RED PRIVADA VIRTUAL

Fernando Martín Moreno

Jefe de Servicio de Sistemas y Comunicaciones en el Area de Proyectos Especiales de la Subdirección General de Proceso de Datos del Ministerio de Trabajo y Asuntos Sociales.

Introducción

Una Red Privada Virtual o genéricamente denominada VPN (Virtual Private Network), es un servicio de comunicación que transfiere datos cifrándolos o encapsulandolos según el caso, desde un punto hacia otro de manera segura; la seguridad de los datos se consigue gracias a una tecnología robusta de cifrado, y los datos que se transfieren pasan a través de una red abierta, enrutada por infraestructuras públicas o privadas de transporte (en general a través de Internet).

La VPN permite al usuario remoto (entre otras opciones), acceder a su red corporativa, asignándole a su ordenador remoto las direcciones y privilegios de la misma, aunque la conexión de haya realizado a través de un acceso publico como es Internet.

En algunos casos por el nivel de protección exigido en la Ley de Protección de Datos, es necesario que la información transmitida, que viaja por el túnel establecido en la red pública, vaya cifrada para permitir una mayor confidencialidad y seguridad.

Con la utilización de las VPN, las organizaciones pueden construir túneles seguros a través de cualquier red basada en IP, dando soporte, tanto para las topologías "Red remota – Red interna" como para "Usuario remoto – Red interna ", proporcionando una solución idónea para ofrecer los servicios de nuestra red corporativa a las redes remotas y usuarios remotos móviles/fijos.

La principal ventaja de usar una VPN es que permite obtener una conexión a la red corporativa con todas las características de la red privada a la que se quiere acceder. El cliente VPN adquiere totalmente la condición de usuario de esa red, con lo cual se le aplican todas las directivas de seguridad y permisos de ese ordenador en esa red privada, pudiendo acceder a la información a la que esta autorizada para esa red privada: bases de datos corporativos, correo electrónico, Intranet, etc.

Las Redes Privadas Virtuales (VPN) proporcionan actualmente un poderoso medio de protección de la privacidad e integridad de las comunicaciones administrativas y comerciales a través de Internet. Ahora las organizaciones cuentan con una alternativa viable ante las costosas líneas alquiladas para conectarse a sus redes privadas. Una VPN es mucho menos costosa y más flexible que una red dedicada privada.

Justificación

Las redes privadas virtuales (VPN´s) persiguen conseguir dos objetivos:

1.- Conectar a nuestros usuarios remotos, de forma independiente o en red a nuestra red corporativa de forma segura

2.- Conexión a un precio reducido.

Tipos de acceso

La velocidad de conexión, es uno de los problemas más importantes a la hora de utilizar VPN´s, si queremos garantizar un tiempo de respuesta razonable. Hoy en día la velocidad utilizando un módem vía RTB es de 56 Kbps., velocidad razonable para la utilización de determinados servicios (emuladores 3270, VT220, acceso a correo sin documentos adjuntos, etc).

Mediante tarjetas pcmcia/teléfonos GSM con velocidades máximas en la transmisión de datos de 9.600 Bps. es difícil garantizar los servicios de red. Los actuales sistemas GPRS con velocidades máximas en la transferencia de datos de 40 Kbps. en los casos más favorables y en las zonas en donde actualmente hay cobertura de este servicio, permiten obtener mejores tiempo de respuesta. Será con la llegada de UMTS, cuando se dé, el verdadero despliegue de la telefonía móvil para la conexión remota.

En todo caso, cuando añadimos los algoritmos de cifrado necesarios de implementar en estas conexiones para garantizar la seguridad de las mismas, obtendremos peor tiempo de respuesta al requerir este proceso un mayor consumo de recursos para procesar el cifrado/descifrado en los extremos de la VPN y por tanto perjudicar los trabajos de acceso a la Intranet. Es por ello por lo que se intenta minimizar el overhead de la cabecera del túnel para ser capaz de llevar trafico sensible al retardo (latencia y jitter), sobre todo en entornos móviles con poco ancho de banda. Es median-

te la utilización de conexiones de alta velocidad (mayores de 64 Kbps.), en donde se pueden ofrecer de forma adecuada estos servicios, bien mediante el uso de accesos RDSI, FR, ADSL, cable, etc, y donde incluso, podemos establecer gestión QoS o del tráfico.

