Configurar ACLs de IP usadas com frequência

Contents

Introdução

Este documento descreve configurações de exemplo para listas de controle de acesso (ACLs) IP comumente usadas, que filtram pacotes IP.

Pré-requisitos

Requisitos

Atenda a estes requisitos antes de tentar esta configuração:

- Compreensão básica do endereçamento IP.

Consultar Endereçamento IP e sub-redes para novos usuários para obter mais informações.

Componentes Utilizados

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

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

As Listas de Controle de Acesso IP filtram pacotes com base em:

- Endereço origem
- Endereço de destino
- Tipo de pacote
- Qualquer combinação desses itens

Para filtrar o tráfego de rede, as ACLs controlam se os pacotes roteados serão encaminhados ou bloqueados na interface do roteador. Seu roteador examina cada pacote para determinar se o pacote será encaminhado ou descartado, com base nos critérios que você especificar dentro da ACL. Os critérios da ACL incluem:

- Endereço de origem do tráfego
- Endereço de destino do tráfego
- Protocolo de camada superior

Conclua estas etapas para construir uma ACL como os exemplos mostrados neste documento:

1. Crie uma ACL.
2. Aplique uma ACL a uma interface.

A ACL do IP é uma coleção sequencial de condições de permissões e negações que se aplicam a um pacote IP. O roteador testa pacotes em relação às condições no ACL, um por vez.

A primeira correspondência determina se o Cisco IOS® Software aceita ou rejeita o endereço. Como o Cisco IOS Software interrompe o teste de condições após a primeira correspondência, a ordem das condições é crítica. Se nenhuma condição for correspondente, o roteador rejeita o pacote devido a uma negação implícita de todas as cláusulas.

Estes são exemplos de ACLs de IP que podem ser configuradas no Software Cisco IOS:

- ACLs padrões
- ACLs estendidos
- ACLs dinâmicas (chave e bloqueio)
- ACLs nomeadas por IP
- ACLs reflexivos
- ACLs baseadas em tempo que usam intervalos de tempo

- Entradas de ACL de IP comentadas
- ACLs baseadas em contexto
- Proxy de autenticação
- Turbo ACLs
- ACLs baseadas em tempo distribuídas

Este documento discute algumas ACLs estendidas e padrão comumente utilizadas. Consulte a opção Configurando listas de acesso IP para obter mais informações sobre diferentes tipos de ACLs compatíveis com o Software Cisco IOS e sobre como configurar e editar ACLs.

O formato de sintaxe de comando de uma ACL padrão é access-list access-list-number {permit|deny} {host|source source-wildcard|any}.

As ACLs padrão comparam o endereço de origem dos pacotes IP para os endereços configurados na ACL com objetivo de controlar o tráfego.

As ACLs estendidas comparam os endereços de origem e destino dos pacotes IP com os endereços configurados na ACL com o objetivo de controlar o tráfego. Você também pode configurar e tornar as ACLs estendidas mais granulares para filtrar o tráfego por critérios, como:

- Protocolo
- Números da porta
- Ponto de código de serviços diferenciados (Differentiated Services Code Point - DSCP)
- Valor de precedência
- Estado do bit do número de sequência de sincronização (SYN)

Os formatos da sintaxe do comando das ACLs estendidas são:

IP

```
access-list access-list-number [dynamic dynamic-name [timeout minutes]]
{deny | permit} protocol source source-wildcard destination destination-wildcard
 [precedence precedence] [tos tos] [log | log-input]
 [time-range time-range-name][fragments]
```

ICMP (Internet Control Message Protocol)

```
access-list access-list-number [dynamic dynamic-name [timeout minutes]]
{deny | permit} icmp source source-wildcard destination destination-wildcard
 [[icmp-type] [icmp-code] | [icmp-message]] [precedence precedence] [tos tos] [log | log-input]
 [time-range time-range-name][fragments]
```

TCP (Transport Control Protocol)

```
access-list access-list-number [dynamic dynamic-name [timeout minutes]]
{deny | permit} tcp source source-wildcard [operator [port]] destination destination-wildcard [operator
 [established] [precedence precedence] [tos tos] [log | log-input]
 [time-range time-range-name][fragments]
```

User Datagram Protocol (UDP)

