

Ciclo Formativo de Grado Superior de Administración de Sistemas Informáticos en Red



**Módulo Profesional: SAD
U.T.8.- Seguridad Perimetral**

*Departamento de Informática y Comunicación
IES San Juan Bosco (Lorca-Murcia)
Profesor: Juan Antonio López Quesada*





Índice de Contenidos

Introducción

Cortafuegos o Firewall

Servidor Proxy

Administración Gráfica del
Firewall/servidor proxy

Referencias WEB

Enlaces a Herramientas SW

Prácticas/Actividades



Objetivos de la Unidad de Trabajo:

Valorar los peligros externos a las redes corporativas y conocer las medidas de seguridad perimetrales para hacerles frente.

Comprender la importancia de los puertos de comunicaciones y su filtrado mediante cortafuegos o firewall.

Aprender el significado de las listas de control de acceso (ACL) en routers y cortafuegos.

Comprender la importancia y aprender a configurar servidores y clientes proxy.

Abstract/Resumen:

- Las redes han permitido que los negocios mejoren sus procesos operativos y productivos y se enlacen con clientes y proveedores, pero también provocado que aumenten los riesgos informáticos. Las organizaciones están expuestas hoy a un importante nivel de amenazas externas e internas que ponen en riesgo la seguridad de la información negocio y de los activos informáticos que soportan las operaciones.
- El problema más frecuente es que estas amenazas no se conocen hasta que se materializa el riesgo y causa daño en la imagen de la empresa o institución. **Conectarse a Internet y no contar con las herramientas adecuadas y con un firewall bien configurado es el equivalente a tener una casa sin cerraduras en las puertas.** Un intruso puede tomar control de los servidores o de las PCs de los usuarios y tener acceso a información privilegiada. Imaginemos el costo económico y de imagen si esta información pierde o cae en manos de la competencia o de gente sin escrúpulos.



Introducción:

□ Actualmente, cuando las empresas disponen ya de sus propias redes internas a las que dan acceso a usuarios desde el exterior, los problemas de seguridad se plantean en tres reas principales:

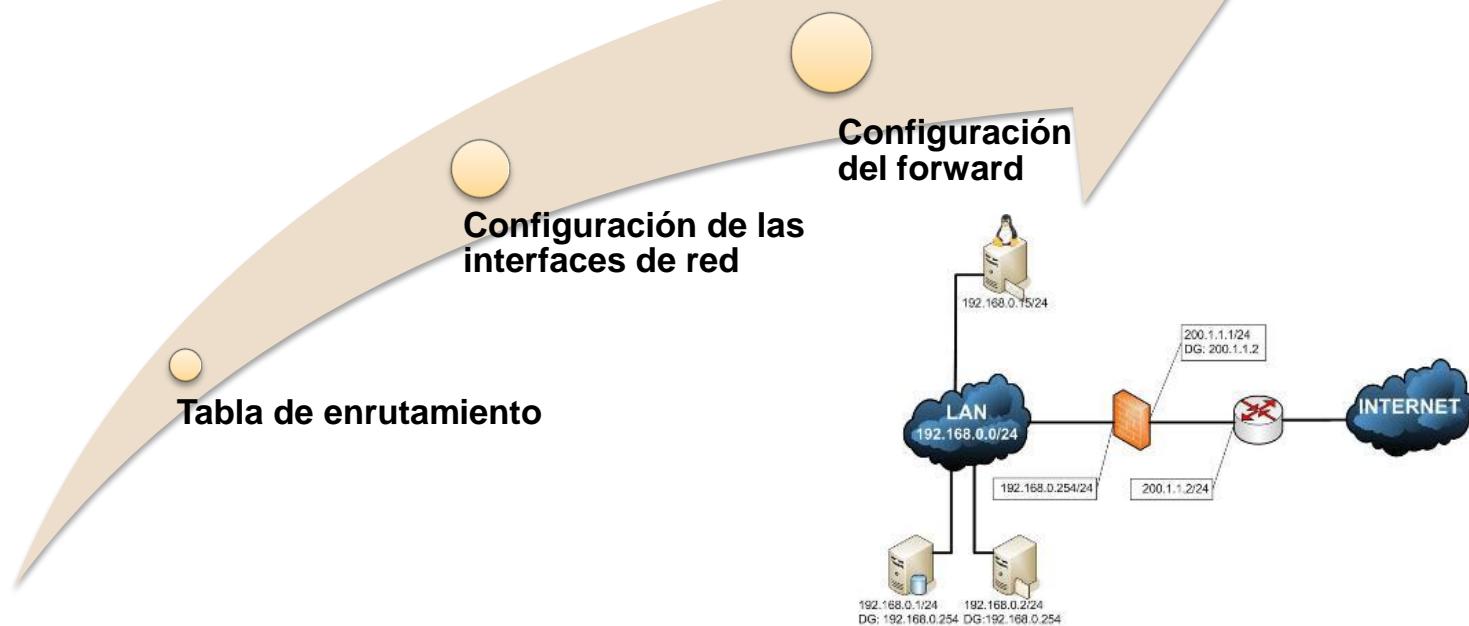
1. ***La seguridad de perímetro:*** protección frente ataques del exterior generalmente basada en cortafuegos (firewalls) y servidores Proxy.
2. ***La seguridad en el canal:*** donde hay que proteger los datos frente a escuchas mediante criptografía
3. ***La seguridad de acceso:*** donde se contemplan tres aspectos, la identificación del usuario, la autorización del acceso y la auditoria de las operaciones

□ Cuando una red corporativa se encuentra interconectada a una red pública, los peligros de ataque a sus servidores, routers y sistemas internos se multiplican. Las medidas de seguridad perimetral suponen la primera línea de defensa entre las redes públicas y redes corporativas o privadas. ***Entre otros aspectos estudiaremos el uso de cortafuegos o firewall destinado a bloquear las conexiones no autorizadas, y de servidores proxy que hagan de intermediario entre clientes y servidores finales, permitiendo el filtrado y monitorización de servicios.***

Introducción:

GNU/LINUX: Tabla de enrutamiento, interfaces y /proc/sys/net/ipv4/ip_forward

- En el marco se la configuración de un **cortafuegos/proxy** es preciso establecer determinadas acciones previas que permitan el adecuado funcionamiento del dispositivo/servicios, entre las que hay que mencionar: La definición adecuada de la tabla de enrutamiento, las interfaces de red y la acción forward para el trasiego de paquetes entre las interfaces en función de la configuración de la tabla de enrutamiento.



Introducción:

GNU/LINUX: Tabla de enrutamiento

Direccionamiento

- ❑ La dirección es el identificador que permite a otras máquinas enviar información, en el protocolo IP indica un punto de unión en la red llamado interfaz. Una máquina puede tener múltiples interfaces, teniendo una dirección IP por cada una de ellas, las interfaces son por lo general conexiones físicas distintas, pero también pueden ser conexiones lógicas compartiendo una misma interfaz.

Estructura de una dirección IP

- ❑ Las direcciones IP poseen 32 bits de longitud y están divididas en cuatro octetos (8 bits). Una dirección IP puede ser escrita en varias formas: binaria, decimal y hexadecimal. Una dirección IP consiste de dos niveles jerárquicos, los cuales son: el identificador de red, netid, y el identificador de máquina, hostid. En el protocolo IP el identificador de red representa un número de máquinas que pueden comunicarse entre ellas a través de la capa dos del modelo de referencia OSI. El identificador de máquina representa el número de la máquina dentro de la red. La dirección IP identifica la máquina de forma única en toda Internet.

Introducción:

GNU/LINUX: Tabla de enrutamiento

Números de red y mascara

- ❑ La división del número de red y de máquina es distinta para cada red. Esto facilita al software de enrutadores y máquinas identificar con facilidad dónde ocurre la división.
- ❑ Cada dirección tiene una máscara de red asociada, la cual es representada por un número de 32 bits, donde todos los bits de la porción de red están en 1 y todos los bits de la porción de máquina están en 0.

Clases de dirección IP.

- ❑ Las redes clase A, utilizan el primer octeto (byte) para referirse al número de red. El primer bit comienza en 0. El rango de direcciones para estas redes está entre el 1.x.x.x y el 126.x.x.x y se pueden asignar direcciones hasta 16194277 hosts. La dirección 127.x.x.x está reservada para designar la interfaz local.
- ❑ Las redes clase B, emplean los dos primeros octetos para referirse al número de red. Los dos primeros bits son 10. El rango de direcciones para estas redes está comprendido entre el 128.1.x.x y el 191.254.x.x, pudiéndose asignar direcciones para 64516 hosts. Las redes clase C, usan los tres primeros octetos para referirse al número de red.

Introducción:

GNU/LINUX: Tabla de enrutamiento

- ❑ Los tres primeros bits son 110; y su rango de direcciones de red está comprendido entre el 192.1.1.x y el 223.254.254.x . A esta clase de red se le pueden asignar direcciones a 254 hosts.
- ❑ Originalmente las redes clase D eran definidas como las redes con los tres primeros bits en 111 y fueron reservadas para usos futuros. Desde entonces las investigaciones han provocado cambios en la definición de la clase D, considerándose actualmente como las redes que comienzan con 1110. Estas redes no representan una máquina sino una colección que forma parte de un grupo multicast IP. Comprende las direcciones de red desde la 224.0.0.0 hasta la 239.255.255.255.
- ❑ Las redes clase E, comienzan con sus cinco primeros bits en 11111 y están compuestas por las redes comprendidas desde la 240.0.0.0 hasta la 247.255.255.255. Estas direcciones de red están reservadas para **uso futuro** y son conocidas como redes "marcianas". Posiblemente una nueva clase podría ser necesaria, así la definición de clase tipo E podría ser modificada por una clase que comience por 11110 y una nueva clase se definiría (y se reservaría para uso futuro) comenzando con 11111.
- ❑ Existen además direcciones IP públicas y privadas, en Internet la manera como son asignadas garantiza su unicidad. El organismo encargado de administrar la asignación de números IP es conocido como Internet Registry. Las direcciones IP que son únicas son las conocidas como públicas. Algunas direcciones no son únicas y son utilizadas por corporaciones que no están conectadas a Internet o que requieren de acceso restringido. Para estos casos se hace necesario el uso de direcciones privadas, las cuales son duplicadas en distintas corporaciones pues por lo general están aisladas.

Introducción:

GNU/LINUX: Tabla de enrutamiento

IPv6

- ❑ El Internet Protocol version 6 (IPv6) (en español: Protocolo de Internet versión 6) es una versión del protocolo Internet Protocol (IP), definida en el RFC 2460 y diseñada para reemplazar a Internet Protocol version 4 (IPv4) RFC 791, que actualmente está implementado en la gran mayoría de dispositivos que acceden a Internet.
- ❑ Diseñado por Steve Deering de Xerox PARC y Craig Mudge, IPv6 está destinado a sustituir a IPv4, cuyo límite en el número de direcciones de red admisibles está empezando a restringir el crecimiento de Internet y su uso, especialmente en China, India, y otros países asiáticos densamente poblados. El nuevo estándar mejorará el servicio globalmente; por ejemplo, proporcionará a futuras celdas telefónicas y dispositivos móviles sus direcciones propias y permanentes.
- ❑ A principios de 2010, quedaban menos del 10% de IPs sin asignar. En la semana del 3 de febrero del 2011, la IANA (Agencia Internacional de Asignación de Números de Internet, por sus siglas en inglés) entregó el último bloque de direcciones disponibles (33 millones) a la organización encargada de asignar IPs en Asia, un mercado que está en auge y no tardará en consumirlas todas.
- ❑ IPv4 posibilita 4.294.967.296 (232) direcciones de red diferentes, un número inadecuado para dar una dirección a cada persona del planeta, y mucho menos a cada vehículo, teléfono, PDA, etcétera. En cambio, IPv6 (128 bits de longitud, se escriben como ocho grupos de cuatro dígitos hexadecimales, 2001:0db8:85a3:08d3:1319:8a2e:0370:7334) admite (340 sextillones de direcciones) — cerca de $6,7 \times 10^{17}$ (670 mil billones) de direcciones por cada milímetro cuadrado de la superficie de La Tierra.

Introducción:

GNU/LINUX: Tabla de enrutamiento

Una dirección IPv6

(en hexadecimal)

2001:0DB8:AC10:FE01:0000:0000:0000:0000



2001:0DB8:AC10:FE01::

Se pueden omitir los ceros



10000000000001:0000110110111000:1010110000010000:1111111000000001:

0000000000000000:0000000000000000:0000000000000000:0000000000000000

Introducción:

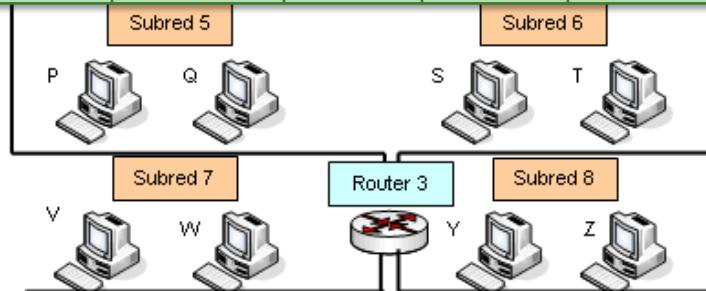
GNU/LINUX: Tabla de enrutamiento

Configuraciones Comunes de Enrutamiento

- Configuraciones comunes de enrutamiento o rutas Mínimas Una red completamente aislada de otra red TCP/IP requiere solo de rutas mínimas. Las rutas mínimas son creadas por el comando ifconfig al momento de configurar una interfaz. Las rutas mínimas son: la ruta de red local y la ruta para loopback. En linux es necesario crear la interfaz y la ruta.

```
# route -n
```

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
150.185.162.0	0.0.0.0	255.255.255.128	U	0	0	2	eth0
127.0.0.0	0.0.0.0	255.0.0.0	U	0	0	1	lo



Introducción:

GNU/LINUX: Tabla de enrutamiento

- ❑ Una entrada es la ruta a la red 150.185.156.0 a través de eth0. La otra entrada es la ruta loopback a localhost establecida cuando lo fue creada. Observe los campos de bandera en cada entrada. Ambas entradas tienen la bandera U (Up), esto indica que la interfaz esta lista para ser usada. Ninguna de las entradas tiene la bandera G (Gateway). Esta bandera indica que un gateway externo esta siendo usado. La bandera G no aparece pues estas rutas son directas a través de interfaces locales y no a través de gateway externos. Observe que sólo tenemos la ruta loopback y la ruta 150.185.156.0. Por lo que mi máquina sólo se podrá comunicar con otras máquinas dentro de la misma red.
- ❑ Esto es fácil de verificar con el comando ping.

```
#ping 189.148.1.10
PING 189.148.1.10: 56 data bytes 64 bytes from 189.148.1.10
: icmp_seq=0 ttl= 234 time=110.0 ms 64 bytes from 189.148.1.10
: icmp_seq=1 ttl= 234 time=100.7 ms
```

^C ---- 189.148.1.10 ping statistics---- 2 packets transmitted, 2 packet received, 0% packets loss
round-trip (ms) min/avg/max = 100/105/110 ms

ping muestra una línea de salida por cada mensaje ICMP de respuesta recibida. Cuando ping es interrumpido muestra un resumen estadístico. Ahora veamos que pasa si intentamos comunicarnos con una máquina fuera de la red.

```
#ping 150.185.128.10 Network is unreachable
```

Este mensaje indica que mi máquina no conoce como enviar paquetes a la red de la maquina 150.185.128.10

Introducción:

GNU/LINUX: Tabla de enrutamiento

Enrutamiento Estático

- ❑ Enrutamiento Estático Una red con un número mínimo de enrutadores puede ser configurada con enrutamiento estático. Para una red con un solo gateway, la mejor opción es el enrutamiento estático. Una tabla de enrutamiento estático es construida manualmente, por el administrador de la red, usando el comando route. Las tablas de enrutamiento estático no se ajustan a los cambios de la red, ellos trabajan mejor cuando las rutas no cambian. Para agregar una ruta se utiliza el comando route. El destino final debe ser conocido. El Linux utiliza el comando route para agregar o borrar entradas manualmente en la tabla de enrutamiento.
- ❑ Por ejemplo, para agregar la ruta 150.185.156.1 a la tabla de enrutamiento en linux se procede de la siguiente forma :
- ❑ #route add -host 150.185.156.1 eth0



Introducción:

GNU/LINUX: Tabla de enrutamiento

COMANDO route:

El comando route muestra la tabla de enrutamiento que reside en el kernel y también se usa para modificarla. La tabla que especifica cómo se enrutan los paquetes a un host se llama tabla de enrutamiento.

SINTAXIS:

La sintaxis es: route [opciones]

-n	Muestra la tabla de enrutamiento en formato numérico [dirección IP]
-e	Muestra la tabla de enrutamiento en formato hostname
add	Añade una nueva ruta a la tabla de enrutamiento
del	Elimina una ruta de la tabla de enrutamiento

-net	Indica que el objetivo es una red
-host	Indica que el objetivo es un host
gw	Especifica el puerta de enlace del host o red objetivo
netmask	Usado para especificar la máscara de subred del host o red de destino
dev	Especifica el dispositivo o interfaz donde se enviarán los paquetes
reject	Rechaza los paquetes enviados a una ruta o host particular

Introducción:

GNU/LINUX: Tabla de enrutamiento

Ejercicios:

1.- Para mostrar la tabla de enrutamiento: route -n

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
192.168.0.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0
169.254.0.0	0.0.0.0	255.255.0.0	U	0	0	0	eth0
0.0.0.0	192.168.0.1	0.0.0.0	UG	0	0	0	eth0

En la tabla anterior:	
Destination	Indica la dirección IP de la red o host de destino
Gateway	Indica el puerta de enlace desde el cual se alcanza el host o red de destino
Genmask	Indica el destino de la máscara de subred
Flags	Indica el estado actual de ruta <input type="checkbox"/> U - La ruta está activa <input type="checkbox"/> H - El objetivo es un host <input type="checkbox"/> G - Utilizar puerta de enlace
Iface	Indica la interfaz

Introducción:

GNU/LINUX: Tabla de enrutamiento

2.- Para añadir ruta estática a una red en la tabla de enrutamiento:

```
route add -net 192.168.1.0 netmask 255.255.255.0 gw 192.168.1.1 dev eth0
```

<i>En el comando anterior:</i>	
add	-Indica que la ruta se añade a la tabla de enrutamiento.
-net	-Indica que el destino es una red
192.168.0.1	-Indica la dirección IP de la red de destino
netmask	-Indica la máscara de subred de la red de destino.
gw 192.168.1.1	-Indica el puerta de enlace de la red de destino.
dev eth0	-Indica que los paquetes se enrutan a través de la interfaz eth0.

3.- Para eliminar una ruta de la tabla de enrutamiento:

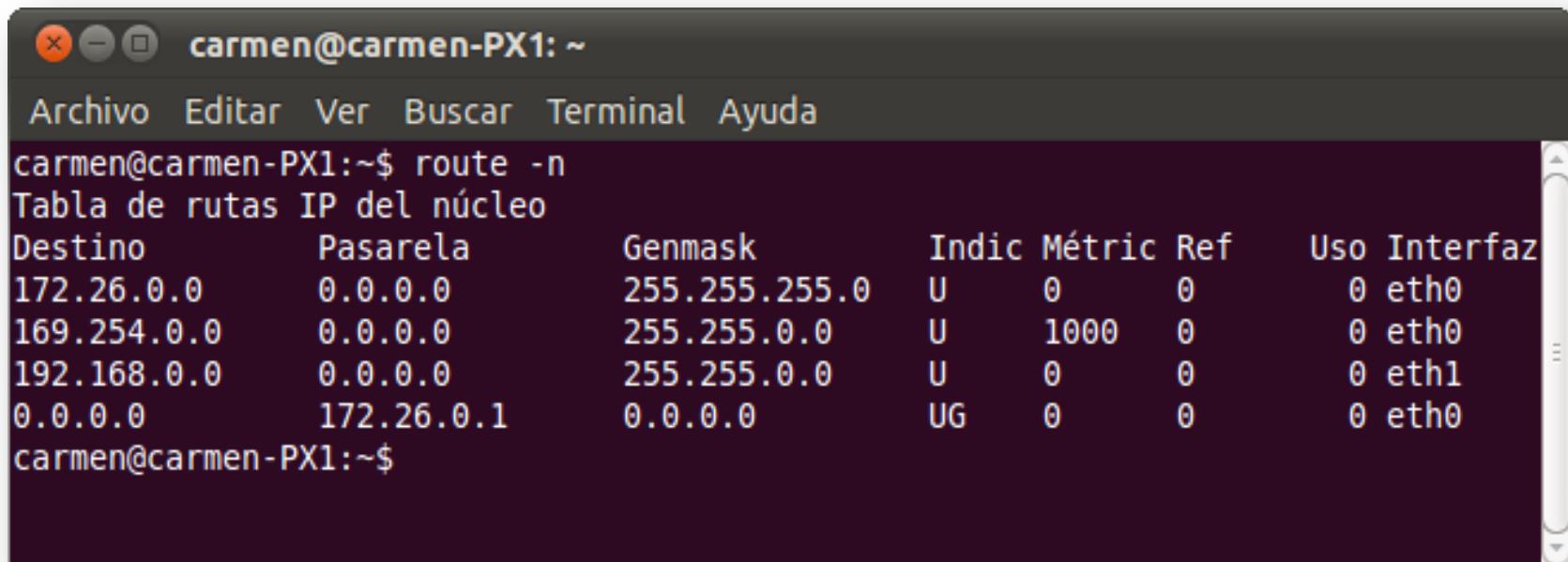
```
route del -net 192.168.1.0 netmask 255.255.255.0 gw 192.168.1.1 dev eth0
```

El comando anterior eliminará la ruta a 192.168.1.0 de la tabla de enrutamiento.