Otro problema es el ancho de banda contratado en nuestra organización para el acceso a/desde Internet a través de las VPN´s generadas por nuestros usuarios remotos. El acceso a determinados recursos requieren un ancho de banda mínimo para acceder de forma adecuada. La saturación de estos circuitos genera problemas en los tiempos de acceso a nuestra red por los usuarios remotos. Para resolver estos problemas se requieren contratar líneas dedicadas, o establecer reservas de ancho de banda especificas para garantizar este servicio.

El mercado de productos de red privada virtual (VPN) incluye una gran variedad de soluciones, desde simples dispositivos de cifrado a creadores de túneles multiprotocolo.

Seguridad

Para conseguir la seguridad exigida en la comunicación entre dos extremos de la red Internet deberemos de garantizar cuatro requisitos:

1.- Autenticidad de conexión: todas las entidades participantes en la transacción deben estar perfecta y debidamente identificadas antes de comenzar la misma. Debemos estar seguros de que la entidad con la que nos comunicamos es realmente quién dice ser, ya que si no podemos estar facilitando datos sensibles a una persona o entidad no deseada.

   La Autenticidad se consigue mediante el uso de los certificados y firmas digitales.

2.- Confidencialidad: debemos estar seguros de que los datos que enviamos no pueden ser leídos por otra persona distinta del destinatario final deseado, o que si ocurre esto, no se pueda reconocer el mensaje

enviado. Es decir, debemos estar seguros de que ninguna persona ajena a la transacción puede tener acceso a los datos de la misma.

La confidencialidad de consigue en las transacciones electrónicas con el uso del cifrado.

3. Integridad de los datos: es necesario estar seguro de que los datos que enviamos llegan íntegros, sin modificaciones, a su destino final.

   La integridad se consigue mediante la utilización de técnicas de firma digital.

4.- No repudio: En una transacción electrónica debe garantizarse que una vez finalizada la misma ninguna de las partes que intervienen pueda negar haber participado en ella.

   Lo ideal sería que al finalizar la transacción quedara algo equivalente a un recibo de compra o factura firmado por todas las partes implicadas.

Estas son las condiciones mínimas que debe cumplir una comunicación por Internet para poder considerarse como segura. Todos estos aspectos se combinan en diferentes tecnologías, que permiten garantizar la seguridad exigida.

Mecanismos de seguridad

No existe un único mecanismo capaz de proveer todos los servicios anteriormente citados. Los más importantes son los siguientes:

1.- Intercambio de autenticación: corrobora que una entidad, ya sea origen o destino de la información, es la deseada, por ejemplo, A envía un número aleatorio cifrado con la clave pública de B, B lo descifra con su clave privada y se lo reenvía a A, demostrando así que es quien pretende ser. Por supuesto, hay que ser cuidadoso a la hora de diseñar estos protocolos, ya que existen ataques para desbaratarlos.

2.- Cifrado: garantiza que la información no es inteligible para individuos, entidades o procesos no autoriza-

dos (confidencialidad). Consiste en transformar un texto en claro mediante un proceso de cifrado en un texto cifrado, gracias a una información secreta o clave de cifrado.

- Cuando se emplea la misma clave en las operaciones de cifrado y descifrado, se dice que el cifrado es simétrico. Estos sistemas son mucho más rápidos que los de clave pública, resultando apropiados para funciones de cifrado de grandes volúmenes de datos. Se pueden dividir en dos categorías: cifradores de bloque, que cifran los datos en bloques de tamaño fijo (típicamente bloques de 64 bits), y cifradores en flujo, que trabajan sobre flujos continuos de bits.

- Cuando se utiliza una pareja de claves para separar los procesos de cifrado y descifrado, se dice que el cifrado es asimétrico o de clave pública. Una clave, la privada, se mantiene secreta, mientras que la segunda clave, la pública, puede ser conocida por todos. De forma general, las claves públicas se utilizan para cifrar y las privadas, para descifrar. El sistema tiene la propiedad de que a partir del conocimiento de la clave pública no es posible determinar la clave privada. Los sistemas de cifrado de clave pública, aunque más lentos que los simétricos, resultan adecuados para las funciones de autenticación, distribución de claves y firmas digitales.

