

ACTIVITE 5

Configurer des ACL étendues

Pour renforcer la sécurité de votre réseau, vous allez configurer des ACL étendues numérotées ou nommées.

1 – Configurer une ACL numérotée étendue

Utilisez le fichier "**Act 5.1 - Configurer des ACL étendues.pkt**" pour la suite de l'activité.

Votre mission

Vous devez créer une liste ACL étendue numérotée respectant la politique de sécurité réseau de l'entreprise :

- Les postes du réseau 1 (PC1) n'ont besoin que d'un accès FTP.
- Les postes du réseau 2 (PC2) n'ont besoin que d'un accès Web.
- Les postes des deux réseaux peuvent envoyer une requête ping au serveur, mais pas entre les deux réseaux.

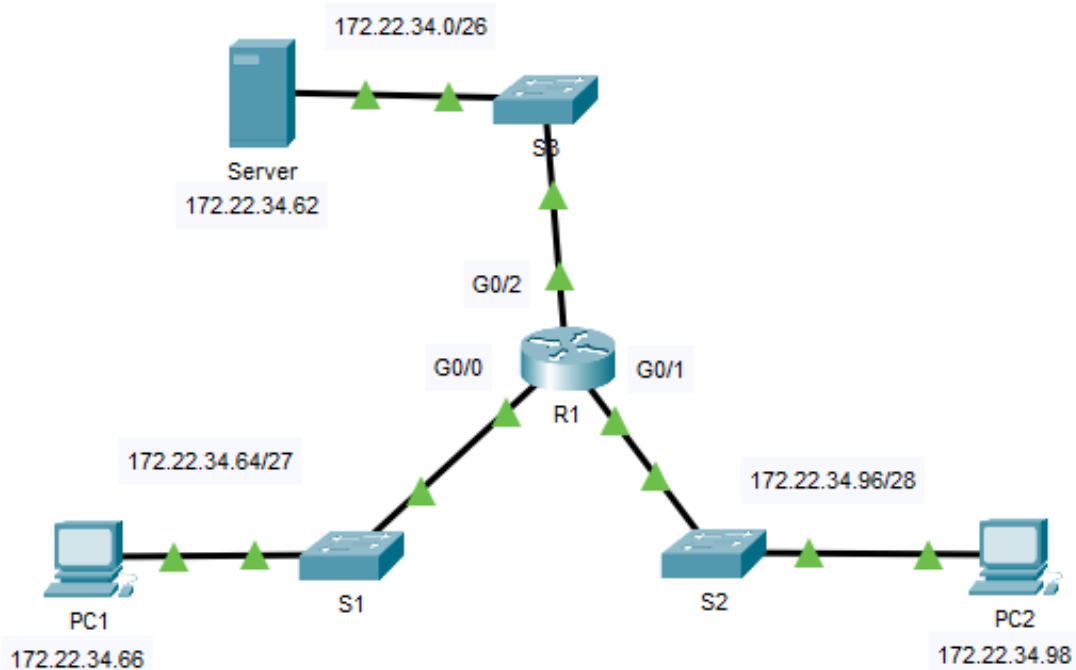


Table de routage

Appareil	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1	G0/0	172.22.34.65	255.255.255.224	N/A
	G0/1	172.22.34.97	255.255.255.240	
	G0/2	172.22.34.1	255.255.255.192	
Serveur	Carte réseau (NIC)	172.22.34.62	255.255.255.192	172.22.34.1
PC1	Carte réseau (NIC)	172.22.34.66	255.255.255.224	172.22.34.65
PC2	Carte réseau (NIC)	172.22.34.98	255.255.255.240	172.22.34.97

👉 1 – Vérification de la connectivité : PC1 et PC2 doivent être en mesure d'envoyer un ping au serveur Web et au serveur FTP. Les deux ordinateurs peuvent s'envoyer une requête ping.

🔪 2 – Quel protocole utilise-t-on lorsque l'on effectue un ping entre deux PC.
C'est le protocole ICMP qui est utilisé lors d'un ping.

