

Firepower 데이터 경로 문제 해결 8단계: 네트워크 분석 정책

목차

- [소개](#)
- [사전 요구 사항](#)
- [네트워크 분석 정책 기능 문제 해결](#)
- ["추적" 톨을 사용하여 전처리기 삭제 찾기\(FTD만 해당\)](#)
- [NAP 설정 확인](#)
- [NAP 설정 보기](#)
- [자동 삭제를 유발할 수 있는 NAP 설정](#)
- [백엔드 설정 확인](#)
- [대상 지정 NAP 생성](#)
- [오탐 분석](#)
- [완화 단계](#)
- [TAC에 제공할 데이터](#)

소개

이 문서는 Firepower 시스템의 데이터 경로 문제를 체계적으로 해결하여 Firepower의 구성 요소가 트래픽에 영향을 미치는지 여부를 확인하는 방법을 설명하는 일련의 문서 중 일부입니다. Firepower 플랫폼의 아키텍처에 대한 자세한 내용은 [개요 문서](#)를 참조하고 다른 데이터 경로 문제 해결 문서에 대한 링크를 참조하십시오.

이 문서에서는 Firepower 데이터 경로 문제 해결의 8단계인 네트워크 분석 정책 기능을 다룹니다.



사전 요구 사항

- 이 문서는 모든 Firepower 플랫폼에 적용됩니다. 추적 기능은 FTD(Firepower Threat Defense) 플랫폼 소프트웨어 버전 6.2.0 이상에서만 사용할 수 있습니다.
- 필수는 아니지만, 오픈 소스 Snort에 대한 지식이 있는 것이 유용합니다. 오픈 소스 Snort에 대한 자세한 내용은 <https://www.snort.org/>를 참조하십시오.

네트워크 분석 정책 기능 문제 해결

NAP(Network Analysis Policy)에는 식별된 애플리케이션을 기반으로 트래픽에 대한 검사를 수행하는 Ssnort 전처리기 설정이 포함되어 있습니다. 전처리기에서 설정에 따라 트래픽을 삭제할 수 있습니다. 이 문서에서는 NAP 설정을 확인하고 전처리기 삭제를 확인하는 방법을 설명합니다.

참고: 전처리기 규칙에는 '1' 또는 '3'(예: 129, 119, 124) 이외의 생성기 ID(GID)가 있습니다. 전처리기 매핑에 대한 GID의 자세한 내용은 FMC [설정 가이드](#)에서 확인할 수 있습니다.

"추적" 톨을 사용하여 전처리기 삭제 찾기(FTD만 해당)

시스템 지원 추적 톨을 전처리기 레벨에서 수행되는 삭제 탐지에 사용할 수 있습니다.

아래 예에서는 TCP 표준화 전처리기에서 변칙을 탐지했습니다. 따라서 TCP 스트림 내에서 누락된 타임스탬프를 찾는 규칙 129:14에 의해 트래픽이 삭제됩니다.

```
> system support trace

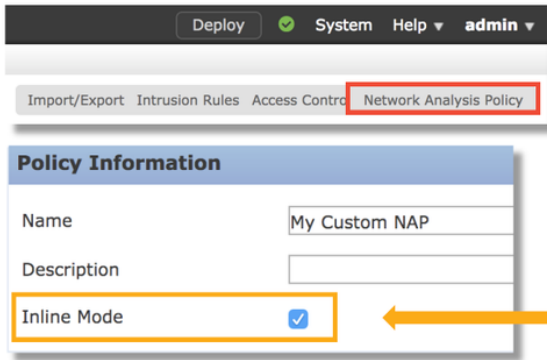
[omitted for brevity...]

172.16.111.226-51174 - 50.19.123.95-443 6 Packet: TCP, ACK, seq 3849839667, ack 1666843207
172.16.111.226-51174 > 50.19.123.95-443 6 Stream: TCP normalization error in timestamp, window, seq, ack, fin, flags, or
unexpected data, drop
172.16.111.226-51174 - 50.19.123.95-443 6 ApplID: service unknown (0), application unknown (0)
172.16.111.226-51174 > 50.19.123.95-443 6 AS 4 | 0 Starting with minimum 3, 'block urls', and SrcZone first with zones -1 -> -1, geo 0 ->
0, vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
172.16.111.226-51174 > 50.19.123.95-443 6 Firewall: starting rule matching, zone -1 -> -1, geo 0 -> 0, vlan 0, sgt 65535, user 9999997,
icmpType 0, icmpCode 0
172.16.111.226-51174 > 50.19.123.95-443 6 AS 4 | 0 pending rule order 3, 'block urls', URL
172.16.111.226-51174 > 50.19.123.95-443 6 Firewall: pending rule-matching, 'block urls', pending URL
172.16.111.226-51174 > 50.19.123.95-443 6 Snort: processed decoder alerts or actions queue, drop
172.16.111.226-51174 > 50.19.123.95-443 6 IPS Event: gid 129, sid 14, drop
172.16.111.226-51174 > 50.19.123.95-443 6 NAP id 1, IPS id 0, Verdict BLOCK
172.16.111.226-51174 > 50.19.123.95-443 6 ==> Blocked by Stream
```

