Firepower 데이터 경로 문제 해결 7단계: 침입 정책

목차

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 문서를 참조하고 다른 데이터 경로 문제 해결 문서에 대한 링크를 참조하십시오.

이 문서에서는 Firepower 데이터 경로 문제 해결의 7단계인 침입 정책 기능을 다룹니다.

사전 요구 사항

- 이 문서는 침입 정책을 실행하는 모든 Firepower 플랫폼에 적용됩니다. **추적** 기능은 Firepower Threat Defense(FTD) 플랫폼 버전 6.2 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.

침입 정책 문제 해결 단계

"추적" 툴을 사용하여 침입 정책 삭제 탐지(FTD만 해당)

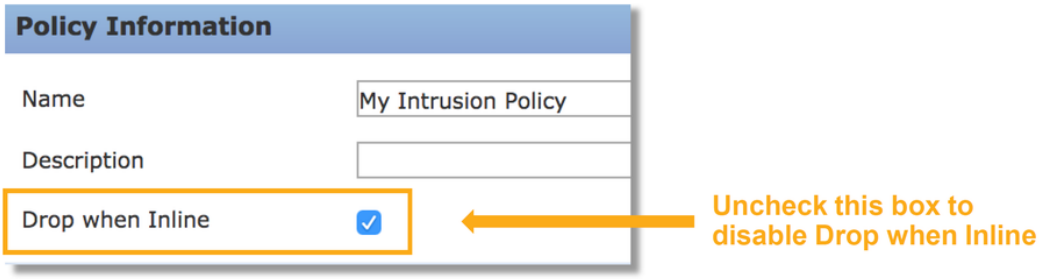
시스템 지원 추적 툴은 FTD CLI(Command Line Interface)에서 실행할 수 있습니다. 이는 Snort의 내부 작동 방식을 자세히 설명한다는 점을 제외하면 액세스 제어 정책 단계 문서에서 언급한 **firewall-engine-debug** 툴과 유사합니다. 이는 침입 정책 규칙이 관심 있는 트래픽에서 트리거되는지 확인하는 데 유용할 수 있습니다.

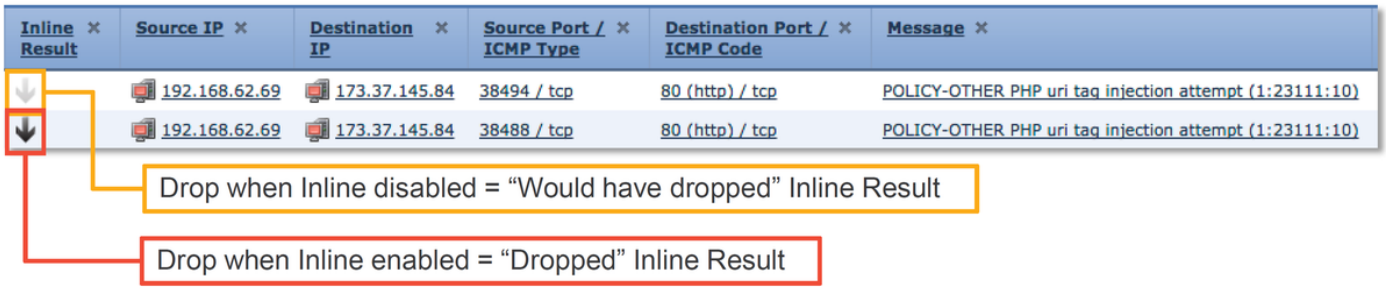
아래 예에서는 IP 주소가 192.168.62.6인 호스트의 트래픽이 침입 정책 규칙(이 경우 **1:23111**)에 의해 차단되고 있습니다.

```
> system support trace

Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.62.69
Please specify a client port:
Please specify a server IP address:
Please specify a server port:
Enable firewall-engine-debug too? [n]: y
Monitoring packet tracer debug messages

[… output omitted for brevity]

173.37.145.84-80 - 192.168.62.69-38488 6 Packet: TCP, ACK, seq 3594105349, ack 3856774965
173.37.145.84-80 - 192.168.62.69-38488 6 AppID: service HTTP (676), application Cisco (2655)
192.168.62.69-38488 > 173.37.145.84-80 6 AS 1 I 0 URL SI: ShmDBLookupURL("http://www.cisco.com/<?php") returned 0
…
192.168.62.69-38488 > 173.37.145.84-80 6 AS 1 I 0 match rule order 5, 'inspect it all', action Allow
192.168.62.69-38488 > 173.37.145.84-80 6 AS 1 I 0 allow action
192.168.62.69-38488 > 173.37.145.84-80 6 Firewall: allow rule, 'inspect it all', allow
192.168.62.69-38488 > 173.37.145.84-80 6 IPS Event: gid 1, sid 23111, drop
192.168.62.69-38488 > 173.37.145.84-80 6 Snort detect_drop: gid 1, sid 23111, drop
192.168.62.69-38488 > 173.37.145.84-80 6 AS 1 I 0 Deleting session
192.168.62.69-38488 > 173.37.145.84-80 6 NAP id 1, IPS id 0, Verdict BLACKLIST
192.168.62.69-38488 > 173.37.145.84-80 6 ===> Blocked by IPS
Verdict reason is sent to DAQ's PDTS
```

