

# Cisco IOS Firewall Feature Set

---

## Feature Summary

This document describes how you can configure your Cisco networking device to function as a firewall, using Cisco IOS security features in Cisco IOS release 12.0(4)T. Cisco IOS release 12.0(4)T introduces firewall support on the Cisco 800 series routers.

This section covers the following Cisco IOS Firewall information:

- “Overview of Firewalls”
- “The Cisco IOS Firewall Solution”
- “Other Guidelines for Configuring a Firewall”
- “CBAC Overview”
- “Benefits”
- “Restrictions”
- “Memory and Performance Impact”

## Overview of Firewalls

Firewalls are networking devices that control access to your organization’s network assets. Firewalls are positioned at the entrance points into your network. If your network has multiple entrance points, you must position a firewall at each point to provide effective network access control.

Firewalls are often placed in between the internal network and an external network such as the Internet. With a firewall between your network and the Internet, all traffic coming from the Internet must pass through the firewall before entering your network.

Firewalls can also be used to control access to a specific part of your network. For example, you can position firewalls at all the entry points into a research and development network to prevent unauthorized access to proprietary information.

The most basic function of a firewall is to monitor and filter traffic. Firewalls can be simple or elaborate, depending on your network requirements. Simple firewalls are usually easier to configure and manage. However, you might require the flexibility of a more elaborate firewall.

## The Cisco IOS Firewall Solution

Cisco IOS software provides an extensive set of security features, allowing you to configure a simple or elaborate firewall, according to your particular requirements. You can configure a Cisco device as a firewall if the device is positioned appropriately at a network entry point. Security features that provide firewall functionality are listed in the section “Create a Customized Firewall.”

In addition to the security features available in standard Cisco IOS feature sets, there is a Cisco IOS Firewall feature set that gives your router additional firewall capabilities.

## The Cisco IOS Firewall Feature Set

The Cisco IOS Firewall feature set combines existing Cisco IOS firewall technology and the 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

## Create a Customized Firewall

To create a firewall customized to fit your organization’s security policy, you should determine which Cisco IOS security features are appropriate, and configure those features. At a minimum, you must configure traffic filtering using access lists to provide a basic firewall. Context-based Access Control (CBAC) provides advanced traffic inspection functionality that operates as an integral part of your network firewall.

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

You can create a customized firewall with a variety of Cisco IOS security features:

- Standard Access Lists and Static Extended Access Lists
- Lock-and-Key (Dynamic Access Lists)
- Reflexive Access Lists
- TCP Intercept
- Context-based Access Control

- Security Server Support
- Network Address Translation
- Cisco Encryption Technology
- IPSec Network Security
- Neighbor Router Authentication
- Event Logging
- User Authentication and Authorization

Table 1 describes Cisco IOS security features and lists the related chapter of the *Security Configuration Guide*.

**Table 1 Cisco IOS Features for a Robust Firewall**

Feature	Chapter	Comments
Standard Access Lists and Static Extended Access Lists	<p>“Access Control Lists: Overview and Guidelines” in the Cisco IOS Release 12.0 <i>Security Configuration Guide</i>.</p> <p>Also refer to the Cisco IOS Release 12.0(1)T feature module “Time-based Access Lists Using Time Ranges.”</p>	<p>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.</p> <p>Additionally, it is possible to implement access lists based on the time of day, providing network administrators with more control over permitting or denying a user access to resources.</p> <p>To configure a basic firewall, you should at a minimum configure basic traffic filtering. You should configure basic access lists for all network protocols that will be routed through your firewall, such as IP, IPX, AppleTalk.</p>
Lock-and-Key (Dynamic Access Lists)	<p>“Configuring Lock-and-Key Security (Dynamic Access Lists)” in the Cisco IOS Release 12.0 <i>Security Configuration Guide</i>.</p>	<p>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. Afterwards, the firewall closes the temporary opening. This provides tighter control over traffic at the firewall than with standard or static extended access lists.</p>
Reflexive Access Lists	<p>“Configuring IP Session Filtering (Reflexive Access Lists)” in the Cisco IOS Release 12.0 <i>Security Configuration Guide</i>.</p>	<p>Reflexive access lists filter IP traffic so that TCP or UDP “session” traffic is only permitted through the firewall if the session originated from within the internal network.</p> <p>You would only configure Reflexive Access Lists when not using Context-based Access Control.</p>
TCP Intercept	<p>“Configuring TCP Intercept (Prevent Denial-of-Service Attacks)” in the Cisco IOS Release 12.0 <i>Security Configuration Guide</i>.</p>	<p>TCP Intercept protects TCP servers within your network from TCP SYN-flooding attacks, a type of denial-of-service attack.</p> <p>You would only configure TCP Intercept when not using Context-based Access Control.</p>

**Table 1 Cisco IOS Features for a Robust Firewall (continued)**

Feature	Chapter	Comments
Context-based Access Control	“Configuring Context-based Access Control” in this document.	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 only available in the Cisco IOS Firewall Feature Set.
Security Server Support	“Configuring TACACS+,” “Configuring TACACS and Extended TACACS,” “Configuring RADIUS,” and “Configuring Kerberos” in the Cisco IOS Release 12.0 <i>Security Configuration Guide</i> .	The Cisco IOS Firewall feature set can be configured as a client of the following supported security servers: <ul style="list-style-type: none"> <li>• TACACS, TACACS+, and Extended TACACS</li> <li>• RADIUS</li> <li>• Kerberos</li> </ul> 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. When users pass authentication, they are granted access according to their specified privileges.
Network Address Translation	“Configuring IP Addressing” chapter in the <i>Network Protocols Configuration Guide, Part 1</i> .	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.  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.
Cisco Encryption Technology	“Configuring Cisco Encryption Technology” in the <i>Security Configuration Guide</i> .	Cisco Encryption Technology (CET) 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.

**Table 1 Cisco IOS Features for a Robust Firewall (continued)**

Feature	Chapter	Comments
IPSec Network Security	“Configuring IPSec Network Security” in the <i>Security Configuration Guide</i> .	IPSec is a framework of open standards developed by the Internet Engineering Task Force (IETF) that provides security for transmission of sensitive information over unprotected networks such as the Internet. IPSec acts at the network layer, protecting and authenticating IP packets between participating IPSec devices (“peers”) such as Cisco routers.  IPSec services are similar to those provided by Cisco Encryption Technology, a proprietary security solution introduced in Cisco IOS Software Release 11.2. (The IPSec standard was not yet available at Release 11.2.) However, IPSec provides a more robust security solution, and is standards-based.
Neighbor Router Authentication	“Neighbor Router Authentication: Overview and Guidelines” in the <i>Security Configuration Guide</i> .	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	“Troubleshooting the Router” chapter in the “System Management” part of the <i>Configuration Fundamentals Configuration Guide</i> .	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.
User Authentication and Authorization	“Configuring Authentication” and “Configuring Authorization” in the <i>Security Configuration Guide</i> .	Authentication and authorization help protect your network from access by unauthorized users.

## Other Guidelines for Configuring a Firewall

As with all networking devices, you should always protect access into the firewall by configuring passwords as described in the “Configuring Passwords and Privileges” chapter in the *Security Configuration Guide*. You should also consider configuring user authentication, authorization, and accounting as described in the “Authentication, Authorization, and Accounting (AAA)” part of the *Security Configuration Guide*.

You should also consider the following recommendations:

- 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.

- Do not enable any local service (such as SNMP or NTP) that you do not use. Cisco Discovery Protocol (CDP) and Network Time Protocol (NTP) are on by default, and you should turn these off if you do not 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. In Cisco IOS Release 12.0 and later, these services are disabled by default.

- 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 do not already have NAT configured to prevent internal addresses from being revealed).
- Keep the firewall in a secured (locked) room.

## CBAC Overview

This section describes how to configure Context-based Access Control (CBAC). CBAC provides advanced traffic inspection functionality and can be used as an integral part of your network's firewall.

For a complete description of the CBAC commands used in this section, refer to the "Context-Based Access Control Commands" chapter in the *Security Command Reference*.

