sco − Context−Based Access Control: Introduction and Configu

Table of Contents

Context−Based Access Control: Introduction and Configuration

Introduction

The Context−Based Access Control (CBAC) feature of Cisco's IOS Firewall Feature Set actively inspects the activity behind a firewall. CBAC specifies what traffic should be let in and what traffic should 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 has not been tampered with before the protocol goes to the systems behind the firewall.

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

Prior to configuration, consider the questions below. Each question is discussed in the following sections.

- 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 is dependent 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. You specify outbound traffic by using an extended access list as follows:

```
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 is dependent on your site security policy, but the logical answer is anything that will 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. Below 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, you must remove the access list, edit it, and reapply the updated access list.

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)
```

What Traffic Do You Want to Inspect?

The CBAC within Cisco IOS supports the following:

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. You apply the keyword name to an interface that you want to inspect. For example, the configuration below inspects FTP, SMTP, and Telnet:

```
router1#conf
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#sh 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
```

In this technical tip, you have addressed 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, follow the steps below:

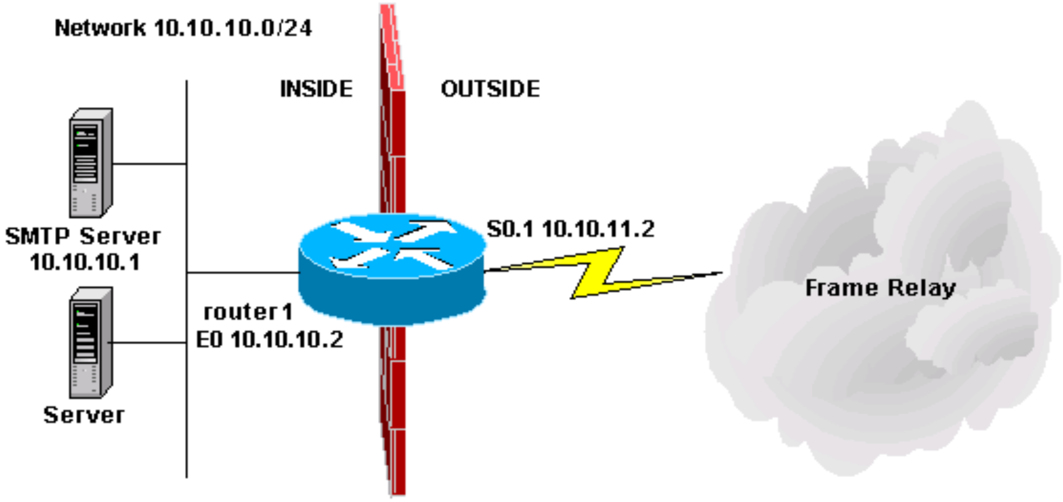
1. Apply the configuration.

2. Enter the access lists as configured above.

3. Configure the inspection statements.

4. Apply the access lists to the interfaces.

After the above steps, your configuration should appear as shown in the diagram and configuration below.



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
ip inspect mysite out

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
```

Tools Information

For additional resources, refer to Cisco TAC Tools for Security Technologies.

Related Information

- **IOS Firewall in IOS Documentation**
- **More IOS Firewall Technical Tips**
- **IOS Firewall Product Support Page**

Updated: Jun 18, 2002 Document ID: 13814