Configurar o Controle de Acesso Baseado em Contexto (CBAC - Context-Based Access Control)

Contents

Introduction

A característica Context-Based Access Control (CBAC) do Conjunto de Características de Firewall do Cisco IOS® inspeciona a atividade por trás do firewall. O CBAC especifica qual tráfego precisa entrar e qual precisa sair usando listas de acesso (da mesma maneira que o Cisco IOS usa as listas de acesso). Contudo, as listas de acesso do CBAC incluem declarações de inspeção de IP que permitem a inspeção do protocolo para garantir que não esteja violado antes do protocolo ir aos sistemas por trás do firewall.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Informações de Apoio

O CBAC também pode ser usado com a Network Address Translation (NAT), mas a configuração neste documento trata principalmente da inspeção pura. Se você executar o NAT, suas listas de acesso precisam refletir os endereços globais, não os endereços reais.

Antes da configuração, considere estas perguntas.

- Qual tráfego você deseja liberar?
- Qual tráfego você deseja permitir?
- Qual tráfego você deseja inspecionar?

Qual tráfego você deseja liberar?

O tráfego que você quer liberar depende da política de segurança do seu site, mas nesse exemplo geral, tudo é permitido para saída. Se sua lista de acesso negar tudo, nenhum tráfego poderá sair. Especifique o tráfego de saída com esta lista de acesso estendida:

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

Qual tráfego você deseja permitir?

O tráfego que você deseja liberar depende da sua política de segurança do site. No entanto, a resposta lógica é tudo o que não danifica a sua rede.

Neste exemplo, há uma lista de tráfego que parece lógico entrar. O tráfego do Internet Control Message Protocol (ICMP) geralmente é aceitável, mas pode permitir algumas possibilidades de ataques de DOS. Esta é uma lista de acesso de exemplo para tráfego de entrada:

Lista de acesso de IP estendida 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
```

Lista de acesso de IP estendido 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
```

A lista de acesso 101 é para o tráfego de saída. A lista de acesso 102 é para o tráfego de entrada. As listas de acesso permitem apenas um Routing Protocol, Enhanced Interior Gateway Routing Protocol (EIGRP) e tráfego de entrada ICMP especificado.

No exemplo, um servidor no lado Ethernet do roteador não pode ser acessado pela Internet. A lista de acessos o impede de estabelecer uma sessão. Para torná-lo acessível, a lista de acesso precisa ser modificada para permitir que a conversação ocorra.l Para alterar uma lista de acesso, remova a lista de acesso, edite-a e reaplique a lista de acesso atualizada.

Observação: o motivo pelo qual você remove a lista de acesso 102 antes de editar e reaplicar, deve-se ao "deny ip any any" no final da lista de acesso. Nesse caso, se você adicionar uma nova entrada antes de remover a lista de acesso, a nova entrada será exibida após a negação. Portanto, nunca é verificado.

Este exemplo adiciona o Simple Mail Transfer Protocol (SMTP) somente para a versão 10.10.10.1.

