EL *ROUTER* CISCO

En forma general los *routers* CISCO están diseñados principalmente para enrutar el tráfico de una red, y como segunda función, tienen incorporada una tecnología de filtrado de paquetes. Esta segunda característica es utilizada por muchas organizaciones como un *firewall* eficiente.

Un *firewall* es un sistema diseñado para prevenir que personas no autorizadas tengan acceso a una red o a un servidor, puede ser implementado en software, en hardware o en ambos. Todos los mensajes recibidos o enviados a una red protegida pasan a través del *firewall*, y este a su vez examina cada mensaje y bloquea los que no cumplen ciertos criterios de seguridad. Un *firewall* puede ser un simple *host* o una red compleja formada por *routers*.

En este capitulo se hablará en especial del *router* CISCO, sus características generales, la seguridad que se debe de tomar para prevenir algunos ataques y sobre todo como mejorar la seguridad de la red utilizando filtrado de paquetes por medio de listas de acceso.

4.1 Routers

El *router* es la estructura básica de las redes, que cuenta con las siguientes capacidades [26]:

- Puede soportar simultáneamente diferentes protocolos (Ethernet, *Token Ring*, RDSI, y otros), haciendo compatible todos los equipos en la capa de red.
- Conecta a la perfección LAN a WAN.
- Filtra al exterior el tráfico no deseado aislando áreas en las que los mensajes se pueden difundir a todos los usuarios de una red.
- Actúan como puertas de seguridad comprobando el tráfico mediante listas de permisos de acceso.
- Asegura fiabilidad, ofreciendo múltiples trayectorias a través de las redes.
- Aprende automáticamente nuevas trayectorias y selecciona las mejores.

En pocas palabras, los *routers* hacen posible la existencia de redes.

Los *routers* son computadoras dedicadas al procesamiento de la interconexión de redes, que no incluyen monitor, ni teclado, ni ratón, por lo que debe comunicarse con ellos de una de las siguientes formas:

- Desde una terminal (PC o estación de trabajo funcionando en modo terminal) conectada a él mediante un cable.
- Mediante un punto de la red.

Dado que los *routers* son los enlaces que mantienen unidas las redes, el diseño de medidas de seguridad dentro de ellos es muy importante; la primera medida que se debe tomar en cuenta es la asignación de contraseña para no permitir el acceso al público en general y en especial a los *hackers*. La tabla 4.1 lista los tipos de contraseñas del *router* y lo que hacen. En los *routers* CISCO se utilizan las contraseñas para restringir el acceso a:

- El dispositivo.
- La parte EXEC privilegiada (modo habilitar) del entorno del software IOS (*Internetwork Operating System*).
- El uso de comandos específicos del IOS.

Punto de control	Tipo de contraseña	¿Qué está restringido?
Puerto consola	Línea	Iniciar una sesión mediante una línea local a través del puerto de consola.
Puerto AUX	Línea	Iniciar una sesión mediante una línea módem (o local) conectada al puerto auxiliar.
Inicio de sesión de red	Terminal virtual	Iniciar la sesión en el *router* mediante una conexión de red usando telnet sobre una línea VTY.
EXEC privilegiado	Enable o Enable Secret	Entrar al nivel más potente del entorno IOS.

Tabla 4.1 Información de las contraseñas y sus usos.

Las contraseñas de línea se usan para controlar quién puede iniciar la sesión en un *router*; se define protección por contraseña en la línea terminal de consola, la línea AUX (auxiliar) y en cualquiera de las cinco líneas de terminal virtual (VTY).

Por ejemplo:

nuyoo% telnet 192.100.170.254
Trying 192.100.170.254...
Connected to 192.100.170.254.
Escape character is '^]'.

User Access Verification

Password: xxxxx
router>

Una vez superada la contraseña de línea, inicia la sesión en el entorno del software IOS del *router*. El IOS se divide en dos niveles de privilegios, *EXEC* y *Privileged EXEC* (*modo habilitar*). El nivel *EXEC* contiene sólo comandos básicos, no destructivos, y el

modo habilitar permite el acceso a comandos más potentes, en el sentido de que permiten volver a configurar el *router*.

4.1.1 Memoria del *router*

Un *router* es parecido a una PC, cuentan con una CPU, memoria, puertos e interfaces para conectar periféricos y diferentes medios de comunicación, lo único que no tienen son discos. Una parte importante es la memoria, dado que con ella puede operar y puede llevar acabo su administración de forma autónoma.

