



# Implementing Security for IPv6

---

This module describes how to configure security features for IPv6. Implementing IPv6 security features in Cisco IOS software consists of creating access control lists (ACLs). Secure Shell (SSH) is also available for IPv6. SSH is documented in the *Managing Cisco IOS Applications over IPv6* module.

## Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [Prerequisites for Implementing Security for IPv6, page 1](#)
- [Information About Implementing Security for IPv6, page 2](#)
- [How to Implement Security for IPv6, page 5](#)
- [Configuration Examples for Security for IPv6, page 24](#)
- [Additional References, page 27](#)

## Prerequisites for Implementing Security for IPv6

- This document assumes that you are familiar with IPv4. Refer to the publications referenced in the “[Related Documents](#)” section for IPv4 configuration and command reference information.
- This module assumes that you are familiar with IPv6 addressing and basic configuration. Refer to the *Implementing Basic Connectivity for IPv6* module for more information.

[Table 1](#) identifies the earliest release for each early-deployment train in which the feature became available.

*Table 1 Minimum Required Cisco IOS Release*

Feature	Minimum Required Cisco IOS Release by Release Train
Standard access control lists	12.2(2)T, 12.0(21)ST, 12.0(22)S, 12.2(14)S, 12.3, 12.3(2)T
Extended access control lists <sup>1</sup>	12.0(23)S, 12.2(13)T, 12.2(14)S, 12.3, 12.3(2)T
IPv6 IPsec to Authenticate OSPFv3	12.3(4)T
IPv6 IOS Firewall	12.3(7)T
IPv6 FTP Firewall inspection	12.3(11)T

1. IPv6 extended access control lists and IPv6 provider edge router over MPLS are implemented with hardware acceleration on the Cisco 12000 series Internet router IP service engineer (ISE) line cards in Cisco IOS routers in Cisco IOS Release 12.0(25)S and later releases.

## Information About Implementing Security for IPv6

To implement security features for IPv6, you need to understand the following concepts:

- [Access Control Lists for IPv6 Traffic Filtering, page 2](#)
- [IPsec for IPv6, page 2](#)
- [Cisco IOS Firewall for IPv6, page 3](#)

## Access Control Lists for IPv6 Traffic Filtering

Cisco IOS Release 12.2(2)T through Cisco IOS Release 12.2(13)T and Cisco IOS Release 12.0(21)ST and later releases only support standard IPv6 ACL functionality. This functionality is similar to standard ACLs in IPv4. It allows 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.

In Cisco IOS Release 12.0(23)S and 12.2(13)T or later releases, the standard IPv6 ACL functionality is extended to support—in addition to traffic filtering based on source and destination addresses—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).

## IPsec for IPv6

IPsec is a framework of open standards developed by the Internet Engineering Task Force (IETF) that provide security for transmission of sensitive information over unprotected networks such as the Internet. IPsec acts at the network layer, protecting and authenticating IP packets between participating IPsec devices (peers), such as Cisco routers. IPsec provides the following network security services. These services are optional. In general, local security policy will dictate the use of one or more of these services:

- Data confidentiality—The IPsec sender can encrypt packets before sending them across a network.

- **Data integrity**—The IPSec receiver can authenticate packets sent by the IPSec sender to ensure that the data has not been altered during transmission.
- **Data origin authentication**—The IPSec receiver can authenticate the source of the IPSec packets sent. This service is dependent upon the data integrity service.
- **Antireplay**—The IPSec receiver can detect and reject replayed packets.

**Note**

---

The term *data authentication* is generally used to mean data integrity and data origin authentication. Within this section it also includes antireplay services, unless otherwise specified.

---

With IPSec, data can be sent across a public network without observation, modification, or spoofing.

IPSec functionality is essentially identical in both IPv6 and IPv4; however, IPSec in IPv6 can be deployed from end-to-end—data may be encrypted along the entire path between a source node and destination node. (Typically, IPSec in IPv4 is deployed between border routers of separate networks.) In IPv6, IPSec is implemented using the authentication extension header and the ESP extension header. The authentication header provides integrity and authentication of the source. It also provides optional protection against replayed packets. The authentication header protects the integrity of most of the IP header fields and authenticates the source through a signature-based algorithm. The ESP header provides confidentiality, authentication of the source, connectionless integrity of the inner packet, antireplay, and limited traffic flow confidentiality.

**Note**

---

Currently, IPv6 IPsec is only available for the control plane. IPv6 IPsec for the data plane will be available in a future release.

---

## Cisco IOS Firewall for IPv6

Cisco IOS Firewall provides advanced traffic filtering functionality as an integral part of a network's firewall. Cisco IOS Firewall for IPv6 enables you to implement Cisco IOS Firewall in IPv6 networks. Cisco IOS Firewall coexists with Cisco IOS Firewall for IPv4 networks and is supported on all dual-stack routers.

Cisco IOS Firewall for IPv6 includes the following features:

- **Fragmented packet inspection.** The fragment header is used to trigger fragment processing. Cisco IOS Firewall virtual fragment reassembly (VFR) examines out-of-sequence fragments and switches the packets into correct order; examines the number of fragments from a single IP given a unique identifier (Denial of Service [DoS] attack); and performs virtual reassembly to hand off packets to upper-layer protocols.
- **IPv6 DoS attack mitigation.** Mitigation mechanisms have been implemented in the same fashion as for the current IPv4 implementation, including SYN half-open connections.
- **Tunneled packet inspection.** Tunneled IPv6 packets terminated at a Cisco IOS firewall router can be inspected by the Cisco IOS Firewall for IPv6.
- **Stateful packet inspection of TCP, UDP, ICMPv6, and FTP sessions.**
- **Stateful inspection of packets originating from the IPv4 network and terminating in an IPv6 environment by providing IPv4-to-IPv6 translation services.**
- **Interpretation or recognition of most IPv6 Extension Header information, including routing header, hop-by-hop Options header, and fragment header.**
- **Port-to-application mapping (PAM)**

## PAM

PAM allows you to customize TCP or UDP port numbers for network services or applications. PAM uses this information to support network environments that run services using ports that are different from the registered or well-known ports associated with an application.

Using the port information, PAM establishes a table of default port-to-application mapping information at the firewall. The information in the PAM table enables Context-based Access Control (CBAC) supported services to run on nonstandard ports. Previously, CBAC was limited to inspecting traffic using only the well-known or registered ports associated with an application. Now, PAM allows network administrators to customize network access control for specific applications and services.

