Redes: Diseño, Configuración, Topologia y Seguridad

Por Paco Aldarias Raya

Impreso: 27 de julio de 2004

Email: pacolinux arroba inicia punto es
Web: `http://pagina.de/pacodebian`
Con Linux Debian. En Valencia (España)

Realizado con: LaTeX

Índice

1. Introducción

Vamos a ver que significa una dirección ip, una máscara, una subred. Veremos ejemplos de redes con sus topologias , e ips.

2. Redes Privadas y Públicas

Si tenemos que diseñar una red, lo normal es coger una ip pública, y el resto de la red deberá usar ips privadas.

2.1. Clases de redes Privadas

Existen direcciones IP reservadas para redes privadas, para usos internos, que se establecieron por convenio. Estas direcciones no son vistas desde el exterior, no son públicas, y sus rangos son:

- Clase A: 10.0.0.0
- Clase B: 172.16.0.0 a 172.31.0.0
- Clase C: 192.168.X.0 (con X variando).

3. Valores de las máscaras de subred: subneting

Dado que los bits en la máscara de subred han de ser contiguos, esto reduce la cantidad de máscaras de subred que se pueden crear.

Tabla Binario - Octeto

BITS DEL OCTETO	DECIMAL
00000000	0
10000000	128
11000000	192
11100000	224
11110000	240
11111000	248
11111100	252
11111110	254
11111111	255

La máscara por defecto de la clase A es 255.0.0.0
La máscara por defecto de la clase B es 255.255.0.0
La máscara por defecto de la clase C es 255.255.255.0
Una máscara de subred por si sola no nos dice nada. Tiene que ir siempre relacionada con una dirección IP, ya que por ejemplo la máscara 255.255.255.0 puede ser relacionada con una clase A o B, porque estamos haciendo Subnetting o con la clase C, sin hacer Subnetting.

4. Máscaras válidas para una red.

4.1. Máscaras válidas para una red de clase A

Aparecen los siguiente valores:

- MÁSCARA: MÁSCARA DE SUBRED
- BITS: NUMERO DE BITS DE RED
- REDES: NUMERO DE REDES
- MÁQUINAS: NUMERO DE MÁQUINAS.

Subnet Mask Networking Bits Number of Networks Number of Hosts. Class A

MÁSCARA	BITS	REDES	MAQUINAS
255.255.255.252	/30	4,194,304	2
255.255.255.248	/29	2,097,152	6
255.255.255.240	/28	1,048,576	14
255.255.255.224	/27	524,288	30
255.255.255.192	/26	262,144	62
255.255.255.128	/25	131,072	126
255.255.255.0	/24	65,536	254
255.255.254.0	/23	32,768	510
255.255.252.0	/22	16,384	1,022
255.255.248.0	/21	8,192	2,046
255.255.240.0	/20	4,096	4,094
255.255.224.0	/19	2,048	8,190
255.255.192.0	/18	1,024	16,382
255.255.128.0	/17	512	32,766
255.255.0.0	/16	256	65,534
255.254.0.0	/15	128	131,070
255.252.0.0	/14	64	262,142
255.248.0.0	/13	32	524,286
255.240.0.0	/12	16	1,048,574
255.224.0.0	/11	8	2,097,150
255.192.0.0	/10	4	4,194,302
255.128.0.0	/9	2	8,388,606
255.0.0.0	/8	1	16,777,216

4.2. Máscaras válidas para una red de clase B

Subnet Mask Networking Bits Number of Networks Number of Hosts.Class B

MÁSCARA	BITS	REDES	MAQUINAS
255.255.255.252	/30	32,768	2
255.255.255.248	/29	8,192	6
255.255.255.240	/28	4,096	14
255.255.255.224	/27	2,048	30
255.255.255.192	/26	1,024	62
255.255.255.128	/25	512	126
255.255.255.0	/24	256	254
255.255.254.0	/23	128	510
255.255.252.0	/22	64	1,022
255.255.248.0	/21	32	2,046
255.255.240.0	/20	16	4,094
255.255.224.0	/19	8	8,190
255.255.192.0	/18	4	16,382
255.255.128.0	/17	2	32,764
255.255.0.0	/16	1	65,534

4.3. Máscaras válidas para una red de clase C

Subnet Mask Networking Bits Number of Networks Number of Hosts. Class C

MÁSCARA	BITS	REDES	MAQUINAS
255.255.255.252	/30	64	2
255.255.255.248	/29	32	6
255.255.255.240	/28	16	14
255.255.255.224	/27	8	30
255.255.255.192	/26	4	62
255.255.255.128	/25	2	126
255.255.255.0	/24	1	254

5. Router

Un router es un elemento de red, que permite cambiar de red. Debemos de darle siempre la puerta de enlaces. Y tiene por tanto una tabla de rutas.

Tipos:

1. Router Adsl: Es el router que nos proporciona el proveedor de internet (ISP).

2. Router Software. Es un pc que permite pasar los paquetes de una red a otra. Linux da soporte para este tipo de software, llamado reenvio (forwarding).

3. Router Hardware. Es un router que permite pasar de una subred a otra. Hace de enmáscaramiento. Es un dispositivo, q está sobre 42 euros. Es una opción interesante si la red es nueva, y no se disponen de ordenadores antiguos para hacerlos por software.

Los router tienes dos ips, por lo que permite comunicarse con las redes de esas ips.

5.1. Un router concreto: Zyxel prestige 650-hw

A fecha de hoy 27.07.04, el router Zyxel prestige 650-hw, cuesta 130 euros.

Tiene un hub 10/100 y ranura pcmcia para wireless. Sin problemas de ningún tipo. La configuración telnet es a base de menús muy cómodos.

6. Concentradores: Hub, Swich

Un concentrador es un dispositivo que permite conectar máquinas para estar en red.

Un concentrador no tiene dirección ip.

Los hubs son dispositivos que retransmiten la información por todas las bocas o conexiones. A diferencia de los swich que son más inteligente, y solo mándan los datos por la boca en donde se encuentra esa ip.

Un switch, es un dispositivo de la capa 2. De hecho, el switch se denomina puente multipuerto, así como el hub se denomina repetidor multipuerto. La diferencia entre el hub y el switch es que los switches toman decisiones basándose en las direcciones MAC y los hubs no toman ninguna decisión. Como los switches son capaces de tomar decisiones, así hacen que la LAN sea mucho más eficiente. Los switches hacen esto çonmutando"datos sólo desde el puerto al cual está conectado el host correspondiente. A diferencia de esto, el hub envía datos a través de todos los puertos de modo que todos los hosts deban ver y procesar (aceptar o rechazar) todos los datos. Esto hace que la LAN sea mas lenta. A primera vista los switches parecen a menudo similares a los hubs. Tanto los hubs como los switches tienen varios puertos de conexión (pueden ser de 8, 12, 24 o 48, o conectando 2 de 24 en serie),

dado que una de sus funciones es la concentración de conectividad (permitir que varios dispositivos se conecten a un punto de la red).

