IP de uso general ACL de la configuración

Contenido

Introducción

En este documento, se proporcionan configuraciones de ejemplo para las listas de control de acceso (ACL) IP que se utilizan comúnmente, que filtran los paquetes IP según:

- Dirección de origen
- Dirección de destino
- Tipo de paquete
- Cualquier combinación de estos elementos

Para filtrar el tráfico de la red, las ACL controlan si los paquetes ruteados se reenvían o bloquean en la interfaz del router. Su router examina cada paquete para determinar si remitir o caer el paquete basado en los criterios que usted especifica dentro del ACL. Los criterios de ACL incluyen:

- Dirección de origen del tráfico
- Dirección de destino del tráfico
- Protocolo de capa superior

Complete estos pasos para construir un ACL como los ejemplos en este documento muestran:

1. Cree una ACL.
2. Aplique la ACL a una interfaz.

El IP ACL es una colección secuencial de permiso y niega las condiciones que se aplican a un paquete del IP. El router prueba los paquetes en relación con las condiciones en la ACL, uno por vez.

La primera coincidencia determina si el Cisco IOS® Software acepta o rechaza el paquete. Debido a que el Cisco IOS Software detiene las condiciones de prueba después de la primera coincidencia, el orden de las condiciones es fundamental. Si no coincide ninguna condición, el router rechaza el paquete debido a una cláusula total de negación implícita.

Estos son ejemplos de las ACL IP que se pueden configurar en el Cisco IOS Software:

- ACL estándar
- ACL Extendidas
- ACL dinámicas (cerradura y llave)
- ACL con nombre IP
- ACL Reflexivas
- ACL basadas en tiempo que utilizan intervalos de tiempo
- Entradas de ACL IP comentadas
- ACL basadas en contexto
- Proxy de Autenticación
- Turbo ACL
- ACL distribuido basado en el tiempo

En este documento, se analizan algunas ACL estándar y extendidas que se utilizan comúnmente. Consulte Configuración de Listas de Acceso IP para obtener más información sobre diferentes tipos de ACL soportados en el Cisco IOS Software y cómo configurar y editar ACL.

El formato de sintaxis del comando de una ACL estándar es **access-list access-list-number {permit|deny} {host|source source-wildcard|ningunos}**.

Los ACL estándar comparan a la dirección de origen de los paquetes del IP a los direccionamientos configurados en el tráfico de control ACL para.

Los ACL ampliados comparan a las direcciones de origen y de destino de los paquetes del IP a los direccionamientos configurados en el tráfico de control ACL para. Usted también puede hacer que las ACL extendidas sean más granulares y se configuren para filtrar el tráfico por criterios, como:

- Protocolo
- Números de puerto
- Valor de punto de código de servicios diferenciados (DSCP)
- Valor de precedencia
- Estado del bit de número de secuencia de sincronización (SYN)

Los formatos de sintaxis del comando de las ACL extendidas son:

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]
```

Transport Control Protocol (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]
```

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

Prerrequisitos

Requisitos

Asegúrese de cumplir este requisito antes de intentar esta configuración:

- Comprensión básica del direccionamiento IP

Consulte Direccionamiento IP y Conexión en Subredes para Usuarios Nuevos para obtener información adicional.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

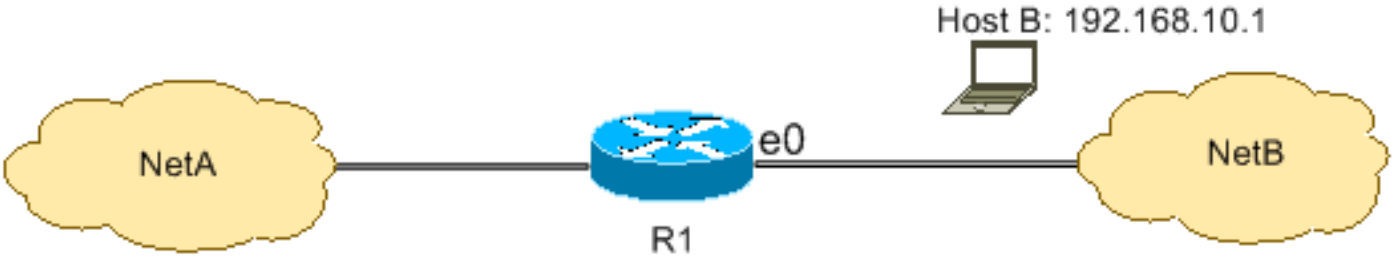
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Configurar

Estos ejemplos de configuración utilizan las ACL IP más comunes.

