UNIVERSIDAD AMERICANA

Seguridad en el Perímetro

Unidad VI – Redes de Comunicación

Ing. Luis Müller

2011

Esta es una recopilación de la teoría referente a la asignatura Redes de Comunicación, a ser estudiada en clases con los alumnos, y que servirá como base para su aplicación también en clases en ejercicios prácticos.

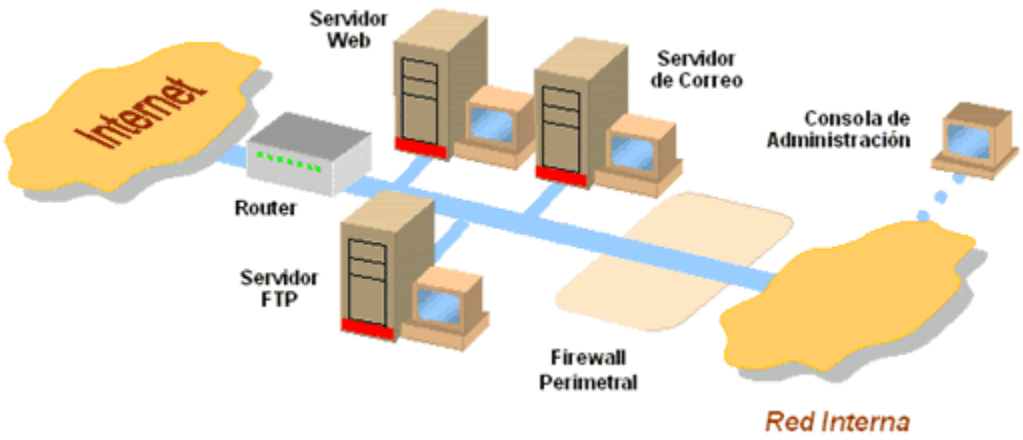
Unidad VI - Seguridad en el perímetro

Conceptos básicos. Perímetros y conceptos asociados. Firewalling. Tipos de firewalls. Accesos remotos. VPNs y túneles.

Seguridad perimetral

La **seguridad perimetral** es un concepto emergente que asume la integración de elementos y sistemas, tanto electrónicos como mecánicos, para la protección de perímetros físicos, detección de tentativas de intrusión y/o disuasión de intrusos en instalaciones especialmente sensibles. Entre estos sistemas cabe destacar los radares tácticos, video sensores, vallas sensorizadas, cables sensores, barreras de microondas e infrarrojos, concertinas, etc.

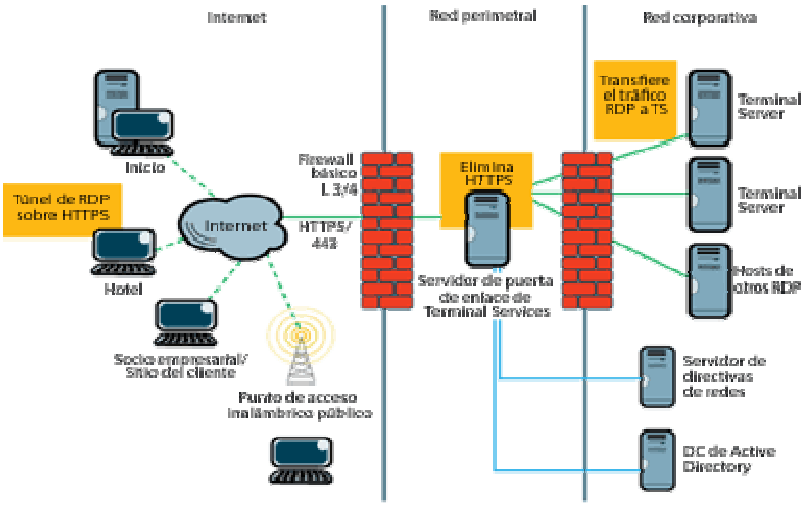
Los sistemas de seguridad perimetral pueden clasificarse según la geometría de su cobertura (volumétricos, superficiales, lineales, etc.), según el principio físico de actuación (cable de fibra óptica, cable de radiofrecuencia, cable de presión, cable microfónico, etc.) o bien por el sistema de soportación (autosoportados, soportados, enterrados, detección visual, etc.).