Los *routers* cuentan con varias clases de memoria. Estas memorias son: RAM/DRAM, NVRAM, FLASH y ROM, cada una se encarga de una tarea especifica. La RAM/DRAM es utilizada para llevar a cabo el trabajo, es decir, cuando el *router* esta funcionando esta memoria contiene una imagen del IOS, el archivo de configuración en ejecución, la tabla de ruteo y el buffer de paquetes. Esta memoria puede ser duplicada o cuadriplicada. La memoria NVRAM conserva una copia del archivo de configuración del router, de esta forma, si el *router* se apaga, la NVRAM permite al *router* iniciar con la configuración correcta. La memoria FLASH es utilizada para almacenar el IOS, y como se puede borrar, permite a los administradores de red copiar nuevas versiones del IOS. La memoria ROM almacena un estado mínimo de configuración del router.

4.2 Reglas de filtrado de paquetes

Los *routers* de sistemas CISCO ejecutan un sistema operativo llamado *Internetwork Operating System* (IOS), el cual esta especialmente diseñado para ejecutar ruteo a alta velocidad. El IOS mantiene un conjunto de tablas de configuración interna que están asociadas con el *router*, el protocolo que el *router* comprende, la interfaz de red, y la interfaz de línea física. Estas tablas de configuración son consultadas por el IOS cada vez que un paquete es recibido. Dichas tablas son configuradas desde la consola cuando el *router* se encuentra en modo de configuración, esta configuración es colocada en el *router* usando el comando *write*; este comando produce un archivo de texto que puede ser almacenado en la memoria NVRAM o guardado usando el servicio TFTP.

La seguridad en un *router* para el filtrado de paquetes esta basado en un conjunto de reglas para filtrado, estas reglas describen paquetes TCP y UDP en términos de las direcciones fuentes y destino, así como el número de puerto de la aplicación.

En forma general los *routers* están diseñados principalmente para enrutar el tráfico de una red, y como segunda función, CISCO tiene incorporada la tecnología de filtrado de paquetes por medio de los comandos de *listas de acceso*. Esta característica es utilizada por muchas organizaciones como un *firewall* eficiente.

Las lista de acceso se definen como una colección secuencial de condiciones de permiso y negación que se aplican a direcciones de Internet. Para decidir que paquetes deben pasar o no, el código revisa todas las reglas contra el contenido del encabezado del paquete; si el encabezado viola alguna de las reglas, se envía un mensaje ICMP de regreso al remitente. Cada una de las reglas

poseen dos contadores asociados, un contador de paquetes y un contador de bytes, estos contadores son actualizados cuando un paquete cumple con una regla.

Por lo general, un filtro de paquetes se coloca entre uno o más segmentos de red, éstos segmentos de red están clasificados como externos o internos. Para realizar el filtrado de paquetes se hace uso de los puertos, cada uno de ellos puede utilizarse para implantar políticas de red que describan el tipo de servicio de red accesible a través de ellos.

Los *routers* CISCO tienen dos tipos de listas de acceso: listas de acceso estándar y listas de acceso extendidas. Una lista de acceso estándar esta limitada en funcionalidad porque solo permite el filtrado basada en las direcciones fuentes, mientras que las listas de acceso extendidas se basan en las direcciones fuentes, direcciones destino y en los datos de la aplicación [28].

1.2.1 Listas de acceso estándar

Las listas de acceso estándar permiten el filtrado de paquetes con base en la dirección fuente del paquete. El formato general para las listas de acceso estándar es el siguiente:

access-list [*número*] [deny | permit] [*fuente*] [*máscara*] [*log*]

Note que la barra horizontal (|) denota que se debe de elegir la palabra clave deny o permit, y el guión (-) en el término access-list es necesario, el *número* de lista de acceso es un número entre 1 y 99 el cual le indica al IOS que la lista de acceso esta asociada con el protocolo IP. En la actualidad CISCO soporta diferentes tipos de protocolos, en la tabla 4.2 se listan por nombre y por número [28].

Las palabras claves *deny* y *permit*, se utilizan para especificar si el paquete IP debe ser bloqueado (no transmitido) o permitido (transmitido), es decir, *permit* permite que los paquetes puedan viajar a través de la interfaz, mientras que la palabra clave *deny* no les permite el paso.

La *fuente* es un valor de 32 bits y esta escrito utilizando la notación de punto decimal. Especifica la dirección IP del *host* o la red desde la cual los paquetes son enviados. La dirección debe ser de la forma estándar ii.jj.kk.ll.

El campo *máscara* es aplicado a la fuente, y debe ser de la forma ii.jj.kk.ll. Un 1 (en binario) en una posición indica que debe ser ignorado, es decir, 0.0.0.255 dice que solo los tres primero octetos de la dirección fuente deben ser considerados.

