Seguridad informática en Centros Educativos

(Valladolid, 3 de julio 2008)

Autor: Josep Pujadas i Jubany

Índice

Autor: Josep Pujadas i Jubany

1. Introducción. Problemas de seguridad habituales en centros educativos

1.1. Estaciones de trabajo

- **Protección antivirus.** En equipos Windows es imprescindible. En servidores UNIX/Linux recomendable, ya que estos sistemas suelen tener carpetas compartidas en las que hay archivos susceptibles de tener virus para equipos Windows. Ocurre los mismo si tienen un servidor de correo funcionando. En un cliente Linux no es necesario tener ningún antivirus instalado.
- **Congelar configuraciones.** Es aconsejable disponer de herramientas que permitan fijar las configuraciones, siendo estas inalterables por los usuarios. En Windows la mejor herramienta es sin duda DeepFreeze, de www.faronics.com. En todo caso, hay una herramienta llamada "antideepfreeze" que, al menos en determinadas versiones, puede dejar sin efecto a DeepFreeze. En UNIX/Linux se obtienen resultados semejantes haciendo que el usuario no pueda escalar nunca superusuario y con scripts en el arranque y en el cierre de los equipos.
- **Antivirus+Congelación.** Aunque se tengan congeladas las configuraciones conviene tener protegidos los equipos con una solución antivirus. En UNIX/Linux bastará con un escaneador de archivos como www.clamav.net y en Windows habrá que tener una protección permanente (por desgracia no es suficiente un escaneador como www.clamwin.com). Si podemos, siempre es mejor un antivirus con administración centralizada. De esta forma tendremos una consola con el estado de todos los equipos y sus incidencias.
- **Recursos compartidos.** Las estaciones Windows tienen recursos compartidos para tareas de administración. Si no se deshabilitan, un usuario administrador puede acceder a toda la máquina desde otra máquina de la red local. En UNIX/Linux no hay nada compartido por defecto, por lo que quien administra la red suele ser más consciente de lo que tiene entre manos.
- **Navegadores.** Aparte de procurar tenerlos actualizados conviene deshabilitar las funcionalidades que tienen de guardar nombres de usuario y contraseñas.
- **Acceso a la BIOS.** El acceso a cambios en las BIOS debe protegerse con contraseña.
- **Orden de arranque en BIOS.** Los equipos deben arrancar sólo desde el disco duro.
- **Dispositivos removibles.** Las unidades de CDs, disqueteras, lápices USB y otros son una fuente (inevitable) de entrada/salida de datos/programas en el Centro.
- **Subida y bajada de archivos.** Aunque se puede limitar, como veremos más adelante, la subida y bajada de archivos de Internet también es un punto de entrada/salida de datos/programas en el Centro, a tener en cuenta.

1.2. Usuarios y contraseñas

- **Personal e intransferible.** Hay que concienciar a los usuarios (alumnos, profesorado y PAS) que su identificador de usuario y contraseña a los servicios que tenga el Centro son personales e intransferibles.
- **Contraseñas seguras.** Hay que establecer contraseñas basadas en letras y números, aunque parezca inicialmente engorroso.
- **Cambio de contraseñas.** Hay que establecer un sistema para que el usuario pueda cambiar su contraseña en caso de duda.
- **Duración de las contraseñas.** Conviene establecer periodos de caducidad de las contraseñas.

1.3. Filtrado de contenidos

La adopción de un servidor proxy (es.wikipedia.org/wiki/Squid) en el Centro permite disponer de una mayor velocidad de navegación, ya que las páginas visitadas suelen verse en diferentes equipos de forma prácticamente simultánea.

Además, hay que tener presente que en caso de tener congeladas las estaciones de trabajo, éstas no almacenarán páginas en su caché entre un arranque y otro.

La legislación vigente (Ley de Protección de Menores), el ideario del Centro y el uso racional y seguro de los recursos de la red local hacen también que sea idóneo que el servidor proxy permita establecer políticas de filtrado.

Algunos servicios web son causa habitual de problemas en las aulas, con lo que un servidor proxy supondrá una mejora de ancho de banda, mayor seguridad y un “estar más por la labor”.

Autor: Josep Pujadas i Jubany

1.4. Filtrado de servicios

¿Qué se puede hacer en nuestra red local? ¿Desde dónde hacia dónde?

- ¿Puede el equipo de un alumno ver el equipo de un profesor?
- ¿Pueden los usuarios descargar archivos con programas punto a punto (P2P), como Ares o eMule?
- ¿Tiene el Centro servicios en Internet? ¿Son seguros?

La seguridad de una red local no consiste en sólo cerciorarse de que estamos protegidos de posibles ataques desde afuera. Hay que pensar en qué pueden hacer los usuarios de dentro hacia afuera y de dentro hacia dentro.

Revisar la topología de nuestra red local, auditarla y disponer de un cortafuegos (es.wikipedia.org/wiki/Cortafuegos_%28inform%C3%A1tica%29) nos permitirán "acotar" los riesgos que estemos dispuestos a correr.

1.5. Servidores

En nuestros servidores deberemos tener en cuenta:

- **Accesibilidad física**. Habitación específica, climatizada, de difícil acceso, cerrada con llave, ...
- **Accesibilidad lógica**. Sólo accesible para los servicios que estemos dando y con control de desde dónde se puede acceder a ellos. Ser conscientes, por ejemplo, de si un determinado servicio de ficheros es público, privado, sólo en la red local o también en Internet, ...
- **Actualizaciones**. Mantener sistemas operativos y aplicaciones actualizados, sobre todo en lo que se refiere a vulnerabilidades.
- **Solución antivirus**. En tiempo real si es Windows, como escaneador periódico si es UNIX/Linux.
- **Copias de seguridad**. Hay que dejar muy claro a los usuarios qué políticas de seguridad se siguen con sus datos. Las copias deben ser periódicas y automatizadas. Pueden hacerse contra una máquina de copias al otro lado del edificio. La información más sensible debe sacarse del edificio. La dirección debe confiar esta tarea a una persona responsable de la misma.
- **Usuario/contraseña administrador.** Emplear distintos usuarios y contraseñas para los servicios. No conviene tener una llave maestra para todo. Tener informada a la dirección del Centro de cuáles son los usuarios y contraseñas del administrador de sistemas y para qué sirven (en lugar seguro).

Autor: Josep Pujadas i Jubany

2. Topología de redes. Direcciones IP y subredes

2.1. Modelo OSI

Es un estándar que define los niveles que debe tener cualquier comunicación en una red, es.wikipedia.org/wiki/Modelo_OSI.

Hablemos del modelo OSI aplicado a nuestras redes ...

- **Nivel 1, físico**. Solemos emplear Ethernet sobre hilo de cuatro pares trenzados, es.wikipedia.org/wiki/RJ-45. Sólo dos de los pares son necesarios para velocidades de 100 Mbit/s. Para 1.000 Mbit/s se usan los cuatro. La información es la unidad mínima, el **bit**.
- **Nivel 2, enlace de datos**. Cada equipo tiene su dirección física, conocida por MAC, es.wikipedia.org/wiki/Direcci%C3%B3n_MAC. Esta dirección es, teóricamente, única para cada dispositivo de red en el mundo y está compuesta por 48 bit, representados (para facilitar la lectura) en 6 bloques hexadecimales. La información se organiza por **tramas** o canales. Es el nivel en que trabajan los switches.
- **Nivel 3, de red**. Es lo que denominamos dirección IP y enrutamiento, es.wikipedia.org/wiki/Direcci%C3%B3n_IP. La información de organiza por **paquetes**. Es el nivel en el que trabajan los routers y cortafuegos, aunque también pueden trabajar en nivel 2.
- **Nivel 4, de transporte**. Es el encargado de tratar los datos recibidos de los niveles superiores y enviarlos al nivel de red. También se encarga de comprobar que la transmisión se ha efectuado sin problemas. La información se organiza por **segmentos**.
- **Nivel 5, de sesión**. Establecimiento, gestión y finalización de comunicación entre dos equipos. Es un nivel que en algunos casos no existe, ya que no todas las comunicaciones de una red implican el establecimiento de una sesión. Los cortafuegos y routers actúan en esta capa, mediante bloqueo, desbloqueo o redireccionamiento de **puertos**.
- **Nivel 6, de presentación**. Es la parte encargada de traducir tablas de caracteres, encriptación y compresión de datos, caso de ser necesario. Este nivel suele estar implementado en los propios equipos de transmisión de datos y en los programas.
- **Nivel 7, de aplicación**. Son los programas que se usan para realizar las comunicaciones. Pueden ser de servidor (dar servicio) o de cliente (usar servicio).

