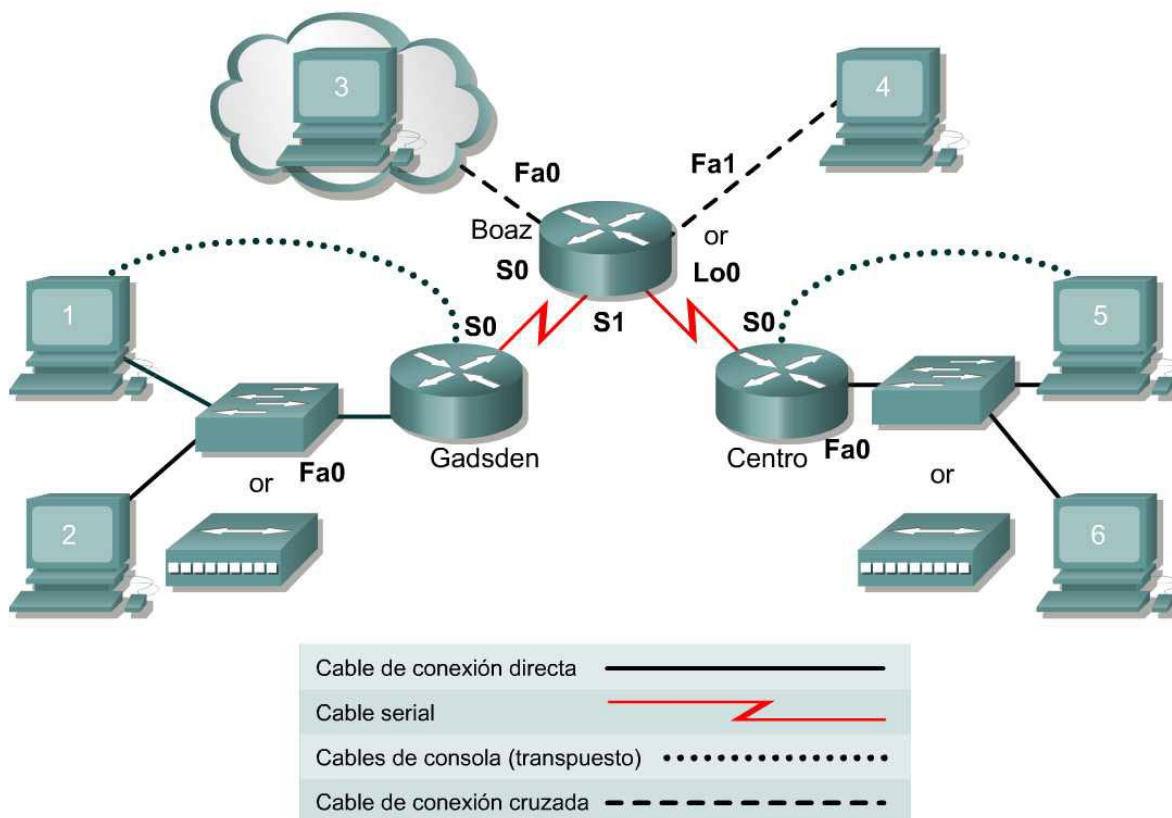


Práctica de laboratorio 11.2.3c Funciones de múltiples listas de acceso (Desafío)



Nombre del router	Tipo de router	Dirección FA0	Dirección FA1	Dirección S0	Dirección S1	Máscara de subred	Enrutamiento	Contraseña enable	Contraseña VTY

Host	Dirección IP	Máscara de subred	Gateway

Objetivo

Configurar y aplicar una lista de control de acceso extendida para controlar el tráfico de Internet mediante uno o más routers.

Situación

La empresa tiene una oficina regional, Boaz, que proporciona servicios a dos sucursales Gadsden y Centro. Cada una de estas oficinas tiene un gerente de sucursal y varias personas a cargo de los servicios al cliente. Ha habido una cantidad considerable de rotación entre el personal de servicio. Después de una auditoría de seguridad, se descubrió que no existían restricciones de red en los computadores usados por el personal de servicio.

El líder del equipo de infraestructura de red desea la creación y la implementación de un plan para aplicar seguridad de red para evitar el acceso.