Por ejemplo, los siguientes comandos permiten todos los paquetes desde el *host* 204.17.195.100:

access-list 1 permit 204.17.195.100

Lo que es lo mismo

access-list 1 permit 204.17.195.100 0.0.0.0

El siguiente comando bloquea todos los paquetes de la red subclase C 198.3.4:

access-list 1 deny 198.3.4.0 0.0.0.255

Protocolos con lista de acceso especificada por nombre	
IP IPX ISO CLNS NetBIOS IPX Source-routing bridging NetBIOS	
Protocolos con lista de acceso especificada por número	
IP	1-99
IP Extendido	100-199
Código de tipo Ethernet	200-299
Dirección Ethernet	700-799
Transparente bridging (tipo protocolo)	200-299
Transparente bridging (código del proveedor)	700-799
Transparente bridging extendido	1100-1199
DECnet y DECnet extendido	300-399
XNS	400-499
Extendido XNS	500-599
AppleTalk	600-699
Ruta fuente bridging (tipo protocolo)	200-299
Ruta fuente bridging (código del proveedor)	700-799
IPX	800-899
IPX extendido	900-999
IPX SAP, IPX SAP SPX	1000-1099
VINES estándar	1-100
VINES extendido	101-200
VINES simple	201-300

Tabla 4.2 Protocolos con lista de acceso especificados por nombre y número.

Existen palabras claves que pueden ser utilizadas con las listas de acceso, dentro de estas tenemos a: *host*, *any* y *log*. La palabra clave *host* es exactamente lo mismo que la mascara 0.0.0.0, por ejemplo, suponga que quiere permitir los paquetes de la fuente 198.228.20.86, entonces se debe colocar la siguiente declaración:

access-list 1 permit 198.228.20.86 0.0.0.0

Utilizando la palabra *host* se puede colocar:

access-list 1 permit host 198.228.20.86

En una lista de acceso estándar la palabra *any* es usada como una abreviación de la dirección fuente 0.0.0.0 y la mascara 255.255.255.255. Por ejemplo, suponga que se quiere bloquear los paquetes de la fuente 198.228.20.86 y permitir los paquetes de todas las demás direcciones, el código que se coloca es

access-list 1 deny host 198.228.20.86
access-list 1 permit any

La palabra clave *log* es aplicada en las versiones de IOS 11.3.x, cuando aplicamos *log* a una lista de acceso en la consola se muestra cada 5 minutos el número de paquetes que cumplieron la regla, por ejemplo si colocamos:

access-list permit 198.228.20.86 0.0.0.0 log

Suponga que se presentaron 10 paquetes en el periodo de 5 minutos, entonces el despliegue será:

list 1 permit 198.228.20.86 1 packet

Y 5 minutos después se desplegará

list 1 permit 198.228.20.86 9 packet

El uso de *log* es útil para examinar las actividades en la red, e indicar ataques potenciales.

4.2.2 Listas de acceso extendidas

Las listas de acceso extendidas permiten filtrar el tráfico de interfaz con base en las direcciones IP origen y destino, protocolo, puerto fuente, puerto destino, y una variedad de opciones que permiten comparar ciertos campos del paquete.

El formato general de las listas de acceso extendidas es:

access-list [*número*] [deny | permit] [*protocolo*|*clave-protocolo*] [*fuente*] [*máscara-fuente*] [*puerto fuente*] [*destino*] [*máscara-destino*] [*puerto destino*] [*log*] [*opciones*]

Similar a las listas de acceso estándar, el *número* de la lista se utiliza para identificar la lista extendida, el *número* en este caso debe ser un entero entre 100 y 199.

El uso de *deny* o *permit* especifica si el paquete IP debe ser bloqueado (no transmitido) o permitido (transmitido)

El *protocolo* especifica el protocolo a ser filtrado, tal como IP, TCP, UDP, ICMP. Es importante colocar de que protocolo se trata ya que si colocamos IP se filtrarán los paquetes cuyo protocolo sea TCP, UDP e ICMP, dado que estos se encapsulan en IP.

La dirección *fuente* y la *mascara* tiene la misma función que en una lista de acceso estándar, en esta lista también se puede utilizar los términos *host* y *any*.

El *puerto fuente* puede ser especificado en forma numérica o por medio de un mnemónico, por ejemplo, se puede usar el número 80 o http para especificar el protocolo de transmisión de hipertexto. Para TCP o UDP también se puede usar los operadores < (lt), >(gt), =(eq) y ≠(neq).

La dirección *destino* y *máscara destino* tiene la misma estructura que la dirección fuente y máscara fuente, aquí también se puede utilizar los términos *any* y *host*.