Snort에 의해 적용된 작업이 **삭제**인 것을 확인할 수 있습니다. Snort에서 삭제가 탐지되면 해당 특정 세션이 블랙리스트에 추가되어 추가 패킷도 함께 삭제됩니다.

Snort가 **삭제** 작업을 수행할 수 있는 이유는 침입 정책 내에서 "인라인 시 삭제" 옵션이 활성화되어 있기 때문입니다. 이는 침입 정책의 초기 랜딩 페이지에서 확인할 수 있습니다. FMC(Firepower Management Center)에서 **정책 > 액세스 제어 > 침입**으로 이동하여 해당 정책 옆의 편집 아이콘을 클릭합니다.





"인라인 시 삭제"가 비활성화된 경우 Snort는 더 이상 문제가 되는 패킷을 삭제하지 않지만, 침입 이벤트에서 "Would Have Dropped"라는 **인라인 결과**를 알림으로 보냅니다.

"인라인 시 삭제"를 비활성화하면 추적 출력에 해당 트래픽 세션에 대한 **would drop** 작업이 표시됩니다.

```
> system support trace


Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.62.69
Please specify a client port:
Please specify a server IP address:
Please specify a server port:
Enable firewall-engine-debug too? [n]: y
Monitoring packet tracer debug messages

[… output omitted for brevity]

173.37.145.84-80 - 192.168.62.69-38494 6 Packet: TCP, ACK, seq 2900935719, ack 691924600
173.37.145.84-80 - 192.168.62.69-38494 6 AppID: service HTTP (676), application Cisco (2655)
…
192.168.62.69-38494 > 173.37.145.84-80 6 AS 1 I 0 match rule order 5, 'inspect it all', action Allow
192.168.62.69-38494 > 173.37.145.84-80 6 AS 1 I 0 allow action
192.168.62.69-38494 > 173.37.145.84-80 6 Firewall: allow rule, 'inspect it all', allow
192.168.62.69-38494 > 173.37.145.84-80 6 IPS Event: gid 1, sid 23111, would drop
192.168.62.69-38494 > 173.37.145.84-80 6 Snort detect_drop: gid 1, sid 23111, would drop
192.168.62.69-38494 > 173.37.145.84-80 6 NAP id 1, IPS id 0, Verdict PASS
192.168.62.69-38494 > 173.37.145.84-80 6 ===> Blocked by IPS
Verdict reason is sent to DAQ's PDTS
```

