Configurar IP de uso geral ACL

Índice

Introdução

Este documento fornece configurações de exemplo para as Listas de Controle de Acesso (ACLs) do IP, o que filtra os pacotes IP baseados em:

- Endereço de origem
- Endereço de destino
- Tipo de pacote
- Alguma combinação destes artigos

A fim filtrar o tráfego de rede, controle ACL se os pacotes roteado estão enviados ou obstruídos na interface do roteador. Seu roteador examina cada pacote a fim determinar se enviar ou deixar cair o pacote baseado nos critérios que você especifica dentro do ACL. Os critérios ACL incluem:

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

Termine estas etapas a fim construir um ACL como os exemplos neste documento mostram:

1. Crie um ACL.
2. Aplique o ACL a uma relação.

O IP ACL é uma coleção sequencial da licença e nega as circunstâncias que se aplicam a um pacote IP. O roteador testa pacotes em relação às condições no ACL, um por vez.

O primeiro fósforo determina se o Cisco IOS ® Software aceita ou rejeita o pacote. Porque as configurações de teste de paradas do Cisco IOS Software após o primeiro fósforo, a ordem das circunstâncias é crítica. Se nenhuma circunstância combina, o roteador rejeita o pacote devido a um implícito nega toda a cláusula.

Estes são os exemplos de IP ACL que podem ser configurados no Cisco IOS Software:

- ACLs padrões
- ACLs estendidos
- (Bloqueio e chave) ACL dinâmicos
- ACL IP-Nomeados
- ACLs reflexivos
- ACL com base no período que usam intervalos de tempo
- Entradas ACL comentadas IP
- ACL Contexto-baseados
- Proxy de autenticação
- Turbo ACLs
- ACLs distribuídos com base no período

Este documento discute algumas ACLs estendidas e padrão comumente utilizadas. Refira configurar listas de acesso IP para obter mais informações sobre dos tipos diferentes de ACL apoiados no Cisco IOS Software e como configurar e editar ACL.

O formato de sintaxe de comando de um padrão ACL é **access-list-number da lista de acesso {licença|negue} {host|widlcard de origem da fonte|alguns}**.

O padrão ACL compara o endereço de origem dos pacotes IP aos endereços configurados no tráfego de controle ACL.

Os ACL extendido comparam os endereços de rementente e destinatário dos pacotes IP aos endereços configurados no tráfego de controle ACL. Você pode igualmente fazer ACL extendido mais granulados e configurados ao filtrar tráfego por critérios como:

- Protocolo
- Números de porta
- Valor do Differentiated Services Code Point (DSCP)
- Valor de precedência
- Estado do bit do número de sequência do sincronizar (SYN)

Os formatos de sintaxe de comando dos ACL extendido 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]
```

Internet Control Message Protocol (ICMP)

