Konfiguration der kontextbasierten Zugriffskontrolle (CBAC)

Inhalt

Einleitung

Die Context-Based Access Control (CBAC)-Funktion des Cisco IOS® Firewall Feature Set überprüft aktiv die Aktivitäten hinter einer Firewall. CBAC legt anhand von Zugriffslisten fest, welcher Datenverkehr ein- und ausgelassen werden muss (genau wie bei Cisco IOS Zugriffslisten). CBAC-Zugriffslisten enthalten jedoch IP-Inspekteanweisungen, mit denen das Protokoll überprüft werden kann, um sicherzustellen, dass es nicht manipuliert wird, bevor das Protokoll zu den Systemen hinter der Firewall gelangt.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

Hintergrundinformationen

CBAC kann auch mit Network Address Translation (NAT) verwendet werden, die Konfiguration in diesem Dokument behandelt jedoch hauptsächlich reine Überprüfungen. Wenn Sie NAT ausführen, müssen Ihre Zugriffslisten die globalen Adressen und nicht die echten Adressen widerspiegeln.

Berücksichtigen Sie diese Fragen vor der Konfiguration.

Welchen Datenverkehr möchten Sie auslassen?

Welchen Datenverkehr Sie freigeben möchten, hängt von Ihrer Sicherheitsrichtlinie für die Website ab. In diesem allgemeinen Beispiel ist jedoch alles nach außen zulässig. Wenn Ihre Zugriffsliste alles versagt, kann kein Datenverkehr gehen. Ausgehenden Datenverkehr mit dieser erweiterten Zugriffsliste angeben:

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

Welchen Datenverkehr möchten Sie einleiten?

Welcher Datenverkehr Sie zulassen möchten, hängt von Ihrer Sicherheitsrichtlinie für die Website ab. Die logische Antwort ist jedoch alles, was Ihr Netzwerk nicht beschädigt.

In diesem Beispiel gibt es eine Liste von Datenverkehr, die logisch einzugeben scheint. Internet Control Message Protocol (ICMP)-Datenverkehr ist allgemein akzeptabel, kann jedoch einige Möglichkeiten für DOS-Angriffe bieten. Dies ist eine Beispielzugriffsliste für eingehenden Datenverkehr:

Erweiterte IP-Zugriffsliste 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
```

Erweiterte IP-Zugriffsliste 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
```

Die Zugriffsliste 101 gilt für den ausgehenden Datenverkehr. Die Zugriffsliste 102 gilt für den eingehenden Datenverkehr. Die Zugriffslisten gestatten nur ein Routing-Protokoll, das Enhanced Interior Gateway Routing Protocol (EIGRP) und den angegebenen eingehenden ICMP-Datenverkehr.

Im Beispiel kann auf einen Server auf der Ethernet-Seite des Routers nicht über das Internet zugegriffen werden. Die Zugriffsliste blockiert die Einrichtung einer Sitzung. Um darauf zugreifen zu können, muss die Zugriffsliste so geändert werden, dass das Gespräch stattfinden kann. Um eine Zugriffsliste zu ändern, entfernen Sie die Zugriffsliste, bearbeiten Sie sie, und wenden Sie die aktualisierte Zugriffsliste erneut an.

Hinweis: Der Grund dafür, dass Sie die Zugriffsliste 102 entfernen, bevor Sie sie bearbeiten und erneut anwenden, liegt in der "deny ip any any any any" am Ende der Zugriffsliste. Wenn Sie in diesem Fall einen neuen Eintrag hinzufügen möchten, bevor Sie die Zugriffsliste entfernen, wird der neue Eintrag nach dem Ablehnen angezeigt. Daher wird sie nie überprüft.

In diesem Beispiel wird das Simple Mail Transfer Protocol (SMTP) nur für 10.10.10.1 hinzugefügt.

