VPN: Seguridad en sus Comunicaciones

En la actualidad tanto las empresas como los organismos oficiales y otras entidades presentan una estructura distribuida, disponiendo de sedes en puntos distantes. La llegada de Internet abre las puertas a la comunicación entre estos puntos. Las Redes Privadas Virtuales proporcionan soluciones para que dicha comunicación sea fiable y segura

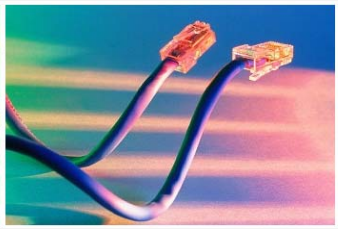
Funcionalidades

- Utilizar una única conexión externa para acceso a Internet e interconexión con las delegaciones, sedes de forma segura
- Eliminación de la necesidad de utilizar líneas dedicadas entre dos puntos
- Disminución de costes asociados a las líneas de interconexión entre delegaciones y sedes
- Posibilidad de expandir los límites de la Intranet al ámbito de Internet.
- Envío de información entre sedes y delegaciones de forma segura a través de protocolos de encriptación (p.e. IPSEC)
- Implantación de topologías virtuales adaptadas a las necesidades de la entidades interconectadas en cada momento.
- Posibilidad de intercambio de información de forma segura con proveedores y/u otros clientes.
- Establecimiento de canales de comunicación seguros para personal desplazado. Teletrabajo
- Ahorro de costes al poder utilizar tarifas de interconexión Internet. (p. Ej. ADSL)
- Tiempos de implantación reducidos.
- Acceso rápido y seguro a todos los servicios de una Intranet.

VPN la Solución Perfecta para la comunicación entre sedes

La implantación de una VPN "Red Privada Virtual", nos permite:

- Establecimiento de comunicaciones seguras entre distintos puntos de una red mediante la utilización de canales públicos (Internet)
- Conseguir una comunicación transparente entre los usuarios de todas las delegaciones.
- Acceso a los recursos de la Intranet desde cualquier punto de Internet manteniendo los niveles de seguridad adecuados.


Objetivos y ventajas. Implantación de una VPN

El principal objetivo a la hora de montar una VPN es conseguir una red a un coste asequible en infraestructura y posterior mantenimiento, pero al mismo tiempo proteger toda la información transmitida.

El implantar una red con enlaces dedicados punto a punto, normalmente alquilados, sería una solución excesivamente costosa, y muy dependiente del operador. La solución que ofrece Divisa IT es la de configurar una Red Privada Virtual sobre la red pública Internet, optimizando de esta forma los recursos y reduciendo costes.

Con una Red Privada Virtual establecemos una serie de túneles entre los centros remotos y la sede principal, permitiendo el acceso a los servidores de la Intranet central a todos los usuarios de cada delegación como si se encontrasen en una misma red local.

Los principales beneficios que obtenemos con esta solución son: privacidad (todos los datos transmitidos van encriptados, por lo que se garantiza la confidencialidad de los mismos), integridad (existen mecanismos por los que se garantiza el mensaje no ha sido modificado durante el envío), autenticación (el emisor firma sus mensajes digitalmente, de forma que el receptor puede comprobar que realmente fue enviado por él).

Se trata de una solución para sus comunicaciones, sencilla de implantar y que proporciona beneficios a corto plazo.

Ficha Técnica

- Encriptación IPSEC
  - Cifrado mixto simétrico-asimétrico
  - Intercambio de claves con Diffie-Hellman
  - Encriptación DES / 3DES
  - Validación del mensaje mediante hash SHA, MD5
- Validación de claves mediante certificados digitales
- Solución global PKI.
- Utilización de tokens para identificación de usuario.
- Firewall stateful inspection
  - DMZ (según modelos).
  - Traducción de direcciones NAT/PAT
  - Detección de Intrusos.
  - Posibilidad de filtrado URL.

Aspectos relevantes en la implantación

- **Número de usuarios en cada centro**
- **Consumo de ancho de banda**
- **Número de delegaciones a interconectar**
- **Tipo de comunicación a establecer**
  - **Remoto Central**
  - **Todos con Todos**
- **Tipos de accesos que se emplearán en la conexión**
  - **ADSL**
  - **Cable**
  - **RDSI**
  - **Modem**
- **Número de teletrabajadores**

Divisa IT S.A.
Parque Tecnológico de Boecillo
47151 Boecillo (Valladolid)
Tel.- +34 983 546 600
Fax.- +34 983 546 602
www.divisait.com
divisait@divisait.com

Solución Divisa IT

Para la creación de estos túneles entre delegaciones, Divisa iT selecciona equipamiento con doble funcionalidad: servicio VPN + Firewall, incrementando de esta forma, el nivel de seguridad frente a posibles accesos no deseados. La experiencia y el conocimiento de Divisa IT sobre una amplia gama de productos de diversos fabricantes, garantiza la elección del producto que mejor se adapte a las necesidades del cliente.

Para dar solución a los usuarios móviles cuyo puesto de trabajo puede variar de localización geográfica y que necesitan acceder a la red corporativa y a los datos que hay en ella, se establecerán conexiones seguras puntuales e independientes del modo de acceso (modem, RDSI, ADSL, red de cable,...).

El usuario móvil se identificará a través de una clave de acceso o "token" (llave, tarjeta inteligente,...) que también se empleará para encriptar y firmar digitalmente sus comunicaciones.

El "token" es un mecanismo de doble seguridad, además de ser necesario el elemento físico, es imprescindible el PIN de usuario.

Conclusiones

La utilización de una Red Privada Virtual, además de proteger las comunicaciones nos permite optimizar los recursos utilizando una única línea para el acceso a Internet y para las comunicaciones con las delegaciones, eliminando de esta forma la necesidad de contratar líneas punto a punto para ello.

La seguridad es uno de los factores fundamentales y de éxito de la utilización de esta tecnología, ya que garantiza en todo momento que sus comunicaciones sean fiables.

La solución de Divisa IT integra la característica de Firewall como elemento de importante valor añadido. Se trata de un Firewall *"stateful inspection"* con la posibilidad de activación de filtrado por URL y detección de intrusismos entre otras funcionalidades.

Divisa IT ofrece también soluciones PKI para garantizar la seguridad en las comunicaciones a través de su VPN.

Con el uso de protocolos de encriptación, la información que atraviesa Internet lo hace de forma cifrada, de modo que sólo el destinatario seleccionado será capaz de leer la misma. Incluso en el caso de escuchas no permitidas, no será posible la recuperación de la información original de forma legible sin conocer las claves que sólo los interlocutores legítimos poseen.

Se establecen topologías virtuales entre las delegaciones, adecuadas siempre a las necesidades del momento y permitiendo la inclusión de nuevas sedes o centros remotos de forma rápida y transparente al usuario.