La diferencia entre un hub y un switch está dada por lo que sucede dentro de cada dispositivo. El propósito del switch es concentrar la conectividad, haciendo que la transmisión de datos sea más eficiente. Por el momento, piense en el switch como un elemento que puede combinar la conectividad de un hub con la regulación de tráfico de un puente en cada puerto. El switch conmuta paquetes desde los puertos (las interfaces) de entrada hacia los puertos de salida, suministrando a cada puerto el ancho de banda total. Básicamente un Switch es un administrador inteligente del ancho de banda.

7. Bastions Hosts

Denominaremos como Bastion Host a un sistema informático catalogado como punto peligroso en la seguridad de nuestro red informática. En base, dispone de una serie de medidas que le diferencia del resto, tales como mejores auditorías, monitorización del sistema, control de accesos al mismo (conexiones de la red interna, conexiones de la red externa ...). Este sistema debe haber sufrido un proceso de testing para catalogar posibles fallos no solo en seguridad, sino también en el propio software que utiliza.

Normalmente se suele permitir el paso del trafico de red autorizado a través del BH debido a que este nos detallara todo en todo momento, y además conociendo correctamente su funcionamiento, podremos asegurar en un gran margen que el sistema esta preparado para evitar posibles ataques o accesos no deseados a nuestra red interna.

Un Bh deberá incluir, entre otros, una serie de normas de seguridad. En principio, el sistema no deberá contener cuentas de de acceso a usuarios. En el caso de GNU/LiNUX, solo deberá mantenerse aquellas derivadas a daemons y la del administrador. Se recomienda eliminar el demonio SysKLogd, e instalar otro de los muchos disponibles en web sites como http://www.freshmeat.net, que nos den un mayor rango de seguridad inherente, de forma que ante posibles ataques a nuestro sistema, los ficheros, de registro, etc corran menor peligro. Un buen ejemplo de ello, seria la codificación y encriptación de los mismos. De cualquier modo, es recomendado leer previamente toda documentación y, como no, la parte relativa a registros de este documento.

Como ya bien se especifico en la parte correspondiente en este documento, el envio de los logs a otra máquina de nuestra red nos puede ser de gran utilidad. Con Syslogd, es bastante sencillo, simplemente indicando en la configuración del demonio que registros y políticas se han de enviar a la máquina mediante el parametro "@z a continuación la IP de la Máquina en cuestión.

Un ejemplo seria:

Deberemos controlar todo lo relativo a enrutado desde el BH. Evitaremos situaciones como encaminamientos no autorizados. También deberemos desechar todos aquellos servicios de red como HTTPd, NNTPd, etc. excepto aquellos que nos permitan a nosotros, administradores, el control remoto de la máquina. Estos podrían ser el telnetd y el ftpd. Deberemos cambiar los puertos de acceso a los mismos, o buscar formas de acceso a la máquina mediante una sola IP de acceso (Revisar Hosts.deny y Hosts.allow). Los métodos personales mios de administración prefiero mantenerlos offside ;-) Simplemente es pensar en como actuaria una persona ajena al encontrarse con un sistema de este tipo. SSH nos ayudará mucho en esta tarea.

8. Firewalls (Cortafuegos - FW)

8.1. ¿Qué es un firewall?

Básicamente, podrías asimilar un firewall a un router al que se le añade seguridad. Esa seguridad hace que para algunas conexiones o paquetes o aplicaciones que tu le defines en lo que se llama política de seguridad, el router se niegue a mandarlo al otro lado. Esto puede valer tanto para cosas que vienen de fuera hacia dentro (lo más habitual) como de cosas que van de dentro hacía afuera.

Si tu política de seguridad es ninguna, un firewall y un router es lo mismo. Si tienes algunas reglas que te interesa que cumpla tu router y que signifiquen que bajo ciertas circunstancias a algún tipo de tráfico debe impedirsele atravesarlo, tienes un firewall.

Un firewall es un dispositivo que filtra el tráfico entre redes, como mínimo dos. El firewall puede ser un dispositivo físico o un software sobre un sistema operativo. En general debemos verlo como una caja con DOS o mas interfaces de red en la que se establecen una reglas de filtrado con las que se decide si una conexión determinada puede establecerse o no. Incluso puede ir más allá y realizar modificaciones sobre las comunicaciones, como el NAT.

Esa sería la definición genérica, hoy en dia un firewall es un hardware especifico con un sistema operativo o una IOS que filtra el tráfico TCP / UDP / ICMP / .. / IP y decide si un paquete pasa, se modifica, se convierte o se descarta. Para que un firewall entre redes funcione como tal debe tener al menos dos tarjetas de red. Esta sería la tipología clásica de un firewall:

En el figura 1 de la página 21, muestra un ejemplo de firewall entre internet y una red local.

Esquema típico de firewall para proteger una red local conectada a inter-

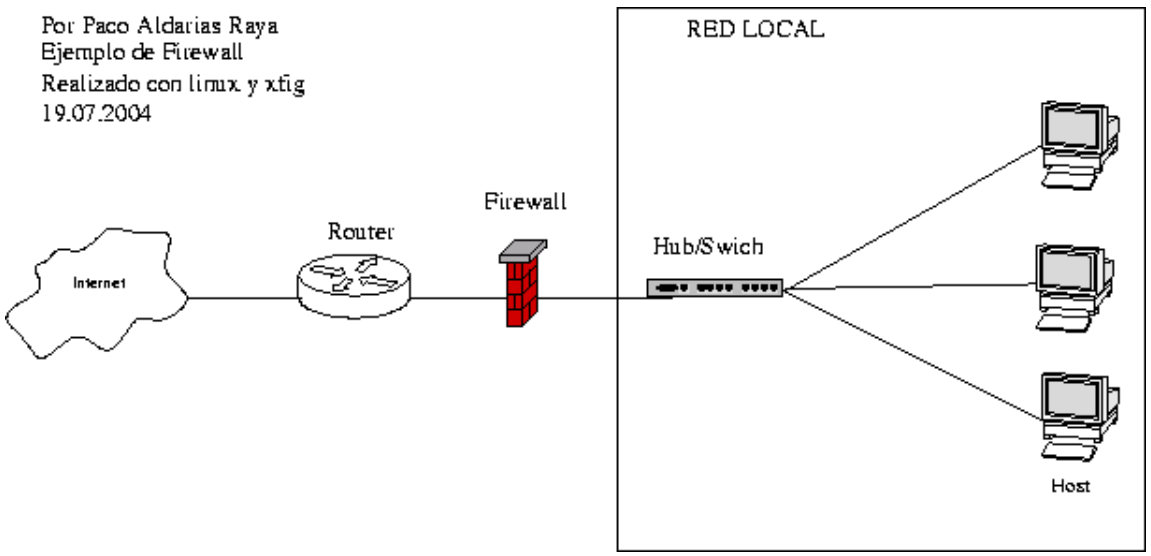

Figura 1: Firewall entre internet y una red local

net a través de un router. El firewall debe colocarse entre el router (con un único cable) y la red local (conectado al switch o al hub de la LAN)

Dependiendo de las necesidades de cada red, puede ponerse uno o más firewalls para establecer distintos perímetros de seguridad en torno a un sistema. Es frecuente también que se necesite exponer algún servidor a internet (como es el caso de un servidor web, un servidor de correo, etc..), y en esos casos obviamente en principio se debe aceptar cualquier conexión a ellos. Lo que se recomienda en esa situación es situar ese servidor en lugar aparte de la red, el que denominamos DMZ o zona desmilitarizada. El firewall tiene entonces tres entradas:

En el figura 2 de la página 22, muestra un ejemplo de firewall entre internet y una red local, con zona dmz.

