



Firewall Support of Skinny Client Control Protocol (SCCP)

The Firewall Support of Skinny Client Control Protocol (SCCP) feature enables Context-Based Access Control (CBAC) inspection to support the Voice over IP (VoIP) protocol, Skinny Client Control Protocol (SCCP). That is, CBAC inspects Skinny control packets that are exchanged between a Skinny client and the Call Manager (CM); CBAC then configures the router (also known as the Cisco IOS Firewall) to enable the Skinny data channels to traverse through the router.

Feature Specifications for the Firewall Support of Skinny Client Control Protocol (SCCP) Feature

Feature History

Release	Modification
12.3(1)	This feature was introduced.

Supported Platforms

For platforms supported in Cisco IOS Release 12.3(1), consult Cisco Feature Navigator.

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 Firewall Support of Skinny Client Control Protocol \(SCCP\)](#), page 2
- [Restrictions for Firewall Support of Skinny Client Control Protocol \(SCCP\)](#), page 2
- [Information About Firewall Support of Skinny Client Control Protocol \(SCCP\)](#), page 2
- [How to Configure Your Firewall for Skinny Support](#), page 4
- [Configuration Examples for Firewall Skinny Support](#), page 9



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

Copyright © 2003 Cisco Systems, Inc. All rights reserved.

- [Additional References, page 10](#)
- [Command Reference, page 11](#)

Prerequisites for Firewall Support of Skinny Client Control Protocol (SCCP)

The Skinny inspection module is part of the inspection subsystem; thus, your router must be running an image that has firewall support.

Restrictions for Firewall Support of Skinny Client Control Protocol (SCCP)

This feature has the following restrictions:

- Skinny inspection will inspect only the SCCP sessions that have been established after the firewall is configured with Skinny inspection. That is, any SCCP sessions that were established through the firewall before the Skinny inspection was configured will not be inspected.
- This feature does not support Music on Hold (MOH) when a device other than the CM is the music server. (This feature does support MOH when the CM is the music server.)
- This feature does not address either the multicast functionality of SCCP or the functionality of multiple active calls on a single Skinny client.

This feature does not support the following Skinny and firewall configurations:

- The firewall and CM cannot be in the same router. Skinny inspection does not support this configuration because the current firewall implementation does not inspect sessions that start or terminate at the router. Thus, Skinny inspection will work only with an external CM.
- The CM and the Skinny client cannot be on three different networks that are separated at the firewall. The current firewall implementation does not inspect sessions that have devices residing on more than two distinct networks that are segregated at the firewall. That is, if there are more than two interfaces at the firewall, session inspection is not supported.

Information About Firewall Support of Skinny Client Control Protocol (SCCP)

To configure the Firewall Support of SCCP feature, you must understand the following concepts:

- [Context-Based Access Control Overview, page 3](#)
- [Skinny Overview, page 3](#)
- [CBAC and Skinny Functionality Overview, page 4](#)

Context-Based Access Control Overview

CBAC extends the concept of static access control lists (ACLs) by introducing dynamic ACL entries that open the necessary application ports on the basis of a specific application and close these ports at the end of the application session. CBAC achieves this functionality by inspecting the application data, checking for conformance of the application protocol, extracting the relevant port information to create the dynamic ACL entries, and closing these ports at the end of the session. CBAC is designed to easily allow a new application inspection whenever support is needed.

Skinny Overview

Skinny enables voice communication between two Skinny clients through the use of a CM. Typically, the CM provides service to the Skinny clients on TCP Port 2000. Initially, a Skinny client connects to the CM by establishing a TCP connection; the client will also establish a TCP connection with a secondary CM, if available. After the TCP connection is established, the client will register with the primary CM, which will be used as the controlling CM until it reboots or there is a keepalive failure. Thus, the Skinny TCP connection between the client and the CM exists forever and is used to establish calls coming to or from the client. If a TCP connection failure is detected, the secondary CM is used. All data channels established with the previous CM remain active and will be closed after the end parties hang up the call.

[Table 1](#) lists the set of messages that are necessary for the data sessions to open and close. Skinny inspection will examine the data sessions that are deemed for opening and closing the access list pin holes.

Table 1 *Skinny Data Session Messages*

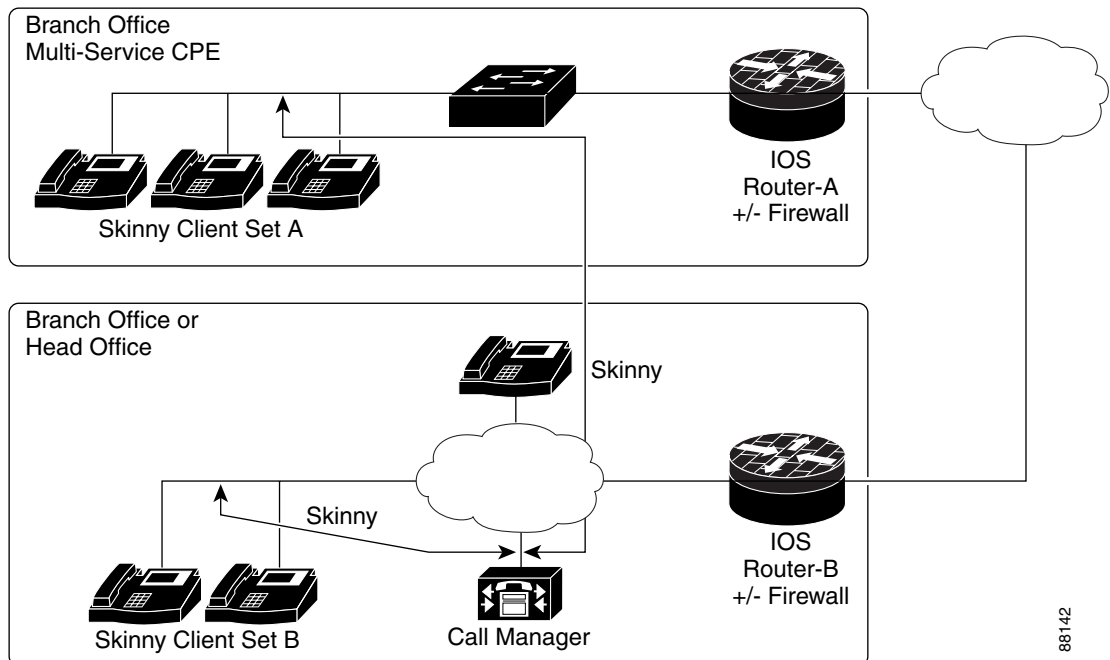
Skinny Inspection Message	Description
StationOpenReceiveChannelAckMessage	Contains the IP address and port information of the Skinny client sending this message. This message also contains the status of whether or not the client is willing to receive the voice traffic.
StationStartMediaTransmissionMessage	Contains the IP address and port information of the remote Skinny client.
StationCloseReceiveChannelMessage	CM instructs the Skinny client (on the basis of the information in this message) to close the receiving channel.
StationStopMediaTransmissionMessage	CM instructs the Skinny client (on the basis of the information in this message) to stop transmitting voice traffic.
StationStopSessionTransmissionMessage	CM instructs the Skinny client (on the basis of the information in this message) to end an indicated session.

