École supérieure de technologie Kenitra
Filière : Génie Informatique S4

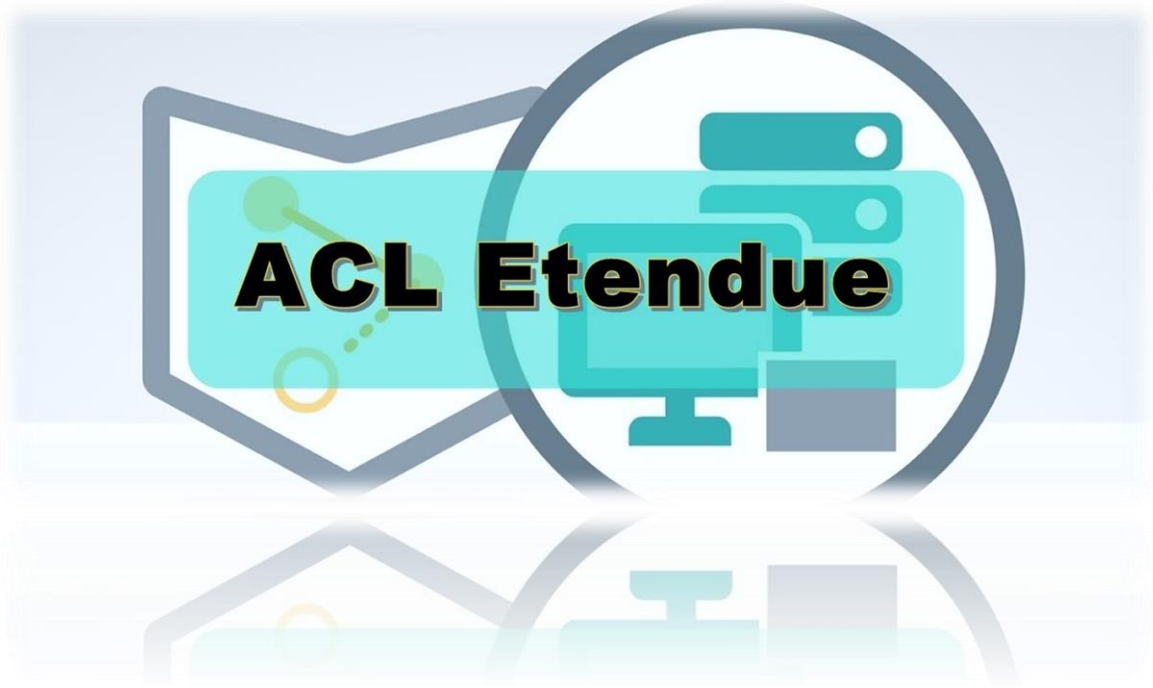
Rapport sur :

TP N.2 : ACL étendu

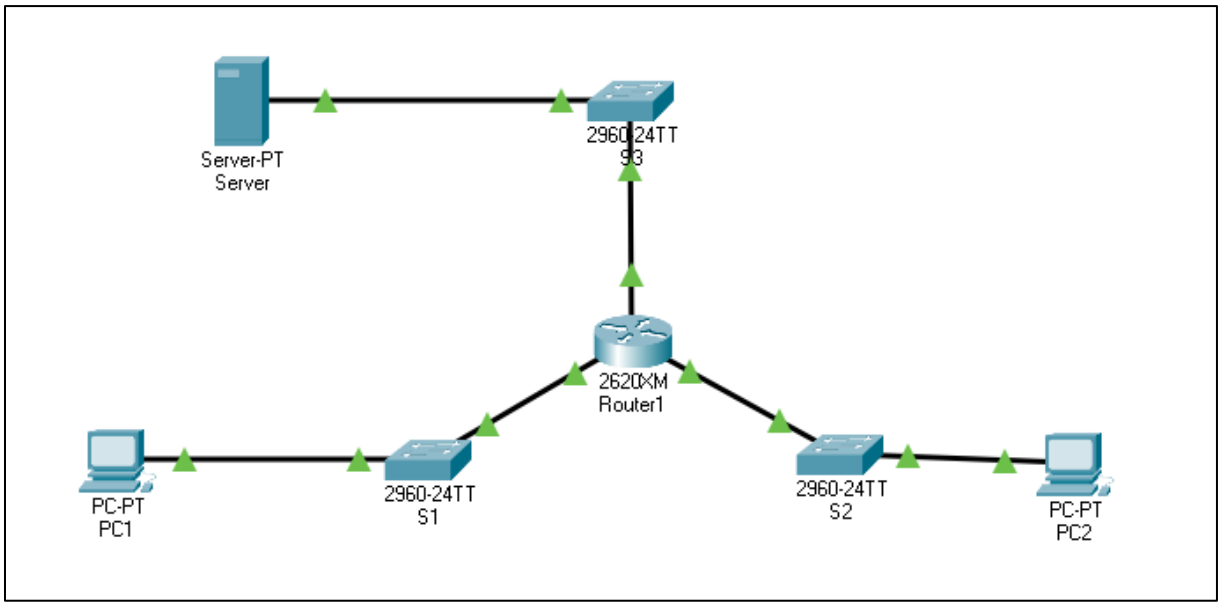
Réalisé par :

