RED ARTERIAS: SERVICIO DE ACCESO REMOTO

Marlen Ripoll, Isabel Sánchez, Mercedes Dobón, Mariam De la Iglesia, José Mª Simón

Área de Organización y Sistemas de Comunicación
Conselleria de Sanitat de la Generalitat Valenciana.

RED ARTERIAS

La Conselleria de Sanitat dispone de una Red de datos de área extensa llamada ARTERIAS. Es una red multiservicio IP de banda ancha, diseñada para gestionar servicios de voz, datos e imagen. Incorpora técnicas de calidad de servicio, optimización de ancho de banda y de seguridad. Ofrece acceso a Internet y dispone de un Centro de Gestión de red desde donde se realiza una gestión integral y centralizada permitiendo administrar sus funcionalidades. En la actualidad da cobertura a más de 800 Centros Sanitarios y Administrativos en la Comunidad Valenciana.

LA OBLIGACIÓN JURÍDICA

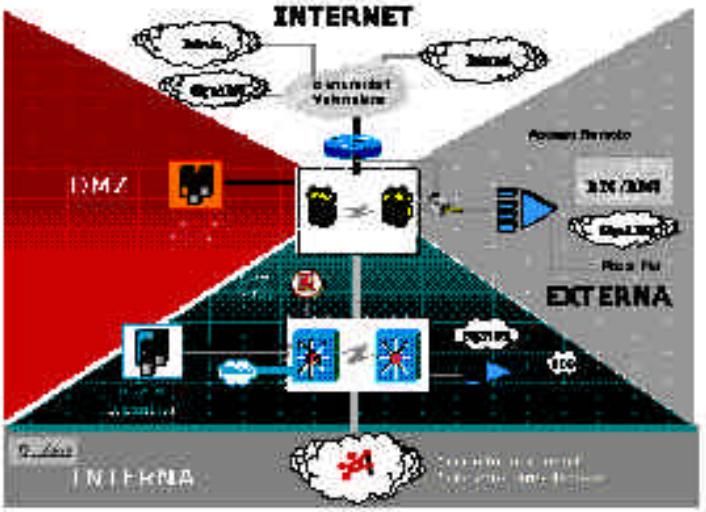
La legislación vigente en materia de Seguridad, marcada fundamentalmente por la Ley de Protección de Datos de Carácter Personal (Ley Orgánica 15/99) y el Reglamento de de Medidas de Seguridad (Real Decreto 994/1999) nos exigen la adecuación de las redes actuales a "*redes más seguras y fiables*". El Reglamento define los datos personales referentes a la salud como de nivel alto en cuanto a medidas de seguridad, especificando en el artículo 26 que "*La transmisión de datos de carácter personal a través de redes de telecomunicaciones se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros*".

Por otra parte, hoy en día, una organización no es un núcleo cerrado, sino que es más bien una comunidad virtual en la que interactúan los empleados, los proveedores, los colaboradores, etc., mediante el intercambio de información, compartición de aplicaciones o bases de datos.

SEGURIDAD EN LA RED ARTERIAS

Arterias está diseñada con un único punto de acceso desde Internet, lo que facilita la aplicación de las políticas de seguridad. Desde el punto de vista de la seguridad está dividida en cuatro zonas, interconectadas mediante un sistema de firewalls o cortafuegos donde se aplican los controles de acceso definidos en la Política de la Conselleria y se lleva a cabo la inspección y el filtrado del tráfico de entrada a la red arterias. Estas cuatro zonas son:

- Internet: Canaliza el tráfico de Internet y el de las Consellerias a través de la Red Corporativa de la Generalitat Valenciana.
- DMZ (Zona desmilitarizada) : En esta zona se encuentran los servidores web accesibles desde Internet.
- Externa: A través de la zona externa la Consellería de Sanitat actúa como "Proveedor de Servicios" ofreciendo acceso a usuarios, empresas u organismos que estén debidamente autorizados.
- Interna: Es la zona donde se encuentran, tanto los Servidores Corporativos de la Conselleria como todos aquellos centros conectados a la Red Arterias.



