tecnimap 2002
www.tecnimap.com
VII JORNADAS SOBRE TECNOLOGÍAS DE LA INFORMACIÓN PARA LA MODERNIZACIÓN DE LAS ADMINISTRACIONES PÚBLICAS
A CORUÑA
15, 16, 17 y 18 de octubre de 2002
Palacio de Congresos y de la Ópera
Ponencias

Cómo afrontar la Seguridad en Redes Abiertas: Consideraciones Técnicas y Escenarios.

Encarnación Sánchez Vicente

1. INTRODUCCIÓN

No cabe ninguna duda que en nuestros días, la información es la clave. Esta información tiene que fluir de forma rápida, pero a la vez tiene que tener el mayor alcance posible. Aprovechando las redes públicas como Internet, podemos cumplir estos objetivos, pero no es suficiente.

Cada día más, la seguridad es un factor importante para el desarrollo de los negocios a través de la red. Los nuevos modelos de negocio hacen que el alcance de una empresa traspase las barreras geográficas tanto a nivel local como nacional e internacional. Por este motivo, la interconexión de los diferentes puntos de negocio de una empresa han de estar perfectamente sincronizados y conectados para el acceso a esta información. Además, adquieren un papel importante los accesos a la red corporativa de una empresa por parte del personal itinerante, así como de los clientes y proveedores.

Ayuntamiento de A Coruña
XUNTA DE GALICIA

Hemos de proporcionar una solución de interconexión que nos permita proveer de confidencialidad, seguridad y privacidad a esta información, así como los medios necesarios para evitar "problemas no deseados" y garantizar a los usuarios servicio la mayor parte del tiempo.

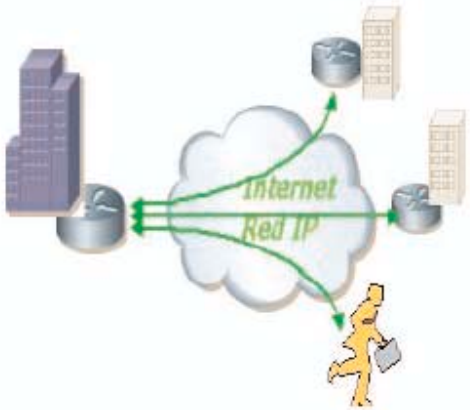
Estos puntos serán los que abordaremos en profundidad a lo largo del presente documento.

2. EVOLUCION DE LAS REDES DE DATOS EN LOS ULTIMOS AÑOS

No hace mucho tiempo, la comunicación de las diferentes oficinas remotas hacia la sede central de una determinada empresa se llevaba a cabo apoyándose en la tecnología Frame Relay como se puede observar en la figura.

El usuario debía contratar al operador correspondiente una serie de líneas Frame Relay de una determinada capacidad, donde lógicamente el ancho de banda contratado para las líneas que dan servicio a las delegaciones remotas era mucho menor que el de la línea asociada a la sede central, que debía ser mayor pues tiene que englobar todo el tráfico de las diferentes delegaciones remotas. Este tipo de tecnología no permitía dar una solución a aquellos usuarios móviles que por motivos de trabajo tenían que desplazarse continuamente, además de ser una solución cara.

Hoy en día, se puede abordar este mismo escenario pero apoyándose en redes privadas IP ó redes públicas compartidas como Internet.



Donde su principal ventaja es el ahorro de costes que supone para el usuario, además de ofrecer una posible solución para el personal itinerante de la empresa, una gran escalabilidad, y mayor rapidez en el acceso, pero presenta dos inconvenientes fundamentales:

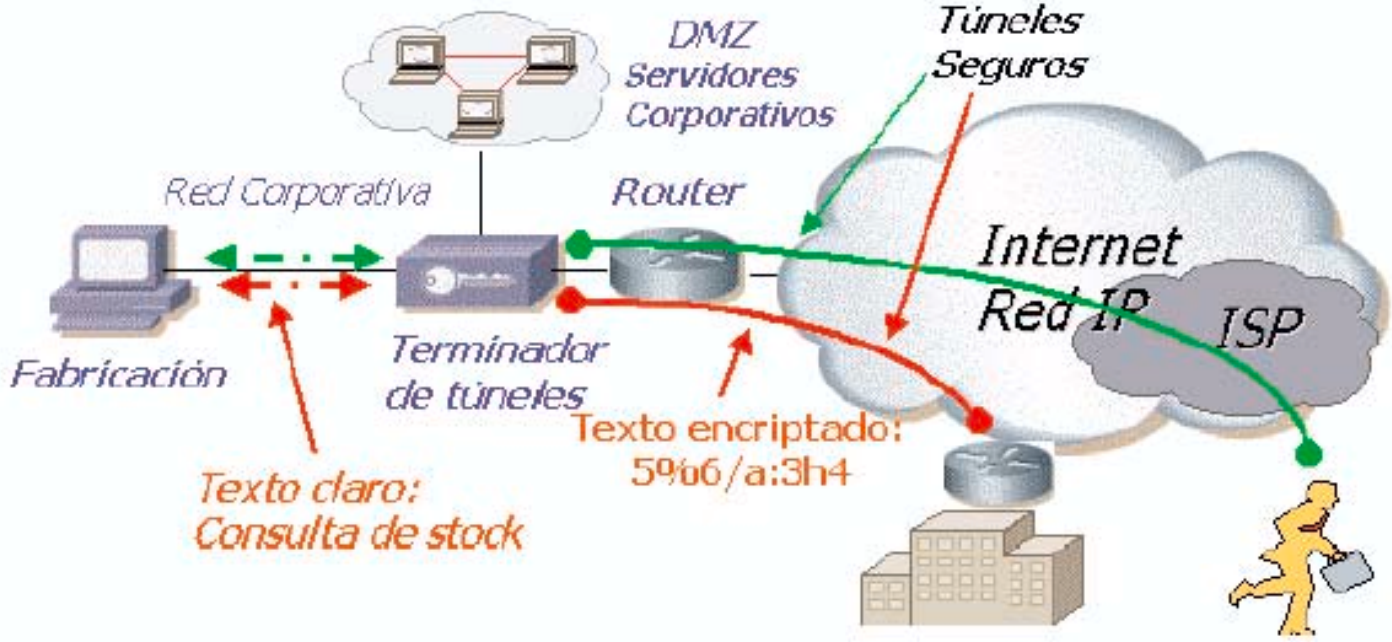
- La imposibilidad de garantizar un rendimiento extremo a extremo.
- La falta de seguridad.

Para solucionar estos inconvenientes surgen las Redes Privadas Virtuales (VPNs)

3. LAS REDES PRIVADAS VIRTUALES (VPNs)

Las Redes Privadas Virtuales (VPNs) es una tecnología que permite establecer comunicaciones seguras y privadas a través de redes privadas IP ó redes públicas compartidas como Internet.

Las VPNs se caracterizan principalmente por su bajo coste y sin lugar a duda, están desplazando poco a poco a tecnologías tradicionales como las líneas punto a punto ó Frame Relay.



Consiste en establecer una conexión segura punto a punto entre los dos extremos de la red, a estas conexiones se les denomina túneles. La información que pasa a través de ellos va encriptada, así cualquier persona malintencionada que pueda escuchar dicha información a través de la red sólo obtiene datos ininteligibles.