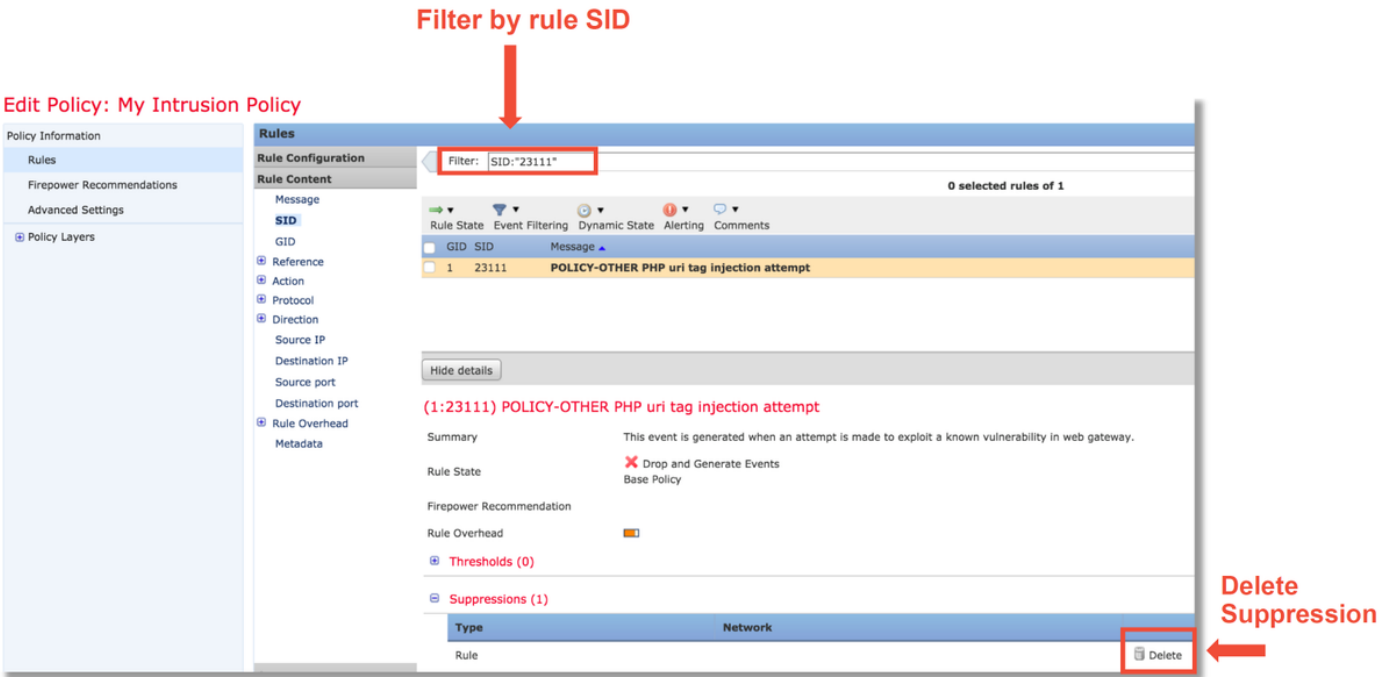
침입 정책에서 억제 확인

Snort는 침입 이벤트를 FMC로 전송하지 않고 트래픽을 삭제할 수 있습니다(자동 삭제). 이 작업은 **억제를 설정하여 수행할 수 있습니다.** 침입 정책에서 억제가 설정되었는지 확인하려면 아래 그림과 같이 백엔드에서 전문가 쉘(shell)을 확인할 수 있습니다.

```
[ Look for suppressions ]
> expert
$ cd /var/sf/detection_engines/*/
$ grep -H '^suppress' intrusion/*/snort_suppression.conf
intrusion/68acdfa2-e31a-11e6-b866-dd9e65c01d56/snort_suppression.conf:suppress gen_id 1, sig_id 23111

[ Get the policy name ]
$ grep Name intrusion/snort.conf.68acdfa2-e31a-11e6-b866-dd9e65c01d56
# Name       : My Intrusion Policy
```

"내 침입 정책"이라고 하는 침입 정책에는 1:23111 규칙에 대한 억제가 포함되어 있습니다. 따라서 이 규칙으로 인해 이벤트 없이 트래픽이 삭제될 수 있습니다. 이는 추적 유틸리티가 도움이 될 수 있는 또 다른 이유로, 여전히 삭제가 발생을 보여주기 때문입니다.