PAM also supports host or subnet specific port mapping, which allows you to apply PAM to a single host or subnet using standard ACLs. Host or subnet specific port mapping is done using standard ACLs.

## Cisco IOS Firewall Alerts, Audit Trails, and SYSLOG

Cisco IOS firewall generates real-time alerts and audit trails based on events tracked by the firewall. Enhanced audit trail features use SYSLOG to track all network transactions; recording time stamps, source host, destination host, ports used, and the total number of transmitted bytes, for advanced, session-based reporting. Real-time alerts send SYSLOG error messages to central management consoles upon detecting suspicious activity. Using IOS firewall inspection rules, you can configure alerts and audit trail information on a per-application protocol basis. For example, if you want to generate audit trail information for TCP traffic, you can specify that in the Cisco IOS firewall rule that defines TCP inspection.

The Cisco IOS Firewall provides audit trail messages to record details about inspected sessions. Audit trail information is configurable on a per-application basis using the context-based access control (CBAC) inspection rules. To determine which protocol was inspected, use the port number associated with the responder. The port number appears immediately after the address.

## IPv6 Packet Inspection

The following header fields are all used for IPv6 inspection:

- Traffic class
- Flow label
- Payload length
- Next header
- Hop limit
- 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 non-terminating, then the traffic is inspected.

## Virtual Fragment Reassembly

When Virtual Fragment 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.

## Cisco IOS Firewall Restrictions

- Cisco IOS Intrusion Detection System (IDS) is not supported for IPv6.

# How to Implement Security for IPv6

The tasks in the following sections explain how to configure security features for IPv6:

- [Configuring IPv6 Traffic Filtering, page 5](#)
- [Controlling Access to a vty, page 10](#)
- [Configuring Cisco IOS Firewall for IPv6, page 13](#)
- [Verifying IPv6 Security Configuration and Operation, page 18](#)
- [Troubleshooting IPv6 Security Configuration and Operation, page 20](#)

## Configuring IPv6 Traffic Filtering

To enable IPv6 traffic filtering, you must perform the following steps:

1. Create an IPv6 ACL
2. Configure the IPv6 ACL to pass or block traffic
3. Apply to IPv6 ACL to an interface

If you are running Cisco IOS Release 12.2(13)T and 12.0(23)S or later releases, proceed to the “[Creating and Configuring an IPv6 ACL for Traffic Filtering](#)” section. If you are running Cisco IOS Release 12.2(11)T, 12.0(22)S, and 12.0(21)ST, or earlier releases, proceed to the “[Creating an IPv6 ACL for Traffic Filtering for Previous Releases](#)” section.

## Restrictions

IPv6 ACLs are defined by a unique name (IPv6 does not support numbered ACLs). An IPv4 ACL and an IPv6 ACL cannot share the same name.

## Creating and Configuring an IPv6 ACL for Traffic Filtering

The following task explains how to create an IPv6 ACL and configure the IPv6 ACL to pass or block traffic in Cisco IOS Release 12.2(13)T and 12.0(23)S or later releases.

## Prerequisites

In Cisco IOS Release 12.2(13)T and 12.0(23)S or later releases, for backward compatibility, the **ipv6 access-list** command with the **deny** and **permit** keywords in global configuration mode is still supported; however, an IPv6 ACL defined with deny and permit conditions in global configuration mode is translated to IPv6 access list configuration mode. See the “[Create and Apply IPv6 ACL: Examples](#)” section for an example of a translated IPv6 ACL configuration.

## Restrictions

- Each IPv6 ACL contains implicit permit rules to enable IPv6 neighbor discovery. These rules can be overridden if desired by placing a deny ipv6 any any statement within an ACL. The IPv6 neighbor discovery process makes use of the IPv6 network layer service; therefore, by default, IPv6 ACLs implicitly 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, makes use of a separate data link layer protocol; therefore, by default, IPv4 ACLs implicitly allow ARP packets to be sent and received on an interface.
- Time-based and reflexive ACLs are not supported for IPv4 or IPv6 on the Cisco 12000 series platform. The **reflect**, **timeout**, and **time-range** keywords of the **permit** command in IPv6 are excluded on the Cisco 12000 series.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 access-list** *access-list-name*
4. **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*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**reflect** *name* [**timeout** *value*]] [**routing**] [**time-range** *name*] [**sequence** *value*]  
or  
**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*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**routing**] [**time-range** *name*] [**undetermined-transport**] [**sequence** *value*]

## DETAILED STEPS

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

Command or Action	Purpose
<p><b>Step 3</b></p> <pre>ipv6 access-list access-list-name</pre> <p><b>Example:</b> Router(config)# ipv6 access-list outbound</p>	<p>Defines an IPv6 ACL and enters IPv6 access list configuration mode. The router prompt changes to Router(config-ipv6-acl)#.</p> <ul style="list-style-type: none"> <li>The <i>access-list name</i> argument specifies the name of the IPv6 ACL. IPv6 ACL names cannot contain a space or quotation mark, or begin with a numeral.</li> </ul>
<p><b>Step 4</b></p> <pre>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]] [dscp value] [flow-label value] [fragments] [log] [log-input] [reflect name] [timeout value]] [routing] [time-range name] [sequence value]</pre> <p>or</p> <pre>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]] [dscp value] [flow-label value] [fragments] [log] [log-input] [routing] [time-range name] [undetermined transport] [sequence value]</pre> <p><b>Example:</b> Router(config-ipv6-acl)# permit tcp 2001:0DB8:0300:0201::/32 eq telnet any reflect reflectout</p> <p><b>Example:</b> Router(config-ipv6-acl)# deny tcp host 1::1 any log-input</p>	<p>Specifies permit or deny conditions for an IPv6 ACL.</p> <ul style="list-style-type: none"> <li>The <i>protocol</i> argument specifies the name or number of an Internet protocol. It can be one of the keywords <b>ahp</b>, <b>esp</b>, <b>icmp</b>, <b>ipv6</b>, <b>pcp</b>, <b>sctp</b>, <b>tcp</b>, or <b>udp</b>, or an integer in the range from 0 to 255 representing an IPv6 protocol number.</li> <li>The <i>source-ipv6-prefix/prefix-length</i> and <i>destination-ipv6-prefix/prefix-length</i> arguments specify the source and destination IPv6 network or class of networks about which to set permit conditions.</li> <li>These arguments must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.</li> <li>The <b>any</b> keyword is an abbreviation for the IPv6 prefix ::/0.</li> <li>The <b>host source-ipv6-address</b> keyword and argument specify the source IPv6 host address about which to set permit conditions.</li> <li>The <i>source-ipv6-address</i> argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.</li> <li>Refer to the <b>permit</b> and <b>deny</b> commands in the <i>IPv6 for Cisco IOS Command Reference</i> document for information on supported arguments and keywords.</li> </ul>

## Apply the IPv6 ACL to an Interface

This task describes how to apply the IPv6 ACL to an interface in Cisco IOS Release 12.2(13)T and 12.0(23)S or later releases.