También cabe destacar la clasificación dependiendo del medio de detección. En esta se clasificarían en:

Sistemas Perimetrales Abiertos: Los que dependen de las condiciones ambientales para detectar. Como ejemplo de estos son la video vigilancia, las barreras infrarrojas, las barreras de microondas. Esta característica provoca falsas alarmas o falta de sensibilidad en condiciones ambientales adversas.

Sistemas Perimetrales Cerrados: Los que no dependen del medio ambiente y controlan exclusivamente el parámetro de control. Como ejemplo de estos son los antiguos cables microfónicos, la fibra óptica y los piezo-sensores. Este tipo de sensores suelen ser de un coste más elevado.

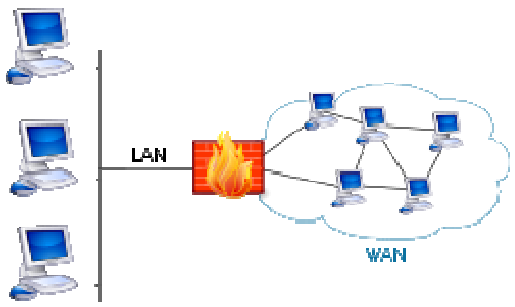


Su aplicación destaca principalmente en Seguridad Nacional (instalaciones militares y gubernamentales, fronteras, aeropuertos, etc.) e instalaciones privadas de alto riesgo (centrales nucleares, sedes corporativas, residencias VIP, etc.).

CORTAFUEGOS O *FIREWALLS*

Los cortafuegos son sistemas de seguridad para evitar incendios que consisten en establecer una barrera física, no inflamable, separando la zona que queremos proteger de la zona de donde puede venir el fuego. En informática, un cortafuego es cualquier sistema utilizado para separar una máquina o una subred del resto de la red para protegerla de intrusiones externas que puedan suponer una amenaza a la seguridad. La zona protegida se llama "perímetro de seguridad" y la protección se realiza separándola de una zona externa, no protegida, llamada zona de riesgo.

Cortafuegos (informática)



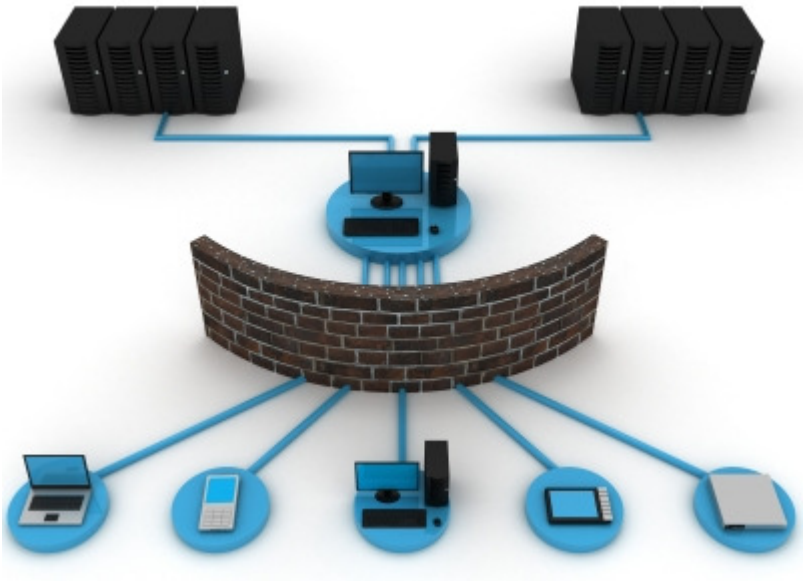
Evidentemente la forma de aislamiento más efectiva para cualquier política de seguridad consiste en el aislamiento físico, es decir, no tener conectada la máquina o la subred a otros equipos o a Internet. Pero de lo que se trata es, precisamente, de proteger datos archivados que tienen que estar disponibles para ser transportados.

Se llama **filtrado de paquetes** la acción de denegar o permitir el flujo de información entre la red interna, protegida con el cortafuegos, y el resto de Internet. Este filtrado se hace de acuerdo a unas normas predefinidas. El filtrado también se conoce como *screening*, y a los dispositivos que lo implementan se les denomina *chokes*; el *choke* puede ser la máquina bastión o un elemento diferente.

Un **proxy** es un programa que permite o niega el acceso a una aplicación determinada entre dos redes. Los clientes *proxy* se comunican sólo con los servidores *proxy*, que autorizan las peticiones y las envían a los servidores reales, o las deniegan y las devuelven a quien las solicitó.

