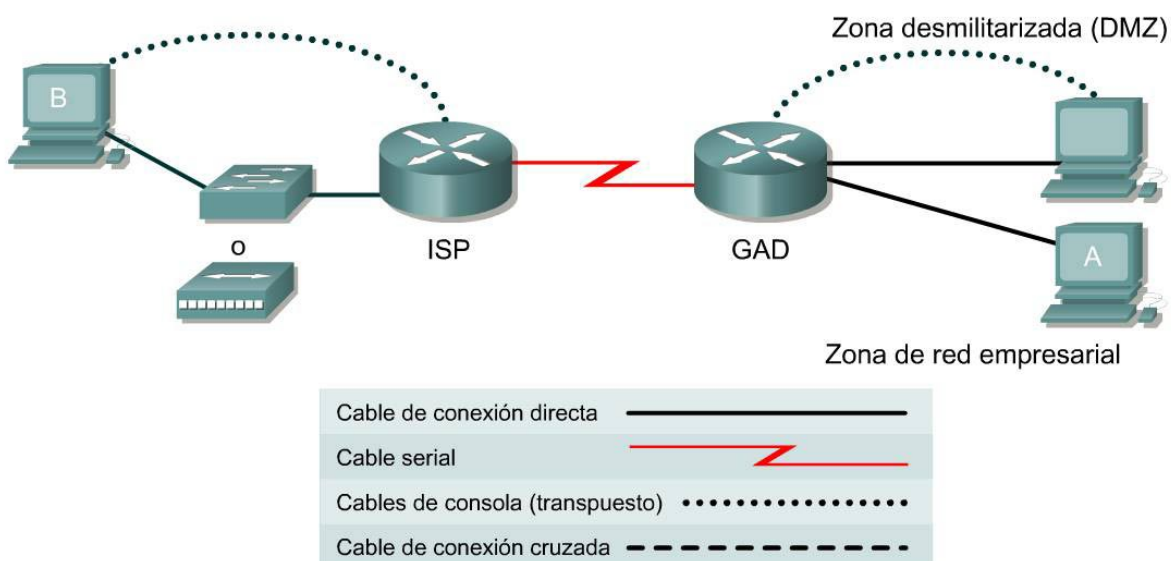


Práctica de laboratorio 11.2.3b Listas de acceso extendidas DMZ sencillas



Designación del router	Nombre del router	Contraseña enable secret	Contraseña enable, VTY y consola	Protocolo de enrutamiento	Sentencias de red RIP
ISP	ISP	class	cisco	RIP	172.16.0.0
GAD	GAD	class	cisco	RIP	10.0.0.0 172.16.0.0

Designación del router	Nombres de host IP	Dirección Fast Ethernet 0	Tipo de interfaz Serial 0	Dirección serial 0	Dirección Fast Ethernet 1
ISP	ISP	172.16.2.1/24	DTE	172.16.1.1/24	N/A
GAD	GAD	10.1.1.1/24	DCE	172.16.1.2/24	10.10.10.1/24

Host	Dirección IP	Máscara de subred	Gateway
Servidor Web	10.1.1.10	255.255.255.0	10.1.1.1
A	10.10.10.10	255.255.255.0	10.10.10.1
B	172.16.2.10	255.255.255.0	172.16.2.1

Objetivo

En esta práctica de laboratorio, se aprende a usar las listas de acceso extendidas para crear una Zona Desmilitarizada (DMZ) sencilla.

Situación

BMTC es una pequeña empresa manufacturera de Gadsden. Decidieron dar a conocer sus productos a través de la Internet. Por lo tanto, su requisito inmediato es promover sus productos a los clientes potenciales ofreciendo descripciones, informes y testimonios sobre los productos. Los requisitos futuros incluirían correo electrónico, FTP, DNS y servicios de comercio electrónico en línea.

Lo han contratado a usted para diseñar y configurar una infraestructura segura que satisfaga sus requisitos de red internos y externos, manteniendo al mismo tiempo la responsabilidad fiscal, lo que significa “que sea segura con bajo costo”.