- enable**
- configure terminal**
- interface** *type number*
- ipv6 traffic-filter** *access-list-name* {**in** | **out**}

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>  Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<code>configure terminal</code>  Example: Router# configure terminal	Enters global configuration mode.
Step 3	<code>interface type number</code>  Example: Router(config)# interface ethernet 0	Specifies the interface type and number, and enters interface configuration mode.
Step 4	<code>ipv6 traffic-filter access-list-name {in   out}</code>  Example: Router(config-if)# ipv6 traffic-filter outbound out	Applies the specified IPv6 access list to the interface specified in the previous step. <ul style="list-style-type: none"> <li>The <b>in</b> keyword filters incoming IPv6 traffic on the specified interface.</li> <li>The <b>out</b> keyword filters outgoing IPv6 traffic on the specified interface.</li> </ul>

## What to Do Next

To secure vty access to the router, proceed to the [“Controlling Access to a vty”](#) section.

## Creating an IPv6 ACL for Traffic Filtering for Previous Releases

This task explains how to create an IPv6 ACL and configure the IPv6 ACL to pass or block traffic in Cisco IOS Release 12.2(11)T, 12.0(22)S, 12.0(21)ST, or earlier releases.

## Restrictions

- The *source-ipv6-prefix* argument filters traffic by packet source address, and the *destination-ipv6-prefix* argument filters traffic by packet destination address.
- The Cisco IOS software compares an IPv6 prefix against the **permit** and **deny** condition statements in the access list. Every IPv6 access list, including access lists that do not have any permit and deny condition statements, has an implicit **deny any any** statement as its last match condition. The priority or sequence value applied to each condition statement dictates the order in which the statement is applied in the access list.

## SUMMARY STEPS

- `enable`
- `configure {terminal}`

3. **ipv6 access-list** *access-list-name* {**permit** | **deny**} {*source-ipv6-prefix/prefix-length* | **any**} {*destination-ipv6-prefix/prefix-length* | **any**} [**priority value**]

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>ipv6 access-list</b> <i>access-list-name</i> { <b>permit</b>   <b>deny</b> } { <i>source-ipv6-prefix/prefix-length</i>   <b>any</b> } { <i>destination-ipv6-prefix/prefix-length</i>   <b>any</b> } [ <b>priority value</b> ]  <b>Example:</b> Router(config)# ipv6 access-list list2 deny fec0:0:0:2::/64 any	Defines an IPv6 ACL and sets deny or permit conditions for the ACL. <ul style="list-style-type: none"> <li>• The <i>access-list name</i> argument specifies the name of the IPv6 ACL. IPv6 ACL names cannot contain a space or quotation mark, or begin with a numeral.</li> <li>• The <b>deny</b> keyword specifies deny conditions for the access list.</li> <li>• The <b>permit</b> keyword specifies permit conditions for the access list.</li> <li>• The <i>prefix-length</i> argument indicates the number of consecutive, most significant bits that are used in the match. A slash mark must precede the decimal value.</li> <li>• The <b>any</b> keyword, when specified instead of the <i>source-ipv6-prefix/prefix-length</i> or <i>destination-ipv6-prefix/prefix-length</i>, matches any prefix and is equivalent to the IPv6 prefix ::/0.</li> <li>• The <b>priority</b> keyword specifies the order in which the statement is applied in the access list. The acceptable range is from 1 to 4294967295.</li> </ul>

## Apply the IPv6 ACL to an Interface in Previous Releases

This task describes how to apply the IPv6 ACL to an interface in Cisco IOS Release 12.2(11)T, 12.0(22)S, 12.0(21)ST, or earlier releases.

## SUMMARY STEPS

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

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>  Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<code>configure terminal</code>  Example: Router# configure terminal	Enters global configuration mode.
Step 3	<code>interface type number</code>  Example: Router(config)# interface ethernet 0	Specifies the interface type and number, and enters interface configuration mode.
Step 4	<code>ipv6 traffic-filter access-list-name {in   out}</code>  Example: Router(config-if)# ipv6 traffic-filter list2 out	Applies the specified IPv6 access list to the interface specified in the previous step. <ul style="list-style-type: none"> <li>The <b>in</b> keyword filters incoming IPv6 traffic on the specified interface.</li> <li>The <b>out</b> keyword filters outgoing IPv6 traffic on the specified interface.</li> </ul>

## Controlling Access to a vty

The following two tasks explain how to restrict access to a vty on a router.

### 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.

### Creating an IPv6 ACL for Access Class Filtering

The following task explains how to control access to a vty on a router by creating an IPv6 ACL to provide access class filtering.

## SUMMARY STEPS

1. **enable**

2. **configure terminal**
3. **ipv6 access-list** *access-list-name*
4. **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*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**reflect name** [*timeout value*]] [**routing**] [**time-range** *name*] [**sequence value**]  
 or  
**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*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**routing**] [**time-range** *name*] [**undetermined-transport**] [**sequence value**]