- El cifrado mixto se da, cuando se utiliza el algoritmo de clave publica para intercambiar la clave simétrica de sesión que será utilizada para cifrar el resto de la sesión.

3.- Integridad de datos: este mecanismo implica el cifrado de una cadena comprimida de datos a transmitir, llamada generalmente valor de comprobación de integridad (Integrity Check Value o ICV). Este mensaje se envía al receptor junto con los datos ordinarios. El receptor repite la compresión y el cifrado posterior de los datos y compara el resultado obtenido con el que le llega, para verificar que los datos no han sido modificados.

4.- Firma digital: este mecanismo implica el cifrado, por medio de la clave secreta del emisor, de una cadena comprimida de datos que se va a transferir. La firma digital se envía junto con los datos ordinarios. Este mensaje se procesa en el receptor, para verificar su integridad. Juega un papel esencial en el servicio de no repudio. Si además esta basado en certificados X509 ofrece autenticación.

5.- Control de acceso: medidas para que sólo aquellos usuarios autorizados accedan a los recursos del sistema o a la red, como por ejemplo mediante las contraseñas de acceso.

6.- Tráfico de relleno: consiste en enviar tráfico sin valor junto con los datos válidos para que el atacante no sepa si se está enviando información, ni qué cantidad de datos útiles se está transmitiendo.

7.- Control de encaminamiento: permite enviar determinada información por determinadas zonas consideradas clasificadas. Asimismo posibilita solicitar otras rutas, en caso que se detecten persistentes violaciones de integridad en una ruta determinada.

8.- Unicidad: consiste en añadir a los datos un número de secuencia, la fecha y hora, un número aleatorio, o alguna combinación de los anteriores, que se incluyen en la firma digital o integridad de datos. De esta forma se evitan amenazas como la reactuación o resecuenciación de mensajes.

Los mecanismos básicos pueden agruparse de varias formas para proporcionar los servicios previamente mencionados. Conviene resaltar que los mecanismos poseen tres componentes principales:

- Una información secreta, como claves y contraseñas, conocidas por las entidades autorizadas.
- Un conjunto de algoritmos, para llevar a cabo el cifrado, descifrado, hash y generación de números aleatorios.
- Un conjunto de procedimientos, que definen cómo se usarán los algoritmos, quién envía qué a quién y cuándo.

Asimismo es importante notar que los sistemas de seguridad requieren una gestión de seguridad. La gestión comprende dos campos bien amplios:

- Seguridad en la generación, localización y distribución de la información secreta, de modo que sólo pueda ser accedida por aquellas entidades autorizadas.
- La política de los servicios y mecanismos de seguridad para detectar infracciones de seguridad y emprender acciones correctivas.

Entre los estándares de IP se incluye IPSEC. El propósito de Ipsec es proporcionar alta seguridad sobre redes publicas. Con sus funciones principales de cifrado y autenticación. Las VPN´s basadas en Ipsec son actualmente la mejor opción para garantizar la seguridad en la comunicación.

Inconvenientes

Entre los inconvenientes podemos citar:

- Una mayor carga en el cliente VPN, situación que se agrava cuando además se realiza cifrado de los datos que produce una mayor lentitud de la mayoría de conexiones. También se produce una mayor complejidad en el tráfico de datos que puede producir efectos no deseados al cambiar la numeración asignada al cliente VPN y que puede requerir cambios en las configuraciones de aplicaciones o programas (proxy, servidor de correo, permisos basados en nombre o número IP, etc.)

- Hay que tener en cuenta que muchas aplicaciones y programas ya hacen el cifrado de la información transmitida y al volver a cifrarlo por el túnel VPN, no nos aporta seguridad adicional. Aplicaciones tales como el correo seguro S/MIME o una conexión SSH (conexión Telnet segura a través del puerto 22 a una maquina Unix), son suficientemente seguras para no requerir el cifrado adicional.

