Cisco IOS Firewall MIB

Last Updated: March 26, 2012

The Cisco IOS Firewall MIB feature introduces support for the Cisco Unified Firewall MIB, which helps to manage and monitor firewall performance via Simple Network Management Protocol (SNMP). Statistics can be collected and monitored via standards-based SNMP techniques for firewall features such as stateful packet inspection and URL filtering.

- Finding Feature Information, page 1
- Prerequisites Cisco IOS Firewall MIB, page 1
- Restrictions for Cisco IOS Firewall MIB, page 2
- Information About Cisco IOS Firewall MIB, page 2
- How to Configure Cisco IOS Firewall MIB, page 7
- Configuration Examples for Cisco IOS Firewall MIB Monitoring, page 10
- Additional References, page 16
- Feature Information for Cisco IOS Firewall MIB, page 17

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.

Prerequisites Cisco IOS Firewall MIB

Before you can provide firewall connection and URL filtering statistics via SNMP, you must set up the firewall by performing the following tasks:

- Configure a firewall policy via the **ip inspect name** command.
- Enable the firewall by applying the firewall on a target via the **interface** command followed by the **ip inspect** command.

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

- Enable URL filtering, if applicable, via the **ip urlfilter server vendor** command.

You must also enable SNMP on the router. For more information on enabling SNMP, see the section "Enabling SNMP for Firewall Sessions" later in this document.

Restrictions for Cisco IOS Firewall MIB

- Cisco does not support all of the MIB variables that are defined in the Cisco Unified Firewall MIB. For a list of variables that are supported by this feature, see the table below.
- MIB statistics are not provided when the firewall is configured using CPL.

Memory and Performance Impact

Depending on the number of targets that have a configured firewall and the number of configured URL filtering servers, the MIB functionality can create an adverse impact on memory. For each firewall policy that is configured on your system, more memory is required to store SNMP statistics.

The following information defines the minimum memory requirements for connection statistics only:

- Global connection statistics: approximately 64 bytes.
- Protocol-specific statistics: multiply the number of configured protocols by 56 to determine the minimum memory requirement.
- Policy-target-protocol statistics: multiply the number of configured protocols and the number of targets for which the firewall policies are configured by 48 to determine the minimum memory requirement.

The following information defines the minimum memory requirements for URL filtering statistics only:

- Global URL filtering statistics: approximately 96 bytes.
- URL filtering server-specific statistics: multiply the number of configured URL filtering servers by 40 to determine the minimum memory requirement.

Information About Cisco IOS Firewall MIB

- Connection Statistics, page 2
- URL Filtering Statistics, page 4
- Firewall MIB Traps, page 6

Connection Statistics

Connection statistics are a record of the firewall traffic streams that have attempted to flow through the firewall system. Connection statistics can be displayed on a global basis (that is, an aggregate of all connection statistics for the entire router), protocol-specific basis, or a firewall-policy-specific basis. The Firewall can allow, drop, or deny the connection based on firewall policies and firewall resources.

The table below lists all supported connection statistics--global, protocol-specific[1], or firewall-policy-specific[2]--that are available via SNMP.

1 All protocol-based statistics can be accessed with the following index--protocol, which is the protocol of interest such as ICMP, UDP, TCP, HTTP, and FTP. The protocols, which are a predefined static list, must be specified

Table 1 Connection Statistics

Statistic Type	Connection Type	Description
• Global • Protocol-specific • Firewall-policy-specific	Aborted	Number of connections that were abnormally terminated after successful establishment
• Global • Protocol-specific • Firewall-policy-specific	Active	Number of connections that are currently active
• Global • Protocol-specific • Firewall-policy-specific	Attempted	Number of connection attempts sent to the firewall system
Global	Embryonic	Number of embryonic-application-layer connections
Global	Expired	Number of connections that were active but have since been terminated normally
• Global • Protocol-specific	Five-Minute Connection Rate	Number of connection attempts that were established per second, averaged over the last 300 seconds
• Global • Protocol-specific • Firewall-policy-specific	Half-Open	Number of connections that are currently in the process of being established (half-open)
• Global • Protocol-specific	One-Minute Connection Rate	Number of connection attempts that were establish per second, averaged over the last 60 seconds
• Global • Protocol-specific • Firewall-policy-specific	Policy Declined	Number of connection attempts that were declined due to application of a firewall security policy
• Global • Protocol-specific • Firewall-policy-specific	Resource Declined	Number of connection attempts that were declined due to firewall resource constraints

