Trabajo de Administración de Sistemas y Servicios Telemáticos

PPTPD (IP sobre IP)

Autor: José Ignacio Laureano Collado

E.T.S.I. de Telecomunicación

PPTPD (IP sobre IP)

1. OBJETIVOS Y DESCRIPCIÓN DEL SERVICIO

Desde hace tiempo se han estado desarrollando protocolos y sistemas que permitan a usuario acceder a la red privada de su empresa remotamente y además de forma segura. Esto es sobre todo necesario en el caso de personas que viajan mucho y necesitan acceder frecuentemente a sus redes corporativas como si estuvieran físicamente conectados a ellas.

Las soluciones hasta ahora pasaban por utilizar una línea dedicada (en el caso de interconexión de LANs) o bien utilizar un módem y llamar a través de la PSTN a la red remota. Esto métodos resultan extremadamente caros, sobre todo en el caso de que sea necesario realizar llamadas internacionales.

Entonces se penso en usar la infraestructura de Internet para poder llevar a cabo esa comunicación. Esto abarataba extraordinariamente los costes ya que el coste se limitaba al precio de una llamada local. Pero surgieron varios problemas:

- La comunicación a través de Internet podría no ser suficientemente segura para ciertas transacciones.
- La mayoría de las empresas disponían de un direccionamiento interno no compatible con el que asigna la IANA.
- La mayoría de las redes privadas de empresas están situadas detrás de firewalls que filtran el trafico proveniente del exterior, por lo tanto para conectar un ordenador remoto a la empresa se debía disponer de un mecanismo que evitase este problema.

Como solución a todo esto Microsoft propuso el protocolo PPTP, que significa : Point-to-Point Tunneling Protocol. Este es el soporte sobre el cual se asienta la tecnología VPN (Virtual Private Network), la cual permite crear redes privadas virtuales a través de Internet. Por supuesto se siguen desarrollando protocolos que permitan la implementación de VPNs, pero en este trabajo solo se hablara de PPTP.

Veamos como funciona:

1. El usuario, que esta ejecutando un cliente de PPTP, llama a través de un módem o de una conexión RDSI al un numero local de un ISP.

2. Mientras tanto la red de la empresa debe estar conectada a Internet y además debe disponer de un servidor de PPTP.

3. Normalmente la red remota esta detrás de un firewall que filtra el trafico proveniente de Internet. Por lo tanto deberemos configurar el firewall para que acepte conexiones a los puertos que maneja el PPTP.

4. El usuario conecta con el servidor PPTP, lo cual le permite crear un túnel virtual entre los dos extremos que permite el al usuario remoto operar como si estuviera físicamente conectado a la LAN de su empresa.

Que beneficios nos trae usarlo:

- Permite establecer conexiones privadas, seguras y de bajo costo, con una red corporativa remota a través de Internet.

- PPTP nos permite interconectar a través de una red basada en el protocolo IP, como es Internet, a redes que pueden utilizar internamente otros protocolos, como pueden ser IPX o NetBEUI. Esto es gracias a que PPTP solo encapsula la información, crea un túnel entre dos sitios, por dentro de ese túnel puede ir lo que nosotros queramos.

- Permite la comunicación entre maquinas que ejecutan distintos sistemas operativos, tales como Windows, UNIX, etc... , lo único necesario es que soporten el protocolo PPTP.

- No necesita ningún cambio en el esquema de direccionamiento que este utilizando la empresa en ese momento. Es necesario comentar esto, ya que, en la actualidad, hay muchas empresas que utilizan internamente direccionamiento privado, que es incompatible con el direccionamiento publico de Internet que asigna la IANA. PPTP solamente crea un túnel, por eso es posible conservar el direccionamiento privado, esto no interferirá con el correcto funcionamiento de Internet. Por supuesto esto posibilita que existan varias organizaciones con las mismas direcciones internas.

- Permite usar varios métodos de encriptación, de forma que se consiga una comunicación segura. Esta encriptación se puede proveer tanto en el cliente como en el ISP como en el servidor.

- PPTP complementa a los firewalls. Lo hace en el sentido de que las firewalls regulan estrictamente el trafico que entra desde Internet, en cambio con PPTP permitimos el que existan conexiones seguras mediante la encriptación de la información.

- Permite al administrador decidir quien tiene acceso y quien no al sistema, en vez de permitir que eso lo maneje el ISP.

2. EL PAQUETE PPTPD.

La implementación de un paquete que soporte el protocolo PPTP, obviamente necesita de un servidor y un cliente.

El paquete servidor se llama PPTPD y es sobre el cual se basara la mayor parte de este trabajo, para encontrar mas información acerca de el :

http://www.moretonbay.com/vpn/pptp.html

El paquete cliente se llama pptp-linux y solamente explicare brevemente como se configura, para encontrar mas información:

http://www.pdos.lcs.mit.edu/~cananian/Projects/PPTP

3. REQUISITOS

1. Que tanto el usuario como la red remota dispongan de una conexión a Internet mediante un ISP, da igual el método que utilicen para esa conexión (modem,RDSI,etc...)