## DETAILED STEPS

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

Command or Action	Purpose
<p><b>Step 3</b></p> <pre>ipv6 access-list access-list-name</pre> <p><b>Example:</b> Router(config)# ipv6 access-list cisco</p>	<p>Defines an IPv6 ACL and enters IPv6 access list configuration mode. The router prompt changes to Router(config-ipv6-acl)#.</p> <ul style="list-style-type: none"> <li>The <i>access-list name</i> argument specifies the name of the IPv6 ACL. IPv6 ACL names cannot contain a space or quotation mark, or begin with a numeral.</li> </ul>
<p><b>Step 4</b></p> <pre>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]] [dscp value] [flow-label value] [fragments] [log] [log-input] [reflect name [timeout value]] [routing] [time-range name] [sequence value]</pre> <p>or</p> <pre>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]] [dscp value] [flow-label value] [fragments] [log] [log-input] [routing] [time-range name] [undetermined transport] [sequence value]</pre> <p><b>Example:</b> Router(config-ipv6-acl)# permit ipv6 host 2001:0DB8:0:4::32 any eq telnet</p> <p><b>Example:</b> Router(config-ipv6-acl)# deny ipv6 host 2001:0DB8:0:6::6/32 any</p>	<p>Specifies permit or deny conditions for an IPv6 ACL.</p> <ul style="list-style-type: none"> <li>The <i>protocol</i> argument specifies the name or number of an Internet protocol. For an access class match against the IPv6 ACL the argument must be either the <b>ipv6</b> or the <b>tcp</b> keyword. If TCP ports are specified within the ACL, the port ranges must include the ports used to gain access. For incoming connections, for example, the destination port must include the Telnet port.</li> <li>The <i>source-ipv6-prefix/prefix-length</i> and <i>destination-ipv6-prefix/prefix-length</i> arguments specify the source and destination IPv6 network or class of networks about which to set permit conditions. These arguments must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.</li> <li>The <b>any</b> keyword is an abbreviation for the IPv6 prefix ::/0.</li> <li>The <b>host source-ipv6-address</b> keyword and argument specify the source IPv6 host address about which to set permit conditions. The <i>source-ipv6-address</i> argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.</li> <li>Refer to the <b>permit</b> and <b>deny</b> commands in the <i>IPv6 for Cisco IOS Command Reference</i> document for information on supported arguments and keywords.</li> </ul>

## Applying the IPv6 ACL for Access Class Filtering

After you have created the IPv6 ACL for access class filtering, you must apply it to a specified virtual terminal line. The following task describes how to apply the 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	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>line [aux   console   tty   vty] line-number</b> [ending-line-number]  <b>Example:</b> Router(config)# line vty 0 4	Identifies a specific line for configuration and enters line configuration mode. <ul style="list-style-type: none"> <li>In this example, the <b>vty</b> keyword is used to specify the virtual terminal lines for remote console access.</li> </ul>
Step 4	<b>ipv6 access-class ipv6-access-list-name {in   out}</b>  <b>Example:</b> Router(config-line)# ipv6 access-class cisco in	Filters incoming and outgoing connections to and from the router based on an IPv6 ACL. <ul style="list-style-type: none"> <li>The <i>ipv6-access-list name</i> argument specifies the name of the IPv6 ACL. IPv6 ACL names cannot contain a space or quotation mark, or begin with a numeral.</li> <li>If the <b>in</b> keyword is used, 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.</li> <li>If the <b>out</b> keyword is used, 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.</li> </ul>

## Configuring Cisco IOS Firewall for IPv6

This task shows how to configure the Cisco IOS Firewall for IPv6 environments. This configuration scenario uses both packet inspection and ACLs.

## SUMMARY STEPS

- enable**
- configure terminal**
- ipv6 unicast-routing**
- ipv6 inspect name inspection-name protocol [alert {on | off}] [audit-trail {on | off}] [timeout seconds]**
- interface type number**

6. **ipv6 address** *ipv6-address/prefix*
7. **ipv6 enable**
8. **ipv6 traffic-filter** [**inbound** | **outbound**]
9. **ipv6 inspect** *inspect-name*
10. **ipv6 access-list** *access-list-name*
11. **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*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**reflect** *name*] [**timeout** *value*]] [**routing**] [**time-range** *name*] [**sequence** *value*]  
or  
**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*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**routing**] [**time-range** *name*] [**undetermined-transport**] [**sequence** *value*]

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>ipv6 unicast-routing</b>  <b>Example:</b> Router(config)# ipv6 unicast-routing	Enables IPv6 unicast routing.
Step 4	<b>ipv6 inspect name</b> <i>inspection-name protocol</i> [ <b>alert</b> { <b>on</b>   <b>off</b> }] [ <b>audit-trail</b> { <b>on</b>   <b>off</b> }] [ <b>timeout</b> <i>seconds</i> ]  <b>Example:</b> Router(config)# ipv6 inspect name ipv6_test icmp timeout 60	Defines a set of IPv6 inspection rules for the firewall.
Step 5	<b>interface type number</b>  <b>Example:</b> Router(config)# interface FastEthernet0/0	Specifies the interface on which the inspection will occur.
Step 6	<b>ipv6 address</b> <i>ipv6-address/prefix</i>  <b>Example:</b> Router(config-if)# ipv6 address 3FFE:C000:0:7::/64 eui-64	Provides the address for the inspection interface.

	Command or Action	Purpose
Step 7	<pre>ipv6 enable</pre> <p><b>Example:</b> Router(config-if)# ipv6 enable</p>	<p>Enables IPv6 routing.</p> <p><b>Note</b> This step is optional if the IPv6 address is specified in step 6.</p>
Step 8	<pre>ipv6 traffic-filter access-list-name {in   out}</pre> <p><b>Example:</b> Router(config-if)# ipv6 traffic-filter outbound out</p>	<p>Applies the specified IPv6 access list to the interface specified in the previous step.</p> <ul style="list-style-type: none"> <li>The <b>in</b> keyword filters incoming IPv6 traffic on the specified interface.</li> <li>The <b>out</b> keyword filters outgoing IPv6 traffic on the specified interface.</li> </ul>
Step 9	<pre>ipv6 inspect inspection-name {in out}</pre> <p><b>Example:</b> Router(config)#ipv6 inspect ipv6_test in</p>	<p>Applies the set of inspection rules.</p>
Step 10	<pre>ipv6 access-list acl-name</pre> <p><b>Example:</b> Router(config)# ipv6 access-list outbound</p>	<p>Defines an IPv6 ACL and enters IPv6 access list configuration mode. The router prompt changes to Router(config-ipv6-acl)#.</p> <ul style="list-style-type: none"> <li>The <i>access-list name</i> argument specifies the name of the IPv6 ACL. IPv6 ACL names cannot contain a space or quotation mark, or begin with a numeral.</li> </ul>
Step 11	<pre>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]] [dscp value] [flow-label value] [fragments] [log] [log-input] [reflect name] [time-range value]] [routing] [time-range name] [sequence value]</pre> <p>or</p> <pre>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]] [dscp value] [flow-label value] [fragments] [log] [log-input] [routing] [time-range name] [undetermined transport] [sequence value]</pre> <p><b>Example:</b> Router(config-ipv6-acl)# permit tcp 2001:0DB8:0300:0201::/32 any reflect reflectout</p> <p><b>Example:</b> Router(config-ipv6-acl)# deny tcp fec0:0:0:0201::/64 any</p>	<p>Specifies permit or deny conditions for an IPv6 ACL.</p> <ul style="list-style-type: none"> <li>The <i>protocol</i> argument specifies the name or number of an Internet protocol. It can be one of the keywords <b>ahp</b>, <b>esp</b>, <b>icmp</b>, <b>ipv6</b>, <b>pcp</b>, <b>sctp</b>, <b>tcp</b>, or <b>udp</b>, or an integer in the range from 0 to 255 representing an IPv6 protocol number.</li> <li>The <i>source-ipv6-prefix/prefix-length</i> and <i>destination-ipv6-prefix/prefix-length</i> arguments specify the source and destination IPv6 network or class of networks about which to set permit conditions.</li> <li>These arguments must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.</li> <li>The <b>any</b> keyword is an abbreviation for the IPv6 prefix ::/0.</li> <li>The <b>host source-ipv6-address</b> keyword and argument specify the source IPv6 host address about which to set permit conditions.</li> <li>The <i>source-ipv6-address</i> argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.</li> <li>Refer to the <b>permit</b> and <b>deny</b> commands in the <i>IPv6 for Cisco IOS Command Reference</i> document for information on supported arguments and keywords.</li> </ul>