El *puerto destino* puede ser especificado igual que el puerto fuente, ya sea por medio de un número, un mnemónico, o usar un operador con un número o con un mnemónico para especificar un rango. Por ejemplo, permitir TCP de cualquier *host* al *host* 198.228.20.86 cuando el paquete transporte datos SMTP.

access-list 101 permit tcp any host 198.228.20.86 eq smtp

Existe también un conjunto de *opciones* que puede soportar una lista de acceso extendida, una de ellas es *log*, la cual ya se comento en las listas de acceso estándar; otra segunda opción es *established*, que es solamente aplicada con el protocolo TCP para restringir el tráfico en una dirección, con esta opción lo que se lleva a cabo es la verificación de los paquetes TCP para determinar si es un ACK o RST. En la tabla 4.3 se muestran las palabras claves que se pueden utilizar con estas listas de acceso.

Palabra clave	Utilización
any	Es usada como una abreviación de una dirección y máscara en lugar del valor 0.0.0.0 255.255.255.255. Aplicada en los campos fuente y destino.
established	Filtra si los bits ACK y RST están colocados (solo en TCP).
host	Usado como una abreviación de la máscara 0.0.0.0. Aplicada en la dirección fuente y destino.
icmp-type	Usado para filtrar los tipos de mensajes ICMP. Se puede también especificar el código de mensaje ICMP (0-255).
port	Usado para definir el número decimal o el nombre del puerto TCP o UDP.
protocol	Usado para definir el protocolo para filtrar. Este puede ser la palabra eigrp, gre, icmp, igmp, igrp, ip, ipinip, nos, ospf, tcp o udp, o un número entero entre 0 y 255 representando un protocolo IP.
precedence/precedence	Usado para filtrar por nivel de precedencia por nombre o número (0-7).
remark	Usado para agregar comentarios a una lista de acceso.
TOS/tos	Usado para el filtrado por nivel de servicio especificado por un número o un nombre.

Tabla 4.3 Palabras claves en una lista de acceso.

Las palabras claves *any, established, host, precedence, remark* y *tos*, son directamente colocadas en una lista de acceso para sustituir un valor numérico o mnemónico. La palabra clave *remark* se empezó a utilizar a partir de la versión 12.0 y se puede aplicar en las listas estándares o en las listas extendidas, por ejemplo:

access-list 101 remark permite tráfico *para la PC de Everth*
access-list 101 permit ip any host 192.100.170.57
access-list 101 remark permite solo el tráfico de Web al servidor de Web
access-list 101 permit tcp any host 192.100.170.4 eq 80

Existen tres elementos necesarios para aplicar una lista de acceso a una interfaz, el primero de ellos son las mismas listas de acceso, el segundo punto es una interfaz para aplicar dichas listas y el tercero es un método para definir la dirección para aplicar estas listas de acceso a la interfaz.

El primer paso ya se discutió, en cuanto al segundo paso se utiliza el comando *interface* para definir la interfaz. En la figura 4.1, se muestra un *router* con tres interfaces, una serial y dos Ethernet, las flechas indican el flujo de información en ambas direcciones. La interfaz serial es usada para conectarse con Internet y las Ethernets para soportar LANs.

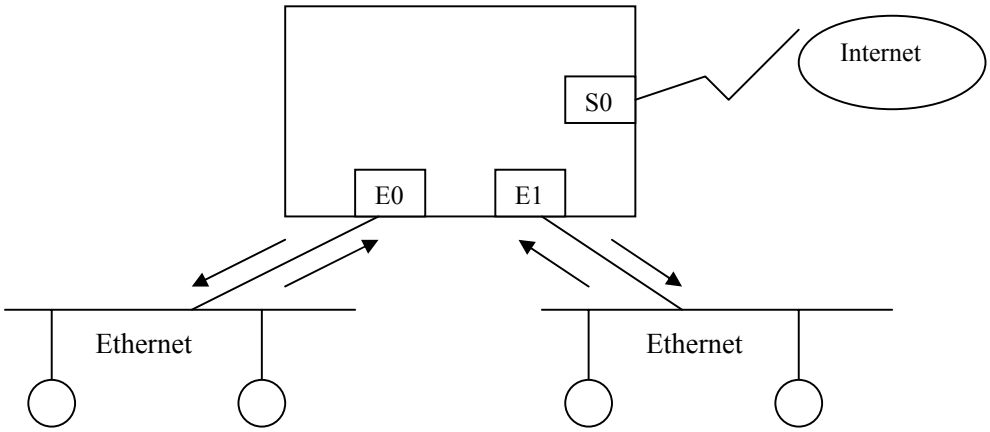

Figura 4.1 *Router* con un puerto serie y dos puertos Ethernet.

