1. ÍNDICE

2. MEMORIA

2.1. INTRODUCCIÓN

_____ precisa la resolución de los problemas de comunicación de su empresa en cuanto a la movilidad de sus viajantes, la velocidad de acceso a los datos de la central y la seguridad contra elementos externos que puedan interferir en el buen funcionamiento de la empresa. Se requiere la interconexión de los 25 viajantes empleados de la empresa con la intranet de la empresa y entre ellos mismos, posibilitando la capacidad a todos ellos de conectarse en cualquier momento y en cualquier lugar de España y poder acceder a los datos del servidor central y a cualquier elemento conectado a ella, tales como ordenadores de la red Lan, otros viajantes conectados a la red, impresoras remotas, faxes, etc.

La solución adoptada es la creación de una Red Privada Virtual, este tipo de red, también llamada red VPN por sus siglas en inglés, es una red privada y segura que discurre por una red pública y no segura, de modo que ambas comparten unos mismos puntos de entrada y de salida. Se configurará una red WAN (Wide Area Network o Red de área extensa) que atraviese la red Internet ya existente, lo que permitirá reducir los costes de mantenimiento al utilizarse sólo una conexión WAN en lugar de dos conexiones distintas. Pero no sólo es posible utilizar una red WAN a través de otra, sino que, además, es posible hacerlo de forma segura para salvaguardar la integridad de los datos que se transmitan ya que éstos son encriptados al pasar por los segmentos públicos. La tecnología de VPN proporciona un medio para usar el canal público de Internet como una canal apropiado para comunicar los datos privados. Con la tecnología de encriptación y encapsulamiento, una VPN, crea un pasillo privado a través de Internet y consigue reducir las responsabilidades de gestión de un red local.

Los posibles escenarios de red privada virtual basados en la configuración habitual de un servidor VPN son:

- Acceso remoto de VPN para empleados.
- Acceso de sucursales a petición.

- Acceso persistente de las sucursales.
- Extranet para socios comerciales.
- VPN y conexión telefónica con autenticación RADIUS.

Las razones que empujaron a adoptar la solución en ese sentido son, fundamentalmente de costes: resulta mucho más barato interconectar a los empleados utilizando una infraestructura pública que desplegar una red físicamente privada, también abaratará los costes en facturas telefónicas debido a que las tarifas de conexión a Internet son sensiblemente más baratas que las de las llamadas directas sobre todo con las relacionadas con la telefonía móvil.

En los enlaces Cliente−Red que se crearán se encapsula PPP(Point To Point Protocol). Las tramas del cliente se encapsulan en PPP, y el PPP resultante se encapsula para crear el VPN. Este tipo de enlace nos proporciona un acceso seguro de un cliente a la red, con total movilidad y con independencia del Proveedor de Servicios de Internet (ISP) por el que se entre.

El encapsulado de las tramas PPP en datagramas se puede realizar de dos formas según el protocolo a usar:

- **PPTP (Point−to−Point Tunneling Protocol)**

Encapsulado de tramas PPP en datagramas IP, utilizando una versión extendida del GRE (Generic Routing Encapsulation, protocolo IP 47). La conexión de control se realiza sobre TCP, puerto 1723.

Actualmente este protocolo, aunque muy popular en el mundo Microsoft, está siendo sustituido por el L2TP. La implementación de Microsoft, además, sufre de varios importantísimos errores de diseño que hacen que su protección criptográfica sea inefectiva para alguien más motivado que un simple observador casual. Por lo tanto, está opción será descartada.

- **L2TP (Layer 2 Tunnelling Protocol)**

Encapsulado de tramas PPP sobre cualquier medio, no necesariamente redes IP. En el caso IP se usa UDP, puerto 1701. Tras un largo proceso como borrador, L2TP pasa a ser una propuesta de estándar en Agosto de 1.999. Debido a las grandes ventajas de este protocolo, éste será el que será instalado en los equipos.

También se hará uso del protocolo:

- **IPSec**

IPSec es el nuevo marco de seguridad IP, definido con el advenimiento del IPv6. Aunque IPv6 está muy poco difundido en este momento, la tecnología marco IPSec se está utilizando ya, lo que asegura, entre otras cosas, la interoperatividad de los sistemas de diversos fabricantes. IPSec integra confidencialidad, integridad y autentificación en un mismo marco interoperante.

La instalación y configuración de la red se verá desde dos puntos:

- Instalación y configuración del servidor VPN.
- Instalación y configuración de los clientes de acceso remoto.

Instalación y configuración del servidor VPN.

Para que los empleados puedan acceder a la intranet de la empresa desde fuera, el servidor VPN debe estar conectado permanentemente a Internet y además debe tener un dirección IP fija, la cual usarán los clientes de acceso remoto para iniciar la conexión VPN.

