Configuración de ACL IP utilizadas frecuentemente

Contenidos

Introducción

En este documento se proporcionan ejemplos de configuraciones para listas de control de acceso (ACL) IP que se usan con frecuencia y que filtran paquetes IP en función de:

- La dirección de origen
- La dirección de destino
- El tipo de paquete
- Cualquier combinación de los elementos anteriores

Para filtrar el tráfico de red, las ACL controlan si los paquetes enrutados se reenvían o bloquean en la interfaz del router. El router examina cada paquete para determinar si debe reenviarlo o descartarlo según los criterios que se especifiquen dentro de la ACL. Los criterios de la ACL son:

- La dirección de origen del tráfico
- La dirección de destino del tráfico
- El protocolo de capa superior

Siga los pasos siguientes para generar una ACL como muestran los ejemplos de este documento:

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

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

La primera coincidencia determina si el software Cisco IOS® acepta o rechaza el paquete. Dado que el software Cisco IOS deja de probar las condiciones tras la primera coincidencia, el orden de las condiciones es esencial. Si no coincide ninguna condición, el router rechaza el paquete debido a una cláusula de negación total implícita.

A continuación se proporcionan algunos ejemplos de las ACL IP que se pueden configurar en el software Cisco IOS:

- ACL estándar
- ACL ampliadas
- ACL dinámicas (Lock-and-Key)
- 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
- ACL turbo
- ACL basadas en tiempo distribuidas

Este documento analiza algunas ACL estándar y ampliadas comúnmente utilizadas. Consulte Configuración de listas de acceso IP para obtener más información sobre los diferentes tipos de ACL compatibles con el software Cisco IOS y sobre cómo configurar y editar las ACL.

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

Las ACL estándar (sólo para clientes registrados) controlan el tráfico por medio de la comparación de la dirección de origen de los paquetes IP con las direcciones configuradas en la ACL.

Las ACL ampliadas (sólo para clientes registrados) controlan el tráfico mediante la comparación de las direcciones de origen y destino de los paquetes IP con las direcciones configuradas en la ACL. También puede hacer que las ACL ampliadas sean más detalladas y configurarlas para que filtren el tráfico según 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 la sintaxis de los comandos de las ACL ampliadas 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]
```

Protocolo de mensajes de control de Internet (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 control de 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 usuario (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]
```

Consulte IP Services Commands (Comandos de servicios IP) para obtener información sobre las referencias de comandos de una ACL.

Requisitos previos

Requisitos

Antes de implementar esta configuración, asegúrese de que cumple con el requisito siguiente:

- Comprensión básica del direccionamiento IP

Consulte IP Addressing and Subnetting for New Users (Direccionamiento IP y conexión en subredes para usuarios nuevos) si desea obtener información adicional.

Componentes utilizados

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

Convenciones

Consulte Cisco Technical Tips Conventions (Convenciones sobre consejos técnicos de Cisco) para obtener más información sobre las convenciones del documento.

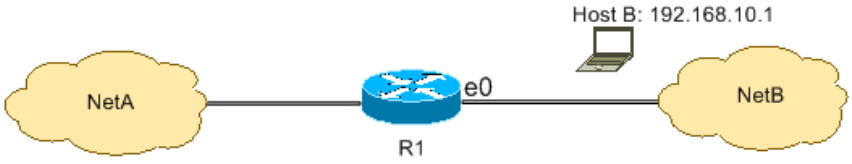
Ejemplos de configuración

En los siguientes ejemplos de configuración se usan las ACL IP más comunes.

Nota: emplee la herramienta de búsqueda de comandos (sólo para clientes registrados) para buscar más información sobre los comandos utilizados en este documento.

Permiso de acceso a la red para un host seleccionado

Esta figura muestra un host seleccionado al que se le ha otorgado permiso para acceder a la red. Se permite todo el tráfico procedente del host B y destinado a la red A, mientras que se rechaza todo el tráfico procedente de la red B y destinado a la red A.



El resultado de esta tabla de R1 muestra cómo otorga la red el acceso al host. Este resultado muestra lo siguiente:

- La configuración sólo permite 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 de la red B tiene acceso a la red A.

- No se ha configurado ninguna sentencia de negación en la ACL.

