Firepower 데이터 경로 문제 해결 4단계: 액세스 제어 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 4단계인 ACP(Access Control Policy)를 다룹니다. 이 정보는 현재 지원되는 모든 Firepower 플랫폼 및 버전에 적용됩니다.

ACP(Access Control Policy) 문제 해결 단계

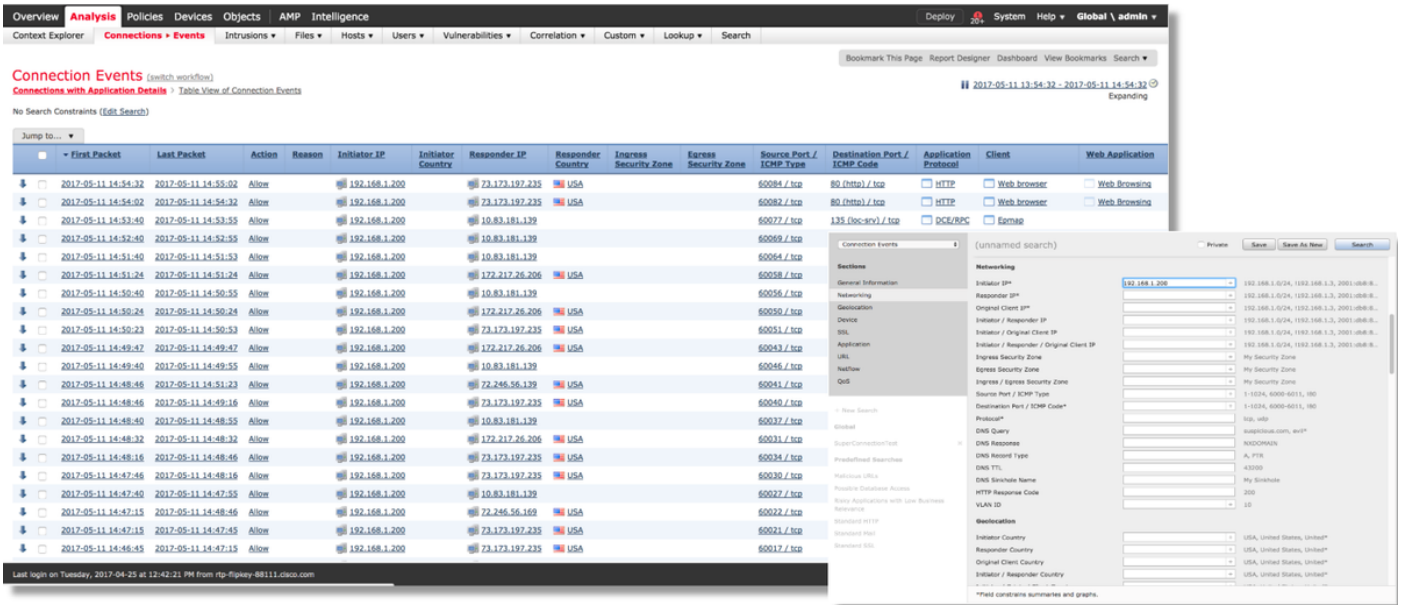
일반적으로 플로우가 일치하는 ACP 규칙을 확인하는 것은 매우 간단합니다. 연결 이벤트를 검토하여 어떤 규칙/작업이 실행되고 있는지 확인할 수 있습니다. ACP에서 트래픽에 수행하는 작업이 명확하게 표시되지 않는 경우 Firepower CLI(Command Line Interface)에서 디버깅을 수행할 수 있습니다.

연결 이벤트 확인

플로우 정보뿐만 아니라 트래픽이 일치해야 하는 인그레스 및 이그레스 인터페이스에 대한 아이디어를 얻은 후, Firepower가 플로우를 차단하고 있는지 여부를 확인하는 첫 번째 단계는 해당 트래픽에 대한 연결 이벤트를 확인하는 것입니다. 이는 Firepower Management Center의 **분석 > 연결 > 이벤트에서 확인할 수 있습니다.**

참고: 연결 이벤트를 확인하기 전에 ACP 규칙에서 로깅이 활성화되어 있는지 확인하십시오.

