FIREWALLS

1 OBJETIVO

En el taller de la clase anterior instalamos un servicio Proxy para dejar una red local utilizando una conexión compartida a Internet. En esta clase vamos a tratar la temática inherente a las medidas de seguridad que tenemos que implementar para repeler los ataques que puede sufrir una red, tanto desde la misma red local como desde Internet. Para poder comprender esto ya habíamos incluido en la clase anterior el concepto de puerto.

2 PUERTOS

Como sabemos estos puertos a los que nos referíamos en el párrafo anterior son las puertas o canales por donde el S.O. atiende a los distintos servicios de Red. Esto es necesario ya que sobre una sola dirección IP que un equipo posea se pueden utilizar diferentes servicios. Un puerto es un número de 16 bits, por lo tanto es posible el uso de hasta 65536 puertos distintos.

3 SEGURIDAD INFORMÁTICA

Las aplicaciones utilizan los puertos para recibir y transmitir mensajes por lo tanto se necesita que los sistemas operativos tengan abiertos algunos puertos en determinados momentos. Esto implica que cualquier computadora conectada a una red pública es potencialmente vulnerable a intrusiones o ataques externos. Este riesgo es la base de lo que se denomina seguridad informática, tema que requiere de nuestra atención para evitar inconvenientes en el funcionamiento de la red y los equipos.

La forma de minimizar las intrusiones es mediante el uso de Firewalls, software dedicado a proteger, restringir y filtrar el tráfico de datos desde y hacia las redes interconectadas.

Normalmente al Firewall se lo define como un sistema que provee de seguridad a una red, bloqueando o permitiendo conexiones o el envío y recepción de datos entre una red Local e Internet, mediante la aplicación de reglas.

Los firewall se dividen en dos categorías basados en redes y los personales, los primeros son construidos en una combinación de hardware y de software y están diseñados para proteger a grupos de servidores o simplemente a grupos de estaciones de trabajos. Los personales son pequeños Firewalls pensados para la protección de computadoras de usuarios particulares.

Las reglas a las que nos referimos con anterioridad definen básicamente como se va a realizar una comunicación y si la misma será permitida o denegada. Para llevar a cabo esta tarea, el Firewall necesita determinada información, por lo tanto y para adquirir esta información se apoya en el principio de funcionamiento de un Proxy, entonces se puede decir que un firewall interceptará todos paquetes (salientes y entrantes), los abrirá para conocer la dirección IP origen y destino (para llevar un control) como también para tomar nota de otros datos tales como los números de puerto que utilizan, los protocolos y las aplicaciones de red.

Con estos datos obtenidos podemos avanzar sobre algunas técnicas que se utilizaran para aplicar seguridad.

- **Filtrado de paquetes:** en este caso inspecciona todos paquetes entrantes y salientes en busca de comandos ilegales en los protocolos de las aplicaciones.
- **Aplicaciones o Aplicaciones de Gateway:** esta técnica posiblemente sea la mas sencilla de configurar y se limita a permitir o denegar el uso de algún servicio como FTP o WWW a ciertas direcciones IP, nombres de host o usuarios (si se tiene una base de datos).

Esta última técnica se encuentra en firewalls personales y su inconveniente es que a veces no figuran todos los servicios que deseamos permitir o denegar, la solución es sencilla siempre que el producto permita el agregado de nuevos servicios (como en el caso del firewall incorporado en Windows XP), en este caso particular se tendrán que completar los datos correspondientes a los números de puerto que utiliza la aplicación, la IP donde atiende y la descripción del servicio.

Si tuviésemos un producto mas elaborado posiblemente necesitaríamos conocer los números de puertos y también cuales son los protocolos de transporte que utilizan para poder completar los datos. A continuación presentamos una lista de los más utilizados.

