Tecnología.

Redes Privadas Virtuales.
Poner puertas al campo.

Juan Blázquez Martín
j.blazquez@danysoft.com

El sustancial incremento de la productividad en el negocio de cualquier empresa que representa la instalación de una red de ordenadores es algo incuestionable desde la aparición en el mercado informático de estas soluciones de gestión. En consecuencia, las redes van evolucionando rápidamente, y con paso firme, a medida que las distintas tecnologías de conexión posibilitan alcanzar más y mejores formas de compartir los servicios y recursos disponibles, expandiéndose ampliamente al amparo de una perspectiva de bajo coste económico.

Esta evolución constante de las tecnologías de conectividad ha traído una rápida propagación de la informática en todos los niveles de la actividad empresarial, el desarrollo de nuevos servicios e, incluso, nuevas formas de plantear el trabajo habitual. También es cierto que el desarrollo de esa tecnología es la responsable directa de generar unas necesidades de acceso global a la red propia que no todas las entidades pueden cubrir para sus empleados por los problemas de gestión, explotación y coste que llevan aparejadas. No resulta inmediato, ni fácil, poder incorporar a toda una estructura de agentes comerciales, desplegada por distintas áreas geográficas a la red, contemplando puestos remotos e incluso móviles. El coste de los equipos, el alquiler de líneas, el esfuerzo de administración y los recursos adicionales que hay que dedicar para hacer realidad una infraestructura de esta magnitud, hacen que sólo esté al alcance de un pequeño grupo de grandes corporaciones.

El rápido desarrollo de Internet como canal de comunicación para todo tipo de propósito, ha incrementado espectacularmente las posibilidades de conexión y ha diluido los problemas técnicos relacionados con la complejidad/costes de infraestructura y estándares.

Sin embargo, las ventajas competitivas en la actividad empresarial que conllevan las facilidades tecnológicas que se implanten, no se reducen a obtener una mejora importante en el rendimiento del trabajo propio. Tampoco tiene porque plantearse únicamente como medio de integrar los elementos de la entidad que se encuentran dispersos. Estas facilidades tecnológicas llevan aparejadas una mayor y mejor relación con el resto de las organizaciones con las que se desenvuelve la empresa en el desarrollo de su negocio. La posibilidad de poder consultar los catálogos de los proveedores “on-line” y, porque no, realizar pedidos directamente manejando una información siempre actualizada, permite una agilización de los procesos que forzosamente se trasladará a los clientes propios, a los que se podrá responder inmediatamente sobre disponibilidad y precios de los productos que soliciten, por ejemplo. No obstante, iniciar el planteamiento de un escenario tan idílico suele acabar muy pronto, en el momento en que se plantea la compatibilidad de los sistemas a conectar y conseguir acuerdos para su gestión.

El rápido desarrollo y consiguiente implantación, arrolladora, de Internet como canal de comunicación para todo tipo de propósito, al alcance de cualquier usuario y corporación, ha incrementado espectacularmente las posibilidades de conexión y ha diluido los problemas técnicos que limitaban la globalización de las comunicaciones empresariales: complejidad/costes de infraestructura y estándares. Con Internet, las

empresas disponen ya del escenario tecnológico adecuado para generar y dimensionar la estructura de conexión interna/externa que les permitan potenciar y optimizar su actividad de negocio.

¿Merece la pena acceder remotamente a la empresa desde Internet?

Cuando un cliente plantea la posibilidad de poder acceder a su red utilizando Internet, la cuestión no es tan sencilla como colocar unos módems y contratar una cuenta con alguno de los proveedor de servicios disponibles. Hay que analizar la situación específica de cada cliente y valorar si realmente interesa este tipo de acceso de igual manera a como se plantearía una ampliación o reconfiguración de su red.

Los aspectos a tener en cuenta para evaluar la conveniencia de implantar este acceso podrían agruparse en tres grandes apartados:

-**Servicio:**
Quién usará el servicio, para qué lo usará, cuando lo usará. Si la información está distribuida o centralizada, lo que determina cómo se accede a ella. Tiempo medio de conexión. Restricciones y seguridad que hay que imponer. Labores de administración añadidas.

-**Comunicaciones:**
Protocolos de red utilizados, su compatibilidad con Internet y la seguridad que ofrecen. Módems necesarios, velocidad de las líneas, conexiones entre las distintas delegaciones.

