Packet Tracer - Configurer les listes de contrôle d'accès IPv4 - Scénario 2

Partie 1: Configurer une liste de contrôle d'accès étendue nommée

Étape 1: Refusez à PC1 l'accès aux services HTTP et HTTPS sur Serveur1 et Serveur2

a) ip access-list extended ACL

Étape 1: Refusez à PC1 l'accès aux services HTTP et HTTPS sur Serveur1 et Serveur2.

a. Créez une liste de contrôle d'accès IP nommée sur le routeur RT1 qui empêchera **PC1** d'accéder aux services HTTP et HTTPS de **Serveur1** et **Serveur2**. Quatre instructions de contrôle d' accès sont requises.

Quelle est la commande pour commencer la configuration d'une liste d'accès étendue avec le nom **ACL**?

b. Commencez la configuration de l'ACL avec l'instruction qui refuse l'accès de **PC1** vers **Serveur1**, uniquement pour HTTP (port 80). Consultez le tableau d'adressage pour l'adresse IP de **PC1** et **Serveur1**.

```
RT1(config-ext-nacl)# deny tcp host 172.31.1.101 host 64.101.255.254
eq 80
```

c. Ensuite, saisissez la déclaration qui refuse l'accès du **PC1** au **Serveur1**, uniquement pour HTTPS (port 443).

```
RT1(config-ext-nacl)# deny tcp host 172.31.1.101 host 64.101.255.254
eq 443
```

d. Saisissez la déclaration qui refuse l'accès du **PC1** au **Serveur2**, uniquement pour HTTP. Consultez la table d'adressage pour l'adresse IP de **Serveur 2.**

```
RT1(config-ext-nacl)# deny tcp host 172.31.1.101 host 64.103.255.254
eq 80
```

e. Saisissez la déclaration qui refuse l'accès du **PC1** au **Serveur2**, uniquement pour HTTPS.

```
RT1(config-ext-nacl)# deny tcp host 172.31.1.101 host 64.103.255.254
eq 443
```

Étape 2: Refusez à PC2 l'accès aux services FTP sur Serveur 1 et Serveur 2.

Consultez la table d'adressage pour l'adresse IP de **PC2**.

a. Saisissez la déclaration qui refuse l'accès du **PC2** au **Serveur1**, uniquement pour FTP (port 21 seulement).

```
RT1(config-ext-nacl)# deny tcp host 172.31.1.102 host 64.101.255.254
eq 21
```

b. Saisissez la déclaration qui refuse l'accès du **PC2** au **Serveur2**, uniquement pour FTP (port 21 seulement).

```
RT1(config-ext-nacl)# deny tcp host 172.31.1.102 host 64.103.255.254
eq 21
```

Étape 3: Empêchez PC3 d'envoyer une requête ping à Serveur1 et Serveur2.

Consultez la table d'adressage pour l'adresse IP de **PC3.**

a. Saisissiez la déclaration qui refuse l'accès ICMP de **PC3** vers **Serveur1**.

```
RT1(config-ext-nacl)# deny icmp host 172.31.1.103 host 64.101.255.254
```

b. Saisissiez la déclaration qui refuse l'accès ICMP de **PC3** vers **Serveur2**.

```
RT1(config-ext-nacl)# deny icmp host 172.31.1.103 host 64.103.255.254
```

Étape 5: Vérifiez la configuration de la liste d'accès avant de l'appliquer à une interface.

Avant d'appliquer une liste d'accès, la configuration doit être vérifiée pour s'assurer qu'il n'y a pas d'erreurs typographiques et que les instructions sont dans le bon ordre. Pour afficher la configuration actuelle de la liste d'accès, utilisez la commande **show access-lists** ou la commande **show running-config** .

```
RT1# show access-lists
Extended IP access list ACL
        10 deny tcp host 172.31.1.101 host 64.101.255.254 eq www
        20 deny tcp host 172.31.1.101 host 64.101.255.254 eq 443
        30 deny tcp host 172.31.1.101 host 64.103.255.254 eq www
        40 deny tcp host 172.31.1.101 host 64.103.255.254 eq 443
        50 deny tcp host 172.31.1.102 host 64.101.255.254 eq ftp
        60 deny tcp host 172.31.1.102 host 64.103.255.254 eq ftp
        70 deny icmp host 172.31.1.103 host 64.101.255.254
        80 deny icmp host 172.31.1.103 host 64.103.255.254
        90 permit ip any any

RT1# show running-config | begin access-list
ip access-list extended ACL
        deny tcp host 172.31.1.101 host 64.101.255.254 eq www
        deny tcp host 172.31.1.101 host 64.101.255.254 eq 443
        deny tcp host 172.31.1.101 host 64.103.255.254 eq www
        deny tcp host 172.31.1.101 host 64.103.255.254 eq 443
        deny tcp host 172.31.1.102 host 64.101.255.254 eq ftp
        deny tcp host 172.31.1.102 host 64.103.255.254 eq ftp
        deny icmp host 172.31.1.103 host 64.101.255.254
        deny icmp host 172.31.1.103 host 64.103.255.254
        permit ip any any
```

Partie 2 : Appliquer et vérifier la liste de contrôle d'accès étendue

Étape 1 : Appliquez la liste de contrôle d'accès à l' interface appropriée dans la bonne direction.

Sur l'interface gigabitEthernet 0/0

Commande pour mettre l'acl sur l'interface :

RT1(config)# interface g0/0

RT1(config-f)# ip access-group ACL in

Accéder au ftp : ftp <adresse ip>