# Secure FTD에서 Snort 3 Rate Filter로 속도 기반 공격 방지 구성

## 문제

특히 SYN 플러드 공격 방지와 관련하여 여러 서브넷을 포괄하는 규칙을 구성하고, 구현을 위한 모범 사례를 이해하고, 알림 또는 차단을 위한 적절한 임계값(초당 개수)을 결정하는 데 중점을 둡니다.

## 환경

- FTD 7.4.2.4를 실행하는 Cisco Secure Firewall Firepower
- Firepower 2110 하드웨어 플랫폼
- FMC(Firepower 관리 센터) 7.6.2.1에서 관리
- Snort 3 Intrusion Prevention System(rate_filter inspector 활성화)
- SYN 플러드로부터 보호해야 하는 여러 내부 서브넷
- 활성 장애가 없습니다. 사전 대응적 방어를 위한 구성 지침

## 해결

이 단계에서는 Cisco Secure Firewall FTD의 Snort 3 rate_filter 인스펙터를 사용하여 속도 기반 공격 방지를 구성하고 구현하는 방법과 여러 서브넷에 대한 규칙 구조 설명 및 모범 사례 권장 사항을 자세히 설명합니다. 이러한 작업은 정상적인 트래픽에 대한 기준을 설정하고 SYN 플러드 공격을 효과적으로 탐지하거나 차단할 수 있도록 하기 위한 것입니다.

