Packet Tracer: firewalls del servidor y ACL del router

Tabla de direccionamiento

Dispositivo	Dirección IP privada	Dirección IP pública	Máscara de subred	Sitio
Servidor web	N/D	209.165.201.10	255.255.255.0	Internet

Objetivos

Parte 1: conectarse al servidor web

Parte 2: evitar las sesiones de HTTP no cifradas

Parte 3: acceder al firewall en el servidor de correo electrónico

Aspectos básicos

En esta actividad, tendrá acceso a un usuario en el sitio de Metropolis y se conectará con HTTP y HTTPS a un servidor web remoto. La asignación de direcciones IP, la configuración de red y las configuraciones de servicio ya están completas. Utilizará un dispositivo cliente en el sitio de Metropolis para probar la conectividad a un servidor web remoto y luego asegurar el sitio de Metropolis al impedir que las sesiones web sin cifrar se conecten con el mundo exterior.

Parte 1: Conéctese con el servidor Web

Paso 1: Acceda al servidor web de Internet de HQ en la computadora de Sally mediante HTTP.

a. Haga clic en el sitio **Metropolis Bank HQ** y luego haga clic en la computadora **Sally**.

b. Haga clic en la ficha **Escritorio** y luego haga clic en **Navegador web**.

c. Introduzca la URL **http://www.cisco.corp** y haga clic en **Ir**.

d. Haga clic en el enlace **Página de inicio de sesión**.

¿Por qué un usuario debería preocuparse al enviar información mediante este sitio web?

Paso 2: Acceda al servidor web de Internet de HQ en la computadora de Sally mediante HTTP.

a. Acceda al **navegador web** en la computadora de Sally.

b. Introduzca la URL **http://www.cisco.corp** y haga clic en Ir.

c. Haga clic en el enlace **Página de inicio de sesión**.

¿Por qué un usuario debería preocuparse al enviar información mediante este sitio web?

d. Cierre la computadora de **Sally**.

Parte 2: Evitar las sesiones de HTTP no cifradas

Paso 1: Configure el router HQ_Router

a. En el sitio **Metropolis Bank HQ** haga clic en **HQ_Router**.

b. Haga clic en la ficha **CLI** y presione **Intro**.

c. Utilice la contraseña **cisco** para iniciar sesión al router.

d. Utilice el comando **habilitar** y luego el comando **configurar terminal** para acceder al modo de configuración global.

Para evitar que el tráfico HTTP sin cifrar pase a través del router HQ, los administradores de redes pueden crear e implementar listas de control de acceso (ACL).

Los siguientes comandos se encuentran más allá de este curso pero se utilizan para demostrar la capacidad para evitar que el tráfico no cifrado se mueva a través del router HQ_Router.

e. En el modo de configuración global **HQ_Router** (config)# copie la siguiente configuración de la lista de acceso y pegúela en el router **HQ_Router**.

```
!
access-list 101 deny tcp any any eq 80
access-list 101 permit ip any any
!
int gig0/0
ip access-group 101 in
!
end
```

f. Cierre el router **HQ_Router**.

Paso 2: Acceda al servidor web de Internet de HQ en la computadora de Sally mediante HTTP.

a. En el sitio **Metropolis Bank HQ** , haga clic en la computadora **Sally**.

b. Haga clic en la ficha **Escritorio** y luego haga clic en **Navegador web**.

c. Introduzca la URL **http://www.cisco.corp** y haga clic en **Ir**.

La computadora de **Sally** ¿es capaz de acceder al servidor web de Internet HQ utilizando HTTP?

Paso 3: Acceda al servidor web de Internet de HQ en la computadora de Sally mediante HTTP.

a. Acceda al **navegador web** en la computadora de Sally.

b. Introduzca la URL **http://www.cisco.corp** y haga clic en Ir.

La computadora de Sally ¿es capaz de acceder al servidor web de Internet HQ utilizando HTTP?

c. Cierre la computadora de **Sally**.

Parte 3: Acceder al firewall en el servidor de correo electrónico

a. En el sitio **Metropolis Bank HQ**, haga clic en el servidor de **correo electrónico**.

b. Haga clic en la ficha **Escritorio** y luego haga clic en **Firewall**. No existen reglas de firewall implementadas.

Para evitar que el tráfico no relacionado con correo electrónico se envíe o reciba de un servidor de correo electrónico, los administradores de redes pueden crear reglas de firewall directamente en el servidor o, como se muestra previamente, pueden usar listas de control de acceso (ACL) en un dispositivo de red como un router.

Tabla de puntuación sugerida

Sección de la actividad	Ubicación de la consulta	Puntos posibles	Puntos obtenidos
Parte 1: conectarse al servidor web	Paso 1	15	
	Paso 2	15	
Parte 2: evitar las sesiones de HTTP no cifradas	Paso 2	15	
	Paso 3	15	
	Preguntas	**60**	
	Puntuación de Packet Tracer	**40**	
	Puntuación total	**100**	