Práctica 5: Listas de acceso estándar y extendidas

Material necesario:

- maqueta de routers, cables de red y consola y ordenadores de consola.

Introducción:

Las listas de acceso (ACLs Access Lists) son filtros que utilizan una numeración para identificarse:

1-99 son ACLs estándar
100-199 son ACLs extendidas.

Las **ACLs estándar** tienen la configuración siguiente:

```
Router(config)# access-list n° permit|deny origen [wild-mask]
```

y se aplican a los interfaces con:

```
Router (config-if)# ip access-group n° in|out
```

siendo **in** la indicación del tráfico a filtrar que ENTRA por la interfaz del router y **out** la indicación para filtrar el tráfico que SALE por la interfaz del router.

Además la *wild-mask*, indica con 0 el bit a evaluar y con 1 indica que el bit correspondiente se ignora. Por ejemplo, si quiero indicar un único host 192.13.13.1 especifico: 192.13.13.1 con *wild-mask* 0.0.0.0 y si quiero especificar toda la red clase C correspondiente lo indico con 192.13.13.0 y *wild-mask* 0.0.0.255.

Las ACLs estándar solo pueden filtrar el tráfico por origen nunca por destino.

Las **ACLs extendidas** tienen la configuración siguiente, donde dependiendo del protocolo especificado (IP, ICMP, TCP, UDP, ...) tendremos opciones de configuración diferente, siempre acorde con el protocolo, es decir con TCP podré utiliza operación de puertos pero con IP no. La sintaxis de las ACLs extendidas es:

```
Router (config)# access-list n° permit|deny protocolo
origen [wild-mask] [operación] [puerto origen] destino
[wild-mask] [operación] [puerto destino] [established]
```

La opción de [**established**] indica que sólo pasarán paquetes TCP con los flags ACK o RST activados, es decir, que no permite pasar ningún comienzo de conexión con el flag SYN=1 ACK=0, de inicio de sesión TCP. Podemos forzar así que el establecimiento de la conexión se realice en el sentido contrario donde está establecida la lista de acceso.

Como operación se suele usar eq que significa igual (equal)

Las ACLs se aplican a los interfaces con la siguiente sintaxis, siendo “out” la opción por defecto:

Router (`config-if)# ip access-group` **`n°`** `in|out`

Importante:

- Es conveniente que desactives el cortafuegos de tu ordenador antes de empezar esta práctica:

```
service iptables stop
```

- Recuerda que solo se pueden definir 2 ACLs por cada interfaz. Una de entrada y otra de salida

Parte 1. Listas de Acceso Estandar

Paso 1.- Configurar la maqueta con RIP (u otro protocolo de routing).

Una vez hecho esto se comprobará que los pings funcionan. Es decir que hay conectividad entre todos los routers y Pcs. Hacer esta vez pruebas de conectividad entre PCs.

Nota importante: Para esta práctica será necesaria la configuración de los host.

Configuración de la IP del host:

```
ifconfig eth0 inet dirección_IP netmask máscara
```

Configuración del router por defecto del host:

```
route add –net 0.0.0.0 netmask 0.0.0.0 gw dirección_IP
```

Comprobación de si lo hemos hecho bien:

```
ifconfig eth0
```

```
route –n
```

Si comprobamos que la información del router de acceso es incorrecta, podemos borrar una entrada con:

```
route del –net 0.0.0.0 netmask 0.0.0.0 gw dirección_IP
```

Para hacer esto se seguirán los siguientes pasos.

1.1 Verificación de las conexiones y encendido de los equipos

En primer lugar los alumnos deberán interconectar los equipos según la maqueta general. Una vez comprobadas las conexiones procedemos a encender los hosts y arrancarlos con el sistema operativo ‘linux redes’.

Una vez ha arrancado el sistema operativo entraremos con el usuario root y la password utilizada en las sesiones anteriores y pondremos en marcha el programa minicom mediante el comando 'minicom –s', pulsando a continuación la tecla escape. Con el programa minicom ya en marcha encenderemos los routers, debiendo ver aparecer por consola los mensajes de arranque.

