



The Cisco IOS Firewall Feature Set and Context-Based Access Control

This document describes the Cisco IOS Firewall feature set, and describes how to configure context-based access control, one of the Cisco IOS Firewall feature set features.

In This Document

This document includes the following sections:

- The Cisco IOS Firewall Feature Set
- Context-Based Access Control:
 - About Context-Based Access Control
 - Configure Context-Based Access Control
 - Interpret Real-Time Alerts Generated by Context-Based Access Control
 - Turn Off Context-Based Access Control
 - Context-Based Access Control Configuration Example
 - Context-Based Access Control Command Reference

The Cisco IOS Firewall Feature Set

The Cisco IOS Firewall feature set combines existing Cisco IOS firewall technology and the new context-based access control (CBAC) feature. When you configure the Cisco IOS Firewall feature set on your Cisco router, you turn your router into an effective, robust firewall.

The Cisco IOS Firewall feature set is designed to prevent unauthorized, external individuals from gaining access to your internal network, and to block attacks on your network, while at the same time allowing authorized users to access network resources.

You can use the Cisco IOS Firewall feature set to configure your Cisco IOS router as:

- An Internet firewall or part of an Internet firewall
- A firewall between groups in your internal network
- A firewall providing secure connections to or from branch offices
- A firewall between your company's network and your company's partners' networks

The Cisco IOS Firewall feature set provides the following benefits:

- Protects internal networks from intrusion
- Monitors traffic through network perimeters
- Enables network commerce via the World Wide Web

Configuring the Cisco IOS Firewall Feature Set

To create a firewall customized to fit your organization's security policy, you should choose which features of the Cisco IOS Firewall feature set are appropriate, and configure those features. At a minimum, you must configure basic traffic filtering to provide a basic firewall. The Cisco IOS Firewall feature set includes the following features (described next):

- Basic and Advanced Traffic Filtering
- Security Server Support
- Network Address Translation
- Network Data Encryption
- Neighbor Router Authentication
- Event Logging

As well as configuring these features, you should follow the guidelines listed afterwards in the section "Other Guidelines for Configuring Your Firewall". This section outlines important security practices to protect your firewall and network.

Note Refer to the Cisco IOS Release 11.3 *Security Configuration Guide* and *Security Command Reference* publications to find the complete configuration and command information for all the firewall elements described in this section, except as noted. (In particular, context-based access control—not available in Release 11.3—is described later in this document.)

Basic and Advanced Traffic Filtering

To configure traffic filtering, configure one or more of the following features:

- **Basic Traffic Filtering: Standard Access Lists and Static Extended Access Lists**

Standard and static extended access lists provide basic traffic filtering capabilities. You configure criteria that describe which packets should be forwarded, and which packets should be dropped at an interface, based on each packet's network layer information. For example, you can block all UDP packets from a specific source IP address or address range. Some extended access lists can also examine transport layer information to determine whether to block or forward packets.

- **Advanced Traffic Filtering: Lock-and-Key (Dynamic Access Lists)**

Lock-and-Key provides traffic filtering with the ability to allow temporary access through the firewall for certain individuals. These individuals must first be authenticated (by a username/password mechanism) before the firewall allows their traffic through the firewall, and afterwards, the firewall closes the temporary opening. This provides tighter control over traffic at the firewall than with standard or static extended access lists.

- **Advanced Traffic Filtering: Context-Based Access Control**

Context-based access control (CBAC) examines not only network layer and transport layer information, but also examines the application layer protocol information (such as FTP information) to learn about the state of TCP and UDP connections. CBAC maintains connection state information for individual connections. This state information is used to make intelligent decisions about whether packets should be permitted or denied, and dynamically creates and deletes temporary openings in the firewall.

CBAC is described in greater detail later in this document.

Security Server Support

The Cisco IOS Firewall feature set can be configured as a client of the following supported security servers:

- TACACS, TACACS+, and Extended TACACS
- RADIUS
- Kerberos

You can use any of these security servers to store a database of user profiles. To gain access into your firewall or to gain access through the firewall into another network, users must enter authentication information (such as a username and password) which is matched against the information on the security server. If the user passes authentication, they are granted access according to their specified privileges.

Network Address Translation

You can use Network Address Translation (NAT) to hide internal IP network addresses from the world outside the firewall.

NAT was designed to provide IP address conservation and for internal IP networks that have unregistered (not globally unique) IP addresses: NAT translates these unregistered IP addresses into legal addresses at the firewall. NAT can also be configured to advertise only one address for the entire internal network to the outside world. This provides security by effectively hiding the entire internal network from the world.

NAT gives you limited spoof protection because internal addresses are hidden. Additionally, NAT removes all your internal services from the external name space.

Note NAT does not work with the application layer protocols RPC, VDOLive, or SQL*Net “Redirected.” (NAT does work with SQL*Net “Bequeathed.”) Do not configure NAT with networks that will carry traffic for these incompatible protocols.

To configure NAT, refer to the “Configuring IP Addressing” chapter in the Cisco IOS Release 11.3 *Network Protocols Configuration Guide, Part 1*.

Network Data Encryption

Network data encryption selectively encrypts IP packets that are transmitted across unprotected networks such as the Internet. You specify which traffic is considered sensitive and should be encrypted. This encryption prevents sensitive IP packets from being intercepted and read or tampered with.

Neighbor Router Authentication

Neighbor router authentication requires the firewall to authenticate all neighbor routers before accepting any route updates from that neighbor. This ensures that the firewall receives legitimate route updates from a trusted source.

Event Logging

Event logging automatically logs output from system error messages and other events to the console terminal. You can also redirect these messages to other destinations such as virtual terminals, internal buffers, or syslog servers. You can also specify the severity of the event to be logged, and you can configure the logged output to be timestamped. The logged output can be used to assist real-time debugging and management, and to track potential security breaches or other nonstandard activities throughout a network.

To configure event logging, refer to the “Troubleshooting the Router” chapter in the “System Management” part of the Cisco IOS Release 11.3 *Configuration Fundamentals Configuration Guide*.

Other Guidelines for Configuring Your Firewall

This section includes guidelines for configuring your firewall.

- When setting passwords for privileged access to the firewall, use the **enable secret** command rather than the **enable password** command, which does not have as strong an encryption algorithm.
- Put a password on the console port. In authentication, authorization, and accounting (AAA) environments, use the same authentication for the console as for elsewhere. In a non-AAA environment, at a minimum configure the **login** and **password password** commands.
- Think about access control *before* you connect a console port to the network in any way, including attaching a modem to the port. Be aware that a BREAK on the console port might give total control of the firewall, even with access control configured.
- Apply access lists and password protection to all virtual terminal ports. Use access lists to limit who can Telnet into your router.
- Don't enable any local service (such as SNMP or NTP) that you don't use. Cisco Discovery Protocol (CDP) and Network Time Protocol (NTP) are on by default, and you should turn these off if you don't need them.

To turn off CDP, enter the **no cdp run** global configuration command. To turn off NTP, enter the **ntp disable** interface configuration command on each interface not using NTP.

If you must run NTP, configure NTP only on required interfaces, and configure NTP to listen only to certain peers.

Any enabled service could present a potential security risk. A determined, hostile party might be able to find creative ways to misuse the enabled services to access the firewall or the network.

For local services that are enabled, protect against misuse. Protect by configuring the services to communicate only with specific peers, and protect by configuring access lists to deny packets for the services at specific interfaces.

- Protect against spoofing: protect the networks on both sides of the firewall from being spoofed from the other side. You could protect against spoofing by configuring input access lists at all interfaces to pass only traffic from expected source addresses, and to deny all other traffic.

You should also disable source routing (for IP, enter the **no ip source-route** global configuration command). Disabling source routing at *all* routers can also help prevent spoofing.

You should also disable minor services (for IP, enter the **no service tcp-small-servers** and **no service udp-small-servers** global configuration commands).

- Prevent the firewall from being used as a relay, by configuring access lists on any asynchronous Telnet ports.
- Normally, you should disable directed broadcasts for all applicable protocols on your firewall and on all your other routers. (For IP, use the **no ip directed-broadcast** command.) Rarely, some IP networks do require directed broadcasts; if this is the case, do not disable directed broadcasts.

Directed broadcasts can be misused to multiply the power of denial-of-service attacks, because every denial-of-service packet sent is broadcast to every host on a subnet. Furthermore, some hosts have other intrinsic security risks present when handling broadcasts.

- Configure the **no proxy-arp** command to prevent internal addresses from being revealed. (This is important to do if you don't already have NAT configured to prevent internal addresses from being revealed).
- Keep the firewall in a secured (locked) room.

About Context-Based Access Control

This section describes:

- What CBAC Does (Overview)
- What CBAC Does Not Do
- How CBAC Works
- When and Where to Configure CBAC
- The CBAC Process
- Supported Protocols
- Restrictions
- Memory and Performance Impact

What CBAC Does (Overview)

Context-based access control (CBAC) intelligently filters TCP and UDP packets based on application-layer protocol session information. CBAC permits specified TCP and UDP traffic through a firewall only when the connection is initiated from within the protected internal network.

Without CBAC, traffic filtering is limited to access list implementations that examine packets at the network layer, or at most, the transport layer. However, CBAC examines not only network layer and transport layer information, but also examines the application-layer protocol information (such as FTP connection information) to learn about the state of the TCP or UDP session. This allows support of protocols that involve multiple channels created as a result of negotiations in the control channel. Most of the multimedia protocols as well as some other protocols (such as FTP, RPC, and SQL*Net) involve multiple channels.

