Configurazione del controllo degli accessi basato sul contesto (CBAC)

Sommario

Introduzione

La funzionalità Context-Based Access Control (CBAC) del gruppo di funzionalità di firewall Cisco IOS® controlla attivamente l'attività dietro un firewall. La funzione CBAC specifica il traffico che deve essere autorizzato ad accedere e il traffico che deve essere autorizzato a uscire utilizzando gli elenchi degli accessi (nello stesso modo in cui Cisco IOS utilizza gli elenchi degli accessi). Tuttavia, gli elenchi degli accessi CBAC includono istruzioni ip inspect che consentono di ispezionare il protocollo per verificare che non venga manomesso prima che venga inviato ai sistemi dietro il firewall.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Premesse

La funzione CBAC può essere utilizzata anche con il protocollo NAT (Network Address Translation), ma la configurazione illustrata in questo documento riguarda principalmente il controllo puro. Se si esegue NAT, gli elenchi degli accessi devono riflettere gli indirizzi globali, non gli indirizzi reali.

Prima di procedere alla configurazione, è opportuno porsi le seguenti domande.

- Traffico da rilasciare
- Quale traffico vuoi far entrare?
- Specificare il traffico da ispezionare.

Traffico di uscita

Il tipo di traffico che si desidera rilasciare dipende dai criteri di protezione del sito, ma in questo esempio generale è consentito tutto il traffico in uscita. Se l'elenco degli accessi nega tutto, il traffico non può partire. Specificare il traffico in uscita con questo elenco accessi esteso:

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

Che traffico vuoi far entrare?

Il tipo di traffico da consentire dipende dai criteri di protezione del sito. Tuttavia, la risposta logica è tutto ciò che non danneggia la rete.

Nell'esempio riportato di seguito viene riportato un elenco del traffico che sembra logico consentire l'accesso. Il traffico ICMP (Internet Control Message Protocol) è generalmente accettabile, ma può consentire alcune possibilità di attacchi DOS. Di seguito viene riportato un elenco degli accessi di esempio per il traffico in entrata:

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
```

L'elenco degli accessi 101 si riferisce al traffico in uscita. L'elenco degli accessi 102 si riferisce al traffico in entrata. Gli elenchi degli accessi consentono solo un protocollo di routing, il protocollo EIGRP (Enhanced Interior Gateway Routing Protocol) e il traffico in entrata ICMP specificato.

Nell'esempio, un server sul lato Ethernet del router non è accessibile da Internet. L'elenco degli accessi impedisce la creazione di una sessione. Per renderla accessibile, è necessario modificare l'elenco degli accessi per consentire la conversazione. Per modificare un elenco degli accessi, rimuoverlo, modificarlo e riapplicare l'elenco degli accessi aggiornato.

Nota: il motivo per cui si rimuove l'elenco degli accessi 102 prima di apportare le modifiche e riapplicare la licenza è dovuto alla voce "deny ip any any" in fondo all'elenco degli accessi. In questo caso, se si desidera aggiungere una nuova voce prima di rimuovere l'elenco degli accessi, la nuova voce verrà visualizzata dopo la voce nega. Pertanto, non viene mai controllato.

In questo esempio viene aggiunto il protocollo SMTP (Simple Mail Transfer Protocol) solo per la versione 10.10.10.1.

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.
```

Specificare il traffico da ispezionare.

La funzione CBAC di Cisco IOS supporta:

Nome parola chiave	Protocollo
cuseeme	Protocollo UCSeeMe
ftp	Protocollo di trasferimento file
h323	Protocollo H.323 (ad esempio Microsoft NetMeeting o Intel Video Phone)
http	Protocollo HTTP
rcmd	Comandi R (r-exec, r-login, r-sh)

audio reale	Protocollo Real Audio
rpc	Remote Procedure Call Protocol
smtp	Protocollo SCEP (Simple Mail Transfer Protocol)
sqlnet	Protocollo SQL Net
streamworks	Protocollo StreamWorks
tcp	Transmission Control Protocol
tftp	Protocollo TFTP
udp	User Datagram Protocol
vdolive	Protocollo VDOLive

Ogni protocollo è associato a un nome di parola chiave. Applicare il nome della parola chiave a un'interfaccia che si desidera ispezionare. Ad esempio, questa configurazione controlla FTP, SMTP e Telnet:

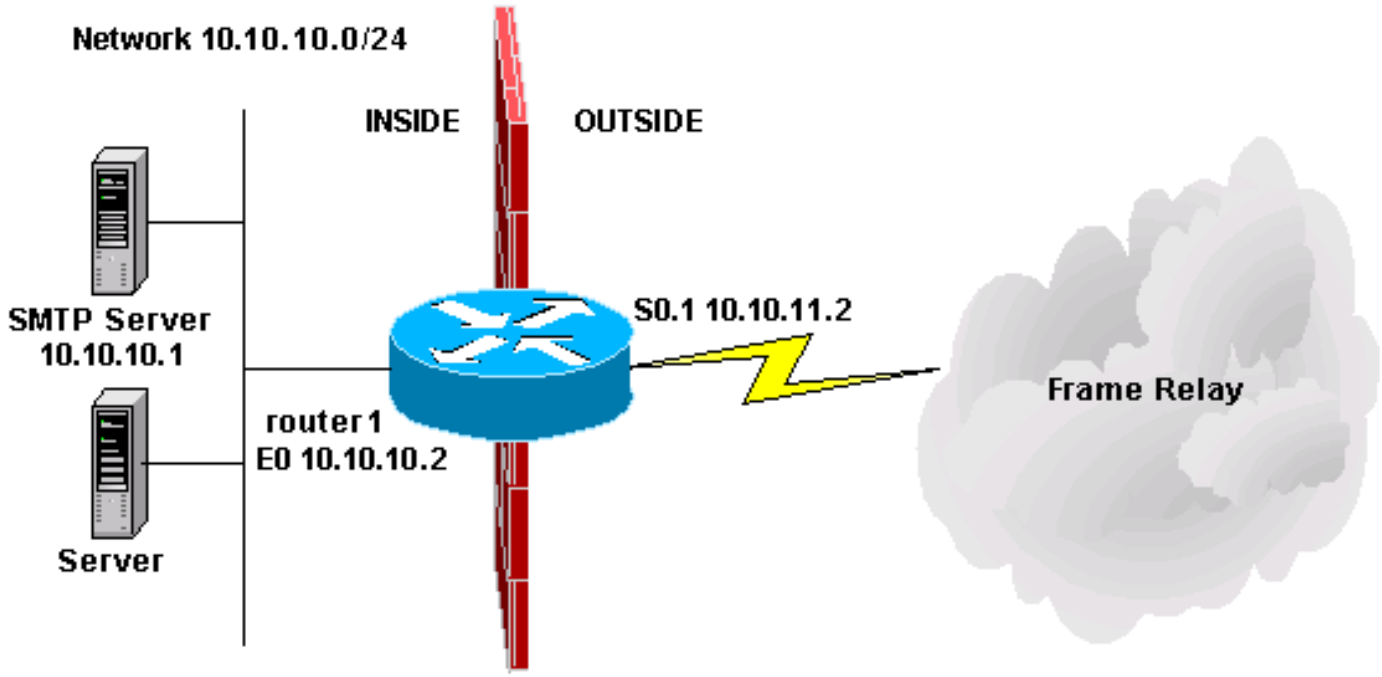
```
router1#configure
Configuring from terminal, memory, or network [terminal]? Enter configuration
commands, one per line. End with CNTL/Z.
router1(config)#ip inspect name mysite ftp
router1(config)#ip inspect name mysite smtp
router1(config)#ip inspect name mysite tcp
router1#show ip inspect config
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
```

In questo documento viene descritto il traffico che si desidera rilasciare, il traffico che si desidera autorizzare ad accedere e il traffico che si desidera ispezionare. Dopo aver configurato la funzione CBAC, attenersi alla seguente procedura:

1. Applicare la configurazione.
2. Immettere gli elenchi degli accessi come configurato in precedenza.
3. Configurare le istruzioni di ispezione.
4. Applicare gli elenchi degli accessi alle interfacce.

Al termine di questa procedura, la configurazione verrà visualizzata come illustrato nel diagramma e nella configurazione seguenti.



Configurazione del controllo degli accessi basato sul contesto

```
!
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
```

Informazioni correlate

- Pagina di supporto di Cisco IOS Firewall
- Documentazione e supporto tecnico – Cisco Systems