Router Control Plane ACL (CoPP/CPPr)

- **Qu'est-ce que le Control Plane Protection (CoPP) ?**
- Le **Control Plane** est la partie du routeur qui gère le **trafic de gestion** : OSPF, BGP, ICMP, SSH, SNMP, etc.
- **CoPP** permet de protéger ce plan contre les attaques DoS (déni de service) ou un trafic excessif.
- Il agit comme un **pare-feu pour le processeur** du routeur.

Router Control Plane ACL (CoPP/CPPr)

Exemple

- Autoriser uniquement ICMP (ping) et SSH vers le routeur.
- Bloquer tout autre type de trafic destiné au control plane.

- R2 veut accéder à R1 via ping et SSH.
- R1 applique CoPP pour filtrer ce qui peut atteindre son processeur.

Router Control Plane ACL (CoPP/CPPr)

- **Étapes de configuration sur R1**

1. Créer une ACL nommée pour définir le trafic autorisé

ip access-list extended PROTECT-CONTROL-PLANE permit icmp any any permit tcp any any eq 22 deny ip any any

*Permet le **ping (ICMP)** et **SSH (port 22)**.*

Bloque tout le reste.

Router Control Plane ACL (CoPP/CPPr)

Exemple

2. Créer une class-map qui fait référence à l'ACL

class-map match-all CM-CTRL-PLANE match access-group name PROTECT-CONTROL-PLANE

Router Control Plane ACL (CoPP/CPPr)

Exemple

3. Créer une policy-map pour appliquer une action (ex : police)

policy-map PM-CTRL-PLANE class CM-CTRL-PLANE police 10000000 8000 8000 conform-action transmit exceed-action drop

4. Appliquer cette policy au control-plane :

control-plane service-policy input PM-CTRL-PLANE

Router Control Plane ACL (CoPP/CPPr)

Exemple

Élément	Signification
police	C’est la commande pour limiter le **trafic** en appliquant une **politique de débit** (traffic policing).
10000000	**Bande passante maximale autorisée** en bits par seconde (**10 Mbps** ici). C'est le **Committed Information Rate** (CIR).
8000	**Taille du burst normal** (Committed Burst Size – CBS), en octets. C’est la quantité de données autorisée instantanément sans pénalité.
8000	**Taille du burst maximal** (Excess Burst Size – EBS), en octets.
conform-action transmit	Si le trafic est **conforme** (dans les limites), il est **transmis**.
exceed-action drop	Si le trafic **dépasse** la limite, il est **supprimé (drop)**.

Router Control Plane ACL (CoPP/CPPr)

Exemple

Ce que fait cette configuration :

Autorise :

- ICMP (ping) vers le routeur R1
- SSH vers R1

Bloque :

- Tout autre trafic non autorisé (ex : Telnet, SNMP, HTTP, etc.)
- Et limite le débit des flux autorisés

- ***show policy-map control-plane***

Router Control Plane ACL (CoPP/CPPr)

Exemple

Ce que fait cette configuration :

Autorise :

- ICMP (ping) vers le routeur R1
- SSH vers R1

Bloque :

- Tout autre trafic non autorisé (ex : Telnet, SNMP, HTTP, etc.)
- Et limite le débit des flux autorisés

VLAN ACL

- Une **VLAN ACL** (aussi appelée **VACL** pour *VLAN Access Control List*) est une liste de contrôle d'accès appliquée **au niveau d'un VLAN** sur un **commutateur Cisco** (généralement un switch de niveau 3, comme le Catalyst 3560 ou supérieur).
- Contrairement aux ACL classiques qui sont appliquées sur des interfaces (entrante ou sortante), les **VACLs s'appliquent à l'ensemble du trafic transitant dans un VLAN donné**, que ce soit du trafic entre ports du même VLAN ou traversant un routeur (*inter-VLAN*).

VLAN ACL

- De **filtrer le trafic entre les hôtes d'un même VLAN** (chose qu'une ACL classique ne fait pas facilement)
- D'**appliquer des règles de sécurité intra-VLAN**
- D'empêcher certaines communications même si les machines sont dans le **même sous-réseau**

VLAN ACL

Configuration

1. Créer une ACL standard

```
ip access-list extended BLOCK-PC1-TO-PC2
 deny ip host 192.168.10.10 host 192.168.10.20
 permit ip any any
```

2. Définir la VLAN access map

```
vlan access-map VACL-MAP 10
 match ip address BLOCK-PC1-TO-PC2
 action drop

vlan access-map VACL-MAP 20
 action forward
```

!3. Appliquer la VACL à un VLAN spécifique

```
vlan filter VACL-MAP vlan-list 10
```

Supposons que vous voulez **empêcher PC1 de communiquer avec PC2,** mais autoriser tout le reste.