Firepower 디바이스의 규칙 확장 이해

목차

소개

이 문서에서는 FMC(Firepower Management Center)에서 구축한 센서에 적용되는 액세스 제어 규칙 변환에 대해 설명합니다.

사전 요구 사항

요건

다음 항목에 대해 알고 있는 것이 좋습니다.

- Firepower 기술에 대한 사항
- FMC에서 액세스 제어 정책을 구성하는 방법에 대한 사항

사용되는 구성 요소

이 문서의 정보는 아래의 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Firepower Management Center 버전 6.0.0 이상
- 소프트웨어 버전 6.0.1 이상을 실행하는 ASA Firepower Defense 이미지(ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X)

- 소프트웨어 버전 6.0.0 이상을 실행하는 ASA Firepower SFR 이미지(ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X)

- Firepower 7000/8000 Series 센서 버전 6.0.0 이상

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

배경 정보

액세스 제어 규칙은 다음 파라미터 중 하나 또는 여러 파라미터의 조합을 사용하여 생성됩니다.

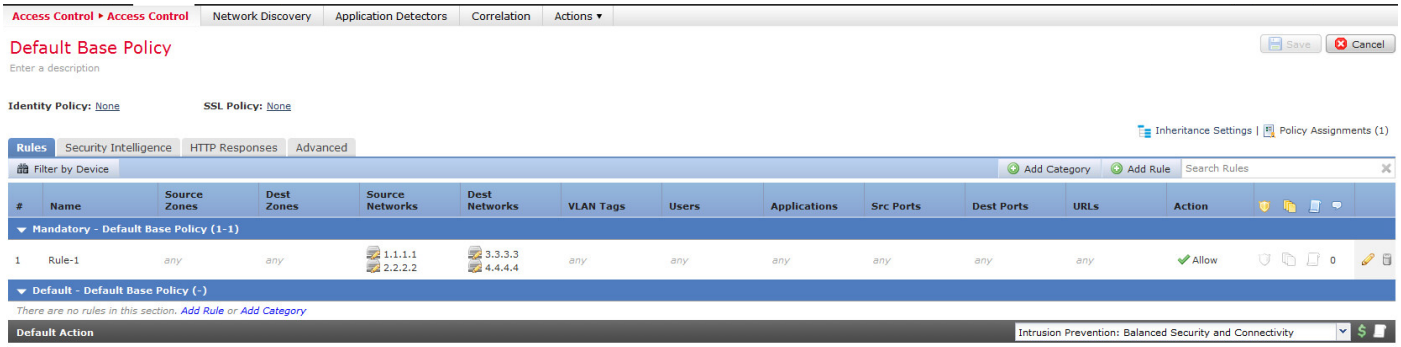
- IP 주소(소스 및 목적지)
- 포트(소스 및 목적지)
- URL(시스템 제공 범주 및 맞춤형 URL)
- Application Detectors
- VLAN
- 영역

액세스 규칙에서 사용되는 파라미터의 조합에 따라 센서에서 규칙 확장이 변경됩니다. 이 문서에서는 FMC의 다양한 규칙 조합과 이러한 각 조합에 연관된 센서의 개별 확장에 대해 중점적으로 설명합니다.

규칙 확장 이해

IP 기반 규칙 확장

아래 그림에 나와 있는 것과 같은 FMC의 액세스 규칙 컨피그레이션을 가정해 보겠습니다.



이 컨피그레이션에는 Management Center의 단일 규칙이 포함되어 있습니다. 그러나 센서에서 구축하고 나면 이 규칙은 그림에 나와 있는 것처럼 **4개** 규칙으로 확장됩니다.

```
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 any any any  (log dcforward flowstart)
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 any any any  (log dcforward flowstart)
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 any any any  (log dcforward flowstart)
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 any any any  (log dcforward flowstart)
268435456 allow any any  any any any  any any any  (ipspolicy 2)
```