Puerto	Protocolo
20	descarga de datos en FTP
21	petición de FTP
23	Telnet
25	SMTP (Protocolo de transferencia de correo simple)
53	búsqueda entre servidores DNS (TCP)
53	búsqueda cliente a servidor DNS (UDP)
79	Finger (servicio de TCP/IP que muestra información de usuario)
80	HTTP (TCP)
110	POP3
113	auth Servicio de autenticación Ident
119	NNTP (Protocolo de transferencia de noticias por red)
143	IMAP (Protocolo de acceso de mensajes Internet)
194	IRC (Chat de relé de Internet)
389	LDAP
443	HTTPS (HTTP seguro)

Una posibilidad que tienen los firewall es la de poder trabajar con los puertos en forma discrecional (o sea ocultando los mismos), para lo cual debemos definir previamente los distintos estados que un puerto puede tener:

- **Puerto Abierto:** se llama así al puerto que se encuentra a la espera de comunicaciones (activo) y atendiendo solicitudes o requerimientos.
- **Puerto Cerrado:** se lo llama al puerto que no tiene un servicio disponible, pero que puede contestar a ciertos requerimientos, por ejemplo una consulta sobre su estado.
- **Puerto bloqueado**: es un puerto cerrado, y que no contesta a requerimientos, entonces decimos que es invisible.

Los puertos abiertos son utilizados por quien desea. A través de ellos se pueden obtener datos como: nombres de usuario, nombre de máquina, recursos compartidos, servicios, etc.

Estas acciones de intento de búsqueda de datos se llevan a cabo con herramientas de diagnostico tan inocentes como el comando Ping (que puede usarse para verificar que un host este activo) y posteriormente tratar de accederlo con alguna aplicación de TCP/IP.

También existen productos avanzados, para diagnósticos en redes conocidos como ***sniffer*** que son dispositivos o software que monitorea el tráfico que circula en una red, también están los ***scanners*** que realizan consultas sobre el estado de puertos y recursos compartidos en un host específico o sobre un rango de direcciones.

Algo muy importante también que brindan los firewalls son los ***Logs*** (registros), estos son archivos de texto donde quedan registradas todas las actividades realizadas, ya sea entrantes o salientes. Los datos aportados incluyen datos como: direcciones IP, puertos, protocolos y horario, tanto en datos entrantes como salientes. Por ejemplo un registro podría informarnos sobre las actividades de scanners que están intentando obtener información acerca de nuestra red, proveyéndonos de fecha, hora, dirección IP de nuestro atacante.

Debido a que estas actividades se han transformado en algo normal en el ámbito de las redes públicas, es que se debe tener cuidado y prevenirse de estas. Un firewall tiene la capacidad de bloquear los puertos cerrados para evitar que contesten a solicitudes desconocidas.

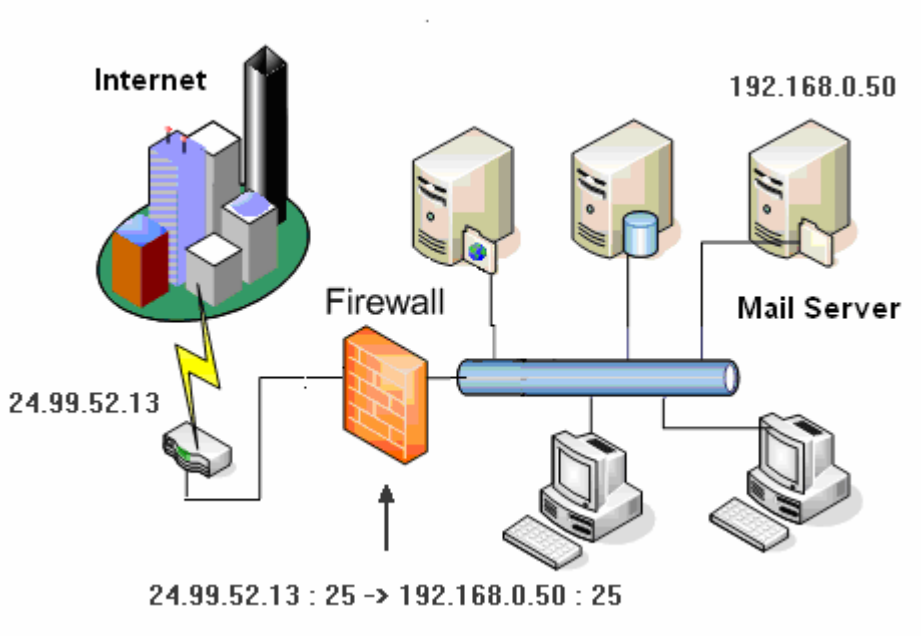
4 PORT FORWARDING

Si planteamos la necesidad de que dentro de una red local exista alguna computadora que se encuentre detrás de un firewall y que a su vez preste un servicio determinado (o sea se comporte como un servidor para la red pública), nos encontraríamos con la dificultad que los clientes de Internet no tendrían acceso a la misma ya que el Firewall lo impediría. Para esto es que se utiliza una técnica configuración (no siempre disponible) denominada ***Port Forwarding*** o Reenvío de Puertos.