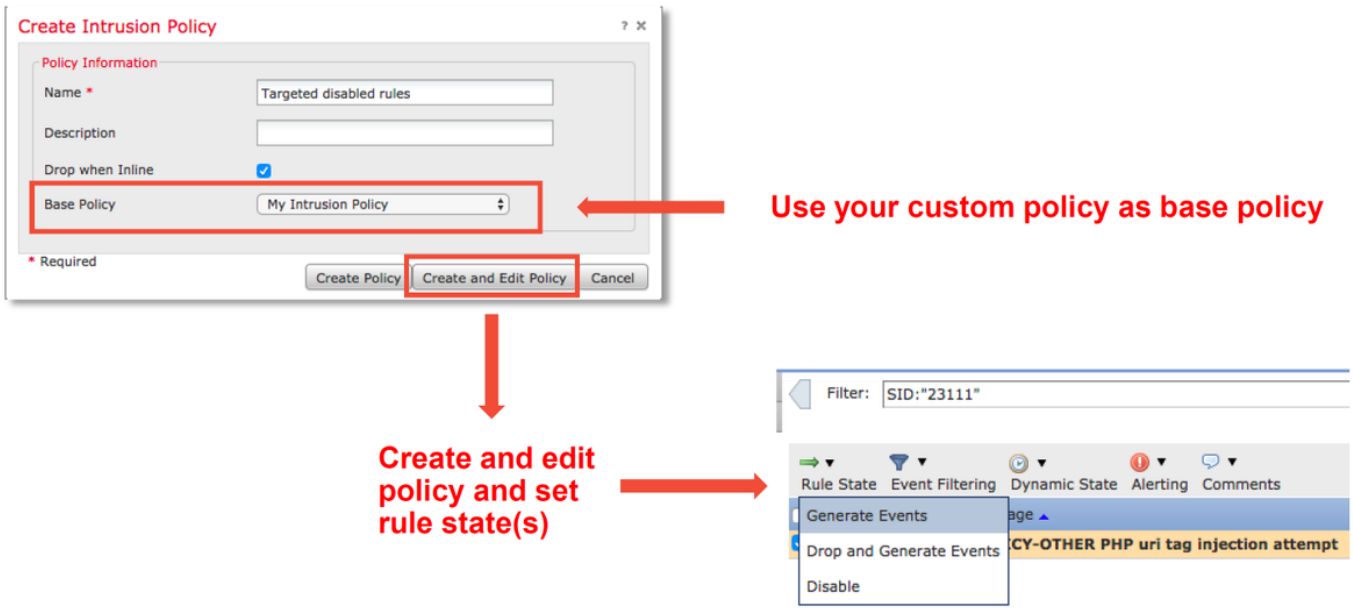
억제를 삭제하려면 침입 정책 **규칙** 보기 내에서 해당 규칙을 필터링할 수 있습니다. 그러면 아래와 같이 억제를 삭제할 수 있는 옵션이 나타납니다.