This section describes:

- What CBAC Does
- What CBAC Does Not Do
- How CBAC Works

- When and Where to Configure CBAC
- The CBAC Process
- Supported Protocols

## What CBAC Does

CBAC intelligently inspects TCP and UDP packets based on application-layer protocol session information and can be used for intranets, extranets, and the Internet. You can configure CBAC to permit specified TCP and UDP traffic through a firewall only when the connection is initiated from within the network you want to protect. (In other words, CBAC can inspect traffic for sessions that originate from the external network.) However, while this example discusses inspecting traffic for sessions that originate from the external network, CBAC can inspect traffic for sessions that originate from either side of the firewall.

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 and additional data connections for permissible sessions (sessions that originated from within the protected internal network).

Inspecting packets at the application layer and maintaining TCP and UDP session information provides CBAC with the ability to detect and prevent certain types of network attacks such as SYN-flooding. A SYN-flooding attack occurs when a network attacker floods a server with a barrage of requests for connection and does not complete the connection. The resulting volume of half-open connections can overwhelm the server, causing it to deny service to valid requests.

Denial-of-service (DoS) detection and prevention inspects packet sequence numbers in TCP connections. If they are not within expected ranges, the router drops suspicious packets. When the router detects unusually high rates of new connections, it issues an alert message. The router drops half-open TCP connection state tables to prevent system resource depletion.

Additional features include Java blocking and real-time alerts and audit trails. Java blocking can be configured to filter based on the server address or completely deny access to Java applets that are not embedded in an archived or compressed file.

Enhanced audit trail features use SYSLOG to track all transactions; recording time stamps, source host, destination host, ports used, and the total number of transmitted bytes, for advanced, session-based reporting.

Real-time alerts send SYSLOG error messages to central management consoles upon detecting suspicious activity. Network managers have the ability to respond immediately to intrusions.

## What CBAC Does Not Do

CBAC does not protect against attacks originating from within the protected network. CBAC only detects and protects against attacks that 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

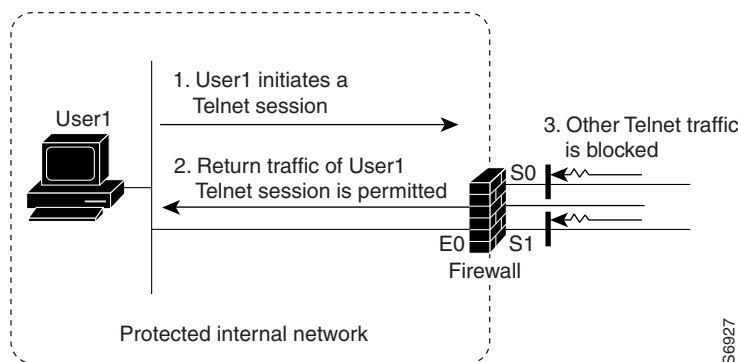
You should understand the material in this section before you configure CBAC. If you do not understand how CBAC works, you might inadvertently introduce security risks by configuring CBAC inappropriately.

### 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) and additional data channels 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.

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 User1’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 User1’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.

**Figure 1 CBAC Opens Temporary Holes in Firewall Access Lists**



S6927

### How CBAC Works—Details

This section describes how CBAC inspects packets and maintains state information about sessions to manage the traffic flow through the interface.

#### 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 is configured.

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 are not inspected. For example, during FTP sessions both the control and data channels (which are created when a data file is transferred) are monitored for state changes, but only the control channel is inspected (that is, the CBAC software parses the FTP commands and responses).

CBAC inspection tracks sequence numbers in all TCP packets, and drops those packets with sequence numbers that are not within expected ranges.

CBAC inspection recognizes application-specific commands (such as illegal SMTP commands) in the control channel, and detects and prevents certain application-level attacks.

When CBAC suspects an attack, the DoS feature can take several actions:

- Generate alert messages
- Protect system resources that could impede performance
- Block packets from suspected attackers

CBAC uses timeout and threshold values to manage session state information, helping to determine when to drop sessions that do not become fully established. Setting timeout values for network sessions helps prevent DoS attacks by freeing up system resources, dropping sessions after a specified amount of time. Setting threshold values for network sessions helps prevent DoS attacks by controlling the number of half-open sessions, which limits the amount of system resources applied to half-open sessions. When a session is dropped, CBAC sends a reset message to the devices at both end points (source and destination) of the session. When the system under DoS attack receives a reset command, it releases, or frees up, processes and resources related to that incomplete session.

CBAC provides three thresholds against DoS attacks:

- the total number of half-open TCP sessions
- the number of half-open sessions based upon time
- the number of half-open sessions per host

If a threshold is exceeded, CBAC has two options: send a reset message to the end points of the oldest half-open session, making resources available to service newly arriving SYN packets; or block all SYN packets temporarily for the duration configured by the threshold value. When the router blocks a SYN packet, the TCP three-way handshake is never initiated, which prevents the router from using memory and processing resources needed for valid connections.

DoS detection and prevention requires that you create a CBAC inspection rule and apply that rule on an interface. The inspection rule must include the protocols that you want to monitor against DoS attacks. For example, if you have TCP inspection enabled on the inspection rule, then CBAC can track all TCP connections to watch for DoS attacks. If the inspection rule includes FTP protocol inspection but not TCP inspection, CBAC tracks only FTP connections to watch for DoS attacks on FTP servers.

For detailed information about setting timeout and threshold values in CBAC to detect and prevent DoS attacks, refer in the “Configure Global Timeouts and Thresholds” section.

## 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. Inspection controls the traffic that belongs to a valid session and forwards the traffic it does not know. 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 and Additional Data Connections

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

CBAC is highly flexible and can be configured on any interface of any firewall for protecting internal networks. Such firewalls should be Cisco routers with the Cisco Firewall feature set configured as described previously in the section “The Cisco IOS Firewall Feature Set.”

Use CBAC when the firewall will be passing TCP, UDP, and common application traffic.

Use CBAC for applications if you want the application’s traffic to be permitted through the firewall only when the traffic session is initiated from a particular side of the firewall (usually from the protected internal network).

In many cases, you will configure CBAC in one direction, in or out, at a single interface. This configuration causes traffic to be permitted back into the internal network only if the traffic is part of a permissible (valid, existing) session. This is a typical configuration for protecting your internal networks from traffic that originates on the Internet.

You can also configure CBAC in both directions on the same interface if you want to inspect sessions initiated on either side of the interface. Configuring CBAC in both directions can be useful in a corporate intranet or extranet environment where you want to manage sessions between different groups of users or between corporate partners.

## The CBAC Process

This section describes a sample 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, a TCP packet exits the internal network through the firewall’s external interface. The TCP packet is the first packet of a Telnet session, and Telnet 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—Telnet—was not configured for CBAC inspection, the packet would simply be forwarded out the interface at this point without being inspected by CBAC. See the section "Define an Inspection Rule" for configuring CBAC inspection information.)
- 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 same Telnet connection previously established with the outbound packet. The inbound packet is evaluated against the inbound access list, and it 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 they 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.

In the sample process just described, the firewall access lists are configured as follows:

- An outbound IP access list (standard or extended) is applied to the external interface. This access list permits all packets that you want to allow to exit the network, including packets you want to be inspected by CBAC. In this case, Telnet packets are permitted.
- An inbound extended IP access list is applied to the external interface. This access list denies any traffic to be inspected by CBAC—including Telnet packets. 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 had been configured to permit *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 the following types of sessions:

- 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)
- HTTP (Java blocking)
- Java
- Microsoft NetShow
- UNIX R-commands (such as rlogin, rexec, and rsh)
- 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.

## Benefits

- CBAC provides internal users secure, per-application-based access control for all traffic across perimeters such as between private enterprise networks and the Internet.
- Denial-of-service detection and prevention defends and protects router resources against common attacks, checking packet headers and dropping suspicious packets.
- Java blocking protects against unidentified, malicious Java applets.
- Audit trail details transactions, recording time stamp, source host, destination host, ports, duration, and total number of bytes transmitted.
- Real-time alerts log alerts in case of denial-of-service attacks or other pre-configured conditions.