Introducción:

GNU/LINUX: Tabla de enrutamiento

Ejemplo Departamento de Informática y comunicaciones:



The screenshot shows a terminal window titled "carmen@carmen-PX1: ~". The window has a dark background and light-colored text. At the top, there is a menu bar with options: Archivo, Editar, Ver, Buscar, Terminal, and Ayuda. Below the menu, the command "route -n" is entered, followed by its output. The output is titled "Tabla de rutas IP del núcleo" (Kernel IP routing table). It lists five network routes with columns for Destino (Destination), Pasarela (Gateway), Genmask (Network Mask), Indic (Flags), Métric (Metric), Ref (Reference count), Uso (Usage), and Interfaz (Interface). The routes include 172.26.0.0 via 0.0.0.0, 169.254.0.0 via 0.0.0.0, 192.168.0.0 via 0.0.0.0, and 0.0.0.0 via 172.26.0.1.

```
carmen@carmen-PX1:~$ route -n
Tabla de rutas IP del núcleo
Destino      Pasarela        Genmask        Indic  Métric  Ref    Uso  Interfaz
172.26.0.0   0.0.0.0        255.255.255.0  U      0       0        0    eth0
169.254.0.0  0.0.0.0        255.255.0.0   U      1000    0        0    eth0
192.168.0.0  0.0.0.0        255.255.0.0   U      0       0        0    eth1
0.0.0.0      172.26.0.1    0.0.0.0       UG     0       0        0    eth0
carmen@carmen-PX1:~$
```

Introducción:

GNU/LINUX: interfaces

- El fichero **/etc/network/interfaces** contiene la configuración de las interfaces de red. Como ejemplo de configuración tenemos:

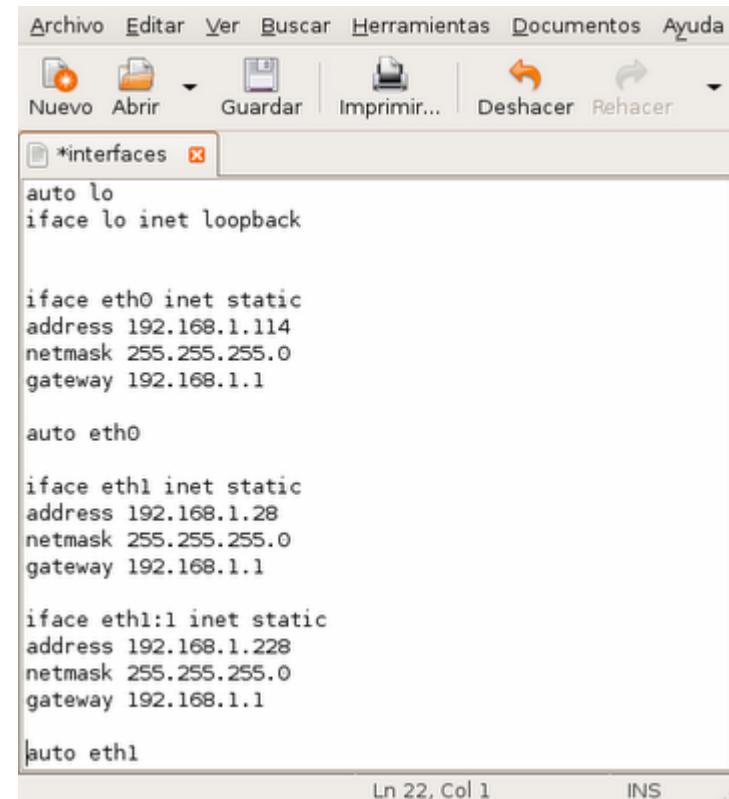
Configuración estática de la interface eth0:

```
iface eth0 inet static  
address 192.168.1.5  
netmask 255.255.255.0  
gateway 192.168.1.254
```

Configuración DHCP de la interface eth0:

```
auto eth0  
iface eth0 inet dhcp
```

Ejemplo de /etc/network/interfaces



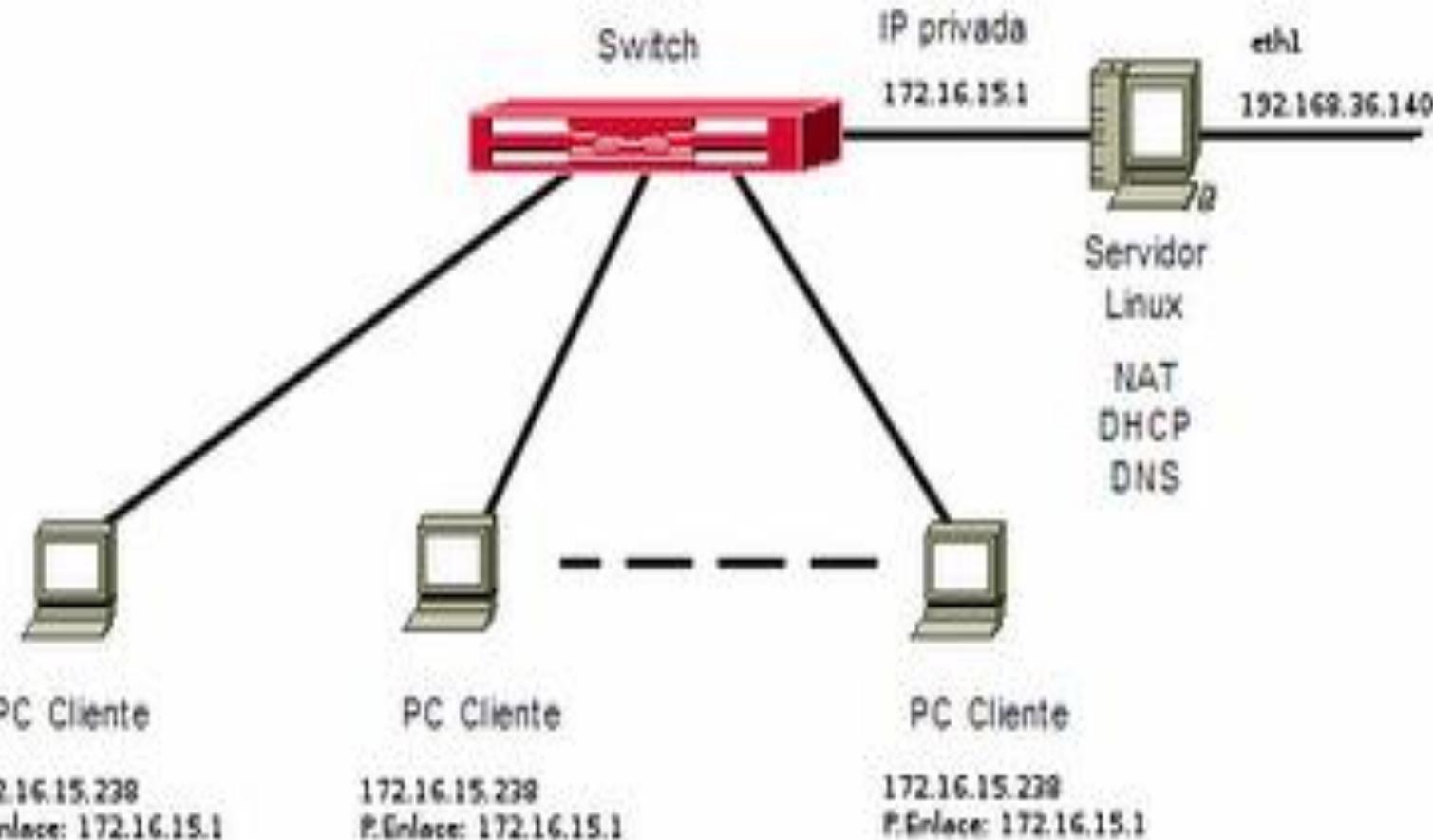
The screenshot shows a window titled 'interfaces' with the following content:

```
Archivo Editar Ver Buscar Herramientas Documentos Ayuda  
Nuevo Abrir Guardar Imprimir... Deshacer Rehacer  
*interfaces  
auto lo  
iface lo inet loopback  
  
iface eth0 inet static  
address 192.168.1.114  
netmask 255.255.255.0  
gateway 192.168.1.1  
  
auto eth0  
  
iface eth1 inet static  
address 192.168.1.28  
netmask 255.255.255.0  
gateway 192.168.1.1  
  
iface eth1:1 inet static  
address 192.168.1.228  
netmask 255.255.255.0  
gateway 192.168.1.1  
  
auto eth1
```

Ln 22, Col 1 INS

Introducción:

GNU/LINUX: /proc/sys/net/ipv4/ip_forward



Introducción:

GNU/LINUX: */proc/sys/net/ipv4/ip_forward*

Activación del enrutamiento en Linux

- ❑ Las funciones de enrutamiento mediante NAT son realizadas por el cortafuegos que analizará los paquetes provenientes de la red local interna cuyo destino sea Internet y los modificará convenientemente para que salgan hacia Internet como si fueran emitidos por el servidor. A partir del núcleo 2.4 de Linux, el cortafuegos empleado es iptables.
- ❑ Para posibilitar que nuestro servidor Linux sea capaz de comportarse como un router y hacer de puerta de enlace para los PCs de nuestra red local, será necesario crear un script que configure el cortafuegos iptables para que realice NAT desde dentro de la red local hacia Internet.

Creación del script para activar enrutamiento

- ❑ Para activar el enrutamiento en un sistema Linux, tan solo basta con poner a '1' la variable ip_forward del sistema, es decir, basta con ejecutar desde una consola de root:

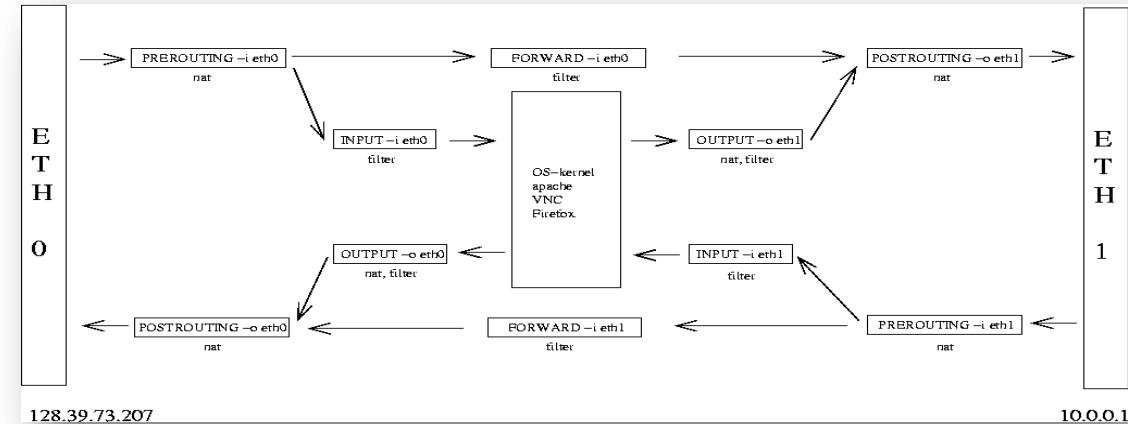
```
echo "1" > /proc/sys/net/ipv4/ip_forward
```

Introducción:

GNU/LINUX: /proc/sys/net/ipv4/ip_forward

- Posteriormente tendríamos que configurar el filtrado de paquetes para que acepte el redireccionamiento de paquetes desde dentro hacia fuera de nuestra red y mediante NAT permita que los PCs de la red interna naveguen con la dirección IP 'publica' del servidor. Supongamos que el router Linux tiene una tarjeta (eth0) conectada a la red local (172.16.15.1/255.255.255.0) y que tenemos una tarjeta (eth1) conectada al router, con la ip 192.168.36.140, los comandos a ejecutar serían:

```
// Haciendo NAT en el servidor
# iptables -A FORWARD -j ACCEPT
# iptables -t nat -A POSTROUTING -s 172.16.15.0/24 -o eth1 -j SNAT --to
192.168.36.140
```



Introducción:

GNU/LINUX: */proc/sys/net/ipv4/ip_forward*

- ❑ Podríamos realizar un script que activara el enrutamiento y el NAT y otro para desactivarlo:

```
// activar-enrutamiento.sh
echo "1" > /proc/sys/net/ipv4/ip_forward
iptables -A FORWARD -j ACCEPT
iptables -t nat -A POSTROUTING -s 172.16.15.0/24 -o eth1 -j SNAT --to 192.168.36.140
```

```
// desactivar-enrutamiento.sh
echo "0" > /proc/sys/net/ipv4/ip_forward
```

Activación automática del enrutamiento al arrancar el equipo

Si hemos creado el script de enrutamiento lo único que tenemos que hacer es dar permisos de ejecución y:

update-rc.d activar-enrutamiento.sh defaults

\$ sudo update-rc.d [servicio] defaults

Cortafuegos o Firewall:

Introducción a la seguridad perimetral mediante cortafuegos

- Un cortafuegos es una de las varias formas de proteger una red de otra red no fiable desde el punto de vista de la seguridad. Los mecanismos reales mediante los cuales se implementan las funciones del cortafuegos son muy variados, pero en general, el cortafuegos puede verse como ***la unión de un mecanismo para boquear tráfico y otro para permitirlo.*** Algunos cortafuegos hacen especial hincapié en el primero, mientras que otros se basan fundamentalmente en el segundo.
- La razón para la instalación de cortafuegos es proteger una red privada de intrusos, pero permitiendo a su vez el acceso autorizado desde y hacia el exterior. Otra razón importante es que pueden proporcionar un bastión en el que centrar los esfuerzos de administración y auditoria. Por último, un cortafuegos puede actuar como representante de la empresa en Internet ya que muchas compañías usan sus cortafuegos para almacenar información pública sobre los servicios y/o productos que ofrece.

Cortafuegos o Firewall: Introducción a la seguridad perimetral mediante cortafuegos

- ❑ Hay muchas formas en las que la seguridad de un cortafuegos puede verse comprometida. Aunque ninguna de estas situaciones es buena, hay algunas que son claramente más peligrosas que otras. Dado qué el propósito de muchos cortafuegos es boquear el acceso externo a una red privada, un claro fallo del sistema es la existencia de algún lazo que permita alcanzar máquinas que se encuentran dentro de la red protegida. Cualquier empleado utilizando un dispositivo para hacer una conexión a Internet mediante el protocolo PPP y comprometer la seguridad de toda la red.
- ❑ Una situación más peligrosa se produce si alguien es capaz de entrar en la máquina cortafuegos y reconfigurarla de modo que toda la red protegida quede accesible. Este tipo de ataque se suele denominar destrucción del cortafuegos. Los daños derivados de este tipo de ataque resultan muy difíciles de evaluar. Una medida importante de cómo un cortafuegos es capaz de soportar un ataque, es la información que almacena los logs para ayudar a determinar cómo se produjo. La peor situación posible es la que resulta de la destrucción de un cortafuegos sin que queden trazas de cómo se perpetró el ataque.

Cortafuegos o Firewall: Introducción a la seguridad perimetral mediante cortafuegos

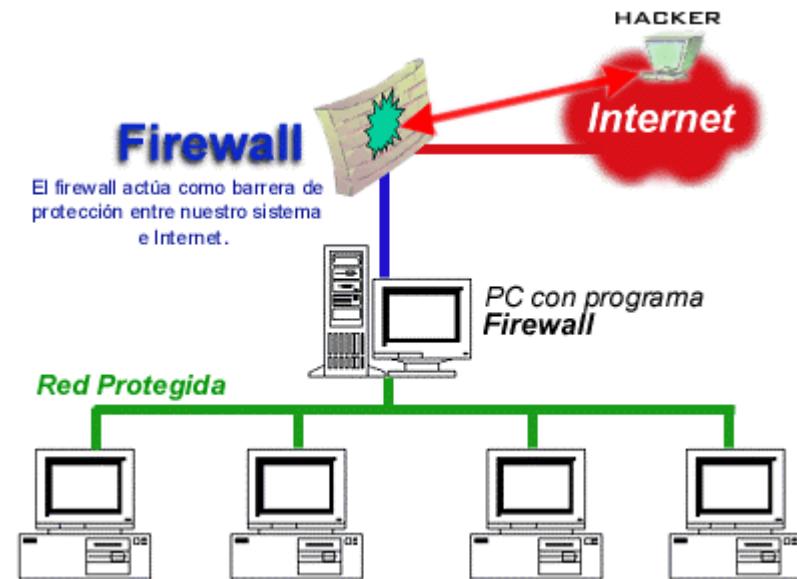
- Una forma de ver el efecto del fallo de un cortafuegos es en términos de la zona de riesgo que crea su fallo. Si una red se encuentra conectada a Internet directamente, toda la red es susceptible de ser atacada (toda es una zona de riesgo). Eso no significa que la red sea necesariamente vulnerable, sino que es necesario reforzar las medidas de seguridad en todas y cada una de las máquinas que forman la red. Esto es extremadamente difícil a medida que aumenta el número de máquinas y el tipo de servicios de red que estas ofrecen a sus usuarios. Aplicaciones como rlogin o telnet representan un peligro potencial, usado habitualmente por los hackers para ir ganando acceso a diferentes máquinas y usarlas como plataformas para nuevos ataques.

Un cortafuegos típico reduce la zona de riesgo al propio cortafuegos o a un reducido grupo de nodos de la red, simplificando notablemente el trabajo del administrador. Si el cortafuegos falla, la zona de riesgo puede expandirse hasta alcanzar a toda la red protegida. Si un hacker gana acceso al cortafuegos, puede utilizarlo como plataforma para lanzar ataques contra las máquinas de la red interna.

Cortafuegos o Firewall:

Introducción a la seguridad perimetral mediante cortafuegos

- Se debe tener claro que un cortafuegos no puede proteger de ataques que no se produzcan a través del mismo. Si una compañía posee información reservada en los ordenadores de su red interna, el contrafuegos no podrá protegerla contra un ataque desde dentro. Por ello, esa parte de la red interna debería estar aislada, o bien contar con medidas extras de protección.
- Un cortafuegos tampoco puede proteger contra virus o contra ataques debidos a los datos que se transfieren salvo que se combine con algún tipo de software antivirus. Es responsabilidad final de los usuarios y de los responsables de cada máquina particular, la protección contra este tipo de riesgos. Se debe prestar especial atención a los troyanos, a fin de evitar ataques desde el interior.



Cortafuegos o Firewall:

Tipos de Cortafuegos

- En la configuración de un cortafuegos, la principal decisión consiste en elegir entre seguridad o facilidad de uso. Este tipo de decisión es tomado en general por las direcciones de las compañías. Algunos cortafuegos sólo permiten tráfico de correo electrónico a través de ellos, y por lo tanto protegen a la red contra cualquier ataque que no sea a través del servicio de correo. Otros son menos estrictos y sólo bloquean aquellos servicios que se sabe que presentan problemas de seguridad.