Teniendo en cuenta que esta red "transporta" datos de carácter sanitario sujetos a las medidas de seguridad más restrictivas y que se van a realizar conexiones tanto desde Internet como desde usuarios remotos que atraviesan "redes públicas" (ADSL, RDSI, RTC, ..), se ha dotado a la red de los "*servicios de acceso remoto*" necesarios para permitir no sólo la conectividad sino también el control de las conexiones y la protección de los datos accedidos

La solución adoptada en Arterias para proporcionar el acceso remoto cumpliendo los requisitos de seguridad anteriormente citados es el establecimiento de "*redes privadas virtuales utilizando IPSec*".

REDES PRIVADAS VIRTUALES

Entendemos por red privada virtual o VPN la interconexión de una o más redes por medio de una infraestructura pública, normalmente compartida, para simular una infraestructura dedicada o privada. Se dice que es Virtual porque el usuario tendrá la "sensación" de estar en una única red y Privada porque la comunicación a través de ella es segura y está protegida.

Para poder establecer una VPN será necesario generar un túnel entre los dos extremos que toman parte en la comunicación. Durante el establecimiento del túnel se negociarán los mecanismos de seguridad que se han de utilizar

El objetivo a conseguir es que todo se haga de forma transparente a la aplicación, es decir, una aplicación debe seguir funcionando a través de la VPN exactamente igual que lo hace cuando se accede a ella desde la red corporativa sin necesidad de realizar ninguna modificación en la misma.

Características de una VPN con IPSec

IPSec es un conjunto de protocolos de la IETF, que proporcionan seguridad en las comunicaciones, actuando en el nivel de red. Debido al hecho de estar situado en este nivel, los usuarios remotos tendrán la misma accesibilidad a los recursos que si se encontraran físicamente en ella.

Entre los protocolos que forman IPSec podemos distinguir :

1) Authentication Header (AH) proporciona autenticación de datos y servicio opcional anti-reenvíos
2) Encapsulating Security Payload (ESP), que proporciona, además de los servicios ofrecidos por AH, la confidencialidad a través del cifrado.
3) Una función de intercambio de claves, integrada en el protocolo IKE.

Los protocolos AH y ESP se pueden utilizar de forma independiente o de forma combinada, utilizándose las diferentes combinaciones para aumentar el nivel de seguridad de IPSec.

Los servicios de seguridad de red que nos ofrece IPSec son:

Confidencialidad: envía los paquetes encriptados para asegurar que el mensaje transmitido sólo es entendible por quien lo envía y por aquel a quien va dirigido, para ello utiliza algoritmos de clave simétrica como DES o 3DES.

Integridad y Autenticación: garantiza que el mensaje no ha sido alterado en el tránsito y autentica los extremos para comprobar que son quienes dicen ser.

Ventajas de la tecnología VPN con IPSec

La movilidad es una exigencia en las organizaciones actuales, buscándose cada vez más el acceso a los recursos desde cualquier punto. Mediante la personalización de los servicios de red y suministrando a los usuarios un acceso rápido y seguro a la información que precisan, se consigue que el funcionamiento de la organización sea mucho más ágil. Las tecnologías inalámbricas han contribuido a proporcionar mayor libertad de acceso, pero no sólo hay que tener en cuenta el ofrecer la posibilidad de acceso, también hay que considerar la forma en que la red permite a los usuarios acceder a la información y a las aplicaciones.