로깅은 각 액세스 제어 정책 규칙의 "로깅" 탭과 보안 인텔리전스 탭에서 설정합니다. 의심스러운 규칙이 로그를 "이벤트 뷰어"로 전송하도록 설정되었는지 확인합니다. 이는 기본 작업에도 적용됩니다.



"검색 편집"을 클릭하고 고유한 소스(이니시에이터) IP로 필터링하면 Firepower에서 탐지한 플로우를 확인할 수 있습니다. 작업 열에 이 호스트의 트래픽에 대해 "허용"이 표시됩니다.

Firepower가 의도적으로 트래픽을 차단하는 경우 작업에 "차단"이라는 단어가 포함됩니다. "연결 이벤트의 테이블 보기"를 클릭하면 추가 데이터가 제공됩니다. 작업이 "차단"인 경우 연결 이벤트에서 다음 필드를 검토하면 됩니다.

- 이유

- 액세스 제어 규칙

빠른 완화 단계

ACP 규칙으로 인해 발생하는 것으로 보이는 문제를 신속하게 완화하기 위해 다음을 수행할 수 있습니다.

- 해당 트래픽에 대해 "신뢰" 또는 "허용" 작업이 포함된 규칙을 생성하여 ACP의 맨 위에 배치하거나 모든 차단 규칙 위에 배치합니다.
- "차단"이라는 단어가 포함된 작업이 있는 규칙을 일시적으로 비활성화합니다.
- 기본 작업이 "모든 트래픽 차단"으로 설정된 경우 일시적으로 "네트워크 검색 한정"으로 전환합니다.

참고: 이러한 빠른 완화에는 정책 변경이 필요하며, 이는 일부 환경에서 가능하지 않을 수 있습니다. 정책을 변경하기 전에 먼저 시스템 지원 추적을 사용하여 트래픽이 일치하는 규칙을 확인하는 것이 좋습니다.

ACP 디버깅

> system support firewall-engine-debug CLI 유틸리티를 통해 ACP 작업에 대한 추가 문제 해결을

수행할 수 있습니다.

> **참고**: Firepower 9300 및 4100 플랫폼에서는 다음 명령을 통해 해당 쉘(shell)에 액세스할 수 있습니다.
>
> **# connect module 1 console**
> Firepower-module1> **connect ftd**
> >
>
> 다중 인스턴스의 경우 다음 명령을 사용하여 논리적 디바이스 CLI에 액세스할 수 있습니다.
> **# connect module 1 telnet**
> Firepower-module1> ftd ftd **1 연결**
> Connecting to container ftd(ftd1) console... enter "exit" to return to Boot CLI
> >

system support firewall-engine-debug 유틸리티에는 ACP에서 평가 중인 각 패킷에 대한 항목이 있습니다. 여기에는 수행되고 있는 규칙 평가 프로세스와 규칙이 일치하거나 일치하지 않는 이유가 표시됩니다.

> **참고**: 버전 6.2 이상에서는 **시스템 지원 추적** 툴을 실행할 수 있습니다. 동일한 매개변수를 사용하지만, 더 많은 세부사항이 포함됩니다. **"Enable firewall-engine-debug too?"**라는 메시지가 표시되면 'y'를 입력하십시오.

예 1: 트래픽이 신뢰 규칙과 일치

아래 예에서는 **system support firewall-engine-debug**를 사용하여 SSH 세션 설정을 평가합니다.

이는 Firepower 디바이스에서 실행 중인 ACP입니다.

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN ...	Users	Applic...	Sourc...	Dest P...	URLs	ISE/S... Attrib...	Acti...
Mandatory - JG AC (all) (1-6)													
1	Trust ssh for host	Any	Any	192.168.0.7	Any	Any	Any	Any	Any	SSH	Any	Any	Trust
2	inspect	Any	Any	10.0.0.0/8	Any	Any	Any	Any	Any	Any	Any	Any	Allow
3	trust server backup	Any	Any	192.168.62.3	10.123.175.22	Any	Any	Any	Any	Any	Any	Any	Trust

ACP에는 세 가지 규칙이 있습니다.

1. 첫 번째 규칙은 SSH에서 사용하는 대상 포트를 가진 192.168.0.7의 모든 트래픽을 신뢰하는 것입니다.
2. 두 번째 규칙은 XFF 헤더 데이터를 기반으로 하여 네트워크 기준이 일치하는 10.0.0.0/8에서 시작되는 모든 트래픽을 검사합니다(네트워크 개체 옆에 아이콘으로 표시됨).
3. 세 번째 규칙은 192.168.62.3에서 10.123.175.22로의 모든 트래픽을 신뢰합니다.

