CBAC(Context-Based Access Control) 구성

목차

소개

Cisco IOS® 방화벽 기능 집합의 CBAC(Context-Based Access Control) 기능은 방화벽 뒤의 활동을 능동적으로 검사합니다. CBAC는 Cisco IOS에서 액세스 목록을 사용하는 것과 동일한 방식으로 액세스 목록을 사용하여 허용할 트래픽과 허용할 트래픽을 지정합니다. 그러나 CBAC 액세스 목록에는 프로토콜이 방화벽 뒤에 있는 시스템으로 이동하기 전에 프로토콜이 손상되지 않았는지 확인하는 ip inspect 문이 포함되어 있습니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참조하십시오.

배경 정보

CBAC는 NAT(Network Address Translation)에도 사용할 수 있지만, 이 문서의 컨피그레이션은 주로 순수 검사를 처리합니다. NAT를 수행하는 경우 액세스 목록은 실제 주소가 아니라 전역 주소를 반영해야 합니다.

구성 전에 이러한 질문을 고려하십시오.

어떤 트래픽을 허용하시겠습니까?

해제하려는 트래픽은 사이트 보안 정책에 따라 다르지만, 이 일반적인 예에서는 모든 트래픽이 아웃바운드로 허용됩니다. 액세스 목록에서 모든 것을 거부하면 트래픽이 떠날 수 없습니다. 이 확장 액세스 목록을 사용하여 아웃바운드 트래픽을 지정합니다.

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

어떤 트래픽을 허용하시겠습니까?

허용할 트래픽은 사이트 보안 정책에 따라 달라집니다. 그러나 논리적인 대답은 네트워크에 손상을 주지 않는 것입니다.

이 예제에서는 허용할 수 있는 논리적 트래픽 목록이 있습니다. ICMP(Internet Control Message Protocol) 트래픽은 일반적으로 허용되지만, DOS 공격에 대한 몇 가지 가능성을 허용할 수 있습니다. 수신 트래픽에 대한 샘플 액세스 목록입니다.

확장 IP 액세스 목록 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
```

확장 IP 액세스 목록 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
```

액세스 목록 101은 아웃바운드 트래픽에 사용됩니다. 액세스 목록 102는 인바운드 트래픽에 대한 것입니다. 액세스 목록은 라우팅 프로토콜, EIGRP(Enhanced Interior Gateway Routing Protocol) 및 지정된 ICMP 인바운드 트래픽만 허용합니다.

이 예에서 라우터의 이더넷 쪽에 있는 서버는 인터넷에서 액세스할 수 없습니다. 액세스 목록은 세션 설정을 차단합니다. 액세스 목록을 수정하여 대화를 진행하도록 해야 합니다. 액세스 목록을 변경하려면 액세스 목록을 제거하고 수정한 다음 업데이트된 액세스 목록을 다시 적용합니다.

참고: 수정 및 재적용하기 전에 access-list 102를 제거한 이유는 액세스 목록 끝에 "deny ip any any"(deny ip any any)가 있기 때문입니다. 이 경우 액세스 목록을 제거하기 전에 새 항목을 추가하려는 경우 새 항목이 거부 뒤에 나타납니다. 따라서 점검되지 않습니다.

이 예에서는 10.10.10.1에 대해서만 SMTP(Simple Mail Transfer Protocol)를 추가합니다.

