ACL Cisco

Cisco offre sur ses matériels de niveau 3 la possibilité de réaliser du filtrage du trafic : on parle **d'ACL (Access Control List)** qui s'appliquent sur les interfaces du matériel, soit en entrée (IN) ou en sortie (OUT).

Principes

Définition et affectation aux interfaces

Les ACL se configurent de la manière suivante :

- Définition de l'ACL :

```
access-list <numéroACL> <actions>
```

- Application de l'ACL à une interface :

```
interface <numInterface>
ip access-group <numéroACL> {in|out}
```

> On ne peut affecter qu'une ACL sur une interface dans un sens (out/in)

Ressources

- Cisco
- https://www.fingerinthenet.com/acl/ : démarches illustrée et bien expliquée

Analyse du trafic et application des règles

Lors de l'analyse du trafic, le principe général du filtrage s'applique :

- parcours des **ACL dans l'ordre** de leur déclaration
- **si une règle correspond au trafic** on **applique l'action** (autorisation ou refus)
- **si aucune règle n'est applicable**, l'action **deny** (refus) est mise en œuvre (règle par défaut)

Les ACL

Cisco offre deux types d'ACL :

- Les **Access-lists Standard** (numéros de 1 à 99): elles permettent de filtrer uniquement sur les IP sources et sont utilisées pour le filtrage, mais aussi pour l'activation du Nat/Pat.
- Les **Access-lists Étendues** (numéros de 100 à 199) : elles permettent de filtrer sur la plupart des champs des en-têtes IP, TCP et UDP.

Syntaxe ACL Standard

Les ACL standard effectuent un filtrage sur l'adressage IP source. Elles peuvent donc servir à :

- gérer le trafic depuis un VLAN
- gérer le trafic depuis une machine

Syntaxe

```
access-list <numero1à99> <action> <ipsource> <masqueInversé>
```

Le **masque inversé** s'écrit à l'opposé du masque de réseau : on place un 0 là ou on veut étudier l'information, et un 1 si on veut l'ignorer. Par exemple :

- Masque inversé pour la classe C : 0.0.0.255
- Masque inversé pour une adresse exacte : 0.0.0.0
- Masque 255.255.192.0 inversé : 0.0.63.255

Exemple

```
access-list 1 permit 192.168.1.254 0.0.0.0
access-list 2 deny 192.168.1 0.0.0.255
```

- L'access-list 1 autorise le trafic depuis un matériel précis
- L'access-list 2 interdit le trafic depuis tout un réseau
- L'ensemble appliqué sur une interface (les deux formulations sont équivalentes) :
  - interdit le trafic pour tout un réseau sauf le matériel .254
  - autorise le trafic pour le matériel .254 et l'interdit pour tous les autres équipements du réseau
- **Remarque** : si on inverse les deux règles (réseau puis équipement), la deuxième ne s'appliquer jamais

Syntaxe ACL étendues

Les ACL étendues correspondent à des règles de filtrage complètes. Elles peuvent porter sur :

- les informations **source** et **destination** du trafic (IP, port, service, etc)
- l'**adressage IP** : any (toute adresse), host pour une machine ou IP+masque inversé pour un (sous)réseau

- les **services réseau**,
  - soit par leur nom pour certains services génériques (ftp, pop3, smtp, telnet, www),
  - soit par leur numéro de port
  - soit any pour toute valeur

Syntaxe

```
access-list <numero> <action> <protocole> <adresseSource> [<service>]
<adresseDestination> [<service>]
```

> La structure de la syntaxe dépendra du **protocole** choisi, certains éléments pouvant ne pas apparaître (les **s<ervice>** si on choisit IP comme protocole par exemple)

Information	Détail
numero	numéro compris entre 100 et 199 ou 2000 et 2699
action	comportement de la règle : * **permit** (autorise) * **deny** (interdit)
protocole	protocole de bas niveau (3 ou 4 du modèle OSI) utilisé * **icmp** * **ip** * **tcp** * **udp** * protocoles de gestion de réseau (RIP, OSPF, GRE, BGP, etc)
adresseSource ou adresseDestination	* **any** : tout adressage * **host <ipMachine>** : une machine précise * **<ipReseau> <masqueInversé>** : un réseau ou sous-réseau IP
service	Définit le ou les ports (source ou destination) à étudier * **eq** :Match only packets on a given port number * **gt** : Match only packets with a greater port number * **lt** : Match only packets with a lower port number * **neq** : Match only packets not on a given port number * **range** :Match only packets in the range of port numbers

Exemples

```
access-list 101 permit tcp any host 192.168.1.254  eq www
access-list 102 permit udp 192.168.1.0 0.0.0.255 any eq domain
access-list 103 permit tcp host 192.168.1.30 host 172.20.2.2 eq 3306
```

- 101 : autorise la communication depuis n'importe où vers le serveur Web (http:80) d'IP 192.168.1.254
- 102 : autorise les postes du réseau 192168/10/24 à interroger tout serveur DNS (domain:53)
- 103 : autorise l'échange depuis la machine 192.168.1.30 vers le serveur 172.20.2.2 en mysql (3306)

ACL nommées et multi-règles

On peut choisir de nommer les ACL plutôt que de les gérer uniquement par des numéros.

De même, il peut être intéressant de gérer une ACL portant sur plusieurs règles pour l'affecter en une seule fois à une interface.

On remplacera la syntaxe

```
access-list
```

par la version

```
ip access-list {extended|standard} <nom>
```

suivi des règles à appliquer.

Exemples

```
ip access-list extended LAN
 permit tcp any host 172.20.1.254  eq www
 permit udp 192.168.1.0 0.0.0.255 any eq domain
 permit tcp host 192.168.1.30 host 172.20.2.2 eq 3306
```

- Définit les échanges du réseau depuis le LAN vers un serveur Web, tout serveur DNS et un échange précis entre une machine et un serveur Mysql

```
ip access-list extended DMZ
 permit 192.168.1.0 0.0.0.255
 permit 192.168.20.0 0.0.0.255
 permit 10.20.0.0 0.0.255.255
```

- Définit les possibilités d'échange depuis les réseaux du LAN. Sera appliqué sur l'interface DMZ en OUT

Affectation aux interfaces

Une fois les ACL définies, on doit les appliquer aux interfaces.

Sur une interface,

From:
https://wiki.sio.bts/ - **WIKI SIO : DEPUIS 2017**

Permanent link:
https://wiki.sio.bts/doku.php?id=ciscoacl&rev=1665395387

Last update: **2022/10/10 09:49**