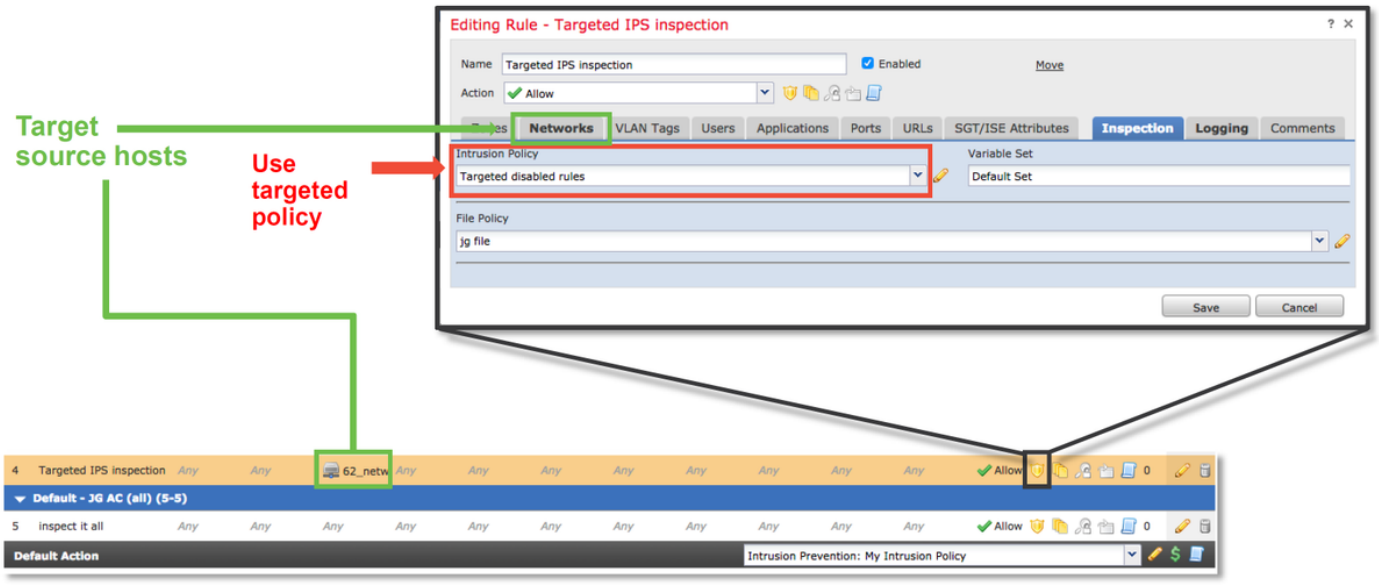
대상 지정 침입 정책 생성

특정 침입 정책 규칙에 의해 트래픽이 삭제되는 경우 해당 트래픽이 삭제되는 것은 원치 않지만, 규칙을 비활성화하는 것도 원치 않을 수 있습니다. 해결책은 문제가 되는 규칙을 비활성화하여 새 침입 정책을 생성한 다음 대상 지정 호스트의 트래픽을 평가하도록 하는 것입니다.

다음은 새 침입 정책을 생성하는 방법에 대한 그림입니다(**정책 > 액세스 제어 > 침입** 아래).



새 침입 정책을 생성한 후에는 새 액세스 제어 정책 규칙 내에서 사용할 수 있는데, 이는 원래 침입 정책에 의해 이전에 트래픽이 삭제되었던 해당 호스트를 대상으로 합니다.



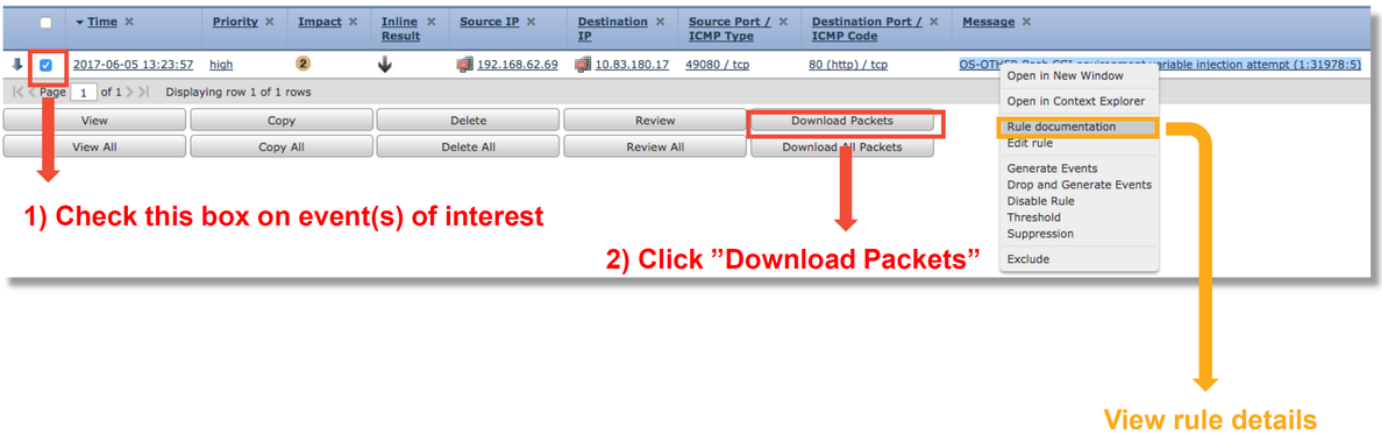
오탐 문제 해결

일반적인 사례 시나리오는 침입 이벤트에 대한 오탐 분석입니다. 오탐 사례를 열기 전에 몇 가지 사항을 확인할 수 있습니다.