En casi todos los cortafuegos existen al menos un *choke* y una *máquina bastión*, aunque también puede ser considerado cortafuegos a un simple *router* que filtre paquetes.

Los **cortafuegos personales** son programas que se instalan de forma residente en nuestra computadora y que permiten filtrar y controlar la conexión a la red. En general necesitan un conocimiento adecuado de nuestra computadora, pues en la actualidad son muchos los programas que realizan conexiones a la red y que son necesarios. Es por ello que no son recomendables para usuarios inexpertos ya que podrían bloquear programas necesarios (incluso hasta la propia posibilidad de navegación por Internet), aunque siempre se tenga a mano la posibilidad de desactivarlos.



Ventajas de un cortafuegos

Bloquea el acceso a personas no autorizadas a redes privadas.

Limitaciones de un cortafuegos

Las limitaciones se desprenden de la misma definición del cortafuegos: filtro de tráfico. Cualquier tipo de ataque informático que use tráfico aceptado por el cortafuegos (por usar puertos TCP abiertos expresamente, por ejemplo) o que sencillamente no use la red, seguirá constituyendo una amenaza. La siguiente lista muestra algunos de estos riesgos:

Un cortafuegos no puede proteger contra aquellos ataques cuyo tráfico no pase a través de él.

El cortafuegos no puede proteger de las amenazas a las que está sometido por ataques internos o usuarios negligentes. El cortafuegos no puede prohibir a espías corporativos copiar datos sensibles en medios físicos de almacenamiento (discos, memorias, etc.) y sustraerlas del edificio.

El cortafuegos no puede proteger contra los ataques de ingeniería social.

El cortafuegos no puede proteger contra los ataques posibles a la red interna por virus informáticos a través de archivos y software. La solución real está en que la organización debe ser consciente en instalar software antivirus en cada máquina para protegerse de los virus que llegan por cualquier medio de almacenamiento u otra fuente.

El cortafuego no protege de los fallos de seguridad de los servicios y protocolos cuyo tráfico esté permitido. Hay que configurar correctamente y cuidar la seguridad de los servicios que se publiquen en Internet.

Políticas del cortafuegos

Hay dos políticas básicas en la configuración de un cortafuegos que cambian radicalmente la filosofía fundamental de la seguridad en la organización:

Política restrictiva: Se deniega todo el tráfico excepto el que está explícitamente permitido. El cortafuegos obstruye todo el tráfico y hay que habilitar expresamente el tráfico de los servicios que se necesiten.

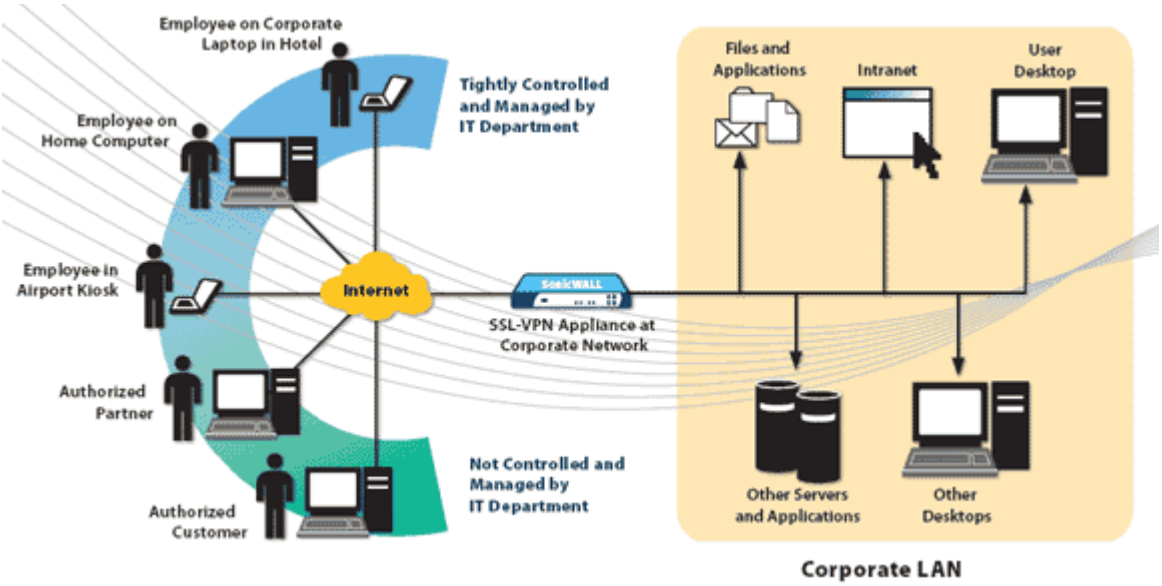
Política permisiva: Se permite todo el tráfico excepto el que esté explícitamente denegado. Cada servicio potencialmente peligroso necesitará ser aislado básicamente caso por caso, mientras que el resto del tráfico no será filtrado.