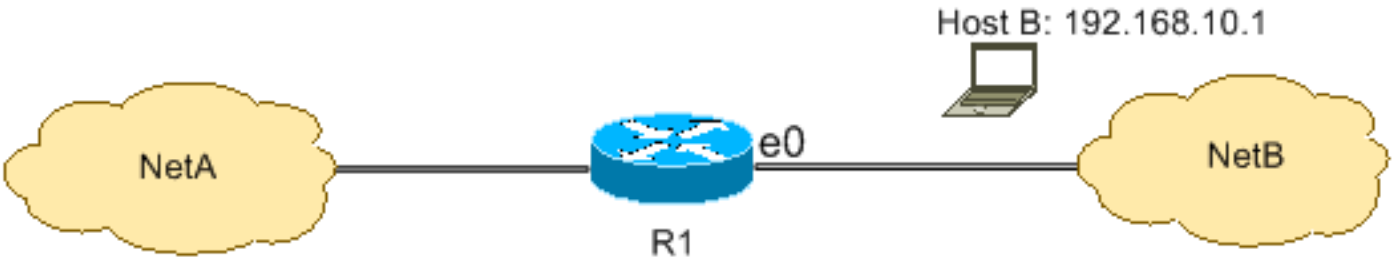
```
access-list access-list-number [dynamic dynamic-name [timeout minutes]]
{deny | permit} udp source source-wildcard [operator [port]] destination destination-wildcard [operator
 [precedence precedence] [tos tos] [log | log-input]
 [time-range time-range-name][fragments]
```

Configurar

Estes exemplos de configuração usam as ACLs de IP mais comuns.

Permitir que um host selecionado acesse a rede

Esta imagem mostra que um host selecionado recebe permissão para acessar a rede. Todo o tráfego originado do Host B destinado à NetA é permitido, e todos os demais tráfegos originados de NetB destinados à NetA são negados.



A saída na tabela R1 mostra como a rede concede acesso ao host. Esta saída mostra que:

- A configuração permite somente o host com o endereço IP 192.168.10.1 por meio da interface Ethernet 0 em R1.
- Este host tem acesso aos serviços IP da NetA.
- Nenhum outro host em NetB tem acesso à NetA.
- Nenhuma declaração de negação está configurada na ACL.

Como padrão, existe uma cláusula deny all implícita no final de cada ACL. Tudo que não for explicitamente permitido é negado.

R1

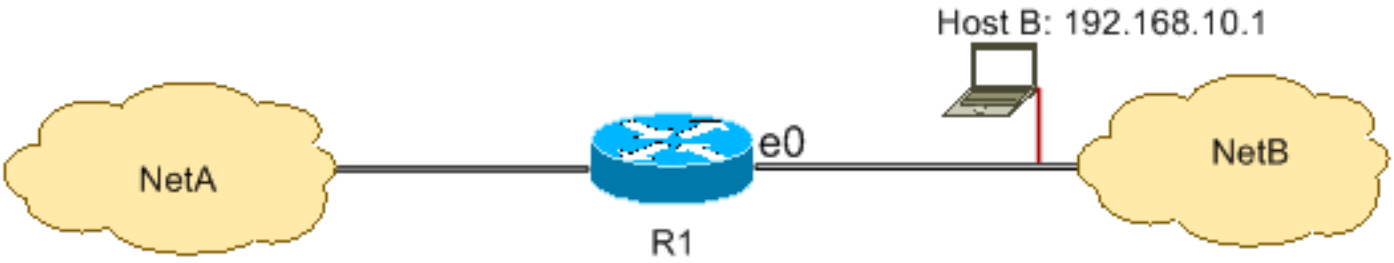
```
hostname R1
!
interface ethernet0
 ip access-group 1 in
!
access-list 1 permit host 192.168.10.1
```

Observação: a ACL filtra pacotes IP de NetB para NetA, exceto pacotes originados do Host B. Os pacotes originados do Host B para NetA ainda são permitidos.

Observação: A ACL access-list 1 permit 192.168.10.1 0.0.0.0 é outra maneira de configurar a mesma regra.

Recusar que um host de seleção acesse a rede

Esta imagem mostra que o tráfego originado no Host B com destino para NetA é negado, enquanto todo o tráfego restante do NetB para acessar NetA é permitido.



Essa configuração nega todos os pacotes do host 192.168.10.1/32 pela Ethernet 0 em R1 e permite o restante. Você deve usar comando access list 1 permit any para permitir explicitamente o restante, porque há uma cláusula deny all implícita em cada ACL.