```
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]] [precedenceprecedence] [tos tos] [log |
 log-input] [time-range time-range-name][fragments]
```

Protocolo de controle do transporte (TCP)

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

Protocolo de datagrama de usuário (UDP)

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

Pré-requisitos

Requisitos

Assegure-se de que você cumpra esta exigência antes que você tente esta configuração:

- Compreensão básica do endereçamento de IP

Refira o Endereçamento e Divisão em Sub-Redes de IP para Novos Usuários para a informação adicional.

Componentes Utilizados

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

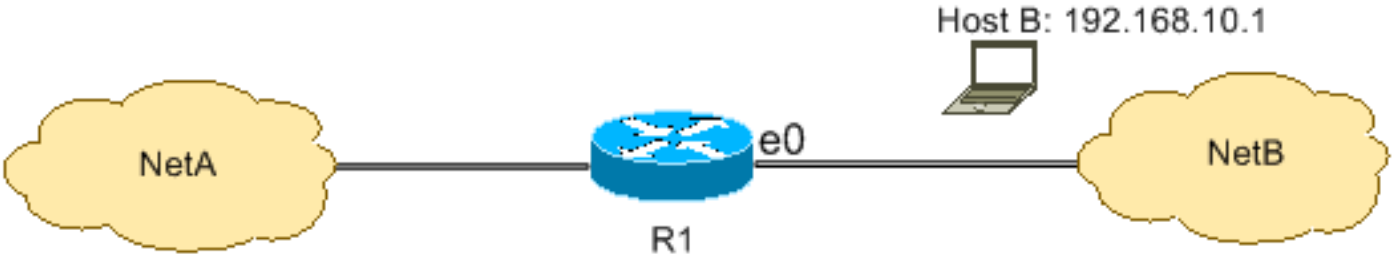
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer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

Configurar

Estes exemplos de configuração usam o IP o mais comum ACL.

Permitir que um host selecionado acesse a rede

Esta figura mostra um host selecionado que está sendo concedida a permissão alcançar a rede. Todos traficam originado do Host B destinado à NETA são permitidos, e todos os outro tráfego originado do NetB destinado à NETA são negados.



A saída na tabela do r1 mostra como a rede concede o acesso ao host. Esta saída mostra aquela:

- 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 o acesso aos Serviços IP da NETA.
- Nenhum outro host no NetB tem o acesso à NETA.
- Nenhuma instrução de negação é configurada no ACL.

Àrevelia, há um implícito nega toda a cláusula no fim de cada ACL. Qualquer coisa que não é permitido explicitamente é negado.

R1

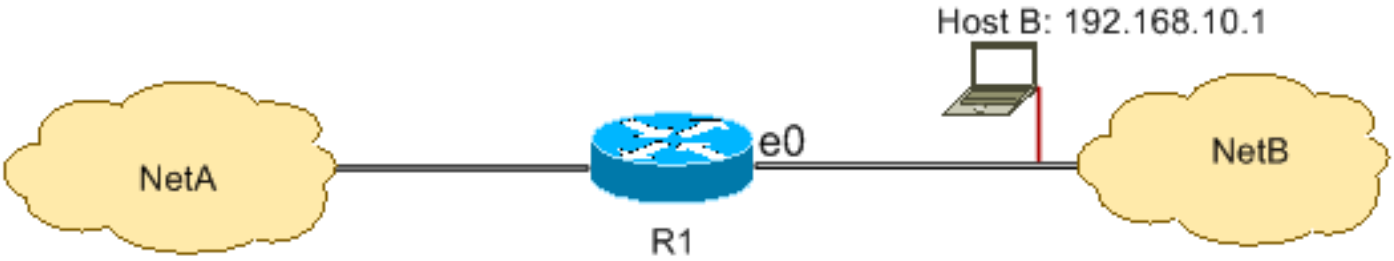
```
hostname R1
!
interface ethernet0
ip access-group 1 in
!
access-list 1 permit host 192.168.10.1
```

> Nota: O ACL filtra pacotes IP do NetB à NETA, exceto pacotes com origem do NetB. Os pacotes com origem do Host B à NETA são permitidos ainda.

> Nota: **A licença 192.168.10.1 0.0.0.0 da lista de acesso 1** ACL é uma outra maneira de configurar a mesma regra.

Recusar que um host de seleção acesse a rede

Esta figura mostra que o tráfego originado do Host B destinado à NETA está negado, quando todo tráfego restante do NetB para alcançar a NETA for permitido.



Esta configuração nega todos os pacotes do host 192.168.10.1/32 com o ethernet0 no r1 e permite tudo mais. Você deve usar o comando access list 1 permit any permitir explicitamente tudo mais porque há um implícito nega toda a cláusula com cada ACL.

R1