Después de un análisis cuidadoso, se propone crear una arquitectura de seguridad de dos escalones que se compone de una zona de red empresarial y una Zona Desmilitarizada (DMZ). La zona de red empresarial constará de servidores privados y clientes internos. La DMZ consistirá en sólo un servidor externo que proporcionaría servicios World Wide Web. Aunque tener un solo servidor crea un solo punto de falla, el servicio sólo tiene fines informativos y no se considera crítico para la empresa.

A la empresa le gustó la propuesta y han firmado un contrato para proceder.

Paso 1 Configuraciones básicas del router y el host

- a. Interconecte los routers y los hosts de acuerdo con el diagrama. Configure todos los aspectos básicos del router, como el nombre de host, interfaces del router y protocolo de enrutamiento. Consulte el diagrama y las tablas que aparecen más arriba.

Las configuraciones de cada router deben ser similares a lo siguiente:

```
GAD#show running-config
```

```
<Resultado omitido>
```

```
!  
hostname GAD  
!  
interface FastEthernet0  
  ip address 10.1.1.1 255.255.255.0  
!  
interface Serial0  
  ip address 172.16.1.2 255.255.255.0  
!  
interface FastEthernet1  
  ip address 10.10.10.1 255.255.255.0  
!  
router rip  
  network 10.0.0.0  
  network 172.16.0.0  
!  
GAD#
```

```
ISP#show running-config
```

```
<Resultado omitido>
```

```
!  
hostname ISP  
!  
interface FastEthernet0  
  ip address 172.16.2.1 255.255.255.0  
!  
interface Serial0
```

```
ip address 172.16.1.1 255.255.255.0
!
router rip
 network 172.16.0.0
!

ISP#
```

- b. Configure los hosts con la información pertinente mediante la información definida anteriormente.
- c. Para que la práctica de laboratorio sea más realista, se debe instalar software de servidor de web en el host de servidor de web. Los ejemplos incluyen Microsoft IIS o Microsoft Personal Web Server (Windows 98). Se puede usar un software de otras empresas, como TinyWeb Server (<http://www.rttlabs.com/tinyweb/>). Si se usa TinyWeb Server, se recomienda instalar también TinyBox (<http://people.freenet.de/ralph.becker/tinybox/>), un programa frontal GUI para TinyWeb Server.

No se olvide de crear una página index.html por defecto. La página web debe incluir un mensaje, como "Hola, mundo". Guarde la página de acuerdo con las instrucciones del software de servidor de Web.

- d. Antes de aplicar cualquier tipo de lista de acceso, es importante verificar la conectividad entre sistemas.

[] Verifique la conectividad haciendo ping a todos los sistemas y routers desde cada sistema.

¿Puede hacer ping el Host A al Host B?

¿Puede hacer ping el Host A al servidor de Web?

¿Puede hacer ping el Host B al Host A?

¿Puede hacer ping el Host B puede al servidor de Web?

Todos los hosts deben poder hacer ping los unos a los otros. Es posible que sea necesario proformar el diagnóstico de fallas si el ping a algunas interfaces no tiene éxito. Siempre se deben verificar las conexiones de la capa física, ya que con frecuencia son la fuente de los problemas de conectividad. A continuación, verifique las interfaces del router. Asegúrese de que no estén apagadas, configuradas de forma incorrecta, y de que RIP esté configurado correctamente. Finalmente, recuerde que junto con las direcciones IP válidas, los hosts también deben tener gateways por defecto especificados.

- e. En el Host A, abra un navegador de Web como Windows Explorer o Netscape Navigator e introduzca la dirección del servidor Web en el espacio para la dirección.

[] Verifique que cada Host tenga acceso Web al servidor de Web.

¿Puede ver el Host A la página index.html?

¿Puede ver el Host B la página index.html?

Ambos hosts deben poder ver la página index.html en el navegador de Web. Haga diagnóstico de fallas según sea necesario.

