Firepower 데이터 경로 문제 해결: 개요

목차

소개

이 가이드는 FirePOWER 서비스가 설치된 FTD(Firepower Threat Defense) 디바이스 또는 ASA(Adaptive Security Appliance)가 네트워크 트래픽에 문제를 일으키는지 여부를 신속하게 식별하는 데 도움이 됩니다. 또한 Cisco TAC(Technical Assistance Center)에 참여하기 전에 조사해야 할 Firepower 구성 요소와 수집해야 할 데이터를 줄이는 데 도움이 됩니다.

다음은 모든 Firepower 데이터 경로 문제 해결 시리즈 문서의 목록입니다.

Firepower 데이터 경로 문제 해결 1단계: 패킷 인그레스

https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214574-firepower-data-path-troubleshooting-phas.html

Firepower 데이터 경로 문제 해결 2단계: DAQ 레이어
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214575-firepower-data-path-troubleshooting-phas.html

Firepower 데이터 경로 문제 해결 3단계: 보안 인텔리전스
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214576-firepower-data-path-troubleshooting-phas.html

Firepower 데이터 경로 문제 해결 4단계: 액세스 제어 정책
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214577-firepower-data-path-troubleshooting-phas.html

Firepower 데이터 경로 문제 해결 5단계: SSL 정책
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214581-firepower-data-path-troubleshooting-phas.html

Firepower 데이터 경로 문제 해결 6단계: 활성 인증
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw-virtual/214608-firepower-data-path-troubleshooting-phas.html

Firepower 데이터 경로 문제 해결 7단계: 침입 정책
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214609-firepower-data-path-troubleshooting-phas.html

Firepower 데이터 경로 문제 해결 8단계: 네트워크 분석 정책

https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214610-firepower-data-path-troubleshooting-phas.html

사전 요구 사항

- 이 문서에서는 사용자가 FTD 및 ASA 플랫폼에 대해 기본적으로 이해하고 있다고 가정합니다.
- 필수는 아니지만, 오픈 소스 Snort에 대한 지식이 있는 것이 좋습니다.

설치 및 설정 가이드를 포함한 Firepower 설명서의 전체 목록은 설명서 로드맵 페이지를 참조하십시오.

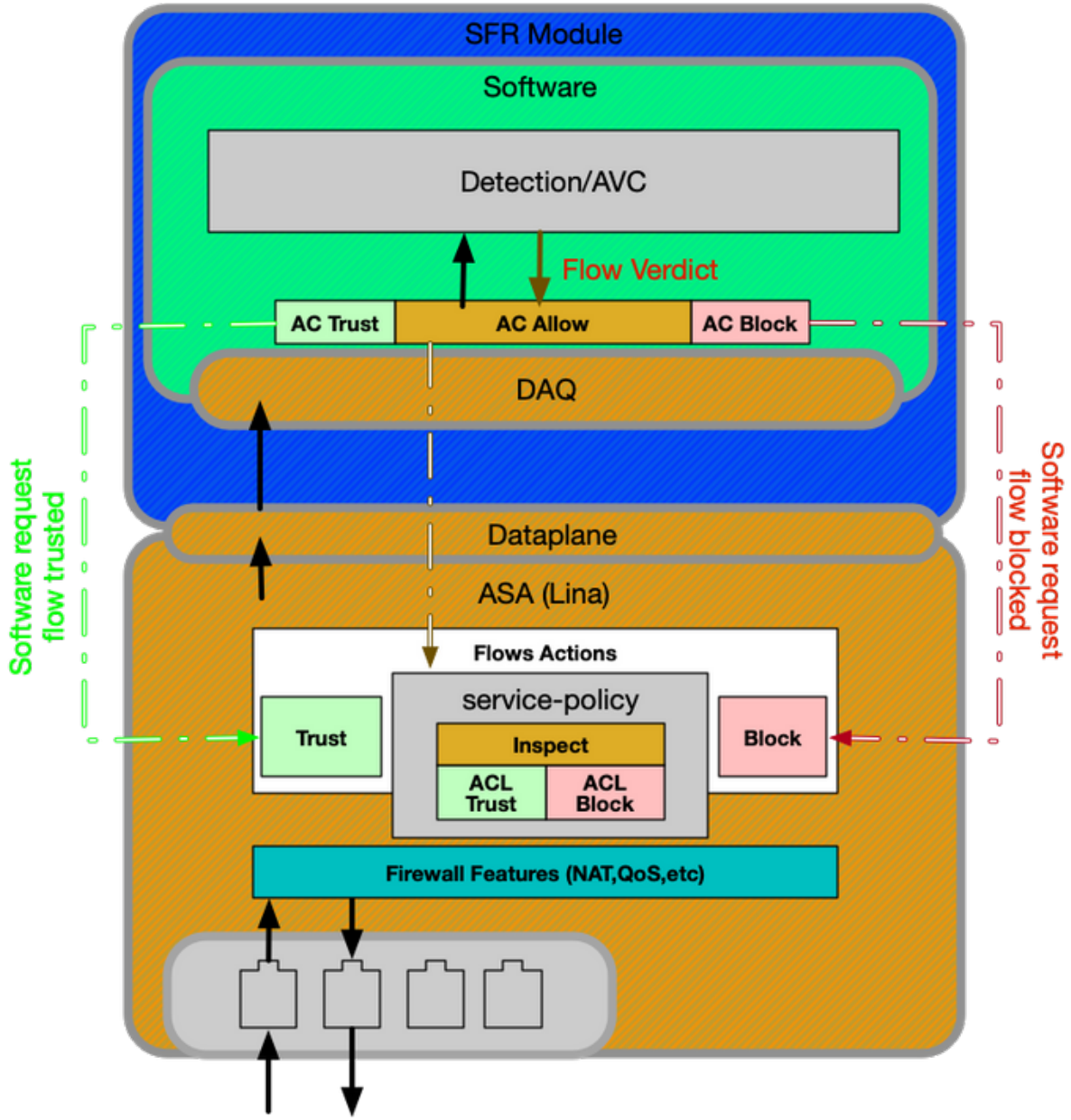
데이터 경로의 아키텍처 개요

다음 섹션에서는 다양한 Firepower 플랫폼의 아키텍처 데이터 경로를 살펴봅니다. 그런 다음, 아키텍처를 염두에 두고 Firepower 디바이스가 트래픽 플로우를 차단하고 있는지 여부를 신속하게 확인하는 방법을 살펴보겠습니다.

> **참고**: 이 문서에서는 레거시 Firepower 7000 및 8000 시리즈 디바이스와 NGIPS(비 FTD) 가상 플랫폼에 대해서는 다루지 않습니다. 이러한 플랫폼의 문제 해결에 대한 자세한 내용은 TechNotes 페이지를 참조하십시오.

FirePOWER 서비스(SFR 모듈)가 설치된 ASA 플랫폼

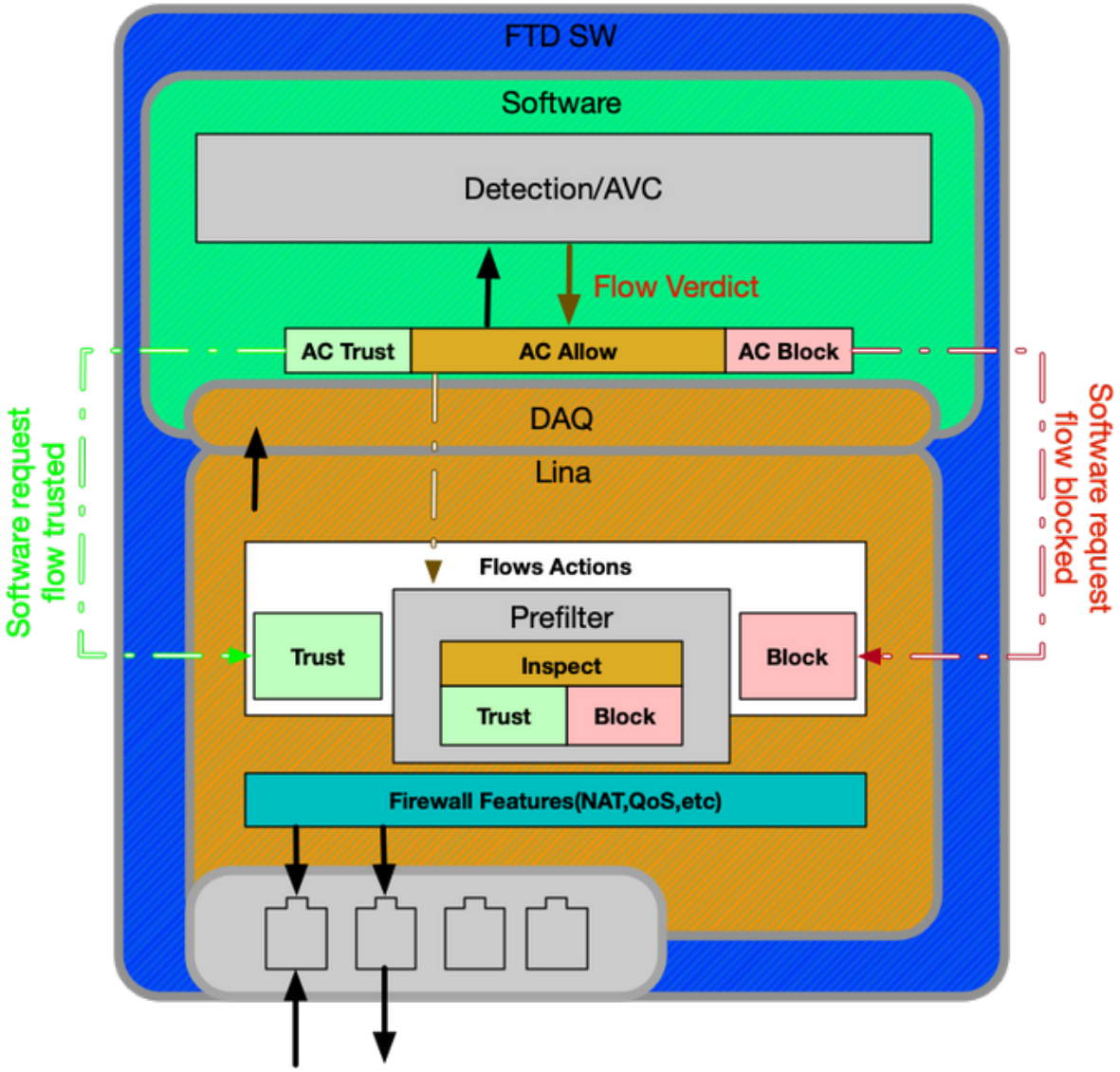
FirePOWER 서비스 플랫폼은 SFR 모듈이라고도 합니다. 이는 기본적으로 5500-X ASA 플랫폼에서 실행되는 가상 머신입니다.