## Configuring PAM for IPv6

The tasks in the following sections explain how to configure PAM for IPv6.

- [Creating an IPv6 Access Class Filter for PAM, page 16](#)
- [Applying the IPv6 Access Class Filter to PAM, page 17](#)

### Creating an IPv6 Access Class Filter for PAM

The following task explains how to create an IPv6 access class filter to use in PAM configuration:

#### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 access-list *acl-name***
4. **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*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**reflect** *name*] [**timeout** *value*] [**routing**] [**time-range** *name*] [**sequence** *value*]  
or  
**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*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**routing**] [**time-range** *name*] [**undetermined-transport**] [**sequence** *value*]

#### DETAILED STEPS

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

Command or Action	Purpose
<p><b>Step 3</b></p> <pre>ipv6 access-list <i>acl-name</i></pre> <p><b>Example:</b> Router(config)# ipv6 access-list outbound</p>	<p>Defines an IPv6 ACL and enters IPv6 access list configuration mode. The router prompt changes to Router(config-ipv6-acl)#.</p> <ul style="list-style-type: none"> <li>The <i>access-list name</i> argument specifies the name of the IPv6 ACL. IPv6 ACL names cannot contain a space or quotation mark, or begin with a numeral.</li> </ul>
<p><b>Step 4</b></p> <pre>permit {<i>protocol</i>} {<i>source-ipv6-prefix/prefix-length</i>   <b>any</b>   <b>host</b> <i>source-ipv6-address</i>} [<i>operator</i> [<i>port-number</i>]] {<i>destination-ipv6-prefix/prefix-length</i>   <b>any</b>   <b>host</b> <i>destination-ipv6-address</i>} [<i>operator</i> [<i>port-number</i>]] [<b>dscp</b> <i>value</i>] [<b>flow-label</b> <i>value</i>] [<b>fragments</b>] [<b>log</b>] [<b>log-input</b>] [<b>reflect</b> <i>name</i>] [<b>timeout</b> <i>value</i>]] [<b>routing</b>] [<b>time-range</b> <i>name</i>] [<b>sequence</b> <i>value</i>]</pre> <p>or</p> <pre>Router(config)# deny {<i>protocol</i>} {<i>source-ipv6-prefix/prefix-length</i>   <b>any</b>   <b>host</b> <i>source-ipv6-address</i>} [<i>operator</i> [<i>port-number</i>]] {<i>destination-ipv6-prefix/prefix-length</i>   <b>any</b>   <b>host</b> <i>destination-ipv6-address</i>} [<i>operator</i> [<i>port-number</i>]] [<b>dscp</b> <i>value</i>] [<b>flow-label</b> <i>value</i>] [<b>fragments</b>] [<b>log</b>] [<b>log-input</b>] [<b>routing</b>] [<b>time-range</b> <i>name</i>] [<b>undetermined transport</b>] [<b>sequence</b> <i>value</i>]</pre> <p><b>Example:</b> Router(config-ipv6-acl)# permit tcp 2001:0DB8:0300:0201::/32 any reflect reflectout</p> <p><b>Example:</b> Router(config-ipv6-acl)# deny tcp fec0:0:0:0201::/64 any</p>	<p>Specifies permit or deny conditions for an IPv6 ACL.</p> <ul style="list-style-type: none"> <li>The <i>protocol</i> argument specifies the name or number of an Internet protocol. It can be one of the keywords <b>ahp</b>, <b>esp</b>, <b>icmp</b>, <b>ipv6</b>, <b>pcp</b>, <b>sctp</b>, <b>tcp</b>, or <b>udp</b>, or an integer in the range from 0 to 255 representing an IPv6 protocol number.</li> <li>The <i>source-ipv6-prefix/prefix-length</i> and <i>destination-ipv6-prefix/prefix-length</i> arguments specify the source and destination IPv6 network or class of networks about which to set permit conditions.</li> <li>These arguments must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.</li> <li>The <b>any</b> keyword is an abbreviation for the IPv6 prefix ::/0.</li> <li>The <b>host</b> <i>source-ipv6-address</i> keyword and argument specify the source IPv6 host address about which to set permit conditions.</li> <li>The <i>source-ipv6-address</i> argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.</li> <li>Refer to the <b>permit</b> and <b>deny</b> commands in the <i>IPv6 for Cisco IOS Command Reference</i> document for information on supported arguments and keywords.</li> </ul>

### Applying the IPv6 Access Class Filter to PAM

Once you have created an IPv6 access class filter, use the following task to apply the filter to PAM:

#### SUMMARY STEPS

- enable**
- configure terminal**
- ipv6 port-map** *application\_name* **port** *port\_num* [**list** *acl\_name*]

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>  Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
Step 2	<code>configure terminal</code>  Example: Router# configure terminal	Enters global configuration mode.
Step 3	<code>ipv6 port-map application_name port port_num</code> [list acl_name]  Example: Router(config)# ipv6 port-map ftp port 8090 list PAM_ACL	Establishes PAM for the system.

## Verifying IPv6 Security Configuration and Operation

This task explains how to display information to verify the configuration and operation of IPv6 security options. Use the following commands as needed to verify configuration and operation. The commands shown in this task are displayed in user EXEC mode, but they can also be used in privileged EXEC mode.