- f. Ahora que la infraestructura está armada, es el momento de implementar la seguridad de la red.

Paso 2 Proteger la red empresarial

- a. La zona de red empresarial consta de servidores privados y clientes internos. Ninguna otra red debe poder acceder a ella.
- b. Configure una lista de acceso extendida para proteger la red empresarial. La protección de una red empresarial empieza por especificar cuál es el tráfico que puede salir de la red. Aunque esto al principio parezca extraño, tiene más sentido al considerar que la mayoría de los hackers son empleados internos. La primera lista de acceso especifica cuál es la red que puede salir de la red.

Introduzca lo siguiente:

```
GAD#conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
GAD(config)#access-list 101 permit ip 10.10.10.0 0.0.0.255 any
GAD(config)#access-list 101 deny ip any any
```

La primera línea definida en la lista de acceso “101” sólo permite que los usuarios empresariales válidos de la red 10.10.10.0 accedan al router. La segunda línea no se requiere realmente debido al deny all implícito, pero se agregó para facilitar la comprensión.

- c. Ahora se necesita aplicar la lista de acceso a una interface de la red de la corporación.

Introduzca lo siguiente:

```
GAD(config)#interface fa1
GAD(config-if)#ip access-group 101 in
```

- d. Ahora se necesita probar la lista de acceso.

[] Verifique la conectividad haciendo ping a todos los sistemas y routers desde cada sistema.

¿Puede hacer ping el Host A al servidor de Web?

¿Puede hacer ping el Host A al Host B?

¿Puede hacer ping el Host B puede al servidor de Web?

¿Puede hacer ping el Host B al Host A?

Todos los hosts deben poder hacer ping a cualquier ubicación.

- d. A continuación, configure una lista de acceso extendida de salida en la interfaz de la red empresarial. El tráfico que entra a la red empresarial vendrá de la Internet o la DMZ. Por este motivo, es importante limitar el tráfico que se permita entrar a la red empresarial.
- e. La primera cuestión que se debe tratar es asegurarse de que sólo el tráfico originado en la red empresarial pueda volver a esa red. Introduzca lo siguiente:

```
GAD(config)#access-list 102 permit tcp any any established
```

La palabra clave **established** en esta línea sólo permite el tráfico TCP que se origina en la red 10.10.10.0.

- f. Para facilitar la gestión de red y el diagnóstico de fallas, también se decide permitir ICMP en la red. Esto permitirá que los hosts internos reciban mensajes ICMP (por ej., mensajes de ping).

Introduzca lo siguiente:

```
GAD(config)#access-list 102 permit icmp any any echo-reply
GAD(config)#access-list 102 permit icmp any any unreachable
```

La primera línea sólo permite que los pings exitosos vuelvan a la red empresarial. La segunda línea permite mostrar los mensajes de los ping que no fueron exitosos.

- g. En este momento no se desea que entre otro tráfico a la red empresarial. Por lo tanto, introduzca lo siguiente:

```
GAD(config)#access-list 102 deny ip any any
```

- h. Finalmente la lista de acceso debe aplicarse al puerto Fast Ethernet de la red empresarial.

```
GAD(config)#interface fa 0
GAD(config-if)#ip access-group 102 out
```

- i. Recuerde que una interfaz puede admitir una lista de acceso de entrada y otra de salida. Para verificar esto, ejecute el comando `show ip interface fa1`. Su salida debe confirmar que la lista de acceso saliente debe ser la 102 y la entrante debe ser la 101.
- j. Use el comando `show access-lists` para verificar la sintaxis de las listas de acceso. El resultado debe ser similar a lo siguiente:

```
GAD#show access-lists
Extended IP access list 101
    permit ip 10.10.10.0 0.0.0.255 any
    deny ip any any
Extended IP access list 102
    permit tcp any any established
    permit icmp any any echo-reply
    permit icmp any any unreachable
    deny ip any any
```

Es posible que se tenga que eliminar las listas de acceso y volver a introducirlas si hay alguna discrepancia entre el resultado anterior y la configuración.