La política restrictiva es la más segura, ya que es más difícil permitir por error tráfico potencialmente peligroso, mientras que en la política permisiva es posible que no se haya contemplado algún caso de tráfico peligroso y sea permitido por omisión.

Acceso remoto

En redes de computadoras, acceder desde una computadora a un recurso ubicado físicamente en otra computadora, a través de una red local o externa (como internet).

En el acceso remoto se ven implicados protocolos para la comunicación entre máquinas, y aplicaciones en ambas computadoras que permitan recibir/enviar los datos necesarios. Además deben contar con un fuerte sistema de seguridad (tanto la red, como los protocolos y las aplicaciones).



Remotamente se puede acceder prácticamente a cualquier recurso que ofrece una o más computadoras.

Se pueden acceder a archivos desde dispositivos periféricos (como impresoras), configuraciones, etc. Por ejemplo, se puede acceder a un servidor de forma remota para configurarlo, controlar el estado de sus servicios, transferir archivos, etc.

Existen múltiples programas que permiten controlar una computadora remotamente, entre ellos uno de los más populares es el VNC, que es gratuito y libre. También existen aplicaciones web que permiten el acceso remoto a determinados recursos utilizando sólo un navegador web, ya sea a través de internet o cualquier otra red.

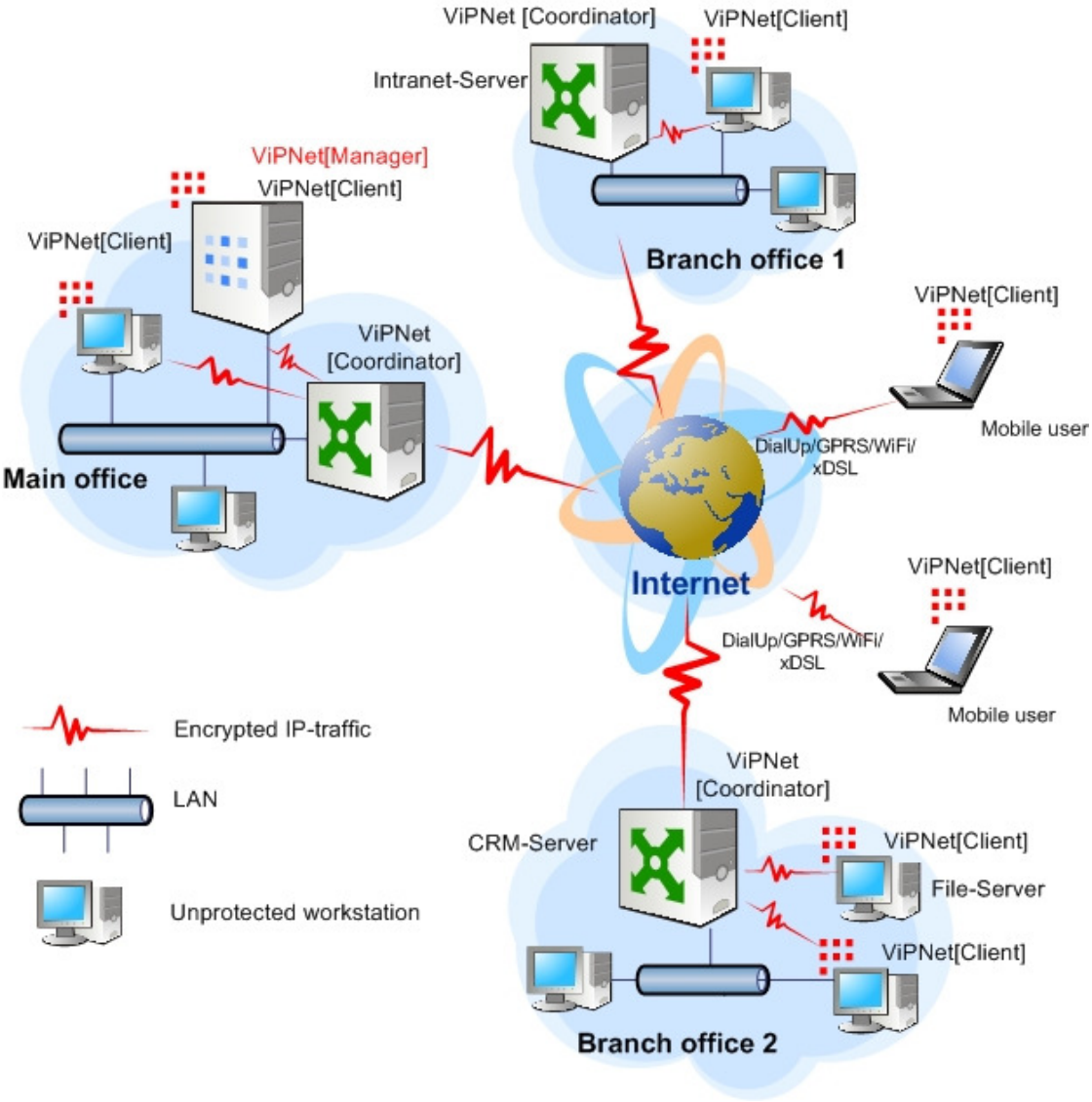
Otra forma fácil (porque es gráfica) de acceso remoto es a través de un Escritorio remoto.