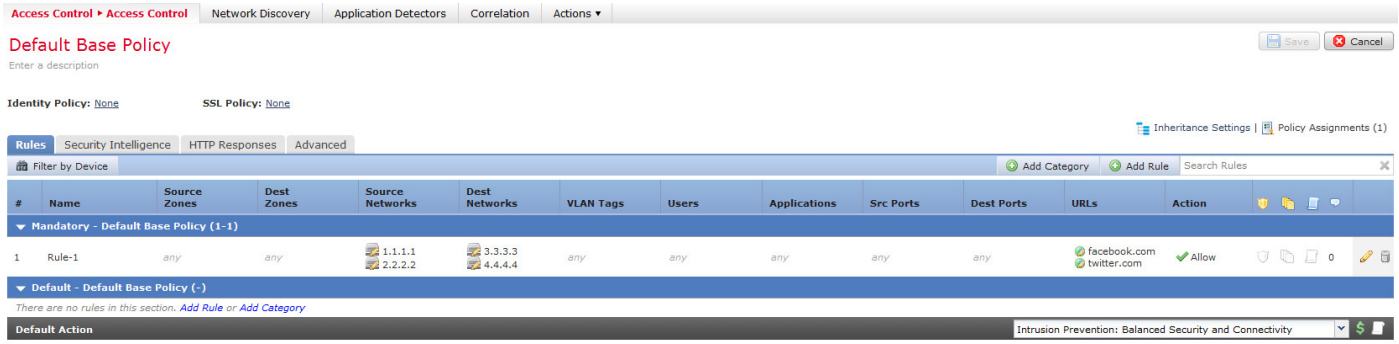
소스로 구성된 2개 서브넷과 대상 주소로 구성된 2개 호스트가 포함된 규칙을 구축하면 센서에서

이 규칙은 4개 규칙으로 확장됩니다.

> **참고**: 대상 네트워크를 기준으로 액세스를 차단하는 요건이 적용되는 경우 보안 인텔리전스의 블랙리스트 기능을 사용하여 이 확장을 수행하는 것이 더욱 효율적입니다.

맞춤형 URL을 사용하여 IP 기반 규칙 확장

아래 그림에 나와 있는 것과 같은 FMC의 액세스 규칙 컨피그레이션을 가정해 보겠습니다.



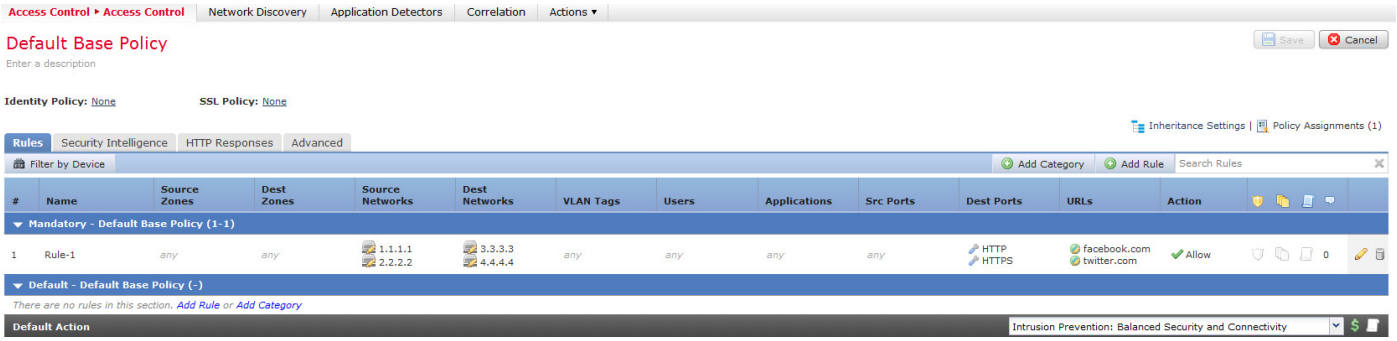
이 컨피그레이션에는 Management Center의 단일 규칙이 포함되어 있습니다. 그러나 센서에서 구축하고 나면 이 규칙은 그림에 나와 있는 것처럼 8개 규칙으로 확장됩니다.

```
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 any any any  (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 any any any  (log dcforward flowstart) (url
"twitter.com")
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 any any any  (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 any any any  (log dcforward flowstart) (url
"twitter.com")
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 any any any  (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 any any any  (log dcforward flowstart) (url
"twitter.com")
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 any any any  (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 any any any  (log dcforward flowstart) (url
"twitter.com")
268435456 allow any any  any any any  any any any  (ipspolicy 2)
```

Management Center의 단일 규칙에서 소스로 구성된 2개 서브넷, 대상 주소로 구성된 2개 호스트, 그리고 맞춤형 URL 개체 2개가 포함된 규칙을 구축하면 센서에서 이 규칙은 8개 규칙으로 확장됩니다. 즉, 각 맞춤형 URL 범주에 대해 소스 및 목적지 IP/포트 범위 조합이 구성 및 생성됩니다.

