Nexus7000 シリーズにおける CoPP を用いたコントロール プレーンへのトラフィック (telnet / ssh) の制限方法

目次

概要

このドキュメントでは、次の設定例について説明します。

Nexus7000 シリーズにおける CoPP を用いたコントロール・プレーンへのトラフィック (telnet/ssh) の制限方法について

前提条件

Nexus7000 シリーズでは、管理インタフェース mgmt 0, cmp-mgmt 上で、アクセス・コントロール・リスト (以降 ACL) によるトラフィック・コントロールをサポートしていますが、ネットワーク・インタフェース (ラインカード上のインタフェース) を経由したコントロール・プレーンへのトラフィックについては、 ACL を用いたトラフィック・コントロールをサポートしておりません。
ここでは代替ソリューションとして、CoPP を用いたコントロール・プレーンへのトラフィック・コントロールについてご紹介させて頂きます。

要件

この設定を開始する前に、次の要件が満たされていることを確認してください。

- Nexus7000 シリーズにおいて、telnet/ssh フィーチャーが有効になっていること

Nexus における telnet/ssh サービスの開始については、コンフィグレーション・ガイドをご参照ください。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- NX-OS 4.0 および 4.1 が Supervisor-1 上で動作する Nexus7000 シリーズ・スイッチ

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。こ

のドキュメント内で使用されているデバイスは、すべてクリアな（デフォルト）設定で作業が開始されています。
対象のネットワークが実稼働中である場合には、すべてのコマンドによる潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

Return to Top

設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を説明します。

注：このドキュメントで使用されているコマンドの詳細情報は、Command Lookup Tool（登録ユーザ専用）を使用してください。

設定例

このドキュメントでは、次の設定を使用します。

- ホスト 192.168.1.1/24 からのみ Nexus への telnet/ssh を許可し、他のホストからの telnet/ssh は許容しない

Step 1 - 既存のアクセスリスト access-list copp-system-acl-telnet, copp-system-acl-ssh を編集し、ホ 192.168.1.1/24 からのみ telnet/ssh アクセスを許容するように変更します。
これらの ACL は、クラスマップcopp-system-class-management で定義されており、デフォ で通信が許可されています。

変更前：
Nexus7000

```
ip access-list copp-system-acl-telnet
  10 permit tcp any any eq telnet
  20 permit tcp any any eq 107
  30 permit tcp any eq telnet any
  40 permit tcp any eq 107 any

ip access-list copp-system-acl-ssh
  10 permit tcp any any eq 22
  20 permit tcp any eq 22 any
```

変更後：
Nexus7000

```
ip access-list copp-system-acl-telnet
```

```
  10 permit tcp 192.168.1.1/24 any eq telnet 20 permit tcp 192.168.1.1/24 any eq 107 ip acc
list copp-system-acl-ssh 10 permit tcp 192.168.1.1/24 any eq 22
```

Nexus7000で許容しない、他のホストからの telnet/ssh トラフィックを copp-system-acl-den
して追加で定義します（アクセスリスト名は任意です）。

Nexus7000

Step 2 -

```
ip access-list copp-system-acl-deny
  10 permit tcp any any eq telnet
  20 permit tcp any any eq 107
  30 permit tcp any any eq 22
```

作成したアクセスリストをもとに 拒否トラフィックを定義するクラスマップを作成します。
ラスマップ名は任意です）

Nexus7000

```
class-map type qos match-all copp-system-class-management-deny
  match access-group name copp-system-acl-deny
```

既存の CoPP として定義されている ポリシーマップ "copp-system-policy" へ Step2 で作成し
ラスマップを "confirm drop violate drop" で適用します。
これにより、192.168.1.1/24 以外のホストからの Nexus7000 に対する telnet/ssh トラフィッ
遮断されます。

Nexus7000

Step 3 -

```
policy-map type control-plane copp-system-policy
  class copp-system-class-critical
    police cir 39600 kbps bc 250 ms conform transmit violate drop
  class copp-system-class-important
    police cir 1060 kbps bc 1000 ms conform transmit violate drop
  class copp-system-class-management
    police cir 10000 kbps bc 250 ms conform transmit violate drop
  class copp-system-class-normal
    police cir 680 kbps bc 250 ms conform transmit violate drop
  class copp-system-class-redirect
    police cir 280 kbps bc 250 ms conform transmit violate drop
  class copp-system-class-monitoring
    police cir 130 kbps bc 1000 ms conform transmit violate drop
  class copp-system-class-exception
    police cir 360 kbps bc 250 ms conform transmit violate drop
  class copp-system-class-undesirable
    police cir 32 kbps bc 250 ms conform drop violate drop
  class copp-system-class-management-deny police cir 100 kbps bc 250 ms conform drop violat
drop class class-dropdefault police cir 100 kbps bc 250 ms conform transmit violate drop
```

ICMP, TFTP, SNMP などのトラフィックについても、ACLを変更することで同様に制御する
が可能です。

Return to Top

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。