CBAC and Skinny Functionality Overview

Figure 1 depicts typical deployment solutions that are supported by CBAC inspection for Skinny. According to Figure 1, a firewall with Skinny inspection can be configured on Cisco IOS Router A, Cisco IOS Router B, or both routers, thereby addressing the following three scenarios:

- A Cisco IOS router with a firewall on the customer premises equipment (CPE) side, supporting Skinny VoIP phone
- A Cisco IOS router with a firewall on the CM side
- A Cisco IOS router with a firewall at both ends of the connection

Figure 1 CBAC Inspection for Skinny Sample Topology



88142

How to Configure Your Firewall for Skinny Support

To configure a Cisco IOS Firewall for SCCP support, perform the following tasks:

- [Configuring Basic Skinny CBAC Inspection, page 5](#)
- [Setting Skinny CBAC Session Timeouts, page 6](#)
- [Configuring Port to Application Mapping, page 6](#)
- [Verifying Cisco IOS Firewall for Skinny Support, page 7](#)
- [Monitoring Cisco IOS Firewall for Skinny Support, page 8](#)

Configuring Basic Skinny CBAC Inspection

Perform the following required steps to configure a basic Skinny CBAC configuration:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip inspect name** *inspection-name protocol* [**alert {on | off}**] [**audit-trail {on | off}**] [**timeout seconds**]
4. **ip inspect name** *inspection-name protocol* [**alert {on | off}**] [**audit-trail {on | off}**] [**timeout seconds**] (Optional. Required if the TFTP server is outside the firewall.)
5. **interface** *type number*
6. **ip access-group** {*access-list-number*} {**in | out**}
7. **ip inspect** *inspection-name* {**in | out**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables higher privilege levels, such as privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip inspect name <i>inspection-name protocol</i> [alert {on off}] [audit-trail {on off}] [timeout seconds] Example: Router(config)# ip inspect name firewall skinny	Enables CBAC Skinny inspections.
Step 4	ip inspect name <i>inspection-name protocol</i> [alert {on off}] [audit-trail {on off}] [timeout seconds] Example: Router(config)# ip inspect name firewall tftp	(Optional. Required if the TFTP server is outside the firewall.) Defines a set of inspection rules.
Step 5	interface <i>type number</i> Example: Router(config)# interface FastEthernet 0/0	Configures an interface type and enters interface configuration mode.

	Command or Action	Purpose
Step 6	<code>ip access-group {access-list-number} {in out}</code> Example: Router(config-if)# ip access-group 100 in	Control access to an interface. Number of the access list that is blocking incoming traffic.
Step 7	<code>ip inspect inspection-name {in out}</code> Example: Router(config-if)# ip inspect firewall out	Applies a set of inspection rules to an interface.

Setting Skinny CBAC Session Timeouts

Session timeouts are triggered when traffic is not seen on a particular session for a configured amount of time. (This value is configured via the **ip inspect name** command.) After the inactivity timeout is triggered, the firewall will clean up the session and deallocate all of the session data.

You must set the inactivity timeout value for Skinny to a greater value than the keepalive timeout value that is configured between the CM and Skinny clients. Otherwise, the Skinny connection may become inaccessible for inspection because the firewall might delete the session-related information due to inactivity.

After the inactivity timeout is triggered, the inspection module will send reset (RST packets) to both ends of the connection. Any data channels that are associated with the control channel will not be closed. After both end parties hang up, there will not be any traffic on the data channels and the connection will eventually timeout.



Note

If the inactivity timeout of the control channel that is connected to the primary CM is less than the keepalive timeout that is sent by the CM to the Skinny client, the firewall will set the inactivity timeout to three times the keepalive timeout. If a timeout is not configured, the default value of 3600 seconds will be used.

Configuring Port to Application Mapping

By default, the Skinny inspection will inspect SCCP messages to or from the CM on TCP port 2000. If you prefer to configure the CM to use a different port, the port to application mapping (PAM) feature should be used to specify the desired port to the Cisco IOS firewall. Thus, the firewall will inspect the SCCP messages in the desired port and in port 2000. To configure the CM to use a different port via PAM, use the **ip port-map** command.

Prerequisites

Before you can configure PAM, you must first configure the steps in the section, “[Configuring Basic Skinny CBAC Inspection](#).”

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip port map** *appl_name* **port** *port_num* [**list** *acl_num*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables higher privilege levels, such as privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip port map <i>appl_name</i> port <i>port_num</i> [list <i>acl_num</i>] Example: Router(config)# ip port map skinny port 2100	(Optional) Creates a port to address mapping for SCCP. This command allows you to indicate additional ports that need to be monitored for SCCP.

Verifying Cisco IOS Firewall for Skinny Support

To display active Skinny session information, perform the following optional steps:

SUMMARY STEPS

1. **enable**
2. **show ip inspect** {**name** *inspection-name* | **config** | **interfaces** | **session** [**detail**] | **all**}
3. **show ip access-list**
4. **show ip port-map** [*appl_name* | **port** *port_num*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables higher privilege levels, such as privileged EXEC mode. • Enter your password if prompted.
Step 2	show ip inspect {name <i>inspection-name</i> config interfaces session [detail] all } Example: Router# show ip inspect session detail	(Optional) Displays existing sessions that are currently being tracked and inspected by CBAC. The optional detail keyword causes additional details about these sessions to be shown.
Step 3	show ip access-list Example: Router# show ip access-list	(Optional) Displays the contents of all current IP access lists, which includes the dynamic access lists created by Skinny inspection.
Step 4	show ip port-map [<i>appl_name</i> port <i>port_num</i>] Example: Router# show ip port-map skinny	(Optional) Displays information about the active port to application mappings on the router. Use this command to view Skinny port map information. • <i>appl_name</i> —Displays Skinny-specific PAM information. (You must specify the <i>skinny</i> argument.)

Monitoring Cisco IOS Firewall for Skinny Support

To monitor debugging messages related to Skinny inspection, perform the following optional steps:

SUMMARY STEPS

1. **enable**
2. **debug ip inspect** {*sccp* | **detailed**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables higher privilege levels, such as privileged EXEC mode. • Enter your password if prompted.
Step 2	debug ip inspect { <i>sccp</i> detailed } Example: Router# debug ip inspect sccp	(Optional) Displays and logs the debugging messages related to SCCP inspection.

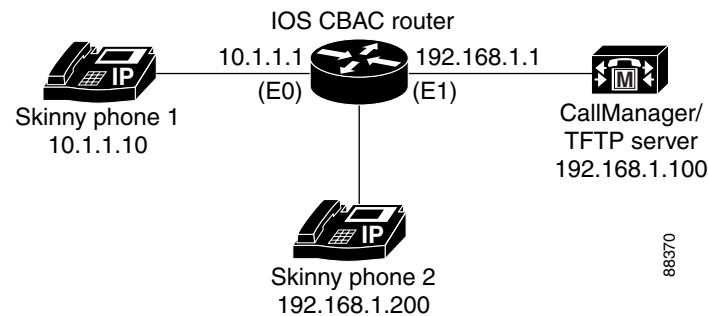
Configuration Examples for Firewall Skinny Support

This section provides the following configuration example:

- [Firewall and Skinny Configuration Example, page 9](#)

