Cómo de Cortafuegos y Servidor Proxy

Mark Grennan, mark@grennan.com

Este documento está diseñado para describir los fundamentos de los sistemas de cortafuegos, al mismo tiempo que le explica cómo instalar un filtro y un cortafuegos proxy en un sistema basado en Linux. La versión HTML de este documento se puede obtener en la siguiente dirección *http://www.grennan.com/Firewall-HOWTO.html*

1. Introducción

David Rudder escribió la versión original de este Cómo de Cortafuegos hace ya algún tiempo y, desde aquí, quiero agradecerle que me permita actualizar su trabajo.

También me gustaría dar las gracias a Ian Gough por ayudarme en el proceso de redacción.

Los cortafuegos han adquirido gran popularidad de un tiempo a esta parte y se consideran el último grito en la seguridad en Internet, pero como ocurre con la mayoría de los temas candentes, los cortafuegos a menudo han dado lugar a malentendidos. En este Cómo se explican las bases de lo que es un cortafuegos y de cómo se pueden instalar.

Hemos utilizado kernel 2.2.13 y RedHat 6.1 para desarrollar este Cómo, y los ejemplos que aquí se utilizan se basan, por lo tanto, en esta distribución. Si encuentra diferencias en la suya, por favor, póngase en contacto conmigo para actualizar este Cómo.

1.1. Retroalimentación

Cualquier apoyo o crítica a este documento serán bienvenidos. *¡POR FAVOR, RUEGO ME COMUNIQUEN CUALQUIER INEXACTITUD QUE VEAN EN ÉL!* No soy un experto, y puedo cometer errores. Si encuentra algún fallo, por favor, hágamelo saber. Intentaré responder a todos los correos electrónicos, pero soy una persona muy ocupada, así que no se enfade si no lo hago.

Mi dirección de correo electrónico es mark@grennan.com (mailto:mark@grennan.com)

1.2. Descargo de Responsabilidad

NO ME HAGO RESPONSABLE POR NINGÚN DAÑO PRODUCIDO POR ACCIONES DERIVADAS DE ESTE DOCUMENTO. Este documento pretende ser una introducción a los cortafuegos y los servidores proxy. No soy, ni lo pretendo ser, un experto en seguridad. Simplemente soy un tipo que ha leído mucho y al que le gustan los computadores más que al resto de la gente. Por favor, escribo esto esto para ayudar a la gente a entender más sobre este tema, y no estoy preparado para hacer depender mi vida de la exactitud de lo que hay aquí.

1.3. Propiedad Intelectual

A menos que se especifique lo contrario, los documentos Cómo de Linux son propiedad intelectual de sus respectivos autores. Estos documentos Cómo de Linux se pueden reproducir y distribuir total o parcialmente en cualquier medio, ya sea físico o electrónico, siempre y cuando aparezca la marca de propiedad intelectual en todas las copias. La redistribución comercial está permitida y, de hecho, se recomienda. No obstante, al autor le gustaría que se le notificara cualquier distribución de este tipo.

Todas las traducciones, trabajos derivados o trabajos de recopilación que incorporen cualquier documento Cómo de Linux deben llevar la marca de propiedad intelectual, es decir, no se puede producir ningún trabajo derivado de un Como y añadirle restricciones adicionales a su distribución. Se podrán establecer excepciones a estas normativas bajo ciertas condiciones. Por favor, contacte co nel coordinador de Cómo de Linux.

En resumen, deseamos promover la difusión de esta información por todos los canales posibles, pero nos gustaría mantener la propiedad intelectual de los Cómos. Por ello, rogamos se nos comunique cualquier intención de redistribución de los Cómos.

Si tiene alguna duda, por favor no dude en ponerse en contacto conmigo. (Véase arriba)

1.4. Las Razones por las que escribí esto

Hace varios años, mientras trabajaba para el estado de Oklahoma como Administrador de Internet, me pidieron que pusiera al Estado en Internet, sin presupuesto alguno. (Nota: En aquella época no había tal puesto de trabajo; simplemente era una persona que lo hacía todo). La mejor manera de conseguirlo era utilizar todos los "software" gratuitos y los "hardwares" que pudiera. Para ello contaba tan sólo con Linux y con algunos equipos 486 obsoletos.

Los cortafuegos comerciales tienen precios EXCESIVOS y la documentación que explica cómo funcionan se considera de alto secreto. Por lo tanto, crear un cortafuegos propio era una tarea casi imposible.

En el siguiente encargo, me pedían instalar un cortafuegos. Linux acababa de introducir un código de cortafuegos. De nuevo, sin presupuesto, empecé a diseñar un cortafuegos con Linux. Seis meses más tarde el cortafuegos ya estaba instalado y comencé a actualizar este documento.

1.5. Lecturas de Interés

- The The Linux Networking Overview HOWTO (http://sunsite.unc.edu/mdw/HOWTO/Networking-Overview-HOWTO.html)

- The Ethernet HOWTO (http://sunsite.unc.edu/mdw/HOWTO/Ethernet-HOWTO.html)
- IPchains Firewalling made Easy! (http://ipchains.nerdherd.org/)
- Linux Network Address Translation (http://www.linas.org/linux/load.html)
- The Net-3 HOWTO (http://sunsite.unc.edu/mdw/HOWTO/NET-3-HOWTO.html)
- The NET-PPP HOWTO (http://sunsite.unc.edu/mdw/HOWTO/PPP-HOWTO.html)
- The easiest way to create Virtual Tunnels over TCP/IP networks (http://vtun.netpedia.net/)

[Haga click aquí para acceder a otras URLS]

2. Cortafuegos: Conceptos básicos

Un cortafuegos es una barrera para evitar que el fuego se expanda. Los edificios disponen de cortafuegos, muros de ladrillos que dividen las diferentes secciones del edificio. En un coche, un cortafuegos es la barra de metal que separa al motor del compartimento de los pasajeros.

La misión de los cortafuegos de Internet es garantizar la seguridad de nuestro equipo ante los peligros cibernéticos de la red de área local (LAN) o bien, mantener a los miembros de esa LAN al margen de las malignas intenciones de Internet.

El primer cortafuegos en un ordenador fue una máquina Unix que no realizaba tareas de encaminamiento con conexiones a dos redes distintas.Una tarjeta de red conectada a Internet y la otra al LAN privado. Si quería acceder a Internet desde la red privada, tenía que registrarse en un servidor (Unix) de cortafuegos. Por lo tanto, se utilizaban los recursos del sistema para acceder a Internet. Por ejemplo, podría utilizar X-windows para ejecutar el navegador de Netscape con el sistema de cortafuegos y poder usarlo en una estación de trabajo. Con el navegador ejecutado en el cortafuegos se tiene acceso a dos redes.

Este tipo de sistema de origen dual (un sistema con dos conexiones de red) es muy bueno si tiene PLENA CONFIANZA en todos sus usuarios. Se puede instalar un sistema Linux y darle una cuenta a todo aquel que quiera tener acceso a Internet. Con esta instalación, el único computador de su red privada que conoce todo sobre el mundo exterior es el cortafuegos. Nadie puede descargar en su computador directamente. Primero deberá descargar el fichero al cortafuegos y después descargarlo del cortafuegos a sus estación de trabajo.

IMPORTANTE: El 99% de las instrusiones comienza con el acceso al sistema que se va a atacar. Por esta razón, no se recomienda este tipo de cortafuegos, además de que es muy limitado.

2.1. Políticas de Cortafuegos

No crea que lo único que necesita es una máquina de cortafuegos. *Establezca las políticas primero*.

Los cortafuegos se utilizan con dos objetivos:

1. para denegar el acceso a los piratas y gusanos
2. para permitir el acceso a empleados, niños, etc.

Cuando empecé a trabajar con los cortafuegos, me llamó la atención ver que la empresa estaba más interesada en espiar a sus empleados que en denegar a su red el acceso a los piratas.

Al menos en el estado de Oklahoma, los empleados tienen derecho a hacer llamadas telefónicas y acceder a Internet siempre y cuando se informa de ello a los encargados.

El Gran Hermano no es el gobierno. Gran Hermano = Gran Negocio.

No me malinterpreten. La gente debe trabajar, y no dedicarse a jugar durante las horas de trabajo. En mi opinión, se está dejando a un lado cada vez más la ética del trabajo. No obstante, también he observado que son los mismos encargados los primeros que no cumplen las normas. He visto trabajadores por hora que han sido reprendidos por utilizar Internet para buscar el recorrido del autobus del trabajo a casa, mientras que los mismos directores durante horas de trabajo se dedicaban a buscar buenos restaurantes y salas de fiesta para llevar a sus futuros clientes.

Mi error antes este tipo de abusos es publicar un acceso a cortafuegos en una página web para que todo el mundo lo pueda leer.

La cuestión de la seguridad puede ser escalofriante. Si es usted un administrador de cortafuegos, cúbrase las espaldas.

2.1.1. Cómo crear una política de seguridad

Hay muchos artículos en los que se explica cómo crear una política de seguridad. Después de muchos años de experiencia, les puedo recomendar que no se fíen en absoluto. Crear una política de seguridad es algo muy simple:

1. describa para qué es el servicio
2. describa el grupo de personas a las que va dirigido el servicio
3. describa a qué servicio necesita acceder cada grupo
4. describa, para cada grupo de servicio, cómo se puede mantener seguro el servicio
5. redacte un informe en el que se considere violación cualquier otro tipo de acceso

Esta política se irá haciendo cada vez más compleja, no intente abarcar demasiado en este punto. Procure que sea sencilla y clara.

2.2. Tipos de Cortafuegos

Hay dos tipos de cortafuegos.

1. Cortafuegos de filtrado - que evitará el acceso no autorizado a determinados paquetes de la red.
2. Sevidores Proxes (a veces llamados cortafuegos) - encargados de establecer las conexiones a la red.

2.2.1. Cortafuegos de Filtrado de Paquetes

El Filtrado de Paquetes es el tipo de cortafuegos integrado en el núcleo de Linux.

Un cortafuegos de filtrado trabaja a nivel de red. Los datos salen del sistema sólo si las reglas del cortafuegos se lo permiten. Cuando los paquetes llegan son filtrados atendiendo al protocolo utilizado, la dirección fuente y destino, y la información que sobre el puerto viene contenida en cada paquete.