ASA의 서비스 정책에 따라 SFR 모듈로 전송되는 트래픽이 결정됩니다. Firepower DAQ(Data Acquisition) 엔진과 통신하는 데 사용되는 데이터 플레인 레이어가 있으며, 이는 Snort가 이해할 수 있는 방식으로 패킷을 변환하는 데 사용됩니다.

ASA500-X 및 가상 FTD 플랫폼의 Firepower Threat Defense

FTD 플랫폼은 Lina(ASA) 및 Firepower 코드를 모두 포함하는 단일 이미지로 구성됩니다. 이 플랫폼과 ASA with SFR 모듈 플랫폼 간의 한 가지 주요 차이점은 Lina와 Snort 간의 통신이 훨씬 효율적이라는 점입니다.

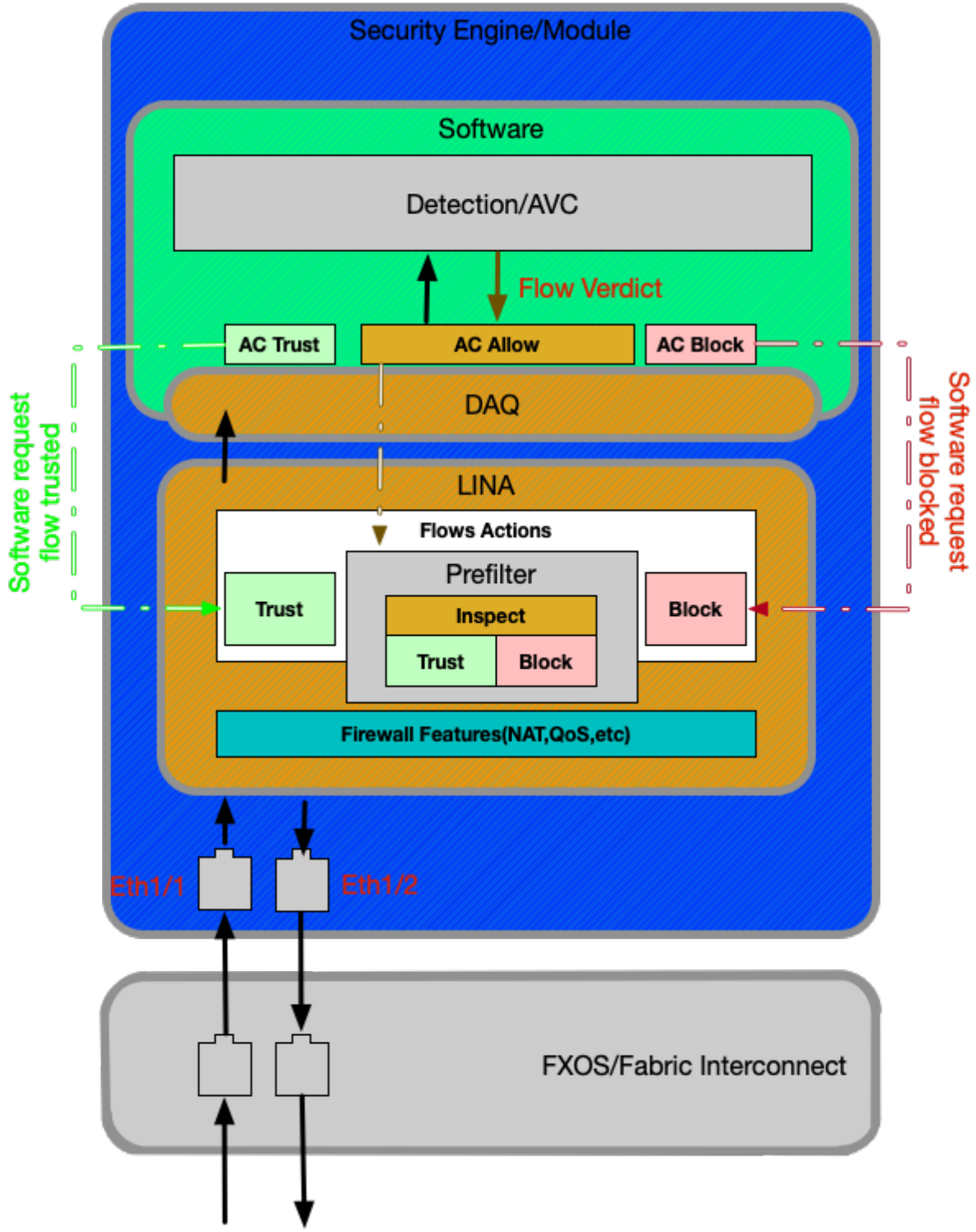


SSP 플랫폼의 FTD

SSP(Security Service Platform) 모델에서 FTD 소프트웨어는 FXOS(Firepower eXtensible Operating System) 플랫폼 위에서 실행되며, 이 플랫폼은 섀시 하드웨어를 관리하고 논리적 디바이스로 알려진 다양한 애플리케이션을 호스팅하는 데 사용되는 기본 OS(Operating System)입니다.

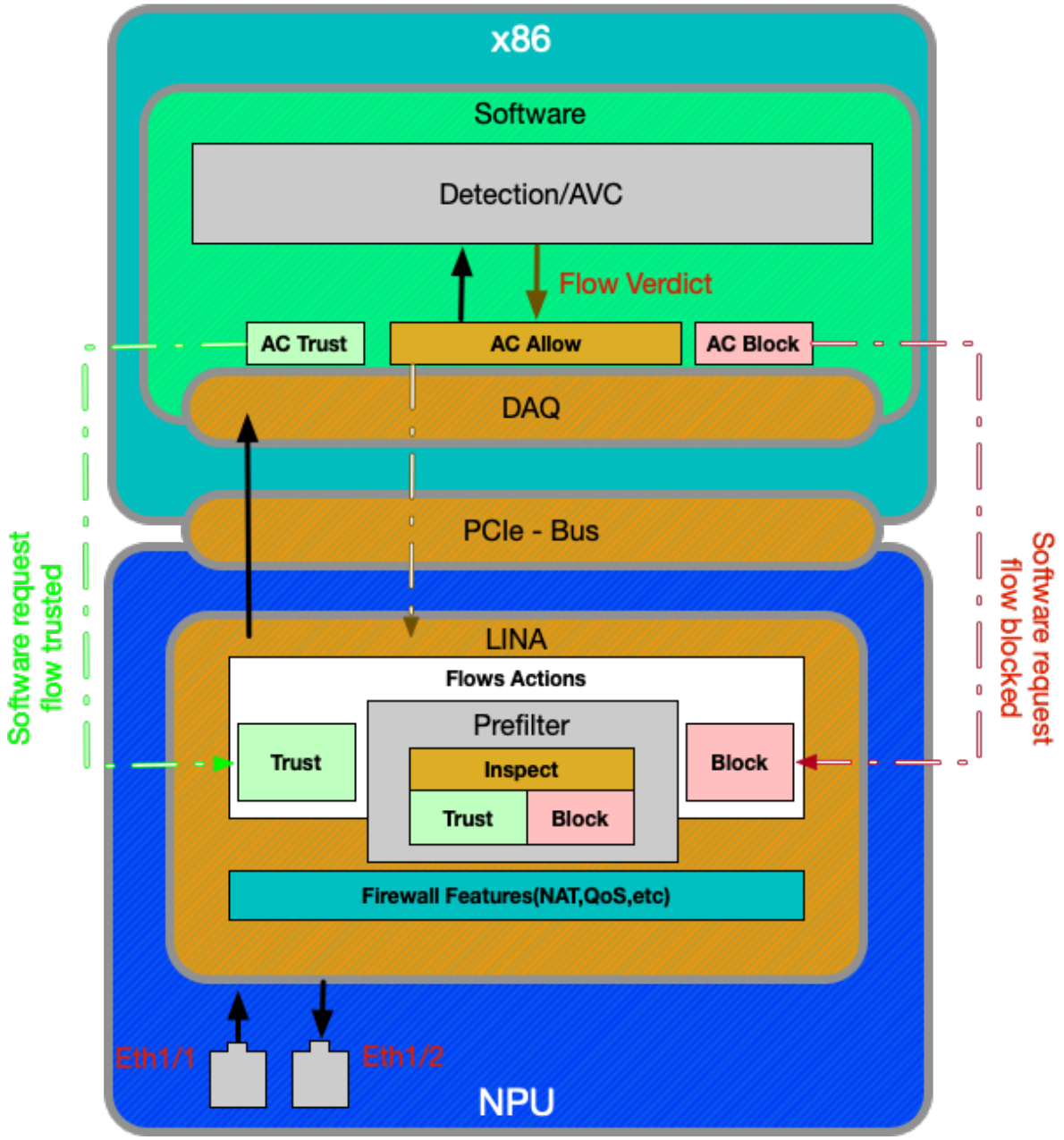
SSP 플랫폼 내에는 아래 다이어그램 및 설명에 나와 있는 것처럼 모델 간에 몇 가지 차이점이 있습니다.

