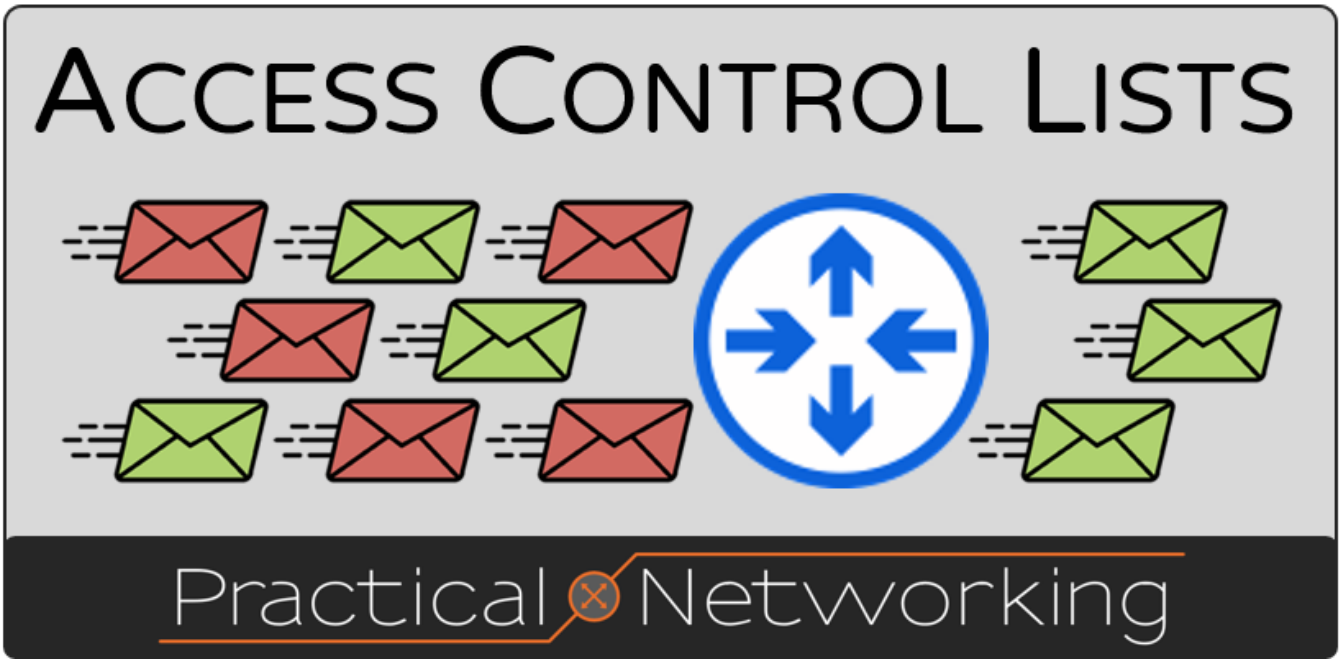
[Cisco] ACL

Introduction

Les **ACLs**, pour *Access Control Lists*, sont des listes de sécurité qui permettent de filtrer les adresses IPs sources pour accéder à certaines ressources.



Configuration

Créer une Access List

Pour une ACL standard :

```
access-list <ACL_ID> <permit|deny> <IP> <REV_MASK>
```

> Le champ **<REV_MASK>** correspond au masque inversé de l'IP à laquelle la règle doit être appliquée.

Et pour une ACL étendue :

```
ip access-list extended <NAME|ID>
```

Puis définissez vos règles :

```
<LINE> <permit|deny> <PROTOCOL> <SRC_IP> <SRC_REV_MASK> <DST_IP> <DST_REV_MASK> eq <PORT>
```

> Notez que les règles fonctionnent de haut en bas et que par défaut, tout le trafic est bloqué.

Appliquer une ACL

Pour appliquer une ACL à une interface :

```
int e0/0
ip access-group <ACL_ID|NAME> <in|out>
```

Pour l'appliquer aux lignes VTY :

```
line vty 0 4
access-class <ACL_ID|NAME> <in|out>
```

Afficher les ACLs

Pour afficher vos ACLs vous pouvez utiliser la commande suivante :

```
show access-lists
```

Vous pouvez aussi afficher une ACL spécifique :

```
show access-lists <ACL_ID|ACL_NAME>
```

Créer une ACL established

```
access-list <ID> permit <tcp|udp> any any established
```

> Puis appliquez-la à à votre interface.

Créer une ACL réflexive

Créez l'access-list du trafic sortant (requêtes) :

```
ip access-list extended TRAFFIC-SORTANT
```

```
permit ip any any reflect MIROIR
```

Puis activez la sur l'interface interne :

```
int e0/0
```

```
ip access-group SORTANT in
```

Créez l'access-list du trafic entrant (réponses) :

```
ip access-list extended TRAFIC-ENTRANT
```

```
evaluate MIROIR
```

Puis activez la sur l'interface externe :

```
int e0/1
```

```
ip access-group ENTRANT in
```

Revision #12
Created 19 March 2024 08:11:46 by Elieroc
Updated 3 April 2025 10:49:37 by Elieroc