Firewall and Skinny Configuration Example

Figure 2 Skinny and CBAC Configuration



The following is an example of how to configure a Cisco IOS firewall for Skinny support and includes PAM (see [Figure 2](#)):

```
! Define the name of the router as "CBAC-Firewall."
!
host CBAC-Firewall
!
! Create a DHCP server process to offer out 10.1.1.x addresses on the
! inside network. Option 150 is used by Cisco IP phones as where to
! look for their configuration file. A default router is required so that all
! the IP phones can talk to networks other than just to the local 10.1.1.x.
!
ip dhcp pool localnetwork
  network 10.1.1.0 255.255.255.0
  option 150 ip 192.168.1.100
  default-router 10.1.1.1
!
! Prevent the DHCP server process from assigning 10.1.1.1 -.9 as an IP
! address on the local network. This is done to hold the addresses .2 - .9 as static-
! defined addresses.
!
ip dhcp excluded-address 10.1.1.1 10.1.1.9
!
! Define firewall rules to all Skinny traffic in/out along with TFTP
! services.
!
ip inspect name fwout tftp
ip inspect name fwout skinny
!
! Prevent any traffic from coming in.
!
access-list 100 deny ip any any
!
interface ethernet 1
  ip access-group 100 in
  ip inspect firewall out
```

If the CallManager is requiring Skinny registration to happen on port tcp/2100, you will still need the above configuration plus the following additional step.

```
ip port map skinny port 2100
```

Additional References

The following sections provide additional references related to the Firewall Support of Skinny Client Control Protocol (SCCP) feature:

- [Related Documents, page 10](#)
- [Standards, page 10](#)
- [MIBs, page 10](#)
- [RFCs, page 11](#)
- [Technical Assistance, page 11](#)

Related Documents

Related Topic	Document Title
Additional CBAC information and configuration tasks	The chapter “Configuring Context-based Access Control” in the <i>Cisco IOS Security Configuration Guide</i> , Release 12.3
CBAC commands	<i>Cisco IOS Security Command Reference</i> , Release 12.3
PAM information and configuration tasks	The chapter “Configuring Port to Application Mapping” in the <i>Cisco IOS Security Configuration Guide</i> , Release 12.3

Standards

Standards	Title
None	—

MIBs

MIBs	MIBs Link
None	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

RFCs ¹	Title
None	—

1. Not all supported RFCs are listed.

Technical Assistance

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

Command Reference

This section documents modified commands. All other commands used with this feature are documented in the Cisco IOS Release 12.3 command reference publications.

- [debug ip inspect](#)
- [ip inspect name](#)
- [ip port-map](#)

debug ip inspect

To display messages about Cisco IOS firewall events, use the **debug ip inspect** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

```
debug ip inspect { function-trace | object-creation | object-deletion | events | timers | protocol | detailed }
```

```
no debug ip inspect detailed
```

Syntax Description

function-trace	Displays messages about software functions called by the Cisco IOS firewall.
object-creation	Displays messages about software objects being created by the Cisco IOS firewall. Object creation corresponds to the beginning of Cisco IOS firewall-inspected sessions.
object-deletion	Displays messages about software objects being deleted by the Cisco IOS firewall. Object deletion corresponds to the closing of Cisco IOS firewall-inspected sessions.
events	Displays messages about Cisco IOS firewall software events, including information about Cisco IOS firewall packet processing.
timers	Displays messages about Cisco IOS firewall timer events such as when the Cisco IOS firewall idle timeout is reached.
<i>protocol</i>	Displays messages about Cisco IOS firewall-inspected protocol events, including details about the packets of the protocol. Table 2 provides a list of <i>protocol</i> keywords.
detailed	Causes detailed information to be displayed for all the other enabled Cisco IOS firewall debugging. Use this form of the command in conjunction with other Cisco IOS firewall debugging commands.

Table 2 Protocol Keywords for the debug ip inspect Command

Application Protocol	Protocol Keyword
Transport-layer protocols	
Internet Control Message Protocol (ICMP)	icmp
TCP	tcp
User Datagram Protocol (UDP)	udp
Application-layer protocols	
CU-SeeMe	cuseeme
FTP commands and responses	ftp-cmd
FTP tokens (enables tracing of the FTP tokens parsed)	ftp-tokens
H.323 (version 1 and version 2)	h323
HTTP	http
Microsoft NetShow	netshow
RealAudio	realaudio

Table 2 Protocol Keywords for the debug ip inspect Command (continued)

Application Protocol	Protocol Keyword
Real Time Streaming Protocol (RTSP)	rtsp
Remote Procedure Call (RPC)	rpc
Session Initiation Protocol (SIP)	sip
Simple Mail Transfer Protocol (SMTP)	smtp
Skiny Client Control Protocol (SCCP)	skinny
StreamWorks	streamworks
Structured Query Language*Net (SQL*Net)	sqlnet
TFTP	tftp
UNIX r-commands (rlogin, rexec, rsh)	rcmd
VDOLive	vdolive

Command Modes Privileged EXEC

Command History	Release	Modification
	11.2 P	This command was introduced.
	12.0(5)T	NetShow support was added.
	12.0(7)T	H.323 V2 and RTSP protocol support was added.
	12.2(11)YU	Support for the ICMP and SIP protocols was added.
	12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
	12.3(1)	Support for the skinny protocol was added.

Examples The following is sample output from the **debug ip inspect function-trace** command:

```
*Mar 2 01:16:16: CBAC FUNC: insp_inspection
*Mar 2 01:16:16: CBAC FUNC: insp_pre_process_sync
*Mar 2 01:16:16: CBAC FUNC: insp_find_tcp_host_entry addr 40.0.0.1 bucket 41
*Mar 2 01:16:16: CBAC FUNC: insp_find_pregen_session
*Mar 2 01:16:16: CBAC FUNC: insp_get_idbsb
*Mar 2 01:16:16: CBAC FUNC: insp_get_idbsb
*Mar 2 01:16:16: CBAC FUNC: insp_get_irc_of_idb
*Mar 2 01:16:16: CBAC FUNC: insp_get_idbsb
*Mar 2 01:16:16: CBAC FUNC: insp_create_sis
*Mar 2 01:16:16: CBAC FUNC: insp_inc_halfopen_sis
*Mar 2 01:16:16: CBAC FUNC: insp_link_session_to_hash_table
*Mar 2 01:16:16: CBAC FUNC: insp_inspect_pak
*Mar 2 01:16:16: CBAC FUNC: insp_l4_inspection
*Mar 2 01:16:16: CBAC FUNC: insp_process_tcp_seg
*Mar 2 01:16:16: CBAC FUNC: insp_listen_state
*Mar 2 01:16:16: CBAC FUNC: insp_ensure_return_traffic
*Mar 2 01:16:16: CBAC FUNC: insp_add_acl_item
*Mar 2 01:16:16: CBAC FUNC: insp_ensure_return_traffic
*Mar 2 01:16:16: CBAC FUNC: insp_add_acl_item
*Mar 2 01:16:16: CBAC FUNC: insp_process_syn_packet
*Mar 2 01:16:16: CBAC FUNC: insp_find_tcp_host_entry addr 40.0.0.1 bucket 41
```

```
*Mar 2 01:16:16: CBAC FUNC: insp_create_tcp_host_entry
*Mar 2 01:16:16: CBAC* FUNC: insp_fast_inspection
*Mar 2 01:16:16: CBAC* FUNC: insp_inspect_pak
*Mar 2 01:16:16: CBAC* FUNC: insp_l4_inspection
*Mar 2 01:16:16: CBAC* FUNC: insp_process_tcp_seg
*Mar 2 01:16:16: CBAC* FUNC: insp_synrcvd_state
*Mar 2 01:16:16: CBAC* FUNC: insp_fast_inspection
*Mar 2 01:16:16: CBAC* FUNC: insp_inspect_pak
*Mar 2 01:16:16: CBAC* FUNC: insp_l4_inspection
*Mar 2 01:16:16: CBAC* FUNC: insp_process_tcp_seg
*Mar 2 01:16:16: CBAC* FUNC: insp_synrcvd_state
*Mar 2 01:16:16: CBAC FUNC: insp_dec_halfopen_sis
*Mar 2 01:16:16: CBAC FUNC: insp_remove_sis_from_host_entry
*Mar 2 01:16:16: CBAC FUNC: insp_find_tcp_host_entry addr 40.0.0.1 bucket 41
```

This output shows the functions called by the Cisco IOS firewall as a session is inspected. Entries with an asterisk (*) after the word “CBAC” are entries when the fast path is used; otherwise, the process path is used.