R1

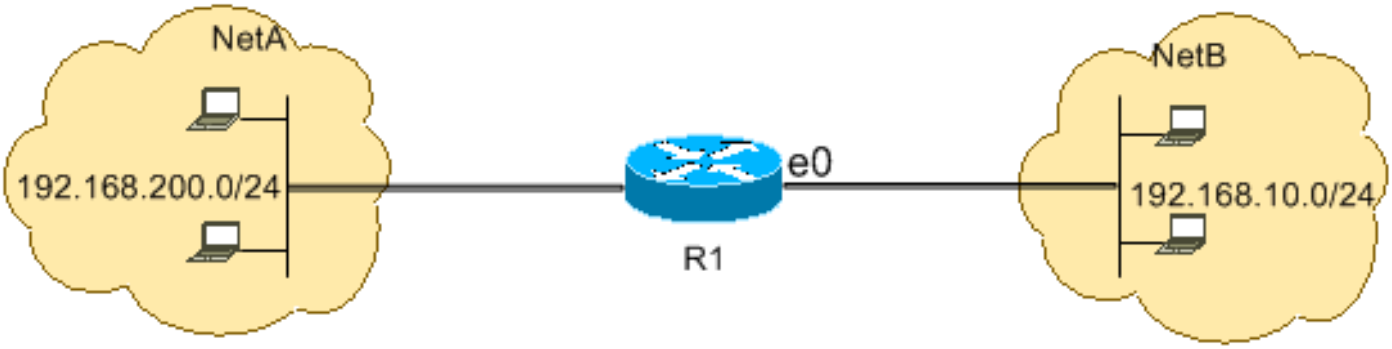
```
hostname R1
!
interface ethernet0
 ip access-group 1 in
!
access-list 1 deny host 192.168.10.1
access-list 1 permit any
```

Observação: a ordem das instruções é essencial para a operação de uma ACL. Se a ordem das entradas for invertida, como mostra este comando, a primeira linha corresponde a cada endereço de origem do pacote. Portanto, a ACL não consegue bloquear o acesso do host 192.168.10.1/32 à NetA.

```
access-list 1 permit any
access-list 1 deny host 192.168.10.1
```

Permita acesso a uma faixa de endereços IP contíguos

Esta imagem mostra que todos os hosts em NetB com o endereço de rede 192.168.10.0/24 podem acessar a rede 192.168.200.0/24 em NetA.



Essa configuração permite que os pacotes IP com um cabeçalho IP e um endereço de origem na rede 192.168.10.0/24 e um endereço de destino na rede 192.168.200.0/24 acessem a NetA. Há uma cláusula deny all implícita no final da ACL que nega todos os outros tráfegos pela entrada Ethernet 0 em R1.

R1

```
hostname R1
!
interface ethernet0
 ip access-group 101 in
!
access-list 101 permit ip 192.168.10.0 0.0.0.255 192.168.200.0 0.0.0.255
```

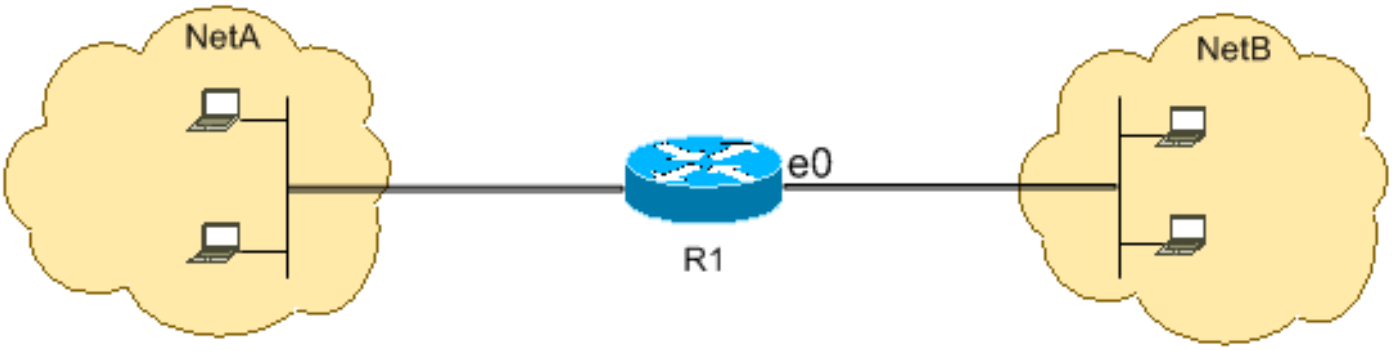
Observação: no comando access-list 101 permit ip 192.168.10.0 0.0.0.255 192.168.200.0 0.0.0.255, 0.0.0.255 é a máscara inversa da rede 192.168.10.0 com a máscara 255.255.255 0. As ACLs usam a máscara inversa para saber quantos bits no endereço de rede precisam ser correspondidos. Na tabela, a ACL permite todos os hosts com endereços de origem na rede 192.168.10.0/24 e endereços de destino na rede 192.168.200.0/24.