- k. Ahora es necesario probar las listas de acceso.
- [] Verifique la conectividad haciendo ping a todos los sistemas y routers desde cada sistema.

¿Puede hacer ping el Host A al servidor de Web?

¿Puede hacer ping el Host A al Host B?

¿Puede hacer ping el Host B al servidor de Web?

¿Puede hacer ping el Host B al Host A?

El Host A debe poder hacer ping a todas las ubicaciones. Sin embargo, ningún otro host debe poder hacer ping al Host A.

- l. En el Host A, abra un navegador de Web como Windows Explorer o Netscape Navigator e introduzca la dirección del servidor Web en el espacio para la dirección.
- [] Verifique que el Host A siga teniendo acceso de Web al servidor de Web.

¿Puede ver el Host A la página index.html?

- m. El Host A todavía debería poder ver la página index.html en el navegador de Web. Haga diagnóstico de fallas según sea necesario.
- n. Ahora, la red empresarial interna es segura. A continuación, es necesario asegurar la red DMZ.

Paso 3 Proteger la red DMZ

- a. La red DMZ consistirá en sólo un servidor externo que proporcionará servicios World Wide Web. Los otros servicios como el correo electrónico, FTP y DNS se implementarán posteriormente. Aunque tener un solo servidor crea un solo punto de falla, el servicio sólo tiene fines informativos y no se considera crítico para la empresa.
- b. Configure una lista de acceso extendida para proteger la red DMZ. Una vez más, como ocurre con la red empresarial, especifique cuál es el tráfico que puede salir de la red y aplíquelo a la interfaz.

Introduzca lo siguiente:

```
GAD#conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
GAD(config)#access-list 111 permit ip 10.1.1.0 0.0.0.255 any
GAD(config)#access-list 111 deny ip any any

GAD(config)#interface fa0
GAD(config-if)#ip access-group 111 in
```

- c. Ahora pruebe las nuevas listas de acceso.
[] Verifique la conectividad haciendo ping a todos los sistemas y routers desde cada sistema.
¿Puede hacer ping el Host A al servidor de Web?

¿Puede hacer ping el Host A al Host B?

¿Puede hacer ping el Host B puede al servidor de Web?

¿Puede hacer ping el Host B al Host A?

El Host A debe poder hacer ping a todas las ubicaciones. Sin embargo, ningún otro host debe poder hacer ping al Host A.

- d. A continuación, se requiere una lista de acceso extendida de salida para especificar el tráfico que puede entrar a la red DMZ. El tráfico que entra a la red DMZ vendrá de la Internet o de la red empresarial que requiera los servicios de la World Wide Web.
- e. Configure una lista de acceso extendida de salida que especifique que las peticiones a la World Wide Web puedan entrar a la red. Introduzca lo siguiente:

```
GAD(config)#access-list 112 permit tcp any host 10.1.1.10 eq www
```

Esta línea permite que los servicios de la World Wide Web destinados al servidor de Web entren a la red DMZ.

¿Qué comando se debe introducir para permitir las peticiones DNS a la DMZ?

¿Qué comando se debe introducir para permitir las peticiones de correo electrónico a la DMZ?

¿Qué comando se debe introducir para permitir las peticiones FTP a la DMZ?

- f. Para fines de gestión, sería útil permitir que los usuarios empresariales hagan **ping** al servidor de Web. Sin embargo, los usuarios de Internet no deben recibir el mismo privilegio. Agregue una línea a la lista de acceso para permitir que sólo los usuarios empresariales tengan acceso ICMP a la red DMZ.

Introduzca lo siguiente:

```
GAD(config)#access-list 112 permit icmp 10.10.10.0 0.0.0.255 host
10.1.1.10
```

Esta línea sólo permite que los hosts de la red empresarial hagan **ping** al servidor de Web. Aunque es posible imponer más restricciones a las opciones ICMP en la configuración, no se considera necesario.