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

## 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.)
- CBAC supports four switching modes: Cisco Express Forwarding (CEF), flow switching, fast switching, and process switching; however, you cannot configure both NAT and CBAC together with CEF on the Cisco 2600 and 3600 routers.
- CBAC does not support redundant routing environments. CBAC keeps track of the state of the connections it monitors, so the packets associated with the same session have to go through the same router. The Cisco IOS Firewall does not communicate this state information to other firewall routers, meaning that sessions must be reestablished on the failover unit after failover occurs.
- If you reconfigure your access lists when you configure CBAC, be aware that if your access lists block TFTP traffic into an interface, you will not 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-party connections (three-way FTP transfer).
  - When CBAC inspects FTP traffic, it only allows data channels with the destination port in the range of 1024 to 65535.
  - CBAC will not open a data channel if the FTP client-server authentication fails.
- Cisco Encryption Technology and CBAC Compatibility
  - 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, 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 multichannel protocols, except for StreamWorks and CU-SeeMe. So if you configure encryption at the firewall, you should configure CBAC for only these protocols: Generic TCP, Generic UDP, StreamWorks.
- IPsec and CBAC Compatibility
  - When CBAC and IPsec are enabled on the same router, and the firewall router is an endpoint for IPsec for the particular flow, then IPsec is compatible with CBAC (that is, CBAC can do its normal inspection processing on the flow).
  - If the router is not an IPsec endpoint, but the packet is an IPsec packet, then CBAC will not inspect the packets because the protocol number in the IP header of the IPsec packet is not TCP or UDP. CBAC only inspects TCP and UDP packets.
  - IPsec is not available on the Cisco 800 series.

## 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.

Sometimes CBAC must evaluate long access lists, which might have presented a negative impact to performance. However, this impact is avoided, because CBAC evaluates access lists using an accelerated method (CBAC hashes access lists and evaluates the hash).

## Platforms

The Cisco IOS Firewall feature set is supported on the following platforms:

- Cisco 800 series
- Cisco uBR904
- Cisco 1600 series
- Cisco 1720 router
- Cisco 2500 series
- Cisco 2600 series
- Cisco 3600 series
- Cisco 7200 series

## Prerequisites

None.

## Supported MIBs and RFCs

None.

## Configuration Tasks

To configure CBAC, 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

You can also perform the tasks described in the following sections. These tasks are optional.

- Display Configuration, Status, and Statistics for Context-based Access Control
- Debug Context-based Access Control

- Interpret Syslog and Console Messages Generated by Context-based Access Control
- Turn Off Context-based Access Control

---

**Note** 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. Be sure you understand what CBAC does before you configure CBAC.

---

For CBAC configuration examples, refer to the “Configuration Examples” section.

## Pick an Interface: Internal or External

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

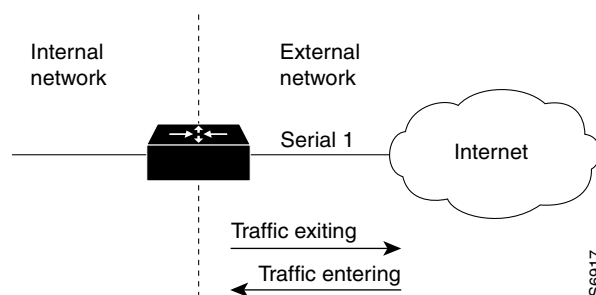
“Internal” refers to the side where sessions must originate for their traffic to be permitted through the firewall. “External” refers to the side where sessions cannot originate (sessions originating from the external side will be blocked).

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 on 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.



- 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 Services” chapter of the Cisco IOS Release 12.0 *Network Protocols Configuration Guide, Part 1*.

## Internal Interface

Here are some tips for your access lists when you will be configuring CBAC on an internal interface:

- If you have an inbound IP access list at the internal interface or an outbound IP access list at external interface(s), these access lists can be either 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 Services” chapter of the Cisco IOS Release 12.0 *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.

---

**Note** If you want to enable the more aggressive TCP host-specific denial-of-service prevention that includes the blocking of connection initiation to a host, you must set the **block-time** specified in the **ip inspect tcp max-incomplete host** command (see the last row in the following table).

---

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

To change a global timeout or threshold listed in the “Timeout or Threshold Value to Change” column, use the global configuration command in the “Command” 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.	<b>ip inspect tcp synwait-time</b> <i>seconds</i>	30 seconds

Timeout or Threshold Value to Change	Command	Default
The length of time a TCP session will still be managed after the firewall detects a FIN-exchange.	<b>ip inspect tcp finwait-time</b> <i>seconds</i>	5 seconds
The length of time a TCP session will still be managed after no activity (the TCP idle timeout). <sup>1</sup>	<b>ip inspect tcp idle-time</b> <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). <sup>1</sup>	<b>ip inspect udp idle-time</b> <i>seconds</i>	30 seconds
The length of time a DNS name lookup session will still be managed after no activity.	<b>ip inspect dns-timeout</b> <i>seconds</i>	5 seconds
The number of existing half-open sessions that will cause the software to start deleting half-open sessions. <sup>2</sup>	<b>ip inspect max-incomplete high</b> <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. <sup>2</sup>	<b>ip inspect max-incomplete low</b> <i>number</i>	400 existing half-open sessions
The rate of new unestablished sessions that will cause the software to start deleting half-open sessions. <sup>2</sup>	<b>ip inspect one-minute high</b> <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. <sup>2</sup>	<b>ip inspect one-minute low</b> <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. <sup>3</sup>	<b>ip inspect tcp max-incomplete host</b> <i>number block-time minutes</i>	50 existing half-open TCP sessions; 0 minutes

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 in the "Context-Based Access Control Commands" chapter of the *Security 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. If the **block-time** timeout is zero, the software will delete the oldest existing half-open session for the host for every new connection request to the host and will let the SYN packet through. If the **block-time** timeout is greater than zero, 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.

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 TCP 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 per 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. The firewall router reviews the “one-minute” rate on an ongoing basis, meaning that the router reviews the rate more frequently than one minute and does not keep deleting half-open sessions for one-minute after a DoS attack has stopped—it will be less time.

## 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 Java Inspection
- Configure Generic TCP and UDP Inspection

## Configure Application-Layer Protocol Inspection

---

**Note** If you want CBAC inspection to work with NetMeeting 2.0 traffic (an H.323 application-layer protocol), you must also configure inspection for TCP, as described later in the section “Configure Generic TCP and UDP Inspection.” This requirement exists because NetMeeting 2.0 uses an additional TCP channel not defined in the H.323 specification.

---

To configure CBAC inspection for an application-layer protocol, use one or both of the following global configuration commands:

Command	Purpose
<b>ip inspect name</b> <i>inspection-name</i> <i>protocol</i> [ <b>timeout</b> <i>seconds</i> ]	Configure CBAC inspection for an application-layer protocol (except for RPC and Java). Use one of the protocol keywords defined in Table 2, following.  Repeat this command for each desired protocol. Use the same <i>inspection-name</i> to create a single inspection rule.
<b>ip inspect name</b> <i>inspection-name</i> <b>rpc program-number</b> <i>number</i> [ <b>wait-time</b> <i>minutes</i> ] [ <b>timeout</b> <i>seconds</i> ]	Enable CBAC inspection for the RPC application-layer protocol.  You can specify multiple RPC program numbers by repeating this command for each program number.  Use the same <i>inspection-name</i> to create a single inspection rule.

Refer to the description of the **ip inspect name (global configuration)** command in the “Context-Based Access Control Commands” chapter in the *Security Command Reference* 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 2 identifies application protocol keywords.

**Table 2 Application Protocol Keywords**

Application Protocol	<i>protocol</i> Keyword
CU-SeeMe	<b>cuseeme</b>
FTP	<b>ftp</b>
Java applets	<b>http</b>
H.323	<b>h323</b>
UNIX R commands (rlogin, rexec, rsh)	<b>rcmd</b>
RealAudio	<b>realaudio</b>
RPC	<b>rpc</b>
SMTP	<b>smtp</b>
SQL*Net	<b>sqlnet</b>
StreamWorks	<b>streamworks</b>
TFTP	<b>tftp</b>
VDOLive	<b>vdolive</b>

## 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 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, use the following global configuration commands:

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



**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 from FTP, gopher, HTTP on a nonstandard port, and so forth.

## 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 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, use one or both of the following global configuration commands:

Command	Purpose
<b>ip inspect name</b> <i>inspection-name</i> <b>tcp</b> [ <b>timeout</b> <i>seconds</i> ]	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.
<b>ip inspect name</b> <i>inspection-name</i> <b>udp</b> [ <b>timeout</b> <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.

## 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 rule to outbound traffic.

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

To apply an inspection rule to an interface, use the following interface configuration command:

Command	Purpose
<b>ip inspect</b> <i>inspection-name</i> { <b>in</b>   <b>out</b> }	Apply an inspection rule to an interface.