Esta consiste en que cuando los clientes externos realizan un requerimiento, el Firewall toma esta solicitud y la reenvía a la computadora que tiene instalado el servicio. Cuando la maquina servidor le responde al solicitante, el firewall se encargará de reenviar la información a la computadora ex-

terna que la haya solicitado. Básicamente lo que está haciendo el Firewall es tomar una solicitud de un cliente en Internet y redirigirlo a la una maquina servidor que presta servicio en una red privada valiéndose del conocimiento de la direcciones IP y puerto de donde atiende cada servicio, de ahí al nombre dado a este procedimiento Port Forwarding.

En la siguiente figura podemos ver el ejemplo de Port Forwarding. En el mismo vemos que un paquete es recibido por el Firewall en su dirección IP pública (24.99.52.13) a través del puerto 25. Como el firewall posee una regla de reenvío declarada, en la cual todos los paquetes recibidos en la IP pública a través del puerto 25 son reenviados hacia la Local a la computadora que tiene la IP privada 192.168.0.50 a su puerto 25. De esta forma la información llegará desde la red pública al Mail Server, tal como si este último fuera visible desde Internet.



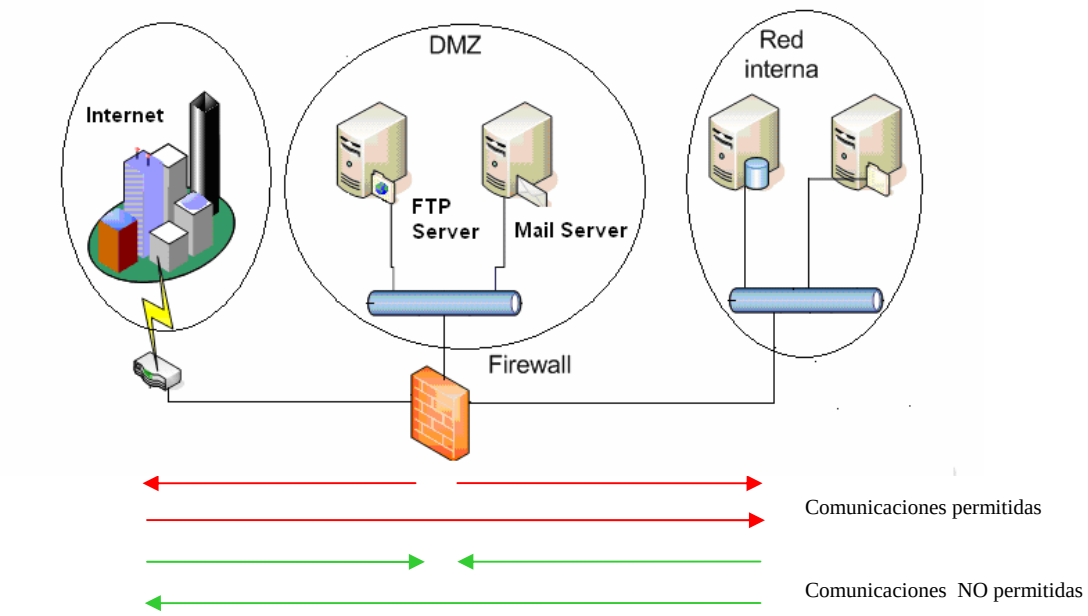
5 ZONAS DMZ (DESMILITARIZADAS)

DMZ significa **Dem**ilitarized **Z**one – Zona Desmilitarizada, la misma es una boca implementada algunos modelos de firewall que proveen una zona intermedia a la cual se la puede acceder tanto desde la red externa como a la interna, pero las máquinas ubicadas dentro de esta no les es permitido acceder a estas redes, tal como podemos ver en la siguiente figura.

