Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

CBAC - Cisco IOS Firewall Feature Set Foundations

With the commercial firewall market dominated by expensive firewall products such as those from Checkpoint, Nokia and Cisco (PIX Firewall), many smaller organizations rely on packet filtering technologies and Access-Control Lists (ACLs) on perimeter routers to provide basic firewall features or perimeter defences. Since IOS 11.2(P), Cisco has enhanced the ability of its perimeter routers to perform a basic firewall function with the introduction of the Cisco IOS Firewall feature set. Although not suitable for all situa...

Copyright SANS Institute
Author Retains Full Rights

AD
ONLY ONE INDEPENDENT TEST
MEASURES REAL-WORLD,
ENDPOINT MALWARE PROTECTION.
TREND MICRO SMART PROTECTION NETWORK

CBAC - Cisco IOS Firewall Feature Set foundations

By
Evan Davies

GIAC Security Essentials Assignment ver. 1.3

© SANS Institute 2002, Author retains full rights.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Contents

1.0 Introduction 3
2.0 CBAC operation 3
2.1 Overview 3
2.2 CBAC's Main Functions 4
2.3 The CBAC Process 5
3.0 Supported protocols 5
4.0 CBAC Benefits and Limitation 6
4.1 CBAC Benefits 6
4.2 CBAC Limitations 7
5.0 Router Security 7
5.1 Overview of Router Security and CBAC 7
5.2 Router Security Resources 8
6.0 Configuring CBAC 9
6.1 CBAC Configuration Overview 9
6.2 Determining Services Required 10
6.3 Selecting an Interface 11
6.4 Configuring IP Access Lists 11
6.5 Configuring Global Timeouts and Thresholds 13
6.6 Defining an Inspection Rule 14
6.7 Applying Inspection Rules 14
6.8 Configuring Logging and Audit Trails 15
6.9 testing and Verifying CBAC 15
7.0 Conclusion 16
8.0 References and Further Reading 17
8.1 Bibliography 17
8.2 General Web Site References 18
Appendix A CBAC show commands and SYSLOG log output 19
Appendix B Example CISCO IOS CBAC configuration 21

© SANS Institute 2002, Author retains full rights.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

1.0 Introduction

With the commercial firewall market dominated by expensive firewall products such as those from Checkpoint, Nokia and Cisco (PIX Firewall), many smaller organizations rely on packet filtering technologies and Access-Control Lists (ACLs) on perimeter routers to provide basic firewall features or perimeter defences. Since IOS 11.2(P), Cisco has enhanced the ability of its perimeter routers to perform a basic firewall function with the introduction of the Cisco IOS Firewall feature set. Although not suitable for all situations the Firewall feature set is a substantial improvement over ACL based filters.

Based on the Context-Based Access Control (CBAC) feature, which delivers stateful inspection of TCP and UDP packets and dynamic modification of Access Control Lists (ACL's), the Cisco IOS Firewall Feature set provides a middle ground between a fully functional firewall solution, such as the PIX and Checkpoint solutions, and a hardened Cisco IOS based router with ACL's.

Although limited, CBAC and other features of the Cisco IOS Firewall feature set allow significant flexibility in managing a perimeter Cisco router when compared to a router running the standard version of the Cisco IOS. There are several other features in the IOS firewall feature set, although this paper will not examine them, instead concentrating on the operation and configuration of CBAC.

The Context-Based Access Control (CBAC) feature forms the backbone of the Cisco IOS firewall feature set. This paper will examine the operation of CBAC, it's benefits, limitations, and finally work through the steps involved in configuring CBAC.
The Cisco IOS Firewall feature set will not be the ideal firewall solution for all network administrators but it does have a place in the perimeter security role. The CBAC feature is both;

- A robust stateful inspection based firewall solution for those smaller organizations that may be operating on a tight budget, and who would traditionally rely on packet filtering through ACL's,
- and a possible solution as an internal firewall to separate sensitive sites within your area of control or security domain.

2.0 CBAC Operation

2.1 Overview

CBAC is a stateful packet inspection system that maintains information about certain connections traversing the firewall. CBAC uses that information to dynamically manage extended Access Control Lists that control and manage sessions between the internal and external networks. CBAC is an IP only feature that recognizes TCP, UDP and some higher-layer protocols. It also provides inspection of data beyond the IP header, which allows CBAC to track the state of the session. By examining some of the packet data CBAC not only manages access between the external and internal network but can also scan for certain protocol violations and suspicious activity, blocking traffic and logging the activity.
CBAC works by creating temporary openings in your extended ip access lists at firewall interfaces. It does this by inspecting traffic specified in an "inspect" list, maintaining session state information in a state table and temporarily opening up access lists to allow permitted

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

return traffic to your internal network, providing it is from the same session that triggered the CBAC inspection in the first place.

2.2 CBAC's Main Functions

As suggested above CBAC operation is made up of three main functions including packet inspection, state table maintenance and Access-List entry updates.

Packet Inspection takes place provided the packet is permitted through any relevant access lists. This may include;

1. An inbound ACL from the internal network or;
2. An outbound ACL to the external network,

You must have also configured CBAC to inspect this type of packet. You should also specify an interface and direction where inspection should take place. Any packets denied by an access list are simply dropped and no inspection takes place.

CBAC uses packet inspection and maintains session information to improve on normal access-list operation by being able to do the following;

- CBAC tracks TCP sequence numbers and drops packets with unexpected sequence numbers.
- CBAC will recognize some application specific commands that can be used in application level attacks, blocking those packets.
- CBAC controls UDP sessions by approximating session information and through the use of UDP idle timeout settings.

Timeout and threshold values are used to manage session state information and are an important part of the IOS firewall feature set. CBAC uses these timeout and threshold values to identify sessions that have not become fully established, causing those sessions to be dropped. CBAC can only inspect those protocols specified in the inspection rule-set, so the ability to protect against DOS attacks for example is only extended to those specified protocols in the rule-set.