## Display Configuration, Status, and Statistics for Context-based Access Control

You can view certain CBAC information by using one or more of the following EXEC commands:

Command	Purpose
<b>show ip inspect name</b> <i>inspection-name</i>	Show a particular configured inspection rule.
<b>show ip inspect config</b>	Show the complete CBAC inspection configuration.
<b>show ip inspect interfaces</b>	Show interface configuration with regards to applied inspection rules and access lists.
<b>show ip inspect session</b> [ <b>detail</b> ]	Show existing sessions that are currently being tracked and inspected by CBAC.
<b>show ip inspect all</b>	Show all CBAC configuration and all existing sessions that are currently being tracked and inspected by CBAC.

## Debug Context-based Access Control

To assist CBAC debugging, you can turn on audit trail messages that will be displayed on the console after each CBAC session closes.

To turn on audit trail messages, use the following global configuration command:

Command	Purpose
<b>ip inspect audit trail</b>	Turn on CBAC audit trail messages.

If required, you can also 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. To disable all debugging, use the privileged EXEC commands **no debug all or undebug all**.)

The available **debug** commands are listed in the following categories:

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

For a complete description of the debug commands, refer to the *Debug Command Reference*.

## Generic Debug Commands

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

Command	Purpose
<b>debug ip inspect function-trace</b>	Display messages about software functions called by CBAC.
<b>debug ip inspect object-creation</b>	Display messages about software objects being created by CBAC. Object creation corresponds to the beginning of CBAC-inspected sessions.
<b>debug ip inspect object-deletion</b>	Display messages about software objects being deleted by CBAC. Object deletion corresponds to the closing of CBAC-inspected sessions.
<b>debug ip inspect events</b>	Display messages about CBAC software events, including information about CBAC packet processing.
<b>debug ip inspect timers</b>	Display messages about CBAC timer events such as when a CBAC idle timeout is reached.
<b>debug ip inspect detail</b>	Enable the detailed option, which can be used in combination with other options to get additional information.

## Transport Level Debug Commands

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

Command	Purpose
<b>debug ip inspect tcp</b>	Display messages about CBAC-inspected TCP events, including details about TCP packets.
<b>debug ip inspect udp</b>	Display messages about CBAC-inspected UDP events, including details about UDP packets.

## Application Protocol Debug Commands

You can use the following application protocol **debug** command, entered in privileged EXEC mode:

Command	Purpose
<b>debug ip inspect</b> <i>protocol</i>	Display messages about CBAC-inspected protocol events, including details about the protocol's packets.  Refer to Table 3 to determine the protocol keyword.

Table 3 identifies application protocol keywords for the **debug ip inspect** command.

**Table 3 Application Protocol Keywords for the debug ip inspect Command**

Application Protocol	<i>protocol</i> keyword
CU-SeeMe	<b>cuseeme</b>
FTP commands and responses	<b>ftp-cmd</b>
FTP tokens (enables tracing of the FTP tokens parsed)	<b>ftp-tokens</b>
H.323	<b>h323</b>
Java applets	<b>http</b>
UNIX R commands (rlogin, rexec, rsh)	<b>rcmd</b>
RealAudio	<b>realaudio</b>
RPC	<b>rpc</b>
SMTP	<b>smtp</b>
SQL*Net	<b>sqlnet</b>
StreamWorks	<b>streamworks</b>
TFTP	<b>tftp</b>
VDOLive	<b>vdolive</b>

## Interpret Syslog and Console Messages Generated by Context-based Access Control

CBAC provides syslog messages, console alert messages and audit trail messages. These messages are useful because they can alert you to network attacks and because they provide an audit trail that provides details about sessions inspected by CBAC. While they are generally referred to as error messages, not all error messages indicate problems with your system.

The following types of error messages can be generated by CBAC:

- Denial-of-Service Attack Detection Error Messages
- SMTP Attack Detection Error Message
- Java Blocking Error Message
- FTP Error Messages
- Audit Trail Error Message

For explanations and recommended actions related to the error messages mentioned in this section, refer to the *Cisco IOS Software System Error Messages*.

## Denial-of-Service Attack Detection Error Messages

CBAC detects and blocks denial-of-service attacks and notifies you when denial-of-service attacks occur. Error messages such as the following may indicate that denial-of-service attacks have occurred:

```
%FW-4-ALERT_ON: getting aggressive, count (550/500) current 1-min rate: 250
%FW-4-ALERT_OFF: calming down, count (0/400) current 1-min rate: 0
```

When %FW-4-ALERT\_ON and %FW-4-ALERT\_OFF error messages appear together, each “aggressive/calming” pair of messages indicates a separate attack. The preceding example shows one separate attack.

Error messages such as the following may indicate that a denial-of-service attack has occurred on a specific TCP host:

```
%FW-4-HOST_TCP_ALERT_ON: Max tcp half-open connections (50) 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 50 exceeded)
%FW-4-UNBLOCK_HOST: New TCP connections to host 172.21.127.242 no longer blocked
```

## SMTP Attack Detection Error Message

CBAC detects and blocks SMTP attacks (illegal SMTP commands) and notifies you when SMTP attacks occur. Error messages such as the following may indicate that an SMTP attack has occurred:

```
%FW-4-SMTP_INVALID_COMMAND: Invalid SMTP command from initiator (192.168.12.3:52419)
```

## Java Blocking Error Message

CBAC detects and selectively blocks Java applets and notifies you when a Java applet has been blocked. Error messages such as the following may indicate that a Java applet has been blocked:

```
%FW-4-HTTP_JAVA_BLOCK: JAVA applet is blocked from (172.21.127.218:80) to
(172.16.57.30:44673).
```

## FTP Error Messages

CBAC detects and prevents certain FTP attacks and notifies you when these attacks occur. Error messages such as the following may appear when CBAC detects these FTP attacks:

```
%FW-3-FTP_PRIV_PORT: Privileged port 1000 used in PORT command -- FTP client 10.0.0.1
FTP server 10.1.0.1
%FW-3-FTP_SESSION_NOT_AUTHENTICATED: Command issued before the session is authenticated
-- FTP client 10.0.0.1
%FW-3-FTP_NON_MATCHING_IP_ADDR: Non-matching address 172.19.148.154 used in PORT
command -- FTP client 172.19.54.143 FTP server 172.16.127.242
```

## Audit Trail Error Message

CBAC provides audit trail messages to record details about inspected sessions. To determine which protocol was inspected use the responder’s port number. The port number follows the responder’s address. The following are sample audit trail messages:

```
%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
%FW-6-SESS_AUDIT_TRAIL: http session initiator (172.16.57.30:44673) sent
1599 bytes -- responder (172.21.127.218:80) sent 93124 bytes
```

## Turn Off Context-based Access Control

You can turn off 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. All existing sessions are deleted and their associated access lists are removed.

---

In most situations, turning off CBAC has no negative security impact because CBAC creates “permit” access lists. Without CBAC configured, no “permit” access lists are maintained. Therefore, no derived traffic (returning traffic or traffic from the data channels) can go through the firewall. The exception is SMTP and Java blocking. With CBAC turned off, unacceptable SMTP commands or Java applets may go through the firewall.

## Configuration Examples

This section provides multiple configuration examples:

- Simple CBAC Configuration
- Remote Office to Internet service provider (ISP)
- Remote Office to Branch Office
- Two Interface Branch Office
- Multiple Interface Branch Office

The first example develops a CBAC inspection rule and a supporting Access Control List (ACL), and applies that inspection rule on an ATM interface. This example focuses on how to configure CBAC; it does not provide a complete router configuration and does not describe other elements of the configuration such as the ATM interface.

The remote-office examples also focus on the firewall configuration and do not provide detailed descriptions of other configuration elements such as the Basic Rate Interface (BRI) and dialer interface configurations.

The other examples provide more complete firewall configurations, illustrating ways to apply CBAC in branch office environments with LAN and serial interfaces.

## Simple CBAC Configuration

In this example, firewall protection is required against inbound traffic on an ATM interface. This example might apply to sites where local hosts require access to hosts or services on a remote network. The security policy for this site uses Access Control Lists (ACL) to restrict outbound traffic on the ATM interface to IP and ICMP protocol traffic, denying outbound access for TCP and UDP protocol traffic. Outbound access for specific TCP and UDP protocol traffic is provided through dynamic access lists, which are generated according to CBAC inspection rules.

