

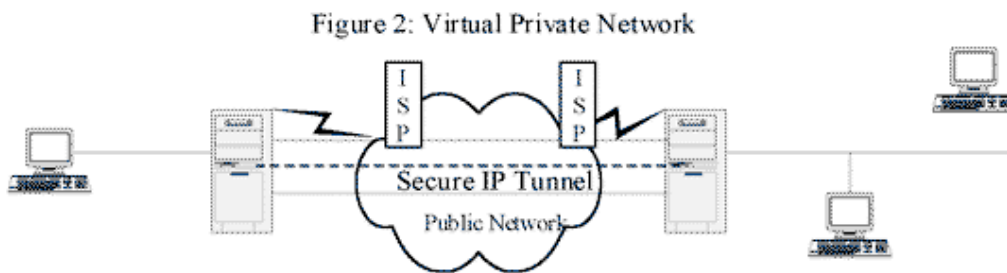
VIRTUAL PRIVATE NETWORKS

Red Privada Virtual

Que es una Red Privada Virtual

Una VPN es un grupo de dos o mas sistemas de ordenadores, generalmente conectados a una red privada (mantenida por una organización independiente), con acceso publico restringido, que se comunican "con seguridad" sobre una red publica. Es decir, es la conexión de dos o mas sistemas, utilizando una red publica, aplicando unos métodos de seguridad para garantizar la privacidad de los datos que se intercambian entre ambas, y protocolos de túneles. Las VPN's extienden la red corporativa de una empresa a las oficinas distantes, por ejemplo. En lugar de alquilar líneas dedicadas con un coste muy elevado, las VPN's utilizan los servicios mundiales de IP, incluyendo la Internet. Usando una VPN, se crea una conexión privada segura a través de una red publica como Internet. Los usuarios remotos pueden hacer una llamada local a Internet, y no usar llamadas de larga distancia.

Hay que hacer una pequeña diferencia entre una Red Privada y una Red Privada Virtual. La primera utiliza líneas alquiladas para formar toda la Red Privada. La VPN lo que hace es crear un túnel entre los dos puntos a conectar utilizando infraestructura publica.



Tipos de VPN's

Sistemas Basados en Hardware

Los sistemas basados en hardware, son routers que encriptan. Son seguros y fáciles de usar, simplemente que conectarlos y ya esta. Ofrecen un gran rendimiento, porque no malgastan ciclos de procesador haciendo funcionar un Sistema Operativo. Es hardware dedicado, muy rápido, y de fácil instalación.

Sistema Basados en Cortafuegos

Estos se implementan con software de cortafuegos (firewall). Tienen las ventajas de los mecanismos de seguridad que utilizan los cortafuegos, incluyendo el acceso restringido a la red interna. También realizan la traducción de direcciones (NAT). Estos satisfacen los requerimientos de autenticación fuerte.

Muchos de los cortafuegos comerciales, aumentan la protección, quitando al núcleo del Sistema Operativo algunos servicios peligrosos que llevan estos de serie, y les provee de medidas de seguridad adicionales, que son mucho mas útiles para los servicios de VPN.

El rendimiento en este tipo decrece, ya que no se tiene hardware especializado de encriptación.

Sistema Basados en Software

Estos sistemas son ideales para las situaciones donde los dos puntos de conexión de la VPN no están controlados por el misma organización, o cuando los diferentes cortafuegos o routers no son implementados por la misma organización. Este tipo de VPN's ofrecen el método mas flexible en cuanto a el manejo de trafico. Con este tipo, el trafico puede ser enviado a través de un túnel, en función de las direcciones o protocolos, en cambio en los VPN por hardware, todo el trafico era enrutado por el túnel. Podemos hacer un enrutamiento inteligente de una manera mucho mas fácil.

Requerimientos básicos de una Red Privada Virtual

Una Red Privada Virtual ha de proveer de los siguientes mecanismos básicos, aunque en ocasiones y situaciones puedes obviarse algunos.

- Autenticación de usuarios, verificar la identidad de los usuarios, para poder restringir el acceso a la VPN solo a los usuarios autorizados.
- Administración de direcciones, debe asignar una dirección del cliente sobre la red privada, y asegurar que las direcciones privadas se mantienen privadas.
- Encriptación de datos, los datos que viajan por la red pública, deben ser transformados para que sean ilegibles para los usuarios no autorizados.
- Administración de claves, debe mantener un mantenimiento de claves de encriptación para los clientes y los servidores.
- Soporte multiprotocolo, ha de ser capaz de manejar protocolos comunes, usando las red pública, por ejemplo IPX, IP, etc...

Como funciona, encriptación y rendimiento en una VPN

La tecnología de VPN se centra en el medio que hay entre las redes privadas y las redes públicas. El dispositivo intermediario, ya se orientado a software, orientado a hardware o la combinación de ambos, actúa como una red privada como a la que protege. Cuando un host local manda un paquete a una red remota, los datos primero pasan de la red privada por el gateway protegido, viajando a través de la red pública, y entonces los datos pasan por el gateway que esta protegiendo el host destino de la red remota. Una VPN protege los datos encriptandolos automáticamente antes de enviarlos de una red privada a otra, encapsulando los datos dentro de un paquete IP. Cuando estos llegan al destino, los datos son desencriptados. El proceso es el siguiente:

- 1- Un ordenador cliente llama a un ISP local y conecta a Internet.
- 2- Un software especial cliente reconoce un destino especificado y negocia una sesión de VPN encriptada
- 3- Los paquetes encriptados son envueltos en paquetes IP para crear el túnel y mandarlos a través de Internet.
- 4- El servidor de VPN negocia la sesión de VPN y desencripta los paquetes.
- 5- El trafico no encriptado fluye a otros servidores y recursos con normalidad.