Firepower 9300 및 4100 어플라이언스



Firepower 9300 및 4100 플랫폼에서 인그레스 및 이그레스 패킷은 FXOS 펌웨어(Fabric Interconnect)로 구동되는 스위치에 의해 처리됩니다. 그런 다음 패킷은 논리적 디바이스(이 경우 FTD)에 할당된 인터페이스로 전송됩니다. 그 후에는 비 SSP FTD 플랫폼과 패킷 처리가 동일합니다.

Firepower 2100 어플라이언스



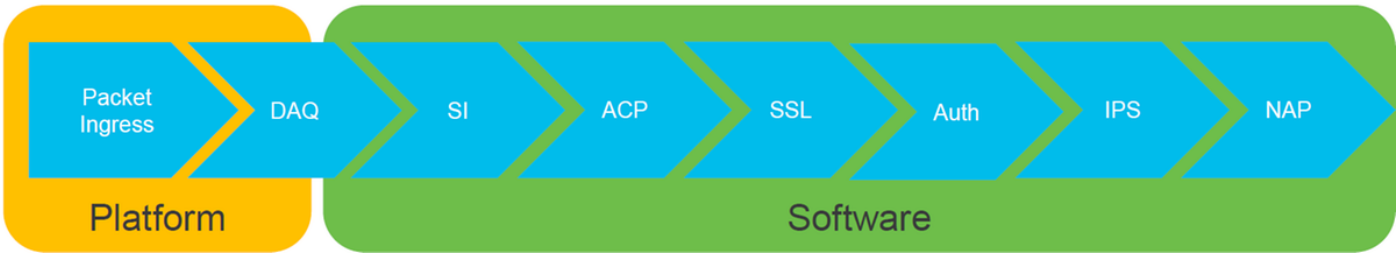
Firepower 2100 디바이스는 비 SSP FTD 플랫폼과 매우 유사하게 작동합니다. 여기에는 9300 및 4100 모델에 있는 패브릭 인터커넥트 레이어가 포함되지 않습니다. 그러나 다른 디바이스와 비교하여 2100 시리즈 디바이스에는 주요 차이점이 있는데, 이는 ASIC(Application-Specific Integrated Circuit)가 있다는 점입니다. 모든 기존 ASA 기능(Lina)은 ASIC에서 실행되며, 모든 NGFW(Next-Generation Firewall) 기능(Snort, URL 필터링 등)은 기존 x86 아키텍처에서 실행됩니다. 이 플랫폼에서 Lina와 Snort는 DMA(Direct Memory Access)를 사용하여 Snort로 가는 패킷을 대기열에 추가하는 다른 플랫폼과 달리 패킷 대기열을 통해 PCIe(Peripheral Component Interconnect Express)로 통신합니다.

참고: FPR-2100 플랫폼에서는 FTD 비 SSP 플랫폼의 문제 해결과 동일한 방법을 따릅니다.

Firepower 데이터 경로 문제 해결을 위한 권장 프로세스

지금까지는 Firepower 플랫폼에서 고유한 트래픽과 기본 데이터 경로 아키텍처를 식별하는 방법을 다루었으므로 이제 패킷을 삭제할 수 있는 특정 위치를 살펴보겠습니다. 데이터 경로 문서에서는 8가지 기본 구성 요소를 다루며, 이를 통해 체계적으로 문제 해결을 수행하여 발생 가능한 패킷 삭제를 확인할 수 있습니다. 그러한 구성 요소는 다음과 같습니다.

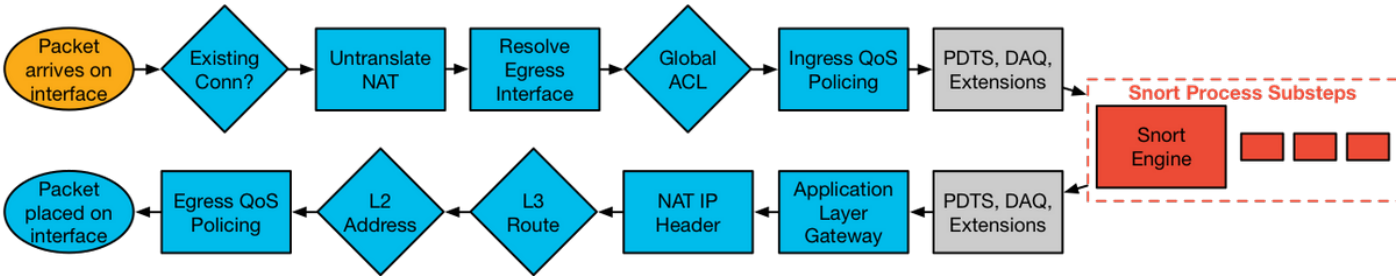
1. 패킷 인그레스
2. Firepower DAQ 레이어
3. 보안 인텔리전스
4. 액세스 제어 정책
5. SSL 정책
6. 활성 인증 기능
7. 침입 정책(IPS 규칙)
8. 네트워크 분석 정책(Snort 전처리기 설정)



참고: 이러한 구성 요소는 Firepower 처리의 정확한 작업 순서로 나열된 것이 아니라, 권장되는 문제 해결 워크플로 순서에 따라 정렬된 것입니다. 패킷 다이어그램의 실제 경로는 아래 그림을 참조하십시오.

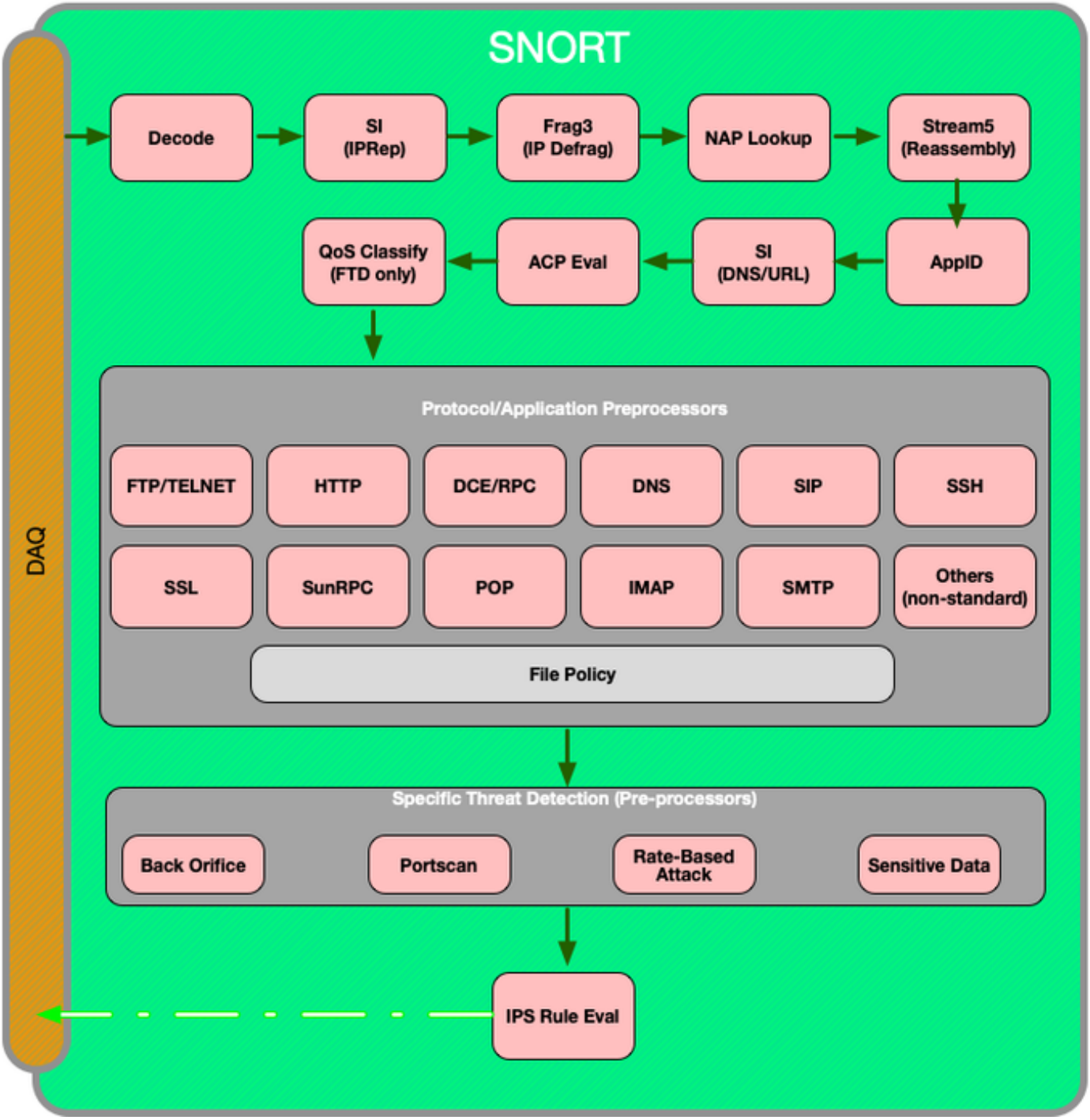
FTD를 통한 패킷의 실제 경로

아래 그림은 FTD를 통과하는 패킷의 실제 경로를 보여줍니다.



Snort 패킷 경로

아래 그림은 Snort 엔진을 통한 패킷의 경로를 보여줍니다.



패킷 인그레스 및 이그레스

첫 번째 데이터 경로 문제 해결 단계는 패킷 처리의 인그레스 또는 이그레스 단계에서 삭제가 발생하지 않는지 확인하는 것입니다. 패킷이 인그레스되고 있지만 이그레스되지 않는 경우라면 데이터 경로 내의 특정 위치에서 디바이스에 의해 패킷이 삭제되고 있음을 확인할 수 있습니다.

이 문서에서는 Firepower 시스템에서 패킷 인그레스 및 이그레스 문제를 해결하는 방법을 안내합니다.

