



Creating an IP Access List to Filter TCP Flags

This module documents the ACL TCP Flags Filtering feature and describes how to use an IP access list to filter IP packets that contain TCP flags. The ACL TCP Flags Filtering feature allows you to select any combination of flags on which to filter. The ability to match on a flag set and on a flag not set gives you a greater degree of control for filtering on TCP flags, thus enhancing security.

The ACL TCP Flags Filtering feature provides a flexible mechanism for filtering on TCP flags. Before this feature, an incoming packet was matched if any TCP flag in the packet matched a flag specified in the access control entry (ACE). This behavior allowed for a security loophole, because packets with all flags set could get past the access control list (ACL).

- [Finding Feature Information, page 1](#)
- [Prerequisites for Creating an IP Access List to Filter TCP Flags, page 1](#)
- [Information About Creating an IP Access List to Filter TCP Flags, page 2](#)
- [How to Create an IP Access List to Filter TCP Flags, page 3](#)
- [Configuration Examples for Configuring an IP Access List to Filter TCP Flags, page 5](#)
- [Additional References for Creating an IP Access List to Filter TCP Flags, page 6](#)
- [Feature Information for Creating an IP Access List to Filter TCP Flags, page 7](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and 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 module.

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.

Prerequisites for Creating an IP Access List to Filter TCP Flags

Before you perform any of the tasks in this module, you should be familiar with the information in the following modules:

- “IP Access List Overview”
- “Creating an IP Access List and Applying It to an Interface”

Information About Creating an IP Access List to Filter TCP Flags

Benefits of Filtering on TCP Flags

The ACL TCP Flags Filtering feature provides a flexible mechanism for filtering on TCP flags. Previously, an incoming packet was matched as long as any TCP flag in the packet matched a flag specified in the access control entry (ACE). This behavior allows for a security loophole, because packets with all flags set could get past the access control list (ACL). The ACL TCP Flags Filtering feature allows you to select any combination of flags on which to filter. The ability to match on a flag set and on a flag not set gives you a greater degree of control for filtering on TCP flags, thus enhancing security.

Because TCP packets can be sent as false synchronization packets that can be accepted by a listening port, it is recommended that administrators of firewall devices set up some filtering rules to drop false TCP packets.

The ACEs that make up an access list can be configured to detect and drop unauthorized TCP packets by allowing only the packets that have a very specific group of TCP flags set or not set. The ACL TCP Flags Filtering feature provides a greater degree of packet-filtering control in the following ways:

- You can select any desired combination of TCP flags on which to filter TCP packets.
- You can configure ACEs to allow matching on a flag that is set, as well as on a flag that is not set.

TCP Flags

The table below lists the TCP flags, which are further described in RFC 793, *Transmission Control Protocol*.

Table 1: TCP Flags

TCP Flag	Purpose
ACK	Acknowledge flag—Indicates that the acknowledgment field of a segment specifies the next sequence number the sender of this segment is expecting to receive.
FIN	Finish flag—Used to clear connections.
PSH	Push flag—Indicates the data in the call should be immediately pushed through to the receiving user.
RST	Reset flag—Indicates that the receiver should delete the connection without further interaction.
SYN	Synchronize flag—Used to establish connections.

TCP Flag	Purpose
URG	Urgent flag—Indicates that the urgent field is meaningful and must be added to the segment sequence number.

How to Create an IP Access List to Filter TCP Flags

Filtering Packets That Contain TCP Flags

This task configures an access list to filter packets that contain TCP flags and verifies that the access list has been configured correctly.

**Note**

- TCP flag filtering can be used only with named, extended ACLs.
- The ACL TCP Flags Filtering feature is supported only for Cisco ACLs.
- Previously, the following command-line interface (CLI) format could be used to configure a TCP flag-checking mechanism:

permit tcp any any rst The following format that represents the same ACE can now be used: **permit tcp any any match-any +rst** Both the CLI formats are accepted; however, if the new keywords **match-all** or **match-any** are chosen, they must be followed by the new flags that are prefixed with “+” or “-”. It is advisable to use only the old format or the new format in a single ACL. You cannot mix and match the old and new CLI formats.

**Caution**

If a device having ACEs with the new syntax format is reloaded with a previous version of the Cisco software that does not support the ACL TCP Flags Filtering feature, the ACEs will not be applied, leading to possible security loopholes.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip access-list extended** *access-list-name*
4. [*sequence-number*] **permit tcp** *source source-wildcard* [*operator* [*port*]] *destination destination-wildcard* [*operator* [*port*]] [**established**]{**match-any** | **match-all**} {+ | -} *flag-name* [**precedence** *precedence*] [**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**]
5. [*sequence-number*] **deny tcp** *source source-wildcard* [*operator* [*port*]] *destination destination-wildcard* [*operator* [*port*]] [**established**]{**match-any** | **match-all**} {+ | -} *flag-name* [**precedence** *precedence*] [**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**]
6. Repeat Step 4 or Step 5 as necessary, adding statements by sequence number where you planned. Use the **no** *sequence-number* command to delete an entry.
7. **end**
8. **show ip access-lists** *access-list-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	ip access-list extended <i>access-list-name</i> Example: Device(config)# ip access-list extended kmd1	Specifies the IP access list by name and enters named access list configuration mode.
Step 4	[<i>sequence-number</i>] permit tcp <i>source source-wildcard</i> [<i>operator</i> [<i>port</i>]] <i>destination destination-wildcard</i> [<i>operator</i> [<i>port</i>]] [established]{ match-any match-all } {+ -} <i>flag-name</i> [precedence <i>precedence</i>] [tos <i>tos</i>] [log] [time-range <i>time-range-name</i>] [fragments] Example: Device(config-ext-nacl)# permit tcp any any match-any +rst	Specifies a permit statement in named IP access list mode. <ul style="list-style-type: none"> • This access list happens to use a permit statement first, but a deny statement could appear first, depending on the order of statements you need. • Use the TCP command syntax of the permit command. • Any packet with the RST TCP header flag set will be matched and allowed to pass the named access list kmd1 in Step 3.

