Implementing Traffic Filters for IPv6 Security

Last Updated: November 14, 2011

This module describes how to configure Cisco IOS XE IPv6 traffic filter and firewall features for your Cisco networking devices. These security features can protect your network from degradation or failure and also from data loss or compromised security resulting from intentional attacks and from unintended but damaging mistakes by well-meaning network users.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for Implementing Traffic Filters for IPv6 Security

- In Cisco IOS XE software, the standard IPv6 access control list (ACL) functionality is extended to support traffic filtering based on IPv6 option headers and optional, upper-layer protocol type information for finer granularity of control (functionality similar to extended ACLs in IPv4).
- The IPv6 Template ACL feature applies only to virtual access interfaces and sessions with ACLs defined using RADIUS. ACLs on vty interfaces or named ACLs on physical interfaces are not supported by this feature.

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

- The IPv6 Template ACL feature supports vendor-specific attribute (VSA) Cisco AV-pairs only. It does not support the Attribute 242 ACL.

Information About Implementing Traffic Filters for IPv6 Security

Access Control Lists for IPv6 Traffic Filtering

The standard ACL functionality in IPv6 is similar to standard ACLs in IPv4. Access lists determine what traffic is blocked and what traffic is forwarded at router interfaces and allow filtering based on source and destination addresses, inbound and outbound to a specific interface. Each access list has an implicit deny statement at the end. IPv6 ACLs are defined and their deny and permit conditions are set using the **ipv6 access-list** command with the **deny** and **permit** keywords in global configuration mode.

Named and tagged ACLs are both supported in IPv6:

- A named ACL consists of one or more access control entry (ACE) and is defined on the Intelligent Service Gateway (ISG) router by name.
- A name for a tagged ACL is dynamically created by the AAA when the ACL is applied. These ACEs are defined on the RADIUS.

IPv6 Packet Inspection

The following header fields are all used for IPv6 inspection--traffic class, flow label, payload length, next header, hop limit, and source or destination address. For further information on and descriptions of the IPv6 header fields, see RFC 2474.

Tunneling Support

IPv6 packets tunneled in IPv4 are not inspected. If a tunnel terminates on a router, and IPv6 traffic exiting the tunnel is nonterminating, then the traffic is inspected.

Virtual Fragmentation Reassembly

When virtual fragmentation reassembly (VFR) is enabled, VFR processing begins after ACL input lists are checked against incoming packets. The incoming packets are tagged with the appropriate VFR information.

Access Class Filtering in IPv6

Filtering incoming and outgoing connections to and from the router based on an IPv6 ACL is performed using the **ipv6 access-class** command in line configuration mode. The **ipv6 access-class** command is similar to the **access-class** command, except the IPv6 ACLs are defined by a name. If the IPv6 ACL is applied to inbound traffic, the source address in the ACL is matched against the incoming connection source address and the destination address in the ACL is matched against the local router address on the interface. If the IPv6 ACL is applied to outbound traffic, the source address in the ACL is matched against the local router address on the interface and the destination address in the ACL is matched against the outgoing connection source address. We recommend that identical restrictions are set on all the virtual terminal lines because a user can attempt to connect to any of them.

IPv6 Template ACL

When user profiles are configured using vendor-specific attribute (VSA) Cisco AV-pairs, similar per-user IPv6 ACLs may be replaced by a single template ACL. That is, one ACL represents many similar ACLs. By using IPv6 template ACLs, you can increase the total number of per-user ACLs while minimizing the memory and Ternary Content Addressable Memory (TCAM) resources needed to support the ACLs.

The IPv6 Template ACL feature can create templates using the following ACL fields:

- IPv6 source and destination addresses
- TCP and UDP, including all associated ports (0 through 65535)
- ICMP neighbor discovery advertisements and solicitations
- IPv6 DSCP with specified DSCP values

ACL names are dynamically generated by this feature; for example:

- 6Temp_#152875854573--Example of a dynamically generated template name for a template ACL parent
- Virtual-Access2.32135#152875854573--Example of a child ACL or an ACL that has not yet been made part of a template.

SSO ISSU Support for Per-User IPv6 ACL for PPP Sessions

The SSO/ISSU Support for per-User IPv6 ACL for PPP Sessions feature reproduces IPv6 ACLs on the active Route Processor to the standby RP and provides a consistent stateful switchover and in-service software upgrade experience for active sessions. The feature also extends the ability to maintain Template ACLs (IPv6 only or dual stack) through ISSU and SSO.

