Contrôle du trafic avec les ACLs

Une liste de contrôle d'accès (ACL, Liste de contrôle d'accès) est une série de commandes qui déterminent si un appareil achemine ou abandonne les paquets en fonction des informations contenues dans l'en-tête de paquet. Une fois configurées, les listes de contrôle d'accès assurent les tâches suivantes:

Elles limitent le trafic du réseau pour accroître ses performances. Si la politique de l'entreprise interdit, par exemple, le trafic vidéo sur le réseau, vous pouvez configurer et appliquer des listes de contrôle d'accès pour bloquer ce trafic. Ainsi, la charge réseau est nettement réduite et les performances réseau sont sensiblement améliorées.

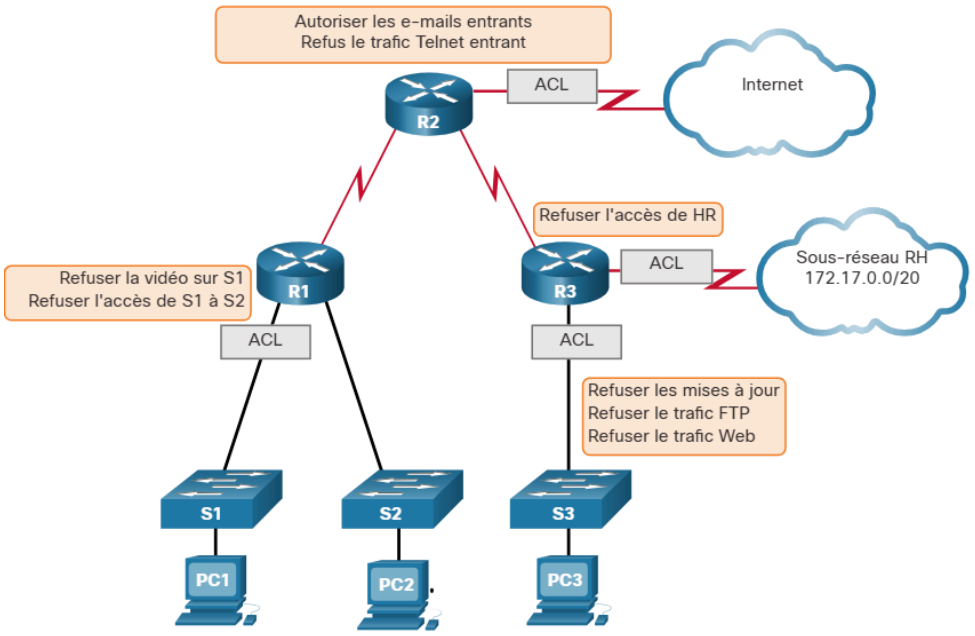
Elles assurent un contrôle du flux de trafic. Les listes de contrôle d'accès peuvent limiter la diffusion des mises à jour de routage pour s'assurer que les mises à jour viennent d'une source reconnue.

Elles offrent un niveau de sécurité de base pour l'accès réseau. Les listes de contrôle d'accès permettent à un hôte d'accéder à une section du réseau tout en empêchant un autre hôte d'y avoir accès. Par exemple, l'accès au réseau du département Ressources humaines peut être limité aux utilisateurs autorisés.

Elles filtrent le trafic selon son type. Ainsi, une liste de contrôle d'accès peut autoriser le trafic des e-mails, mais bloquer tout le trafic Telnet.

Elles filtrent les hôtes pour permettre ou refuser l'accès aux services réseau. Les listes de contrôle d'accès peuvent autoriser ou refuser à un utilisateur l'accès à certains types de fichiers, tels que FTP ou HTTP.

En dehors de l'autorisation ou du blocage du trafic, les listes de contrôle d'accès peuvent être utilisées pour sélectionner les types de trafic à analyser, à acheminer et à traiter selon d'autres méthodes. Par exemple, les listes de contrôle d'accès permettent de classer le trafic par ordre de priorité. Cette fonction s'assimile à une carte VIP pour un concert ou un événement sportif. La carte VIP offre aux spectateurs privilégiés des avantages qui ne sont pas proposés aux détenteurs d'un billet standard, notamment l'entrée prioritaire ou le droit d'accéder à une zone privée.