El fuerte de los componentes en VPN es la encriptación. El objetivo es restringir el acceso a los usuarios y hosts apropiados, y asegurar que los datos transmitidos por Internet sean encriptados para que solo estos usuarios y los hosts sean capaces de ver los datos. La técnica usada es envolver las datos de carga encriptados, con cabeceras que pueden ser leídas. Esto es lo que se llama Túnel. Una vez conectado, una VPN abre un Túnel seguro, en el cual el contenido será encapsulado y encriptado y los usuarios son autenticados.

Pero por supuesto, todos estos mecanismos empleados, aumenta la seguridad en el intercambio de datos pero no añade una reducción en el rendimiento de la comunicación por las sobrecargas. Muchas VPN, ya sean basadas en hardware o en software, deberían ser capaces de procesar la encriptación en conexiones hasta al menos una velocidad de 10BaseT. En velocidades superiores, el consumo de CPU necesaria en las VPN basadas en software es tan elevada que el rendimiento decrece. En los sistemas orientados a hardware, que usas máquinas dedicadas estas velocidades aumentan. En conexiones como módems, el procesamiento en las VPN es mucho más rápido que los retardos introducidos por el ancho de banda disponible. Las pérdidas de paquetes y la latencia en conexiones a Internet de baja calidad afecta más al rendimiento más, que la carga añadida por la encriptación.

Que es Tunneling

Tunneling es una técnica que usa una infraestructura entre redes para transferir datos de una red a otra. Los datos o la carga pueden ser transferidas como tramas de otro protocolo. El protocolo de tunneling encapsula las tramas con una cabecera adicional, en vez de enviarla como la produjo en nodo original. La cabecera adicional proporciona información de routing para hacer capaz a la carga de atravesar la red intermedia. Las tramas encapsuladas son

enrutadas a través de un túnel que tiene como puntos finales los dos puntos entre la red intermedia. El túnel es un camino lógico a través del cual se encapsulan paquetes viajando entre la red intermedia. Cuando un trama encapsulada llega a su destino en la red intermedia, se desencapsula y se envía a su destino final dentro de la red. Tunneling incluye todo el proceso de encapsulado, desencapsulado y transmisión de las tramas.

Las tecnologías de Tunneling son:

- DLSW- Data Link Switching (SNA over IP)
- IPX for Novell Netware over IP
- GRE – Generic Routing Encapsulation (RFC 1701/2)
- ATMP – Ascend Tunnel Management Protocol
- Mobile IP – For mobile users
- IPsec – Internet Protocol Security Tunnel Mode
- PPTP - Point-to-Point Tunneling Protocol
- L2F – Layer 2 Forwarding
- L2TP – Layer 2 Tunneling Protocol

Que es el PPTP

El protocolo fue originalmente designado como un mecanismo de encapsulamiento, para permitir el transporte de protocolos diferentes del TCP/IP, como por ejemplo IPX sobre la red Internet. La especificación es bastante genérica, y permite una variedad de mecanismos de autenticación y algoritmos de encriptación.

El Protocolo de Túnel Punto-a-Punto (Point to Point Tunneling Protocol) es un protocolo que permite establecer conexiones con túneles PPP, a través de una red IP, creando una VPN. La compañía Microsoft, ha implementado sus propios algoritmos y protocolos con soporte PPTP, el Microsoft PPTP, y este es uno de los más ampliamente extendidos, por la popularidad de los productos Microsoft (Windows 98/ME, NT4, 2000) los cuales llevan incluidos de serie estos protocolos.

Fue desarrollado por el Forum PPTP que está constituido por las siguientes organizaciones: Ascend Communications, Microsoft Corporation, 3Com/Primary Access, ECI Telematics, and U.S. Robotics.

PPTP and VPN

Generalmente hay tres ordenadores involucrados en el uso del PPTP. Hay un cliente PPTP, un servidor de acceso a la red y un servidor de PPTP. En el caso de una LAN, el servidor de acceso a la red no es necesario, porque ya está en la misma red. La comunicación segura creada usando el protocolo PPTP conlleva tres fases, cada una de las cuales requiere la finalización correcta de las anteriores. Estas son: PPP conexión y comunicación, PPTP control de conexión, PPTP data tunneling.

PPP conexión y comunicación

Primero el cliente necesita una conexión a Internet, conectando con un Servidor de Acceso a Red (NAS Network Access Server) vía un Proveedor de Servicios de Internet (ISP). Un cliente PPTP usa el PPP para establecer esta conexión. La conexión requerida por un cliente consiste en unas credenciales de acceso (usuario, password) y un protocolo de autenticación para que el servidor de PPTP pueda autenticar al cliente. Una vez conectado el cliente puede enviar y recibir paquetes sobre Internet.