Existen programas para el acceso remoto a través de comandos de texto, pero suelen ser más complicados de usar.

Red privada virtual

Una **red privada virtual** o **VPN** (siglas en inglés de *virtual private network*), es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet.

Ejemplos comunes son, la posibilidad de conectar dos o más sucursales de una empresa utilizando como vínculo Internet, permitir a los miembros del equipo de soporte técnico la conexión desde su casa al centro de cómputo, o que un usuario pueda acceder a su equipo doméstico desde un sitio remoto, como por ejemplo un hotel. Todo ello utilizando la infraestructura de Internet.



Características básicas de la seguridad

Para hacerlo posible de manera segura es necesario proporcionar los medios para garantizar la autenticación, integridad y confidencialidad de toda la comunicación:

Autentificación y autorización: ¿Quién está del otro lado? Usuario/equipo y qué nivel de acceso debe tener.

Integridad: de que los datos enviados no han sido alterados. Para ello se utiliza *funciones de Hash*. Los algoritmos de hash más comunes son los *Message Digest* (MD2 y MD5) y el *Secure Hash Algorithm* (SHA).

Confidencialidad: Dado que sólo puede ser interpretada por los destinatarios de la misma. Se hace uso de algoritmos de cifrado como *Data Encryption Standard* (DES), Triple DES (3DES) y *Advanced Encryption Standard* (AES).

No repudio: es decir, un mensaje tiene que ir firmado, y el que lo firma no puede negar que el mensaje lo envió él o ella.

Requerimientos básicos

Identificación de usuario: las VPN deben verificar la identidad de los usuarios y restringir su acceso a aquellos que no se encuentren autorizados.

Codificación de datos: los datos que se van a transmitir a través de la red pública (Internet), antes deben ser cifrados, para que así no puedan ser leídos. Esta tarea se realiza con algoritmos de cifrado como DES o 3DES que sólo pueden ser leídos por el emisor y receptor.