Firepower DAQ 레이어

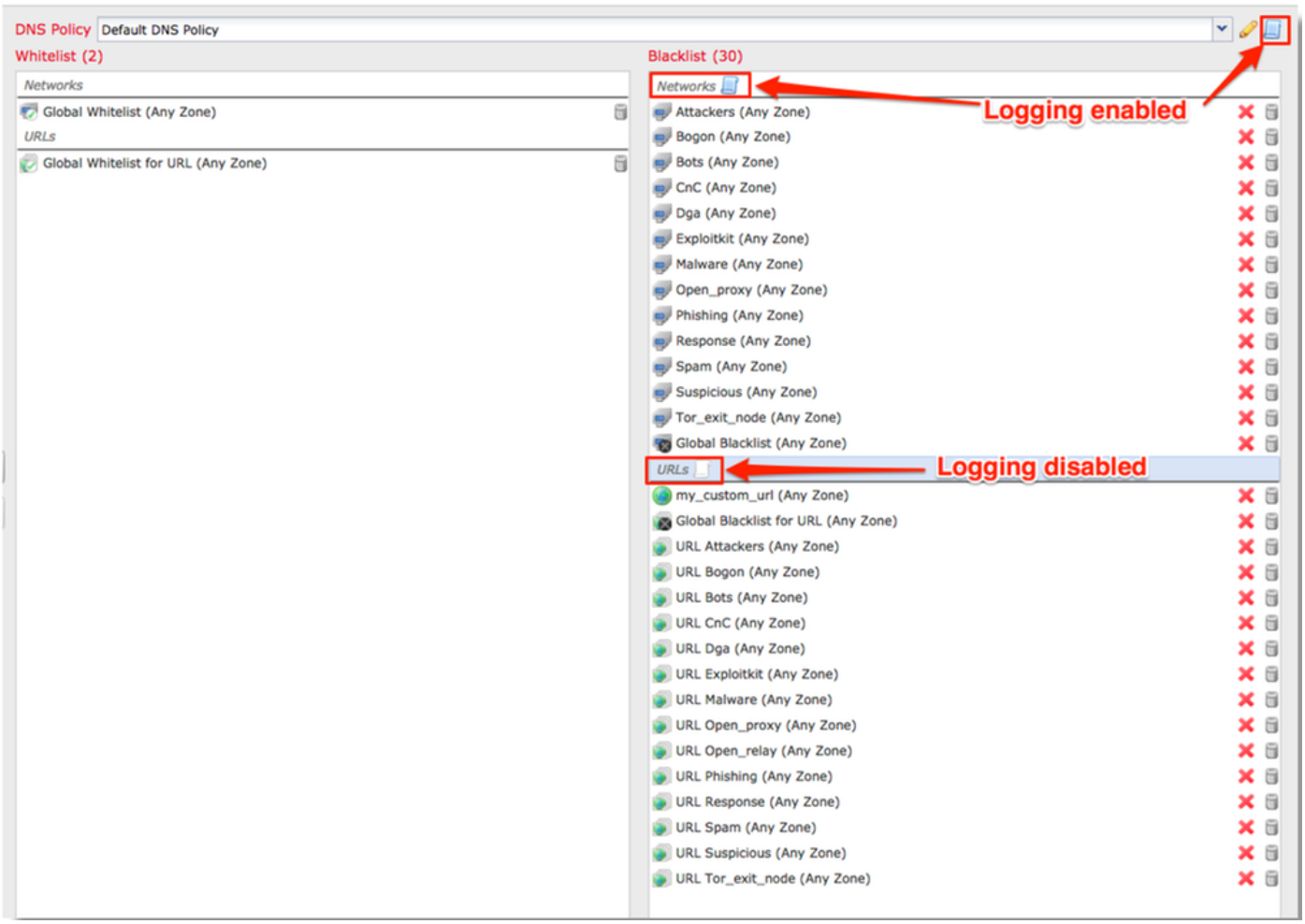
패킷이 인그레스되고 있지만 이그레스되고 있지 않은 것으로 확인된 경우, 데이터 경로 문제 해결의 다음 단계로 Firepower DAQ(Data Acquisition) 레이어에서 문제의 트래픽이 검사를 위해 Firepower로 전송되고 있는지, 만약 그렇다면 삭제 또는 수정되는 중인지 확인해야 합니다.

이 문서에서는 Firepower에서 트래픽의 초기 처리 문제를 해결하는 방법과 어플라이언스 전체에서 트래픽이 이동하는 경로를 살펴봅니다.

또한 Firepower 디바이스를 완전히 우회하여 Firepower 구성 요소가 트래픽 문제의 원인인지 여부를 확인하는 방법도 다룹니다.

보안 인텔리전스

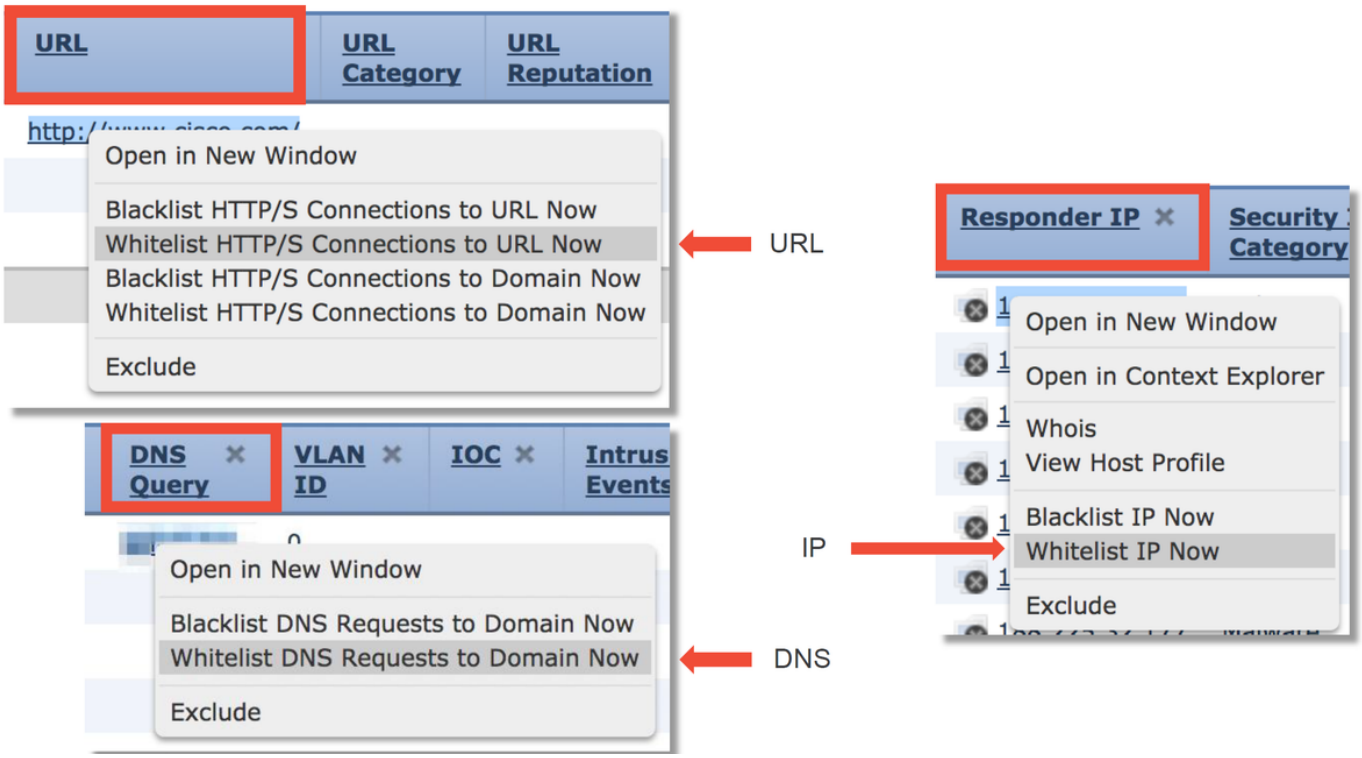
보안 인텔리전스는 트래픽을 검사하는 Firepower 내의 첫 번째 구성 요소입니다. 로깅이 활성화되어 있으면 이 레벨의 차단은 쉽게 확인할 수 있습니다. 이는 FMC GUI에서 **정책 > 액세스 제어 > 액세스 제어 정책**으로 이동하여 확인할 수 있습니다. 해당 정책 옆에 있는 편집 아이콘을 클릭한 후 **보안 인텔리전스** 탭으로 이동합니다.



로깅이 활성화되어 있으면 **분석 > 연결 > 보안 인텔리전스 이벤트**에서 보안 인텔리전스 이벤트를 볼 수 있습니다. 트래픽이 차단되는 이유가 명확해야 합니다.

First Packet	Last Packet	Action	Reason	Initiator IP	Responder IP	Security Intelligence Category
2017-05-16 17:00:16		Domain Not Found	DNS Block	192.168.1.95		DNS Response
2017-05-16 16:57:50	2017-05-16 16:57:50	Block	URL Block	192.168.1.95	10.83.48.40	my_custom_url
2017-05-16 16:50:05		Block	IP Block	192.168.1.95		Malware

빠른 완화 단계로, 보안 인텔리전스 기능에 의해 차단되는 IP, URL 또는 DNS 쿼리를 마우스 오른쪽 버튼으로 클릭하고 화이트리스트 옵션을 선택할 수 있습니다.



블랙리스트에 무언가 잘못 추가된 것으로 의심되거나 평판 변경을 요청하려는 경우 다음 링크에서 Cisco Talos를 사용하여 직접 티켓을 열 수 있습니다.

https://www.talosintelligence.com/reputation_center/support

또한 차단된 항목에 대해 보고하기 위해 TAC에 데이터를 제공할 수 있으며, 블랙리스트에서 항목을 제거할 수도 있습니다.

