Capítulo 7

LISTAS DE ACCESO IP EXTENDIDAS

Comparadas con las listas de control de acceso (ACL) estándar, las listas de control de acceso extendidas son más flexibles y tienen un mayor potencial de aplicación en la configuración de los equipos de una red. En general, las listas de control de acceso revisten mucha importancia debido a que la implementación de una red medianamente compleja hace necesario su uso. Cisco tiene diferentes clases de ACL, las más comunes son las listas de control de acceso numeradas, un subconjunto perteneciente a ellas son las listas de control de acceso extendidas, las cuales dan soporte al protocolo TCP/IP; en este capítulo se aborda el estudio y manejo de estas últimas.

Es importante indicar que existen otros tipos de listas de acceso, también de mucha importancia: listas de acceso con nombres, listas de acceso reflexivas, listas de acceso de tiempo, listas de acceso basadas en el contexto (Context-Based Access Control) y listas de acceso para limitar velocidad. Algunas de ellas se abordan en la sección de "Problemas".

Objetivo

Al finalizar este capítulo, el estudiante estará en capacidad de:

- Diferenciar las listas de control de acceso estándar de las listas de control de acceso extendidas.
- Configurar filtros de tráfico utilizando la lista de acceso IP extendidas.

Procedimiento

Controlando el acceso IP

Las listas de control de acceso IP estándar permiten realizar una configuración rápida, presentando un bajo sobrecosto (overhead) en la función de limitar el tráfico con base en la dirección IP origen. Las listas de acceso extendidas proporcionan un mayor grado de control, permitiendo crear filtros basados en: la dirección IP origen y destino, los tipos de protocolos (tal como IP, TCP, UDP, ICMP, etc.) y los números de puerto usados por las aplicaciones. Estas características hacen posible limitar el tráfico con base en el uso que se le de a la red.

Para que un datagrama IP (paquete) cumpla las diferentes condiciones configuradas en una línea (o expresión) de una lista de acceso, y mediante dicha línea se pueda permitir o negar el tránsito del paquete, es necesario que cada condición que se coteje en dicha línea coincida (haga match) con el respectivo campo del paquete. Tan pronto como el paquete no cumpla una condición de la línea, se pasa a comparar las condiciones de la próxima línea de la lista de acceso frente a los respectivos campos del paquete.

La lista de acceso extendida tiene la capacidad de revisar: la dirección IP origen, la dirección IP destino y diferentes opciones que dependan del protocolo seleccionado.

Comandos para la configuración de listas de acceso IP extendidas

Tareas a realizar:

Configurar parámetros de entrada en la lista

Una de las mayores diferencias entre la lista de acceso IP estándar y la lista de acceso IP extendida es que en la última se puede especificar tanto la dirección IP origen como la dirección IP destino. A diferencia de la lista de acceso IP estándar, en la de acceso IP extendida, el "*comodín*" (wildcard) no es opcional. A continuación se presenta la sintaxis y se describen los parámetros de este comando en mayor detalle.

R1(config)#
access-list access-list-number {**permit | deny**} {protocol | protocol keyword}
{source address with wildcard mask | any} ["operator" "source port number"]
{destination address with wildcard mask | any} ["operator" "destination port number"]
[**established**] [**log**]

Descripción de los parámetros del comando *access-list*:

Accest-list-number: se escoge un número en el rango de 100 hasta 199 para identificar la lista de acceso IP extendida (que contiene una o más entradas).

Pemit/deny: especifica la acción que se ejecutará sobre el paquete (permitir o bloquear su paso), en caso que éste cumpla las condiciones definidas en la línea.

Protocol | protocol keyword: define el protocolo que se desea comparar en el paquete. Estos protocolos incluyen a: ip, icmp, tcp, udp, igrp, eigrp, igmp, ipinip, nos, ospf, gre.

Source address* y *destination address: identifican las direcciones IP origen e IP destino del paquete, respectivamente.

Source wildcard mask* y *destination wildcard mask: identifican cuáles bits del campo de dirección deben tenerse en cuenta. Los bits que tengan 0 en cualquier posición deben examinarse estrictamente y los bits que tengan 1 en cualquier posición no deben examinarse (no importan).