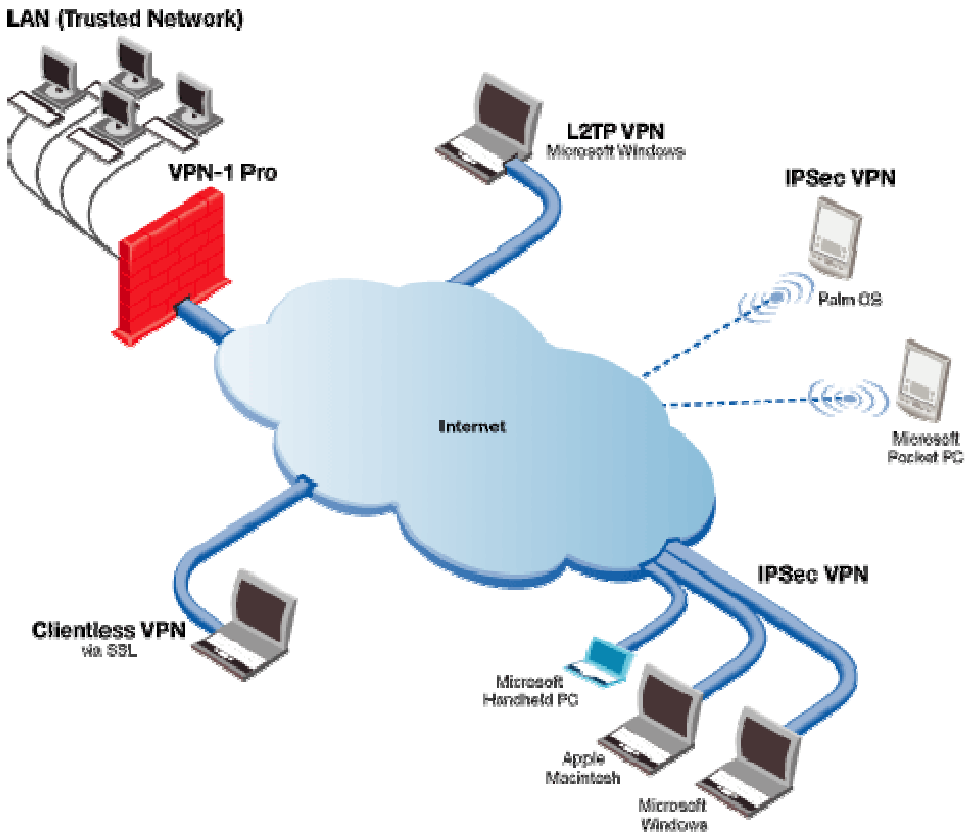
Administración de claves: las VPN deben actualizar las claves de cifrado para los usuarios.

Tipos de VPN

Básicamente existen tres arquitecturas de conexión VPN:

VPN de acceso remoto

Es quizás el modelo más usado actualmente, y consiste en usuarios o proveedores que se conectan con la empresa desde sitios remotos (oficinas comerciales, domicilios, hoteles, aviones preparados, etcétera) utilizando Internet como vínculo de acceso. Una vez autenticados tienen un nivel de acceso muy similar al que tienen en la red local de la empresa. Muchas empresas han reemplazado con esta tecnología su infraestructura dial-up (módems y líneas telefónicas).