De manera predeterminada, hay una cláusula de negación total implícita al final de cada ACL. Se rechaza todo lo que no se permite de forma explícita.

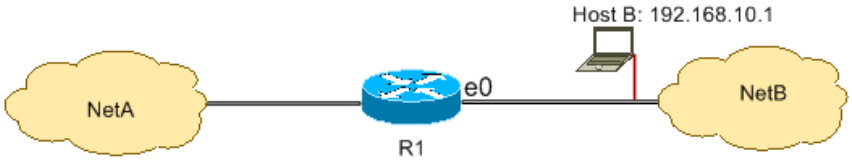
R1
hostname R1 ! interface ethernet0 ip access-group 1 in ! access-list 1 permit host 192.168.10.1

Nota: la ACL filtra paquetes IP desde la red B a la red A, a excepción de los paquetes procedentes de la red B. Se permiten los paquetes destinados al host B cuyo origen sea la red A.

Nota: el comando **access-list 1 permit 192.168.10.1 0.0.0.0** de la ACL es otra forma de configurar la misma regla.

Negación del acceso a la red para un host seleccionado

Esta figura muestra que se rechaza el tráfico procedente del host B y destinado a la red A, mientras que sí se permite que el resto del tráfico procedente de la red B tenga acceso a la red A.



Esta configuración rechaza todos los paquetes del host 192.168.10.1/32 a través de Ethernet 0 en R1 y permite todo lo demás. Debe usar el comando **access list 1 permit any** para permitir de forma explícita todo lo demás, ya que hay una cláusula de negación total implícita en cada ACL.

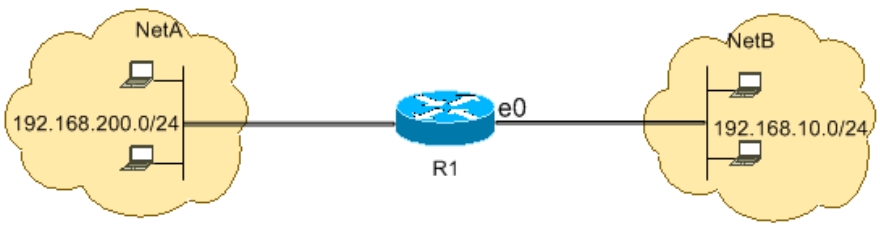
R1
hostname R1 ! interface ethernet0 ip access-group 1 in ! access-list 1 deny host 192.168.10.1 access-list 1 permit any

Nota: el orden de las sentencias 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 del paquete. Por lo tanto, la ACL no puede bloquear el acceso a la red A del host 192.168.10.1/32.

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

Permiso de acceso a un intervalo de direcciones IP contiguas

Esta figura muestra que todos los hosts en la red B con la dirección de red 192.168.10.0/24 pueden tener acceso a la red 192.168.200.0/24 en la red A.



Esta configuración permite que los paquetes IP cuyo encabezado IP tenga 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 obtengan acceso a la red A. Una cláusula de negación total implícita al final de la ACL rechaza cualquier otro tráfico que pueda haber en Ethernet 0 de entrada en R1.

R1

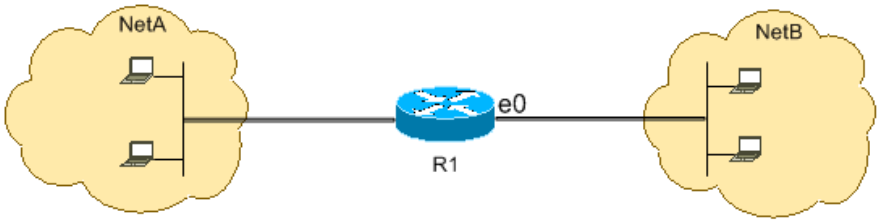
```
hostname R1
!
interface ethernet0
ip access-group 101 in
!
access-list 101 permit ip 192.168.10.0  0.0.0.255
 192.168.200.0  0.0.0.255
```

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**, "0.0.0.255" es la máscara inversa de la red 192.168.10.0 con la máscara 255.255.255.0. Las ACL usan la máscara inversa para saber cuántos bits deben coincidir en la dirección de la red. En la tabla, la ACL permite todos los hosts con direcciones de origen en la red 192.168.10.0/24 y 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 o sobre cómo calcular la máscara inversa necesaria para las ACL.