참고: TCP 스트림 설정 전처리기에서 트래픽을 삭제하더라도 인라인 표준화 전처리기도 활성화되어 있으므로 그렇게 할 수 있습니다. 인라인 표준화에 대한 자세한 내용은 이 [문서](#)를 참조하십시오.

NAP 설정 확인

FMC(Firepower Management Center) UI의 정책 > 액세스 제어 > 침입에서 NAP를 볼 수 있습니다. 그런 다음, 오른쪽 상단에서 네트워크 분석 정책 옵션을 클릭하면 NAP를 확인하여 새 NAP를 생성하고 기존 NAP를 수정할 수 있습니다.



Edit or create a Network Analysis Policy

Uncheck this box to disable Inline Mode

Inline Result	Source IP	Destination IP	Source Port / ICMP Type	Destination Port / ICMP Code	Message
	172.16.111.226	50.19.123.95	51177 / tcp	443 (https) / tcp	STREAM5_NO_TIMESTAMP (129:14:2)
	172.16.111.226	50.19.123.95	51174 / tcp	443 (https) / tcp	STREAM5_NO_TIMESTAMP (129:14:2)

Inline Mode disabled = No Inline Result

Inline Mode enabled = "Dropped" Inline Result

위의 그림에 나와 있는 것처럼 NAP에는 침입 정책의 "인라인 시 삭제" 옵션에 해당하는 "인라인 모드" 기능이 포함되어 있습니다. NAP가 트래픽을 삭제하지 못하도록 하는 빠른 완화 단계는 인라인 모드를 선택 취소하는 것입니다. NAP에 의해 생성된 침입 이벤트는 인라인 모드가 비활성화된 인라인 결과 탭에 아무것도 표시하지 않습니다.

NAP 설정 보기

NAP 내에서 현재 설정을 볼 수 있습니다. 여기에는 활성화된 총 전처리기가 포함되며 그 뒤에

아래 그림과 같이 기본 설정이 아닌 설정으로 활성화된 전처리기(수동으로 조정된 전처리기) 및 기본 설정으로 활성화된 전처리기가 있습니다.

Edit Policy: My Custom NAP

View preprocessors → Settings

Currently Enabled → [List of preprocessors]

Enabled with non-default settings → [List of preprocessors]

Enabled with default settings → [List of preprocessors]

Settings

Application Layer Preprocessors

- DCE/RPC Configuration: Enabled
- DNS Configuration: Enabled
- FTP and Telnet Configuration: Enabled
- HTTP Configuration: Enabled
- Sun RPC Configuration: Enabled
- SIP Configuration: Enabled
- GTP Command Channel Configuration: Enabled
- IMAP Configuration: Disabled
- POP Configuration: Disabled
- SMTP Configuration: Enabled
- SSH Configuration: Enabled
- SSL Configuration: Enabled