Following packet inspection, CBAC creates a state table entry or updates existing entries to include information about the state of the session. Any traffic returning to the network from an external source is permitted through based on valid session information existing in the state table. The session information in the state table is updated constantly as traffic passes through the firewall.

Access-list entries are added or deleted dynamically by CBAC based on the session information contained in the state table. Entries are inserted and deleted as the session information changes. Openings created in the ACL's are only temporary and are maintained as long as the session is valid.

Before traffic inspection begins CBAC inspection rules must be created and applied to an interface. CBAC inspection rules are created and applied to an interface, either inbound or outbound in much the same way as access-lists. When a packet attempts to initiate a connection CBAC will use the inspection ruleset to determine if the packet should be inspected and the session state monitored.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

2.3 The CBAC Process

Cisco System's paper on CBAC, *Context-Based Access Control*,
http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t5/iosfw2/iosfw2_2.htm,
outlines the sequence of events in more detail as follows;

- A packet arrives at the router's external interface.
- The router examines the packet and checks it against any applied access lists on any interfaces the packet will pass, and passes or drops the packet accordingly. (Note if the packet is dropped no CBAC inspection takes place).
- The packet is "inspected" by CBAC if a rule exists, (and the protocol is specified for inspection by the inspection rule) and information about the state of the packet's connection is recorded in a new state table created for the connection. If there is no rule specified to inspect that packet type then it is simply forwarded or dropped in accordance with any appropriate access-lists.
- CBAC then creates temporary openings in the inbound access list on the external interface to allow return traffic for this connection. These entries are maintained, added and removed based on changes to the state of the connection as maintained in the state table created above. Note that the access list that is modified must be an extended access list (the Cisco IOS Security Configuration Guide is a good place to start for more information on access lists).
- The outbound packet is then forwarded out the external interface.
- Any return packets for the same connection are allowed back in through the external interface because of openings made in the inbound access list by CBAC.
- Return packets are examined by CBAC and the state table is updated accordingly. Further modifications may be made to the access list to reflect the current state of connection.
- Finally the state table is deleted and any entries in the inbound access-list for this connection are deleted at the completion or timeout of the session.[1]

3.0 Supported Protocols

You need to configure CBAC to inspect protocols that you wish to be inspected from the list of supported protocols below. No packet inspection takes place until you create your ip inspection list(s), which include the protocols or sessions you want inspected. The list is then applied to an interface.
Some packets or sessions may be allowed through the firewall by your existing router access-lists but are not inspected by CBAC. These could be either not specified for inspection in the inspection list, or are not from the available list of protocols below. They are still able to establish sessions and operate through the firewall (if they can pass through all access lists including those affecting the return path) but no session-state monitoring or auditing will take place.

Cisco System's paper on CBAC, *Context-Based Access Control*,

[1] Unknown. *Context-Based Access Control*, Cisco Systems, Date Unknown. Page 7
http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t5/iosfw2/iosfw2_2.htm

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t5/iosfw2/iosfw2_2.htm,
lists the supported protocols as follows;
You can configure CBAC to inspect the following types of sessions;

- All TCP sessions, regardless of the application layer protocol
- All UDP sessions, regardless of the application layer protocol

Specific application layer protocols for inspection. The following application layer protocols can be specified for inspection;

- CU-SeeMe (white pine version only)
- FTP
- H.323
- HTTP (Java blocking)
- Microsoft NetShow
- Unix R-commands
- RealAudio
- RPC (Sun RPC)
- Microsoft RPC
- SMTP
- SQL*Net
- StreamWorks
- TFTP
- VDOLive[2]

ICMP is often a required service for many networks but it is not a supported protocol for CBAC inspection. This is an example of a protocol that, should you wish to allow it through the firewall it must be managed by traditional access-lists. CBAC will still allow the protocol to pass through the firewall (should access-lists applied on the firewall permit the traffic) but no session-state inspection and monitoring, and associated auditing that could be enabled, will take place.

4.0 CBAC Benefits and Limitations

4.1 CBAC Benefits

CBAC has a number of benefits over an IOS based perimeter router using ACLs to control external access to the internal network.

- The stateful packet inspection feature provides a more comprehensive and flexible alternative to controlling traffic flow than normal ACLs, while enabling the Cisco IOS firewall to perform rudimentary attack detection and prevention e.g. DoS attacks can be identified and blocked.
- CBAC controlled session and subsequent changes to ACLs are dynamic and temporary. This greatly reduces the period of time that permitted traffic flows are allowed into the network, reducing the duration of any vulnerabilities for that session type.

[2] Unknown. *Context-Based Access Control*, Cisco Systems, Date Unknown. Page 8
http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t5/iosfw2/iosfw2_2.htm

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

- The alert and audit trail feature enables comprehensive logging of session statistics and can be used in conjunction with host-based and network-based intrusion detection systems to correlate information and identify attempted attacks.
- In environments where traffic flow is largely originated from inside the network the ability of CBAC to dynamically update ACLs enables much tighter control, stronger access-list configuration and potentially less administrative overhead on managing external access-lists.

4.2 CBAC Limitations

CBAC has a number of limitations that may limit its effectiveness in some circumstances.

- CBAC only supports IP protocol traffic and then only TCP and UDP packets are inspected. ICMP traffic is not inspected and must be managed with normal access-lists.
- CBAC will not inspect packets where the source or destination address is the firewall itself, access to the router from the external network must be tightly controlled with traditional access-lists.
- CBAC compatibility with some other Cisco security features is limited with CBAC unable to accurately inspect the payloads of encrypted traffic passing through the firewall and protocol inspection support is limited further if both CBAC and encryption are configured on the firewall itself. CBAC only operates with IPSec if the firewall is an endpoint for IPSec for the traffic flow, CBAC can't inspect the header of an IPSec packet passing through the firewall.
- Redundant IOS firewall's are not supported as firewall session states are internal to a single router (limited interface redundancy within the router itself is supported).
- When enabled, the Cisco IOS Firewall feature set does impact on system resource utilization and you must ensure the router has enough memory and processing power to meet your performance requirements.