Hay, pues, un total de 7 niveles y, pensando en la seguridad, cada uno tiene cuestiones a tener en cuenta. Por citar un ejemplo sobre el **Nivel 1**, no es lo mismo hacer pasar toda la red de un Centro por un cableado único que tenerlo segmentado y conectado a un cortafuegos.

2.2. Protocolo IP (Internet Protocol)

Aunque parezca un nombre erróneo, nuestra red local emplea seguramente el mismo protocolo que Internet, es.wikipedia.org/wiki/Protocolo_de_Internet.

Esto es, los equipos son capaces de comunicarse entre ellos gracias a que tienen una dirección lógica, llamada **dirección IP** (Nivel 3 del modelo OSI).

2.2.1. Direcciones IP

Las direcciones IP constan de 4 Byte (IPv4) o de 6 Byte (IPv6), siendo más usual el primer formato.

Estos cuatro Byte se representan por su equivalente decimal, separados por un punto, con el fin de facilitar la lectura.

Por ejemplo, la dirección 192.168.10.26 corresponde a los siguientes cuatro Bytes:

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	128 + 64 = 192	192
128	64	32	16	8	4	2	1		
1	**1**	**0**	**0**	**0**	**0**	**0**	**0**		
2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	128 + 32 + 8 = 168	168
128	64	32	16	8	4	2	1		
1	**0**	**1**	**0**	**1**	**0**	**0**	**0**		
2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	8 + 2 = 10	10
128	64	32	16	8	4	2	1		
0	**0**	**0**	**0**	**1**	**0**	**1**	**0**		
2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	16 + 8 + 2 = 26	26
128	64	32	16	8	4	2	1		
0	**0**	**0**	**1**	**1**	**0**	**1**	**0**		

Nota: el profesorado de Matemáticas y de Tecnología seguramente ya estarán familiarizados respecto al manejo de cifras en diferentes bases (binaria y decimal).

La mínima dirección IP será, por tanto, 0.0.0.0 (todos los bit a cero) y la máxima la 255.255.255.255 (todos los bit a 1).

Sin embargo, el 0 y el 255 tienen significados especiales, como veremos más adelante.

2.2.2. Máscaras de las direcciones IP

Para que las redes sean manejables se crearon las llamadas subredes, es.wikipedia.org/wiki/Subred. Es por ello que una dirección IP lleva asociada siempre una máscara. En IPv4 la máscara es también de 4 Byte.

Así, la máscara 255.255.255.0 corresponde a los siguientes Byte:

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	128 + ... + 2 +1 = 255	255
128	64	32	16	8	4	2	1		
1	**1**	**1**	**1**	**1**	**1**	**1**	**1**		
2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	128 + ... + 2 + 1 = 255	255
128	64	32	16	8	4	2	1		
1	**1**	**1**	**1**	**1**	**1**	**1**	**1**		
2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	128 + ... + 2 + 1 = 255	255
128	64	32	16	8	4	2	1		
1	**1**	**1**	**1**	**1**	**1**	**1**	**1**		
2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	0	0
128	64	32	16	8	4	2	1		
0	**0**	**0**	**0**	**0**	**0**	**0**	**0**		

Dos equipos se ven entre sí si pertenecen a una misma subred. En caso contrario, tendrá que haber algún dispositivo capaz de unir (enrutar) las dos subredes (router, bridge, gateway, ...).

Dos equipos pertenecen a la misma subred si haciendo una operación lógica AND entre su dirección IP y su máscara obtenemos la misma numeración. Ejemplo:

Dirección IP	192.168.10.26	11000000.10101000.00001010.00011010
Máscara	255.255.255.0	11111111.11111111.11111111.00000000
Subred	192.168.10.0	11000000.10101000.00001010.00000000

Dirección IP	192.168.10.1	11000000.10101000.00001010.00000001
Máscara	255.255.255.0	11111111.11111111.11111111.00000000
Subred	192.168.10.0	11000000.10101000.00001010.00000000

En el ejemplo puede verse el significado de una dirección IP terminada en cero:

Una dirección IP terminada en cero se refiere a la subred y no a una máquina en concreto.

Se deduce fácilmente que con una máscara 255.255.255.0 la subred de nuestro ejemplo podrá tener un máximo de 255 IPs distintas, de la 192.168.10.0 a la 192.168.10.255.

Ya hemos dicho que la 192.168.10.0 no la podemos emplear para un equipo, ya que está reservada para referirse a la subred.

Tampoco podremos emplear la 255 para un equipo, ya que tiene una utilidad especial, el **broadcast**. El **broadcast** sirve para enviar anuncios dentro de una subred. Cuando se envían **paquetes** a la dirección 255 los reciben todos los equipos de la subred.

En conclusión, con nuestra máscara 255.255.255.0 sólo podremos tener 254 equipos distintos en nuestra subred.

Dirección IP y máscara suelen representarse separadas por una barra (siguiendo con nuestros ejemplos):

192.168.10.26/255.255.255.0 o 192.168.10.26/24

La segunda notación se denomina CIDR, es.wikipedia.org/wiki/CIDR, siendo una mejora de la primera. La cifra representa el número de bits más significativos que emplea la máscara, en nuestro ejemplo 24.

2.2.3. Clases de redes

En un Centro no es habitual tener más de 254 equipos en una misma subred, pero en grandes corporaciones (y, por supuesto, en Internet) sí lo es.

De ahí que hayan normalizado las subredes en tres grandes clases:

- **Clase A.** La red viene definida por el primer Byte, es decir, la máscara de la mayor subred posible es 255.0.0.0 (8 bit). Con ello se pueden tener hasta (2^{24} – 2) equipos.
- **Clase B.** La red está definida por los dos primeros Byte, es decir, la máscara de la mayor subred posible es 255.255.0.0 (16 bit). Con ello se pueden tener hasta (2^{16} – 2) equipos.
- **Clase C.** La red está definida por los tres primeros Byte, siendo la máscara de la mayor subred posible 255.255.255.0 (24 bit). Es el tipo de red de los ejemplos que hemos visto antes, 2^8 –2 equipos (254).

Dada la complejidad que puede entrañar el diseño de subredes existe un buen número de aplicaciones que lo facilitan, incluso en Internet. Por ejemplo, www.subnet-calculator.com.

2.2.4. Direcciones públicas

Son las empleadas en Internet. Nunca deberemos emplear direcciones públicas en una red privada.

Están asignadas por una serie de registros internacionales. Para saber a quién pertenece una dirección IP puede emplearse el registro norteamericano, www.arin.net/whois, que también facilita el acceso al resto de registros.

Autor: Josep Pujadas i Jubany

2.2.5. Direcciones privadas

Son las empleadas en redes locales, es.wikipedia.org/wiki/Red_privada.

Nunca deben emplearse en equipos que están en Internet. A veces no es así y es una posible fuente de ataques a redes privadas. Un cortafuegos debe impedir que nos llegue tráfico procedente de direcciones privadas más allá de nuestra red local.

Debemos cerciorarnos de que nuestra red local sólo emplee direcciones privadas. Véase la tabla de es.wikipedia.org/wiki/Red_privada.

2.2.6. Direcciones especiales

- **127.0.0.1**. Se emplea para el propio equipo. De esta forma pueden realizarse acciones refiriéndose a la propia máquina.
- **Bogon networks**. Son direcciones públicas que no han sido asignadas nunca. Por tanto, no pueden existir. Un cortafuegos debe cortar cualquier paquete que proceda de una dirección de este tipo, www.completewhois.com/bogons.

2.2.7. Enrutamiento

es.wikipedia.org/wiki/Protocolo_IP - Enrutamiento

Una de las características más importantes del protocolo IP es la posibilidad de definir caminos hacia IPs de destino.

El ejemplo más simple de esto es cuando le indicamos a un equipo cuál es su puerta de enlace predeterminada, que equivale a decirle “todo lo que no sea de tu subred tiene que salir por ahí” ...

3. Protocolos más habituales, TCP, UDP e ICMP

¿Hemos hablado del protocolo IP y ahora hablamos de más protocolos? No me aclaro ...

Recordemos que hemos dicho que el protocolo IP pertenece al nivel 3 (red) del modelo ISO, mientras que ahora vamos a hablar del nivel 4 (transporte) del modelo ISO.