Les règles à configurer sont :

- Le réseau 1 est autorisé à accéder au serveur 172.22.34.62 pour le service FTP.
- Le réseau 2 est autorisé à accéder au serveur 172.22.34.62 pour le service HTTP.
- Le protocole ICMP est autorisé du réseau 1 vers le serveur.
- Le protocole ICMP est autorisé du réseau 2 vers le serveur.
- Tous les autres accès ICMP ne sont pas autorisés.

Configurer une liste de contrôle d'accès étendue pour autoriser FTP et ICMP depuis le réseau 1

Dans la séquence qui suit, vous allez configurer l'ACL étape par étape. Commencez par la règle :

- **Le réseau 1 est autorisé à accéder au serveur 172.22.34.62 pour le service FTP.**

✍ 3 – En mode de configuration globale sur R1, entrez la commande suivante pour déterminer le premier numéro valide pour une liste d'accès étendue.

Commande : R1(config)#**access-list ?** (Le ? est important)

Réponse du routeur :

```
<1-99>  IP standard access list
<100-199> IP extended access list
```

✍ 4 – Choisir le premier numéro disponible dans la liste d'accès étendue. Tapez la commande suivit d'un ?

Commande : R1(config)#**access-list 100 ?**

Réponse du routeur :

```
deny  Specify packets to reject
permit Specify packets to forward
remark Access list entry comment
```

✍ 5 – On veut autoriser le trafic FTP, choisissez le bon terme suivit d'un ?

Commande : **R1(config)#access-list 100 permit ?**

Réponse du routeur :

```
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
```

✍ 6 – Une fois configurée et appliquée, cette liste de contrôle d'accès devrait autoriser FTP et ICMP. ICMP est indiqué ci-dessus, mais FTP non. En effet, FTP est un protocole de couche d'application (couche 7 du modèle OSI) qui utilise TCP au niveau de la couche transport. On filtrera le trafic FTP à partir du protocole TCP. Entrez TCP pour affiner l'aide ACL.

Commande : R1(config)#**access-list 100 permit tcp ?**

Réponse routeur :

```
A.B.C.D Source address
any  Any source host
host  A single source host
```

✍ 7 – L'adresse source peut représenter un seul périphérique, tel que PC1, en utilisant le mot clé **host** puis l'adresse IP du PC1. L'utilisation du mot-clé **any** autorise tout hôte sur n'importe quel réseau. Le filtrage peut également être effectué sur une adresse réseau. Dans ce cas, il s'agit de tout hôte qui possède une adresse appartenant au réseau 172.22.34.64 /27.

Saisissez cette adresse de réseau, suivie d'un point d'interrogation.

Commande : R1(config)#**access-list 100 permit tcp 172.22.34.64 ?**

Réponse routeur :

A.B.C.D Source wildcard bits

✍ 8 – Vous devez préciser le masque générique (wildcard) pour le réseau en /27.

Calculez le masque (wildcard) en déterminant l'opposé binaire du masque de sous-réseau /27.

11111111.11111111.11111111.11100000 = 255.255.255.224

Réponse routeur :

00000000.00000000.00000000.00011111 = 0.0.0.31

✍ 9 – Ajoutez le wildcard à la commande de la question 7 suivi d'un point d'interrogation.

Commande : R1(config)#**access-list 100 permit tcp 172.22.34.64 0.0.0.31 ?**

Réponse routeur :

A.B.C.D Destination address

any Any destination host

eq Match only packets on a given port number

gt Match only packets with a greater port number

host A single destination host

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

✍ 10 – Configurez l'adresse de destination. Dans ce scénario, nous filtrons le trafic pour une seule destination, qui est le serveur. Saisissez le mot clé host suivi de l'adresse IP du serveur.