CBAC inspects traffic that travels through the firewall to discover and manage state information for TCP and UDP sessions. This state information is used to create temporary openings in the firewall's access lists to allow return traffic for permissible sessions (sessions that originated from within the protected internal network).

CBAC also provides the following benefits:

- Java blocking
- Denial-of-Service prevention and detection
- Real-time alerts and audit trails

What CBAC Does Not Do

CBAC does not provide intelligent filtering for all protocols; it only works for the protocols that you specify. If you don't specify a certain protocol for CBAC, the existing access lists will determine how that protocol is filtered. No temporary openings will be created for protocols not specified for CBAC inspection.

CBAC does not protect against attacks originating from within the protected network. CBAC only detects and protects against attacks which travel through the firewall.

CBAC protects against certain attacks, but should not be considered a perfect, impenetrable defense. Determined, skilled attackers might be able to launch effective attacks. While there is no such thing as a perfect defense, CBAC detects and prevents most of the popular attacks on your network.

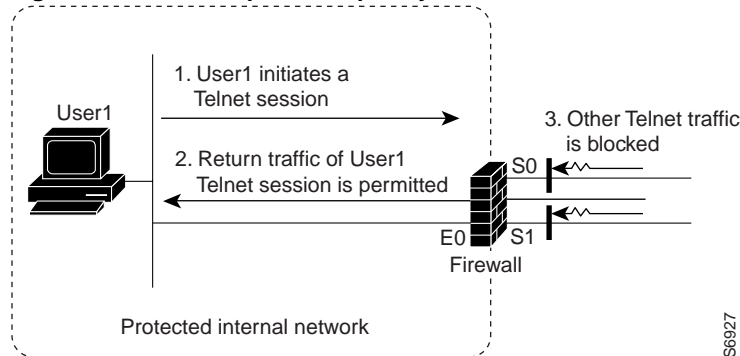
How CBAC Works

You should understand the material in this section before you configure CBAC. If you don't understand how CBAC works, you might inadvertently introduce security risks by configuring CBAC inappropriately.

How CBAC Works—Overview

CBAC creates temporary openings in access lists at firewall interfaces. These openings are created when specified traffic exits your internal network through the firewall. The openings allow returning traffic (that would normally be blocked) to enter your internal network back through the firewall. The traffic is allowed back through the firewall only if it is part of the same session as the original traffic that triggered CBAC when exiting through the firewall.

Figure 1 CBAC Opens Temporary Holes in Firewall Access Lists



In Figure 1, the inbound access lists at S0 and S1 are configured to block Telnet traffic, and there is no outbound access list configured at E0. When the connection request for John's Telnet session passes through the firewall, CBAC creates a temporary opening in the inbound access list at S0 to permit returning Telnet traffic for John's Telnet session. (If the same access list is applied to both S0 and S1, the same opening would appear at both interfaces.) If necessary, CBAC would also have created a similar opening in an outbound access list at E0 to permit return traffic.

How CBAC Works—Details

This section describes how CBAC inspects packets and maintains state information about sessions to provide intelligent filtering.

Packets Are Inspected

With CBAC, you specify which protocols you want to be inspected, and you specify an interface and interface direction (in or out) where inspection originates. Only specified protocols will be inspected by CBAC. For these protocols, packets flowing through the firewall in any direction are inspected, as long as they flow through the interface where inspection originates.

Packets entering the firewall are inspected by CBAC only if they first pass the inbound access list at the interface. If a packet is denied by the access list, the packet is simply dropped and not inspected by CBAC.

CBAC inspects and monitors only the control channels of connections; the data channels (payload) are not inspected. For example, with a NetMeeting video conference, only the TCP connections used to establish the media channels are inspected; the media and media control channels for audio and video are not inspected or monitored.

CBAC inspection recognizes application-specific commands in the control channel, and detects and prevents certain application-level attacks.

A State Table Maintains Session State Information

Whenever a packet is inspected, a state table is updated to include information about the state of the packet's connection.

Return traffic will only be permitted back through the firewall if the state table contains information indicating that the packet belongs to a permissible session. When return traffic is inspected, the state table information is updated as necessary.

UDP "Sessions" Are Approximated

With UDP—a connectionless service—there are no actual sessions, so the software approximates sessions by examining the information in the packet and determining if the packet is similar to other UDP packets (for example, similar source/destination addresses and port numbers) and if the packet was detected soon after another similar UDP packet. "Soon" means within the configurable UDP idle timeout period.

Access List Entries Are Dynamically Created and Deleted to Permit Return Traffic

CBAC dynamically creates and deletes access list entries at the firewall interfaces, according to the information maintained in the state tables. These access list entries are applied to the interfaces to examine traffic flowing back into the internal network. These entries create temporary openings in the firewall to permit only traffic that is part of a permissible session.

The temporary access list entries are never saved to NVRAM.

When and Where to Configure CBAC

Use CBAC with:

- Standard TCP and UDP Internet applications
- Multimedia applications
- Oracle support

Use CBAC when you want to permit traffic for such applications only when the traffic session is initiated from a particular side of the firewall (usually from the protected internal network).

Configure CBAC at a firewall protecting an internal network. This firewall is a Cisco router with the Cisco Firewall feature set configured as described previously in the section "The Cisco IOS Firewall Feature Set."

In many cases, you will configure CBAC in one direction only at a single interface, which causes traffic to be permitted back into the internal network only if the traffic is part of a permissible (valid, existing) session.

In rare cases, you might want to configure CBAC in two directions at one or more interface, which is a more complex solution. CBAC is usually only configured in two directions when the networks on both sides of the firewall should be protected, such as with extranet or intranet configurations. For example, if the firewall is situated between two partner companies' networks, you might wish to restrict traffic in one direction for certain applications, and restrict traffic in the other direction for other applications.

The CBAC Process

This section describes an example sequence of events that occurs when CBAC is configured at an external interface that connects to an external network such as the Internet.

In this example, the following sequence of events occurs when a TCP packet leaves the internal network through the firewall's external interface. The TCP packet is the first in a session, and the packet's application layer protocol is configured for CBAC inspection:

- 1 The packet reaches the firewall's external interface.
- 2 The packet is evaluated against the interface's existing outbound access list, and the packet is permitted. (A denied packet would simply be dropped at this point.)
- 3 The packet is inspected by CBAC to determine and record information about the state of the packet's connection. This information is recorded in a new state table entry created for the new connection.

(If the packet's application was not configured for CBAC inspection, the packet would simply be forwarded out the interface at this point.)

- 4 Based on the obtained state information, CBAC creates a temporary access list entry which is inserted at the beginning of the external interface's inbound extended access list. This temporary access list entry is designed to permit inbound packets that are part of the same connection as the outbound packet just inspected.
- 5 The outbound packet is forwarded out the interface.
- 6 Later, an inbound packet reaches the interface. This packet is part of the connection previously established with the outbound packet. The inbound packet is evaluated against the inbound access list, and is permitted because of the temporary access list entry previously created.
- 7 The permitted inbound packet is inspected by CBAC, and the connection's state table entry is updated as necessary. Based on the updated state information, the inbound extended access list temporary entries might be modified, in order to permit only packets that are valid for the current state of the connection.
- 8 Any additional inbound or outbound packets that belong to the connection are inspected to update the state table entry and to modify the temporary inbound access list entries as required, and are forwarded through the interface.
- 9 When the connection terminates or times out, the connection's state table entry is deleted, and the connection's temporary inbound access list entries are deleted.

The example process just described only works if you have:

- An outbound IP access list (standard or extended) applied to the interface. This access list should permit all packets that you want to allow to exit the network, including packets you want to be inspected by CBAC.

- An inbound extended IP access list applied to the interface. This access list should deny any traffic to be inspected by CBAC. When CBAC is triggered with an outbound packet, CBAC creates a temporary opening in the inbound access list to permit only traffic that is part of a valid, existing session.

If the inbound access list permitted all traffic, CBAC would be creating pointless openings in the firewall for packets that would be permitted anyway.

Supported Protocols

You can configure CBAC to inspect

- all TCP sessions, regardless of the application-layer protocol (sometimes called “single-channel” or “generic” TCP inspection)
- all UDP sessions, regardless of the application-layer protocol (sometimes called “single-channel” or “generic” UDP inspection)

You can also configure CBAC to specifically inspect certain application-layer protocols. The following application-layer protocols can all be configured for CBAC:

- CU-SeeMe (only the White Pine version)
- FTP
- H.323 (such as NetMeeting, ProShare)
- Java
- UNIX R-commands (such as r-login, r-exec, and r-sh)
- RealAudio
- RPC (Sun RPC, not DCE RPC or Microsoft RPC)
- SMTP
- SQL*Net
- StreamWorks
- TFTP
- VDOLive

When a protocol is configured for CBAC, the protocol’s traffic will be inspected, state information will be maintained, and in general, packets will be allowed back through the firewall only if they belong to a permissible session.

Restrictions

CBAC is available only for IP protocol traffic. Only TCP and UDP packets are inspected. (Other IP traffic, such as ICMP, cannot be filtered with CBAC and should be filtered with basic access lists instead.)

You can use CBAC together with all the other firewall features mentioned previously in the section “The Cisco IOS Firewall Feature Set.”

CBAC works with fast switching and process switching.

If you reconfigure your access lists when you configure CBAC, be aware that if your access lists block TFTP traffic into an interface, you won't be able to netboot over that interface. (This is not a CBAC-specific limitation, but is part of existing access list functionality.)