8.2. ¿Por qué es necesaria la seguridad en las redes?

Actualmente, Internet se compone de decenas de miles de redes conectadas entre sí. La seguridad en las redes resulta esencial en este entorno, ya que toda red organizada es accesible desde cualquier computadora de la red y potencialmente es vulnerable a las amenazas de personas que no necesitan acceso físico a ella. En un sondeo reciente dirigido por el Computer Security Institute (CSI), el 70 % de las organizaciones encuestadas declararon que las defensas de sus redes habían sido atacadas y el 60 % afirmaba que los

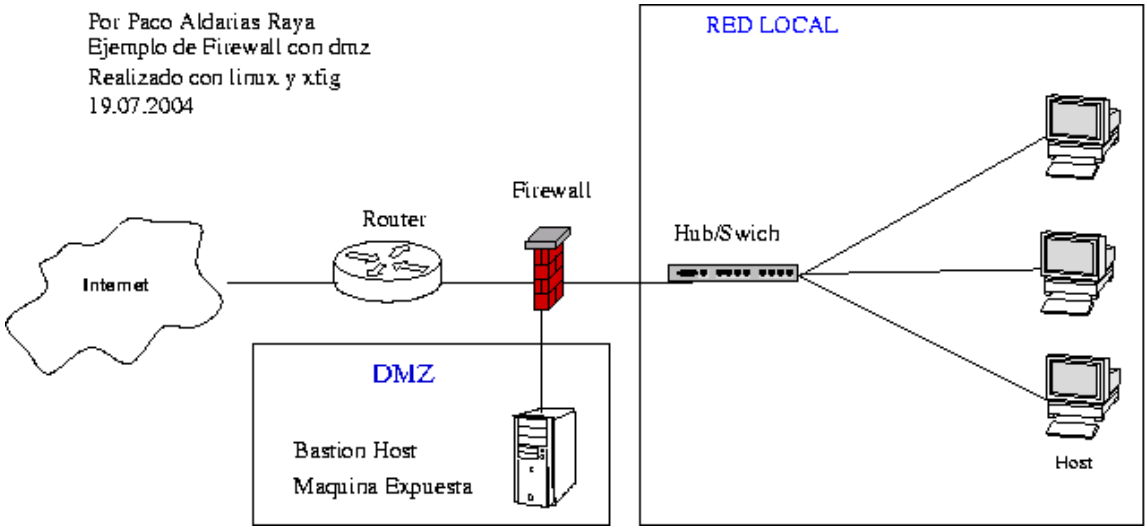

Figura 2: Firewall entre internet y una red local, con zona dmz

incidentes procedían desde dentro de las propias empresas.

Aunque sea difícil calcular el número de empresas que tiene problemas de seguridad relacionados con Internet y las pérdidas financieras debidas a tales problemas, queda claro que los problemas existen. Definición del diseño de redes seguras Una internetwork se compone de muchas redes que están conectadas entre sí. Cuando se accede a información en un entorno de internetwork, hay que crear áreas seguras. El dispositivo que separa cada una de estas áreas se denomina firewall. Aunque un firewall suele separar una red privada de una red pública, esto no siempre es así. Lo normal es usar un firewall para separar los segmentos de una red privada.

NOTA: Un firewall, tal y como lo define el Dictionary of Internetworking Terms and Acronyms (Diccionario para términos y acrónimos de Internetworking), es un router o servidor de acceso, o varios routers o servidores de acceso, que actúan como búfer entre las redes públicas y una red privada.

Un router firewall utiliza listas de acceso y otros métodos para garantizar la seguridad de la red privada . Un firewall suele tener un mínimo de tres interfaces, aunque las primeras implementaciones sólo incluían dos.

Todavía resulta habitual instalar firewalls de dos interfaces.

Cuando se usa un firewall con tres interfaces, se crea un mínimo de tres redes. Las tres redes que crea el firewall se describen de este modo:

Interior El interior es el área de confianza de la internetwork. Los dispositivos que están en el interior forman la red privada de la organización. Estos

dispositivos comparten unas directivas de seguridad comunes con respecto a la red exterior (Internet). Sin embargo, resulta muy habitual que un firewall segmente el entorno de confianza. Si un departamento, como Recursos Humanos, tiene que ser protegido del resto de usuarios de confianza, se puede utilizar un firewall.

Exterior El exterior es el área de no confianza de la internetwork. El firewall protege los dispositivos del interior y de la DMZ (Zona desmilitarizada) de los dispositivos del exterior. Para ofrecer servicios, ya sean Web, FTP publico u otros, las empresas suelen permitir el acceso a la DMZ desde el exterior. En ocasiones, es necesario configurar un firewall para el acceso selectivo desde el 2 exterior hasta los hosts y servicios de la DMZ. Si es inevitable, es posible configurar un firewall para permitir el acceso desde un dispositivo del exterior hasta un dispositivo de confianza del interior, siendo la razón principal para esto, el que no todas las empresas quieren invertir en tener varios servidores. Esto es mucho más arriesgado que permitir el acceso, desde el exterior hasta la DMZ aislada.

DMZ (Zona desmilitarizada) La DMZ es una red aislada, a la que pueden acceder los usuarios del exterior. Es necesario configurar el firewall para permitir el acceso desde el exterior o el interior hasta la DMZ. La creación de una DMZ posibilita que una empresa ponga la información y los servicios a disposición de los usuarios del exterior dentro de un entorno seguro y controlado. Esto permite el acceso a los usuarios del exterior, sin permitir el acceso al interior. Los hosts o servidores que residen en la DMZ suelen denominarse hosts bastión. En este caso, un host bastión es un host que está actualizado con respecto a su sistema operativo y las modificaciones experimentadas por este último. El hecho de que esté actualizado generalmente lo hará menos vulnerable a los ataques, ya que el fabricante habrá establecido o "parcheado"todos los defectos conocidos. El host bastión es un host que sólo ejecuta los servicios necesarios para realizar sus tareas de aplicación. Los servicios innecesarios (y a veces más vulnerables) son desactivados o eliminados.