Negación del tráfico Telnet (TCP, puerto 23)

Con el objetivo de cumplir con los requisitos de seguridad más estrictos, quizá tenga que inhabilitar el acceso Telnet a su red privada desde la red pública. Esta figura muestra cómo se deniega el tráfico Telnet de la red B (pública) destinado a la red A (privada), lo que permite a la red A iniciar y establecer una sesión de Telnet con la red B mientras se permite cualquier otro tráfico IP.



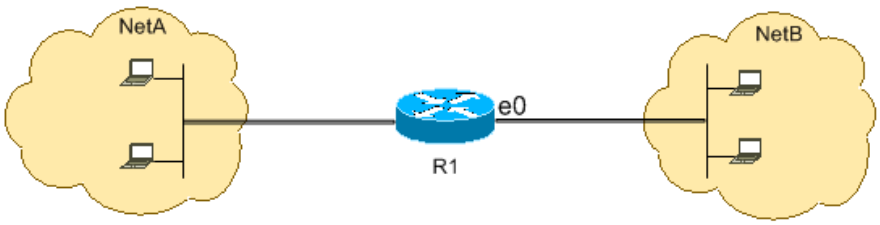
Telnet usa TCP, puerto 23. Esta configuración muestra que todo el tráfico TCP destinado a la red A para el puerto 23 está bloqueado y que se permite todo el resto del tráfico IP.

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
```

Permiso de inicio de sesión TCP sólo para redes internas

Esta figura muestra que se permite el tráfico TCP procedente de la red A y destinado a la red B, mientras que se rechaza el tráfico TCP procedente de la red B y destinado a la red A.



El objetivo de la ACL en este ejemplo es el siguiente:

- Permitir a los hosts en la red A iniciar y establecer una sesión TCP con los hosts en la red B.
- No permitir a los hosts en la red B iniciar y establecer una sesión TCP destinada a los hosts de la red A.

Esta configuración permite que un datagrama se transfiera por la interfaz Ethernet 0 de entrada a R1 cuando el datagrama tenga:

- definidos los bits de reconocimiento (ACK) o restablecimiento (RST) (indicando una sesión TCP establecida)
- Un valor de puerto de destino superior a 1023

R1

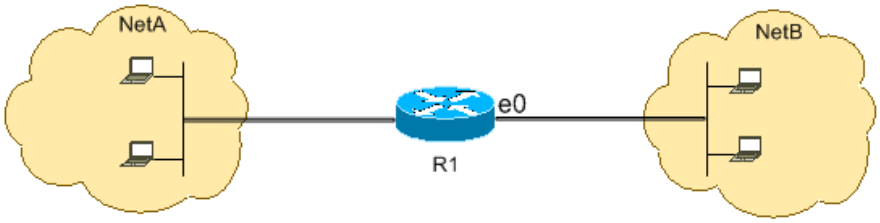
```
hostname R1
!
interface ethernet0
ip access-group 102 in
!
access-list 102 permit tcp any any gt 1023 established
```

Dado que la mayoría de puertos conocidos para los servicios IP usan valores menores que 1023, ACL 102 deniega cualquier datagrama que tenga un puerto de destino inferior a 1023, o que no tenga definido ningún bit ACK/RST. Por lo tanto, cuando un host de la red B inicia una conexión TCP mediante el envío del primer paquete TCP (sin el bit sincronización/inicio de paquete (SYN/RST) definido) para un número de puerto inferior a 1023, se rechaza la conexión y se produce un error en la sesión TCP. Las sesiones TCP iniciadas desde la red A y destinadas a la red B se permiten porque tienen definido el bit ACK/RST para la devolución de paquetes y usan valores de puerto mayores que 1023.

Consulte RFC 1700 para obtener una lista completa de los puertos.

Negación del tráfico FTP (TCP, puerto 21)

Esta figura muestra que se ha denegado el tráfico FTP (TCP, puerto 21) y el tráfico de datos FTP (puerto 20) procedente de la red B y destinado a la red A, mientras que se permite otro tráfico IP.



FTP usa el puerto 21 y el puerto 20. Se rechaza el tráfico TCP destinado a estos dos puertos y todo lo demás se permite explícitamente.

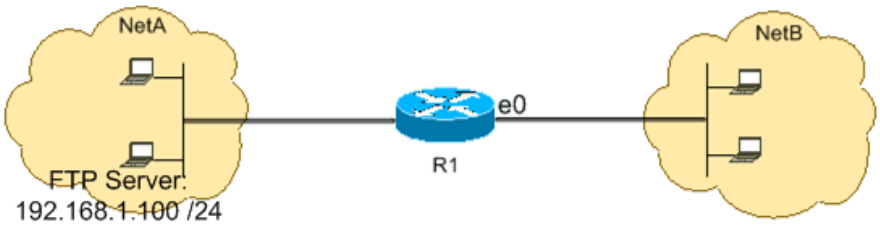
R1