Cómo Permitir el Acceso de un Host Seleccionado a la Red

En esta figura, se muestra un host seleccionado al que se le ha otorgado permiso para acceder a la red. Se permite todo el tráfico con origen en el Host B y destino en la Red A, y se niega el resto del tráfico con origen en la Red B y destino en la Red A.



El resultado en la tabla R1 muestra cómo la red le otorga acceso al host. Este resultado muestra que:

- La configuración solo admite el host con la dirección IP 192.168.10.1 a través de la interfaz Ethernet 0 en R1.
- Este host tiene acceso a los servicios IP de la Red A.
- Ningún otro host en la Red B tiene acceso a la Red A.
- No se configura ninguna declaración de negación en la ACL.

De forma predeterminada, hay una cláusula total de negación implícita al final de cada ACL. Se niega todo lo que no esté explícitamente permitido.

R1

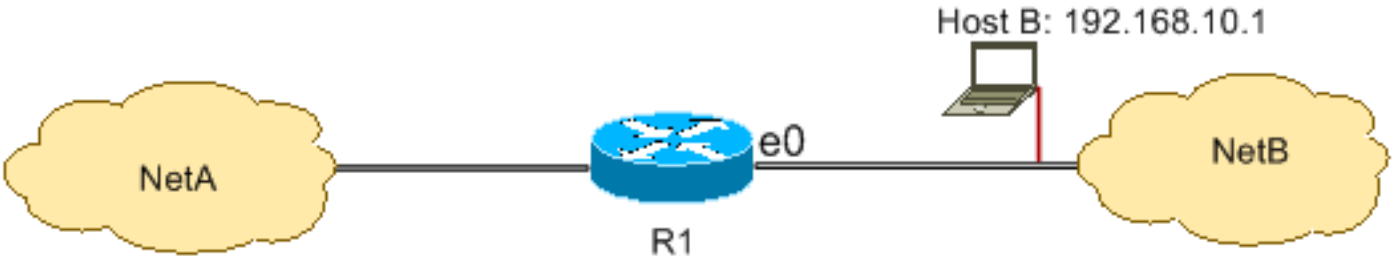
```
hostname R1
!
interface ethernet0
ip access-group 1 in
!
access-list 1 permit host 192.168.10.1
```

> Nota: La ACL filtra los paquetes IP de la Red B a la Red A, excepto los paquetes con origen en la Red B. Los paquetes originados del host B al NetA todavía se permiten.

> Nota: La ACL **access-list 1 permit 192.168.10.1 0.0.0.0** es otra manera de configurar la misma regla.

Denegación del Acceso de un Host Seleccionado a la Red

En esta figura, se muestra que se niega el tráfico con origen en el Host B y destino en la Red A, mientras que se permite el resto del tráfico de la Red B para acceder a la Red A.



Esta configuración niega todos los paquetes del host 192.168.10.1/32 a través de Ethernet 0 en R1 y permite todo lo demás. Debe utilizar el comando access list 1 permit any para permitir explícitamente todo lo demás porque hay una cláusula total de negación implícita con cada ACL.