Both named and tagged ACLs can be configured and applied in the following ways:

- Virtual-template ACL:
  - Virtual-template ACLs (also called interface ACLs) are configured under a virtual-template definition on the ISG router.
  - Only named ACLs can be configured under a virtual-template definition. Named ACLs applied to virtual templates get cloned to all virtual access interfaces created using that virtual-template definition.
- Per-user ACLs are always applied through RADIUS:
  - User profile--The ACL is configured in the user profile on RADIUS and is applied when the session is up.

- Change of Authorization (CoA) per-user push--The ACL is applied through a RADIUS CoA push from a subscriber profile.

The table below shows information about support for functionality and SSO for these ACL configurations:

Table 1 SSO Support for Named and Tagged ACLs

ACL Configuration	Functionality Supported	SSO Supported
Named ACL		
Virtual-Template	Yes	Yes
User Profile	Yes	Yes
CoA per-User Push	Yes	No
Tagged ACL		
Virtual-Template	No	No
User Profile	Yes	Yes
CoA per-User Push	Yes	No

How to Implement Traffic Filters for IPv6 Security

Configuring IPv6 Traffic Filtering

Creating and Configuring an IPv6 ACL for Traffic Filtering

Note IPv6 ACLs on the Cisco ASR 1000 platform do not contain implicit permit rules. The IPv6 neighbor discovery process uses the IPv6 network-layer service; therefore, to enable IPv6 neighbor discovery, you must add IPv6 ACLs to allow IPv6 neighbor discovery packets to be sent and received on an interface. In IPv4, the Address Resolution Protocol (ARP), which is equivalent to the IPv6 neighbor discovery process, uses a separate data-link-layer protocol; therefore, by default IPv4 ACLs implicitly allow ARP packets to be sent and received on an interface.

>

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 access-list** *access-list-name*
4. Do one of the following:
   - **permit protocol** {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix / prefix-length* | **any** | **host** *destination-ipv6-address*} [**operator** [*port-number*]] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*]
   -
   -
   - **deny** *protocol* {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*} [*operator port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*] [**undetermined-transport**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

Command or Action	Purpose
Step 3 **ipv6 access-list** *access-list-name* **Example:** `Router(config)# ipv6 access-list outbound`	Defines an IPv6 ACL, and enters IPv6 access list configuration mode. • The *access-list name*argument specifies the name of the IPv6 ACL. IPv6 ACL names cannot contain a space or quotation mark, or begin with a numeral.

Step 4 Do one of the following:
• **permit protocol** {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix / prefix-length* | **any** | **host** *destination-ipv6-address*} [**operator** [*port-number*]] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*]
•
•
• **deny** *protocol* {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*} [*operator port-number*]] {*destination-ipv6-prefix/ prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*] [**undetermined-transport**
 	
Example:
`Router(config-ipv6-acl)# permit tcp 2001:DB8:0300:0201::/32 eq telnet any`
 	
Example:
 	
Example:
 	
Example:
`Router(config-ipv6-acl)# deny tcp host 2001:DB8:1::1 any log-input`
	Specifies permit or deny conditions for an IPv6 ACL.

Applying the IPv6 ACL to an Interface

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 traffic-filter** *access-list-name* {**in**| **out**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface gigabitethernet 0/0/0`	Specifies the interface type and number, and enters interface configuration mode.
Step 4	**ipv6 traffic-filter** *access-list-name* {**in**| **out**} **Example:** `Router(config-if)# ipv6 traffic-filter outbound out`	Applies the specified IPv6 access list to the interface specified in the previous step.

Controlling Access to a vty

Creating an IPv6 ACL to Provide Access Class Filtering

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 access-list** *access-list-name*
4. Do one of the following:
   - **permit protocol** {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix / prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*
   -
   -
   - **deny** *protocol* {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address*} [*operator port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*] [**undetermined-transport**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 access-list** *access-list-name* **Example:** `Router(config)# ipv6 access-list cisco`	Defines an IPv6 ACL, and enters IPv6 access list configuration mode.