Consulte a seção Máscaras de Configuração de listas de acesso de IP para obter mais informações sobre a máscara de um endereço de rede e como calcular a máscara inversa necessária para ACLs.

Negar tráfego Telnet (TCP, porta 23)

Para atender a preocupações de segurança mais elevadas, você pode desativar o acesso Telnet

à sua rede privada a partir da rede pública. Esta imagem mostra como o tráfego Telnet de NetB (público) destinado a NetA (privado) é negado, o que permite que NetA inicie e estabeleça uma sessão Telnet com NetB enquanto todo o tráfego IP restante é permitido.



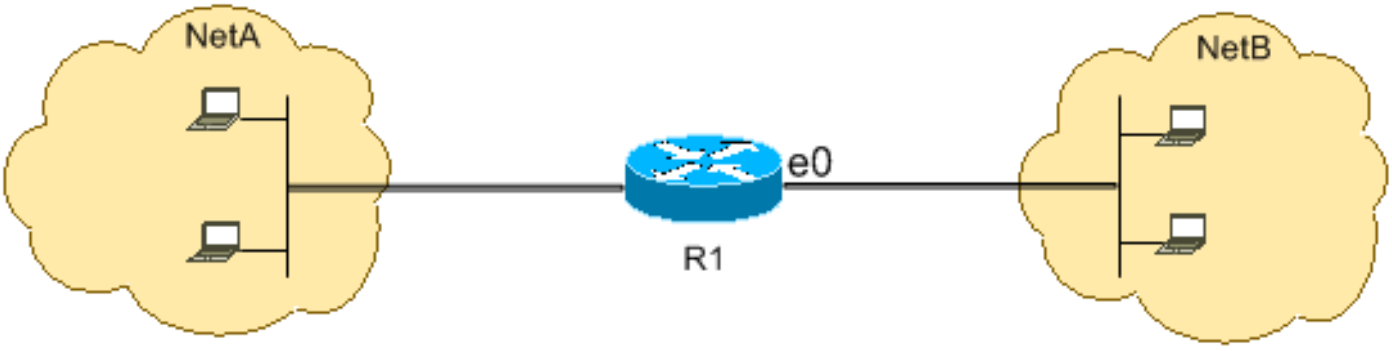
O Telnet usa a porta 23. Esta configuração mostra que todo o tráfego TCP destinado à NetA para a porta 23 é bloqueado e todos os outros tráfegos IP são permitidos.

R1

```
hostname R1
!
interface ethernet0
 ip access-group 102 in
!
access-list 102 deny tcp any any eq 23
access-list 102 permit ip any any
```

Permitir que apenas redes internas iniciem uma sessão de TCP

Esta figura mostra que o tráfego TCP originado de NetA e destinado à NetB é permitido, enquanto o tráfego TCP de NetB com destino à NetA é negado.



O objetivo da ACL neste exemplo é:

- Permitir que hosts na NetA iniciem e estabeleçam uma sessão TCP aos hosts em NetB.
- Nega que os hosts em NetB iniciem e estabeleçam uma sessão TCP destinada a hosts em NetA.

Essa configuração permite que um datagrama passe pela interface Ethernet 0 de entrada em R1, quando o datagrama tem:

- Conjunto de bits confirmado (ACK) ou redefinido (RST) (indica uma sessão TCP estabelecida)
- Um valor da porta de destino maior que 1.023

R1

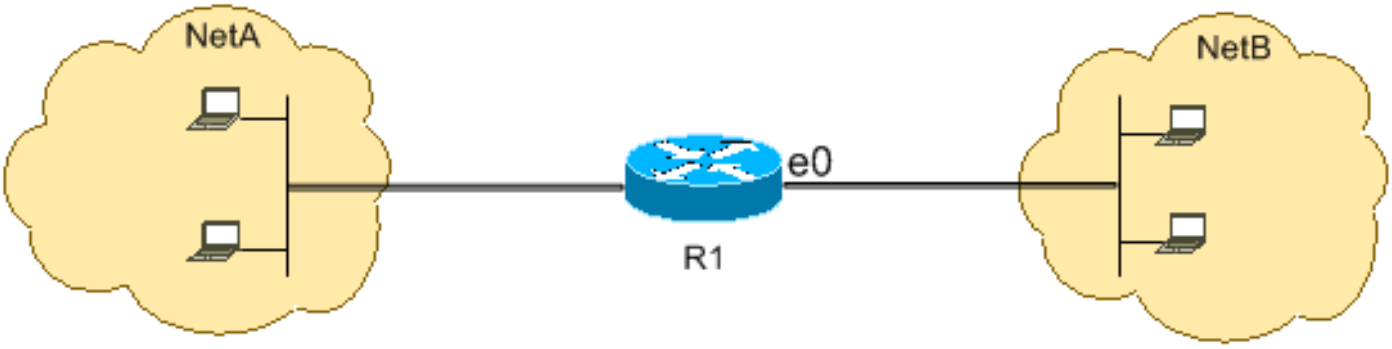
```
hostname R1
!
interface ethernet0
 ip access-group 102 in
!
access-list 102 permit tcp any any gt 1023 established
```