R1

```
hostname R1
!
```

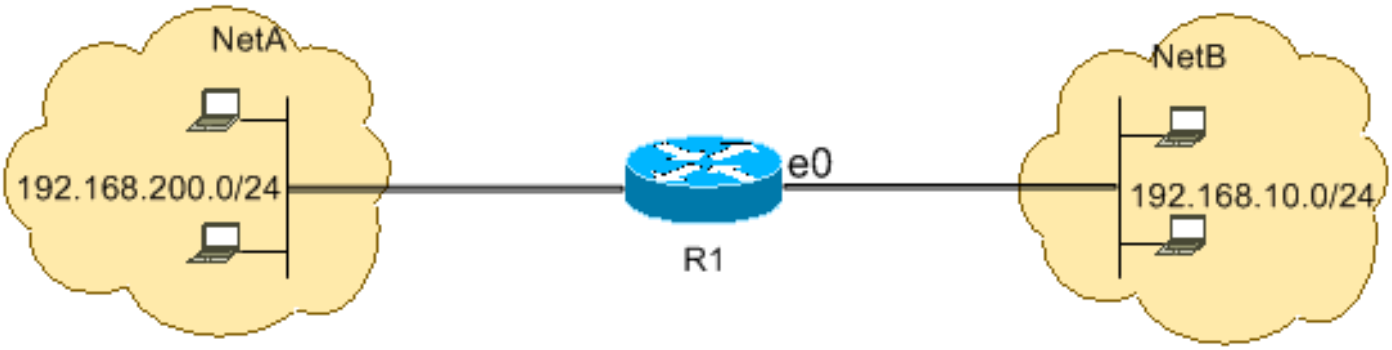
```
interface ethernet0
ip access-group 1 in
!
access-list 1 deny host 192.168.10.1
access-list 1 permit any
```

Nota: El orden de las declaraciones es fundamental para el funcionamiento de una ACL. Si el orden de las entradas se invierte como muestra este comando, la primera línea coincide con cada dirección de origen de paquete. Por lo tanto, la ACL no puede bloquear el acceso del host 192.168.10.1/32 a la Red A.

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

Permita el acceso a un rango de direcciones IP contiguas

En esta figura, se muestra que todos los hosts en la Red B con la dirección de red 192.168.10.0/24 pueden acceder a la red 192.168.200.0/24 en la Red A.



Esta configuración permite que los paquetes IP con un encabezado IP que tengan una dirección de origen en la red 192.168.10.0/24 y una dirección de destino en la red 192.168.200.0/24 accedan a la Red A. Hay una cláusula total de negación implícita al final de la ACL que niega el paso del resto del tráfico a través de Ethernet 0 entrante en R1.

R1

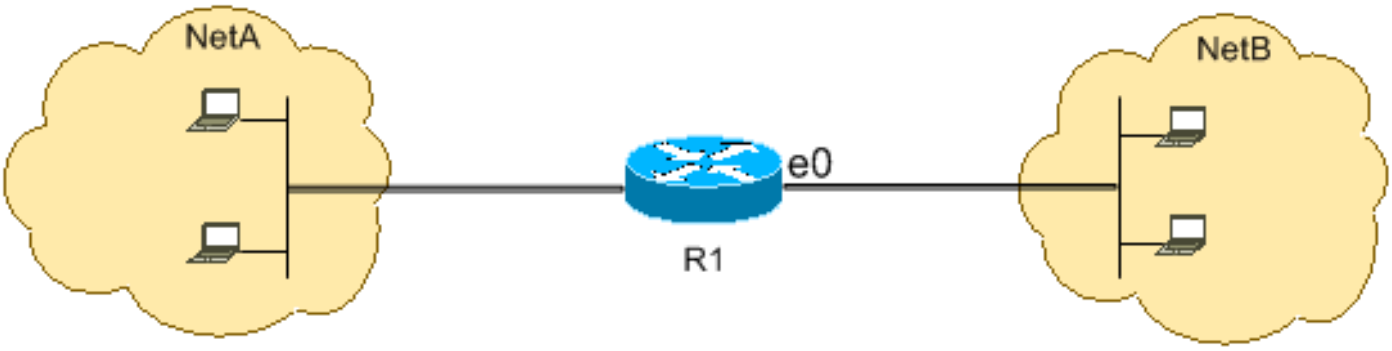
```
hostname R1
!
interface ethernet0
ip access-group 101 in
!
access-list 101 permit ip 192.168.10.0  0.0.0.255
  192.168.200.0  0.0.0.255
```

Nota: En el comando access-list 101 permit ip 192.168.10.0 0.0.0.255 192.168.200.0 0.0.0.255, el "0.0.0.255" es la máscara inversa de la red 192.168.10.0 con la máscara 255.255.255.0. Las ACL utilizan la máscara inversa para saber cuántos bits en la dirección de red deben coincidir. En la tabla, la ACL permite todos los hosts con las direcciones de origen en la red 192.168.10.0/24 y las direcciones de destino en la red 192.168.200.0/24.