SCADA Preprocessors

- Modbus Configuration: Disabled
- DNP3 Configuration: Disabled

Transport/Network Layer Preprocessors

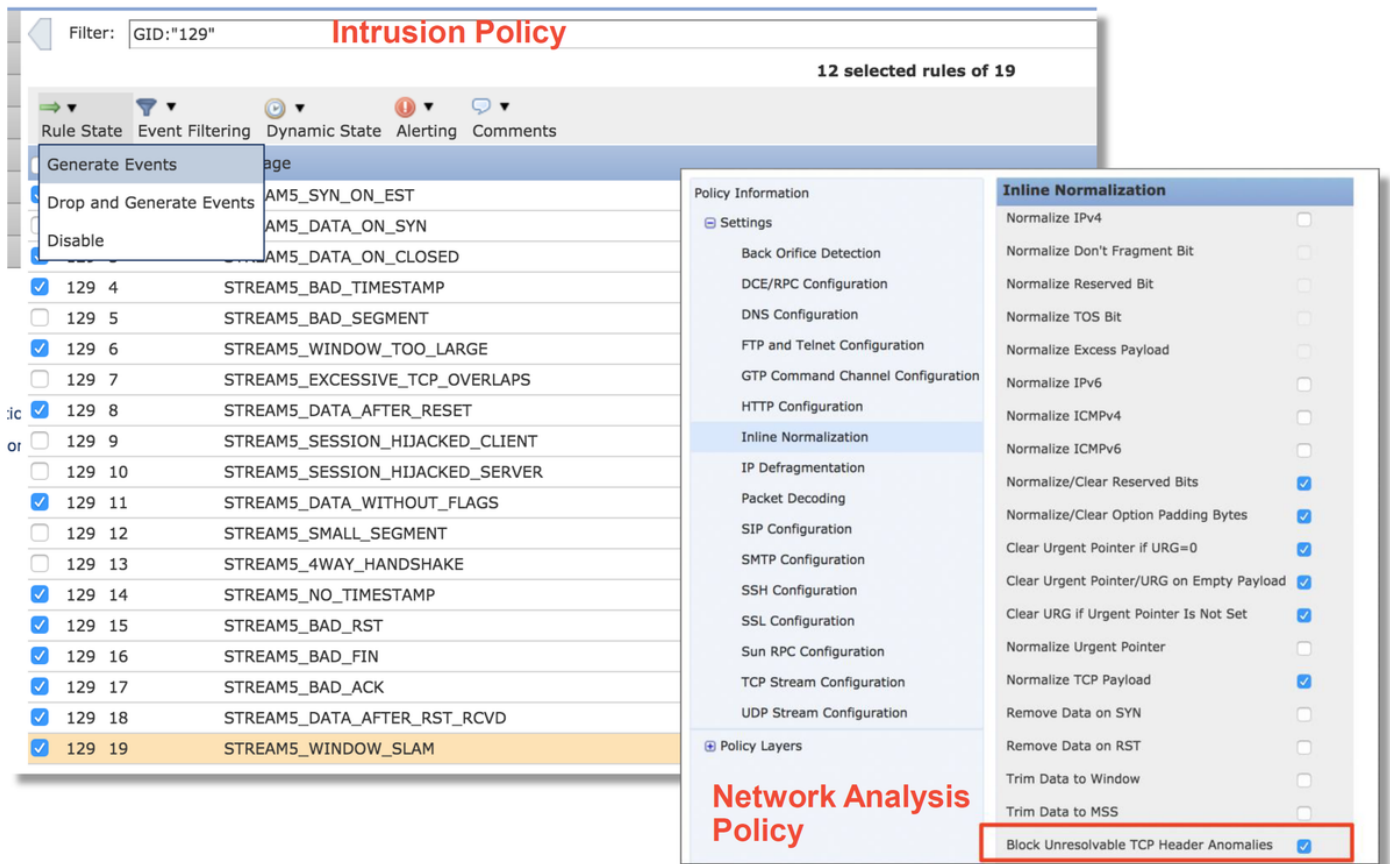
- Checksum Verification: Disabled
- Inline Normalization: Enabled

자동 삭제를 유발할 수 있는 NAP 설정

추적 섹션에 언급된 예에서는 TCP 스트림 설정 규칙인 129:14 규칙이 트래픽을 삭제합니다. 이는 시스템 지원 추적 출력을 보면 확인됩니다. 그러나 각 침입 정책 내에서 해당 규칙이 활성화되지 않은 경우, 침입 이벤트가 FMC로 전송되지 않습니다.

이러한 현상은 인라인 표준화 전처리 내의 해결할 수 없는 TCP 헤더 변칙 차단 설정 때문입니다. 이 옵션을 사용하면 기본적으로 특정 GID 129 규칙이 TCP 스트림에서 변칙을 탐지할 때 Snort가 차단 작업을 수행할 수 있습니다.

해결할 수 없는 TCP 헤더 변칙 차단이 활성화된 경우 아래 그림에 따라 GID 129 규칙을 켜는 것이 좋습니다.



GID 129 규칙을 켜면 트래픽에 대한 작업을 수행할 때 침입 이벤트가 FMC로 전송됩니다. 그러나 해결할 수 없는 TCP 변칙 차단이 활성화되어 있으면 침입 정책의 규칙 상태가 이벤트 생성으로 설정된 경우에도 여전히 트래픽을 삭제할 수 있습니다. 이 동작은 FMC 설정 가이드에 설명되어 있습니다.