Infraestructura

El Host 3 representa la Internet. Una alternativa es usar la interfaz loopback 0 en Boaz y ejecutar el comando `Boaz(config)#ip http server`.

Host 4 representa un servidor de web interno que contiene información confidencial de personal y nómina.

El Host 4 también representará a el computador de administración de red

Todas las cuatro direcciones de host más bajas de cada subred están reservadas para los computadores de los gerentes de sucursal (hosts 1 y 5).

Las interfaces del router usan las direcciones más altas de las subredes.

La dirección restante de cada subred de la sucursal será utilizada por los computadores del personal de servicio (hosts 2 y 6).

Paso 1 Interconexión básica del router

- Interconecte los routers de acuerdo al diagrama.

Paso 2 Diseño de dirección de red

- a. Utilizando una dirección IP privada clase C para la red interna, diseñe y documente la red. Complete las tablas anteriores e incluya el tipo y número de interfaz, dirección IP, máscara de subred y tipo de cable. La red "Internet" (nube) puede ser cualquier dirección de espacio privado. Asegúrese de que los intervalos de direcciones asignados a los routers y hosts cumplan con los criterios descritos en la sección de infraestructura anterior.

Paso 3 Configuración básica del router

- a. Es posible que el router tenga configuraciones de un uso anterior. Por este motivo, borre la configuración inicial y vuelva a cargar el router para eliminar cualquier configuración residual. Mediante la información creada anteriormente, configure el router con RIP o IGRP y verifique la conectividad haciendo ping a todos los sistemas y routers desde cada sistema.

Para simular ubicaciones específicas de la Internet, agregue la siguiente configuración al router Boaz.

```
Boaz (config) #interface loopback 1
Boaz (config-if) #ip address 192.168.255.1 255.255.255.255
Boaz (config-if) #exit
Boaz (config) #interface loopback 2
Boaz (config-if) #ip address 192.168.255.2 255.255.255.255
Boaz (config-if) #exit
Boaz (config) #interface loopback 3
Boaz (config-if) #ip address 192.168.255.3 255.255.255.255
Boaz (config-if) #exit
Boaz (config) #interface loopback 4
Boaz (config-if) #ip address 192.168.255.4 255.255.255.255
Boaz (config-if) #exit
Boaz (config) #interface loopback 5
Boaz (config-if) #ip address 192.168.255.5 255.255.255.255
Boaz (config-if) #exit
Boaz (config) #interface loopback 6
Boaz (config-if) #ip address 192.168.255.6 255.255.255.255
Boaz (config-if) #exit
Boaz (config) #interface loopback 7
Boaz (config-if) #ip address 192.168.255.7 255.255.255.255
Boaz (config-if) #exit
Boaz (config) #interface loopback 8
Boaz (config-if) #ip address 192.168.255.8 255.255.255.255
Boaz (config-if) #exit
Boaz (config) #interface loopback 9
Boaz (config-if) #ip address 192.168.255.9 255.255.255.255
Boaz (config-if) #exit
Boaz (config) #interface loopback 10
Boaz (config-if) #ip address 192.168.255.10 255.255.255.255
Boaz (config-if) #exit
```

Agregue una sentencia de red al protocolo de enrutamiento de Boaz para publicar esta red.

```
Boaz (config-router) #network 192.168.255.0
```

Paso 4 Configuraciones de cliente

- a. Configure los hosts con la información pertinente mediante la información definida anteriormente.
☐ Verifique la conectividad haciendo ping a todos los sistemas y routers desde cada sistema.
- b. En los hosts 3 y 4 instale y configure un servidor Web como el servidor Tiny Web.
(<http://www.simtel.net/pub/pd/13103.html>) (El Host 3 representa la Internet. El Host 4 representa un servidor de web interno que contiene información confidencial de personal y nómina). (El Host 4 puede ser el loopback del router de Boaz)
☐ Verifique que todos los sistemas puedan usar un navegador de web para acceder a las páginas web del servidor intranet (host 4) y el servidor de Internet (host 3).
- c. En el host 3, instale y configure un servidor telnet como TelnetXQ
(http://www.datawizard.net/Free_Software/TelnetXQ_Free/telnetxq_free.htm).
☐ Verifique que todos los sistemas puedan hacer Telnet a la Internet (host 3).
- d. Ahora que la infraestructura está armada, es el momento de implementar la seguridad de la red.