Muchos encabezamientos de la red tienen la posibilidad de desarrollar servicios cortafuegos. Los cortafuegos de filtrado nos lo podemos imaginar como un tipo de encaminador. Por este motivo usted necesita tener un profundo conocimiento de la estructura de paquete IP para trabajar con uno.

Puesto que son muy pocos los datos que se analizan y registran, los cortafuegos de filtrado de paquetes requieren menos CPU y crean menos latencia en su red.

Los cortafuegos de filtrado no preven los controles mediante el uso de contraseña. Los usuarios no se identifican a sí mismos. Lo único que identifica a un usuario es el número IP asignado a su estación de trabajo. Esto puede convertirse en un problema is usted tiene la intención de usar DHCP (Dynamic IP assignments). Esto se debe a que las reglas se basan en los números IP que tendrá que ajustar a las reglas cuando se asignen los nuevos números IP. Desconozco la forma de automatizar este proceso.

Los cortafuegos de filtrado resultan más transparentes para el usuario, que no tiene que establecer reglas en sus aplicaciones para acceder a Internet. No sucede los mismo con la mayoría de los servidores proxy.

2.2.2. Servidores Proxy

Este tipo de servidores se usa principalmente para controlar, o supervisar, el tráfico hacia el exterior. Algunos proxy de aplicación ocultan los datos solicitados. Esto reduce el ancho de banda así como el acceso a los mismos datos al siguiente usuario. Ofrece una inequívoca prueba de lo que fue transferido.

Existen dos tipos de servidores proxy

1. Servidores Proxy de Aplicación - son los que hacen el trabajo por usted.
2. Servidores Proxy SOCKS - establecen conexiones entre puertos.

2.2.3. Sevidor Proxy de Aplicación

El mejor ejemplo es el de una persona que se comunica con otro computador y, desde allí, establece contacto con el mundo exterior. Con un servidor proxy de aplicación el proceso se automatiza. Cuando usted se comunica con el mundo exterior el cliente le envía primero al servidor proxy. El servidor proxy establece la comunicación con el servidor que ha solicitado (el mundo exterior) y le devuelve los datos.

Los servidores proxy se encargan de manejar todas las comunicaciones, característica que le permite registrar todo lo que ellos (usted) haga. Los servidores proxy HTTP (web) tienen muy en cuenta las URL que ellos o usted visiten. Los proxy FTP incluyen cada fichero que usted descargue. Incluso pueden filtrar las palabras inapropiadas de los sitios que visite o escanear esos lugares en busca de virus.

Los servidores proxy de aplicación pueden autenticar a los usuarios. Antes de establecer una conexión con el exterior, el servidor le puede pedir que se identifique primero. A un usuario de la red le pediría una identificación para cada sitio que visite.

2.2.4. Servidor Proxy SOCKS

Un servidor proxy SOCKS se parece bastante a un panel de conmutación. Tan sólo establece la conexión entre su sistema y otro sistema externo.

La mayoría de los servidores SOCKS presentan el inconveniente de que sólo trabajan con conexiones del tipo TCP y como cortafuegos no suministran autenticación para los usuarios. Sin embargo, su ventaja es que registran los sitios a los que cada usuario se ha conectado.

3. Arquitectura Cortafuegos

Existen muchas maneras de estructurar su red para proteger su sistema mediante el uso de un cortafuegos

Si tiene una conexión exclusiva para Internet a través de un encaminador, podría conectarlo directamente a su sistema cortafuegos o podría pasar por un núcleo para proporcionar a los servidores que se encuentran fuera del cortafuegos un acceso completo.

3.1. Arquitectura Conmutada

Si usa un servicio conmutado como una línea ISDN, se podría usar una tercera tarjeta de red que permita disponer de una red perimétrica (DMZ). Esto proporciona un control absoluto sobre los servicios de Internet, manteniéndolos separados de la red regular.

__________ _/__/_ | | ________________ | | | Cortafuegos | (LAN) | | / Internet \----| Sistema |--(HUB)--| Estación/ones de trabajo | _ _ _ _/ |__________| |________________| \/ \/ \/ | (DMZ) (HUB)

3.2. Arquitectura de Encaminador Único

En el encaminador existe la posibilidad de establecer algunas reglas estrictas para el filtro, siempre y cuando haya un encaminador o un módem de cable entre usted e Internet y usted sea el propietario del encaminador. Si el propietario del encaminador es su ISP y, en este caso, no tiene los controles que necesita, puede pedir a su ISP que agregue los filtros.

__________ ___________ _/__/_ | Encaminador | | | ________________ | | | o | (DMZ) | Cortafuegos | (LAN) | | / Internet \----|Módem de Cable|--(HUB)--| Sistema |--(HUB)--| Estación/ones de trabajo | _ _ _ _/ |__________| | | |___________| | |________________| \/ \/ \/ | (Externo) (Servidor)

3.3. Cortafuegos con Servidor Proxy

Si tiene que controlar por dónde se mueven los usuarios de su red, la cual es pequeña, puede integrar un servidor proxy en su cortafuegos. Algunas veces, los ISP lo hacen para confeccionar una lista de interés de sus usuarios con el fin de revenderlas a agencias de marketing.

___________ _/__/_ | Proxy / | ________________ | | | Cortafuegos | (LAN) | | / Internet \----| Sistema |--(HUB)--| Estación/ones de trabajo | _ _ _ _/ |___________| |________________| \/ \/ \/

Si lo prefiere, puede integrar el servidor proxy en su LAN, en cuyo caso, el cortafuegos debe poseer unas órdenes que hagan posible que el servidor proxy sólo se conecte a Internet para aquellos servicios que ofrece. De esta manera, los usuarios sólo podrán acceder a Internet a través del proxy.

___________ _/__/_ | | ________________ | | | Cortafuegos | (LAN) | | / Internet \----| Sistema |--(HUB)--| Estación/ones de trabajo | _ _ _ _/ |___________| | |________________| \/ \/ \/ | _______________ | | | +----| Servidor Proxy | |_______________|

3.4. Configuración Redundante de Internet

Si va a ejecutar un servicio como YAHOO o, tal vez, SlashDot, puede que desee compilar un programa multimódulo en su sistema empleando encaminadores redundantes y cortafuegos. (Vea el Cómo de Alta Disponibilidad.)

Mediante la utilización de técnicas de circuito cíclico DNS para dar acceso a varios servidores web desde una URL y varios ISP, es posible crear un servicio de funcionamiento óptimo del 100% con encaminadores y cortafuegos que usan técnicas de alta disponibilidad.

_/__/_ _/__/_ | | | | / ISP #1 ______ (WAN)_____/ Combinaciones \ _ _ _ _/ |
(HUB) _ _ _ _/ \/ \/ \/ | ___|____ \/ \/ \/ __|___ |_______ | _/__/_ |_____ |
|Cortafuegos|| ______ | | | || (DMZ) | Sistema || (LAN) | | / ISP #2
\--|Encaminador||--(HUB)--| (VPN) ||--(HUB)--| ET/s | _ _ _ _/ |______| | |________| |
|______| \/ \/ \/ | | | ______ | (Externo) (Compartido) | | | ------ | (Servidor) (Servidor)
+----|Proxy | | ET/s | | |______| | VPN |-+ |______|

Es muy fácil que la red se le vaya de las manos. Verifique cada conexión. Todo lo que necesita es un usuario con su módem para comprometer su LAN.

4. Instalación del Cortafuegos Filtrado de Linux

4.1. Requerimientos del Hardware

Los cortafuegos filtrados no requieren de un hardware muy sofisticado. Son poco más que simples encaminadores.

Todo lo que necesita es:

1. un 486-DX66 con 32 megas de memoria RAM
2. un disco 250m (se recomienda uno de 500)

3. conexiones a la red (tarjetas LAN, puertos serie, ¿inalámbricos?)
4. monitor y teclador

Algunos sistemas que usan una consola con puerto serie pueden, incluso, prescindir del monitor y del teclado.

Si necesita un servidor proxy que soporte mucho tráfico, debería conseguir el sistema más completo que pueda permitirse. Esto se debe a que cada vez que un usuario se conecta al sistema, éste creará otro proceso.Si tuviese 50 o más usuarios fijos, estimo que necesitará:

1. un Pentium II con 64 megas de memoria
2. un disco duro con dos gigas para almacenar todas las operaciones de registro
3. dos conexiones a la red
4. un monitor y un teclado

Las conexiones a la red pueden ser de cualquier tipo (tarjetas NIC, ISDN, modems compatibles).

5. Requerimientos del Software

5.1. Selección del Núcleo

Para crear un cortafuegos de filtrado no es necesario ningún software especial. Linux lo hará. En el momento de escribir este Cómo, estoy usando RedHat 6.1.

La construcción en Linux del cortafuegos ha cambiado varias veces. Si está utilizando un núcleo antiguo de Linux (1.0.x o anterior) hágase con una nueva copia. Los más antiguos usaban ipfwadm de *http://www.xos.nl/linux/ipfwadm/* y ya no los admite.

Si está usando 2.2.13 o superior, estará usando ipchaining, que aparecía en *http://www.rustcorp.com/linux/ipchains/*

Si está utilizando el núcleo más reciente 2.4, hay una nueva utilidad de cortafuegos con más características. Pronto escribiré sobre ello.

5.2. Selección de un Servidor Proxy

Si desea establecer un servidor proxy, necesitará uno de estos dos paquetes:

1. Squid
2. El TIS Firewall Toolkit (FWTK)
3. SOCKS

Squid es un gran paquete y trabaja con el característico Proxy Transparente de Linux. Le indicaré cómo instalar este servidor.

En el momento de redactar este Cómo, han aparecido Network Associates (http://www.networkassociates.com/) y Trusted Information System's (TIS). Así que manténgase atento a los sitios web para ver más información sobre Tool Kit puede aún ser descargado desde*http://www.tis.com/research/software/*

Trusted Information System saca a la luz una colección de programas diseñados para facilitar la creación de cortafuegos. Con este toolkit, usted instala un demonio para el servicio (WWW, telnet ect.) que esté usando en cada momento.

6. Preparación del Sistema Linux

Instale tan sólo lo imprescindible del sistema Linux. Mi instalación comenzó con la configuración del servidor y luego desactivé todos los servicios en /etc/inetd.conf. Para más seguridad, deberá desinstalar los servicios innecesarios.