1. **Intrusion Events 페이지의 테이블** 보기에서 해당 이벤트의 확인란을 클릭합니다

2. Download Packets(**패킷 다운로드**)를 클릭하여 침입 이벤트가 트리거될 때 Snort에서 캡처한 패킷을 가져옵니다.

3. **메시지** 열에서 규칙 이름을 마우스 오른쪽 단추로 누른 다음 **규칙 문서**를 눌러 규칙 구문 및 기타 관련 정보를 확인합니다.



다음은 위의 예에서 이벤트를 트리거한 규칙의 규칙 구문입니다. 이 규칙에 대해 FMC에서 다운로드한 패킷 캡처(PCAP) 파일에 대해 확인할 수 있는 규칙 부분은 굵게 표시되어 있습니다.

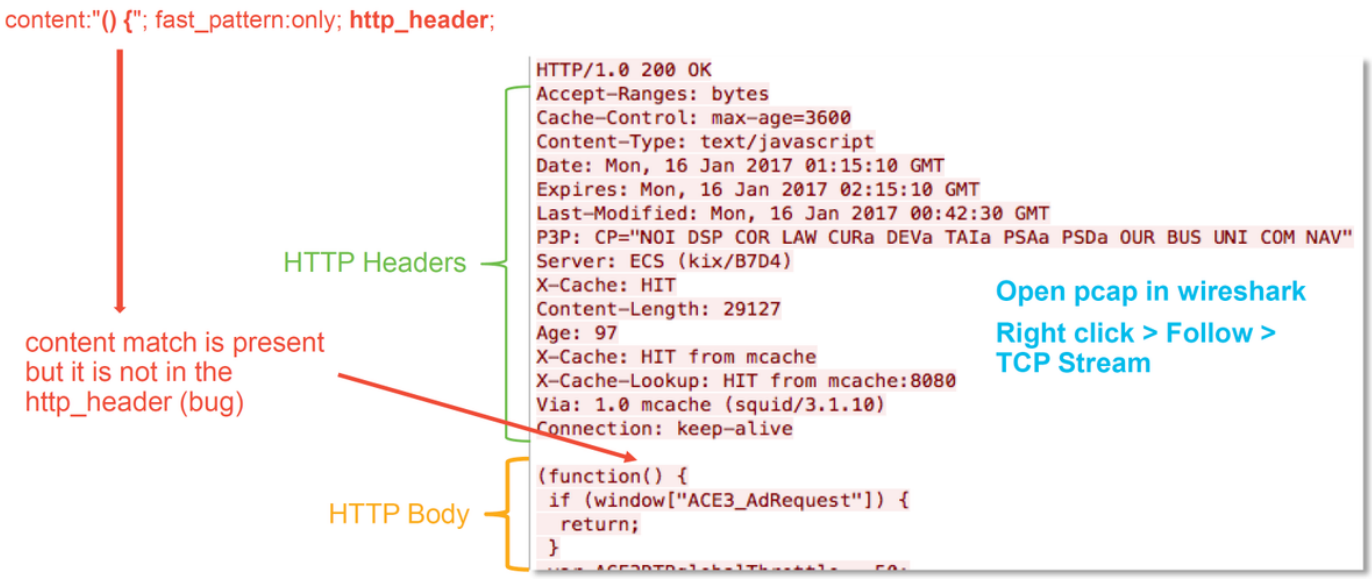
alert **tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS** \
(msg:"OS-OTHER Bash CGI environment variable injection threat"; \
flow:to_server,established; \
content:"() {"; fast_pattern:only; http_header; \
metadata:policybalanced-ipsdrop, policy max-detect-ipsdrop, policy security-ipsdrop, ruleset community, **service http**; \

reference:cve,2014-6271; reference:cve,2014-6277; reference:cve,2014-6278;
reference:cve,2014-7169; \
classtype:attempted-admin; \
sid:31978; rev:5;)

그런 다음 이러한 초기 단계를 따라 분석 프로세스를 수행하여 트래픽이 트리거된 규칙과 일치해야 하는지 확인할 수 있습니다.