For information on how to select the interface on which to apply CBAC, refer in the “Pick an Interface: Internal or External” section.

---

**Note** For Frame Relay or ATM interfaces, you can apply CBAC inspection rules separately on each sub-interface, even though the sub-interfaces are physically connected through one interface.

---

```

!-----
!Create the Inspection Rule
!-----
!
!Create the CBAC inspection rule "test", allowing inspection of the protocol traffic
!specified by the rule. This inspection rule sets the timeout value to 30 seconds for
!each protocol (except for RPC). The timeout value defines the maximum time that a
!connection for a given protocol can remain active without any traffic passing through
!the router. When these timeouts are reached, the dynamic ACLs that are inserted to
!permit the returning traffic are removed, and subsequent packets (possibly even valid
!ones) are not permitted.
ip inspect name test cuseeme timeout 30
ip inspect name test ftp timeout 30
ip inspect name test h323 timeout 30
ip inspect name test realaudio timeout 30
ip inspect name test rpc program-number 100000
ip inspect name test streamworks timeout 30
ip inspect name test vdolive timeout 30
!
!-----
!Create the Access Control List
!-----
!
!In this example, ACL 105 denies all TCP and UDP protocol traffic. IP traffic is
!permitted to allow access for routing and control traffic. This means that only the
!return traffic for protocols defined in the inspection rule is allow access through
!the interface where this rule is applied.
access-list 105 deny TCP any any
access-list 105 deny UDP any any
access-list 105 permit ip any any
!

!-----
!Apply the Inspection Rule and ACL
!-----
!
!In this example, the inspection rule "test" is applied at ATM interface 3/0 for
!connections initiated in the outbound direction; that is, from hosts that are located
!on a local network. ACL 105 is applied at ATM interface 3/0 in the inbound direction;
!that is, return traffic in response to local host initiated connections. If inbound
!traffic at the interface matches an inspection rule, CBAC creates a dynamic access
!list allowing inbound (returning) traffic for that connection. This combination of the
!ACL and CBAC inspection rules means that TCP and UDP traffic that is not part of a
!connection that initiated from a local host is not permitted access through the
!interface.
interface ATM3/0
 ip address 10.1.10.1 255.0.0.0
 ip access-group 105 in
 no ip directed-broadcast
 ip nat outside
 ip inspect test out
 no shutdown
 atm clock INTERNAL
 atm pvc 7 7 7 aal5snap
 map-group atm

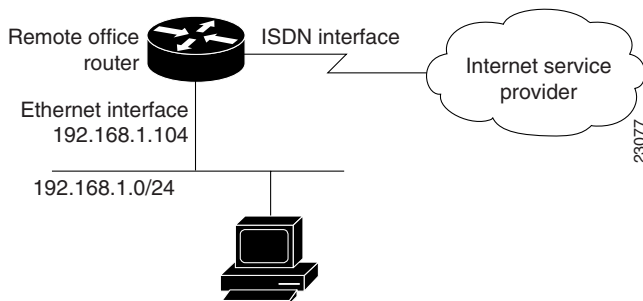
```

## Remote Office to ISP

This example describes one possible Cisco IOS Firewall configuration for a remote office router, such as a Cisco 800 series, connected to an ISP. In this configuration, the site security policy allows hosts on the local network to initiate traffic to the ISP while traffic inbound to the router from the

ISP is blocked at the ISDN interface. Specific ICMP control message traffic is permitted through the firewall. No mail or Web services are available from the local network. Figure 4 illustrates this example.

**Figure 4 Remote Office to ISP Sample Configuration**



The firewall has two interfaces:

- An Ethernet interface connects to the internal protected network.

Interface Ethernet0 has no ACL applied to it, meaning that all traffic initiated on the LAN is allowed access to the ISP. In this configuration example, Network Address Translation (NAT) is not turned on, and the addresses on interface Ethernet0 are reserved IP addresses. In a production environment, addresses on Ethernet0 either must be registered network addresses, or you must turn on NAT to hide these inside addresses from being visible on the Internet.

- An ISDN Basic Rate Interface (BRI) connects the router to the ISP. In this example, a dialer profile is used to control the BRI interface. This means that the ACL and CBAC inspection rules are applied at the dialer interface, not directly at the physical ISDN (BRI) interface using a dialer map.

```

!-----
!General Cisco IOS Firewall Guidelines
!-----
!The following global configuration entries illustrate good security practices.
enable secret 5 <elided>
no ip source-route
no cdp run
!
!-----
!Create the CBAC inspection rule
!-----
!Create the CBAC inspection rule STOP to allow inspection of the protocol traffic
!specified by the rule.
ip inspect name STOP tcp
ip inspect name STOP ftp
ip inspect name STOP smtp
ip inspect name STOP h323
ip inspect name STOP rcmd
!
!-----
!Create Access Control List 105
!-----
!ACL 105 denies all IP protocol traffic except for specific ICMP control traffic.
!This means that only the return traffic for protocols defined in the
!inspection rule and the specified ICMP traffic is allowed access through the
!interface where this rule is applied.
!
!Deny broadcast messages with a source address of 255.255.255.255; this helps to

```

```

!prevent broadcast attacks.
access-list 105 deny ip host 255.255.255.255 any
!
!Add anti-spoofing protection by denying traffic with a source address matching a host
!on the Ethernet interface.
acl 105 deny ip 192.168.1.0 0.0.0.255 any
!
!ICMP traffic is not inspected by CBAC. To control the type of ICMP traffic at the
!interface, add static access list entries. This example has the following ICMP
!requirements: outgoing ping commands require echo-reply messages to come back,
!outgoing traceroute commands require time-exceeded messages to come back, path MTU
!discovery requires "too-big" messages to come back, and incoming traceroute
!messages must be allowed. Additionally, permit all "unreachable" messages to come
!back; that is, if a router cannot forward or deliver a datagram, it sends an ICMP
!unreachable
!message back to the source and drops the datagram.
access-list 105 permit icmp any any echo-reply
access-list 105 permit icmp any 192.168.1.0 0.0.0.255 time-exceeded
access-list 105 permit icmp any 192.168.1.0 0.0.0.255 packet-too-big
access-list 105 permit icmp any 192.168.1.0 0.0.0.255 traceroute
access-list 105 permit icmp any 192.168.1.0 0.0.0.255 unreachable
!
!Final deny for explicitness. This entry is not required but helps complete the access
!list picture. By default, the final entry in any access list is an implicit deny of IP
!protocol traffic. This ensures that the firewall blocks any traffic not explicitly
!permitted by the access list.
access-list 105 deny ip any any
!
!-----
!Configure the interface
!-----
!In this example, no ACLs or inspection rules are applied at interface Ethernet0,
!meaning that all traffic on the local network is allowed to go out. This assumes a
!high-level of trust for the users on the local network.
interface Ethernet0
 ip address 192.168.1.104 255.255.255.0
 no ip directed-broadcast
!
!This example uses a dialer profile, so the ACL and CBAC inspection rules are applied
!at the dialer interface, not the physical BRI interface. The dialer pool-member
!command is used to associate the physical interface with a dialer profile.
interface BRI0
 no ip address
 no ip directed-broadcast
 encapsulation ppp
 dialer pool-member 1
 isdn switch-type basic-5ess
!
!-----
!Create the dialer profile.
!-----
!Through the dialer profile, the ACL and CBAC inspection rules are
!applied to every pool member. In this example, the ACL is applied in, meaning that it
!applies to traffic inbound from the ISP. The CBAC inspection rule STOP is applied out,
!meaning that CBAC monitors the traffic through the interface and controls return
!traffic to the router for an existing connection.
interface Dialer0
 ip address negotiated
 ip access-group 105 in
 no ip directed-broadcast
 ip inspect STOP out
 encapsulation ppp
 dialer remote-name <ISP router>
 dialer idle-timeout 500
 dialer string <elided>

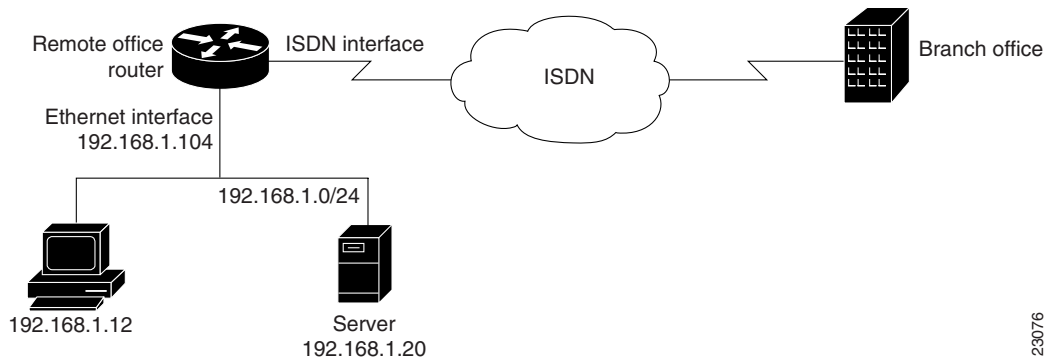
```

```
dialer pool 1
dialer-group 1
ppp authentication callin
!
!-----
!Additional entries
!-----
!Configure the router to forward packets destined for an unrecognized subnet of
!a directly connected network.
ip classless
!Route traffic to the dialer interface.
ip route 0.0.0.0 0.0.0.0 Dialer0
!Include a dialer list protocol entry to specify the protocol that triggers dialing.
dialer-list 1 protocol ip permit
!Add a user name (name of the router your are configuring) and password for caller
!identification and password authentication with the ISP router.
username <router host name> password 5 <elided>
```