Puesto que la mayoría de las distribuciones no disponen de un núcleo que se adapte a sus necesidades, será preciso que compile su propio núcleo. Lo mejor será hacerlo con otro computador que no sea el cortafuegos. Si usted ha instalado un compilador C y otras utilidades en su cortafuegos, desinstálelos después de completar la configuración del núcleo.

6.1. Compilación del núcleo

Comience con una instalación mínima de su distribución Linux. Cuantos menos programas cargue, menos agujeros, puertas traseras o fallos introducirán problemas de seguridad en su servidor.

Use un núcleo estable. Yo uso el núcleo 2.2.13 en mi sistema, por lo que esta documentación se basa en la instalación en ese núcleo.

Necesitará recompilar el núcleo Linux con las opciones apropiadas. Si usted no ha recompilado antes su núcleo, lea el Cómo Núcleo, el Cómo Ethernet, y el Cómo NET-2.

Aquí tiene la configuración relativa a la red en la que trabajo. He marcado algunas líneas con ?. Si usted usa esta aplicación, actívela también.

Yo uso "make menuconfig" para editar la configuración de mi núcleo.

<*> Packet socket [ ] Kernel/User netlink socket [*] Network firewalls [ ] Socket Filtering <*> Unix domain sockets [*] TCP/IP networking [ ] IP: multicasting [*] IP: advanced router [ ] IP: kernel level autoconfiguration [*] IP: firewalling [?] IP: always defragment (required for masquerading) [?] IP: transparent proxy support [?] IP: masquerading --- Protocol-specific masquerading support will be built as modules. [?] IP: ICMP masquerading --- Protocol-specific masquerading support will be built as modules. [ ] IP: masquerading special modules support [*] IP: optimize as router not host < > IP: tunneling < > IP: GRE tunnels over IP [?] IP: aliasing support [*] IP: TCP syncookie support (not enabled per default) --- (it is safe to leave these untouched) < > IP: Reverse ARP [*] IP: Allow large windows (not recommended if <16Mb of memory) < > The IPv6 protocol (EXPERIMENTAL) --- < > The IPX protocol < > Appletalk DDP < > CCITT X.25 Packet Layer (EXPERIMENTAL) < > LAPB Data

Link Driver (EXPERIMENTAL) [ ] Bridging (EXPERIMENTAL) [ ] 802.2 LLC (EXPERIMENTAL) < > Acorn Econet/AUN protocols (EXPERIMENTAL) < > WAN router [ ] Fast switching (read help!) [ ] Forwarding between high speed interfaces [ ] PU is too slow to handle full bandwidth QoS and/or fair queueing --->

Después de realizar la configuración que usted necesita, deberá recompilar, reinstalar el núcleo y reiniciar.

Use la orden:

make dep;make clean;make bzlilo;make modules;make modules_install;init 6 to accomplish all of this in one step.

6.2. Configuración de dos tarjetas de red

Si su ordenador dispone de dos tarjetas de red, necesitará añadir una línea adicional a su fichero /etc/lilo.conf para describir el IRQ y la dirección de ambas tarjetas. La línea adicional será similar a ésta:

append=ether=12,0x300,eth0 ether=15,0x340,eth1

6.3. Configuración de las Direcciones de Red

Ahora comienza la parte divertida de la instalación. No entraré en detalles sobre cómo instalar una LAN, para ello, lea el Cómo Networking.

Nuestro objetivo es disponer de dos conexiones a red para su sistema de filtro cortafuegos. Uno en el lado de Internet (el lado inseguro) y el otro en el LAN (el lado seguro).

De todas formas, tendrá que tomar decisiones.

1. ¿Usará un número IP real o realizará alguno para su LAN?
2. ¿Su ISP asignará el número o usará números IP fijos?

Si lo que usted quiere es que desde Internet no se pueda acceder a su red privada, no deberá utilizar direcciones reales, simplemente cree direcciones para su LAN privada. Esto no es muy recomendable, porque si los datos salen de su LAN, podrían terminar en el puerto de otro sistema.

Existe un rango de números de dirección para Internet destinado a redes privadas. Este rango es 192.168.1.xxx, el mismo que usaremos en nuestros ejemplos.

Para ello necesitará usar la máscara IP. Con este proceso, el cortafuegos enviará paquetes y los traducirá a una dirección IP REAL para navegar por Internet.

Usando una dirección IP sin ruta, su red será más segura. Los encaminadores de Internet no pasarán paquetes con estas direcciones.

Llegado este punto puede resultar aconsejable que lea el Cómo IP Masquering.

24.94.1.123 __________ 192.168.1.1 _/__/_ \ | | / _______________ | | \| Cortafuegos |/ | | / Internet \--------| Sistema |------------| Estación/ones de trabajo | _ _ _ _/ |__________| |_______________| \/ \/ \/

Deberá tener una dirección IP real para asignarle su tarjeta IP de red. Esta dirección le podrá ser asignada permanentemente. (Una dirección IP fija) o se le podrá asignar un tiempo de corrección a la red por el proceso PPP.

Elija el número IP interno. Por ejemplo, 192.168.1.1 a la tarjeta LAN. Esta será su dirección IP de puerta de enlace. De la misma forma, se podrá asignar a los demás computadores de la red protegida (LAN) un número del rango 192.168.1.xxx. (192.168.1.2 hasta 192.168.1.254)

Yo uso RedHat Linux para configurar la red y añado un fichero ifcfg-eth1 en el directorio /etc/sysconfig/network-scripts. También podrá encontrar un fichero ifcfg-ppp0 o ifcfg-tr0 en este directorio. Estos ficheros 'ifcfg-' se usan en RedHat para configurar y desactivar los dispositivos de red al reiniciar el equipo, y se ejecutan después de la conexión. Se nombran después del tipo de conexión.

Aquí mostramos el fichero ifcfg-eth1 (segunda tarjeta ehternet) como ejemplo;

DEVICE=eth1 IPADDR=192.168.1.1 NETMASK=255.255.255.0

NETWORK=192.168.1.0 BROADCAST=192.168.1.255 GATEWAY=24.94.1.123 ONBOOT=yes

Si usa una conexión conmutada, necesitará ver los ficheros ifcfg-ppp0 y chat-ppp0, quecontrolan su conexión PPP.

El fichero ifcfg debe tener un aspecto parecido al siguiente:

DEVICE=ppp0 ONBOOT=yes USERCTL=no MODEMPORT=/dev/modem LINESPEED=115200 PERSIST=yes DEFABORT=yes DEBUG=yes INITSTRING=ATZ DEFROUTE=yes HARDFLOWCTL=yes ESCAPECHARS=no PPPOPTIONS= PAPNAME=LoginID REMIP= NETMASK= IPADDR= MRU= MTU= DISCONNECTTIMEOUT= RETRYTIMEOUT=5 BOOTPROTO=none

6.4. Comprobando su Red

Empiece usando las órdenes ifconfig y route. Si usted tiene dos tarjetas de red ifconfig, deberá presentar un aspecto similar a éste:

#ifconfig lo Link encap:Local Loopback inet addr:127.0.0.1 Mask:255.0.0.0 UP LOOPBACK RUNNING MTU:3924 Metric:1 RX packets:1620 errors:0 dropped:0 overruns:0 TX packets:1620 errors:0 dropped:0 overruns:0 collisions:0 txqueuelan:0 eth0 Link encap:10Mbps Ethernet HWaddr 00:00:09:85:AC:55 inet addr:24.94.1.123 Bcast:24.94.1.255 Mask:255.255.255.0 UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1 RX packets:1000 errors:0 dropped:0 overruns:0 TX packets:1100 errors:0 dropped:0 overruns:0 collisions:0 txqueuelan:0 Interrupt:12 Base address:0x310 eth1 Link encap:10Mbps Ethernet HWaddr 00:00:09:80:1E:D7 inet addr:192.168.1.1 Bcast:192.168.1.255 Mask:255.255.255.0 UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1 RX packets:1110 errors:0 dropped:0 overruns:0 TX packets:1111 errors:0 dropped:0 overruns:0 collisions:0 txqueuelan:0 Interrupt:15 Base address:0x350

y su tabla de encaminado similar a:

#route -n Kernel routing table Destination Gateway Genmask Flags MSS Window Use Iface 24.94.1.0 * 255.255.255.0 U 1500 0 15 eth0 192.168.1.0 * 255.255.255.0 U 1500

0 0 eth1 127.0.0.0 * 255.0.0.0 U 3584 0 2 lo default 24.94.1.123 * UG 1500 0 72 eth0

Nota: 24.94.1.0 se encuentra en lado de Internet del cortafuegos y 192.168.1.0 en el lado de la red privada (LAN).

Asegúrese de que todos los computadores de su LAN puedan conectar con la dirección interna de su sistema cortafuegos. (192.168.1.1 en este ejemplo) Si no conectan, vuelva al Cómo NET-2 y trabaje en la red un poco más.

Luego, desde el cortafuegos, trate de conectar con Internet. Yo uso www.internic.net com página de prueba. Si no funciona, inténtelo con un servidor de su ISP. Si aún así no funciona, es que alguna parte de su conexión a Internet es errónea. Desde el cortafuegos, debería poder conectarse a cualquier direcció de Internet. Trate de revisar la configuración de su puerta de enlace por defecto. Si usted usa una conexión conmutada, revise su nombre (ID) y contraseña (Password), relea el Cómo Net-2, e inténtelo de nuevo.

A continuación, trate de conectar con la dirección externa del cortafuegos (24.94.1.123) desde el computador de su LAN. Esto no debería ser posible, pero si lo consigue es que la máscara o el IP Forwarding están activados, o que ya se han filtrado grupos de paquetes. Apague los equipos e inténtelo de nuevo, puesto que necesita saber si el filtro está activo.

Para núcleos posteriores al 2.1.102 pueder usar la orden;

echo "0" > /proc/sys/net/ipv4/ip_forward

Si usa un núcleo anterior (WHY), necesitará recompilar su núcleo con el reenvío de paquetes apagado. (Simplemente actualícelo)

Intente conectar de nuevo con la dirección externa del cortafuegos (24.94.1.123). Ahora no debería conseguirlo.

Conecte a continuación el reenvío de paquetes o la máscara. Debería ser capaz de conectar con cualquier página de Internet desde cualquier equipo de su LAN.

echo "1" > /proc/sys/net/ipv4/ip_forward

NOTA IMPORTANTE: Si usted usa una dirección IP REAL (que no sea 192.168.1.*) y no puede conectar con Internet, pero PUEDE hacerlo desde el lado de Internet del cortafuegos, asegúrese de que su IPS enviando paquetes por la dirección de su red privada.