Khadir Nassima

Mrabet Ahmed



La topologie dont on va travailler avec :



Partie 1 : Configurer, appliquer et vérifier une ACL numérotée étendue

Étape 1 : Configurons une ACL pour autoriser FTP et ICMP.

1. À partir du mode de configuration globale sur R1, on a tapé la commande « access-list ? », ce qui nous donne ce qui est représenté dans la figure ci-dessous :

```
R1(config)#access-list ?
  <1-99>     IP standard access list
  <100-199>  IP extended access list
R1(config)#access-list
```

Alors pour une ACL standard on utilise des valeurs dans l'intervalle <1-99>, et pour l'étendue des valeurs entre <100-199>

2. On ajoute la valeur 100 a la commande, ce qui nous donne des informations sur les paramètres deny, permit et ramark de la commande access-list pour une ACL étendue

```
R1(config)#access-list 100 ?
  deny    Specify packets to reject
  permit  Specify packets to forward
  remark  Access list entry comment
R1(config)#access-list 100
```

3. Ajoutant le paramètre permit à la commande on obtient plus de détail, c'est-à-dire les paramètre qui correspond au protocole qu'on peut permise l'accès.

```
R1(config)#access-list 100 permit ?
  ahp    Authentication Header Protocol
  eigrp  Cisco's EIGRP routing protocol
  esp    Encapsulation Security Payload
  gre    Cisco's GRE tunneling
  icmp   Internet Control Message Protocol
  ip     Any Internet Protocol
  ospf   OSPF routing protocol
  tcp    Transmission Control Protocol
  udp    User Datagram Protocol
R1(config)#access-list 100 permit
```

4. Après qu'on a spécifier le protocole TCP, en trouve qu'il y a 3 manier dont en peut structurer la commande ACL avec, soit en spécifie les adresses des machine sources qu'on veut lui donne l'accès a travers le protocole TCP, ou ajoutant le paramètre « any » qui signifie toutes les machines, ou bien le paramètre « host » après l'adresse d'une machine pour donner la permission a cette seule et pas plus.

```
R1(config)#access-list 100 permit tcp ?
  A.B.C.D  Source address
  any      Any source host
  host     A single source host
R1(config)#access-list 100 permit tcp
```

5. Puisque le FTP utilise le TCP alors on va structurer la commande comme utilisant « permit tcp » + l'adresse du PC1 dont on veut autoriser sont trafic FTP + host « pour indiquer que c'est seulement cette adresse » + l'adresse du serveur + le paramètre eq FTP.

```
R1(config)#access-list 100 permit tcp 172.22.34.66 255.255.255.224 host 172.22.34.62 eq
FTP
R1(config)#
```

6. On créer l'instruction qui autorise le trafic ICMP de la même manière que FTP seulement on indique que c'est ICMP au lieu de TCP et aussi on n'ajoute pas de paramètre à la fin de la commande

```
R1(config)#access-list 100 permit icmp 172.22.34.66 255.255.255.224 host 172.22.34.62
R1(config)#
```

7. Utilisant la commande « do show access-list » on affiche les trafics accepter alors que tout autre trafic est refusé par défaut.

```
R1(config)#do show access-list
Extended IP access list 100
    10 permit tcp 0.0.0.2 255.255.255.224 host 172.22.34.62 eq ftp
    20 permit icmp 0.0.0.2 255.255.255.224 host 172.22.34.62

R1(config)#
```

Étape 2 : Appliquons l'ACL sur la bonne interface pour filtrer le trafic.