Command or Action	Purpose

Step 4 Do one of the following:
• **permit protocol** {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix / prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*
•
•
• **deny** *protocol* {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address*} [*operator port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*] [**undetermined-transport**
Example:
`Router(config-ipv6-acl)# permit ipv6 host 2001:DB8:0:4::32 any eq telnet`
Example:
Example:
Example:
`Router(config-ipv6-acl)# deny ipv6 host 2001:DB8:0:6::6/32 any`
	Specifies permit or deny conditions for an IPv6 ACL.

Applying an IPv6 ACL to the Virtual Terminal Line

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **line** [**aux**| **console**| **tty**| **vty**] *line-number*[*ending-line-number*]
4. **ipv6 access-class** *ipv6-access-list-name* {**in**| **out**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**line** [**aux**| **console**| **tty**| **vty**] *line-number*[*ending-line-number*] **Example:** `Router(config)# line vty 0 4`	Identifies a specific line for configuration and enters line configuration mode. • In this example, the **vty** keyword is used to specify the virtual terminal lines for remote console access.
Step 4	**ipv6 access-class** *ipv6-access-list-name* {**in**| **out**} **Example:** `Router(config-line)# ipv6 access-class cisco in`	Filters incoming and outgoing connections to and from the router based on an IPv6 ACL.

Enabling IPv6 Template Processing

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **access-list template** [*number-of-rules*]
4. **exit**
5. **show access-list template** {**summary** | *aclname* | **exceed** *number* | **tree**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**access-list template** [*number-of-rules*] **Example:** `Router(config)# access-list template 50`	Enables template ACL processing. • The example in this task specifies that ACLs with 50 or fewer rules will be considered for template ACL status. • The *number-of-rules* argument default is 100.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and places the router in privileged EXEC mode.
Step 5	**show access-list template** {**summary** | *aclname* | **exceed** *number* | **tree**} **Example:** `Router# show access-list template summary`	Displays information about ACL templates.

Troubleshooting IPv6 Security Configuration and Operation

SUMMARY STEPS

1. **enable**
2. **clear ipv6 access-list** [*access-list-name*]
3. **clea r ipv6 inspect** {**session** *session-number* | **all**}
4. **clear ipv6 prefix-list** [*prefix-list-name*] [*ipv6-prefix*/*prefix-length*
5. **debug platform software acl config**
6. **debug platform software acl interface**
7. **debug platform software acl statistics**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router# enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**clear ipv6 access-list** [*access-list-name*] **Example:** `Router# clear ipv6 access-list list1`	Resets the IPv6 access list match counters.
Step 3	**clea r ipv6 inspect** {**session** *session-number* | **all**} **Example:** `Router# clear ipv6 inspect all`	Removes a specific IPv6 session or all IPv6 inspection sessions.
Step 4	**clear ipv6 prefix-list** [*prefix-list-name*] [*ipv6-prefix*/*prefix-length* **Example:** `Router# clear ipv6 prefix-list`	Resets the hit count of the IPv6 prefix list entries.
Step 5	**debug platform software acl config** **Example:** `Router# debug platform software acl config`	Enables debugging for ACL configuration changes, such as addition, deletion, or editing of an ACL and ACL entries.
Step 6	**debug platform software acl interface** **Example:** `Router# debug platform software acl interface`	Enables debugging for interface ACL configurations, such as applying or removing an ACL to or from an interface.
Step 7	**debug platform software acl statistics** **Example:** `Router# debug platform software acl statistics`	Enables statistics update messages from the Forwarding Processor Forwarding Manager.