El servidor conectará a Internet a través de un MODEM que estará conectado al ISP continuamente y conectado a la red LAN con una tarjeta de red. En la maquina servidor se instalará el paquete Windows 2000 Server el cual incluirá el servicio de servidor de acceso remoto (RAS) y los protocolos necesarios para la conexión (PPTP, L2TP, IPsec).

Cuando un cliente pide una conexión VPN al servidor central, el servidor VPN lo autentica y a partir de entonces se reciben paquetes del cliente, el servidor desencapsula y desencripta los paquetes y, a continuación, los coloca en la red.

Instalación y configuración de los clientes de acceso remoto.

El equipo del cliente de acceso remoto consta de un ordenador portátil con el paquete de Windows 2000 instalado, una tarjeta PCMCIA, un teléfono móvil y un cable de datos para conectar el portátil con el teléfono. En la ranura PCMCIA del ordenador portátil elegido se insertará la tarjeta PCMCIA, necesaria para realizar la conexión teléfono− PC. portátil, éste posee un MODEM por si existiera la posibilidad de realizar la conexión a Internet a través de la Red Telefónica Básica, lo cual abarataría aún más el coste de la comunicación.

Un cliente de acceso remoto realiza una conexión VPN de acceso remoto que conecta a la red privada mediante la creación de una conexión de acceso *telefónico a redes*, la cual incluirá la dirección de Internet de la red local de la empresa, los protocolos y software necesarios para realizarlo están incluidos en el paquete de Windows 2000.

El servidor VPN proporciona acceso a los recursos del servidor VPN o a toda la red a la que está conectado el servidor VPN. Los paquetes enviados desde el cliente remoto a través de la conexión VPN se originan en el equipo cliente de acceso remoto.

El cliente de acceso remoto (el cliente VPN) se autentica ante el servidor de acceso remoto (el servidor VPN) y, para realizar la autenticación mutua, el servidor se autentica ante el cliente.

El cliente estará conectado a la red local de la empresa y aparecerá como un usuario más de la misma, con los mismos privilegios y recursos disponibles, sin importar en qué lugar del mundo se encuentre.

2.2. OBJETIVOS

1º. Proporcionar movilidad a los empleados.

2º. Acceso a la base de datos central sin utilización de operadores telefónicos .

3º. Interconexión total a la red de todos los comerciales (empleados), de forma segura a través de una infraestructura pública.

4º. Intercambio de información en tiempo real.

5º.Correo electrónico corporativo

6º.Acceso remoto a la información corporativa

7º. Teletrabajo.

8º. Flexibilidad y facilidad de uso.

9º. Obtención de la máxima velocidad de transferencia de datos usando con eficiencia los recursos empleados.

10º. Fácil adaptación a las nuevas tecnologías.

2.3. ANTECEDENTES

Inicialmente los viajantes empleados de la empresa accedían a los datos que necesitaban de la central mediante llamadas telefónicas, en ella se encontraban varias operadoras que se encargaban de acceder a los datos y comunicárselos a los empleados.

Ante al gran desarrollo de las tecnologías de telecomunicaciones se pensó en una reestructuración total en el modo de acceder a los datos por parte de los viajantes, creando una red que interconectara a éstos con la central y posibilitando que tuvieran acceso total a todos los equipos conectados a la red con independencia del tiempo o del lugar donde se encontraran.

La empresa deseaba también una garantía de seguridad en las transferencias de información que evitara que sus datos fuesen interceptados por personas ajenas a la empresa.

2.4. ESTADO DEL ARTE

Pasamos a describir el estado actual de la tecnologías existentes en el momento para la posible realización del proyecto, y discerniremos entre una u otra, dependiendo del punto de vista económico, prestaciones, fiabilidad y posible ampliaciones de servicios en el futuro.

- Tecnología GPRS

Con el sistema GPRS (General Packet Radio Service), el acceso a la red de paquetes se lleva al nivel del usuario del móvil a través de protocolos como los TCP/IP (Transmission Control Protocol/Internet Protocol), X.25, y CLNP (Connectionless Network Protocol), sin ninguna otra necesidad de utilizar conexiones intermedias por conmutación de circuitos. La tecnología GPRS representa un paso más hacia los sistemas móviles de 3ª Generación o UMTS, al posibilitar que los terminales estén permanentemente conectados a la red, con una velocidad dependiente de la aplicación, pudiendo tarificar únicamente el volumen de datos transferidos y no como ahora por el tiempo de la conexión.

En el ámbito de los servicios, las posibilidades del GPRS son innumerables, ya que la velocidad de transmisión de los datos es muy superior a la actual. Mientras que en el GSM básico los datos circulan a 9,6 kbit/s por segundo, GPRS proporciona velocidades de hasta 50 kbit/s por segundo, dependiendo del tipo de terminal con el que se realice la transmisión.