포트를 사용하여 IP 기반 규칙 확장

아래 그림에 나와 있는 것과 같은 FMC의 액세스 규칙 컨피그레이션을 가정해 보겠습니다.



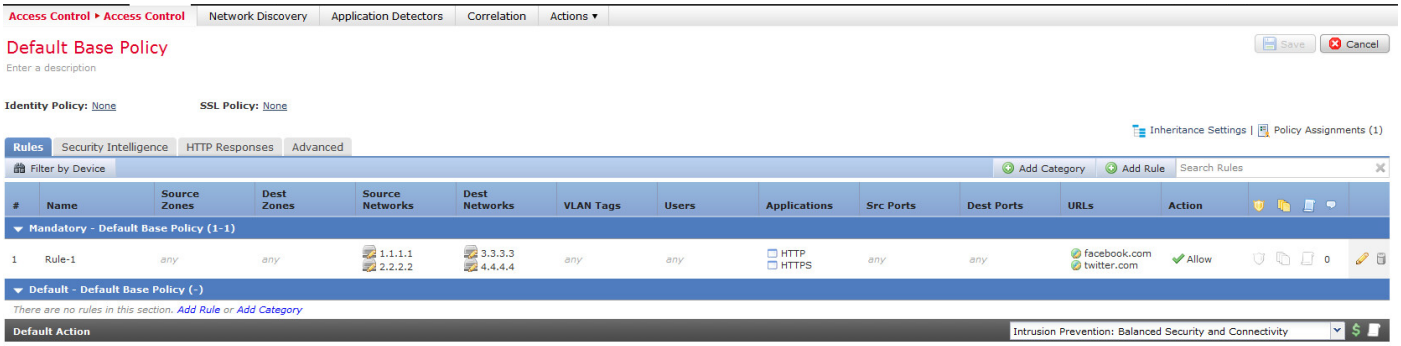
이 컨피그레이션에는 Management Center의 단일 규칙이 포함되어 있습니다. 그러나 센서에서 구축하고 나면 이 규칙은 그림에 나와 있는 것처럼 16개 규칙으로 확장됩니다.

```
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 80 any 6 (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 80 any 6 (log dcforward flowstart) (url
"twitter.com")
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 443 any 6 (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 443 any 6 (log dcforward flowstart) (url
"twitter.com")
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 80 any 6 (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 80 any 6 (log dcforward flowstart) (url
"twitter.com")
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 443 any 6 (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 443 any 6 (log dcforward flowstart) (url
"twitter.com")
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 80 any 6 (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 80 any 6 (log dcforward flowstart) (url
"twitter.com")
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 443 any 6 (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 443 any 6 (log dcforward flowstart) (url
"twitter.com")
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 80 any 6 (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 80 any 6 (log dcforward flowstart) (url
"twitter.com")
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 443 any 6 (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 443 any 6 (log dcforward flowstart) (url
"twitter.com")
268435456 allow any any any any any any any any (ipspolicy 2)
```

소스로 구성된 2개 서브넷, 대상 주소로 구성된 2개 호스트, 그리고 2개 포트를 대상으로 하는 맞춤형 URL 개체 2개가 포함된 규칙을 구축하면 센서에서 이 규칙은 16개 규칙으로 확장됩니다.

> **참고**: 액세스 규칙에 포트를 사용해야 하는 요건이 있으면 표준 애플리케이션용으로 포함되어 있는 **애플리케이션 탐지기**를 사용합니다. 이렇게 하면 효율적인 방식으로 규칙을 확장할 수 있습니다.

아래 그림에 나와 있는 것과 같은 FMC의 액세스 규칙 컨피그레이션을 가정해 보겠습니다.