Commande : R1(config)#**access-list 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 ?**

Réponse routeur :

dscp Match packets with given dscp value

eq Match only packets on a given port number

established established

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

precedence Match packets with given precedence value

range Match only packets in the range of port number

<cr>

✍ 11 – Remarquez que l'une des options est **<cr>** (retour chariot). En d'autres termes, vous pouvez appuyer sur **Entrée** et la déclaration autorisera tout le trafic TCP. Cependant, nous n'autorisons que le trafic FTP ; par conséquent, entrez le mot clé **eq**, suivi d'un point d'interrogation pour afficher les options disponibles.

Commande : R1(config)#**access-list 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 eq ?**

Réponse routeur :

<0-65535> Port number

ftp File Transfer Protocol (21)

pop3 Post Office Protocol v3 (110)

smtp Simple Mail Transport Protocol (25)

telnet Telnet (23)

www World Wide Web (HTTP, 80)

✍ 12 – Ensuite, ajoutez **ftp** à la commande précédente puis appuyez sur **Entrée**.

Commande : **R1(config)#access-list 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 eq ftp**

Maintenant que la première règle est configurée, passez à la seconde :

- **Le protocole ICMP est autorisé du réseau 1 vers le serveur.**

✍ 13 – Créez une deuxième règle pour autoriser le trafic ICMP (ping) du réseau 1 vers le serveur. Notez que le numéro de la liste d'accès reste le même et qu'il n'est pas nécessaire d'indiquer un type de trafic ICMP spécifique.

Commande :

R1(config)# access-list 100 permit icmp 172.22.34.64 0.0.0.31 host 172.22.34.62

✍ 14 – il faudrait créer une dernière règle pour refuser tout autre trafic : **access-list 100 deny any any**

L'exécution par défaut d'une liste d'accès est que si un paquet ne correspond pas à une instruction dans la liste d'accès, il n'est pas autorisé via l'interface. Donc, il n'est pas nécessaire d'ajouter la règle "**access-list 100 deny any any**" car le routeur le fait par défaut.

✍ 15 – Exécutez la commande **show access-list** et vérifiez que la liste d'accès 100 contient les déclarations correctes.

Réponse routeur :

R1# show access-lists

Extended IP access list 100

10 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 eq ftp

20 permit icmp 172.22.34.64 0.0.0.31 host 172.22.34.62

Appliquer l'ACL sur l'interface du routeur

✍ 16 – Du point de vue de R1, le trafic auquel s'applique l'ACL 100 est entrant depuis le réseau connecté à l'interface G0/0.

Passez en mode de configuration d'interface et appliquez la liste de contrôle d'accès.

Commande :

R1(config)#interface gigabitEthernet 0/0

R1(config-if)#ip access-group 100 in

✍ 17 – Testez l'ensemble des règles pour l'interface G0/0 du routeur R1.

- Depuis PC1, faire un ping vers le Serveur Web. Le ping doit aboutir. Si les requêtes ping n'aboutissent pas, vérifiez les adresses IP avant de continuer.
- Exécutez la commande **show access-lists** pour voir le nombre de paquets qui correspondent à chaque déclaration. Le nombre en fin de ligne vous indique le nombre de fois que la règle a été validée.
- Testez l'accès FTP depuis PC1 : à partir de l'application "**command prompt**", tapez **ftp 172.22.34.62**. Le nom d'utilisateur et le mot de passe sont tous deux **cisco**.
(Pour quitter le service FTP : ftp> **quit**)
- Ping de PC1 à PC2. L'hôte de destination doit être injoignable, car l'ACL n'a pas explicitement autorisé le trafic.

2 - Configurer, appliquer et vérifier une ACL nommée étendue

Configurer une ACL pour autoriser l'accès HTTP et ICMP depuis le LAN PC2

✍ 18 - Les ACL nommées commencent par le mot clé "ip". En mode de configuration globale de R1, entrez la commande suivante, suivie d'un point d'interrogation :

Commande : R1(config)# **ip access-list ?**

Réponse routeur :

extended Extended Access List
standard Standard Access List

✍ 19 - Vous allez configurer une ACL étendue nommée. Saisissez **HTTP_ONLY** comme nom. (Pour la notation Packet Tracer, le nom est sensible à la casse et les instructions de liste d'accès doivent être dans l'ordre correct.)