Una manera de comprobarlo es que algún amigo, usando un proveedor local, se conecte con su red. Si la conexión se detiene en su encaminador, entonces no permiten la entrada de información.

¿Funciona? Estupendo. La parte más difícil ha terminado.

6.5. Protección del Cortafuegos

Un cortafuegos es inútil si el sistema en el que está instalado es vulnerable a ataques externos. Un chico malo podría acceder desde un servicio sin cortafuegos y modificar el sistema según sus propias necesidades. Usted tendrá que desactivar cualquier servicio innecesario.

Mire el fichero /etc/inetd.conf Con él se configurará el inetd, también llamado super servidor, que controla varios servidores demonio y los inicia, cuando se requiere, por un paquete que llega a un puerto bien conocido.

Deberá desactivar cualquier eco, discard, daytime, chargen, ftp, gopher, shell, login, exec, talk, ntalk, pop-2, pop-3, netstat, systat, tftp, bootp, finger, cfinger, time, swat que tenga en su cortafuegos.

Para apagarlo, ponga # como primer carácter de la línea de servicio. Una vez hecho esto, envíe un SIG-HUP al proceso mediante la orden *kill -HUP <pid>*, donde <pid> es el número de preocesos de inetd. Con esto, el inetd se releerá su fichero de configuractión (inetd.conf) y reiniciará el equipo sin apagar el sistema.

Compruébelo con una emulación en el puerto 15 (netstat) de su cortafuegos. Si se produce una salida, no ha desactivado todos los servicios.

El sistema local de telnet 19

Usted también puede crear el fichero /etc/nologin. Escriba unas cuantas líneas de texto en el Cómo (BUZZ OFF). Una vez creado el fichero, la entrada de identificación no permitirá la conexión al usuario. Podrá ver los contenidos de este fichero pero no podrá conectar. Sólo la raíz puede hacerlo.

También puede editar el fichero /etc/securetty. Si el usuario es raíz, entonces la entrada de identificación debe estar registrada en un listado tty en /etc/securetty. Los errores se registrarán en la utilidad syslog. Con estas dos medidas activadas, la única manera de conectar con el cortafuegos será desde la consola raíz.

NUNCA REALICE LA EMULACIÓN de un sistema que SEA RAÍZ. Si necesita realizar acceso remoto a la raíz SSH (Secure Shell), tendrá que desconectar el emulador.

Si es usted realmente un paranoico tendrá que usar el "lids" (Linux Intrusion Detect System), un parche para el núcleo de Linux que detecta cualquier intrusión en el sistema; el "lids" protege ficheros importantes impidiendo su modificación. Una vez activado, nadie (including root) puede modificar ficheros, directorios o subdirectorios, a menos que reinicie el sistema con el fichero de seguridad=1 LILO, especialmente concebido para modificar ficheros protegidos. (Deberá iniciarse el equipo en el modo de usuario único).

7. Instalación de Filtros IP (IPFWADM)

Si está usando el núcleo 2.1.102 o uno más reciente, vaya directamente a la sección sobre cadenas IPCHAINS.

En versiones anteriores al reenvío de paquetes IP se activa por defecto en el núcleo y, por eso, su red deberá comenzar denegándole el acceso a todo y purgando cualquier orden ipfw que fuera ejecutada por últimas vez. Este fragmento del guión debe entrar en el de arranque de red. (/etc/rc.d/init.d/network)

setup IP packet Accounting and Forwarding # # Forwarding # # By default DENY all services ipfwadm -F -p deny # Flush all commands ipfwadm -F -f ipfwadm -I -f ipfwadm -O -f

Este es el último cortafuegos y nada podrá atravesarlo.

Ahora cree el fichero /etc/rc.d/rc.firewall. This script should allow email, Web and DNS traffic through. ;-)

#! /bin/sh # # rc.firewall # # Source function library. . /etc/rc.d/init.d/functions # Get config. . /etc/sysconfig/network # Check that networking is up. if [${NETWORKING} = "no"] then exit 0 fi case "$1" in start) echo -n "Starting Firewall Services: " # Allow email to got to the server /sbin/ipfwadm -F -a accept -b -P tcp -S 0.0.0.0/0 1024:65535 -D 192.1.2.10 25 # Allow email connections to outside email servers /sbin/ipfwadm -F -a accept -b -P tcp -S 192.1.2.10 25 -D 0.0.0.0/0 1024:65535 # Allow Web connections to your Web Server /sbin/ipfwadm -F -a accept -b -P tcp -S 0.0.0.0/0 1024:65535 -D 192.1.2.11 80 # Allow Web connections to outside Web Server /sbin/ipfwadm -F -a accept -b -P tcp -S 192.1.2.* 80 -D 0.0.0.0/0 1024:65535 # Allow DNS traffic /sbin/ipfwadm -F -a accept -b -P udp -S 0.0.0.0/0 53 -D 192.1.2.0/24 ;; stop) echo -n "Stooping Firewall Services: " ipfwadm -F -p deny ;; status) echo -n "Now do you show firewall stats?" ;; restart|reload) $0 stop $0 start ;; *) echo "Usage: firewall {start|stop|status|restart|reload}" exit 1 esac

NOTA: En este ejemplo tenemos el servidor de e-mail (smtp) ejecutándose en el 192.1.2.10, el cual debe ser capaz de recibir y enviar al puerto 25 (servidor web ejecutándose en el 192.1.2.11). Así, estamos permitiendo a cualquiera en el LAN acceder a redes externas y servidores DNS.

Sin embargo, esto no es muy seguro, ya que el puerto 80 no tiene que usarse como puerto de web, pues un hacker habilidoso podría usar este puerto para crear una red virtual privada (VPN) a través del cortafuegos. La forma de evitar esto es instalar una web proxy y sólo permitir actuar al proxy a través del cortafuegos. Así, los usuarios de LAN tendrían que atravesar el proxy para acceder a servidores de web externos.

Usted podrá estar interesado en eliminar tráfico a través de su cortafuegos. Este guión contabilizará cualquier paquete y usted podrá añadir una o dos líneas para eliminar los paquetes destinados a un único sistema.

Flush the current accounting rules ipfwadm -A -f # Accounting /sbin/ipfwadm -A -f /sbin/ipfwadm -A out -i -S 192.1.2.0/24 -D 0.0.0.0/0 /sbin/ipfwadm -A out -i -S 0.0.0.0/0 -D 192.1.2.0/24 /sbin/ipfwadm -A in -i -S 192.1.2.0/24 -D 0.0.0.0/0 /sbin/ipfwadm -A in -i -S 0.0.0.0/0 -D 192.1.2.0/24

Si todo lo que usted necesita es un cortafuegos de filtro, puede parar aquí. Pruébelo y disfrútelo.

8. Instalación de Filtros IP (IPCHAINS)

Ipchains es una nueva versión del código cortafuegos en Linux IPv4 y de ipfwadm, que, según creo, deriva del código de filtrado en BSD (ipfw). Para poder administrar los filtros de paquete IP en Linux, se requiere una versión del núcleo 2.1.102 o superior.

Las limitaciones del código de filtrado BSD (ipfw) son que no trabaja con fragmentos, tiene contadores de 32 bits (al menos en Intel), sólo puede manejar los protocolos TCP, UDP o ICMP, no permite hacer grandes cambios de forma automática, no permite especificar reglas inversas, presenta algunas anomalías, y, sin embargo, puede servir para gestionar (aunque es más fácil que se comentan errores). Al menos, eso es lo que dice el autor.

En realidad, no voy a profundizar sobre cómo controlar un cortafuegos IPChains, porque sobre ello ya existe un ¡GRAN! Cómo en la dirección http://www.rustcorp.com/linux/ipchains/HOWTO.html. I'd just end up duplicating it here. Here are the basics.

Empieza con tres listas de reglas denominadas "chains" (cadenas): input, output y forward, que no se pueden borrar. Usted mismo puede crear cadenas y, entonces, las reglas pueden ser insertadas o eliminadas desde ese conjunto de reglas.

Las operaciones para trabajar con cadenas completas son:

1. Crear una nueva cadena (-N).
2. Borar un cadena vacía (-X).
3. Cambiar la política por defecto de una cadena (-P).
4. Listar las reglas contenidas en una cadena (-L).
5. Vaciar una cadena eliminando las reglas que contiene (-F).
6. Poner a cero los contadores de bytes y de paquetes en todas las reglas de una cadena (-Z).

Existen varias formas de maninpular las reglas de una cadena:

1. Añadir una nueva reglas a una cadena ya existente (-A).
2. Insertar una nueva reglas en una posición determinada en una cadena (-I).
3. Reemplazar la regla que ocupa una posición determinada en una cadena (-R).
4. Eliminar la regla que ocupa una posición determinada en una cadena (-D).
5. Eliminar la primera regla igual a la especificada de entre todas las reglas de una cadena (-D).

También hay algunas operaciones relativas al enmascaramiento IP, a falta de un lugar mejor donde colocarlas:

1. Ver una lista de todas las conexiones actuales que están siendo enmascaradas (-M -L).
2. Establecer el tiempo de espera máximo para una conexión enmascarada (-M -S).

Hay algunos elementos de la temporalización que pueden alterar las reglas del cortafuegos; por ello, si no es usted cuidadoso, podría dejar pasar algún paquete mientras realiza los cambios. Una aproximación simple es hacer lo siguiente:

ipchains -I input 1 -j DENY # ipchains -I output 1 -j DENY # ipchains -I forward 1 -j DENY

... hacer los cambios ...

ipchains -D input 1 # ipchains -D output 1 # ipchains -D forward 1

Esto evitará que entren paquetes mientras usted esté realizando los cambios.

Aquí le presento un duplicado de las reglas del cortafuegos anterior en una IPChains.