문제 해결 시나리오에서는 192.168.62.3에서 10.123.175.22로의 SSH 연결을 분석합니다.

예상은 세션이 AC 규칙 3 "서버 백업 신뢰"와 일치하는 것입니다. 문제는 이 세션이 이 규칙과 일치하는 데 필요한 패킷 수입니다. AC 규칙을 확인하기 위해 첫 번째 패킷에서 모든 정보가 필요한가? 또는 여러 패킷이 필요한가? 필요하다면 몇 개가 필요한가? 등을 고려해야 합니다.

Firepower CLI에서 다음을 입력하여 ACP 규칙 평가 프로세스를 확인합니다.

```
>system support firewall-engine-debug

Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.62.3
Please specify a client port:
Please specify a server IP address: 10.123.175.22
Please specify a server port: 22
Monitoring firewall engine debug messages
```

> **팁**: 관심 있는 디버그 메시지만 화면에 출력되도록 **firewall-engine-debug**를 실행할 때 최대한 많은 매개변수를 입력하는 것이 가장 좋습니다.

아래의 디버그 출력에서 평가 중인 세션 중 첫 4개의 패킷을 확인할 수 있습니다.

SYN

SYN/ACK

ACK

첫 번째 SSH 패킷(클라이언트와 서버 간)

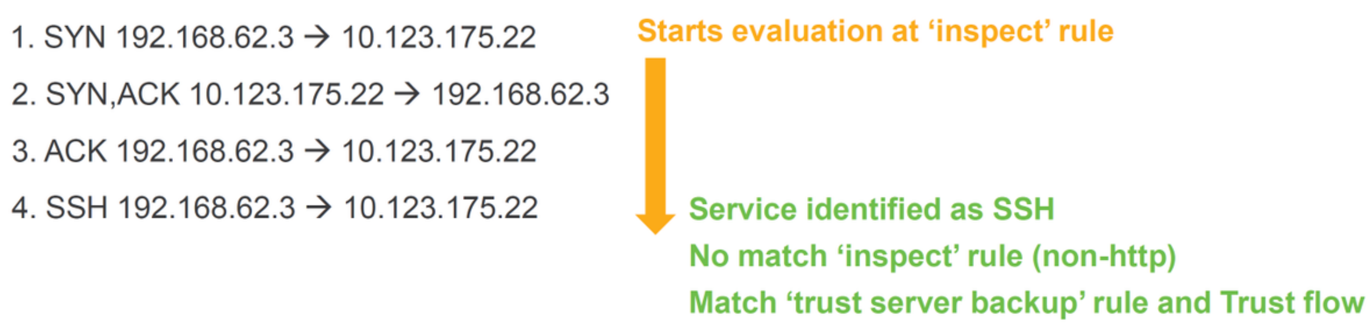
```
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 New session
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 4, 'inspect', and IPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0,
inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 pending rule order 4, 'inspect', XFF wait for AppId

192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 4, 'inspect', and IPProto first with zones 1 -> 2, 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
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 pending rule order 4, 'inspect', XFF wait for AppId

192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 4, 'inspect', and IPProto first with zones 1 -> 2, 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
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 pending rule order 4, 'inspect', XFF wait for AppId

192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 4, 'inspect', and IPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0,
inline sgt tag: untagged, ISE sgt id: 0, svc 846, payload -1, client 2000000846, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 no match rule order 4, 'inspect', XFF non-http
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 match rule order 5, 'trust server backup', action Trust
```

다음은 디버그 로직을 자세히 설명하는 차트입니다.



이 플로우에서는 디바이스가 규칙과 일치하는 데 4개의 패킷이 필요합니다.

다음은 디버그 출력에 대한 자세한 설명입니다.

- IP 주소가 요구 사항과 일치하지 않아 "호스트용 SSH 신뢰" 규칙이 일치하지 않았으므로 ACP 평가 프로세스가 "검사" 규칙에서 시작됩니다. 이 규칙이 일치해야 하는지 확인하는 데 필요한

모든 정보가 첫 번째 패킷(IP 및 포트)에 있으므로 이는 빠른 일치입니다.