Consulte la sección Máscaras de Configuración de Listas de Acceso IP para obtener más información sobre la máscara de una dirección de red y cómo calcular la máscara inversa necesaria para las ACL.

Denegación de Tráfico Telnet (TCP, puerto 23)

Para responder a las preocupaciones de mayor seguridad, es posible que deba inhabilitar el acceso Telnet a su red privada de la red pública. En esta figura, se muestra cómo se niega el tráfico Telnet de la Red B (pública) con destino en la Red A (privada), lo que permite que la Red A inicie y establezca una sesión Telnet con la Red B, mientras que se permite el resto del tráfico IP.



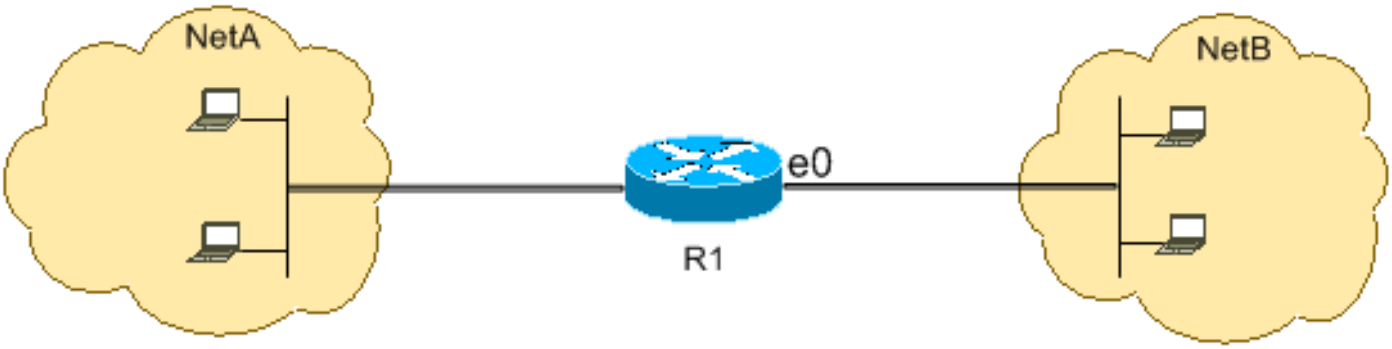
Telnet utiliza TCP, puerto 23. Esta configuración muestra que todo el tráfico TCP con destino en la Red A para el puerto 23 está bloqueado y que se permite el resto del tráfico IP.