Configuration Examples for Implementing Traffic Filters for IPv6 Security

Example Configuring an Access List on the Router

Example Route Processor Forwarding Manager ACL Configuration

```
Router# show running-config interface port-channel 3.2
Building configuration...
Current configuration : 328 bytes
!
interface Port-channel3.2
 encapsulation dot1Q 2 primary GigabitEthernet0/0/4 secondary GigabitEthernet1/2/4
 ip address 10.1.1.1 255.255.255.0
 ipv6 address 2001:DB8:1111:1111::1/64
 ipv6 traffic-filter OutFilter_IPv6 out
 ipv6 nd reachable-time 180000
 ipv6 nd ra suppress
 ipv6 ospf 100 area 0
 snmp trap link-status
end
Router# show ipv6 access-list OutFilter_IPv6
IPv6 access list OutFilter_IPv6
    permit icmp any any mld-query sequence 30
    permit icmp any any router-advertisement sequence 40
    deny 103 any any sequence 50
    permit icmp any any packet-too-big sequence 60
    deny icmp any any sequence 70
    deny ipv6 2404:1A8:1100:9::/64 any sequence 74
    deny ipv6 2404:1A8:1100:10::/64 any sequence 75
    permit ipv6 any 2050::/16 log-input sequence 80
    deny ipv6 2404:1A8:1100:13::/64 any sequence 90
    deny ipv6 2404:1A8:1100:14::/64 any sequence 100
    deny ipv6 2408:40:2000::/35 2408:40:2000::/35 dscp default sequence 110
    permit ipv6 any any (3974749339 matches) sequence 120
Router# show platform software access-list R0 statistics
Forwarding Manager Access-list Messaging Statistics
Set Log Threshold: 0, Interval: 0
IPv4 Access-list Entry Add: 1, Delete: 0
IPv4 Access-list Bind: 0, Unbind: 0
IPv4 Access-list Resequence: 0, Delete: 1
IPv6 Access-list Entry Add: 82, Delete: 0
IPv6 Access-list Bind: 3003, Unbind: 0
IPv6 Access-list Resequence: 0, Delete: 0
Access-list Sync Start: 0, End: 0
CPP Match Add: 0, Replace: 0, ACK Success: 0, ACK Error: 0
CPP Match Delete: 0, ACK Success: 0, ACK Error: 0
CPP Action Edit: 0, ACK Success: 0, ACK Error: 0
CPP Action Replace: 0, ACK Success: 0, ACK Error: 0
CPP Bind: 0, ACK Success: 0, ACK Error: 0
CPP Unbind: 0, ACK Success: 0, ACK Error: 0
```

```
Router# show platform software access-list R1 name OutFilter_IPv6 ace 100
Access-list: OutFilter_IPv6
Access-list Entry Sequence: 100
  Type: Permanent, Operation: Add
  Action: Deny
  Destination Address: ::, Length: 00
  Source Address: 2404:1a8:1100:14::, Length: 0x24
```

Example Forwarding Processor Forwarding Manager ACL Configuration

```
Router# show platform software access-list F0 statistics
Forwarding Manager Access-list Messaging Statistics
Set Log Threshold: 0, Interval: 0
IPv4 Access-list Entry Add: 0, Delete: 0
IPv4 Access-list Bind: 0, Unbind: 0
IPv4 Access-list Resequence: 0, Delete: 1
IPv6 Access-list Entry Add: 82, Delete: 0
IPv6 Access-list Bind: 3003, Unbind: 0
IPv6 Access-list Resequence: 0, Delete: 0
Access-list Sync Start: 0, End: 0
CPP Match Add: 86, Replace: 0, ACK Success: 86, ACK Error: 0
CPP Match Delete: 4, ACK Success: 4, ACK Error: 0
CPP Action Edit: 83, ACK Success: 83, ACK Error: 0
CPP Action Replace: 0, ACK Success: 0, ACK Error: 0
CPP Bind: 3003, ACK Success: 3003, ACK Error: 0
CPP Unbind: 0, ACK Success: 0, ACK Error: 0
Router# show platform software access-list F0 name OutFilter_IPv6 ace 100
  Access-list: OutFilter_IPv6
  Access-list Entry Sequence: 100
  Match Class Index: 11
  Epoch: 0
  State: Downloaded
  Requested Operation: No-op
  Issued Operation: No-op
  Type: Permanent
Action: Deny
Router# access-list F0 name OutFilter_IPv6 ace 100 max-records 20
Access-list: OutFilter_IPv6
Access-list Index: 2, Protocol: IPv6, Type: IPv6
  Security References: 2001, Classifier References: 0, Shared target: 2001
  Pending Download Access-list Entry: 0
  Pending Acknowledgements Matches: 0, Actions: 0
  Downloaded Access-list Entry: 12
  Total Access-list Entry after pending updates are processed: 12
  AOM object identifier: 141
  State: Normal
  Number of Access-list Entry Shown: 3
  ACE Number  Class Index  State
  ----------------------------------------------------------------------
  100         11           Downloaded
  110         12           Downloaded
  120         13           Downloaded
```

The following command summarizes the number of entries and references in the access list:

```
Router# show platform software access-list F0 summary
Access-list                          Index       Num Ref      Num ACEs
-------------------------------------------------------------------------------
icmp2                                1           1            2
OutFilter_IPv6                       2           2001         12
p11                                  3           1000         3
```

