CHAPTER 4

CPU の保護

この章では、Denial of Service（DoS; サービス拒絶）攻撃から CPU を保護するための推奨ベスト プラクティスについて説明します。

この章で説明する内容は、次のとおりです。

CoPP ポリシー

ここでは、Control Plane Policing（CoPP）ポリシーの概略について説明します。CoPP ポリシーは、スーパーバイザ モジュール CPU に影響を及ぼすおそれがある Denial of Service（DoS; サービス拒絶）攻撃を防ぐための、重要なセキュリティ機能です。Cisco NX-OS ソフトウェアでは、最も共通の脅威から CPU を守るために開発された「strict」ポリシーが、デフォルトで適用されます。イーサネット ポート、SVI、ポート チャネルなどの I/O ポートに IP アドレスが設定されている場合には、常に、CoPP ポリシーをイネーブルにすることを推奨します。CoPP ポリシーについての詳細な説明および推奨事項は、このマニュアルの範囲外で、このマニュアルには含まれていません。

インバンド管理プロトコルの拒否

導入：Cisco NX-OS Release 4.0(1)

このマニュアルでは、CoPP ポリシーの詳細については説明していませんが、Cisco Nexus 7000 シリーズ スイッチ宛てのインバンド管理トラフィックをドロップするには、CoPP ポリシーを変更することを推奨します。すべての IP 管理トラフィックがアウトオブバンド管理ネットワークを経由する場合、IP 管理トラフィックをインバンドで受信する必要はありません。CoPP ポリシーは、mgmt0 インターフェイスで受信されるトラフィックには適用されません。

推奨手順：

1. SSHv2、SNMP、SCP、TFTP、FTP など、インバンドでドロップする必要があるトラフィックがある、イネーブルになっている管理プロトコルを特定します。
2. 新しいアクセス コントロール リストおよび新しいクラス マップを作成するか、または、既存のアクセス コントロール リストを参照する **class-map type control-plane match-any copp-system-class-management** コマンドで、既存のクラス マップを参照します。
3. 既存の CoPP サービス ポリシー（copp-system-policy）で、新しいクラス マップを挿入するか、または、手順 2 で特定された既存のクラス マップを変更し、次に、ポリシーに準拠するすべてのトラフィックをドロップするよう設定します。

次に、既存の **copp-system-class-management** クラス マップおよび関連付けられている ACL を使用する例を示します。ポリシーに準拠するトラフィックが積極的にドロップされるよう、ポリシー レートが変更されました。

```
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
```

（注）　Cisco NX-OS Release 5.1(1) から、デフォルトの **copp-system-class-management** クラス マップには、FTP、NTP、NTP6、RADIUS、SFTP、SNMP、SSH、SSH6、TACACS、Telnet、TFTP、TFTP6、RADIUS、TACACS6、および Telnet6 の各プロトコルが含まれます。

Syslog メッセージのしきい値

導入：Cisco NX-OS Release 5.1(1)

Syslog メッセージのしきい値は、コントロール プレーンのポリシー マップで、CoPP クラス マップごとに設定できます。CoPP ポリシーがトラフィックをドロップしていることを、適切な人員に通知する方式として、クラス マップの Syslog メッセージのしきい値を設定することを推奨します。次に、クラスが Critical（ルーティング プロトコル）以内のパケットのドロップが記録されるよう、重大度レベル 5 で 39,600 Kb/s にしきい値を設定する例を示します。

```
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 メッセージの例：

```
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 レート制限のロギング

導入：Cisco NX-OS Release 5.1(1)

この項は、参考のために記載しており、必要のない場合があります。

スーパーバイザ モジュール CPU へ、または、スーパーバイザ モジュール CPU から、送信されるパケットが、設定された packet per second（pps）のしきい値を超過した場合、グローバルに、および、インターフェイスごとに、レート制限を設定し、システム ログ メッセージを作成できます。レート リミッタを設定し、**input**（受信）オプション、**output**（送信）オプション、または **both**（送受信を同時に設定）オプションを使用して、方向に基づいてトラフィックを測定できます。**both** に設定されるグローバルなデフォルトしきい値は 10,000 pps です。しきい値は、0 ～ 100,000 pps の値に変更できます。この機能は、グローバルに、および、インターフェイスごとに、設定できます。この機能では、パケットはドロップされず、通知ログ メッセージが送信されるだけです。

グローバルに設定：

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

インターフェイスごとに設定：

```
n7000(config)# interface ethernet 1/26
```

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

確認：

グローバルに確認：

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

インターフェイスごとの確認：

```
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
```