```
hostname R1
!
interface ethernet0
```

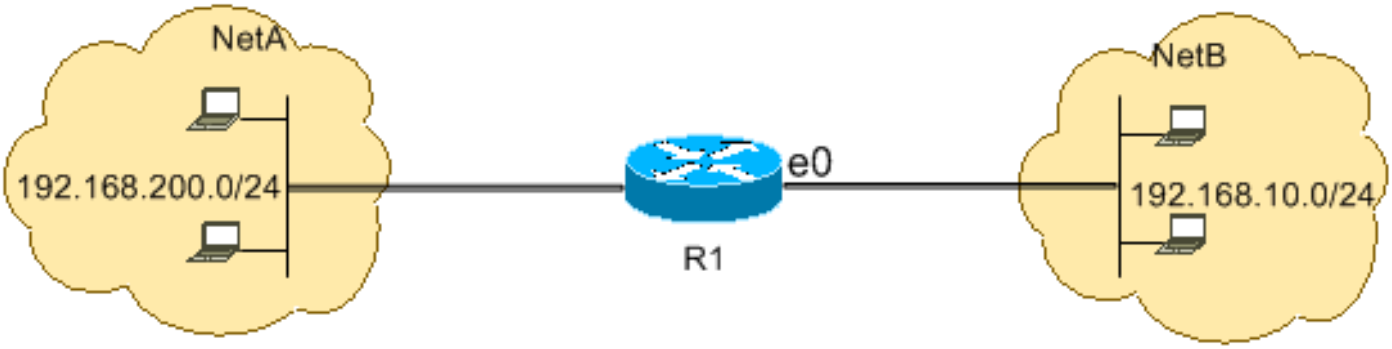
```
ip access-group 1 in
!
access-list 1 deny host 192.168.10.1
access-list 1 permit any
```

Nota: A ordem das instruções é essencial para a operação de um ACL. Se a ordem das entradas é invertida enquanto este comando mostra, a primeira linha combina cada endereço de origem de pacote. Consequentemente, o ACL não obstrui o host 192.168.10.1/32 da NETA de acesso.

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

Permita acesso a uma faixa de endereços IP contíguos

Esta figura mostra que todos os anfitriões no NetB com o endereço de rede 192.168.10.0/24 podem a rede de acesso 192.168.200.0/24 na NETA.



Esta configuração permite os pacotes IP com um cabeçalho IP que tenha um endereço de origem na rede 192.168.10.0/24 e um endereço de destino no acesso da rede 192.168.200.0/24 à NETA. Há o implícito nega toda a cláusula no fim do ACL que nega toda passagem restante do tráfego com o ethernet0 de entrada no 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
```

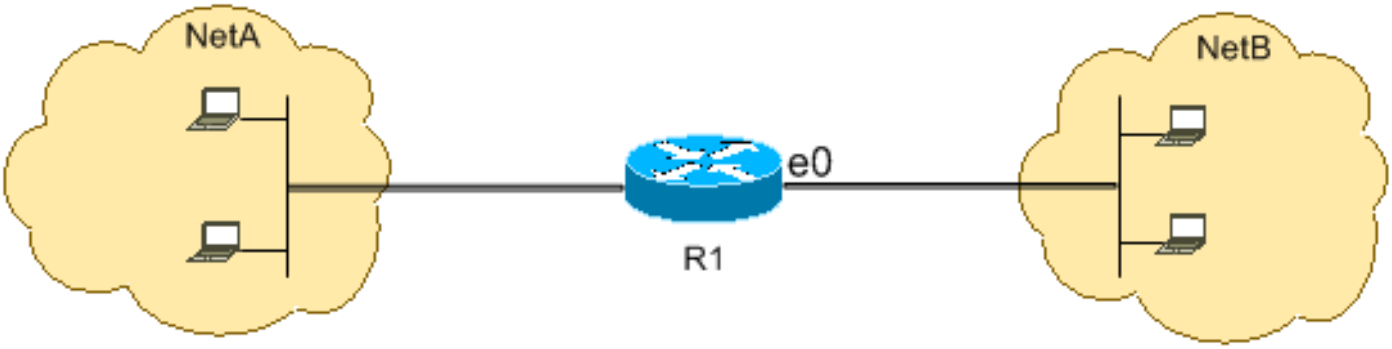
Nota: **Na licença IP 192.168.10.0 0.0.0.255 192.168.200.0 0.0.0.255 do** comando access-list 101, o "0.0.0.255" é a máscara de rede inversa 192.168.10.0 com máscara 255.255.255.0. Os ACL usam a máscara inversa para saber quantos bit no endereço de rede precisam de combinar. Na tabela, o ACL permite todos os anfitriões com endereços de origem nos 192.168.10.0/24 rede e endereços de destino na rede 192.168.200.0/24.

