Configuration of an IPv6 Access Control List

Note This chapter is *not* applicable on the Cisco ASR 900 RSP3 Module.

IPv6 Access Control Lists (ACLs) determine what traffic is blocked and what traffic is forwarded at device interfaces. ACLs allow filtering based on source and destination addresses, inbound and outbound to a specific interface.

- Restrictions, on page 1
- Configuring IPv6 Access Control List, on page 2
- Example for Configuration of IPv6 ACL, on page 4
- Verifying the Configuration, on page 4

Restrictions

The following restrictions apply when configuring IPv6 ACLs:

- ACE-specific counters are not supported.
- Layer 3 IPv4 and IPv6 ACLs are not supported on same EVC.
- MAC ACLs are not supported on EFP or trunk EFP interfaces to which Layer 3 IPv4 or IPv6 ACLs are applied.
- Up to 500 ACEs per ACL or 1500 total ACEs are supported.
- Egress v4/v6 ACL on EVC is not supported.

The following ACE parameters are supported:

- Source address
- Destination address
- TCP ports
- UDP ports
- DSCP value

- ICMP

Other ACE parameters are not supported.

Configuring IPv6 Access Control List

The sections below describe how to configure an IPv6 ACL on the Cisco ASR 903 Series Router:

Before you begin

Creating an IPv6 Access List

Before you begin

SUMMARY STEPS

1. **configure terminal**
2. **ipv6 access-list** *access-list-name*
3. **permit** *protocol* {*source-ipv6-prefix/prefix-length* | any | host *source-ipv6-address*} [port-number] {*destination-ipv6-prefix/prefix-length* | any | host *destination-ipv6-address*} [*port-number*] [dscp *value*] [log] [log-input] [sequence *value*]
4. **deny** *protocol* {*source-ipv6-prefix/prefix-length* | any | host *source-ipv6-address*} [port-number] {*destination-ipv6-prefix/prefix-length* | any | host *destination-ipv6-address*} [*port-number*] [dscp *value*] [log] [log-input] [sequence *value*]
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ipv6 access-list** *access-list-name* **Example:** `Device(config)# ipv6 access-list ipv6-acl`	Defines an IPv6 ACL, and enters IPv6 access list configuration mode.

Step 3	**permit** *protocol* {*source-ipv6-prefix/prefix-length* | any | host *source-ipv6-address*} [port-number] {*destination-ipv6-prefix/prefix-length* | any | host *destination-ipv6-address*} [*port-number*] [dscp *value*] [log] [log-input] [sequence *value*]
	Example:
	`Device(config-ipv6-acl)# permit`
	`0-255 An IPv6 protocol number`
	`X:X:X:X::X IPv6 source address x:x::y`
	`X:X:X:X::X/0-128 IPv6 source prefix x:x::y/z`
	`ahp Authentication Header Protocol`
	`any Any source prefix`
	`esp Encapsulation Security Payload`
		Sets permit conditions for the IPv6 ACL.

	Command or Action	Purpose
	hbh Hop by Hop options header host A single source host icmp Internet Control Message Protocol ipv6 Any IPv6 pcp Payload Compression Protocol sctp Streams Control Transmission Protocol tcp Transmission Control Protocol udp User Datagram Protocol	
Step 4	**deny** *protocol* {*source-ipv6-prefix/prefix-length* | any | host *source-ipv6-address*} [port-number] {*destination-ipv6-prefix/prefix-length* | any | host *destination-ipv6-address*} [*port-number*] [dscp *value*] [log] [log-input] [sequence *value*] **Example:** Device(config-ipv6-acl)# deny 0-255 An IPv6 protocol number X:X:X:X::X IPv6 source address x:x::y X:X:X:X::X/0-128 IPv6 source prefix x:x::y/z ahp Authentication Header Protocol any Any source prefix esp Encapsulation Security Payload hbh Hop by Hop options header host A single source host icmp Internet Control Message Protocol ipv6 Any IPv6 pcp Payload Compression Protocol sctp Streams Control Transmission Protocol tcp Transmission Control Protocol udp User Datagram Protocol	Sets deny conditions for the IPv6 ACL.
Step 5	**end**	Return to privileged EXEC mode.

Applying an IPv6 Access Control List to a Physical Interface

Before you begin

SUMMARY STEPS

1. **configure terminal**
2. **interface** *interface-id*
3. **ipv6 traffic-filter** *access-list-name [*in | out*]*
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode.

	Command or Action	Purpose
Step 2	**interface** *interface-id*	Specify the port to attach to the policy map, and enter interface configuration mode. Valid interfaces are physical ports.
Step 3	**ipv6 traffic-filter** *access-list-name [*in | out*]* **Example:** `Device(config)# ipv6 traffic-filter ipv6-acl`	Defines an IPv6 ACL, and enters IPv6 access list configuration mode.
Step 4	**end**	Return to privileged EXEC mode.

Example for Configuration of IPv6 ACL

```
Router(config)# ipv6 access-list ipv6_acl
Router(config-ipv6-acl)# permit tcp any any
Router(config-ipv6-acl)# permit udp any any
Router(config-ipv6-acl)# permit any any
Router(config-ipv6-acl)# hardware statistics
Router(config-ipv6-acl)# exit

! Assign an IP address and add the ACL on the interface.

Router(config)# interface GigabitEthernet3/1/0
Router(config-if)# no ip address
Router(config-if)# negotiation auto
Router(config-if)# ipv6 address 2001:1::1/64
Router(config-if)# ipv6 enable
Router(config-if)# ipv6 traffic-filter ipv6_acl in
Router(config-if)# exit
Router(config)# exit
Router# clear counters
Clear "show interface" counters on all interfaces [confirm]
Router#

! Verify the configurations.

Router# show running-config interface GigabitEthernet3/1/0

Building configuration...

Current configuration : 114 bytes
!
interface GigabitEthernet3/1/0
 no ip address
 negotiation auto
 ipv6 address 1001::1/64
 ipv6 traffic-filter ipv6_acl in
end
```

Verifying the Configuration

You can use the following commands to verify your IPv6 ACL configuration on the Cisco ASR 903 Series Router:

- **show platform hardware pp active** acl label *label-number*—Displays ACL information for a given label.
- **show platform hardware pp active** acl name *acl-name*—Displays ACL information for a given ACL name.
- **show platform hardware pp active** acl *acl-name* stats—Displays statistics for a given IPv6 ACL.
- **show platform hardware pp active** tcam utilization acl detail *id*—Displays TCAM usage for a given IPv6 ACL.

Before you begin