-**Programas:**
Hay que considerar que para el desarrollo del servicio la utilización de uno u otro programa en el equipo cliente incide directamente en el rendimiento esperado y en el coste final de implantación de esta facilidad. No es lo mismo emplear un navegador, un programa propio o una aplicación desarrollada por terceros. Cada una de ellos tendrá su correspondiente incidencia en la formación de usuarios, volumen de datos transmitidos, adaptación de los datos, tiempo de instalación, licencias necesarias y otros aspectos más.

Planteamiento de las VPN

Sin embargo La Red, aunque proporciona el medio ideal para poder conectar distintos sistemas entre sí y con sus usuarios estén donde estén, de forma asequible económicamente y con total flexibilidad, en su propio planteamiento lleva implícita la característica de “público”. Esta circunstancia hace que no siempre sea Internet el escenario idóneo para que las compañías desplieguen su infraestructura de comunicación, debido, sobre todo, a los problemas de seguridad, fiabilidad y gestión que un soporte tan abierto lleva aparejado. No obstante, si Internet plantea el problema, Internet también ofrece la solución. La Red es un ente complemente “lógico”, que utiliza unos recursos de conexión públicos y que se sustenta en unas reglas, protocolos, de carácter universal que posibilita la relación entre aquellos que participan en ella. Si esa “abstracción” se reinterpreta con los protocolos adecuados, ese flujo de datos que inicialmente son de acceso público se convierte en un tráfico restringido al que sólo tendrá acceso aquellos que dispongan de los mecanismos adecuados para interpretarlos. Así surgen las Redes Privadas Virtuales. Una VPN (Virtual Private Network), es una red de carácter privado, perteneciente a una organización, que se extiende usando medios cuya propiedad o explotación corresponde a otras redes/entidades de ámbito público, codificando el tráfico que ha de transitar por esos intermediarios.

Esta idea, que parece ser la última “moda” tecnológica en redes, no es algo nuevo. Para conseguir esa privacidad virtual, una VPN transfiere los datos entre dos redes a través una red intermedia, mediante la encapsulación de los paquetes de datos dentro de los paquetes de otro protocolo, que en el caso de Internet se trata de TCP/IP. Y en ésta tecnología, desde hace ya algún tiempo, distintos fabricantes han desarrollado protocolos que realizan funciones de este tipo en lo que se conoce como “Tunelación” (Tunneling), y que han sido considerados más o menos estándares. Sin

embargo, los protocolos que utilizaban esta técnica de transferencia de datos eran usados y contemplados, en la mayoría de las ocasiones, más como pasarelas o gateways entre sistemas que utilizaban diferentes protocolos de transporte, que verdaderas vías de conexión. Las Redes Privadas Virtuales han conseguido su lugar al sol en la conectividad de las empresas al añadir una nueva dimensión al proceso de encapsulación utilizado por esos veteranos protocolos: la encriptación. Una VPN utiliza técnicas de tunelación encapsulando unos datos que son encriptados, de tal forma que esa información resulta ilegible para aquellos que son ajenos a la Red Privada Virtual establecida. Así, los datos pueden enrutarse por Internet con garantías suficientes de que sólo podrán ser interpretados en el destino, en donde los paquetes de datos serán extraídos y traducidos a su formato original. Los procedimientos de autentificación que se implementan en esta tecnología, refuerzan la seguridad frente a intrusos y usuarios no autorizados, proporcionando, además, los mecanismos de control necesarios para su total gestión.

Una VPN (Virtual Private Network), es una red de carácter privado, perteneciente a una organización, que se extiende usando medios cuya propiedad o explotación corresponde a otras redes/entidades de ámbito público, codificando el tráfico que ha de transitar por esos intermediarios.

VPN segura

Para que la Red Privada Virtual proporcione una comunicación segura se han de contemplar varios aspectos que ha de cubrir perfectamente el sistema que se implante.

Confidencialidad: Capaz de proteger la información
Integridad: Capaz de garantizar la validez de la información
Autentificación: Capacidad para verificar el origen de la información
No repudio: Debe garantizar el acceso al servicio
Identificación: Capaz de comprobar la identidad de usuarios.
Control de acceso: Debe permitir el control de los usuarios a los distintos recursos
Viabilidad: Capaz de asegurar la perfecta recepción de la información

Los beneficios que aportan estas técnicas de transmisión son evidentes en cuanto a la reducción de costes por equipamiento, abaratamiento sustancial de las comunicaciones a larga distancia, menor carga de operación y más facilidad y rapidez en la conectividad al simplificar la estructura WAN a soportar. Si la utilización de VPN no se ha extendido como cabía esperar, hay que achacarlo a factores ajenos completamente a la propia tecnología. Por un lado, la diversidad de protocolos y sistemas utilizados en las compañías, no siempre compatibles con las redes IP, dificultaba la interconexión de distintas redes. La proliferación de Proveedores de Servicios de Internet con dudosa infraestructura, por otro lado, dejaban una imagen de mala calidad de servicio, lentitud exasperante y pocas garantías sobre seguridad que obligaban a los responsables informáticos a posponer sus proyecto o buscar otras soluciones más caras, pero viables.