- Otro problema es que no se garantiza la calidad del servicio (QoS), en la comunicación a través de Internet. Esto limita ofrecer servicios que requieren una determinada calidad como vídeo online, VoIP, etc.

Clases de VPN´s

Los distintos fabricantes las han dividido en tres tipos basados en los niveles 2, 3 y 4 (enlace, red y transporte) del modelo de referencia OSI:

1.- En el nivel más bajo, el 2, las VPN encapsulan protocolos tanto IP como no IP (IPX, Apple Talk, etc). También proporcionan independencia de la plataforma porque los sistemas clientes generalmente no requieren de más hardware o software especial que un adaptador de red. Sin embargo, está orientada a un puesto remoto, no a las redes remotas.

Las VPN´s de Nivel 2 incluyen productos basados en protocolos como Point to Point Tunneling Protocol (PPTP) creado por la Industry Forum (3 Com, Ascend, Microsoft y ECI Telematics), Layer 2 Forwarding (L2F) creado por Cisco Systems y el nuevo estándar Layer 2 Tunneling Protocol (L2TP) como una combinación de PPTP y L2F que evoluciono a través del proceso de estándares del Internet Engineering Task Force (IETF) . Las VPN´s de este nivel requieren que la comunicación sea a través del mismo operador.

Es frecuente utilizar este nivel sobre tecnologías de comunicación Frame Relay o ATM

2.- Mientras que los productos de Nivel 2 encapsulan todos los protocolos en IP, los productos de Nivel 3 encapsulan IP en IP. Actualmente, este mercado gira en torno a IP Security (IPSec), cifrado IP, autenticación y el protocolo de tunneling estandarizado por el IETF.

Este nivel utiliza las Redes IP Públicas teniendo un amplio acceso geográfico.

3.- Las herramientas VPN de Nivel 4, esta basadas en técnicas de cifrado especificas y de encapsulación. No obstante, los productos de este nivel suelen estar restringidos a una sola aplicación, como el correo electrónico. Ejemplos comunes como HTTP sobre Secure Sockets Layer (SSL) HTTPS, el correo electrónico cifrado, S/MIME, están presentes en todos los navegadores

En la actualidad la mayoría del mercado VPN se encuentra en los productos de Nivel 3; se implementan en routers, cortafuegos, software y hardware dedicado.

Una de las piezas claves todavía inexistentes en el mercado de VPN es una verdadera infraestructura de clave pública (PKI-Public-Key Infreaestructure). Con una PKI global, los usuarios pueden disponer de comunicaciones seguras sin necesidad de contar con una relación especial preestablecida. PKI es más que una autoridad de certificación, ya que incluye otras partes, como los servicios de registro.

IPSEC

Este protocolo de seguridad esta basado en estándares de facto recogidos por la IETF y que proporcionan Confidencialidad, Integridad y Autenticidad en el transporte de la información y así asegurar comunicaciones privadas con el protocolo de comunicaciones IP.

Ipsec proporciona seguridad a nivel de red para IP proporcionando una solución end-to-end.

Se basa en diferentes técnicas entre las que destacamos:

- Uso de algoritmos Hash (MD5 o SHA1) para proporcionar la autenticación de paquetes. Una función Hash toma un mensaje de entrada de longitud variable y produce un resultado de longitud fija. Un valor Hash de un mensaje es un valor único generado por el algoritmo Hash correspondiente que es conocido públicamente. Una función Hash es unidireccional, a partir del valor obtenido no se pueden obtener los datos originales de los que parte.

- Uso de algoritmos de cifrado (AES, DES, 3DES, RC5, CAST, BlowFish, etc.) para proporcionar confidencialidad de la información. Consisten en la aplicación de una función matemática a los bloques originales y obtención de otros bloques modificados por ella. Uno de los algoritmos más usados actualmente por su robustez es el 3DES. Este algoritmo permite el cifrado por software o utilizando hardware especifico, consiguiendo en este segundo caso una velocidad de cifrado mucho más alta. En este algoritmo se pueden utilizar claves de hasta 192 bits aunque se pueden utilizar claves de menor longitud.