Any (opcional): Se utiliza como abreviación de "0.0.0.0 255.255.255.255" para los parámetros: "source address", "source wildcard mask", "destination address" y "destination wildcard mask".

Operator: Para los protocolos TCP y UDP. En la expresión se puede especificar el número del puerto o, algunas veces, el nombre del mismo. Cuando se requiere buscar una coincidencia sobre un puerto, es necesario utilizar un operador. El propósito del operador es proporcionar alguna flexibilidad sobre el(los) número(s) de puerto(s) que se desea(n) hacer coincidir. Los operadores válidos son:

- lt less than (menor que)
- gt greater than (mayor que)
- neq not equal to (no igual a)
- eq equal to (igual a)
- range range of port numbers (rango)

Port number* y *message type: La información referente al protocolo puede dividirse en dos áreas: números de puerto ("port Lumber" para los protocolos TCP y UDP) y tipos de mensajes ("message type" para otros protocolos, incluyendo a ICMP). Para los números de puerto de TCP y UDP, se puede usar el número de puerto reservado para la aplicación como, por ejemplo, el *21* para telnet, o se puede usar el nombre de la aplicación, como *ftp* para el puerto 21. ICMP no usa números de puerto, en su lugar, usa tipos de mensajes (esto reemplaza los parámetros *operator* y *port number* usados en TCP y UDP). Si en una expresión de la lista de acceso IP extendida se

omite el *port number* (para TCP o UDP), o el *message type* (para ICMP), significa que se acepta cualquier puerto o tipo de mensaje del paquete.

Established: verifica si el datagrama IP forma parte de una conexión TCP previamente establecida, es decir, si el segmento TCP tiene el bit ACK o el bit RST en uno. Esta opción tiene aplicación en situaciones en las que desde una red privada se establecen conexiones hacia Internet y se quiere permitir solamente el tráfico de respuesta a dichas conexiones.

Es importante recordar que cada lista de control de acceso (ACL) tiene una línea implícita tipo "*deny all*" al final de la lista. Como consecuencia, si no se presenta una coincidencia (match) con las líneas explícitamente definidas, el paquete será bloqueado.

A modo de ejemplo, a continuación se explican las listas de acceso IP extendida número 100 y 101.

Lista de acceso número 100

```
access-list 100 permit tcp any 172.16.0.0 0.0.255.255 established log
access-list 100 permit udp any host 172.16.1.1 eq dns log
access-list 100 permit tcp 172.17.0.0 0.0.255.255 host 172.16.1.2 eq telnet log
access-list 100 permit icmp any 172.16.0.0 0.0.255.255 echo-reply log
access-list 100 deny ip any any log

Router(config)# interface ethernet 0
Router(config-if)# ip access-group 100 in
```

En la primera línea de la lista de acceso IP extendida se establece que cualquier sesión TCP que venga desde cualquier dirección IP con destino a la red 172.16.0.0/16 será permitida, siempre y cuando el encabezado TCP tenga el bit ACK o el bit RST puesto en uno; adicionalmente, cualquier coincidencia con esta sentencia será impresa en la consola del encaminador. Otra observación de este comando es que no tiene especificado los números de puerto, esto significa que todos los puertos serán incluidos y que cualquier valor en el número del puerto será aceptado como coincidencia.

La segunda línea de la lista de acceso IP extendida establece que permitirá una operación de búsqueda DNS (DNS lookup) proveniente de cualquier dirección IP con destino al servidor DNS con dirección IP 172.16.1.1.

La tercera línea permite tener conexiones telnet provenientes de la red 172.17.0.0/16, siempre y cuando la dirección destino sea 172.16.1.2; este comando restringe a que se haga telnet solamente a la máquina 172.16.1.2.

La cuarta línea permite respuestas de un mensaje ping, siempre y cuando la dirección IP destino pertenezca a la red 172.16.0.0/16. Esta sentencia no permite solicitudes de ping (echo-request).

La quinta línea no es necesaria debido a la negación implícita (implicit deny) que hay al final de cada lista de acceso. No obstante, los paquetes que no coincidan con las primeras cuatro líneas serán registrados en la consola mediante esta quinta línea (debido al parámetro "log").