Por ejemplo, para aplicar una lista de acceso al puerto serie 0, se debe primero que definir la interfaz con el siguiente comando:

interface serial0

De forma similar, para aplicar la lista de acceso a un puerto que conecta a una LAN Ethernet, se utiliza:

interface ethernet0

En forma abreviada:

interface e0

El tercer paso en el proceso de aplicar una lista de acceso es definir la dirección de la interfaz que la lista de acceso afectará, esto se realiza utilizando el comando *ip access-group*, cuya sintaxis es:

ip access-group [*numero_de_lista*] [*in* | *out*]

El número de lista identifica la lista de acceso, mientras que la palabra *in* o *out* identifican la dirección en la cual la lista de acceso es aplicada, esta dirección indica si los paquetes son examinados cuando llegan (in) o cuando salen (out) de la interfaz del *router*. El siguiente ejemplo muestra los tres pasos juntos:

interface serial0
ip access-group 109 in
access-list 109 remark permite el tráfico *a la pc de Everth*
access-list 109 permit ip any host 192.100.170.57
access-list 109 remark permite solo el tráfico de Web al servidor de Web

access-list 109 permit tcp any host 192.100.170.4 eq 80
access-list 109 remark bloquea todo lo demás
access-list 109 deny ip any any

Si se quiere colocar esta configuración al *router* desde una terminal se deben llevar a cabo los siguientes pasos:

nuyoo% telnet router
Connected to router.utm.mx.
Escape character is '^]'.

User Access Verification

*Password: *****
router>enable
*Password: *****
router# config terminal
Enter configuration commands, one per line. End with CTRL./Z
Router (config)# interface serial0
router (config-if)# ip access-group 109 in
router (config)# access-list 109 remark permite el tráfico *a la pc de Everth*
router (config)# access-list 109 permit ip any host 192.100.170.57
router (config)# access-list 109 remark permite solo el tráfico de Web al servidor de Web
router (config)# access-list 109 permit tcp any host 192.100.100.4 eq 80
router (config)# access-list 109 remark bloquea todo lo demás
router (config)# access-list 109 deny ip any any
router (config)# exit
router# write terminal

Lo que falta mencionar es cómo borramos una lista de acceso, la sintaxis que se debe seguir es:

no access-list *número*

La palabra clave *no* que se antepone a la lista de acceso le indica al *router* que debe borrar la lista asociada a cierto *número.*

Las listas de acceso se pueden colocar en el *router* desde una terminal o enviando un archivo ASCII vía TFTP. Cabe hacer notar que el orden de las listas de acceso es importante, no se puede reordenar o borrar una sola declaración de la lista en el *router*, para realizar esto es mejor que se creen todos los criterios de listas de acceso en un servidor TFTP, y después cargarlas en el *router*.

El *router* es el punto clave para poder comunicarnos con el mundo exterior, y si se llega a dañar o alguien entra a cambiar alguna parte de su configuración podría causar gran daño a la red o a las redes que soporta. Así, en la siguiente sección se tocará el punto de seguridad en el *router*.

4.3 Implementando seguridad en el router

En esta sección se mencionan algunas configuraciones de CISCO que se deben considerar para mejorar la seguridad del *router*. El IOS de CISCO tiene muchas características para especificar la seguridad, tales como las ya mencionadas listas de acceso para el filtrado de paquetes, la intercepción TCP, AAA (*Autentication, Authorization and Accounting*), *logging* de paquetes, calidad de servicio y encriptación [30].

4.3.1 Administración de password

Los password son la primera defensa en contra de los accesos no autorizados, una forma de mejorar al máximo el uso de password es mantenerlos en un servidor de autenticación TACACS+ (*Terminal Access Controller Access Control System*) o RADIUS (*Remote Authentication Dial-In User Service*).

El comando ***enable secret*** es usado para colocar un password que garantice el privilegio de acceso de administración al sistema IOS, este comando es recomendable utilizarlo dado que el password de consola TTY o el de sesión remota VTY puede ser usado para obtener privilegios de acceso. Este password de acceso al *router* se encuentra almacenado en el archivo de configuración del *router*, por lo que es recomendable que se utilice el comando ***service password-encryption*** para poder encriptarlo, y no sea visto en texto claro cuando se consulta el archivo de configuración.

Para prevenir el acceso no autorizado se deben controlar los *logins* interactivos con el *router*, dado que cualquiera que pueda conectarse al *router* puede desplegar información que probablemente no se quiera tener disponible para el público en general. Aunque el acceso interactivo es deshabilitado por omisión, hay excepciones; las más obvias son las sesiones interactivas que se realizan directamente de terminales asíncronas, tales como la terminal de la consola, y de las líneas modem integradas.

Es importante recordar que el puerto de consola de un dispositivo IOS tiene privilegios especiales, en particular, si se envía una señal de BREAK al puerto de consola durante los primeros segundos de la inicialización del dispositivo, se puede usar el procedimiento de recuperación de password para tomar el control del sistema. Esto significa que atacantes pueden entrar o inducir a la ruptura del sistema, y quien tiene acceso al puerto de consola vía una terminal de hardware, modem, terminal, servidor, o algún otro dispositivo, puede tomar el control del sistema, aun si ellos no tienen acceso físico a él.