## SUMMARY STEPS

1. `show crypto ipsec policy [name policy-name]`
2. `show crypto ipsec sa ipv6 [interface-type interface-number] [detailed]`
3. `show ipv6 access-list [access-list-name]`
4. `show ipv6 inspect {name inspection-name | config | interfaces | session [detail] | all}`
5. `show ipv6 prefix-list [detail | summary] [list-name]`
6. `show ipv6 virtual-reassembly interface interface-type`
7. `show logging [slot slot-number | summary]`
8. `show ipv6 port-map [application-name | port port-number]`

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<pre>show crypto ipsec policy [name policy-name]</pre> <p><b>Example:</b> Router&gt; show crypto ipsec policy</p>	Displays the parameters for each IPsec policy.
Step 2	<pre>show crypto ipsec sa ipv6 [interface-type interface-number] [detailed]</pre> <p><b>Example:</b> Router&gt; show crypto ipsec sa ipv6</p>	Displays the settings used by current security associations (SAs).
Step 3	<pre>show ipv6 access-list [access-list-name]</pre> <p><b>Example:</b> Router&gt; show ipv6 access-list</p>	Displays the contents of all current IPv6 access lists.
Step 4	<pre>show ipv6 inspect {name inspection-name   config   interfaces   session [detail]   all}</pre> <p><b>Example:</b> Router&gt; show ipv6 inspect interfaces</p>	Displays CBAC configuration and session information.
Step 5	<pre>show ipv6 prefix-list [detail   summary] [list-name]</pre> <p><b>Example:</b> Router&gt; show ipv6 prefix-list</p>	Displays information about an IPv6 prefix list or IPv6 prefix list entries.
Step 6	<pre>show ipv6 virtual-reassembly interface interface-type</pre> <p><b>Example:</b> Router&gt; show ipv6 virtual-reassembly interface e1/1</p>	Displays configuration and statistical information of VFR.
Step 7	<pre>show logging [slot slot-number   summary]</pre> <p><b>Example:</b> Router&gt; show logging</p>	Displays the state of system logging (syslog) and the contents of the standard system logging buffer. <ul style="list-style-type: none"> <li>• Access list entries with the <b>log</b> or <b>log-input</b> keywords will be logged when a packet matches the access list entry.</li> </ul>
Step 8	<pre>show ipv6 port-map [application-name   port port-number]</pre> <p><b>Example:</b> Router&gt; show ipv6 port-map ftp</p>	Verifies PAM configuration.

## Troubleshooting IPv6 Security Configuration and Operation

This optional task explains how to display information to troubleshoot the configuration and operation of IPv6 security options. Use the following commands only as needed to verify configuration and operation.

### SUMMARY STEPS

1. **enable**
2. **clear ipv6 access-list** [*access-list-name*]
3. **clear ipv6 inspect** {*session session-number* | **all**}
4. **clear ipv6 prefix-list** [*prefix-list-name*] [*ipv6-prefix/prefix-length*]
5. **debug crypto ipv6 ipsec**
6. **debug crypto ipv6 packet**
7. **debug ipv6 inspect** {*function-trace* | *object-creation* | *object-deletion* | *events* | *timers* | *protocol* | *detailed*}
8. **debug ipv6 packet** [*access-list access-list-name*] [**detail**]

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router# enable	Enables higher privilege levels, such as privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>clear ipv6 access-list</b> [ <i>access-list-name</i> ]  <b>Example:</b> Router# clear ipv6 access-list tin	Resets the IPv6 access list match counters. <ul style="list-style-type: none"> <li>• If the <i>access-list-name</i> argument is specified, only the specified access list counters will be reset.</li> </ul>
Step 3	<b>clear ipv6 inspect</b> { <i>session session-number</i>   <i>all</i> }  <b>Example:</b> Router# clear ipv6 inspect all	Removes a specific IPv6 session or all IPv6 inspection sessions.
Step 4	<b>clear ipv6 prefix-list</b> [ <i>prefix-list-name</i> ] [ <i>ipv6-prefix/prefix-length</i> ]  <b>Example:</b> Router# clear ipv6 prefix-list	Resets the hit count of the IPv6 prefix list entries.
Step 5	<b>debug crypto ipv6 ipsec</b>  <b>Example:</b> Router# debug crypto ipv6 ipsec	Displays IPsec events for IPv6 networks.

	Command or Action	Purpose
Step 6	<code>debug crypto ipv6 packet</code>  <b>Example:</b> Router# <code>debug crypto ipv6 packet</code>	Displays the contents of IPv6 packets.
Step 7	<code>debug ipv6 inspect {function-trace   object-creation   object-deletion   events   timers   protocol   detailed}</code>  <b>Example:</b> Router# <code>debug ipv6 inspect timers</code>	Displays messages about Cisco IOS Firewall events.
Step 8	<code>debug ipv6 packet [access-list access-list-name] [detail]</code>  <b>Example:</b> Router# <code>debug ipv6 packet access-list PAK-ACL</code>	Displays debugging messages for IPv6 packets. <ul style="list-style-type: none"> <li>• If the <b>access-list</b> keyword and <i>access-list-name</i> argument is specified, only packets matching the access list permit entries are displayed.</li> </ul>

## Verifying IPv6 Security Configuration and Operation Examples

This section provides the following output examples:

- [Sample Output for the show crypto ipsec policy Command](#)
- [Sample Output for the show crypto ipsec sa ipv6 Command](#)
- [Sample Output for the show ipv6 access-list Command](#)
- [Sample Output for the show ipv6 prefix-list Command](#)
- [Sample Output for the show ipv6 virtual-reassembly Command](#)
- [Sample Output for the show logging Command](#)

### Sample Output for the show crypto ipsec policy Command

The following is sample output from the **show crypto ipsec policy** command:

```
Router# show crypto ipsec policy

Crypto IPsec client security policy data

Policy name:      OSPFv3-1-1000
Policy refcount: 1
Inbound  AH SPI: 1000 (0x3E8)
Outbound AH SPI: 1000 (0x3E8)
Inbound  AH Key: 1234567890ABCDEF1234567890ABCDEF
Outbound AH Key: 1234567890ABCDEF1234567890ABCDEF
Transform set:   ah-md5-hmac
```