	Command or Action	Purpose
Step 5	<p>[<i>sequence-number</i>] deny tcp <i>source source-wildcard</i> [<i>operator</i> [<i>port</i>]] <i>destination destination-wildcard</i> [<i>operator</i> [<i>port</i>]] [established {match-any match-all} {+ -} <i>flag-name</i>] [precedence <i>precedence</i>] [tos <i>tos</i>] [log] [time-range <i>time-range-name</i>] [fragments]</p> <p>Example:</p> <pre>Device(config-ext-nacl)# deny tcp any any match-all -ack -fin</pre>	<p>(Optional) Specifies a deny statement in named IP access list mode.</p> <ul style="list-style-type: none"> • This access list happens to use a permit statement first, but a deny statement could appear first, depending on the order of statements you need. • Use the TCP command syntax of the deny command. • Any packet that does not have the ACK flag set, and also does not have the FIN flag set, will not be allowed to pass the named access list <i>kmdl</i> in Step 3. • See the deny(IP) command for additional command syntax to permit upper-layer protocols (ICMP, IGMP, TCP, and UDP).
Step 6	Repeat Step 4 or Step 5 as necessary, adding statements by sequence number where you planned. Use the no <i>sequence-number</i> command to delete an entry.	Allows you to revise the access list.
Step 7	<p>end</p> <p>Example:</p> <pre>Device(config-ext-nacl)# end</pre>	(Optional) Exits the configuration mode and returns to privileged EXEC mode.
Step 8	<p>show ip access-lists <i>access-list-name</i></p> <p>Example:</p> <pre>Device# show ip access-lists kmdl</pre>	<p>(Optional) Displays the contents of the IP access list.</p> <ul style="list-style-type: none"> • Review the output to confirm that the access list includes the new entry.

Configuration Examples for Configuring an IP Access List to Filter TCP Flags

Example: Filtering Packets That Contain TCP Flags

The following access list allows TCP packets only if the TCP flags ACK and SYN are set and the FIN flag is not set:

```
ip access-list extended aaa
 permit tcp any any match-all +ack +syn -fin
end
```

The **show access-list** command has been entered to display the ACL:

```
Device# show access-list aaa
Extended IP access list aaa
 10 permit tcp any any match-all +ack +syn -fin
```

Additional References for Creating an IP Access List to Filter TCP Flags

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Security Commands	<ul style="list-style-type: none"> • Cisco IOS Security Command Reference: Commands A to C • Cisco IOS Security Command Reference: Commands D to L • Cisco IOS Security Command Reference: Commands M to R • Cisco IOS Security Command Reference: Commands S to Z
Order of access list entries	"Refining an IP Access List"
Access list entries based on time of day or week	"Refining an IP Access List"
Packets with noninitial fragments	"Refining an IP Access List"
Filtering on IP Options, TCP flags, noncontiguous ports, or TTL values	"Creating an IP Access List to Filter IP Options, TCP Flags, Noncontiguous Ports, or TTL Values"
Access to virtual terminal lines	"Controlling Access to a Virtual Terminal Line"
Routing updates and policy routing	"Configuring Routing Protocol-Independent Features" modules in the <i>Cisco IOS IP Routing Protocols Configuration Guide</i>
Traffic identification or classification for features such as congestion avoidance, congestion management, and priority queuing	"Regulating Packet Flow on a Per-Interface Basis--Using Generic Traffic Shaping" module in the <i>Quality of Service Solutions Configuration Guide</i>

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 Creating an IP Access List to Filter TCP Flags

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 Creating an IP Access List to Filter TCP Flags

Feature Name	Releases	Feature Configuration Information
ACL TCP Flags Filtering	12.2(25)S 12.3(4)T	This feature provides a flexible mechanism for filtering on TCP flags. Before Cisco IOS Release 12.3(4)T, an incoming packet was matched if any TCP flag in the packet matched a flag specified in the access control entry (ACE). This behavior allowed for a security loophole, because packets with all flags set could get past the access control list (ACL). The ACL TCP Flags Filtering feature allows you to select any combination of flags on which to filter. The ability to match on a flag set and on a flag not set gives you a greater degree of control for filtering on TCP flags, thus enhancing security.