## Remote Office to Branch Office Configuration

This example describes one possible Cisco IOS Firewall configuration for a remote office router, such as a Cisco 800 series, connected to a branch office. In this configuration, the site security policy allows hosts on the local network to initiate traffic to the branch office. Mail or Web services are available from a server on the local network, and access to these services is available from the branch office. Traffic from the branch office, except for mail and Web traffic, is blocked at the outside interface. Specific ICMP control message traffic is permitted through the firewall. Figure 5 illustrates this example.

**Figure 5 Remote Office to Branch Office Sample Configuration**



The firewall has two interfaces:

- An Ethernet interface connects to the internal protected network.  
Interface Ethernet0 has no ACL applied to it, meaning that all traffic initiated from the LAN is allowed access through the firewall.
- An ISDN Basic Rate Interface (BRI) connects the router to the branch office. In this example, a dialer profile is used to control the BRI interface. This means that the ACL and CBAC inspection rules are applied at dialer interface, not directly at the physical ISDN (BRI) interface.

```
!-----
!General firewall configuration guidelines
!-----
!The following global configuration entries illustrate good security practices.
enable secret 5 <elided>
no ip source-route
no cdp run
!
!-----
!Create the Inspection Rule
!-----
!Create the CBAC inspection rule STOP to allow inspection of the specified protocol
!traffic. Create the inspection rule GO to allow inspection of HTTP and SMTP
!traffic. Note that Java applets will be permitted according to access list 51, which
!is defined later in this sample configuration.
ip inspect name STOP tcp
ip inspect name STOP ftp
ip inspect name STOP smtp
ip inspect name STOP h323
ip inspect name STOP rcmd
ip inspect name GO http java-list 51
ip inspect name GO smtp
!
!-----
!Create Access Control Lists 106 and 51
!-----
!ACL 106 permits mail and Web traffic from any host to the specified server. ACL 106
!denies all other ip protocol traffic except for specific ICMP control traffic.
!This means that only the return traffic for protocols defined in the
!inspection rule and the specified ICMP traffic is allowed access through the
!interface where this rule is applied.
!
!Deny broadcast messages with a source address of 255.255.255.255; this helps to
!prevent broadcast attacks.
access-list 106 deny ip host 255.255.255.255 any
!
!Add anti-spoofing protection by denying traffic with a source address matching a host
!on the Ethernet interface.
access-list 106 deny ip 192.168.1.0 0.0.0.255 any
!
!ICMP traffic is not inspected by CBAC. To control the type of ICMP traffic at the
!interface, add static access list entries. This example has the following ICMP
!requirements: outgoing ping commands require echo-reply messages to come back,
!outgoing traceroute commands require time-exceeded messages to come back, path MTU
!discovery requires "too-big" messages to come back, and incoming traceroute must be
!allowed. Additionally, permit all "unreachable" messages to come back; that is, if a
!router cannot forward or deliver a datagram, it sends an ICMP unreachable message back
!to the source and drops the datagram.
access-list 106 permit icmp any any echo-reply
access-list 106 permit icmp any 192.168.1.0 0.0.0.255 time-exceeded
access-list 106 permit icmp any 192.168.1.0 0.0.0.255 packet-too-big
access-list 106 permit icmp any 192.168.1.0 0.0.0.255 traceroute
access-list 106 permit icmp any 192.168.1.0 0.0.0.255 unreachable
!
!Permit mail and Web access to a specific server.
access-list 106 permit tcp any host 192.168.1.20 eq smtp
access-list 106 permit tcp any host 192.168.1.20 eq www
!
!Final deny for explicitness. This entry is not required but helps complete the access
!list picture. By default, the final entry in any access list is an implicit deny of IP
!protocol traffic. This ensures that the firewall blocks any traffic not explicitly
!permitted by the access list.
access-list 106 deny ip any any
!
!Access list 51 defines the sites for Java applet blocking. If the access list denies a
```

```

!site, that site is deemed "hostile" and applets from that site are blocked. If the
!access list permits a site, that site is deemed "friendly" and applets from that
!site are not blocked. Java applet blocking is defined in the inspection rule "GO",
!meaning applets are permitted or denied from the sites defined in the access list. In
!this example, access list 51 permits Java applets from any site (source address).
access-list 51 permit any
!
!-----
!Configure the interface.
!-----
!In this example, no ACLs or inspection rules are applied at interface Ethernet0,
!meaning that all traffic on the local network is allowed to go out. This assumes a
!high-level of trust for the users on the local network.
interface Ethernet0
 ip address 192.168.1.104 255.255.255.0
 no ip directed-broadcast
!
!This example uses a dialer profile, so the ACL and CBAC inspection rules are applied
!at the dialer interface, not the physical BRI interface. The dialer pool-member
!command is used to associate the physical interface with a dialer profile.
interface BRI0
 no ip address
 no ip directed-broadcast
 encapsulation ppp
 dialer pool-member 1
 isdn switch-type basic-5ess
!
!-----
!Apply the ACL and CBAC inspection rules at the dialer interface.
!-----
!Through the dialer profile, the ACL and CBAC inspection rules are
!applied to every pool member. In this example, the ACL is applied in, meaning that it
!applies to traffic inbound from the branch office. The CBAC inspection rule STOP is
!applied out, meaning that CBAC monitors the traffic and controls return traffic to the
!router for an existing connection. The CBAC inspection rule GO is applied in,
!protecting against certain types of DoS attacks as described in this document. Note
!that the GO inspection rule does not control return traffic because there is no ACL
!blocking traffic in that direction; however, it does monitor the connections.
interface Dialer0
 ip address <ISDN interface address>
 ip access-group 106 in
 no ip directed-broadcast
 ip inspect STOP out
 ip inspect GO in
 encapsulation ppp
 dialer remote-name <branch office router>
 dialer idle-timeout 500
 dialer string <elided>
 dialer pool 1
 dialer-group 1
 ppp authentication
!
!-----
Additional entries
!-----
!Configure the router to forward packets destined for an unrecognized subnet of
!a directly connected network.
ip classless
!Route traffic to the dialer interface.
ip route 0.0.0.0 0.0.0.0 Dialer0
!Include a dialer list protocol entry to specify the protocol that triggers dialing.
dialer-list 1 protocol ip permit
!Add a user name (name of the router your are configuring) and password for caller
!identification and password authentication with the ISP router.
username <router host name> password 5 <elided>

```

## Two-interface Branch Office Configuration

This sample configuration file describes a firewall configured with CBAC. The firewall is positioned 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 two interfaces configured:

- Interface Ethernet0 connects to the internal protected network
- Interface Serial0 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.
!-----
!
hostname user1-examplecorp-fr
!
boot system flash c1600-fw1600-1
enable secret 5 <elided>
!
username user1 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
!
!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 user1
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 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 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
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 are not 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
```