### Sample Output for the show crypto ipsec sa ipv6 Command

The following is sample output from the **show crypto ipsec sa ipv6** command:

```
Router# show crypto ipsec sa ipv6

IPv6 IPsec SA info for interface Ethernet0/0
```

```

protected policy name:OSPFv3-1-1000
IPsec created ACL name:Ethernet0/0-ipsecv6-ACL

local ident (addr/prefixlen/proto/port):(FE80::/10/89/0)
remote ident (addr/prefixlen/proto/port):(::/0/89/0)
current_peer::
  PERMIT, flags={origin_is_acl,}
  #pkts encaps:21, #pkts encrypt:0, #pkts digest:21
  #pkts decaps:20, #pkts decrypt:0, #pkts verify:20
  #pkts compressed:0, #pkts decompressed:0
  #pkts not compressed:0, #pkts compr. failed:0
  #pkts not decompressed:0, #pkts decompress failed:0
  #send errors 0, #recv errors 0

local crypto endpt. ::, remote crypto endpt. ::
path mtu 1500, media mtu 1500
current outbound spi:0x3E8(1000)

inbound ESP SAs:

inbound AH SAs:
spi:0x3E8(1000)
  transform:ah-md5-hmac ,
  in use settings ={Transport, }
  slot:0, conn_id:2000, flow_id:1, crypto map:N/R
  no sa timing (manual-keyed)
  replay detection support:N

inbound PCP SAs:

outbound ESP SAs:

outbound AH SAs:
spi:0x3E8(1000)
  transform:ah-md5-hmac ,
  in use settings ={Transport, }
  slot:0, conn_id:2001, flow_id:2, crypto map:N/R
  no sa timing (manual-keyed)
  replay detection support:N

outbound PCP SAs:

```

## Sample Output for the show ipv6 access-list Command

In the following example, the **show ipv6 access-list** user EXEC command is used to verify that IPv6 ACLs are configured correctly:

```
Router> show ipv6 access-list
```

```
IPv6 access list inbound
  permit tcp any any eq bgp reflect tcptraffic (8 matches) sequence 10
  permit tcp any any eq telnet reflect tcptraffic (15 matches) sequence 20
  permit udp any any reflect udptraffic sequence 30

IPv6 access list tcptraffic (reflexive) (per-user)
  permit tcp host 2001:0DB8:1::32 eq bgp host 2001:0DB8:2::32 eq 11000 timeout 300 (time
    left 243) sequence 1
  permit tcp host 2001:0DB8:1::32 eq telnet host 2001:0DB8:2::32 eq 11001 timeout 300
    (time left 296) sequence 2

IPv6 access list outbound
  evaluate udptraffic
  evaluate tcptraffic
```



Note

For a description of each output display field, refer to the **show ipv6 access-list** command in the *IPv6 for Cisco IOS Command Reference* document.

## Sample Output for the show ipv6 prefix-list Command

The following example shows the output of the **show ipv6 prefix-list** command with the **detail** keyword:

```
Router# show ipv6 prefix-list detail
```

```
Prefix-list with the last deletion/insertion: bgp-in
ipv6 prefix-list 6to4:
  count: 1, range entries: 0, sequences: 5 - 5, refcount: 2
  seq 5 permit 2001::/32 (hit count: 313, refcount: 1)
ipv6 prefix-list aggregate:
  count: 2, range entries: 2, sequences: 5 - 10, refcount: 30
  seq 5 deny 3FFE:C00::/24 ge 25 (hit count: 568, refcount: 1)
  seq 10 permit ::/0 le 48 (hit count: 31310, refcount: 1)
ipv6 prefix-list bgp-in:
  count: 6, range entries: 3, sequences: 5 - 30, refcount: 31
  seq 5 deny 5F00::/8 le 128 (hit count: 0, refcount: 1)
  seq 10 deny ::/0 (hit count: 0, refcount: 1)
  seq 15 deny ::/1 (hit count: 0, refcount: 1)
  seq 20 deny ::/2 (hit count: 0, refcount: 1)
  seq 25 deny ::/3 ge 4 (hit count: 0, refcount: 1)
  seq 30 permit ::/0 le 128 (hit count: 240664, refcount: 0)
```

## Sample Output for the show ipv6 virtual-reassembly Command

```
Router# show ipv6 virtual-reassembly interface e1/1
```

```
Configuration Information:
```

```
-----
Virtual Fragment Reassembly (VFR) is ENABLED...
Maximum number of datagram that can be reassembled at a time: 64
Maximum number of fragments per datagram: 8
Timeout value of a datagram: 3 seconds
```

```

Statistical Information:
-----
Number of datagram being reassembled:12
Number of fragments being processed:48
Total number of datagram reassembled:6950
Total number of datagram failed: 9

```

## Sample Output for the show logging Command

In the following example, the **show logging** command is used to display logging entries that match the first line (sequence 10) of the access list named tin:

```

Router> show logging

00:00:36: %IPV6-6-ACCESSLOGP: list tin/10 permitted tcp 2000:1::1(11001) (Ethernet0/0) ->
2000:1::2(179), 1 packet

```

## Troubleshooting IPv6 Security Configuration and Operation Examples

This section provides the following output examples:

- [Sample Output for the clear ipv6 access-list Command](#)

## Sample Output for the clear ipv6 access-list Command

In the following example, the **show ipv6 access-list** command is used to display some match counters for the access list named tin. Privileged EXEC mode is entered using the **enable** command (not shown) and the **clear ipv6 access-list EXEC** command is issued to reset the match counters for the access list named tin. The **show ipv6 access-list EXEC** command is used again to show that the match counters have been reset.

```

Router> show ipv6 access-list tin

IPv6 access list tin
  permit tcp any any log-input (6 matches) sequence 10
  permit icmp any any echo-request log-input sequence 20
  permit icmp any any echo-reply log-input sequence 30

Router# clear ipv6 access-list tin

Router# show ipv6 access-list tin

IPv6 access list tin
  permit tcp any any log-input sequence 10
  permit icmp any any echo-request log-input sequence 20
  permit icmp any any echo-reply log-input sequence 30

```

## Configuration Examples for Security for IPv6

This section provides the following configuration example:

- [Create and Apply IPv6 ACL: Examples, page 25](#)
- [Controlling Access to a vty: Example, page 26](#)
- [Configuring Cisco IOS Firewall for IPv6: Example, page 26](#)

## Create and Apply IPv6 ACL: Examples

### Create and Apply an IPv6 ACL Example for Release 12.2(13)T or 12.0(23)S

The following example is from a router running Cisco IOS Release 12.2(13)T.

The example configures two IPv6 ACLs named OUTBOUND and INBOUND and applies both ACLs to outbound and inbound traffic on Ethernet interface 0. The first and second permit entries in the OUTBOUND list permit all TCP and User Datagram Protocol (UDP) packets from network 2001:0DB8:0300:0201::/32 to exit out of Ethernet interface 0. The entries also configure the temporary IPv6 reflexive ACL named REFLECTOUT to filter returning (incoming) TCP and UDP packets on Ethernet interface 0. The first deny entry in the OUTBOUND list keeps all packets from the network fec0:0:0:0201::/64 (packets that have the site-local prefix fec0:0:0:0201 as the first 64 bits of their source IPv6 address) from exiting out of Ethernet interface 0.