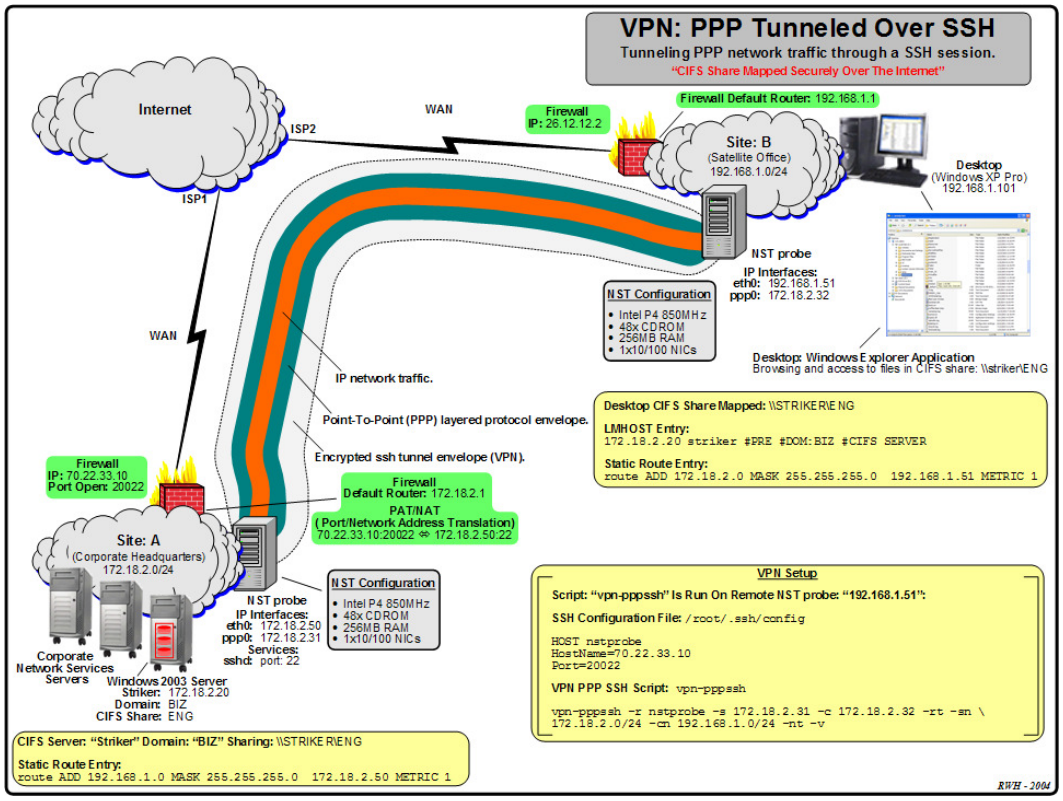


VPN punto a punto

Este esquema se utiliza para conectar oficinas remotas con la sede central de la organización. El servidor VPN, que posee un vínculo permanente a Internet, acepta las conexiones vía Internet provenientes de los sitios y establece el túnel VPN. Los servidores de las sucursales se conectan a Internet utilizando los servicios de su proveedor local de Internet, típicamente mediante conexiones de banda ancha. Esto permite eliminar los costosos vínculos punto a punto tradicionales (realizados comúnmente mediante conexiones de cable físicas entre los nodos), sobre todo en las comunicaciones internacionales. Es más común el siguiente punto, también llamado tecnología de túnel o *tunneling*.

Tunneling

La técnica de tunneling consiste en encapsular un protocolo de red sobre otro (protocolo de red encapsulador) creando un túnel dentro de una red de computadoras. El establecimiento de dicho túnel se implementa incluyendo una PDU determinada dentro de otra PDU con el objetivo de transmitirla desde un extremo al otro del túnel sin que sea necesaria una interpretación intermedia de la PDU encapsulada. De esta manera se encaminan los paquetes de datos sobre nodos intermedios que son incapaces de ver en claro el contenido de dichos paquetes. El túnel queda definido por los puntos extremos y el protocolo de comunicación empleado, que entre otros, podría ser SSH.

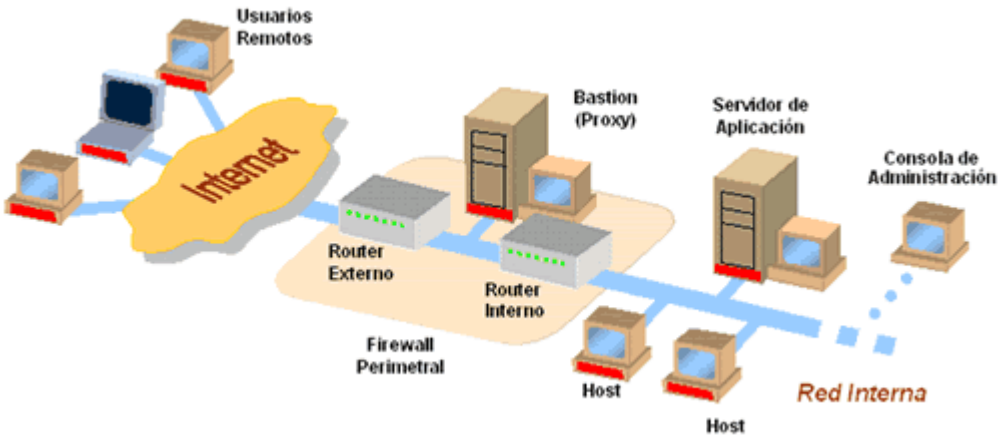


VPN over LAN

Este esquema es el menos difundido pero uno de los más poderosos para utilizar dentro de la empresa. Es una variante del tipo "acceso remoto" pero, en vez de utilizar Internet como medio de conexión, emplea la misma red de área local (LAN) de la empresa. Sirve para aislar zonas y servicios de la red interna. Esta capacidad lo hace muy conveniente para mejorar las prestaciones de seguridad de las redes inalámbricas (WiFi).

Un ejemplo clásico es un servidor con información sensible, como las nóminas de sueldos, ubicado detrás de un equipo VPN, el cual provee autenticación adicional más el agregado del cifrado, haciendo posible que sólo el personal de recursos humanos habilitado pueda acceder a la información.

Otro ejemplo es la conexión a redes WIFI haciendo uso de túneles cifrados IPSEC o SSL que además de pasar por los métodos de autenticación tradicionales (WAP, WEP, MAcaddress, etc.) agregan las credenciales de seguridad del túnel VPN creado en la LAN internas o externas.