Como a maioria das portas bem conhecidas para serviços IP usa valores menores que 1.023, qualquer datagrama com uma porta de destino menor que 1.023 ou um bit ACK/RST não definido é negado pela ACL 102. Portanto, quando um host de NetB inicia uma conexão TCP e envia o primeiro pacote TCP (sem o conjunto de bits SYN/RST) para um número de porta menor que 1023, ele é negado e a sessão TCP falha. As sessões TCP iniciadas em NetA destinadas à NetB são permitidas porque têm bit RST/ACK definido para retornar os pacotes e usar valores de portas maiores que 1.023.

Consulte o RFC 1700 para obter uma lista completa de portas.

Recusar tráfego FTP (TCP, Porta 21)

Esta imagem mostra que o tráfego FTP (TCP, porta 21) e de dados FTP (porta 20) originado em NetB com destino a NetA é negado, enquanto todo o tráfego IP restante é permitido.



O FTP usa as portas 21 e 20. O tráfego TCP destinado às portas 21 e 20 é negado e todo o restante é explicitamente permitido.

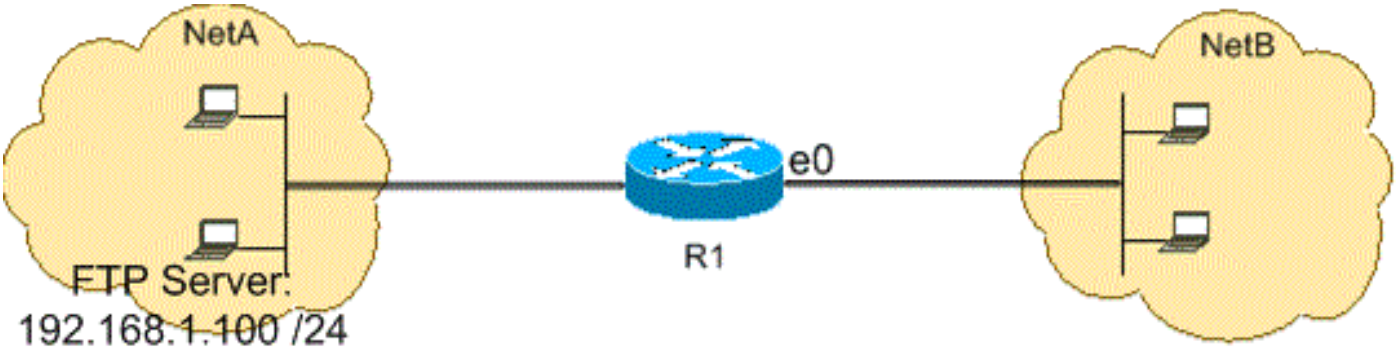
R1

```
hostname R1
!
interface ethernet0
 ip access-group 102 in
!
access-list 102 deny tcp any any eq ftp
access-list 102 deny tcp any any eq ftp-data
access-list 102 permit ip any any
```

Permitir tráfego de FTP (FTP ativo)

O FTP pode operar em dois modos diferentes, chamados de ativo e passivo.

Quando o FTP opera no modo ativo, o servidor FTP usa a porta 21 para controle e a porta 20 para dados. O servidor FTP (192.168.1.100) está localizado na NetA. Esta imagem mostra que o tráfego FTP (TCP, porta 21) e de dados FTP (porta 20) originado em NetB com destino ao servidor FTP (192.168.1.100) é permitido, enquanto todo o tráfego IP restante é negado.