The following is sample output from the **debug ip inspect object-creation** and **debug ip inspect object-deletion** command:

```
*Mar 2 01:18:30: CBAC OBJ_CREATE: create pre-gen sis 25A3574
*Mar 2 01:18:30: CBAC OBJ_CREATE: create acl wrapper 25A36FC -- acl item 25A3634
*Mar 2 01:18:30: CBAC OBJ_CREATE: create sis 25C1CC4
*Mar 2 01:18:30: CBAC OBJ_DELETE: delete pre-gen sis 25A3574
*Mar 2 01:18:30: CBAC OBJ_CREATE: create host entry 25A3574 addr 10.0.0.1 bucket 31
*Mar 2 01:18:30: CBAC OBJ_DELETE: delete sis 25C1CC4
*Mar 2 01:18:30: CBAC OBJ_DELETE: delete create acl wrapper 25A36FC -- acl item 25A3634
*Mar 2 01:18:31: CBAC OBJ_DELETE: delete host entry 25A3574 addr 10.0.0.1
```

The following is sample output from the **debug ip inspect object-creation**, **debug ip inspect object-deletion**, and **debug ip inspect events** commands:

```
*Mar 2 01:18:51: CBAC OBJ_CREATE: create pre-gen sis 25A3574
*Mar 2 01:18:51: CBAC OBJ_CREATE: create acl wrapper 25A36FC -- acl item 25A3634
*Mar 2 01:18:51: CBAC Src 10.1.0.1 Port [1:65535]
*Mar 2 01:18:51: CBAC Dst 10.0.0.1 Port [46406:46406]
*Mar 2 01:18:51: CBAC Pre-gen sis 25A3574 created: 10.1.0.1[1:65535]
30.0.0.1[46406:46406]
*Mar 2 01:18:51: CBAC OBJ_CREATE: create sis 25C1CC4
*Mar 2 01:18:51: CBAC sis 25C1CC4 initiator_addr (10.1.0.1:20) responder_addr
(30.0.0.1:46406) initiator_alt_addr (40.0.0.1:20) responder_alt_addr (10.0.0.1:46406)
*Mar 2 01:18:51: CBAC OBJ_DELETE: delete pre-gen sis 25A3574
*Mar 2 01:18:51: CBAC OBJ_CREATE: create host entry 25A3574 addr 10.0.0.1 bucket 31
*Mar 2 01:18:51: CBAC OBJ_DELETE: delete sis 25C1CC4
*Mar 2 01:18:51: CBAC OBJ_DELETE: delete create acl wrapper 25A36FC -- acl item 25A3634
*Mar 2 01:18:51: CBAC OBJ_DELETE: delete host entry 25A3574 addr 10.0.0.1
```

The following is sample output from the **debug ip inspect timers** command:

```
*Mar 2 01:19:15: CBAC Timer Init Leaf: Pre-gen sis 25A3574
*Mar 2 01:19:15: CBAC Timer Start: Pre-gen sis 25A3574 Timer: 25A35D8 Time: 30000
milisecs
*Mar 2 01:19:15: CBAC Timer Init Leaf: sis 25C1CC4
*Mar 2 01:19:15: CBAC Timer Stop: Pre-gen sis 25A3574 Timer: 25A35D8
*Mar 2 01:19:15: CBAC Timer Start: sis 25C1CC4 Timer: 25C1D5C Time: 30000 milisecs
*Mar 2 01:19:15: CBAC Timer Start: sis 25C1CC4 Timer: 25C1D5C Time: 3600000 milisecs
*Mar 2 01:19:15: CBAC Timer Start: sis 25C1CC4 Timer: 25C1D5C Time: 5000 milisecs
*Mar 2 01:19:15: CBAC Timer Stop: sis 25C1CC4 Timer: 25C1D5C
```

The following is sample output from the **debug ip inspect tcp** command:

```
*Mar 2 01:20:43: CBAC* sis 25A3604 pak 2541C58 TCP P ack 4223720032 seq 4200176225(22)
(10.0.0.1:46409) => (10.1.0.1:21)
*Mar 2 01:20:43: CBAC* sis 25A3604 ftp L7 inspect result: PROCESS-SWITCH packet
*Mar 2 01:20:43: CBAC sis 25A3604 pak 2541C58 TCP P ack 4223720032 seq 4200176225(22)
(10.0.0.1:46409) => (10.1.0.1:21)
*Mar 2 01:20:43: CBAC sis 25A3604 ftp L7 inspect result: PASS packet
*Mar 2 01:20:43: CBAC* sis 25A3604 pak 2544374 TCP P ack 4200176247 seq 4223720032(30)
(10.0.0.1:46409) <= (10.1.0.1:21)
*Mar 2 01:20:43: CBAC* sis 25A3604 ftp L7 inspect result: PASS packet
*Mar 2 01:20:43: CBAC* sis 25A3604 pak 25412F8 TCP P ack 4223720062 seq 4200176247(15)
(10.0.0.1:46409) => (10.1.0.1:21)
*Mar 2 01:20:43: CBAC* sis 25A3604 ftp L7 inspect result: PASS packet
*Mar 2 01:20:43: CBAC sis 25C1CC4 pak 2544734 TCP S seq 4226992037(0) (10.1.0.1:20) =>
(10.0.0.1:46411)
*Mar 2 01:20:43: CBAC* sis 25C1CC4 pak 2541E38 TCP S ack 4226992038 seq 4203405054(0)
(10.1.0.1:20) <= (10.0.0.1:46411)
```

This sample shows TCP packets being processed and lists the corresponding acknowledge (ACK) packet numbers and sequence (SEQ) numbers. The number of data bytes in the TCP packet is shown in parentheses—for example, (22). For each packet shown, the addresses and port numbers are shown separated by a colon. For example, (10.1.0.1:21) indicates an IP address of 10.1.0.1 and a TCP port number of 21.

Entries with an asterisk (*) after the word “CBAC” are entries when the fast path is used; otherwise, the process path is used.