#!/bin/sh # # rc.firewall # ## Flush everything, start from scratch /sbin/ipchains -F input /sbin/ipchains -F output /sbin/ipchains -F forward ## Redirect for HTTP Transparent Proxy #$IPCHAINS -A input -p tcp -s 192.1.2.0/24 -d 0.0.0.0/0 80 -j REDIRECT 8080 ## Create your own chain /sbin/ipchains -N my-chain # Allow email to got to the server

/sbin/ipchains -A my-chain -s 0.0.0.0/0 smtp -d 192.1.2.10 1024:-j ACCEPT # Allow email connections to outside email servers /sbin/ipchains -A my-chain -s 192.1.2.10 -d 0.0.0.0/0 smtp -j ACCEPT # Allow Web connections to your Web Server /sbin/ipchains -A my-chain -s 0.0.0.0/0 www -d 192.1.2.11 1024: -j ACCEPT # Allow Web connections to outside Web Server /sbin/ipchains -A my-chain -s 192.1.2.0/24 1024: -d 0.0.0.0/0 www -j ACCEPT # Allow DNS traffic /sbin/ipchains -A my-chain -p UDP -s 0.0.0.0/0 dns -d 192.1.2.0/24 -j ACCEPT ## If you are using masquerading # don't masq internal-internal traffic /sbin/ipchains -A forward -s 192.1.2.0/24 -d 192.1.2.0/24 -j ACCEPT # don't masq external interface direct /sbin/ipchains -A forward -s 24.94.1.0/24 -d 0.0.0.0/0 -j ACCEPT # masquerade all internal IP's going outside /sbin/ipchains -A forward -s 192.1.2.0/24 -d 0.0.0.0/0 -j MASQ ## Deny everything else /sbin/ipchains -P my-chain input DENY

No se detenga aquí. Este cortafuegos no es muy grande y estoy seguro de que usted tiene otros servicios que le pueden ayudar. Por ello, lea de nuevo el Cómo IPCHAINS.

9. Instalación de un Servidor Proxy SQUID Transparente

El servidor proxy squid está disponible en *http://squid.nlanr.net/*.

Los desarrolladores SQUID incluyen los paquetes RedHat y Debian. Si quiere, use uno de ellos.

10. Instalación del Servidor Proxy TIS

10.1. Cómo conseguir el Software

El TIS FWTK se puede conseguir en *http://www.tis.com/research/software/ (http://www.tis.com/research/software/)*.

No cometa el mismo error que yo cometí. Cuando transfiera los archivos desde TIS, LEA EL APARTADO "LÉAME". El TIS fwtk se encuentra bloqueado en un directorio oculto de su servidor.

TIS requiere que lea sus condiciones en http://www.tis.com/research/software/fwtk_readme.html (http://www.tis.com/research/software/fwtk_readme.html) y luego *envíe un e-mail a fwtk-request@tislabs.com (mailto:fwtk-request@tislabs.com)* con la palabra *accepted* en el cuerpo del mensaje para conocer el nombre del directorio oculto. No es necesario que escriba ningún asunto en el mensaje. Posteriormente, su sistema le enviará el nombre del directorio (válido durante 12 horas) para descargar la fuente.

La versión 2.1. del FWTK resulta más fácil de compilar que cualquier versión previa.

10.2. Compilación del TIS FWTK

La versión 2.1 del FWTK se compila mucho más fácilmente que cualquiera de las versiones anteriores.

¡EXPLICAR AQUÍ!

Ejecute *make* ahora.

10.3. Instalación del TIS FWTK

Ejecute *make install*.

El directorio de la instalación por defecto es /usr/local/etc. Podría cambiarlo a un directorio más seguro. Yo opté por cambiar el acceso a este directorio por ’chmod 700’.

Por último, sólo queda configurar el cortafuegos.

10.4. Configuración del TIS FWTK

Ahora es cuando realmente empieza lo divertido. Debemos enseñar al sistema a denominar a estos nuevos servicios y a crear las tablas para controlarlos.

No voy a intentar rescribir aquí el manual de TIS FWTK. Le mostraré la configuración que encontré hecha y explicaré los problemas que me surgieron y cómo los solucioné.

Los archivos que componen estos controles son tres:

- /etc/services
  - Le dice al sistema en qué puertos se encuentra un servicio.
- /etc/inetd.conf
  - Le dice a inetd a qué programa llamar cuando alguien intenta conectarse a un puerto de servicio.
- /usr/local/etc/netperm-table
  - Le dice a los servicios FWTK a quién admitir y a quién denegar el servicio.

Para conseguir que el FWTK funcione, debe editar estos archivos de abajo hacia arriba. Editar el archivo de servicios sin haber configurado correctamente el archivo inetd.conf o netperm-table, podría hacer su sistema inaccesible.

10.4.1. El fichero netperm-table

Este archivo controla quién puede acceder a los servicios del TIS FWTK. Debería pensar en el tráfico y usar el cortafuegos desde ambos lados. La gente que se encuentre fuera de su red debería identificarse antes de poder tener acceso, y la que se encuentre dentro podría acceder directamente.

Para que la gente pueda identificarse, el cortafuegos utiliza un program llamado *authsrv* para tener una base de datos con los números de identificación (IP) y contraseñas de los usuarios. La sección de autenticación de netperm-table controla dónde se guarda la base de datos y quién puede tener acceso a ella.

Tuve algunos problemas a la hora de cerrar el acceso a este servicio. Observe que la entrada premit-hosts que muestro usa un *' para dar acceso a cualquiera. Si consigue que funcione, la configuración correcta para esta línea es " `authsrv: premit-hosts localhost`.

Proxy configuration table # # Authentication server and client rules authsrv: database /usr/local/etc/fw-authdb authsrv: permit-hosts * authsrv: badsleep 1200 authsrv: nobogus true # Client Applications using the Authentication server *: authserver 127.0.0.1 114

Para iniciar la base de datos debe hacerlo desde la raíz y ejecutar *./authsrv* en el directorio /var/local/etc para crear el registro administrativo del usuario. A continuación tiene un ejemplo de una sesión.

Lea la documentación FWTK para aprender a añadir usuarios y grupos.

authsrv authsrv# list authsrv# adduser admin Auth DB admin ok - user added initially disabled authsrv# ena admin enabled authsrv# proto admin pass changed authsrv# pass admin plugh Password changed. authsrv# superwiz admin set wizard authsrv# list Report for users in database user group longname ok? proto last ------ ------ ------------------ ----- ------ ----- admin Auth DB admin ena passw never authsrv# display admin Report for user admin (Auth DB admin) Authentication protocol: password Flags: WIZARD authsrv# ^D EOT

Los controles de la puerta de enlace telnet (tn-gw), son muy sencillos y son los primeros que debería instalar.

En mi ejemplo, dejo que el sistema que se encuentra en la red privada tenga acceso sin tener que identificarse (permit-hosts 19961.2.* -passok), pero el resto de los usuarios deben introducir su número de identificación y contraseña para poder usar el proxy (permit-hosts * -auth)

También dejo que otro sistema aparte (192.1.2.202) tenga acceso directo al cortafuegos sin tener que pasar por éste. Existen dos líneas inetacl-in.telnetd para hacerlo. Más tarde explicaré cómo se llaman estas líneas.

El intervalo de espera de Telnet deberá ser corto.

telnet gateway rules: tn-gw: denial-msg /usr/local/etc/tn-deny.txt tn-gw: welcome-msg /usr/local/etc/tn-welcome.txt tn-gw: help-msg /usr/local/etc/tn-help.txt tn-gw: timeout 90 tn-gw: permit-hosts 192.1.2.* -passok -xok tn-gw: permit-hosts * -auth # Only the Administrator can telnet directly to the Firewall via Port 24 netacl-in.telnetd: permit-hosts 192.1.2.202 -exec /usr/sbin/in.telnetd

Las órdenes -r funcionan de la misma manera que telnet.

rlogin gateway rules: rlogin-gw: denial-msg /usr/local/etc/rlogin-deny.txt rlogin-gw: welcome-msg /usr/local/etc/rlogin-welcome.txt rlogin-gw: help-msg /usr/local/etc/rlogin-help.txt rlogin-gw: timeout 90 rlogin-gw: permit-hosts 192.1.2.* -passok -xok rlogin-gw: permit-hosts * -auth -xok # Only the Administrator can telnet directly to the Firewall via Port netacl-rlogind: permit-hosts 192.1.2.202 -exec /usr/libexec/rlogind -a

No debería permitir que nadie, incluyendo el FTP, acceda directamente a su cortafuegos; por lo tanto, no le ponga un servidor FTP.

Una vez más, la línea de acceso de los sitemas principales permite que cualquiera que se encuentre en la red protegida tenga libre acceso a Internet, mientras que los demás deben identificarse. Incluí el registro de cada fichero enviado, así como los que recibí en mis controles. (-log { retr stor })

El intervalo de espera ftp controla el tiempo que tardará en cortarse una mala conexión, así como el tiempo que se mantendrá abierta la conexión sin que sea usada.

ftp gateway rules: ftp-gw: denial-msg /usr/local/etc/ftp-deny.txt ftp-gw: welcome-msg /usr/local/etc/ftp-welcome.txt ftp-gw: help-msg /usr/local/etc/ftp-help.txt ftp-gw: timeout 300 ftp-gw: permit-hosts 192.1.2.* -log { retr stor } ftp-gw: permit-hosts * -authall -log { retr stor }

La web, el gopher y el navegador basado en el ftp se modifican con el http-gw. Las dos primeras líneas crean un directorio para almacenar el ftp y los documentos de la web a medida que pasan por el cortafuegos.Estos ficheros los creo bajo una raíz y los coloco en un directorio al que sólo se puede acceder a través de esa raíz.

La conexión a la web deberá ser corta. Controla el tiempo que tendrá esperar el usuario en el transcurso de una mala conexión.

www and gopher gateway rules: http-gw: userid root http-gw: directory /jail http-gw: timeout 90 http-gw: default-httpd www.afs.net http-gw: hosts 192.1.2.* -log { read write ftp } http-gw: deny-hosts *

Realmente, la ssl-gw es una puerta de enlace. Tenga cuidado con esto. En este ejemplo dejo que cualquiera que se encuentre en la red protegida se conecte a cualquier servidor externo a la red, excepto a las direcciones 127.0.0.* y 192.1.1.*, y sólo de los puertos del 443 al 563. Los puertos del 443 al 563 se conocen como puertos SSL.

ssl gateway rules: ssl-gw: timeout 300 ssl-gw: hosts 192.1.2.* -dest { !127.0.0.* !192.1.1.* *:443:563 } ssl-gw: deny-hosts *

A continuación hay un ejemplo sobre cómo usar la conexión gw para permitir las conexiones a un servidor de noticias. En este ejemplo, dejo que cualquiera que se encuentre dentro de la red protegida se conecte a un solo sistema y a su puerto de noticias.

La segunda línea permite al servidor de noticias transferir sus datos a la red protegida.