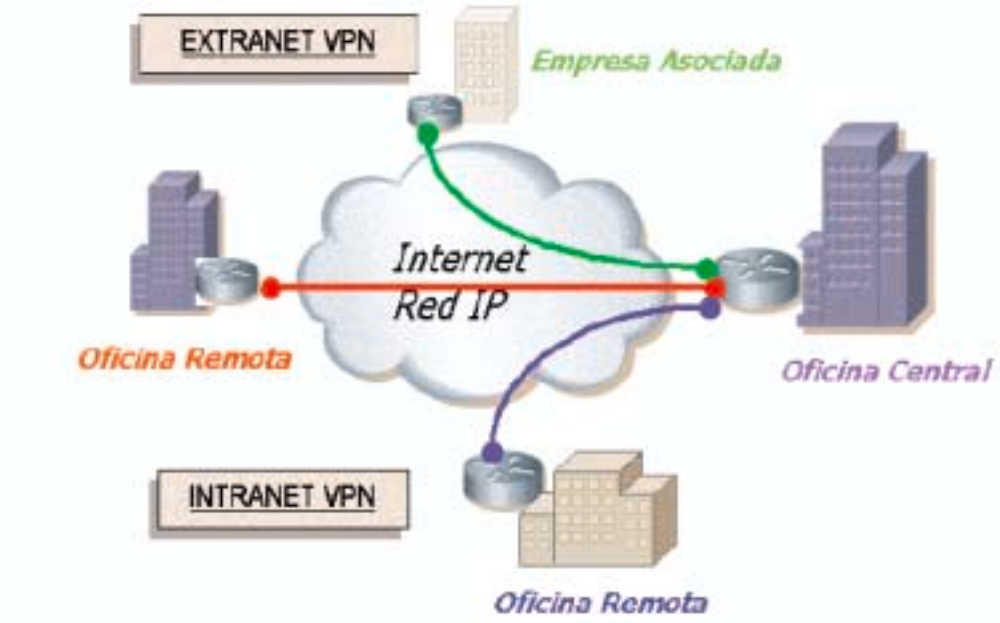
Los dispositivos que permiten establecer túneles son: routers, firewalls, concentradores de VPNs. También se pueden crear conexiones seguras por software, es decir, instalando una determinada aplicación en el portátil del usuario correspondiente. A esta aplicación se le denomina "Cliente de VPN". Por defecto, hay ya algunos sistemas operativos que la incluyen por defecto como Windows 2000 ó Windows XP.

3.1 Escenarios Posibles.

3.1.1 Site-to-Site

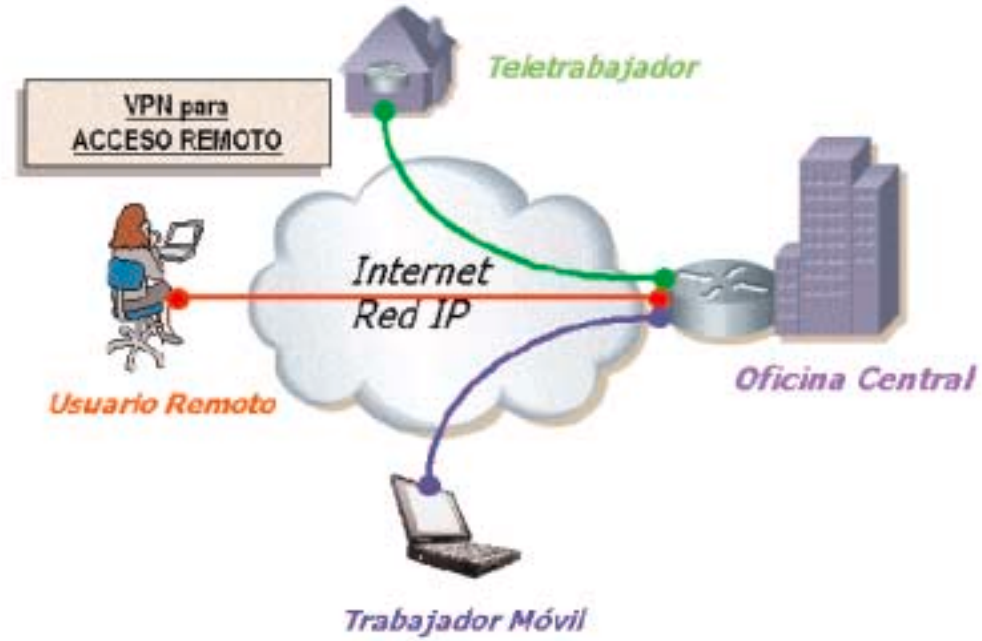
Las VPNs nos permiten afrontar la comunicación de las distintas delegaciones remotas hacia la sede central con total seguridad. A este escenario se le denomina Intranet y está desplazando poco a poco a las líneas Frame Relay ó líneas punto a punto.

