Packet Tracer : configuration des listes de contrôle d'accès IPv6

Topologie

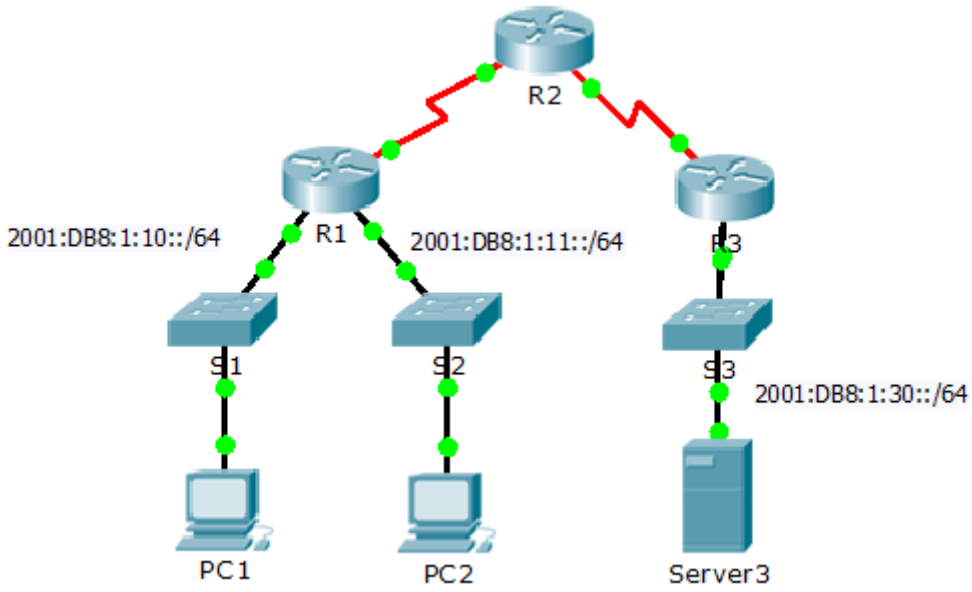

Table d'adressage

Périphérique	Interface	Adresse/Préfixe IPv6	Passerelle par défaut
Server3	NIC	2001:DB8:1:30::30/64	FE80::30

Objectifs

Partie 1 : configuration, application et vérification d'une liste de contrôle d'accès IPv6

Partie 2 : configuration, application et vérification d'une seconde liste de contrôle d'accès IPv6

Partie 1 : Configuration, application et vérification d'une liste de contrôle d'accès IPv6

Les journaux indiquent qu'un ordinateur du réseau 2001:DB8:1:11::0/64 actualise à plusieurs reprises sa page Web, ce qui provoque une attaque par défini de service contre **Server3**. Jusqu'à ce que le client puisse être identifié et nettoyé, vous devez bloquer l'accès HTTP et HTTPS à ce réseau avec une liste d'accès.

Étape 1 : Configurez une liste de contrôle d'accès qui bloquera l'accès HTTP et HTTPS.

Configurez une liste de contrôle d'accès nommée **BLOCK_HTTP** sur **R1** avec les instructions suivantes.

a. Bloquez le routage du trafic HTTP et HTTPS jusqu'à **Server3**.

```
R1(config)# deny tcp any host 2001:DB8:1:30::30 eq www
R1(config)# deny tcp any host 2001:DB8:1:30::30 eq 443
```

b. Autorisez tout autre trafic IPv6.

Étape 2 : Appliquez la liste de contrôle d'accès à l'interface appropriée.

Appliquez la liste de contrôle d'accès à l'interface la plus proche de la source du trafic à bloquer.

```
R1(config-if)# ipv6 traffic-filter BLOCK_HTTP in
```

Étape 3 : Vérifiez l'implémentation de la liste de contrôle d'accès.

Vérifiez que la liste de contrôle d'accès fonctionne correctement en effectuant les tests suivants :

- Ouvrez le **navigateur Web** de **PC1** sur http:// 2001:DB8:1:30::30 ou https://2001:DB8:1:30::30. Le site Web devrait s'afficher.
- Ouvrez le **navigateur Web** de **PC2** sur http:// 2001:DB8:1:30::30 ou https://2001:DB8:1:30::30. Le site Web doit être bloqué.
- Envoyez une requête ping à partir de **PC2** vers 2001:DB8:1:30::30. La requête ping devrait aboutir.

Partie 2 : Configuration, application et vérification d'une seconde liste de contrôle d'accès IPv6

Les journaux indiquent désormais que votre serveur reçoit des requêtes ping de plusieurs adresses IPv6 différentes dans une attaque par déni de service distribuée (DDoS). Vous devez filtrer les requêtes ping ICMP envoyées à votre serveur.

Étape 1 : Créez une liste de contrôle d'accès pour bloquer ICMP.

Configurez une liste de contrôle d'accès nommée **BLOCK_ICMP** sur **R3** avec les instructions suivantes :

a. Bloquez tout le trafic ICMP, quels que soient l'hôte et la destination.

b. Autorisez tout autre trafic IPv6.

Étape 2 : Appliquez la liste de contrôle d'accès à l'interface appropriée.

Dans ce cas, le trafic ICMP peut provenir de n'importe quelle source. Pour garantir que le trafic ICMP est bloqué indépendamment de sa source ou de modifications de la topologie du réseau, appliquez la liste de contrôle d'accès la plus proche de la destination.

Étape 3 : Vérifiez que la liste de contrôle d'accès appropriée fonctionne.

a. Envoyez une requête ping à partir de **PC2** vers 2001:DB8:1:30::30. La requête ping devrait échouer.

b. Envoyez une requête ping à partir de **PC1** vers 2001:DB8:1:30::30. La requête ping devrait échouer.

Ouvrez le **navigateur Web** de **PC1** sur http:// 2001:DB8:1:30::30 ou https://2001:DB8:1:30::30. Le site Web devrait s'afficher.