On applique l'ACL à l'interface fa0/0 du routeur R1 :

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#
R1(config)#int fa0/0
R1(config-if)#ip access-group 100 in
R1(config-if)#
```

Étape 3 : Vérifiez l'implémentation de l'ACL.

1. Le PING du PC1 vers le serveur et réaliser avec succès :

```
C:\>ping 172.22.34.62

Pinging 172.22.34.62 with 32 bytes of data:

Reply from 172.22.34.62: bytes=32 time<1ms TTL=127
Reply from 172.22.34.62: bytes=32 time<1ms TTL=127
Reply from 172.22.34.62: bytes=32 time<1ms TTL=127
Reply from 172.22.34.62: bytes=32 time<1ms TTL=127

Ping statistics for 172.22.34.62:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

2. Utilisant le FTP, le PC1 et connecter avec succès au serveur :

```
C:\>ftp 172.22.34.62
Trying to connect...172.22.34.62
Connected to 172.22.34.62
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```

3. On quitte le serveur FTP :

```
ftp>quit

221- Service closing control connection.
C:\>
```

4. Le PING vers PC2 est refusé, car comme on a dit tous autre trafic qui n'a pas indiquer dans l'access-list est refusé par défaut.

```
C:\>ping 172.22.34.198

Pinging 172.22.34.198 with 32 bytes of data:

Reply from 172.22.34.65: Destination host unreachable.
Reply from 172.22.34.65: Destination host unreachable.
Reply from 172.22.34.65: Destination host unreachable.
Reply from 172.22.34.65: Destination host unreachable.

Ping statistics for 172.22.34.198:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Partie 2 : Configurer, appliquer et vérifier une ACL nommée étendue.

Étape 1 : Configurons une ACL pour autoriser l'accès HTTP et ICMP.

1. On configure une ACL étendue avec le nom « HTTP_ONLY »

```
R1(config)#ip access-list extended HTTP_ONLY
R1(config-ext-nacl)#
```

2. On autorise le trafic http du PC1 vers le serveur utilisant l'instruction suivante :

```
R1(config-ext-nacl)#permit tcp 172.22.34.98 255.255.255.240 host 172.22.34.62 eq 80
R1(config-ext-nacl)#
```

3. On autorise le trafic ICMP du PC1 vers le serveur utilisant l'instruction suivante :

```
R1(config-ext-nacl)#permit icmp 172.22.34.98 255.255.255.240 host 172.22.34.62
R1(config-ext-nacl)#
```

4. Lest trafics permises sont les suivants (alors tous autre trafic est refuser par défaut) :

```
R1(config-ext-nacl)#do show access-list
Extended IP access list 100
    10 permit tcp 0.0.0.2 255.255.255.224 host 172.22.34.62 eq ftp (19 match(es))
    20 permit icmp 0.0.0.2 255.255.255.224 host 172.22.34.62 (5 match(es))
Extended IP access list HTTP_ONLY
    10 permit tcp 0.0.0.2 255.255.255.240 host 172.22.34.62 eq www
    20 permit icmp 0.0.0.2 255.255.255.240 host 172.22.34.62
```

On quitte le mode de configuration ACL :

```
R1(config-ext-nacl)#exit
R1(config)#
```

Étape : Appliquons l'ACL sur la bonne interface pour filtrer le trafic.

On applique l'ACL à l'interface fa1/0 du routeur R1 :

```
R1(config)#int fa1/0
R1(config-if)#ip access-group HTTP_ONLY in
R1(config-if)#
```

Étape 3 : Vérifions l'implémentation de l'ACL.

1. Le PING du PC1 vers le serveur et réaliser avec succès :

```
C:\>ping 172.22.34.62

Pinging 172.22.34.62 with 32 bytes of data:

Reply from 172.22.34.62: bytes=32 time<1ms TTL=127
Reply from 172.22.34.62: bytes=32 time<1ms TTL=127
Reply from 172.22.34.62: bytes=32 time<1ms TTL=127
Reply from 172.22.34.62: bytes=32 time<1ms TTL=127

Ping statistics for 172.22.34.62:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

2. La connexion avec le serveur FTP est échouer.

```
C:\>ftp 172.22.34.62
Trying to connect...172.22.34.62

%Error opening ftp://172.22.34.62/ (Timed out)
.



(Disconnecting from ftp server)



C:\>
```

3. La connexion avec le serveur par le protocole http est réussie.