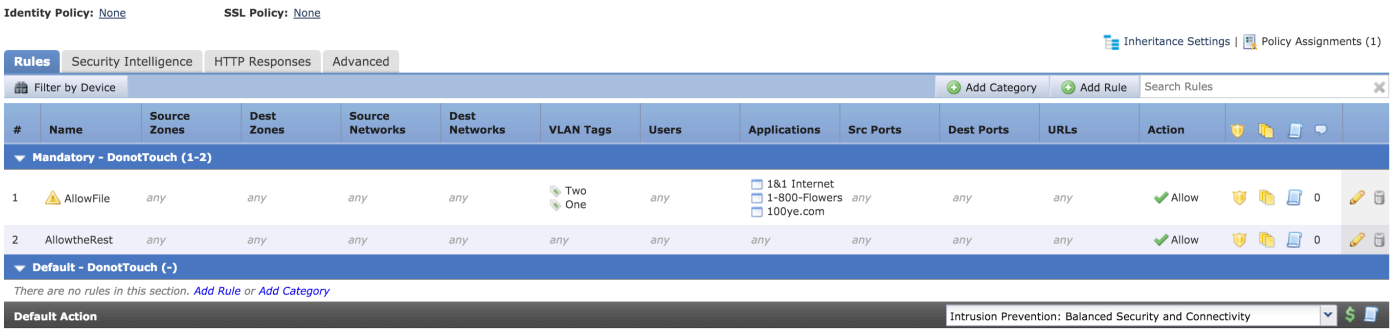


포트 대신 애플리케이션 탐지기를 사용하면 그림에 나와 있는 것처럼 확장되는 규칙의 수가 16개에서 8개로 줄어듭니다.

```
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 any any any (log dcforward flowstart) (appid
676:1, 1122:1) (url "facebook.com")
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 any any any (log dcforward flowstart) (appid
676:1, 1122:1) (url "twitter.com")
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 any any any (log dcforward flowstart) (appid
676:1, 1122:1) (url "facebook.com")
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 any any any (log dcforward flowstart) (appid
676:1, 1122:1) (url "twitter.com")
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 any any any (log dcforward flowstart) (appid
676:1, 1122:1) (url "facebook.com")
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 any any any (log dcforward flowstart) (appid
676:1, 1122:1) (url "twitter.com")
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 any any any (log dcforward flowstart) (appid
676:1, 1122:1) (url "facebook.com")
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 any any any (log dcforward flowstart) (appid
676:1, 1122:1) (url "twitter.com")
```

VLAN을 사용하여 IP 기반 규칙 확장

아래 그림에 나와 있는 것과 같은 FMC의 액세스 규칙 컨피그레이션을 가정해 보겠습니다.



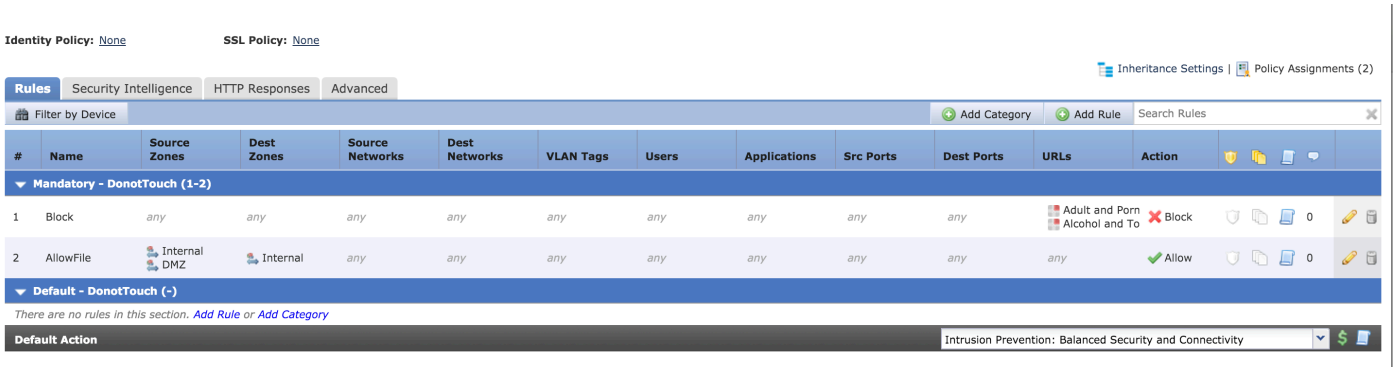
AllowFile 규칙에는 일부 애플리케이션 탐지기, 침입 정책 및 파일 정책의 2개 VLAN ID와 일치하는 줄 하나가 있습니다. AllowFile 규칙은 아래와 같이 2개 규칙으로 확장됩니다.

```
268436480 allow any any any any any any 1 any (log dcforward flowstart) (ipspolicy 5)
(filepolicy 1 enable) (appid 535:4, 1553:4, 3791:4)
268436480 allow any any any any any any 2 any (log dcforward flowstart) (ipspolicy 5)
(filepolicy 1 enable) (appid 535:4, 1553:4, 3791:4)
```

IPS 정책 및 파일 정책은 각 액세스 제어 규칙에 대해 고유하지만, 같은 규칙에서 여러 애플리케이션 탐지기를 참조하므로 애플리케이션 탐지기는 확장에 포함되지 않습니다. 즉, VLAN ID 2개와 애플리케이션 탐지기 3개가 포함된 규칙이 있다고 가정하면 각 VLAN에 대해 하나씩 2개의 규칙만 생성됩니다.