Refira a seção das máscaras de configurar listas de acesso IP para obter mais informações sobre da máscara de um endereço de rede e como calcular a máscara inversa necessária para ACL.

Negar tráfego Telnet (TCP, porta 23)

A fim encontrar interesses de segurança mais elevada, você pôde ter que desabilitar o acesso do

telnet a sua rede privada da rede pública. Esta figura mostra como o tráfego do telnet do NetB (público) destinado à NETA (privada) é negado, que permite a NETA iniciar e estabelecer uma sessão de Telnet com NetB quando todo tráfego IP restante for permitido.



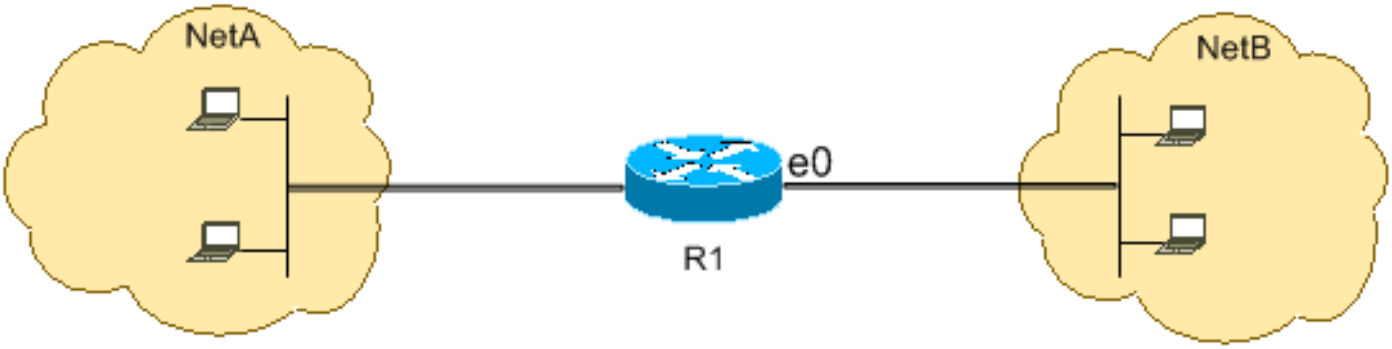
O telnet usa o TCP, a porta 23. Esta configuração mostra que todo o tráfego TCP destinado à NETA para a porta 23 está obstruído, e todo tráfego IP restante é permitido.

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 da NETA destinada ao NetB está permitido, quando o tráfego TCP do NetB destinado à NETA for negado.



A finalidade do ACL neste exemplo está a:

- Permita que os anfitriões na NETA iniciem e estabeleçam uma sessão de TCP aos anfitriões no NetB.
- Negue anfitriões no NetB de iniciar e de estabelecer uma sessão de TCP destinada aos anfitriões na NETA.

Esta configuração permite que uma datagrama passe com o interface ethernet 0 de entrada no r1 quando a datagrama tem:

- Bit reconhecido (ACK) ou da restauração (RST) ajustados (indicando uma sessão de TCP estabelecida)
- Um valor de porta do destino maior de 1023