Packets with the firewall as the source or destination address are not inspected by CBAC or evaluated by access lists.

CBAC ignores ICMP Unreachable messages.

FTP Traffic and CBAC

With FTP, CBAC does not allow third-part connections (three-way FTP transfer).

When CBAC inspects FTP traffic, it only allows data channels with the destination port in the range of 1024–65535.

CBAC won't open a data channel if the FTP client-server authentication fails.

Network Data Encryption and CBAC

If encrypted traffic is exchanged between two routers, and the firewall is in between the two routers, CBAC might not work as anticipated. This is because the packets' payloads are encrypted, and so CBAC cannot accurately inspect the payloads.

Also, if both encryption and CBAC are configured at the same firewall, CBAC will not work for certain protocols. In this case, CBAC will work with single-channel TCP and UDP, except for Java and SMTP. But CBAC will not work with multi-channel protocols, except for StreamWorks and CU-SeeMe. So if you configure encryption at the firewall, you should configure CBAC for only the following protocols:

- generic TCP
- generic UDP
- CU-SeeMe
- StreamWorks

Memory and Performance Impact

Using CBAC uses less than approximately 600 bytes of memory per connection. Because of the memory usage, you should use CBAC only when you need to. There is also a slight amount of additional processing that occurs whenever packets are inspected.

Configure Context-Based Access Control

If you try to configure context-based access control (CBAC) but do not have a good understanding of how CBAC works, you might inadvertently introduce security risks to the firewall and to the protected network. You should be sure you understand exactly what CBAC does before you configure CBAC..

To configure CBAC, you must complete the tasks described in the following sections:

- Pick an Interface: Internal or External
- Configure IP Access Lists at the Interface
- Configure Global Timeouts and Thresholds
- Define An Inspection Rule
- Apply the Inspection Rule to an Interface

Pick an Interface: Internal or External

You must decide whether to configure CBAC on an internal or external interface of your firewall.

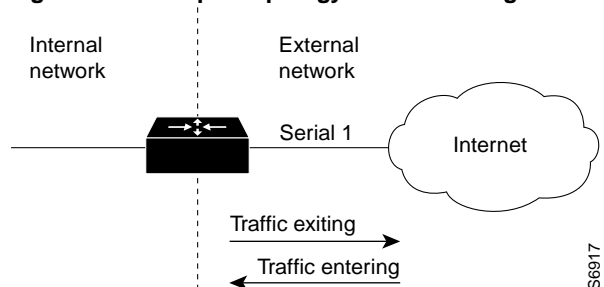
“Internal” refers to the side where sessions must originate for their traffic to be permitted through the firewall. “External” refers to the side where sessions cannot originate (sessions originating from the external side will be blocked).

If you will be configuring CBAC in two directions, you should configure CBAC in one direction first, using the appropriate “internal” and “external” interface designations. When you configure CBAC in the other direction, the interface designations will be swapped. (CBAC is rarely configured in two directions, and usually only when the firewall is between two networks that need protection from each other, such as with two partners’ networks connected by the firewall.)

The firewall is most commonly used with one of two basic network topologies. Determining which of these topologies is most like your own can help you decide whether to configure CBAC on an internal interface or with an external interface.

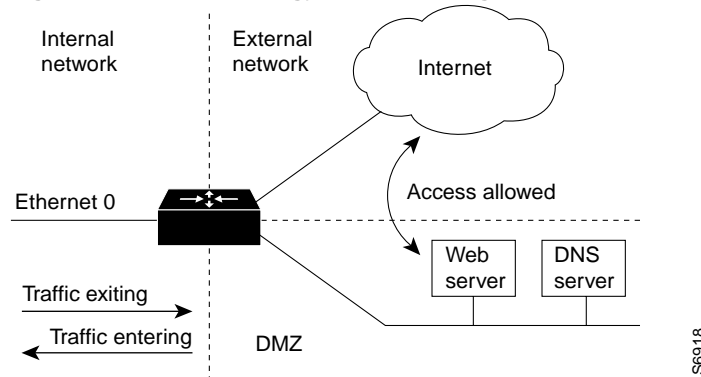
The first topology is shown in Figure 2. In this simple topology, CBAC is configured for the *external* interface Serial 1. This prevents specified protocol traffic from entering the firewall and the internal network, unless the traffic is part of a session initiated from within the internal network.

Figure 2 Simple Topology—CBAC Configured at the External Interface



The second topology is shown in Figure 3. In this topology, CBAC is configured for the *internal* interface Ethernet 0. This allows external traffic to access the services in the Demilitarized Zone (DMZ), such as DNS services, but prevents specified protocol traffic from entering your internal network—unless the traffic is part of a session initiated from within the internal network.

Figure 3 DMZ Topology—CBAC Configured at the Internal Interface



Using these two example topologies, decide whether to configure CBAC on an internal or external interface.

Configure IP Access Lists at the Interface

For CBAC to work properly, you need to make sure that you have IP access lists configured appropriately at the interface.

For temporary openings to be created in an access list, the access list must be an extended access list. So wherever you have access lists that will be applied to returning traffic, you must use extended access lists.

Also remember that all access lists that evaluate traffic leaving the protected network should permit traffic that will be inspected by CBAC.

If your firewall only has two connections, one to the internal network and one to the external network, using all inbound access lists works well because they stop packets before they get a chance to affect the router itself.

External Interface

Here are some tips for configuring CBAC on an external interface:

- The outbound IP access list at the external interface can be a standard or extended access list. This outbound access list should permit traffic that you want to be inspected by CBAC. If traffic is not permitted, it will not be inspected by CBAC, but will be simply dropped.
- The inbound IP access list at the external interface must be an extended access list. This inbound access list should deny traffic that you want to be inspected by CBAC. (CBAC will create temporary openings in this inbound access list as appropriate to permit only return traffic that is part of a valid, existing session.)
- For complete information about how to configure IP access lists, refer to the “Configuring IP” chapter of the Cisco IOS Release 11.2 *Network Protocols Configuration Guide, Part 1*.

Internal Interface

Here are some tips for configuring CBAC on an internal interface:

- The inbound IP access list at the internal interface and the outbound IP access list at external interface(s) can be a standard or extended access list. These access lists should permit traffic that you want to be inspected by CBAC. If traffic is not permitted, it will not be inspected by CBAC, but will be simply dropped.
- The outbound IP access list at the internal interface and the inbound IP access list at the external interface must be extended access lists. These outbound access lists should deny traffic that you want to be inspected by CBAC. (CBAC will create temporary openings in these outbound access lists as appropriate to permit only return traffic that is part of a valid, existing session.) You do not necessarily need to configure an extended access list at both the outbound internal interface and the inbound external interface, but at least one is necessary to restrict traffic flowing through the firewall into the internal protected network.
- For complete information about how to configure IP access lists, refer to the “Configuring IP” chapter of the Cisco IOS Release 11.2 *Network Protocols Configuration Guide, Part 1*.

Configure Global Timeouts and Thresholds

CBAC uses timeouts and thresholds to determine how long to manage state information for a session, and to determine when to drop sessions that do not become fully established. These timeouts and thresholds apply globally to all sessions.

You can use the default timeout and threshold values, or you can change to values more suitable to your security requirements. You should make any changes to the timeout and threshold values before you continue configuring CBAC.

All the available CBAC timeouts and thresholds are listed in the table below, along with the corresponding command and default value.

To change a global timeout or threshold listed in the left column, use the global configuration command in the middle column:

Timeout or Threshold Value to Change	Command	Default
The length of time the software waits for a TCP session to reach the established state before dropping the session.	ip inspect tcp synwait-time <i>seconds</i>	30 seconds
The length of time a TCP session will still be managed after the firewall detects a FIN-exchange.	ip inspect tcp finwait-time <i>seconds</i>	5 seconds
The length of time a TCP session will still be managed after no activity (the TCP idle timeout). ¹	ip inspect tcp idle-time <i>seconds</i>	3600 seconds (1 hour)
The length of time a UDP session will still be managed after no activity (the UDP idle timeout). ¹	ip inspect udp idle-time <i>seconds</i>	30 seconds
The length of time a DNS name lookup session will still be managed after no activity.	ip inspect dns-timeout <i>seconds</i>	5 seconds
The number of existing half-open sessions that will cause the software to start deleting half-open sessions. ²	ip inspect max-incomplete high <i>number</i>	500 existing half-open sessions
The number of existing half-open sessions that will cause the software to stop deleting half-open sessions. ²	ip inspect max-incomplete low <i>number</i>	400 existing half-open sessions

Timeout or Threshold Value to Change	Command	Default
The rate of new unestablished sessions that will cause the software to start deleting half-open sessions. ²	ip inspect one-minute high <i>number</i>	500 half-open sessions per minute
The rate of new unestablished sessions that will cause the software to stop deleting half-open sessions. ²	ip inspect one-minute low <i>number</i>	400 half-open sessions per minute
The number of existing half-open TCP sessions with the same destination host address that will cause the software to start dropping half-open sessions to the same destination host address. ³	ip inspect tcp max-incomplete host <i>number block-time seconds</i>	50 existing half-open TCP sessions; 0 seconds

1. The global TCP and UDP idle timeouts can be overridden for specified application layer protocols' sessions as described in the **ip inspect name (global configuration)** command description, found later in the section, "Context-Based Access Control Command Reference."
2. See the following section, "Half-Open Sessions," for more information.
3. Whenever the **max-incomplete host** threshold is exceeded, the software will drop half-open sessions differently depending on whether the **block-time** timeout is zero or a positive non-zero number. For details please refer to the complete command description later in this document.

