

ASA FAQ: ASA가 IPS 정책 컨피그레이션이 없는 IPS 모듈에 패킷을 전송하는 이유는 무엇입니까?

목차

[소개](#)

[Q. 구성된 IPS 정책이 없는 경우 ASA가 검사를 위해 IPS 모듈에 패킷을 전송하는 이유는 무엇입니까?](#)

[관련 정보](#)

소개

이 문서에서는 컨피그레이션에 IPS(Intrusion Prevention System) 모듈 정책이 없을 때 Cisco ASA(Adaptive Security Appliance)가 검사를 위해 임베디드 서비스 모듈로 트래픽을 보내는 이유에 대해 설명합니다.

Q. 구성된 IPS 정책이 없는 경우 ASA가 검사를 위해 IPS 모듈에 패킷을 전송하는 이유는 무엇입니까?

A.

ASA가 구성되었을 때 검사를 위해 트래픽을 IPS 모듈로 전송하도록 연결이 구축되었고 해당 연결이 여전히 활성 상태일 수 있습니다.

예를 들어, ASA5515-IPS를 사용하는 고객은 정책 맵에 트래픽을 소프트웨어 IPS 모듈로 전송하도록 구성된 정책이 없습니다. 그러나 트래픽은 ASA에서 모듈에 도착합니다.

IPS에서 패킷 표시 기능을 사용하면 ASA에서 IPS로 들어오는 트래픽을 확인할 수 있습니다.

```
14:34:38.341927 IP 192.168.1.2.1719 > 192.168.10.39.1888: UDP, length 128
14:34:38.341992 IP 192.168.1.2.1719 > 192.168.10.39.1888: UDP, length 128
14:34:38.345031 IP 192.168.1.2.1719 > 192.168.110.39.1888: UDP, length 34
14:34:38.345068 IP 192.168.1.2.1719 > 192.168.110.39.1888: UDP, length 34
IPS 센싱 인터페이스의 인터페이스 통계가 지워지고 패킷이 수신되었습니다.
```

```
sensor# show interfaces portChannel
MAC statistics from interface PortChannel0/0
Interface function = Sensing interface
Description =
Media Type = backplane
Default Vlan = 0
InlineMode = Unpaired
```

Pair Status = N/A
Hardware Bypass Capable = No
Hardware Bypass Paired = N/A
Link Status = Up
Admin Enabled Status = Enabled
Link Speed = N/A
Link Duplex = N/A
Missed Packet Percentage = 0
Total Packets Received = 128
Total Bytes Received = 17904
Total Packets Transmitted = 128
Total Bytes Transmitted = 17904

문제의 원인은 과거에 ASA에 트래픽을 IPS 모듈로 전송하기 위해 컨피그레이션이 추가되었고 ASA에서 IPS 컨피그레이션이 제거된 후 연결이 해제되지 않았기 때문입니다. 이는 트래픽을 지속적으로 전달하는 비 TCP 프로토콜에서 흔히 발생합니다.

ASA에서 **show conn** 명령을 입력하여 IPS 모듈에 있는 패킷에 연결 항목이 있는지 확인합니다. 업타임을 보려면 **show conn detail** 명령을 입력합니다. 연결이 IPS로 리디렉션되지 않도록 하려면 특정 연결을 지우려면 ASA에서 **clear conn<address>** 명령을 입력해야 합니다.

```
ASA# clear conn address 192.168.1.2
3 connection(s) deleted.
ASA#
```

관련 정보

- [기술 지원 및 문서 - Cisco Systems](#)