Erweiterte IP-Zugriffsliste 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.
```

Welchen Datenverkehr möchten Sie überprüfen?

CBAC in Cisco IOS unterstützt:

Schlüsselwortname	Protokolle
Cuseeme	CUSeeMe-Protokoll
ftp	File Transfer Protocol
h323	H.323-Protokoll (z. B. Microsoft NetMeeting oder Intel Video Phone)
http	HTTP-Protokoll
rcmd	R-Befehle (r-exec, r-login, r-sh)
realAudiowiedergabe	Real Audio Protocol

RPC	Anrufprotokoll für Remote-Verfahren
SMTP	Simple Mail Transfer Protocol
sqlnet	SQL Net-Protokoll
optimieren	StreamWorks-Protokoll
tcp	Transmission Control Protocol
tftp	TFTP-Protokoll
udp	User Datagram Protocol
Vdolive	VDOLive-Protokoll

Jedes Protokoll ist an einen Schlüsselwortnamen gebunden. Wenden Sie den Schlüsselwortnamen auf eine Schnittstelle an, die Sie überprüfen möchten. Bei dieser Konfiguration werden beispielsweise FTP, SMTP und Telnet überprüft:

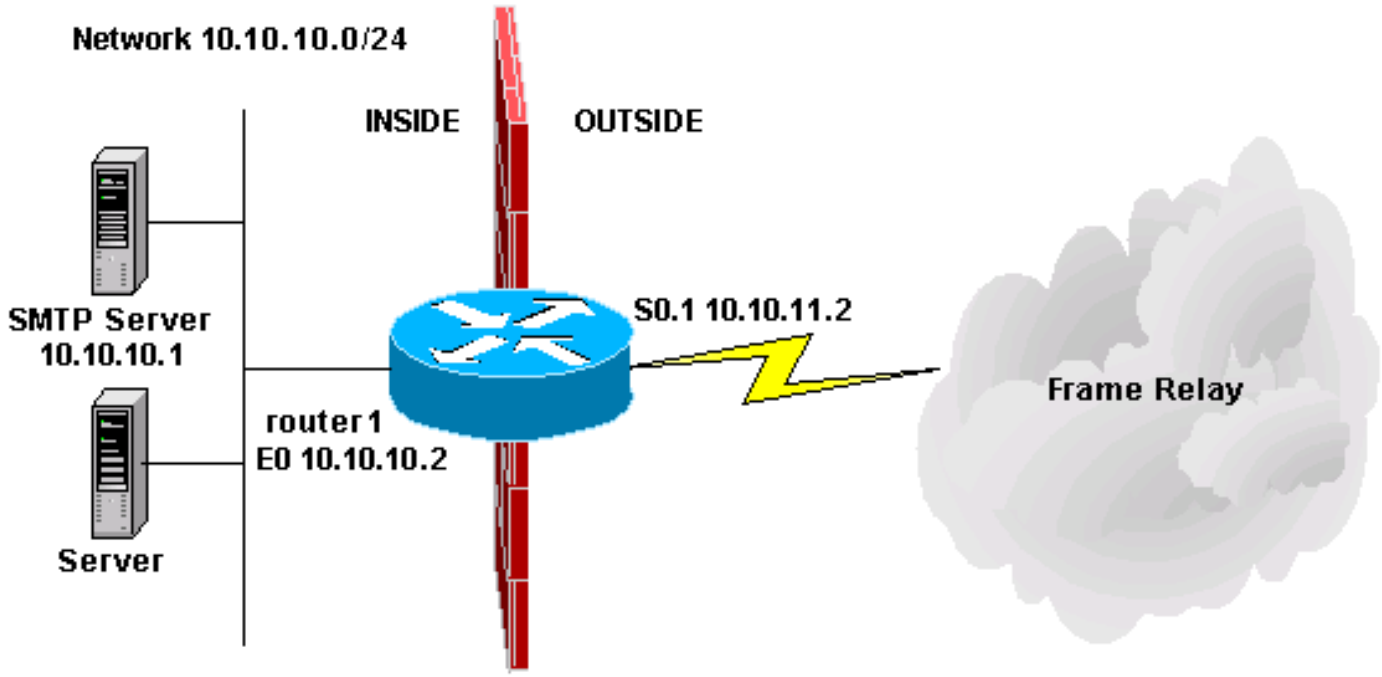
```
router1#configure
Configuring from terminal, memory, or network [terminal]? Enter configuration
commands, one per line. End with CNTL/Z.
router1(config)#ip inspect name mysite ftp
router1(config)#ip inspect name mysite smtp
router1(config)#ip inspect name mysite tcp
router1#show ip inspect config
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 diesem Dokument wird beschrieben, welchen Datenverkehr Sie auslassen möchten, welchen Datenverkehr Sie zulassen möchten und welchen Datenverkehr Sie überprüfen möchten. Führen Sie die folgenden Schritte aus, da Sie bereit sind, CBAC zu konfigurieren:

1. Wenden Sie die Konfiguration an.
2. Geben Sie die Zugriffslisten wie oben konfiguriert ein.
3. Konfigurieren Sie die Anweisungen zur Überprüfung.
4. Anwenden der Zugriffslisten auf die Schnittstellen

Nach diesem Verfahren wird die Konfiguration wie in diesem Diagramm und in dieser Konfiguration dargestellt angezeigt.



Konfiguration der kontextbasierten Zugriffskontrolle

```
!
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
```

Zugehörige Informationen

- Support-Seite für Cisco IOS Firewall
- Technischer Support und Dokumentation für Cisco Systeme