No obstante, la situación actual ha cambiado. Las estructuras empresariales actuales se organizan a fin de responder a un entorno cada vez más competitivo en un marco de globalización imparable, en donde las empresas están obligadas a desplegar una presencia lo más amplia posible. Para cubrir estas necesidades las empresas demandan soluciones informáticas y de comunicaciones que, en primer lugar, les permitan desarrollar su infraestructura y, en segundo lugar, que les aporte alguna ventaja competitiva, cubriendo perfectamente los aspectos críticos inherentes al proyecto diseñado, como son la seguridad, disponibilidad, calidad y capacidad, entre otros. La respuesta de la industria en el desarrollo de la tecnología de VPN, el avance de las propias comunicaciones y la clarificación que ha sufrido el mercado en operadores y proveedores de servicios, junto con el espectacular abaratamiento de tarifas, ha dado como resultado que las empresas de todo tipo de sectores se planteen la incorporación de Redes Privadas Virtuales, para el despliegue de su infraestructura,

como una alternativa más que factible frente a las soluciones disponibles hasta hace poco, difíciles de afrontar en costes y resultados eficaces.

La progresiva implantación de este tipo de tecnología de conectividad que contempla la red desde la perspectiva de una utilización de medios públicos como si fueran privados, en donde las VPN se limitan a proporcionar un soporte para las comunicaciones, ha provocado la revisión de distintos conceptos de red. Las soluciones de Redes Privadas Virtuales que se pueden encontrar en la actualidad cubren la Intranet, la Extranet y, también, el simple acceso remoto a la red de usuarios individuales. En el primer caso, la Intranet sobre VPN son conocidas como VPN Red a Red ó VPN Site-to-Site, en donde el alcance de la Intranet se extiende más allá de los límites tradicionales y engloba, bajo esta modalidad de conexión, redes que antes debían contemplarse como Intranet independientes y separadas, aunque fuera de la misma corporación. El concepto de Extranet bajo VPN, sin embargo, se mantiene, pero queda reservada ya para aquellos escenarios en donde la conexión se establece entre redes de distintas entidades que manteniendo su independencia de gestión y funcionamiento, quedan interconectadas para un mejor esfuerzo colaborativo en la actividad que realizan juntas las corporaciones implicadas: proveedores con clientes, con distribuidores y otras entidades. Situación ésta muy frecuente en proyectos de comercio electrónico, en donde organizaciones dispares se unen para lanzar proyectos de gran envergadura y cada una de las entidades se ocupa, por separado, de uno o varios de los aspectos de la gestión, pero se presentan y actúan conjuntamente, al estar sus sistemas interconectados con esta lógica. En lo que se refiere al acceso del cliente individual, son varios las denominaciones con las que se referencia a la configuración del acceso de los clientes utilizando comunicaciones de VPN. Las Redes Privadas Virtuales a las que acceden los usuarios mediante accesos remotos son conocidas como Client-to-Site, Cliente-a-Red, o también como Dial VPN.

Los escenarios en donde es viable la creación de Redes Privadas Virtuales, suelen escoger entre tres tipos básicos de configuración. Uno de ellos, consiste en crear los túneles IP entre usuario y red corporativa directamente entre ellos, es decir entre el ordenador del cliente con línea directa con el cortafuegos de la empresa. En este caso todo el proceso de creación y gestión de la comunicación está bajo el control de la propia compañía. Un segundo caso, plantea la utilización de las líneas de un proveedor de servicios intermedio que es quien habilita la conexión entre cliente y cortafuegos de la empresa. La creación del túnel y su gestión queda en manos del proveedor de servicios. En el tercer caso, se plantea que los túneles IP se crea entre redes o entre cliente y corporación sobre las líneas públicas de la infraestructura de Internet directamente en el acceso que tiene la compañía a La Red, o bien mediante el alquiler a un proveedor de servicios, de líneas con infraestructura de Internet pero que están separadas de ese ámbito. El control en la creación y gestión del circuito VPN está en el lado de la empresa, el proveedor de servicios sólo mantiene abierto el medio de comunicación. En los escenarios contemplados, es frecuente que las conexiones RSDI, Frame Relay o ATM utilizadas, se diferencie el tráfico entre los distintos usuarios, situación cotidiana cuando la gestión de la VPN la lleva el proveedor de servicios.