En el figura 3 de la página 23, muestra una red general.

El cometido básico de un firewall consiste en llevar a cabo las siguientes funciones:

- No permitir acceso desde el exterior hasta el interior
- Permitir un acceso limitado desde el exterior hasta la DMZ
- Permitir todo el acceso desde el interior hasta el exterior

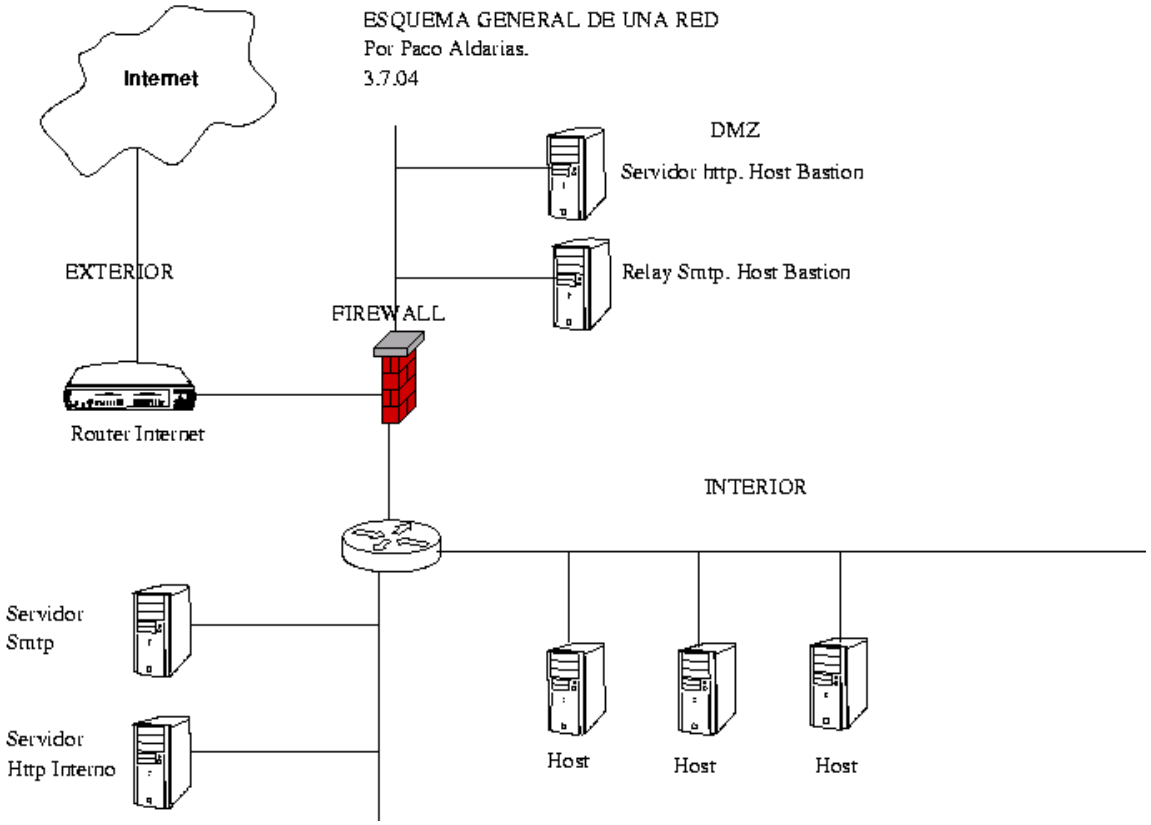

Figura 3: Red General

- Permitir un acceso limitado desde el interior hasta la DMZ

En muchos diseños de red existen excepciones a algunas de estas reglas (o a todas ellas). Por ejemplo, podría ser necesario permitir los mensajes SMTP desde el exterior hasta el interior. Si un entorno no tiene un servidor SMTP en la DMZ o carece de un host de relay de correo SMTP en la DMZ, sería necesario permitir acceder al servidor SMTP que resida físicamente en el interior. El hecho de permitir este tráfico incrementa considerablemente el riesgo en la red interna. Otra excepción podría ser que no se permitiera a la totalidad del tráfico pasar del interior al exterior. Potencialmente, una dirección IP, una subred, o la totalidad de la red del interior, podrían estar limitadas a la hora de usar una determinada aplicación (puerto). Otra restricción podría ser el filtrado de los URL.

8.3. Seguridad

En principio, el propósito genérico de un firewall es controlar y auditar los accesos a un servicio determinado. Su función es la de multiplexar los accesos a una red interna desde Internet; es una puerta entre una IntraNET ÁéInterNET. La vigilancia que otra el firewall requiere unas normativas de seguridad impuestas por el propio administrador.

Una política bastante correcta y fiable, es la de hacer pasar siempre por el firewall el trafico que se necesite originar entre a e Internet y viceversa, de forma que se audite y controle todo lo que accede a A y/o sale de la misma. Esto nos permitirá sistemas de autentificación segura, detección de posibles intentos de acceso no autorizados, etc etc.

Una falacia es la idea que establece que un Firewall es inatacable. Esto es totalmente falso, existen métodos, con mayor o menor riesgo para el sistema, pero existen. Un ejemplo seria dar la oportunidad al atacante de restablecer las políticas de filtrado y selección. esto crearía un gran agujero de seguridad que posiblemente le permita acceder a cualquier host de la red interna que desee.

El firewall debe ser capaz de evaluar los posibles daños ofertados por un ataque e informar al administrador de ello. Tengamos en cuenta el bug propuesto antes. Una eliminación de políticas de auditoría podría darnos muchos dolores de cabeza.

Bajo GNU/LiNUX, tenemos a nuestra disposición numerosos programas capaces de convertir nuestro sistema en un potente firewall. El ejemplo mas conocido quizás sea iptables.

9. Diseño de redes

9.1. Diseño de red básico. Sin Cortafuegos

Suponemos que estamos en el caso básico que están los centros de enseñanza secundaria cuando llevan internet al centro.

Un router adsl en multipuesto:

- la ip externa la tiene el router
- tiene la ip local 192.168.0.1 (sera la puerta de enlace de los pcs de la red)
- dhcp dinámico 192.168.0.1 - 192.168.0.254
- máscara 255.255.255.0

- Tiene todos los puertos cerrados.

Con lo que se crea una red local de tipo C privada, con una única subred 192.168.0.0 El número máximo de máquinas es: 2 elevado a 8 - 2 = 254 pcs.

En el figura 4 de la página 24, muestra la topología.

Ventajas:

1. Fácil de instalar y mantener. Sólo hay q activar el dhcp en los pcs.
2. Limite de 254 pcs.

Inconvenientes:

1. Se podría instalar un proxy, pero abría que añadirlo en el navegador su ip.
2. Red poco segura, todas las máquinas tienen acceso a toda la red.
3. No se pueden poner servidores web al exterior, por tener el acceso al router bloqueado.
4. Tiene un gran tráfico de paquetes de broadcast.