PPTP control de conexión

Cuando el cliente tiene establecida la conexión PPP con el ISP, se realiza un segundo establecimiento de llamada, sobre la conexión PPP existente. Esto crea la conexión VPN (conexión de control) a un servidor PPTP de una LAN privada a una empresa y actúa como un túnel a través de la cual fluyen los paquetes de red. Un set de ocho mensajes de control establecerán, mantendrán y finalizarán el túnel PPTP. Los mensajes son los siguientes:

- PPTP_START_SESSION_REQUEST Starts Session
- PPTP_START_SESSION_REPLY Replies to Start Session Request
- PPTP_ECHO_REQUEST Maintains Session

- PPTP_ECHO_REPLY Replies to Maintain Session Request
- PPTP_WAN_ERROR_NOTIFY Reports an error in the PPP connection
- PPTP_SET_LINK_INFO Configures PPTP Client/Server Connection
- PPTP_STOP_SESSION_REQUEST Ends Session
- PPTP_STOP_SESSION_REPLY Replies to End Session Request
- PPTP Data Tunneling

Después de establecer el túnel PPTP, los datos son transmitidos entre el cliente y el servidor PPTP. Los datos son enviados en formato de datagramas IP que contienen paquetes PPP, a los que referimos normalmente como paquetes PPP encapsulados. Los datagramas IP contienen paquetes IPX, NetBEUI, o TCP/IP y tiene el siguiente formato:

PPP Delivery Header	IP Header	GRE Header	PPP Header	IP Header	TCP Header	Data
---------------------	-----------	------------	------------	-----------	------------	------

Figure 1: IP datagram containing encrypted PPP packets as created by PPTP

La cabecera IP de entrega proporciona la información necesaria para que el datagrama atraviese la red Internet. La cabecera GRE se usa para encapsular el paquete PPP dentro de un datagrama IP. La zona ensombrecida representa los datos encriptados.

Después de que la conexión VPN esta establecida, el usuario remoto (cliente) puede realizar cualquier operación como si fuera un usuario local.

La seguridad en PPTP

Una de las características de este protocolo es la característica disponibles de seguridad. Hay tres áreas en la seguridad PPTP que lo hace mas atrayente. Son la autenticación, encriptación de datos y filtrado de paquetes PPTP.

Autenticación

La autenticación de un cliente PPTP remoto se hacen de la misma manera que la autenticación PPP usado por cualquier cliente RAS (Remote Access Service). Las cuentas de usuarios son configuradas para que solo los usuarios específicos tengan acceso a la red a través del domino de confianza. El uso de passwords seguras es uno de las mejores formas de utilización exitosa del PPTP.

Encriptación de Datos

Los datos enviados por el túnel PPTP en los dos sentidos son encriptados. La paquetes de red son encriptados en la fuente (cliente o servidor), viajan a través del túnel, y son desencriptados en el destino. Como todos los datos en una conexión PPTP fluyen dentro del túnel, los datos son invisibles al resto del mundo. La encriptación de datos dentro del túnel da un nivel adicional de seguridad.

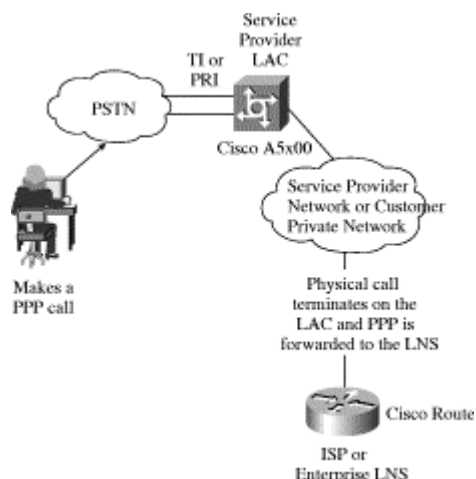
Filtrado de Paquetes PPTP

Esta opción incrementa el rendimiento y fiabilidad de la seguridad de red si esta activada en el servidor PPTP. Cuando esta activa acepta y enjuta solo los paquetes PPTP de los usuarios autorizados. Esto prevé el resto de paquetes entren el red privada y en el servidor de PPTP.

L2TP, Layer 2 Tunneling Protocol

El protocolo de túneles L2TP, ha nacido de la combinación de las características del protocolo PPTP y L2F (Layer 2 Forwarding). L2TP es un protocolo de red que facilita la creación de túneles para enviar tramas PPP. Encapsula las tramas PPP para que puedan ser enviadas sobre redes IP, X.25, Frame Relay o ATM. La carga útil de las tramas PPP, puede ser encriptada y/o comprimida. Se puede usar L2TP directamente sobre diferentes tipos de WAN, por ejemplo, Frame Relay, sin una capa de transporte IP. L2TP usa UDP y una serie de

mensajes de L2TP para los mantenimiento de túneles sobre redes IP. L2TP permite múltiples túneles entre los dos puntos finales.



L2TP esta compuesto de dos partes, el concentrador de acceso L2TP (LAC) y el servidor de red L2TP (LNS). El LAC se sitúa entre un LNS y un sistema remoto, manda paquetes a cada uno de los dos. El LNS es el par del LAC, y es un punto de terminación lógica de una sesión PPP que a la cual se le esta siendo aplicado el túnel desde el sistema remoto por el LAC. El L2TP soporta dos modos de túneles, el modo Obligatorio y el Voluntario.