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
```

Permita que Solo las Redes Internas Puedan Iniciar una Sesión TCP

En esta figura, se muestra que se permite el tráfico TCP con origen en la Red A y destino en la Red B, mientras que se niega el tráfico TCP de la Red B con destino en la Red A.



El propósito de la ACL en este ejemplo es:

- Permitir que los hosts en la Red A inicien y establezcan una sesión TCP para los hosts en la Red B.
- Negar que los hosts en la Red B inicien y establezcan una sesión TCP destinada a los hosts en la Red A.

Esta configuración permite que un datagrama pase a través de la interfaz Ethernet 0 entrante en R1 cuando el datagrama tiene:

- Bits reconocidos (ACK) o de restauración (RST) configurados (indicando una sesión TCP establecida)

- Un valor de puerto de destino mayor que 1023

R1

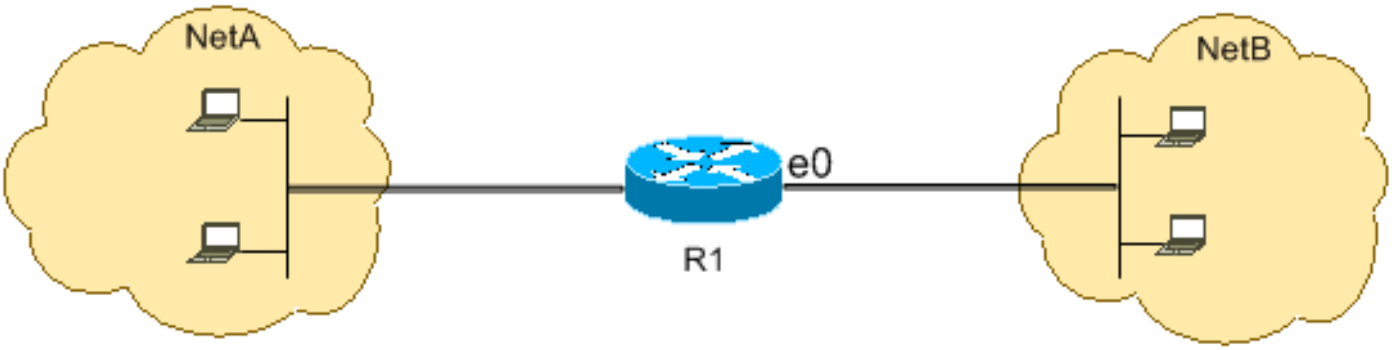
```
hostname R1
!
interface ethernet0
ip access-group 102 in
!
access-list 102 permit tcp any any gt 1023 established
```

Dado que la mayoría de los puertos conocidos para los servicios IP utilizan valores menores que 1023, cualquier datagrama con un puerto de destino menor que 1023 o un bit ACK/RST no configurado es negado por la ACL 102. Por lo tanto, cuando un host de la Red B inicia una conexión TCP enviando el primer paquete TCP (sin el bit de paquete de inicio/sincronización [RST/SYN] configurado) para un número de puerto menor que 1023, se niega y la sesión TCP falla. Se permiten las sesiones TCP iniciadas de la Red A con destino en la Red B porque tienen el bit ACK/RST configurado para la devolución de los paquetes y utilizan valores de puerto mayores que 1023.

Consulte RFC 1700 para obtener una lista completa de puertos.

Denegación de Tráfico FTP (TCP, Puerto 21)

En esta figura, se muestra que se niega el tráfico FTP (TCP, puerto 21) y de datos FTP (puerto 20) con origen en la Red B y destino en la Red A, mientras que se permite el resto del tráfico IP.



FTP utiliza el puerto 21 y el puerto 20. Se niega el tráfico TCP con destino en el puerto 21 y el puerto 20, y se permite explícitamente todo lo demás.

R1

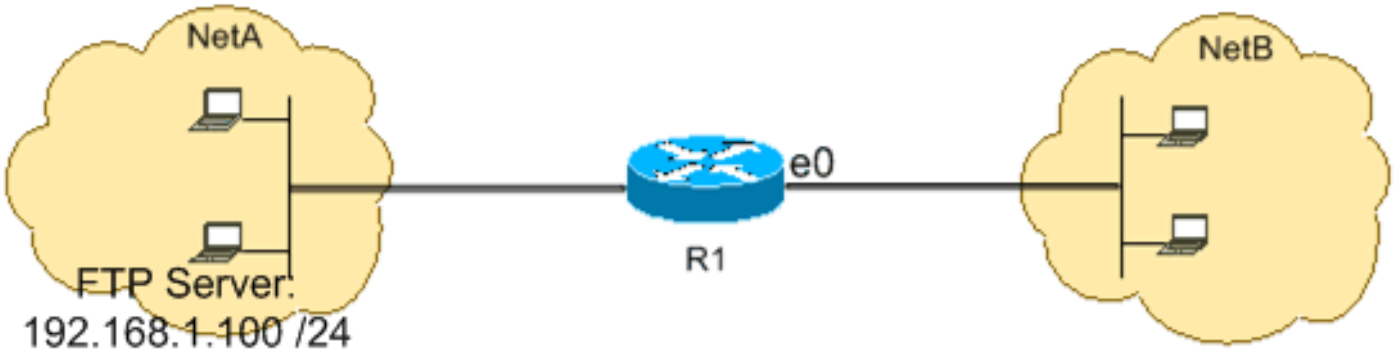
```
hostname R1
!
interface ethernet0
ip access-group 102 in
!
access-list 102 deny tcp any any eq ftp
access-list 102 deny tcp any any eq ftp-data
access-list 102 permit ip any any
```

Cómo Permitir el Tráfico FTP (FTP Activo)

FTP puede funcionar en dos modos diferentes, nombrados activo y pasivo. Consulte Funcionamiento de FTP para comprender cómo funciona el FTP activo y el pasivo.

Cuando FTP funciona en modo activo, el servidor FTP utiliza el puerto 21 para el control y el puerto 20 para los datos. El servidor FTP (192.168.1.100) está ubicado en la Red A. En esta

figura, se muestra que se permite el tráfico FTP (TCP, puerto 21) y de datos FTP (puerto 20) con origen en la Red B y destino en el servidor FTP (192.168.1.100), mientras que se niega el resto del tráfico IP.



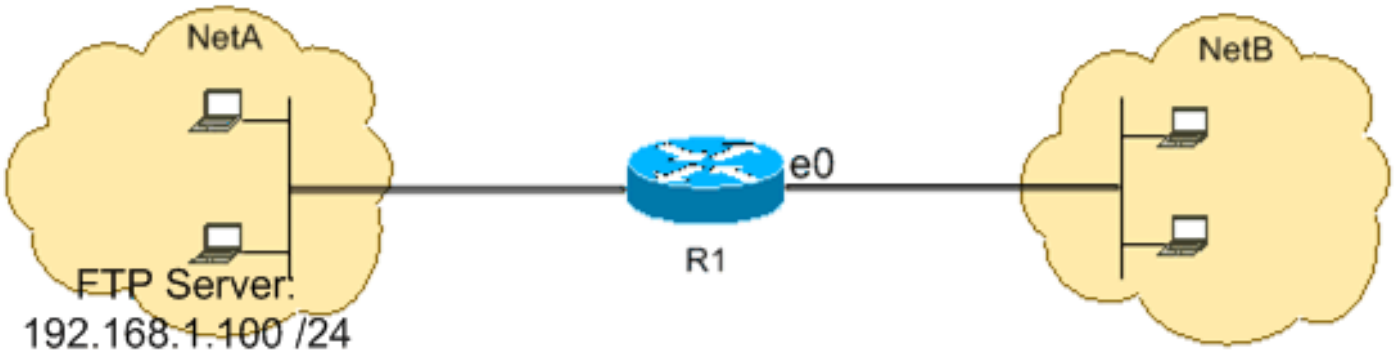
R1