Lista de acceso número 101

```
access-list 101 permit tcp host 199.199.199.1 200.200.200.1 eq dns
access-list 101 permit udp any host 200.200.200.1 eq dns
access-list 101 permit tcp any host 200.200.200.2 eq www
access-list 101 permit icmp any 200.200.200.0 0.0.0.255
access-list 101 permit tcp any host 200.200.200.3 eq smtp
access-list 101 permit udp any any eq rip

Router(config)# interface ethernet 0
Router(config-if)# ip access-group 101 in
```

1. La primera línea de la lista de acceso número 101 establece que se permite la transferencia de zona DNS desde el servidor DNS 199.199.199.1 hacia el equipo 200.200.200.1.
2. La segunda línea permite una solicitud de búsqueda DNS desde cualquier dirección IP hacia el servidor DNS con dirección IP 200.200.200.1.
3. La tercera sentencia de la lista 101 permite cualquier conexión web, siempre y cuando dicho tráfico tenga como destino la dirección IP 200.200.200.2; restringe que el tráfico web tenga como destino a la máquina 200.200.200.2.
4. La cuarta sentencia permite cualquier tipo de mensaje ICMP, siempre y cuando tenga como destino un equipo cuya dirección IP se encuentre en la red 200.200.200.0/24.
5. La quinta sentencia permite el tráfico correspondiente al correo electrónico, siempre y cuando éste tenga como destino al servidor de correo cuya dirección es 200.200.200.3.
6. La sexta sentencia permite el tráfico del protocolo de enrutamiento RIP IP (desde cualquier encaminador vecino RIP).

Activar la lista sobre una interfaz:

R1(config-if)# *ip access-group* access-list-number {in | out}

El comando *ip access-group* asocia una lista existente a una interfaz. Sólo se permite una lista de acceso por protocolo para cada interfaz.

Descripción de los parámetros del comando *ip access-group*:

Access-list-number: indica el número de la lista a ser asociado a la interfaz.

In/out: selecciona si la lista de acceso será aplicada a los paquetes que entran o salen de la interfaz; cuando no se especifica este parámetro, por defecto es out.

Protocolos que se pueden configurar con la lista de acceso IP extendida

Para la pila de protocolos TCP/IP, los diferentes protocolos que pueden servir como parámetros del filtro son:

R1(config)# *access-list* 101 permit ?

```
<0-255>      An IP protocol number
dvmrp        DVMRP IP over IP encapsulation
gre          Cisco's GRE tunneling
icmp         Internet Control Message Protocol
igmp         Internet Gateway Message Protocol
igrp         Cisco's IGRP routing protocol
ip Internet  Protocol
nos          KA9Q NOS compatible IP over IP tunneling
tcp          Transmission Control Protocol
udp          User Datagram Protocol
```

Por ejemplo, si se escoge ICMP, las opciones son las siguientes:

R1(config)# *access-list* 101 permit icmp any any ?

<0-255>	ICMP message type
administratively-prohibited	Administratively prohibited
alternate-address	Alternate address
conversion-error	Datagram conversion
dod-host-prohibited	Host prohibited
dod-net-prohibited	Net prohibited
echo	Echo (ping)
echo-reply	Echo reply
general-parameter-problem	Parameter problem
host-isolated	Host isolated
host-precedence-unreachab	Host unreachable for precedence
host-redirect	Host redirect
host-tos-redirect	Host redirect for TOS
host-tos-unreachable	Host unreachable for TOS
host-unknown	Host unknown
host-unreachable	Host unreachable
information-reply	Information replies
information-request	Information requests
log	Log matches against this entry
mask-reply	Mask replies
mask-request	Mask requests
mobile-redirect	Mobile host redirect
net-redirect	Network redirect
net-tos-redirect	Net redirect for TOS
net-tos-unreachable	Network unreachable for TOS
net-unreachable	Net unreachable
network-unknown	Network unknown
no-room-for-option	Parameter required but no room
option-missing	Parameter required but not present

En otro caso, si se escoge TCP, entonces las opciones son las siguientes:

R1(config)# *access-list* 101 permit tcp any any eq ?