- HTTP 애플리케이션 트래픽에서 XFF(X-Forwarded-For) 정보가 발견되고 애플리케이션이 아직 알려지지 않았으므로 애플리케이션이 식별될 때까지 트래픽이 "검사" 규칙과 일치하는지 여부를 확인할 수 없습니다. 따라서 이로 인해 세션이 규칙 2에 대해 보류 상태, 애플리케이션 데이터 보류 상태가 됩니다.
- 네 번째 패킷에서 애플리케이션이 식별되면 애플리케이션이 HTTP가 아니라 SSH이므로 "검사" 규칙 결과는 비일치(non-match)가 됩니다.
- 그런 다음 IP 주소를 기반으로 "서버 백업 신뢰" 규칙이 일치합니다.

요약하면, 규칙 2에는 애플리케이션 제약 조건이 있어 방화벽에서 애플리케이션을 식별할 때까지 기다려야 하므로 세션과 일치시키기 위해 연결에 4개의 패킷이 사용됩니다.

규칙 2에 소스 네트워크만 있고 XFF가 아닌 경우 세션과 일치시키기 위해 1개의 패킷이 사용됩니다.

레이어 1-4 규칙은 일반적으로 결정을 내리는 데 1개의 패킷이 필요하므로 가능한 경우 항상 정책의 다른 모든 규칙 위에 해당 규칙을 배치해야 합니다. 그러나 레이어 1-4 규칙만 사용하는 경우에도 AC 규칙과 일치하는 패킷이 1개 이상일 수 있으며, 그 이유는 URL/DNS 보안 인텔리전스 때문입니다. 이 중 하나가 활성화된 경우 방화벽은 AC 정책에 의해 평가되는 모든 세션에 대한 애플리케이션을 확인해야 하며 이는 HTTP 또는 DNS인지를 확인해야 하기 때문입니다. 그런 다음 블랙리스트를 기반으로 세션을 허용해야 하는지 여부를 결정해야 합니다.

다음은 관련 필드가 빨간색으로 강조 표시된 **firewall-engine-debug** 명령의 잘린 출력입니다. 식별된 애플리케이션의 이름을 가져오는 데 사용된 명령을 확인하십시오.

```
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 New session
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 4, 'inspect', and IPProto first with zones 1 -> 2, 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
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 pending rule order 4, 'inspect', XFF wait for AppId

[…omitted for brevity]

192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 4, 'inspect', and IPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0,
inline sgt tag: untagged, ISE sgt id: 0, svc 846, payload -1, client 2000000846, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 no match rule order 4, 'inspect', XFF non-http
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 match rule order 5, 'trust server backup', action Trust


[! How to map service/application ID to name]
> expert
$ grep "^846[^0-9]" /var/sf/appid/odp/appMapping.data
846 SSH 32 0 0 ssh
```

예 2: 신뢰 규칙과 일치하는 트래픽이 차단됨

일부 시나리오에서는 ACP의 신뢰 규칙과 일치하더라도 트래픽이 차단될 수 있습니다. 아래 예에서는 동일한 액세스 제어 정책 및 호스트를 사용하여 트래픽을 평가합니다.

```
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 New session
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 4, 'inspect', and IPProto first with zones 1 -> 2, 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
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 pending rule order 4, 'inspect', XFF wait for AppId
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 Deleting session

[!Session was deleted because we hit a drop IPS rule and blacklisted the flow.
This happened before AC rule was matched (Intrusion policy before AC rule match dropped).
Firewall engine will re-evaluate from top of AC policy to find a rule for logging decision]

192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 0, id 0 and IPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0, inline
sgt tag: 0, ISE sgt id: 0, svc -1, payload -1, client -1, misc -1, user 9999997, icmpType 102, icmpCode 22
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 no match rule order 3, 'Trust ssh for host', src network and GEO
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 no match rule order 4, 'inspect', XFF non-http
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 match rule order 5, 'trust server backup', action Trust
```

Action	Reason	Initiator IP	Responder IP	Source Port / ICMP Type	Destination Port / ICMP Code	Application Protocol	Client	Intrusion Events	Access Control Policy	Access Control Rule
Block	Intrusion Block	192.168.62.3	10.123.175.22	55654 / tcp	22 (ssh) / tcp				JG AC (all)	trust server backup

위에서 볼 수 있듯이 **firewall-engine-debug** 출력은 트래픽이 "신뢰"와 일치하는 것을 보여 주는 반면, 연결 이벤트는 침입 정책 규칙으로 인해 **차단** 작업을 표시합니다(이유 열에 **침입 차단**이 표시되어 확인됨).