Example Applying an IPv6 Access List to an Interface

- Example Route Processor Forwarding Manager ACL Application to an Interface, page 15
- Example Forwarding Processor Forwarding Manager ACL Application to an Interface, page 15

Example Route Processor Forwarding Manager ACL Application to an Interface

The following examples show how to configure and verify the Route Processor Forwarding Manager access list application to Gigabit Ethernet interface 1/0/1:

```
Router(config)# interface GigabitEthernet 1/0/1
Router(config-if)# ip access-group test in
Router# show platform software access-list R0 statistics
Forwarding Manager Access-list Messaging Statistics
Set Log Threshold: 0, Interval: 0
IPv4 Access-list Entry Add: 1, Delete: 0
IPv4 Access-list Bind: 0, Unbind: 0
IPv4 Access-list Resequence: 0, Delete: 1
IPv6 Access-list Entry Add: 82, Delete: 0
IPv6 Access-list Bind: 3003, Unbind: 0
IPv6 Access-list Resequence: 0, Delete: 0
Access-list Sync Start: 0, End: 0
CPP Match Add: 0, Replace: 0, ACK Success: 0, ACK Error: 0
CPP Match Delete: 0, ACK Success: 0, ACK Error: 0
CPP Action Edit: 0, ACK Success: 0, ACK Error: 0
CPP Action Replace: 0, ACK Success: 0, ACK Error: 0
CPP Bind: 0, ACK Success: 0, ACK Error: 0
CPP Unbind: 0, ACK Success: 0, ACK Error: 0
Router# show platform software access-list R0 bind interface Port-channel1.2
Interface: Port-channel1.2, Index: 35, Protocol: IPv6, Direction: Output
  Access-list: OutFilter_IPv6
  Operation: Add
```

Example Forwarding Processor Forwarding Manager ACL Application to an Interface

The following examples show how to configure and verify the Forwarding Processor Forwarding Manager access list application to Gigabit Ethernet interface 1/0/1:

```
Router(config)# interface GigabitEthernet 1/0/1
Router(config-if)# ip access-group test in
Router# show platform software access-list F0 statistics

Forwarding Manager Access-list Messaging Statistics
Set Log Threshold: 0, Interval: 0
IPv4 Access-list Entry Add: 0, Delete: 0
IPv4 Access-list Bind: 0, Unbind: 0
IPv4 Access-list Resequence: 0, Delete: 1
IPv6 Access-list Entry Add: 82, Delete: 0
IPv6 Access-list Bind: 3003, Unbind: 0
IPv6 Access-list Resequence: 0, Delete: 0
Access-list Sync Start: 0, End: 0
CPP Match Add: 86, Replace: 0, ACK Success: 86, ACK Error: 0
CPP Match Delete: 4, ACK Success: 4, ACK Error: 0
CPP Action Edit: 83, ACK Success: 83, ACK Error: 0
CPP Action Replace: 0, ACK Success: 0, ACK Error: 0
CPP Bind: 3003, ACK Success: 3003, ACK Error: 0
CPP Unbind: 0, ACK Success: 0, ACK Error: 0
```

The following example provides a summary of the access list with number of entries and number of references:

```
Router# show platform software access-list F0 summary
Access-list                          Index        Num Ref      Num ACEs
-------------------------------------------------------------------------
icmp2                                  1            1             2
OutFilter_IPv6                         2            2001         12
p11                                    3            1000          3
m1                                     4            1             2
p1                                     5            0             3
```

Example IPv6 Template ACL Processing

In this example, the contents of ACL1 and ACL2 are the same, but the names are different:

```
ipv6 access-list extended ACL1 (PeerIP: 2001:1::1/64)
permit igmp any                 2003:1::1/64
permit icmp 2002:5::B/64        any
permit udp  any                 host 2004:1::5
permit udp  any                 host 2002:2BC::a
permit icmp host 2001:BC::7     host 2003:3::7
ipv6 access-list extended ACL2 (PeerIP: 2007:2::7/64)
permit igmp any                 2003:1::1/64
permit icmp 2002:5::B/64        any
permit udp  any                 host 2004:1::5
permit udp  any                 host 2002:2BC::a
permit icmp host 2001:BC::7     host 2003:3::7
```