Paso 5 Asegurar el servidor de Intranet

- a. Host 4 representa un servidor de web interno que contiene información confidencial de personal y nómina. SÓLO los gerentes de sucursal deben tener acceso a la información en este servidor. Es necesario crear una lista o listas de control de acceso para asegurar el servidor a fin de que sólo las máquinas de los gerentes de sucursal tengan acceso de web (protocolo http) a este servidor interno.

¿Cuántas listas de control de acceso se utilizarán?

¿Dónde se aplicará la lista (o listas) de control de acceso?

¿En qué dirección se aplicará la lista (o listas) de control de acceso?

¿Por qué motivos puede ser mejor usar varias listas de control de acceso?

¿Por qué motivos puede ser mejor usar una sola lista de control de acceso?

- b. Mediante un editor de texto, como el Bloc de notas, desarrolle la lógica de la(s) lista(s) de acceso, y luego escriba los comandos correspondientes. Cuando la lista esté correctamente desarrollada, péguela en el o los routers y aplíquela a las interfaces correspondientes.
- c. Confirme que la ACL funcione correctamente.
☐ Verifique la conectividad haciendo ping a todos los sistemas y routers desde cada sistema.
☐ Verifique que todos los sistemas informáticos puedan usar un navegador de web para acceder a las páginas web en la internet (en cualquier lugar salvo en el servidor de web interno).
☐ Verifique que los computadores del personal de servicio NO PUEDAN usar un navegador de web para acceder (protocolo http) al servidor de intranet.
☐ Verifique que los computadores desde la Internet (host 3) NO PUEDAN usar un navegador de web para acceder (protocolo http) al servidor de intranet.

Paso 6 Asegurar los documentos de Intranet

- a. Existe la preocupación de que los documentos de procedimientos y políticas internas se distribuyan fuera de la empresa. Para asegurarse de que los usuarios de la red interna no puedan enviar estos documentos, no permita que ningún computador tenga acceso de telnet o FTP a la Internet.

¿Será necesario crear una nueva lista (o listas) de control de acceso o modificar la lista o listas actual(es)?

Si es necesario crear una nueva lista (o listas):

¿Cuántas listas de control de acceso se crearán? _____

¿Dónde se aplicará la nueva lista (o listas) de control de acceso?

¿En qué dirección se aplicará la nueva lista (o listas) de control de acceso?

- b. Nuevamente, use un editor de texto, como el Bloc de notas, para desarrollar la lógica de la(s) lista(s) de acceso, y luego escriba los comandos correspondientes. Cuando la lista esté correctamente desarrollada, péguela en el o los routers y aplíquela a las interfaces correspondientes.
- c. Confirme que la ACL funcione correctamente.
- [] Verifique la conectividad haciendo ping a todos los sistemas y routers desde cada sistema.
 - [] Verifique que todos los sistemas informáticos puedan usar un navegador de web para acceder a las páginas web en la internet (en cualquier lugar salvo en el servidor de web interno).
 - [] Verifique que los computadores del personal de servicio NO PUEDAN usar un navegador de web para acceder (protocolo http) al servidor de intranet.
 - [] Verifique que los computadores desde la Internet (host 3) NO PUEDAN usar un navegador de web para acceder (protocolo http) al servidor de intranet.
 - [] Verifique que los computadores NO PUEDAN hacer telnet a la Internet (host 3 e interfaces de loopback en Boaz) pero puedan hacer telnet a los routers.

Paso 7 Impedir el abuso de Internet

- a. Se han presentado algunas quejas de que los empleados abusan del acceso a Internet. Han estado accediendo a sitios de contenido ofensivo. Para ayudar a poner fin a esta práctica, no permita ningún tráfico IP desde la red a los siguientes sitios:

192.168.255.1
192.168.255.4
192.168.255.8
192.168.255.9

¿Será necesario crear una nueva lista (o listas) de control de acceso o modificar la lista o listas actual(es)?

Si es necesario crear una nueva lista (o listas):

¿Cuántas listas de control de acceso se crearán?

¿Dónde se aplicará la nueva lista (o listas) de control de acceso?