The following is sample output from the **debug ip inspect tcp** and **debug ip inspect detailed** commands:

```
*Mar 2 01:20:58: CBAC* Pak 2541E38 Find session for (30.0.0.1:46409) (40.0.0.1:21) tcp
*Mar 2 01:20:58: P ack 4223720160 seq 4200176262(22)
*Mar 2 01:20:58: CBAC* Pak 2541E38 Addr:port pairs to match: (30.0.0.1:46409)
(40.0.0.1:21)
*Mar 2 01:20:58: CBAC* sis 25A3604 SIS_OPEN
*Mar 2 01:20:58: CBAC* Pak 2541E38 IP: s=30.0.0.1 (Ethernet0), d=40.0.0.1 (Ethernet1),
len 76,proto=6
*Mar 2 01:20:58: CBAC sis 25A3604 Saving State: SIS_OPEN/ESTAB iisn 4200176160 i_rcvnxt
4223720160 i_sndnxt 4200176262 i_rcvwnd 8760 risn 4223719771 r_rcvnxt 4200176262 r_sndnxt
4223720160 r_rcvwnd 8760
*Mar 2 01:20:58: CBAC* sis 25A3604 pak 2541E38 TCP P ack 4223720160 seq 4200176262(22)
(30.0.0.1:46409) => (40.0.0.1:21)
*Mar 2 01:20:58: CBAC* sis 25A3604 pak 2541E38 SIS_OPEN/ESTAB TCP seq 4200176262(22)
Flags: ACK 4223720160 PSH
*Mar 2 01:20:58: CBAC* sis 25A3604 pak 2541E38 --> SIS_OPEN/ESTAB iisn 4200176160
i_rcvnxt 4223720160 i_sndnxt 4200176284 i_rcvwnd 8760 risn 4223719771 r_rcvnxt 4200176262
r_sndnxt 4223720160 r_rcvwnd 8760
*Mar 2 01:20:58: CBAC* sis 25A3604 L4 inspect result: PASS packet 2541E38
(30.0.0.1:46409) (40.0.0.1:21) bytes 22 ftp
*Mar 2 01:20:58: CBAC sis 25A3604 Restoring State: SIS_OPEN/ESTAB iisn 4200176160
i_rcvnxt 4223
720160 i_sndnxt 4200176262 i_rcvwnd 8760 risn 4223719771 r_rcvnxt 4200176262 r_sndnxt
4223720160 r_rcvwnd 8760
*Mar 2 01:20:58: CBAC* sis 25A3604 ftp L7 inspect result: PROCESS-SWITCH packet
*Mar 2 01:20:58: CBAC* sis 25A3604 ftp L7 inspect result: PROCESS-SWITCH packet
*Mar 2 01:20:58: CBAC* Bump up: inspection requires the packet in the process
path(30.0.0.1) (40.0.0.1)
*Mar 2 01:20:58: CBAC Pak 2541E38 Find session for (30.0.0.1:46409) (40.0.0.1:21) tcp
*Mar 2 01:20:58: P ack 4223720160 seq 4200176262(22)
*Mar 2 01:20:58: CBAC Pak 2541E38 Addr:port pairs to match: (30.0.0.1:46409)
(40.0.0.1:21)
*Mar 2 01:20:58: CBAC sis 25A3604 SIS_OPEN
*Mar 2 01:20:58: CBAC Pak 2541E38 IP: s=30.0.0.1 (Ethernet0), d=40.0.0.1 (Ethernet1), len
76, proto=6
```

The following is sample output from the **debug ip inspect icmp** and **debug ip inspect detailed** commands:

```

1w6d:CBAC sis 81073F0C SIS_CLOSED
1w6d:CBAC Pak 80D2E9EC IP:s=192.168.133.3 (Ethernet1), d=0.0.0.0 (Ethernet0), len 98,
proto=1
1w6d:CBAC ICMP:sis 81073F0C pak 80D2E9EC SIS_CLOSED ICMP packet (192.168.133.3:0) =>
(0.0.0.0:0) datalen 56
1w6d:CBAC ICMP:start session from 192.168.133.3
1w6d:CBAC sis 81073F0C --> SIS_OPENING (192.168.133.3:0) (0.0.0.0:0)
1w6d:CBAC sis 81073F0C L4 inspect result:PASS packet 80D2E9EC (192.168.133.3:0)
(0.0.0.0:0) bytes 56 icmp
1w6d:CBAC sis 81073F0C SIS_OPENING
1w6d:CBAC Pak 80E72BFC IP:s=0.0.0.0 (Ethernet0), d=192.168.133.3 (Ethernet1), len 98,
proto=1
1w6d:CBAC ICMP:sis 81073F0C pak 80E72BFC SIS_OPENING ICMP packet (192.168.133.3:0) <=
(0.0.0.0:0) datalen 56
1w6d:CBAC sis 81073F0C --> SIS_OPEN (192.168.133.3:0) (0.0.0.0:0)
1w6d:CBAC sis 81073F0C L4 inspect result:PASS packet 80E72BFC (0.0.0.0:0)
(192.168.133.3:0) bytes 56 icmp
1w6d:CBAC* sis 81073F0C SIS_OPEN
1w6d:CBAC* Pak 80D2F2C8 IP:s=192.168.133.3 (Ethernet1), d=0.0.0.0 (Ethernet0), len 98,
proto=1
1w6d:CBAC* ICMP:sis 81073F0C pak 80D2F2C8 SIS_OPEN ICMP packet (192.168.133.3:0) =>
(0.0.0.0:0) datalen 56
1w6d:CBAC* sis 81073F0C --> SIS_OPEN (192.168.133.3:0) (0.0.0.0:0)
1w6d:CBAC* sis 81073F0C L4 inspect result:PASS packet 80D2F2C8 (192.168.133.3:0)
(0.0.0.0:0) bytes 56 icmp
1w6d:CBAC* sis 81073F0C SIS_OPEN
1w6d:CBAC* Pak 80E737CC IP:s=0.0.0.0 (Ethernet0), d=192.168.133.3 (Ethernet1), len 98,
proto=1
1w6d:CBAC* ICMP:sis 81073F0C pak 80E737CC SIS_OPEN ICMP packet (192.168.133.3:0) <=
(0.0.0.0:0) datalen 56
1w6d:CBAC* sis 81073F0C --> SIS_OPEN (192.168.133.3:0) (0.0.0.0:0)
1w6d:CBAC* sis 81073F0C L4 inspect result:PASS packet 80E737CC (0.0.0.0:0)
(192.168.133.3:0) bytes 56 icmp
1w6d:CBAC* sis 81073F0C SIS_OPEN
1w6d:CBAC* Pak 80F554F0 IP:s=192.168.133.3 (Ethernet1), d=0.0.0.0 (Ethernet0), len 98,
proto=1
1w6d:CBAC* ICMP:sis 81073F0C pak 80F554F0 SIS_OPEN ICMP packet (192.168.133.3:0) =>
(0.0.0.0:0) datalen 56
1w6d:CBAC* sis 81073F0C --> SIS_OPEN (192.168.133.3:0) (0.0.0.0:0)
1w6d:CBAC* sis 81073F0C L4 inspect result:PASS packet 80F554F0 (192.168.133.3:0)
(0.0.0.0:0) bytes 56 icmp
1w6d:CBAC* sis 81073F0C SIS_OPEN
1w6d:CBAC* Pak 80E73AC0 IP:s=0.0.0.0 (Ethernet0), d=192.168.133.3 (Ethernet1), len 98,
proto=1
1w6d:CBAC* ICMP:sis 81073F0C pak 80E73AC0 SIS_OPEN ICMP packet (192.168.133.3:0) <=
(0.0.0.0:0) datalen 56
1w6d:CBAC* sis 81073F0C --> SIS_OPEN (192.168.133.3:0) (0.0.0.0:0)
1w6d:CBAC* sis 81073F0C L4 inspect result:PASS packet 80E73AC0 (0.0.0.0:0)
(192.168.133.3:0) bytes 56 icmp

```

ip inspect name

To define a set of inspection rules, use the **ip inspect name** command in global configuration mode. To remove the inspection rule for a protocol or to remove the entire set of inspection rules, use the **no** form of this command.

```
ip inspect name inspection-name protocol [alert {on | off}] [audit-trail {on | off}]
[timeout seconds]
```

```
no ip inspect name [inspection-name protocol]
```