9.2. Diseño básico de un red C/B

Una solución intermedia, sería montar un router linux, que cambie las ips, anulando la red 192.168.0.0/255.255.255.0, y crear nosotros subredes de clase B, 172.16.0.0/255.255.255.0 a a partir del firewall.

Es decir, tendremos una clase C (192.168.0.0), solo hasta el firewall, y el resto de la red privada, será un clase B (172.16.0.0). La clase B, permitirá aislar y crear subredes.

Ventajas:

1. Fácil de instalar y mantener. Sólo hay q activar el dhcp en los pcs.
2. Se bloquea el acceso de las aulas a otros pcs.
3. Se podría instalar un proxy transparente en cada servidor de aula y encadenarlos.
4. Red segura, ya que todas las máquinas no tienen tienen acceso a toda la red.
5. Tiene un gran tráfico de paquetes de broadcast más bajo.

Inconvenientes:

1. Los routers linux que tienen varias ips, deben tener su tabla de rutas.
2. No se pueden poner servidores web al exterior, por tener el acceso al router bloqueado.
3. El dhcp se hara segmentado por subredes.
4. Hay que añadir un firewall.

Tabla de rutas del firewall (FW)

Destination	Gateway	Genmask	Descripción
172.16.253.1	-	255.255.255.0	IP local
172.16.254.100	-	255.255.255.0	IP local
192.168.0.2	-	255.255.255.0	IP local
172.16.1.0	172.16.100.253.2	255.255.255.0	Acceso a la red 172.16.1.0 por 172.16.100.25
172.16.2.0	172.16.100.253.2	255.255.255.0	Acceso a la red 172.16.2.0 por 172.16.100.25
172.16.100.0	172.16.100.253.2	255.255.255.0	Acceso a la red 172.16.100.0 por 172.16.100.
172.16.252.0	172.16.100.253.2	255.255.255.0	Acceso a la red 172.16.252.0 por 172.16.100.
0.0.0.0	192.168.0.2	0.0.0.0	Resto de redes/pcs por 192.168.0.2

Tabla de rutas del Router1

Destination	Gateway	Genmask	Descripción
172.16.253.2	-	255.255.255.0	IP local
172.16.252.100	-	255.255.255.0	IP local
192.168.100.100	-	255.255.255.0	IP local
172.16.1.0	172.16.100.1	255.255.255.0	Acceso a la red 172.16.1.0 por 172.16.100.1
172.16.2.0	172.16.100.2	255.255.255.0	Acceso a la red 172.16.2.0 por 172.16.100.2
172.16.254.0	172.16.100.253.1	255.255.255.0	Acceso a la red 172.16.254.0 por 172.16.100
0.0.0.0	192.168.0.2	0.0.0.0	Resto de redes/pcs por 192.168.0.2

Tabla de rutas del Router2 (Aula1)

Destination	Gateway	Genmask	Descripción
172.16.100.1	-	255.255.255.0	IP local
172.16.100.1.100	-	255.255.255.0	IP local
172.16.2.0	172.16.100.2	255.255.255.0	Acces a la red 172.16.2.0 por 172.16.100.2
172.168.254.0	172.16.100.100	255.255.255.0	Acces a la red 172.16.254.0 por 172.16.100.
0.0.0.0	192.168.100.100	0.0.0.0	Resto de redes/pcs por 192.168.0.2

En el figura 5 de la página 25, muestra la topología.

9.3. Diseño de red clase B con DMZ y firewall: Red Segura

Suponemos que queremos varias subredes por aulas y departamentos. Queremos que los pcs de las aulas de vean entre ellos (esto deberá contemplarse en la cuadro de encaminamientos).

Usaremos la red de tipo B privada:

172.16.0.0 / 255.255.255.0 o lo que es lo mismo 172.16.0.0 /24

Esto significa que tenemos, esta máscara:

11111111. 11111111.11111111.00000000

Es decir, podemos tener:

- Subredes : 2 elevado a 8 (11111111 del tercer número de la máscara) =256
- Hosts: 2 elevado a 8 - 2 : (00000000 del cuarto número de la máscara) =256-2=254

Subredes para 172.16.0.0/255.255.255.0

Subred	De	A	Broadcast	Mascara
172.16.1.0	172.16.1.1	172.16.1.254	172.16.1.255	255.255.255.0
172.16.2.0	172.16.2.1	172.16.2.254	172.16.2.255	255.255.255.0
172.16.3.0	172.16.3.2	172.16.3.254	172.16.3.255	255.255.255.0
...	...	...	...	...
172.16.254.0	172.16.254.0	172.16.254.254	172.16.254.255	255.255.255.0

No se toman en cuenta la red 172.16.0.0 por representar la red, ni la 172.16.255.0, por representar el broadcasting.

En el figura 6 de la página 26, muestra la topología.

- Las ips 172.16.0.1, 172.16.0.2, ... son ips locales
- La red 172.16.2.0/24, se encuentra accesible por la ip del router del aula 2, 172.16.2.100
- Para el resto de redes, ir a la 172.16.100.100

Tabla de rutas (encaminamientos) del router del aula 1, con acceso al aula 2:

Núm	Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
1	172.16.1.0	-	255.255.255.0	U	0	0	0	eth1
2	172.16.100.0	-	255.255.255.0	U	0	0	0	eth0
3	172.16.2.0	172.16.2.100	255.255.255.0	U	0	1	1	eth0
4	0.0.0.0	172.16.100.100	0.0.0.0	U	0	1	1	eth0

El significado es el siguiente:

1. 172.16.1.0 con máscara es ip de la máquina.
2. 172.16.100.0 con máscara es ip de la máquina.
3. Para el ir al aula 2 (Red 172.16.2.0), debemos ir por la ip 172.16.2.100.
4. Para ir a otra red debemos ir por la ip 172.16.100.100

Si no quisiéramos que los pcs del aula 1, puedan ver las máquinas del aula2, seria:

Núm	Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
1	172.16.1.0	-	255.255.255.0	U	0	0	0	eth1
2	172.16.100.0	-	255.255.255.0	U	0	0	0	eth0
4	0.0.0.0	172.16.100.100	0.0.0.0	U	1	0	0	eth0

10. Dirección de Broadcast

Se utiliza para emitir paquetes que deben recibir todas las máquinas de la subred.

Así pues, si el número de host de la subred se obtiene mediante el último octeto de la dirección IP (o sea, la máscara es 255.255.255.0), su dirección de broadcast será su dirección de red y haciendo un OR con 0.0.0.255. Pero esto sólo es cierto cuando no hay subneting.