```

!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 igrp any any
!
!These are the ICMP types actually used...
!administratively-prohibited is useful when you are trying to figure out why
!you cannot 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 unreachable or no unreachable 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
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
    
```

## Multiple Interface Branch Office Configuration

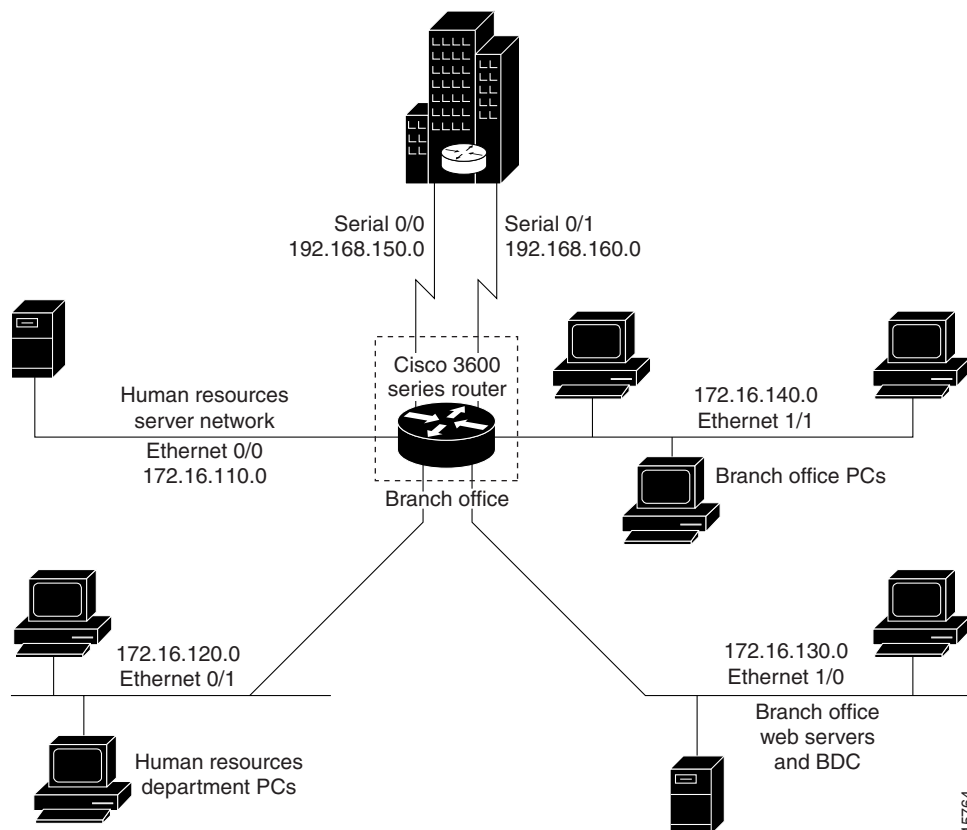
In this configuration example, a single Cisco 3600 series firewall router is positioned at a branch office. It has four internal networks and two WAN connections to the corporate headquarters. CBAC is configured on the firewall to protect two of the internal networks from potential network threats coming from the WAN side and from less secure internal networks. Anti-spoofing protection is added at each interface with client systems. Figure 6 illustrates this configuration.

---

**Note** This example shows a moderately high level of trust by the administrators toward the expected users. Additional protection could be added to this configuration for a situation in a lower level of trust. That configuration would include ICMP filtering statements, significantly more protocol and address control through the use of more restrictive Access Control Lists, and anti-spoofing applied everywhere. This configuration does not contain those additional restrictions because that would detract from the CBAC example.

---

**Figure 6** Sample Cisco IOS Firewall Application Environment



15764

The branch office has this sample network configuration:

- Ethernet interface 0/0 supports the Human Resources department servers. This network includes an email (SMTP and POP3) host and a Windows NT server. The Windows NT server is the Primary Domain Controller (PDC) for the Human Resources domain and has a trust relationship with the rest of the company; however, it contains applications and databases that must not be accessed by the rest of the company or the other groups in the branch office. The devices on this LAN are accessible only by users in the Human Resources department on Ethernet interface 0/1. The Mail server must be able to send and receive email (through SMTP sessions) with all other devices. The Windows 95 machines can use this machine as their email server (for sending email through SMTP sessions) and as a repository for accumulating email that they can then download through POP3 sessions. No one else in the company is allowed to form POP3 sessions to any machine on this LAN.
- Ethernet interface 0/1 supports the Windows 95 computers in the Human Resources department. These users must have access to the Human Resources mail servers located on Ethernet interface 0/0 as well as access to the rest of the company. Access to the Windows NT server resources are controlled through the Windows NT permissions assigned to each user in the Windows NT domain.
- Ethernet interface 1/0 supports the branch office web servers, which can be accessed by everyone in the company. These servers use TCP ports 80 (HTTP) and 443 (SHTTP) for inbound Web access. This network also includes a backup domain controller (BDC) for the overall domain that is also used as file, print, and service server.

Ethernet interface 1/1 supports all users who are not in the Human Resources department. These users have no access to the Human Resources department servers, but they can access the other network interfaces and the serial interfaces for WAN connectivity. Serial interface 0/0 and 0/1 connect to the WAN with T1 links (links to corporate headquarters). In this sample configuration, the Domain Name System (DNS) servers are located somewhere within the rest of the company.

Additionally, network management (SNMP) and Telnet sessions are limited to the management network (192.168.55.0), which is located somewhere within the rest of the company across the serial interface.

```

! -----
! This first section contains some configuration that is not required
! for CBAC, but illustrates good security practices.
! -----
!Add this line to get timestamps on the syslog messages.
service timestamps log datetime localtime show-timezone
!
hostname Router1
!
boot system flash c3600-fw3600-1
!
! Configure AAA user authentication.
aaa new-model
aaa authentication login lista tacacs+ enable
!
enable secret 5 <elided>
ip subnet-zero
!
! Disable source routing to help prevent spoofing.
no ip source-route
!
! Set up the domain name and server IP addresses.
ip domain-name example.com
ip name-server 192.168.55.132
ip name-server 192.168.27.32
!

```

## Configuration Examples

---

```
! The audit-trail command enables the delivery of specific CBAC messages
! through the syslog notification process.
ip inspect audit-trail
!
! Establish the time-out values for DNS queries. When this idle-timer expires,
! the dynamic ACL entries that were created to permit the reply to a DNS request
! will be removed and any subsequent packets will be denied.
ip inspect dns-timeout 10
!
!-----
!The next section includes configuration statements required
!specifically for CBAC.
!-----
! Define the CBAC inspection rule "inspect1", allowing the specified protocols to be
! inspected. The first rule enables SMTP specific inspection. SMTP inspection causes
! the exchange of the SMTP session to be inspected for illegal commands. Any packets
! with illegal commands are dropped, and the SMTP session will hang and eventually
! time out.
ip inspect name inspect1 smtp timeout 300
!
! In the next two lines of inspect1, define the maximum time that each of the UDP and
! TCP sessions are allowed to continue without any traffic passing
! through the router. When these timeouts are reached, the dynamic ACLs that
! are inserted to permit the returning traffic are removed and subsequent packets
! (possibly even valid ones) will not be permitted.
ip inspect name inspect1 udp timeout 300
ip inspect name inspect1 tcp timeout 300
!
! Define the CBAC inspection rule "inspect2", allowing the specified protocols to be
! inspected. These rules are similar to those used in the inspection rule "inspect1,"
! except that on the interfaces where this rule is applied, SMTP sessions are not
! expected to go through; therefore, the SMTP rule element is not applied here.
ip inspect name inspect2 udp timeout 300
ip inspect name inspect2 tcp timeout 3600
!
!-----
! The next section shows the Ethernet interface configuration statements for each
! interface, including access lists and inspections rules.
!-----
! Apply the "inspect1" inspection rule to sessions that are initiated in the outbound
! direction (toward the LAN) at Ethernet interface 0/0. All packets in these sessions
! will be inspected by CBAC. Provided that network traffic passes the Access Control
! List (ACL) restrictions, traffic is then inspected by CBAC for access through the
! Cisco IOS Firewall. Traffic blocked by the access list is not inspected by CBAC.
! Access list 110 is applied to outbound traffic on this interface.
interface Ethernet0/0
description HR_Server Ethernet
ip address 172.16.110.1 255.255.255.0
ip access-group 110 out
no ip directed-broadcast
no ip proxy-arp
ip inspect inspect1 out
no cdp enable
!
! Apply access list 120 to inbound traffic on Ethernet interface 0/1.
! Applying access list 120 to inbound traffic provides anti-spoofing on this interface
! by dropping traffic with a source address matching the IP address on a network other
! than Ethernet 0/1. The IP helper address lists the IP address of the DHCP server on
! Ethernet interface 1/0.
interface Ethernet0/1
description HR_client Ethernet
ip address 172.16.120.1 255.255.255.0
ip access-group 120 in
ip helper-address 172.16.130.66
no ip directed-broadcast
```

