ESTUDIO SOBRE LAS VPN
(REDES PRIVADAS VIRTUALES)

AMPLIACIÓN DE REDES.
4º INGENIERÍA INFORMÁTICA.
UNIVERSIDAD DE VALLADOLID.

Autores del Trabajo:

Mª Nieves Gutiérrez González
Ana Rosa Sancho Buzón
Amadeo Casas Cuadrado

CAPÍTULO 0:

ÍNDICE

CAPÍTULO 1:

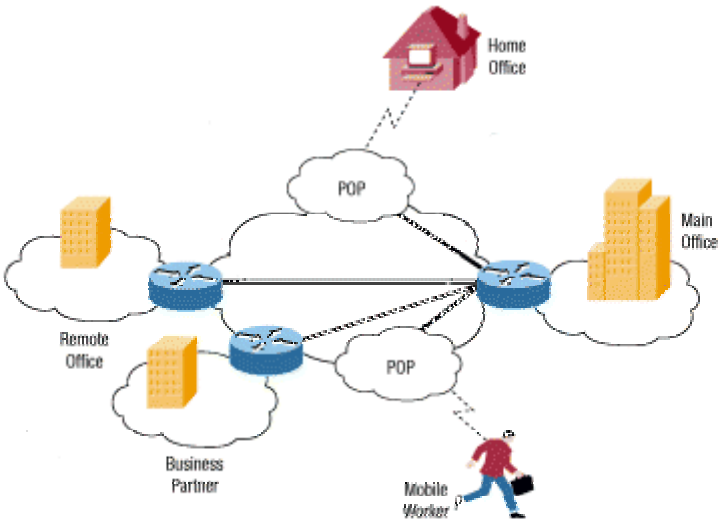
DEFINICIÓN DE VPN

Para poder habilitar redes privadas distribuidas para comunicar de forma segura cada uno de los nodos de una red pública hay una necesidad de evitar que los datos sean interceptados.

Con una **Red Privada Virtual (VPN)**, los usuarios remotos, que pertenecen a una red privada, pueden comunicarse de forma libre y segura entre redes remotas a través de redes públicas.

Una VPN normalmente usa la red Internet como transporte para establecer enlaces seguros, extendiendo las comunicaciones a oficinas aisladas. Significativamente, decrece el coste de las comunicaciones porque el acceso a Internet es generalmente local y mucho más barato que las conexiones mediante *Acceso Remoto a Servidores*.

Una Red Privada Virtual (VPN) transporta de manera segura por Internet por un **túnel** establecido entre dos puntos que negocian un esquema de encriptación y autentificación para el transporte. Una VPN permite el acceso remoto a servicios de red de forma transparente y segura con el grado de conveniencia y seguridad que los usuarios conectados elijan. Las VPN están implementadas con firewalls, routers para lograr esa encriptación y autentificación.



¿Por qué esta idea no ha sido tomada con anterioridad? Posiblemente porque Internet no puede proporcionar la seguridad, el ancho de banda, o la calidad del servicio que garantice la asociación con redes privadas. Por ejemplo, Internet soporta sólo TCP/IP, mientras la mayoría de las redes se acomodan a varios protocolos, y de esta forma si se desea correr una red corporativa bajo Internet se obtendrá un servicio inferior (pero con un menor coste).

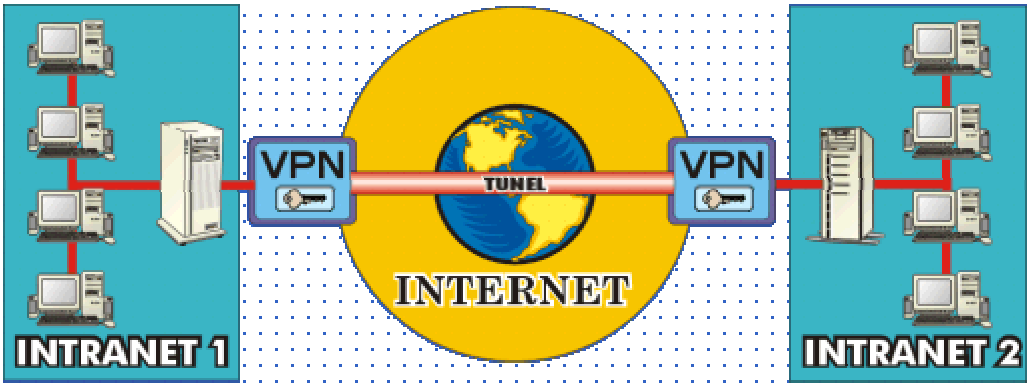
CAPÍTULO 2:

CARACTERÍSTICAS DE VPN

2.1. Descripción de VPN

Una **Red Privada Virtual (VPN)** consiste en dos máquinas (una en cada "extremo" de la conexión) y una ruta o "túnel" que se crea dinámicamente en una red pública o privada. Para asegurar la privacidad de esta conexión los datos transmitidos entre ambos ordenadores son encriptados por el *Point-to-Point Protocol*, también conocido como PPP, un protocolo de acceso remoto, y posteriormente enrutados o encaminados sobre una conexión previa (también remota, LAN o WAN) por un dispositivo PPTP.

Una **Red Privada Virtual** es una forma de compartir y transmitir información entre un círculo cerrado de usuarios que están situados en diferentes localizaciones geográficas. Es una red de datos de gran seguridad que permite la transmisión de información confidencial entre la empresa y sus sucursales, socios, proveedores, distribuidores, empleados y clientes, utilizando Internet como medio de transmisión. Aunque Internet es una red pública y abierta, la transmisión de los datos se realiza a través de la creación de túneles virtuales, asegurando la **confidencialidad e integridad** de los datos transmitidos.



Así, las **VPN** constituyen una estupenda combinación entre la seguridad y garantía que ofrecen las costosas redes privadas y el gran alcance, lo asequible y lo escalable del acceso a través de Internet. Esta combinación hace de las Redes Privadas Virtuales o VPNs una **infraestructura confiable y de bajo costo** que satisface las necesidades de comunicación de cualquier organización.

Las VPNs permiten:

- La **administración y ampliación** de la red corporativa al mejor costo-beneficio.
- La **facilidad y seguridad** para los usuarios remotos de conectarse a las redes corporativas.

Los requisitos indispensables para esta interconectividad son:

- Políticas de seguridad.
- Requerimiento de aplicaciones en tiempo real.
- Compartir datos, aplicaciones y recursos.
- Servidor de acceso y autentificación.
- Aplicación de autentificación.

2.2. Protocolos de VPN

Han sido implementados varios protocolos de red para el uso de las VPN. Estos protocolos intentan cerrar todos los "hoyos" de seguridad inherentes en VPN. Estos protocolos continúan compitiendo por la aceptación, ya que ninguno de ellos ha sido más admitido que otro.

Estos protocolos son los siguientes:

- **Point-to-Point Tunneling Protocol (PPTP)**: PPTP es una especificación de protocolo desarrollada por varias compañías. Normalmente, se asocia PPTP con Microsoft, ya que Windows incluye soporte para este protocolo. Los primeros inicios de PPTP para Windows contenían características de seguridad demasiado débiles para usos serios. Por eso, Microsoft continúa mejorando el soporte PPTP. La mejor característica de PPTP radica en su habilidad para soportar protocolos no IP. Sin embargo, el principal inconveniente de PPTP es su fallo a elegir una única encriptación y autentificación estándar: dos productos que acceden con la especificación PPTP pueden llegar a ser completamente incompatibles simplemente porque la encriptación de los datos sea diferente.