- La autenticidad de los interlocutores (son quienes dicen ser) se pueden implementar por dos métodos:

  a) Mediante secreto compartido. Palabra clave que intercambian a la hora de autenticar a su interlocutor

  b) Mediante el uso de certificados digitales expedidos por una autoridad de certificación (CA).

  En ambos casos se emplea como protocolo de intercambio de claves (IKE).

Pasos para establecer una comunicación sesión segura.

Antes de enviar la información cifrada, es necesario establecer dos sesiones IPSEC entre los equipos que se quieran comunicar.

Las sesiones IPSEC vienen precedidas de la creación de una sesión IKE. La sesión IKE se crea exclusivamente para intercambiar los datos necesarios para crear posteriormente las definitivas sesiones IPSEC.

Sesión IKE:

Tiene dos componentes: ISAKMP y OAKLEY

1. ISAKMP: Procedimientos y formatos de paquete para establecer, negociar, modificar y eliminar SA (Asociación de Seguridad).
2. OAKLEY: Protocolo de intercambio de claves. Utiliza el algoritmo de Diffi-Hellman

Sesión IPSEC:

Una sesión IPSEC define el método de cifrado de los paquetes y la información que hay que añadir a los paquetes para conseguir la confidencialidad, integridad y autenticidad.

Las sesiones IPSEC se basan en la creación de Asociaciones de Seguridad (SA) entre las dos entidades que se comunican.

Una asociación de seguridad describe:

- Que algoritmo va a ser usado en la autenticación y las claves para él.
- El algoritmo de cifrado y las claves
- Tiempo de vida de las claves
- Tiempo de vida de la SA
- Dirección IP origen de la SA

Hay que tener en cuenta en una SA lo siguiente:

- Una SA es unidireccional, esto significa que cada par de sistemas que se comunican por lo menos tiene dos, una de A a B y otra de B a A.
- Cada SA es única y se identifica por un número aleatorio único (SPI), por la dirección IP destino y por el método empleado (AH o ESP).

Métodos de seguridad en IPSEC

- AH (Solo autenticación)
    1. Detecta los cambios de contenido
    2. Los destinatarios pueden autenticar el origen
    3. Previene los ataques de IP-Spoofing
    4. Protege el ataque de retransmisión

- ESP (Cifrado y si se quiere autenticación)
    1. Confidencialidad de contenido
    2. Confidencialidad limitada de flujo de trafico
    3. Opcionalmente, servicio de autenticación como AH