Funcionamiento.

En su funcionamiento, las Redes Privadas Virtuales no tienen porque circunscribirse a TCP/IP. Se puede trabajar y formar túneles con los principales protocolos de transporte utilizados en la actualidad. IPX, Appletalk, SNA o

Para los protocolos que trabajan en el nivel dos, un túnel se plantea de manera similar como se plantea una sesión. Los extremos deben aceptar el túnel que se establece entre ellos y negociar la configuración de las variables implicadas en la transmisión que se va a producir entre ellos.

DECnet, como algunos de los protocolos que soportan plenamente esta forma de operar. Sin embargo, con la pila de protocolos de Internet se consigue los mejores resultados en cuanto al alcance efectivo de red tipo WAN que se pueden requerir.

Estándares para Redes Privadas Virtuales

El número de RFC relacionadas con VPN es elevado porque están implicadas distintas tecnologías que se entrelazan entre sí: Protocolos de seguridad, de establecimiento de conexión, algoritmos de encriptación y autenticación son algunos de los elementos que se contemplan en el desarrollo de esta tecnología.

RFC 2401 - RFC 2406 - RFC 2412 - RFC 2405 - RFC 2404 - RFC 2085 - RFC 2661
RFC 2411 - RFC 2402 - RFC 2367 - RFC 2451 - RFC 2857 - RFC 2393 - RFC 2888
RFC 2521 - RFC 2407 - RFC 2522 - RFC 2104 - RFC 2410 - RFC 2394 - RFC 2809
RFC 2709 - RFC 2408 - RFC 2423 - RFC 2202 - RFC 1828 - RFC 2395
RFC 2409 - RFC 2523 - RFC 2403 - RFC 1829 - RFC 2637 - RFC 2764

Si tunelación es el método para crear la red virtual, túnel es el camino lógico por el que los datos son enrutados desde un extremo a otro del circuito que se crea. Para que un túnel pueda establecerse es necesario que los extremos implicados utilicen el mismo protocolo de tunelación. Estos protocolos trabajan en los niveles dos y tres del modelo de conectividad de OSI. En el nivel dos, enlace de datos, se encuentran protocolos como PPTP, Protocolo de Tunelación Punto a Punto, L2TP, Protocolo de Tunelación de la Capa 2, y L2F, Reenvio de Capa 2, en donde su unidad de trabajo es la trama. En el nivel tres, en el nivel de red, se encuentra el protocolo IPSec, que emplea como unidad de funcionamiento el paquete.

La diferencia entre los protocolos de uno y otro nivel reside en el grado de mantenimiento del túnel que hacen respectivamente. Los protocolos del nivel dos, el corredor virtual de datos debe ser creado, mantenido y terminado. Los protocolos de nivel tres asumen que todas estas operaciones se realizan de forma independiente, ajena a su funcionamiento. Los protocolos de nivel dos son los encargados de mantener túneles mediante conexiones vía MODEM, mientras que los protocolos de nivel tres están orientados más a la conexión desde la propia red.

PPTP-L2TP, iguales pero distintos

Si bien los protocolos PPTP y L2TP tienen un mismo propósito de cara a la VPN, presentan diferencias sustanciales en cuanto a capacidad y operación. Entre las diferencias más significativas que pueden existir entre ambos destaca que mientras PPTP sólo opera sobre redes IP, L2TP sólo necesita que se le proporcione una conexión punto a punto, ya que puede operar sobre IP, con el protocolo UDP, con circuitos virtuales de X.25 o en ATM. Tambien, L2TP ofrece mayor flexibilidad que PPTP a la hora de gestionar túneles. Mientras que el segundo sólo puede ocuparse de uno cada vez, el primero puede gestionar simultáneamente varios túneles en los nodos finales, lo que le permite adaptarse a los requerimientos impuestos por la calidad de servicio, QoS.