- g. Se pueden permitir otros servicios en la red DMZ en el futuro. Sin embargo, en este momento no se debe permitir que otro tráfico entre a la red DMZ. Por lo tanto, introduzca lo siguiente:

```
GAD(config)#access-list 112 deny ip any any
```

- h. Aplique la lista de acceso de salida al puerto Fast Ethernet de la red DMZ.

```
GAD(config)#interface fa 0
GAD(config-if)#ip access-group 112 out
```

- i. Para verificar la sintaxis de las listas de acceso, use el comando **show-access-lists**. El resultado debe ser similar a lo siguiente:

```
GAD#show access-lists
Extended IP access list 101
    permit ip 10.10.10.0 0.0.0.255 any (70 matches)
    deny ip any any
Extended IP access list 102
    permit tcp any any established (8 matches)
    permit icmp any any echo-reply (12 matches)
    permit icmp any any unreachable
    deny ip any any (4 matches)
Extended IP access list 111
    permit ip 10.1.1.0 0.0.0.255 any (59 matches)
    deny ip any any
Extended IP access list 112
    permit tcp any host 10.1.1.10 eq www (29 matches)
    permit icmp 10.10.10.0 0.0.0.255 host 10.1.1.10 (4 matches)
    deny ip any any (14 matches)
```

Es posible que sea necesario eliminar las listas de acceso y volverlas a introducir si hay alguna discrepancia entre el resultado anterior y la configuración.

- j. Ahora, es necesario probar las listas de acceso.

[] Verifique la conectividad haciendo ping a todos los sistemas y routers desde cada sistema.

¿Puede hacer ping el Host A al servidor de Web?

¿Puede hacer ping el Host A al Host B?

¿Puede hacer ping el Host B al servidor de Web?

¿Puede hacer ping el Host B al Host A?

- k. El Host A debe poder hacer ping a todas las ubicaciones. Sin embargo, host externos no deberían poder hacer ping al Host A.

Use un navegador de Web como Windows Explorer o Netscape Navigator en cada host e introduzca la dirección del servidor Web en el espacio para la dirección.

[] Verifique que los hosts sigan teniendo acceso Web al servidor de Web.

¿Puede ver el Host A la página index.html?

¿Puede ver el Host B la página index.html?

Ambos hosts todavía deben poder ver la página index.html en el navegador de Web. Haga diagnóstico de fallas según sea necesario.

- l. Ahora, la red DMZ es segura. A continuación, necesitamos configurar nuestra interfaz externa para impedir las prácticas de spoofing y hacking.

Paso 4 Impedir el spoofing

- Las redes son cada vez más vulnerables a los ataques de usuarios externos. Hackers, “crackers” y “script kiddies” son algunos de los nombres que se dan a las personas que, con el objeto de hacer daño, intentan penetrar en las redes o impedir que las redes respondan a peticiones legítimas (ataques de Servicio Denegado (DoS)). Esto se ha convertido en un problema importante para la comunidad de la Internet.
- Usted conoce bien las prácticas empleadas por algunos de estos hackers. Un método común es intentar falsificar direcciones IP origen internas válidas. Esta práctica se conoce como “spoofing”.
- Para impedir el spoofing, se decide configurar una lista de acceso de manera que los hosts de Internet no puedan hacer fácilmente spoof de las direcciones de red internas. Hay tres direcciones IP origen comunes que los hackers intentan falsificar, que son las direcciones internas válidas (es decir, 10.10.10.0), las direcciones de loopback (es decir, 127.x.x.x) y las direcciones multicast (es decir, 224.x.x.x – 239.x.x.x).
- Configure una lista de acceso de entrada que haga más difícil que los usuarios externos hagan spoof de las direcciones internas y aplíquela a la interfaz Serial 0.