Si no aparece nada deberemos comprobar los cables, los equipos y la configuración del minicom, que debe ser:

- Velocidad 9600 bits/s
- 8 bits de datos
- Un bit de parada (8N1)
- Sin paridad
- Control de flujo: ninguno
- Dispositivo de entrada: /dev/ttyS0

(El uso del dispositivo ttyS0 se debe a que estamos utilizando el puerto COM1 del ordenador.)

1.2. Configuración de los routers

Configurar los routers de la maqueta usando RIP (esta práctica también funcionaría con cualquier otro protocolo de routing de los vistos hasta la fecha) y comprobar que los ping entre routers. Es decir que hay conexión entre todos ellos.

1.3. Configuración de los hosts

Debemos asignar la dirección IP que corresponde a cada host, según se indica en la maqueta. Para ello utilizaremos los comandos vistos en la página anterior.

Además algunos comandos Linux cuando se utilizan direcciones IP intentan realizar la resolución inversa de las direcciones en el DNS, para averiguar el nombre correspondiente. En algunos casos (por ejemplo los comandos 'ping', 'route' o 'traceroute') esto puede evitarse con la opción ' -n', pero en otros comandos como 'telnet' no existe esta opción, por lo que es necesario esperar a que expire el timeout del DNS (unos 30 segundos aproximadamente).

Para evitar este retardo cuando utilicemos el comando telnet cambiaremos de nombre el fichero resolv.conf en el directorio /etc mediante el comando:

```
mv /etc/resolv.conf /etc/resolv.conf.old
```

De esta forma evitamos la consulta al DNS y por tanto la espera. Podemos prescindir entonces de la opción '–n' en los comandos 'ping', 'route' o 'traceroute'.

Si el fichero resolv.conf no existe en el directorio /etc/ el cambio de nombre nos dará un error, pero en ese caso ya no se producirá el timeout así que no debemos preocuparnos.

Paso 2.- ACL Estándar

Esta parte sólo se realiza desde Lab-A: En los routers de la maqueta, configurar una lista de acceso estándar, de forma que no permita salir el tráfico procedente de **ET1.**

Este es el caso de que sepamos que un ordenador de nuestra red (en este caso ET1 está transmitiendo virus o

Acordaros que las listas de acceso llevan implícito al final el “deny any”, por tanto si no se indica lo contrario, el tráfico desde el resto de ordenador en la LAN de **ET1** también estará denegado, cosa que no queremos. Sólo debemos denegar salida del ordenador **ET1**.

Escribe la configuración necesaria:

```
Router(config)# _____________________________________
Router(config)# _____________________________________
Router(config)# _____________________________________
Router(config-if)# _____________________________________
```

Comprobaciones:

Ejecuta las siguiente ordenes y comprueba que todo es correcto:

- **show run**
- **show access-list**
- **show ip interfaces**

Puedes comprobar su correcto funcionamiento si conectas en dicha LAN un host con una IP distinta a la de **ET1** o cambias directamente la IP de **ET1**.

Con ello, podemos comprobar que si hacemos *ping* desde otro ordenador en una LAN diferente a donde está **ET1**, nos indicará que el tiempo de espera está agotado, y si hacemos *ping* desde **ET1**, el router nos indicará con un ICMP que el destino es inalcanzable.

¿Por qué? Analiza la respuesta.

Paso 3.- TODOS.

Ahora en el resto de ordenadores **ETx** de la maqueta, configuramos en sus routers una ACL estándar para que no salga ningún tráfico de ellos.

Acordaros que si denegamos el tráfico de una IP determinada, además deberemos de indicar que el resto de tráfico está permitido.

Desde consola de todos los routers, podemos comprobar que los **ETx** no pueden contestar (tiempo de espera agotado) pero sí las interfaces FastEthernet de cada router

Paso 4.- Borrar.

Ahora borramos las listas de acceso creadas y comprueba con “show run” que se han borrado correctamente. Se recuerda que es necesario usar “no” delante de cada comando de configuración para poder borrarlo.

```
Router(config)#_____________________________
Router(config)# _____________________________
Router(config)# _____________________________
Router(config-if)# _____________________________
```

Comprobar que otra vez hay conectividad entre todos los PCs.