Implementaciones

El protocolo estándar de hecho es el IPSEC, pero también tenemos PPTP, L2F, L2TP, SSL/TLS, SSH, etc. Cada uno con sus ventajas y desventajas en cuanto a seguridad, facilidad, mantenimiento y tipos de clientes soportados.

Actualmente hay una línea de productos en crecimiento relacionada con el protocolo SSL/TLS, que intenta hacer más amigable la configuración y operación de estas soluciones.

Las soluciones de hardware casi siempre ofrecen mayor rendimiento y facilidad de configuración, aunque no tienen la flexibilidad de las versiones por software.

Las aplicaciones VPN por software son las más configurables y son ideales cuando surgen problemas de interoperabilidad en los modelos anteriores. Obviamente el rendimiento es menor y la configuración más delicada, porque se suma el sistema operativo y la seguridad del equipo en general.

En ambos casos se pueden utilizar soluciones de firewall ("cortafuego"), obteniendo un nivel de seguridad alto por la protección que brinda, en pérdida del rendimiento.

Ventajas

- Integridad, confidencialidad y seguridad de datos.
- Las VPN reducen los costos y son sencillas de usar.
- Facilita la comunicación entre dos usuarios en lugares distantes.
- Se utiliza más en campus de universidades.

Tipos de conexión

Conexión de acceso remoto

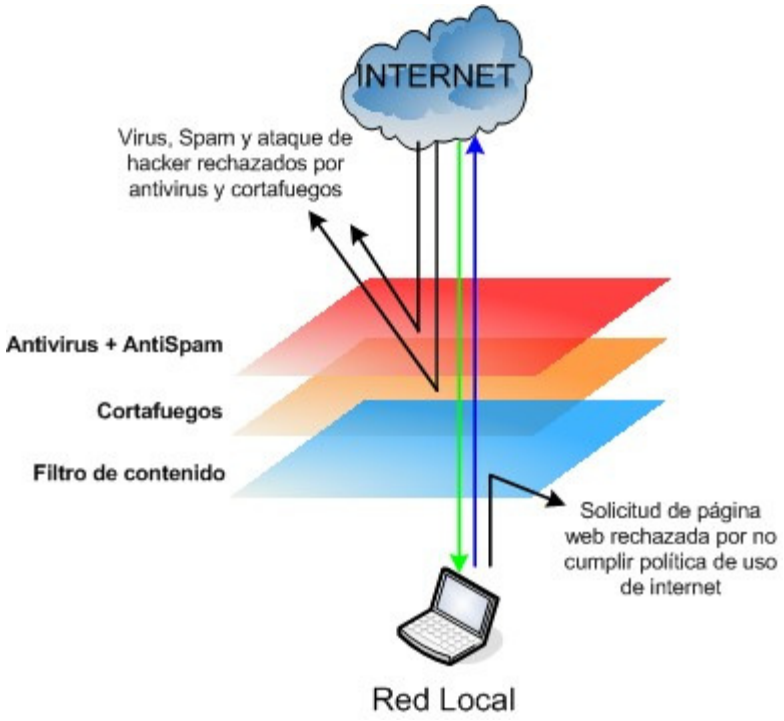
Una conexión de acceso remoto es realizada por un cliente o un usuario de una computadora que se conecta a una red privada, los paquetes enviados a través de la conexión VPN son originados al cliente de acceso remoto, y éste se autentifica al servidor de acceso remoto, y el servidor se autentifica ante el cliente.

Conexión VPN router a router

Una conexión VPN router a router es realizada por un router, y este a su vez se conecta a una red privada. En este tipo de conexión, los paquetes enviados desde cualquier router no se originan en los routers. El router que realiza la llamada se autentifica ante el router que responde y este a su vez se autentica ante el router que realiza la llamada y también sirve para la intranet.

Conexión VPN firewall a firewall

Una conexión VPN firewall a firewall es realizada por uno de ellos, y éste a su vez se conecta a una red privada. En este tipo de conexión, los paquetes son enviados desde cualquier usuario en Internet. El firewall que realiza la llamada se autentifica ante el que responde y éste a su vez se autentifica ante el llamante..


INTERNET
Virus, Spam y ataque de hacker rechazados por antivirus y cortafuegos
Antivirus + AntiSpam
Cortafuegos
Filtro de contenido
Solicitud de página web rechazada por no cumplir política de uso de internet
Red Local