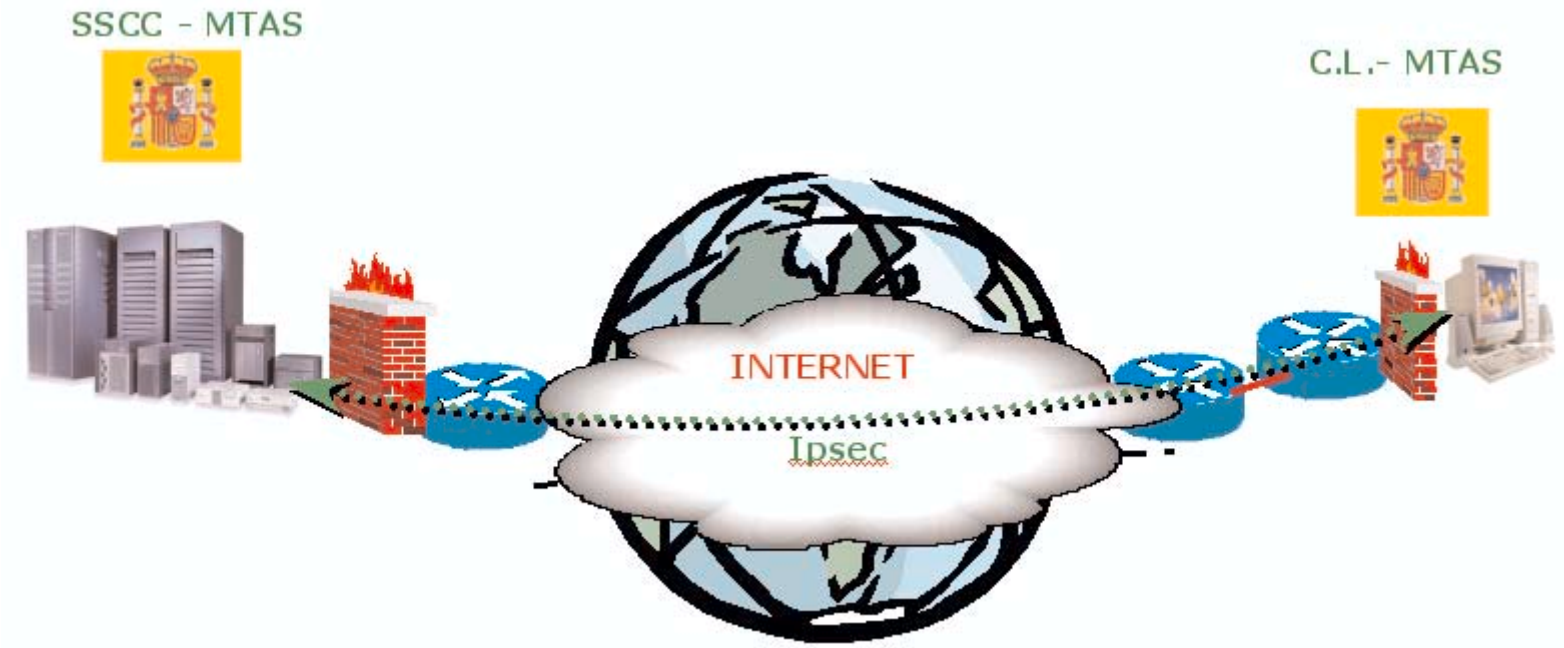
Modos de operación en IPSEC

IPSEC proporciona 2 modos de operación:

- Modo Transporte: Solo se cifran los datos, las cabeceras IP quedan igual.

- Modo Túnel: Todo el paquete se cifra y se inserta en un nuevo paquete. La ventaja de este modo radica en que los sistemas finales no necesitan ser modificados y que las direcciones originales no son accesibles por terceros.

Esquema de conexión:



Proyecto VPN Consejerías Laborales - SSCC MTAS

Este proyecto está destinado a crear una RED PRIVADA VIRTUAL entre veintisiete Consejerías Laborales (ubicadas en diferentes países) y los Servicios Centrales del MTAS, aprovechando la conexión a través de Internet y el protocolo de seguridad Ipsec.

Cada vez era mas necesario dotar a todas las redes y usuarios remotos del Ministerio, independientemente de su ubicación física, de los servicios que necesitan para desarrollar su trabajo (correo electrónico, acceso a Internet e Intranet, acceso a las bases de datos corporativas, transferencia de ficheros, etc.)

Sin embargo el alto coste de contratar y mantener líneas privadas hacía difícil su implementación.

El uso de la red pública Internet como medio de transporte para crear una red privada virtual (VPN) entre las diferentes Consejerías Laborales y los SSCC, es la solución que hemos considerado más idónea en la actualidad para ofrecer este servicio.

La seguridad y privacidad en las comunicaciones pasa a ser un factor muy importante en éste nuevo entorno de interconexión y más al utilizar una infraestructura de comunicación pública como es Internet. Para conseguir garantizar la confidencialidad, integridad y autenticidad en las VPN´s creadas, hemos utilizado tecnologías de seguridad IPSEC (descritas anteriormente).

Para definir la seguridad en una red de comunicaciones se requiere:

- Política de seguridad
- Procedimientos para implementar dicha política
- Tecnologías que proporcionen la protección.

Un problema que surgió fue las distintas configuraciones que se tenían que realizar en los equipos (routers), según el tipo de línea contratada en cada Consejería Laboral, lo que obligaba a configurar y parametrizar nuestro equipo (router) según el acceso, fuese a través de RDSI, xDSL, etc. Para resolver este problema se determinó que fuese en cada caso el operador, el que suministrara una conexión ethernet (a través de un equipo de acceso instalado al efecto), y así evitar los problemas que se pudieran generar sí intentábamos realizar nosotros la conexión directamente al módem instalado por el operador. De esta forma además nuestros equipos eran todos de iguales características y no específicos para cada tipo de conexión.