R1

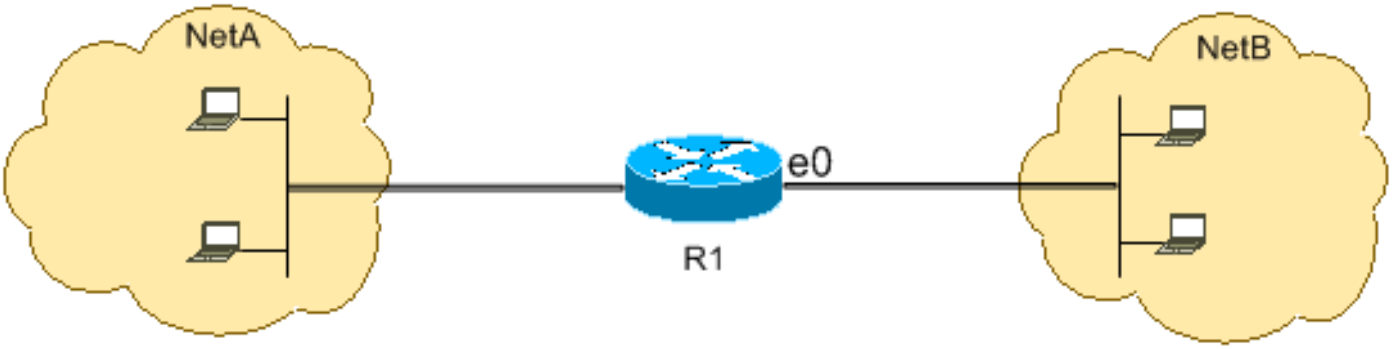
```
hostname R1
!
interface ethernet0
ip access-group 102 in
!
access-list 102 permit tcp any any gt 1023 established
```

Desde a maioria das portas bem conhecidas para valores do uso dos Serviços IP menos de 1023, toda a datagrama com uma porta do destino menos de 1023 ou um ACK/RST mordidos não ajustado é negado pelo ACL 102. Consequentemente, quando um host do NetB inicia uma conexão de TCP enviando o primeiro pacote de TCP (sem sincronizar/iniciar o conjunto de bit de pacote (SYN/RST)) para um número de porta menos de 1023, nega-se e a sessão de TCP falha. As sessões de TCP iniciadas da NETA destinada ao NetB são permitidas porque têm o jogo do bit ACK/RST para pacotes de retorno e usam os valores de porta maiores de 1023.

Refira o RFC 1700 para uma lista completa das portas.

Recusar tráfego FTP (TCP, Porta 21)

Esta figura mostra que FTP (TCP, porta 21) e o tráfego dos dados FTP (porta 20) originado do NetB destinado à NETA está negado, quando todo tráfego IP restante for permitido.



O FTP usa a porta 21 e a porta 20. O tráfego TCP destinou à porta 21 e a porta 20 é negada e tudo mais é permitido explicitamente.

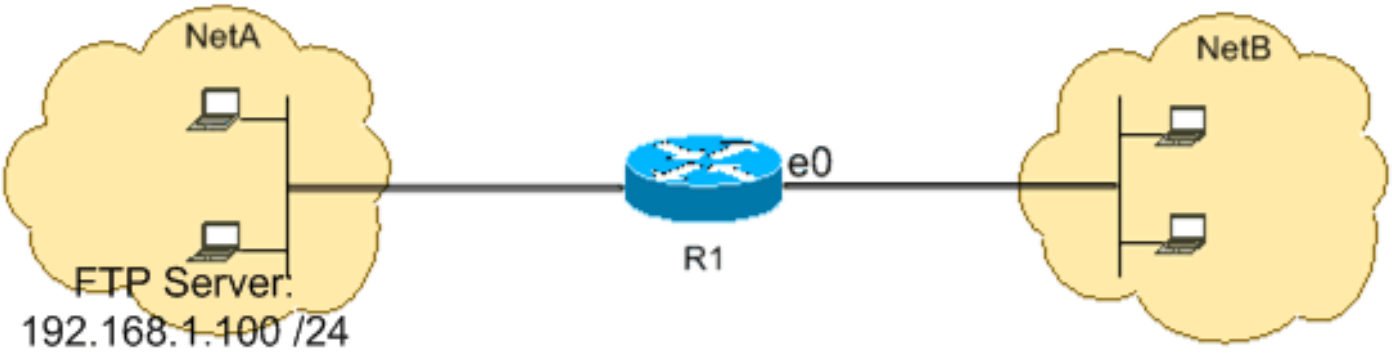
R1

```
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
```

Permita o tráfego FTP (o FTP ativo)

O FTP pode operar-se em dois modos diferentes nomeados active e voz passiva. Refira a operação de FTP para compreender como o active e o FTP passivo trabalham.