The **evaluate** command in the INBOUND list applies the temporary IPv6 reflexive ACL named REFLECTOUT to inbound TCP and UDP packets on Ethernet interface 0. When outgoing TCP or UDP packets are permitted on Ethernet interface 0 by the OUTBOUND list, the INBOUND list uses the REFLECTOUT list to match (evaluate) the returning (incoming) TCP and UDP packets.

```
ipv6 access-list OUTBOUND
 permit tcp 2001:0DB8:0300:0201::/32 any reflect REFLECTOUT
 permit udp 2001:0DB8:0300:0201::/32 any reflect REFLECTOUT
 deny fec0:0:0:0201::/64 any

ipv6 access-list INBOUND
 evaluate REFLECTOUT

interface ethernet 0
 ipv6 traffic-filter OUTBOUND out
 ipv6 traffic-filter INBOUND in
```



#### Note

Given that a **permit any any** statement is not included as the last entry in the OUTBOUND or INBOUND ACL, only TCP and UDP packets matching the configured permit entries in the ACL and ICMP packets matching the implicit permit conditions in the ACL are permitted out of and in to Ethernet interface 0 (the implicit deny all condition at the end of the ACL denies all other packet types on the interface).

The following example can be run on a router running Cisco IOS Release 12.2(13)T or 12.0(23)S.

The example configures HTTP access to be restricted to certain hours during the day, and to log any activity outside of the permitted hours.

```
time-range lunchtime
 periodic weekdays 12:00 to 13:00

ipv6 access-list OUTBOUND
 permit tcp any any eq www time-range lunchtime
 deny tcp any any eq www log-input
 permit tcp 2001:0DB8::/32 any
 permit udp 2001:0DB8::/32 any
```

### Create and Apply an IPv6 ACL Example for Previous Releases

The following example is from a router running Cisco IOS Release 12.2(11)T or earlier releases, 12.0(21)ST, or 12.0(22)S.

The example configures the IPv6 ACL named list2 and applies the ACL to outbound traffic on Ethernet interface 0. Specifically, the first ACL entry keeps all packets from the network fec0:0:0:2::/64 (packets that have the site-local prefix fec0:0:0:2 as the first 64 bits of their source IPv6 address) from exiting out

of Ethernet interface 0. The second entry in the ACL permits all other traffic to exit out of Ethernet interface 0. The second entry is necessary because an implicit deny all condition is at the end of each IPv6 ACL.

```
ipv6 access-list list2 deny fec0:0:0:2::/64 any
ipv6 access-list list2 permit any any
```

```
interface ethernet 0
  ipv6 traffic-filter list2 out
```

If the same configuration was used on a router running Cisco IOS Release 12.2(13)T, 12.0(23)S, or later releases, the configuration would be translated into IPv6 access list configuration mode as follows:

```
ipv6 access-list list2
  deny ipv6 fec0:0:0:2::/64 any
  permit ipv6 any any
```

```
interface ethernet 0
  ipv6 traffic-filter list2 out
```


**Note**


---

IPv6 is automatically configured as the protocol type in **permit any any** and **deny any any** statements that are translated from global configuration mode to IPv6 access list configuration mode.

---

## Controlling Access to a vty: Example

In the following example, incoming connections to the virtual terminal lines 0 to 4 are filtered based on the IPv6 access list named cisco.

```
ipv6 access-list cisco
  permit ipv6 host 2001:0DB8:0:4::2/32 any
!
line vty 0 4
  ipv6 access-class cisco in
```

## Configuring Cisco IOS Firewall for IPv6: Example

This Cisco IOS Firewall configuration example uses inbound and outbound filters for inspection and makes use of access lists to manage the traffic. The inspect mechanism is the method of permitting return traffic based upon a packet being valid for an existing session for which the state is being maintained.

```
enable
configure terminal
  ipv6 unicast-routing
  ipv6 inspect name ipv6_test icmp timeout 60
  ipv6 inspect name ipv6_test tcp timeout 60
  ipv6 inspect name ipv6_test udp timeout 60

interface FastEthernet0/0
  ipv6 address 3FFE:C000:0:7::/64 eui-64
  ipv6 enable
  ipv6 traffic-filter INBOUND out
  ipv6 inspect ipv6_test in

interface FastEthernet0/1
  ipv6 address 3FFE:C000:1:7::/64 eui-64
  ipv6 enable
  ipv6 traffic-filter OUTBOUND in
```

```
! This is used for 3745b connection to tftpboot server
interface FastEthernet4/0
  ip address 192.168.17.33 255.255.255.0
  duplex auto
  speed 100

ip default-gateway 192.168.17.8
! end of tftpboot server config

! Access-lists to deny everything except for Neighbor Discovery ICMP messages
ipv6 access-list INBOUND
  permit icmp any any nd-na
  permit icmp any any nd-ns
  deny ipv6 any any log

ipv6 access-list OUTBOUND
  permit icmp any any nd-na
  permit icmp any any nd-ns
  deny ipv6 any any log
```

## Additional References

For additional information related to implementing security for IPv6, see the following sections:

- [Related Documents, page 28](#)
- [Standards, page 28](#)
- [MIBs, page 28](#)
- [RFCs, page 28](#)
- [Technical Assistance, page 29](#)

## Related Documents

Related Topic	Document Title
Security configuration tasks	<i>Cisco IOS Security Configuration Guide</i> , Release 12.3
Security commands: complete command syntax, command mode, defaults, usage guidelines, and examples	<i>Cisco IOS Security Command Reference</i> , Release 12.3
OSPF for IPv6 authentication support with IPSec	<i>Implementing OSPF for IPv6</i> , Release 12.3
IPv6 supported feature list	<i>Start Here: Cisco IOS Software Release Specifics for IPv6 Features</i>
IPv6 commands: complete command syntax, command mode, defaults, usage guidelines, and examples	<i>IPv6 for Cisco IOS Command Reference</i>
IPv4 configuration and command reference information	<i>Cisco IOS Release 12.3 Configuration Guides and Command References</i>

## 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
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## RFCs

RFCs	Title
RFC 2428	<i>FTP Extensions for IPv6 and NATs</i>

## Technical Assistance

Description	Link
<p>Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, tools, and lots more. Registered Cisco.com users can log in from this page to access even more content.</p>	<p><a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a></p>

