Packet Tracer : configuration des listes de contrôle d'accès étendues, scénario 3

Topologie

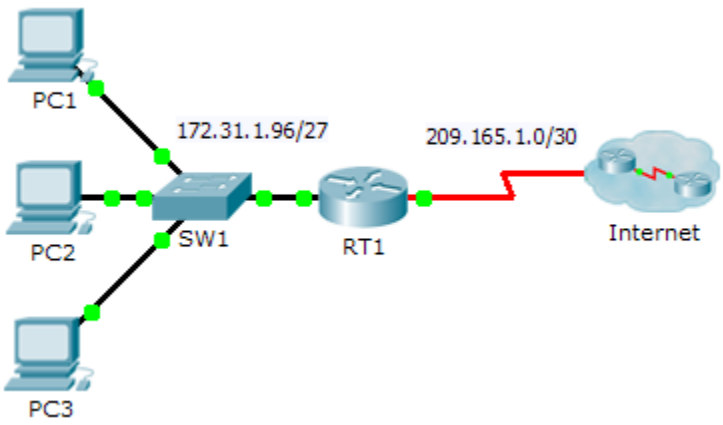

Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
RT1	G0/0	172.31.1.126	255.255.255.224	N/A
	S0/0/0	209.165.1.2	255.255.255.252	N/A
PC1	NIC	172.31.1.101	255.255.255.224	172.31.1.126
PC2	NIC	172.31.1.102	255.255.255.224	172.31.1.126
PC3	NIC	172.31.1.103	255.255.255.224	172.31.1.126
Server1	NIC	64.101.255.254		
Server2	NIC	64.103.255.254		

Objectifs

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

Partie 2 : application et vérification de la liste de contrôle d'accès étendue

Contexte/scénario

Dans ce scénario, certains périphériques du LAN sont autorisés à accéder à différents services sur des serveurs sur Internet.

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

Utilisez une liste de contrôle d'accès nommée pour implémenter la stratégie suivante :

- Bloquez les accès HTTP et HTTPS de **PC1** à **Server1** et **Server2** .Les serveurs sont dans le cloud et vous connaissez uniquement leurs adresses IP.
- Bloquez l'accès FTP de **PC2** à **Server1** et **Server2**.
- Bloquez l'accès ICMP de **PC3** à **Server1** et **Server2**.

Remarque : à des fins d'évaluation, vous devez configurer les instructions dans l'ordre indiqué dans les étapes suivantes.

Étape 1 : Refusez à PC1 l'accès aux services HTTP et HTTPS sur Server1 et Server2.

a. Créez une liste de contrôle d'accès IP baptisée ACL qui empêchera **PC1** d'accéder aux services HTTP et HTTPS de **Server1** et de **Server2**. Comme il est impossible d'observer directement le sous-réseau des serveurs sur Internet, quatre règles sont requises.

Quelle est la commande pour débuter la liste de contrôle d'accès nommée ?

b. Notez l'instruction refusant l'accès de **PC1** à **Server1**, uniquement pour HTTP (port 80).

c. Notez l'instruction refusant l'accès de **PC1** à **Server1**, uniquement pour HTTPS (port 443).

d. Notez l'instruction refusant l'accès de **PC1** à **Server2**, uniquement pour HTTP.

e. Notez l'instruction refusant l'accès de **PC1** à **Server2**, uniquement pour HTTPS.

Étape 2 : Refusez à PC2 l'accès aux services FTP sur Server1 et Server2.

a. Notez l'instruction refusant l'accès de **PC2** à **Server1**, uniquement pour FTP (port 21 seulement).

b. Notez l'instruction refusant l'accès de **PC2** à **Server2**, uniquement pour FTP (port 21 seulement).

Étape 3 : Empêchez PC3 d'envoyer une requête ping à Server1 et Server2.

a. Notez l'instruction refusant l'accès ICMP de **PC3** vers **Server1**.

b. Notez l'instruction refusant l'accès ICMP de **PC3** vers **Server2**.

Étape 4 : Autorisez tout autre trafic IP.

Par défaut, une liste d'accès refuse tout trafic qui ne correspond à aucune règle de la liste. Quelle commande autorise tout autre trafic ?

Partie 2 : Application et vérification de la liste de contrôle d'accès étendue

Le trafic à filtrer provient du réseau 172.31.1.96/27 et est à destination des réseaux distants. L'emplacement approprié de la liste de contrôle d'accès dépend également de la relation du trafic par rapport à **RT1**.

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

a. Quelles sont les commandes nécessaires pour appliquer la liste de contrôle d'accès à l'interface appropriée et vers la direction appropriée ?

Étape 2 : Testez l'accès pour chaque PC.

a. Accédez aux sites Web de **Server1** et **Server2** avec le navigateur Web de **PC1** en utilisant les protocoles HTTP et HTTPS.

b. Accédez aux services FTP de **Server1** et **Server2** en utilisant **PC1**. Le nom d'utilisateur et le mot de passe sont **cisco**.

c. Envoyez une requête ping à **Server1** et **Server2** depuis **PC1**.

d. Répétez les étapes 2a à 2c avec **PC2** et **PC3** pour vérifier le bon fonctionnement de la liste d'accès.