R1

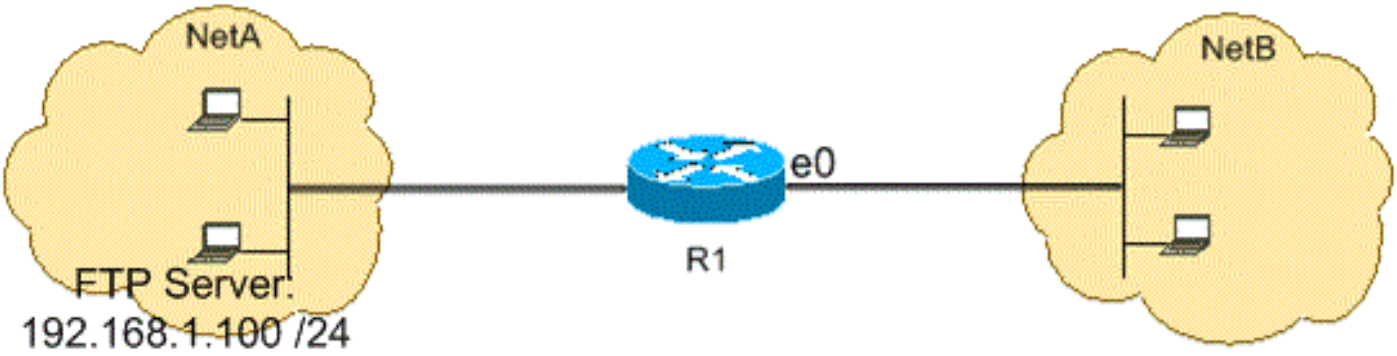
```
hostname R1
!
interface ethernet0
 ip access-group 102 in
!
access-list 102 permit tcp any host 192.168.1.100 eq ftp
access-list 102 permit tcp any host 192.168.1.100 eq ftp-data established
!
interface ethernet1
 ip access-group 110 in
!
access-list 110 permit host 192.168.1.100 eq ftp any established
access-list 110 permit host 192.168.1.100 eq ftp-data any
```

Permitir tráfego de FTP (FTP passivo)

O FTP pode operar em dois modos diferentes, chamados de ativo e passivo.

Quando o FTP opera no modo passivo, o servidor FTP usa a porta 21 para controle e as portas

dinâmicas maiores ou iguais a 1.024 para dados. O servidor FTP (192.168.1.100) está localizado na NetA. Esta imagem mostra que o tráfego FTP (TCP, porta 21) e de dados FTP (portas maiores ou iguais a 1024) originado de NetB destinado ao servidor FTP (192.168.1.100) é permitido, enquanto todo o tráfego IP restante é negado.

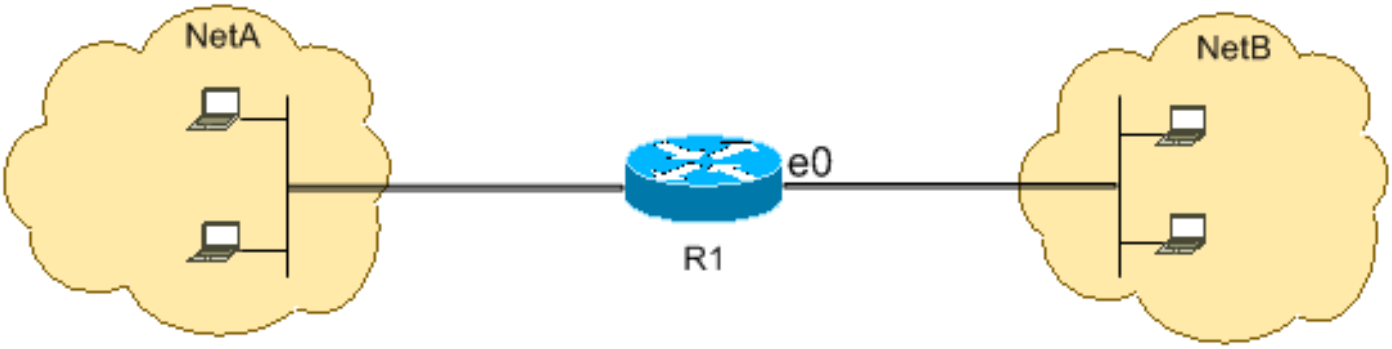


R1

```
hostname R1
!
interface ethernet0
 ip access-group 102 in
!
access-list 102 permit tcp any host 192.168.1.100 eq ftp
access-list 102 permit tcp any host 192.168.1.100 gt 1023
!
interface ethernet1
 ip access-group 110 in
!
access-list 110 permit host 192.168.1.100 eq ftp any established
access-list 110 permit host 192.168.1.100 gt 1023 any established
```

Permitir pings (ICMP)

Esta imagem mostra que o ICMP originado de NetA com destino a NetB é permitido, e os pings originados de NetB com destino a NetA são negados.