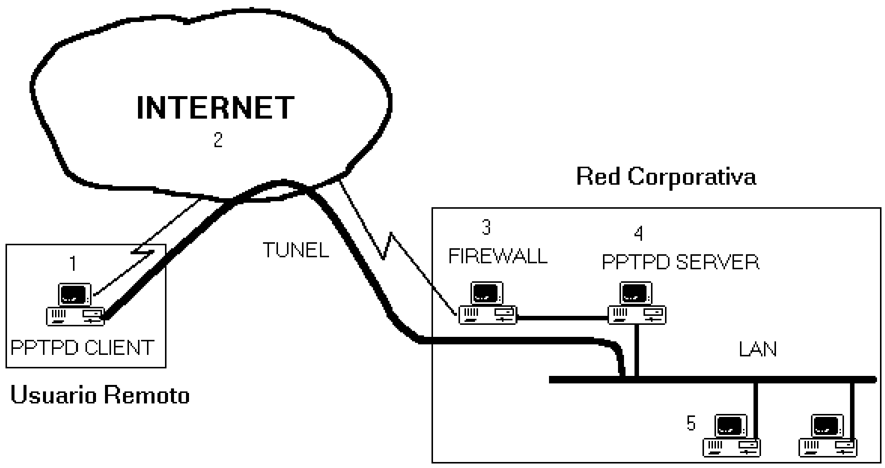
2. Una distribución moderna de linux con el kernel 2.2.x, aunque con el kernel 2.0.x debería funcionar bien.

3. El paquete PPP 2.3.8 (Con el parche MSCHAPv2/MPPE si queremos disponer de la encriptacion y autenticación mejorada de Microsoft)

4. PPTPD 1.0.0 (o la ultima versión disponible). Puede conseguirse en el sitio: http://www.moretonbay.com/vpn/download_pptp.html

5. El paquete PPTP-linux 1.0.2 en el caso del cliente de PPTP.

4. ARQUITECTURA DEL SERVICIO



Un sistema básico consta de estos elementos:

1. Una maquina remota ejecutando un cliente pptp, que disponga de una conexión con un ISP, ya sea a través de un módem, RDSI, etc...

2. La red WAN, en este caso Internet.

3. Un cortafuegos que filtra el trafico proveniente de Internet. Este cortafuegos debe ser configurado para admitir conexiones pptp. No daré muchos detalles de como se configura un cortafuegos porque podría ser extensisimo (aparte de por mi desconocimiento de los cortafuegos), solo comentare que para habilitar pptp se debe permitir:
   La conexión con el puerto 1723, que lleva a cabo las funciones de control.
   La conexión con el puerto 47 (o GRE) que maneja la transferencia de datos real.

   Además podríamos suponer que la red utiliza direccionamiento privado y que por lo tanto el cortafuegos tiene también que ejecutar NAT (Network Address Translation) para convertir las direcciones privadas en direcciones publicas validas en Internet

4. Una maquina que ejecute un servidor pptp que es la que permitirá que la maquina remota opere como si estuviese conectada a la LAN.

5. La red LAN de la empresa a la cual queremos conectar.

Como se aprecia en el diagrama el mecanismo consiste en crear un túnel a través de Internet entre el usuario remoto y la red de la empresa.

5. CONFIGURACIÓN DEL SERVIDOR (PPTPD)

1. Conseguir la ultima versión de PPTPD
2. Conseguir también una versión reciente de PPPD (Por ejemplo 2.3.8)
3. Comprobar que el pppd esta en el directorio /usr/bin/
4. Copiar el fichero pptpd-0.9.x.tgz al directorio /usr/local/src/ (o cualquier otro directorio)

   - **cd /usr/local/src/**
     - **tar xvzf pptpd-0.9.x.tgz**
     - **cd pptpd-0.9.x**
     - **./configure**
     - **make**
     - **make install**

     Nota: la instrucción make install copia los binarios a /usr/local/bin , pptpd busca sus binarios en ese directorio

5. Comprobar que pptpf y pptpctrl esta en /usr/local/bin/.
6. Asegurarnos de que somos root antes de lanzar pptpd.
7. Vamos a activar el debugging para el pptpd, parar ello hay que ir a /etc/ y abrir el fichero syslog.conf. Añadir la línea:

     - **daemon.debug /var/log/pptpd.log**

8. Matamos el syslogd actual y arrancamos uno nuevo (/usr/sbin/syslogd)
9. Asegurarnos de que tenemos PTY's y PPP en el kernel. Si no los tenemos hay que recompilar el kernel, de lo contrario, no funcionara.
10. Comprobar que existen los siguientes ficheros y son similares a:

   - /etc/ppp/options

     debug
     name servername
     auth
     require-chap
     proxyarp

   - /etc/pptpd.conf

     speed 115200
     localip 192.168.0.234-238

remoteip 192.168.1.234-238

- /etc/ppp/chap-secrets

billy servername bob *

11. Ahora ya estamos listos, ejecutamos:
    - **pptpd**

12. Para probarlo, podemos arrancar un cliente pptpd o bien en Linux o en Windows. Hacemos login usando como nombre de usuario billy y como clave bob

6. CONFIGURACIÓN DEL CLIENTE(PPTP-linux)

1. Conseguir el paquete pptp-linux (a ultima versión estable que este disponible).
2. Comprobar que tenemos instalado ppp 2.3.8.
3. Supondremos que la maquina que corre el servidor pptp al que queremos conectarnos se llama "org" y pertenece al domino "domain"
4. También supondremos, por consistencia con la configuración del servidor anteriormente descrita, que nuestro nombre de usuario (con el cual haremos login) es "billy" y la clave es "bob".
5. Buscar el fichero chap-secrets que debería estar en /etc/ppp/. Este fichero debería contener algo así:

```
#chap-secrets
#client          Server          Secret     IPadresses
domain\\billy    org             bob
```

6. Lanzamos PPTP:

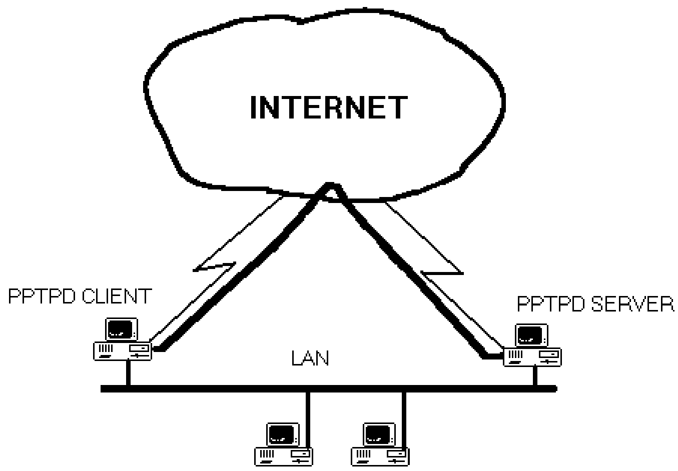
   - **pptp org debug name domain\\billy remotename org**

7. Deberíamos ver tres procesos relacionados con pptp: Un manager de llamadas, un GRE/PPP encapsulador-deencapsulador y pppd. Para parar la conexión pptp hay que matar al proceso pppd.
8. Si recibimos el error 691 (bastante frecuente), ello se debe a que hemos dado una pareja nombre/clave incorrecta.
9. Para testear que realmente esta funcionando podemos ejecutar los siguientes comandos:

   - Ejecutar 'ifconfig' y comprobar que el interfaz ppp0 existe.
   - Encontrar la dirección IP del servidor P-t-P a través del output de ifconfig.
   - Ejecutar 'netstat -i' y guardar los valores de Rx y Tx para el interfaz ppp0.

- Ejecutar un ping a la dirección del servidor pptp
- Volver a ejecutar 'netstat -i' y si los valores de Rx y Tx se han incrementado eso quiere decir que aparentemente esta funcionando

7. PRUEBAS



Una arquitectura como la presentada en la figura nos permitirá efectuar pruebas de nuestro servidor y cliente pptpd sin movernos de la habitación.

- Para ello una vez configurados el servidor y el cliente pptpd haremos lo siguiente.
- Establecemos una conexión con un ISP a través de un módem desde el PPTPD client.
- EL PPTPD server ya debería estar conectado a la red y deberá tener al menos una dirección IP publica valida de forma que podamos conectarnos a el desde el cliente.
- Necesitamos cambiar en el cliente las rutas de acceso al servidor, ya que ahora mismo esta en la misma LAN. Un método por ejemplo podría ser cambiar la métrica. Esto es, poner que el acceso a la LAN a través de la dirección IP que nos ha asignado el ISP es 1, mientras que el acceso directo tiene una métrica 2.
- Lanzamos pptpd en el servidor.
- Lanzamos pptpd en el cliente.
- Una vez hecho eso ahora todo lo que mandemos al servidor ira a través del túnel. Una forma de comprobarlo es haciendo un traceroute.

8. GESTION DIARIA

Una vez que el servicio este operativo, la únicas gestiones que tenemos que realizar son:

Asignación de login y claves a los usuarios que queremos que dispongan del servicio pptpd.

Comprobación cada cierto tiempo de que no ha intentado gente no autorizada conectarse, esto es, toda la política de seguridad que un sistema de este tipo debe llevar consigo.