To return any threshold or timeout to the default value, use the **no** form of the command in the preceding table.

Half-Open Sessions

An unusually high number of half-open sessions (either absolute or measured as the arrival rate) could indicate that a denial-of-service attack is occurring. For TCP, "half-open" means that the session has not reached the established state—the TDP three-way handshake has not yet been completed. For UDP, "half-open" means that the firewall has detected no return traffic.

CBAC measures both the total number of existing half-open sessions and the rate of session establishment attempts. Both TCP and UDP half-open sessions are counted in the total number and rate measurements. Measurements are made once a minute.

When the number of existing half-open sessions rises above a threshold (the **max-incomplete high** number), the software will delete half-open sessions as required to accommodate new connection requests. The software will continue to delete half-open requests as necessary, until the number of existing half-open sessions drops below another threshold (the **max-incomplete low** number).

When the rate of new connection attempts rises above a threshold (the **one-minute high** number), the software will delete half-open sessions as required to accommodate new connection attempts. The software will continue to delete half-open sessions as necessary, until the rate of new connection attempts drops below another threshold (the **one-minute low** number). The rate thresholds are measured as the number of new session connection attempts detected in the last one-minute sample period.

Define An Inspection Rule

After you configure global timeouts and thresholds, you must define an inspection rule. This rule specifies what IP traffic (which application-layer protocols) will be inspected by CBAC at an interface.

Normally, you define only one inspection rule. The only exception might occur if you want to enable CBAC in two directions as described earlier in the section “When and Where to Configure CBAC.” For CBAC configured in both directions at a single firewall interface, you should configure two rules, one for each direction.

An inspection rule should specify each desired application-layer protocol as well as generic TCP or generic UDP if desired. The inspection rule consists of a series of statements each listing a protocol and specifying the same inspection rule name.

To define an inspection rule, follow the instructions in the following sections:

- Configure Application-Layer Protocol Inspection
- Configure Generic TCP and UDP Inspection

Configure Application-Layer Protocol Inspection

Note If you want CBAC inspection to work with NetMeeting traffic (an H.323 application layer protocol), you must also configure inspection for TCP, as described later in the section “Configure Generic TCP and UDP Inspection.” This requirement exists because NetMeeting uses an additional TCP channel not in the H.323 specification.

To configure CBAC inspection for an application layer protocol, perform one or more of the following global configuration tasks:

Task	Command
<p>Configure CBAC inspection for an application layer protocol (except for RPC and Java). Use one of the protocol keywords defined in Table 1, following.</p> <p>Repeat this command for each desired protocol. Use the same <i>inspection-name</i> to create a single inspection rule.</p>	<p>ip inspect name <i>inspection-name</i> <i>protocol</i> [timeout <i>seconds</i>]</p>
<p>Enable CBAC inspection for the RPC application layer protocol.</p> <p>You can specify multiple RPC program numbers by repeating this command for each program number.</p> <p>Use the same <i>inspection-name</i> to create a single inspection rule.</p>	<p>ip inspect name <i>inspection-name</i> rpc program-number <i>number</i> [wait-time <i>minutes</i>] [timeout <i>seconds</i>]</p>

Refer to the description of the **ip inspect name (global configuration)** command in the “Context-Based Access Control Command Reference” section later in this document for complete information about how the command works with each application layer protocol.

To enable CBAC inspection for Java, see the following section, “Configure Java Inspection.”

Table 1 Application Protocol keywords

Application Protocol	<i>protocol</i> Keyword
CU-See-Me	cuseeme
FTP	ftp
H.323	h323
UNIX R commands (r-login, r-exec, r-sh)	rcmd
RealAudio	realaudio
SMTP	smtp
SQL*Net	sqlnet
StreamWorks	streamworks
TFTP	tftp
VDOLive	vdolive

Configure Java Inspection

With Java, you must protect against the risk of users inadvertently downloading destructive applets into your network. To protect against this risk, you could require all users to disable Java in their browser. If this is not an agreeable solution, you can use context-based access control (CBAC) to filter Java applets at the firewall, which allows users to download only applets residing within the firewall and trusted applets from outside 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 external sites except for those you specifically designate as hostile.)

To block all Java applets except for applets from friendly locations, perform the following global configuration tasks:

Task	Command
Create a standard access list that permits traffic only from friendly sites, and denies traffic from hostile sites.	ip access-list standard <i>name</i> permit ... deny ... (Use permit and deny statements as appropriate.)
If you want all internal users to be able to download friendly applets, use the any keyword for the destination as appropriate—but be careful to not misuse the any keyword to inadvertently allow all applets through.	or access-list <i>access-list-number</i> { deny permit } <i>source</i> [<i>source-wildcard</i>]
Block all Java applets except for applets from the friendly sites defined previously in the access list.	ip inspect <i>name</i> <i>inspection-name</i> http [java-list <i>access-list</i>] [timeout <i>seconds</i>]
Use the same <i>inspection-name</i> as when you specified other protocols, to create a single inspection rule.	



Caution 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, HTTP on a nonstandard port, etc.

Configure Generic 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 than 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 to the FTP state information.

With TCP and UDP inspection, packets entering the network must exactly match the corresponding packet that previously exited the network: the entering packets must have the same source/destination addresses and source/destination port numbers as the exiting packet (but reversed). Otherwise, the entering packets will be blocked at the interface. Also, all TCP packets with a sequence number outside of the window are dropped.

With TCP inspection configured, no application-layer data is inspected, and dynamic data connections will be dropped.

With UDP inspection configured, replies will only be permitted back in through the firewall if they are received within a configurable time after the last request was sent out. (This time is configured with the **ip inspect udp idle-time** command.)

To configure CBAC inspection for TCP or UDP packets, perform one or both of the following global configuration tasks:

Task	Command
Enable CBAC inspection for TCP packets. Use the same <i>inspection-name</i> as when you specified other protocols, to create a single inspection rule.	ip inspect name <i>inspection-name</i> tcp [timeout <i>seconds</i>]
Enable CBAC inspection for UDP packets. Use the same <i>inspection-name</i> as when you specified other protocols, to create a single inspection rule.	ip inspect name <i>inspection-name</i> udp [timeout <i>seconds</i>]

Apply the Inspection Rule to an Interface

After you define an inspection rule, you apply this rule to an interface.

Normally, you apply only one inspection rule to one interface. The only exception might occur if you want to enable CBAC in two directions as described earlier in the section “When and Where to Configure CBAC.” For CBAC configured in both directions at a single firewall interface, you should apply two rules, one for each direction.

If you are configuring CBAC on an external interface, apply the rules to outbound traffic.

If you are configuring CBAC on an internal interface, apply the rules to inbound traffic.

To apply a set of inspection rules to an interface, perform the following interface configuration task:

Task	Command
Apply a set of inspection rules to an interface.	ip inspect <i>inspection-name</i> {in out}

Display Configuration, Status, and Statistics for Context-Based Access Control

You can view certain context-based access control (CBAC) information by performing one or more of the following EXEC commands:

Task	Command
Show the CBAC inspection configuration.	show ip inspect config
Show the interface configuration with regards to the applied inspection rules and access lists.	show ip inspect interfaces
Show existing inspected sessions.	show ip inspect session [detail]
Show the configured inspection rules.	show ip inspect name <i>inspection-name</i>
Show all available information about CBAC inspection.	show ip inspect all

Debug Context-Based Access Control

If required, you can use the CBAC debug commands listed in this section. (Debugging can be turned off for each of the commands in this section by using the **no** form of the command, and to disable all debugging, use the privileged EXEC command **no debug all**.)

The available debug commands are listed in the following categories:

- Generic Debug Commands
- Transport Level Debug Commands
- Application Protocol Debug Commands

Generic Debug Commands

You can use the following generic debug commands, entered in privileged EXEC mode:

Task	Command
Enable the tracing of the function calls.	debug ip inspect function-trace
Enable the tracing of the object creations.	debug ip inspect object-creation
Enable the tracing of the object deletions.	debug ip inspect object deletion
Enable the tracing of important events.	debug ip inspect events
Enable the detailed option, which can be used in combination with other options to get additional information.	debug ip inspect details
Enable the tracing of timer events.	debug ip inspect timers

Transport Level Debug Commands

You can use the following transport-level debug commands, entered in privileged EXEC mode:

Task	Command
Enable the tracing of the TCP state machine and events	debug ip inspect tcp
Enable the tracing of the UDP events.	debug ip inspect udp

Application Protocol Debug Commands

You can use the following generic debug command, entered in privileged EXEC mode:

Task	Command
Enable the tracing of the protocol inspection.	debug ip inspect <i>protocol</i>
Refer to Table 2 to determine the protocol keyword.	

Table 2 Application Protocol Keywords for the debug ip inspect Command

Application Protocol	<i>protocol</i> keyword
CU-See-Me	cuseeme
FTP	ftp
FTP tokens (enables tracing of the ftp tokens parsed)	ftp-tokens
H.323	h323
UNIX R commands (r-login, r-exec, r-sh)	rcmd
RealAudio	realaudio
SMTP	smtp
SQL*Net	sqlnet
StreamWorks	streamworks
TFTP	tftp
VDOLive	vdolive
RPC	rpc
Java applets	http

Interpret Real-Time Alerts Generated by Context-Based Access Control

Context-based access control (CBAC) provides real-time alerts in the form of syslog messages. These messages can inform you that

- A denial-of-service attack is occurring
- An SMTP attack is occurring
- Java blocking has occurred

The real-time alerts also provide an audit trail to provide details about sessions inspected by CBAC.