Objectifs

Partie 1: Vérification de la connectivité locale et test de la liste de contrôle d'accès

Partie 2: Suppression de la liste de contrôle d'accès et répétition du test

Contexte

Dans cet exercice, vous allez observer comment une liste de contrôle d'accès peut être utilisée pour empêcher une requête ping d'atteindre les hôtes sur des réseaux distants. Après le retrait de la liste de contrôle d'accès de la configuration, les requêtes ping aboutiront.

Instructions

Partie 1: Vérifier la connectivité locale et Tester la liste de contrôle d'accès

Étape 1: Ping des périphériques sur le réseau local pour vérifier la connectivité.

a. À partir de l'invite de commande de **PC1**, envoyez une requête ping à **PC2**.

Capture d'écran de votre résultat :

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.11

Pinging 192.168.10.11 with 32 bytes of data:

Reply from 192.168.10.11: bytes=32 time<1ms TTL=128
Reply from 192.168.10.11: bytes=32 time<1ms TTL=128
Reply from 192.168.10.11: bytes=32 time<1ms TTL=128
Reply from 192.168.10.11: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

b. À partir de l'invite de commande de **PC1**, envoyez une requête ping à **PC3**.

Capture d'écran de votre résultat :

```
C:\>ping 192.168.11.10

Pinging 192.168.11.10 with 32 bytes of data:

Reply from 192.168.11.10: bytes=32 time<1ms TTL=127
Reply from 192.168.11.10: bytes=32 time<1ms TTL=127
Reply from 192.168.11.10: bytes=32 time<1ms TTL=127
Reply from 192.168.11.10: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.11.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Pourquoi les requêtes ping ont-elles abouti?

Car PC1, PC2 et PC3 sont dans le même sous réseau qui R1. Car L'ACL est configuré en interface série.Dans cette configuration l'ACL ne filtre pas le trafic qui reste à l'intérieur du sous réseau car elle est en mode interface série.

Étape 2: Envoyez une requête ping aux périphériques sur les réseaux distants pour tester le fonctionnement des listes de contrôle d'accès.

a. À partir de l'invite de commande de PC1, envoyez une requête ping à PC4.

Capture d'écran de votre résultat :

```
C:\>
C:\>ping 192.168.30.12

Pinging 192.168.30.12 with 32 bytes of data:

Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.

Ping statistics for 192.168.30.12:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

b. À partir de l'invite de commande de PC1, envoyez une requête ping à DNS Server.

Capture d'écran de votre résultat :

```
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.31.12

Pinging 192.168.31.12 with 32 bytes of data:

Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.

Ping statistics for 192.168.31.12:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Question:

Pourquoi les requêtes ping ont-elles échoué? (Conseil: utilisez le mode de simulation ou afficher les configurations des routeurs pour élucider la question.)

Donnez la configuration de vos routeurs :

Les requêtes ping de PC1 vers PC4 et Serveur DNS ont échoué, car une Liste de Contrôle d'Accès (ACL) est configurée sur le routeur R1.

```
R1#show access-lists
Standard IP access list 11
    10 deny 192.168.10.0 0.0.0.255 (8 match(es))
    20 permit any

R1#

!
access-list 11 deny 192.168.10.0 0.0.0.255
access-list 11 permit any
!
```

Partie 2: Supprimer l'ACL et répéter le test

Étape 1: Utilisez les commandes show pour étudier la configuration du ACL.

a. Utilisez les commandes show run et show access-lists pour afficher les listes de contrôle d'accès actuellement configurées. Pour afficher rapidement les listes de contrôle d'accès actuelles, utilisez show access-lists. Entrez la commande show access-lists suivie d'un espace et d'un point d'interrogation (?) pour afficher les options disponibles:

```
R1# show access-lists ?
  <1-199>  ACL number
  WORD ACL name
  <cr>
```

Capture d'écran de votre résultat :

```
R1#
R1#show access-lists ?
  <1-199>  ACL number
  WORD     ACL name
  |        Output Modifiers
  <cr>
```

Si vous connaissez le numéro ou le nom de la liste de contrôle d'accès, vous pouvez limiter davantage les résultats de la commande show . Toutefois, R1 a une seule ACL (liste de contrôle d'accès). Par conséquent, la commande show access-lists suffira.