Quando o FTP se opera no modo ativo, o servidor FTP usa a porta 21 para o controle e a porta 20 para dados. O servidor FTP (192.168.1.100) é ficado situado na NETA. Esta figura mostra que FTP (TCP, porta 21) e o tráfego dos dados FTP (porta 20) originado do NetB destinado ao servidor FTP (192.168.1.100) está permitido, quando todo tráfego IP restante for negado.



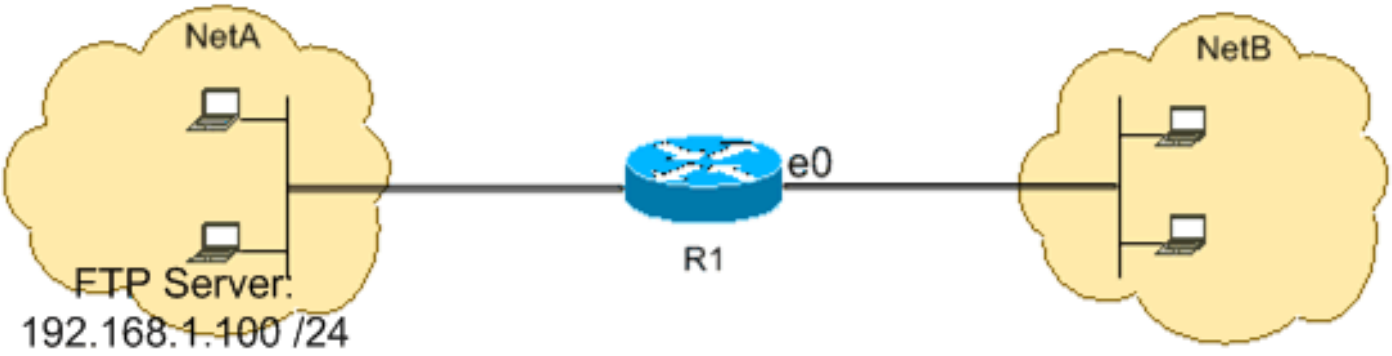
R1

```
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
```

Permita o tráfego FTP (o FTP passivo)

O FTP pode operar-se em dois modos diferentes nomeados active e voz passiva. Refira a operação de FTP a fim compreender como o active e o FTP passivo trabalham.

Quando o FTP se opera no modo passivo, o servidor FTP usa a porta 21 para o controle e as portas dinâmica superior ou igual a 1024 para dados. O servidor FTP (192.168.1.100) é ficado situado na NETA. Esta figura mostra que FTP (TCP, porta 21) e o tráfego dos dados FTP (portas superior ou igual a 1024) originado do NetB destinado ao servidor FTP (192.168.1.100) está permitido, quando todo tráfego IP restante for negado.



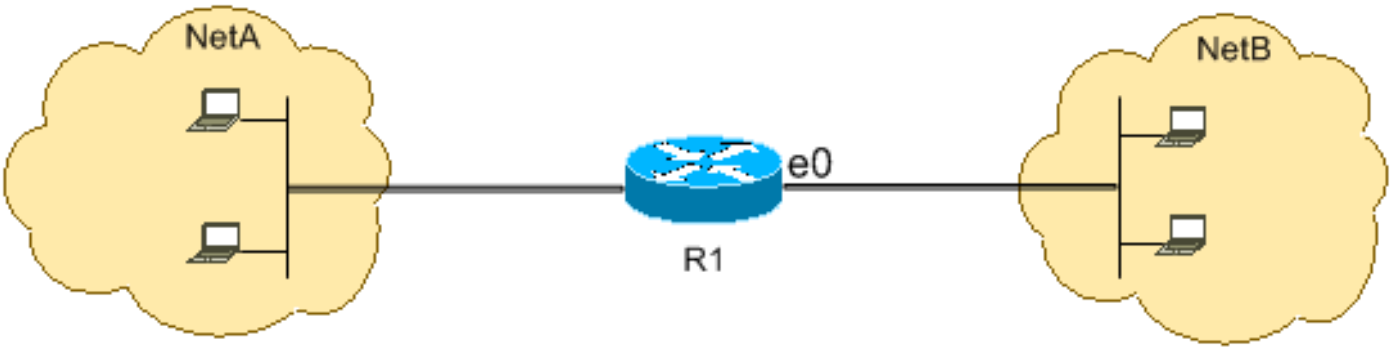
R1

```
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 1024
!
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 1024 any established
```

Permitir pings (ICMP)

Esta figura mostra que o ICMP originado da NETA destinada ao NetB está permitido, e os sibilos originado do NetB destinado à NETA são negados.



