ASA FAQ: Why does the ASA send packets to the IPS module with no IPS policy configuration?

Document ID: 116145

Contributed by Prapanch Ramamoorthy and Abhishek Prabhakar, Cisco
TAC Engineers.

Jun 07, 2013

Contents

Introduction

This document describes why the Cisco Adaptive Security Appliance (ASA) might send traffic to an embedded service module for inspection when there is no Intrusion Prevention System (IPS) module policy in the configuration.

Q. Why does the ASA send packets to the IPS module for inspection when there is no IPS policy configured?

A.

It is possible that a connection was built to send traffic to the IPS module for inspection when the ASA was configured, and that connection is still active.

For example, a customer with an ASA5515−IPS has no configured policy in a policy map to send the traffic to the software IPS module; however, traffic arrives at the module from the ASA.

When you use the packet display feature on the IPS, you can see the traffic that comes to the IPS from the ASA:

```
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
```

The interface statistics on the IPS sensing interface were cleared, and packets were received:

```
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
```

The cause of the issue is that sometime in the past a configuration was added to the ASA to send traffic to the IPS module, and the connnections were not cleared out after the IPS configuration was removed on the ASA. This is common with non−TCP protocols that constantly pass traffic.

On the ASA, enter the ***show conn*** command to determine if the packets that you see on the IPS module have connection entries. In order to see the uptimes, enter the ***show conn detail*** command. In order to ensure the connections are not re−directed to the IPS, you might have to enter the ***clear conn <address>*** command on the ASA to clear those specific connections:

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

Related Information

- ***Technical Support & Documentation − Cisco Systems***

Updated: Jun 07, 2013 Document ID: 116145