設定內容型存取控制(CBAC)

目錄

簡介

Cisco IOS®防火牆功能集的內容型存取控制(CBAC)功能會主動檢查防火牆背後的活動。CBAC使用存取清單（與Cisco IOS使用存取清單的方式相同）指定哪些流量需要放入，哪些流量需要放出。但是，CBAC訪問清單包括ip inspect語句，該語句允許檢查協定，以確保該協定在進入防火牆後的系統之前未被篡改。

必要條件

需求

本文件沒有特定需求。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

背景資訊

CBAC也可以用於網路位址轉譯(NAT)，但本檔案中的組態主要處理純粹的檢查。如果執行NAT，則訪問清單需要反映全域性地址，而不是實際地址。

在配置之前，請考慮以下問題。

您想釋放哪些流量？

您要放出的流量取決於您的站點安全策略，但在此常規示例中，所有流量都允許出站。如果您的存取清單拒絕所有封包，則沒有流量可以離開。使用此擴展訪問清單指定出站流量：

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

您希望允許哪些流量進入？

您希望傳入的流量取決於您的站點安全策略。但是，符合邏輯的答案是任何不會損壞您網路的資訊。

在此範例中，有一列流量看起來合乎邏輯地允許進入。網際網路控制訊息通訊協定(ICMP)流量通常可接受，但可能會產生一些DOS攻擊。以下是傳入流量的存取清單範例：

延伸型IP存取清單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
```

延伸型IP存取清單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
```

存取清單101用於傳出流量。存取清單102用於傳入流量。存取清單僅允許路由通訊協定、增強型內部閘道路由通訊協定(EIGRP)和指定的ICMP傳入流量。

在本示例中，無法從Internet訪問路由器乙太網端的伺服器。訪問清單阻止其建立會話。要使訪問清單可訪問，需要修改訪問清單以允許進行會話。要更改訪問清單，請刪除訪問清單，編輯它，然後重新應用更新的訪問清單。

注意：在編輯和重新應用之前刪除訪問清單102的原因是由於訪問清單結尾有「deny ip any any」。在這種情況下，如果在移除存取清單之前新增專案，則新專案會顯示在deny之後。因此，它從未被檢查。

此示例僅新增用於10.10.10.1的簡單郵件傳輸協定(SMTP)。

延伸型IP存取清單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.
```

您要檢查哪些流量？

Cisco IOS中的CBAC支援：

關鍵字名稱	通訊協定
庫西梅	CUSeeMe協定
ftp	檔案傳輸通訊協定
h323	H.323協定（例如Microsoft NetMeeting或Intel Video Phone）
http	HTTP協定
rcmd	R命令(r-exec、r-login、r-sh)
realaudio	Real Audio通訊協定
rpc	遠端過程呼叫協定
smtp	簡單郵件傳輸協定
sqlnet	SQL Net協定
streamworks	StreamWorks通訊協定
tcp	傳輸控制通訊協定
tftp	TFTP通訊協定
udp	使用者資料包通訊協定
夫多利夫	VDOLive通訊協定

每個協定都與一個關鍵字名稱關聯。將關鍵字名稱應用於要檢查的介面。例如，此配置檢查FTP、SMTP和Telnet:

```
router1#configure
Configuring from terminal, memory, or network [terminal]? Enter configuration
commands, one per line. End with CNTL/Z.
```

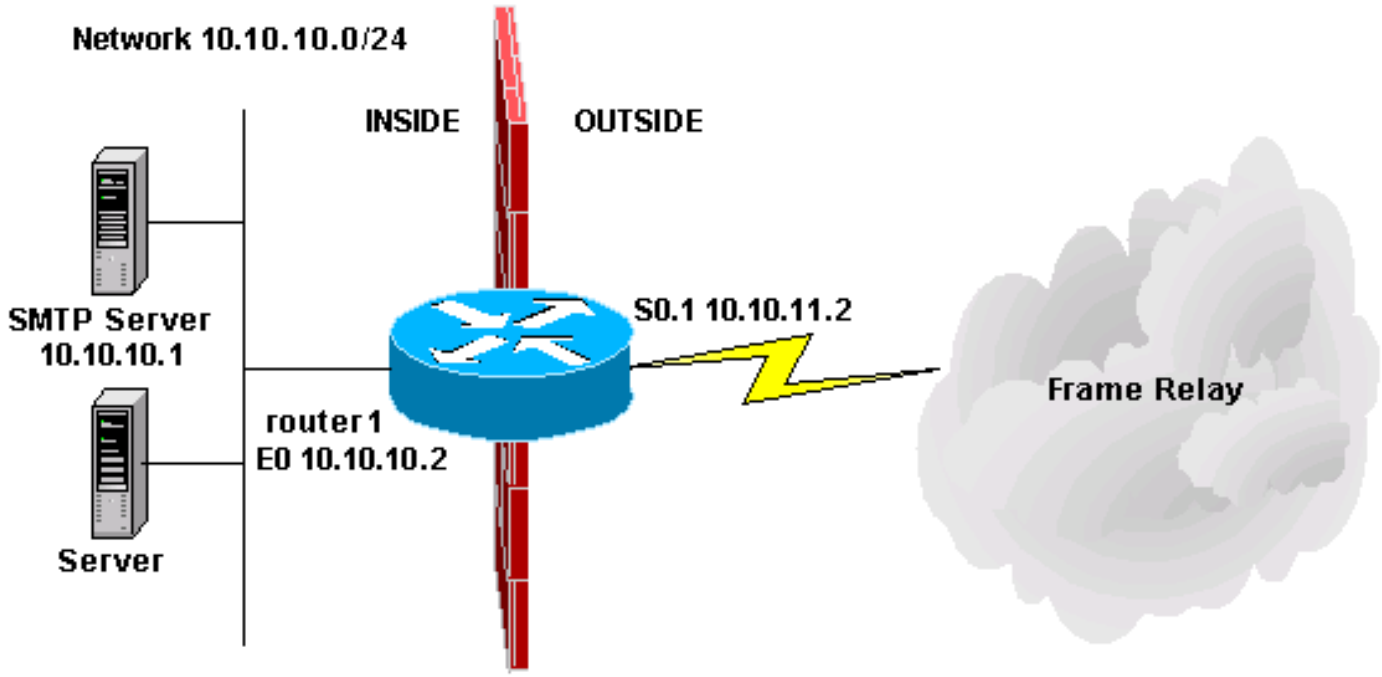
```
router1(config)#ip inspect name mysite ftp
router1(config)#ip inspect name mysite smtp
router1(config)#ip inspect name mysite tcp
router1#show ip inspect config
Session audit trail is disabled
one-minute (sampling period) thresholds are [400:500]connections
max-incomplete sessions thresholds are [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
```

本文說明您要放出的流量、要放出的流量以及要檢查的流量。現在您已準備好配置CBAC，請完成以下步驟：

1. 套用組態。
2. 輸入如上配置的訪問清單。
3. 配置檢查語句。
4. 將存取清單套用到介面。

完成此過程後，您的配置將顯示如圖所示。



內容型存取控制組態
`` ! 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
```

相關資訊

- Cisco IOS防火牆支援頁面
- 技術支援與文件 - Cisco Systems