Cuando trabajemos con un dispositivo de comunicaciones veremos muchos protocolos a nivel de transporte, siendo los más importantes TCP, UDP e ICMP.

3.1. TCP (Transmission Control Protocol)

es.wikipedia.org/wiki/Transmission_Control_Protocol

Establece un diálogo entre equipos, asegurándose de que la información llega correctamente a su destino. Transmite datos, recibe confirmación del destino y, si es necesario, repite (hasta un cierto límite) el envío de paquetes.

Esto último es muy importante, ya que por el lado positivo garantiza la calidad de la comunicación. Por el lado negativo, cuando hay problemas de cableado en una red puede ser motivo de colapso. Por tanto, un buen cableado es esencial.

La mayoría de aplicaciones en red funcionan por TCP. Es, por tanto, el transporte por excelencia.

3.2. UDP (User Datagram Protocol)

es.wikipedia.org/wiki/UDP

No existe el concepto de establecimiento de conexión y, por tanto, no hay confirmación por parte del destinatario. Simplemente hay un envío a la red y, en todo caso, una respuesta pero sin esperar una confirmación de recepción.

Se emplea para servicios tales como anuncios en la red, en los que un equipo dice algo a los otros, estos escuchan y a lo sumo envían una respuesta aunque sin cerciorarse de que ha sido recibida.

Un caso típico son los servicios de sincronización horaria, es.wikipedia.org/wiki/NTP. El cliente pide la hora al servidor horario, éste contesta con ella pero no espera a que el cliente le diga si recibió o no la hora.

Puede suceder que en una red local haya excesivo “ruido” con UDP, cuestión que hay que controlar para que nuestra red sea eficiente.

3.3. ICMP (Internet Control Message Protocol)

es.wikipedia.org/wiki/ICMP

De hecho no pertenece al nivel de transporte, sino que es una parte del nivel de red y, por tanto, del propio protocolo IP. Se trata pues de un subprotocolo de red.

Es la parte que se encarga de la gestión de errores en una transmisión, indicando si un servicio está o no disponible en un equipo remoto.

Esto hace que haya aplicaciones diseñadas para administradores de red que empleen este subprotocolo, tales como ping o tracert/traceroute.

4. ¿Qué es un puerto? Puertos normalizados y puertos no normalizados

es.wikipedia.org/wiki/TCP - Puertos_TCP

Los protocolos de transporte precisan emplear una numeración adicional a la dirección IP para diferenciar unas aplicaciones de otras. De esta manera los equipos pueden establecer múltiples comunicaciones, con distintos servicios y/o equipos.

Para los puertos se añaden 16 bit a la dirección IP, con lo que una dirección IP puede tener 2^{16} = 65.536 puertos distintos.

Los números de puertos están normalizados por www.iana.org.

Existen tres categorías de puertos:

- **Los bien conocidos**, que van del 0 al 1023. Son los empleados en los servicios más habituales de la red. Por ejemplo, la navegación web suele emplear el 80 cuando en nuestro navegador indicamos HTTP y el 443 cuando indicamos HTTPs.
- **Los registrados**, que van del 1024 al 49151. Son los que www.iana.org ha asignado a los servicios que dependen de grandes fabricantes de sistemas o como puertos alternativos/temporales de otros servicios. Por ejemplo, el 3389 es para escritorios remotos de Microsoft (RDP). Y el 8008 está asignado como puerto alternativo para HTTP (el 80).
- **Los dinámicos**, que van del 49152 al final. También se les denomina privados. Son los que los equipos van tomando (normalmente de forma automática) a medida que necesitan nuevos puertos para las comunicaciones que van estableciendo. De ahí el nombre de dinámicos.

La lista de puertos completos y al día puede encontrarse en:

www.iana.org/assignments/port-numbers

Una comunicación entre dos equipos suele pues representarse por las dos IPs de los equipos, seguidas cada una de ellas por dos puntos y el número de puerto. Ejemplo:

192.168.10.26:1598 -> 88.221.22.9:80

En muchas herramientas de análisis de comunicaciones la IP y/o el puerto son sustituidos por el nombre de máquina o de servicio, respectivamente:

mi_maquina:1598 -> 88.221.22.9:http

4.1. Sobre los puertos dinámicos

Es normal que un equipo cliente tenga puertos dinámicos en uso. Cuando nuestro ordenador establece, por ejemplo, una sesión con un servidor web, emplea un número de puerto que tenga libre (de forma dinámica) para ir al puerto 80 del servidor web.

Menos normal es que nuestro ordenador tenga como destino IPs con puertos dinámicos, salvo FTP. Si no es el caso, será bastante probable que el equipo tenga funcionando una aplicación punto a punto (P2P), como Ares o eMule.

4.2. ¿Pueden cambiarse los puertos?

La asignación de números de puertos que hace IANA es sólo un convenio que se debe respetar siempre que sea posible.

Sin embargo, hay razones por las cuales un servicio (en nuestra red local o en Internet) puede cambiarse de número de puerto:

- **Por seguridad**. Si queremos "esconder" un servicio una buena medida es cambiarlo de puerto. Por ejemplo, el acceso seguro a consolas de UNIX/Linux (SSH) suele hacerse por el puerto 22. Si tenemos este servicio abierto en Internet con este puerto habrá intentos continuos de logueo con usuarios y contraseñas aleatorios. Una forma de minimizar esto es poner otro puerto que no usemos.
- **Para diferenciar servicios**. Si en una misma IP tenemos dos servicios parecidos tendremos que ponerlos en puertos distintos. Por ejemplo, la IP pública de nuestro Centro puede dar acceso a más de un servidor web interno: el oficial por el puerto 80 (HTTP) y el no-oficial por un puerto entre 8000 y 8100 (que suelen ser los empleados como HTTP alternativo aunque IANA los haya asignado a otras cosas).
- **Por conflicto entre servicios**. Debido a que la asignación de IANA no es de obligado cumplimiento a veces podemos encontrarnos con algún conflicto y tener que asignar un puerto distinto al inicialmente previsto por el servicio.

Autor: Josep Pujadas i Jubany

5. Servicios más usuales (Samba/CIFS, NetBIOS, HTTP, DNS, NTP, FTP, SSH, ...)

Visto qué es un puerto podemos concentrarnos en los servicios. Viene a ser lo mismo, pero hay servicios que emplean más de un puerto. Los servicios más usuales en nuestras redes son:

5.1. Compartición de archivos e impresoras de Windows

Cuando un equipo Windows comparte sus archivos y/o sus impresoras en una red está actuando como un servidor de archivos y/o de impresoras, aunque pensemos en él como una estación de trabajo.

Para que una máquina UNIX/Linux comparta archivos y/o impresoras como lo hace Windows tiene que tener instalado el servicio Samba, también llamado CIFS.

En consecuencia, la compartición de archivos e impresoras de Windows, Samba y CIFS son prácticamente lo mismo.

Es más, un servidor Samba/CIFS (en UNIX/Linux) puede ser un controlador de dominio (Active Directory) al estilo de Windows 2000 Server:

es.wikipedia.org/wiki/Samba_(programa)

Para dar todos estos servicios es necesario establecer múltiples comunicaciones entre los equipos, por lo que se emplean varios protocolos de transporte y puertos:

- UDP 137, UDP 138, TCP 139 y TCP 445

Hay autores que denominan el servicio de archivos/impresoras de Windows (Samba/CIFS) como NetBIOS, lo que no deja de ser un error. Creado por Microsoft para redes primitivas, NetBIOS sigue empleándose como parte del servicio de archivos/impresoras en red y es el responsable de que nuestro PC nos presente los “equipos próximos”:

es.wikipedia.org/wiki/NetBIOS

5.2. Navegación por Internet

La navegación web emplea (habitualmente) los puertos:

- TCP 80 para navegación HTTP.
- TCP 443, para navegación HTTPs (HTTP + SSL). La comunicación es encriptada, es.wikipedia.org/wiki/Transport_Layer_Security.

5.3. Resolución de nombres (DNS)

Manejar IPs resulta complejo y engorroso. Es más cómodo emplear nombres de equipo. El paradigma de esto es Internet.

¿Alguien sabe qué web es 69.147.83.33? Seguramente no. En estos momentos, en mi máquina, sé que es www.freebsd.org.

Hagámoslos al revés ahora. Abro mi navegador y le digo que vaya a www.freebsd.org. ¿Cómo sabe mi navegador a qué IP tiene que ir?