The following types of messages can be generated by CBAC:

- Denial-of-Service Attack Detection Alert Messages
- SMTP Attack Detection Alert Messages
- Java Blocking Alert Messages
- Audit Trail Messages

Denial-of-Service Attack Detection Alert Messages

CBAC detects and blocks denial-of-service attacks, and notifies you with alert messages when denial-of-service attacks occur.

If you see messages similar to the following, a denial-of-service attack is probably occurring:

```
Sep  9 19:37:07 sifi-5 104: %FW-4-ALERT_ON: getting aggressive, count
(25/25) current 1-min rate: 103
Sep  9 19:37:37 sifi-5 105: %FW-4-ALERT_OFF: calming down, count (9/10)
current 1-min rate: 108
Sep  9 19:38:35 sifi-5 107: %FW-4-ALERT_ON: getting aggressive, count
(25/25) current 1-min rate: 99
Sep  9 19:39:10 sifi-5 108: %FW-4-ALERT_OFF: calming down, count (9/10)
current 1-min rate: 99
Sep  9 19:40:48 sifi-5 109: %FW-4-ALERT_ON: getting aggressive, count
(25/25) current 1-min rate: 94
Sep  9 19:41:24 sifi-5 110: %FW-4-ALERT_OFF: calming down, count (9/10)
current 1-min rate: 106
Sep  9 19:52:52 sifi-5 112: %FW-4-ALERT_ON: getting aggressive, count
(2/2147483647) current 1-min rate: 39
```

(Each “aggressive/calming” pair of messages indicate a separate attack.)

If you see messages similar to the following, a denial-of-service attack on a specific TCP host is probably occurring:

```
%FW-4-HOST_TCP_ALERT_ON: Max tcp half-open connections (5) exceeded for host
172.21.127.242.
%FW-4-BLOCK_HOST: Blocking new TCP connections to host 172.21.127.242 for 2 minutes
(half-open count 5 exceeded)
%FW-4-UNBLOCK_HOST: New TCP connections to host 172.21.127.242 no longer blocked
```

(For the example messages, the **block-time** timeout is set to 2 minutes (120 seconds) and the **max-incomplete host** number is set to 5 half-open sessions, using the **ip inspect tcp max-incomplete host** command.)

SMTP Attack Detection Alert Messages

CBAC detects and blocks SMTP attacks (illegal SMTP commands), and notifies you with alert messages when SMTP attacks occur.

If you see messages similar to the following messages, an SMTP attack is probably occurring:

```
Sep 23 19:58:07 sifi-5 22: %FW-4-SMTP_INVALID_COMMAND: Invalid SMTP
command from initiator (192.168.12.3:52419)
Sep 23 19:59:05 sifi-5 23: %FW-4-SMTP_INVALID_COMMAND: Invalid SMTP
command from initiator (192.168.12.3:52420)
```

Java Blocking Alert Messages

CBAC detects and selectively blocks Java applets, and notifies you when a Java applet has been blocked.

If you see messages similar to the following messages, Java applets have been blocked:

```
%FW-4-HTTP_JAVA_BLOCK: JAVA applet is blocked from (172.21.127.218:80) to
(171.69.57.30:44673) .
%FW-4-HTTP_JAVA_BLOCK: JAVA applet is blocked from (172.21.127.218:80) to
(171.69.57.30:44678) .
%FW-4-HTTP_JAVA_BLOCK: JAVA applet is blocked from (172.21.127.218:80) to
(171.69.57.30:44676) .
%FW-4-HTTP_JAVA_BLOCK: JAVA applet is blocked from (172.21.127.218:80) to
(171.69.57.30:44679) .
%FW-4-HTTP_JAVA_BLOCK: JAVA applet is blocked from (172.21.127.218:80) to
(171.69.57.30:44677) .
%FW-4-HTTP_JAVA_BLOCK: JAVA applet is blocked from (172.21.127.218:80) to
(171.69.57.30:44680) .
```

Audit Trail Messages

CBAC provides audit trail messages to record details about inspected sessions.

The following messages are examples of audit trail messages. To determine which protocol was inspected, use the responder's port number. The port number follows the responder's address.

```
Sep 10 13:02:19 sifi-5 124: %FW-6-SESS_AUDIT_TRAIL: tcp session initiator
(192.168.1.13:33192) sent 22 bytes -- responder (192.168.129.11:25) sent
208 bytes
Sep 10 13:07:33 sifi-5 125: %FW-6-SESS_AUDIT_TRAIL: ftp session initiator
(192.168.1.13:33194) sent 336 bytes -- responder (192.168.129.11:21) sent
325 bytes
Sep 10 13:08:26 sifi-5 126: %FW-6-SESS_AUDIT_TRAIL: tcp session initiator
(192.168.1.13:33195) sent 76 bytes -- responder (192.168.129.11:25) sent
167 bytes

%FW-6-SESS_AUDIT_TRAIL: http session initiator (171.69.57.30:44673) sent
1599 bytes -- responder (172.21.127.218:80) sent 93124 bytes
%FW-6-SESS_AUDIT_TRAIL: http session initiator (171.69.57.30:44678) sent
198 bytes -- responder (172.21.127.218:80) sent 288 bytes
%FW-6-SESS_AUDIT_TRAIL: http session initiator (171.69.57.30:44676) sent
1358 bytes -- responder (172.21.127.218:80) sent 55954 bytes
%FW-6-SESS_AUDIT_TRAIL: http session initiator (171.69.57.30:44679) sent
197 bytes -- responder (172.21.127.218:80) sent 288 bytes
%FW-6-SESS_AUDIT_TRAIL: http session initiator (171.69.57.30:44677) sent
1128 bytes -- responder (172.21.127.218:80) sent 131766 bytes
```

```
%FW-6-SESS_AUDIT_TRAIL: http session initiator (171.69.57.30:44680) sent  
195 bytes -- responder (172.21.127.218:80) sent 288 bytes
```

Turn Off Context-Based Access Control

If you so desire, you can turn off context-based access control (CBAC), with the **no ip inspect** global configuration command.

Note The **no ip inspect** command removes all CBAC configuration entries and resets all CBAC global timeouts and thresholds to the defaults.

Context-Based Access Control Configuration Example

This example configuration file shows a firewall configured with CBAC. The firewall is positioned in between a protected field office's internal network, and a WAN connection to the corporate headquarters. CBAC is configured on the firewall in order to protect the internal network from potential network threats coming from the WAN side.

The firewall has 2 interfaces configured:

- Ethernet 0 connects to the internal protected network
- Serial 0 connects to the WAN with Frame Relay

```

!-----
! This first section contains some configuration that is not required for CBAC,
! but illustrates good security practices. Note that there are no services
! on the Ethernet side. Email is picked up via POP from a server on the corporate
! side.
!-----
!
!
version 11.2
!
! The following three commands should appear in almost every config
!
service password-encryption
service udp-small-servers
no service tcp-small-servers
!
hostname fred-examplecorp-fr
!
boot system flash c1600-fw1600-l
enable secret 5 <elided>
!
username fred password <elided>
ip subnet-zero
no ip source-route
ip domain-name example.com
ip name-server 172.19.2.132
ip name-server 198.92.30.32
!
!
!-----
!The next section includes configuration required specifically for CBAC
!-----
!
!The following commands define the inspection rule "myfw", allowing
! the specified protocols to be inspected. Note that Java applets will be permitted
! according to access list 51, defined later in this configuration.
!
ip inspect name myfw cuseeme timeout 3600
ip inspect name myfw ftp timeout 3600
ip inspect name myfw http java-list 51 timeout 3600
ip inspect name myfw rcmd timeout 3600
ip inspect name myfw realaudio timeout 3600
ip inspect name myfw smtp timeout 3600
ip inspect name myfw tftp timeout 30
ip inspect name myfw udp timeout 15
ip inspect name myfw tcp timeout 3600
!