보안 인텔리전스 구성 요소에 대한 심층적 문제 해결은 관련 데이터 경로 문제 해결 문서를 참조하십시오.

액세스 제어 정책

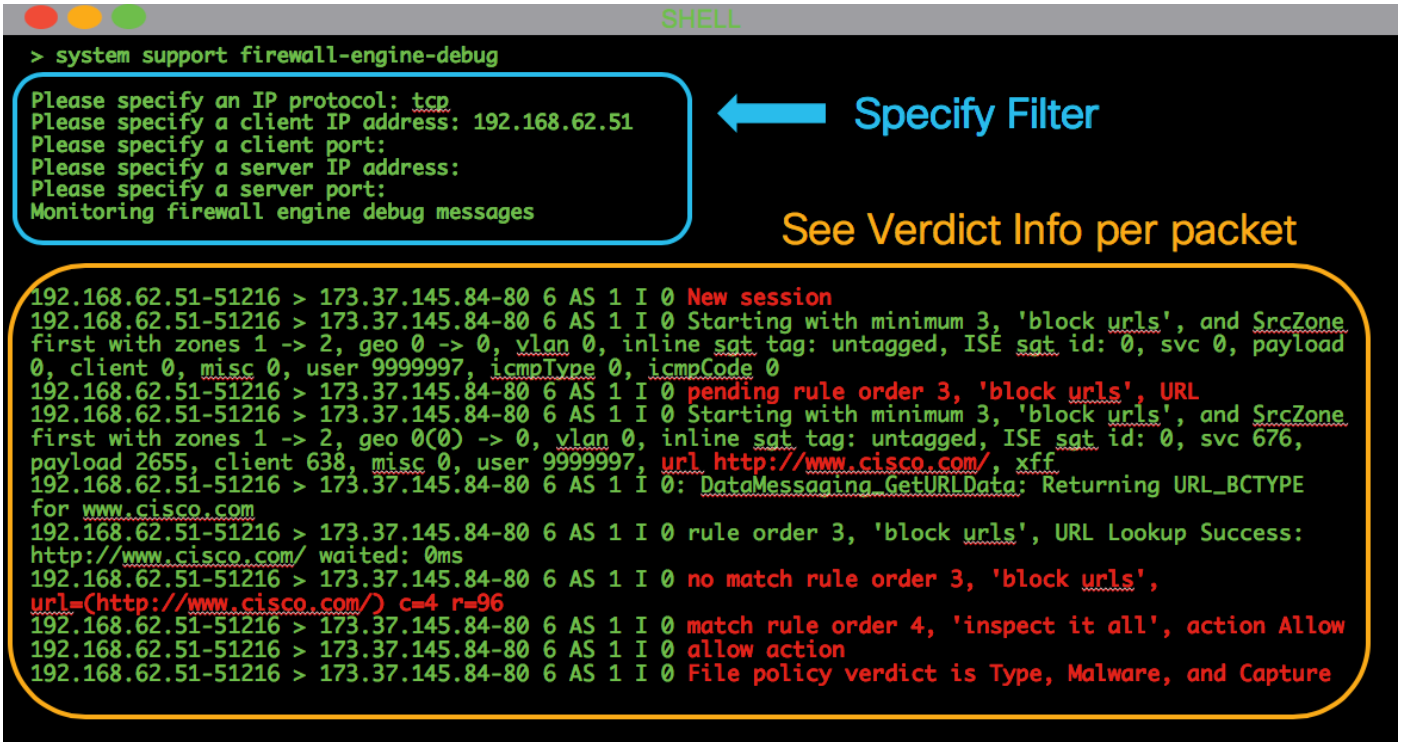
보안 인텔리전스 기능이 트래픽을 차단하지 않는 것으로 확인된 경우, 다음으로 권장되는 단계는 액세스 제어 정책 규칙의 문제를 해결하여 '차단' 작업이 포함된 규칙이 트래픽을 삭제하는지 확인하는 것입니다.

"firewall-engine-debug" 명령을 사용하여 시작하거나 추적을 사용하여 캡처하는 것이 좋습니다. 일반적으로 이러한 툴은 즉시 답변을 제공하고 트래픽이 적용되는 규칙과 이유를 알려줍니다.

- 다음 명령을 통해 Firepower CLI에서 디버깅을 실행하여 어떤 규칙이 트래픽을 차단하고 있는지 확인합니다(최대한 많은 매개변수를 입력해야 함). **> system support firewall-engine-debug**

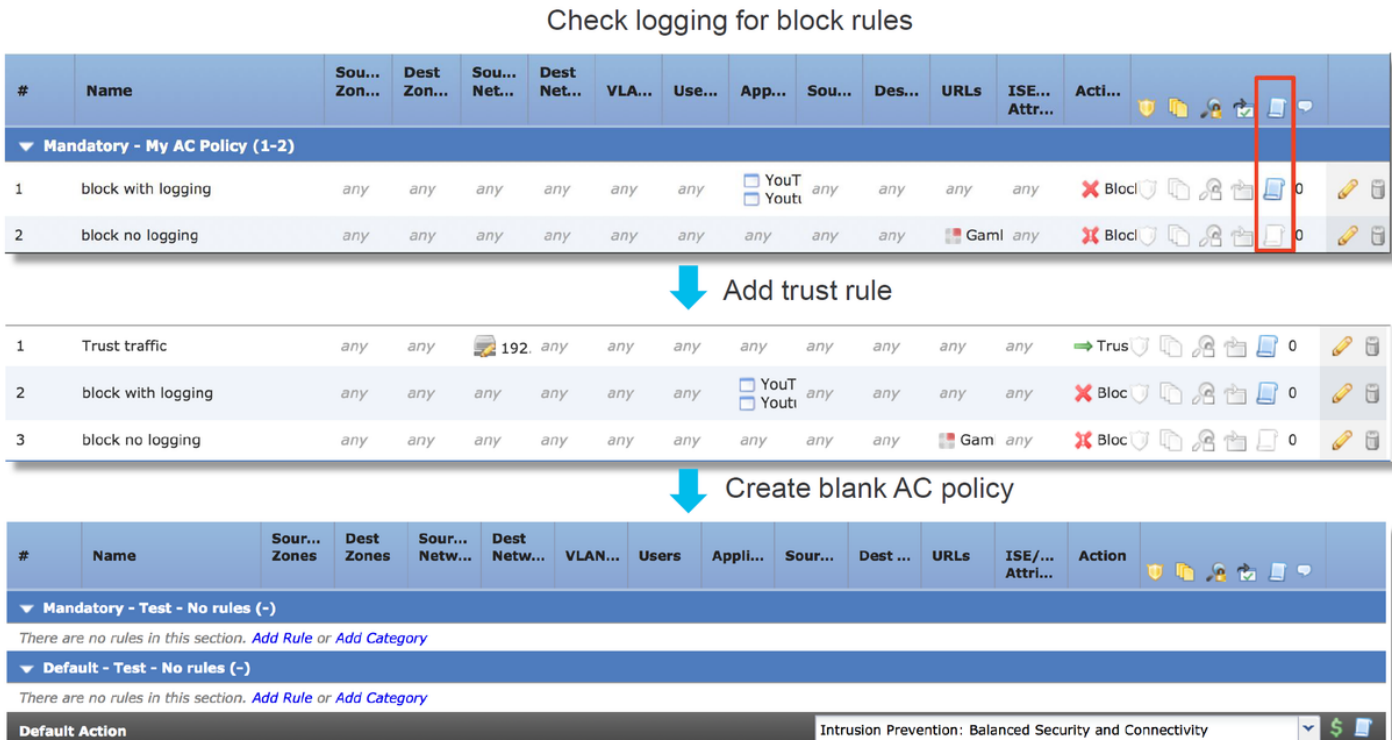
- 분석을 위해 TAC에 디버그 출력을 제공할 수 있습니다.

다음은 '허용' 작업이 있는 액세스 제어 규칙과 일치하는 트래픽에 대한 규칙 평가를 보여주는 샘플 출력입니다.



일치하는 AC(액세스 제어) 규칙을 확인할 수 없거나 위의 툴을 사용하여 AC 정책이 문제인지 확인할 수 없는 경우, 다음 몇 가지 기본 단계를 수행하여 액세스 제어 정책 문제 해결을 수행합니다(이러한 옵션은 정책 변경/구축이 필요하므로 첫 번째 옵션이 아님).

- '차단' 작업이 있는 규칙에 대한 로깅 활성화
- 트래픽에 대한 연결 이벤트가 여전히 표시되지 않고 차단되는 경우, 다음 완화 단계로 해당 트래픽에 대한 신뢰 규칙을 생성합니다.
- 트래픽에 대한 신뢰 규칙으로 여전히 문제가 해결되지 않지만, AC 정책에 결함이 있는 것으로 계속 의심되는 경우 그다음으로는 가능하다면 '모든 트래픽 차단' 이외의 기본 작업을 사용하여 새 빈 액세스 제어 정책을 생성합니다.