Pues yendo a un servicio de traducción de nombres a IPs, un servicio DNS (Domain Name Server). En redes pequeñas este servicio está en el exterior, en Internet. En redes grandes conviene tener un servicio local (conectado a su vez con uno o varios externos).

es.wikipedia.org/wiki/Domain_Name_System

Las peticiones a servidores DNS emplean el puerto 53 y pueden ser tanto UDP como TCP.

Si nuestro equipo no tiene acceso a un servicio DNS no podrá navegar por Internet, a menos que vayamos indicando números de IP en nuestro navegador ...

5.4. Servicio de horario

Aunque hay distintos servicios para sincronizar horarios de equipos el más usual es NTP, es.wikipedia.org/wiki/NTP. Emplea el puerto:

- UDP 123

En algunos casos este servicio puede ser problemático. Es importante escoger un servidor horario que no esté colapsado, tener bien configurado tanto el huso horario como el horario de verano y hacer una sincronización inicial del cliente con un horario próximo al real (si hay una gran diferencia, el cliente no sincroniza).

Otro aspecto a considerar es que hay configuraciones de estación de trabajo que tienden a realizar sincronizaciones horarias a la puesta en marcha del equipo. Esto puede generar bastante “ruido” NTP en nuestra red local. Tener un servidor NTP local puede ser conveniente (si se emplea Active Directory el controlador de dominio ya hace esta función).

Como servidor de horario externo recomiendo cualquiera de los listados en www.pool.ntp.org/zone/europe. Por ejemplo, 1.europe.pool.ntp.org.

5.5. Transferencia de archivos por FTP

Es uno de los servicios más populares. ¿Quién no se ha bajado algún software de un servidor FTP anónimo?

O quién no ha subido su página web por FTP?

es.wikipedia.org/wiki/Ftp. Emplea los puertos:

- TCP 21, para control.
- TCP 20, para datos si el servidor opera en modo activo.
- TCP entre 1024 y 5000, para datos si el servidor opera en modo pasivo.

Esto es un auténtico quebradero de cabeza para los administradores de red ya que las conexiones FTP son pues multipuerto y, en muchos casos, emplean puertos complicados de controlar.

Hay que añadirle el hecho de que es una transmisión en Internet no encriptada y, por tanto, no segura. Incluso el usuario y la contraseña (en caso de existir) viajan sin encriptar.

Si tenemos un servicio FTP en el Centro que requiera confidencialidad tenemos que migrarlo a SFTP (FTP sobre SSH).

5.6. Secure Shell (SSH)

Este servicio se creó para poder acceder a consolas UNIX/Linux de modo seguro, mediante encriptación. Toda la comunicación se realiza de forma encriptada, incluyendo el nombre de usuario y contraseña. Se puede obviar el nombre de usuario y contraseña si se trabaja con certificados y llaves de servidor y cliente, es.wikipedia.org/wiki/Ssh

Debe emplearse siempre la versión 2 de este servicio, ya que la 1 tenía problemas de seguridad. El puerto habitual es:

- TCP 22

Autor: Josep Pujadas i Jubany

Dado que este servicio permite el acceso a la consola de un equipo puede entrañar algunos problemas de seguridad, en el sentido de que hay que acotar qué puede hacer el usuario con su consola.

Se suele emplear SSH para realizar transferencia de archivos, recibiendo dos nombres:

- SFTP, FTP sobre SSH (ya comentado).
- SCP (Secure Copy). Es parecido a una copia de archivos entre carpetas de distintos equipos, pero a través de una comunicación SSH.

SSH también se emplea para la tunelización. La tunelización consiste en hacer pasar una segunda comunicación (entre nuestro equipo local y otro remoto) por la comunicación SSH establecida, es.wikipedia.org/wiki/Protocolo_tunelizado. Es una herramienta extraordinaria (administración remota de equipos, encriptación de comunicaciones, ...)

5.7. Telnet

Antes de existir SSH el acceso a las consolas de los equipos se realizaba mediante Telnet. El puerto utilizado es:

- TCP 23

Es un protocolo no encriptado, por lo que es altamente inseguro. Sin embargo todavía es utilizado en muchas redes locales para acceder a dispositivos de comunicaciones.

No debemos poner nunca un servicio Telnet en Internet.

5.8. SMTP (transferencia de correo)

es.wikipedia.org/wiki/SMTP. Emplea el puerto:

- TCP 25

El servicio SMTP sirve para emitir, transferir y recibir correo. Se entiende esta última acción (la de recibir) desde el punto de vista de servidor de correo, no de usuario (los usuarios suelen leer el correo con el servicio POP3).

Es un servicio muy problemático, por lo que si tenemos un SMTP hay que tenerlo muy bien asegurado contra spam (correo basura), relay (uso de nuestro SMTP para emitir correo) y virus.

El tráfico SMTP puede ir encriptado por SSL o no. La mayoría de servicios SMTP no emplean encriptación.

5.9. POP3 (lectura de correo)

http://es.wikipedia.org/wiki/POP3. Emplea los puertos:

- TCP 110 en modo no seguro.
- TCP 995 en modo seguro (SSL).

Es el servicio que usualmente empleamos para leer nuestro correo electrónico con un cliente de correo como ThunderBird o Outlook.

No entraña grandes problemas de seguridad, aunque la mayoría de servicios POP3 trabajan sin encriptación.

5.10.RDP (escritorio remoto)

es.wikipedia.org/wiki/RDP. Emplea el puerto:

- TCP 3389

Se emplea para acceder remotamente a escritorios Windows.

Aunque el diálogo es encriptado no conviene tener directamente este servicio en Internet.

Se emplea para tareas de administración de equipos y/o para ejecución remota de aplicaciones Windows (servidor de aplicaciones).

5.11.VNC (acceso remoto)

http://es.wikipedia.org/wiki/VNC. Emplea el puerto:

- TCP 5900

Permite acceder remotamente a un equipo, como si estuviéramos delante. Por tanto, podemos ver qué está haciendo el usuario. Empleado para tareas de administración. No encriptado, por lo que no es conveniente poner este servicio directamente en Internet.

En en.wikipedia.org/wiki/Comparison_of_remote_desktop_software hay una interesante comparación de aplicaciones de acceso remoto, tanto para la parte servidora como la de cliente.

www.tightvnc.com es una de las mejores soluciones libres VNC.

6. Herramientas de análisis de redes (ping, traceroute, nslookup, nmap ...)

Nuestro sistema operativo trae consigo un buen número de herramientas que nos pueden servir para analizar nuestra red y detectar problemas.

Evidentemente hay un buen número de aplicaciones (libres y comerciales), algunas de las cuales veremos.

No pretendo ser exhaustivo, tan solo mostrar las herramientas que empleo más habitualmente ...

6.1. ping (sistema operativo, consola)

Nos sirve para ver si un equipo es accesible y el tiempo empleado para verlo. Ejemplos:

ping 192.168.10.1
ping www.freebsd.org

Obsérvese que:

- Podemos hacer ping tanto por IP como por nombre. En el caso de emplear nombre tenemos que estar seguro de que nuestra máquina tiene acceso a un servicio DNS (traducción del nombre a IP).
- Si la máquina de destino tiene bloqueado el acceso por ping no nos responderá, por lo que podemos creer que no existe o que está apagada. ping suele emplearse muchas veces para comprobar si hay conexión con otro equipo y más concretamente con Internet. Debemos pues cerciorarnos que estamos empleando un destino que responde a ping.

Manuales de ping:

- En Windows, teclear **ping /?**
- En Windows, **ping /? > manual_ping.txt** y luego abrir **manual_ping.txt** con notepad.
- En UNIX/Linux, **man ping** o manual en Internet de distribución preferida, www.freebsd.org/cgi/man.cgi?query=ping

Como suele suceder en la mayoría de herramientas, la sintaxis de Windows y de UNIX/Linux tienen diferencias. Además, el comando de UNIX/Linux tiene muchas más funciones.

Autor: Josep Pujadas i Jubany

6.2. traceroute (sistema operativo, consola)

El ping nos dice si llegamos a un equipo pero no nos da información del camino seguido. Traceroute nos dirá el camino seguido y el tiempo empleado en cada tramo (salto). Ejemplos:

traceroute 192.168.10.1
traceroute www.freebsd.org

En Windows, el comando recibe el nombre de tracert y es mucho menos potente.

Manuales de traceroute:

- En Windows, teclear **tracert /?**
- En UNIX/Linux, **man traceroute** o manual en Internet de distribución preferida, www.freebsd.org/cgi/man.cgi?query=traceroute

Nos puede servir para verificar si nuestras rutas son correctas, tanto a nivel interno como en relación con nuestro proveedor de Internet.