URL 범주가 포함된 IP 기반 규칙 확장

아래 그림에 나와 있는 것과 같은 FMC의 액세스 규칙 컨피그레이션을 가정해 보겠습니다.



차단 규칙은 **Adult and pornography Any Reputation(성인 및 음란물 모든 평판)** 및 **Alcohol and Tobacco Reputations 1-3(주류 및 담배 평판 1~3)**의 URL 범주를 차단합니다. 이 규칙은 Management Center의 단일 규칙이지만 센서에 구축하면 아래에 나와 있는 것처럼 2개 규칙으로 확장됩니다.

```
268438530 deny any any  any any any  any any any  (log dcforward flowstart) (urlcat 11)
268438530 deny any any  any any any  any any any  (log dcforward flowstart) (urlcat 76) (urlrep
le 60)
```

소스로 구성된 2개 서브넷, 대상 주소로 구성된 2개 호스트, 2개 포트를 대상으로 하는 맞춤형 URL 개체 2개 및 URL 범주 2개가 포함된 단일 규칙을 구축하면 센서에서 이 규칙은 32개 규칙으로 확장됩니다.

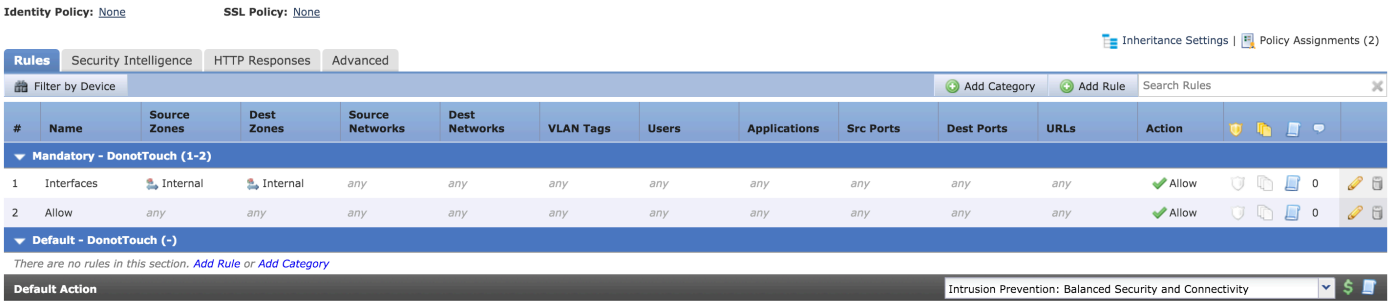
영역이 포함된 IP 기반 규칙 확장

영역은 정책에서 참조하는 할당된 번호입니다.

정책에서 참조하는 영역이 정책을 푸시하는 디바이스의 인터페이스에 할당되어 있지 않으면 해당 영역은 **임의**로 간주되며, 영역이 **임의** 인 경우 규칙은 확장되지 않습니다.

규칙에서 보안 영역과 대상 영역이 같으면 영역 요소는 **임의**로 간주되며, 영역이 임의이면 규칙은 확장되지 않으므로 규칙이 하나만 생성됩니다.

아래 그림에 나와 있는 것과 같은 FMC의 액세스 규칙 컨피그레이션을 가정해 보겠습니다.