Tablas de broadcast:

Dirección de Red	Mascara	Dirección Broadcast
192.168.0.0/24	255.255.255.0	192.168.0.255
192.168.0.0/25	255.255.255.128	192.168.0.128 y 192.168.0.255
172.16.0.0/16	255.255.0.0	172.16.0.255
172.16.0.0/24	255.255.255.0	172.16.255.255

10.1. Ejemplo

La dirección de broadcast siempre es la última IP de la red que tengas definida. Por eso en el caso de una red de 4 ip's (máscara 255.255.255.252) solo tenemos 2 ip's para equipos.

- Red: 192.168.0.0/30
- Mascara: 255.255.255.252 (11111111.11111111.11111111.11111100)
- Subredes: 1
- Máquinas: 2 elevado a 2 (2 elevado al números de ceros) - 2 = 4-2=2
- Ips Validas: 192.168.0.1, 192.168.0.2
- Broadcast: 192.168.0.3

10.2. Ejemplo

Este es un caso de red segmentada.

- Red: 192.168.0.0/25
- Mascara: 255.255.255.128 (11111111.11111111.11111111.10000000)
- Subredes: 2 elevado a 1 (2 elevado al número de unos del último octeto) = 2
- Máquinas: 2 elevado a 7 (2 elevado al números de ceros) - 2 = 128-2=126
- Ips Validas:
  Red 1: 192.168.0.1 a 192.168.0.127 Broadcast: 192.168.0.128
  Red 2: 192.168.0.129 a 192.168.0.254 Broadcast: 192.168.0.255

11. Saber en que red se encuentra un ip

Para saber si dos máquinas son visibles entre ellas, estas debe estar en la misma red.

La forma de comprobar q están en la misma red, es haciendo un and BIT A BIT entre la ip y su máscara, y comprobar q da la misma red.

11.1. Ejemplo

Red: 192.168.0.0
Máscara: 255.255.255.0
Subredes= 2 elevado a 0 = 1
Ip1: 192.168.0.1 AND 255.255.255.0 = Red 192.168.0.0
Ip2: 192.168.0.2 AND 255.255.255.0 = Red 192.168.0.0

11.2. Ejemplo

Red: 192.168.0.0
Máscara: 255.255.255.128 (11111111.11111111.11111111.10000000)
Subredes = 2 elevado a 1 = 2
Ip1: 192.168.0.1 AND 255.255.255.128 = Red 192.168.0.0
Ip2: 192.168.0.2 AND 255.255.255.128 = Red 192.168.0.0
Ip3: 192.168.0.129 (x.x.x.10000001) AND 255.255.255.128 = Red 192.168.0.128
Ip4: 192.168.0.130(x.x.x.10000010) AND 255.255.255.128 = Red 192.168.0.128

12. Segmentar una clase C en subredes

Podemos tener una red de tipo C, 192.168.0.0, y podemos crear varias subredes a través de la máscara.

Es importante remarcar que : **las direcciones de subred y broadcast están reservadas y no se usan para host**.

Podemos ver las subredes 192.168.0.0 según su máscara:

Subredes	Rango	Subredes
192.168.0.0/24	255.255.255.0	1
192.168.0.0/25	255.255.255.128	2
192.168.0.0/26	255.255.255.192	4
192.168.0.0/27	255.255.255.224	8

Veamos detalladamente las subredes.

12.1. Dirección de Red: 192.168.0.0/24

Subredes: 1

Hosts por subred: 2 elevado a 8 = 256 (Incluye dirección de subred y broadcast).

Mascara: 255.255.255.0

Núm	Binario	Rango	Subred	Broadcast
1	00000000	192.168.0.0-255	192.168.0.0	192.168.0.255

12.2. Dirección de Red: 192.168.0.0/25

Subredes: 2
Hosts por subred: 2 elevado a 7 = 128 (Contando subred y broadcast)
Máscara: 255.255.255.128

Subred	Rango	Subred	Broadcast
1	192.168.0.0-127	192.168.0.0	192.168.0.127
2	192.168.0.128-255	192.168.0.0.	192.168.0.255

12.3. Dirección de Red: 192.168.0.0/26

Subredes: 4
Hosts por subred: 2 elevado a 6= 64 (Contando subred y broadcast)
Máscara: 255.255.255.192

Núm	Binario	Rango	Subred	Broadcast
1	**00**000000	192.168.0.0-63	192.168.0.0	192.168.0.63
2	**01**000000	192.168.0.64-127	192.168.0.64	192.168.0.127
3	**10**000000	192.168.128-191	192.168.0.128	192.168.0.191
4	**11**000000	192.168.0.192-255	192.168.0.192	192.168.0.255

Nota: Las direcciones de subred y broadcast están reservadas y no se gastan para hosts.

12.4. Dirección de Red: 192.168.0.0/27

Subredes: 8
Hosts por subred: 2 elevado a 5= 32 (Contando subred y broadcast)
Máscara: 255.255.255.224

Núm	Ultimo Octeto	Rango	Subred	Broadcast
1	**000**00000	192.168.0.0-31	192.168.0.0	192.168.0.31
2	**001**00000	192.168.0.32-63	192.168.0.32	192.168.0.63
3	**010**00000	192.168.0.64-95	192.168.0.64	192.168.0.95
4	**011**00000	192.168.0.96-127	192.168.0.96	192.168.0.127
5	**100**00000	192.168.0.128-159	192.168.0.128	192.168.0.159
6	**101**00000	192.168.0.160-191	192.168.0.160	192.168.0.191
7	**110**00000	192.168.0.192-223	192.168.0.192	192.168.0.223
8	**111**00000	192.168.100.224-255	192.168.0.224	192.168.0.255

13. Calcular parámetros de una red: ipcalc

Parameter calculator for IPv4 addresses. Calcula parámetros de direcciones.

Instalación: apt-get install ipcalc

Ejemplo: ipcalc 192.168.0.1/24

```
Address:   192.168.0.1          11000000.10101000.00000000 .00000001
Netmask:   255.255.255.0 = 24   11111111.11111111.11111111 .00000000
Wildcard:  0.0.0.255            00000000.00000000.00000000 .11111111
=>
Network:   192.168.0.0/24       11000000.10101000.00000000 .00000000 (Class C)
Broadcast: 192.168.0.255        11000000.10101000.00000000 .11111111
HostMin:   192.168.0.1          11000000.10101000.00000000 .00000001
HostMax:   192.168.0.254        11000000.10101000.00000000 .11111110
Hosts/Net: 254                  (Private Internet RFC 1918)
```

14. Programa para simular redes: Network Simulator

"Nam is a Tcl/TK based animation tool for viewing network simulation traces and real world packet traces. It supports topology layout, packet level animation, and various data inspection tools.", es decir, es un herramienta para ver simulación de redes y trazas de paquetes. Soporta topologia por capas, y animación por nivel, y varias herramientas de inspección de datos.

Hay versión para windows y para linux. Nosotros nos centraremos en linux.