<0-65535>	Port number
bgp	Border Gateway Protocol (179)
chargen	Character generator (19)
cmd	Remote commands (rcmd, 514)
daytime	Daytime (13)
discard	Discard (9)
domain	Domain Name Service (53)
echo	Echo (7)
exec	Exec (rsh, 512)
finger	Finger (79)
ftp	File Transfer Protocol (21)
ftp-data	FTP data connections (used infrequently, 20)
gopher	Gopher (70)
hostname	NIC hostname server (101)
irc	Internet Relay Chat (194)
klogin	Kerberos login (543)
kshell	Kerberos shell (544)
login	Login (rlogin, 513)
lpd	Printer service (515)
nntp	Network News Transport Protocol (119)
pop2	Post Office Protocol v2 (109)
pop3	Post Office Protocol v3 (110)
smtp	Simple Mail Transport Protocol (25)
sunrpc	Sun Remote Procedure Call (111)
syslog	Syslog (514)
tacacs	TAC Access Control System (49)
talk	Talk (517)
telnet	Telnet (23)
time	Time (37)
uucp	Unix-to-Unix Copy Program (540)
whois	Nicname (43)
www	World Wide Web (HTTP, 80)

Finalmente, cuando se escoge UDP, las opciones son las siguientes:

R1(config)# *access-list* 102 permit udp any any eq ?

<0-65535>	Port number
biff	Biff (mail notification, comsat, 512)
bootpc	Bootstrap Protocol (BOOTP) client (68)
bootps	Bootstrap Protocol (BOOTP) server (69)
discard	Discard (9)
dnsix	DNSIX security protocol auditing (195)
domain	Domain Name Service (DNS, 53)
echo	Echo (7)
mobile-ip	Mobile IP registration (434)
nameserver	IEN116 name service (obsolete, 42)
netbios-dgm	NetBios datagram service (138)
netbios-ns	NetBios name service (137)
ntp	Network Time Protocol (123)
rip	Routing Information Protocol (520)
snmp	Simple Network Management Protocol (161)
snmptrap	SNMP Traps (162)
sunrpc	Sun Remote Procedure Call (111)
syslog	System Logger (514)
tacacs	TAC Access Control System (49)
tftp	Trivial File Transfer Protocol (69)
time	Time (37)
who	Who service (rwho, 513)
xdmcp	X Display Manager Control Protocol (177)

Ejemplo 1. Firewall que permite acceso a Internet y tráfico de correo electrónico

En este ejemplo, la red 128.88.3.0/24 (clase B) de la Figura 7.1 es una red desprotegida que no tiene restricción en comunicarse con Internet. Para proteger la red a la izquierda de Router1 (red 172.16.0.0) se crea un filtro en la interfaz Ethernet 1 del Router1, de tal manera que los equipos de la red protegida puedan iniciar cualquier tipo de sesión hacia la red desprotegida y hacia Internet, pero impidiendo que desde la parte derecha de Router1 se pueda iniciar cualquier tipo de sesión hacia la red protegida (intranet), con excepción del equipo 128.88.3.2, el cual puede iniciar una sesión de correo electrónico hacia la red protegida.