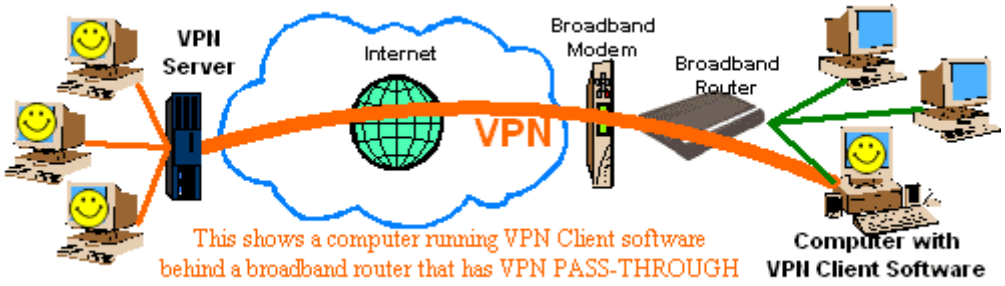
- **Layer Two Tunneling Protocol (L2TP)**: El principal competidor de PPTP en soluciones VPN fue L2F, desarrollado por Cisco. Con el fin de mejorar L2F, se combinaron las mejores características de PPTP y L2F para crear un nuevo estándar llamado L2TP. L2TP existe en el nivel de *enlace* del modelo OSI. L2TP, al igual que PPTP soporta clientes no IP, pero también da problemas al definir una encriptación estándar.

- **Internet Protocol Security (IPsec)**: IPsec es en realidad una colección de múltiples protocolos relacionados. Puede ser usado como una solución completa de protocolo VPN o simplemente como un esquema de encriptación para L2TP o PPTP. IPsec existe en el nivel de *red* en OSI, para extender IP para el propósito de soportar servicios más seguros basados en Internet.

- **SOCKS Networks Security Protocol**: El sistema SOCKS proporciona otra alternativa a los protocolos de VPN. SOCKS se aloja en el nivel de *sesión* de OSI. Como SOCKS trabaja en un nivel OSI más alto que los protocolos anteriores, permite a los administradores limitar el tráfico VPN.

2.3. Clientes / Servidores en VPN

Un **Servidor VPN** normalmente es un componente hardware, aunque también lo puede ser software. Puede actuar como un gateway en una red o en un único computador. Debe estar siempre conectado y esperando a que clientes VPN se conecten a él. El software para el Servidor VPN es bastante frecuente. Sistemas como **Windows 2000 Server** permiten alojar un Servidor VPN. El hardware de los Servidores VPN es bastante caro: el precio, a finales del año 2001, oscilaba entre los *170$* y los *300$*.



Un **Cliente VPN** es en la mayoría de los casos un componente software, aunque puede ser también un componente hardware. Un cliente realiza una llamada al servidor y se conecta. Entonces la computadora cliente podrá comunicarse con el Servidor VPN, ya que ellos se encuentran en la misma red virtual. El software para un cliente VPN es bastante común. Cuando se carga en la computadora este software permite crear un túnel seguro VPN a través de Internet para poder comunicarse con el Servidor VPN.

Un **Router** basado en Servidores VPN tiene una velocidad de **600Kbps** debido a sus microprocesadores.

CAPÍTULO 3:

EJEMPLO DE VPN: PAQUETE F-SECURE

F-Secure VPN es una solución flexible y de coste aprovechable para obtener los beneficios de Internet comprometiéndose a mantener la seguridad en la misma. Dota a la gestión de la red de túneles entre los puntos de empresa manteniendo el acceso a puntos externos si se quiere. Es mejor usar este paquete junto con un firewall para conseguir un control total sobre el tráfico de datos de toda la organización.

3.1. Características de F-Secure

Las características principales son las siguientes:

- **Fácil de instalar**: Requiere muy pocos parámetros de instalación para el Administrador.
- **Fácil de configurar**: Posee un editor de red gráfico que permite configurar la totalidad de la red VPN desde una simple estación de trabajo.
- **Seguro**: Usa una extensa variedad de algoritmos de encriptación, tales como DES, Blowfish, RSA, etc.
- **Basado en una tecnología ampliamente testeada y usada**: Está basado en la tecnología SSH, la cual es utilizada incluso por la NASA.
- **Disponible a nivel global, con una fuerte encriptación**: Se puede enviar el software encriptado a todo el mundo, sin ningún compromiso.

3.2. Beneficios de F-Secure

Los beneficios de F-Secure son los siguientes:

- Cualquier PC con ciertos requerimientos mínimos puede utilizar el software de F-Secure VPN.
- La red VPN es dinámicamente ampliable de modo que nuevas LANs se pueden añadir sin demasiada configuración.

- Se pueden usar conexiones a Internet de bajo coste para formar la VPN. Tradicionalmente, las redes privadas virtuales seguras han estado construyéndose usando líneas alquiladas muy caras.

- Automáticamente se encriptan y protegen contra alteraciones, todas las conexiones F-Secure VPN.

- F-Secure VPN se integra con cualquiera de las firewalls existentes.

- F-Secure VPN soporta conexiones Extranet seguras.

CAPÍTULO 4:

VPN DINÁMICAS

4.1. Conceptos de las VPN Dinámicas

Internet no fue diseñada, originalmente, para el ámbito de los negocios. Carece de la tecnología necesaria para la seguridad en las transacciones y comunicaciones que se producen en los negocios. Entonces, ¿Cómo establecer y mantener la confianza en un entorno el cual fue diseñado desde el comienzo para permitir un acceso libre a la información?, es decir, ¿Cómo conseguir seguridad en una intranet sin chocar con los principios básicos de Internet sobre la flexibilidad, interoperatibilidad y facilidad de uso?

La respuesta apropiada se encuentra en la utilización de **VPNs Dinámicas**. A diferencia de una VPN tradicional, una VPN Dinámica proporciona, además de un alto nivel de seguridad a ambos extremos, una flexibilidad necesaria para acoplarse dinámicamente a la información que necesitan los distintos grupos de usuarios. Las VPNs Dinámicas pueden ofrecer esta flexibilidad ya que están basadas en una única arquitectura. Además, una VPN Dinámica proporciona más recursos y servicios a una Intranet, para hacer mayor uso de los recursos de la información.

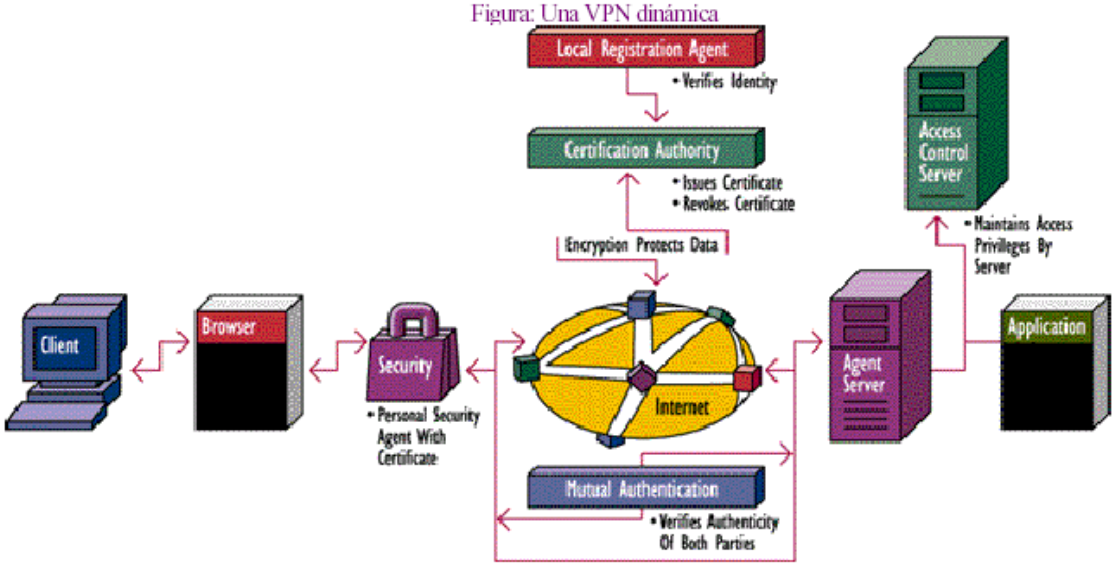
Alguna de las características que se proporciona son las siguientes:

- Proporciona una seguridad importante para la empresa.
- Se ajusta dinámicamente al colectivo dispar de usuarios.
- Permite la posibilidad de intercambio de información en diversos formatos.
- El ajuste que hace para cada usuario lo consigue gracias a los diferentes navegadores, aplicaciones, sistemas operativos, etc...
- Permite a los usuarios unirse a distintos grupos, así como a los administradores asignar identidades en un entorno simple pero controlado.
- Mantiene la integridad total, independientemente del volumen administrativo, cambios en la tecnología o complejidad del sistema de información corporativo.

4.2. Funcionamiento de las VPN Dinámicas

Las VPNs Dinámicas constan de una plataforma de seguridad de red y un conjunto de aplicaciones para usar en la plataforma de seguridad.

Figura: Una VPN dinámica



Siguiendo los pasos ilustrados en la figura, un usuario realiza una petición de información a un servidor, por ejemplo, pulsando con su ratón en un hipervínculo. Los pasos seguidos se pueden describir en los siguientes puntos:

- **Un usuario solicita información usando una aplicación tal como un navegador de Internet, desde un ordenador de sobremesa**: El intercambio de información comienza cuando un usuario envía información a otro usuario o solicita información al servidor. En el supuesto de que un usuario haya accedido a un hipervínculo desde dentro de algún documento Web, dicho hipervínculo será seguro y solamente podrá ser accedido por usuarios autorizados.

- **La aplicación envía y asegura el mensaje**: Cuando un cliente y un servidor detectan que se necesita seguridad para transmitir la petición y para ver el nuevo documento, ellos se interconectan en un mutuo protocolo de autentificación. Este paso verifica la identidad de ambas partes antes de llevar a cabo cualquier acción. Una vez que se produce la autentificación se asegura el mensaje encriptándolo. Adicionalmente, se puede atribuir un certificado o firma electrónica al usuario.

- **El mensaje se transmite a través de Internet**: Para que la petición alcance el servidor debe dejar la LAN y viajar a través de Internet, lo cual le permitirá alcanzar el servidor en algún punto de la misma. Durante este viaje, puede darse el caso de que atraviese uno o más firewalls antes de alcanzar su objetivo. Una vez atravesado el firewall, la petición circula a lo largo del pasillo Internet hasta alcanzar el destino.
- **El mensaje recibido debe pasar controles de seguridad**: El mensaje se transfiere al servidor. El servidor conoce la identidad del usuario cliente cuando recibe la petición.

- **Durante la petición, se verifican los derechos de acceso de los usuarios**: En una VPN dinámica, el sistema debe poder restringir que usuarios pueden y no

pueden acceder a la misma. El servidor debe determinar si el usuario tiene derechos para realizar la petición de información. Esto lo hace usando mecanismos de control, alojados en el *Servidor de Control de Acceso*. De este modo, incluso si un usuario presenta un certificado válido, puede ser que se le deniegue el acceso basándose en otros criterios.

- **La petición de información es devuelta por Internet, previamente asegurada**: El servidor de información encripta la información y opcionalmente la certifica. Las claves establecidas durante los pasos de autentificación mutua se usan para encriptar y desencriptar el mensaje. De esta forma, un usuario tiene su documento asegurado.

CAPÍTULO 5:

CONFIGURAR UNA VPN BAJO WINDOWS

5.1. Necesidades

Se necesita lo siguiente para instalar una VPN:

- **Una conexión a Internet rápida para el servidor local de NT y para los PC remotos**.
- **Una IP ADDRESS estática para el servidor NT**.
- **Un proxy que se ejecuta en el servidor NT**, para evitar que la gente desautorizada tenga acceso al sistema.
- **Una IP ADDRESS para cada recurso que será compartido**: Recursos, como una impresora, a los que deseamos poder tener acceso a través de Internet necesitan tener su propia IP.
- **Adaptador virtual de la red instalado en el PC remoto o cliente.**

5.2. Pasos de la configuración del Cliente VPN

Deberemos seguir los siguientes pasos:

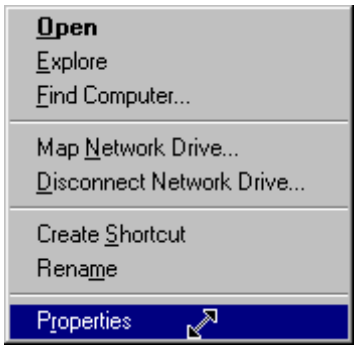
- Hacer una lista de todas las IP internas que contendrán recursos que serán accedidos a través de Internet.
- Instalar y ejecutar el proxy.
- En el servidor del NT, configurar los ficheros del usuario de NT para permitir que cada usuario pueda llamar y conectar al Servidor de NT. Hay que garantizar a cada usuario que tendrá acceso al sistema con su permiso de VPN de marca en el servidor NT.

Después de esto, habrá que instalar el adaptador privado de la red en el PC cliente. Indicamos a continuación los pasos a realizar:

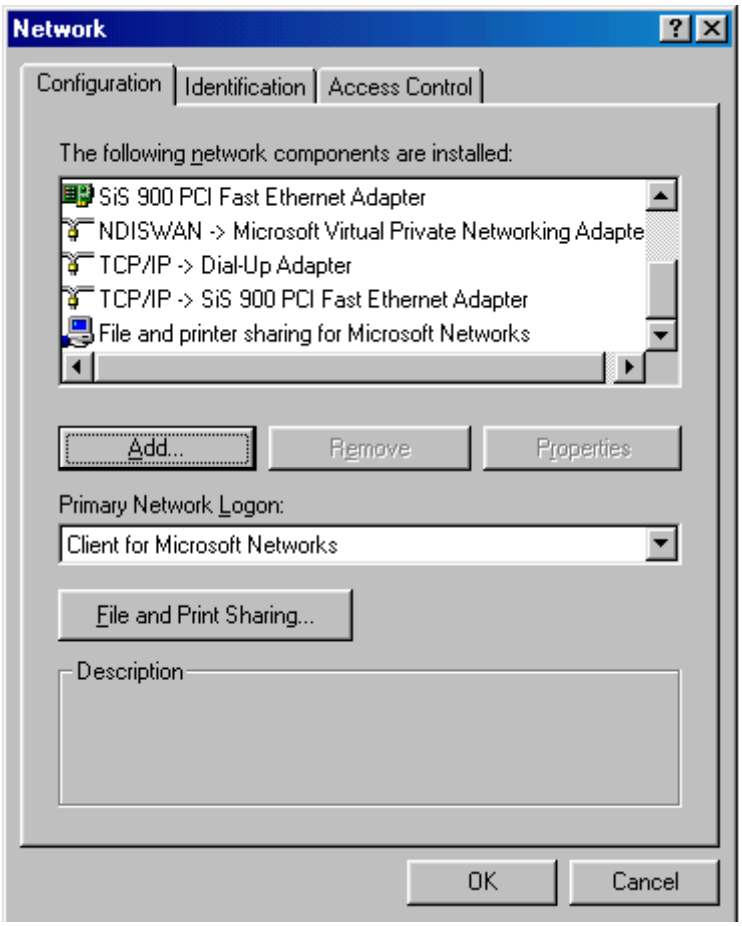
1º) INSTALAR EL ADAPTADOR PRIVADO VIRTUAL DE LA RED EN EL PC CLIENTE:

- En el Escritorio del PC hacer click en el icono del **Entorno de Red**:

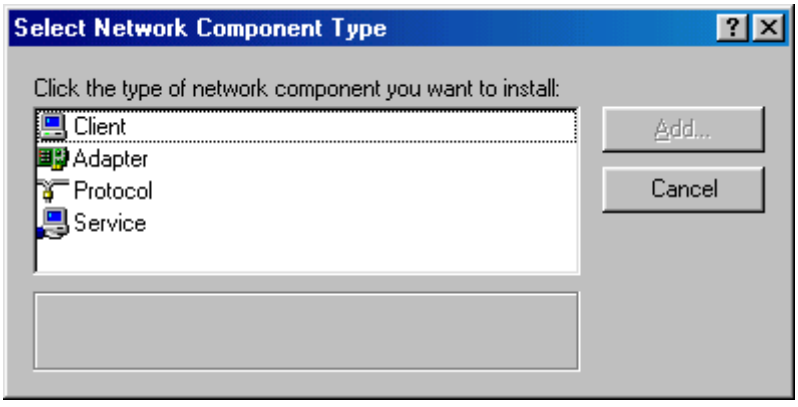
- Pulsar con el botón derecho y seleccionar las **Propiedades**:



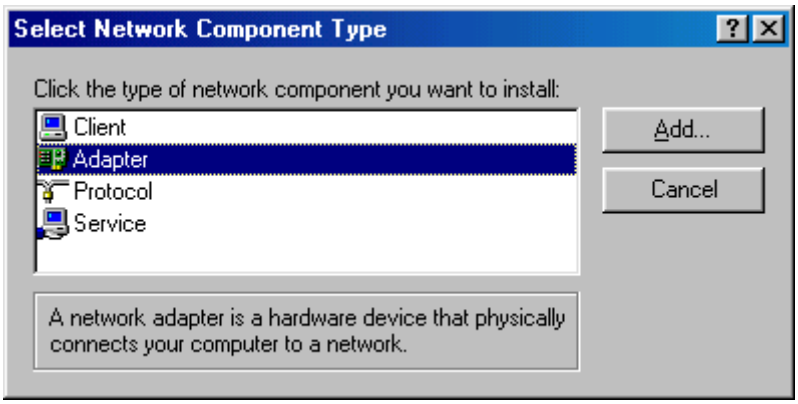
- Entonces, se abrirá el **Diálogo de Red**:



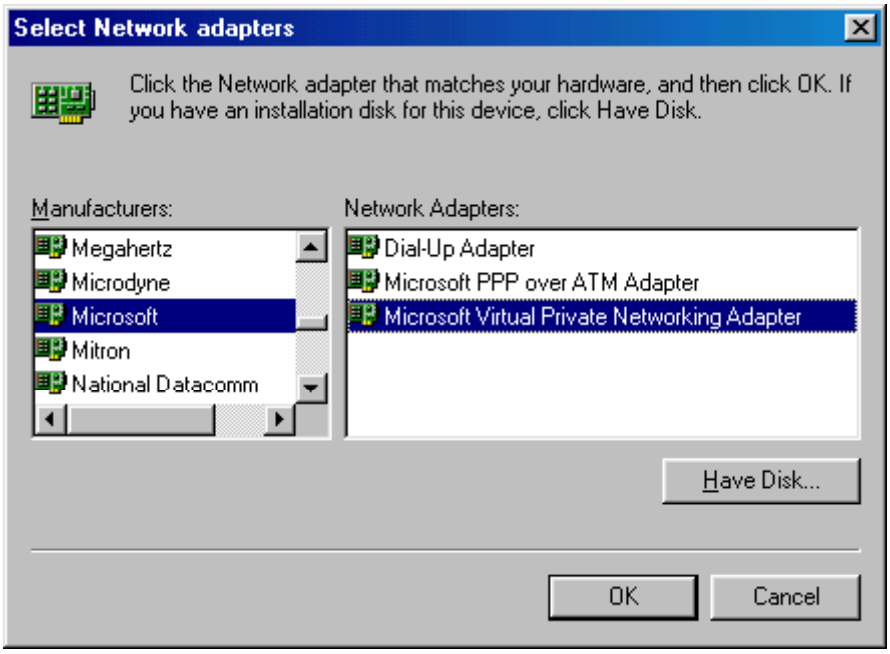
- Verificar que el **adaptador de redes privadas virtuales** está instalado. Si no, hacer click en **Agregar**. El diálogo **Seleccionar Nuevo Componente de la Red** se abrirá:



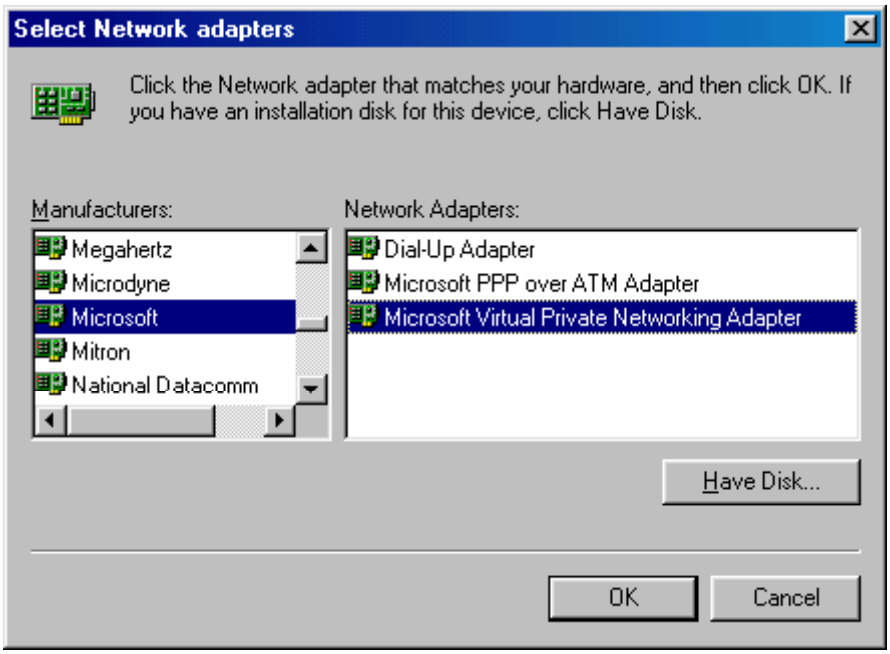
- Seleccionar el adaptador de la lista y hacer click en **Agregar**:



- Cuando el **Diálogo Seleccionar el Adaptador** se abre seleccionar Microsoft de la lista de los fabricantes, ya que la explicación es sobre un adaptador fabricado por Microsoft:

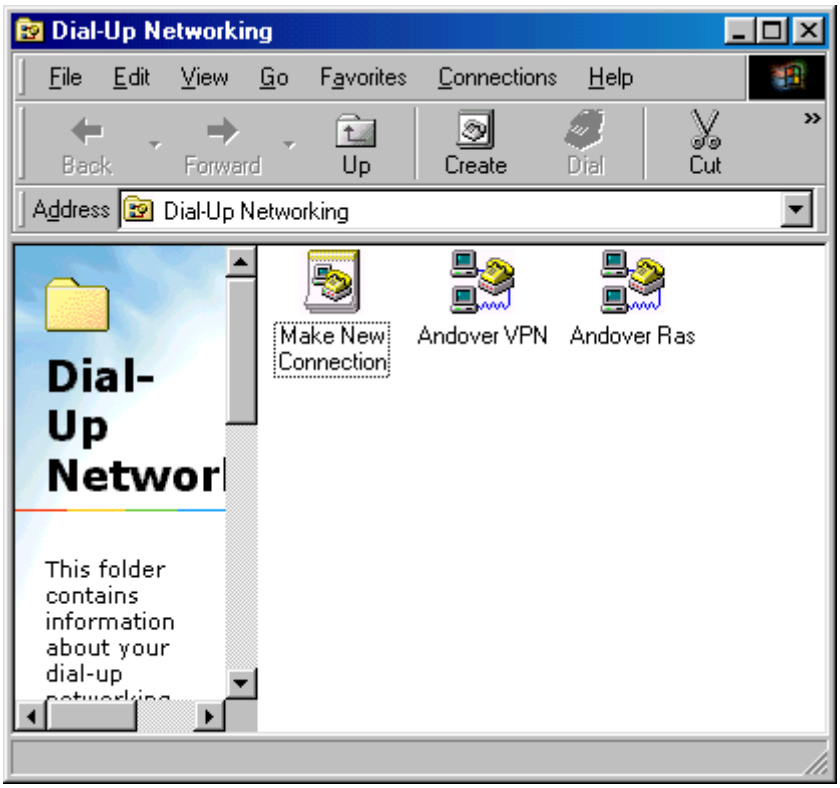


- Seleccionar el **adaptador de redes privadas** de la lista de los adaptadores de la red, y hacer click en **OK**:

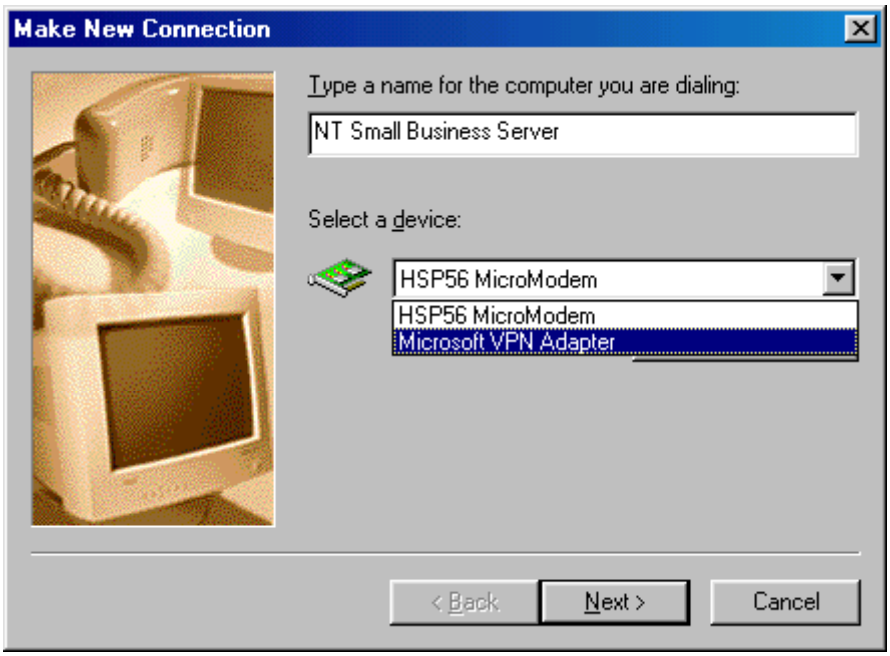


2º) INSTALAR LA CONEXIÓN A LA LAN:

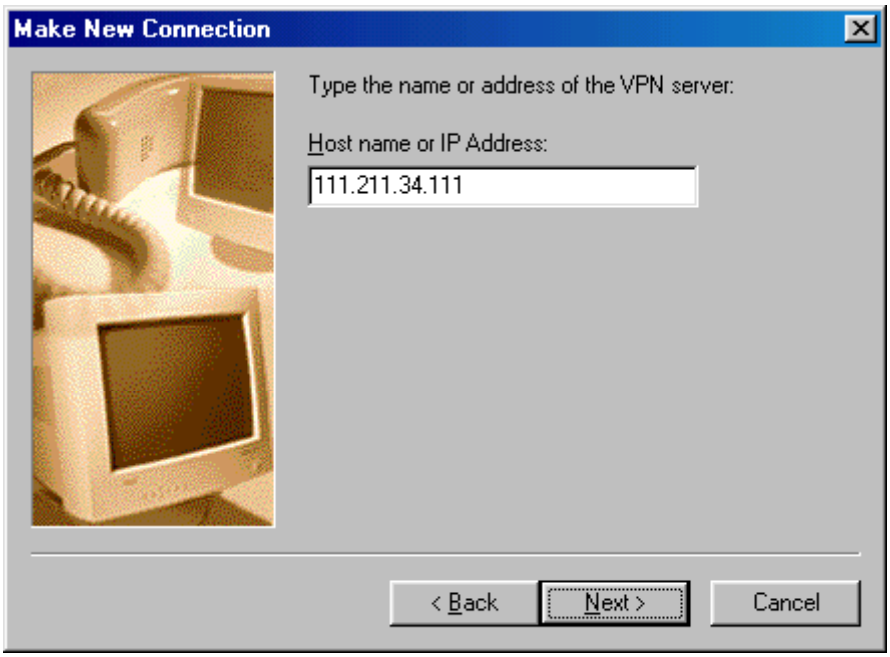
- Acceder al **Acceso Remoto a Redes**:



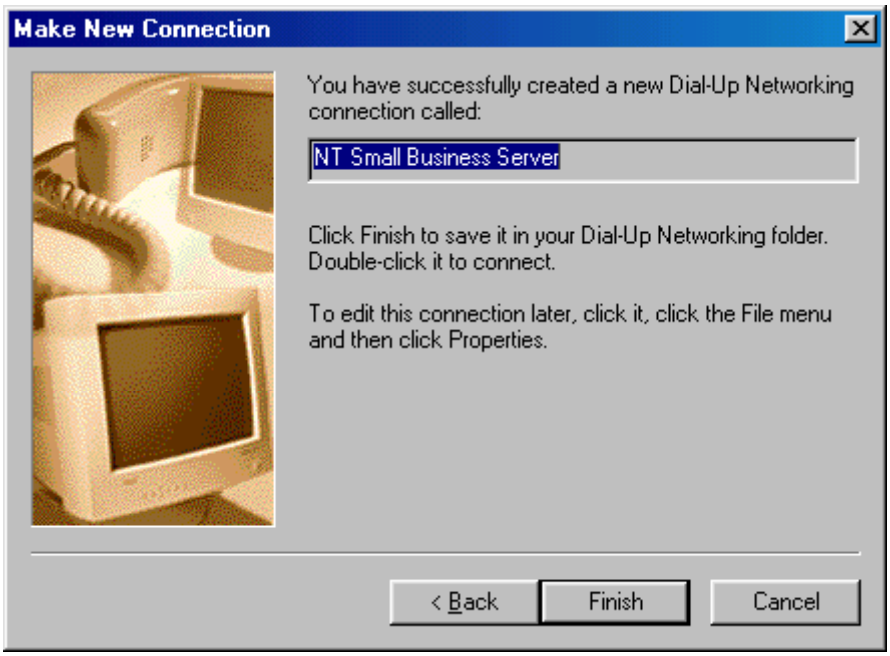
- Pulsar doble click en el icono de **Nueva Conexión**. Después, en el selector de lista de dispositivos, haga click en la flecha y seleccione el adaptador de VPN:



- Se abre el nuevo **Diálogo de la Conexión** y espera a que introducir la dirección IP del Servidor VPN al que se conectará:

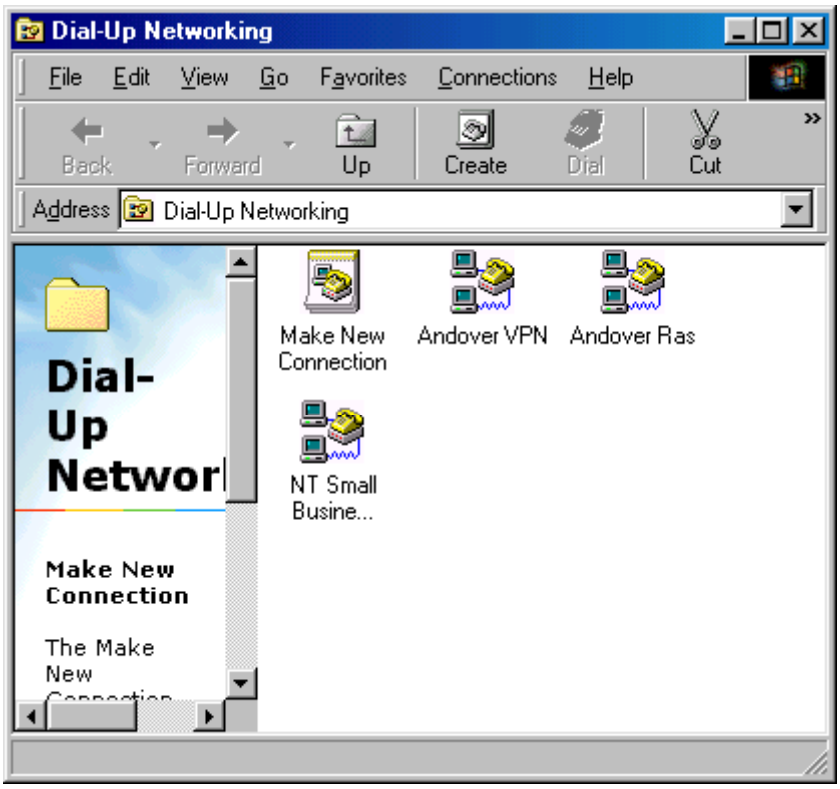


- De esta forma, se crea la nueva conexión:

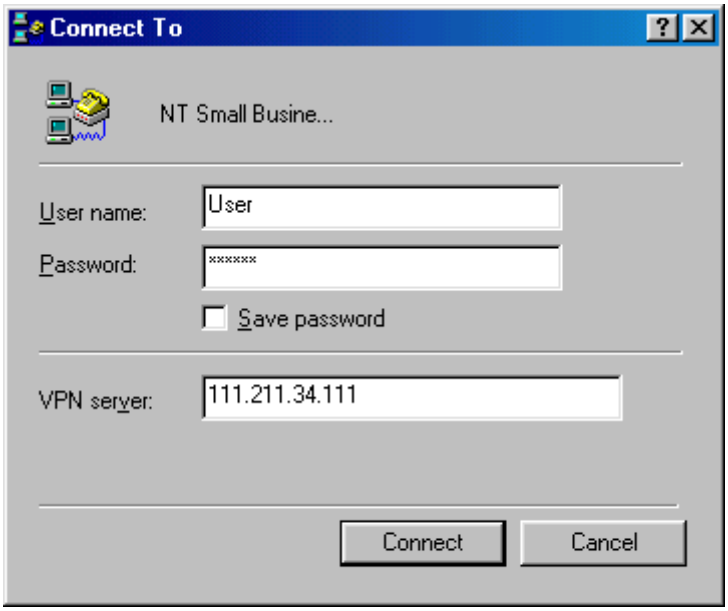


3º) CONECTAR CON EL SERVIDOR DEL NT:

- Acceder al **Acceso Remoto a Redes**:



- Pulsar doble click en el icono para la conexión de VPN:



- Por último, simplemente deberá introducir el **login** y el **password** y ya quedará conectado con el servidor.

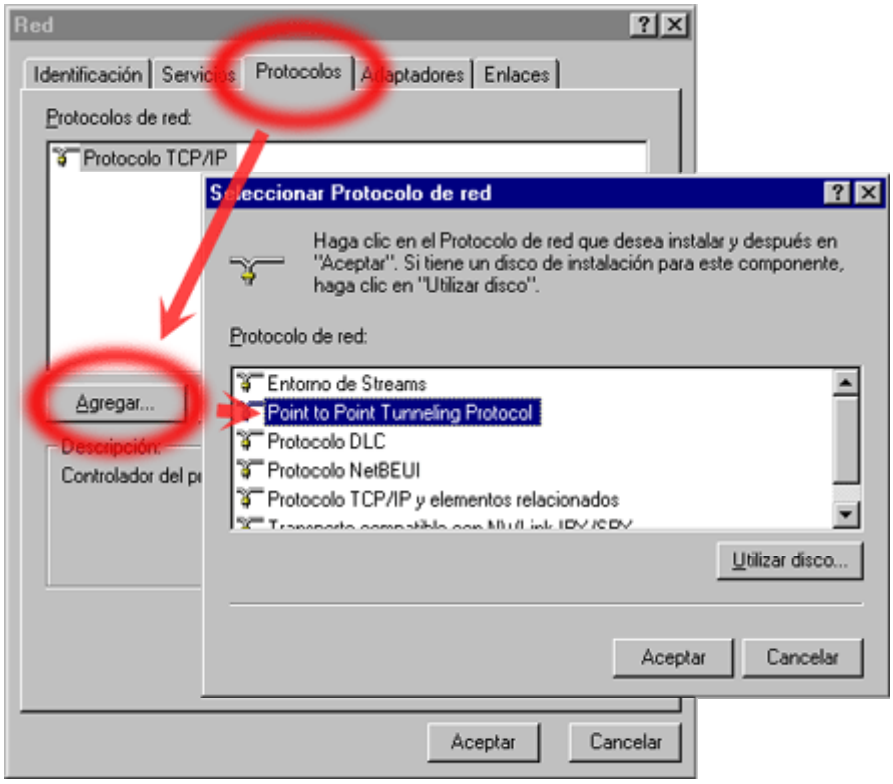
5.3 Pasos de la configuración del Servidor VPN

Deberemos seguir los siguientes pasos:

1º) CONFIGURACIÓN DE PPTP:

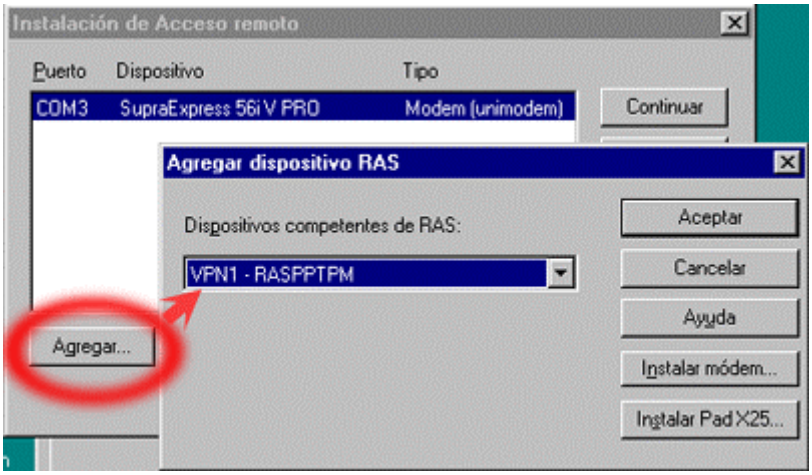
PPTP debe activarse en el **Servidor RAS** (Remote Access Server) y en los **Clientes** que vayan a utilizarlo. Para ello, seguimos los siguientes pasos:

- Utilice la herramienta **Red** del **Panel de control**, sitúese en la ficha **Protocolos** y pulse **Agregar**:



- Escoja **Point to Point Tunneling Protocol**. Una vez copiados los archivos, aparece el cuadro de diálogo **Configuración de PPTP**. El campo **Número de redes privadas virtuales** indica el número de conexiones PPTP admitidas. En el ejemplo se establecen dos VPN:

- A continuación se inicia la herramienta de configuración RAS. Debe **añadir los puertos virtuales** que darán servicio a las redes privadas virtuales que desee establecer. Pulse **Agregar** para acceder al diálogo Agregar dispositivo RAS:



El ejemplo muestra dos puertos virtuales que corresponden al valor especificado en el paso 2. Seleccione una entrada (por ejemplo **VPN1 RASPPTPM**) y pulse **Aceptar**.

- Seleccione cada entrada del diálogo **Instalación de Acceso remoto** y pulse **configurar** para acceder al diálogo Configurar uso del puerto. Seleccione una de las opciones disponibles: Sólo para hacer llamadas, Sólo para recibir llamadas o hacer y recibir llamadas.

- Repita los pasos anteriores para cada dispositivo virtual que desee añadir.

- Pulse **Continuar** después de añadir todos los dispositivos virtuales. Pulse **Cerrar** cuando vuelva a la ficha Protocolos. Reinicie la computadora.

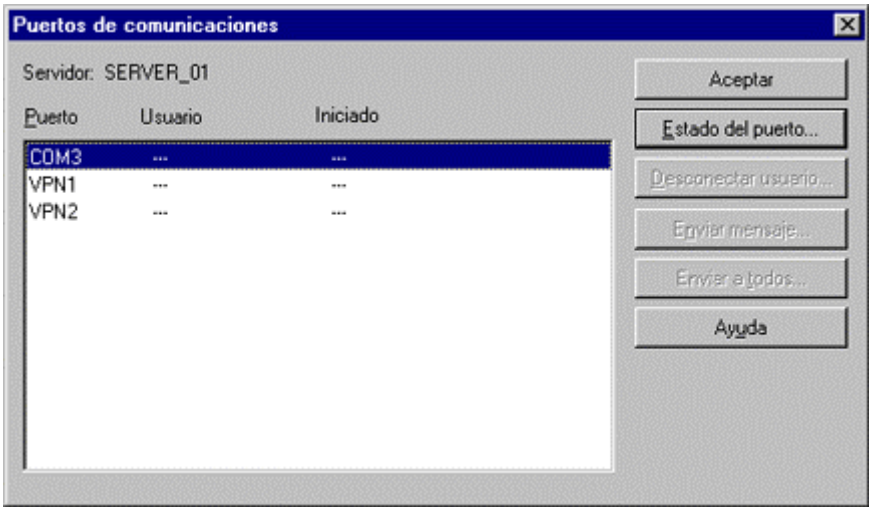
2º) ACTIVAR EL FILTRO PPTP:

- Seleccione la ficha **Protocolos** de la herramienta **Red**.

- Seleccione **Protocolo TCP/IP** y pulse el botón **Propiedades**.
- Sitúese en la ficha **Dirección IP**.
- Seleccione el **adaptador de red** sobre el que desee aplicar el filtro.
- Pulse el botón **Avanzadas**.
- Marque la casilla **Activar filtro PPTP**.
- Repita los pasos anteriores para cada interfaz que deba utilizar el filtro **PPTP**.
- Reinicie la computadora para activar los cambios.

3º) SUPERVISIÓN DEL SOPORTE DE SERVIDOR PPTP:

Es posible supervisar los puertos PPTP utilizando la herramienta **Administrador de Acceso remoto**. Seleccione la orden **Puertos de comunicaciones** del menú **Servidor**. Sólo aparecen los puertos configurados para recibir llamadas.



4º) ACTIVAR EL SOPORTE PPTP EN LOS CLIENTES:

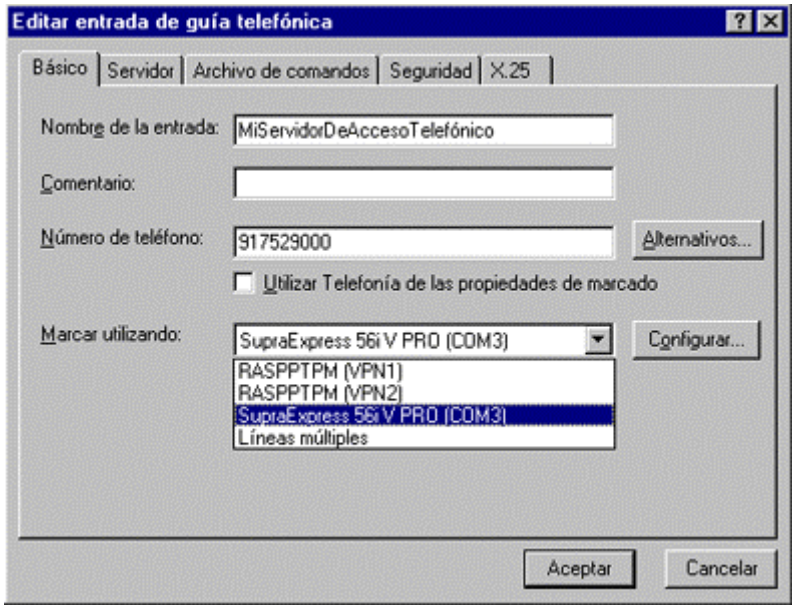
Cuando un cliente llama a Internet, el procedimiento para establecer un túnel PPTP consta de dos pasos:

- El cliente establece una conexión de acceso telefónico a Internet a través de un proveedor de acceso.
- El cliente establece una conexión PPTP con el servidor RAS.

Cuando un cliente se conecta directamente a Internet, no es necesario establecer una conexión de acceso telefónico. Sin embargo, el procedimiento para iniciar la conexión PPTP con el servidor RAS es idéntico. Para establecer una conexión PPTP es necesario crear una entrada especial en la guía telefónica. Esta entrada se distingue por dos características:

- El campo **Marcar** utilizando contiene uno de los dispositivos virtuales VPN añadidos a la configuración RAS al instalar PPTP. Esta lista sólo muestra los VPN configurados para hacer llamadas.