Parte 2. Listas de Acceso Extendidas

Paso 5.- En esta parte vamos a habilitar primero las conexiones telnet en los routers, para ello configuraremos en cada router:

```
line vty 0 4
     login
     password cisco
```

Ahora debemos poder conectarnos por telnet a todos los routers conectados en la maqueta. Probarlo.

Paso 6.- Vamos a configurar la red, para que las conexiones por telnet a los routers, sólo sean admitidas localmente por LAN, es decir cualquier equipo con una IP que no proceda de la LAN local, no podrá acceder al servicio telnet del router en cuestión. Configúrelo y compruebe su funcionamiento. Tener en cuenta que denegar el servicio telnet es equivalente a denegar una conexión TCP al puerto 23.

Escribe la configuración necesaria:

```
Router(config)# _____________________________
Router(config)# _____________________________
Router(config)# _____________________________
Router(config)# _____________________________
```

(y aplicarla a las interfaces necesarias del router)

Una vez aplicada probar desde tu PC a tu router y a la IP de otro router

Paso 7.- Proxy.

Por motivos de seguridad y flexibilidad en una empresa, podemos configurar un proxy web cache dentro de la red. Para ello deberíamos configurar todos los navegadores que accedieran al puerto 80 localmente, pero no al exterior. Un proxy web cache se utiliza para acelerar las peticiones al exterior y convertirlas en accesos locales, de forma que queden registradas en el proxy siempre localmente para otros usuarios y sólo el proxy puede acceder al exterior.

Como no disponemos de servidores web en nuestra red local vamos a usar servidores DAYTIME sobre TCP.

7.1. Activar servicio DAYTIME en todos los PCs

Este servicio se ofrece a través del puerto 13 y para ello haremos lo siguiente en todos los PCs.

Ir al directorio `/etc/xinetd.d`

Editar el fichero `daytime` por ejemplo con vi

Comprobar que incluye una línea que pone

```
disable = no
```

Si el valor es igual a yes, cambiarlo por no.

Rearrancar el servicio con:

```
service xinetd restart
```

En el caso de que no estuviera arrancado ya poner:

```
service xinetd start
```

Comprobar que el puerto 13 está abierto:

```
nmap localhost
```

Acceder desde cada PC al servicio poniendo:

```
telnet dir_IP_del_servidor 13
```

Y comprobar que recibes información del servicio DAYTIME. Es decir información de la fecha y hora actual.

7.2. Configurar ACL

Vamos a suponer que la dirección IP del proxy acaba en .101 dentro de cada LAN. Esta dirección es la de los PCs ET1, ET2, ET3 y ET4, pero no la de ET5. Eso quiere decir que una vez implementada la ACL los PCs ET1…ET4 podrá seguir recibiendo el servicio pero el ET5 no. Comprobar que pos paquetes ICMP (pings) si que siguen saliendo.

Escribir una ACL que permita realizar esto:

```
Router(config)# _____________________________
Router(config)# _____________________________
Router(config)# _____________________________
Router(config)# _____________________________
Router(config-if)# _____________________________
```

7.2. ¿Qué pasaría con la siguiente configuración?

```
Router(config)# access-list 101 deny tcp any eq 13 any
Router(config)# access-list 101 permit ip any any
Router(config)# interface F0
Router(config-if)# ip access-group 101 in
```

Paso 8.- Borrar

Borrar las ACLs anteriores y comprobar su correcto borrado con “show run”.

Paso 9.- Established

Crear una ACL en los routers para que permita conexiones TCP salientes desde las diferentes LANs pero no entrantes. Es decir la comunicación que se inicia en la LAN será permitida y las que se inicien fuera no. Probarla con telnet a las interfaces del router.

```
Router(config)# _____________________________
Router(config)# _____________________________
Router(config)# _____________________________

(y aplicarla a los interfaces necesarios del router)
```

Paso 10.- Finalización

Una vez finalizada la práctica los alumnos deberán realizar las siguientes tareas:

Volverán a poner el nombre habitual al fichero de los DNS (en caso de que lo hubieran cambiado) mediante el comando

```
mv /etc/resolv.conf.old /etc/resolv.conf
```

Apagar los ordenadores y routers y las regletas de enchufes que tengan interruptores.

Volver a poner conexiones de red de los hosts a las tomas de la pared en las que se encontraban inicialmente.