5.0 Router Security

5.1 Overview of Router Security and CBAC

Before diving into configuring CBAC, it is critical to get the router IOS configuration securely locked down. No matter how good the CBAC configuration is, if the router itself is open to attack then you may as well not have the firewall software installed in the first place.
The security policy should also be written or updated at this point, to form the basis of configuring security on the router itself, and also configuring the CBAC inspection policies later. Whether you configure the Cisco IOS firewall running on your perimeter router or you have a separate firewall you should still think of this router as a separate device from the firewall and apply the principles of "defense in depth" in insuring security at all levels of your network. The perimeter router and firewall act together to enhance network security and provide perimeter defense.

Building a Cisco IOS firewall installation on a "securely" configured external router is essential as;

1. CBAC relies on the effectiveness of access-list configuration on the router and
2. CBAC can't inspect traffic with a source or destination address of the router.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

This means you cannot rely on CBAC to provide any security for the actual router itself.

5.2 Router Security Resources

Several resources are available online that provide excellent information on securing the perimeter router including (see bibliography for http addresses);

- *Improving Security on Cisco Routers*, Cisco Systems
- *Network Security Policy: Best Practices White Paper*, Cisco Systems
- *Cisco ISP Essentials*, Cisco Systems
- *NSA/SNAC Router Security Configuration Guide*, National Security Agency (NSA)

I would recommend the last two sources for anyone configuring a perimeter router for the first time. There are also several papers submitted by GIAC students that detail Cisco perimeter router configuration guidelines. Below is a brief outline of some of the key points taken from the NSA Guide, however you should refer to the mentioned guide or other sources for more detailed explanations, specific IOS commands and information that may be relevant to your particular situation.

The below mentioned security checklist is taken from the NSA/SNAC Router Security Configuration Guide, and provides a good base to work off when securing your perimeter router; Security Checklist;

- Router security Policy written and up to date.
- Router IOS version checked and up to date.
- Router configuration kept off-line, backed up, access to it limited.
- Router configuration is well documented, commented.
- Router users and passwords configured and maintained.
- Enable passwords difficult to guess, knowledge of it strictly limited.
- Access restrictions imposed on Console, Aux, VTY's.
- Unneeded network services disabled.
- Unused interfaces disabled.
- Risky interface services disabled.
- Port and protocol needs of the network identified and checked.
- Access lists limit traffic to identified ports and protocols.
- Access lists block reserved and inappropriate addresses.
- Static routes configured where necessary.
- Routing protocols configured to use integrity mechanisms.
- Logging enabled and log recipient hosts identified and configured.
- Router's time of day set accurately, maintained with NTP.
- Logging set to include time information.
- Logs checked, reviewed, archived in accordance with local policy.
- SNMP disabled or enabled with hard-to-guess community strings.[3]

[3] Antoine, Vanessa, et al., *NSA/SNAC Router Security Configuration Guide, Executive Summary, Version 1.0c*, National Security Agency, November 2001
http://nsa1.www.conxion.com/cisco/index.html

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

There is a wealth of information in this guide exploring and explaining each point and also providing references to further resources.
All points are important but it is worth taking a close look at the points on SNMP, especially in light of the recent advisory concerning SNMP vulnerabilities;
http://www.cert.org/advisories/CA-2002-03.html

6.0 Configuring CBAC;

6.1 CBAC Configuration Overview

Make sure you have a clear picture of your security policy on which to base your CBAC configuration before continuing, and ensure you have taken the necessary steps to protect your perimeter router. An IOS firewall could easily be compromised by poor router security practices.

The following tasks are required for effectively configuring CBAC, This list is largely based on similar lists from the *NSA/SNAC Router Security Configuration Guide*, page 188, and Cisco System's paper on CBAC, *Context-Based Access Control*, page 11 (both referenced in the Bibliography).

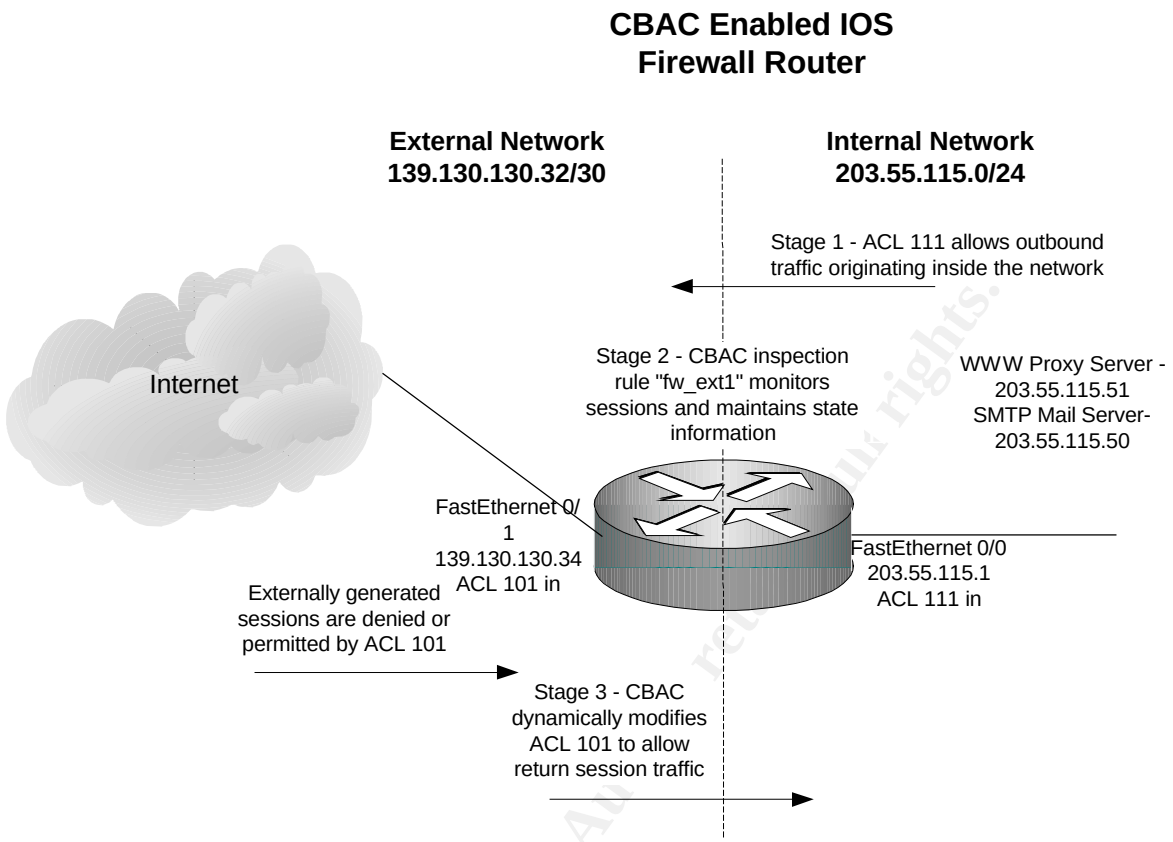
1. Determine the list of services that users from your network need to access from the external untrusted network.
2. Select an interface – either internal or external
3. Configure IP access lists at the interface
4. Configure global timeouts and thresholds
5. Define an inspection rule
6. Apply the inspection rule to an interface
7. Configure logging and Audit Trail
8. Test and Verify CBAC