```

Context-Based Access Control Configuration Example

```
!The following interface configuration applies the "myfw" inspection rule to
! inbound traffic at Ethernet 0. Since this interface is on the internal network
! side of the firewall, traffic entering Ethernet 0 is actually exiting the
! internal network.
!Applying the inspection rule to this interface causes inbound traffic (which is
! exiting the network) to be inspected; return traffic will only be permitted back
! through the firewall if part of a session which began from within the network.
!Also note that access list 101 is applied to inbound traffic at Ethernet 0.
! Any traffic that passes the access list will be inspected by CBAC.
! (Traffic blocked by the access list will not be inspected.)
!
interface Ethernet0
  description ExampleCorp Ethernet chez fred
  ip address 172.19.139.1 255.255.255.248
  ip broadcast-address 172.19.131.7
  no ip directed-broadcast
  no ip proxy-arp
  ip inspect myfw in
  ip access-group 101 in
  no ip route-cache
  no cdp enable
!
interface Serial0
  description Frame Relay (Telco ID 22RTQQ062438-001) to ExampleCorp HQ
  no ip address
  ip broadcast-address 0.0.0.0
  encapsulation frame-relay IETF
  no ip route-cache
  no arp frame-relay
  bandwidth 56
  service-module 56k clock source line
  service-module 56k network-type dds
  frame-relay lmi-type ansi
!
!Note that the following interface configuration applies access list 111 to
! inbound traffic at the external serial interface. (Inbound traffic is
! entering the network.) When CBAC inspection occurs on traffic exiting the
! network, temporary openings will be added to access list 111 to allow returning
! traffic that is part of existing sessions.
!
interface Serial0.1 point-to-point
  ip unnumbered Ethernet0
  ip access-group 111 in
  no ip route-cache
  bandwidth 56
  no cdp enable
  frame-relay interface-dlci 16
!
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0.1
!
!The following access list defines "friendly" and "hostile" sites for Java
! applet blocking. Because Java applet blocking is defined in the inspection
! rule "myfw" and references access list 51, applets will be actively denied
! if they are from any of the "deny" addresses and allowed only if they are from
! either of the two "permit" networks.
!
access-list 51 deny 172.19.1.203
access-list 51 deny 172.19.2.147
access-list 51 permit 172.18.0.0 0.1.255.255
access-list 51 permit 192.168.1.0 0.0.0.255
access-list 51 deny any
```

```

!
!The following access list 101 is applied to interface Ethernet 0 above.
! This access list permits all traffic that should be CBAC inspected, and also
! provides anti-spoofing. The access list is deliberately set up to deny unknown
! IP protocols, because no such unknown protocols will be in legitimate use.
!
access-list 101 permit tcp 172.19.139.0 0.0.0.7 any
access-list 101 permit udp 172.19.139.0 0.0.0.7 any
access-list 101 permit icmp 172.19.139.0 0.0.0.7 any
access-list 101 deny ip any any
!
!The following access list 111 is applied to interface Serial 0.1 above.
! This access list filters traffic coming in from the external side. When
! CBAC inspection occurs, temporary openings will be added to the beginning of
! this access list to allow return traffic back into the internal network.
!This access list should restrict traffic that will be inspected by
! CBAC. (Remember that CBAC will open holes as necessary to permit returning traffic.)
!Comments precede each access list entry. These entries aren't all specifically related
! to CBAC, but are created to provide general good security.
!
! Anti-spoofing.
access-list 111 deny ip 172.19.139.0 0.0.0.7 any
! Port 22 is SSH... encrypted, RSA-authenticated remote login. Can be used to get to field
! office host from ExampleCorp headquarters.
access-list 111 permit tcp any host 172.19.139.2 eq 22
! Sometimes EIGRP is run on the Frame Relay link. When you use an
! input access list, you have to explicitly allow even control traffic.
! This could be more restrictive, but there would have to be entries
! for the EIGRP multicast as well as for the office's own unicast address.
access-list 111 permit igmp any any
! These are the ICMP types actually used...
! administratively-prohibited is useful when you're trying to figure out why
! you can't reach something you think you should be able to reach.
access-list 111 permit icmp any 172.19.139.0 0.0.0.7 administratively-prohibited
! This allows network admins at headquarters to ping hosts at the field office:
access-list 111 permit icmp any 172.19.139.0 0.0.0.7 echo
! This allows the field office to do outgoing pings
access-list 111 permit icmp any 172.19.139.0 0.0.0.7 echo-reply
! Path MTU discovery requires too-big messages
access-list 111 permit icmp any 172.19.139.0 0.0.0.7 packet-too-big
! Outgoing traceroute requires time-exceeded messages to come back
access-list 111 permit icmp any 172.19.139.0 0.0.0.7 time-exceeded
! Incoming traceroute
access-list 111 permit icmp any 172.19.139.0 0.0.0.7 traceroute
! Permits all unreachable because if you are trying to debug
! things from the remote office, you want to see them. If nobody ever did
! any debugging from the network, it would be more appropriate to permit only
! port unreachables or no unreachables at all.
access-list 111 permit icmp any 172.19.139.0 0.0.0.7 unreachable
! These next two entries permit users on most ExampleCorp networks to telnet to
! a host in the field office. This is for remote administration by the network admins.
access-list 111 permit tcp 172.18.0.0 0.1.255.255 host 172.19.139.1 eq telnet
access-list 111 permit tcp 192.168.1.0 0.0.0.255 host 172.19.139.1 eq telnet
! Final deny for explicitness
access-list 111 deny ip any any
!
no cdp run
snmp-server community <elided> RO
!
line con 0
 exec-timeout 0 0
 password <elided>
 login local

```

Context-Based Access Control Configuration Example

```
line vty 0
  exec-timeout 0 0
  password <elided>
  login local
  length 35
line vty 1
  exec-timeout 0 0
  password 7 <elided>
  login local
line vty 2
  exec-timeout 0 0
  password 7 <elided>
  login local
line vty 3
  exec-timeout 0 0
  password 7 <elided>
  login local
line vty 4
  exec-timeout 0 0
  password 7 <elided>
  login local
!
scheduler interval 500
end
```

Context-Based Access Control Command Reference

This section documents the new commands that implement CBAC.

This section does *not* include **show** and **debug** command descriptions. For a list of available **show** and **debug** commands, refer to the previous sections, “Display Configuration, Status, and Statistics for Context-Based Access Control” and “Debug Context-Based Access Control,” respectively.

The existing access list commands are documented in the Cisco IOS Release 11.3 command references.

This section documents the following commands:

- **ip inspect dns-timeout**
- **ip inspect (interface configuration)**
- **ip inspect max-incomplete high**
- **ip inspect max-incomplete low**
- **ip inspect name (global configuration)**
- **ip inspect one-minute high**
- **ip inspect one-minute low**
- **ip inspect tcp finwait-time**
- **ip inspect tcp max-incomplete host**
- **ip inspect tcp synwait-time**
- **ip inspect tcp idle-time**
- **ip inspect udp idle-time**
- **no ip inspect**

ip inspect dns-timeout

To specify the DNS idle timeout (the length of time a DNS name lookup session will still be managed after no activity), use the **ip inspect dns-timeout** global configuration command. Use the **no** form of this command to reset the timeout to the default of 5 seconds.

```
ip inspect dns-timeout seconds  
no ip inspect dns-timeout
```

Syntax Description

seconds Specifies the length of time a DNS name lookup session will still be managed after no activity.

Default

5 seconds

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.2P.

When the software detects a valid UDP packet for a new DNS name lookup session, if context-based access control (CBAC) inspection is configured for UDP, the software establishes state information for the new DNS session.

If the software detects no packets for the DNS session for a time period defined by the DNS idle timeout, the software will not continue to manage state information for the session.

The DNS idle timeout applies to all DNS name lookup sessions inspected by CBAC.

The DNS idle timeout value always overrides the global UDP timeout. The DNS idle timeout value also always overrides any timeouts specified for specific interfaces when you define a set of inspection rules with the **ip inspect name (global configuration)** command.

Examples

The following example sets the DNS idle timeout to 30 seconds:

```
ip inspect dns-timeout 30
```

The following example sets the DNS idle timeout back to the default (5 seconds):

```
no ip inspect dns-timeout
```

ip inspect (interface configuration)

To apply a set of inspection rules to an interface, use the **ip inspect** interface configuration command. Use the **no** form of this command to remove the set of rules from the interface.

```
ip inspect inspection-name {in | out}  
no ip inspect inspection-name {in | out}
```

Syntax Description

inspection-name Identifies which set of inspection rules to apply.

in Applies the inspection rules to inbound traffic.

out Applies the inspection rules to outbound traffic.

Default

If no set of inspection rules is applied to an interface, no traffic will be inspected by CBAC.

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.2P.

Use this command to apply a set of inspection rules to an interface.

Typically, if the interface connects to the external network, you apply the inspection rules to outbound traffic; alternately, if the interface connects to the internal network, you apply the inspection rules to inbound traffic.

If you apply the rules to outbound traffic, then return inbound packets will be permitted if they belong to a valid connection with existing state information. This connection had to have initiated with an outbound packet.

If you apply the rules to inbound traffic, then return outbound packets will be permitted if they belong to a valid connection with existing state information. This connection had to have initiated with an inbound packet.

Example

The following example applies a set of inspection rules named “outboundrules” to an external interface’s outbound traffic. This causes inbound IP traffic to be permitted only if the traffic is part of an existing session, and to be denied if the traffic is not part of an existing session.

```
interface serial0  
ip inspect outboundrules out
```

Related Commands

ip inspect name (global configuration)

ip inspect max-incomplete high

To define the number of existing half-open sessions that will cause the software to start deleting half-open sessions, use the **ip inspect max-incomplete high** global configuration command. Use the **no** form of this command to reset the threshold to the default of 500 half-open sessions.

```
ip inspect max-incomplete high number  
no ip inspect max-incomplete high
```

Syntax Description

number Specifies the number of existing half-open sessions that will cause the software to start deleting half-open sessions.

(This number must be greater than the **max-incomplete low** threshold specified with the **ip inspect max-incomplete low** command.)

Default

500 half-open sessions

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.2P.

An unusually high number of half-open sessions (either absolute or measured as the arrival rate) could indicate that a denial-of-service attack is occurring. For TCP, “half-open” means that the session has not reached the established state. For UDP, “half-open” means that the firewall only has detected traffic from one direction only.

Context-based access control (CBAC) measures both the total number of existing half-open sessions and the rate of session establishment attempts. Both TCP and UDP half-open sessions are counted in the total number and rate measurements. Measurements are made once a minute.

When the number of existing half-open sessions rises above a threshold (the **max-incomplete high** number), the software will delete half-open sessions as required to accommodate new connection requests. The software will continue to delete half-open requests as necessary, until the number of existing half-open sessions drops below another threshold (the **max-incomplete low** number).

The global value specified for this threshold applies to all TCP and UDP connections inspected by CBAC.