Commande : **R1(config)# ip access-list extended HTTP_ONLY**

✍ 20 - L'invite change. Vous êtes maintenant en mode de configuration de liste de contrôle d'accès étendue nommée. Tous les appareils du réseau local PC2 ont besoin d'un accès TCP. Saisissez l'adresse du réseau, suivie d'un point d'interrogation.

Commande : R1(config-ext-nacl)# **permit tcp 172.22.34.96 ?**

Réponse routeur :

A.B.C.D Source wildcard bits

✍ 21 – Vous devez préciser le masque générique (wildcard) pour le réseau en 255.255.255.240. Calculez le masque (wildcard) en déterminant l'opposé binaire du masque de sous-réseau.

11111111.11111111.11111111.11110000 = 255.255.255.240

Réponse :

00000000.00000000.00000000.00001111 = 0.0.0.15

Remarque

Une autre façon de calculer un masque de remplacement consiste à soustraire le masque de sous-réseau de 255.255.255.255.

$$\begin{array}{r} 255.255.255.255 \\ - 255.255.255.240 \\ \hline = 0.0.0.15 \end{array}$$

✍ 22 – Ajoutez le wildcard à la fin de la commande précédente.

Commande : **R1(config-ext-nacl)#permit tcp 172.22.34.96 0.0.0.15**

✍ 23 – Terminez l'instruction en spécifiant l'adresse du serveur comme vous l'avez fait dans la Partie 1 et en filtrant le trafic **www**.

Commande : **R1(config-ext-nacl)#permit tcp 172.22.34.96 0.0.0.15 host 172.22.34.62 eq www**

✍ 24 – Créez une deuxième déclaration de liste d'accès pour autoriser le trafic ICMP (ping, etc.) de PC2 vers le serveur.

Remarque :

L'invite reste identique et un type de trafic ICMP spécifique n'a pas besoin d'être spécifié.

Commande : **R1(config-ext-nacl)#permit icmp 172.22.34.96 0.0.0.15 host 172.22.34.62**

✍ 25 – Tout autre trafic est refusé, par défaut. Quittez le mode de configuration de liste de contrôle d'accès étendue nommée.

✍ 26 – Exécutez la commande **show access-list** et vérifiez que la liste d'accès **HTTP_ONLY** contient les déclarations correctes.

Commande : R1# **show access-lists**

Réponse routeur :

```
Extended IP access list 100
10 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 eq ftp
20 permit icmp 172.22.34.64 0.0.0.31 host 172.22.34.62
Extended IP access list HTTP_ONLY
10 permit tcp 172.22.34.96 0.0.0.15 host 172.22.34.62 eq www
20 permit icmp 172.22.34.96 0.0.0.15 host 172.22.34.62
```

Appliquer l'ACL sur l'interface du routeur R1

Du point de vue de R1, le trafic auquel la liste d'accès **HTTP_ONLY** s'applique est entrant depuis le réseau connecté à l'interface Gigabit Ethernet 0/1. Passez en mode de configuration d'interface et appliquez la liste de contrôle d'accès.

Commande :

```
R1(config)#interface gigabitEthernet 0/1
R1(config-if)#ip access-group HTTP_ONLY in
```

☞ 27 – Testez l'ensemble des règles pour l'interface G0/1 du routeur R1.

- Depuis PC2, faire un ping vers le Serveur. Le ping doit aboutir. Si les requêtes ping n'aboutissent pas, vérifiez les adresses IP avant de continuer.
- Depuis le PC2, ouvrez un navigateur web et entrez l'adresse IP du serveur. La page Web du serveur doit être affichée.
- Testez l'accès FTP depuis PC2 : à partir de l'application "**command prompt**", tapez [ftp 172.22.34.62](ftp://172.22.34.62). La connexion devrait échouer. Si ce n'est pas le cas, résolvez les instructions de liste d'accès et les configurations de groupe d'accès sur les interfaces.