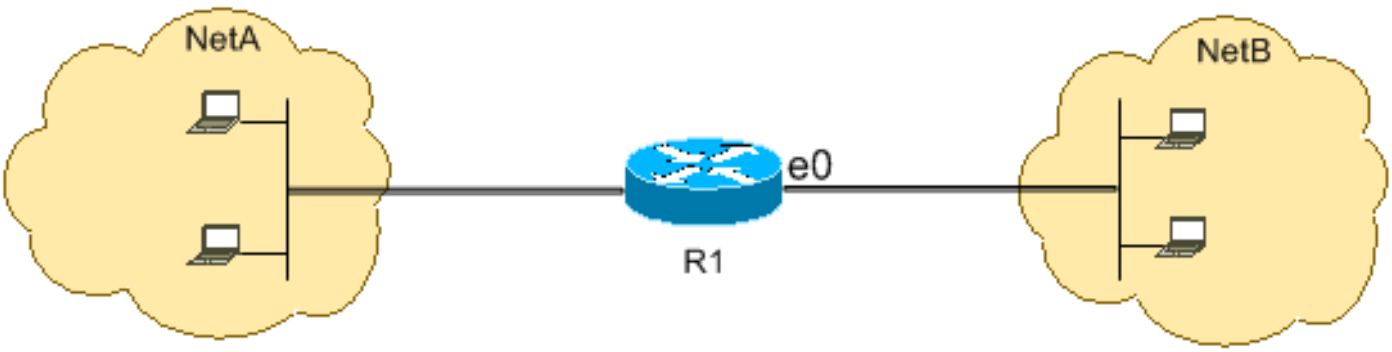
Esta configuração permite somente pacotes da resposta de eco (resposta de ping) vir dentro no interface ethernet 0 do NetB para a NETA. Contudo, a configuração obstrui todos os pacotes ICMP da requisição de eco quando os sibilos são originado no NetB e são destinados à NETA. Consequentemente, os anfitriões na NETA podem sibilar anfitriões no NetB, mas os anfitriões no NetB não podem sibilar anfitriões 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 figura mostra que o tráfego somente HTTP, de telnet, de Simple Mail Transfer Protocol (SMTP), POP3, e FTP está permitido, e o resto do tráfego originado do NetB destinado à NETA é negado.



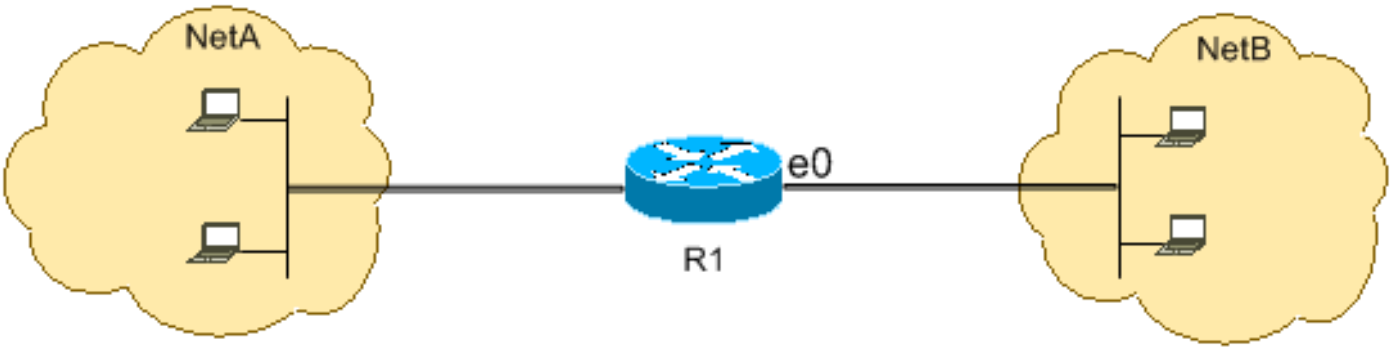
Esta configuração permite o tráfego TCP com valores de porta do destino que combinam dados WWW (porta 80), de telnet (porta 23), S TP (porta 25), POP3 (porta 110), FTP (porta 21), ou FTP (porta 20). Observe que um implícito para negar toda a cláusula no fim de um ACL nega todo tráfego restante, que não combina as cláusulas da licença.