Por otro lado los equipos se han configurado previamente (tanto para la creación de las VPN´s, reglas del Firewall y el servicio de detección de intrusión- IDS) desde los SSCC y su puesta en funcionamiento es inmediata, al tener únicamente que conectar una puerta ethernet de nuestro router al equipo de acceso del operador y la otra al switch de la red interna de cada Consejería Laboral.

Por otro lado se requiere que el operador ofrezca directamente acceso a Internet y poder además utilizar este acceso para establecer las VPN´s con los servicios centrales. Esto nos obligaba a proteger estas redes remotas de accesos no deseados mediante un Firewall, ya que el acceso directo a Internet desde estas redes permiten ser objeto de ataques desde la misma.

Dentro de las distintas soluciones analizadas, hemos considerado la más idónea el router CISCO 1710, por incorporar la opción VPN con soporte IPSEC, Firewall y detección de intrusión (IDS), en el mismo equipo, a un precio competitivo.

Las características de este equipo pueden verse en:

“ http://www.cisco.com/univercd/cc/td/doc/pcat/1710.htm “

Para implementar las VPN´s entre los SSCC y las Consejerías laborales del MTAS, se necesitan cubrir los siguientes requerimientos:

1.- En cada país se contratará un acceso a Internet a través de un proveedor local y utilizando accesos vía RDSI, ADSL, etc. (La velocidad mínima será de 64 Kbps)

2.- El proveedor elegido deberá suministrar un equipo (que de acceso a Internet), al cual se conectara a nuestro router a través de una puerta Ethernet y además deberá proveer dos direcciones IP públicas fijas, una para el puerto ethernet de su equipo y otra para la de nuestro router.

Terminador de túneles en los SSCC:

La VPN se hará entre el Cisco 1710 y un terminador de túneles en los SSCC. Inicialmente se utilizará el propio Firewall corporativo y según el incremento de utilización que pudiera generarse por los algoritmos de cifrado y el numero de túneles simultáneos, se ampliara este equipo o se instalar un equipo específico como terminador de túneles en la red interna.

Configuración de Ipsec

- La autenticación entre el router y el firewall se realiza actualmente mediante la opción de

  - clave compartida -. La opción de usar certificados digitales no la hemos considerado inicialmente, por ser nuestra red en forma de estrella y solo con 27 delegaciones fijas, sin necesidad de conectarse directamente entre ellas. Esta opción se implementara en un futuro, para unificarlo con la política de seguridad de la Organización.

- Para el cifrado hemos utilizado el algoritmo - 3DES -, y el método de seguridad – ESP -.

- Como algoritmo de hash utilizamos el - SHA -.
- Como método de operación utilizamos – modo túnel -.

En el router de cada Consejería Laboral estableceremos las reglas del Firewall (en base a la política de seguridad establecida para nuestra Organización), a través de listas de acceso en las que podemos controlar:

- Tipo de tráfico (tcp, udp,..)
- Filtrado en entrada, salida o ambos.
- Tipo de servicio (esp, icmp,..)
- Host o red origen y destino
- Etc.

Este tipo de listas de acceso se aplican al interface que conecta el router con Internet tanto en entrada como en salida, con lo que el control y protección que tenemos sobre la red interna es bastante fuerte.

Se realizó una primera prueba piloto, simulando en nuestras instalaciones a través de un acceso ADSL en un equipo aislado de nuestra red, una primera conexión VPN´s a la red interna, lo cual nos ayudo a conocer las peculiaridades en la configuración de este equipo y asegurarnos de su perfecto funcionamiento. Una vez depurada su configuración se realizó una segunda prueba en la Consejería Laboral de Washington, comprobando una vez mas el perfecto funcionamiento, tanto en la creación de la VPN's de forma simultanea por los distintos usuarios de esta red, como la protección de la misma mediante la política de seguridad configurada en el Firewall.

Podemos finalmente indicar, que el resultado de las pruebas del proyecto piloto realizado al efecto, han dado un resultado satisfactorio y que con esta solución tendremos a todos nuestros usuarios remotos conectados a nuestra red interna, de forma segura, ofreciéndoles los mismos servicios, que los que tiene actualmente cualquier otro usuario de la red corporativa.