HTTP Inspection Syntax

```
ip inspect name inspection-name http [urlfilter] [java-list access-list] [alert {on | off}]
[audit-trail {on | off}] [timeout seconds] (Java protocol only)
```

```
no ip inspect name inspection-name protocol (removes the inspection rule for a protocol)
```

remote-procedure call (RPC) Inspection Syntax

```
ip inspect name inspection-name rpc program-number number [wait-time minutes] [alert {on | off}]
[audit-trail {on | off}] [timeout seconds] (RPC protocol only)
```

```
no ip inspect name inspection-name protocol (removes the inspection rule for a protocol)
```

Fragment Inspection Syntax

```
ip inspect name inspection-name fragment [max number timeout seconds]
```

```
no ip inspect name inspection-name fragment (removes fragment inspection for a rule)
```

Syntax Description

<i>inspection-name</i>	Names the set of inspection rules. If you want to add a protocol to an existing set of rules, use the same <i>inspection-name</i> as the existing set of rules. Note The <i>inspection-name</i> cannot exceed 16 characters; otherwise, the name will be truncated to the 16-character limit.
<i>protocol</i>	A protocol keyword listed in Table 3 or Table 4 .
alert { on off }	(Optional) For each inspected protocol, the generation of alert messages can be set be on or off . If no option is selected, alerts are generated on the basis of the setting of the ip inspect alert-off command.
audit-trail { on off }	(Optional) For each inspected protocol, audit trail can be set on or off . If no option is selected, an audit trail message are generated on the basis of the setting of the ip inspect audit-trail command.
http	Specifies the HTTP protocol for Java applet blocking.
urlfilter	(Optional) Associates URL filtering with HTTP inspection.

timeout <i>seconds</i>	(Optional) To override the global TCP or User Datagram Protocol (UDP), or Internet Control Message Protocol (ICMP) idle timeouts for the specified protocol, specify the number of seconds for a different idle timeout. This timeout overrides the global TCP, UDP, or ICMP timeouts but will not override the global Domain Name System (DNS) timeout.
java-list <i>access-list</i>	(Optional) Specifies the numbered standard access list to use to determine “friendly” sites. This keyword is available only for the HTTP protocol, for Java applet blocking. Java blocking only works with numbered standard access lists.
rpc program-number <i>number</i>	Specifies the program number to permit. This keyword is available only for the remote-procedure call protocol.
wait-time <i>minutes</i>	(Optional) Specifies the number of minutes to keep a small hole in the firewall to allow subsequent connections from the same source address and to the same destination address and port. The default wait-time is zero minutes. This keyword is available only for the RPC protocol.
fragment	Specifies fragment inspection for the named rule.
max <i>number</i>	(Optional) Specifies the maximum number of unassembled packets for which state information (structures) is allocated by Cisco IOS software. Unassembled packets are packets that arrive at the router interface before the initial packet for a session. The acceptable range is 50 through 10000. The default is 256 state entries. Memory is allocated for the state structures, and setting this value to a larger number may cause memory resources to be exhausted.
timeout <i>seconds</i> (fragmentation)	(Optional) Configures the number of seconds that a packet state structure remains active. When the timeout value expires, the router drops the unassembled packet, freeing that structure for use by another packet. The default timeout value is one second. If this number is set to a value greater than one second, it will be automatically adjusted by the Cisco IOS software when the number of free state structures goes below certain thresholds: when the number of free states is less than 32, the timeout will be divided by 2. When the number of free states is less than 16, the timeout will be set to 1 second.

Table 3 Protocol Keywords—Transport-Layer Protocols

Protocol	Keyword
ICMP	icmp
TCP	tcp
UDP	udp

Table 4 Protocol Keywords—Application-Layer Protocols

Protocol	Keyword
CU-SeeMe	cuseeme
FTP	ftp
Java	http
H.323	h323
Microsoft NetShow	netshow
RealAudio	realaudio
remote-procedure call (RPC)	rpc
Session Initiation Protocol (SIP)	sip
Simple Mail Transfer Protocol (SMTP)	smtp
Skiny Client Control Protocol (SCCP)	skinny
StreamWorks	streamworks
Structured Query Language*Net (SQL*Net)	sqlnet
TFTP	tftp
UNIX R commands (rlogin, rexec, rsh)	rcmd
VDOLive	vdolive

Defaults

No inspection rules are defined until you define them using this command.

Command Modes

Global configuration

Command History

Release	Modification
11.2 P	This command was introduced.
12.0(5)T	Introduced configurable alert and audit trail, IP fragmentation checking, and NetShow protocol support.
12.2(11)YU	Support was added for ICMP and SIP protocols and the urlfilter keyword was added to the HTTP inspection syntax.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.3(1)	Skiny protocol support was added.

Usage Guidelines

To define a set of inspection rules, enter this command for each protocol that you want the Cisco IOS firewall to inspect, using the same *inspection-name*. Give each set of inspection rules a unique *inspection-name*, which should not exceed the 16-character limit. Define either one or two sets of rules per interface—you can define one set to examine both inbound and outbound traffic, or you can define two sets: one for outbound traffic and one for inbound traffic.

To define a single set of inspection rules, configure inspection for all the desired application-layer protocols, and for TCP, UDP, or ICMP as desired. This combination of TCP, UDP, and application-layer protocols join together to form a single set of inspection rules with a unique name. (There are no application-layer protocols associated with ICMP.)

To remove the inspection rule for a protocol, use the **no** form of this command with the specified inspection name and protocol; to remove the entire set of inspection rules, use the **no** form of this command only; that is, do not list any inspection names or protocols.

In general, when inspection is configured for a protocol, return traffic entering the internal network will be permitted only if the packets are part of a valid, existing session for which state information is being maintained.

TCP and UDP Inspection

You can configure TCP and UDP inspection to permit TCP and UDP packets to enter the internal network through the firewall, even if the application-layer protocol is not configured to be inspected. However, TCP and UDP inspection do not recognize application-specific commands, and therefore might not permit all return packets for an application, particularly if the return packets have a different port number from the previous exiting packet.

Any application-layer protocol that is inspected will take precedence over the TCP or UDP packet inspection. For example, if inspection is configured for FTP, all control channel information will be recorded in the state table, and all FTP traffic will be permitted back through the firewall if the control channel information is valid for the state of the FTP session. The fact that TCP inspection is configured is irrelevant.

With TCP and UDP inspection, packets entering the network must exactly match an existing session: the entering packets must have the same source or destination addresses and source or destination port numbers as the exiting packet (but reversed). Otherwise, the entering packets will be blocked at the interface.

ICMP Inspection

An ICMP inspection session is on the basis of the source address of the inside host that originates the ICMP packet. Dynamic access control lists (ACLs) are created for return ICMP packets of the allowed types (echo-reply, time-exceeded, destination unreachable, and timestamp reply) for each session. There are no port numbers associated with an ICMP session, and the permitted IP address of the return packet is wild-carded in the ACL. The wild-card address is because the IP address of the return packet cannot be known in advance for time-exceeded and destination-unreachable replies. These replies can come from intermediate devices rather than the intended destination.

Application-Layer Protocol Inspection

In general, if you configure inspection for an application-layer protocol, packets for that protocol should be permitted to exit the firewall (by configuring the correct access control list), and packets for that protocol will only be allowed back in through the firewall if they belong to a valid existing session. Each protocol packet is inspected to maintain information about the session state.

Java, H.323, RPC, SIP, and SMTP inspection have additional information, described in the next five sections.