이러한 상황이 발생할 수 있는 이유는 ACP의 **고급** 탭에 있는 **액세스 제어 규칙이 결정되기 전에 사용되는 침입 정책** 설정입니다. 규칙 작업에 따라 트래픽이 신뢰되기 전에 해당 침입 정책이 패턴 일치를 식별하고 트래픽을 삭제합니다. 그러나 IP 주소가 "서버 백업 신뢰" 규칙의 기준과 일치하므로 ACP 규칙 평가 결과는 신뢰 규칙과 일치합니다.

트래픽이 침입 정책 검사를 거치지 않도록 하려면 신뢰 규칙을 "검사" 규칙 위에 배치할 수 있는데, 이는 두 경우 모두 모범 사례에 해당합니다. 애플리케이션 식별은 "검사" 규칙의 일치 및 비일치에 필요하므로 **액세스 제어 규칙이 결정되기 전에 사용되는 침입 정책**이 동일한 규칙에 의해 평가되는 트래픽에 사용됩니다. "검사" 규칙 위에 "서버 백업 신뢰" 규칙을 배치하면 규칙이 IP 주소를 기반으로 하므로 첫 번째 패킷이 표시될 때 트래픽이 규칙과 일치하게 되는데 이는 첫 번째 패킷에서 확인할 수 있습니다. 따라서 **액세스 제어 규칙이 결정되기 전에 사용되는 침입 정책**을 사용할 필요가 없습니다.

시나리오 3: 애플리케이션 태그에 의해 차단된 트래픽

이 시나리오에서 사용자는 cnn.com이 차단되고 있음을 보고합니다. 그러나 CNN을 차단하는 특정 규칙은 없습니다. **Firewall-engine-debug** 출력과 함께 연결 이벤트에 차단 이유가 표시됩니다.

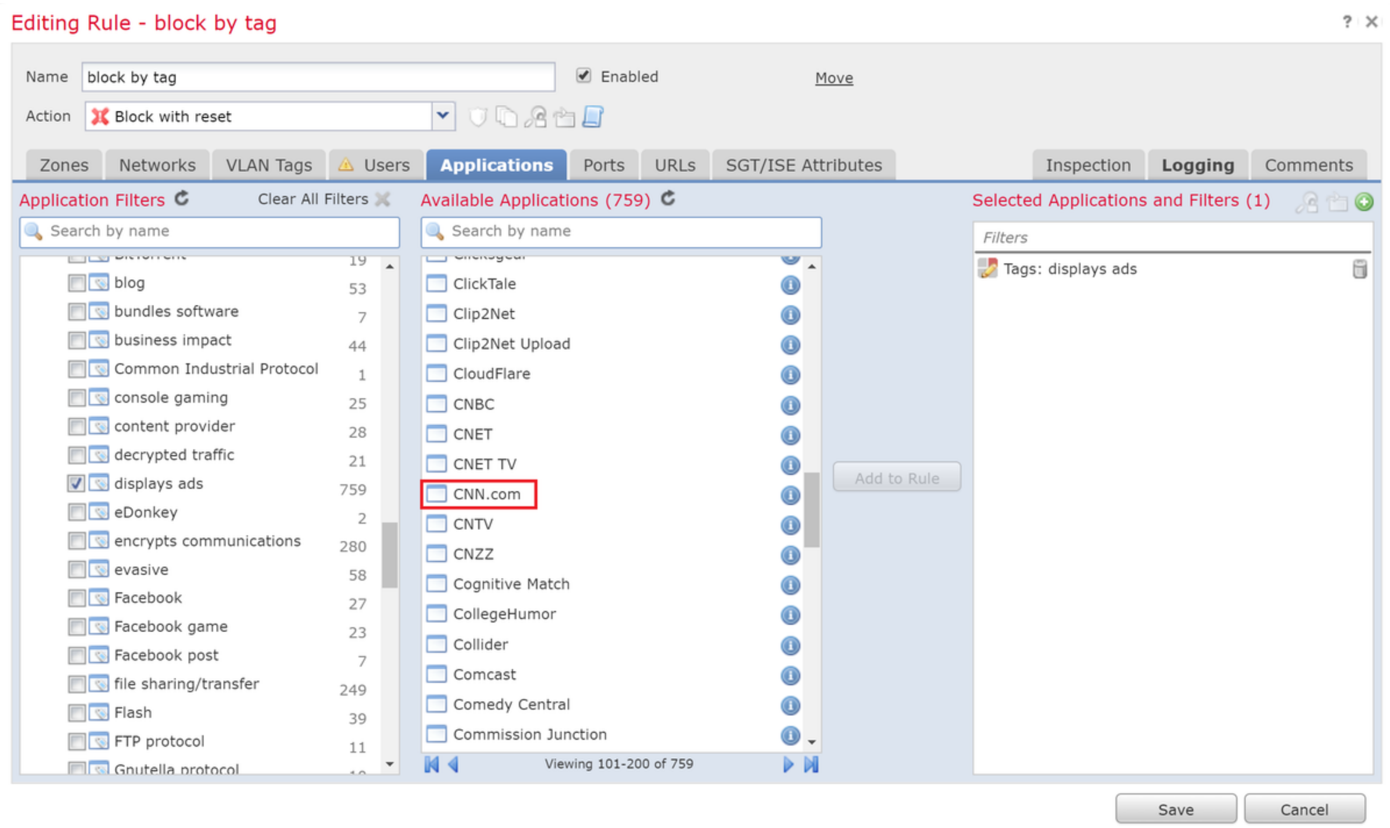
먼저 연결 이벤트에는 애플리케이션 필드 옆에 애플리케이션에 대한 정보와 Firepower가 해당 애플리케이션을 분류하는 방법을 보여 주는 정보 상자가 있습니다.