Interaction Between the **max-incomplete high** and **max-incomplete low** Values

The CBAC software ensures that the **max-incomplete high** number is always greater than or equal to the **max-incomplete low** number (specified with the **ip inspect max-incomplete low** command).

If you try to set the **max-incomplete high** number to lower than the current **max-incomplete low** number, the software will not accept your command and will display an error message.

However, if you use the **no ip inspect max-incomplete high** command, the software *will* reset the **max-incomplete high** number to the default of 500, even if the current **max-incomplete low** number is greater than 500. In this case, the software will reset the **low** number to 500 and then reset the **high** number to 500.

Examples

The following example causes the software to start deleting half-open sessions when the number of existing half-open sessions rises above 900, and to stop deleting half-open sessions with the number of existing half-open sessions drops below 800:

```
ip inspect max-incomplete high 900
ip inspect max-incomplete low 800
```

If you then try to set the **high** value to 400, the software will disallow it, because the **low** value is 800 (higher than 400).

If you then reset the **high** value to the default of 500 using the **no** form of the command, the software will reset both **high** and **low** values to 500:

```
no ip inspect max-incomplete high
```

Related Commands

ip inspect max-incomplete low

ip inspect max-incomplete low

To define the number of existing half-open sessions that will cause the software to stop deleting half-open sessions, use the **ip inspect max-incomplete low** global configuration command. Use the **no** form of this command to reset the threshold to the default of 400 half-open sessions.

```
ip inspect max-incomplete low number  
no ip inspect max-incomplete low
```

Syntax Description

number Specifies the number of existing half-open sessions that will cause the software to stop deleting half-open sessions.

(This number must be lower than the **max-incomplete high** threshold specified with the **ip inspect max-incomplete high** command.)

Default

400 half-open sessions

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.2P.

An unusually high number of half-open sessions (either absolute or measured as the arrival rate) could indicate that a denial-of-service attack is occurring. For TCP, “half-open” means that the session has not reached the established state. For UDP, “half-open” means that the firewall only has detected traffic from one direction only.

Context-based access control (CBAC) measures both the total number of existing half-open sessions and the rate of session establishment attempts. Both TCP and UDP half-open sessions are counted in the total number and rate measurements. Measurements are made once a minute.

When the number of existing half-open sessions rises above a threshold (the **max-incomplete high** number), the software will delete half-open sessions as required to accommodate new connection requests. The software will continue to delete half-open requests as necessary, until the number of existing half-open sessions drops below another threshold (the **max-incomplete low** number).

The global value specified for this threshold applies to all TCP and UDP connections inspected by CBAC.

Interaction Between the **max-incomplete high** and **max-incomplete low** Values

The CBAC software ensures that the **max-incomplete high** number is always greater than or equal to the **max-incomplete low** number (specified with the **ip inspect max-incomplete low** command).

If you try to set the **max-incomplete low** number to higher than the current **max-incomplete high** number, the software will not accept your command and will display an error message.

However, if you use the **no ip inspect max-incomplete low** command, the software *will* reset the **max-incomplete low** number to the default of 400, even if the current **max-incomplete high** number is less than 400. In this case, the software will reset the **high** number to 400 and then reset the **low** number to 400.

Examples

The following example causes the software to start deleting half-open sessions when the number of existing half-open sessions rises above 900, and to stop deleting half-open sessions with the number of existing half-open sessions drops below 800:

```
ip inspect max-incomplete high 900
ip inspect max-incomplete low 800
```

Related Commands

ip inspect max-incomplete high

ip inspect name (global configuration)

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

ip inspect name *inspection-name protocol* [**timeout** *seconds*]

or

ip inspect name *inspection-name http* [**java-list** *access-list*] [**timeout** *seconds*]

(Java protocol only)

or

ip inspect name *inspection-name rpc program-number number* [**wait-time** *minutes*] [**timeout** *seconds*] (RPC protocol only)

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

no ip inspect name (removes the entire set of inspection rules)

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.
<i>protocol</i>	Specify a protocol according to Table 3 below.
timeout <i>seconds</i>	(Optional) To override the global TCP or UDP idle timeouts for the specified protocol, specify the number of seconds for a different idle timeout. This timeout overrides the global TCP and UDP timeouts but will not override the global DNS timeout.
java-list <i>access-list</i>	This argument is available only for the HTTP protocol, for Java applet blocking. Specify the access list (name or number) to use to determine “friendly” sites.
program-number <i>number</i>	(Optional) This argument is available only for the RPC protocol. Specify the program number to permit.
wait-time <i>minutes</i>	(Optional) This argument is available only for the RPC protocol. Specify 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.

Table 3 Protocol keywords

Protocol	<i>protocol</i> Keyword
Transport Layer Protocols	
TCP	tcp
UDP	udp
Application-Layer Protocols	

Table 3 Protocol keywords (Continued)

Protocol	<i>protocol</i> Keyword
CU-See-Me	cuseeme
FTP	ftp
Java (see the section “Java Inspection” following)	http
H.323 (see the section “H.323 Inspection,” following)	h323
UNIX R commands (r-login, r-exec, r-sh)	rcmd
RealAudio	realaudio
RPC (see the section, “RPC Inspection,” following)	rpc
SMTP (see the section, “SMTP Inspection,” following)	smtp
SQL*Net	sqlnet
StreamWorks	streamworks
TFTP	tftp
VDOLive	vdolive

Default

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

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.2P.

To define a set of inspection rules, enter this command for each protocol that you want context-based access control (CBAC) to inspect, using the same *inspection-name*. Give each set of inspection rules a unique *inspection-name*. 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 or UDP 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.

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 than 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 the corresponding packet that previously exited the network: the entering packets must have the same source/destination addresses and source/destination port numbers as the exiting packet (but reversed). Otherwise, the entering packets will be blocked at the interface. Also, all TCP packets with a sequence number outside of the window are dropped.

Application-Layer Protocol Inspection

In general, if you configure inspection for an application-layer protocol, packets for that protocol will be permitted to exit the firewall, 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 and to determine if that packet belongs to a valid existing session.

Java, H.323, RPC, and SMTP, and SQL*Net inspection have additional information, described in the next three sections.

Java Inspection

With Java, you must protect against the risk of users inadvertently downloading destructive applets into your network. To protect against this risk, you could require all users to disable Java in their browser. If this is not an agreeable solution, you can use CBAC to filter Java applets at firewall, which allows users to download only applets residing within the firewall and trusted applets from outside the firewall.

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 for sites specifically designated as “hostile.”

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



Caution 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, HTTP on a nonstandard port, etc.

H.323 Inspection

If you want CBAC inspection to work with NetMeeting traffic (an H.323 application layer protocol), you must also configure inspection for TCP, as described later in the section “Configure Generic TCP and UDP Inspection.” This requirement exists because NetMeeting uses an additional TCP channel not 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.

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
- EHLO
- EXPN
- HELO
- HELP
- MAIL
- NOOP
- QUIT
- RCPT
- RSET
- SAML
- SEND
- SOML
- TURN
- VRFY

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 that the set of inspection rules is applied to.

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.

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 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
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
```

Related Commands

ip inspect (interface configuration)

ip inspect one-minute high

To define the rate of new unestablished sessions that will cause the software to start deleting half-open sessions, use the **ip inspect one-minute high** global configuration command. Use the **no** form of this command to reset the threshold to the default of 900 half-open sessions.

```
ip inspect one-minute high number  
no ip inspect one-minute high
```

Syntax Description

number Specifies the rate of new unestablished TCP sessions that will cause the software to start deleting half-open sessions.

(This number must be greater than the **one-minute low** threshold specified with the **ip inspect one-minute low** command.)

Default

900 half-open sessions

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.2P.

An unusually high number of half-open sessions (either absolute or measured as the arrival rate) could indicate that a denial-of-service attack is occurring. For TCP, “half-open” means that the session has not reached the established state. For UDP, “half-open” means that the firewall only has detected traffic from one direction only.

Context-based access control (CBAC) measures both the total number of existing half-open sessions and the rate of session establishment attempts. Both TCP and UDP half-open sessions are included in the total number and rate measurements. Measurements are made once a minute.

When the rate of new connection attempts rises above a threshold (the **one-minute high** number), the software will delete half-open sessions as required to accommodate new connection attempts. The software will continue to delete half-open sessions as necessary, until the rate of new connection attempts drops below another threshold (the **one-minute low** number). The rate thresholds are measured as the number of new session connection attempts detected in the last one-minute sample period.

The global value specified for this threshold applies to all TCP and UDP connections inspected by CBAC.

Interaction Between the **one-minute high** and **one-minute low** Values

The CBAC software ensures that the **one-minute high** number is always greater than or equal to the **one-minute low** number (specified with the **ip inspect one-minute low** command).

If you try to set the **one-minute high** number to lower than the current **one-minute low** number, the software will not accept your command and will display an error message.

However, if you use the **no ip inspect one-minute high** command, the software *will* reset the **one-minute high** number to the default of 900, even if the current **one-minute low** number is greater than 900. In this case, the software will reset the **low** number to 900 and then reset the **high** number to 900.

Examples

The following example causes the software to start deleting half-open sessions when more than 1000 session establishment attempts have been detected in the last minute, and to stop deleting half-open sessions when fewer than 950 session establishment attempts have been detected in the last minute:

```
ip inspect one-minute high 1000
ip inspect one-minute low 950
```

Related Commands

ip inspect one-minute low

ip inspect one-minute low

To define the rate of new unestablished TCP sessions that will cause the software to stop deleting half-open sessions, use the **ip inspect one-minute low** global configuration command. Use the **no** form of this command to reset the threshold to the default of 400 half-open sessions.

