IPv6 Traffic Filtering Access List Configuration Example

Document ID: 113126

Contents

Introduction
Prerequisites
Requirements
Components Used
Conventions
Configure
Network Diagram
Configurations
Verify
Troubleshoot
Related Information

Introduction

This document provides a sample configuration for IPv6 access lists. In the example described in this document, routers R1 and R2 are configured with IPv6 addressing scheme and connected through serial link. The routing protocol enabled on the two routers is IPv6 OSPF, and the loopback addresses configured on both the routers (R1 and R2) are advertised to each other in area 0 with this command: **ipv6 ospf process−id area area−id [***instance instance−id***]** . In this example, it is required to deny telnet traffic that originates from the loopback 0 interface of router R2 and reaches loopback interface 4 of router R1.

This configuration example uses the **ipv6 access−list access−list−name** command in order to construct an IPv6 access list (named **DENY_TELNET_Lo4**) on router R1. A deny statement ***deny tcp host 400A:0:400C::1 host 1001:ABC:2011:7::1 eq telnet*** is followed by a permit statement ***permit ipv6 any any*** .

In order to assign an IPv6 ACL to an interface, use this command in interface configuration mode: **ipv6 traffic−filter access−list−name {in | out}**

Prerequisites

Requirements

Ensure that you meet these requirements before you attempt this configuration:

- Knowledge of IPv6 Addressing Scheme
- Knowledge of Implementing OSPF for IPv6

Components Used

The information in this document is based on the Cisco 7200 series router on Cisco IOS Software Release 15.1 (for routers R1 and R2 configurations).

Conventions

Refer to Cisco Technical Tips Conventions for information on document conventions.

Configure

In this section, you are presented with the information to configure the features described in this document.

Note: Use the Command Lookup Tool (registered customers only) to find more information on the commands used in this document.

Network Diagram

This document uses this network setup:



Configurations

This document uses these configurations:

- Router R1
- Router R2

Router 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 looback1 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
```

Router 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
```

Verify

In order to verify the configuration, use the **ping** command.

On Router R2

This sample output shows that router R2 can reach the loopback interface of router 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
```

Try **telent** loopback 4 interface of router R1 from the loopback 0 interface of router R2.

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

The above ouput confirms that the telnet is denied by the remote host (that is, by router R1).

Use the **show ipv6 access-list DENY_TELNET_Lo4** command in order to check the access list created in router R1 as shown in this example:

On Router 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
```

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Related Information

- **IPv6 Configuration Guide, Cisco IOS Release 15.1 M&T**
- **IPv6 Technology Support**
- **Technical Support & Documentation − Cisco Systems**

Contacts & Feedback | Help | Site Map
© 2014 − 2015 Cisco Systems, Inc. All rights reserved. Terms & Conditions | Privacy Statement | Cookie Policy | Trademarks of Cisco Systems, Inc.

Updated: Nov 19, 2014 Document ID: 113126