Java Inspection

Java inspection enables Java applet filtering at the firewall. Java applet filtering distinguishes between trusted and untrusted applets by relying on a list of external sites that you designate as “friendly.” If an applet is from a friendly site, the firewall allows the applet through. If the applet is not from a friendly site, the applet will be blocked. Alternately, you could permit applets from all sites except sites specifically designated as “hostile.”



Note

Before you configure Java inspection, you must configure a numbered standard access list that defines “friendly” and “hostile” external sites. You configure this numbered standard access list to permit traffic from friendly sites, and to deny traffic from hostile sites. If you do not configure a numbered standard access list, but use a “placeholder” access list in the **ip inspect name inspection-name http** command, all Java applets will be blocked.



Caution

Context-Based Access Control (CBAC) does not detect or block encapsulated Java applets. Therefore, Java applets that are wrapped or encapsulated, such as applets in .zip or .jar format, are *not* blocked at the firewall. CBAC also does not detect or block applets loaded via FTP, gopher, or HTTP on a nonstandard port.

H.323 Inspection

If you want CBAC inspection to work with NetMeeting 2.0 traffic (an H.323 application-layer protocol), you must also configure inspection for TCP, as described in the chapter “Configuring Context-Based Access Control” in the *Cisco IOS Security Configuration Guide*. This requirement exists because NetMeeting 2.0 uses an additional TCP channel not defined in the H.323 specification.

RPC Inspection

RPC inspection allows the specification of various program numbers. You can define multiple program numbers by creating multiple entries for RPC inspection, each with a different program number. If a program number is specified, all traffic for that program number will be permitted. If a program number is not specified, all traffic for that program number will be blocked. For example, if you created an RPC entry with the NFS program number, all NFS traffic will be allowed through the firewall.

SIP Inspection

You can configure SIP inspection to permit media sessions associated with SIP-signaled calls to traverse the firewall. Because SIP is frequently used to signal both incoming and outgoing calls, it is often necessary to configure SIP inspection in both directions on a firewall (both from the protected internal network and from the external network). Because inspection of traffic from the external network is not done with most protocols, it may be necessary to create an additional inspection rule to cause only SIP inspection to be performed on traffic coming from the external network.

SMTP Inspection

SMTP inspection causes SMTP commands to be inspected for illegal commands. Any packets with illegal commands are dropped, and the SMTP session will hang and eventually time out. An illegal command is any command except for the following legal commands:

- DATA
- EXPN
- HELO
- HELP

- MAIL
- NOOP
- QUIT
- RCPT
- RSET
- SAML
- SEND
- SOML
- VRFY

Use of the **urlfilter** Keyword

If you specify the **urlfilter** keyword, the Cisco IOS firewall will interact with a URL filtering software to control web traffic for a given host or user on the basis of a specified security policy.



Note

Enabling HTTP inspection with or without any option triggers the Java applet scanner, which is CPU intensive. The only way to stop the Java applet scanner is to specify the **java-list** *access-list* option. Configuring URL filtering without enabling the **java-list** *access-list* option will severely impact performance.

Use of the **timeout** Keyword

If you specify a timeout for any of the transport-layer or application-layer protocols, the timeout will override the global idle timeout for the interface to which the set of inspection rules is applied.

If the protocol is TCP or a TCP application-layer protocol, the timeout will override the global TCP idle timeout. If the protocol is UDP or a UDP application-layer protocol, the timeout will override the global UDP idle timeout.

If you do not specify a timeout for a protocol, the timeout value applied to a new session of that protocol will be taken from the corresponding TCP or UDP global timeout value valid at the time of session creation.

The default ICMP timeout is deliberately short (10 seconds) due to the security hole that is opened by allowing ICMP packets with a wild-carded source address back into the inside network. The timeout will occur 10 seconds after the last outgoing packet from the originating host. For example, if you send a set of 10 ping packets spaced one second apart, the timeout will expire in 20 seconds or 10 seconds after the last outgoing packet. However, the timeout is not extended for return packets. If a return packet is not seen within the timeout window, the hole will be closed and the return packet will not be allowed in. Although the default timeout can be made longer if desired, it is recommended that this value be kept relatively short.

IP Fragmentation Inspection

CBAC inspection rules can help protect hosts against certain denial-of-service attacks involving fragmented IP packets. Even though the firewall keeps an attacker from making actual connections to a given host, the attacker may still be able to disrupt services provided by that host. This is done by sending many non-initial IP fragments or by sending complete fragmented packets through a router with an ACL that filters the first fragment of a fragmented packet. These fragments can tie up resources on the target host as it tries to reassemble the incomplete packets.

Using fragmentation inspection, the firewall maintains an *interfragment state* (structure) for IP traffic. Non-initial fragments are discarded unless the corresponding initial fragment was permitted to pass through the firewall. Non-initial fragments received before the corresponding initial fragments are discarded.

**Note**

Fragmentation inspection can have undesirable effects in certain cases, because it can result in the firewall discarding any packet whose fragments arrive out of order. There are many circumstances that can cause out-of-order delivery of legitimate fragments. Apply fragmentation inspection in situations where legitimate fragments, which are likely to arrive out of order, might have a severe performance impact.

Because routers running Cisco IOS software are used in a very large variety of networks, and because the CBAC feature is often used to isolate parts of internal networks from one another, the fragmentation inspection feature is not enabled by default. Fragmentation detection must be explicitly enabled for an inspection rule using the **ip inspect name** command. Unfragmented traffic is never discarded because it lacks a fragment state. Even when the system is under heavy attack with fragmented packets, legitimate fragmented traffic, if any, will still get some fraction of the firewall's fragment state resources, and legitimate, unfragmented traffic can flow through the firewall unimpeded.

Examples

The following example causes the software to inspect TCP sessions and UDP sessions, and to specifically allow CU-SeeMe, FTP, and RPC traffic back through the firewall for existing sessions only. For UDP traffic, audit-trail is on. For FTP traffic, the idle timeout is set to override the global TCP idle timeout. For RPC traffic, program numbers 100003, 100005, and 100021 are permitted.

```
ip inspect name myrules tcp
ip inspect name myrules udp audit-trail on
ip inspect name myrules cuseeme
ip inspect name myrules ftp timeout 120
ip inspect name myrules rpc program-number 100003
ip inspect name myrules rpc program-number 100005
ip inspect name myrules rpc program-number 100021
```

The following example adds fragment checking to software inspection of TCP and UDP sessions for the rule named "myrules." In this example, the firewall software will allocate 100 state structures, and the timeout value for dropping unassembled packets is set to 4 seconds. If 100 initial fragments for 100 different packets are sent through the router, all of the state structures will be used up. The initial fragment for packet 101 will be dropped. Additionally, if the number of free state structures (structures available for use by unassembled packets) drops below the threshold values, 32 or 16, the timeout value is automatically reduced to 2 or 1, respectively. Changing the timeout value frees up packet state structures more quickly.

```
ip inspect name myrules tcp
ip inspect name myrules udp audit-trail on
ip inspect name myrules cuseeme
ip inspect name myrules ftp timeout 120
ip inspect name myrules rpc program-number 100003
ip inspect name myrules rpc program-number 100005
ip inspect name myrules rpc program-number 100021
ip inspect name myrules fragment max 100 timeout 4
```

The following firewall and SIP example shows how to allow outside-initiated calls and internal calls. For outside-initiated calls, an ACL needs to be punched to allow for the traffic from the initial signaling packet from outside. Subsequent signaling and media channels will be allowed by the inspection module.

```
ip inspect name voip sip
interface FastEthernet0/0
 ip inspect voip in
!
!
interface FastEthernet0/1
 ip inspect voip in
 ip access-group 100 in
!
!
access-list 100 permit udp host <gw ip> any eq 5060
access-list 100 permit udp host <proxy ip> any eq 5060
access-list deny ip any any
```