Direcciones web:

- Fichero ns-allinone-2.27.tar.gz. `http://www.isi.edu/nsnam/ns/ns-build.html`
- Tutorial: `http://www.isi.edu/nsnam/ns/tutorial/`
- Manual: `http://www.isi.edu/nsnam/nam/index.html`

Pasos:

- Bajarse el fichero: ns-allinone-2.27.tar.gz
- Descomprimirlo: tar xzf ns-allinone-2.27.tar.gz
- Instalarlo: ./install
- Testearlo: ./test

15. Bibliografía

1. IPTABLES. Manual práctico. http://www.pello.info/filez/firewall/iptables.html
2. Linux Networking-concepts HOWTO http://www.insflug.org/COMOs/conceptos-de-redes-COMO/conceptos-de-redes-COMO.html
3. Redes en Linux Como (Previamente Net-3 Como) http://www.insflug.org/COMOs/Redes-En-Linux-Como/Redes-En-Linux-Como.html
4. Enrutamiento avanzado y control de tráfico en Linux http://www.gulic.org/comos/LARTC/lartc.html
5. Subredes. http://www.htmlweb.net/redes/subredes/subredes_1.html
6. Valores de las máscaras de subred: subneting http://www.consultasccna.com/informacion/tcpip/subneti/valores.php
7. Guia de Administración de redes linux. http://es.tldp.org/Manuales-LuCAS/GARL2/garl-2.0.pdf
8. Seguridad en Redes http://members.fortunecity.es/mardedudascom/Informatica/_inf_redes/seguridadredes.htm
9. Seguridad en redes unix. http://es.tldp.org/Manuales-LuCAS/doc-unixsec/unixsec-html/
10. Firewall. http://www.redes.upv.es/~mperez/rc2/trabajos/FireWallstxt.pdf
11. Cortafuegos. http://es.tldp.org/COMO-INSFLUG/COMOs/Cortafuegos-Como/Cortafuegos-Como.html
12. The Network Simulator: Building Ns http://www.isi.edu/nsnam/ns/ns-build.html