Dependiendo de las necesidades de cada red, puede darse el caso de 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 se deben aceptar cualquier tipo de conexión a ellos. En esta situación se sitúa a ese servidor en un lugar aparte de la red, al que se denomina zona DMZ o zona desmilitarizada. En la zona desmilitarizada se pueden poner tantos servidores como se

necesiten. Con esta arquitectura se permite que el servidor sea accesible desde Internet y en el supuesto caso de que fuera atacado y se gana acceso a él, la red local seguiría estando protegida por un segundo firewall.



5.1 COYOTE LINUX

Coyote, es una distribución gratuita basada en Linux de un Firewall basado en software que permite conectar una red privada con una publica, o sea permitir la conexión de una red Local a Internet a través de una única computadora y que además posee un muy poderoso y ampliamente configurable Firewall. Desde la URL www.coyotelinux.com podemos descargar el asistente (llamado ***Windows disk creation Wizard***) que permite generar el disquete desde Windows el cual va a permitir la conexión de los equipos de forma segura y confiable.

Como se planteo anteriormente Coyote enlaza una red privada con una pública, por lo tanto se requerirá de una Placa de Red para conectarse con la red Local y de algún dispositivo para conectarse a Internet. Este puede ser un Módem telefónico (ISA o Externo) o si utilizamos Banda Ancha de una placa de Red para conectarse con el dispositivo de conexión suministrado por el proveedor del servicio. En este sentido Coyote trae una gran variedad de drivers para placas de red con tecnología PCI como ISA.

Coyote Linux es un NAT (Network Address Translation – Traductor de Direcciones de Internet) que además posee un servidor DHCP y un muy potente Firewall, configurable de la misma manera que el producto, ya sea desde la PC (de forma local) como también remotamente a través del Internet Explorer invocando a su dirección IP. Esto es una ventaja, ya que de esta forma no sería necesario contar ni con el teclado, ni con el monitor en la PC que corre el programa.

Requerimientos mínimos de hardware:

- ✓ *CPU 386SX.*
- ✓ *RAM 8Mb.*

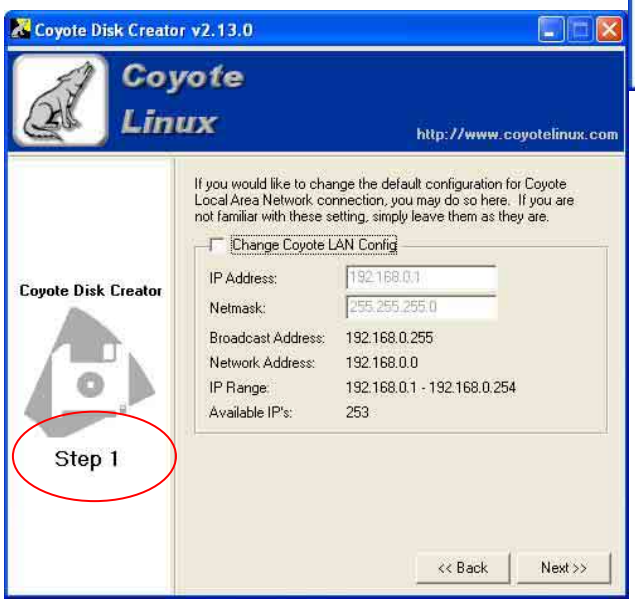
Requerimientos de hardware recomendados para una conexión de banda ancha:

- ✓ *CPU Pentium 66 MHz.*
- ✓ *RAM 12Mb.*

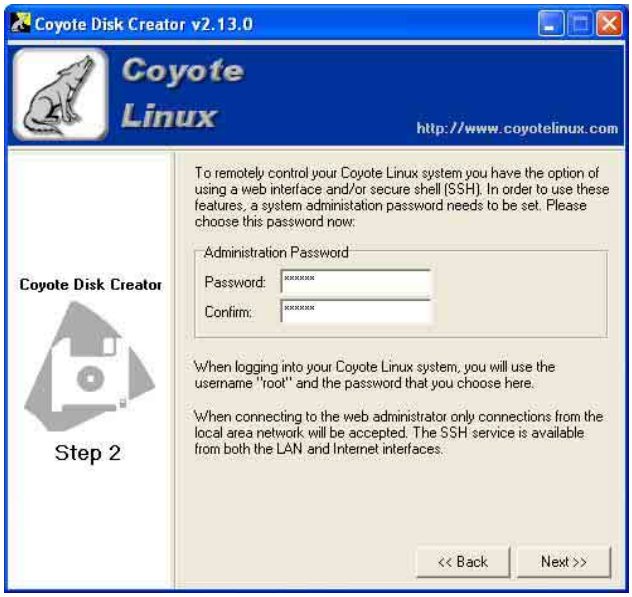
Generación del disquete

Para la generación del disquete se podrá utilizar cualquier máquina, no siendo necesario realizarlo sobre la maquina de destino. Como primer paso luego de descargado el asistente del sitio mencionado será necesario descomprimir el mismo en alguna carpeta del disco rígido, luego de realizado esto se deberá ejecutar el archivo *coyote.exe*, encargado de lanzar el asistente para la creación del disquete booteable de Coyote Linux.

La primera pantalla es una bienvenida al producto de la saldremos presionando la opción *Next*.



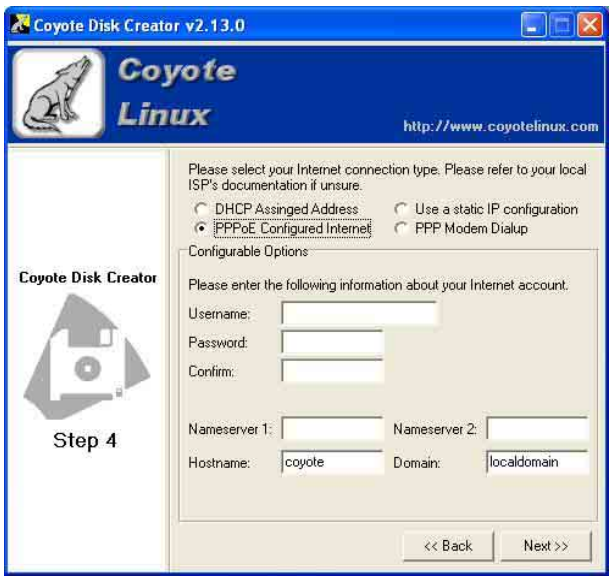
La pantalla siguiente es la correspondiente al paso1 referenciado en el borde inferior derecho, esta nos permite cambiar o definir la configuración de coyote en lo inherente a la red Local, pudiéndose establecer la dirección IP y máscara de Subred de Coyote. Si no modificamos dicha configuración quedará definida la IP interna como 192.168.0.1 y Mascara predeterminada 255.255.255.0

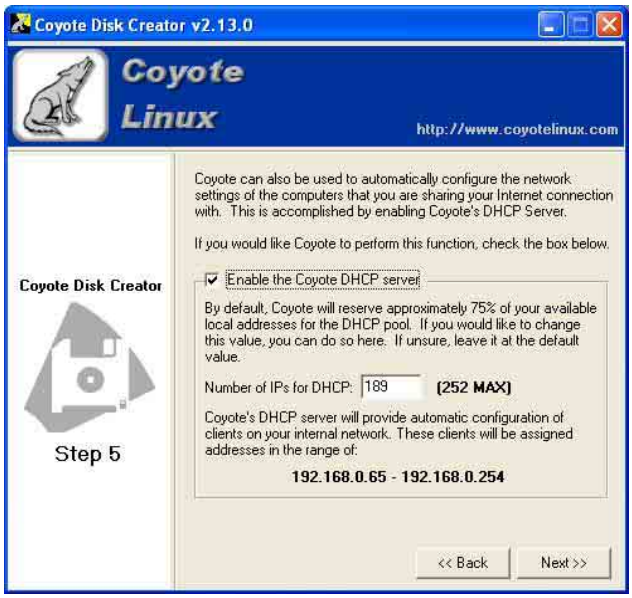


El paso que sigue es definir la contraseña de administración del programa.

En esta pantalla se permite declarar y establecer un servidor de logs, o sea una máquina que se dedique a recibir los logs que genera el software. Si existiera se debería declarar la dirección del mismo aquí.