The following example shows two configured inspections named “fw_only” and “fw_urlf”; URL filtering will work only on the traffic that is inspected by fw_urlf. Note that the **java-list access-list** option has been enabled, which disables java scanning.

```
ip inspect name fw_only http java-list 51 timeout 30
interface e0
 ip inspect fw_only in
!
ip inspect name fw_urlf http urlfilter java-list 51 timeout 30
interface e1
 ip inspect fw_urlf in
```

Related Commands

Command	Description
ip inspect	Applies a set of inspection rules to an interface.
ip inspect alert-off	Disables CBAC alert messages.
ip inspect audit trail	Turns on CBAC audit trail messages, which will be displayed on the console after each CBAC session close.

ip port-map

To establish port to application mapping (PAM), use the **ip port-map** command in global configuration. To delete user-defined PAM entries, use the **no** form of this command.

```
ip port-map appl_name port port_num [list acl_num]
```

```
no ip port-map appl_name port port_num [list acl_num]
```

Syntax Description		
<i>appl_name</i>	Specifies the name of the application with which to apply the port mapping.	
port	Indicates that a port number maps to the application.	
<i>port_num</i>	Identifies a port number in the range 1 to 65535.	
list	(Optional) Indicates that the port mapping information applies to a specific host or subnet.	
<i>acl_num</i>	(Optional) Identifies the standard access control list (ACL) number used with PAM.	

Defaults No default behavior or values

Command Modes Global configuration

Command History	Release	Modification
	12.0(5)T	This command was introduced.
	12.3(1)	Skippy Client Control protocol (SCCP) support was added.

Usage Guidelines The **ip port-map** command associates TCP or User Datagram Protocol (UDP) port numbers with applications or services, establishing a table of default port mapping information at the firewall. This information is used to support network environments that run services using ports that are different from the registered or well-known ports associated with a service or application.

The port mapping information in the PAM table is of one of three types:

- System-defined
- User-defined
- Host-specific

System-Defined Port Mapping

Initially, PAM creates a set of system-defined entries in the mapping table using well-known or registered port mapping information set up during the system start-up. The Cisco IOS Firewall Context-Based Access Control feature requires the system-defined mapping information to function properly. System-defined mapping information cannot be deleted or changed; that is, you cannot map HTTP services to port 21 (FTP) or FTP services to port 80 (HTTP).

[Table 5](#) lists the default system-defined services and applications in the PAM table.

Table 5 System-Defined Port Mapping

Application Name	Well-Known or Registered Port Number	Protocol Description
cuseeme	7648	CU-SeeMe Protocol
exec	512	Remote Process Execution
ftp	21	File Transfer Protocol (control port)
h323	1720	H.323 Protocol (for example, MS NetMeeting, Intel Video Phone)
http	80	Hypertext Transfer Protocol
login	513	Remote login
msrpc	135	Microsoft Remote Procedure Call
netshow	1755	Microsoft NetShow
real-audio-video	7070	RealAudio and RealVideo
sccp	2000	Skinny Client Control Protocol (SCCP)
smtp	25	Simple Mail Transfer Protocol (SMTP)
sql-net	1521	SQL-NET
streamworks	1558	StreamWorks Protocol
sunrpc	111	SUN Remote Procedure Call
tftp	69	Trivial File Transfer Protocol
vdolive	7000	VDOLive Protocol

**Note**

You can override the system-defined entries for a specific host or subnet using the **list** option in the **ip port-map** command.

User-Defined Port Mapping

Network applications that use non-standard ports require user-defined entries in the mapping table. Use the **ip port-map** command to create default user-defined entries in the PAM table.

To map a range of port numbers with a service or application, you must create a separate entry for each port number.

**Note**

If you try to map an application to a system-defined port, a message appears warning you of a mapping conflict.

Use the **no** form of the **ip port-map** command to delete user-defined entries from the PAM table.

To overwrite an existing user-defined port mapping, use the **ip port-map** command to associate another service or application with the specific port.

Host-Specific Port Mapping

User-defined entries in the mapping table can include host-specific mapping information, which establishes port mapping information for specific hosts or subnets. In some environments, it might be necessary to override the default port mapping information for a specific host or subnet, including a system-defined default port mapping information. Use the **list** option for the **ip port-map** command to specify an ACL for a host or subnet that uses PAM.



Note

If the host-specific port mapping information is the same as existing system-defined or user-defined default entries, host-specific port changes have no effect.

Examples

The following example provides examples for adding and removing user-defined PAM configuration entries at the firewall.

In the following example, non-standard port 8000 is established as the user-defined default port for HTTP services:

```
ip port-map http port 8000
```

The following example shows PAM entries establish a range of nonstandard ports for HTTP services:

```
ip port-map http 8001
ip port-map http 8002
ip port-map http 8003
ip port-map http 8004
```

In the following example the command fails because it tries to map port 21, which is the system-defined default port for FTP, with HTTP:

```
ip port-map http port 21
```

In the following example, a specific host uses port 8000 for FTP services. ACL 10 identifies the server address (192.168.32.43), while port 8000 is mapped with FTP services:

```
access-list 10 permit 192.168.32.43
ip port-map ftp port 8000 list 10
```

In the following example, port 21, which is normally reserved for FTP services, is mapped to the RealAudio application for the hosts in list 10. In this configuration, hosts in list 10 do not recognize FTP activity on port 21.

```
ip port-map realaudio port 21 list 10
```

In the following example, the **ip port-map** command fails and generates an error message:

```
ip port-map netshow port 21
Command fail: the port 21 has already been defined for ftp by the system.
No change can be made to the system defined port mappings.
```

The **no** form of this command deletes user-defined entries from the PAM table. It has no effect on the system-defined port mappings. This command deletes the host-specific port mapping of FTP.

```
no ip port-map ftp port 1022 list 10
```

In the following example, the command fails because it tries to delete the system-defined default port for HTTP:

```
no ip port-map http port 80
```

In the following example, a specific host uses port 8000 for FTP services. ACL 10 identifies the server address (192.168.32.43), while port 8000 is mapped with FTP services.

```
access-list 10 permit 192.168.32.43
ip port-map ftp port 8000 list 10
```

In the following example, a specific subnet runs HTTP services on port 8080. ACL 50 identifies the subnet, while the PAM entry maps port 8080 with HTTP services.

```
access-list 50 permit 192.168.92.0
ip port-map http 8080 list 50
```

In the following example, a specific host runs HTTP services on port 25, which is the system-defined port number for SMTP services. This requires a host-specific PAM entry that overrides the system-defined default port mapping for HTTP, which is port 80. ACL 15 identifies the host address (192.168.33.43), while port 25 is mapped with HTTP services.

```
access-list 15 permit 192.168.33.43
ip port-map http port 25 list 15
```

In the following example, the same port number is required by different services running on different hosts. Port 8000 is required for HTTP services by host 192.168.3.4, while port 8000 is required for Telnet services by host 192.168.5.6. ACL 10 and ACL 20 identify the specific hosts, while PAM maps the ports with the services for each ACL.

```
access-list 10 permit 192.168.3.4
access-list 20 permit 192.168.5.6
ip port-map http port 8000 list 10
ip port-map http ftp 8000 list 20
```

Related Commands

Command	Description
show ip port-map	Displays the PAM information.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSF, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Copyright © 2003 Cisco Systems, Inc. All rights reserved.