```
ip inspect one-minute low number  
no ip inspect one-minute low
```

Syntax Description

number Specifies the rate of new unestablished TCP sessions that will cause the software to stop deleting half-open sessions.

(This number must be lower than the **one-minute high** threshold specified with the **ip inspect one-minute high** command.)

Default

400 half-open sessions

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.2P.

An unusually high number of half-open sessions (either absolute or measured as the arrival rate) could indicate that a denial-of-service attack is occurring. For TCP, “half-open” means that the session has not reached the established state. For UDP, “half-open” means that the firewall only has detected traffic from one direction only.

Context-based access control (CBAC) measures both the total number of existing half-open sessions and the rate of session establishment attempts. Both TCP and UDP half-open sessions are included in the total number and rate measurements. Measurements are made once a minute.

When the rate of new connection attempts rises above a threshold (the **one-minute high** number), the software will delete half-open sessions as required to accommodate new connection attempts. The software will continue to delete half-open sessions as necessary, until the rate of new connection attempts drops below another threshold (the **one-minute low** number). The rate thresholds are measured as the number of new session connection attempts detected in the last one-minute sample period.

The global value specified for this threshold applies to all TCP and UDP connections inspected by CBAC.

Interaction Between the **one-minute high** and **one-minute low** Values

The CBAC software ensures that the **one-minute high** number is always greater than or equal to the **one-minute low** number (specified with the **ip inspect one-minute low** command).

If you try to set the **one-minute low** number to higher than the current **one-minute high** number, the software will not accept your command and will display an error message.

However, if you use the **no ip inspect one-minute low** command, the software *will* reset the **one-minute low** number to the default of 400, even if the current **one-minute high** number is less than 400. In this case, the software will reset the **high** number to 400 and then reset the **low** number to 400.

Examples

The following example causes the software to start deleting half-open sessions when more than 1000 session establishment attempts have been detected in the last minute, and to stop deleting half-open sessions when fewer than 950 session establishment attempts have been detected in the last minute:

```
ip inspect one-minute high 1000
ip inspect one-minute low 950
```

Related Commands

ip inspect one-minute high

ip inspect tcp finwait-time

To define how long a TCP session will still be managed after the firewall detects a FIN-exchange, use the **ip inspect tcp finwait-time** global configuration command. Use the **no** form of this command to reset the timeout to the default of 5 seconds.

```
ip inspect tcp finwait-time seconds  
no ip inspect tcp finwait-time
```

Syntax Description

seconds Specifies how long a TCP session will be managed after the firewall detects a FIN-exchange.

Default

5 seconds

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.2P.

When the software detects a valid TCP packet that is the first in a session, if context-based access control (CBAC) inspection is configured for the packet's protocol, the software establishes state information for the new session.

Use this command to define how long TCP session state information will be maintained after the firewall detects a FIN-exchange for the session. The FIN-exchange occurs when the TCP session is ready to close.

The global value specified for this timeout applies to all TCP sessions inspected by CBAC.

The timeout set with this command is referred to as the "finwait" timeout.

Note If the -n option is used with rsh, and the commands being executed do not produce output before the "finwait" timeout, the session will be dropped and no further output will be seen.

Examples

The following example changes the "finwait" timeout to 10 seconds:

```
ip inspect tcp finwait-time 10
```

The following example changes the "finwait" timeout back to the default (5 seconds):

```
no ip inspect tcp finwait-time
```

ip inspect tcp max-incomplete host

To specify threshold and timeout values for TCP host-specific denial-of-service detection and prevention, use the **ip inspect tcp max-incomplete host** global configuration command. Use the **no** form of this command to reset the threshold and timeout to the default values.

```
ip inspect tcp max-incomplete host number block-time seconds  
no ip inspect tcp max-incomplete host
```

Syntax Description

<i>number</i>	Specifies how many half-open TCP sessions with the same host destination address can exist at a time, before the software starts deleting half-open sessions to the host. Use a number from 1 to 250.
<i>seconds</i>	Specifies how long the software will continue to delete new connection requests to the host.

Default

50 half-open sessions and 0 seconds.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.2P.

An unusually high number of half-open sessions with the same destination host address could indicate that a denial-of-service attack is being launched against the host. For TCP, “half-open” means that the session has not reached the established state.

Whenever the number of half-open sessions with the same destination host address rises above a threshold (the **max-incomplete host** number), the software will delete half-open sessions according to one of the following methods:

- If the **block-time** *seconds* timeout is 0 (the default):
The software will delete the oldest existing half-open session for the host for every new connection request to the host. This ensures that the number of half-open sessions to a given host will never exceed the threshold.
- If the **block-time** *seconds* timeout is greater than 0:
The software will delete all existing half-open sessions for the host, and then block all new connection requests to the host. The software will continue to block all new connection requests until the **block-time** expires.

The software also sends syslog messages whenever the **max-incomplete host** number is exceeded.

The global values specified for the threshold and timeout apply to all TCP connections inspected by CBAC.

Examples

The following example changes the **max-incomplete host** number to 40 half-open sessions, and changes the **block-time** timeout to 2 minutes (120 seconds):

```
ip inspect tcp max-incomplete host 40 block-time 120
```

The following example resets the defaults (50 half-open sessions and 0 seconds):

```
no ip inspect tcp max-incomplete host
```

ip inspect tcp synwait-time

To define how long the software will wait for a TCP session to reach the established state before dropping the session, use the **ip inspect tcp synwait-time** global configuration command. Use the **no** form of this command to reset the timeout to the default of 30 seconds.

```
ip inspect tcp synwait-time seconds  
no ip inspect tcp synwait-time
```

Syntax Description

seconds Specifies how long the software will wait for a TCP session to reach the established state before dropping the session.

Default

30 seconds

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.2P.

Use this command to define how long software will wait for a TCP session to reach the established state before dropping the session. The session is considered to have reached the established state after the session's first SYN bit is detected.

The global value specified for this timeout applies to all TCP sessions inspected by context-based access control (CBAC).

Examples

The following example changes the "synwait" timeout to 20 seconds:

```
ip inspect tcp synwait-time 20
```

The following example changes the "synwait" timeout back to the default (30 seconds):

```
no ip inspect tcp synwait-time
```

ip inspect tcp idle-time

To specify the TCP idle timeout (the length of time a TCP session will still be managed after no activity), use the **ip inspect tcp idle-time** global configuration command. Use the **no** form of this command to reset the timeout to the default of 3600 seconds (1 hour).

```
ip inspect tcp idle-time seconds  
no ip inspect tcp idle-time
```

Syntax Description

seconds Specifies the length of time a TCP session will still be managed after no activity.

Default

3600 seconds (1 hour)

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.2P.

When the software detects a valid TCP packet that is the first in a session, if context-based access control (CBAC) inspection is configured for the packet's protocol, the software establishes state information for the new session.

If the software detects no packets for the session for a time period defined by the TCP idle timeout, the software will not continue to manage state information for the session.

The global value specified for this timeout applies to all TCP sessions inspected by CBAC. This global value can be overridden for specific interfaces when you define a set of inspection rules with the **ip inspect name (global configuration)** command.

Note This command does not affect any of the currently defined inspection rules. If you change the TCP idle timeout with this command, this timeout will apply only to any new inspection rules you define.

Examples

The following example sets the global TCP idle timeout to 1800 seconds (30 minutes):

```
ip inspect tcp idle-time 1800
```

The following example sets the global TCP idle timeout back to the default of 3600 seconds (one hour):

```
no ip inspect tcp idle-time
```

ip inspect udp idle-time

To specify the UDP idle timeout (the length of time a UDP “session” will still be managed after no activity), use the **ip inspect udp idle-time** global configuration command. Use the **no** form of this command to reset the timeout to the default of 30 seconds.

```
ip inspect udp idle-time seconds  
no ip inspect udp idle-time
```

Syntax Description

seconds Specifies the length of time a UDP “session” will still be managed after no activity.

Default

30 seconds

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.2P.

When the software detects a valid UDP packet, if context-based access control (CBAC) inspection is configured for the packet’s protocol, the software establishes state information for a new UDP “session.” Because UDP is a connectionless service, there are no actual sessions, so the software approximates sessions by examining the information in the packet and determining if the packet is similar to other UDP packets (for example, similar source/destination addresses) and if the packet was detected soon after another similar UDP packet.

If the software detects no UDP packets for the UDP session for the a period of time defined by the UDP idle timeout, the software will not continue to manage state information for the session.

The global value specified for this timeout applies to all UDP sessions inspected by CBAC. This global value can be overridden for specific interfaces when you define a set of inspection rules with the **ip inspect name (global configuration)** command.

Note This command does not affect any of the currently defined inspection rules. If you change the UDP idle timeout with this command, this timeout will apply only to any new inspection rules you define.

Examples

The following example sets the global UDP idle timeout to 120 seconds (2 minutes):

```
ip inspect udp idle-time 120
```

The following example sets the global UDP idle timeout back to the default of 30 seconds:

```
no ip inspect udp idle-time
```

no ip inspect

To turn off context-based access control (CBAC) completely at a firewall use the **no ip inspect** global configuration command.

no ip inspect

Syntax Description

This command has no arguments or keywords.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.2P.

If you so desire, you can turn off CBAC, with the **no ip inspect** global configuration command.

Note The **no in inspect** command removes all CBAC configuration entries and resets all CBAC global timeouts and thresholds to the defaults.

Example

The following example turns off CBAC at a firewall:

```
no ip inspect
```