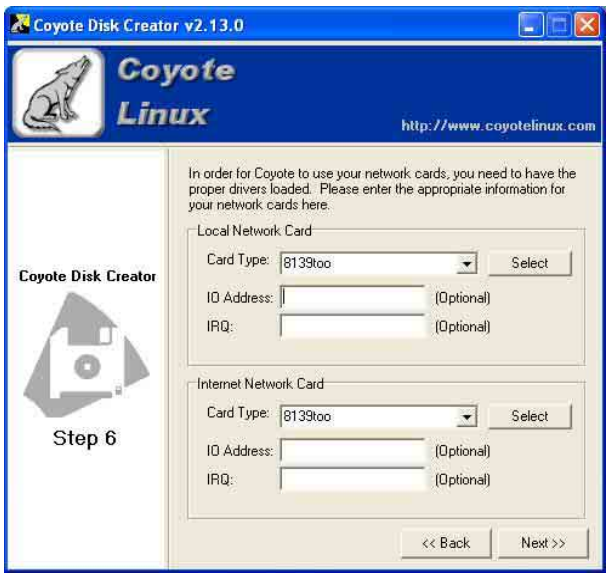
Posteriormente tendremos que configurar el tipo de conexión a Internet que disponemos. Las opciones soportadas son: Dirección IP automática (Tipo Cable Módem), PPoE (del tipo ADSL o Wireless), IP estática o PPP (Conexión por módem telefónico ISA o Externo). En el caso que corresponda deben llenarse los campos de nombre de Usuario, contraseña y direcciones de los servidores DNS. Además puede definirse el nombre del equipo que correrá Coyote y si correspondiera el dominio (el predeterminado es *coyote y localdomain*)

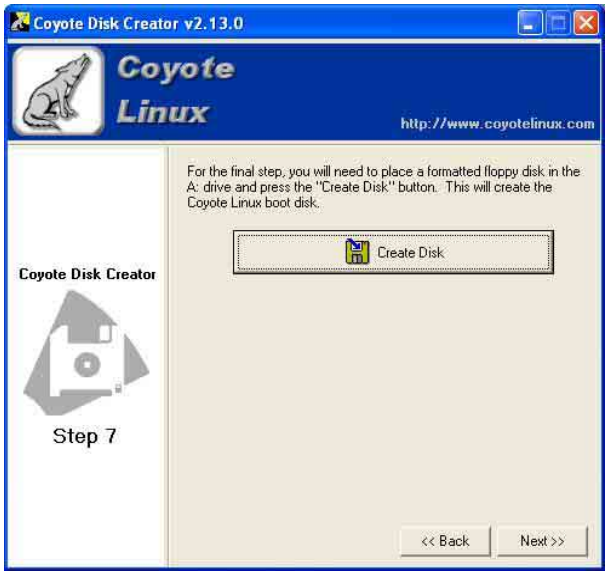




En esta nueva ventana habilitaremos si es necesario el servicio de DHCP del que dispone este producto, en el caso de habilitarlo se podrá establecer la cantidad de IP's disponibles para el servicio.

La tarea posterior es definir el tipo de placa de red que hemos de utilizar, escogiendo de una lista los drivers correspondiente a las mismas, tanto de la placa Local como de la que permitirá la conexión a Internet. Dentro de la mencionada lista existen drivers para la mayoría de las placas de uso común existentes en el mercado.





Por último bastará con presionar el botón ***Create disk*** para que nuestro disquete sea automáticamente generado.

Luego de finalizada dicha tarea solo restará iniciar el equipo que actuará de nexo con Internet con el disquete obtenido.

NOTAS

CUESTIONARIO CAPITULO 14

1.- ¿Un WEB Server conectado a Internet y brindando servicio. ¿Deberá tener algún puerto abierto? ¿Por que?

2.- ¿Es posible publicar servicios en máquinas ubicadas en la LAN para que sean accedidos desde Internet? ¿Como?

3.- ¿Cual es el objetivo de la DMZ?

4.- ¿Que herramienta utilizaría para verificar el estado de los puertos de un servidor? ¿Que datos necesitaría tener previamente?

5.- ¿Podría publicar en Internet dos servidores FTP, si mi LAN cuenta con una única dirección IP pública? ¿Como?