L2TP usa el Protocolo de Control de Red (Network Control Protocol NCP) para asignar la IP y autentificar en PPP, llama comúnmente, PAP o CHAP. La seguridad en L2TP requiere para el transporte seguro es necesario que estén disponibles los servicios de encriptación, integridad y autentificación para todo el trafico L2TP. Este transporte seguro opera en todo el paquete L2TP y es funcionalmente independiente de PPP y del protocolo que este transporta.

Túnel Obligatorio L2TP

1. El usuario remoto inicializa una conexión PPP a un ISP
2. El ISP acepta la conexión y el enlace PPP se establece
3. El ISP solicita la autentificación parcial para saber el nombre de usuario
4. El ISP mantiene una lista de todos los usuarios admitidos, para servir el final del túnel LNS
5. El LAC inicializa el túnel L2TP al LNS
6. Si el LNS acepta la conexión, el LAC encapsulara el PPP con el L2TP, y entonces enviara a través del túnel
7. El LNS acepta estas tramas, y las procesa como si fueran tramas PPP.
8. El LNS la autentificación PPP para validar al usuario y entonces asigna una dirección IP

Túnel Voluntario L2TP

1. El usuario remoto tiene una conexión a un ISP ya establecida
2. El cliente L2TP (LAC), inicializa el túnel L2TP al LNS
3. Si el LNS acepta la conexión, LAC encapsula con PPP y L2TP, y lo manda a través del túnel
4. El LNS acepta estas tramas, y las procesa como si fueran tramas normales de entrada
5. el LNS entonces usa la autentificación PPP para validar al usuario y asignarle una IP

Que es IPSec

IPSec es un protocolo de seguridad para Internet. IPSec proporciona confidencialidad y/o integridad de los paquetes IP. Los paquetes normales de IPv4 están compuestos de una cabecera y carga, y ambas partes contienen información útil para el atacante. La cabecera contiene la dirección IP, la cual es utilizada para el routing, y puede ser aprehendida para ser usada mas tarde con técnicas de spoofing. La parte de la carga esta compuesta de la

información que se supone confidencial para una empresa o una organización. Ni que decir tiene, que esta información es la mas valiosa. IPSEC proporciona seguridad mediante dos protocolos ESP, Encapsulating Security Payload, o AH, Authentication Header.

Básicamente ESP cifra los datos y los autentica, mientras que AH sólo los autentica. La diferencia entre ESP sólo autenticando y AH es que AH autentica también la cabecera IP del paquete. AH, firma digitalmente el paquete, verificando la identidad del emisor y del receptor del paquete. La manera en que se autentican los paquetes es mediante funciones HMAC (funciones HASH con clave), mientras que la manera de proporcionar confidencialidad es cifrando los paquetes con uno de los algoritmos de cifrado definidos.

IPSec es una buena solución para mantener la confidencialidad de los datos. Ofrece una comunicación segura host a host. Tiene dos modos de funcionamiento, modo transporte y modo túnel. En el modo transporte la encriptación se realiza extremo a extremo, del host origen al host destino, por lo tanto todos los hosts han de tener IPSec. En el modo túnel el encriptado se efectúa únicamente entre los routers de acceso a los hosts implicados. Con el modo túnel la encriptación se integra de manera elegante, los mismos dispositivos que se encargan que crean los túneles se encargan de integrar el encriptamiento.

Ejemplos Prácticos

Puesta en marcha de un servidor de VPN en Linux

Para poder poner en marcha un servidor de VPN necesitamos un software capaz de soportar algún tipo de protocolo para poder crear algún tipo de túnel. Se ha usado el software llamado PoPToP, que utiliza el protocolo PPTP. Es compatible con los clientes de Windows para el uso de VPN's. Este programa hace uso del pppd, programa muy conocido en el mundo de Linux para hacer conexiones punto a punto (PPP). Con unos parches adecuados para este ultimo programa, el PoPToP es compatible con la encriptación y la autenticación de Microsoft Windows MSCHAPv2 y MPPE 40-128 bit RC4.

En el servidor Linux hay que crear los siguientes 2 archivos de configuración:

```
/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
```

- servername, será el nombre de la maquina que hará de servidor de VPN
- localip y remoteip, son el rango de direcciones IP que tendremos para la conexión simultanea de clientes VPN
- require-chap, opción para realizar la autenticación en el sistema con cifrado de datos.

```
/etc/ppp/chap-secrets
```

```
billy servername bob *
```

En el fichero chap-secrets, añadimos todos los usuarios que tendran acceso al sistema.

A continuación lo ejecutamos:

```
/usr/local/sbin/pptpd
```

El programa, el mismo, se pone en background y se queda a la escucha de conexiones en el puerto TCP 1723.

Ahora con una conexión con un cliente, por ejemplo el que lleva Windows ME, podemos conectar con es servidor y tener acceso a cualquier recurso dentro de la red interna.

Imaginemos que tenemos una red de cincuenta ordenadores en una empresa. Dicha empresa tiene dos sucursales, que corresponden a con redes similares. Dichas redes utilizan la red Windows para compartir recursos, comparación ficheros, etc. Para conectar las dos redes, y que para el usuario final pareciera toda una, podríamos utilizar los túneles. Cada sucursal podría contratar una ADSL, el cual le da acceso a Internet, y sobre Internet podríamos hacer un túnel entre las dos redes, para conseguir así que las dos redes de las sucursales parecieran una sola red.