2 All firewall-policy-specific statistics can be accessed with the following indexes: Policy, which is the name of the firewall security policy of interest. (The policy name is specified via the ip inspect name command.) Policy target type, which is the type of physical or virtual target that has the policy name applied to it. Currently, only include interface targets are supported.

URL Filtering Statistics

URL Filtering feature provides an Internet management application that allows you to control web traffic for a given host or user on the basis of a specified security policy. URL filtering statistics include the status of distinct URL filtering servers that are configured on the firewall and the impact of the performance of the URL filtering servers on the latency and throughput of the firewall.

The tables below list all supported URL filtering statistics--on a global basis or per server--that are available via SNMP.

Table 2 Global URL Filtering Statistics (across all servers)

Connection Type	Description
Five minute URL Filtering Requests Declined Rate	Rate at which URL access requests were declined by the firewall via the URL filtering server or the firewall exclusive domain configuration, averaged over the last 300 seconds.
Five minute URL Filtering Requests Resource Dropped Rate	Rate at which URL access requests were dropped by the firewall due to firewall resource constraints, averaged over the last 300 seconds.
One minute URL Filtering Requests Declined Rate	Rate at which URL access requests were declined by the firewall via the URL filtering server or the firewall exclusive domain configuration, averaged over the last 60 seconds.
One minute URL Filtering Requests Resource Dropped Rate	Rate at which URL access requests were dropped by the firewall due to firewall resource constraints, averaged over the last 60 seconds.
URL Filtering Allow Mode On	Displays whether the firewall has allowed or discarded URL requests when the URL filtering server is not available. Returns a “true” statistics if the firewall allows all requested URLs to be retrieved from the remote host when the URL server is not available; returns a “false” statistic of the firewall discards all URL.
URL Filtering Allow Mode Requests Allowed	Number of URL access requests that were allowed by the firewall when the URL filtering server was not available.
URL Filtering Allow Mode Requests Denied	Number of URL access requests that were denied by the firewall when the URL filtering server was not available.
URL Filtering Enabled	Displays whether or not URL filtering is enabled. Returns a “false” statistic if the firewall will not perform URL filtering, even if the system contains configuration information that pertains to other aspects of URL filtering.

Connection Type	Description
URL Filtering Late Responses	Number of responses from the URL filtering server that were received after the original URL access request was dropped by the Firewall.
URL Filtering Requests Allowed	Number of URL access requests allowed by the firewall via the use of the URL filtering server or the firewall exclusive domain configuration.
URL Filtering Requests Declined	Number of URL access requests that were declined by the firewall via the URL filtering server or the firewall exclusive domain configuration.
URL Filtering Requests Processed	Number of URL access requests that were processed by the firewall.
URL Filtering Request Process Rate	Number of URL access requests that were processed per second by the firewall, averaged over the last 300 seconds.
URL Filtering Requests Resource Dropped	Number of incoming URL access requests that were dropped by the Firewall due to firewall resource constraints.
URL Filtering Responses Resource Dropped	Number of responses to URL access requests from remote hosts that were dropped by the firewall due to resource constraints while the firewall was waiting for a response from the URL filtering server.
URL Filtering Server Timeouts	Number of times the firewall did not receive a response from the URL Filtering server.

Table 3 Per server URL Filtering Statistics

Connection Type	Description
URL Filtering Protocol Version	Version of the transport protocol that is used by the firewall to communicate with the URL filtering server. For TCP, valid version values are 1 and 4. For UDP, 1 is the only valid version.
URL Filtering Server Late Responses	Number of URL access responses received by the firewall from the URL filtering server after the original URL access request was dropped by the firewall.
URL Filtering Server Requests	Number of URL access requests forwarded by the firewall to the URL filtering server.