Todos los mecanismos de acceso interactivo usan la abstracción IOS TTY (es decir, todos invocan las sesiones en "línea"), las terminales asíncronas locales y los modems dialup usan líneas estándares "TTYs", las conexiones remotas de red, indiferentes del protocolo, usan TTYs virtuales, o VTYs, por lo que, el mejor camino para proteger al sistema es hacer seguros los controles que son aplicados a las líneas VTY y las líneas TTY. Como es difícil asegurar que todos los posibles modos de acceso estén bloqueados, se debe asegurar que los *logins* de todas las líneas estén controlados usando alguna clase de mecanismo de autenticación, y además se debe controlar el acceso de máquinas que pertenezcan a redes no confiables. Los *logins* interactivos pueden ser impedidos en cualquier línea, configurándolos con los comandos ***login*** y ***no password***, esta configuración se aplica por default a las VTYs, pero no a las TTYs.

Un dispositivo de CISCO IOS cuenta con un número limitado de líneas VTY (usualmente cinco). Cuando todas las VTYs están usados, no se pueden establecer más conexiones, esto da lugar al ataque de denegado de servicio, si un atacante puede abrir sesiones para todas las VTYs del sistema, el administrador legítimo no podrá accesar al sistema. Una forma de reducir esto es configurar restricciones por medio del comando **ip access-class** en el último VTY que contiene el sistema. El último VTY (usualmente VTY 4) debe estar restringido para aceptar conexiones solamente desde una única estación (específicamente de una estación de administración), mientras que las otras VTYs deben aceptar conexiones desde cualquier dirección de red. Otra táctica útil es configurar el tiempo de salida de VTY usando el comando **exec-timeout**. Esto previene una sesión ociosa que consuma indefinidamente una VTY.

4.3.2 Servicios de administración comúnmente configurables

Muchos usuarios administran sus redes usando protocolos para interactuar remotamente, los protocolos más comunes para este propósito son SNMP y HTTP. Ninguno de estos protocolos esta habilitado por default y, como cualquier otro servicio, la opción más segura es tenerlos deshabilitados.

SNMP es ampliamente usado para el monitoreo de *router*, y configuración del *router*. Desafortunadamente, la versión 1 del protocolo SNMP, la cual es comúnmente usada, utiliza un esquema muy débil de autenticación basado en una "cadena común". SNMP versión 2, soporta un compendio de esquemas de autenticación basado en MD-5, y permite restringir acceso a varios datos de administración. Si utilizamos SNMP versión 1 lo recomendable es que solo se le permita el acceso al *router* a las estaciones administradoras que cuente con cierta dirección IP, para llevar a cabo esto se usa la opción de número de lista de acceso en el comando **snmp-server community.** Si se utiliza SNMP versión 2, lo recomendable es configurar el compendio de autenticación con las palabras **authentication** y **md5** del comando de configuración **snmp-server party.**

Las recientes versiones de software CISCO IOS soportan configuración remota y monitoreo usando el protocolo http. El protocolo de autenticación usado por http es equivalente a enviar un password de texto claro a través de la red, esto hace que http sea una elección riesgosa. Si se elige http para administración, se debe restringir el acceso usando el comando **ip http access-class**, debe además configurar autenticación usando el comando **ip http authentication**. Al igual que los *logins* interactivos, la mejor elección para autenticación http es probablemente usando un servidor TACACS+ o RADIUS.

4.3.3 Administración y acceso interactivo vía Internet

Algunos usuarios administran sus *routers* remotamente, y algunas veces se hace sobre Internet. Cualquier acceso remoto no encriptado con lleva algunos riesgos, pero el acceso sobre una red pública tal como Internet es especialmente peligroso. Todos los esquemas de administración remota, incluyendo el acceso interactivo, http, y SNMP, son vulnerables. Todas las precauciones aplicadas para los *hosts* también son aplicadas a los *routers*.

4.3.3.1 Sniffers

Los atacantes frecuentemente entran a las computadoras que proporcionan servicios de Internet, o en computadoras que se encuentran a lo largo de la red, e instalan programas "sniffer", los cuales monitorean el tráfico que pasa a través de la red y roban datos tales como password y cadenas comunes SNMP, esto implica una mayor dificultad para proporcionar seguridad en la red. Así enviar información por un canal no encriptado es un riesgo, porque se pueden observar en forma clara los *login* y los password de los *routers*.