Below is a network diagram that we will base a CBAC configuration on, while working through each of the above tasks.
The network diagram details

1. Our internal and external networks for our configuration example
2. Their associated ip address ranges,
3. The main stages of CBAC operation (stages 1 – 3),
4. The ACL implementation.

Refer back the this diagram while working through each step in the configuration process;

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.



6.2 Determine Services Required

We need to determine what services users require access to that are located on the external network. We also need to determine if any services are located on the external network that are to be allowed to establish a session to any internal services e.g. SMTP.

Keep this in the context of your security policy. Identify which protocols will be permitted using CBAC from the list of supported protocols above (section 3.0).

Generally we would deny all protocols except those we have identified as needed. If the protocol is not on the list of specific application layer protocols above and is a TCP or UDP protocol, then you must include TCP or UDP in your inspection ruleset.

ICMP is not supported by CBAC, and if required the ACLs must allow both outbound and inbound sessions, rather than relying on CBAC to open a return path in the external access list.

This list of supported services will be the basis of our access lists and our inspection rulesets.

In our example we have a WEB proxy server and an SMTP mail server on the internal network. We want to allow the following access through the firewall;

Services allowed originating from trusted Network to untrusted network;

Source	Destination	Services Required
Web Proxy Server – 203.55.115.51	Any	HTTP DNS

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

		FTP
SMTP Server – 203.55.115.50	Any	SMTP DNS
203.55.115.0/24	Any	ICMP

Services Allowed originating from untrusted network to trusted network;

Source	**Destination**	**Services Required**
Any external addresses	SMTP Server – 203.55.115.50	SMTP

6.3 Selecting an Interface

You will need to determine which interface to configure CBAC on. If your network configuration involves only a single internal interface and a single external interface you would most likely apply CBAC configurations on the external interface (that connected to the untrusted or external network).
Should you have a configuration including a DMZ or multiple external network connections terminated at the router you may opt to configure CBAC on the internal interface.
This would allow for more open access to the DMZ from any external source while restricting access into the internal network to only that of return traffic for sessions initiated from inside your network (you should still implement strategies to protect your DMZ, including limiting permitted traffic to required services, host based IDS etc. – something in line with your security policy).

In our example we only have 2 interfaces and we will apply the CBAC ruleset on the external interface.

6.4 Configure IP Access Lists

Make sure you have a good understanding of how access lists work. There is a wealth of information on the Cisco web site; you can start with (hyperlinks below in Bibliography);

- *The Cisco IOS Security Configuration Guide*, Cisco Systems,
- *Configuring Network Security*, Cisco Systems,
- *NSA/SNAC Router Security Configuration Guide*, National Security Agency (NSA)

The access lists provide the foundation upon which CBAC builds and if they are not configured correctly you run the risk of introducing security risks to the firewall.

In a basic configuration we would usually have two access-lists;

1. An access-list that permits the desired protocols you have determined from step 1 to pass from the trusted network to the untrusted network (this access-list will pass traffic that CBAC will inspect).
2. A second access-list must be configured to block all traffic from the untrusted network to the trusted network.

This would be configured to block sessions that you wish CBAC to inspect.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

NOTE - CBAC will update this access-list(s) dynamically and add rules to allow return traffic to enter the trusted network. Exceptions to this rule would be to allow sessions you have deemed necessary that can be established from the untrusted network e.g. in our example we want to allow SMTP servers to establish sessions with our internal SMTP server and we want to allow some ICMP traffic – this traffic will not be managed by CBAC.

For our configuration we will apply two extended access-lists;

1. Access-list 101 will be applied on the internal interface (FastEthernet 0/0), and will permit traffic from our internal network to pass through the firewall to the external network. In our example we only want to allow traffic from the web and smtp server. You may want to start with a less restrictive access-list and allow all addresses from the internal network to access the external environment (this will largely be influenced by your internal security policy – in our case we don't want to allow users to connect to the web without going through the proxy server).
2. Access-list 111 will be applied to the external interface (FastEthernet 0/1), and will deny nearly all traffic that originates from the external network. In our case we have elected to allow some ICMP traffic through, and also SMTP sessions that will originate from the external network when sending mail to our SMTP server on the internal network (these sessions will not be monitored by CBAC).

