CHAPTER 4

Protecting the CPU

This chapter provides the recommended best practices for protecting the CPU against Denial of Service (DoS) attacks.

This chapter includes the following sections:

CoPP Policy

This section contains a brief overview of the Control Plane Policing (CoPP) Policy. The CoPP policy is an important security feature that prevents Denial of Service (DoS) attacks that can impact the supervisor module CPU. The Cisco NX-OS software defaults to a “strict” policy that was developed to protect the CPU from the most common threats. We recommend that you enable a CoPP policy any time IP addresses are configured on an I/O module port such as an Ethernet port, SVI, port-channel, etc. A detailed explanation and recommendation for the CoPP Policy is outside the of scope for this document.

Denying In-Band Management Protocols

Introduced: Cisco NX-OS Release 4.0(1)

While this document does not cover the CoPP policy in detail, we recommend that you modify the CoPP policy to drop in-band management traffic destined to the Cisco Nexus 7000 Series switches to increase security. If all IP management traffic is traversing the out-of-band management network, there should not be any need to receive any IP management traffic in-band. The CoPP policy does not get applied to traffic received on the mgmt0 interface.

Recommended steps:

1. Identify the enabled management protocols that should have their traffic dropped in-band, such as SSHv2, SNMP, SCP, TFTP, FTP, etc.
2. Create a new access control list(s) and a new class map(s), or reference the existing class map with the **class-map type control-plane match-any copp-system-class-management** command that references existing access control lists.
3. Insert the new class map or modify the existing class map identified in step 2 in the existing CoPP service policy (copp-system-policy), and then configure it to drop all traffic that conforms to the policy.

This example uses the existing **copp-system-class-management** class-map and associated ACLs. The police rate was modified to aggressively drop traffic that conforms to the policy.

```
n7000(config)# policy-map type control-plane copp-system-policy
n7000(config-pmap)# class copp-system-class-management
n7000(config-pmap-c)# police 1 conform drop
```


Note As of Cisco NX-OS Release 5.1(1), the default **copp-system-class-management** class map contains the following protocols: FTP, NTP, NTP6, RADIUS, SFTP, SNMP, SSH, SSH6, TACACS, Telnet, TFTP, TFTP6, RADIUS, TACACS6, and Telnet6.

Syslog Message Thresholds

Introduced: Cisco NX-OS Release 5.1(1)

A Syslog message threshold can be configured per CoPP class map under the control plane policy map. We recommend that you configure a Syslog message threshold for class maps as a method to inform the proper personnel that the CoPP policy is dropping traffic. The following example configures a threshold at 39,600 kb/s with a severity level of 5, so packet drops within the critical class (routing protocols) are logged.

```
n7000(config)# policy-map type control-plane copp-system-policy
n7000(config-pmap)# class copp-system-class-critical
n7000(config-pmap-c)# logging drop threshold 39600000 level 5
```

Syslog Message Example:

```
n7000# show log logfile

%COPP-5-COPP_DROPS5: CoPP drops exceed threshold in class: copp-system-class-critical,
check show policy-map interface control-plane for more info.
```

CPU Rate Limit Logging

Introduced: Cisco NX-OS Release 5.1(1)

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

Rate limiting can be configured globally and per interface to create a system log message if packets sent to or from the supervisor module CPU exceed the configured packet per second (pps) threshold. The rate limiter can be configured to measure traffic based on direction using the **input** (received), **output** (transmitted) or **both** (configures received and transmitted simultaneously) options. The global default threshold is 10,000 pps configured for **both**. The threshold can be modified to a value between 0 and 100,000 pps. This feature can be applied globally and per interface. This feature does not drop packets; it only sends a notification log message.

Global Configuration:

```
n7000(config)# rate-limit cpu direction both pps 2000 action log
```

Per Interface Configuration:

```
n7000(config)# interface ethernet 1/26
n7000(config-if)# rate-limit cpu direction both pps 2000 action log
```

Verification:

Global Verification:

```
n7000# show system internal pktmgr internal control sw-rate-limit
inband pps global threshold 2000  outband pps global threshold 2000
```

Per Interface Verification:

```
n7000# show system internal pktmgr interface ethernet 1/26
Ethernet1/26, ordinal: 305
  SUP-traffic statistics: (sent/received)
    Packets: 5412033 / 6677105
    Bytes: 1614312187 / 2003104556
    Instant packet rate: 2872 pps / 2871 pps
    Packet rate limiter (Out/In): 2000 pps / 2000 pps
    Average packet rates(1min/5min/15min/EWMA):
    Packet statistics:
      Tx: Unicast 5365387, Multicast 46640
          Broadcast 6
      Rx: Unicast 6677093, Multicast 0
          Broadcast 12
```

Syslog:

```
n7000# show log logfile

%NETSTACK-5-NOTICE:  netstack [3647]  Ingress PPS (2861) exceeding threshold on i/f
Ethernet1/26
```