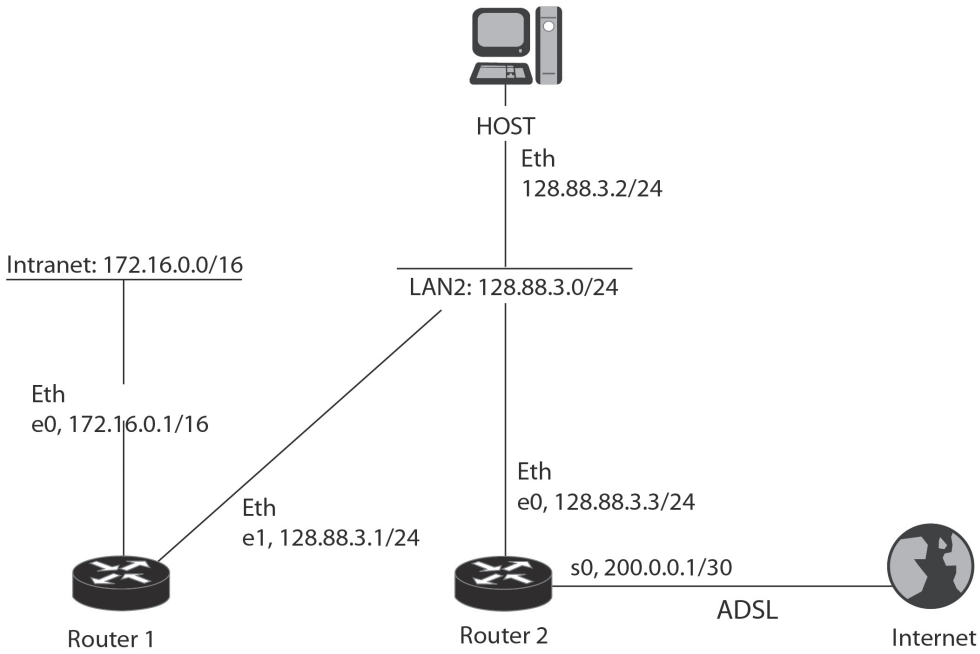

Figura 7.1 El Router1 permite iniciar cualquier tipo de sesión desde la intranet, pero solamente permite tráfico de correo electrónico desde el equipo 128.88.3.2/24 (HOST) hacia la intranet

Router1(config)# *access-list* 103 permit tcp any 172.16.0.0 0.0.255.255 established
(config)# *access-list* 103 permit tcp host 128.88.3.2 172.16.0.0 0.0.255.255 eq smtp

(config)# *(access-list* 103 deny 0.0.0.0 255.255.255.255) *o access-list* 103 deny any
(niega todo implícitamente, creada por el sistema, no está visible en la lista)

Router1 (config)# *interface* ethernet 1
Router1 (config-if)# *ip access-group* 103 in

Ejemplo 2. Permitir acceso a Internet, correo, DNS y PING

En este ejemplo, el Router1 de la Figura 7.2 permite que desde cualquier equipo de la red 172.16.0.0/16 (clase B) se pueda iniciar una o más sesiones hacia Internet y que dichos equipos, en consecuencia, puedan recibir los datagramas IP correspondientes a sus respectivas sesiones. También se permite: el servicio de correo electrónico SMTP bajo TCP; el servicio DNS bajo los protocolos TCP y UDP, y el mensaje PING bajo el protocolo ICMP.

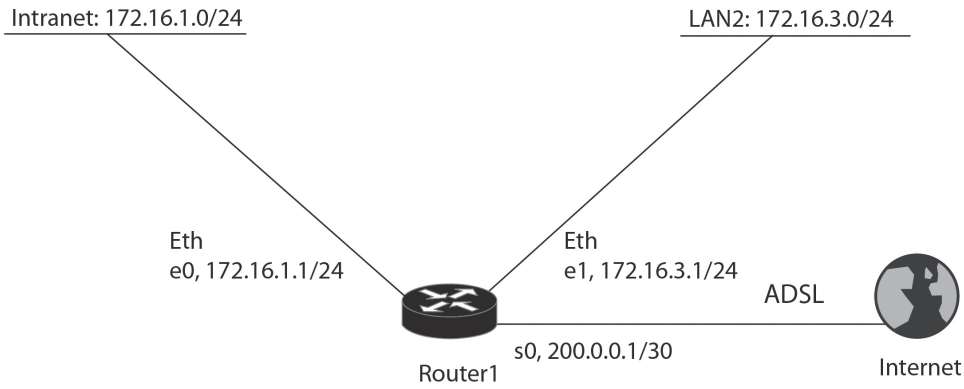

Figura 7.2 El Router1 permite iniciar cualquier tipo de sesión desde la red 172.16.0.0/16 hacia Internet, pero solamente permite tráfico SMTP, DNS y PING desde Internet

Router1(config)# *access-list* 104 permit tcp any 172.16.0.0 0.0.255.255 established
Router1(config)# *access-list* 104 permit tcp any 172.16.0.0 0.0.255.255 eq smtp
Router1(config)# *access-list* 104 permit tcp any 172.16.0.0 0.0.255.255 eq domain
Router1(config)# *access-list* 104 permit udp any 172.16.0.0 0.0.255.255 eq domain
Router1(config)# *access-list* 104 permit icmp any 172.16.0.0 0.0.255.255 echo
Router1(config)# *access-list* 104 permit icmp any 172.16.0.0 0.0.255.255 echo-reply

Router1(config)# (access-list 104 deny 0.0.0.0 255.255.255.255) o *access-list* 104 deny any (Niega todo implícitamente, no está visible en la lista)

Router1(config)# *interface* serial 0
Router1(config-if)# *ip access-group* 104 in

Informe

El programa Configmaker de Cisco tiene un tutorial de EasyIP y NAT que se recomienda leer con atención. Una vez hecho lo anterior, use el software Configmaker de Cisco para interconectar una intranet con la Internet global; utilizando un Firewall con EasyIP y NAT. Revise el archivo de configuración generado y haga los respectivos comentarios acerca de las líneas de configuración que determinan el funcionamiento de EasyIP y NAT.