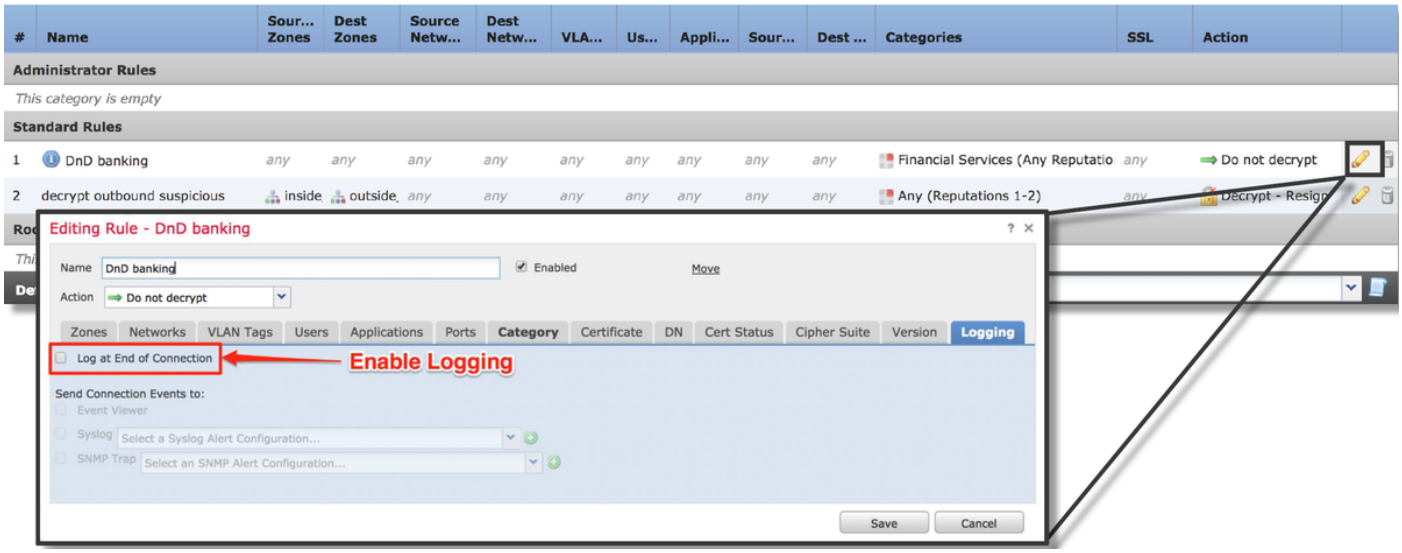


액세스 제어 정책에 대한 심층적 문제 해결은 관련 데이터 경로 문제 해결 문서를 참조하십시오.

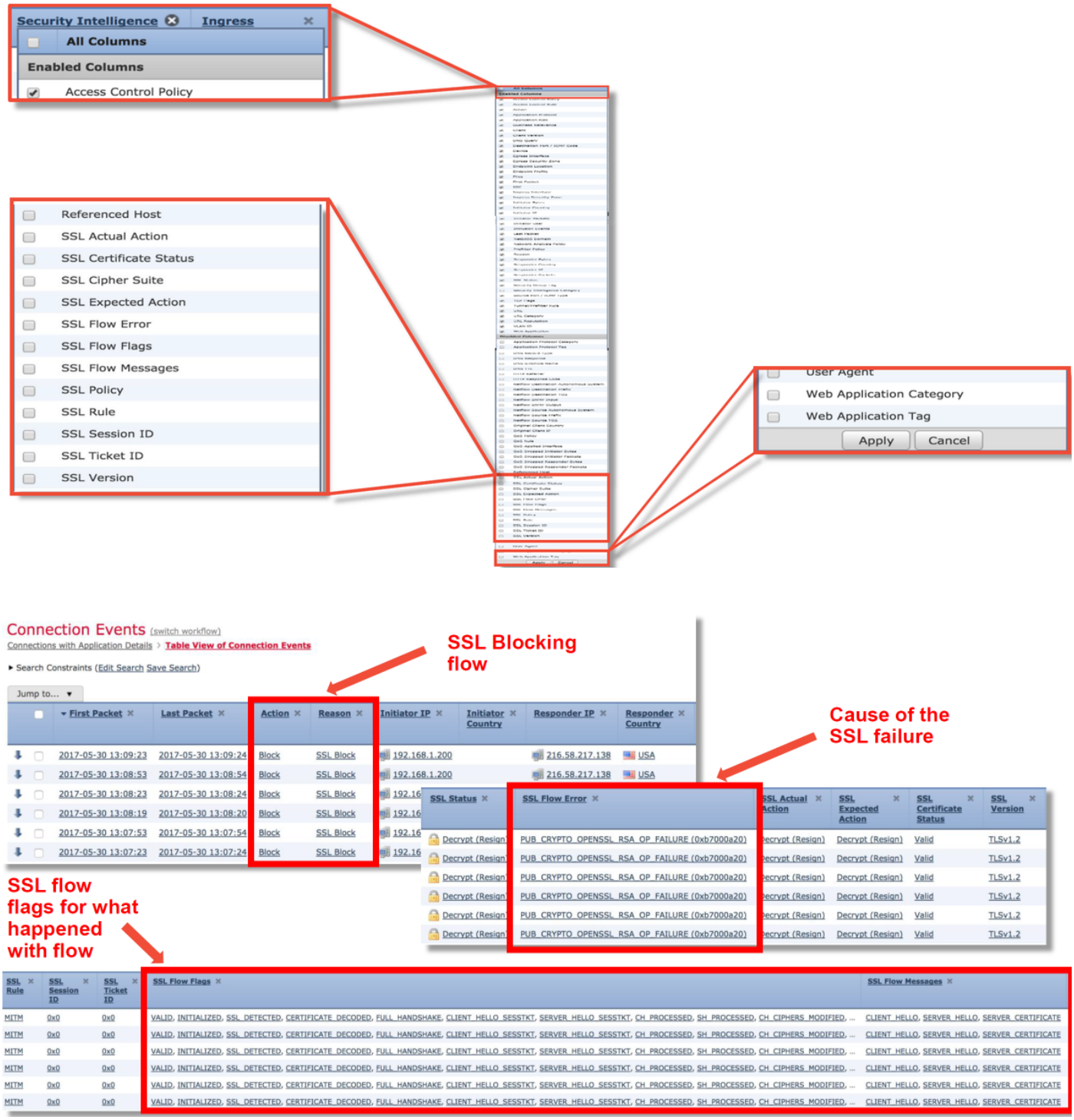
SSL 정책

SSL 정책을 사용 중인 경우 해당 정책에서 트래픽을 차단할 수 있습니다. 다음은 SSL 정책 문제 해결을 위한 몇 가지 기본 단계입니다.

- '기본 작업'을 포함하여 모든 규칙에 대한 로깅 활성화



- 암호 해독 불가 작업 탭에서 트래픽 차단 옵션이 설정되어 있는지 확인
- 연결 이벤트 섹션에서 이름에 'SSL'이 포함된 모든 필드 확인
  대부분은 기본적으로 비활성화되어 있으며 연결 이벤트 뷰어에서 열 이름 옆에 있는 십자 표시를 클릭하여 활성화해야 함



- 완화 단계로서 암호 해독 안 함을 기본 작업으로 지정하여 빈 SSL 정책 생성
- 완화 단계로서 액세스 제어 정책에서 SSL 정책 제거
  이는 고급 탭에서 설정됨

SSL 정책이 트래픽을 삭제하는 것으로 의심되는 경우 정책 설정과 함께 연결 이벤트를 TAC로 전송할 수 있습니다.

SSL 정책에 대한 보다 심층적인 문제 해결은 관련 데이터 경로 문제 해결 문서를 참조하십시오.

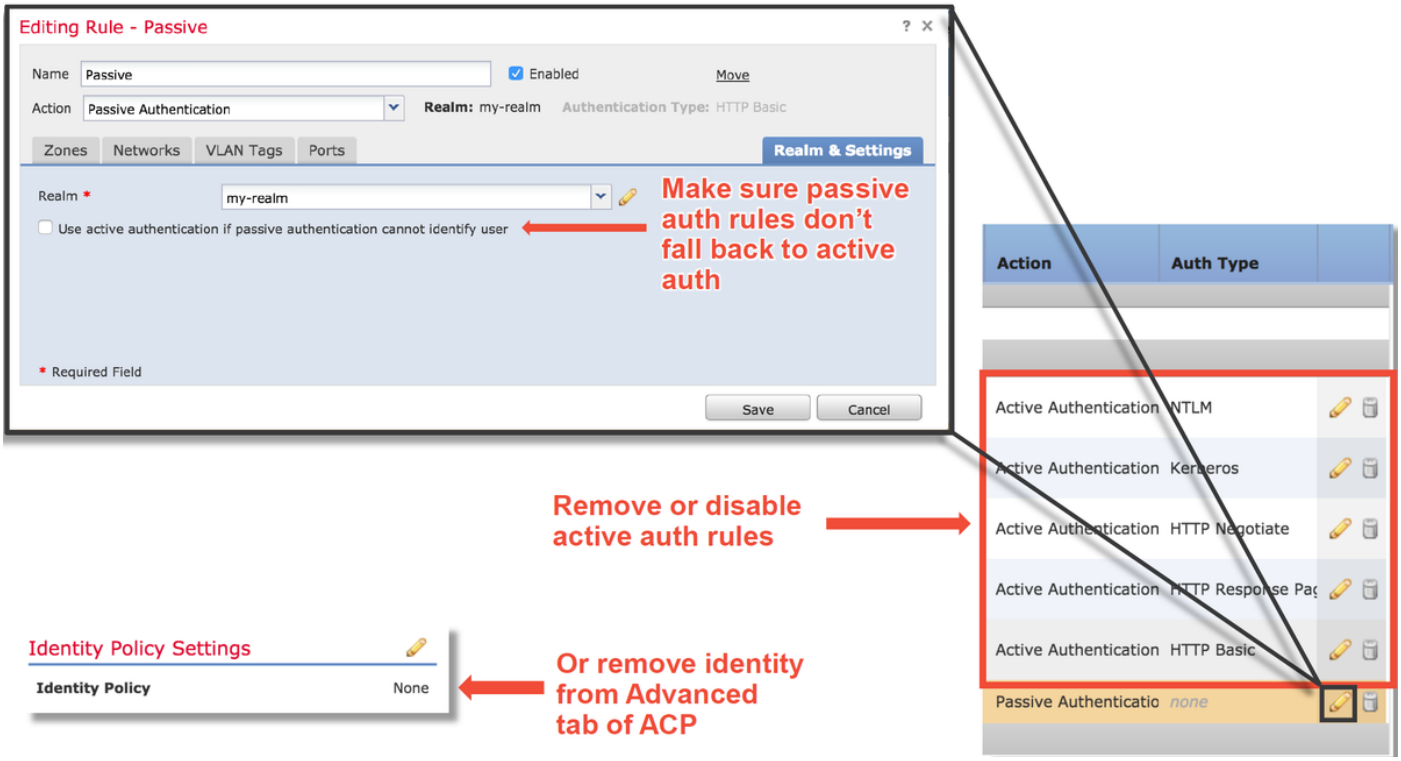
활성 인증

ID 정책에서 활성 인증을 사용할 경우, 어떤 문제가 발생하면 활성 인증에서 허용해야 할 트래픽을 삭제할 수 있습니다. 활성 인증 기능 자체는 모든 HTTP/HTTPS 트래픽에 직접적으로 영향을 줄 수