En lo posible, se debe evitar conectarnos a los *routers* usando un protocolo no encriptado sobre cualquier red no confiable. Si el software del *router* soporta esto, es una buena idea usar un protocolo de encriptación de *login* tal como SSH o Telnet Kerberized. Otra posibilidad es usar la encriptación IPSec para todo el tráfico del *router*, incluyendo Telnet, SNMP y HTTP.

4.3.3.2 Logging

Los *routers* CISCO pueden registrar información acerca de una variedad de eventos, muchos de los cuales tienen una seguridad significativa. Los *logs* pueden ser invaluables en la caracterización y respuesta de incidentes de seguridad. Los principales tipos de *logging* usados por los *routers* CISCO son:

- Logging AAA, los cuales coleccionan información acerca del uso de conexiones *dial-in*, *logouts*, accesos http, cambios en el nivel de privilegios, ejecución de comandos, y eventos similares. Las entradas al log AAA son enviadas a servidores de autenticación usando los protocolos TACACS+ y/o RADIUS, y son registrados localmente por estos servidores, típicamente en archivos. Si se usando servidores TACACS+ o RADIUS, se puede habilitar logging AAA de varias formas usando comandos de configuración tales como **aaa accounting**.
- SNMP trap logging, los cuales envían notificaciones de cambios significativos en el estado del sistema a estaciones administradoras SNMP.
- System logging, registra una gran variedad de eventos, dependiendo de la configuración del sistema. Los eventos de system logging pueden ser reportados por una variedad de destinatarios, entre los que se encuentran:
    - El puerto de consola del sistema (**logging console**)
    - Servidores que usan el protocolo de UNIX "syslog" (**logging** *ip-address,* **logging trap**)
    - Sesiones remotas en VTYs y sesiones locales en TTYs (**logging monitor**, **terminal monitor**)
    - Un buffer logging local en un *router* RAM (**logging buffered**)

Desde el punto de vista de la seguridad, los eventos más importantes usualmente registrados por *system logging* son los cambios de estado de la interfaz, cambios a la configuración del sistema, listas de acceso y la detección de intrusos. Por default, la información de system logging es enviada solo al puerto de consola asíncrona. Algunos puertos de consola no son monitoreados, o están conectados a terminales con salida de memoria histórica y con un pequeño despliegue, esta información puede no estar disponible cuando se necesite, especialmente cuando un problema empieza a inspeccionarse en la red. Sin embargo cada *router* debe almacenar la información de

system logging en un buffer local RAM. El buffer logging es de un tamaño fijo, y guarda sola la información nueva, esta información desaparece cuando el *router* es apagado. Para crear el buffer se usa el comando de configuración **logging buffered** *buffer-size*. Puede usar el comando **show memory** para estar seguro que el *router* tiene bastante memoria libre para soportar un buffer *logging*.

4.3.4 Registro de violaciones de listas de acceso

Si se usan listas de acceso para filtrar el tráfico, se pueden requerir los logs de los paquetes que violen los criterios de filtrado. Las viejas versiones del software CISCO IOS soportan *logging* usando la palabra clave **log**, la cual causa logging de las direcciones IP y los números de puerto asociados con los paquetes marcados en las entradas de las listas de acceso. Las nuevas versiones proporcionan la palabra clave **log-input**, la cual agrega información acerca de la interfaz que recibió el paquete, y la dirección MAC del *host* que lo envío.

No es una buena idea configurar *logging* para marcar los paquetes que coinciden con las entradas de la lista de acceso porque causa archivos log excesivamente grandes, y puede llegar a tirar el sistema, sin embargo, los mensajes log frecuentemente son limitados para que el impacto no sea catastrófico.

Los *logging* de lista de acceso puede además ser usados para caracterizar el tráfico asociado con los ataques de red por *logging* de tráfico sospechoso.

4.3.5 Securing IP routing

En esta sección se discuten algunas medidas de seguridad básica relacionadas con la forma en la cual los *routers* reenvían los paquetes IP.

4.3.5.1 Anti-spoofing

Muchos ataques de red están asociados con los ataques de falsificación, o "*spoofing*", de direcciones fuentes de *datagramas* IP. Algunos ataques trabajan absolutamente con *spoofing*, y otros ataques son muchos más difíciles de rastrear si el atacante puede usar alguna otra dirección en lugar de la suya. Por lo tanto, es invaluable para los administradores de red prevenir los spoofing.

Los Anti-spoofing deben realizarse en los puntos de red donde sea practico, pero es más fácil y efectivo en las fronteras de los bloques de direcciones grandes o entre los dominios de la administración de red; es impractico hacer un anti-spoofing en cada *router* de red, por la dificultad de determinar cuales direcciones fuentes pueden legítimamente aparecer en cada interfaz.