Ejercicios de laboratorio

En este ejercicio se requiere configurar una lista de acceso numerada en el encaminador Router_A de la Figura 6.4 para obtener lo siguiente:

- Cualquier equipo estará en capacidad de realizar una solicitud DNS al servidor DNS de la red 192.168.1.0/24.
- Cualquier equipo de la red 192.168.3.0/24 estará en capacidad de acceder al servidor Web de la red 192.168.1.0/24.
- Solamente el PC_B podrá hacer FTP al servidor de FTP de la red 192.168.1.0/24.
- Cualquier equipo de la red 192.168.1.0/24, incluyendo al encaminador Router_A, será capaz de hacer ping a cualquier equipo del lado derecho de la red y recibir respuestas (echo-reply) de los equipos destinos.

Información complementaria

Ubicación de las listas de acceso

La ubicación del equipo de red seleccionado para aplicarle una lista de acceso específica, es crítica. Las listas de acceso IP estándar deberán colocarse tan cerca del destino como sea posible. En contraste, las listas de acceso IP extendidas deberán colocarse tan cerca del origen como sea posible.

Listas de acceso con nombres

La versión 11.2 o superior del IOS de Cisco soporta las nuevas "listas de acceso con nombres" (named access lists). La limitación de las "listas de acceso numeradas" tradicionales consiste en que el máximo número de listas que se pueden configurar es 100. La ventaja de usar "listas de acceso con nombres" es que éstas no tienen la anterior limitación. Además, proporcionan un poco más de control en el proceso de edición de la lista: se puede borrar una entrada de la lista; no obstante, no puede insertarse ni modificarse individualmente una entrada en la lista. Las "listas de acceso con nombres" son soportadas para los protocolos IP e IPX en la versión 11.2 del IOS.

Crear Listas de acceso con nombres

Para crear una lista de acceso con nombres, se usa el siguiente comando en modo de configuración global:

Router(config)# **ip | ipx** access-list **standard | extended** "name of the list"

El nombre de la lista ("name of list") debe ser único para cada lista de acceso configurada dentro del encaminador. Al ejecutarse el comando de la "lista de acceso con nombres", el sistema cambia el indicador (prompt) al modo de configuración de lista de acceso:

```
Router(config-std-acl)#
-o-
Router(config-ext-acl)#
```

En este modo se pueden digitar los comandos para construir las sentencias de la lista de acceso, tal como se hace con las "listas de acceso numeradas", pero omitiendo la palabra *access-list* y el número de la lista de acceso (ACL#).

Activando una Lista de acceso con nombres

Para aplicar una lista de acceso con nombres, se usa el siguiente comando en la interfaz sobre la que se desea aplicar:

```
Router(config)# interface "type" "port #"
Router(config-if)# ip access-group "name of list" in |out
```

La única diferencia entre activar una "lista de acceso nombrada" y "una lista de acceso numerada" sobre la interfaz es que con la primera se debe especificar el nombre que la identifica, mientras que con la segunda se especifica el número que la identifica.

A continuación se ilustra cómo construir una "lista de acceso nombrada":

```
Router(config)# ip access-list extended no_entrar
Router(config-ext-acl)# permit tcp any 172.16.0.0 0.0.255.255 established log
Router(config-ext-acl)# permit udp any host 172.16.1.1 eq dns log
Router(config-ext-acl)# permit tcp 172.17.0.0 0.0.255.255 host 176.16.1.2 eq telnet log
Router(config-ext-acl)# permit icmp any 172.16.0.0 0.0.255.255 echo-reply log
Router(config-ext-acl)# deny ip any any

Router(config)# interface ethernet 0
Router(config-if)# ip access-group no_entrar in
```