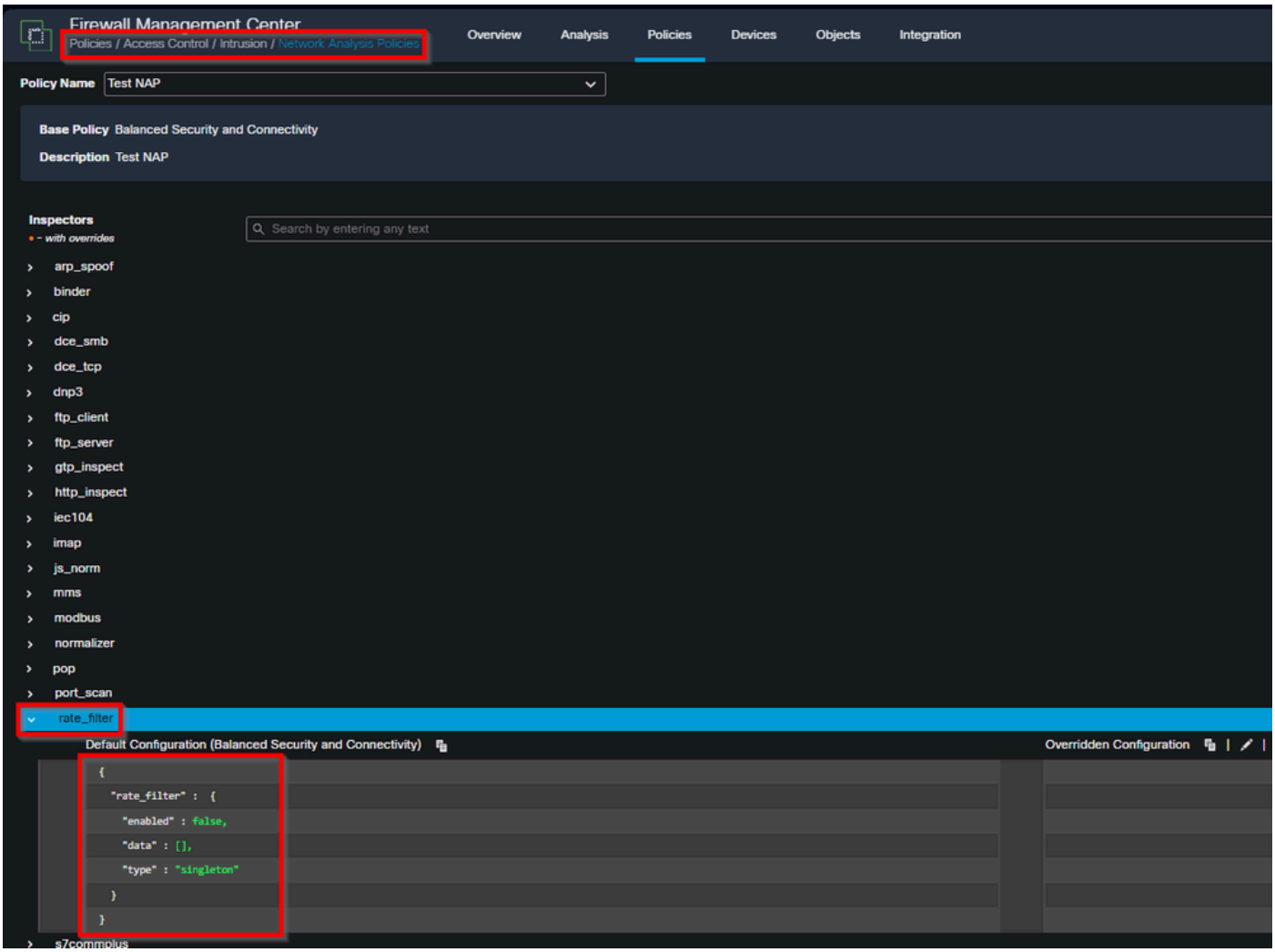
---

참고: 이러한 규칙 필터에 대한 특정 값을 제안하거나 권장하는 것은 TAC 작업 범위에 포함되지 않습니다. 각 환경은 다르며 이러한 필터에 가장 적합한 값을 결정하기 위해 트래픽 패턴에 대한 심층 분석 및 네트워크 설계가 필요합니다.

---

## 1: Snort 3 rate_filter로 이동합니다

이러한 필터는 Policies(정책) > Access Control(액세스 제어): Intrusion(침입) > Network Analysis Policies(네트워크 분석 정책)에서 NAP 정책에 대한 Snort 3 Version(Snort 3 버전)을 클릭한 다음 왼쪽 패널에서 rate_filter 드롭다운 목록을 클릭하여 구성합니다.




inline_image_0.png

## 2: Snort 3 속도 필터 규칙 구조 이해

Snort 3의 rate_filter 관리자를 사용하면 특정 트래픽 유형(예: SYN 패킷)을 모니터링하고 정의된 임계값을 초과할 때 작업(경고 또는 삭제)을 수행하는 규칙을 정의할 수 있습니다. 이러한 규칙은 여러 서브넷을 대상으로 할 수 있습니다.

여러 서브넷에 대한 rate_filter 컨피그레이션 예:

```
{
  "rate_filter": {
```

```
    "data": [
      {
        "apply_to": ["10.1.2.0/24", "10.1.3.0/24"],
        "count": 5,
        "gid": 135,
        "sid": 1,
        "new_action": "alert",
        "seconds": 10,
        "timeout": 15,
        "track": "by_src"
      }
    ],
    "enabled": true,
    "type": "singleton"
  }
}
```

매개변수 설명:

- apply_to: 필터가 적용되는 IP 주소 또는 서브넷 목록입니다(여러 서브넷 지원).
- count + seconds: 이벤트에 대한 임계값(예: 10초 내에 5개의 SYN 패킷)입니다.
- gid/sid: Snort 이벤트를 식별합니다(예: GID 135, SYN 플러드 탐지를 위한 SID 1).
- new_action: 임계값을 초과할 때 수행할 작업(예: alert, drop).
- timeout: 동일한 조건에 대해 새 경고/작업이 트리거되기 전의 기간입니다.
- track: 추적 모드(예: 소스 IP별로 by_src, 대상 IP별로 by_dst).

## 3: 임계값 조정 및 정책 구축을 위한 모범 사례

- 경고 모드에서 시작: 오탐을 방지하려면 new_action을 경고로 설정하고 보존적 임계값(예: 더 높은 개수 및 초)을 사용합니다.
- 기본 네트워크 트래픽: 생성된 이벤트를 모니터링하여 환경 및 서브넷에 대한 "정상적인" SYN 속도를 파악합니다.
- 반복적인 매개변수 조정: 관찰된 트래픽 패턴 및 운영 요구에 따라 카운트, 초 및 시간 제한을 조정합니다.
- 차단으로 이동: 임계값에 비정상적인 동작이 정확히 반영되었다고 확신하면, new_action을 alert에서 drop 또는 그에 준하는 것으로 변경하여 능동적으로 공격을 차단합니다.
- 필요에 따라 별도의 필터: 트래픽 패턴이 다를 경우 서로 다른 세그먼트 또는 역할(예: 서버 대 사용자 서브넷)에 대해 서로 다른 속도 제한을 고려하십시오.
- 지속적인 모니터링: rate_filter 이벤트에 대한 경고 및 모니터링을 유지하여 튜닝 문제 또는 활성 위협을 신속하게 식별합니다.

## 원인

없음. 이전 SYN 플러드 인시던트로 인해 사전 보안 및 지침으로 구성이 요청되었습니다.

## 관련 콘텐츠

- Snort 3 인스펙터 참조: 속도 필터
- Cisco Secure Firewall Management Center Device Configuration Guide, 7.4: 속도 기반 공격 방지
- Cisco 기술 지원 및 다운로드

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.