- El campo **Presentación preliminar de número de teléfono** contiene el nombre DNS o la dirección IP del servidor PPTP.



La creación de una conexión a PPTP conlleva dos pasos:

- Abra la aplicación Acceso telefónico a redes y utilice la entrada de la guía telefónica que le permite acceder a su proveedor de acceso a Internet a través de un número de teléfono y un módem.

- Una vez establecida la conexión, utilice la entrada de la guía telefónica que le conecta al túnel PPTP mediante un nombre DNS o una dirección IP.

Si el cliente está conectado directamente a Internet, sólo es necesario utilizar la entrada del túnel PPTP.

CAPÍTULO 6:

CONFIGURAR UNA VPN BAJO LINUX

6.1. Diferentes soluciones

Hay muchos productos que aplican IPsec, entre los que se encuentran PGPnet y Windows 2000. La mayoría de los firewalls comerciales cuentan con módulos para VPN, Linux nos ofrece diversas soluciones para aplicar VPN e intercomunicar dispositivos en la red que manejan IPsec. Algunos de estos productos pueden ser:

- **Freeswan**
- **CIPE**
- **VPND**
- **...**

De las distintas herramientas que podemos emplear vemos el caso de **vpnd**. En el siguiente apartado se muestra brevemente como crear una Red Privada Virtual usando **GNU/Linux** y **vpnd**.

6.2. GNU/Linux y vpnd

Vpnd es muy fácil de instalar y configurar. En este caso ha sido montado con **Debian GNU/Linux** aunque en principio no debería suponer ningún problema hacerlo funcionar con otra distribución.

Vpnd permite crear enlaces seguros sobre TCP/IP, con claves de hasta 512 bits con algoritmo de encriptación **BLOWFLISH**, montando una interface serie virtual que proporciona la posibilidad de enrutar tráfico IP entre dos subredes. Los pasos que se deberán realizar son:

- Para empezar, se deberá tener soporte SLIP en el núcleo.

- Después de configurar el núcleo, hay que compilarlo y probar que funciona correctamente, podemos pasar a instalar el paquete vpnd con '**apt-get install vpnd**'.

- Una vez instalado es necesario crear una clave de sesión con '**vpnd –m /etc/vpnd/vpnd.key**'. Esta clave debe ser la misma en los dos extremos de la VPN, por lo que se tendrá que pasar la clave por un medio seguro al otro equipo. Después

de esto sólo queda configurar los dos extremos de la VPN y cómo se comunicarán a través de TCP siguiendo la estructura C*liente/Servidor* (uno actuará de cliente y el otro de servidor de la VPN).

- A continuación, mostramos el contenido de los ficheros **vpnd.conf** de configuración para el servidor y para el cliente:

Fichero /etc/vpn/vpnd.conf de configuración en el Servidor:

```
mode server
# Dirección IP y puerto del servidor
server a.b.c.d 2001
# Dirección IP y puerto del cliente
client w.x.y.z 2001
# Dirección IP privada del servidor
local a.b.c.d
# Dirección IP privada del cliente
remote w.x.y.z
# Opciones generales
autoroute
Keepalive 10
noanswer 3
keyfile /etc/vpnd/vpnd.key
pidfile /var/run/vpnd.pid
keyttl 120
randomdev /dev/urandom
mtu 1600
```

Fichero /etc/vpn/vpnd.conf de configuración en el cliente:

```
mode client
# Dirección IP y puerto del cliente
client w.x.y.z 2001
# Dirección IP y puerto del servidor
server a.b.c.d 2001
# Dirección IP privada del cliente
local w.x.y.z
# Dirección IP privada del servidor
remote a.b.c.d
# Opciones generales
autoroute
Keepalive 10
noanswer 3
keyfile /etc/vpnd/vpnd.key
pidfile /var/run/vpnd.pid
keyttl 120
randomdev /dev/urandom
mtu 1600
```

- Una vez hechas estas modificaciones ya podemos levantar la VPN iniciando los demonios con '**/etc/init.d/vpnd start**'. Para comprobar que todo ha funcionado de forma correcta podemos hacer *pings* a nuestra IP privada y a la IP del otro extremo y ver con '**ifconfig –a**' que tenemos una interfaz nueva como la siguiente:

```
sl0       Link encap:VJ Serial Line IP
          inet addr:10.0.0.1 P-t-P:10.0.0.2 Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST MTU:1600 Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
                Compressed:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          Collisions:0 compressed:0 txqueuelen:10
          RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)
```

CAPÍTULO 7:

CONCLUSIONES

⇒ Las redes VPN proporcionan principalmente **dos ventajas**:

- **Bajo coste de una VPN**:
  - ✓ Una forma de reducir coste en las VPN es eliminando la necesidad de largas líneas de coste elevado. Con las VPN, una organización sólo necesita una conexión relativamente pequeña al proveedor del servicio.
  - ✓ Otra forma de reducir costes es disminuir la carga de teléfono para accesos remotos. Los clientes VPN sólo necesitan llamar al proveedor del servicio más cercano, que en la mayoría de los casos será una llamada local.

- **Escalabilidad de las VPNs**: Las redes VPN evitan el problema que existía en el pasado al aumentar las redes de una determinada compañía, gracias a Internet. Internet simplemente deriva en accesos distribuidos geográficamente.

⇒ Las redes VPN contraen **cuatro inconvenientes**:

- Las redes VPN requieren un conocimiento en profundidad de la seguridad en las redes públicas y tomar precauciones en su desarrollo.

- Las redes VPN dependen de un área externa a la organización, Internet en particular, y por lo tanto depende de factores externos al control de la organización.

- Las diferentes tecnologías de VPN podrían no trabajar bien juntas.

- Las redes VPN necesitan diferentes protocolos que los de IP.

⇒ Se estima que una solución VN para una determinada empresa puede reducir sus costes **entre un 30% y un 50%** comparada con las conexiones punto a punto.

⇒ Hay **dos aplicaciones** principales para las redes VPN:

- **Teletrabajo**: Es la solución ideal, por su efectividad y sus bajos costes, para aquellas organizaciones que necesiten que sus empleados accedan a la red corporativa, independientemente de su ubicación geográfica.

- **VPN Empresa**: Solución de conectividad entre sucursales de la empresa o entre la empresa y sus socios, proveedores, etc. Gracias a su flexibilidad se adapta al tamaño y necesidades de la organización.

CAPÍTULO 8:

BIBLIOGRAFÍA Y ENLACES DE INTERÉS

Para la realización de este trabajo se han consultado las siguientes páginas de Internet, con el fin de obtener la suficiente información:

http://www.vpnlabs.org/

http://compnetworking.about.com/

http://www.pcworld.com/

http://www.homenethelp.com/

http://www.infoworld.com/

http://www.rad.com/networks/

http://www.nwfusion.com/

http://www.vpnlabs.org/all-vpn-categories.html

http://madridwireless.net/vpnd.shtml

http://www.xtech.com.ar/html/NuevasSoluciones.htm

http://adslnet.ws/vpn.htm

http://adslnet.ws/vpn_server.htm

http://www.canariasi.com/pg/vpn.html

http://www.canariasi.com/pg/vpntecnica.html

http://www.adpsoft.com/Linux/servicios.htm

http://congreso.hispalinux.es/actividades/ponencias/rodriguez/html/x28.html

http://www.gulp.org.mx/articulos/vpn.html