Access-List 101

```
! IP address spoof protection, deny internal addresses
access-list 101 deny   ip 203.55.115.0 0.0.0.255 any log
! Protect against Land attack
access-list 101 deny   ip host 139.130.130.34 host 139.130.130.34
log
! IP address spoof protection
access-list 101 deny   ip 127.0.0.0 0.255.255.255 any log
access-list 101 deny   ip 10.0.0.0 0.255.255.255 any log
access-list 101 deny   ip 0.0.0.0 0.255.255.255 any log
access-list 101 deny   ip 172.16.0.0 0.15.255.255 any log
access-list 101 deny   ip 192.168.0.0 0.0.255.255 any log
access-list 101 deny   ip 192.0.2.0 0.0.0.255 any log
access-list 101 deny   ip 169.254.0.0 0.0.255.255 any log
access-list 101 deny   ip any host 203.55.115.255 log
access-list 101 deny   ip any host 203.55.115.0 log
access-list 101 deny   ip host 255.255.255.255 any log
access-list 101 deny   ip host 0.0.0.0 any log
! Permit external SMTP traffic to internal SMTP server
access-list 101 permit tcp any host 203.55.115.50 eq smtp
! ICMP filters
access-list 101 deny   icmp any any redirect log
access-list 101 deny   icmp any any echo log
access-list 101 deny   icmp any any mask-request log
access-list 101 permit icmp any 203.55.115.0 0.0.0.255
! Deny all and log port numbers
access-list 101 deny   tcp any range 0 65535 any range 0 65535 log
access-list 101 deny   udp any range 0 65535 any range 0 65535 log
access-list 101 deny   ip any any log
```


© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Access-List 111

```
! Permit internal traffic from approved list
access-list 111 permit tcp host 203.55.115.51 any eq www
access-list 111 permit tcp host 203.55.115.50 any eq smtp
access-list 111 permit udp host 203.55.115.50 any eq domain
access-list 111 permit udp host 203.55.115.51 any eq domain
access-list 111 permit tcp host 203.55.115.51 any eq ftp
access-list 111 permit icmp 203.55.115.0 255.255.255.0 any
! Deny all and log port numbers
access-list 111 deny   tcp any range 0 65535 any range 0 65535 log
access-list 111 deny   udp any range 0 65535 any range 0 65535 log
access-list 111 deny   ip any any log
```

6.5 Configuring Global Timeouts and Thresholds

A critical part of the session management that CBAC performs is achieved through timeout and threshold values that can be set globally. CBAC uses these timeout and threshold values to determine how long to manage state information and make decisions on whether or not to drop sessions. The values are set to determine such timeouts as;

- The length of time to wait for a TCP session to reach established state
- The length of time to manage a TCP session after no activity
- DNS name lookup inspection timeouts
- Maximum number of half-open sessions maintained
- UDP idle timeouts.

You should refer to Cisco documentation for a complete list of timeout and threshold settings available including their default values. The NSA/SNAC Router Security Configuration guide recommends adjusting the following default values depending on your network speed.

Timeout Name	Description	Default	Suggested
Synwait-time	Length of time CBAC waits for a new TCP session to reach established state	30 sec	15 sec
Finwait-time	Length of time CBAC continues to manage a TCP session after it has been closed down by a FIN exchange	5 sec	1 sec
TCP idle-time	Length of time that CBAC continues to manage a TCP session with no activity	1 hour	30 min
UDP idle-time	Length of time that CBAC continues to manage a UCP "session" with no activity	30 sec	15 sec

The IOS configuration commands to set these parameters are as follows;

```
Router(config)# ip inspect udp idle-time 15
Router(config)# ip inspect tcp idle-time 1800
Router(config)# ip inspect tcp finwait-time 1
Router(config)# ip inspect tcp synwait-time 15
```


© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

6.6 Defining an Inspection Rule

You must define at least one inspection rule that specifies what IP traffic you want CBAC to inspect from the above list of supported protocols (section 3.0). The inspection rule is made up of series of statements with each statement containing the following;

- The inspect "name" used to describe this inspection rule
- The protocol you wish to be inspected,
  - either an application layer protocol
  - generic TCP or
  - generic UDP.
- Options including;
  - alert on or off,
  - audit-trail on or off,
  - a specific timeout value, which overrides the TCP or UDP global timeout settings.

Application protocol inspection takes precedence over TCP or UDP inspection. Should a rule have settings configured for both an application, e.g. HTTP, as well as TCP, then the HTTP settings will be used for any HTTP sessions CBAC inspects.

NOTE - that if a protocol is allowed through the access-lists (inbound and outbound) but is not specified in an inspection rule, then any sessions for that protocol will be allowed through the firewall and will not be monitored by CBAC.

In our example we will configure CBAC to inspect sessions as determined in step 1. These include http, ftp, smtp and dns.

```
Router(config)# ip inspect name fw_ext1 ftp audit-trail on
Router(config)# ip inspect name fw_ext1 smtp audit-trail on
Router(config)# ip inspect name fw_ext1 http audit-trail on
Router(config)# ip inspect name fw_ext1 udp audit-trail on
```

The last line allows inspection of DNS. In each case we have enabled an audit-trail to log session information to a syslog server.

6.7 Applying Inspection Rules

Inspection rules need to be applied to an interface much like access-lists. You would usually only apply an inspection rule in one direction, however it is possible to apply inspection rules both ways. Most configurations would apply an outbound inspection rule to be placed on the external interface. The following interface command is used to apply an inspection rule;

Router(config-if)# **ip inspect *inspection-name* {in | out}**

In our example we want to enable the inspection ruleset "fw_ext1" defined above on the external interface to inspect traffic outbound from the interface.

```
Router(config)# interface fastethernet 0/1
Router(config-if)# ip inspect fw_ext1 out
```


© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

6.8 Configure Logging and Audit Trail

The Cisco IOS firewall feature set supports logging to a syslog server. Logging and audit-trails are valuable tools in maintaining your perimeter security and provide information to enhance your intrusion detection capability. Refer to the Router Security Configuration Guide from NSA as mentioned above and/or Cisco documentation for global configuration commands to turn on logging and audit trail messages. Ensure that you have an external syslog server available to send logs to. They can quickly fill up allocated space on the firewall should they be stored locally and older messages will be purged. Ensure the server is secure and that logs are reviewed and backed up regularly. Also ensure you have the correct date and time stamp on messages being logged, use an NTP server to set the router clock.

Below, we will

- Turn on logging
- Set the syslog server ip address (in this case our Web Proxy 203.55.115.51 but normally you would probably want to have a separate syslog server and ensure it is secure),
- Set the logging level (level 6 and above),
- Ensure logging includes time and date stamp (make sure you verify the router has the correct time, and better still, use a NTP server to set accurate time on the router).

```
Router(config)# logging on
Router(config)# logging 203.55.115.50
Router(config)# logging facility local6
Router(config)# logging trap debugging
Router(config)# service timestamps log datetime localtime show-timezone
```

6.9 Testing and Verifying CBAC

In testing the CBAC configuration, verify internal users can access resources they require from a host on the internal network using the protocols you specified in the inspection rule. Test each inspected protocol and verify CBAC operation with the following show commands;

Router# **show ip inspect session [detail]**
Shows sessions currently being maintained by CBAC

Router# **show ip inspect name *inspection-name***
Shows a configured inspection rule

Router# **show ip inspect config**
Shows complete inspection configuration

Router# **show ip inspect all**
Shows all CBAC configuration and existing session information

I would suggest you also verify the effectiveness of your ACL's protecting your external network and the security of your firewall for direct access from an external source. Finally, review the syslog messages regularly.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Appendix A includes some example output from the above show commands and sections of logs from our example configuration;

5.0 Conclusion

The Cisco IOS Firewall Feature Set is a valuable enhancement to the standard IOS feature set. It fills the middle ground between a fully featured firewall solution and a packet filtering strategy based on ACLs. It is an attractive option for organizations that want to leverage existing hardware in their perimeter router to provide some firewall functionality. The IOS firewall can also play an important role in a layered defense strategy.

Organizations with a tight budget and/or organizations that may have a requirement for several distributed firewalls internal to the organizations network, will find the IOS firewall feature set worth a look.

This paper has only touched on the CBAC features of the firewall feature set and it is worth looking further at some of the other features supported. These include;

- Limited intrusion detection capabilities,
- Authentication proxy capabilities,
- Customized port to application mapping (PAM) etc.

It will be interesting to see just how much the integration of additional security features, and improvements to the firewall feature set's existing features, will develop over time. Performance will be an issue in many situations, and some people will argue that the perimeter router is there to route and the firewall function should be performed elsewhere. Planning for the extra demand the IOS firewall feature set will make on the router is critical. You need to ensure adequate memory is available to support the anticipated number of sessions through the firewall. Although from a pure security point of view a Checkpoint, PIX or Nokia solution may be superior, the Cisco IOS firewall feature set could provide a better fit for specific scenarios.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

8.0 References and Further Reading

8.1 Bibliography

Antoine, Vanessa, et al., *NSA/SNAC Router Security Configuration Guide Version 1.0j*, National Security Agency, November 2001
http://nsa1.www.conxion.com/cisco/index.html

Antoine, Vanessa, et al., *NSA/SNAC Router Security Configuration Guide, Executive Summary, Version 1.0c*, National Security Agency, November 2001
http://nsa1.www.conxion.com/cisco/index.html

Wenstrom, Michael., *Managing Cisco Network Security*, Cisco Press, 2001.

McIntyre, Robert., *Cisco's hidden gem: The IOS firewall*, TechRepublic 13 December 2001.
URL: http://www.zdnet.com.au/newstech/security/story/0,2000024985,20262359-1,00.htm

Unknown. *Benefits and Limitations of Context Based Access Control*, Cisco Systems, Date Unknown.
http://www.cisco.com/warp/public/110/36.html

Unknown. *Cisco IOS Firewall Feature Set and Context-Based Access Control*, Cisco Systems, Date Unknown.
http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113t/113t_3/firewall.htm

Unknown. *Cisco IOS Firewall Overview*, Cisco Systems, Date Unknown.
http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/secur_c/scprt3/scfirewl.htm

Unknown. *Cisco IOS Security Configuration Guide, Release 12.2*, Cisco Systems, Date Unknown.
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/

Unknown. *Cisco IOS Security Command Reference, Release 12.2*, Cisco Systems, Date Unknown.
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_r/

Unknown. *Configuring Context-Based Access Control*, Cisco Systems, Date Unknown.
http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/secur_c/scprt3/sccbac.htm

Unknown. *Configuring Network Security*, Cisco Systems, Date Unknown.
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/ios127xe/config/secure.htm

Unknown. *Context-Based Access Control*, Cisco Systems, Date Unknown.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t5/iosfw2/iosfw2_2.htm

Unknown. *Context-Based Access Control Commands*, Cisco Systems, Date Unknown.
http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/secur_r/srprt3/srdcbac.htm

Unknown. *Context-Based Access Control: Introduction and Configuration*, Cisco Systems, Date Unknown.
http://www.cisco.com/warp/public/110/32.html

Unknown. *Cisco ISP Essentials*, Cisco Systems, Date Unknown.
http://www.cisco.com/public/cons/isp/essentials/IOS_Essentials_2-9.pdf

Unknown. *Improving Security on Cisco Routers*, Cisco Systems, Date Unknown.
http://www.cisco.com/warp/public/707/21.html

Unknown. *Increasing Security on IP Networks*, Cisco Systems, Date Unknown
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ics/cs003.htm

Unknown. *Network Security Policy: Best Practices White Paper*, Cisco Systems, Date Unknown
http://www.cisco.com/warp/public/126/secpol.html

8.2 General Web Site References

Cisco Documentation

Cisco Security Technical Tips page
http://www.cisco.com/warp/public/707/index.shtml

Documentation Home Page
http://www.cisco.com/univercd/home/home.htm

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Appendix A – CBAC show commands and SYSLOG log output.

```
Router#show ip inspect session detail
Terminating Sessions
Session 8107AC3C (203.55.115.51:1574)=>(139.130.130.33:80) http SIS_CLOSING
  Created 00:00:03, Last heard 00:00:02
  Bytes sent (initiator:responder) [338:455] acl created 1
  Inbound access-list 101 applied to interface FastEthernet0/1

Router#sh ip inspect name fw_ext1
Inspection name fw_ext1
   ftp alert is on audit-trail is on timeout 1800
   smtp alert is on audit-trail is on timeout 1800
   http alert is on audit-trail is on timeout 1800
   udp alert is on audit-trail is on timeout 15

Router#sh ip inspect config
Session audit trail is disabled
Session alert is enabled
one-minute (sampling period) thresholds are [400:500] connections
max-incomplete sessions thresholds are [400:500]
max-incomplete tcp connections per host is 50. Block-time 0 minute.
tcp synwait-time is 15 sec -- tcp finwait-time is 1 sec
tcp idle-time is 1800 sec -- udp idle-time is 15 sec
dns-timeout is 5 sec
Inspection Rule Configuration
 Inspection name fw_ext1
   ftp alert is on audit-trail is on timeout 1800
   smtp alert is on audit-trail is on timeout 1800
   http alert is on audit-trail is on timeout 1800
   udp alert is on audit-trail is on timeout 15

Router#sh ip inspect all
Session audit trail is disabled
Session alert is enabled
one-minute (sampling period) thresholds are [400:500] connections
max-incomplete sessions thresholds are [400:500]
max-incomplete tcp connections per host is 50. Block-time 0 minute.
tcp synwait-time is 15 sec -- tcp finwait-time is 1 sec
tcp idle-time is 1800 sec -- udp idle-time is 15 sec
dns-timeout is 5 sec
Inspection Rule Configuration
 Inspection name fw_ext1
   ftp alert is on audit-trail is on timeout 1800
   smtp alert is on audit-trail is on timeout 1800
   http alert is on audit-trail is on timeout 1800
```


© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

udp alert is on audit-trail is on timeout 15

Interface Configuration
Interface FastEthernet0/1
Inbound inspection rule is not set
Outgoing inspection rule is fw_ext1
ftp alert is on audit-trail is on timeout 1800
smtp alert is on audit-trail is on timeout 1800
http alert is on audit-trail is on timeout 1800
udp alert is on audit-trail is on timeout 15

Example SYSLOG output;

Output of the auditing logs from CBAC;
Including;

- date/time on syslog server
- address of source device sending the logs
- date/time from source
- description of the source of the logs (e.g AUDIT_TRAIL: http)
- Source and destination IP and port numbers

Feb 15 10:23:40 203.55.115.1 199: Feb 15 10:23:19 UTC: %FW-6-SESS_AUDIT_TRAIL: http session initiator (203.55.115.51:1109) sent 260 bytes -- responder (139.130.130.33:80) sent 3368 bytes

Feb 15 10:23:40 203.55.115.1 200: Feb 15 10:23:19 UTC: %FW-6-SESS_AUDIT_TRAIL: http session initiator (203.55.115.51:1107) sent 383 bytes -- responder (139.130.130.33:80) sent 13715 bytes

Feb 15 10:23:40 203.55.115.1 201: Feb 15 10:23:19 UTC: %FW-6-SESS_AUDIT_TRAIL: http session initiator (203.55.115.51:1110) sent 260 bytes -- responder (139.130.130.33:80) sent 455 bytes

Feb 15 10:23:40 203.55.115.1 202: Feb 15 10:23:19 UTC: %FW-6-SESS_AUDIT_TRAIL: http session initiator (203.55.115.51:1111) sent 269 bytes -- responder (139.130.130.33:80) sent 1367 bytes

Output of access-list violations logged from the router;

Feb 15 09:15:09 203.55.115.1 111: Feb 15 09:14:47 UTC: %SEC-6-IPACCESSLOGP: list 111 denied tcp 203.55.115.51(1552) -> 139.130.130.33(23), 2 packets

Feb 15 09:15:57 203.55.115.1 112: Feb 15 09:15:35 UTC: %SEC-6-IPACCESSLOGP: list 101 denied tcp 139.130.130.33(1217) -> 203.55.115.1(23), 1 packet

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Feb 15 09:16:38 203.55.115.1 113: Feb 15 09:16:16 UTC: %SEC-6-IPACCESSLOGP: list 111 denied tcp 203.55.115.51(1593) -> 139.130.130.33(25), 1 packet

Appendix B – Example CISCO IOS CBAC configuration.

The router configuration below is from a lab test configuration. Any IP addressing used is randomly selected and does not represent a real network on the internet.

```
Current configuration : 3268 bytes
!
version 12.2
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log datetime localtime show-timezone
service password-encryption
!
hostname Router
!
logging rate-limit console 10 except errors
enable secret 5 <removed>
!
no ip subnet-zero
no ip source-route
!
!
no ip finger
!
no ip bootp server
ip inspect udp idle-time 15
ip inspect tcp idle-time 1800
ip inspect tcp finwait-time 1
ip inspect tcp synwait-time 15
ip inspect name fw_ext1 ftp audit-trail on
ip inspect name fw_ext1 smtp audit-trail on
ip inspect name fw_ext1 http audit-trail on
ip inspect name fw_ext1 udp audit-trail on
ip audit notify log
ip audit po max-events 100
no ip dhcp-client network-discovery
!
!
!
interface FastEthernet0/0
 ip address 203.55.115.1 255.255.255.0
 ip access-group 111 in
 duplex auto
 speed auto
 no cdp enable
!
interface Serial0/0
 no ip address
 shutdown
 no cdp enable
```


© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

```
!
interface FastEthernet0/1
 ip address 139.130.130.34 255.255.255.252
 ip access-group 101 in
 ip inspect fw_ext1 out
 duplex auto
 speed auto
 no cdp enable
!
ip classless
no ip http server
!
logging trap debugging
logging facility local6
logging 203.55.115.51
access-list 9 permit 203.55.115.39
access-list 9 permit 203.55.115.38
access-list 101 deny   ip 203.55.115.0 0.0.0.255 any log
access-list 101 deny   ip host 139.130.130.34 host 139.130.130.34 log
access-list 101 deny   ip 127.0.0.0 0.255.255.255 any log
access-list 101 deny   ip 10.0.0.0 0.255.255.255 any log
access-list 101 deny   ip 0.0.0.0 0.255.255.255 any log
access-list 101 deny   ip 172.16.0.0 0.15.255.255 any log
access-list 101 deny   ip 192.168.0.0 0.0.255.255 any log
access-list 101 deny   ip 192.0.2.0 0.0.0.255 any log
access-list 101 deny   ip 169.254.0.0 0.0.255.255 any log
access-list 101 deny   ip any host 203.55.115.255 log
access-list 101 deny   ip any host 203.55.115.0 log
access-list 101 deny   ip host 255.255.255.255 any log
access-list 101 deny   ip host 0.0.0.0 any log
access-list 101 permit tcp any host 203.55.115.50 eq smtp
access-list 101 deny   icmp any any redirect log
access-list 101 deny   icmp any any echo log
access-list 101 deny   icmp any any mask-request log
access-list 101 permit icmp any 203.55.115.0 0.0.0.255
access-list 101 deny   tcp any range 0 65535 any range 0 65535 log
access-list 101 deny   udp any range 0 65535 any range 0 65535 log
access-list 101 deny   ip any any log
access-list 111 permit tcp host 203.55.115.51 any eq www
access-list 111 permit tcp host 203.55.115.50 any eq smtp
access-list 111 permit udp host 203.55.115.50 any eq domain
access-list 111 permit udp host 203.55.115.51 any eq domain
access-list 111 permit tcp host 203.55.115.51 any eq ftp
access-list 111 permit icmp 203.55.115.0 0.0.0.255 any
access-list 111 deny   tcp any range 0 65535 any range 0 65535 log
access-list 111 deny   udp any range 0 65535 any range 0 65535 log
access-list 111 deny   ip any any log
no cdp run
!
line con 0
 exec-timeout 5 0
 password 7 <removed>
 login
 transport input telnet
line aux 0
line vty 0 4
 access-class 9 in
```


© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

```
 exec-timeout 5 0
 password 7 <removed>
 login
 transport input telnet
line vty 5 15
 access-class 9 in
 exec-timeout 5 0
 password 7 <removed>
 login
 transport input telnet
!
no scheduler allocate
end
```

© SANS Institute 2002, Author retains full rights.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: August 28th, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

FOR578 Cyber Threat Intelligence	**Tysons Corner, VAUS**	**Aug 31, 2015 - Sep 04, 2015**	**Live Event**
SANS Milan 2015	**Milan, IT**	**Sep 07, 2015 - Sep 12, 2015**	**Live Event**
SANS Crystal City 2015	**Crystal City, VAUS**	**Sep 08, 2015 - Sep 13, 2015**	**Live Event**
SANS Network Security 2015	**Las Vegas, NVUS**	**Sep 12, 2015 - Sep 21, 2015**	**Live Event**
SANS Seoul 2015	**Seoul, KR**	**Sep 14, 2015 - Sep 19, 2015**	**Live Event**
SANS Baltimore 2015	**Baltimore, MDUS**	**Sep 21, 2015 - Sep 26, 2015**	**Live Event**
Data Breach Investigation Summit & Training	**Dallas, TXUS**	**Sep 21, 2015 - Sep 26, 2015**	**Live Event**
SANS Perth 2015	**Perth, AU**	**Sep 21, 2015 - Sep 26, 2015**	**Live Event**
SANS Tallinn 2015	**Tallinn, EE**	**Sep 21, 2015 - Sep 26, 2015**	**Live Event**
SANS ICS Amsterdam 2015	**Amsterdam, NL**	**Sep 22, 2015 - Sep 28, 2015**	**Live Event**
SANS Bangalore 2015	**Bangalore, IN**	**Sep 28, 2015 - Oct 17, 2015**	**Live Event**
SANS DFIR Prague 2015	**Prague, CZ**	**Oct 05, 2015 - Oct 17, 2015**	**Live Event**
SANS Seattle 2015	**Seattle, WAUS**	**Oct 05, 2015 - Oct 10, 2015**	**Live Event**
SOS: SANS October Singapore 2015	**Singapore, SG**	**Oct 12, 2015 - Oct 24, 2015**	**Live Event**
SANS Tysons Corner 2015	**Tysons Corner, VAUS**	**Oct 12, 2015 - Oct 17, 2015**	**Live Event**
GridSecCon 2015	**Philadelphia, PAUS**	**Oct 13, 2015 - Oct 13, 2015**	**Live Event**
SANS Gulf Region 2015	**Dubai, AE**	**Oct 17, 2015 - Oct 29, 2015**	**Live Event**
SANS Cyber Defense San Diego 2015	**San Diego, CAUS**	**Oct 19, 2015 - Oct 24, 2015**	**Live Event**
SANS Tokyo Autumn 2015	**Tokyo, JP**	**Oct 19, 2015 - Oct 31, 2015**	**Live Event**
SANS Sydney 2015	**Sydney, AU**	**Nov 09, 2015 - Nov 21, 2015**	**Live Event**
SANS South Florida 2015	**Fort Lauderdale, FLUS**	**Nov 09, 2015 - Nov 14, 2015**	**Live Event**
SANS London 2015	**London, GB**	**Nov 14, 2015 - Nov 23, 2015**	**Live Event**
Pen Test Hackfest Summit & Training	**Alexandria, VAUS**	**Nov 16, 2015 - Nov 23, 2015**	**Live Event**
SANS Hyderabad 2015	**Hyderabad, IN**	**Nov 24, 2015 - Dec 04, 2015**	**Live Event**
SANS Chicago 2015	**OnlineILUS**	**Aug 30, 2015 - Sep 04, 2015**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**