Connection Type	Description
URL Filtering Server Requests Allowed	Number of URL access requests allowed by the URL filtering server. The count does not include late responses.
URL Filtering Server Requests Declined	Number of URL access requests declined by the URL filtering server. The count does not include late responses.
URL Filtering Server Responses	Number of URL access responses received by the firewall from the URL filtering server. The count does not include late responses.
URL Filtering Server Response Time Rate	Average round-trip response time of the URL filtering server, averaged over the last 300 seconds. A value of zero indicates that there was insufficient data to compute this value over the last time interval.
URL Filtering Server Status	Status of the URL filtering server: ONLINE or OFFLINE.
URL Filtering Server Timeouts	Number of times the URL filtering server failed to respond to URL access requests sent by the firewall.
URL Filtering Server Transport Protocol	Transport protocol that is used by the firewall to communicate with the URL filtering server. The protocol will be TCP, UDP, or DEFAULT. DEFAULT is used in implementations that do not explicitly specify a transport protocol.
URL Filtering Server Vendor	Vendor who provided the URL filtering server. Currently only Websense and N2H2 servers are supported.

A URL filtering server is identified by the following items, which also form the indexes into the URL filtering server statistics table:

- URL Filtering Server Address Type--Type of IP address of the URL filtering server. For example, IPv4 or IPv6.
- URL Filtering Server Address--IP address of the URL filtering server.
- URL Filtering Server Port--Port number that the URL filtering server uses to receive filtering requests.

Firewall MIB Traps

To receive firewall MIB traps, you need a management station, and you must enable the **snmp-server enable trap firewall serverstatuschange** command (as shown in the configuration task table below).

Output for the SNMP trap fields, which are displated in on the management station, are as follows:

- Server IP Address Type (IPv4 or IPv6)
- Server IP Address Type Length. (4 for IPv4 and 16 for IPv6)

- Server IP Address
- Server Port

Note Only IPv4 is currently supported.

How to Configure Cisco IOS Firewall MIB

- Enabling SNMP for Firewall Sessions, page 7
- Verifying Firewall Connection and URL Filtering Statistics, page 8

Enabling SNMP for Firewall Sessions

Perform this task to enable SNMP for firewall-related session management.

Before you can begin monitoring firewall performance via SNMP, you must set up the firewall by performing the following tasks:

- Configure a firewall policy via the **ip inspect name** command.

Note Statistics are collected only for protocols that are specified via the **ip inspect name** command.

- Enable the firewall by applying the firewall on a target via the **interface** command followed by the **ip inspect** command.
- Enable URL filtering, if applicable, via the **ip urlfilter server vendor** command.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server community** *string*
4. **snmp-server host** *hostname community-string*
5. **snmp-server enable traps firewall** [**serverstatuschange**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**snmp-server community** *string* **Example:** `Router(config)# snmp-server community public`	Sets up the community access string to permit access to the SNMP.
Step 4	**snmp-server host** *hostname community-string* **Example:** `Router(config)# snmp-server host 192.168.1.1 version 2c public`	Specifies the recipient of the firewall-related SNMP notifications.
Step 5	**snmp-server enable traps firewall** [**serverstatuschange** **Example:** `Router(config)#  snmp-server enable traps firewall serverstatuschange`	Enables firewall-related SNMP notifications.

- What to Do Next, page 8

What to Do Next

After the firewall and SNMP have been properly enabled, statistics will begin to accumulate after the traffic flow starts. To verify whether statistics are being collected and view MIB counters, you can perform at least one of the steps in the task “Verifying Firewall Connection and URL Filtering Statistics.”

Verifying Firewall Connection and URL Filtering Statistics

Use this task to verify firewall connection and URL filtering statistics via command-line interface (CLI). (These statistics can also be collected via any SNMP-capable client.)

Note Effective with Cisco IOS Release 12.4(20)T, the **debug ip inspect** command is replaced by the **debug policy-firewall** command. See the Cisco IOS Debug Command Reference for more information.