Dado que la mayoría de clientes permanecen conectados mientras el usuario lee los datos, el intervalo de espera de un servidor de datos deberá ser largo.

NetNews Pluged gateway plug-gw: timeout 3600 plug-gw: port nntp 192.1.2.* -plug-to 24.94.1.22 -port nntp plug-gw: port nntp 24.94.1.22 -plug-to 192.1.2.* -port nntp

La puerta de enlace finger es sencilla. Cualquiera que se encuentre en la red protegida debe, en primer lugar, acceder al sistema y, posteriormente, nosotros le permitimos usar el programa finger, que se localiza en el cortafuegos. Los demás tan solo recibirán un mensaje como el siguiente:

Enable finger service netacl-fingerd: permit-hosts 192.1.2.* -exec /usr/libexec/fingerd netacl-fingerd: permit-hosts * -exec /bin/cat /usr/local/etc/finger.txt

No he instalado los servicios de Mail y X-windows, así que no voy a dar ejemplos. Si alguien tiene un ejemplo, le agradecería que me enviase un e-mail.

10.4.2. El fichero /etc/services

Aquí es donde empieza todo. Cuando un cliente se conecta al cortafuegos, éste se conecta a un puerto desconocido (inferior al 1024); por ejemplo, telnet se conecta al puerto 23. El demonio de inetd verifica esta conexión y busca el nombre del servicio en el fichero /etc/services. Luego llama al programa que tiene asignado este nombre en el fichero /etc/inetd.conf.

Algunos de los servicios que estamos creando no suelen encontrarse en el fichero /etc/services. Puede asignar algunos al puerto que desee; por ejemplo, he asignado el del administrador telnet (telnet-a) al puerto 24. Si hubiese querido, podría haberle asignado el puerto 2323. Para que el administrador (USTED) se conecte directamente al cortafuegos, tendrá que realizar una conexión telnet al puerto 24 y no al 23, y si instala su fichero netperm-table, como yo lo hice, sólo podrá hacerlo desde uno de los sistemas que se encuentran en su red protegida.

telnet-a 24/tcp ftp-gw 21/tcp # this named changed auth 113/tcp ident # User Verification ssl-gw 443/tcp

11. El Servidor Proxy SOCKS

11.1. Instalación del Servidor Proxy

El servidor proxy SOCKS se encuentra disponible en *http://www.socks.nec.com/*.

Una vez descomprimidos, introduzca los archivos en un directorio de su sistema, y siga las instrucciones sobre cómo hacerlo. Tuve algunos problemas cuando lo hice. Asegúrese de que sus Makefiles son correctos.

Una cuestión importante que se debe tener en cuenta es que el servidor proxy necesita ser incluido en /etc/inetd.conf. Para ello debe añadir la línea:

socks stream tcp nowait nobody /usr/local/etc/sockd sockd

, que le comunica al servidor cuándo ha de ejecutarse.

11.2. Configuración del Servidor Proxy

El programa SOCKS necesita dos ficheros de configuración: uno para comunicarnos que se nos permite el acceso, y otro para enviar las peticiones al servidor proxy correspondiente. El fichero de acceso debería estar en el servidor y el fichero encaminador debería incluirse en cada sistema UNIX. Los computadores DOS y, supuestamente, Macintosh encaminarán por sí mismos.

11.2.1. El fichero de Acceso

Con socks4.2 Beta, el fichero de acceso se llama sockd.conf. Debería contener dos tipos de líneas: las de permiso y las de prohibición. Cada línea tendrá tres entradas:

- El Identificador (permit/deny)
- La dirección IP
- El modificador de dirección

El identificador es o "permit" (permitir) o "deny" (denegar). Debería tener una línea de cada.

La dirección IP se compone de cuatro octetos según la típica anotación de puntos; por ejemplo, 192.168.1.0.

El modificador de dirección es también una dirección IP de cuatro octetos. Funciona como una máscara de red. Hay que verlo como 32 bits (unos o ceros). Si el bit es 1, el bit correspondiente de la dirección que esté comprobando debe coincidir con el bit correspondiente del campo de dirección IP; por ejemplo, si la línea es:

permit 192.168.1.23 255.255.255.255

admitirá sólo direcciones IP en las que coincida cada bit de 192.168.1.23; por ejemplo, sólo 192.168.1.3. La línea:

permit 192.168.1.0 255.255.255.0

admitirá todas las direcciones desde la 192.168.1.0 hasta la 192.168.1.255, la subred de clase C completa. No debería aparecer la línea:

permit 192.168.1.0 0.0.0.0

ya que ésta permitiría el acceso a cualquier dirección, pase lo que pase.

Así que, permita primero todas las direcciones que quiera admitir, y luego prohiba el resto. Para permitir a cualquiera de la subred 192.168.1.xxx, las líneas:

permit 192.168.1.0 255.255.255.0 deny 0.0.0.0 0.0.0.0

trabajarán perfectamente. Observe los primeros 0.0.0.0 en la línea de deny. Con un modificador de 0.0.0.0, el campo de dirección IP no importa. Se suele poner 0 porque es más fácil de teclear.

Se permite más de una entrada de cada clase.

También se puede conceder o denegar el acceso a usuarios concretos. Esto se consigue gracias a la autenticación ident. No todos los sistemas admiten ident, incluyendo Trumpet Winsock, así que no entraré en ello aquí. La documentación que acompaña a socks trata este tema adecuadamente.

11.2.2. El Fichero de Encaminado

El fichero de encaminado tiene el desafortunado nombre de socks.conf. Digo que es desafortunado porque se parece mucho al fichero de control de acceso, por lo que resulta fácil confundirlos.

El fichero de encaminado tiene la función de comunicar a los clientes de SOCKS cuándo usar socks y cuándo no. Por ejemplo, en nuestra red 192.168.1.3 no necesita usar socks para comunicarse con la 192.168.1.1, el cortafuegos. Tiene una conexión directa vía Ethernet. La dirección 127.0.0.1 define la vuelta atrás automáticamente. Por supuesto que no se necesita SOCKS para hablar consigo mismo. Existen tres tipos de entradas:

- deny
- direct
- sockd

La entrada deny (denegar) comunica a SOCKS cuándo rechazar una petición. Esta entrada dispone de los mismos tres campos que en sockd.conf, identifier, address y modifier. Generalmente, dado que de esto también se encarga el fichero sockd.conf, el fichero de control de acceso, el campo del modificador se pone a 0.0.0.0. Si quiere abstenerse de conectar a un determinado lugar, se puede hacer aquí.

La entrada direct nos dice para qué direcciones no se usa socks. Estas son todas las direcciones a las que se puede llegar sin el servidor proxy. De nuevo hay tres campos: identifier, address y modifier. Nuestro ejemplo tendría

direct 192.168.1.0 255.255.255.0

Lo que nos llevaría directamente a cualquier máquina de nuestra red protegida.

La entrada sockd comunica en qué computador se encuentra el servidor demonio de socks. La sintaxis es:

sockd @=<serverlist> <IP address> <modifier>

Observe la entrada @=. Esta permite establecer las direcciones IP de una lista de servidores proxy. En nuestro ejemplo, sólo utilizamos un servidor proxy, pero puede tener muchos para admitir una carga mayor y un margen para redundancia en caso de fallo.

Los campos del modificador y de la dirección IP funcionan exactamente igual que en los otros ejemplos. Especifican a qué direcciones se van a través de los servidores 6.2.3. DNS desde detrás de un cortafuegos.

Instalar un servicio de nombres de dominio (DNS) desde detrás de un cortafuegos es una tarea relativamente sencilla. Sólo necesita instalar el DNS en el sistema cortafuegos. A continuación, configure cada sistema detrás del cortafuegos para usar este DNS.

11.3. Cómo trabajar con un Servidor Proxy

11.3.1. Unix

Para que sus aplicaciones funcionen con el servidor proxy, necesitan ser sockificadas. Será necesario disponer de dos telnets distintos: uno para la comunicación directa y otro para la comunicación por medio del servidor proxy. SOCKS se acompaña de instrucciones sobre cómo SOCKificar un programa, así como un par de programas pre-SOCKificados. Si se usa la versión SOCKificada para conectar con algún sitio con el que se tiene acceso directo, SOCKS cambiará de manera automática a la versión para acceso directo. Por ello, tendremos que dar un nuevo nombre a todos los programas de nuestra red protegida y reemplazarlos por los programas SOCKificados. Así, Finger pasará a ser finger.orig, telnet pasará a ser telnet.orig, etc. Todo esto se dará a conocer a SOCKS mediante el fichero include/socks.h.

Algunos programas encaminarán y sockificarán por sí mismos. Netscape es uno de ellos. Se puede usar un servidor proxy con Netscape simplemente introduciendo la dirección del servidor (en nuestro caso 192.168.1.1) en el campo SOCKs de Proxies. Todas las aplicaciones necesitarán algún retoque, independientemente de cómo procese un servidor proxy.

11.3.2. Trumpet Winsock con MS Windows

Trumpet Winsock viene con capacidad para el servidor proxy incorporada. En el menú setup, se debe poner la dirección IP del servidor, y las direcciones de todos los computadores a los que llega directamente. Trumpet se encargará entonces de todos los paquetes de salida.

11.3.3. Cómo preparar al Servidor Proxy para trabajar con Paquetes UDP

El paquete SOCKS trabaja sólo con paquetes TCP, no con UDP. Esto le resta utilidad. Muchos programas útiles, tales como talk y Archie, usan UDP. Existe un programa de aplicación diseñado para ser utilizado como servidor proxy para los paquetes UDP, denominados UDPrelay de Tom Fitzgerald <fitz@wang.com>. Desafortunadamente, en estos momentos, no es compatible con Linux.

11.4. Inconvenientes con los Servidores Proxy

El servidor proxy es, por encima de todo, un `dispositivo de seguridad`. Usarlo para aumentar el acceso a Internet cuando se tienen pocas direcciones IP presentan muchos inconvenientes. Un servidor proxy permite un mayor acceso desde dentro de la red protegida al exterior, pero mantiene el interior completamente inaccesible desde el exterior. Esto significa la ausencia de servidores, de conexiones talk o archive, o el envío directo de correo a los computadores interiores. Estos inconvenientes podrían parecer insignificantes, pero piense en ello de la siguiente forma:

- Ha dejado un informe que está haciendo en su computador dentro de una red cortafuegos protegida. Está en casa y decide repasarla. No puede. No puede acceder a su computador, porque está detrás del cortafuegos. Intenta entrar primero al `cortafuegos`, pero como todo el mundo tiene acceso al exterior desde el servidor proxy, nadie se ha preocupado de abrirle una cuenta en él.
- Su hija va a la universidad. Quiere enviarle un e-mail. Tiene cosas privadas que comentarle y preferiría que el correo llegara directamente a su computador. Confía plenamente en el administrador de su sistema; pero, sin embargo, es correo privado.