Esta configuração permite apenas que os pacotes de resposta em eco (resposta de ping) entrem na interface Ethernet 0 de NetB para NetA. No entanto, a configuração bloqueia todos os pacotes ICMP de solicitação de eco quando pings são originados em NetB e destinados à NetA. Portanto,

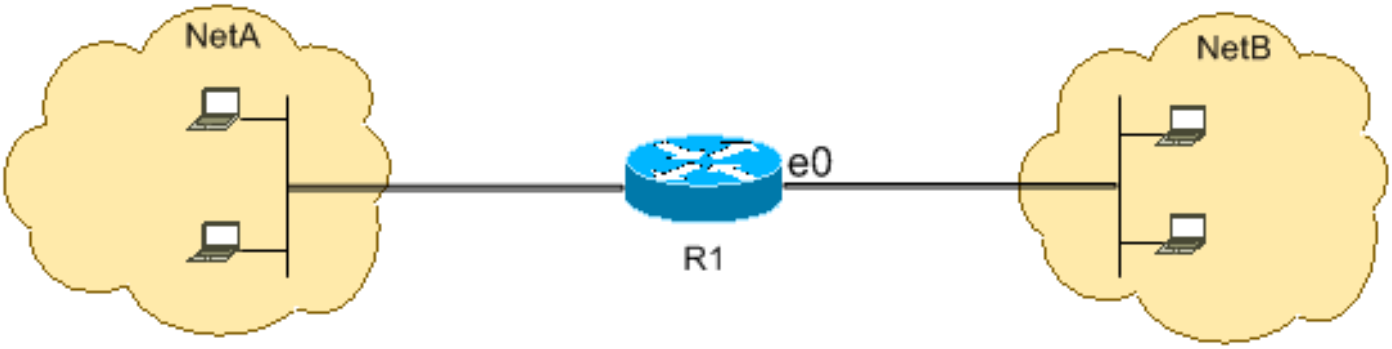
os hosts em NetA podem fazer ping aos hosts em NetB, mas os hosts em NetB não podem fazer ping em hosts na NetA.

R1

```
hostname R1
!
interface ethernet0
 ip access-group 102 in
!
access-list 102 permit icmp any any echo-reply
```

Permitir HTTP, Telnet, Correio, POP3, FTP

Esta imagem mostra que somente tráfego HTTP, Telnet, SMTP (Simple Mail Transfer Protocol), POP3 e FTP são permitidos, e o restante do tráfego originado de NetB com destino a NetA é negado.



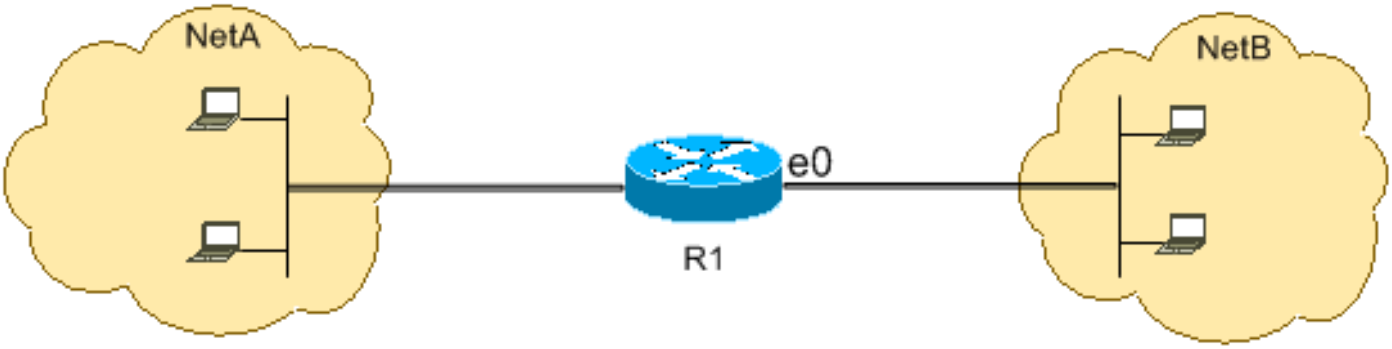
Esta configuração permite o tráfego TCP com valores de porta de destino que correspondem a WWW (porta 80), Telnet (porta 23), SMTP (porta 25), POP3 (porta 110), FTP (porta 21) ou dados de FTP (porta 20). Observe que uma cláusula deny all implícita no final de uma ACL nega todo o tráfego restante, o que não corresponde com as cláusulas permit.

R1

```
hostname R1
!
interface ethernet0
 ip access-group 102 in
!
access-list 102 permit tcp any any eq www
access-list 102 permit tcp any any eq telnet
access-list 102 permit tcp any any eq smtp
access-list 102 permit tcp any any eq pop3
access-list 102 permit tcp any any eq 21
access-list 102 permit tcp any any eq 20
```

Permitir DNS

Esta imagem mostra que somente o tráfego do Sistema de Nome de Domínio (DNS) é permitido, e o restante do tráfego originado de NetB com destino a NetA é negado.