First Packet	Last Packet	Action	Initiator IP	Responder IP	Source Port / ICMP Type	Destination Port / ICMP Code	Application Protocol	Web Application	Application Risk	Business Relevance	URL
2017-05-19 16:02:29		Block	192.168.62.63	151.101.65.67	54308 / tcp	80 (http) / tcp	HTTP	CNN.com	Medium	Medium	http://cnn.com/

이 정보를 염두에 두고 **firewall-engine-debug**를 실행합니다. 디버그 출력에서 트래픽은 애플리케이션 태그에 따라 차단됩니다.

```
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 New session
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 Starting with minimum 4, 'block by tag', and SrcZone first with zones 1 -> 2, 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
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 pending rule order 4, 'block by tag', AppID
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 Starting with minimum 4, 'block by tag', and SrcZone first with zones 1 -> 2, 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
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 pending rule order 4, 'block by tag', AppID
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 Starting with minimum 4, 'block by tag', and SrcZone first with zones 1 -> 2, 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
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 pending rule order 4, 'block by tag', AppID
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 URL SI: ShmDBLookupURL("http://cnn.com/") returned 0
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 Starting with minimum 4, 'block by tag', and SrcZone first with zones 1 -> 2, geo 0(0) -> 0,
vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 676, payload 1190, client 638, misc 0, user 9999997, url http://cnn.com/, xff
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 match rule order 4, 'block by tag', action Block
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 sending block response of 605 bytes
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 Deleting session
```

http://cnn.com을 명시적으로 차단한 규칙은 없지만, 태그가 지정된 **디스플레이 광고**는 ACP 규칙의 **애플리케이션** 탭 내에서 차단되고 있습니다.



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/1176
system support firewall-engine-debug 및 **system-support-trace** 출력	지침은 이 문서를 참조하십시오.
액세스 제어 정책 내보내기	**시스템 > 툴 > 가져오기/내보내기**로 이동하여 액세스 제어 정책을 선택하고 **내보내기**

주의: ACP에 SSL 정책이 포함된 경우 내보내기 전에 ACP에서 SSL 정책을 제거하여 민감한 PKI 정보가 노출되지 않도록 하십시오.

다음 단계: SSL 정책 레이어 문제 해결

SSL 정책을 사용 중이고 액세스 제어 정책 문제 해결에서 문제가 발견되지 않는 경우 다음 단계로 SSL 정책의 문제 해결을 수행합니다.

다음 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.