Lista de acesso de IP estendido 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.
```

Qual tráfego você deseja inspecionar?

O CBAC no Cisco IOS suporta:

Nome da palavra-chave	Protocolo
cuseeme	Protocolo CUSeeMe
ftp	Protocolo de transferência de arquivo
h323	Protocolo H.323 (por exemplo, Microsoft NetMeeting ou Intel Video Phone)
http	Protocolo HTTP
rcmd	Comandos R (r-exec, r-login, r-sh)
realaudio	Protocolo de Real Áudio
rpc	Protocolo de chamada de procedimento

	remoto
smtp	Protocolo Simples de Transferência de Correspondência (SMTP)
sqlnet	Protocolo de rede SQL
streamworks	Protocolo StreamWorks
tcp	Protocolo de controle de transmissão
tftp	Protocolo TFTP
udp	Protocolo de Datagrama do Usuário
vdolive	Protocolo VDOLive

Cada protocolo está vinculado a um nome de palavra-chave. Aplique o nome da palavra-chave a uma interface que você deseja inspecionar. Por exemplo, essa configuração inspeciona FTP, SMTP e Telnet:

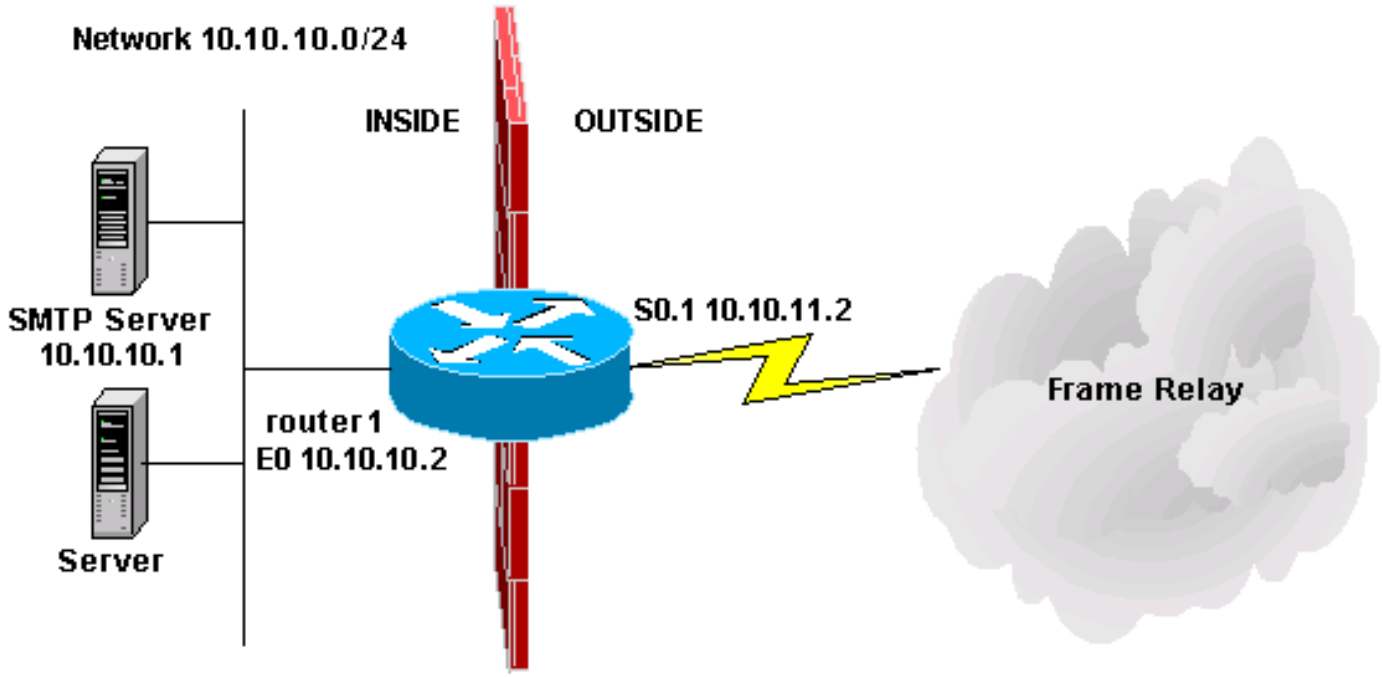
```
router1#configure
Configuring from terminal, memory, or network [terminal]? Enter configuration
commands, one per line. End with CNTL/Z.
router1(config)#ip inspect name mysite ftp
router1(config)#ip inspect name mysite smtp
router1(config)#ip inspect name mysite tcp
router1#show ip inspect config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

Este documento aborda o tráfego que você deseja liberar, o tráfego que deseja liberar e o tráfego que deseja inspecionar. Agora que você está preparado para configurar o CBAC, faça o seguinte:

1. Aplique a configuração.
2. Digite as listas de acesso conforme configuradas acima.
3. Configure as instruções de inspeção.
4. Aplique as listas de acesso às interfaces.

Após esse procedimento, sua configuração aparece como mostrado neste diagrama e na configuração.



Configuração de Controle de Acesso Baseado em Contexto

```
!
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
```

Informações Relacionadas

- Página de suporte do Cisco IOS Firewall
- Suporte Técnico e Documentação - Cisco Systems