```

no ip proxy-arp
no cdp enable
!
! Apply the "inspect2" inspection rule to sessions that are initiated in the outbound
! direction (toward the LAN) at Ethernet interface 1/0. Provided that network traffic
! passes the Access Control List (ACL) restrictions, traffic is then inspected by CBAC
! through the Cisco IOS Firewall. Traffic blocked by the access list is not inspected
! by CBAC. Access list 130 is applied to outbound traffic on this interface.
interface Ethernet1/0
description Web_server Ethernet
ip address 172.16.130.1 255.255.255.0
ip access-group 130 out
no ip directed-broadcast
no ip proxy-arp
ip inspect inspect2 out
no cdp enable
!
! Apply access list 140 to inbound traffic at Ethernet interface 1/1. This
! provides anti-spoofing on the interface by dropping traffic with a source address
! matching the IP address of a network other than Ethernet 1/1. The IP helper address
! lists the IP address of the DHCP server on Ethernet interface 1/0.
interface Ethernet1/1
description Everyone_else Ethernet
ip address 172.16.140.1 255.255.255.0
ip access-group 140 in
ip helper-address 172.16.130.66
no ip directed-broadcast
no ip proxy-arp
no cdp enable
!
!-----
! The next section configures the serial interfaces, including access lists.
!-----
! Apply access list 150 to Serial interfaces 0/0. This provides anti-spoofing on the
! serial interface by dropping traffic with a source address matching the IP address
! of a host on Ethernet interface 0/0, 0/1, 1/0, or 1/1.
interface Serial0/0
description T1 to HQ
ip address 192.168.150.1 255.255.255.0
ip access-group 150 in
bandwidth 1544
!
interface Serial1/1
description T1 to HQ
ip address 192.168.160.1 255.255.255.0
ip access-group 150 in
bandwidth 1544
!
! -----
! Configure routing information.
! -----
router igrp 109
network 172.16.0.0
network 192.168.150.0
network 192.168.160.0
!
! Define protocol forwarding on the firewall. When you turn on a related command,
! ip helper-address, you forward every IP broadcast in the ip forward protocol
! command list, including several which are on by default: TFTP (port 69),
! DNS (port 53), Time service (port 37), NetBIOS Name Server (port 137),
! NetBIOS Datagram Server (port 138), BOOTP client and server datagrams
! (ports 67 and 68), and TACACS service (port 49). One common
! application that requires helper addresses is Dynamic Host Configuration
! Protocol (DHCP). DHCP information is carried inside of BOOTP packets. The
! "no ip forward protocol" statements turn off forwarding for the specified protocols.

```

## Configuration Examples

---

```
no ip forward-protocol udp netbios-ns
no ip forward-protocol udp netbios-dgm
no ip forward-protocol udp tacacs
no ip forward-protocol udp tftp
ip forward-protocol udp bootpc
!
! Add this line to establish where router SYSLOG messages are sent. This includes the
! CBAC messages.
logging 192.168.55.131
!
! -----
! Define the configuration of each access list.
! -----
! Defines Telnet controls in access list 12.
access-list 12 permit 192.168.55.0 0.0.0.255
!
! Defines SNMP controls in access list 13.
access-list 13 permit 192.168.55.12
access-list 13 permit 192.168.55.19
!
! Access list 110 permits TCP and UDP protocol traffic for
! specific ports and with a source address on Ethernet interface 0/1. The access list
! denies IP protocol traffic with any other source and destination address. The
! access list permits ICMP access for any source and destination
! address. Access list 110 is deliberately set up to deny unknown IP protocols
! because no such unknown protocols will be in legitimate use. Access list
! 110 is applied to outbound traffic at Ethernet interface 0/0. In ACL 110,
! network traffic is being allowed access to the ports on any server on the HR server
! network. In less trusted environments, this can be a security problem; however, you
! can limit access more severely by specifying specific destination addresses in the
! ACL statements.
access-list 110 permit tcp 172.16.120.0 0.0.0.255 any eq smtp
access-list 110 permit tcp 172.16.120.0 0.0.0.255 any eq pop3
access-list 110 permit tcp 172.16.120.0 0.0.0.255 any eq 110
access-list 110 permit udp any any eq 137
access-list 110 permit udp any any eq 138
access-list 110 permit udp any any eq 139
access-list 110 permit icmp any any
access-list 110 deny ip any any!
!
! Access-list 120 permits TCP, UDP, and ICMP protocol traffic with a source address
! on Ethernet interface 0/1, but denies all other IP protocol traffic. Access list
! 120 is applied to inbound traffic on Ethernet interface 0/1.
access-list 120 permit tcp 172.16.120.0 0.0.0.255 any
access-list 120 permit udp 172.16.120.0 0.0.0.255 any
access-list 120 permit icmp 172.16.120.0 0.0.0.255 any
access-list 120 deny ip any any
!
! Access list 130 permits TCP, UDP, and ICMP protocol traffic for specific ports and
! with any source and destination address. It opens access to the web server and to
! all NBT services to the rest of the company, which can be controlled through the
! trust relations on the Windows NT servers. The bootpc entry permits access to the
! DHCP server. Access list 130 denies all other IP protocol traffic. Access list 130 is
! applied to outbound traffic at Ethernet interface 1/0.
access-list 130 permit tcp any any eq www
access-list 130 permit tcp any any eq 443
access-list 130 permit tcp any any eq 110
access-list 130 permit udp any any eq 137
access-list 130 permit udp any any eq 138
access-list 130 permit udp any any eq 139
access-list 130 permit udp any any eq bootpc
access-list 130 permit icmp any any
access-list 130 deny ip any any
!
! Access list 140 permits TCP, UDP, and ICMP protocol traffic with a source address on
```

```
! Ethernet interface 1/1, and it denies all other IP protocol traffic. Access list 140
! is applied to inbound traffic at Ethernet interface 1/1.
access-list 140 permit tcp 172.16.140.0 0.0.0.255 any
access-list 140 permit udp 172.16.140.0 0.0.0.255 any
access-list 140 permit icmp 172.16.140.0 0.0.0.255 any
access-list 140 deny ip any any
!
! Access list 150 denies IP protocol traffic with a source address on Ethernet
! interfaces 0/0, 0/1, 1/0, and 1/1, and it permits IP protocol traffic with any other
! source and destination address. Access list 150 is applied to inbound traffic
! on each of the serial interfaces.
access-list 150 deny ip 172.16.110.0 0.0.0.255 any
access-list 150 deny ip 172.16.120.0 0.0.0.255 any
access-list 150 deny ip 172.16.130.0 0.0.0.255 any
access-list 150 deny ip 172.16.140.0 0.0.0.255 any
access-list 150 permit ip any any
!
! Disable Cisco Discovery Protocol.
no cdp run
!
snmp-server community <elided> ro 13
tacacs-server host 192.168.55.2
tacacs-server key <elided>
!
! -----
! Configures the router console port and the virtual terminal line interfaces,
! including AAA authentication at login. Authentication is required for users defined
! in "lista." Access-class 12 is applied on each line, restricting Telnet access to
! connections with a source address on the network management network.
! -----
line console 0
exec-timeout 3 00
login authentication lista
line aux 0
exec-timeout 3 00
login authentication lista
line vty 0
exec-timeout 1 30
login authentication lista
access-class 12 in
line vty 1
exec-timeout 1 30
login authentication lista
access-class 12 in
line vty 2
exec-timeout 1 30
login authentication lista
access-class 12 in
line vty 3
exec-timeout 1 30
login authentication lista
access-class 12 in
line vty 4
exec-timeout 1 30
login authentication lista
access-class 12 in
!
end
```

## Command Reference

None. Cisco IOS Firewall feature set command descriptions are included in the *Security Command Reference*.