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
```

Permita o DNS

Esta figura mostra que somente o tráfego do Domain Name System (DNS) está permitido, e o resto do tráfego originado do NetB destinado à NETA é negado.



Esta configuração permite o tráfego TCP com valor de porta do 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 112 permit udp any any eq domain
access-list 112 permit udp any eq domain any
access-list 112 permit tcp any any eq domain
access-list 112 permit tcp any eq domain any
```

Permitir Atualizações de Roteamento

Quando você aplica um em-limite ACL sobre a uma relação, assegure-se de que as atualizações de roteamento não estejam filtradas para fora. Use o ACL relevante desta lista para permitir pacotes de protocolo de roteamento:

Incorpore este comando a fim permitir o Routing Information Protocol (RIP):

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

Incorpore este comando a fim permitir o Interior Gateway Routing Protocol (IGRP):

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

Incorpore este comando a fim permitir o IGRP aprimorado (EIGRP):

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

Incorpore este comando a fim permitir o Open Shortest Path First (OSPF):

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

Incorpore este comando a fim permitir o Border Gateway Protocol (BGP):

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

Debugar o tráfego baseado no ACL

O uso dos **comandos debug** exige a atribuição de recursos de sistema como a memória e a potência de processamento e nas situações extremas pode fazer com que um sistema pesado-carregado pare. Use **comandos debug** com cuidado. Use um ACL a fim definir seletivamente o tráfego que precisa de ser examinado para reduzir o impacto do comando do thedebug. Tal configuração não filtra nenhuns pacotes.

Esta configuração gerencie sobre o **comando debug ip packet** somente para pacotes entre os anfitriões 10.1.1.1 e 172.16.1.1.

```
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
```

Refira a informação importante em comandos Debug para obter informações adicionais sobre do impacto dos comandos debug.

Refira o uso à seção de comando Debug de compreender os comandos ping and traceroute para obter informações adicionais sobre do uso dos ACL com **comandos debug**.

Filtração do MAC address

Você pode filtrar quadros com um endereço de origem ou de destino particular da estação da camada de MAC. Todo o número de endereços pode ser configurado no sistema sem uma penalidade de desempenho. A fim filtrar pelo endereço de camada MAC, use este comando no modo de configuração global:

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

Aplique o Bridge Protocol a uma relação que você precise o filtrar tráfego junto com a lista de acessos criada:

```
Router#int fa0/0
       no ip address
       bridge-group 1 {input-address-list 700 | output-address-list 700}
       exit
```

Crie um Bridged Virtual Interface e aplique o endereço IP de Um ou Mais Servidores Cisco ICM NT que é atribuído à interface Ethernet:

```
Router#int bvi1
       ip address
       exit
!
```

```
!
       access-list 700 deny <mac address> 0000.0000.0000
       access-list 700 permit 0000.0000.0000 ffff.ffff.ffff
```

Com esta configuração, o roteador permite somente os endereços MAC configurados na lista de acesso 700. Com a lista de acessos, negue os adddress MAC que não podem ter o acesso e permita então o resto.

> Nota: Crie cada linha de lista de acessos para cada MAC address.

Verificar

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

Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta 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 dos protocolos roteados de IP
- Suporte Técnico e Documentação - Cisco Systems