```
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
```

Cómo Permitir el Tráfico FTP (FTP Pasivo)

FTP puede funcionar en dos modos diferentes, nombrados activo y pasivo. Consulte Funcionamiento de FTP para comprender cómo funciona el FTP activo y el pasivo.

Cuando FTP funciona en modo pasivo, el servidor FTP utiliza el puerto 21 para el control y los puertos dinámicos mayores o iguales que 1024 para los datos. El servidor FTP (192.168.1.100) está ubicado en la Red A. En esta figura, se muestra que se permite el tráfico FTP (TCP, puerto 21) y de datos FTP (puertos mayores o iguales que 1024) con origen en la Red B y destino en el servidor FTP (192.168.1.100), mientras que se niega el resto del tráfico IP.



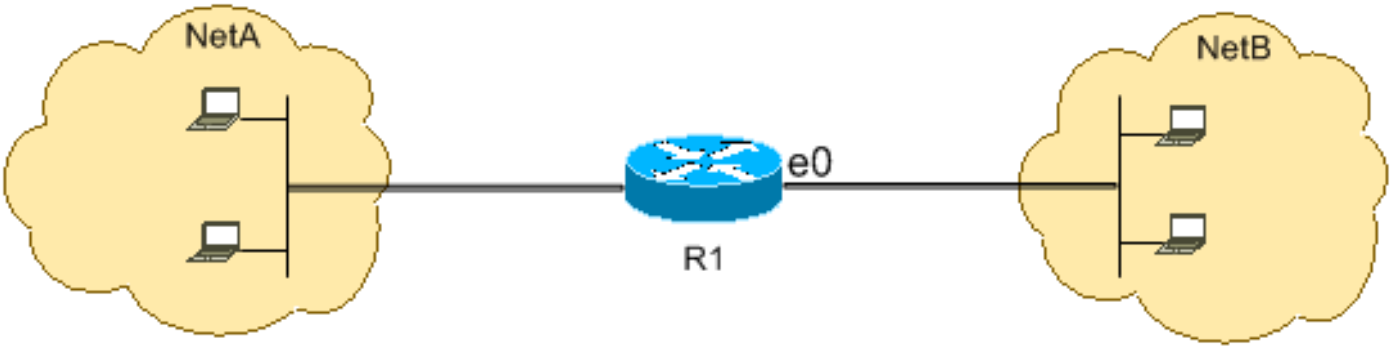
R1