Esta tecnología también nos permite establecer comunicaciones seguras a través de redes privadas IP ó redes públicas compartidas como Internet con los proveedores o distribuidores de la empresa. En este caso, a este escenario se le denomina Extranet y está desplazando poco a poco a las líneas punto a punto ó a las líneas de baja velocidad que se utilizaban para cubrir este tipo de escenarios.



3.1.2 Acceso Remoto

Internet proporciona una alternativa de bajo coste para permitir a los usuarios remotos acceder a los servicios que le proporciona la red corporativa de su empresa, ya que con una simple llamada local al proveedor de Internet correspondiente, un usuario puede acceder a la red corporativa. Para dotar de seguridad a la comunicación entre un usuario remoto y su oficina central se puede establecer una VPN entre ambos extremos, para ello en el portátil del usuario remoto tiene que haber instalada el "Cliente de VPN" que le va a permitir establecer comunicaciones seguras a través de redes privadas IP ó públicas compartidas como Internet. Esta tecnología no sólo va a permitir cubrir de forma segura la comunicación entre un usuario remoto y su oficina central, sino que también nos va a permitir dar una solución a los usuarios móviles y teletrabajadores.



4. VULNERABILIDADES EN LA RED

Internet proporciona grandes oportunidades tanto para los clientes como para las empresas, pero no sin algún riesgo. Los datos en su paso sin ningún tipo de control a través de redes privadas IP ó redes públicas compartidas como Internet pueden sufrir múltiples ataques. Los principales ataques que pueden sufrir se comentan a continuación.

- Pérdida de la Privacidad.

  Una persona malintencionada puede escuchar datos confidenciales en su paso a través de Internet, por ejemplo instalando algún sniffer en un punto clave puede obtener los nombres y claves de acceso de los usuarios a la red corporativa como también información comprometida para la empresa.

- Pérdida de la Integridad.

  Hay algunas veces que no sólo esta persona malintencionada se puede limitar a escuchar esta información sino que también puede llegar incluso a modificarla.

- Suplantación de la Personalidad.

  A parte de la protección de los datos propiamente dicha, hay que tener en cuenta que también se debe proteger nuestra identidad a través de Internet, ya que un intruso puede ser capaz de suplantar a una determinada persona y tener acceso a información confidencial. Para evitar todos estos posibles ataques que pueden sufrir los datos sin ningún tipo de control en su paso a través de redes IP ó de Internet surge IPSec.

4.1 IPSec

Es un conjunto de protocolos y algoritmos que nos permite garantizar comunicaciones seguras y privadas sobre redes IP.

Proporciona a los datos:

- Integridad mediante los mecanismos de Hashing

- Confidencialidad aplicando el algoritmo de encriptación correspondiente
- Autenticidad mediante la Firma Digital

4.2 Integridad de los Datos: Hashing

El hash garantiza la integridad de los datos a su paso a través de redes IP, es decir que ningún intruso pueda modificar dicha información. Para ello, se añade a los datos una serie de datos en la cabecera parecidos al checksum, que se denominan compendio. Este compendio se obtiene de aplicar a los datos un mecanismo de Hash. Éste consiste en una forma matemática de resumir unos datos de forma que, partiendo del dato modificado no se pueda llegar fácilmente a la información original, inclusive conociendo el algoritmo empleado.

Los algoritmos de Hashing existentes actualmente son:

- MD5 (Message Digest V5)
  - Es el más antiguo pero más ampliamente soportado.
- SHA (Secure Hash Algorithm)
  - Más nuevo y más seguro que MD5
- HMAC (Hash-based Message Authentication Code)
  - Además de proporcionar integridad permite autentificar a los extremos.

4.3 Confidencialidad de los Datos: Encriptación

La encriptación protege a los datos durante su paso a través de redes IP ó redes públicas como Internet, de tal forma que si un intruso escucha esos datos le resulten ininteligibles y que sólo sean claros para el destinatario al cual van dirigidos.