El acceso a una red corporativa por medio de una VPN con IPsec supone una serie de ventajas, frente a otras soluciones (líneas dedicadas tradicionales), entre las que podemos destacar:

- ✍ Ahorro en costes, tanto de equipamiento de backbone como operacionales.
- ✍ Entorno de trabajo independiente del tiempo y el lugar, puesto que permiten el acceso a los servicios de la red corporativa a usuarios móviles sin necesidad de realizar llamadas a larga distancia.
- ✍ Mayor flexibilidad y escalabilidad, ya que permiten conectar y desconectar oficinas remotas de manera más rápida y barata, con el mismo nivel de seguridad que si estuvieran en una misma red.
- ✍ Posibilidad de ofrecer servicios de red a usuarios externos de una forma segura y controlada.

RED ARTERIAS: ACCESO REMOTO

El acceso remoto a la red de la Consellería de Sanitat mediante VPN se realiza a través de un concentrador Cisco VPN 3060 en el que se configura el estándar IPSEC.

Las posibilidades de acceso son:

A través de INTERNET

Internet se ha convertido en una infraestructura de bajo coste para las comunicaciones. Su alcance universal nos ha llevado a considerar la construcción de una red privada virtual segura sobre esta red pública. Se permite al acceso a la red Arterias con el único requisito de tener una conexión a Internet de cualquier tipo (RTC, RDSI, ADSL, FR, CABLE, GPRS ...)
El utilizar Internet como medio de trasporte supone que no podemos garantizar el ancho de banda disponible y la calidad de servicio extremo a extremo. Por tanto, el acceso a los Sistemas de Información a través de VPN sobre Internet puede no ser la solución más apropiada, fundamentalmente, cuando se necesita trabajar con aplicaciones sensibles a retardos.

A través de infraestructura de ISP de la Conselleria de Sanitat

Arterias dispone de la infraestructura de red necesaria para actuar como un "proveedor de servicios ISP " y permitir el acceso directo a usuarios, por distintos medios físicos. Esta solución de acceso directo contempla actualmente un amplio abanico de posibilidades.

- *Arterias RTB /RDSI*

Enfocada e conexiones individuales sobre una línea telefónica clásica o RDSI Permite una conexión de hasta 56Kbps o 128Kbps por RDSI. En el caso de utilizar RDSI es posible conectar una LAN a través de un router . Hay que tener en cuenta que este tipo de acceso puede elevar el coste si la llamada no es local. Una vez establecida la conexión, y para aquellos usuarios que tengan que acceder a datos críticos, se crea la VPN sobre el concentrador para que el tráfico vaya cifrado, cumpliendo así con la legislación vigente en materia de protección de datos.

- *Accesos ADSL GVA corporativo.*

Permite el acceso directo (sin pasar por Internet) a la red Arterias a través del ADSL corporativo de la GVA. Este tipo de acceso esta orientado a aquellos usuarios que tengan que trabajar continuamente desde una localización remota determinada. Para estos casos resulta más económico que un acceso por medio de RDSI y tiene un mayor ancho de banda. Este servicio queda limitado a las zonas donde la GVA tiene cobertura.

- *Accesos por líneas punto a punto.*

También es posible utilizar una línea punto a punto, Nx64. Esta solución puede llegar a tener un coste muy elevado y sólo se debería emplear cuando sea estrictamente necesario por razones de ancho de banda y sensibilidad a los retardos de las aplicaciones que se vayan a utilizar.

VPN definidas en la Red Arterias

En la actualidad este tipo de solución se está aplicando para resolver las necesidades de acceso seguro desde el exterior de la Red Arterias a Sistemas de Información de la Consellería de Sanitat,.

Los usuarios remotos definidos hasta el momento se pueden englobar en los siguientes grupos:

- Organismos Oficiales, como el Ministerio de Sanidad o La Tesorería de la Seguridad Social, que requieren el acceso a datos mantenidos en la propia Consellería.
- Empresas de mantenimiento, que deben llevar a cabo, de forma remota, el mantenimiento de aplicaciones o equipos.
- Empresas de Desarrollo y soporte de Aplicaciones. En este apartado se incluye a empresas contratadas, para el desarrollo de aplicaciones y que necesitan acceder desde sus locales a los equipos de la Consellería de forma continuada.