Esta fue la primera opción que se barajó para la solución del problema pero tuvo que ser descartada ya que al ser una tecnología en fase de implantación en España, no era viable la realización de un proyecto que usara este método. Sin embargo el equipo para la realización del proyecto se ha elegido con vista a que si la empresa lo cree oportuno y llegado el día en que GPRS sea comercializada, sea fácil la implantación de esta tecnología.

- Conexión a través de RTB o RDSI gestionada por un servidor RAS

Tanto RTB como RDSI son redes que nos proporcionan una comunicación más rápida que a través de la red GSM, pero debido a que el coste necesario para instalar este servicio se incrementa bastante, a que la necesidad de buscar una toma para acceder a estas redes por parte de los empleados reduce su movilidad y a que si se usan teléfonos móviles en las comunicaciones tendremos una velocidad de datos de 9,6 kbit/s por lo que se desaprovecha el ancho de banda que nos proporcionan estas redes, esta opción fue rechazada.

- Interconexión a través de una VPN (Red Privada Virtual)

Esta fue la opción elegida finalmente ya que brinda la mejor escalabilidad y rendimiento del mercado ofreciendo conectividad segura a través de una infraestructura pública. Además ofrece gran reducción de costos debido a que el usuario tiene la posibilidad de conectarse a la empresa desde cualquier lugar donde se encuentre simplemente con una conexión a Internet, se estima que una solución VPN puede rebajar los costos entre un 20% y un 40% comparada con las conexiones punto a punto.

2.5. DESCRIPCIÓN DEL PROYECTO.

A continuación se describe la manera en que el escenario de red privada virtual se configurará mediante el sistema operativo Windows 2000.

El uso tanto de redes públicas como privadas para crear una conexión de red se denomina red privada virtual (VPN).

Una red privada virtual es la extensión de una red privada que comprende vínculos en redes compartidas o públicas como Internet. Con una VPN se pueden transmitir datos entre dos equipos a través de una red compartida o pública imitando el funcionamiento de un vínculo privado punto a punto. La interconexión de una red privada virtual es la creación y configuración de este tipo de redes.

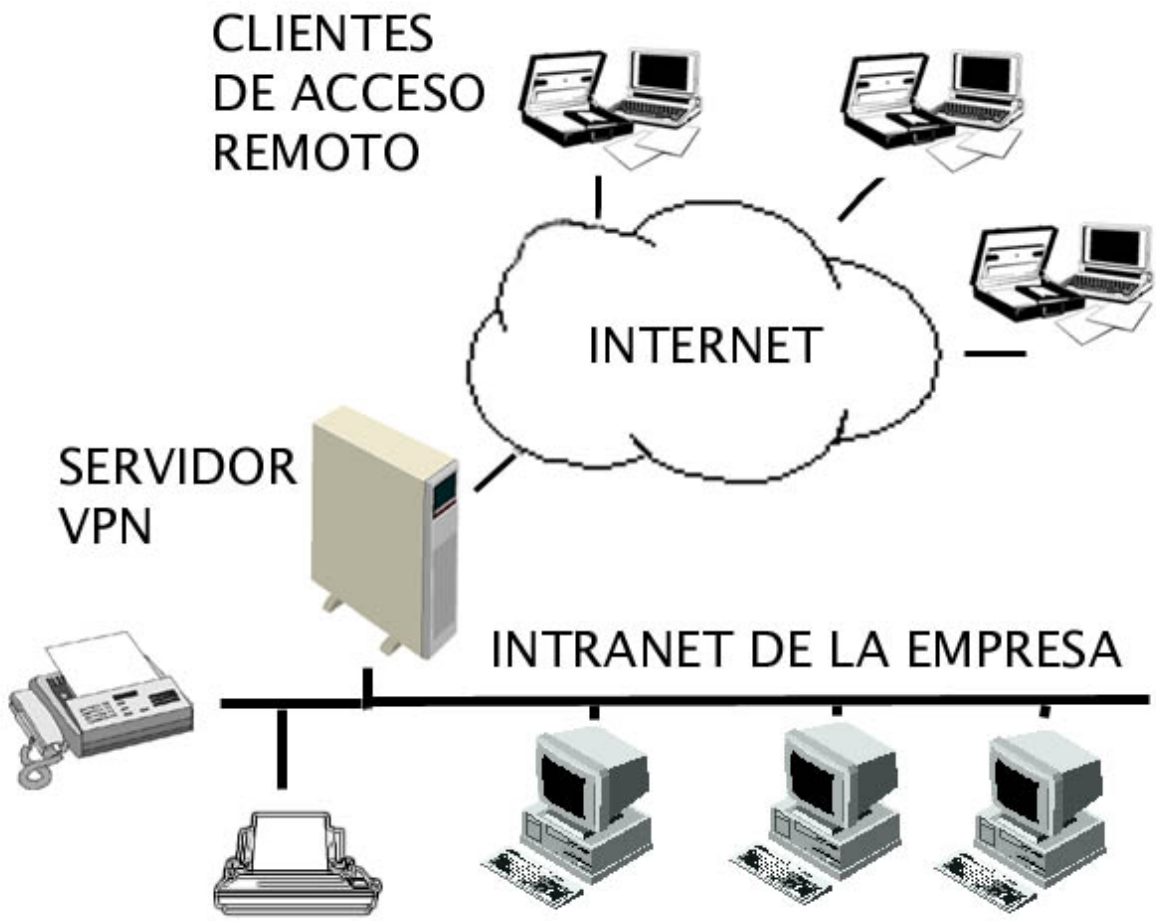
Para imitar un vínculo punto a punto, los datos se encapsulan o se envuelven con un encabezado que proporciona información de enrutamiento, lo que permite que los datos atraviesen la red compartida o pública hasta llegar a su punto de destino. Para imitar un vínculo privado, los datos se cifran para conservar la confidencialidad. Los paquetes interceptados en la red compartida o pública no se pueden descifrar sin las claves de cifrado. El vínculo en el que se encapsulan y se cifran los datos privados es una conexión de red privada virtual (VPN).