Aunque el equipo de destino no responda a ping sabremos el recorrido a hacer para llegar hasta él. En el último tramo nos dirá que el destino no es accesible.

6.3. nslookup (sistema operativo, consola)

Este comando nos permite saber cómo se están resolviendo los nombres en nuestro equipo. En otras palabras, qué IP corresponde al nombre que indicamos y qué servidor DNS nos ha resuelto el nombre.

Ejemplos:

nslookup www.freebsd.org
nslookup www.bellera.cat

Manuales de nslookup:

- En Windows no hay comandos adicionales.
- En UNIX/Linux, **man nslookup** o manual en Internet de distribución preferida, www.freebsd.org/cgi/man.cgi?query=nslookup

En UNIX/Linux nslookup está considero como obsoleto, existiendo el comando dig que es mucho más potente:

- **man dig** o manual en Internet de distribución preferida, www.freebsd.org/cgi/man.cgi?query=dig

6.4. Telnet (sistema operativo, consola)

El cliente Telnet de nuestro sistema operativo puede servirnos como herramienta para ver si un destino tiene un servicio en funcionamiento. Ejemplos:

telnet www.freebsd.org 80
telnet www.freebsd.org 443
telnet www.freebsd.org 22
telnet www.freebsd.org 21
telnet www.freebsd.org 23

Si la pantalla se queda pensando o nos da la bienvenida al servicio entonces es que el servicio existe. Si nos da error al establecer la conexión, no existe el servicio.

Para salir:

- En Windows, cerrar ventana. La salida es un tanto aparatosa ...
- En UNIX/Linux Ctl+] y el comando quit.

De los ejemplos anteriores podemos deducir que www.freebsd.org tiene en funcionamiento los servicios HTTP (puerto 80), SSH (puerto 22) y FTP (puerto 21). Sin embargo no tiene servicios web seguros (puerto 443) ni telnet (puerto 23), a menos que los haya colocado en puertos no habituales.

Manuales de telnet:

- En Windows, teclear **telnet /?**
- En UNIX/Linux, **man telnet** o manual en Internet de distribución preferida, www.freebsd.org/cgi/man.cgi?query=telnet

6.5. netstat (sistema operativo, consola)

El comando netstat nos da información sobre las conexiones de red de nuestro ordenador y de los puertos que están a la escucha. La forma más simple de emplearlo es tecleando el comando sin parámetros:

netstat

Manuales de netstat:

- En Windows, teclear **netstat /?**
- En UNIX/Linux, **man netstat** o manual en Internet de distribución preferida, www.freebsd.org/cgi/man.cgi?query=netstat

Para saber no sólo las conexiones sino también los puertos que están a la escucha (nuestros servicios) se emplea el parámetro –a:

netstat –a

Para saber las rutas que tiene nuestro equipo se emplea el parámetro –r:

netstat –r

En Windows el comando **route print** es equivalente a **netstat –r** pero es un mal hábito emplearlo ya que **route** sirve más (especialmente en UNIX/Linux) para definir rutas "en caliente" que para verlas.

6.6. net (s.o. Windows, consola)

El comando net de Windows contiene parámetros que nos permiten examinar:

- Los recursos compartidos que tiene nuestro equipo:

net share

- Los "equipos próximos":

net view

- Las conexiones a otros equipos mediante Samba/CIFS (compartición de archivos e impresoras de Windows):

net use

Para el manual:

net help > manual_net.txt y abrir **manual_net.txt** con notepad.

Nota: En caso de que nuestro equipo UNIX/Linux tenga Samba/CIFS instalado, uno de los comandos de Samba/CIFS recibe también el nombre de net. Sin embargo, es una herramienta que tiene pocas coincidencias con el net de Windows. El comando Windows **net view** tiene el equivalente **findsmb** si además de Samba/CIFS nuestro equipo tiene PERL. Ejemplo:

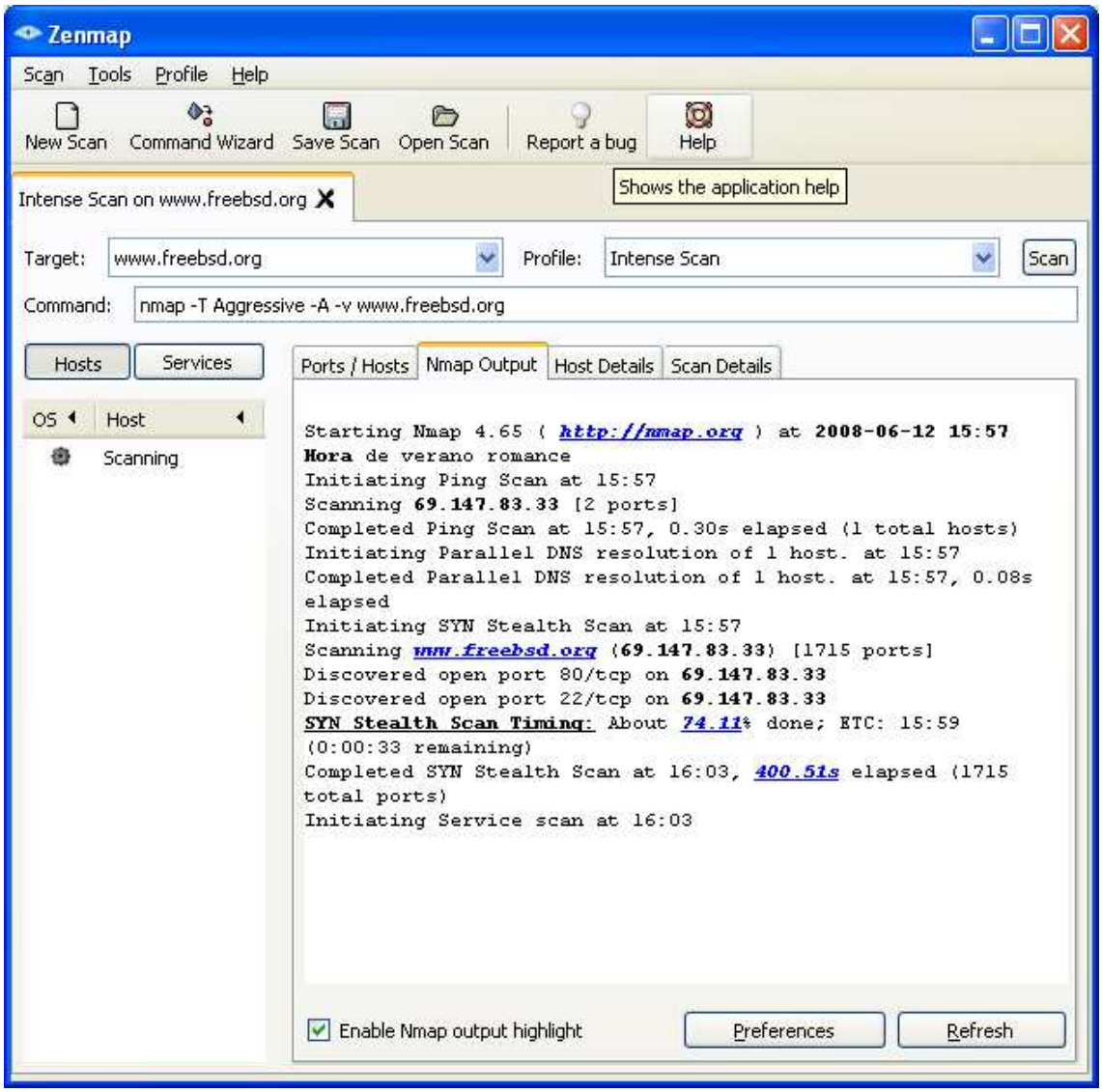
findsmb 192.168.10.0/24

6.7. nmap (aplicación multiplataforma, consola o interfase gráfica)

Es el escaneador de puertos más popular, siendo su página oficial nmap.org.

Instalamos la aplicación con las opciones estándar en nuestro sistema operativo favorito ...

Ejemplo de la interfase gráfica de nmap con escaneado de www.freebsd.org:



El resultado nos informa de que hay servicios HTTP (TCP 80) y SSH (TCP 22). Hay que tener en cuenta que el escaneado, aparte de tener muchos parámetros configurables, toma su tiempo.

Manual de nmap en castellano, nmap.org/man/es. Como curiosidad, existe un nmap online en nmap-online.com.