Still drops after setting to generate

Inline Result	Source IP	Destination IP	Source Port / ICMP Type	Destination Port / ICMP Code	Message
↓	172.16.111.226	50.19.123.95	51174 / tcp	443 (https) / tcp	STREAMS_NO_TIMESTAMP (129:14:2)
↓	172.16.111.226	50.19.123.95	51174 / tcp	443 (https) / tcp	STREAMS_NO_TIMESTAMP (129:14:2)

Check configuration guide for relative protocols/preprocessors:

Block Unresolvable TCP Header Anomalies

When you enable this option, the system blocks anomalous TCP packets that, if normalized, would be invalid and likely would be blocked by the receiving host. For example, the system blocks any SYN packet transmitted subsequent to an established session.

The system also drops any packet that matches any of the following TCP stream preprocessor rules, regardless of whether the rules are enabled:

- 129:1
- 129:3
- 129:4
- 129:6
- 129:8
- 129:11
- 129:14 through 129:19

The Total Blocked Packets performance graph tracks the number of packets blocked in inline deployments and, in passive deployments and inline deployments in tap mode, the number that would have been blocked in an inline deployment.

위의 문서는 이 [문서](#)에서 찾을 수 있습니다(버전 6.4: 이 문서 게시 시점의 최신 버전).

백엔드 설정 확인

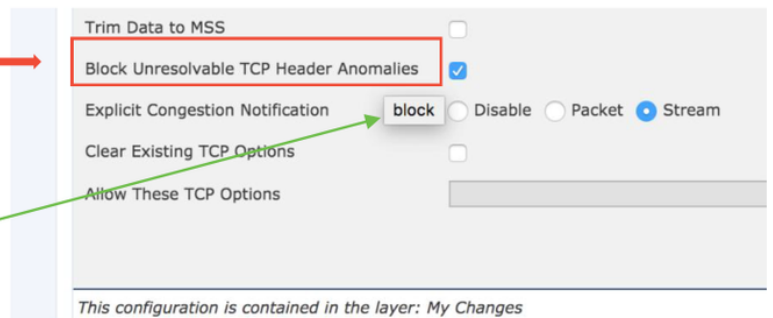
특정 설정이 FMC에 반영되지 않고 백엔드에서 활성화될 수 있다는 점에서 전처리기의 동작에 또 다른 복잡성이 추가됩니다. 다음과 같은 몇 가지 이유가 있습니다.

- 활성화된 다른 기능에는 전처리기 설정을 강제로 활성화하는 기능이 있습니다(기본 설정은 파일 정책).
- 일부 침입 정책 규칙은 탐지를 수행하기 위해 특정 전처리기 옵션을 요구합니다.
- 결함이 동작을 유발할 수 있습니다. 이에 대한 인스턴스 예: [CSCuz50295](#) - "악성코드 차단이 있는 파일 정책이 차단 플래그를 사용하여 TCP 표준화 활성화"

백엔드 설정을 살펴보기 전에, NAP 내의 특정 설정 위에 마우스를 올려놓으면 백엔드 Snort 설정 파일에서 사용되는 Snort 키워드를 확인할 수 있습니다. 아래 그림을 참조하십시오.

Hover over option to see backend snort configuration keyword

Snort config keyword is "block"



NAP 탭의 차단할 수 없는 TCP 헤더 변칙 옵션은 백엔드에서 차단 키워드로 변환됩니다. 이 정보를 옆두에 두고 전문가 셸(shell)에서 백엔드 설정을 확인할 수 있습니다.

```
root@ciscoasa:~# de_info.pl
```

```
DE Name      : Primary Detection Engine (c9ef19d6-e187-11e6-ba76-99617d53da68)
DE Type      : ids
DE Description : Primary detection engine for device c9ef19d6-e187-11e6-ba76-99617d53da68
DE Resources  : 1
DE UUID      : 0d82120c-e188-11e6-8606-a4827d53da68
```

```
root@ciscoasa:~# cd /var/sf/detection_engines/0d82120c-e188-11e6-8606-a4827d53da68/network_analysis/
root@ciscoasa:network_analysis# ls
b50f27b0-e31a-11e6-b866-dd9e65c01d56 object_b50f27b0-e31a-11e6-b866-dd9e65c01d56 snort.conf.b50f27b0-e31a-11e6-b866-
dd9e65c01d56 snort.conf.b50f27b0-e31a-11e6-b866-dd9e65c01d56.default
root@ciscoasa:network_analysis# cat b50f27b0-e31a-11e6-b866-dd9e65c01d56/normalize.conf
#
# generated from My Changes
#
preprocessor normalize_tcp: ips, rsv, pad, req_urg, req_pay, req_urp, block
```

“block” option is enabled in normalize.conf

대상 지정 NAP 생성

특정 호스트가 전처리 이벤트를 트리거하는 경우, 맞춤형 NAP를 사용하여 해당 호스트를 오가는 트래픽을 검사할 수 있습니다. 맞춤형 NAP 내에서 문제를 일으키는 설정을 비활성화할 수 있습니다.