¿En qué dirección se aplicará la nueva lista (o listas) de control de acceso?

- b. Nuevamente, use un editor de texto, como el Bloc de notas, para desarrollar la lógica de la(s) lista(s) de acceso, y luego escriba los comandos correspondientes. Cuando la lista esté correctamente desarrollada, péguela en el o los routers y aplíquela a las interfaces correspondientes.
- c. Confirme que la ACL funcione correctamente.
 - ☐ Verifique que los computadores del personal de servicio NO PUEDAN usar un navegador de web para acceder (protocolo http) al servidor de intranet.
 - ☐ Verifique que los computadores desde la Internet (host 3) NO PUEDAN usar un navegador de web para acceder (protocolo http) al servidor de intranet.
 - ☐ Verifique que los computadores NO PUEDAN hacer telnet a la Internet (host 3 e interfaces de loopback en Boaz) pero puedan hacer telnet a los routers.
 - ☐ Verifique que los computadores NO PUEDAN hacer telnet, acceder con un navegador de web ni hacer ping a 192.168.255.1.
 - ☐ Verifique que los computadores NO PUEDAN hacer telnet, acceder con un navegador de web ni hacer ping a 192.168.255.4.
 - ☐ Verifique que los computadores NO PUEDAN hacer telnet, acceder con un navegador de web ni hacer ping a 192.168.255.8.
 - ☐ Verifique que los computadores NO PUEDAN hacer telnet, acceder con un navegador de web ni hacer ping a 192.168.255.9.
 - ☐ Verifique la conectividad haciendo ping a todos los demás sistemas y routers desde cada sistema.
 - ☐ Verifique que todos los sistemas informáticos puedan usar un navegador de web para acceder a las páginas web en la internet (host 3 e interfaces de loopback en Boaz).

Paso 8 Impedir los ataques de Servicio Denegado (DoS)

- a. En las últimas semanas la red de la empresa ha sufrido varios ataques de Servicio Denegado. Muchos de estos ataques han asumido la forma del envío del "ping de la muerte" (paquetes de eco ICMP de tamaño excesivo) o broadcasts dirigidos (x.x.x.255). Para impedir los ataques mediante el "ping de la muerte", no permita que ningún paquete de eco ICMP entre a la red. También para detener el broadcast dirigido, impida la entrada a la red de todos los paquetes IP dirigidos a la dirección de broadcast dirigida.

¿Será necesario crear una nueva lista (o listas) de control de acceso o modificar la lista o listas actual(es)?

Si es necesario crear una nueva lista (o listas):

¿Cuántas listas de control de acceso se crearán?

¿Dónde se aplicará la nueva lista (o listas) de control de acceso?

¿En qué dirección se aplicará la nueva lista (o listas) de control de acceso?

- b. Nuevamente, use un editor de texto, como el Bloc de notas, para desarrollar la lógica de la(s) lista(s) de acceso, y luego escriba los comandos correspondientes. Cuando la lista esté correctamente desarrollada, péguela en el o los routers y aplíquela a las interfaces correspondientes.
- c. Confirme que la ACL funcione correctamente.
 - [] Verifique que los computadores del personal de servicio NO PUEDAN usar un navegador de web para acceder (protocolo http) al servidor de intranet.
 - [] Verifique que los computadores desde la Internet (host 3) NO PUEDAN usar un navegador de web para acceder (protocolo http) al servidor de intranet.
 - [] Verifique que los computadores NO PUEDAN hacer telnet a la Internet (host 3 e interfaces de loopback en Boaz) pero puedan hacer telnet a los routers.
 - [] Verifique que los computadores NO PUEDAN hacer telnet, acceder con un navegador de web, ni hacer ping a 192.168.255.1.
 - [] Verifique que los computadores NO PUEDAN hacer telnet, acceder con un navegador de web ni hacer ping a 192.168.255.4.
 - [] Verifique que los computadores NO PUEDAN hacer telnet, acceder con un navegador de web ni hacer ping a 192.168.255.8.
 - [] Verifique que los computadores NO PUEDAN hacer telnet, acceder con un navegador de web ni hacer ping a 192.168.255.9.
 - [] Verifique que todos los sistemas informáticos puedan usar un navegador de web para acceder a las páginas web en la internet (host 3 y otras interfaces de loopbacks en Boaz).
 - [] Verifique que el host 3 NO PUEDA hacer ping con éxito a nada en la red.
 - [] Verifique que los sistemas puedan hacer ping con éxito a los demás hosts de Internet.
 - [] Verifique la conectividad haciendo ping a todos los demás sistemas y routers desde cada sistema.