6.8. tcpdump (aplicación multiplataforma, consola)

La página oficial es www.tcpdump.org. Sirve para capturar todo lo que pueda ver una tarjeta de red. Es lo que en inglés se denomina *sniffer*.

La versión Windows se encuentra en www.winpcap.org/windump/install y precisa que winpcap haya sido instalado en el ordenador. En nuestro caso, como acabamos de instalar winpcap-nmap ya tenemos winpcap en nuestro ordenador.

Descargado pues windump.exe sólo tenemos que ejecutarlo. Si queremos que siempre esté disponible cuando vayamos a la consola de Windows lo copiaremos a c:\windows.

Manual de windump (tcpdump), www.winpcap.org/windump/docs/manual.htm.

6.9. Netstumbler (aplicación Windows, gráfica)

Permite escanear y diagnosticar redes wireless. Se puede descargar desde www.netstumbler.com/downloads.

6.10.ipconfig (s.o. Windows, consola)

El comando ipconfig en la consola de Windows tiene diferentes utilidades. Para su manual, **ipconfig /?**

Ejemplos de utilización:

- Para saber qué configuración de red tenemos: **ipconfig /all**
- Para saber la caché de nombres en el equipo (direcciones ya consultadas en un servidor DNS): **ipconfig /displaydns**

6.11.ifconfig (UNIX/Linux, consola)

El comando ifconfig de UNIX/Linux sirve para configurar interfases de red “en caliente” y para ver su estado. Para su manual, **man ifconfig** o manual en www.freebsd.org/cgi/man.cgi?query=ifconfig

Bastará con invocar el comando sin ningún parámetro para ver nuestras interfaces de red:

ifconfig

7. Cortafuegos. ¿Qué son? ¿Para qué sirven? ¿Cuáles hay?

es.wikipedia.org/wiki/Cortafuegos_%28inform%C3%A1tica%29

Es un equipo (hardware y software) o una aplicación (en nuestro ordenador o en un servidor) destinado/a a controlar las comunicaciones con la red.

Un cortafuegos puede operar en distintos niveles del modelo OSI, según sus características:

- Nivel 2, de enlace de datos. Filtrado por dirección física (MAC).
- Nivel 3, de red. Filtrado por protocolo de red (por direcciones IP).
- Niveles 4 y 5, de transporte y sesión. Filtrado por protocolo de transporte y por puertos.
- Nivel 7, de aplicación. Caso de los servidores proxy.

Vamos a comentar algunos de los cortafuegos más conocidos.

7.1. Cortafuegos de Windows (aplicación)

en.wikipedia.org/wiki/Windows_firewall

Desde Windows XP SP2 (Service Pack 2), este sistema operativo incorpora un cortafuegos capaz de bloquear comunicaciones no autorizadas.

El cortafuegos tiene una lista de excepciones, donde figuran las aplicaciones permitidas o puertos específicos.

Dentro de cada aplicación o puerto puede configurarse el ámbito desde el que se puede acceder a la máquina: desde cualquier dirección IP (esto incluye Internet), desde la red local (nuestra subred) o desde una lista personalizada (uno o varios equipos, una o varias subredes).

Se puede acceder al cortafuegos de Windows desde el [Centro de Seguridad] o yendo a [Entorno de Red] [botón derecho] [Propiedades] [Cambia la configuración del cortafuegos de Windows].

Aunque ha sido muy criticado, lo encuentro cómodo, bastante silencioso y sin demasiados problemas de compatibilidades con aplicaciones. En este último aspecto cabe decir que soluciones como OpenVPN para Windows, openvpn.se, dicen no ser compatibles con cortafuegos de “terceros”.

Es una buena solución a nivel doméstico si hemos tenido la precaución de no emplear un módem USB para nuestra conexión ADSL a Internet y trabajamos con un router multipuesto que nos haga de “parapeto”.

7.2. Cortafuegos de Linux (sistema operativo y aplicaciones)

El sistema operativo Linux lleva en su núcleo (kernel) la posibilidad de interceptar y manipular paquetes de red.

es.wikipedia.org/wiki/Netfilter/iptables

Las funciones de cortafuegos se configuran mediante un juego de instrucciones del sistema operativo llamado netfilter.

Para facilitar la configuración de cortafuegos empleando netfilter existe un buen número de aplicaciones. Cada distribución opta por una o varias de ellas. Quizás los más populares sean:

- shorewall.net.
- www.fwbuilder.org

Suele ser frecuente confundir netfilter con iptables. iptables es sólo una parte de netfilter.

Como veremos más adelante, existen también distribuciones Linux especializadas en hacer de cortafuegos, empleando diversidad de herramientas.

7.3. Cortafuegos de UNIX libres BSD (sistema operativo y aplicaciones)

Los sistemas BSD (UNIX libres) llevan también en su kernel la posibilidad de interceptar y manipular paquetes de red.

Por razones de prestaciones e históricas, los BSD tienen tres sistemas distintos de cortafuegos, los cuales pueden operar de forma independiente y simultánea. Por supuesto en caso de operar con más de un cortafuegos habrá que trabajar con reglas coherentes entre sí.

Los cortafuegos disponibles, por ejemplo, en FreeBSD son:

- IPF (IP Filter), cortafuegos existente en múltiples distribuciones de UNIX.
- IPFW (FreeBSD IP FireWall), cortafuegos originario del propio FreeBSD.
- PF (OpenBSD Packet Filter), cortafuegos originario de OpenBSD.

Al igual que ocurre con netfilter de Linux existen aplicaciones (y distribuciones BSD especializadas) para facilitar la configuración de estos cortafuegos.

7.4. Un equipo cortafuegos de ejemplo, ZyXEL ZyWALL

La mayoría de routers ADSL del mercado incorporan funciones de cortafuegos. Es más que recomendable hacerse con el manual del fabricante de nuestro router ADSL y activar/ajustar sus funciones cortafuegos.

Aparte de esto (o si no tenemos control sobre nuestro router) existen en el mercado equipos de bajo coste (y pequeño tamaño) que nos pueden hacer de cortafuegos.

Uno de mis preferidos es la gama ZyWALL de ZyXEL. En la web de www.34t.com (un proveedor de estos equipos) hay documentos interesantes, www.34t.com/box-docs.asp?area=76&suba=06&doc=544.

Los ZyWALL pueden configurarse vía interface web y vía interface Telnet.

7.5. Distribuciones cortafuegos

Tanto en Linux como en BSD existen distribuciones orientadas a operar como cortafuegos. Las más conocidas son:

- SmoothWall. (www.smoothwall.org). Basada en Linux.
- IPCop. (es.wikipedia.org/wiki/IPCop, www.ipcop.org). Basada en Linux y en sus inicios en SmoothWall.
- m0n0wall. (m0n0.ch/wall/). Basada en FreeBSD.
- pfSense. (www.pfsense.org). Basada en FreeBSD y en sus inicios en m0n0wall.

Las distribuciones-cortafuegos persiguen varios objetivos:

- Interface amigable, normalmente vía web.
- Pocos recursos de hardware. Por ejemplo, ordenadores monotarjeta con las interfaces de red integradas y discos duros de estado sólido (tarjetas Compact Flash y otros).
- Integrar distintas aplicaciones de gestión de redes, tales como servidores proxy (squid), detectores de intrusos (snort), monitorización y análisis de redes.

Autor: Josep Pujadas i Jubany

7.6. Comparativa de cortafuegos

En en.wikipedia.org/wiki/Comparison_of_firewalls hay una comparativa de cortafuegos, aunque algo vieja. ¿Cuál es mejor? No lo dicen ...

En www.matousec.com/projects/firewall-challenge/results.php están expuestos los resultados de un banco de pruebas de aplicaciones cortafuegos para Windows.