El servidor VPN, que se encuentra en la oficina central, proporciona acceso remoto y conexiones VPN PPTP y L2TP. Además, el servidor VPN proporciona el enrutamiento de paquetes hacia ubicaciones en intranet o Internet.

Esta empresa será provista de una dirección IP fija con un dominio en Internet proporcionado por un proveedor PSI que además proveerá una página Web , cuentas de correo electrónico y servidor FTP.

Todo esto será creado, mantenido y administrado por dicha empresa a la que se le pagará una cuota mensual.

El esquema general de la red es el indicado por la siguiente figura:



Esquema general de la red

2.5.1. Instalación y configuración del servidor VPN.

El equipo servidor VPN se conectará a la Intranet de la empresa a través de la tarjeta de red instalada en él y se instalará el MODEM conectándolo a su puerto serie y éste a su vez a la Red Telefónica Básica.

Se instalará en el equipo servidor el paquete Windows 2000 Server, el cual contiene el software y los protocolos necesarios para establecer conexiones con los clientes de acceso remoto.

Configuración común del servidor VPN.

Para distribuir una solución VPN a la empresa interesada, se realizará un análisis y una toma de decisiones acerca de su diseño teniendo en cuenta lo siguiente:

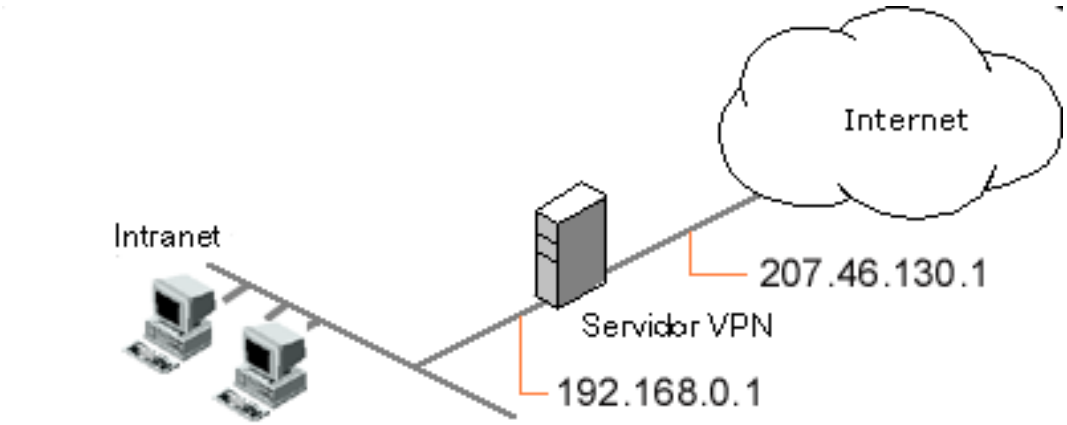
- Configuración de la red.
- Configuración de las directivas de acceso remoto.
- Configuración del dominio.
- Configuración de la seguridad.

Configuración de la red

Los elementos clave de la configuración de la red son:

- La intranet de la empresa utiliza las direcciones 192.168.0.1 con la máscara de subred 255.255.255.0. El equipo servidor VPN está conectado a Internet las 24 horas a través de un ISP con una dirección IP fija.
- La dirección IP fija de Internet, asignada por el proveedor de servicios Internet (ISP) a la empresa, se supondrá que será la 207.46.130.1. En Internet se alude a la dirección IP mediante el nombre de dominio vpn.francisco.comerciales.com.
- El equipo servidor VPN está configurado con una dirección IP estática, con el fin de asignar clientes de acceso remoto.