있는데, 이는 사용자를 인증해야 하는 경우 이 모든 것이 HTTP 프로토콜을 통해서만 이루어지기 때문입니다. 이는 사용자를 기준으로 차단하는 특정 액세스 제어 규칙이 없고 사용자가 FTD의 활성 인증 서비스를 통해 인증할 수 없는 경우를 제외하고 활성 인증이 다른 네트워크 서비스(예: DNS, ICMP 등)에 영향을 미치지 않아야 한다는 것을 의미합니다. 하지만 이는 활성 인증 기능의 직접적인 문제가 아니라 사용자가 인증할 수 없고 인증되지 않은 사용자를 차단하는 정책을 가지고 있기 때문에 발생하는 문제입니다.

빠른 완화 단계는 '활성 인증' 작업을 사용하는 ID 정책 내에서 모든 규칙을 비활성화하는 것입니다.

또한 '패시브 인증' 작업이 포함된 규칙에서 '패시브 인증이 사용자를 식별할 수 없는 경우 활성 인증 사용' 옵션이 선택되어 있지 않은지 확인합니다.



활성 인증에 대한 보다 심층적인 문제 해결은 관련 데이터 경로 문제 해결 문서를 참조하십시오.

침입 정책

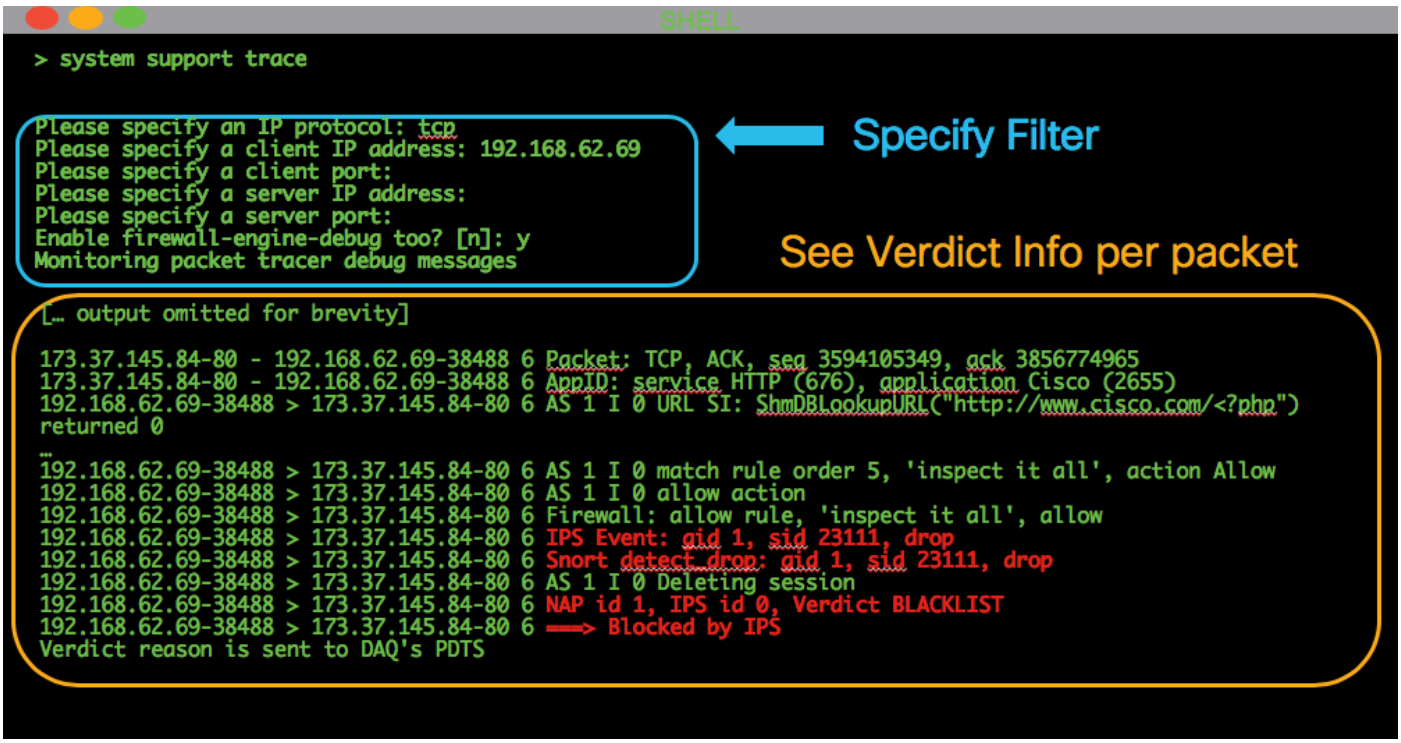
침입 정책이 트래픽을 삭제하거나 네트워크 레이턴시를 유발할 수 있습니다. 침입 정책은 액세스 제어 정책 내의 다음 세 위치 중 하나에서 사용할 수 있습니다.

- 액세스 제어 규칙의 "검사" 탭
- 기본 작업
- 고급 탭의 **네트워크 분석 및 침입 정책 > 액세스 제어 규칙이 결정되기 전에 사용되는 침입 정책** 섹션

침입 정책 규칙이 트래픽을 차단하고 있는지 확인하려면 FMC의 **분석 > 침입 > 이벤트** 페이지로 이동합니다. **침입 이벤트의 테이블 보기** 보기는 이벤트와 관련된 호스트에 대한 정보를 제공합니다. 이벤트 분석과 관련된 정보는 관련 데이터 경로 문제 해결 문서를 참조하십시오.

IPS(침입 정책 서명)가 트래픽을 차단하는지 확인하는 첫 번째 권장 단계는 FTD의 CLI에서 **> 시스템 지원 추적** 기능을 활용하는 것입니다. 이 디버그 명령은 firewall-engine-debug와 유사한 방식으로 작동하며, 추적과 함께 firewall-engine-debug를 활성화할 수도 있습니다.

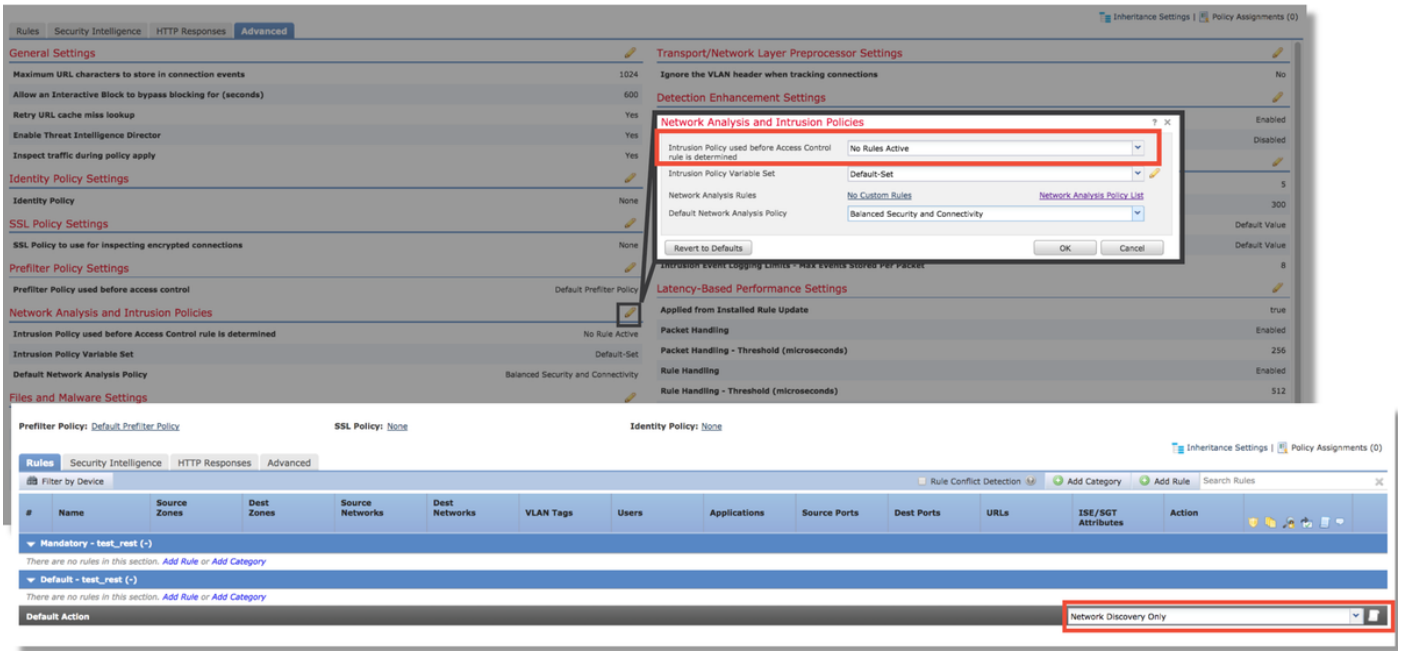
아래 그림은 침입 규칙으로 인해 패킷이 차단된 결과가 표시된 시스템 지원 추적 툴 사용의 예를 보여줍니다. 이는 GID(Group Identifier), SID(Signature Identifier), NAP(Network Analysis Policy) ID 및 IPS ID와 같은 모든 세부 정보를 제공하므로 이 트래픽을 차단하는 정책/규칙을 정확히 확인할 수 있습니다.