SUMMARY STEPS

1. **enable**
2. show ip inspect mib connection-statistics {global | l4-protocol {all | icmp | tcp | udp} | l7-protocol {all | other | telnet | ftp} | policy policy-name target target name {l4-protocol {all | icmp | tcp | udp} | l7-protocol {all | other | telnet | ftp}}
3. show ip urlfilter [mib] statistics [{global | server {ip-address [port] | all}}]
4. debug ip inspect mib {object-creation | object-deletion | events | retrieval | update}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	show ip inspect mib connection-statistics {global | l4-protocol {all | icmp | tcp | udp} | l7-protocol {all | other | telnet | ftp} | policy policy-name target target name {l4-protocol {all | icmp | tcp | udp} | l7-protocol {all | other | telnet | ftp}} **Example:** `Router# show ip inspect mib connection-statistics global`	Displays firewall performance summary statistics that are monitored via SNMP. • **global** --Provides global connection statistics. • **l4-protocol** --Provides Layer 4 statistics for a specified protocol. • **l7-protocol** --Provides Layer 7 statistics for a specified protocol. • **policy** *policy-name* **target** *target-name* --Provides statistics on a per-policy target basis. For example, per firewall policy name and the interface on which the firewall is configured.
Step 3	show ip urlfilter [mib] statistics [{global | server {ip-address [port] | all}}] **Example:** `Router# show ip urlfilter mib statistics global`	Displays URL filtering statistics for firewall-related MIB events.
Step 4	debug ip inspect mib {object-creation | object-deletion | events | retrieval | update} **Example:** `Router# debug ip inspect mib events`	Displays messages about firewall MIB events.

• Troubleshooting Tips, page 10

Troubleshooting Tips

All statistics are accumulated since the last reboot of the firewall system. Thus, you must reboot the system to clear MIB connection statistics from your system.

Configuration Examples for Cisco IOS Firewall MIB Monitoring

- Example Sample Cisco IOS Firewall Configuration, page 10
- Example Sample URL Filtering Configuration, page 12
- Example show ip inspect mib Output, page 14
- Example show ip urlfilter mib statistics command output, page 15

Example Sample Cisco IOS Firewall Configuration

The following output from the **show running-config** command shows how to configure a Cisco IOS Firewall:

```
Router# show running-config
Building configuration...
Current configuration : 2205 bytes
!
version 12.4
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service internal
!
hostname Router
!
boot-start-marker
boot-end-marker
!
no logging console
!
no aaa new-model
!
resource policy
!
clock timezone MST -8
clock summer-time MDT recurring
no ip cef
!
!
!
!
ip inspect name test tcp
ip inspect name test udp
ip inspect name test icmp timeout 30
ip inspect name test ftp
ip inspect name test http
!
!
!
!
!
!
!
```

```
!
!
!
!
!
!
!
!
!
!
policy-map ratelimit
class class-default
police cir 10000000
conform-action transmit
exceed-action drop
!
!
!
!
!
!
!
interface FastEthernet0/0
ip address 192.168.27.2 255.255.255.0
ip access-group 101 out
ip inspect test in
duplex full
service-policy input ratelimit
!
interface FastEthernet1/0
no ip address
no ip route-cache
shutdown
duplex half
!
interface FastEthernet4/0
ip address 192.168.127.2 255.255.255.0
ip access-group 102 in
duplex full
service-policy input ratelimit
!
router eigrp 100
network 192.168.27.0
network 192.168.127.0
no auto-summary
no eigrp log-neighbor-changes
no eigrp log-neighbor-warnings
!
ip default-gateway 192.168.27.116
ip route 192.168.100.0 255.255.255.0 192.168.27.1
ip route 192.168.200.0 255.255.255.0 192.168.127.1
no ip http server
no ip http secure-server
!
!
!
logging alarm informational
access-list 101 permit tcp any any fragments
access-list 101 permit udp any any fragments
access-list 101 deny tcp any any
access-list 101 deny udp any any
access-list 101 permit ip any any
access-list 102 permit tcp any any fragments
access-list 102 permit udp any any fragments
access-list 102 permit udp any gt 1024 any eq snmp
access-list 102 deny tcp any any
access-list 102 deny udp any any
access-list 102 permit ip any any
snmp-server community public RO
snmp-server location FW Testbed UUT
snmp-server contact STG/IOS FW Devtest
!
!
```

```
!
!
!
!
control-plane
!
!
!
!
!
!
gatekeeper
shutdown
!
!
line con 0
exec-timeout 0 0
stopbits 1
line aux 0
stopbits 1
line vty 0 4
login
!
exception core-file sisu-devtest/coredump/Router.core
exception dump 192.168.27.116
!
end
```