- La incapacidad de utilizar paquetes UDP representa un gran inconveniente con los servidores proxy. Supongo que no por mucho tiempo.

FTP causa otro problema con un servidor proxy. Cuando se hace un `ls`, el servidor FTP establece una conexión con la máquina cliente y manda la información por ella. Un servidor proxy no lo permitirá, así que el FTP no funciona demasiado bien.

Además, un servidor proxy tarda en ejecutarse. Debido a la gran sobrecarga, casi cualquier otro medio de lograr acceso será más rápido.

En resumen, si tiene suficientes direcciones IP, y no le preocupa la seguridad, no use cortafuegos o servidores proxy. Si no dispone de suficientes direcciones IP, y tampoco le preocupa la seguridad, podría considerar la idea de utilizar un emulador IP, como Term, Slirp o TIA. Term está disponible en `ftp://sunsite.unc.edu`, Slirp se encuentra en `ftp://blitzen.canberra.edu.au/pub/slirp`, y TIA, en marketplace.com. Estos programas de aplicación van más rápido, permiten mejores conexiones y proporcionan un mayor nivel de acceso a la red interior desde Internet. Los servidores proxy están bien para las redes que tienen muchos sistemas que quieren conectar con Internet sobre la marcha, con una instalación y un mantenimiento mínimo.

12. Configuraciones Avanzadas

Hay un configuración que me gustaría repasar antes de concluir este documento. La que acabo de esbozar posiblemente será suficiente para la mayoría de la gente; sin embargo, creo que el siguiente ejemplo mostrará una configuración más avanzada que puede aclarar algunas cuestiones. Si tiene duda sobre cualquier otro aspecto no tratado, o simplemente está interesado en la versatilidad de los servidores proxy y cortafuegos, siga leyendo.

12.1. Una gran red con el énfasis en la seguridad

Digamos, por ejemplo, que usted es el líder del clan millisha y quiere poner su sitio web. Dispone de 50 computadores y una subnet de 32 (5 bits) direccions IP. Necesita varios niveles de acceso dentro de su red porque comunica cosas diferentes a sus discípulos; por consiguiente, necesitará proteger ciertas partes de la red del resto.

Los niveles son:

1. El nivel externo. Este es nivel que se enseña a todo el mundo. Aquí es donde hecha una perorata para conseguir adeptos.
2. *Nivel iniciado* Este es el nivel de la gente que ha superado el nivel externo. Es el lugar en el que les enseñan sobre el maldito gobierno y sobre cómo fabricar bombas.
3. *Nivel adepto* Aquí es donde se guardan los *auténticos* planes. En este nivel se almacena toda la información sobre cómo el gobierno del tercer mundo va a hacerse con el poder mundial, subplanes que involucran a Newt Gingrich, Oklahoma City, productos de escasa garantía y lo que realmente se almacena en ese angár del área 51.

12.1.1. Instalación de Red

Los números IP están dispuestos de la siguiente forma:

- un número es 192.168.1.255, que es la difusión y no es utilizable.
- 23 de las 32 direcciones IP se asignan a las 23 máquinas que serán accesibles a Internet.
- una dirección IP extra es para una máquina Linux en esa red
- una dirección IP extra es para otra máquina Linux en esa red
- dos direcciones IP#son para el encaminador

- sobran cuatro, pero se les da los nombres de paul, ringo, john, y george, sólo para confundir las cosas un poco.
- Las dos redes protegidas tienen direcciones del tipo 192.168.1.xxx

Entonces, se crean dos redes diferentes, cada una en espacios diferentes. Son enviadas por medio de Ethernet infrarrojo, de manera que sean completamente invisibles al espacio exterior.

Cada una de estas redes está conectada a una máquina Linux con una dirección IP extra.

Existe un servidor de ficheros que conecta a las dos redes protegidas. Esto se debe a que los planes para hacerse con el poder mundial implica a algunos de los iniciados más aventajados. El servidor de ficheros presenta la dirección 192.168.1.17 para la red de iniciados y la 192.168.1.23 para los adeptos. Tiene que tener asociadas diferentes direcciones IP ya que tiene dos tarjetas Ethernet. El reenvío de paquetes IP está desconectado.

El reenvío de paquetes IP también está conectado en ambas máquinas Linux. El encaminador no enviará paquetes destinados a 192.168.1.xxx a menos que se le indique explícitamente lo contrario, así que Internet no podrá entrar. La razón para desconectar el reenvío de paquetes IP aquí es para que los paquetes de la red de adeptos no llegue a la de iniciados, y viceversa.

El servidor NFS también se puede utilizar para ofrecer diferentes ficheros a las diferentes redes. Esto puede venir muy bien, y el empleo de algunos trucos con enlaces simbólicos puede hacer que se compartan ficheros comunes a todos. Con esta instalación y otra tarjeta Ethernet, el mismo servidor de ficheros puede dar servicio al conjunto de las tres redes.

12.1.2. Instalación del Servidor Proxy

Ahora, dado que los tres niveles quieren navegar por Internet en beneficio de sus propios intereses, los tres necesitan tener acceso a ella. La red externa está conectada directamente a Internet, así que aquí no tenemos que modificar los servidores proxy.

Las redes de adeptos e iniciados están detrás del cortafuegos, así que es necesario instalar aquí los servidores proxy.

Ambas redes se instalarán de forma muy parecida. Ambas tienen asignadas las mismas direcciones IP. Expondré un par de requisitos, sólo para añadir mayor interés.

1. Nadie puede usar el servidor de ficheros para acceder a Internet. Esto expone al servidor de ficheros a virus y a otras cosas desagradables, y es muy importante, por lo que queda prohibido.
2. No se permitirá a los iniciados acceso a la World Wide Web. Están en pruebas y la adquisición de este tipo de información podría resultar perjudicial.

Así que, el fichero sockd.conf en el Linux de los iniciados presentará esta línea:

deny 192.168.1.17 255.255.255.255

y en la máquina de los adeptos:

deny 192.168.1.23 255.255.255.255

Y, la máquina Linux de los iniciados tendrá estea línea

deny 0.0.0.0 0.0.0.0 eq 80

Esto significa denegar el acceso a todas las máquinas que traten de acceder al puerto igualr (eq) a 80, el puerto http. Aunque esto aún permita el acceso al resto de los servicios, deniega el acceso a la Web.

A continuación, ambos ficheros tendrán:

permit 192.168.1.0 255.255.255.0

para permitir a todos los computadores de la red 192.168.1.xxx usar este servidor proxy, exceptuando aquéllos a los que ya se le ha denegado (por ejemplo, cualquier acceso desde el servidor de ficheros y el acceso a la Web desde la red iniciados)

El fichero sockd.conf de los iniciados será:

deny 192.168.1.17 255.255.255.255 deny 0.0.0.0 0.0.0.0 eq 80 permit 192.168.1.0 255.255.255.0

y el de los adeptos:

deny 192.168.1.23 255.255.255.255 permit 192.168.1.0 255.255.255.0

Con esto, todo debería quedar configurado correctamente. Cada red se encuentra aislada como corresponde, con el grado de interaccón adecuado. Todos deberíamos estar satisfechos.

13. Cómo facilitar la Gestión

13.1. Herramientas Cortafuegos

Existen varios paquetes de software que facilitarán la gestión de su cortafuegos.

Tenga cuidado, no utilice estas herramientas a menos que pueda prescindir de ellas. Estas programaciones de guiones tanto pueden facilitarle la tarea como conducirle a errores.

Tanto las interfaces de la web como las gráficas han sido diseñadas para trabajar con las normas de filtración de Linux. Algunas compañías incluso han creado cortafuegos comerciales basados en Linux introduciéndolo en su propia máquina con su propio código de gestión. (todo un detalle)

En realidad, no soy un tipo GUI. Sin embargo, llevo utilizando cortafuegos con interfaces GUI desde hace algún tiempo. He descubierto que ayudan proporcionando un buen informe de todas las reglas de forma muy clara.

gfcc (GTK+ Firewall Control Center) es una aplicación GTK+ capaz de controlar las reglas y directrices del cortafuegos de Linux, basadas en el paquete ipchains. Vaya a http://icarus.autostock.co.kr (http://icarus.autostock.co.kr/) y hágase con una copia. Sinceramente es una excelente herramienta.

He incluido programaciones de guiones RC en el apéndice A. Estos guiones funcionan con y sin gfcc.

Existen muchas programaciones de guiones disponibles para instalar un cortafuegos. Una línea de guión bastante completo está disponible en http://www.jasmine.org.uk/~simon/bookshelf/papers/instant-firewall/instant-firewall.html. Otra se encuentra en http://www.pointman.org/.

El cortafuegos K es un punto de inicio GUI para cadenas ipchains o ipfwadm (dependiendo de la versión de su núcleo). http://megaman.ypsilonia.net/kfirewall/

FCT es una herramienta basada en HTML para la configuración de un cortafuegos. Genera programación de guiones de manera automática para órdenes de filtración IP (ipfwadm) en un cortafuegos para múltiples interfaces y cualquier servicio de Internet. http://www.fen.baynet.de/~ft114/FCT/firewall.htm

13.2. Herramientas Generales

WebMin es un paquete de aplicación admin para sistemas. No le ayudará a gestionar las reglas, pero le ayudará a la hora de activar y desactivar demonios y procesos. Es un programa MUY bueno, estoy esperando que el señor J. Cameron incluya un módulo de cadenas IPCHAINS. http://www.webmin.com/

Si es usted un ISP, querrá saber sobre IPFA (Contabilidad para Cortafuegos IP) http://www.soaring-bird.com/ipfa/. Le permite hacer registros cronológicos Al-Mes/Al-día/por-minuntos/ y dispone de una administración GUI basada en la Web.