Los algoritmos de encriptación que se pueden emplear son:

- DES (Data Encryption Standard)
  - Usa una clave de 56 bits para encriptar datagramas de 64 bits.
- 3DES (Triple Data Encryption Standard)
  - Se basa en DES, pues encripta los datos tres veces seguidas apoyándose en este algoritmo.
  - Para encriptar puede utilizar dos claves distintas, obteniendo una clave de 112 bits ó tres claves distintas, obteniendo en este caso una clave de 168 bits.

Debido a que en los últimos años se ha producido una gran evolución en los PCs que existen en el mercado tanto en capacidad de procesamiento como de memoria, se dispone de máquinas muy poderosas que pueden llegar a vulnerar una clave DES, por lo que se están desarrollando nuevos algoritmos de encriptación como AES (Advanced Encryption Standard) que en los próximos años se convertirá en un algoritmo estándar de encriptación desplazando a DES.

4.4 Autenticidad: Firma Digital

La Firma Digital garantiza la identidad de los extremos durante su transporte sobre redes privadas IP ó públicas como Internet, es decir autentica la identidad de la persona que envía esos datos ó que los firma.

Consiste en un mecanismo de intercambio de claves entre los dos extremos. Se utiliza una clave privada secreta para la generación de la firma y una clave pública para verificar en el otro extremo que esa persona es quien dice ser.

La Firma Digital suele ir ligada al concepto de compendio ya que aparte de garantizar la autenticidad de los extremos se asegura la integridad de los mismos en su paso a través de Internet ó de las redes privadas IP.

Los algoritmos de Firma Digital que existen son:

- RSA (Rivest, Shamir, Adelman)
  - Es el algoritmo de Firma más popular, puede ser utilizado tanto para firmar los datos como para encriptarlos aunque es mucho más lento que DES.

- DSA (Digital Signature Algoritm)
    - Es el algoritmo estándar de Firma Digital. Genera una clave de 512 ó 1024 bits por lo que es más lento que RSA.

Si el número de usuarios ó oficinas remotas que se tienen que autenticar aumenta considerablemente, la gestión de las claves se complica bastante; por lo que el mecanismo que se aconseja para autenticar los extremos son los Certificados Digitales en lugar de la Firma Digital.

5. DISPONIBILIDAD DE LOS DATOS

La Red de Datos es un elemento clave y crítico en cualquier organización para el desarrollo de las tareas y la comunicación de los departamentos y usuarios de la misma; por ello, se debe de cuidar de forma muy especial que ofrezca unas elevadas garantías.

La disponibilidad ó alta disponibilidad es un concepto utilizado cuando nos referimos a que la Red de Datos sea capaz de proporcionar servicio la mayor parte del tiempo. Con ello lo que se quiere evitar es posibles fallos, errores ó averías que se puedan producir y que impidan que los usuarios accedan a determinados servicios durante un cierto periodo de tiempo. Por lo que el objetivo será garantizar la máxima disponibilidad a distintos niveles: líneas de comunicaciones, equipos y servicios.

Para ello, se debe ser capaz de:

- Prevenir fallos
    - Dotando a la red de mecanismos que eviten y eliminen la aparición de fallos como por ejemplo duplicando los equipos centrales de la red ó dotando de líneas de backup a las líneas principales de comunicación.
- Estudiar la tolerancia a fallos
    - En caso de la aparición de fallos, el grado de fiabilidad de la red consistirá en su capacidad para man-

tener la conectividad y servicios disponibles. Para ello, los equipos que integran la red deben estar basados en arquitecturas que tiendan a incorporar la duplicación de los elementos más críticos para su funcionamiento.

- Sustituir los fallos
  - Es decir, simplificar las tareas a realizar en caso de fallo, de tal forma que si se produce el fallo, su reparación y mantenimiento, sean lo más sencillo posible, llegando incluso al funcionamiento ininterrumpido del equipo durante la intervención.