Siguiendo los pasos anteriores, se ha instalado un servidor de VPN en una maquina con Linux, en la cual también esta instalado Samba, implementación de NetBEUI de Microsoft, pero para Unix. Desde un ordenador remoto, con una conexión a un ISP se ha establecido un túnel hasta la maquina con Linux. Hay que puntualizar que la maquina con el servidor de VPN pertenece a una pequeña red donde también hay algún ordenador con Windows 98 instalado, y esta red esta conectada a Internet con un Router ADSL 3Com 812. El Router esta configurado para que haga NAT, por lo tanto el puerto TCP 1723, esta redirigido a la maquina que tiene el servidor de VPN instalado.

Tabla de rutas antes de ejecutar la conexión VPN en el ordenador remoto:

```

=====
Interface List
0x1 ..... MS TCP Loopback interface
0x3000002 ...44 45 53 54 00 00 ..... PPP Adapter.
0x3000003 ...44 45 53 54 00 01 ..... PPP Adapter.
=====
Active Routes:
Network Destination    Netmask          Gateway          Interface        Metric
        0.0.0.0          0.0.0.0          62.36.189.146   62.36.189.146   1
        62.0.0.0          255.0.0.0          62.36.189.146   62.36.189.146   1
        62.36.189.146    255.255.255.255    127.0.0.1       127.0.0.1       1
        62.255.255.255    255.255.255.255    62.36.189.146   62.36.189.146   1
        127.0.0.0          255.0.0.0          127.0.0.1       127.0.0.1       1
        224.0.0.0          224.0.0.0          62.36.189.146   62.36.189.146   1
        255.255.255.255    255.255.255.255    62.36.189.146   62.36.189.146   1
Default Gateway:        62.36.189.146
=====
Persistent Routes:
None

```

Tabla de rutas después de ejecutar la conexión VPN en el ordenador remoto:

```

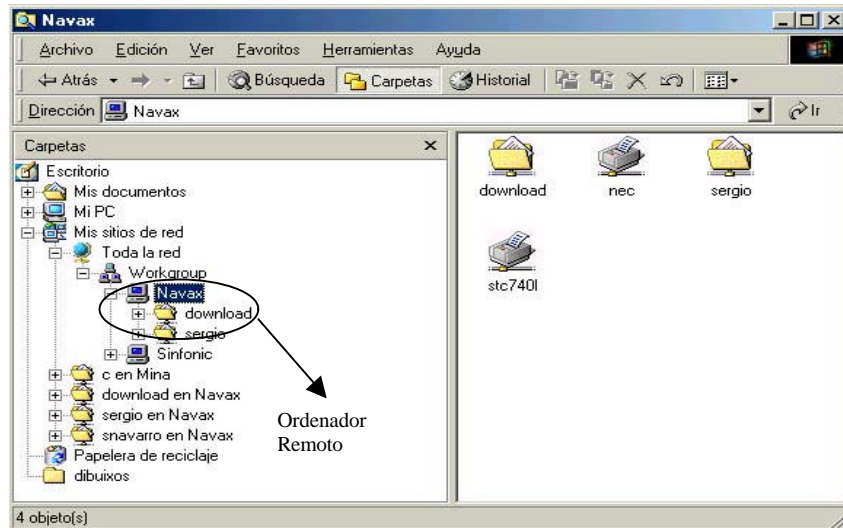
=====
Interface List
0x1 ..... MS TCP Loopback interface
0x3000002 ...44 45 53 54 00 00 ..... PPP Adapter.
0x3000003 ...44 45 53 54 00 01 ..... PPP Adapter.
=====
Active Routes:
Network Destination    Netmask          Gateway          Interface        Metric
        0.0.0.0          0.0.0.0          62.36.189.146   62.36.189.146   2
        0.0.0.0          0.0.0.0          192.168.1.234   192.168.1.234   1
        62.0.0.0          255.0.0.0          62.36.189.146   62.36.189.146   2
        62.36.189.146    255.255.255.255    127.0.0.1       127.0.0.1       1
        62.255.255.255    255.255.255.255    62.36.189.146   62.36.189.146   1
        127.0.0.0          255.0.0.0          127.0.0.1       127.0.0.1       1
        192.168.1.0        255.255.255.0      192.168.1.234   192.168.1.234   1
        192.168.1.234      255.255.255.255    127.0.0.1       127.0.0.1       1
        192.168.1.255      255.255.255.255    192.168.1.234   192.168.1.234   1
        217.127.44.243     255.255.255.255    62.36.189.146   62.36.189.146   1
        224.0.0.0          224.0.0.0          62.36.189.146   62.36.189.146   1
        224.0.0.0          224.0.0.0          192.168.1.234   192.168.1.234   1
        255.255.255.255    255.255.255.255    62.36.189.146   62.36.189.146   1
Default Gateway:        192.168.1.234
=====
Persistent Routes:
None

```

Captura del log del PoPToP en el servidor, cuando se establece una conexión VPN:

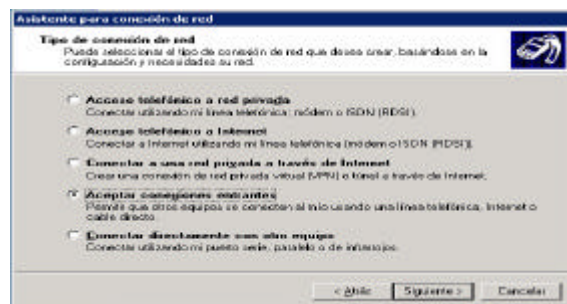
```
Aug 29 23:37:47 navax pptpd[2669]: CTRL: Client 62.36.189.146 control connection started
Aug 29 23:37:47 navax pptpd[2669]: CTRL: Starting call (launching pppd, opening GRE)
Aug 29 23:37:47 navax pppd[2671]: pppd 2.4.1 started by root, uid 0
Aug 29 23:37:47 navax pppd[2671]: using channel 28
Aug 29 23:37:47 navax pppd[2671]: Using interface ppp0
Aug 29 23:37:47 navax pppd[2671]: Connect: ppp0 <--> /dev/tty7
Aug 29 23:37:47 navax pppd[2671]: sent [LCP ConfReq id=0x1 <mru 576> <asynctest 0xa0000>
<auth chap MD5> <magic 0x7c9b6f50> <pcomp> <accomp>]
Aug 29 23:37:48 navax pptpd[2669]: GRE: Discarding duplicate packet
Aug 29 23:37:51 navax pppd[2671]: sent [LCP ConfReq id=0x1 <mru 576> <asynctest 0xa0000>
<auth chap MD5> <magic 0x7c9b6f50> <pcomp> <accomp>]
Aug 29 23:37:51 navax pppd[2671]: rcvd [LCP ConfAck id=0x1 <mru 576> <asynctest 0xa0000>
<auth chap MD5> <magic 0x7c9b6f50> <pcomp> <accomp>]
Aug 29 23:37:51 navax pppd[2671]: rcvd [LCP ConfReq id=0x2 <magic 0xed1f08> <pcomp>
<accomp>]
Aug 29 23:37:51 navax pppd[2671]: sent [LCP ConfAck id=0x2 <magic 0xed1f08> <pcomp>
<accomp>]
Aug 29 23:37:51 navax pppd[2671]: sent [CHAP Challenge id=0x1
<40b62764f3e34c8d4a1d5923837645bd3919a06d>, name = "192.168.1.1"]
Aug 29 23:37:51 navax pppd[2671]: rcvd [CHAP Response id=0x1
<f666d9a14de3997fbd20cd5e31e36459>, name = "billy"]
Aug 29 23:37:51 navax pppd[2671]: sent [CHAP Success id=0x1 "Welcome to navax."]
Aug 29 23:37:51 navax pppd[2671]: sent [IPCP ConfReq id=0x1 <addr 192.168.0.234>
<compress VJ 0f 01>]
Aug 29 23:37:51 navax pppd[2671]: sent [CCP ConfReq id=0x1 <deflate 15> <deflate(old#)
15> <bsd vl 15>]
Aug 29 23:37:51 navax pppd[2671]: CHAP peer authentication succeeded for billy
Aug 29 23:37:51 navax pppd[2671]: rcvd [IPCP ConfReq id=0x1 <compress VJ 0f 01> <addr
0.0.0.0> <ms-dns1 0.0.0.0> <ms-wins 0.0.0.0> <ms-dns3 0.0.0.0> <ms-wins 0.0.0.0>]
Aug 29 23:37:51 navax pppd[2671]: sent [IPCP ConfReq id=0x1 <ms-dns1 0.0.0.0> <ms-wins
0.0.0.0> <ms-dns3 0.0.0.0> <ms-wins 0.0.0.0>]
Aug 29 23:37:51 navax pppd[2671]: rcvd [IPCP ConfAck id=0x1 <addr 192.168.0.234>
<compress VJ 0f 01>]
Aug 29 23:37:51 navax pppd[2671]: rcvd [LCP ProtRej id=0x3 80 fd 01 01 00 0f 1a 04 78 00
18 04 78 00 15 03 2f]
Aug 29 23:37:52 navax pppd[2671]: rcvd [IPCP ConfReq id=0x2 <compress VJ 0f 01> <addr
0.0.0.0>]
Aug 29 23:37:52 navax pppd[2671]: sent [IPCP ConfNak id=0x2 <addr 192.168.1.234>]
Aug 29 23:37:52 navax pppd[2671]: rcvd [IPCP ConfReq id=0x3 <compress VJ 0f 01> <addr
192.168.1.234>]
Aug 29 23:37:52 navax pppd[2671]: sent [IPCP ConfAck id=0x3 <compress VJ 0f 01> <addr
192.168.1.234>]
Aug 29 23:37:52 navax pppd[2671]: not replacing existing default route to eth0
[192.168.1.100]
Aug 29 23:37:52 navax pppd[2671]: found interface eth0 for proxy arp
Aug 29 23:37:52 navax pppd[2671]: local IP address 192.168.0.234
Aug 29 23:37:52 navax pppd[2671]: remote IP address 192.168.1.234
```

Una vez establecida la conexión VPN, el cliente puede ver y usar todos los recursos de la red remota. En la siguiente captura se puede apreciar como podemos ver las carpetas compartidas por Samba.