Paso 9 Bloquear telnet a los routers

- a. También ha habido algunos intentos de hacer telnet a los routers desde el interior y el exterior de la red. El único host que debe tener acceso por telnet a los routers es el computador de administración de la red. Para impedir el acceso por telnet a los routers, cree una lista de control de acceso y aplíquela a las líneas VTY de los routers que permitan que sólo el computador de administración de la red haga telnet.

¿Qué tipo de lista de acceso se utilizará?

¿Qué comando se utilizará para aplicar la lista a las líneas de VTY?

- b. Use un editor de texto, como el Bloc de notas, para desarrollar la lógica de la(s) lista(s) de acceso, y luego escriba los comandos correspondientes. Cuando la lista esté correctamente desarrollada, péguela en el o los routers y aplíquela a las líneas VTY.
- c. Confirme que la ACL funcione correctamente.
 - [] Verifique que los computadores del personal de servicio NO PUEDAN usar un navegador de web para acceder (protocolo http) al servidor de intranet.
 - [] Verifique que los computadores desde la Internet (host 3) NO PUEDAN usar un navegador de web para acceder (protocolo http) al servidor de intranet.
 - [] Verifique que los computadores NO PUEDAN hacer telnet a la Internet (host 3 e interfaces de loopback en Boaz) pero puedan hacer telnet a los routers.

- [] Verifique que los computadores NO PUEDAN hacer telnet, acceder con un navegador de web, ni hacer ping a 192.168.255.1.
- [] Verifique que los computadores NO PUEDAN hacer telnet, acceder con un navegador de web ni hacer ping a 192.168.255.4.
- [] Verifique que los computadores NO PUEDAN hacer telnet, acceder con un navegador de web ni hacer ping a 192.168.255.8.
- [] Verifique que los computadores NO PUEDAN hacer telnet, acceder con un navegador de web ni hacer ping a 192.168.255.9.
- [] Verifique que todos los sistemas informáticos puedan usar un navegador de web para acceder a las páginas web en la internet (host 3 y otras interfaces de loopbacks en Boaz).
- [] Verifique que el host 3 NO PUEDA hacer ping con éxito a nada en la red.
- [] Verifique que los sistemas puedan hacer ping con éxito a los demás hosts de Internet.
- [] Verifique que los sistemas puedan hacer ping con éxito al host 3.
- [] Verifique que el computador de administración de la red (host 4) pueda hacer telnet a todos los routers.
- [] Verifique que los demás computadores internos NO PUEDAN hacer telnet a ninguno de los routers.
- [] Verifique que los demás computadores externos (host 3) NO PUEDAN hacer telnet a ninguno de los routers.

Paso 10 Verificar las listas de acceso

- a. Ahora que se han aplicado las listas de acceso, es necesario verificarlas.

En primer lugar, verifique qué listas se han definido. Desde una sesión CLI en uno de los routers con listas de acceso, muestre las listas de acceso con el comando `Boaz#show ip access-lists`. Anote la información acerca de una de las listas de acceso.

¿Qué representa el “(# matches)” en el resultado?

- b. A continuación, confirme qué lista de acceso se ha aplicado a cada interfaz. Esto se hace desde la sesión de terminal de uno de los routers con listas de acceso, con el comando `Boaz#show ip interface`. Observe el resultado desde cada interfaz y anote las listas aplicadas a cada interfaz.

Interfaz _____

La lista de acceso de salida es _____

La lista de acceso de entrada es _____

Interfaz _____

La lista de acceso de salida es _____

La lista de acceso de entrada es _____

Interfaz _____

La lista de acceso de salida es _____

La lista de acceso de entrada es _____

Interfaz _____

La lista de acceso de salida es _____

La lista de acceso de entrada es _____

- c. Al terminar la práctica, borre la configuración inicial de los routers, quite y guarde los cables y el adaptador. Termine la sesión y apague el router.