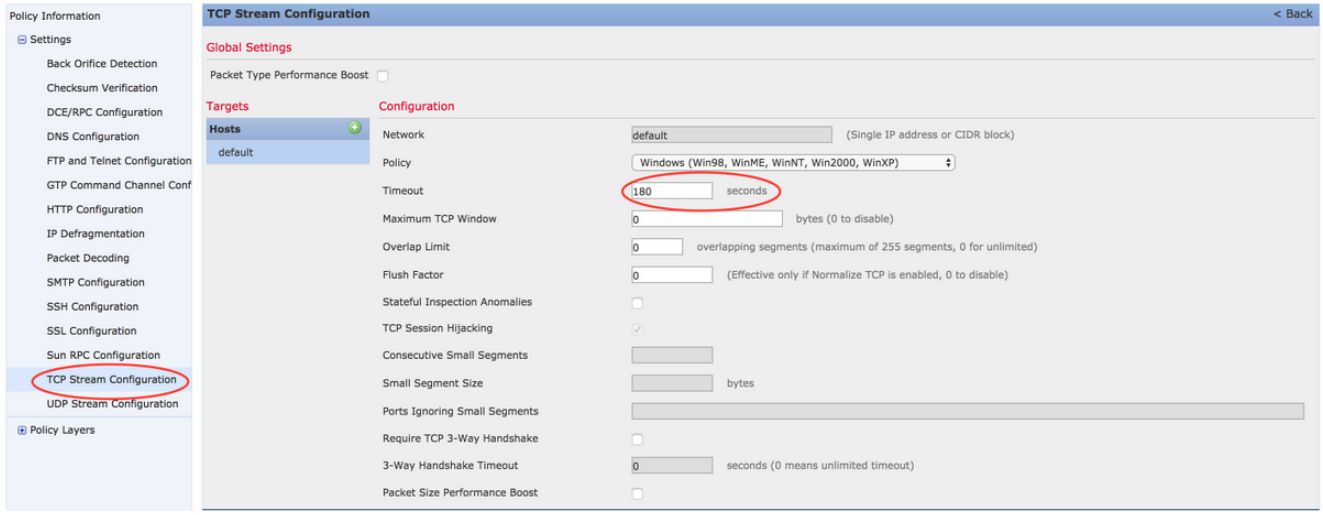


3. Create **Policy(정책 생성)**를 선택하고 이름을 선택한 다음 Create and Edit Policy(정책 생성 **및 수정)를 클릭합니다.기본 정책**을 수정하지 마십시오

.

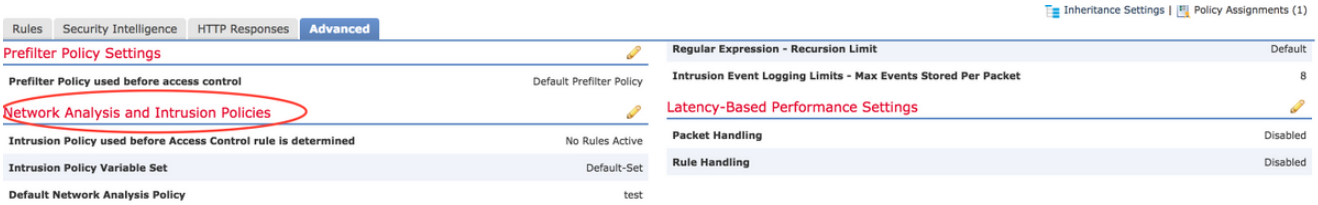


4. Settings(**설정**) 옵션을 확장하고 **TCP Stream Configuration(TCP 스트림 컨피그레이션)을** 선택합니다.
5. 컨피그레이션 섹션으로 이동하고 원하는 대로 **Timeout** 값을 변경합니다



6. Policies(**정책) > Access Control(액세스 제어) > Access Control(액세스 제어)로 이동합니다.**
7. 관련 관리 디바이스에 적용된 정책을 수정하거나 새 정책을 생성하려면 **Edit** 옵션을 선택합니다

8. Access 정책에서 **Advanced** 탭을 선택합니다.
9. Network **Analysis and Intrusion Policies(네트워크 분석 및 침입 정책)** 섹션을 찾고 Edit(수정) 아이콘**을** 클릭합니다



10. **Default Network Analysis Policy(기본 네트워크 분석 정책)**의 드롭다운 메뉴에서 2단계에서 생성한 정책을 선택합니다.
11. 확인**을** 클릭하고 변경 사항을 저장합니다.

12. Deploy(구축) 옵션을 클릭하여 관련 관리되는 디바이스에 정책을 구축합니다.

주의:시간 초과가 증가하면 메모리 사용률이 높아질 것으로 예상되며, FirePOWER는 엔드포인트에서 더 오랫동안 닫히지 않는 흐름을 추적해야 합니다.실제 메모리 사용률 증가는 네트워크 애플리케이션이 TCP 연결을 유휴 상태로 유지하는 기간에 따라 다르므로 각 고유한 네트워크에 대해 다릅니다.

결론

TCP 연결의 유휴 시간 초과에 대한 모든 네트워크의 벤치마크는 다릅니다.사용 중인 애플리케이션에 따라 전적으로 달라집니다.네트워크 애플리케이션이 TCP 연결을 유휴 상태로 유지하는 시간을 관찰하여 최적의 값을 설정해야 합니다.Cisco ASA의 FirePOWER 서비스 모듈과 관련된 문제의 경우, 최적의 값을 추론할 수 없는 경우 ASA의 시간 제한 값에 대한 단계별로 시간 제한을 늘려 시간 제한을 조정할 수 있습니다.

관련 정보

- ASA용 Cisco Firepower Threat Defense 빠른 시작 가이드
- 기술 지원 및 문서 – Cisco Systems
- ASA Firepower 빠른 시작 가이드