Los administradores de *firewall*s o *router* perimetrales algunas veces instalan medidas anti-spoofing para prevenir que los *hosts* en la Internet asuman direcciones de *hosts* internos, pero no toman medidas para prevenir que *hosts* internos asuman direcciones de *hosts* de Internet. Esto es hasta ahora la mejor idea para tratar de prevenir spoofing en ambas direcciones. Existen al menos tres buenas razones para hacer anti-spoofing en ambas direcciones en una organización:

1. Los usuarios internos realizan menos ataques a la red y tienen menos probabilidades de éxito.
2. La mal configuración de los *hosts* internos es la menor causa de problemas para sitios remotos (y por lo tanto es menos probable el daño a la reputación de la organización).
3. Los crackers frecuentemente entran a las redes para utilizarlas como trampolín para realizar más ataques. Estos crackers pueden tener menos interés en una red con protección spoofing de salida.

La configuración de la lista de acceso depende mucho de la red individual, de modo que la meta básica es simple: descartar los paquetes que lleguen de direcciones fuentes no confiables. Por ejemplo, en un *router* con dos interfaces conectando a una corporación de red a Internet se puede configurar para que cualquier *datagrama* que llegue en la interfaz de Internet, con campo de dirección fuente indicando que viene de una máquina de la corporación de red, sea descartado. Similarmente, cualquier *datagrama* que llegue en la interfaz conectada a la red de la corporación, pero cuyo campo de dirección fuente indique que viene de una máquina fuera de la corporación de red, debe ser descartado. Si los medios de CPU permiten esto, el anti-spoofing debe ser aplicado en cualquier interfaz donde es posible determinar que tráfico puede llegar legítimamente .

En general, los filtros anti-spoofing pueden ser construidos con listas de acceso de entrada; esto es, los paquetes deben ser filtrados en las interfaces a través de las cuales llegan al *router*, no en las interfaces a través de las cuales salen del *router*. Esto se configura con el comando de configuración de interfaz **ip access-group** *list* **in**. Además, una lista de entrada protege al mismo *router* de ataques *spoofing*, mientras que una lista de salida protege solo a los dispositivos "atrás" del *router*.

Cuando existen listas de acceso anti-spoofing, estás deben siempre rechazar *datagramas* con broadcast o direcciones fuente multicast, y los *datagramas* con las direcciones reservadas "loopback" como una dirección fuente. Esto es usualmente apropiado para una lista de acceso anti-spoofing para filtrar salida de todos los ICMP redirigidos, sin importar la dirección fuente o destino. Los comandos adecuados pueden ser por ejemplo:

ip access-list number deny icmp any any redirect
ip access-list number deny ip host 127.0.0.0 0.255.255.255 any
ip access-list number deny ip 224.0.0.0 31. 255.255.255 any
ip access-list number deny ip host 0.0.0.0 any

4.3.5.2 Controlando broadcasts dirigidos

Los broadcast IP dirigidos son usados en el popular ataque de negación de servicio "*smurf*". En un ataque "*smurf*", los atacantes envían solicitudes ICMP de eco desde una dirección fuente falsificada a una dirección broadcast dirigida, causando que todos los *hosts* en la subred objetivo envíen replicas a la dirección fuente falsificada.

Un IP broadcast dirigido es un *datagrama* enviado a las direcciones broadcast de una subred por una máquina que no realiza el ataque. El broadcast dirigido sigue una ruta a través de la red como un paquete anycast hasta que este llega a la red objetivo, donde este es convertido en un broadcast de capa de enlace. De esta forma sólo el último *router* que se encuentra conectado directamente a la subred objetivo puede identificar el broadcast dirigido. Aunque los broadcast dirigidos son algunas veces usados como propósitos legítimos, no se usan comúnmente. Para

configurar una interfaz CISCO para que no reciba broadcast dirigidos se utiliza el comando **no ip directed-broadcast. no ip direct-broadcast** debe ser configurado en *cada* interfaz de *cada router* que esta conectado a una subred. El comando **no ip directed-broadcast** es el default en el software CISCO IOS versión 12.0 en adelante, en anteriores versiones, el comando debe ser aplicado a cada interfaz LAN.

Como se ha visto el *router* es una gran herramienta para la administración de una red, además de realizar su funcionamiento habitual de enrutado de paquetes, se puede utilizar como una línea de defensa eficiente, por lo que se le debe proporcionar seguridad, dado que si alguien entrar a él y asume privilegios podría dañar las redes a las cuales les da servicio.

Los *routers* que permiten la selección de paquetes ofrecen una manera de protección contra intrusos, por lo general son utilizados como primera línea de defensa contra una red no confiable. Esta defensa en contra de intrusos es mejorada con la utilización de dispositivos dedicados al monitoreo y rechazo de tráfico, así como software que permita el control de acceso.