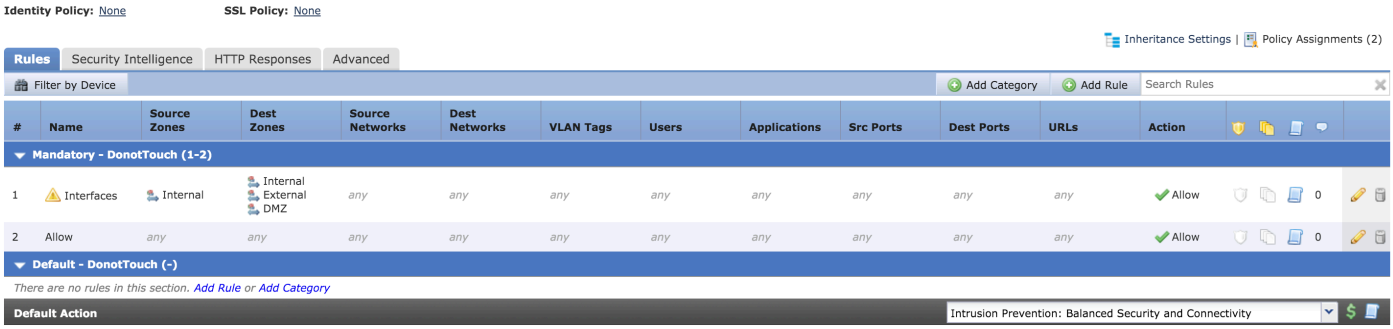
이 컨피그레이션에는 두 개의 규칙이 있는데, 한 규칙에는 영역이 구성되어 있지만 소스 영역과 대상 영역이 같으며 다른 규칙에는 구체적인 컨피그레이션이 없습니다. 이 예에서 **Interfaces(인터페이스)** 액세스 규칙은 규칙으로 변환되지 않습니다.

```
268438531 allow any any any any any any any any (log dcforward flowstart)<-----Allow Access Rule
268434432 allow any any any any any any any any (log dcforward flowstart) (ipspolicy 17)<-------
---Default Intrusion Prevention Rule
```

영역 기반 제어가 같은 인터페이스에 적용되는 경우에는 규칙이 확장되지 않으므로 센서에서는 두 규칙이 모두 동일하게 표시됩니다.

규칙에서 참조되는 영역이 디바이스의 인터페이스에 할당되어 있어야 영역 기반 액세스 제어 규칙 액세스를 위한 규칙이 확장됩니다.

아래에 나와 있는 것과 같은 FMC의 액세스 규칙 컨피그레이션을 가정해 보겠습니다.



여기서 규칙 인터페이스에는 소스 영역에 영역 기반 규칙이 적용되어 있으며 내부 영역과 대상 영역이 내부, 외부, DMZ로 포함되어 있습니다. 이 규칙에서는 인터페이스에 내부 및 DMZ 인터페이스 영역이 구성되어 있으며 외부 영역은 디바이스에 없습니다. 이와 동일한 규칙은 아래와 같이 확장됩니다.

```
268436480 allow 0 any any 2 any any any any (log dcforward flowstart) <------Rule for Internal
to DMZ)
268438531 allow any any any any any any any any (log dcforward flowstart)<--------Allow Access
rule
268434432 allow any any any any any any any any (log dcforward flowstart) (ipspolicy 17)<-------
-Default Intrusion Prevention: Balanced Security over Connectivity
```

여기서는 영역이 명확하게 지정된 특정 인터페이스 페어, 즉 **Internal(내부) > DMZ**에 대해서는 규칙이 생성되지만, **Internal(내부) > Internal(내부)** 규칙은 생성되지 않습니다.

확장되는 규칙의 수는 **유효한** 연결된 영역에 대해 생성할 수 있는 영역 소스 및 대상 페어의 수에 비례하며, 여기에는 동일한 소스 및 대상 영역 규칙이 포함됩니다.

규칙 확장을 위한 일반 공식

센서의 규칙 수 = (소스 서브넷 또는 호스트의 수) * (대상 서브넷의 수) * (소스 포트 수) * (목적지 포트 수) * (맞춤형 URL의 수) * (VLAN 태그의 수) * (URL 범주의 수) * (유효한 소스 및 대상 영역 페어의 수)

> **참고**: 계산 시에는 필드의 **임의** 값이 1로 대체됩니다. 즉, 규칙 조합에서 **임의** 값은 1로 간주되며 규칙은 증가하거나 확장되지 않습니다.

규칙 확장으로 인한 구축 장애 트러블슈팅

액세스 규칙에 항목을 추가한 후에 구축에서 장애가 발생하는 경우 규칙 확장 제한에 도달했다면

아래에 나와 있는 단계를 수행합니다.

/var/log/action.queue.log에서 다음 키워드가 포함된 메시지를 확인합니다.

오류 - 너무 많은 규칙 - 작성 중인 규칙 28개, 최대 규칙 수 9094개

위의 메시지는 확장 중인 규칙 수에 문제가 있음을 나타냅니다. 이 경우 FMC의 컨피그레이션을 확인하여 위에서 설명한 시나리오에 따라 규칙을 최적화하십시오.

- **Firepower Management Center ， 6.0**
- ** & - Cisco Systems**