IPS가 추적 출력에서 차단하고 있는지 확인할 수는 없지만 맞춤형 침입 정책으로 인해 IPS가 삭제하고 있는 것으로 의심되는 경우, 침입 정책을 "보안 및 연결성의 균형 유지" 정책 또는 "보안보다 연결성 우선" 정책으로 대체할 수 있습니다. 이러한 정책은 시스코에서 제공하는 침입 정책입니다. 이렇게 변경하여 문제가 해결되면 TAC에서 이전에 사용된 맞춤형 침입 정책의 문제 해결을 할 수 있습니다. 기본 시스코 정책을 이미 사용 중인 경우에는 기본 정책을 덜 안전한 정책으로 변경해 볼 수 있습니다. 이러한 정책에는 규칙이 더 적으므로 범위를 좁히는 데 도움이 될 수 있습니다. 예를 들어 트래픽이 차단되고 균형 유지 정책을 사용 중인 경우, 보안보다 연결성 우선 정책으로 전환하면 문제가 해결됩니다. 균형 유지 정책에 보안보다 연결성 우선 정책에서 삭제하도록 설정되지 않은 트래픽을 삭제하는 규칙이 있었을 수 있습니다.

모든 침입 정책 검사 차단 가능성을 제거하기 위해 액세스 제어 정책 내에서 다음을 변경할 수 있습니다(보안 효능을 변경하지 않도록 가능한 한 적게 변경하는 것이 좋으며, 전체 정책에서 IPS를 비활성화하는 것이 아니라 해당 트래픽에 대한 대상 지정 AC 규칙을 만드는 것이 권장됨).

- 모든 액세스 제어 규칙(또는 영향을 받는 특정 트래픽이 일치하는 규칙만)에서 검사 탭의 침입 정책을 제거합니다.
- 고급 탭의 **네트워크 분석 및 침입 정책 > 액세스 제어 규칙 결정 전에 사용되는 침입 정책** 섹션에서 "활성 규칙 없음" 정책을 선택합니다.



그래도 문제가 해결되지 않으면 네트워크 분석 정책 문제 해결을 진행합니다.

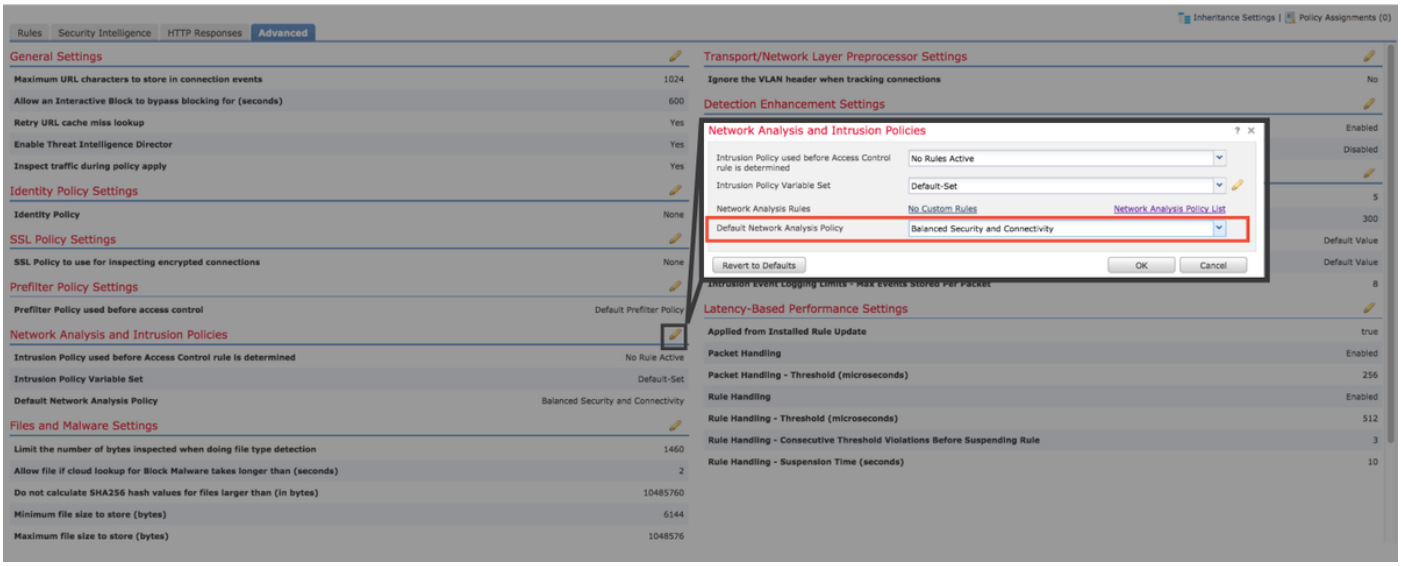
침입 정책 기능에 대한 보다 심층적인 문제 해결은 관련 데이터 경로 문제 해결 문서를 참조하십시오.

네트워크 분석 정책

NAP(네트워크 분석 정책)에는 Firepower 전처리기 설정이 포함되어 있으며, 이 중 일부에서 트래픽을 삭제할 수 있습니다. 이 문제 해결을 위한 첫 번째 권장 단계는 IPS 문제 해결의 경우와 동일합니다. 즉, **> 시스템 지원 추적** 툴을 사용하여 Snort에서 트래픽을 차단하는 항목을 찾는 것입니다. 이 툴 및 사용 예에 대한 보다 자세한 내용은 위의 "침입 정책" 섹션을 참조하십시오.

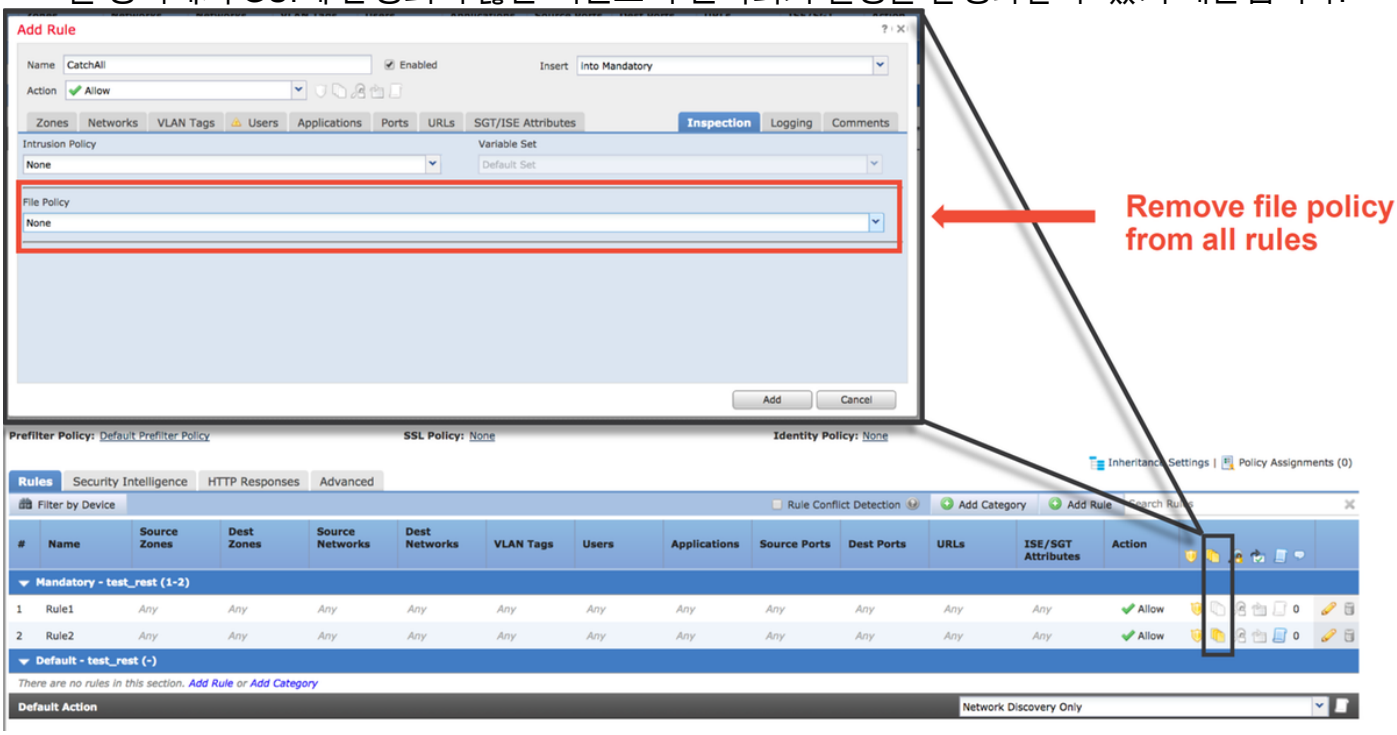
NAP에서 발생할 수 있는 문제를 신속하게 완화하기 위해 다음 단계를 수행할 수 있습니다.

- 맞춤형 NAP를 사용 중인 경우 "보안 및 연결성 균형 유지" 또는 "보안보다 연결성 우선" 정책으로 교체합니다.



- "맞춤형 규칙"을 사용 중인 경우 NAP를 위에서 언급한 기본값 중 하나로 설정해야 합니다.
- 액세스 제어 규칙에서 파일 정책을 사용하는 경우 해당 규칙을 일시적으로 제거합니다. 이는 파

일 정책에서 GUI에 반영되지 않는 백엔드의 전처리기 설정을 활성화할 수 있기 때문입니다.



이 문서에서는 네트워크 분석 정책 기능의 심층적인 문제 해결을 살펴볼 수 있습니다.

관련 정보

Firepower 설명서 링크

https://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html

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.