Existen dos aproximaciones básicas:

- ✓ *Todo lo que no es expresamente permitido está prohibido.*
- ✓ *Todo lo que no es expresamente prohibido está permitido.*

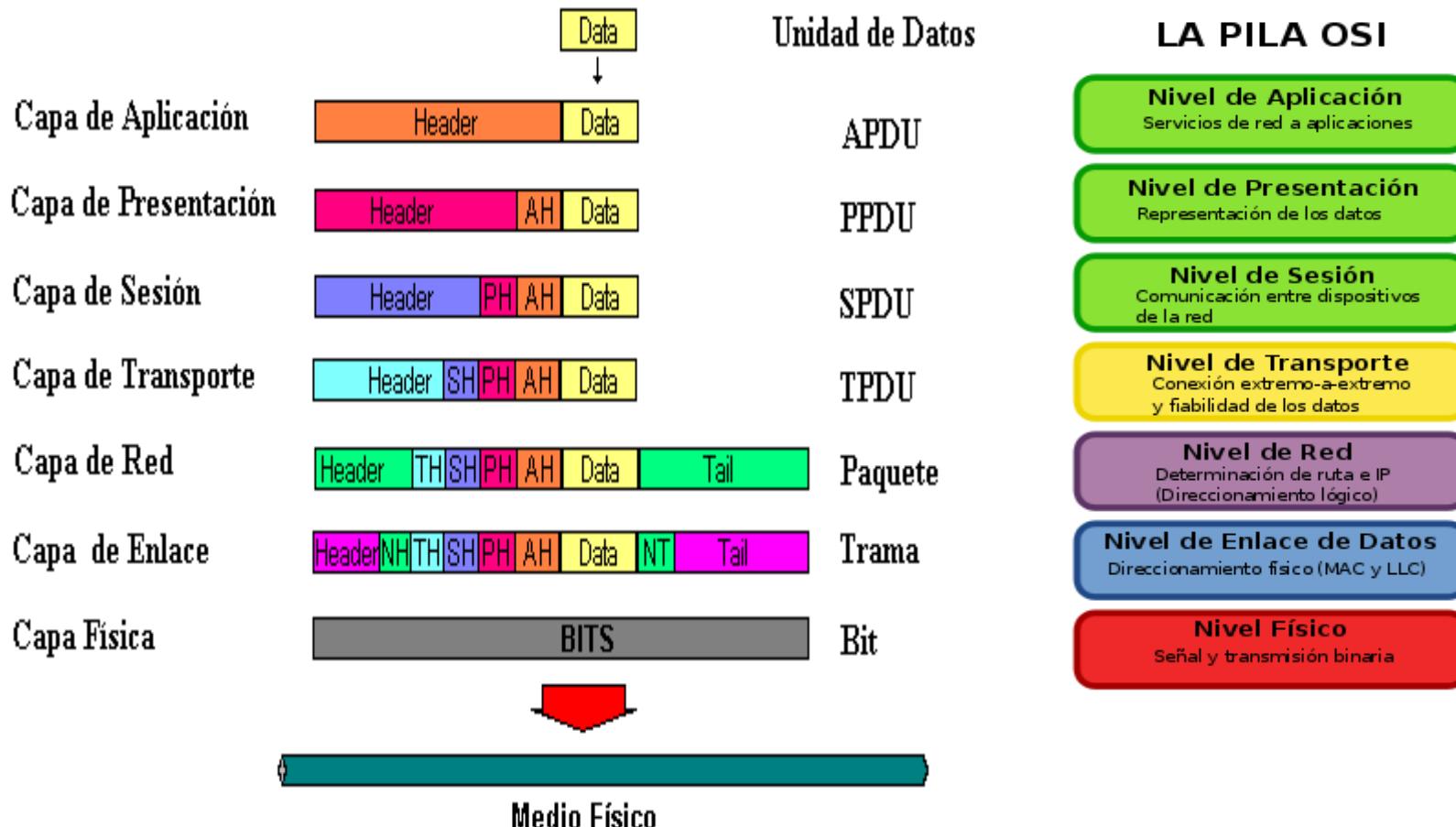
Cortafuegos o Firewall:

Tipos de Cortafuegos

- ❑ En el primer caso, el cortafuegos se diseña para bloquear todo el tráfico, y los distintos servicios deben ser activados de forma individual tras el análisis del riesgo que representa su activación y la necesidad de su uso. Esta política incide directamente sobre los usuarios de las comunicaciones, que pueden ver el cortafuegos como un estorbo.
- ❑ En el segundo caso, el administrador del sistema debe predecir que tipo de acciones pueden realizar los usuarios que pongan en entredicho la seguridad del sistema, y preparar defensas contra ellas. Esta estrategia penaliza al administrador frente a los usuarios. Los usuarios pueden comprometer inadvertidamente la seguridad del sistema si no conocen y cumplen unas consideraciones de seguridad mínimas. El problema se magnifica si existen usuarios que tengan cuenta en la propia máquina que hace de cortafuegos (situación muy poco recomendable). En este tipo de estrategia hay un segundo peligro latente, y es que el administrador debe conocer todos los posibles agujeros de seguridad existentes en los protocolos y las aplicaciones que están ejecutando los usuarios. El problema se agrava debido al hecho de que los fabricantes no suelen darse prisa en notificar los riesgos de seguridad que presentan sus productos.

Cortafuegos o Firewall:

Capa de trabajo del Cortafuegos



Cortafuegos o Firewall:

Capa de trabajo del Cortafuegos

- Podemos clasificar los cortafuegos por la capa de la pila de protocolos en la que trabajen.

Cortafuegos a nivel de Red

Por lo general se trata de un encaminador (router) o una computadora especial que examina las características de los paquetes IP para decidir cuáles deben pasar y cuáles no. Por ejemplo se podría configurar el encaminador para que bloquee todos los mensajes que provengan de un sitio, así como todos los mensajes destinados a un determinado. Los profesionales de las redes a menudo denominan a este proceso como lista negra.

Normalmente se suele configurar un router para que tenga en cuenta la siguiente información para cada paquete antes de decidir si debe enviarlo:

- ✓ *Dirección IP de origen y destino (cabecera IP, nivel 3)*
- ✓ *Puerto origen y destino (campo de datos IP, cabecera nivel 4)*
- ✓ *Protocolo de los datos (TCP, UDP o ICMP) (cabecera IP, nivel 3)*
- ✓ *Si el paquete es inicio de una petición de conexión (campo de datos IP, cabecera nivel 4)*

Si se instala y se configura correctamente un cortafuegos a nivel de red, este será muy rápido y casi totalmente transparente para los usuarios. Para servidores Linux un software que permite realizar funciones de filtrado para implementar un cortafuegos a nivel de red es el IPChains o IPTables.

Cortafuegos o Firewall:

Capa de trabajo del Cortafuegos

Cortafuegos a nivel de circuito

- Se trata de una versión avanzada de los cortafuegos vistos en el punto anterior que trabajan en la **capa de transporte**. La seguridad en este caso está basada en el establecimiento, seguimiento y liberación de las conexiones que se realizan entre las máquinas internas y externas.
- Observan la conveniencia o no de la existencia de esas conexiones en función del tipo de aplicación que realiza la conexión y la procedencia de la petición. Además, realizan seguimiento en los números de secuencia de la conexión buscando aquellos paquetes que no corresponden con conexiones establecidas. Durante este seguimiento, se establece un circuito virtual entre el cliente y el servidor a través del cortafuegos, que hace transparente la existencia de dicho cortafuegos.

Cortafuegos o Firewall:

Capa de trabajo del Cortafuegos

Cortafuegos a nivel de aplicación

- Suele ser un ordenador que ejecuta software de servidor Proxy. La palabra "proxy" significa "actuar por poderes" o "en nombre de otro". Los servidores proxy hacen precisamente esto, se comunican con otros servidores del exterior de la red en nombre de los usuarios.
- En otras palabras un servidor proxy controla el tráfico entre dos redes estableciendo la comunicación entre el usuario y él mismo y entre él mismo y el ordenador destino. De este modo la red local queda oculta para el resto de Internet. Un usuario que acceda a Internet a través de un servidor proxy aparecerá para los otros ordenadores como si en realidad fuera el servidor proxy (se muestra la dirección IP de este). Esto combinado con un servicio NAT, puede hacer completamente invisibles las direcciones IP de los ordenadores de la red interna hacia el exterior.

Cortafuegos o Firewall:

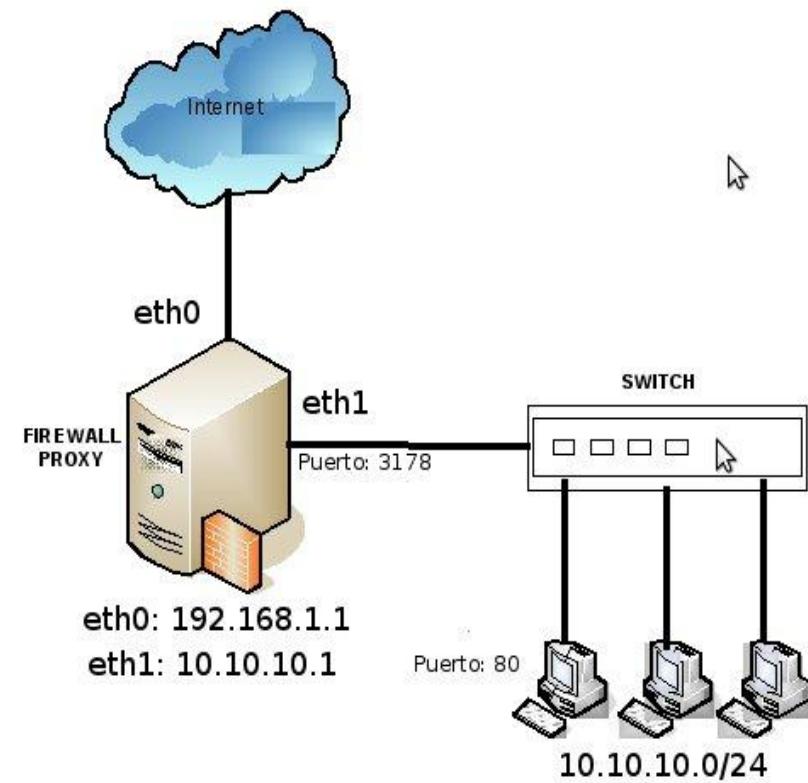
Capa de trabajo del Cortafuegos

- ❑ Como trabaja a nivel de aplicación, este tipo de cortafuegos es más seguro y potente, pero también menos transparente y rápido que un encaminador. Existen servidores proxy disponibles para diferentes servicios como HTTP, FTP, Gopher, SMTP y Telnet. Es necesario configurar un servidor proxy diferente (aunque pueden residir en la misma máquina) para cada servicio que se desee proporcionar.
- ❑ Dos de los servidores proxy más populares para las redes basadas en UNIX y Linux son TIS Internet Firewall Toolkit y SOCKS. Para servidores Windows NT tanto el Internet Information Server (IIS) de Microsoft, como el Commerce Server de Netscape incluyen servidores proxy.
- ❑ Al implementar un servidor proxy a nivel de aplicación, los usuarios de la red deberán utilizar programas clientes que puedan trabajar con un proxy. Los diseñadores han creado muchos protocolos TCP/IP, como HTTP, FTP y otros, pensando en la posibilidad de utilizar un proxy. En la mayoría de los navegadores web, los usuarios pueden establecer fácilmente sus preferencias de configuración para seleccionar el servidor proxy a utilizar.

Cortafuegos o Firewall:

Capa de trabajo del Cortafuegos

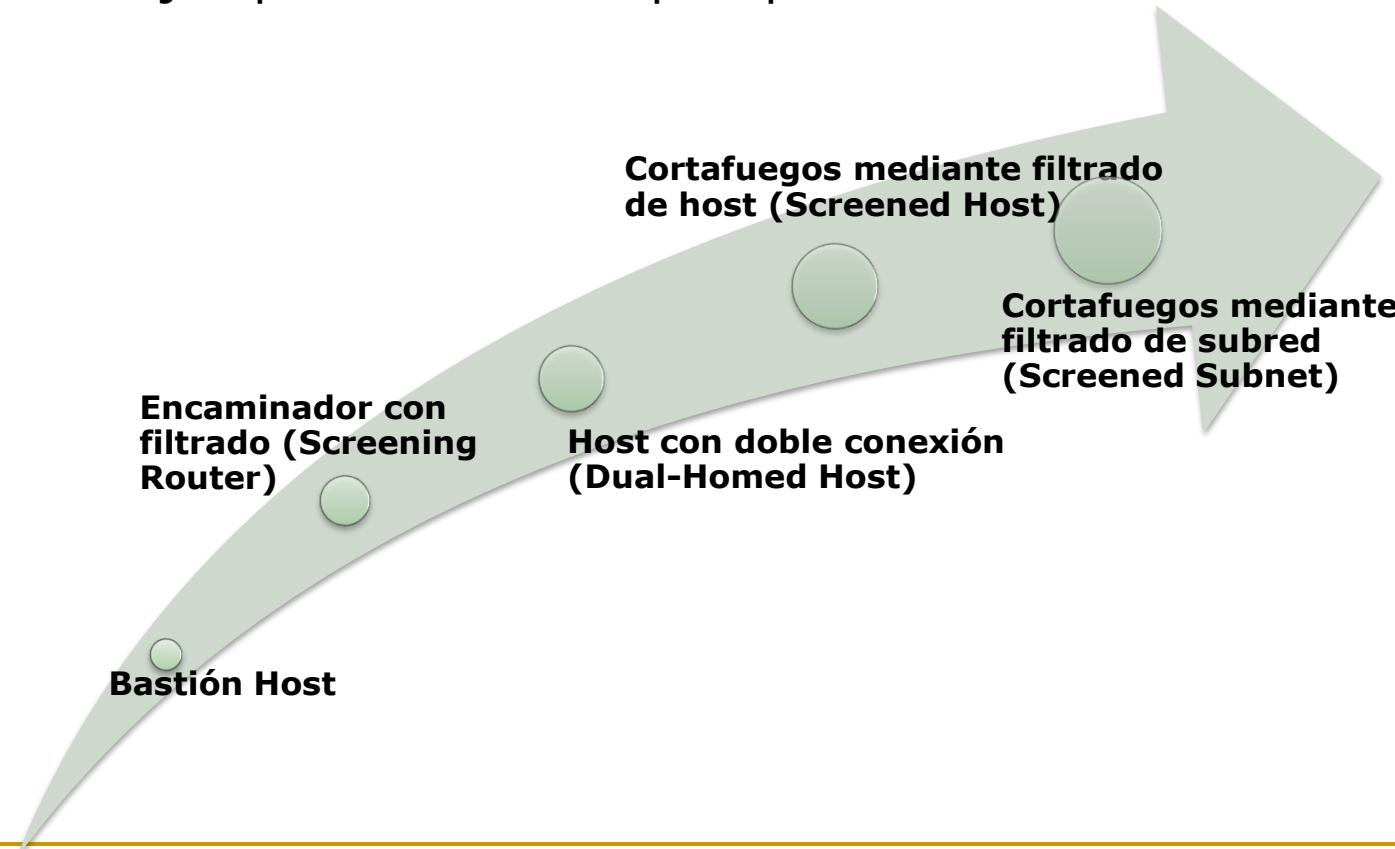
- Desgraciadamente no todos los protocolos están pensados para utilizar un proxy, y en esos casos puede ser necesario seleccionar las aplicaciones para Internet según su compatibilidad con un protocolo proxy habitual, por ejemplo SOCKS.
- Como contrapartida a todos los posibles inconvenientes, el software de proxy se pueden combinar la utilización de antivirus para detectar, dentro de los contenidos que se intercambian las aplicaciones a través del proxy, las huellas de virus en los mensajes de correo, documentos, applets embebidos en páginas HTML (Java, ActiveX, ...), ejecutables, etc. y eliminarlos o advertir del riesgo al usuario.



Cortafuegos o Firewall:

Topología de Cortafuegos

- Aunque el propósito da todos los cortafuegos es el mismo, existen diferencias en sus topologías y prestaciones. Los siguientes son algunos ejemplos de las múltiples posibilidades existentes:

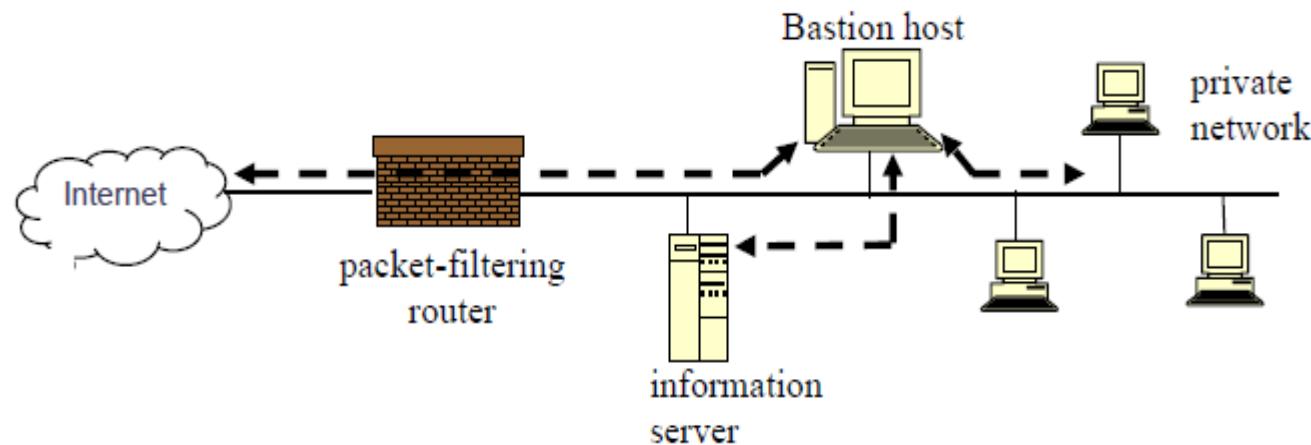


Cortafuegos o Firewall:

Topología de Cortafuegos

Bastión Host

- Son sistemas identificados por el administrador de la red como puntos clave en la seguridad de la red. Son auditados regularmente y pueden tener software modificado para filtrar y bloquear determinados intentos de conexión, trazar las comunicaciones y reparar fallos de seguridad del sistema.
- Un ejemplo simple es el caso de la instalación de un software de cortafuegos personal en el equipo del usuario. Mediante este tipo de software el usuario puede controlar, bloquear y filtrar el tráfico de datos que entra y sale por cada uno de los puertos de comunicación de su ordenador personal, tanto si utiliza aplicaciones cliente, como si ofrece servicios a equipos remotos.



Cortafuegos o Firewall:

Topología de Cortafuegos

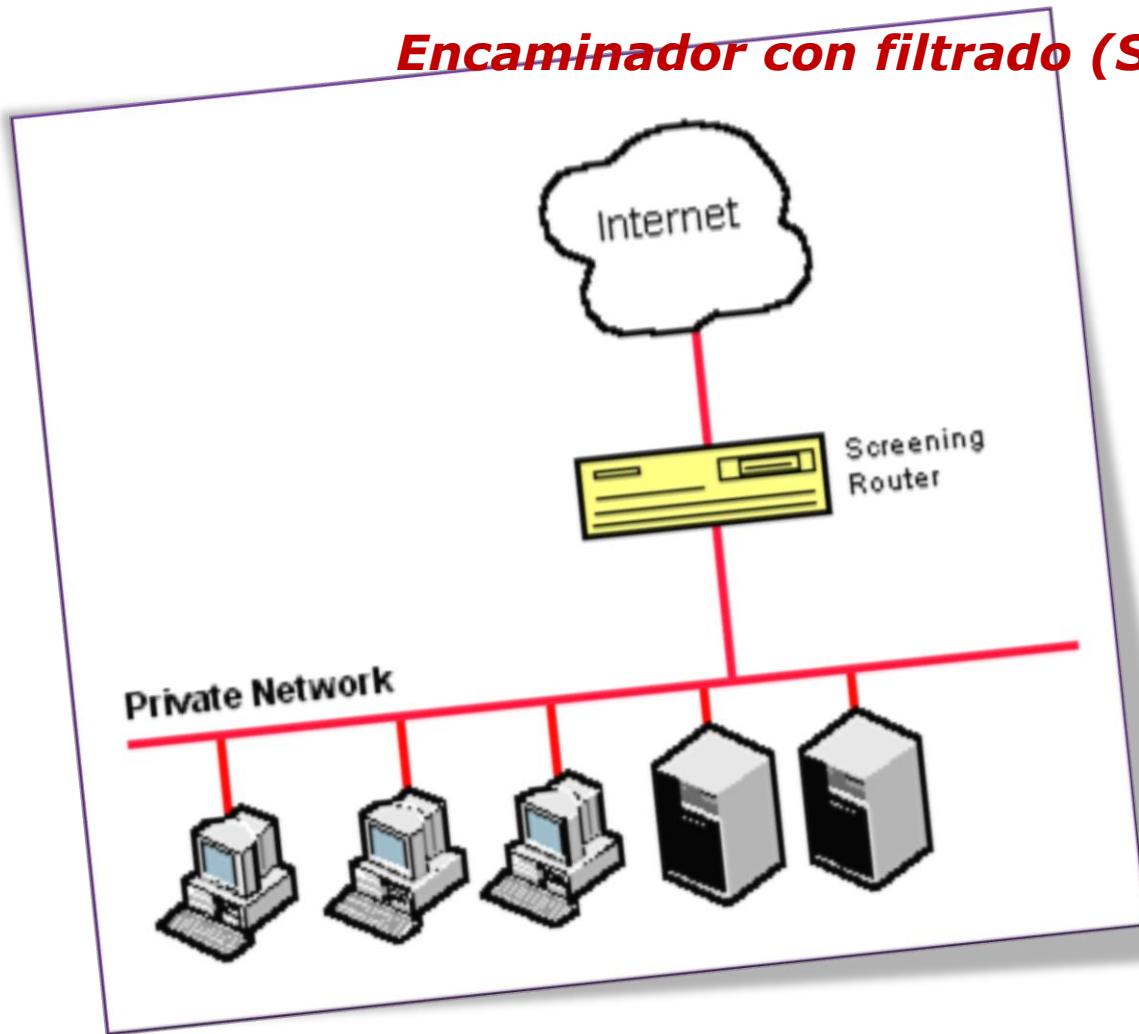
Encaminador con filtrado (Screening Router)

- Son un componente básico de la mayor parte de los cortafuegos. Pueden ser un router comercial o basado en un ordenador convencional, con capacidad para filtrar paquetes. Tienen la capacidad para bloquear el tráfico entre redes o nodos específicos basándose en direcciones y puertos TCP/IP (trabajan a nivel de red). Algunos cortafuegos sólo consisten en un "screening router" entre la red privada e Internet.
- En general permite la comunicación entre múltiples nodos de la red protegida y de Internet. La zona de riesgo es igual al número de nodos de la red protegida y el número y tipo de servicios para los que se permite el tráfico. Es difícil controlar los daños que pueden producirse dado que el administrador de la red debe examinar regularmente cada host para buscar trazas de ataques.
- Es casi imposible reconstruir un ataque que haya llevado a la destrucción del cortafuegos, e incluso puede ser difícil detectar la propia destrucción, aunque algunos poseen capacidades de registro de eventos para paliar esto. En general responden a configuraciones en las que lo que no está expresamente prohibido, está permitido. No son la solución más segura, pero son muy populares dado que permiten un acceso a Internet bastante libre desde cualquier punto de la red privada.