La figura 1 muestra la configuración de red del servidor VPN



Configuración de red del servidor VPN.

El equipo servidor VPN se configura de la siguiente manera:

- Se instala el hardware en el servidor VPN.

Se instalará el adaptador de red utilizado para conectar al segmento de Intranet, y el MODEM utilizado para la conexión a Internet siguiendo las instrucciones del fabricante de ambos adaptadores. Cuando los controladores estén instalados y en funcionamiento, ambos adaptadores aparecerán como conexiones de área local en la carpeta Conexiones de red y de acceso telefónico.

- Configuración TCP/IP en los adaptadores LAN y WAN.

Para el adaptador de red de área local se configura la dirección IP 192.168.0.1 con la máscara de subred 255.255.255.0. Para el MODEM se configura la dirección IP 207.46.130.1 con la máscara de subred 255.255.255.255. Para ninguno de los dos elementos se configurará una puerta de enlace, o *gateway*, predeterminada. También se configurarán las direcciones de servidor DNS y WINS.

- Instalación del Servicio de enrutamiento y acceso remoto.

Se ejecutará el Asistente para la instalación del servidor de enrutamiento y acceso remoto. En el asistente, se seleccionará la opción ***Servidor configurado manualmente***. Para obtener más información, consultar el procedimiento "Habilitar el Servicio de enrutamiento y acceso remoto" en el anexo A.

Cuando el asistente finalice, se habrá configurado un conjunto de direcciones IP estáticas con la dirección IP inicial 192.168.0.1 y la dirección IP final 192.168.0.254. Esto crea un conjunto de direcciones estáticas para

un máximo de 253 clientes VPN.

Para obtener más información, consulte el procedimiento "Crear un grupo de direcciones IP estáticas" en el anexo B.

El método predeterminado para autenticar el acceso remoto y las conexiones de marcado a petición consiste en utilizar la autenticación de Windows, que resulta apropiada para esta configuración que contiene únicamente un servidor VPN.

- Configuración de rutas estáticas en el servidor VPN para llegar a ubicaciones de Internet.

Para llegar a ubicaciones de Internet, se establecerá una ruta estática con la siguiente configuración:

- Interfaz: el MODEM conectado a Internet
- Destino: 0.0.0.0
- Máscara de red: 0.0.0.0
- Puerta de enlace: 0.0.0.0
- Métrica: 1

Esta ruta estática resume todos los destinos en Internet. Permite que el servidor VPN responda a un cliente de acceso remoto o a una conexión VPN de enrutador de marcado a petición desde cualquier parte en Internet.

- Aumentar el número de puertos PPTP y L2TP.

De forma predeterminada, únicamente cinco puertos L2TP y otros cinco PPTP están habilitados para conexiones VPN. El número de puertos L2TP y PPTP aumenta hasta 253. Para obtener más información, consultar el procedimiento "Agregar puertos PPTP o L2TP" en el anexo C.

- Configuración de filtros de paquetes PPTP y L2TP sobre IPSec.

Tanto PPTP como L2TP sobre filtros de paquetes IPSec se configurarán en el MODEM conectado a Internet. Para evitar que el servidor VPN envíe o reciba tráfico en su interfaz de Internet, excepto el tráfico PPTP o L2TP sobre IPSec proveniente de clientes de acceso remoto, se configurarán PPTP y L2TP sobre filtros de entrada y salida IPSec en la interfaz de Internet. Debido a que el enrutamiento IP está habilitado en la interfaz de Internet, si no se configura L2TP sobre filtros IPSec y PPTP en la interfaz de Internet del servidor VPN, todo el tráfico recibido en esta interfaz se enrutará y es posible que se reenvíe tráfico no deseado a la intranet. Para obtener más información, consultar los procedimientos "Agregar filtros de paquetes PPTP" y "Agregar filtros de paquetes L2TP" en el anexo D.

- Establecimiento del número de teléfono para los dispositivos PPTP y L2TP.

Para ayudar en la configuración de directivas de acceso remoto que limiten las conexiones VPN provenientes de usuarios de Internet, las propiedades de puerto para los dispositivos ***minipuerto WAN (PPTP)*** *y* ***minipuerto WAN (L2TP)*** se modificarán con la dirección IP de la interfaz de Internet del servidor VPN en el campo ***Número de teléfono para este dispositivo***. Para obtener más información, consulte el procedimiento "Configurar un número de teléfono en un dispositivo" en el anexo E.

Configuración de la directiva de acceso remoto

El permiso de acceso remoto en todas las cuentas de usuario se establecerá como ***Controlar acceso a través de la directiva de acceso remoto***. La concesión de permisos de acceso remoto a intentos de conexión se controlará mediante la configuración de permisos de acceso remoto en la primera directiva de acceso remoto

correspondiente. Las directivas de acceso remoto se usan para aplicar diferentes configuraciones de conexión VPN basadas en la pertenencia a grupos y la directiva de acceso remoto predeterminada llamada ***Permitir el acceso si está habilitado el permiso de acceso telefónico*** se eliminará.