Introduzca lo siguiente:

```
GAD(config)#access-list 121 deny ip 10.10.10.0 0.0.0.255 any
GAD(config)#access-list 121 deny ip 127.0.0.0 0.255.255.255 any
GAD(config)#access-list 121 deny ip 224.0.0.0 31.255.255.255 any
GAD(config)#access-list 121 permit ip any any

GAD(config)#interface serial 0
GAD(config-if)#ip access-group 121 in
```

La primera línea impide que los usuarios externos falsifiquen una dirección IP de origen válida. La segunda línea impide que usen el intervalo de direcciones loopback. La tercera línea contrarresta la práctica de los hackers de usar un intervalo multicast de direcciones (es decir, 224.0.0.0 – 239.255.255.255) para crear tráfico interno innecesario.

- e. Verifique la sintaxis de las listas de acceso con el comando **show-access-lists**. El resultado debe ser similar a lo siguiente:

```
GAD#show access-lists
GAD#show access-lists
Extended IP access list 101
    permit ip 10.10.10.0 0.0.0.255 any (168 matches)
    deny ip any any
Extended IP access list 102
    permit tcp any any established (24 matches)
    permit icmp any any echo-reply (28 matches)
    permit icmp any any unreachable
    deny ip any any (12 matches)
Extended IP access list 111
    permit ip 10.1.1.0 0.0.0.255 any (122 matches)
    deny ip any any
Extended IP access list 112
    permit tcp any host 10.1.1.10 eq www (69 matches)
    permit icmp 10.10.10.0 0.0.0.255 host 10.1.1.10 (12 matches)
    deny ip any any (22 matches)
Extended IP access list 121
    deny ip 10.10.10.0 0.0.0.255 any
    deny ip 127.0.0.0 0.255.255.255 any
    deny ip 224.0.0.0 31.255.255.255 any
    permit ip any any (47 matches)
```

Es posible que sea necesario eliminar las listas de acceso y volverlas a introducir si hay alguna discrepancia entre el resultado anterior y la configuración.

- f. Por último, verifique que todavía haya conectividad.

[] Verifique la conectividad haciendo ping a todos los sistemas y routers desde cada sistema.

¿Puede hacer ping el Host A al servidor de Web?

¿Puede hacer ping el Host A al Host B?

¿Puede hacer ping el Host B al servidor de Web?

¿Puede hacer ping el Host B al Host A?

Sólo el Host A debe poder hacer ping a todas las ubicaciones.

- g. Use un navegador de Web como Windows Explorer o Netscape Navigator en cada host e introduzca la dirección del servidor Web en el espacio para la dirección.

[] Verifique que los hosts sigan teniendo acceso Web al servidor de Web.

¿Puede ver el Host A la página index.html?

¿Puede ver el Host B la página index.html?

Ambos hosts todavía deben poder ver la página index.html en el navegador de Web. Haga diagnóstico de fallas según sea necesario.

- h. Ahora, la red BMTC es segura.

Nota: La práctica de laboratorio anterior es una solución básica para proporcionar una red segura. Esto no pretende ser una solución completa.

Para proteger de manera adecuada las redes empresariales, se deben implementar dispositivos de red dedicados como Cisco PIX. También se recomienda enfáticamente usar las funciones

avanzadas como la Traducción de Direcciones de Red y las opciones de listas de acceso avanzadas como las listas de acceso reflexivas y las Listas de Acceso Basadas en Contenido (CBAC); estas funciones no se incluyen en la certificación CCNA.

Por último, se recomienda que los administradores de red mantengan relaciones sólidas con sus proveedores de servicios, para obtener ayuda cuando se vea comprometida la seguridad de la red.

Paso 5 Documente la ACL

- a. Como parte de toda la gestión de red, es necesario elaborar documentación. Agregue comentarios adicionales al archivo de texto creado para la configuración. Este archivo también debe contener resultados de los comandos `show access-list` y `show ip interface`.
- b. El archivo debe guardarse junto con la demás documentación de red. La convención de nombres de archivos debe reflejar la función del archivo y la fecha de implementación.
- c. Al terminar, borre la configuración inicial de los routers, quite y guarde los cables y el adaptador. Termine la sesión y apague el router.