Cortafuegos o Firewall:

Topología de Cortafuegos

Encaminador con filtrado (Screening Router)

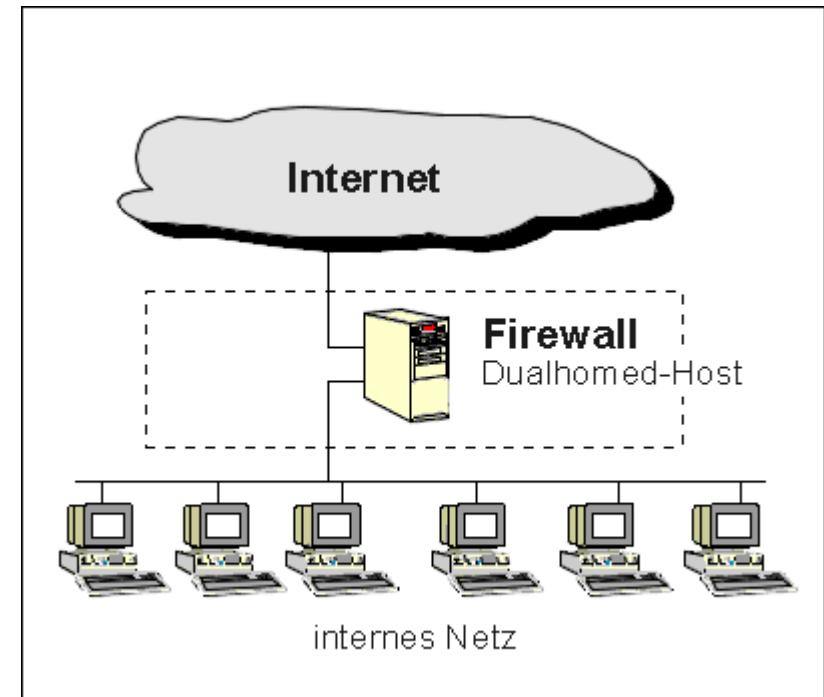


Cortafuegos o Firewall:

Topología de Cortafuegos

Host con doble conexión (Dual-Homed Host)

- Algunos cortafuegos son implementados sin necesidad de un screening router. Para ello se conecta un servidor mediante dos tarjetas independientes a la red que se quiere proteger y a Internet, desactivando las funciones de reenvío TCP/IP. Este dispositivo puede ser un bastion host y funcionar como servidor (Web, FTF, ...) tanto para la red interna como para la red externa. Los hosts de la red privada pueden comunicarse con el bastión host, al igual que los nodos de Internet, pero el tráfico directo entre ambos tipos de nodos está bloqueado.



Cortafuegos o Firewall:

Topología de Cortafuegos

Host con doble conexión (Dual-Homed Host)

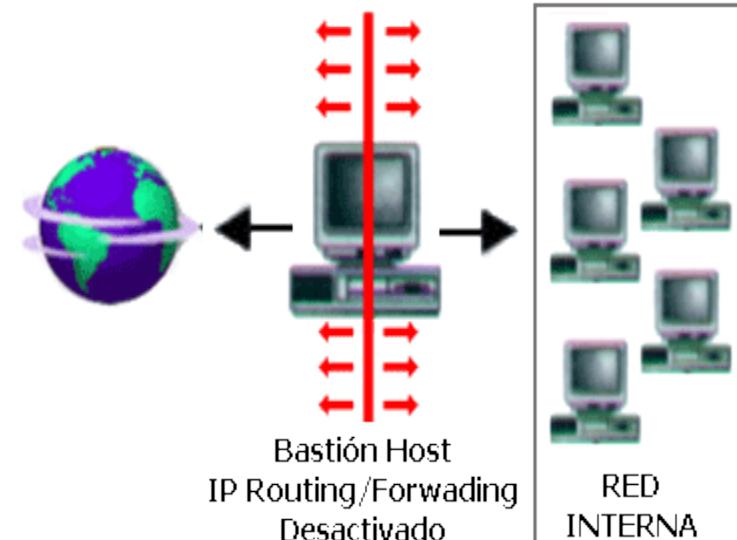
- ❑ Esta estructura de cortafuegos es empleada habitualmente debido a que es fácil de implementar. Al no reenviar el tráfico TCP/IP, bloquea completamente la comunicación entre ambas redes. Su facilidad de uso depende de la forma en la que el administrador proporciona el acceso a los usuarios:
 - ✓ Proporcionando pasarelas para las aplicaciones.
 - ✓ Proporcionando cuentas a los usuarios en el bastion host.
- ❑ En el primer caso se está en una situación en la que lo que no está explícitamente permitido, está prohibido. El permiso para el uso de cada aplicación se suele habilitar instalando el software de proxy adecuado para cada una de ellas.
- ❑ En el segundo caso, el acceso de los usuarios a Internet es más sencillo, pero la seguridad puede verse comprometida. Si un hacker gana acceso a una cuenta de usuario, tendrá acceso a toda la red protegida. La cuenta de un usuario puede verse comprometida por elegir una contraseña sencilla de adivinar, o por algún descuido. El principal inconveniente es que un hacker mínimamente preparado puede borrar sus huellas fácilmente, lo que hace muy difícil descubrir el ataque. Si el único usuario es el administrador, la detección del intruso es mucho más fácil, ya que el simple hecho de que alguien entrado en el sistema es un indicativo de que sucede algo raro.

Cortafuegos o Firewall:

Topología de Cortafuegos

Host con doble conexión (Dual-Homed Host)

- Esta estructura de cortafuegos ofrece la ventaja sobre un screening router, de que es más fácil actualizar el software del sistema para obtener registros del sistema en distintos tipos de soporte, lo que facilita el análisis de la situación en caso de que la seguridad se haya visto comprometida.
- El aspecto más débil de esta estructura es su modo de fallo. Si el cortafuegos es destruido, es posible que un hacker preparado reactive el reenvío TCP/IP teniendo libre acceso a toda la red protegida. Para detectar esta situación conviene tener al día las revisiones del software con el fin de eliminar los bugs de seguridad. Además no conviene hacer público el tipo y versión del sistema operativo instalado en la máquina para no facilitar el trabajo de los posibles atacantes.



Cortafuegos o Firewall:

Topología de Cortafuegos

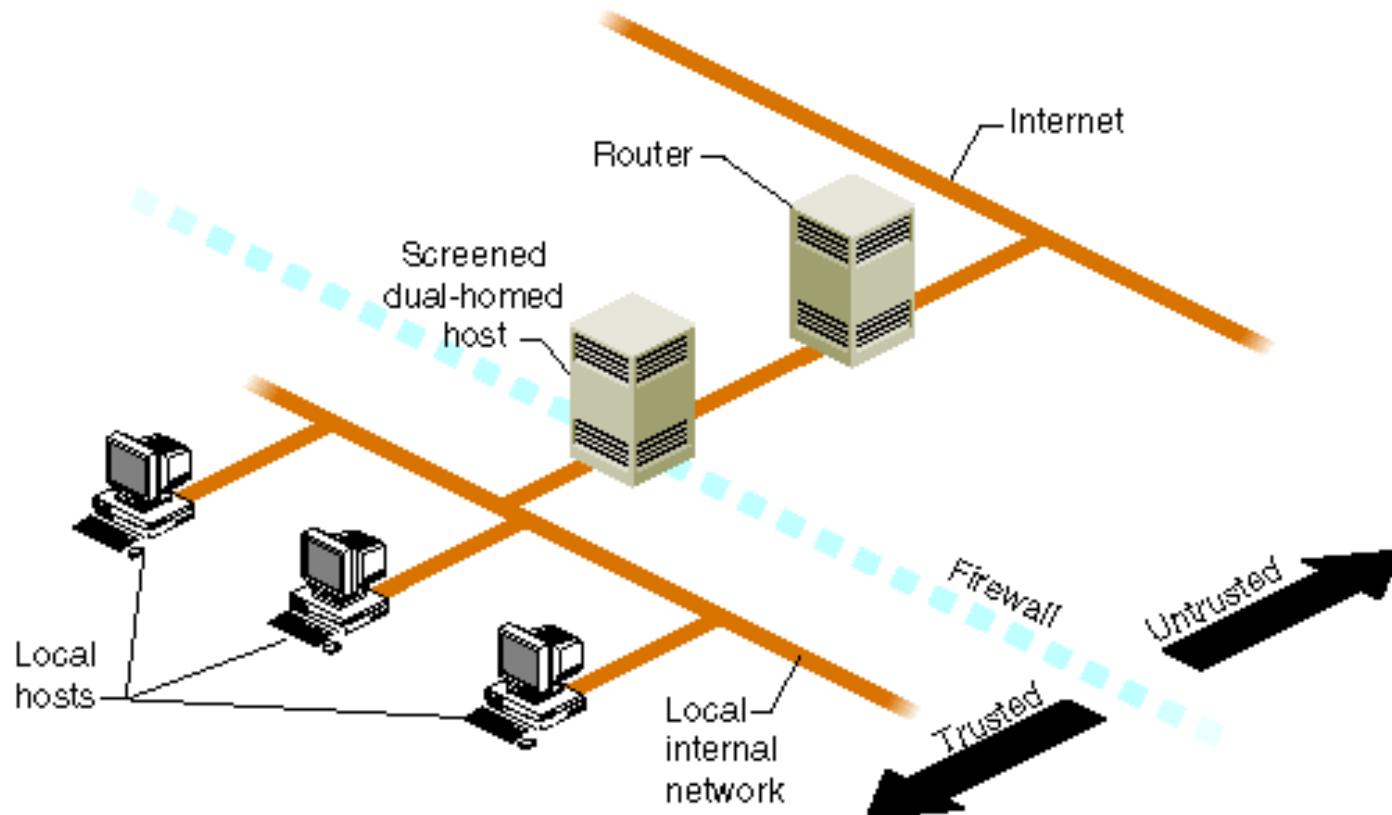
Cortafuegos mediante filtrado de host (Screened Host)

- ❑ Es la configuración de cortafuegos más común. Está implementada usando un bastion host/Dual-Homed Host y un screening ruter. Habitualmente el bastion host/Dual-Homed Host está en la red privada, y el screening router está configurado de modo que el bastion host/Dual-Homed Host es el único nodo de dicha red que es accesible desde Internet para un pequeño número de servicios.
- ❑ Como el bastion host/Dual-Homed Host está en la red privada, la conectividad para los usuarios es muy buena, eliminando los problemas que suelen aparecer al tener definidas rutas extrañas. Si la red privada es una red local virtual extensa, el esquema funciona sin necesidad de cambios en las direcciones de la red local siempre que ésta este usando direcciones IP válidas. La zona de riesgo se circumscribe bastion host/Dual-Homed Host y el screening router. La seguridad de éste último depende del software que execute. Para el bastion host/Dual-Homed Host , las consideraciones sobre seguridad y protección son similares a las hechas para un sistema del tipo host de doble conexión.

Cortafuegos o Firewall:

Topología de Cortafuegos

Cortafuegos mediante filtrado de host (Screened Host)

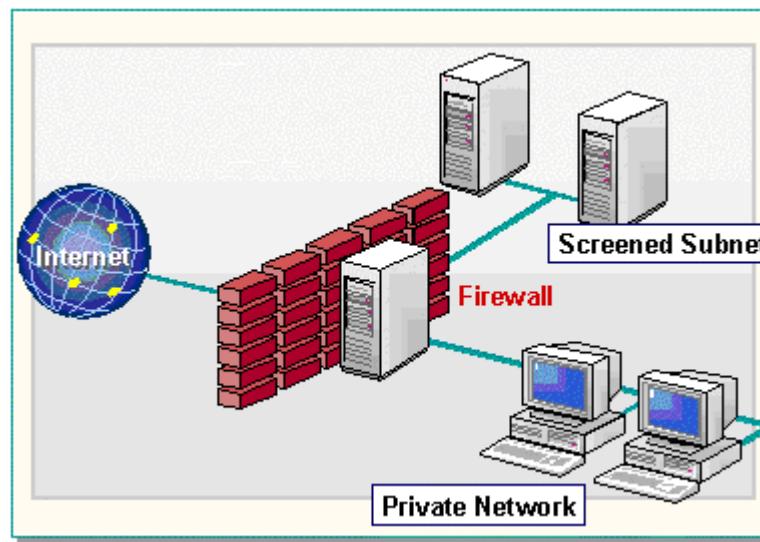


Cortafuegos o Firewall:

Topología de Cortafuegos

Cortafuegos mediante filtrado de subred (Screened Subnet)

- En algunas configuraciones de cortafuegos se crea una subred aislada, situada entre la red privada e Internet. La forma habitual de usar esta red consiste en emplear screening routers configurados de forma que los nodos de dicha subred son alcanzables desde Internet y desde la red privada. Sin embargo, el tráfico desde Internet hacia la red privada es bloqueado.

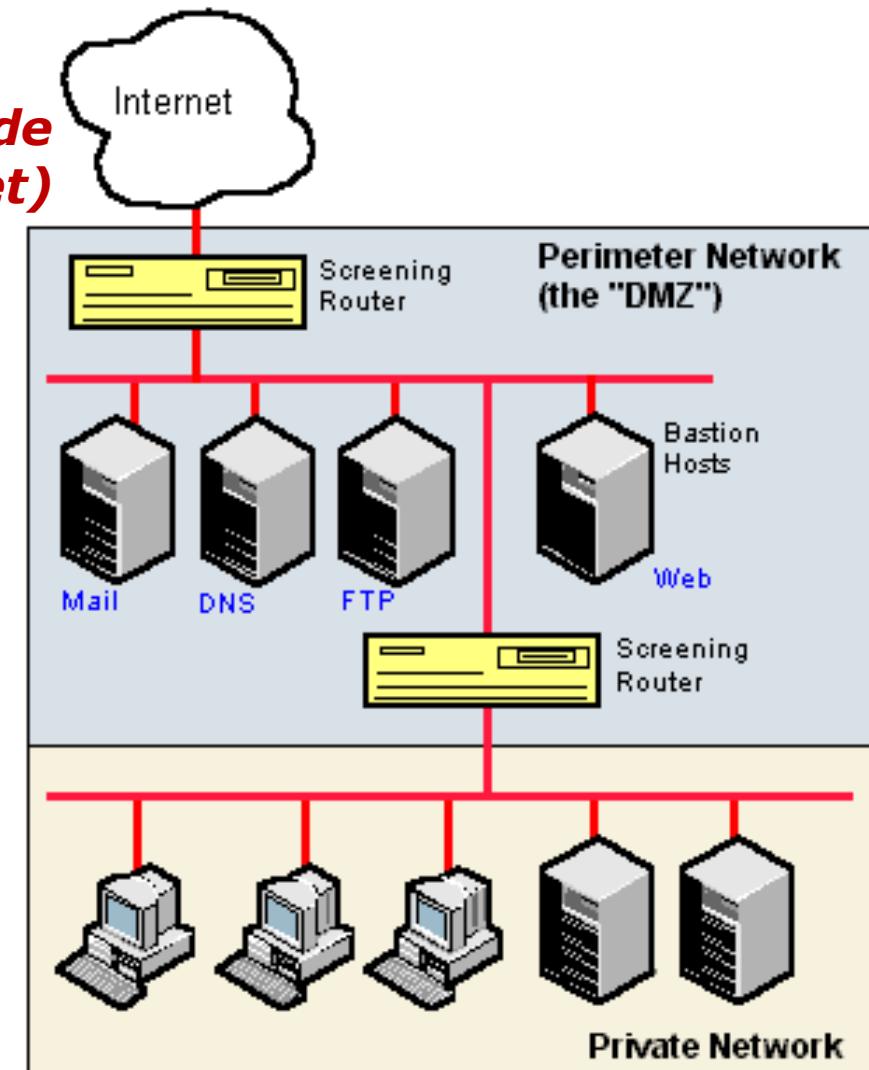


Cortafuegos o Firewall:

Topología de Cortafuegos

Cortafuegos mediante filtrado de subred (Screened Subnet)

- Si este tipo de cortafuegos es atacado en un intento de destruirlo, la hacker debe reconfigurar el tráfico en tres redes, sin desconectarlas, sin dejarse encerrado a si mismo. y sin que los cambios sean detectados por máquinas y usuarios. Aunque esto puede ser posible, todavía puede dificultarse más si los routes sólo son accesibles para su reconfiguración desde máquinas situadas en la red privada.



Cortafuegos o Firewall:

Topología de Cortafuegos

Cortafuegos mediante filtrado de subred (Screened Subnet)

- Otra ventaja de este tipo de cortafuegos es que pueden ser instalados de forma que oculten la estructura de la red privada. La subred expuesta es muy dependiente del conjunto de software que se ejecute en el screening routers. La funcionalidad es similar a la obtenida en los casos anteriores, sin embargo la complejidad de configuración y encaminamiento es mucho mayor.

La subred que incluye el cortafuegos y los encaminadores se denomina Zona Neutra o Zona Desmilitarizada (Demilitarized Zone - DMZ). En esta zona desmilitarizada pueden encontrarse más servidores, bien orientados a dar servicios a usuarios que acceden desde la red externa (red abierta), o bien para facilitar los servicios de proxy y el acceso a internet a los usuarios de la red interna.

Cortafuegos o Firewall:

Aplicabilidad

- ❑ No se puede hablar de que tipo de cortafuegos es el mejor, ya que dicha afirmación depende de muchos factores que hacen que cada caso pueda tener una respuesta diferente. Entre dichos factores figuran el coste, la política de la empresa, la tecnología de red y el personal que se tiene disponible. Todos estos factores pueden pesar más que consideraciones puramente técnicas.
- ❑ Conviene tener en cuenta que un cortafuegos es un dispositivo de red de importancia creciente, al menos desde el punto de vista de administración y seguridad. Debe considerarse como un punto desde el que poder controlar con más facilidad los riesgos a los que puede estar sometida una red. El concepto de zona de riesgo es fundamental. Lo ideal sería que cada nodo de la red protegida tuviese un alto nivel de seguridad de modo que el cortafuegos fuese redundante. Sin embargo, siendo realistas esta alternativa es poco viable.
- ❑ Otro aspecto fundamental es que un cortafuegos no puede ser considerado como una vacuna. No debe instalarse un determinado tipo de cortafuegos porque para alguien sea suficientemente seguro. Dicho concepto debe ser resultado de un análisis del coste de implantación, administración, nivel de protección obtenido y valor de los datos que se protegen. Es importante no tener prisas a la hora de tomar este tipo de decisiones, ya que el uso del cortafuegos no se reduce a su diseño e implementación, ya que para garantizar su éxito en la defensa de la red privada es necesario una cuidada labor de administración y vigilancia del mismo.

Cortafuegos o Firewall:

Configuración de un Cortafuegos. Sistemas GNU/Linux.