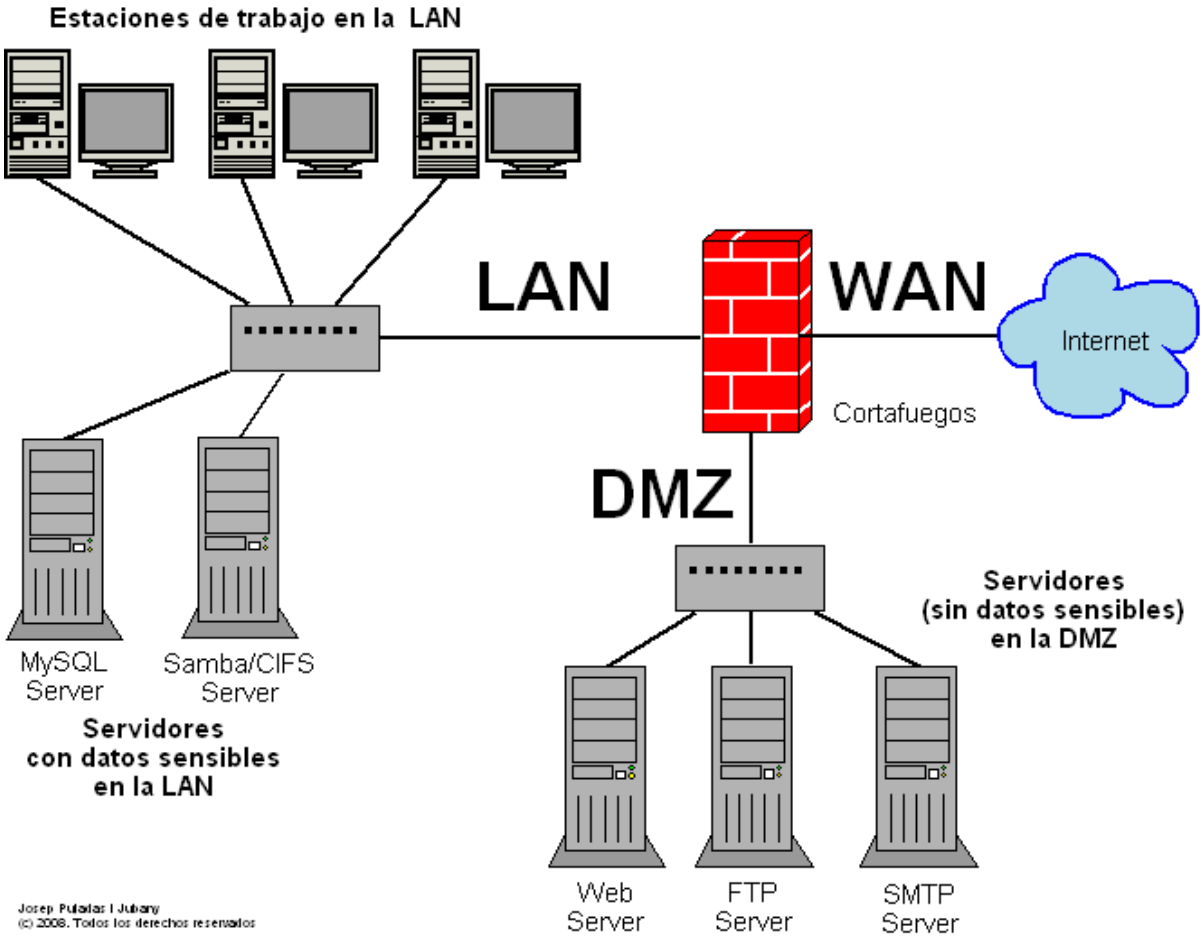
“Cada maestrillo tiene su librillo”. Hace tiempo que trabajo con FreeBSD en servidores. Dicen que la gestión de IP es mejor con sistemas BSD ... Sé de personas que han pasado de IPCop a pfSense (basado en FreeBSD) por este motivo. Pero seguro que también habrá quien haya hecho el camino inverso ...

Autor: Josep Pujadas i Jubany

8. Cómo organizar la red o redes de mi Centro (LAN, WAN, DMZ, wireless)

8.1. Terminología

- LAN (Local Area Network), red de área local. Nuestra red local. Pueden ser una o varias, es.wikipedia.org/wiki/Lan.
- WAN (Wide Area Network), red de área amplia. Más allá de nuestra LAN. Normalmente identificamos la WAN como Internet, pero puede ser cualquier red más allá de la nuestra, es.wikipedia.org/wiki/Wan.
- DMZ (DeMilitarized Zone), zona desmilitarizada. Es una red accesible desde LAN y WAN. Puede acceder a WAN pero no a LAN. En consecuencia, cualquier ordenador en la WAN que acceda a la DMZ está en un callejón sin salida y no puede llegar a la LAN, es.wikipedia.org/wiki/DMZ. Es necesario un cortafuegos para poder tener una DMZ.
- WLAN (Wireless LAN), red inalámbrica. Suele emplearse para extender una LAN a zonas difíciles de cablear y para dar autonomía a equipos portátiles/móviles. Al no existir cableado presenta problemas de seguridad importantes, a tener en cuenta.



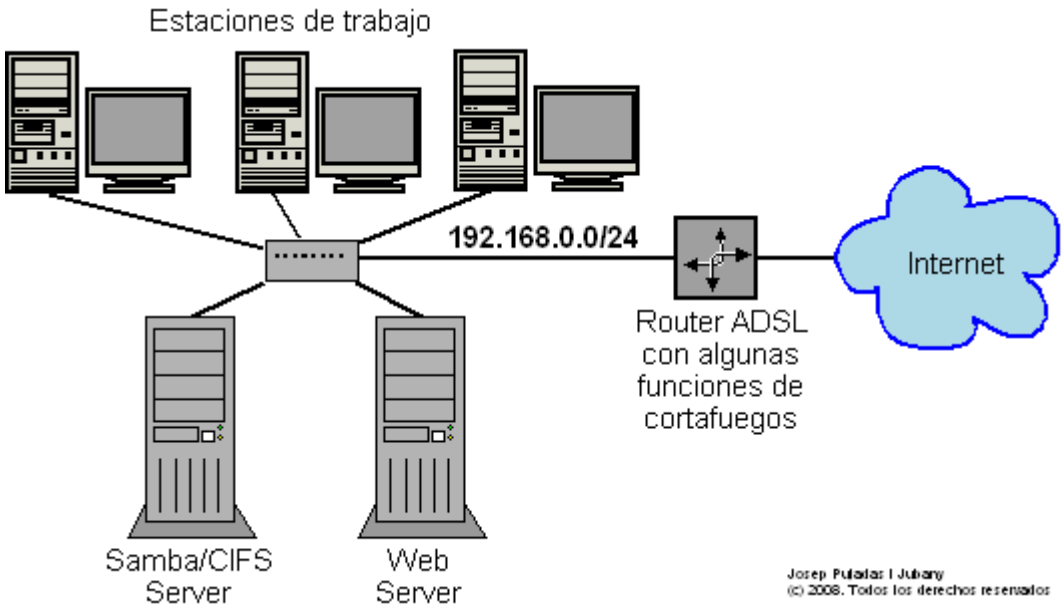
8.2. Una sola red física y lógica

Esta es una configuración habitual en muchos Centros. Las únicas protecciones existentes son:

- Las funciones de cortafuegos que pueda tener el router ADSL.
- La (posible) aplicación de cortafuegos de cada equipo.

Los problemas más importantes en esta configuración son:

- El administrador de red no tiene un control centralizado
- Los usuarios pueden hacer P2P, a no ser que se hayan aprovechado las (limitadas) posibilidades del cortafuegos del router ADSL.
- Todos los equipos se ven entre sí.
- Es fácil que, por descuido, los usuarios dejen ver carpetas de sus equipos desde otros equipos.



8.3. Dos (o más) redes lógicas en una misma red física

En un solo cableado podemos tener más de una red lógica. Esto se puede hacer de dos formas distintas:

- Mediante subredes, en base a direcciones IP y sus máscaras.
- Mediante redes virtuales (VLAN), es.wikipedia.org/wiki/VLAN.