Esta configuração permite o tráfego TCP com o valor de porta de destino 53. A cláusula implicit deny all no final de uma ACL nega todos os outros tráfegos, o que não corresponde às cláusulas de permissão.

R1

```
hostname R1
!
interface ethernet0
 ip access-group 102 in
!
access-list 102 permit udp any any eq domain
access-list 102 permit udp any eq domain any
access-list 102 permit tcp any any eq domain
access-list 102 permit tcp any eq domain any
```

Permitir Atualizações de Roteamento

Ao aplicar uma ACL de chegada a uma interface, verifique se as atualizações de roteamento não foram removidas. Use a ACL relevante desta lista para permitir pacotes de protocolo de roteamento:

Digite este comando para permitir o Protocolo RIP:

```
access-list 102 permit udp any any eq rip
```

Digite este comando para permitir o protocolo IGRP:

```
access-list 102 permit igrp any any
```

Digite este comando para permitir o IGRP aprimorado (EIGRP):

```
access-list 102 permit eigrp any any
```

Digite este comando para permitir o protocolo OSPF:

```
access-list 102 permit ospf any any
```

Digite este comando para permitir o protocolo BGP:

<#root>

```
access-list 102 permit tcp any any eq
179

access-list 102 permit tcp any eq
179
 any
```

Depurar tráfego baseado na ACL

O uso de debug command requer a alocação de recursos de sistema, como poder de processamento e memória e, em situações extremas, pode provocar a parada de um sistema muito pesado. Use o debug command com cuidado. Use uma ACL para definir seletivamente o tráfego que precisa ser examinado para reduzir o impacto do comando debug. Essa configuração não filtra todos os pacotes.

Essa configuração ativa o comando debug ip packet somente para pacotes entre os hosts 10.1.1.1 e 172.16.1.1.

<#root>

```
R1(config)#
access-list 199 permit tcp host 10.1.1.1 host 172.16.1.1
R1(config)#
access-list 199 permit tcp host 172.16.1.1 host 10.1.1.1
R1(config)#
```

```
end
```

```
R1#debug ip packet 199 detail
IP packet debugging is on (detailed) for access list 199
```

Consulte as informações importantes sobre os debug commands para obter mais informações sobre o impacto dos debug commands.

Consulte a seção Uso do debug command em Compreensão dos comandos ping e traceroute para obter mais informações sobre o uso das ACLs com debug commands.

Filtragem de endereços MAC

Você pode filtrar quadros com um endereço de origem e de destino de estação de camada MAC. Qualquer quantidade de endereços pode ser configurada para o sistema, sem uma penalidade de desempenho. Para filtrar por endereço de camada MAC, use este comando no modo de configurações globais:

<#root>

```
Router#
config terminal
Router(config)#
bridge irb
Router(config)#
bridge 1 protocol ieee
Router(config)#
bridge 1 route ip
```

Aplique o protocolo de ponte a uma interface de que você precisa para filtrar o tráfego junto com a lista de acesso criada com o comando bridge-group <group number> {input-address-list <ACL number> | output-address-list <número da ACL>}:

<#root>

```
Router#
config terminal
Router(config-if)#
interface fastEthernet0/0
```

```
Router(config-if)#
no ip address

Router(config-if)#
bridge-group 1 input-address-list 700

Router(config-if)#
exit
```

Crie uma interface virtual com bridge e aplique o endereço IP que foi atribuído à interface Ethernet física:

```
<#root>
Router#
config terminal

Router(config-if)#
int bvi1

Router(config-if)#
ip address 192.168.1.1 255.255.255.0

Router(config-if)#
exit

Router(config)#
access-list 700 deny aaaa.bbbb.cccc 0000.0000.0000

Router(config)#
access-list 700 permit 0000.0000.0000 ffff.ffff.ffff
```

Com essa configuração, o roteador só permite os endereços MAC configurados na lista de acesso 700. Com o comando access list access-list <número ACL> deny <endereço MAC> 0000.0000.0000, negue o endereço MAC que não pode ter acesso e permita o resto (para este exemplo, aaaa.bbb.cccc).

Observação: crie cada linha da lista de acesso para cada endereço MAC.

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshooting

No momento, não há informações específicas disponíveis para solucionar esse problema de configuração.

Informações Relacionadas

- Configurando listas de acesso de IP
- Página de Suporte das Listas de Acesso
- Página de Suporte do IP Routing
- Página de suporte aos protocolos de roteamento IP
- Suporte Técnico e Documentação - Cisco Systems

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.