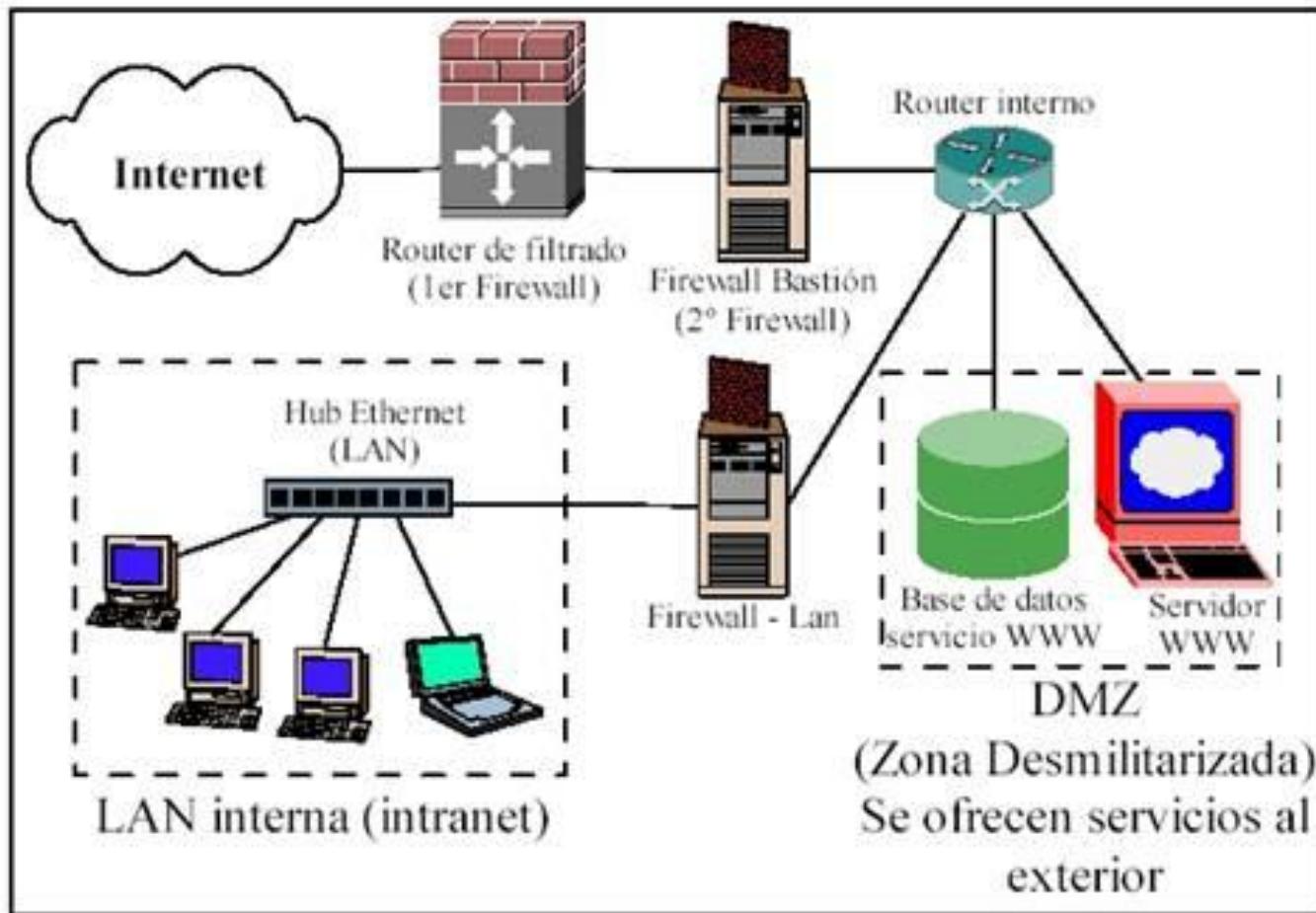
IPTABLES

- Como recordatorio y aunque no quiero aburrir nos volvemos a preguntar, *¿Qué es un firewall?* La traducción más acertada de este término inglés al Castellano es la palabra cortafuegos. Veamos cual es la definición en el DRAE. <<Cortafuego o cortafuegos. (De cortar y fuego). m. Agr. Vereda ancha que se deja en los sembrados y montes para que no se propaguen los incendios. || 2. Arq. Pared toda de fábrica, sin madera alguna, y de un grueso competente, que se eleva desde la parte inferior del edificio hasta más arriba del caballete, con el fin de que, si hay fuego en un lado, no se pueda este comunicar al otro.>>
- Estas dos definiciones nos dan una idea aproximada del significado de la palabra firewall en términos informáticos, en ellas, aparecen términos como lado, lo que implica la existencia de dos o más partes y comunicar lo que pone de manifiesto que las partes están conectadas.
- Un firewall en términos de sistemas computacionales es un sistema informático, simple o compuesto que actúa como punto de conexión segura entre otros dos o más ordenadores o redes.

Cortafuegos o Firewall:

Configuración de un Cortafuegos. Sistemas GNU/Linux.

IPTABLES



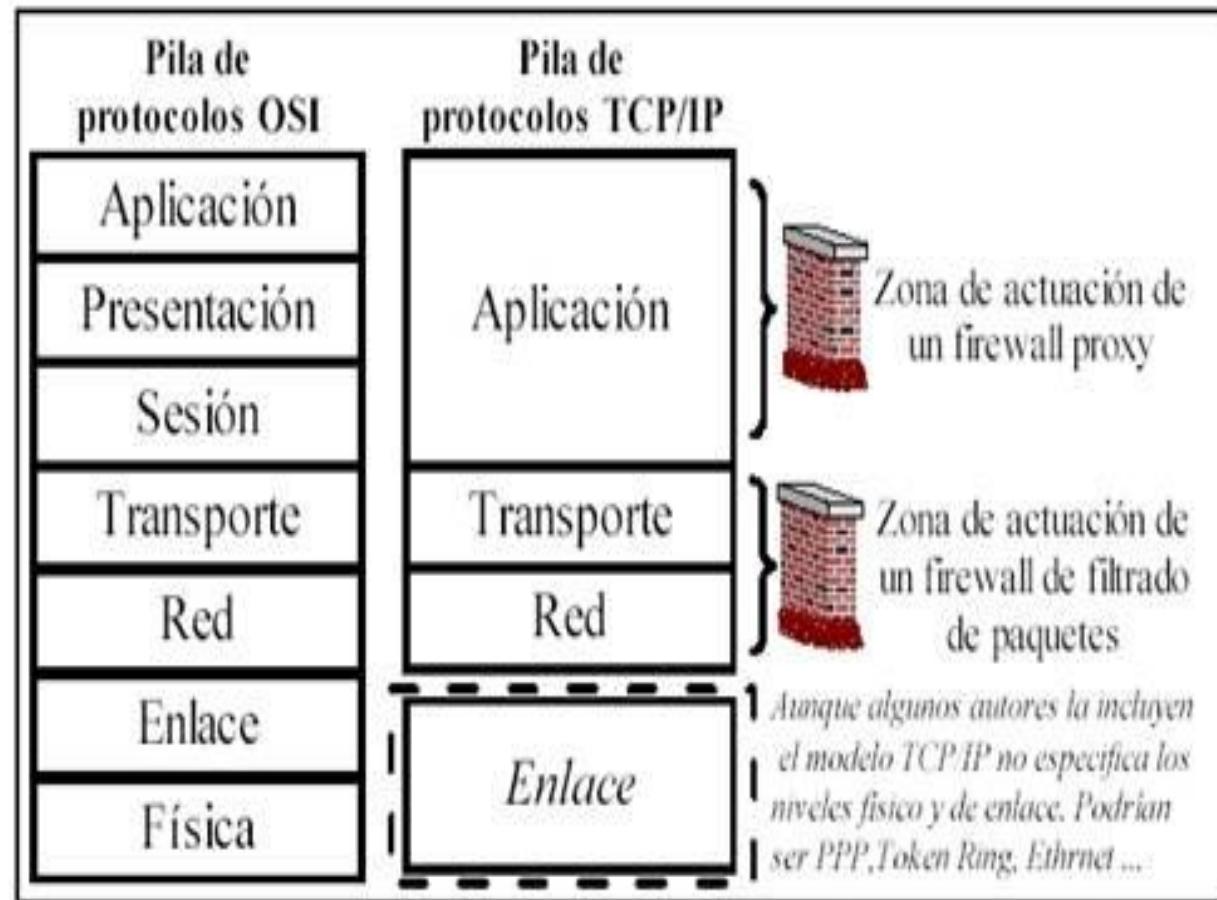
Cortafuegos o Firewall:

Configuración de un Cortafuegos. Sistemas GNU/Linux.

IPTABLES

❑ No se pretende realizar un estudio sobre la infinidad de familias y variedades de firewalls, seremos más concret@s, y nos centraremos en el estudio de un modelo de cortafuegos, la familia de los firewalls de filtrado de paquetes sobre la pila de protocolos TCP/IP, los llamados IPFW.

❑ Los IPFW funcionan como indican las dos primeras letras de IPFW, sobre paquetes IP, es decir, en el nivel de transporte y red de TCP/IP.



Cortafuegos o Firewall:

Configuración de un Cortafuegos. Sistemas GNU/Linux.

IPTABLES

- ❑ Los cortafuegos de filtrado de paquetes IP, suelen implementarse dentro del sistema operativo y funcionan en las capas de transporte y red, trabajando sobre la información de las cabeceras de los paquetes IP, es decir, que no analizarán el área de datos, sino que únicamente utilizan la información que puede obtenerse de una cabecera IP. Como ya habíamos dicho, habitualmente, un cortafuego se sitúa entre dos o más redes, lo que implica que tiene al menos dos interfaces de red.
- ❑ A pesar de que un cortafuegos separa dos redes cualquiera entre si, lo habitual, es que separe redes propietarias distintas. Es decir, aunque pueden utilizarse cortafuegos dentro de una misma red, filtrando las comunicaciones entre las distintas subredes internas, lo habitual, es que forme parte de una red propia y sea él quien vigile las comunicaciones con otra red o redes ajena en las que no se confía, por ejemplo, y sobre, todo Internet.
- ❑ Los firewalls, son principalmente, una herramienta de seguridad y prevención ante ataques externos. Es decir, un IPFW funciona filtrando las comunicaciones en ambos sentidos entre su interfaz interna (la que lo conecta a su red) y la externa. *El mecanismo de funcionamiento para realizar este filtrado es a través de una lista de reglas - reglas de filtrado -.*

Cortafuegos o Firewall: Configuración de un Cortafuegos. Sistemas GNU/Linux. **IPTABLES**

- En los sistemas GNU/Linux, Iptables es una de las herramientas cortafuegos más empleadas, que permite el filtrado de paquetes así como realizar funciones NAT (Network Address Translation) – Traducción de Dirección de Red-. No es necesario instalarlo porque viene incorporado en el núcleo de GNU/Linux

Nota: ¿¿NAT???

- ✓ *La idea básica que hay detrás de NAT es traducir las IPs privadas de la red en una IP pública para que la red pueda enviar paquetes al exterior; y traducir luego esa IP pública, de nuevo a la IP privada del PC que envió el paquete, para que pueda recibirla una vez llega la respuesta.*
- ✓ *Cuando uno de los PCs de la red local quiere enviar un paquete a Internet, se lo envía al router (o a la puerta de enlace o gateway), y éste hace lo que se conoce como SNAT (Source-NAT) y cambia la dirección de origen por su IP pública. Así, el host remoto sabrá a qué IP pública ha de enviar sus paquetes. Cuando una respuesta o un paquete pertenecientes a esa conexión llegue al router, éste traducirá la dirección IP de destino del paquete (que ahora es la IP del router) y la cambiará por la dirección privada del host que corresponde, para hacer la entrega del paquete a la red local.*

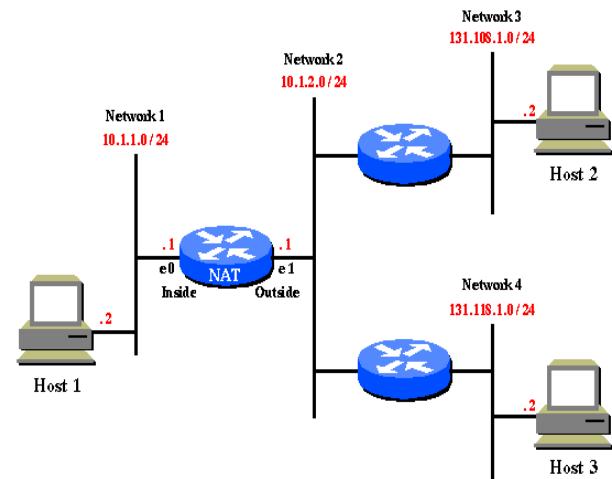
Cortafuegos o Firewall:

Configuración de un Cortafuegos. Sistemas GNU/Linux.

IPTABLES

DNAT: Destination-NAT

- ✓ Hasta ahora hemos visto como actúa el software de NAT para permitir que un PC de una red privada pueda acceder a Internet y recibir respuestas. El mecanismo que utiliza NAT para las asociaciones entre IP pública y IP privada es una tabla (tabla de NAT) en la que guarda una entrada por cada conexión. Cuando un host de la red local inicia una conexión hacia el exterior, el software de NAT asigna una entrada en la tabla, para que a partir de ahora, todo lo que llegue perteneciente a esa conexión sea traducido hacia la IP privada que inició la conexión.
- ✓ Pero ¿qué pasa si la conexión se inicia desde el exterior? Por ejemplo, si montamos en nuestra red local un servidor web, lo que queremos es que se puedan iniciar conexiones hacia él. Para poder hacer esto se utiliza DNAT (Destination-NAT).



Cortafuegos o Firewall:

Configuración de un Cortafuegos. Sistemas GNU/Linux.

IPTABLES

- ✓ Cuando iniciábamos una conexión desde la red local, se creaba automáticamente una entrada en la tabla de NAT para que todo lo que perteneciera a esa conexión fuera dirigido hacia el PC correspondiente. Pero si la conexión se inicia desde fuera ¿como y cuando se crea esa entrada en la tabla de NAT? La respuesta es que si queremos permitir conexiones desde el exterior a un PC de nuestra red local, hemos de añadir una entrada fija en la tabla de NAT, indicando que todo el tráfico que llegue que vaya a determinado puerto, sea dirigido al PC en cuestión. El puerto es el único elemento que tenemos para “distinguir” conexiones, ya que todo llegará a la IP del router, pero tendrán un puerto de destino según sea una conexión u otra. Así que, en nuestro ejemplo, deberíamos crear una entrada fija en la tabla de NAT en la que indicáramos que lo que llegue al puerto 80 (web) sea dirigido al PC en el que corre el servidor web.
- ✓ Esto es lo que se conoce habitualmente como “abrir puertos” en el router. Al abrir puertos, simplemente estamos añadiendo una entrada a la tabla de NAT del router para que sepa hacer la traducción y sepa a qué PC enviar los paquetes. Ya que desde el exterior, aunque nuestra red tenga varios PCs, se verá como si sólo fuera uno (solo se conoce la IP del router, éste lo traduce todo) y necesitamos que éste router al que le llega todo el tráfico sepa a quién ha de entregárselo.

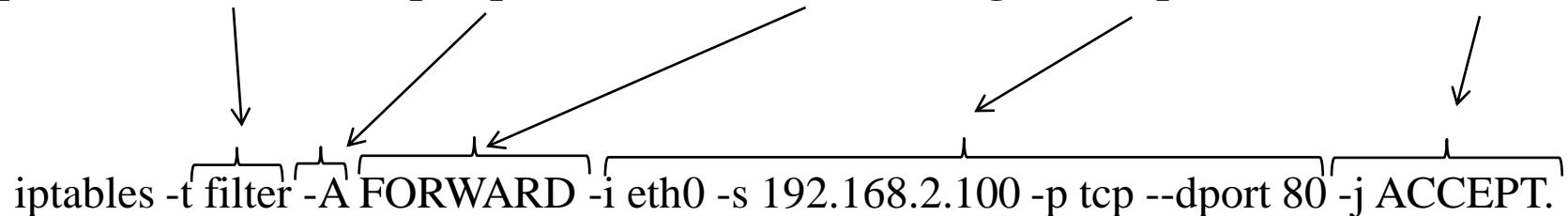
Cortafuegos o Firewall:

Configuración de un Cortafuegos. Sistemas GNU/Linux.

IPTABLES

1.- La estructura de una orden/regla de iptables sigue el siguiente patrón:

iptables -t [tabla] - -[tipo operación] -- [cadena]-- [regla_con_parametros] - - [acción]



- ❑ El tipo de operación es añadir una regla (A), sobre la tabla filter (tabla por defecto de filtrado), y cadena FORWARD (tráfico enrutado).
- ❑ La regla: aceptar (ACCEPT) el tráfico TCP cuyo puerto de destino sea el 80 (HTTP), en el interfaz eth0, con IP origen 192.168.2.100.

Cortafuegos o Firewall:

Configuración de un Cortafuegos. Sistemas GNU/Linux.

IPTABLES

2.- Las opciones más usadas de iptables son: *iptables -L*

- L: listar las cadenas de reglas de una determinada tabla (por defecto filter).
- F: elimina y reinicia a los valores por defecto todas las cadenas de una determinada tabla.
- A: añadir cadena de regla a una determinada tabla.
- P: añadir regla por defecto, en caso de que no cumpla ninguna de las cadenas de regla definidas.

□ Para sistemas en los que no se haya definido anteriormente reglas para Iptables el resultado de ejecutar el comando iptables -L tiene que ser similar a permitir todo el tráfico.

Cortafuegos o Firewall:

Configuración de un Cortafuegos. Sistemas GNU/Linux.

IPTABLES

Existen tres tablas incorporadas, cada una de las cuales contiene ciertas cadenas predefinidas:

□ Filter table (Tabla de filtros): Esta tabla es la responsable del filtrado (es decir, de boquear o permitir que un paquete continúe su camino). Todos los paquetes pasan a través de la tabla de filtros. Contiene las siguientes cadenas predefinidas y cualquier paquete pasará por una de ellas:

INPUT chain (Cadena de ENTRADA) - Todos los paquetes destinados a este sistema atraviesan esta cadena (también denominada LOCAL INPUT o ENTRADA_LOCAL).

OUTPUT chain (Cadena de SALIDA) - Todos los paquetes creados por este sistema atraviesan esta cadena (también denominada LOCAL_OUTPUT o SALIDA_LOCAL).

FORWARD chain (Cadena de REDIRECCIÓN) - Todos los paquetes que pasan por este sistema para ser encaminados a su destino recorren esta cadena.

Cortafuegos o Firewall:

Configuración de un Cortafuegos. Sistemas GNU/Linux.

IPTABLES

□ Nat table (Tabla de traducción de direcciones de red) - Esta tabla es la responsable de configurar las reglas de traducción de direcciones o de puertos de los paquetes. Contiene las siguientes cadenas redefinidas:

PREROUTING chain (Cadena de PRERUTEO) - Los paquetes entrantes pasan a través de esta cadena antes de que se consulte la tabla de enrutado.

POSTROUTING chain (Cadena de POSRUTEO) - Los paquetes salientes pasan por esta cadena después de haberse tomado la decisión de enrutado.

OUTPUT chain (Cadena de SALIDA).

□ Mangle table (Tabla de destrozo) - Esta tabla es la responsable de ajustar las opciones de los paquetes, como por ejemplo la calidad de servicio. Todos los paquetes pasan por esta tabla. Está diseñada para efectos avanzados, y contiene todas las cadenas predefinidas anteriormente.

A la hora de definir una orden de iptables podremos seleccionar la tabla a la que va destinada dicha orden mediante el parámetro **-t**:

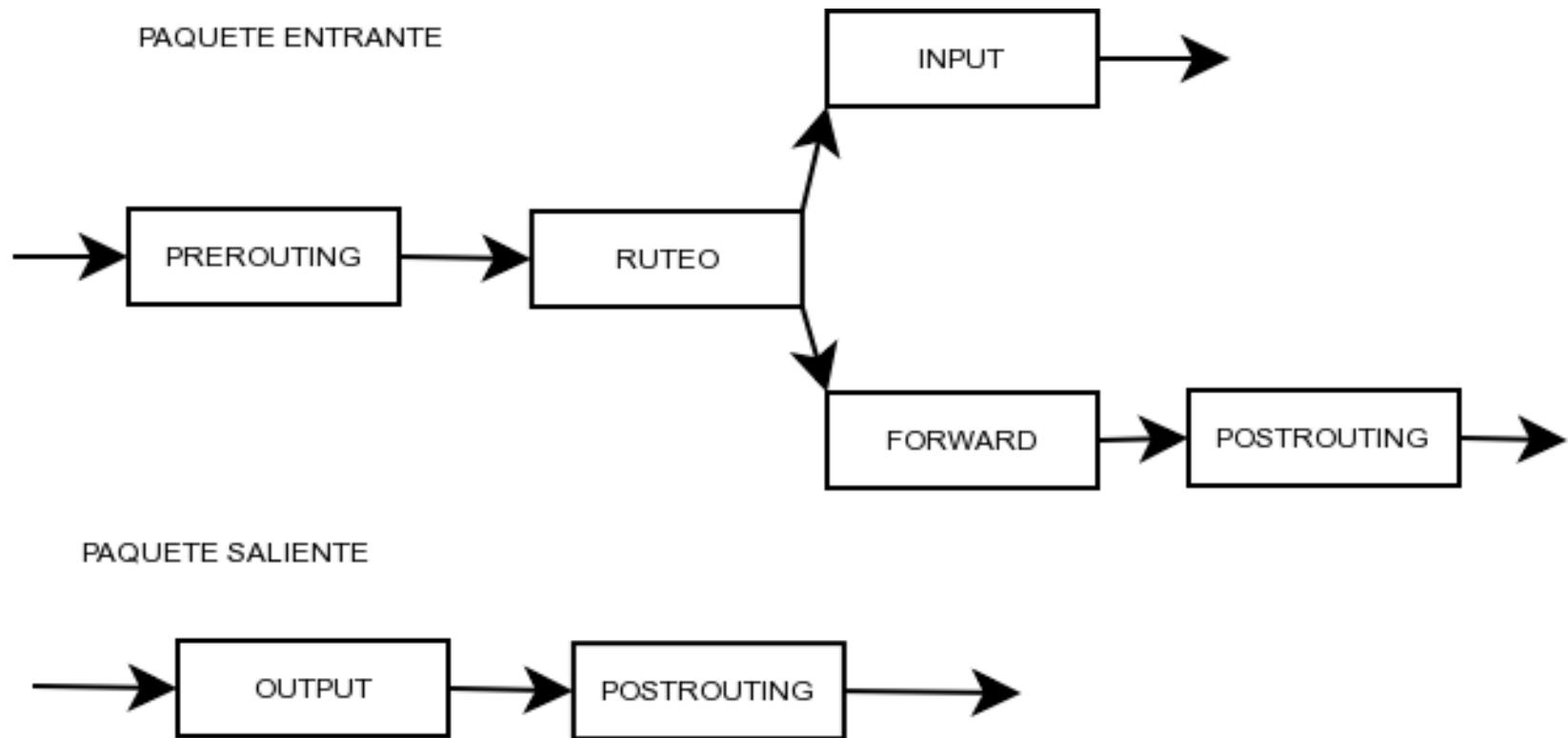
iptables -t [nat | filter | mangle]

Cortafuegos o Firewall:

Configuración de un Cortafuegos. Sistemas GNU/Linux.