14. Cómo burlar un Sistema Cortafuegos

Le revelaré lo fácil que resulta burlar un sistema cortafuegos tan solo para arruinarle el día y para que se mantenga alerta en lo que respecta al tema de la seguridad. Precisamente ahora que ha seguido todos los pasos de este documento y tiene un servidor y una red muy seguros. Dispone de una red perimétrica (DMZ) y nadie puede acceder a su red; además, cualquier conexión que se haga al exterior queda registrada. Cualquier usuario que quiera acceder a la red debe hacerlo a través de un servidor proxy. Entonces uno de sus usuarios, con conexión propia, averigua lo dehttptunnel (http://www.nocrew.org/software/httptunnel.html). httptunnel crea un túnel bidireccional de datos virtuales en los HTTP solicitados. Estos HTTP pueden ser enviados a través de un servidor proxy HTTP si así se desea. O, en sus sistemas instalan una Red Privada Virtual (VPN). Véase a este respecto: http://sunsite.auc.dk/vpnd/O, quizá este usuario simplemente ponga un módem en su sistema NT y establezca el encaminado. Por último, en la estación de trabajo, en la LAN privada, cambia la puerta de enlace por defecto para indicarle la nueva ruta que debe seguir para acceder a Internet. Ahora, desde esta estación de trabajo, puede ir a cualquier parte. La única cosa que el admin del cortafuegos podría ver sería una conexión que no deja ver que es realmente una larga visita DNS. Ahora, !tome el control del mundo!

15. APÉNDICE A - Guiones de ejemplo

15.1. Guión RC usando GFCC

```
#!/bin/bash # # Firewall Script - Version 0.9.1 # # chkconfig: 2345 09 99 # description:
firewall script for 2.2.x kernel # Set for testing # set -x # # NOTES: # # This script is
written for RedHat 6.1 or better. # # Be careful about offering public services like web
or ftp servers. # # INSTALLATION: # 1. place this file in /etc/rc.d/init.d (you'll have to
be root..) # call it something like "firewall" :-) # make it root owned --> "chown
root.root (filename)" # make it executable --> "chmod 755 (filename)" # # 2. use GFCC
to create your firewall rules and export them to a file # named
/etc/gfcc/rules/firewall.rule.sh. # # 3. add the firewall to the RH init structure -->
"chkconfig --add (filename)" # next time the router boots, things should happen
automagically! # sleep better at night knowing you are *LESS* vulnerable than
before... # # RELEASE NOTES # 30 Jan, 2000 - Changed to GFCC script # 11 Dec,
1999 - updated by Mark Grennan <mark@grennan.com> # 20 July, 1999 - initial
writing - Anthony Ball <tony@LinuxSIG.org> #
################################################ # Source function library. .
/etc/rc.d/init.d/functions # Source networking configuration. . /etc/sysconfig/network #
```

Check that networking is up. [${NETWORKING} = "no"] && exit 0 # See how we are called case "$1" in start) # Start providing access action "Starting firewall: " /bin/true /etc/gfcc/rules/firewall.rule.sh echo ;; stop) action "Stoping firewall: " /bin/true echo 0 > /proc/sys/net/ipv4/ip_forward /sbin/ipchains -F input /sbin/ipchains -F output /sbin/ipchains -F forward echo ;; restart) action "Restarting firewall: " /bin/true $0 stop $0 start echo ;; status) # List out all settings /sbin/ipchains -L ;; test) action "Test Mode firewall: " /bin/true /sbin/ipchains -F input /sbin/ipchains -F output /sbin/ipchains -F forward echo 1 > /proc/sys/net/ipv4/ip_forward /sbin/ipchains -A input -j ACCEPT /sbin/ipchains -A output -j ACCEPT /sbin/ipchains -P forward DENY /sbin/ipchains -A forward -i $PUBLIC -j MASQ echo ;; *) echo "Usage: $0 {start|stop|restart|status|test}" exit 1 esac

15.2. Guión GFCC

Este guión fue generado por el programa de Cortafuegos Gráfico (GFCC). Este no es el conjunto de reglas en funcionamiento, sino el conjunto de reglas exportadas.

#!/bin/sh # Generated by Gtk+ firewall control center IPCHAINS=/sbin/ipchains localnet="192.168.1.0/24" firewallhost="192.168.1.1/32" localhost="172.0.0.0/8" DNS1="24.94.163.119/32" DNS2="24.94.163.124/32" Broadcast="255.255.255.255/32" Multicast="224.0.0.0/8" Any="0.0.0.0/0" mail_grennan_com="192.168.1.1/32" mark_grennan_com="192.168.1.3/32" $IPCHAINS -P input DENY $IPCHAINS -P forward ACCEPT $IPCHAINS -P output ACCEPT $IPCHAINS -F $IPCHAINS -X # input rules $IPCHAINS -A input -s $Any -d $Broadcast -j DENY $IPCHAINS -A input -p udp -s $Any -d $Any netbios-ns -j DENY $IPCHAINS -A input -p tcp -s $Any -d $Any netbios-ns -j DENY $IPCHAINS -A input -p udp -s $Any -d $Any netbios-dgm -j DENY $IPCHAINS -A input -p tcp -s $Any -d $Any netbios-dgm -j DENY $IPCHAINS -A input -p udp -s $Any -d $Any bootps -j DENY $IPCHAINS -A input -p udp -s $Any -d $Any bootpc -j DENY $IPCHAINS -A input -s $Multicast -d $Any -j DENY $IPCHAINS -A input -s $localhost -d $Any -i lo -j ACCEPT $IPCHAINS -A input -s $localnet -d $Any -i eth1 -j ACCEPT $IPCHAINS -A input -s $localnet -d $Broadcast -i eth1 -j ACCEPT $IPCHAINS -A input -p icmp -s $Any -d $Any -j ACCEPT $IPCHAINS -A input -p tcp -s $Any -d $Any -j ACCEPT ! -y $IPCHAINS -A input -p udp -s $DNS1 domain -d $Any 1023:65535 -j ACCEPT $IPCHAINS -A input -p udp -s $DNS2 domain -d $Any 1023:65535 -j ACCEPT $IPCHAINS -A input -p tcp -s $Any -d $Any ssh -j ACCEPT $IPCHAINS -A input -p tcp -s $Any -d $Any telnet -j ACCEPT $IPCHAINS -A input -p tcp -s $Any -d $Any smtp -j ACCEPT $IPCHAINS -A input -p tcp -s $Any -d $Any pop-3 -j ACCEPT $IPCHAINS -A input -p tcp -s $Any -d $Any auth -j ACCEPT $IPCHAINS -A input -p tcp -s $Any -d $Any www -j ACCEPT $IPCHAINS -A input -p tcp -s $Any -d $Any ftp -j ACCEPT $IPCHAINS -A input -s $Any -d $Any -j DENY -l # forward rules $IPCHAINS -A forward -s $localnet -d $Any -j MASQ # output rules

15.3. Guión RC sin GFCC. Este es el conjunto de reglas de cortafuegos hecho por mí. No utiliza GFCC.

```
#!/bin/bash
#
# Firewall Script - Version 0.9.1
#
# chkconfig: 2345 09 99
# description: firewall script for 2.2.x kernel
# Set for testing
# set -x
#
# NOTES:
#
#  This script is written for RedHat 6.1 or better.
#
#  Be careful about offering public services like web or ftp servers.
#
# INSTALLATION:
#  1. place this file in /etc/rc.d/init.d  (you'll have to be root..)
#     call it something like "firewall"    :-)
#     make it root owned -->  "chown root.root (filename)"
#     make it executable -->  "chmod 755 (filename)"
```

```
#
#  2. use GFCC to create your firewall rules and export them to a file
#     named /etc/gfcc/rules/firewall.rule.sh.
#
#  3. add the firewall to the RH init structure --> "chkconfig --
add (filename)"
#     next time the router boots, things should happen automagically!
#     sleep better at night knowing you are *LESS* vulnerable than before...
#
# RELEASE NOTES
#   30 Jan, 2000 - Changed to GFCC script
#   11 Dec, 1999 - updated by Mark Grennan <mark@grennan.com>
#   20 July, 1999 - initial writing - Anthony Ball <tony@LinuxSIG.org>
#

################################################

# Source function library.
. /etc/rc.d/init.d/functions

# Source networking configuration.
. /etc/sysconfig/network

# Check that networking is up.
[ ${NETWORKING} = "no" ] && exit 0

# See how we are called
case "$1" in

  start)
# Start providing access
action "Starting firewall: " /bin/true
/etc/gfcc/rules/firewall.rule.sh
echo
;;

  stop)
```

```
action "Stoping firewall: " /bin/true
echo 0 > /proc/sys/net/ipv4/ip_forward
/sbin/ipchains -F input
/sbin/ipchains -F output
/sbin/ipchains -F forward

echo
;;

  restart)
action "Restarting firewall: " /bin/true
$0 stop
$0 start

echo
;;

  status)
# List out all settings
/sbin/ipchains -L
;;

  test)
action "Test Mode firewall: " /bin/true
/sbin/ipchains -F input
/sbin/ipchains -F output
/sbin/ipchains -F forward
echo 1 > /proc/sys/net/ipv4/ip_forward
/sbin/ipchains -A input -j ACCEPT
/sbin/ipchains -A output -j ACCEPT
/sbin/ipchains -P forward DENY
/sbin/ipchains -A forward -i $PUBLIC -j MASQ

echo
;;

  *)
```

```
echo "Usage: $0 {start|stop|restart|status|test}"
exit 1

esac
```

16. APÉNDICE B - Un guión VPN RC para RedHat

#!/bin/sh # # vpnd This shell script takes care of starting and stopping # vpnd (Vertual Privage Network connections). # # chkconfig: - 96 96 # description: vpnd # # Source function library. . /etc/rc.d/init.d/functions # Source networking configuration. . /etc/sysconfig/network # Check that networking is up. [${NETWORKING} = "no"] && exit 0 [-f /usr/sbin/vpnd] || exit 0 [-f /etc/vpnd.conf] || exit 0 RETVAL=0 # See how we were called. case "$1" in start) # Start daemons. echo -n "Starting vpnd: " daemon vpnd RETVAL=$? [$RETVAL -eq 0] && touch /var/lock/subsys/vpnd echo ;; stop) # Stop daemons. echo -n "Shutting down vpnd: " killproc vpnd RETVAL=$? [$RETVAL -eq 0] && rm -f /var/lock/subsys/vpnd echo ;; restart) $0 stop $0 start ;; *) echo "Usage: vpnd {start|stop|restart}" exit 1 esac exit $RETVAL