Example Sample URL Filtering Configuration

The following sample output from the **show running-config** command shows how to configure a Websense server for URL filtering:

```
Router# show running-config


Building configuration...
Current configuration : 2043 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service internal
!
hostname Router
!
boot-start-marker
boot-end-marker
!
no logging console
!
no aaa new-model
!
resource policy
!
clock timezone MST -8
clock summer-time MDT recurring
no ip cef
!
!
ip inspect name test tcp
ip inspect name test udp
ip inspect name test http urlfilter
!
!
ip urlfilter allow-mode on
ip urlfilter exclusive-domain deny www.cnn.com
ip urlfilter exclusive-domain permit www.cpp.com
ip urlfilter server vendor websense 192.168.29.116
!
```

```
!
!
!
!
!
!
!
!
interface FastEthernet0/0
ip address 192.168.29.2 255.255.255.0
ip access-group 101 out
ip inspect test in
speed auto
full-duplex
!
interface FastEthernet0/1
ip address 192.168.129.2 255.255.255.0
ip access-group 102 in
duplex auto
speed auto
!
router eigrp 100
network 192.168.29.0
network 192.168.129.0
no auto-summary
no eigrp log-neighbor-changes
no eigrp log-neighbor-warnings
!
ip default-gateway 192.168.28.116
ip route 192.168.100.0 255.255.255.0 192.168.29.1
ip route 192.168.200.0 255.255.255.0 192.168.129.1
!
!
ip http server
no ip http secure-server
!
access-list 101 permit tcp any any fragments
access-list 101 permit udp any any fragments
access-list 101 deny tcp any any
access-list 101 deny udp any any
access-list 101 permit ip any any
access-list 102 permit tcp any any fragments
access-list 102 permit udp any any fragments
access-list 102 permit udp any gt 1024 any eq snmp
access-list 102 deny tcp any any
access-list 102 deny udp any any
access-list 102 permit ip any any
snmp-server community public RO
snmp-server location FW Testbed UUT
snmp-server contact STG/IOS FW Devtest
!
!
!
!
control-plane
!
!
!
line con 0
exec-timeout 0 0
transport output all
line aux 0
transport output all
line vty 0 4
login
!
exception core-file sisu-devtest/coredump/Router.core
exception dump 192.168.28.116
!
webvpn context Default_context
ssl authenticate verify all
!
no inservice
```

```
!
!
end
```

Example show ip inspect mib Output

The following examples are sample outputs from the **show ip inspect mib**command with global or protocol-specific keywords:

Global MIB Statistics

```
Router# show ip inspect mib connection-statistics global

------------------------------------------------
Connections Attempted 7
Connections Setup Aborted 0
Connections Policy Declined 0
Connections Resource Declined 0
Connections Half Open 2 Connections Active 3
Connections Expired 2
Connections Aborted 0
Connections Embryonic 0
Connections 1-min Setup Rate 5
Connections 5-min Setup Rate 7
```