IPTABLES

3.- Veamos por donde pasan los paquetes...

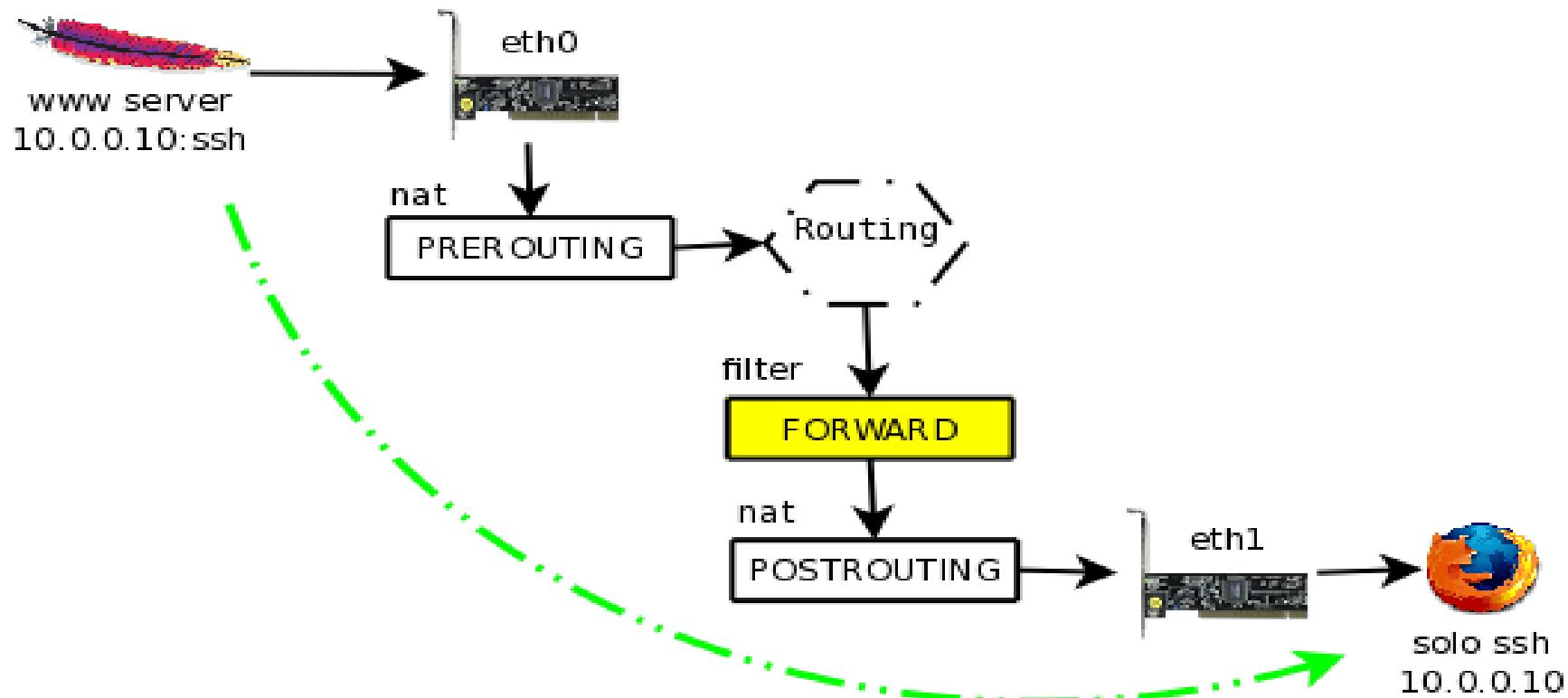


Cortafuegos o Firewall:

Configuración de un Cortafuegos. Sistemas GNU/Linux.

IPTABLES

3.-Veamos por donde pasan los paquetes...



Cortafuegos o Firewall:

Configuración de un Cortafuegos. Sistemas GNU/Linux.

IPTABLES

- ❑ Esos nombres -PREROUTING -INPUT -FORWARD -OUTPUT -POSTROUTING son instancias por las cuales puede atravesar un paquetes cuando entra a un linux (o cuando sale).
- ❑ Para entender mejor la explicación, agreguemos una instancia que llamaremos RUTEO. Esta instancia es el momento en el cual el kernel de linux decide que hacer con un paquete en base a la dirección IP de destino del mismo. Las alternativas son dos:
 - ✓ dejar el paquete en el equipo y pasar a la instancia de INPUT, si la dirección IP de destino es una de las direcciones que tiene el linux configurado.
 - ✓ Reenviar (FORWARD) el paquete por algunas de las interfaces de acuerdo a la tabla de ruteo, si la dirección IP destino no es una de las dirección IP que el linux tiene configurada.
- ❑ Hasta aquí ya sabemos que el paquete pasa por la instancia de RUTEO y luego podrá pasar por INPUT o FORWARD, pero... que es PREROUTING y POSTROUTING? en castellano sería ANTES DE ROUTEAR y DESPUES DE ROUTEAR. Todos paquetes que ingresa a un linux pasa por la instancia de PREROUTING. En el caso del POSTROUTING, es la instancia final de todos los paquetes que se FORWARDean (los paquetes que pasan por INPUT no pasan por POSTROUTING).

Cortafuegos o Firewall:

Configuración de un Cortafuegos. Sistemas GNU/Linux.

IPTABLES

4.- *Limpieza de reglas específicas.*

A fin de poder crear nuevas reglas, se deben borrar las existentes, para el tráfico entrante, tráfico reenviado y tráfico saliente así como el NAT.

```
iptables -F INPUT
```

```
iptables -F FORWARD
```

```
iptables -F OUTPUT
```

```
iptables -F -t nat
```

Cortafuegos o Firewall:

Configuración de un Cortafuegos. Sistemas GNU/Linux.

IPTABLES

Los modificadores o parámetros más usuales en las regla de iptables son los siguientes

- t <tabla> Para especificar la tabla sobre la que trabajamos. Por ejemplo: -t nat
- i <interfaz> Para especificar la interfaz de red por la que entra el paquete. Por ejemplo: -i eth0
- o <interfaz> Para especificar la interfaz de red por la que sale el paquete. Por ejemplo: -o eth0
- p <protocolo> Para especificar el protocolo del paquete. Por ejemplo: -p tcp
- s <ip> Para especificar la ip de origen (o red de la que procede) del paquete. Por ejemplo: -s 192.168.0.2 para especificar una ip, o bien -s 192.168.0.0/24 para especificar una red de origen.
- d <ip> Igual que en el caso anterior pero para la ip destinataria del paquete.
- dport <puerto> Para especificar el puerto al que va dirigido el paquete. Por ejemplo: --dport 22, o bien --dport 1:1024 (para especificar un rango de puertos).
- j <accion> Para especificar la acción que realizaremos con el paquete si al regla se acepta. Por ejemplo -j ACCEPT para aceptar el paquete.

Cortafuegos o Firewall:

Configuración de un Cortafuegos. Sistemas GNU/Linux.

IPTABLES

Las acciones que estarán siempre al final de cada regla (después de -j) que determinará que hacer con los paquetes afectados por la regla pueden ser:

- ACCEPT: Paquete paquete aceptado.
- REJECT: Paquete paquete rechazado. Se envía notificación a través del protocolo ICMP.
- DROP: Paquete paquete rechazado. Sin notificación.
- MASQUERADE: Enmascaramiento de la dirección IP origen de forma dinámica. Esta acción es solo válida en la tabla NAT en la cadena postrouting.
- DNAT: Enmascaramiento de la dirección destino, muy conveniente para reenrutado de paquetes.
- SNAT: Enmascaramiento de la IP origen de forma similar a masquerade, pero con IP fija.

Cortafuegos o Firewall:

Configuración de un Cortafuegos. Sistemas GNU/Linux.

IPTABLES

5.- Nuestro primer cortafuegos con Iptables. Ejemplo I

- Visto los elementos anteriores podemos empezar ya a diseñar nuestro cortafuegos, ya que Iptables se aprende mucho mejor viendo ejemplos que con líneas y líneas de explicación. Lo que haremos será crear un fichero, y en él colocar una detrás de otra todas las reglas de filtrado que queramos poner, teniendo en cuenta el orden, ya que **cuando una regla puede ser aplicada, se aplica esa y no se revisan el resto**. Vamos a ver un primer ejemplo de script de iptables.
- Supondremos que tenemos un servidor web y un ftp al que queremos dejar acceso a todo el mundo, y también un servidor mysql al que sólo queremos dejar acceso a un amigo que nos ayuda a administrar la base de datos.

Cortafuegos o Firewall: Configuración de un Cortafuegos. Sistemas GNU/Linux. **IPTABLES**

```
#!/bin/bash
```

```
echo "Aplicando reglas del firewall..."
```

```
# Borramos las reglas que ya pudieran existir, y los contadores
```

```
iptables -F
```

```
iptables -X
```

```
iptables -Z
```

```
# Establecemos las políticas por defecto
```

```
iptables -P INPUT ACCEPT
```

```
iptables -P OUTPUT ACCEPT
```

```
iptables -P FORWARD DROP
```

```
### Filtrado de paquetes ###
```

Cortafuegos o Firewall: Configuración de un Cortafuegos. Sistemas GNU/Linux. **IPTABLES**

Permitimos acceso desde la propia máquina
iptables -A INPUT -i lo -j ACCEPT

Permitimos acceso a los puertos 80 (web), 20 y 21 (ftp)
iptables -A INPUT -i eth0 -p tcp --dport 80 -j ACCEPT
iptables -A INPUT -i eth0 -p tcp --dport 20:21 -j ACCEPT

permitimos a nuestro amigo el acceso a mysql (puerto 3306)
iptables -A INPUT -i eth0 -p tcp -s 80.37.45.123 --dport 3306 -j ACCEPT

Ahora cerramos los puertos de gestión típicos
iptables -A INPUT -i eth0 -p tcp --dport 1:1024 -j DROP
iptables -A INPUT -i eth0 -p udp --dport 1:1024 -j DROP

Cerramos el puerto de mysql para que nadie más pueda acceder
iptables -A INPUT -i eth0 -p tcp --dport 3306 -j DROP

Cerramos el puerto de webmin
iptables -A INPUT -i eth0 -p tcp --dport 10000 -j DROP

Cortafuegos o Firewall: Configuración de un Cortafuegos. Sistemas GNU/Linux. IPTABLES

Expliquemos un poco más el script

- ❑ Primero borramos todas las reglas de iptables que pudiera haber cargadas. Esto es importante si no sabemos si el sistema operativo o alguna ejecución nuestra anterior nos han dejado reglas ya cargadas.
- ❑ *Lo segundo que hacemos (y muy importante) es establecer las políticas por defecto. Estas políticas definen la acción que se realizará con el paquete si ninguna regla especificada llega a cumplirse.* Nosotros, por defecto, hemos aceptado todo lo de la cadena OUTPUT (dejamos salir todo), aceptamos por defecto todo lo de la cadena INPUT, ya filtraremos luego lo que no nos interese, y no dejamos pasar los paquetes de FORWARD (ya que esto solo debería permitirse en equipos que van a hacer de routers de una red). Podríamos haber establecido la política de INPUT a DROP por defecto, así no permitiríamos nada, y luego establecer reglas para permitir el acceso a todo aquello que queramos; pero eso ya va a elección de cada uno.
- ❑ Luego ya empezamos a filtrar. Lo primero que hacemos es dejar a localhost acceso a todo, ya que desde nuestro PC podremos iniciar conexiones al servidor web local, etc. Estas conexiones irán por la interfaz de *lo* (loopback).
- ❑ Luego permitimos explícitamente acceso a los puertos 20,21 y 80. Esto es necesario ya que en las siguientes reglas cerramos el acceso a los puertos del 1 al 1024. Puede parecer contradictorio, pero tiene sentido ya que las reglas se miran en orden, y si un paquete coincide, por ejemplo, con la regla del puerto 80, se admitirá y no se mirarán más reglas.
- ❑ Seguidamente permitimos el acceso a mysql (puerto 3306) sólo a una ip en concreto (la de nuestro amigo). Luego ya cerramos los puertos típicos de gestión (1:1024), el de webmin (10000) y el de mysql, ya que no queremos que nadie más acceda a él.

Cortafuegos o Firewall: Configuración de un Cortafuegos. Sistemas GNU/Linux. IPTABLES

Pautas generales para cortafuegos básicos

- ❑ Habiendo entendido el script vamos a resumir los pasos que deberían seguirse a la hora de configurar un cortafuegos básico como este. Evidentemente, cualquier variación para adaptarlo a las necesidades de cada uno es perfectamente válida.
- ✓ Borrar las reglas y las cadenas que hubiera, para asegurarnos de que sólo estén cargadas nuestras reglas.
- ✓ Establecer las políticas por defecto para saber qué hacer si un paquete no coincide con ninguna regla.
- ✓ Empezar el filtrado de paquetes con las reglas que queramos, cuidando el orden: pondremos las reglas de más específicas a más generales.

Para terminar

- ❑ Pues esto es un script básico de iptables. Una vez lo hemos creado guardaremos el fichero y le daremos permiso de ejecución (con el comando `$ chmod u+x fichero`) para poder ejecutarlo.
- ❑ Una cosa importante es que las reglas de iptables no se guardan; cuando reiniciemos la máquina, esas reglas no permanecerán, así que si queremos que se apliquen las reglas cada vez que el ordenador arranque podremos poner este script como demonio.

Cortafuegos o Firewall:

Configuración de un Cortafuegos. Sistemas GNU/Linux.

IPTABLES

6.- Ejemplos de reglas

Reenvío de paquetes desde una interfaz de red local (eth1) hacia una interfaz de red pública (eth0):

```
iptables -A FORWARD -i eth1 -o eth0 -j ACCEPT
```

Aceptar reenviar los paquetes que son parte de conexiones existentes (ESTABLISHED) o relacionadas de tráfico entrante desde la interfaz eth1 para tráfico saliente por la interfaz eth0:

```
iptables -A FORWARD -i eth0 -o eth1 -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Permitir paquetes en el propio muro cortafuegos para tráfico saliente a través de la interfaz eth0 que son parte de conexiones existentes o relacionadas:

```
iptables -A INPUT -i eth0 -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Cortafuegos o Firewall:

Configuración de un Cortafuegos. Sistemas GNU/Linux.

IPTABLES

Permitir (ACCEPT) todo el tráfico entrante (INPUT) desde (-s) cualquier dirección (0/0) la red local (eth1) y desde el retorno del sistema (lo) hacia (-d) cualquier destino (0/0):

```
iptables -A INPUT -i eth1 -s 0/0 -d 0/0 -j ACCEPT  
iptables -A INPUT -i lo -s 0/0 -d 0/0 -j ACCEPT
```

Hacer (-j) SNAT para el tráfico saliente (-o) a través de la interfaz eth0 proveniente desde (-s) la red local (**192.168.0.0/24**) utilizando (--to-source) la dirección IP **w.x.y.z**.

```
iptables -A POSTROUTING -t nat -s 192.168.0.0/24 -o eth0 -j SNAT --to-source x.y.z.c
```

Descartar (DROP) todo el tráfico entrante (-i) desde la interfaz eth0 que trate de utilizar la dirección IP pública del servidor (**w.x.y.z**), alguna dirección IP de la red local (**192.168.0.0/24**) o la dirección IP del retorno del sistema (127.0.0.1)

```
iptables -A INPUT -i eth0 -s w.x.y.z/32 -j DROP  
iptables -A INPUT -i eth0 -s 192.168.0.0/24 -j DROP  
iptables -A INPUT -i eth0 -s 127.0.0.0/8 -j DROP
```

Cortafuegos o Firewall:

Configuración de un Cortafuegos. Sistemas GNU/Linux.

IPTABLES

Aceptar (**ACCEPT**) todos los paquetes SYN (--syn) del protocolo TCP (-p tcp) para los puertos (**--destination-port**) de los protocolos SMTP (25), HTTP(80), HTTPS (443) y SSH (22):

```
iptables -A INPUT -p tcp -s 0/0 -d 0/0 --destination-port 25 --syn -j ACCEPT  
iptables -A INPUT -p tcp -s 0/0 -d 0/0 --destination-port 80 --syn -j ACCEPT  
iptables -A INPUT -p tcp -s 0/0 -d 0/0 --destination-port 443 --syn -j ACCEPT  
iptables -A INPUT -p tcp -s 0/0 -d 0/0 --destination-port 22 --syn -j ACCEPT
```

Aceptar (**ACCEPT**) todos los paquetes SYN (--syn) del protocolo TCP (-tcp) para los puertos (**--destination-port**) del protocolos SMTP (25) en el servidor (**w.x.y.z/32**), desde (**-s**) cualquier lugar (0/0) hacia (**-d**) cualquier lugar (0/0).

```
iptables -A INPUT -p tcp -s 0/0 -d w.x.y.z/32 --destination-port 25 --syn -j ACCEPT
```

Aceptar (**ACCEPT**) todos los paquetes SYN (--syn) del protocolo TCP (-p tcp) para los puertos (**--destination-port**) de los protocolos POP3 (110), POP3S (995), IMAP (143) y IMAPS (993):

Cortafuegos o Firewall: Configuración de un Cortafuegos. Sistemas GNU/Linux. **IPTABLES**

```
iptables -A INPUT -p tcp -s 0/0 -d 0/0 --destination-port 110 --syn -j ACCEPT  
iptables -A INPUT -p tcp -s 0/0 -d 0/0 --destination-port 995 --syn -j ACCEPT  
iptables -A INPUT -p tcp -s 0/0 -d 0/0 --destination-port 143 --syn -j ACCEPT  
iptables -A INPUT -p tcp -s 0/0 -d 0/0 --destination-port 993 --syn -j ACCEPT
```

Aceptar (**ACCEPT**) el tráfico entrante (**-i**) proveniente desde la interfaz eth1 cuando las conexiones se establezcan desde el puerto (**--sport**) 67 por protocolos (**-p**) TCP y UDP.

```
iptables -A INPUT -i eth1 -p tcp --sport 68 --dport 67 -j ACCEPT  
iptables -A INPUT -i eth1 -p udp --sport 68 --dport 67 -j ACCEPT
```

Aceptar (**ACCEPT**) conexiones de tráfico entrante (INPUT) por protocolo (**-p**) UDP cuando se establezcan desde (**-s**) el servidor DNS 200.33.145.217 desde el puerto (**--source-port**) 53 hacia (**-d**) cualquier destino (0/0):

```
iptables -A INPUT -p udp -s 200.33.146.217/32 --source-port 53 -d 0/0 -j ACCEPT
```

Cortafuegos o Firewall:

Configuración de un Cortafuegos. Sistemas GNU/Linux.

IPTABLES

Descartar (**DROP**) el tráfico entrante (INPUT) para el protocolo (-p) TCP hacia los puertos (**--destination-port**) de SSH (22) y Telnet (23):

```
iptables -A INPUT -p tcp --destination-port 22 -j DROP
iptables -A INPUT -p tcp --destination-port 23 -j DROP
```

Descartar (**DROP**) todo tipo de conexiones de tráfico entrante (INPUT) desde (**-s**) la dirección IP a.b.c.d:

```
iptables -A INPUT -s a.b.c.d -j DROP
```

Rechazar (**REJECT**) conexiones hacia (OUTPUT) la dirección IP a.b.c.d desde la red local:

```
iptables -A OUTPUT -d a.b.c.d -s 192.168.0.0/24 -j REJECT
```

Eliminar la regla que descarta (**DROP**) todo tipo de conexiones de tráfico entrante (INPUT) desde (**-s**) la dirección IP a.b.c.d:

```
iptables -D INPUT -s a.b.c.d -j DROP
```

Cortafuegos o Firewall:

Configuración de un Cortafuegos. Sistemas GNU/Linux.

IPTABLES

7.- Mostrar la lista de Iptables.