Puesta en marcha de un servidor de VPN en Windows 2000 Server o Advanced Server

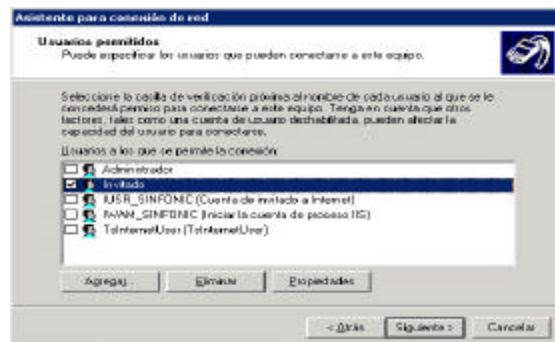
Lo primero que habremos de hacer es crear una conexión de red para que el servidor acepte llamadas entrantes. Esto se realiza como se muestra. Abrimos el asistente para crear conexiones de red. Elegimos la opción de Aceptar conexiones entrantes, y pulsamos en siguiente.



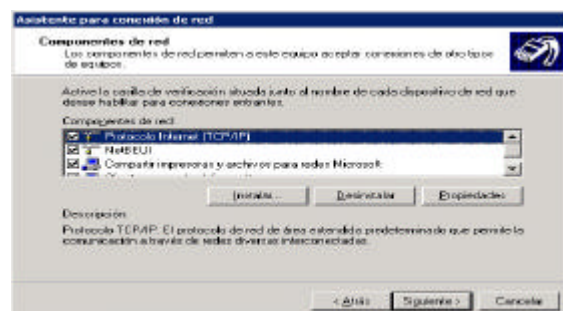
En este paso seleccionaremos todos los dispositivos por los que esperamos que hayan llamadas o conexiones entrantes. Si solo queremos que puedan acceder a nuestro servidor de VPN por red local o Internet, las desactivamos todas, y le damos a siguiente. A continuación activaremos la opción de Aceptar Conexiones Privadas Virtuales, para poder establecer los túneles, y le damos a siguiente.



Uno de los pasos mas importantes, es elegir que usuarios tienen derecho a realizar llamadas entrantes al sistema, porque en el caso de no tener permisos, el servidor de VPN funcionara correctamente pero no nos dejara autentificarnos en el sistema y no podremos establecer el túnel. El usuario que tenga privilegios para realizar llamadas entrantes ha de tener una contraseña asignada. Le damos a siguiente.



Por ultimo elegimos los protocolos de red que serán negociados cuando sea aceptada la conexión entrante. Le damos a siguiente, y a Finalizar. Con esto ya hemos conseguido que



el sistema acepte llamadas entrantes, paso necesario para que el sistema acepte las conexiones de VPN.

A continuación, configuraremos el servidor de VPN. Lo primero será configurar en servidor de enrutamiento y acceso remoto. Accederemos al servidor de enrutamiento y acceso remoto, y abriremos Configurar y Habilitar enrutamiento y acceso remoto, con el botón derecho del ratón.

En el asistente elegiremos la opción de Servidor configurado manualmente. Le damos a siguiente y a Finalizar.

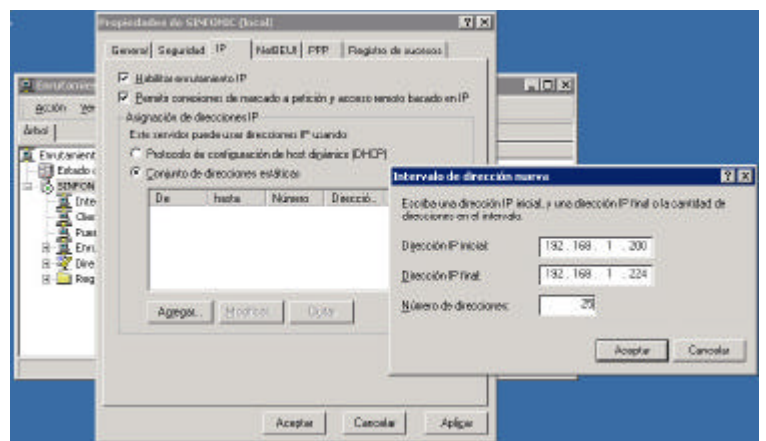
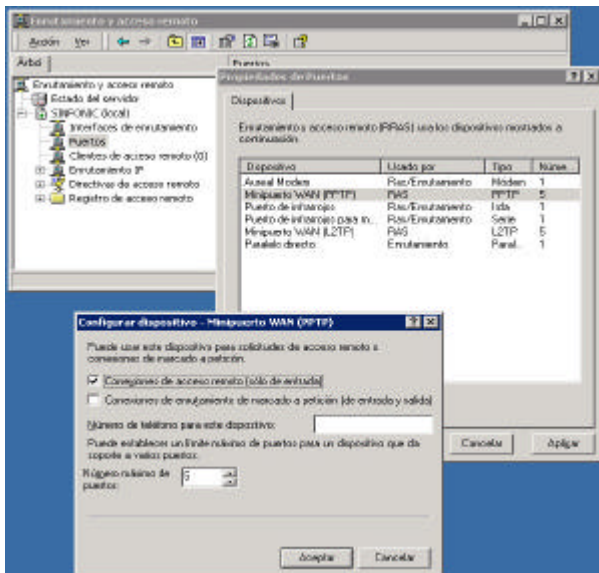
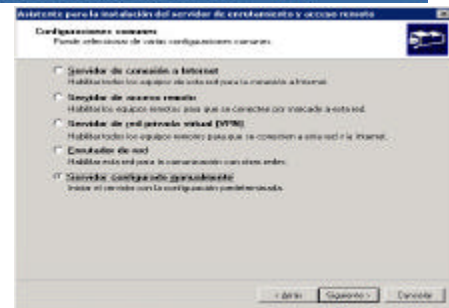
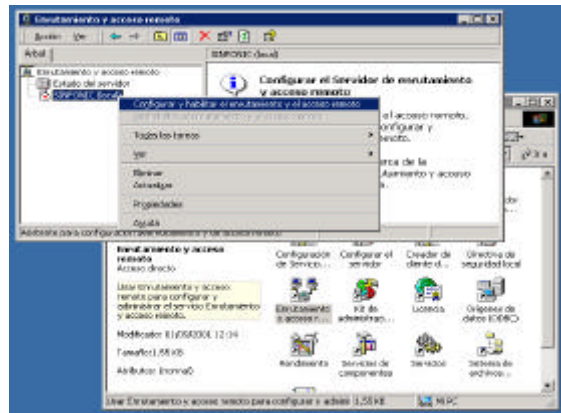
Ahora, después de decir que si para que habilite el servicio, pulsamos en la pestaña de IP, y seleccionamos agregar un conjunto de direcciones estáticas. Estas serán las que asigne el servidor a los clientes de VPN.

