

Exemple de configuration de liste d'accès de filtrage du trafic IPv6

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Conventions](#)

[Configuration](#)

[Diagramme du réseau](#)

[Configurations](#)

[Vérification](#)

[Dépannage](#)

[Informations connexes](#)

[Introduction](#)

Ce document fournit un exemple de configuration pour les listes d'accès IPv6. Dans l'exemple décrit dans ce document, les routeurs R1 et R2 sont configurés avec un schéma d'adressage IPv6 et connectés via une liaison série. Le protocole de routage activé sur les deux routeurs est le protocole OSPF IPv6 et les adresses de bouclage configurées sur les deux routeurs (R1 et R2) sont annoncées dans la zone 0 avec cette commande : `ipv6 ospf process-id area area area-id [instance instance-id]`. Dans cet exemple, il est nécessaire de refuser le trafic Telnet qui provient de l'interface de bouclage 0 du routeur R2 et qui atteint l'interface de bouclage 4 du routeur R1.

Cet exemple de configuration utilise la commande `ipv6 access-list access-list-name` afin de construire une liste d'accès IPv6 (nommée `DENY_TELNET_Lo4`) sur le routeur R1. Une instruction `deny deny tcp host 400A:0:400C::1 host 1001:ABC:2011:7::1 eq telnet` est suivie d'une instruction `permit ipv6 any any`.

Afin d'attribuer une liste de contrôle d'accès IPv6 à une interface, utilisez cette commande en mode de configuration d'interface : `ipv6 traffic-filter access-list-name {in | sortant}`

[Conditions préalables](#)

[Conditions requises](#)

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

- Connaissance du [schéma d'adressage IPv6](#)
- Connaissance de la [mise en oeuvre du protocole OSPF pour IPv6](#)

Components Used

Les informations de ce document sont basées sur le routeur de la gamme Cisco 7200 sur le logiciel Cisco IOS Version 15.1 (pour les configurations des routeurs R1 et R2).

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à [Conventions relatives aux conseils techniques Cisco](#).

Configuration

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque : Utilisez [l'outil de recherche de commandes](#) (clients [inscrits](#) seulement) pour en savoir plus sur les commandes figurant dans le présent document.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Configurations

Ce document utilise les configurations suivantes :

- Routeur R1
- Routeur R2

Routeur R1

```
R1#show running-config

version 15.0
!
hostname R1
ip source-route
ip cef
!
no ip domain lookup
ipv6 unicast-routing
!--- Enables the forwarding of IPv6 packets. ipv6 cef
interface Loopback1 no ip address ipv6 address
100A:0:100C::1/64 ipv6 enable ipv6 ospf 10 area 0 !---
Enables OSPFv3 on the interface and associates !--- the
interface loopback1 to area 0. !! interface Loopback2 no
ip address ipv6 address 200A:0:200C::1/64 ipv6 ospf 10
area 0 !! interface Loopback3 no ip address ipv6
```

```
address 300A:0:300C::1/64 ipv6 enable ipv6 ospf 10 area
0 ! ! interface Loopback4 no ip address ipv6 address
400A:0:400C::1/64 ipv6 enable ipv6 ospf 10 area 0 !
interface Serial1/0 no ip address ipv6 address
AB01:2011:7:100::/64 eui-64 ipv6 enable ipv6 ospf
network point-to-point !--- Sets the OSPFv3 network type
as point-to-point. ipv6 ospf 10 area 0 ipv6 traffic-
filter DENY_TELNET_Lo4 in !--- Filters the traffic based
on access list. serial restart-delay 0 clock rate 64000
! ipv6 router ospf 10 router-id 1.1.1.1 log-adjacency-
changes ! ipv6 access-list DENY_TELNET_Lo4 sequence 20
deny tcp host 400A:0:400C::1 host 1001:ABC:2011:7::1 eq
telnet !--- Denies telnet access to Lo4 from Lo1 of
router R2. permit ipv6 any any ! end
```

Routeur R2

```
R2#show running-config

version 15.0
hostname R2
ip source-route
ip cef
!
no ip domain lookup
ipv6 unicast-routing
ipv6 cef
!
interface Loopback0
 no ip address
 ipv6 address 1001:ABC:2011:7::1/64
 ipv6 enable
 ipv6 ospf 10 area 0
 !
!
interface Serial1/0
 no ip address
 ipv6 address AB01:2011:7:100::/64 eui-64
 ipv6 enable
 ipv6 ospf network point-to-point
 ipv6 ospf 10 area 0
 serial restart-delay 0
 !
ipv6 router ospf 10
 router-id 2.2.2.2
 log-adjacency-changes
!
end
```

Vérification

Afin de vérifier la configuration, utilisez la commande **ping**.

Sur le routeur R2

Cet exemple de résultat montre que le routeur R2 peut atteindre l'interface de bouclage du routeur R1 :

```
R2#ping ipv6 400A:0:400C::1 source lo0
```

Type escape sequence to abort.

```
Sending 5, 100-byte ICMP Echos to 400A:0:400C::1, timeout is 2 seconds:  
Packet sent with a source address of 1001:ABC:2011:7::1  
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/32/44 ms
```

Essayez **telnet** loopback 4 interface du routeur R1 à partir de l'interface de bouclage 0 du routeur R2.

```
R2#telnet 400A:0:400C::1 /source-interface lo0  
Trying 400A:0:400C::1, 23 ...  
% Connection refused by remote host
```

La sortie ci-dessus confirme que la connexion Telnet est refusée par l'hôte distant (c'est-à-dire par le routeur R1).

Utilisez la commande [show ipv6 access-list DENY_TELNET_Lo4](#) afin de vérifier la liste d'accès créée dans le routeur R1 comme indiqué dans cet exemple :

Sur le routeur R1

```
R1#show ipv6 access-list DENY_TELNET_Lo4
```

```
IPv6 access list DENY_TELNET_Lo4  
  deny tcp host 400A:0:400C::1 host 1001:ABC:2011:7::1 eq telnet sequence 20  
  permit ipv6 any any (82 matches) sequence 30
```

L'[Outil Interpréteur de sortie \(clients enregistrés uniquement\) \(OIT\)](#) prend en charge certaines [commandes show](#). Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show**.

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- [Guide de configuration IPv6, Cisco IOS version 15.1 M&T](#)
- [Prise en charge de la technologie IPv6](#)
- [Support et documentation techniques - Cisco Systems](#)