Una vez cargadas todas las cadenas y reglas de **iptables** es posible visualizar éstas utilizando el mandato **iptables** con las opciones **-n**, para ver las listas en formato numérico, y **-L**, para solicitar la lista de éstas cadenas.

```
iptables -nL
```

Cuando no hay reglas ni cadenas cargadas, la salida **debe** devolver lo siguiente:

Chain INPUT (policy ACCEPT)

target prot opt source

destination

Chain FORWARD (policy ACCEPT)

target prot opt source

destination

Chain OUTPUT (policy ACCEPT)

target prot opt source

destination

Cortafuegos o Firewall: Configuración de un Cortafuegos. Sistemas GNU/Linux. **IPTABLES**

8.- Nuestro 2º cortafuegos con Iptables. Ejemplo II

A continuación, se va a configurar el cortafuegos para que permita que la red Interna pueda conectarse a Internet. Para establecer que el sistema active como router hay que ejecutar:

```
# echo "1" >/proc/sys/net/ipv4/ipforward
```

Limpie la configuraci6n del cortafuegos:

```
# iptables -F
```

```
# iptables -t nat -F
```

Indique que la red interna tiene salida al exterior por NAT:

```
# iptables -t nat -A POSTROUTING -s 10.0.0.0/24 -d 0/0 -j MASQUERADE
```

Se permite todo el tráfico de la red interna y todo lo demás se deniega:

```
# iptables -A FORWARD -s 10.0.0.0/24--j ACCEPT
```

```
# iptables -A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
```

```
# iptables -A FORWARD -j DROP
```

Guarde la configuraci6n del cortafuegos ejecutando:

```
# iptables-save >/etc/iptables.rules
```

y modifique el fichero /etc/sysctl.conf para establecer la variable net.ipv4.ipforward=1.

Cortafuegos o Firewall: Configuración de un Cortafuegos. Sistemas GNU/Linux. **IPTABLES**

Se va a realizar una mejora del supuesto en la que la red interna solo tiene acceso al exterior para ver páginas web (puerto 80/TCP) y para la resolución de nombres (53/EJDP y 53/TCP). Además, se va a publicar un servidor web interno que se encuentra en la dirección 10.0.0.100.

Limpie la configuración del cortafuegos:

```
# iptables -F
```

```
# iptables -t nat -F
```

Indique que la red interna tiene salida al exterior por NAT:

```
# iptables -t nat -A POSTROUTING -s 10.0.0.0/24 -d 0/0 -j MASQUERADE
```

Se permite solo el tráfico web (80/tcp) y DNS (53/udp y 53/tcp). Todo lo demás se deniega:

```
# iptables -A FORWARD -s 10.0.0.0/24 -p TCP --dport 80 -j ACCEPT
```

```
# iptables -A FORWARD -s 10.0.0.0/24 -p TCP --dport 53 -j ACCEPT
```

```
# iptables -A FORWARD -s 10.0.0.0/24 -p UDP --dport 53 -j ACCEPT
```

```
# iptables -A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
```

```
# iptables -A FORWARD -j DROP
```

Redirija el tráfico web que entra por la interfaz externa (eth0) al servidor de la red interna:

```
# iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j DNAT --to 10.0.0.100:80
```

Guarde la configuración del cortafuegos ejecutando:

```
# iptables-save >/etc/iptables.rules
```

Cortafuegos o Firewall:

Configuración de un Cortafuegos. Sistemas GNU/Linux.

IPTABLES

9.- Ejemplo III

- Realizaremos la configuración de un cortafuegos mediante un script que defina:
 - ✓ Enrutamiento con NAT y registro o log de paquetes FORWARD y PREROUTING. Se crea un registro en /var/log/iptables.log para tener un control de lo que entra y sale de nuestro cortafuegos.
 - ✓ Reglas que permita el acceso a los protocolos HTTP, DNS y FTP en Internet, pero solo a dos direcciones Ip determinadas desde una red local (192.168.2.100 y 192.168.2.114), todos los demás equipos no tendrán acceso.
 - ✓ Redirección del tráfico web en el puerto 80 por el puerto 3128 (Proxy-Squid). Luego veremos su utilidad .

Cortafuegos o Firewall:

Configuración de un Cortafuegos. Sistemas GNU/Linux.

IPTABLES

```
#! /bin/bash  
# borrar todas las reglas existentes.
```

```
iptables -F  
iptables -t nat -F  
iptables -t mangle -F  
iptables -x
```

```
# Aceptar el tráfico desde loopback
```

```
iptables -A INPUT -i lo -j ACCEPT
```

```
# Habilitar logs de todo lo que entra por FORWARD
```

```
iptables -A FORWARD -j LOG --log-prefix `IPTABLESFORWARD :`
```

```
# Permitimos acceso a los puertos 80 (web), 20-21 (ftp/FTP), 53 (dns-tcp y udp)  
# a los equipos: 192.168.2.100 y 192.168.2.114
```

Cortafuegos o Firewall:

Configuración de un Cortafuegos. Sistemas GNU/Linux.

IPTABLES

```
iptables -A FORWARD -i eth0 -s 192.168.2.100 -p tcp ---dport 80 -j ACCEPT  
iptables -A FORWARD -i eth0 -s 192.168.2.114 -p tcp --dport 80 -j ACCEPT  
iptables -A FORWARD -1 eth0 -s 192.168.2.100 -p tcp --dport 20:21 -j ACCEPT  
iptables -A FORWARD -i eth0 -s 192.168.2.114 -p tcp --dport 20:21 -j ACCEPT  
iptables -A FORWARD -i eth0 -s 192.168.2.100 -p udp --dport 53 -j ACCEPT  
iptables -A FORWARD -i eth0 -s 192.168.2.100 -p tcp --dport 53 -j ACCEPT  
iptables -A FORWARD -1 eth0 -s 192.168.2.114 -p udp --dport 53 -j ACCEPT  
iptables -A FORWARD -i eth0 -s 192.168.2.114 -p tcp --dport 53 -j ACCEPT  
iptables -A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
```

#Cerramos los puertos bien conocidos (1-1024)

```
iptables -A FORWARD -i eth0 -p tcp --dport 1:1024 -j DROP  
iptables -A FORWARD -i eth0 -p udp --dport 1:1024 -j DROP
```

#Hacemos log de todo lo entra por ei PREROUTING

```
iptables -t nat -A PREROUTING -j LOG --log-prefix 'IPTABLESPREROUTING: '
```

Cortafuegos o Firewall: Configuración de un Cortafuegos. Sistemas GNU/Linux. **IPTABLES**

#Redirección de puerto 80, hacia el Proxy, puerto 3128.

```
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j REDIRECT --to-port 3128
```

#Enmascarar mediante NAT, todo el tráfico (la IP origen de los paquetes) de la red interna por la IP de la tarjeta de red externa o pública.

```
iptables -t nat -A POSTROUTING -s 192.168.2.0/24 -o eth1-j MASQUERADE
```

Habilitamos enrutamiento entre tarjetas de red de nuestro equipo.

```
echo "1" > /proc/sys/net/ipv4/ipforward
```

#Fin del script

Cortafuegos o Firewall:

Configuración de un Cortafuegos. Sistemas GNU/Linux.

IPTABLES

9.- Ejemplo IV

- El comando **iptables-save** es una herramienta para guardar el conjunto de reglas existente en iptables a un fichero que puede utilizar **iptables-restore**. Este comando es bastante fácil de usar y sólo tiene dos argumentos. Échale un vistazo al siguiente ejemplo para entender la sintaxis apropiada del comando.

iptables-save [-c] [-t tabla]

- La opción **-c** le indica a **iptables-save** que guarde también los valores existentes en los contadores de bytes y de paquetes. Ésto puede ser útil si queremos reiniciar el cortafuegos sin perder los valores de estos contadores, que servirán, por ejemplo, para continuar con nuestras rutinas estadísticas sin problemas. Por supuesto el valor por defecto es no conservar los datos de los contadores.

Cortafuegos o Firewall:

Configuración de un Cortafuegos. Sistemas GNU/Linux.

IPTABLES

La opción **-t** indica a **iptables-save** qué tablas guardar. Sin este argumento el comando guardará en el fichero todas las tablas disponibles. A continuación tienes un ejemplo de la salida que puedes esperar del comando **iptables-save** si no tienes ningún conjunto de reglas cargado (lógicamente la salida es en inglés).

La acción **- para cada tabla** que se aplica si no se cumple ninguna regla. Ejem diap. 70

```
# Generated by iptables-save v1.2.6a on Wed Apr 24 10:19:17 2002
*filter
:INPUT ACCEPT [404:19766]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [530:43376]
COMMIT
# Completed on Wed Apr 24 10:19:17 2002
# Generated by iptables-save v1.2.6a on Wed Apr 24 10:19:17 2002
*mangle
:PREROUTING ACCEPT [451:22060]
:INPUT ACCEPT [451:22060]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [594:47151]
:POSTROUTING ACCEPT [594:47151]
COMMIT
# Completed on Wed Apr 24 10:19:17 2002
# Generated by iptables-save v1.2.6a on Wed Apr 24 10:19:17 2002
*nat
:PREROUTING ACCEPT [0:0]
:POSTROUTING ACCEPT [3:450]
:OUTPUT ACCEPT [3:450]
COMMIT
# Completed on Wed Apr 24 10:19:17 2002
```

Cortafuegos o Firewall:

Configuración de un Cortafuegos. Sistemas GNU/Linux.

IPTABLES

```
# sudo iptables-save -c > /etc/iptables.conf
```

El comando anterior guardará el conjunto de reglas con los valores de sus contadores en un fichero llamado /etc/iptables.conf

```
# sudo getedit /etc/iptables.conf
# sudo iptables – F
# sudo iptables-restore < /etc/iptables.conf
```

El proceso anterior me permite modificar, insertar o eliminar las reglas de filtrado, nat ...



Servidor Proxy

Introducción

Definición

- En el contexto de las ciencias de la computación, el término proxy hace referencia a un programa o dispositivo que realiza una acción en representación de otro. La finalidad más habitual es la del servidor proxy, que sirve para permitir el acceso a Internet a todos los equipos de una organización cuando sólo se puede disponer de un único equipo conectado, esto es, una única dirección IP.
- Un ejemplo de esto sería un aula sin conexión a Internet, pero uno de los ordenadores si tiene acceso, le instalamos un servidor proxy para poder acceder a recursos del exterior usando ese ordenador.

Que es un proxy Cache o proxy Web

- Se trata de un proxy para una aplicación específica: el acceso a la web. Aparte de la utilidad general de un proxy, proporciona una cache para las páginas web y los contenidos descargados, que es compartida por todos los equipos de la red, con la consiguiente mejora en los tiempos de acceso para consultas coincidentes. Al mismo tiempo libera la carga de los enlaces hacia Internet.

Servidor Proxy

Introducción

Funcionamiento

1. El cliente realiza una petición (p.e. mediante un navegador web) de un recurso de Internet (una página web o cualquier otro archivo) especificado por una URL.
2. Cuando el proxy caché recibe la petición, busca la URL resultante en su caché local. Si la encuentra, devuelve el documento inmediatamente, si no es así, lo captura del servidor remoto, lo devuelve al que lo pidió y guarda una copia en su caché para futuras peticiones.

Ventajas de utilizar un proxy caché:

- Ahorro de Tráfico:** Las peticiones de páginas Web se hacen al servidor Proxy y no a Internet directamente. Por lo tanto, aligera el tráfico en la red y descarga los servidores destino, a los que llegan menos peticiones.
- Velocidad en Tiempo de respuesta:** El servidor Proxy crea un caché que evita transferencias idénticas de la información entre servidores durante un tiempo configurado por el administrador) así que el usuario recibe una respuesta más rápida.

Servidor Proxy

Introducción

- **Demandas a Usuarios:** Puede cubrir a un gran número de usuarios, para solicitar, a través de él, los contenidos Web.
- **Filtrado de contenidos:** El servidor proxy puede hacer un filtrado de páginas o contenidos basándose en criterios de restricción establecidos por el administrador dependiendo valores y características de lo que no se permite, creando una restricción cuando sea necesario.
- Puede ser usado para **acceso intermedio a servidores web**, proxy transversal, acceso a servidores web que se encuentran en la intranet, por ejemplo terra utiliza este método de acceso a sus páginas web, esto permite información extra sobre el acceso a las páginas que se acceden por ejemplo para registrar ataques, se registran en el servidor web y además en el proxy.
- **Acelerar descargas** por ejemplo usar el proxy para descargar ciertos programas, por ejemplo actualmente telefónica activa el proxy para que a los usuarios que contratan los 3 megas puedan descargarse el antivirus de una forma mas rápida, además el uso del proxy permite que al usuario le aparezca una ventana para descargarse el antivirus. Cuando se lo descarga o se conecta varias veces sin descargarlo se desactiva el proxy.

Servidor Proxy

Introducción

Inconvenientes

- Las páginas mostradas pueden no estar actualizadas si éstas han sido modificadas desde la última carga que realizó el proxy caché.
- Un diseñador de páginas web puede indicar en el contenido de su web que los navegadores no hagan una caché de sus páginas, pero este método no funciona habitualmente para un proxy.
`<meta http-equiv="Pragma" content="nocache">`
- El hecho de acceder a Internet a través de un Proxy, en vez de mediante conexión directa, impide realizar operaciones avanzadas a través de algunos puertos o protocolos.
- Almacenar las páginas y objetos que los usuarios solicitan puede suponer una violación de la intimidad para algunas personas (reforma de la Ley de Protección de Datos)
- Servidores de descargas: Algunos servidores de Internet tienen políticas que cambia la localización de un fichero dentro de una URL o usan servidores alternativos. Por ejemplo MEGAUPLOAD, source forge.
- Muchas peticiones pueden hacer que el servidor proxy se colapse, si no se tiene en cuenta la cantidad de conexiones que se va a soportar el proxy puede hacer que este se sature.
- Dejar un proxy abierto en internet y se podría utilizar para navegar anonimamente, incluso podría ser usado para realizar ataques.
- Bloquear accesos que deberían estar permitidos.

Servidor Proxy

Squid

- Squid es un Servidor Intermediario (Proxy) de alto desempeño que se ha venido desarrollando desde hace varios años y es hoy en día un muy popular y ampliamente utilizado entre los sistemas operativos como GNU/Linux y derivados de Unix.

- Es muy confiable, robusto y versátil y se distribuye bajo los términos de la Licencia Pública General GNU (GNU/GPL). Siendo sustento lógico libre, está disponible el código fuente para quien así lo requiera.



Servidor Proxy

Squid

Puertos por defecto.

- ❑ Squid viene preconfigurado por defecto para funcionar en el puerto 3128, aunque puede usarse otros puertos. Normalmente los servidores proxy utilizan los puertos: 80, 3128, 8000 y 8080.
- ❑ Squid no debe ser utilizado como Servidor Intermediario (Proxy) para protocolos como SMTP, POP3, TELNET, SSH, IRC. Solo puede ser utilizado con los protocolos HTTP, HTTPS, FTP, GOPHER, WAIS.

Ventajas de Squid frente a otros proxys web.

- ❑ Soporta peticiones entre proxys, permite crear un árbol de servidores proxys lo cual acelera la navegación en grandes infraestructuras.
- ❑ Soporta el modo seguro HTTPS, permite en envío recepción de información encriptada de páginas webs.
- ❑ Soporta FTP permite almacenar descargas.
- ❑ Hace Cache de peticiones DNS.

Servidor Proxy

Squid: Instalación y configuración

Vamos a indicar las opciones más relevantes de la configuración del proxy mediante el fichero de configuración /etc/squid/squid.conf

1.- Instalación: **apt-get install squid** indicar que la última versión es squid3

2.- Funcionamiento del proxy en Linux:

Para arrancarlo tenemos que escribir

/etc/init.d/squid start

Para detenerlo

/etc/init.d/squid stop

Y para reiniciarlo:

/etc/init.d/squid restart

Servidor Proxy

Squid: Instalación y configuración

3.- Configuración

Squid utiliza el archivo de configuración localizado en /etc/squid/squid.conf, y se puede editar con el siguiente comando, en modo consola (terminal)

sudo gedit /etc/squid/squid.conf

En que editaremos los parámetros de nuestro Proxy, entre la que nos encontramos:

*http_port
cache_dir*

Al menos una Lista de Control de Acceso

Al menos una Regla de Control de Acceso

*httpd_accel_host
httpd_accel_port
httpd_accel_with_proxy*

.....

Servidor Proxy

Squid: Instalación y configuración

Parámetro http_port

Para cambiar el puerto de escucha por defecto debemos modificar la opción:

http_port 3128

Solo sustituimos 3128 por el puerto que queramos.

Parámetro cache_mem.

El parámetro cache_mem establece la cantidad ideal de memoria para lo siguiente:
Objetos en tránsito.

Objetos frecuentemente utilizados (Hot).

Objetos negativamente almacenados en el caché.

De modo predefinido se establecen 8 MB. Si se posee un servidor con al menos 128 MB de RAM, 16 MB es el valor para este parámetro:

cache_mem 16 MB

Servidor Proxy

Squid: Instalación y configuración

Parámetro cache_dir:

El parámetro `cache_dir` se utiliza para establecer que tamaño se desea que tenga el caché en el disco duro para Squid. De modo predefinido Squid utilizará un caché de 100 MB, de modo tal que encontrará la siguiente línea:

`cache_dir ufs /var/spool/squid 100 16 256`

Mientras más grande sea el caché, más objetos se almacenarán en éste y por lo tanto se utilizará menos el ancho de banda. La siguiente línea establece un caché de 700 MB:

`cache_dir ufs /var/spool/squid 700 16 256`

Los números 16 y 256 significan que el directorio del caché contendrá 16 directorios subordinados con 256 niveles cada uno.

Servidor Proxy

Squid: Instalación y configuración

Parámetro *ftp_user*.

Al acceder a un servidor FTP de manera anónima, de modo predefinido Squid enviará como clave de acceso Squid@. Puede establecerse una dirección de correo especificada como clave de acceso:

ftp_user proxy@gmail.com

Controles de acceso.

Las Listas de Control de Acceso definen una red o bien ciertas máquinas en particular. A cada lista se le asignará una Regla de Control de Acceso que permitirá o denegará el acceso a Squid.

Listas de control de acceso, se establecen con la siguiente sintaxis:

acl [nombre de la lista] src [lo que compone a la lista]

Servidor Proxy

Squid: Instalación y configuración

Si se desea establecer una lista de control de acceso que abarque a toda la red local, basta definir la IP correspondiente a la red y la máscara de la sub-red. Por ejemplo, si se tiene una red donde las máquinas tienen direcciones IP 10.140.111.n con máscara de sub-red 255.255.255.0, podemos utilizar lo siguiente:

```
acl miredlocal src 10.140.111.0/255.255.255.0
```

Más conveniente es definir una Lista de Control de Acceso especificando un archivo localizado en cualquier parte del disco duro, y la cual contiene una lista de direcciones IP.:

```
acl permitidos src "/etc/squid/permitidos"
```

El archivo /etc/squid/permitidos contendría algo como siguiente:

10.140.111.2
10.140.111.3
10.140.111.4
10.140.111.5
10.140.111.6

En caso de querer restringir el acceso de una pc, basta con eliminarla de la lista.

Servidor Proxy

Squid: Instalación y configuración

Listas de control de acceso: Bloqueo de Dominios de Destino.

Es conveniente definir una Lista de Control de Acceso especificando los dominios bloqueados en un archivo localizado en cualquier parte del disco duro, y la cual contiene una lista de los dominios:

```
acl bloqueados dstdomain '/etc/squid/bloqueados'
```

El archivo /etc/squid/bloqueados contendría algo como siguiente:

www.microsoft.com
www.ibm.com
www.hotmail.com

Servidor Proxy

Squid: Instalación y configuración

Reglas de Control de Acceso.

Las Reglas de control de Aceso definen si se permite o no el acceso hacia Squid. Se aplican a las Listas de Control de Acceso. Deben colocarse en la sección de reglas de control de acceso definidas por el administrador, es decir, a partir de donde se localiza la siguiente leyenda:

La sintaxis básica es la siguiente: ***http_access [deny o allow] [lista de control de acceso]***

En este ejemplo la regla que establece acceso permitido a Squid a la Lista de Control de Acceso denominada permitidos:

http_access allow permitidos

La expresión !, significa no. Pueden definirse así respecto de dos listas de control de acceso, lista1 y lista2, que se permite el acceso a Squid a lo que comprenda lista1 excepto aquello que comprenda lista2:

http_access allow lista1 !lista2

Esta regla es útil cuando se tiene un gran grupo de IP dentro de un rango de red al que se debe permitir acceso, y otro grupo dentro de la misma red al que se debe denegar el acceso.

Servidor Proxy

Squid: Instalación y configuración

Parámetro cache mgr.

De modo predefinido, si algo ocurre con el caché, se envia un mensaje de aviso a la cuenta webmaster del servidor, puede especificarse una distinta si se considera conveniente;

cache_mgr webmaster@gmail.com

Caché con aceleración.