1. 트래픽이 일치하는 액세스 제어 규칙을 확인합니다. 이 정보는 침입 이벤트 탭의 열에 포함되어 있습니다.
2. 해당 액세스 제어 규칙에 사용된 변수 집합을 찾습니다. 그런 다음 **개체 > 개체 관리 > 변수 집합에서 변수 집합을 검토할 수 있습니다.**
3. PCAP 파일의 IP 주소가 변수와 일치하는지 확인합니다(이 경우 **$HOME_NET** 변수 설정에 포함된 호스트에 연결하는 **$EXTERNAL_NET** 변수에 포함된 호스트).
4. **플로우**의 경우 전체 세션/연결을 캡처해야 할 수 있습니다. Snort는 성능상의 이유로 전체 플로우를 캡처하지 않습니다. 그러나 대부분의 경우 flow:established가 포함된 규칙이 트리거된 경우 규칙이 트리거될 때 세션이 설정되었다고 가정하는 것이 안전합니다. 따라서 Snort 규칙에서 이 옵션을 확인하는 데 전체 PCAP 파일이 필요하지 않습니다. 그러나 트리거된 이유를 더 잘 이해하는 데 유용할 수 있습니다.
5. **service http**의 경우 Wireshark에서 PCAP 파일을 확인하여 HTTP 트래픽처럼 보이는지 확인합니다. 호스트에 대해 네트워크 검색이 활성화되어 있고 검색에서 이전에 애플리케이션 "HTTP"를 확인한 적이 있는 경우 서비스가 세션에서 일치하게 될 수 있습니다.

이러한 정보를 염두에 두고 FMC에서 다운로드한 패킷을 Wireshark에서 추가로 검토할 수 있습니다. 트리거된 이벤트가 오탐인지 여부를 확인하기 위해 PCAP 파일을 평가할 수 있습니다.



위 그림에서, 규칙이 탐지하는 콘텐츠는 PCAP 파일에 존재했습니다. **"() {"**

그러나 규칙이 패킷의 HTTP 헤더에서 콘텐츠가 탐지되도록 지정합니다. **http_header**

이 경우 콘텐츠가 HTTP 본문에서 발견되었습니다. 따라서 이는 오탐입니다. 그러나 규칙이 잘못 작성되었다는 점에서 이는 오탐이 아닙니다. 규칙이 올바르며 이 경우 개선할 수 없습니다. 이 예에서는 Snort에 버퍼 혼동을 일으키는 Snort 버그가 발생이 발생했을 가능성이 있습니다. 이는 Snort가 http_headers를 잘못 식별했음을 의미합니다.

이 경우 디바이스가 실행 중인 버전에서 Snort/IPS 엔진에 대한 기존 버그를 확인할 수 있으며, 버그가 없는 경우 Cisco TAC(Technical Assistance Center)를 통해 케이스를 열 수 있습니다. 시스코 팀

에서는 Snort가 해당 상태로 전환된 방법을 검토해야 하며 이는 단일 패킷으로 수행할 수 없기 때문에 이러한 문제를 조사하려면 전체 세션 캡처가 필요합니다.

참양성(True Positive) 예

아래 그림은 동일한 침입 이벤트에 대한 패킷 분석을 보여줍니다. 이번에는 콘텐츠가 HTTP 헤더에 표시되므로 이벤트는 참양성입니다.

TAC에 제공할 데이터

데이터	지침
트래픽을 검사하는 Firepower 디바이스에서 파일 문제 해결	http://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-tech
FMC에서 다운로드한 패킷 캡처	지침은 이 문서를 참조하십시오.
수집된 모든 관련 CLI 출력(예: **추적** 출력)	지침은 이 문서를 참조하십시오.

다음 단계

침입 정책 구성 요소가 문제의 원인이 아닌 것으로 확인된 경우, 다음 단계로 네트워크 분석 정책 기능의 문제 해결을 수행합니다.

마지막 문서로 이동하려면 여기를 클릭하십시오.

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.