Protocol-Based MIB Statistics

```
Router# show ip inspect mib connection-statistics l4-protocol tcp


------------------------------------------------
Protocol tcp
Connections Attempted 3
Connections Setup Aborted 0
Connections Policy Declined 0
Connections Resource Declined 0
Connections Half Open 1
Connections Active 2
Connections Aborted 0
Connections 1-min Setup Rate 3
Connections 5-min Setup Rate 3
Router# show ip inspect mib connection-statistics l7-protocol http


------------------------------------------------
Protocol http
Connections Attempted 3
Connections Setup Aborted 0
Connections Policy Declined 2
Connections Resource Declined 0
Connections Half Open 0
Connections Active 1
Connections Aborted 0
Connections 1-min Setup Rate 1
Connections 5-min Setup Rate 2
```

Policy-Target-Based MIB Statistics

```
Router# show ip inspect mib connection-statistics policy ftp interface GigabitEthernet0/0
l4-protocol tcp


! Policy Target Protocol Based Connection Summary Stats
------------------------------------------------------
Policy ftp-inspection
Target GigabitEthernet0/0
```

```
Protocol tcp
Connections Attempted 3
Connections Setup Aborted 0
Connections Policy Declined 0
Connections Resource Declined 0
Connections Half Open 1
Connections Active 2
Connections Aborted 0
Router# show ip inspect mib connection-statistics policy ftp interface GigabitEthernet0/0
l7-protocol ftp


! Policy Target Protocol Based Connection Summary Stats
-----------------------------------------------------
Policy ftp-inspection
Target GigabitEthernet0/0
Protocol ftp
Connections Attempted 3
Connections Setup Aborted 0
Connections Policy Declined 0
Connections Resource Declined 0
Connections Half Open 1
Connections Active 2
Connections Aborted 0
```

Example show ip urlfilter mib statistics command output

The following example is sample output when MIBs are enabled to track URL filtering statistics across the entire device (global):

```
Router# show ip urlfilter mib statistics global

URL Filtering Group Summary Statistics
------------------------------------------------------
URL Filtering Enabled
Requests Processed 260
Requests Processed 1-minute Rate 240
Requests Processed 5-minute Rate 215
Requests Allowed 230
Requests Denied 30
Requests Denied 1-minute Rate 15
Requests Denied 5-minute Rate 0
Requests Cache Allowed 5
Requests Cache Denied 5
Allow Mode Requests Allowed 15
Allow Mode Requests Denied 15
Requests Resource Dropped 0
Requests Resource Dropped 1-minute Rate 0
Requests Resource Dropped 5-minute Rate 0
Server Timeouts 0
Server Retries 0
Late Server Responses 0
Access Responses Resource Dropped 0
```

The following example is sample output when MIBs are enabled to track URL filtering statistics across the server with IP address 192.168.27.116:

```
Router# show ip urlfilter mib statistics server address 192.168.27.116
URL Filtering Server Statistics
------------------------------------------------------
URL Server Host Name 192.168.27.116
Server Address 192.168.27.116
Server Port 15868
Server Vendor Websense
Server Status Online
Requests Processed 4
Requests Allowed 1
Requests Denied 3
Server Timeouts 0
Server Retries 9
```

```
Responses Received 1
Late Server Responses 12
1 Minute Average Response Time 0
5 Minute Average Response Time 0
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Security commands	*Cisco IOS Security Command Reference*
Description of SNMP, SNMP MIBs, and how to configure SNMP on Cisco devices	"Configuring SNMP Support"
Description of Cisco IOS firewalls and functions such as how to configure a firewall and URL filtering	"Configuring Context-based Access Control"

Standards

Standard	Title
None	--

MIBs

MIB	MIBs Link
• CISCO-UNIFIED-FIREWALL-MIB.my • CISCO-FIREWALL-TC.my	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	--

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 Cisco IOS Firewall MIB

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 4 Feature Information for Cisco IOS Firewall MIB

Feature Name	Releases	Feature Information
Cisco IOS Firewall MIB	12.4(6)T	Introduces support for the Cisco Unified Firewall MIB, which helps to manage and monitor firewall performance via SNMP. Statistics can be collected and monitored via standards-based SNMP techniques for firewall features such as stateful packet inspection and URL filtering. The following commands were introduced or modified: **debug ip inspect**, **show ip inspect**, **show ip urlfilter statistics**, **snmp-server enable traps firewall**.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.