Cuando un usuario hace petición hacia un objeto en Internet, este es almacenado en el caché de Squid. Si otro usuario hace petición hacia el mismo objeto, y este no ha sufrido modificación alguna desde que lo accedió el usuario anterior, Squid mostrará el que ya se encuentra en el caché en lugar de volver a descargarlo desde Internet.

Servidor Proxy

Squid: Instalación y configuración

Proxy Acelerado

En la sección HTTPD-ACCELERATOR OPTIONS deben habilitarse los siguientes parámetros:

httpd_accel_host virtual

httpd_accel_port 0

httpd_accel_with_proxy on

Opciones de los ficheros que recibimos y enviamos.

Como administradores puede ser que sea necesario que limitemos el tamaño del acceso a ficheros de páginas webs, porque sean demasiado extensos o porque tengan demasiado código.

request_header_max_size 10 KB

Servidor Proxy

Squid: Instalación y configuración

Esto limitaría el tamaño de la cabecera del HTML a 10KB, esto puede ser un engorro en caso de que el programador incluya código script de java en la cabecera, haciendo que la pagina no se cargue.

request_body_max_size 512 KB

Este es el tamaño del cuerpo máximo que se pide a un servidor.

reply_body_max_size 512 KB

Este es el tamaño del cuerpo máximo que se envía a un servidor, podemos limitarlo por ejemplo a 512Kb esto haría que no pudiésemos adjuntar ficheros de mas de ese tamaño cuando usamos un webmail por ejemplo.

Servidor Proxy

Squid: Instalación y configuración

4.- Configurar un Proxy Transparente

IPTABLES:

```
IPTABLES -A PREROUTING -i eth1 -p tcp -m tcp --dport 80 -j  
REDIRECT --to-ports 8080
```

SQUID:

```
http_port 8080 transparent
```

Servidor Proxy

Squid: Instalación y configuración

5.- Algunos ejemplos



Servidor Proxy

Squid: Instalación y configuración

6.- Configuración mediante - WEBMIN

The screenshot shows the Squid Proxy Server configuration interface within a Webmin module. The top navigation bar includes links for Help.., Module Config, Apply Changes, Stop Squid, and Search Docs.. On the left, a sidebar lists various server modules: screenshots, Webmin, System, Servers (Apache Webserver, BIND DNS Server, CVS Server, DHCP Server, Dovecot IMAP/POP3 Server, Fetchmail Mail Retrieval, Frox FTP Proxy, Jabber IM Server, Majordomo List Manager, Manage HTPasswd File, MySQL Database Server, OpenSLP Server, Postfix Configuration, PostgreSQL Database Server, ProFTPD Server, Procmail Mail Filter, QMail Configuration, Read User Mail, SSH Server, Samba Windows File Sharing, Sendmail Configuration, Shared Folders, SpamAssassin Mail Filter, Squid Analysis Report Generator, and Squid Proxy Server. The main content area is titled "Squid Proxy Server" (Squid version 2.4) and contains a grid of icons representing different configuration sections: Ports and Networking, Other Caches, Memory Usage (circled in green), Access Control (circled in green), Logging, Administrative Options, Refresh Rules, and Clear and Rebuild Cache. Below the grid are buttons for "Apply Configuration" and "Stop Squid". A note below the "Stop Squid" button states: "Click this button to stop the running Squid proxy server. Once stopped, clients using it will be unable to make web or FTP requests."

Administración Gráfica del Firewall/servidor proxy: WEBMIN (<http://webmin.com/>)

The screenshot shows the Webmin graphical interface running on a Linux server. The title bar indicates the URL is <https://192.168.1.5:10000>. The left sidebar lists various management modules: Webmin, System, Servers, Others, Networking, Hardware, Cluster, and Un-used Modules. A search bar is also present. The main content area features the Webmin logo and displays system status information. Below the status table, there are three horizontal progress bars representing memory and disk usage.

System hostname	servidor
Operating system	Ubuntu Linux 9.04
Webmin version	1.480
Time on system	Mon Aug 31 12:31:39 2009
Kernel and CPU	Linux 2.6.28-11-server on i686
System uptime	12 hours, 40 minutes
CPU load averages	0.03 (1 min) 0.02 (5 mins) 0.00 (15 mins)
Real memory	244.76 MB total, 96.30 MB used
Virtual memory	243.99 MB total, 3.27 MB used
Local disk space	2.83 GB total, 1.77 GB used

Terminado 192.168.1.5:10000

Administración Gráfica del Firewall/servidor proxy: WEBMIN (<http://webmin.com/>)

Login: screenshots
Webmin
System
Servers
Apache Webserver
BIND DNS Server
CVS Server
DHCP Server
Dovecot IMAP/POP3 Server
Fetchmail Mail Retrieval
Frox FTP Proxy
Jabber IM Server
Majordomo List Manager
Manage HTPasswd File
MySQL Database Server
OpenSLP Server
Postfix Configuration
PostgreSQL Database Serve
ProFTPD Server
Procmail Mail Filter
QMail Configuration
Read User Mail
SSH Server
Samba Windows File Sharing
Sendmail Configuration
Shared Folders
SpamAssassin Mail Filter
Squid Analysis Report
Generator
Squid Proxy Server

Help..
Module Config

Squid Proxy Server
Squid version 2.4

Apply Changes
Stop Squid
Search Docs..

 Ports and Networking
 Other Caches
 Memory Usage
 Logging

 Cache Options
 Helper Programs
 Access Control
 Administrative Options

 Proxy Authentication
 Authentication Programs
 Delay Pools
 Refresh Rules

 Miscellaneous Options
 Port Redirection Setup
 Cache Manager Statistics
 Clear and Rebuild Cache

 Calamaris Log Analysis

Click this button to activate the current Squid configuration.
 Click this button to stop the running Squid proxy server. Once stopped, clients using it will be unable to make web or FTP requests.

Administración Gráfica del Firewall/servidor proxy: WEBMIN (<http://webmin.com/>)

Help... Module Config Linux Firewall Rules file /etc/sysconfig/iptables Search Docs...

Showing iptable: Packet filtering (filter) Add a new chain named: []

Incoming packets (INPUT)
Select all. | Invert selection.

Action	Condition	Move	Add
<input type="checkbox"/> Log packet	If input interface is eth0	↓	I.T.
<input type="checkbox"/> Run chain RH-Firewall-1-INPUT	Always	↑	I.T.

Select all. | Invert selection.
Set Default Action To: Accept Delete Selected Add Rule

Forwarded packets (FORWARD)
Select all. | Invert selection.

Action	Condition	Move	Add
<input type="checkbox"/> Log packet	If output interface is eth0	↓	I.T.
<input type="checkbox"/> Log packet	If input interface is eth0	↓↑	I.T.
<input type="checkbox"/> Run chain RH-Firewall-1-INPUT	Always	↑	I.T.

Select all. | Invert selection.
Set Default Action To: Accept Delete Selected Add Rule

Outgoing packets (OUTPUT)
Select all. | Invert selection.

Action	Condition	Move	Add
<input type="checkbox"/> Log packet	If output interface is eth0	↓	I.T.

Select all. | Invert selection.
Set Default Action To: Accept Delete Selected Add Rule

Chain RH-Firewall-1-INPUT
Select all. | Invert selection.

Action	Condition	Move	Add
<input type="checkbox"/> Accept	If input interface is lo	↓	I.T.
<input type="checkbox"/> Accept	If protocol is ICMP and ICMP type is any	↓↑	I.T.
<input type="checkbox"/> Accept	If protocol is 50	↓↑	I.T.
<input type="checkbox"/> Accept	If protocol is 51	↓↑	I.T.
<input type="checkbox"/> Accept	If protocol is UDP and destination is 224.0.0.251 and destination port is 5353	↓↑	I.T.
<input type="checkbox"/> Accept	If protocol is UDP and destination port is 631	↓↑	I.T.
<input type="checkbox"/> Accept	If protocol is TCP and destination port is 633	↓↑	I.T.
<input type="checkbox"/> Accept	If state of connection is ESTABLISHED,RELATED	↓↑	I.T.
<input type="checkbox"/> Accept	If protocol is TCP and destination port is 22 and state of connection is NEW	↓↑	I.T.
<input type="checkbox"/> Accept	If protocol is TCP and destination port is 443 and state of connection is NEW	↓↑	I.T.
<input type="checkbox"/> Accept	If protocol is TCP and destination port is 80 and state of connection is NEW	↓↑	I.T.
<input type="checkbox"/> Reject	Always	↑	I.T.

Select all. | Invert selection.
Delete Chain Clear All Rules Delete Selected Add Rule

Apply Configuration Click this button to make the firewall configuration listed above active. Any firewall rules currently in effect will be flushed and replaced.

Revert Configuration Click this button to reset the configuration listed above to the one that is currently active.

Activate at boot: Yes No Change this option to control whether your firewall is activated at boot time or not.

Reset Firewall Click this button to clear all existing firewall rules and set up new rules for a basic initial configuration.

Administración Gráfica del Firewall/servidor proxy: WEBMIN

- Webmin es una interfaz web para la administración de sistemas Linux (Unix). Usando cualquier navegador podemos configurar las cuentas de usuario, Apache, DNS, apagado del equipo, compartir archivos, etc. Además, elimina la necesidad de editar manualmente los archivos de configuración (como /etc/passwd) y nos permite manejar el sistema desde el propio equipo o remotamente.
- Webmin está escrito en Perl y ejecuta tanto su propio proceso como su servidor web por lo que no necesitamos tener instalado Apache o cualquier otro servidor web, pero convive sin problemas con ellos. Por defecto se comunica a través del puerto TCP 10.000, y puede ser configurado para usar SSL.



Administración Gráfica del Firewall/servidor proxy: WEBMIN - *instalación*

□ Los pasos para instalar Webmin en Ubuntu son los siguientes:

- ✓ Descargamos la última versión de webmin:

```
wget http://freefr.dl.sourceforge.net/project/webadmin/webmin/1.520/webmin_1.520_all.deb
```

- ✓ Una vez descargado lo instalamos con dpkg:

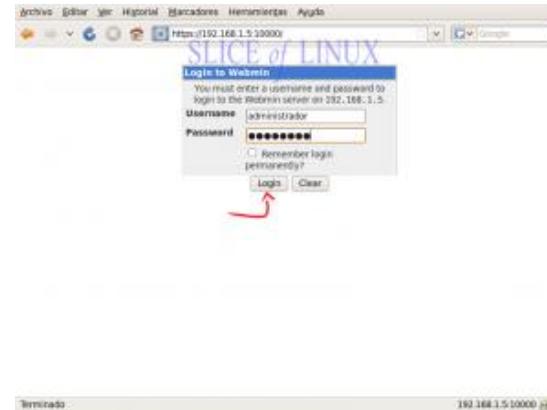
```
dpkg -i webmin_1.520_all.deb
```

- ✓ Al intentarlo instalar nos da un error porque el sistema no tiene todas las librerías necesarias para la ejecución de webmin, para solucionarlo ejecutamos (si lo instalamos en modo gráfico este paso se puede saltar).

```
sudo apt-get install -f
```

Administración Gráfica del Firewall/servidor proxy: WEBMIN - instalación

- ✓ Una vez instalado podemos acceder a la interfaz web de Webmin usando un navegador y escribiendo la dirección IP del equipo donde está instalado seguido del puerto donde está escuchando, por defecto, el 10.000. Eso sí, debemos estar atentos porque en vez de usar el protocolo HTTP, usaremos el HTTPS. En mi caso la IP de mi Ubuntu Server es 192.168.1.3: **https://192.168.1.3:10000**
- ✓ Ahora ya podemos iniciar sesión en Webmin. Como nombre de usuario podemos usar *root* (si lo tenemos habilitado) o cualquier usuario del sistema con privilegios de administrador.



- ✓ *Y así accedemos a la interfaz de Webmin.*

Referencias WEB:

- Completa información práctica sobre iptables:
 - <http://www.kriptopolis.org/iptables-0>
- Listado de cortafuegos personales:
 - <http://www.infospyware.com/cortafuegos/>
- Configuraciones prácticas de cortafuegos:
 - <http://www.pello.info/filez/firewall/iptables.html>
- Configuraciones de enrutamiento, Proxy y cortafuegos para GNU/Linux:
 - http://www.ite.educacion.es/formacion/materiales/85/cd/REDES_LINUX/frames/frameset_14.html
- Configuraciones de enrutamiento para Windows:
 - http://www.ite.educacion.es/formacion/materiales/85/cd/REDES_W2000/frames/frameset_enrutamiento.htm
- Configuraciones de funciones de cortafuegos, proxy-caché y servidor VPN para Windows, mediante ISA Server:
 - http://www.ite.educacion.es/formacion/materiales/85/cd/REDES_W2000/frames/frameset_isa.htm
- Blacklist o listado de URL y dominios maliciosos, categorizados, para ser intergados en servidores Proxy como Dansguardians y Squid.
 - <http://urlblacklist.com>
- Manual práctico Iptables:
 - <http://lucas.hispalinux.es/Manuales-LuCAS/doc-iptables-firewall/doc-iptables-firewall-html/>

Enlaces a Herramientas SW:

■ **Simuladores de configuración de dispositivos como router-punto de acceso inalámbrico TP-LINK.**

- <http://www.tp-link.com/support/simulator.asp>
- <http://www.tp-link.com/simulator/TL-WA501G/userRpm/index.htm>

■ **Simulador del router inalámbrico Linksys WRT54GL:**

- <http://ui.linksys.com/files/WRT54GL/4.30.0/Setup.htm>

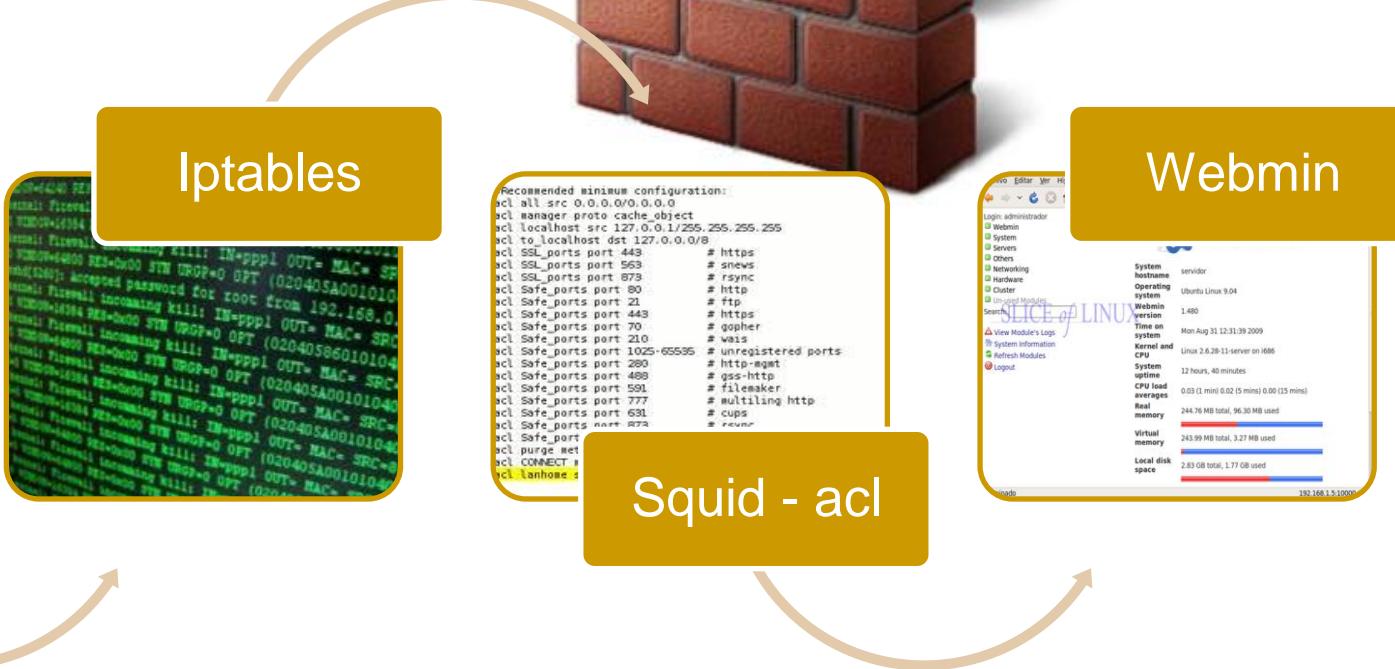
■ **Simuladores de routers inalámbricos D-Link:**

- <http://support.dlink.com/emulators/dwlq820/HomeWizard.html>
- <http://support.dlink.com/emulators/dsl2640b/306041/vpivci.html>
- <http://support.dlink.com/emulators/dwl2100ap>
- http://support.dlink.com/emulators/di604_reve

Enlaces a Herramientas SW:

- ISA Server: Microsoft Internet Security and Acceleration Server, gestión integral de seguridad para entornos Windows Server.
 - <http://www.microsoft.com/spain/isaserver/default.mspx>
- Forefront TMG: Microsoft Forefront Threat Management Gateway, Nuevo entorno de gestión integral de seguridad para entornos Windows Server.
 - <http://www.microsoft.com/forefront/en/us/default.aspx>
- Iptables: cortafuegos de sistemas GNU/Linux.
 - <http://www.netfilter.org/>
- Squid: servidor Proxy, entornos GNU/Linux.
 - <http://www.squid-cache.org/>
- Dansguardians: servidor Proxy, entornos GNU/Linux.
 - <http://dansguardian.org/>
- WinGate: software Proxy Server para sistemas Windows.
 - <http://www.wingate.com/>
- Webmin: gestión integral de servicios como Proxy en sistemas operativos GNU/Linux, desde entorno web.
 - <http://www.webmin.com/>
- Kerio Winroute firewall: gestión integral bajo Windows, con funciones de enrutamiento y cortafuegos.
 - <http://www.kerio.com/>
- Zone Alarm: Software cortafuegos - firewall
 - <http://www.zonealarm.com/security/es/zonealarm-pc-security-free-firewall.htm?lid=es>

Prácticas/Actividades



Prácticas/Actividades



Herramientas
Sw

Actividad 1.- Búsqueda de Información

Búsqueda de información con el fin de elaborar un diccionario de herramientas mencionadas en este tema, y de aquellos que resulten de la búsqueda de información, en el que se describan los siguientes elementos: descripción, http de descarga y http de tutorial/manual de uso, http de ejemplo de aplicación/uso, otros aspectos.

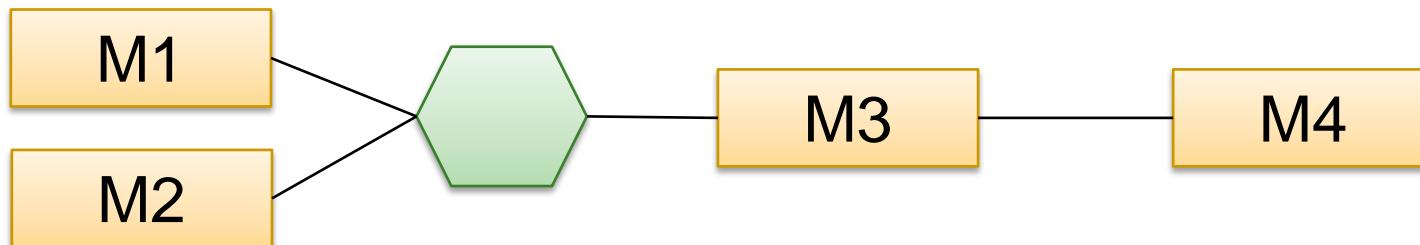


Prácticas/Actividades

Actividad 2.- Configuración de un Firewall y un Servidor Proxy Squid

Supongamos que tenemos 4 máquinas:

- 1.- M1 – eth0 (192.168.1.1/24) – Puerta de enlace (192.168.3.1/16)
- 2.- M2 – eth0 (192.168.2.1/24) – Puerta de enlace (192.168.3.1/16)
- 3.- M3 (Firewall/Proxy) – eth0 (192.168.3.1/16) y eth1 (10.0.0.1)
- 4.- M4 – eth0 (10.0.0.2)



Prácticas/Actividades

Actividad 2.- Configuración de un Firewall y un Servidor Proxy Squid

Realiza la configuración del equipo M3 de forma que actué como Firewall/Proxy:

1. Tabla de route
2. /proc/sys/net/ipv4/ip_forward
3. Interfaces
4. Instalación del Webmin
5. Configurar Iptables sin utilizar Webmin. Con un Script o utilizando un iptables.conf, medíate iptables-save y iptables-restore.
6. Instalación y configuración del Squid mediante el entorno gráfico.

NOTA: El alumno deberá definir de forma coherente un caso específico que implicará la configuración de los elementos anteriores. Deberá incluir en la resolución de la actividad los ficheros y/o script de configuración

Prácticas/Actividades

Formato de entrega:

Documento en formato XHTML 1.0, elaborado individualmente, con enlaces a elementos multimedia, que resuelvan la actividad 1 y la actividad 2 indicadas anteriormente.

De la actividad 2 también hay que incluir los ficheros y/o script de configuración