확장 IP 액세스 목록 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.
```

어떤 트래픽을 검사하시겠습니까?

Cisco IOS 내의 CBAC는 다음을 지원합니다.

키워드 이름	프로토콜
쿠세미	CUSeeMe 프로토콜
ftp	FTP(File Transfer Protocol)
h323	H.323 프로토콜(예: Microsoft NetMeeting 또는 Intel Video Phone)
http	HTTP 프로토콜
rcmd	R 명령(r-exec, r-login, r-sh)
오디오	실제 오디오 프로토콜
rpc	원격 프로시저 통화 프로토콜
smtp	단순 메일 전송 프로토콜
sqlnet	SQL Net 프로토콜
가연성	StreamWorks 프로토콜
tcp	전송 제어 프로토콜
tftp	TFTP 프로토콜
udp	사용자 데이터그램 프로토콜
vdol	VDOLive 프로토콜

각 프로토콜은 키워드 이름에 연결됩니다. 검사할 인터페이스에 키워드 이름을 적용합니다. 예를 들어 이 컨피그레이션은 FTP, SMTP 및 텔넷을 검사합니다.

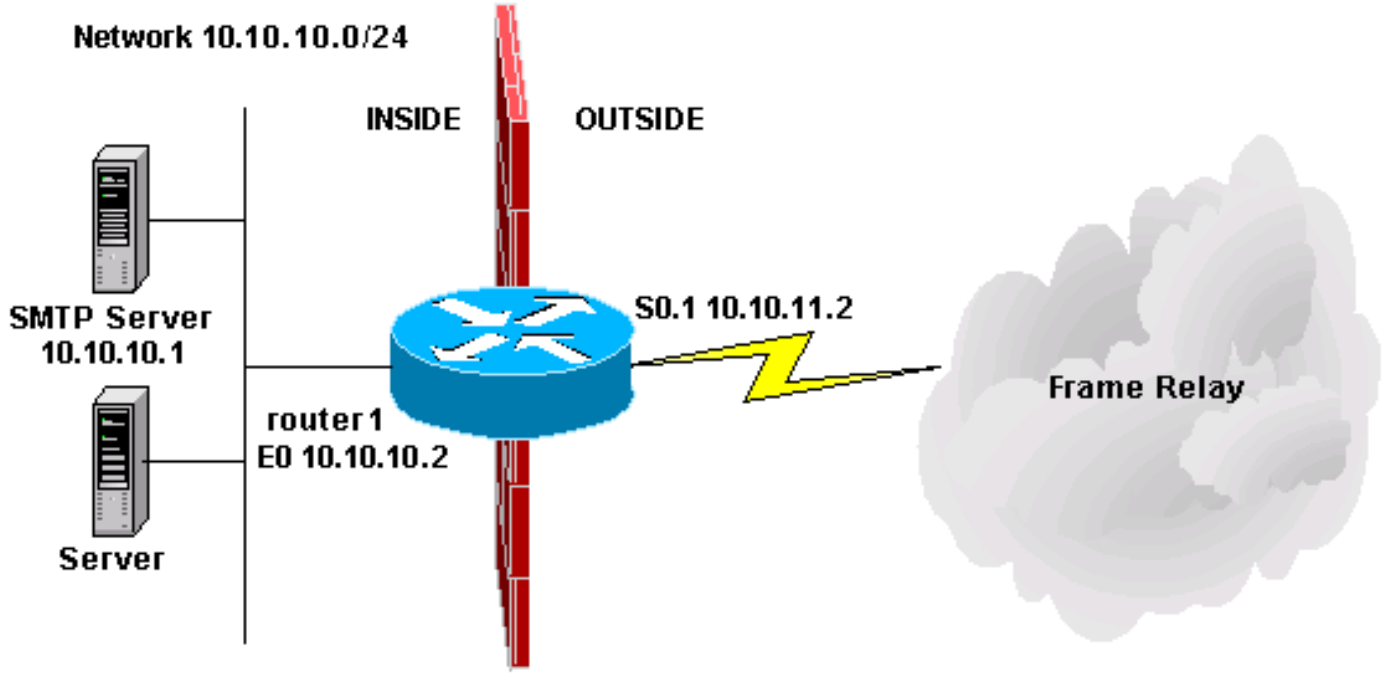
```
router1#configure
Configuring from terminal, memory, or network [terminal]? Enter configuration
commands, one per line. End with CNTL/Z.
router1(config)#ip inspect name mysite ftp
router1(config)#ip inspect name mysite smtp
router1(config)#ip inspect name mysite tcp
router1#show ip inspect config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

이 문서에서는 허용할 트래픽, 허용할 트래픽, 검사할 트래픽을 다룹니다. 이제 CBAC를 구성할 준비가 되었으므로 다음 단계를 완료하십시오.

1. 컨피그레이션을 적용합니다.
2. 위에서 구성한 액세스 목록을 입력합니다.
3. 검사 문을 구성합니다.
4. 인터페이스에 액세스 목록을 적용합니다.

이 절차를 마치면 구성이 이 다이어그램 및 구성에 표시된 것처럼 나타납니다.



컨텍스트 기반 액세스 제어 컨피그레이션
!

```
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
```

관련 정보

- Cisco IOS 방화벽 지원 페이지
- 기술 지원 및 문서 – Cisco Systems