Configuración del dominio

Para aprovechar la capacidad para aplicar las diferentes configuraciones de conexión a distintos tipos de conexiones VPN se creará el siguiente grupo de Windows 2000:

- VPN_Usuarios (VPN_Users)

Se usa para las conexiones VPN de acceso remoto

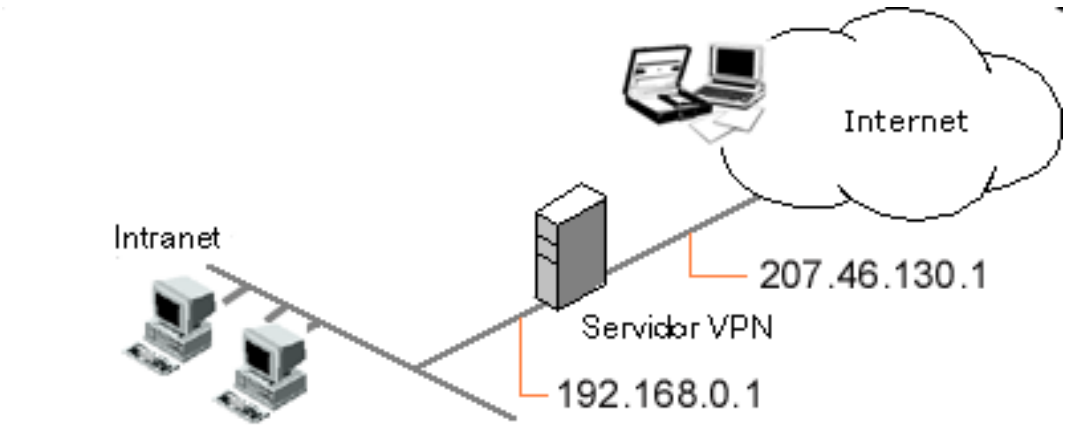
Configuración de la seguridad

Para habilitar las conexiones L2TP sobre IPSec, el dominio de la empresa se configura para inscribir automáticamente certificados de equipo para todos los miembros del dominio.

Para obtener más información, consulte el procedimiento "Configurar la asignación automática de certificados" en el anexo F.

El acceso remoto para empleados de la empresa se distribuirá por Internet mediante las conexiones VPN de acceso remoto en función de la configuración establecida en la sección "Configuración común del servidor VPN" de este documento y en la configuración adicional siguiente.

La figura 2 muestra el servidor VPN que proporciona conexiones VPN de acceso remoto.



El servidor VPN que proporciona conexiones VPN de acceso remoto

Configuración del dominio

Para cada empleado con acceso a la red privada virtual:

- El permiso de acceso remoto en las propiedades de acceso telefónico de la cuenta del usuario se establecerá a ***Controlar acceso a través de la directiva de acceso remoto.***
- La cuenta de usuario se agregará al grupo VPN_Usuarios de Windows 2000.

Configuración de la directiva de acceso remoto

Para definir los parámetros de autenticación y de cifrado para los clientes VPN de acceso remoto se creará la siguiente directiva de acceso remoto:

- Nombre de directiva: clientes VPN de acceso remoto

Condiciones:

- ***Puerto−NAS*** se establecerá a Virtual (VPN).
- ***Grupos−Windows*** se establecerá a VPN_Usuarios.
- ***Id−estación−llamada*** se establecerá a 207.46.130.1.

- El permiso se establecerá a ***Conceder permiso de acceso remoto*.**

Configuración del perfil:

- Ficha ***Autenticación***: se seleccionará ***Protocolo de autenticación extensible*** para usar el certificado de equipo instalado. También se seleccionarán Autenticación cifrada de Microsoft versión 2 (MS−CHAP v2) y ***Autenticación cifrada de Microsoft (MS−CHAP).***
- Ficha ***Cifrado: Básica y Fuerte*** son las únicas opciones seleccionadas.

Nota.− La condición ***Id−estación−llamada*** se establecerá como la dirección IP de la interfaz de Internet para el servidor VPN. Únicamente se permitirán los túneles iniciados desde Internet. No se permiten los túneles iniciados desde la Intranet. Aquellos usuarios de la empresa que necesiten tener acceso a Internet desde la intranet deben pasar por el servidor proxy donde se controla y supervisa el acceso a Internet.

2.5.2. Instalación y configuración de los clientes de acceso remoto.

En cada ordenador portátil se instalará el paquete Windows 2000. Se instalará también el software incluido con el cable de datos del teléfono móvil que se observa en la siguiente figura:

Teléfono móvil conectado a la tarjeta PCMCIA a través del cable de datos

El cable se conectará a la tarjeta PCMCIA insertada en el PC. portátil y a la salida de datos del móvil. El terminal (teléfono) debe encenderse después de haber sido conectado a la tarjeta PCMCIA, con lo que se producirán dos breves pitidos señalando que todo es correcto.