Para los protocolos que trabajan en el nivel dos, un túnel se plantea de manera similar como se plantea una sesión. Los extremos deben aceptar el túnel que se establece entre ellos y negociar la configuración de las variables implicadas en la transmisión que se va a producir entre ellos. Los datos circulan mediante protocolos basados en datagramas y el mantenimiento del corredor se realiza también con los correspondientes protocolos que actúan como mecanismos de gestión del circuito. Estas comunicaciones se inician con el establecimiento de la conexión serie, con un enlace punto a punto entre extremos. En esta fase inicial se produce la negociación del uso de la compresión y encriptación de datos y el método de autentificación empleado. Sin embargo, en el primer momento de establecer la comunicación no ocurren estos hechos. Una vez que se han acordado estos parámetros, el cliente presentará sus credenciales con las que se validará frente al servidor remoto, utilizando alguno de los protocolos diseñados para tal fin, como puede ser PAP o CHAP. El servidor remoto validará la entrada del

usuario comprobando su cuenta en la base de clientes propia o bien mediante un servidor Radius. Completada esta fase de la comunicación, comienza la transmisión de datos que son encapsulados en el origen, comprimidos y encriptados, para ser desencapsulados en el destino. Aquí intervienen los protocolos PPTP, L2F o L2TP.

Las comunicaciones por Red Privada Virtual en la capa tres, en el nivel de Red, se establece mediante el protocolo IPSec, Protocolo de Seguridad Internet, en donde la conexión entre los extremos ya se ha realizado y este protocolo se encarga de securizar el tráfico que circula por el túnel que se genera al utilizar este protocolo en la comunicación. El túnel que se forma mediante este protocolo se consigue mediante el formato del paquete utilizado en la transmisión de los datos. Aquí no hay in circuito propiamente dicho. El cliente encapsula los datos en un paquete IP normal que llegan al servidor que se encarga de desechar el paquete normal, desencapsular los datos y reenviarlos a su destinatario.

Para crear la VPN, se puede recurrir a dos modos de generar los túneles. Uno de estos métodos son los túneles voluntarios. Estos corredores se forman entre ordenadores de usuario o servidores de enrutamiento que utilizan software que actúa como agente cliente para establecer conexión virtual contra un servidor que tiene la función de ser el destino de la comunicación. En este caso, tanto los clientes como los servidores finales han de tener instalados y configurados los protocolos con los que entibar el camino, ya sea en conexiones series o por red. Las máquinas implicadas, tanto las finales como las intermedias, son de propósito general y no están específicamente diseñadas para operar con Redes Privadas Virtuales. Cuando se utilizan dispositivos dedicados, es cuando se habla de tunelación obligatoria o impuesta, en donde los servidores de destino están diseñados con capacidad para generar el túnel al recibir la comunicación del cliente. Estos dispositivos, reciben el nombre de Procesadores Front End, (FEP), cuando emplean el protocolo PPTP, Concentrador de Acceso, (LAC), cuando trabajan con L2TP o Pasarela de Seguridad IP cuando emplean IPSec en su funcionamiento.
El empleo de estos dispositivos como receptores de la conexión de los clientes es la característica que marca la obligatoriedad de emplear conexiones virtuales de túnel cuando se establece la comunicación entre los extremos, puesto que todos los datos que ellos reciben son inmediatamente redirigidos por los corredores que gestionan. En este caso, los clientes que inician la comunicación no tienen porque comprimir o encriptar datos, son estos dispositivos los que se encargan de formar el túnel desde el punto que ellos ocupan hasta el destino. Estos dispositivos, no obstante, suelen tener capacidadad para discriminar a los clientes y enrutar o no sus conexiones por túneles, así como la de poder dedicar caminos subterráneos específicos a unos u otros clientes. A diferencia de los túneles voluntarios, en los túneles obligatorios, los dispositivos que los gestionan, se puede manejar un mismo túnel para diferentes clientes.

Seguridad.

Pero el punto crítico de las Redes Privadas Virtuales no es la confección de túneles, si no la seguridad. Este aspecto se encuentra muy reforzado en esta tecnología ante la perspectiva de operar en un entorno completamente público. Además de los mecanismos para la autentificación de usuarios, el flujo de datos está protegido mediante encriptación y la posible interceptación del tráfico que circula por ese camino virtual está defendido por la propia fortaleza de los algoritmos de cifrado que se emplean. Estos mismos mecanismos están

Las comunicaciones por Red Privada Virtual en la capa tres, en el nivel de Red, se establece mediante el protocolo IPSec, Protocolo de Seguridad Internet, en donde la conexión entre los extremos ya se ha realizado y este protocolo se encarga de securizar el tráfico que circula por el túnel que se genera al utilizar este protocolo en la comunicación.

preparados para detectar posibles modificaciones en el flujo de información y rechazar los datos que hayan sido generados en fuentes no fiables.