다음은 대상 지정 NAP를 구현하기 위한 단계입니다.

1. 이 문서의 NAP 설정 확인 섹션에 나와 있는 지침에 따라 NAP를 생성합니다.
2. 액세스 제어 정책의 고급 탭에서 네트워크 분석 및 침입 정책 섹션으로 이동합니다. 규칙 추가를 클릭하고 대상 지정 호스트를 사용하여 규칙을 생성한 다음 네트워크 분석 정책 섹션에서 새로 생성된 NAP를 선택합니다.

Network Analysis and Intrusion Policies

#	Source Zo...	Dest Zones	Source Networ...	Dest Networks	VLAN T...	Network Analysis ...
1	Any	Any	62_network	Any	Any	My Custom NAP

Click to expand NA Rules

Add rule(s) to target traffic with certain NAP

오탐 분석

전처리 규칙에 대한 침입 이벤트에서 오탐을 확인하는 것은 규칙 평가에 사용되는 Snort 규칙 (GID 1과 3 포함)과는 매우 다릅니다.

전처리 규칙 이벤트에 대한 오탐 분석을 수행하려면 TCP 스트림 내에서 변칙을 찾기 위해 전체 세션 캡처가 필요합니다.

아래 예에서는 규칙 129:14에서 오탐 분석이 수행되고 있으며, 위의 예에서는 트래픽을 삭제하는 것으로 표시되어 있습니다. 129:14는 타임스탬프가 누락된 TCP 스트림을 찾으므로 아래에 나와 있는 패킷 캡처 분석에 따라 규칙이 트리거된 이유를 분명히 확인할 수 있습니다.

Full session pcap

```

Internet Protocol Version 4, Src: 172.16.111.226, Dst: 50.19.123.95
Transmission Control Protocol, Src Port: 51174, Dst Port: 443, Seq: 3849839666, Len: 0
  Source Port: 51174
  Destination Port: 443
  [Stream index: 2]
  [TCP Segment Len: 0]
  Sequence number: 3849839666
  Acknowledgment number: 0
  Header Length: 40 bytes
  Flags: 0x002 (SYN)
  Window size value: 8192
  [Calculated window size: 8192]
  Checksum: 0x70ba [correct]
  [Checksum Status: Good]
  [Calculated Checksum: 0x70ba]
  Urgent pointer: 0
  Options: 20 bytes), Maximum segment size, No-Operation (NOP), Window scale, SACK permitted, Timestamps
    Maximum segment size: 1380 bytes
    No-Operation (NOP)
    Window scale: 8 (multiply by 256)
    TCP SACK Permitted Option: True
    Timestamps: TSval 2054852, TSecr 0
  
```

Packet that triggered event

```

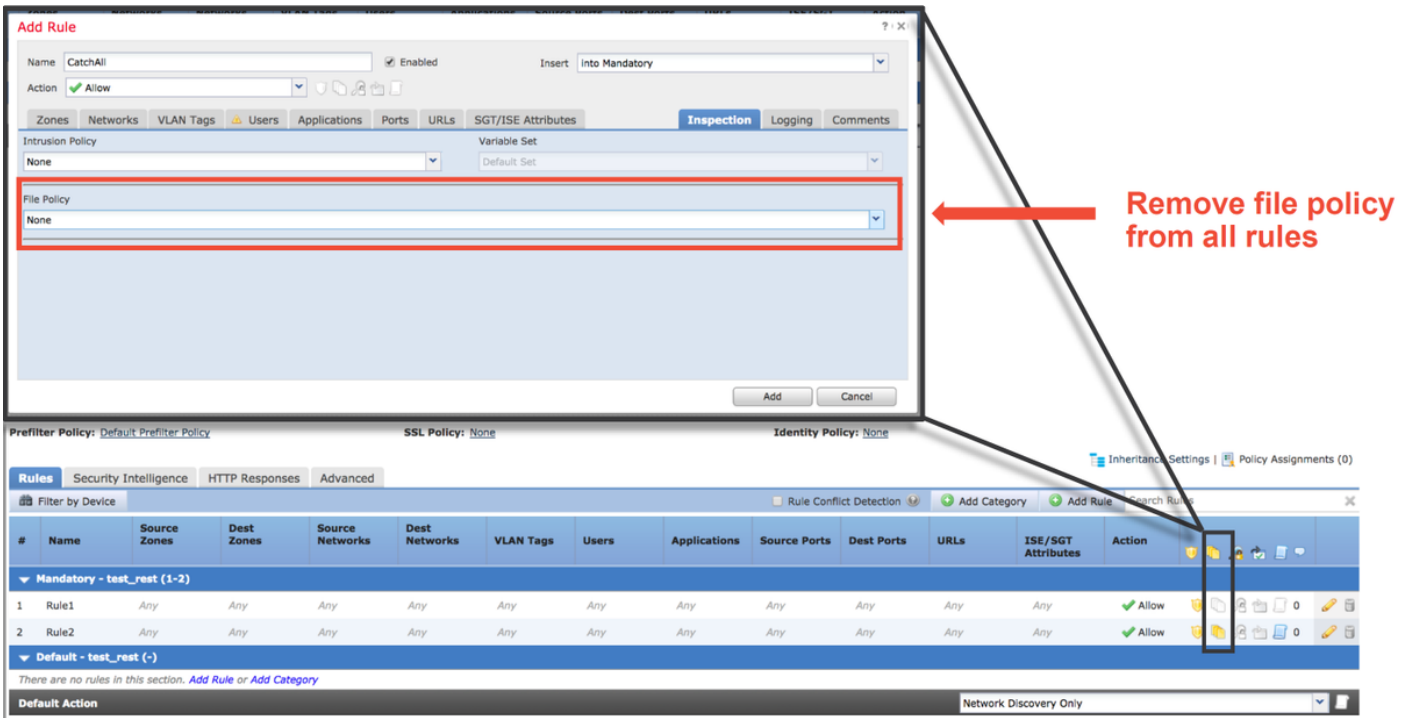
Internet Protocol Version 4, Src: 172.16.111.226, Dst: 50.19.123.95
Transmission Control Protocol, Src Port: 51174, Dst Port: 443, Seq: 3849839667, Ack: 1666843207, Len: 0
  Source Port: 51174
  Destination Port: 443
  [Stream index: 0]
  [TCP Segment Len: 0]
  Sequence number: 3849839667
  Acknowledgment number: 1666843207
  Header Length: 20 bytes
  Flags: 0x010 (ACK)
  Window size value: 57
  [Calculated window size: 57]
  [Window size scaling factor: -1 (unknown)]
  Checksum: 0xed47 [correct]
  [Checksum Status: Good]
  [Calculated Checksum: 0xed47]
  Urgent pointer: 0
  Options:
    Timestamps:
  
```

완화 단계

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

- 맞춤형 NAP를 사용 중이고 NAP 설정이 트래픽을 삭제하고 있는지 확실하지 않지만 의심되는 경우 "보안 및 연결성의 균형 유지" 또는 "보안보다 연결성 우선" 정책으로 대체할 수 있습니다.

- "맞춤형 규칙"을 사용 중인 경우 NAP를 위에서 언급한 기본값 중 하나로 설정해야 합니다.
- 액세스 제어 규칙에서 파일 정책을 사용하는 경우, 해당 규칙을 일시적으로 제거해야 할 수 있습니다. 파일 정책이 FMC에 반영되지 않은 전처리기를 백엔드에서 활성화할 수 있으며 이는 "전역" 레벨에서 이루어지며 모든 NAP가 수정됨을 의미합니다.



각 프로토콜에는 서로 다른 전처리기가 있으며, 이러한 문제 해결은 전처리기에 따라 매우 다를 수 있습니다. 이 문서에서는 모든 전처리기 설정 및 각각에 대한 문제 해결 방법을 다루지 않습니다.

각 전처리기에 대한 설명서를 확인하여 각 옵션의 기능을 더 잘 이해할 수 있습니다. 이는 특정 전처리기 문제를 해결할 때 유용합니다.

TAC에 제공할 데이터

데이터 지침

Firepower 디
바이스에서
파일 문제 해
결

<http://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-tech>

Firepower 디
바이스의 전
체 세션 패킷
캡처

<http://www.cisco.com/c/en/us/support/docs/security/sourcefire-firepower-8000-series-applia>

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.