CHAPTER 5

Integrated Intrusion Detection Security

The Cisco NX-OS software provides IPv4 and IPv6 Intrusion Detection packet checks to increase security in the network by dropping packets that match specific criteria that are typically not required in most production networks. Most Intrusion Detection System (IDS) packet checks are enabled by default and should be left enabled unless there is a specific reason to disable them.

This chapter includes the following sections:

Verifying IDS Check Status and Counters

Introduced: Cisco NX-OS Release 4.0(1)

The **show hardware forwarding ip verify** command should be used to verify the IDS packet check status and associated counters. The **module** option displays counters for a specific module as opposed to all modules. The "Packets Failed" counter displays the number of packets dropped for each IDS packet check. This output can be useful when troubleshooting potential network related application issues. In some rare situations, an IDS packet check may need to be disabled if an application meets the IDS packet check criteria. Cisco NX-OS Release 5.0(3) introduced Syslog messages and Embedded Event Manager (EEM) trigger support when packets are dropped. The IDS packet check counters can be cleared using the **clear hardware forwarding ip verify protocol** command. The **module** option allows the administrator to clear the counters for a specific module.

```
n7000# show hardware forwarding ip verify

IPv4 and v6 IDS Checks          Status     Packets Failed
-----------------------------+---------+------------------
address source broadcast        Enabled    0
address source multicast        Enabled    0
address destination zero        Enabled    0
address identical               Enabled    0
address reserved                Enabled    0
address class-e                 Disabled   --
checksum                        Enabled    0
protocol                        Enabled    0
fragment                        Disabled   --
length minimum                  Enabled    0
length consistent               Enabled    0
length maximum max-frag         Enabled    0
length maximum udp              Disabled   --
length maximum max-tcp          Enabled    0
```

```
tcp flags                       Disabled   --
tcp tiny-frag                   Enabled    0
version                         Enabled    0
-----------------------------+---------+------------------
IPv6 IDS Checks                 Status     Packets Failed
-----------------------------+---------+------------------
length consistent               Enabled    0
length maximum max-frag         Enabled    0
length maximum udp              Disabled   --
length maximum max-tcp          Enabled    0
```

Disabling/Enabling IDS Packet Checks

Introduced: Cisco NX-OS Release 4.0(1)

This section was included for reference and may not be required.

There may be some situations when an IDS packet check needs to be disabled for an application to function properly. The following global command can be used to disable and enable a packet check. This example disables and enables the “length maximum max-tcp” IDS check. Other packet checks can be configured using the same procedure.

```
n7000(config)# no hardware ip verify length maximum max-tcp

n7000(config)# hardware ip verify length maximum max-tcp
```