```
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
```

Permita Pings (ICMP)

En esta figura, se muestra que se permite ICMP con origen en la Red A y destino en la Red B, y que se niegan los pings con origen en la Red B y destino en la Red A.



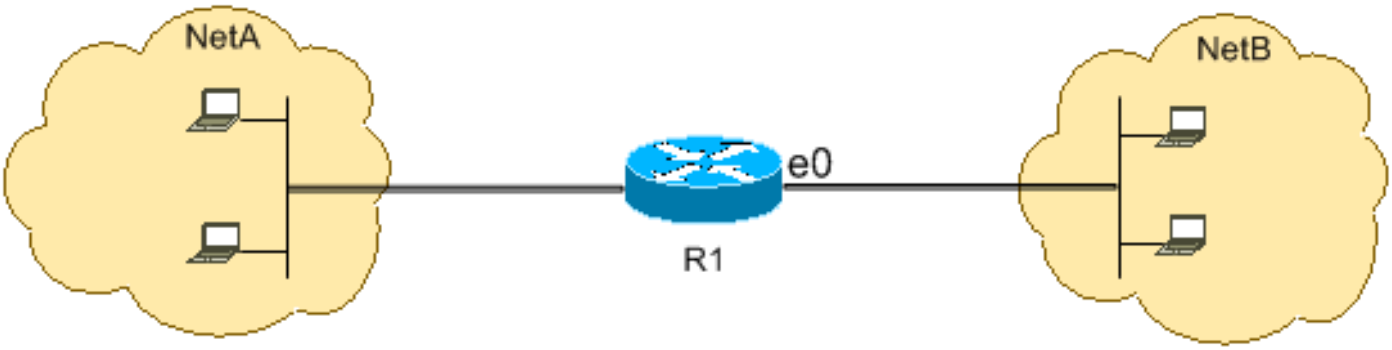
Esta configuración permite que solo los paquetes de respuesta de eco (respuesta de ping) lleguen en la interfaz Ethernet 0 desde la Red B hacia la Red A. Sin embargo, la configuración bloquea todos los paquetes ICMP de solicitud de eco cuando los pings se originan en la Red B y se destinan a la Red A. Por lo tanto, los hosts en la Red A pueden hacer ping con los hosts en la Red B, pero los hosts en la Red B no pueden hacer ping con los hosts en la Red A.

R1

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

Permita HTTP, Telnet, Mail, POP3, FTP

En esta figura, se muestra que se permite solo el tráfico FTP, POP3, Simple Mail Transfer Protocol (SMTP), Telnet y HTTP, y que se niega el resto del tráfico con origen en la Red B y destino en la Red A.



Esta configuración permite el tráfico TCP con valores de puerto de destino que coincidan con

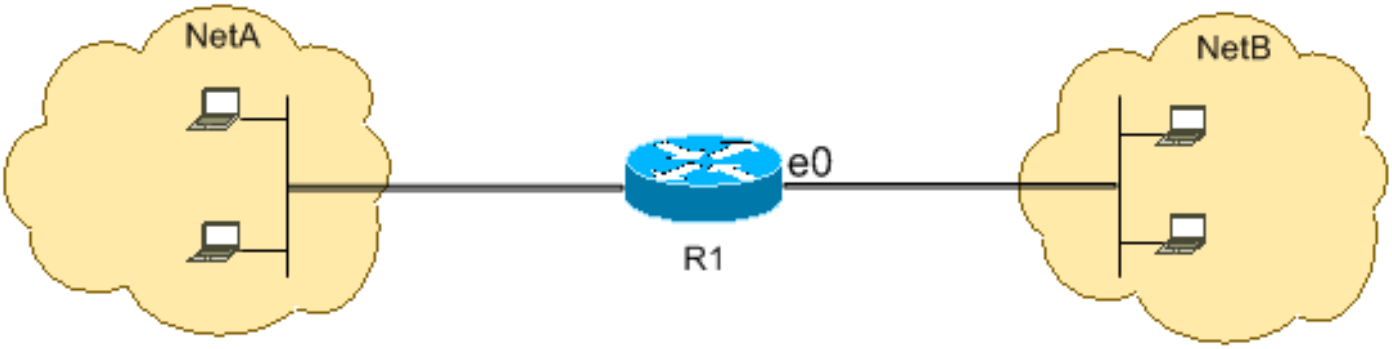
datos FTP (puerto 20), FTP (puerto 21), POP3 (puerto 110), SMTP (puerto 25), Telnet (puerto 23) y WWW (puerto 80). Tenga en cuenta que una cláusula total de negación implícita al final de una ACL niega el resto del tráfico, que no coincide con las cláusulas de permiso.

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
```