```
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
```

Permiso de tráfico FTP (FTP activo)

FTP puede operar en dos modos, el activo y el pasivo. Consulte FTP Operation (Funcionamiento de FTP) para conocer el funcionamiento de FTP activo y pasivo.

Cuando FTP funciona en modo activo, el servidor FTP emplea el puerto 21 para el control y el 20 para los datos. El servidor FTP (192.168.1.100) se encuentra en la red A. Esta figura muestra que se permite el tráfico FTP (TCP, puerto 21) y el tráfico de datos FTP (puerto 20) procedente de la red B y destinado al servidor FTP (192.168.1.100), mientras que se rechaza cualquier otro tráfico IP.



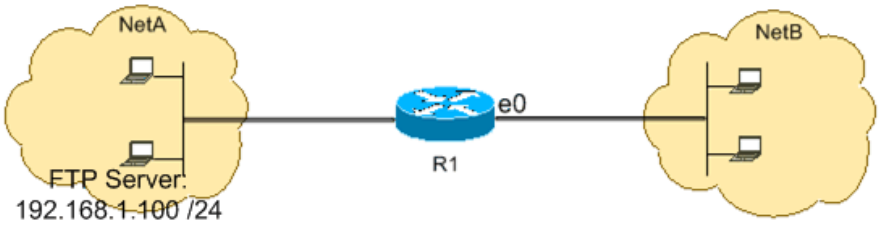
R1

```
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
```

Permiso de tráfico FTP (FTP pasivo)

FTP puede operar en dos modos, el activo y el pasivo. Consulte FTP Operation (Funcionamiento de FTP) para conocer el funcionamiento de FTP activo y pasivo.

Cuando FTP funciona en modo pasivo, el servidor FTP emplea el puerto 21 para el control y los puertos dinámicos mayores o iguales a 1024 para los datos. El servidor FTP (192.168.1.100) se encuentra en la red A. Esta figura muestra que se permite el tráfico FTP (TCP, puerto 21) y el tráfico de datos FTP (puertos mayores o iguales a 1024) procedente de la red B y destinado al servidor FTP (192.168.1.100), mientras que se rechaza cualquier otro tráfico IP.

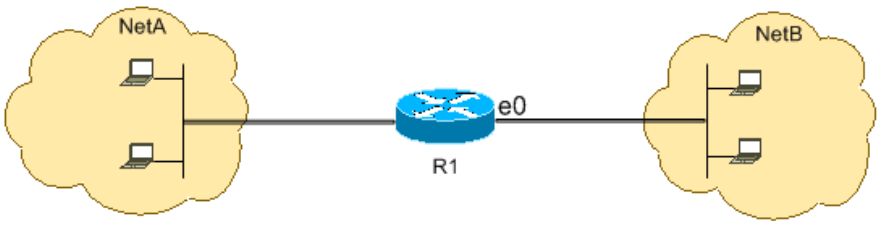


R1