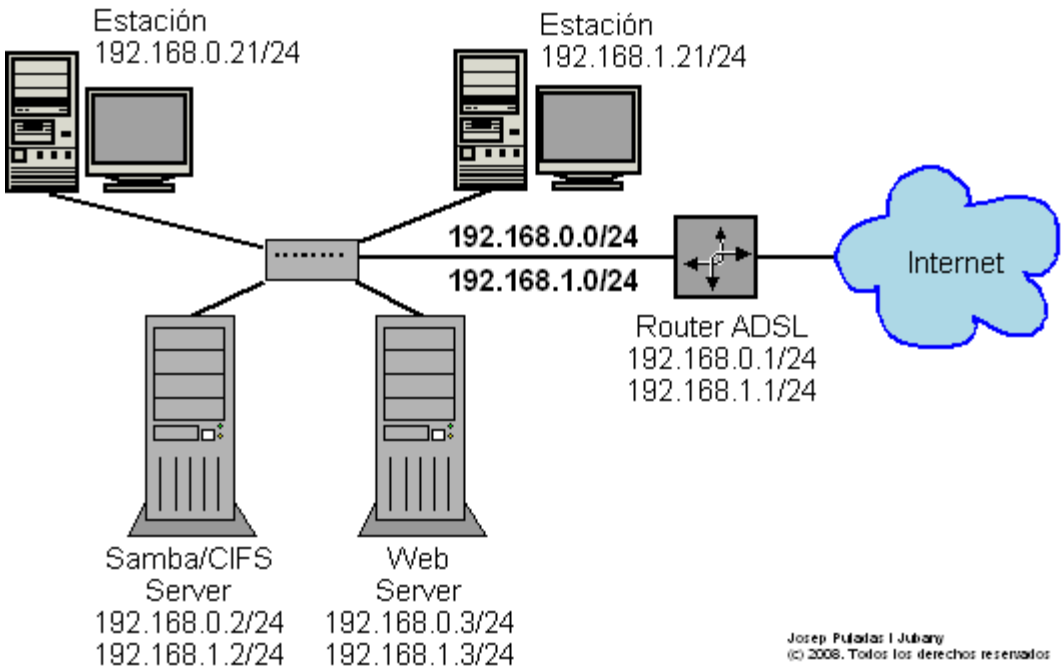
La segunda solución es, sobre el papel, la mejor. Sin embargo implica tener:

- Switches administrables que soporten VLAN.
- Tarjetas de red que soporten VLAN.
- Drivers para las tarjetas de red que soporten VLAN.

Desgraciadamente esto no es posible en la mayoría de entornos en los que nos movemos, de redes con equipos muy diversos y de bajo coste.

En cuanto a tener varias subredes la solución consiste en que haya equipos que tengan:

- Una única dirección IP (como suele ser habitual).
- Una dirección IP en cada subred en que queramos que sea visible. A estas direcciones IP adicionales se les suele denominar “alias”.



Resulta bastante evidente que este método no nos aportará un gran incremento de seguridad, pero ya es algo. Sobre todo si hacemos que los usuarios no puedan cambiar la dirección IP o “confiamos” en su “ignorancia”.

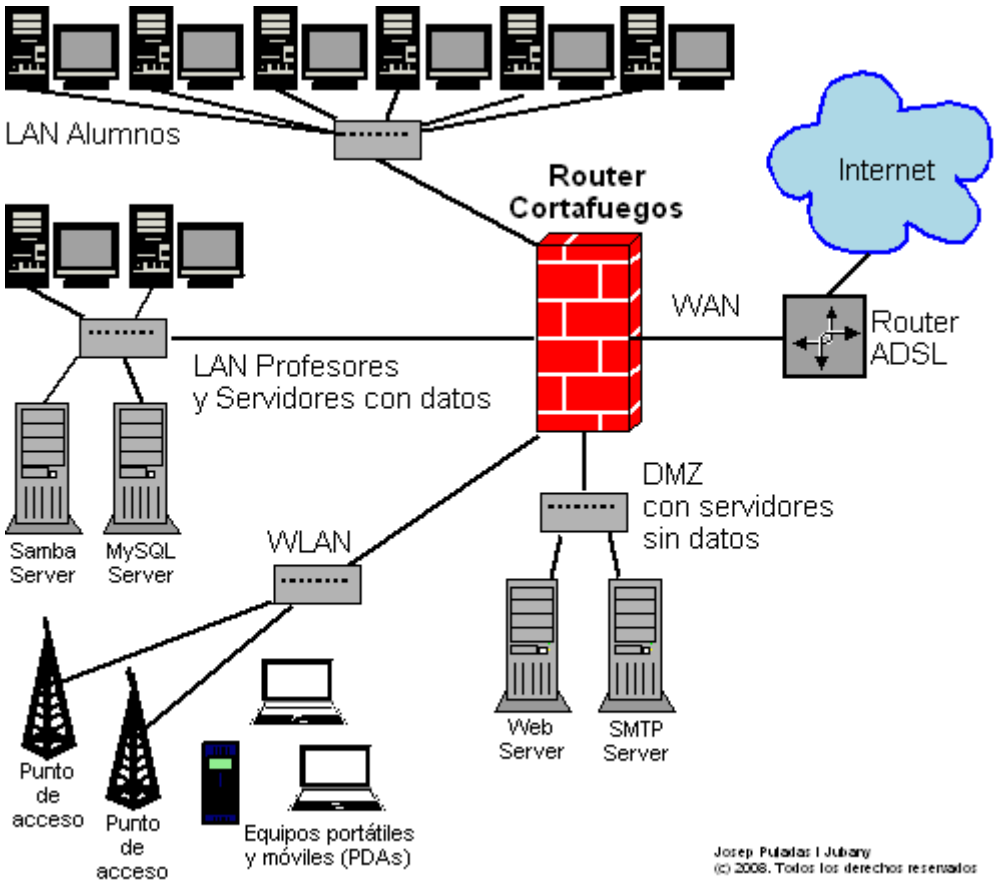
8.4. Varias redes físicas (con una red lógica en cada una)

Aunque nos obligue a replantear algunos tramos de nuestro cableado (switches incluidos), la opción más clara es separar físicamente nuestras redes.

Evidentemente tendremos que partir de un cableado mínimamente estructurado (es.wikipedia.org/wiki/Cableado_estructurado) con armarios que nos centralicen las comunicaciones, cerrados con llave.

Puede que tengamos que pasar algunos cables adicionales, pero vale la pena separar físicamente las secciones que tengamos en el Centro (servidores, profesorado, alumnos, administración, wireless, ...)

Una vez tengamos nuestra red dividida por secciones pasaremos a sustituir el switch que las une por un cortafuegos. El esquema ideal sería el que figura a continuación:



Insisto en que esto es la solución ideal, pero tendremos que adecuarla a nuestra realidad.

También hay que considerar que la DMZ ideal es difícil de implementar, ya que los servidores que están en ella tienen que acceder muchas veces a servidores con datos que, por razones de seguridad, están en la LAN. Por ejemplo, un servidor web con páginas dinámicas (PHP u otro) suele llevar asociado un servidor de datos (MySQL u otro). En este caso si un atacante llegase a hacerse con el control del servidor web (en la DMZ) podría llegar a atacar el servidor de datos (en la LAN) a través de alguna vulnerabilidad en el servicio de datos (MySQL u otro).

Otro problema que puede aparecer es que deseemos que los datos estén accesibles vía Internet. Por ejemplo, queremos que los usuarios puedan subir y bajar archivos del servidor Samba desde su casa. En este caso tendremos que montar un servicio de transferencia de archivos (mejor que sea SFTP que FTP) para el servidor que tenemos en la LAN.

También podríamos discutir qué son datos sensibles y qué no son datos sensibles. Se suele colocar el servidor de correo (SMTP) en la DMZ. Pero esto incluye nombres de usuario y contraseñas ... Y quizás le hayamos dado también a los usuarios (en este servidor) un correo-web donde puede almacenar no solo sus correos sino también archivos.

La conclusión es que la seguridad al cien por cien no existe, pero tenemos que pensar en cuál es la estructura más segura que podemos permitirnos.

Con una estructura como la propuesta (o que tienda a la misma) podremos:

- Acotar qué se puede hacer desde cada red hacia las otras redes.
- Acotar qué se puede hacer desde cada red hacia la WAN (Internet).
- Acotar qué se puede hacer desde la WAN (Internet) hacia las LAN y la DMZ, en caso de que el Centro tenga servicios en Internet.
- Auditar qué está sucediendo con nuestras conexiones de red.
- Si lo deseamos, podemos equipar a nuestro cortafuegos con aplicaciones de filtrado de contenidos y de detección de intrusos.

El aumento de seguridad y “saneamiento” de nuestras redes supondrán una mejora en el servicio a los usuarios. Por ejemplo, tendremos un mayor ancho de banda en Internet al acotar o incluso prohibir las actividades ilícitas.

9. Instalación y configuración del cortafuegos pfSense

La documentación de este apartado se encuentra disponible en:

www.bellera.cat/josep/pfsense/indice.html

10. Anexo

En www.bellera.cat/descarrega está disponible el documento (dos formatos posibles):

- bellera_cs.pps
- bellera_cs.pdf

donde puede se explica cómo se emplean las TIC en www.bellera.cat, centro del que soy coordinador de TIC.

Gracias por vuestra atención,

Josep Pujadas i Jubany

11. Agradecimientos

A mi familia, por su continuada paciencia.

A Jesús Martín, por los consejos y correcciones del documento.