# Context-Based Access Control (CBAC): Introdução e configuração

## Índice



## Introdução

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.

## Pré-requisitos

### Requisitos

Não existem requisitos específicos para este documento.

### Componentes Utilizados

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

### Convenções

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas

técnicas Cisco.

# Informações de Apoio

O CBAC pode igualmente ser usado com Network Address Translation (NAT), mas a configuração em negócios deste documento primeiramente com inspeção pura. Se você executa o NAT, suas Listas de acesso precisam de refletir os endereços globais, não os endereços reais.

Antes da configuração, considere estas perguntas.

- Que tráfego você quer deixar para fora?
- Que tráfego você quer deixar dentro?
- Qual tráfego você deseja inspecionar?

# Qual tráfego você deseja liberar?

Que tráfego você quer deixar para fora depende de sua política de segurança do local, mas neste exemplo geral tudo é de partida permitido. Se sua lista de acessos nega tudo, a seguir o sem tráfego pode sair. Especifique o tráfego de saída com esta lista de acesso extendida:

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

# Qual tráfego você deseja permitir?

Que tráfego você quer deixar dentro depende de sua política de segurança do local. Contudo, a resposta lógica é qualquer coisa que não danifica sua rede.

Neste exemplo, há uma lista de tráfego que parece lógico para deixar dentro. O tráfego de ICMP geralmente é aceitável, mas pode permitir algumas possibilidades de ataques de DOS. Esta é uma lista de acessos da amostra para o 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 mudar uma lista de acessos, remover a lista de acessos, editá-la, e reaplicar a lista de acessos actualizado.

**Note**: A razão que você remove a lista de acesso 102 antes que edite e reaplique, é devido ao “deny ip any any” na extremidade da lista de acessos. Neste caso, se você devia adicionar uma entrada nova antes que você remova a lista de acesso, a entrada nova aparece após a negação. Consequentemente, nunca verifica-se.

Este exemplo adiciona o protocolo SMTP somente para 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 dentro dos apoios do Cisco IOS:

| Nome da palavra-chave | Protocolo |
|---|---|
| cuseeme | Protocolo do CUSeeMe |
| ftp | Protocolo de transferência de arquivo |
| h323 | Protocolo de H.323 (por exemplo Microsoft NetMeeting ou telefone de vídeo de Intel) |
| 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 Protocolo de control de transmisión (TCP) |
| 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 de palavra-chave a uma relação que você queira inspecionar. Por exemplo, esta configuração inspeciona o FTP, o S TP, e o telnet:

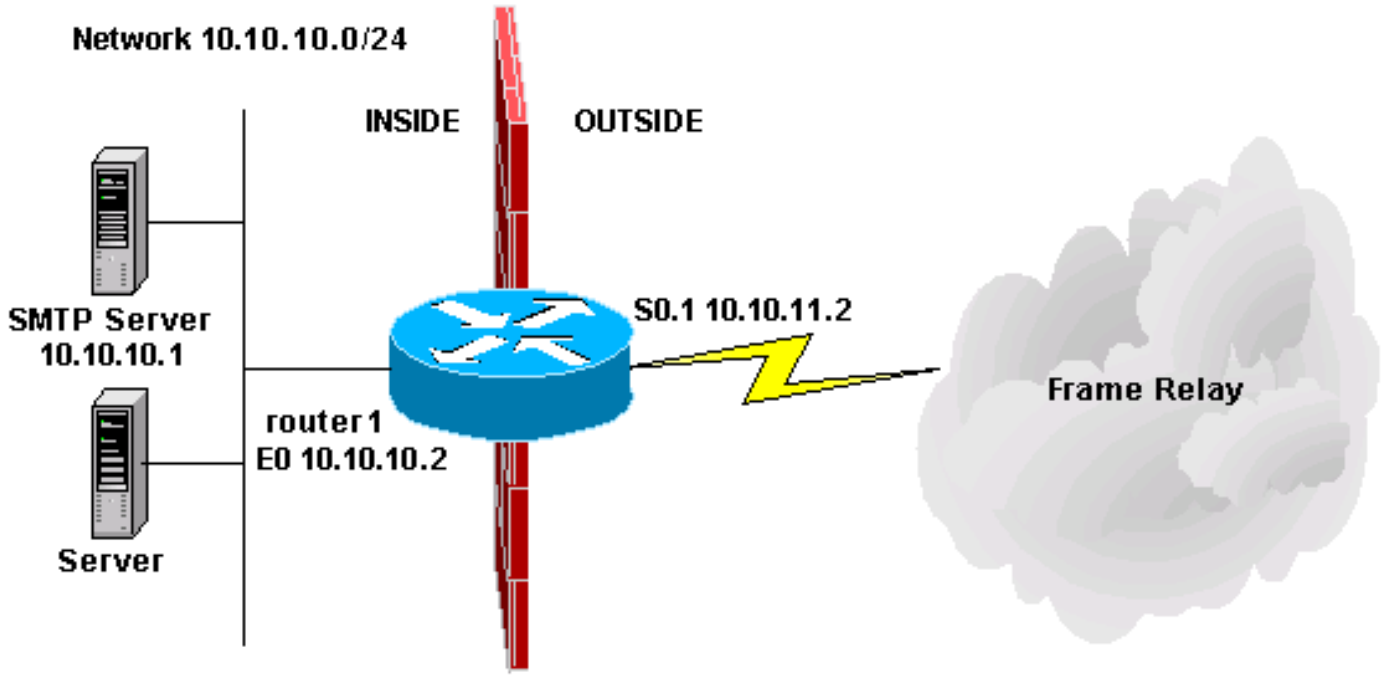
```
router1#configure
Configuring from terminal, memory, or network [terminal]? Enter configuration
commands, one per line. End with CNTL/Z.
router1(config)#ip inspect name mysite ftp
router1(config)#ip inspect name mysite smtp
router1(config)#ip inspect name mysite tcp
router1#show ip inspect config
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 endereça que tráfego você quer deixar para fora, que tráfego você quer deixar dentro, e que tráfego você quer inspecionar. Agora que você é preparado para configurar o CBAC, termine estas etapas:

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 este procedimento, sua configuração aparece segundo as indicações destes diagrama e configuração.




| Configuração de Controle de Acesso Baseado em Contexto |
| --- |
| router1#**configure**<br>Configuring from terminal, memory, or network<br>[terminal]? Enter configuration<br>commands, one per line. End with CNTL/Z.<br>router1(config)#**ip inspect name mysite ftp**<br>router1(config)#**ip inspect name mysite smtp**<br>router1(config)#**ip inspect name mysite tcp**<br>router1#**show ip inspect config**<br>Session audit trail is disabled<br>one-minute (sampling period) thresholds are<br>[400:500]connections<br>max-incomplete sessions thresholds are [400:500]<br>max-incomplete tcp connections per host is 50.<br>Block-time 0 minute.<br>tcp synwait-time is 30 sec -- tcp finwait-time is 5 sec<br>tcp idle-time is 3600 sec -- udp idle-time is 30 sec<br>dns-timeout is 5 sec<br>Inspection Rule Configuration<br>Inspection name mysite<br><br>ftp timeout 3600<br>smtp timeout 3600<br>tcp timeout 3600 |

# Informações Relacionadas

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