```
R1# show access-lists
```

Capture d'écran de votre résultat :

```
R1#show access-lists
Standard IP access list 11
    10 deny 192.168.10.0 0.0.0.255 (8 match(es))
    20 permit any
```

La première ligne de la liste ACL bloque tous les paquets provenant du réseau 192.168.10.0/24, notamment les échos (requêtes ping) du protocole ICMP (Internet Control Message Protocol). La deuxième ligne de la liste ACL permet à tous les autres trafics ip provenant de n'importe quelle source de traverser le routeur.

b. Pour que la liste ACL influence le fonctionnement du routeur, elle doit être appliquée à une interface dans une direction définie. Dans ce scénario, la liste ACL est utilisée pour filtrer le trafic sortant d'une interface. Par conséquent, chaque trafic provenant de l'interface spécifiée du routeur R1 sera inspecté selon ACL 11.

Bien que vous puissiez voir les informations IP avec la commande show ip interface, il peut être plus efficace dans certaines situations d'utiliser simplement la commande show run .

Question:

En utilisant l'une de ces commandes ou les deux, à quelle interface et vers quelle direction la liste ACL est-elle appliquée?

Capture d'écran de votre résultat :

```
!
interface Serial0/0/0
 ip address 10.10.1.1 255.255.255.252
 ip access-group 11 out
!
```

Commande 1 : show run

Commande 2 : show ip interface Serial0/0/0

Étape 2: Supprimez la liste d'accès 11 de la configuration.

Vous pouvez supprimer des listes de contrôle d'accès de la configuration en exécutant la commande :

no access list [*numéro de la liste de contrôle d'accès*] .

La commande **no access-list** permet de supprimer toutes les listes ACL configurées sur le routeur. La commande **no access-list** [*numéro de la liste de contrôle d'accès*] permet de supprimer uniquement une liste ACL précise.

a. Sous l'interface Serial0/0/0, supprimez la liste d'accès 11 précédemment appliquée à l'interface comme un filtre **outgoing** (sortant):

```
R1(config)# int se0/0/0
R1(config-if)#no ip access-group 11 out
```

Capture d'écran de votre résultat :

```
!
interface Serial0/0/0
 ip address 10.10.1.1 255.255.255.252
!
```

b. En mode de configuration globale, supprimez la liste de contrôle d'accès en saisissant la commande suivante:

```
R1(config)# no access-list 11
```

Capture d'écran de votre résultat :

```
R1#show access-lists
R1#
```

c. Vérifiez que le **PC1** peut maintenant envoyer une requête ping vers le **Serveur DNS** et **PC4**.

Capture d'écran de votre résultat :

```
C:\>ping 192.168.31.12

Pinging 192.168.31.12 with 32 bytes of data:

Reply from 192.168.31.12: bytes=32 time=9ms TTL=125
Reply from 192.168.31.12: bytes=32 time=8ms TTL=125
Reply from 192.168.31.12: bytes=32 time=7ms TTL=125
Reply from 192.168.31.12: bytes=32 time=7ms TTL=125

Ping statistics for 192.168.31.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 7ms, Maximum = 9ms, Average = 7ms
```

```
C:\>ping 192.168.30.12

Pinging 192.168.30.12 with 32 bytes of data:

Reply from 192.168.30.12: bytes=32 time=9ms TTL=125
Reply from 192.168.30.12: bytes=32 time=7ms TTL=125
Reply from 192.168.30.12: bytes=32 time=7ms TTL=125
Reply from 192.168.30.12: bytes=32 time=9ms TTL=125

Ping statistics for 192.168.30.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 7ms, Maximum = 9ms, Average = 8ms
```