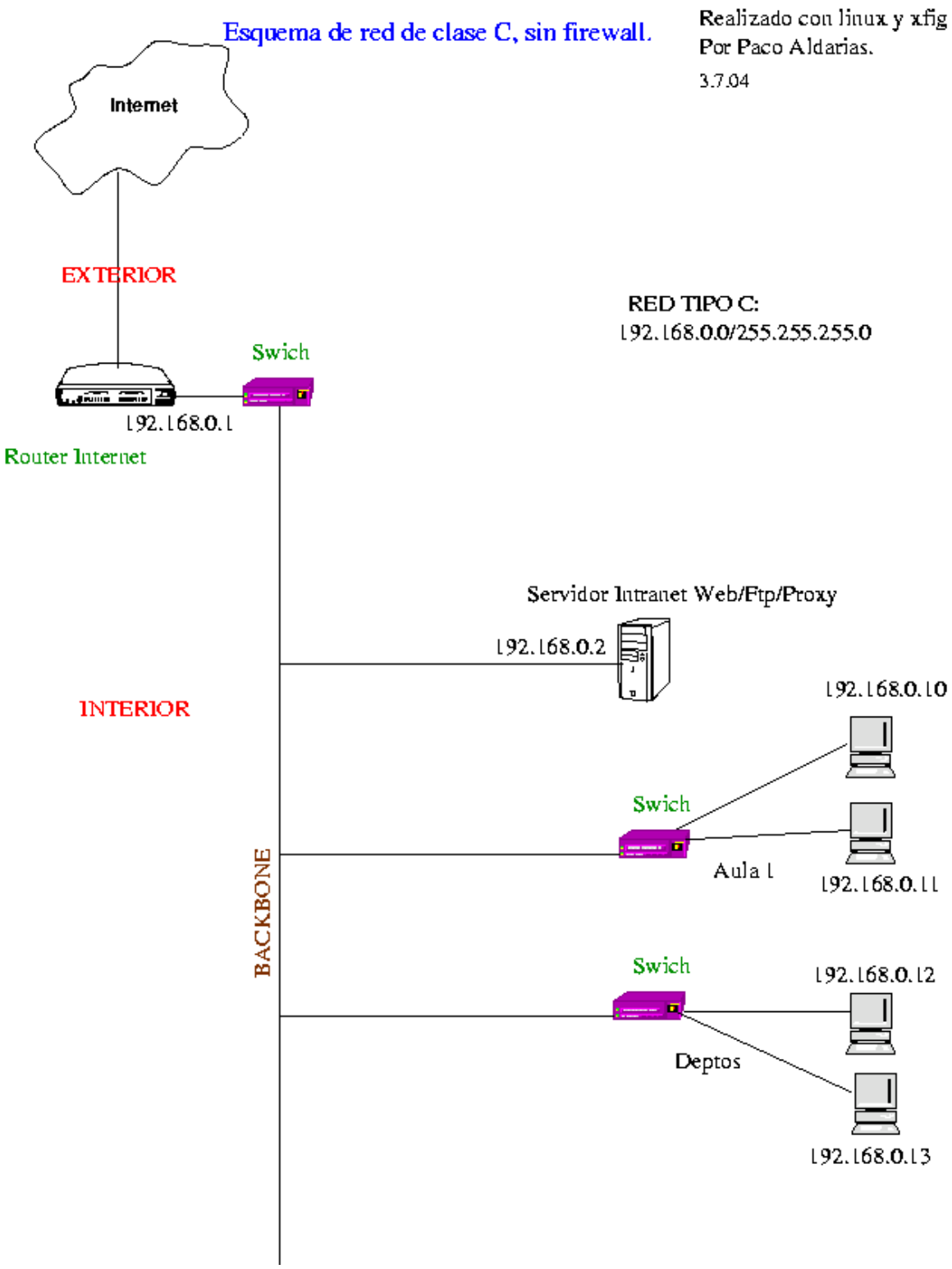

Figura 4: Ejemplo red de clase C

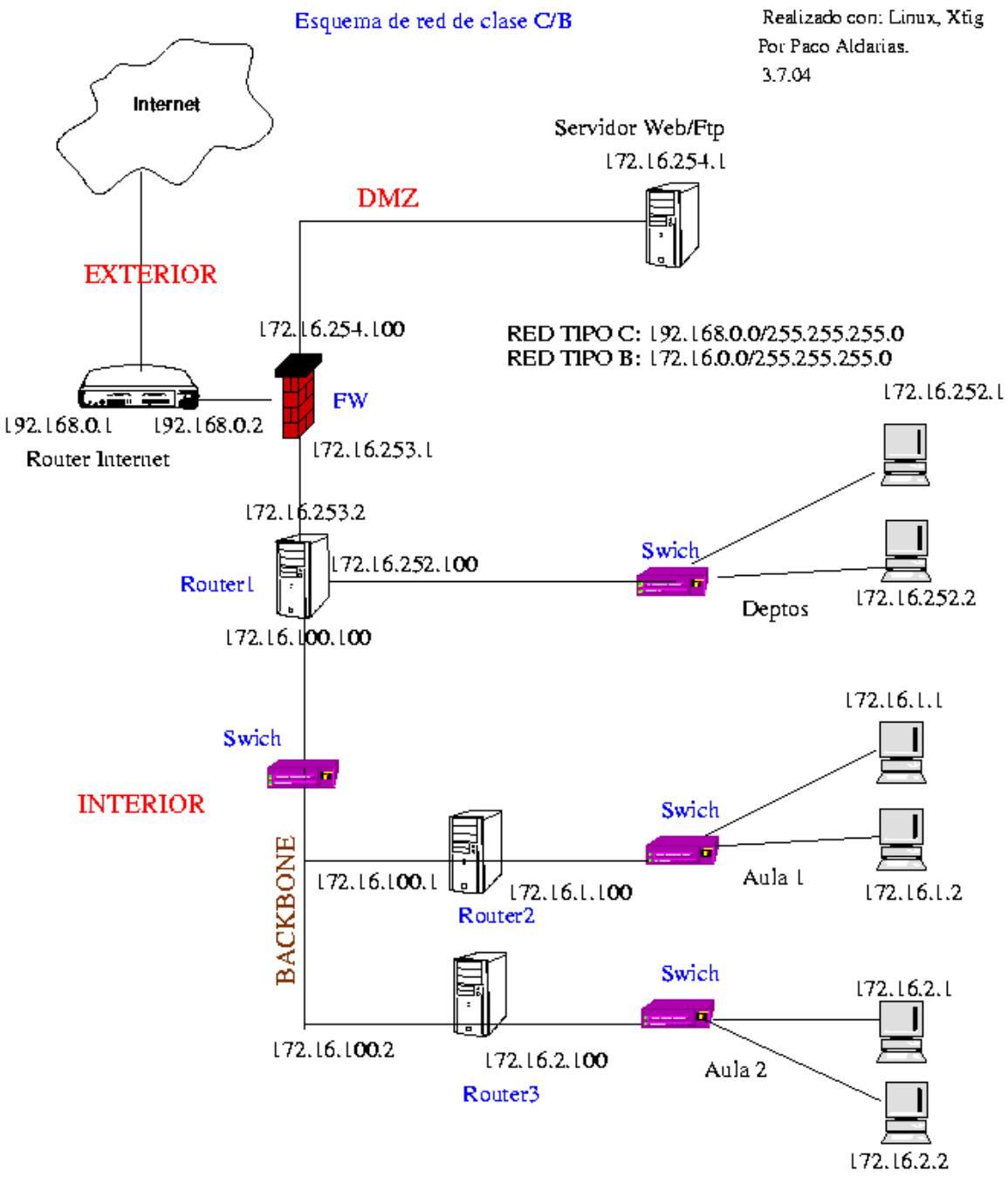

Figura 5: Ejemplo red de clase C/B

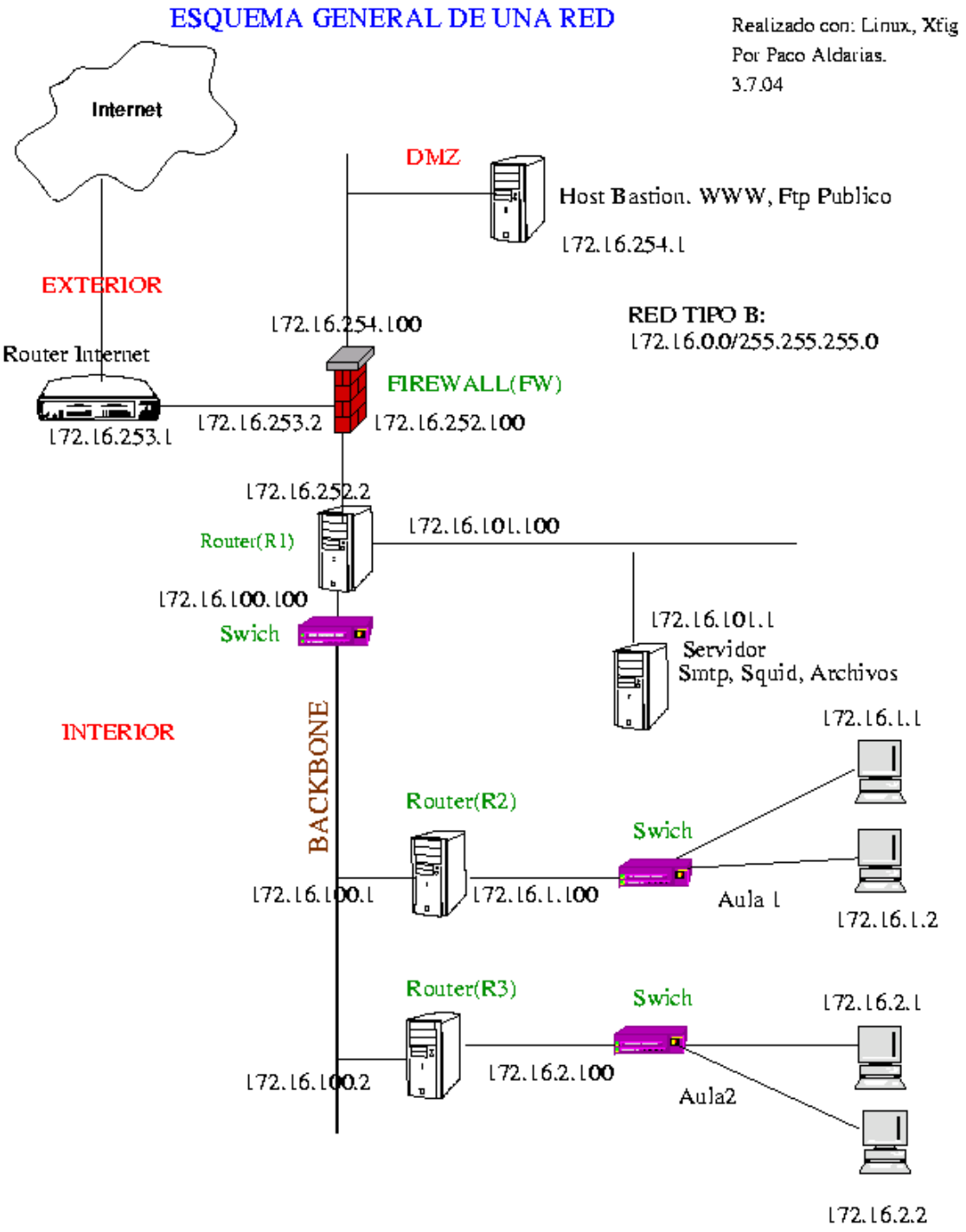

Figura 6: Ejemplo red con DMZ