Configuración de clientes de acceso remoto basada en L2TP

El equipo de acceso remoto iniciará una sesión en el dominio de la empresa mediante una conexión de red de área local (LAN) con la intranet de esta organización y recibirá un certificado por la inscripción automática. A continuación, el Asistente para realizar conexión nueva se usará para crear una conexión VPN con la siguiente configuración:

- Nombre de host o dirección IP: vpn.francisco.comerciales.com

La configuración de la conexión VPN se modificará de la siguiente manera:

- En la ficha Funciones de red, el Tipo de servidor de acceso telefónico al que estoy llamando se establecerá a Protocolo de túnel de capa 2 (L2TP). Cuando Tipo de servidor de acceso telefónico al que estoy llamando se establece a Automático, se probará primero con una asociación de seguridad IPSec (SA) para una conexión L2TP. Si la asociación de seguridad IPSec no se efectúa correctamente, se intentará una conexión PPTP.

2.6. CONCLUSIONES

Se han cumplido sobradamente nuestros tres principales objetivos en cuanto a la interconexión de todos los equipos con los usuarios móviles, la capacidad de los viajantes de tener una libre movilidad lo que facilitará enormemente su trabajo y la protección de los datos que viajan por la red. El uso de este tipo de red nos ha facilitado un menor coste en el presupuesto de equipos, así como menor complejidad de manejo por parte de los usuarios finales. Por último, el uso del protocolo Ipsec nos proporciona una gran garantía de privacidad y autenticación de los datos transmitidos.

En cuanto a los aspectos negativos, reseñar que el plazo de ejecución total del proyecto va a depender en parte de la puntualidad en los plazos por parte de los proveedores de materiales y de servicios.

2.7. ANEXOS.

ANEXO A. Habilitar el Servicio de enrutamiento y acceso remoto

Se hará clic en ***Inicio***, seleccionar ***Programas, Herramientas administrativas*** y, a continuación, se hará clic en ***Enrutamiento y acceso remoto***.

De manera predeterminada, el equipo local aparecerá en la lista como un servidor.

Para agregar otro servidor, en el árbol de la consola se hará clic con el botón secundario del *mouse* en ***Estado de servidor*** y, a continuación, en ***Agregar Servidor***.

En el cuadro de diálogo ***Agregar Servidor***, se hará clic en la opción que corresponda y, a continuación, se hará clic en ***Aceptar***.

En el árbol de la consola, se hará clic con el botón secundario del *mouse* (ratón) en el servidor que desea habilitar y, a continuación, se hará clic en ***Configurar y habilitar el enrutamiento y el acceso remoto***.

En el Asistente para la instalación del servidor de enrutamiento y acceso remoto se hará clic en ***Continuar***.

En ***Configuraciones comunes***, se hará clic en ***Servidor configurado manualmente***, en ***Siguiente*** y, a continuación, en ***Finalizar***.

Cuando se indique, se reiniciará el servicio de ***Enrutamiento y acceso remoto***.

Nota.– Si este servidor es un miembro de un dominio de Active Directory en Windows 2000 y usted no es administrador de dominios, indique a su administrador de dominios que agregue la cuenta del equipo de este servidor a los grupos de seguridad de los servidores RAS e IAS en el dominio del que este servidor es miembro. El administrador de dominios puede agregar la cuenta del equipo al grupo de seguridad de los servidores RAS e IAS mediante ***Usuarios y equipos de Active Directory*** o mediante el comando ***netsh ras***

add registeredserver.

ANEXO B. Crear un grupo de direcciones IP estáticas

Se hará clic en ***Inicio***, se seleccionará ***Programas***, ***Herramientas administrativas*** y, a continuación, se hará clic en ***Enrutamiento y acceso remoto***.

En el árbol de la consola, se hará clic con el botón secundario del *mouse* (ratón) en el servidor para el que desea crear un grupo de direcciones IP estáticas y, a continuación, se hará clic en ***Propiedades***.

En la ficha ***IP***, se hará clic en ***Conjunto de direcciones estáticas*** y, a continuación, se hará clic en ***Agregar***.

En ***Dirección IP inicial***, se escribirá una dirección IP inicial y, a continuación, se escribirá una dirección IP final para el intervalo en ***Dirección IP final*** o el número de direcciones IP en el intervalo de ***Número de direcciones***.

Se hará clic en ***Aceptar*** y, a continuación, se repetirán los pasos 3 y 4 para todos los intervalos que desee agregar.