Bien es cierto que estas funciones de seguridad, el proceso de los datos, implica el consumo de recursos de la red para su correcta aplicación y ello puede incidir directamente en el rendimiento general de los servicios prestados. Sin embargo, cuando se trata de acceso a servicios o recursos compartidos, la aplicación de procesos de encriptado no tiene una incidencia relevante, cosa que no ocurre cuando se trata de aplicaciones críticas que se han de ejecutar en tiempo real. Para estos casos más delicados, se recurre a la utilización de hardware específico, que ya se ha comentado, especializado en el cifrado del tráfico que ha de transitar por ellos que aportan una velocidad de proceso suficiente como para que no se vea afectada significativamente el ancho de banda disponible, ni el tiempo de tratamiento.

Las expectativas y, consiguiente, auge de ésta tecnología con la que abordar las comunicaciones desde una perspectiva más asequible, ha hecho que todos los fabricantes en componentes para red hayan incorporado en sus catálogos productos que incorporan funciones que posibilitan la implementación de Redes Privadas Virtuales. Tanto en hardware como en software. En lo que se refiere a componentes de conectividad para red, todos los principales fabricantes de dispositivos incluyen en ellos capacidades para trabajar según el modelo que plantea la VPN. routers, switches, dispositivos para acceso remoto entre otros, como elementos habituales de la red, pero también se han incorporado otros dispositivos orientados y especializados en esta tecnología, como pueden ser aparatos para la autenticación de usuarios y la encriptación de los datos que circulan por la Red Privada Virtual. Y este interés por la tecnología de los túneles también abarca a empresas dedicadas a la comunicación pero que su actividad principal no era la informática, como ocurre con algunas compañías especializadas en telefonía móvil que si bien no están sacando productos específicos para VPN, si siguen de cerca y contribuyen en su investigación, desarrollo y despliegue con la idea de incorporarlas en un futuro inmediato.

Consorcio VPN

A fin de promover la difusión para la implantación de Redes Privadas Virtuales y sus productos relacionados varios fabricantes de distintas áreas se han unido para formar VPNC, Virtual Private Networks Consortium, una entidad que surge con el único objetivo de servir de altavoz para la propagación de esta tecnología y como lugar de coordinación de los esfuerzos que realizan sus componentes, entre los que se encuentran Cisco, 3Com, Intel, Microsoft, Nokia y un largo etc. No tiene ninguna facultad para dictar estándares y, bien al contrario, los integrantes de esta organización están comprometidos en desarrollar sus productos según las normas del IETF, presentes y futuras.

En el otro lado, los desarrolladores de sistemas operativos de red tampoco han permanecido ajenos a las expectativas que ha generado la tecnología de VPN y han incorporado el correspondiente soporte para este nuevo modo de entender las vías de comunicación. Para Microsoft, la tecnología y forma de operación que sostiene una Red Privada Virtual ha sido completamente incorporada en la plataforma de sistema operativo a partir de Windows 2000, como no podía ser de otra manera. Con el propio sistema operativo se incorpora todo lo necesario para poder operar en este tipo de redes, tanto desde la perspectiva del cliente como en el lado del servidor, contemplando su utilización directa dentro de la propia red LAN como en conexiones asíncronas, con accesos remotos vía MODEM.

La disponibilidad de esta capacidad de la red bajo Windows 200X se consigue mediante la configuración oportuna de los correspondientes puertos durante la instalación/configuración del servicio de Enrutado y Acceso Remoto del servidor de Microsoft. Este servicio habilita la utilización de los protocolos implicados en la tunelación, PPTP, L2TP, IPSec y EAP Los dos primeros como soporte de la comunicación y los últimos como mecanismos de privacidad y seguridad que amplian

el soporte utilizado en la saga anterior de sistemas operativos de este fabricante, Windows 9X y NT 4.0. Los algoritmos de encriptación contemplados son todos los que se pueden requerir, lo que asegura una total compatibilidad de esta plataforma de Microsoft con cualquier cliente que pueda acceder a la Red Privada Virtual echa en Windows 200X. La gestión del servicio se realiza mediante el nuevo interfaz de administración que incorpora Windows 2000, Microsoft Management Console, MMC, y su configuración previa se realiza mediante un asistente que simplifica y facilita la tarea. El control del servicio de VPN puede ser administrado mediante paquetes de directivas que se pueden asociar a grupos de usuarios y máquinas en función de su ubicación dentro del Directorio Activo, proporcionando una administración centralizada del entorno.