Problemas

1. Analice y pruebe la operación de la ACL 105, la cual tiene el propósito de registrar el número de sesiones telnet que transitan por la interfaz serie 0/0 de un encaminador R1. Para confirmar el número de sesiones establecidas, usar el comando *show access list 105*.

```
R1(config)# access-list 105 permit tcp any any eq telnet syn log
R1(config)# access-list 105 permit tcp any any eq telnet
R1(config)# access-list 105 permit ip any any
R1(config)# interface serial0/0
R1(config-if)# ip access-group 105 in
```

2. Analice y pruebe la operación de las listas de acceso extendidas "ICMP-SALIENTE" e "ICMP-ENTRANTE" aplicadas a la interfaz serial 0/0 de R1. La lista de acceso "ICMP-SALIENTE crea la regla reflejada "REGLA-ICMP-REFLEJADA" cuando salen paquetes ICMP por la interfaz serie 0/0 de R1, dicha regla dura 10 segundos. La lista de acceso "ICMP-ENTRANTE" hace uso de la expresión "evaluate REGLA-ICMP-REFLEJADA" para permitir solamente los mensajes ICMP entrantes que respondan a los mensajes ICMP salientes.

```
R1(config)# ip access-list extended ICMP-SALIENTE
R1(config-ext-nacl)# permit icmp any any reflect REGLA-ICMP-REFLEJADA timeout 10
R1(config-ext-nacl)# permit ip any any
R1(config-ext-nacl)# exit
R1(config)# ip access-list extended ICMP-ENTRANTE
R1(config-ext-nacl)# evaluate REGLA-ICMP-REFLEJADA
R1(config-ext-nacl)# deny icmp any any log
R1(config-ext-nacl)# permit ip any any
R1(config-ext-nacl)# exit
R1(config)# interface Serial0/0
R1(config-if)# ip access-group ICMP-SALIENTE out
R1(config-if)# ip access-group ICMP-ENTRANTE in
```

3. Analice y pruebe la operación de la lista de acceso extendida NO-NAVEGAR, la cual tiene en cuenta la hora del día y el día de la semana. Dicha lista se aplica a la interfaz FastEthernet 0/0 de R1. ¿Cuáles aplicaciones se prohíben en el horario LABORAL?

```
R1(config)# time-range LABORAL
R1(config-time-range)# periodic weekdays 8:00 to 18:00
R1(config-time-range)# exit
R1(config)# ip access-list extended NO-NAVEGAR
R1(config-ext-nacl)# deny tcp any any eq 80 23 25 time-range LABORAL
R1(config-ext-nacl)# permit ip any any
R1(config-ext-nacl)# exit
R1(config)# interface FastEthernet0/0
R1(config-if)# ip access-group NO-NAVEGAR in
```

4. ¿Cuál es la diferencia de usar la expresión A o la expresión B en una lista de acceso extendida?

   A. R1(config-ext-nacl)# *permit* tcp any any match-all +syn
   B. R1(config-ext-nacl)# *permit* tcp any any match-any +syn

5. ¿Cuál es el propósito de la lista de acceso "LISTA-IPV6" definida a continuación? ¿Cuál es la diferencia en la sintaxis que usa la lista de acceso "LISTA-IPV6" respecto a la sintaxis de una lista IPv4 tradicional?

```
R1(config)# ipv6 access-list LISTA-IPV6
R1(config-ipv6-acl)# permit ipv6 AAAA:1::/64 any
R1(config-ipv6-acl)# exit
R1(config)# interface FastEthernet0/0
R1(config-if)# ipv6 traffic-filter LISTA-IPV6 in
R1(config-if)# exit
```

Glosario

Bit ACK: indica acuse de recibo del segmento TCP. Este bit es usado en conjunto con el campo "Aknowledge number" del segmento TCP para que un extremo de la conexión TCP confirme positivamente la recepción continua del flujo de datos e indique al otro extremo la secuencia del próximo octeto que está esperando.

Bit RST: indica el cierre abrupto de la conexión TCP.

Coincidencia (match): se presenta cuando los campos de un datagrama IP (incluido el campo de datos) cumplen las condiciones definidas en una línea de la lista de control de acceso IP.

Comodín (del término wildcard): cadena de 32 bits que determinan la posición de los bits de la dirección IP que se deben tener en cuenta (bits