```
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
```

Permiso de pings (ICMP)

Esta figura muestra que se permite ICMP procedente de la red A y destinado a la red B, mientras que se rechazan los pings procedentes de la red B y destinados a la red A.



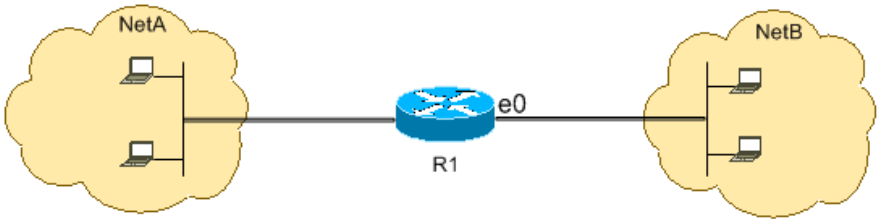
Esta configuración permite solamente la transmisión de paquetes de respuesta de eco (respuesta ping) en una interfaz Ethernet 0 desde la red B hacia la red A. Sin embargo, bloquea todos los paquetes ICMP de petición de eco cuando los pings proceden de la red B y están destinados a la red A. Por lo tanto, los hosts en la red A pueden hacer ping en los hosts de la red B, pero los hosts de la red B no pueden hacer lo mismo con los de la red A.

R1

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

Permiso de HTTP, Telnet, Mail, POP3, FTP

Esta figura muestra que sólo está permitido el tráfico HTTP, Telnet, Protocolo simple de transferencia de correo (SMTP), POP3 y FTP, mientras que se rechaza el resto del tráfico procedente de la red B y destinado a la red A.



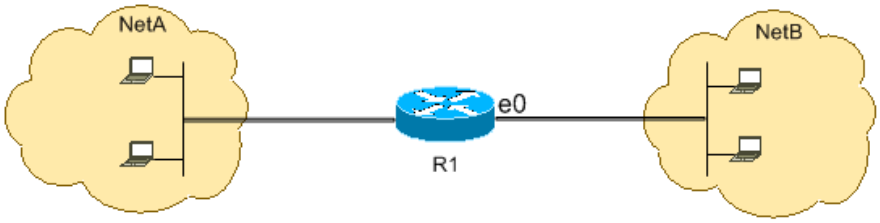
Esta configuración permite el tráfico TCP con valores de puerto de destino que coincidan con WWW (puerto 80), Telnet (puerto 23), SMTP (puerto 25), POP3 (puerto 110), FTP (puerto 21) o datos FTP (puerto 20). Tenga en cuenta que la cláusula de negación total implícita al final de una ACL rechaza cualquier otro tráfico que no coincida 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
```

Permiso de DNS

Esta figura muestra que sólo está permitido el tráfico del sistema de nombres de dominio (DNS), mientras que se rechaza el resto del tráfico procedente de la red B y destinado a la red A.



Esta configuración permite el tráfico TCP con el valor de puerto de destino 53. La cláusula de negación total implícita al final de una ACL deniega 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
```

Permiso de actualizaciones de enrutamiento

Cuando aplique una ACL de entrada en una interfaz, asegúrese de que no se filtren las actualizaciones de enrutamiento. Use la ACL correspondiente de esta lista para permitir paquetes de protocolo de enrutamiento:

Ejecute este comando para permitir el Protocolo de información de enrutamiento (RIP):

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

Ejecute este comando para permitir el Protocolo de enrutamiento de gateway interior (IGRP):

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

Ejecute este comando para permitir IGRP mejorado (EIGRP):

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

Ejecute este comando para permitir el protocolo Abrir trayecto más corto primero (OSPF):

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

Ejecute este comando para permitir el Protocolo de gateway de frontera (BGP):

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

Depuración de tráfico basada en ACL

El uso de los comandos **debug** requiere la asignación de recursos del sistema como memoria y capacidad de procesamiento y, en situaciones extremas, podría causar que se detuviera un sistema cargado en exceso. Use los comandos **debug** con precaución. Emplee una ACL para definir de forma selectiva el tráfico que debe examinarse para reducir el impacto del comando **debug**. Una configuración de este tipo no filtra ningún paquete.

Esta configuración activa el comando **debug ip packet** solamente para los paquetes que se encuentran 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 Important Information on Debug Commands (Información importante sobre los comandos de depuración) para obtener información adicional sobre el impacto de estos comandos.

Consulte la sección Use the Debug Command (Uso del comando Debug) de Understanding the Ping and Traceroute Commands (Funcionamiento de los comandos Ping y Traceroute) para obtener información adicional sobre el uso de las ACL con comandos **debug**.

Verificación

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

Resolución de problemas

Actualmente, no hay información específica disponible sobre solución de problemas para esta configuración.

Fecha de Generación del PDF: 23 Junio 2008

http://www.cisco.com/cisco/web/support/LA/7/76/76154_ACLsamples.html