serán direcciones que pertenecerán a nuestra red. Le damos al aceptar y finalizamos.

Ahora abriremos las propiedades de los puertos, Pulsaremos sobre el Minipuerto WAN(PPTP), que será el que utilizemos para negociar nuestra conexiones de VPN. Dejaremos las opciones como muestra la figura, y pondremos un numero máximo de puertos que serán las conexiones simultaneas que soportara nuestro servidor de VPN.

Con el Minipuerto WAN(L2TP), haremos lo mismo pero con cero numero de puertos para que desactive este protocolo. Le damos a aceptar y finalizamos.

Con esto ya tenemos configurado el servidor de VPN



Puesta en marcha de un cliente de VPN en Windows 2000/ME/98

Mirar en la pagina de la Universidad de Valencia:

<http://www.uv.es/ciuv/cat/vpn/>

Puesta en marcha de un cliente de VPN en Linux

Necesitamos el cliente PPTP para Linux, que se puede conseguir en código fuente en:

<http://cag.lcs.mit.edu/~cananian/Projects/PPTP/>

Después de compilarlo, necesitamos añadir en nuestro fichero `/etc/pap-secrets`, nuestro nombre de usuario y nuestra contraseña que utilizamos para autenticarse en el servidor VPN.

A continuación, establecemos la conexión con nuestro ISP, y acto seguido ejecutamos el `pptp` de la siguiente forma:

```
# pptp vpn.uv.es debug name usuario
```

Esto establecerá el túnel con el servidor de túneles, en este caso el de la Universidad de Valencia. Ahora cambiamos las rutas adaptándolas a nuestras necesidades, de esta forma, podremos hacer que todo el tráfico que va dirigido a la red de la Universidad, lo mande por el túnel, y el resto lo mandamos por nuestro ISP directamente. Lo hacemos de la siguiente forma:

```
# route del vpn.uv.es ppp1
# route add vpn.uv.es ppp0
# route add -net 147.156.0.0 netmask 255.255.0.0 ppp1
```

Otro ejemplo es si utilizamos un router ADSL, estando configurado como gateway. En este caso la rutas serán un poco diferentes:

```
# route del vpn.uv.es ppp0
# route add vpn.uv.es gw 192.168.1.100 eth0
# route add -net 147.156.0.0 netmask 255.255.0.0 ppp0
```

La ip 192.168.1.100 es la dirección del router ADSL.

Hay que destacar, que en Windows 9x/2000/Me, cuando se establece un túnel, todo el tráfico es desviado por dentro de él. Esto provoca, que en el navegador tengamos que poner la dirección del proxy de la Universidad para poder navegar. En cambio, con las rutas definidas en Linux, no es necesario.

Bibliografía

Virtual Private Networks (VPN / PPTP)
http://www.helmig.com/j_helmig/vpn.htm

Understanding Virtual Private Networks (VPN)
http://www.sans.org/infosecFAQ/encryption/understanding_VPN.htm

Understanding PPTP and VPN's
http://www.aliceinwonderland.com/library/website_archives/rhino9/pptp.html

PoPToP - The PPTP Server for Linux
<http://poptop.lineo.com/>

PPTP
<http://www.cas.mcmaster.ca/~wmfarmer/SE-4C03-01/papers/Silva-PPTP.html>

Acceso remoto por VPN (Red privada virtual)
<http://www.uv.es/ciuv/cat/vpn/>

Cisco - Layer 2 Tunnel Protocol
http://www.cisco.com/warp/public/cc/pd/iosw/tech/l2pro_tc.htm

VPN FAQ
<http://kubarb.phsx.ukans.edu/~tbird/vpn/FAQ.html>