The template for these ACLs is as follows:

```
ipv6 access-list extended Template_1
permit igmp any                 2003:1::1/64
permit icmp 2002:5::B/64        any
permit udp  any                 host 2004:1::5
permit udp  any                 host 2002:2BC::a
permit icmp host 2001:BC::7     host 2003:3::7
```

Example Displaying Access List Statistics

The following example output for ACL statistics provides information about the counter aggregation and poll timer:

```
Router# show ipv6 access-list OutFilter_IPv6
IPv6 access list OutFilter_IPv6
    permit icmp any any mld-query sequence 30
    permit icmp any any router-advertisement sequence 40
    deny 103 any any sequence 50
    permit icmp any any packet-too-big sequence 60
    deny icmp any any sequence 70
    deny ipv6 2001:DB8:1100:9::/64 any sequence 74
    deny ipv6 2001:DB8:1100:10::/64 any sequence 75
    permit ipv6 any 2050::/16 log-input sequence 80
    deny ipv6 2001:DB8:1100:13::/64 any sequence 90
    deny ipv6 2001:DB8:1100:14::/64 any sequence 100
    deny ipv6 2001:DB8:2000::/35 2408:40:2000::/35 dscp default sequence 110
    permit ipv6 any any (175392444 matches) sequence 120
```

Additional References

Related Documents

Related Topic	Document Title
Basic IPv6 configuration	" Implementing IPv6 Addressing and Basic Connectivity ," *Cisco IOS XE IPv6 Configuration Guide*

Related Topic	Document Title
IPv6 supported feature list	" Start Here: Cisco IOS XE Software Release Specifics for IPv6 Features ," *Cisco IOS XE IPv6 Configuration Guide*
Stateful Switchover	Configuring Stateful Switchover
In Service Software Upgrade	Cisco IOS XE In Service Software Upgrade Process
IPv6 commands: complete command syntax, command mode, defaults, usage guidelines, and examples	*Cisco IOS IPv6 Command Reference*
Cisco IOS master command list, all releases	Cisco IOS Master Command List, All Releases

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIBs	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
RFC 2401	*Security Architecture for the Internet Protocol*
RFC 2402	*IP Authentication Header*
RFC 2428	*FTP Extensions for IPv6 and NATs*
RFC 2460	*Internet Protocol, Version 6 (IPv6) Specification*
RFC 2474	*Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*
RFC 3576	*Change of Authorization*

RFCs	Title
RFC 4241	*A Model of IPv6/IPv4 Dual Stack Internet Access Service*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Implementing Traffic Filters for IPv6 Security

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 2 Feature Information for Implementing Traffic Filters for IPv6 Security

Feature Name	Releases	Feature Information
IPv6 Services--Extended Access Control Lists	Cisco IOS XE Release 2.1	Standard IPv6 ACL functionality was extended to support traffic filtering based on IPv6 option headers and optional, upper-layer protocol type information for finer granularity of control. The following commands were modified by this feature: **clear ipv6 access-list**, **clear ipv6 inspect**, **clear ipv6 prefix-list**, **deny**, **ipv6 access-class**, **ipv6 access-list**, **ipv6 traffic-filter**, **line**, **permit**, **show ipv6 access-list**.

Feature Name	Releases	Feature Information
IPv6 Services--Standard Access Control Lists	Cisco IOS XE Release 2.1	Access lists determine what traffic is blocked and what traffic is forwarded at router interfaces and allow filtering based on source and destination addresses, inbound and outbound to a specific interface. The following commands were modified by this feature: **clear ipv6 access-list**, **clear ipv6 inspect**, **clear ipv6 prefix-list**, **deny**, **ipv6 access-class**, **ipv6 access-list**, **ipv6 traffic-filter**, **line**, **permit**, **show ipv6 access-list**.
IPv6 ACL--Template ACL	Cisco IOS XE Release 3.2S	This feature allows similar per-user IPv6 ACLs to be replaced by a single template ACL. The following commands were modified by this feature: **access-list template**, **show access-list template**.
SSO/ISSU Support for Per-User IPv6 ACL for PPP Sessions	Cisco IOS XE Release 3.2.1S	Reproducing IPv6 ACLs on the active RP to the standby RP provides a consistent SSO and ISSU experience for active sessions. The following section provides information about this feature: