

Context–Based Access Control (CBAC): Introduction and Configuration

Document ID: 13814

Introduction

Prerequisites

- Requirements

- Components Used

- Conventions

Background Information

What Traffic Do You Want to Let Out?

What Traffic Do You Want to Let In?

- Extended IP Access List 101

- Extended IP Access List 102

- Extended IP Access List 102

What Traffic Do You Want to Inspect?

Related Information

Introduction

The Context–Based Access Control (CBAC) feature of the Cisco IOS® Firewall Feature Set actively inspects the activity behind a firewall. CBAC specifies what traffic needs to be let in and what traffic needs to be let out by using access lists (in the same way that Cisco IOS uses access lists). However, CBAC access lists include ip inspect statements that allow the inspection of the protocol to make sure that it is not tampered with before the protocol goes to the systems behind the firewall.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Background Information

CBAC can also be used with Network Address Translation (NAT), but the configuration in this document deals primarily with pure inspection. If you perform NAT, your access lists need to reflect the global addresses, not the real addresses.

Prior to configuration, consider these questions.

- What traffic do you want to let out?
- What traffic do you want to let in?
- What traffic do you want to inspect?

What Traffic Do You Want to Let Out?

What traffic you want to let out depends on your site security policy, but in this general example everything is permitted outbound. If your access list denies everything, then no traffic can leave. Specify outbound traffic with this extended access list:

```
access-list 101 permit ip [source-network] [source-mask] any
access-list 101 deny ip any any
```

What Traffic Do You Want to Let In?

What traffic you want to let in depends on your site security policy. However, the logical answer is anything that does not damage your network.

In this example, there is a list of traffic that seems logical to let in. Internet Control Message Protocol (ICMP) traffic is generally acceptable, but it can allow some possibilities for DOS attacks. This is a sample access list for incoming traffic:

Extended IP Access List 101

```
permit tcp 10.10.10.0 0.0.0.255 any (84 matches)
permit udp 10.10.10.0 0.0.0.255 any
permit icmp 10.10.10.0 0.0.0.255 any (3 matches)
deny ip any any
```

Extended IP Access List 102

```
permit eigrp any any (486 matches)
permit icmp any 10.10.10.0 0.0.0.255 echo-reply (1 match)
permit icmp any 10.10.10.0 0.0.0.255 unreachable
permit icmp any 10.10.10.0 0.0.0.255 administratively-prohibited
permit icmp any 10.10.10.0 0.0.0.255 packet-too-big
permit icmp any 10.10.10.0 0.0.0.255 echo (1 match)
permit icmp any 10.10.10.0 0.0.0.255 time-exceeded
deny ip any any (62 matches)

access-list 101 permit tcp 10.10.10.0 0.0.0.255 any
access-list 101 permit udp 10.10.10.0 0.0.0.255 any
access-list 101 permit icmp 10.10.10.0 0.0.0.255 any
access-list 101 deny ip any any

access-list 102 permit eigrp any any
access-list 102 permit icmp any 10.10.10.0 0.0.0.255 echo-reply
access-list 102 permit icmp any 10.10.10.0 0.0.0.255 unreachable
access-list 102 permit icmp any 10.10.10.0 0.0.0.255 administratively-prohibited
access-list 102 permit icmp any 10.10.10.0 0.0.0.255 packet-too-big
access-list 102 permit icmp any 10.10.10.0 0.0.0.255 echo
access-list 102 permit icmp any 10.10.10.0 0.0.0.255 time-exceeded
access-list 102 deny ip any any
```

Access list 101 is for the outbound traffic. Access list 102 is for the inbound traffic. The access lists permit only a routing protocol, Enhanced Interior Gateway Routing Protocol (EIGRP), and specified ICMP inbound traffic.

In the example, a server on the Ethernet side of the router is not accessible from the Internet. The access list blocks it from establishing a session. To make it accessible, the access list needs to be modified to allow the conversation to occur. To change an access list, remove the access list, edit it, and reapply the updated access list.

Note: The reason that you remove the access-list 102 before edit and reapply, is due to the "deny ip any any" at the end of the access list. In this case, if you were to add a new entry before you remove the access-list, the new entry appears after the deny. Therefore, it is never checked.

This example adds the Simple Mail Transfer Protocol (SMTP) for 10.10.10.1 only.

Extended IP Access List 102

```

permit eigrp any any (385 matches)
permit icmp any 10.10.10.0 0.0.0.255 echo-reply
permit icmp any 10.10.10.0 0.0.0.255 unreachable
permit icmp any 10.10.10.0 0.0.0.255 administratively-prohibited
permit icmp any 10.10.10.0 0.0.0.255 packet-too-big
permit icmp any 10.10.10.0 0.0.0.255 echo
permit icmp any 10.10.10.0 0.0.0.255 time-exceeded
permit tcp any host 10.10.10.1 eq smtp (142 matches)

```

*!--- In this example, you inspect traffic that has been
!--- initiated from the inside network.*

What Traffic Do You Want to Inspect?

The CBAC within Cisco IOS supports:

Keyword Name	Protocol
cuseeme	CUSEeMe Protocol
ftp	File Transfer Protocol
h323	H.323 Protocol (for example Microsoft NetMeeting or Intel Video Phone)
http	HTTP Protocol
rcmd	R commands (r-exec, r-login, r-sh)
realaudio	Real Audio Protocol
rpc	Remote Procedure Call Protocol
smtp	Simple Mail Transfer Protocol
sqlnet	SQL Net Protocol
streamworks	StreamWorks Protocol
tcp	Transmission Control Protocol
tftp	TFTP Protocol
udp	User Datagram Protocol
vdolive	VDOLive Protocol

Each protocol is tied to a keyword name. Apply the keyword name to an interface that you want to inspect. For example, this configuration inspects FTP, SMTP, and Telnet:

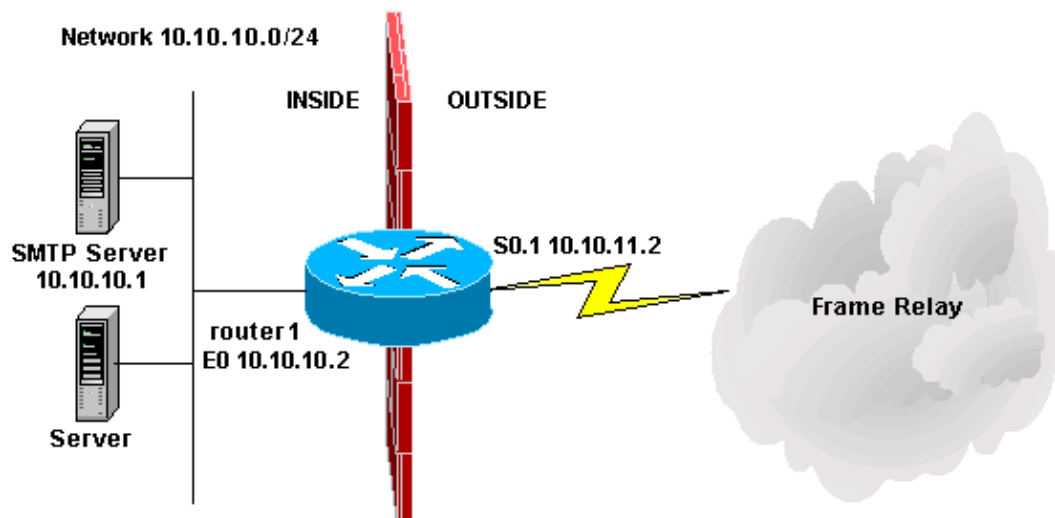
```
router1#configure
Configuring from terminal, memory, or network [terminal]? Enter configuration
commands, one per line. End with CNTL/Z.
router1(config)#ip inspect name mysite ftp
router1(config)#ip inspect name mysite smtp
router1(config)#ip inspect name mysite tcp
router1#show ip inspect config
Session audit trail is disabled
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 30 sec -- tcp finwait-time is 5 sec
tcp idle-time is 3600 sec -- udp idle-time is 30 sec
dns-timeout is 5 sec
Inspection Rule Configuration
Inspection name mysite

ftp timeout 3600
smtp timeout 3600
tcp timeout 3600
```

This document addresses what traffic you want to let out, what traffic you want to let in, and what traffic you want to inspect. Now that you are prepared to configure CBAC, complete these steps:

1. Apply the configuration.
2. Enter the access lists as configured above.
3. Configure the inspection statements.
4. Apply the access lists to the interfaces.

After this procedure, your configuration appears as shown in this diagram and configuration.



Context-Based Access Control Configuration

```
!
version 11.2
no service password-encryption
service udp-small-servers
service tcp-small-servers
!
```

```
hostname router1
!
!
no ip domain-lookup
ip inspect name mysite ftp
ip inspect name mysite smtp
ip inspect name mysite tcp
!
interface Ethernet0
ip address 10.10.10.2 255.255.255.0
ip access-group 101 in
ip inspect mysite in

no keepalive
!
interface Serial0
no ip address
encapsulation frame-relay
no fair-queue
!
interface Serial0.1 point-to-point
ip address 10.10.11.2 255.255.255.252
ip access-group 102 in
frame-relay interface-dlci 200 IETF
!
router eigrp 69
network 10.0.0.0
no auto-summary
!
ip default-gateway 10.10.11.1
no ip classless
ip route 0.0.0.0 0.0.0.0 10.10.11.1
access-list 101 permit tcp 10.10.10.0 0.0.0.255 any
access-list 101 permit udp 10.10.10.0 0.0.0.255 any
access-list 101 permit icmp 10.10.10.0 0.0.0.255 any
access-list 101 deny ip any any
access-list 102 permit eigrp any any
access-list 102 permit icmp any 10.10.10.0 0.0.0.255 echo-reply
access-list 102 permit icmp any 10.10.10.0 0.0.0.255 unreachable
access-list 102 permit icmp any 10.10.10.0 0.0.0.255 administratively-prohibited
access-list 102 permit icmp any 10.10.10.0 0.0.0.255 packet-too-big
access-list 102 permit icmp any 10.10.10.0 0.0.0.255 echo
access-list 102 permit icmp any 10.10.10.0 0.0.0.255 time-exceeded
access-list 102 permit tcp any host 10.10.10.1 eq smtp
access-list 102 deny ip any any
!
line con 0
line vty 0 4
login
!
end
```

Related Information

- [IOS Firewall Support Page](#)
- [Cisco IOS Software Configuration](#)
- [Technical Support – Cisco Systems](#)