Cómo Permitir DNS

En esta figura, se muestra que se permite solo el tráfico de sistema de nombres de dominio (DNS) y que se niega el resto del tráfico con origen en la Red B y destino en la Red A.



Esta configuración permite el tráfico TCP con el valor de puerto de destino 53. La cláusula total de negación implícita al final de una ACL niega cualquier otro tráfico que no coincida con las cláusulas de permiso.

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
```

Permita Actualizaciones de Ruteo

Cuando aplica una ACL entrante a una interfaz, asegúrese de que las actualizaciones de ruteo no se filtren. Utilice la ACL relevante de esta lista para permitir los paquetes de protocolo de ruteo:

Ingrese este comando para permitir el Routing Information Protocol (RIP):

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

Ingrese este comando para permitir el Interior Gateway Routing Protocol (IGRP):

```
access-list 102 permit igrp any any
```
Ingrese este comando para permitir el (EIGRP) del IGRP mejorado:

```
access-list 102 permit eigrp any any
```
Ingrese este comando para permitir el Open Shortest Path First (OSPF):

```
access-list 102 permit ospf any any
```
Ingrese este comando para permitir el Border Gateway Protocol (BGP):

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

Cómo Ejecutar un Debug del Tráfico Basado en ACL

El uso de los **comandos debug** requiere la asignación de recursos del sistema (como memoria y potencia de procesamiento) y, en situaciones extremas, puede hacer que un sistema muy cargado se atasque. Utilice los **comandos debug** con cuidado. Utilice una ACL para definir selectivamente el tráfico que se debe examinar para reducir el impacto del comando de debug. Dicha configuración no filtra ningún paquete.

Esta configuración activa el **comando debug ip packet** solo para los paquetes entre los hosts 10.1.1.1 y 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
```
Consulte Información Importante sobre Comandos de Debug para obtener más información sobre el impacto de los comandos de debug.

Consulte la sección Uso del Comando de Debug de **Comprensión de los Comandos de Traceroute y Ping** para obtener más información sobre el uso de las ACL con los **comandos debug**.

Filtrado de Direcciones MAC

Usted puede filtrar tramas con una dirección de origen o de destino de estación de capa MAC determinada. Se puede configurar cualquier número de direcciones en el sistema sin una multa de rendimiento. Para filtrar por la dirección de capa MAC, utilice este comando en el modo de configuración global:

```
Router#config terminal
       bridge irb
       bridge 1 protocol ieee
       bridge 1 route ip
```
Aplique el protocolo de bridge a una interfaz que deba filtrar el tráfico junto con la lista de acceso creada:

```
Router#int fa0/0
       no ip address
       bridge-group 1 {input-address-list 700 | output-address-list 700}
       exit
```
Cree una interfaz virtual puenteada y aplique la dirección IP que se asigna a la interfaz de 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
```

Con esta configuración, el router solo permite las direcciones MAC configuradas en la lista de acceso 700. Con la lista de acceso, niegue las direcciones MAC que no pueden tener acceso y después permita el resto.

> Nota: Cree cada línea de lista de acceso para cada dirección MAC.

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- Configuración de Listas de Acceso IP
- Páginas de Soporte de Listas de Acceso
- Página de Soporte de IP Routing
- Página de Soporte de IP Routed Protocols
- Soporte Técnico y Documentación - Cisco Systems