Nota.– Si el conjunto de direcciones IP estáticas se compone de intervalos de direcciones IP de una subred independiente, se tendrá que habilitar un protocolo de enrutamiento IP en el equipo servidor de acceso remoto o agregar rutas IP estáticas que están formadas por {Dirección IP, Máscara} de cada intervalo de las rutas de la intranet. Si no se agregan las rutas, los clientes de acceso remoto no podrán recibir el tráfico de los recursos de la intranet.

ANEXO C. Agregar puertos PPTP o L2TP

Se hará clic en ***Inicio***, se seleccionará ***Programas***, ***Herramientas administrativas*** y, a continuación, se hará clic en ***Enrutamiento y acceso remoto***. En el árbol de consola, se hará clic en el servidor para el que se desea configurar los puertos PPTP o L2TP.

En el panel de detalles, se hará clic con el botón secundario del *mouse* en ***Puertos*** y, a continuación, se hará clic en ***Propiedades***.

En el cuadro de diálogo ***Propiedades de puertos*** se hará clic en ***Minipuerto WAN (PPTP)*** o ***Minipuerto WAN (L2TP)*** y, a continuación, se hará clic en ***Configurar***.

En ***Número máximo de puertos*** se escribirá el número de puertos y, a continuación, se hará clic en ***Aceptar***.

Se hará clic en ***Aceptar*** para guardar los cambios efectuados en las propiedades de puertos.

ANEXO D. Agregar filtros de paquetes PPTP

Se hará clic en ***Inicio***, se seleccionará ***Programas***, ***Herramientas administrativas*** y, a continuación, se hará clic en ***Enrutamiento y acceso remoto***.

En el árbol de la consola, se hará doble clic en el servidor para el que se desea configurar el filtrado de paquetes PPTP.

Se hará doble clic en ***Enrutamiento IP***.

Se hará clic en ***General***.

En el panel de detalles, se hará clic con el botón secundario del *mouse* en la interfaz que esté conectada a Internet y, a continuación, se hará clic en ***Propiedades***.

En la ficha ***General***, se hará clic en ***Filtros de entrada***.

En el cuadro de diálogo ***Filtros de entrada***, se hará clic en ***Agregar***.

En el cuadro de diálogo ***Agregar filtro IP***, se activará la casilla de verificación ***Red de destino***. En ***Dirección IP*** se escribirá la dirección IP del servidor VPN o de la interfaz de Internet del enrutador de marcado a petición, y en ***Máscara de subred*** se escribirá ***255.255.255.255***. En ***Protocolo***, se hará clic en ***Otros***. En ***Número de proto*****colo** se escribirá ***47*** y, a continuación, se hará clic en ***Aceptar***.

En el cuadro de diálogo ***Filtros de entrada***, se hará clic en ***Agregar***.

En el cuadro de diálogo ***Agregar filtro IP***, se activará la casilla de verificación ***Red de destino***. En ***Dirección IP*** se escribirá la dirección IP del servidor VPN o de la interfaz de Internet del enrutador de marcado a petición, y en ***Máscara de subred*** se escribirá ***255.255.255.255***. En ***Protocolo***, se hará clic en ***TCP***. En ***Puerto de destino*** se escribirá ***1723*** y, a continuación, sehará clic en ***Aceptar***.

En el cuadro de diálogo ***Filtros de entrada***, se hará clic en ***Agregar***.

En el cuadro de diálogo ***Agregar filtro IP***, se activará la casilla de verificación ***Red de destino***. En ***Dirección IP*** se escribirá la dirección IP del servidor VPN o de la interfaz de Internet del enrutador de marcado a petición, y en ***Máscara de subred*** se escribirá ***255.255.255.255***. En ***Protocolo***, se hará clic en ***TCP [establecido]***. En ***Puerto de origen*** se escribirá ***1723*** y, a continuación, se hará clic en ***Aceptar***.

En el cuadro de diálogo ***Filtros de entrada***, se hará clic en ***Omitir todos los paquetes que no cumplen el criterio especificado abajo*** y, después, se hará clic en ***Aceptar***.

En la ficha ***General***, se hará clic en ***Filtros de salida***.

En el cuadro de diálogo ***Filtros de salida***, se hará clic en ***Agregar***.

En el cuadro de diálogo ***Agregar filtro IP*** se activará la casilla de verificación ***Red de origen***. En ***Dirección IP*** se escribirá la dirección IP del servidor VPN o de la interfaz de Internet del enrutador de marcado a petición, y en ***Máscara de subred*** se escribirá ***255.255.255.255***. En ***Protocolo***, se hará clic en ***Otros***. En ***Número de protocolo*** se escribirá ***47*** y, a continuación, se hará clic en ***Aceptar***.

En el cuadro de diálogo ***Filtros de salida***, se hará clic en ***Agregar***.

En el cuadro de diálogo ***Agregar filtro IP*** se activará la casilla de verificación ***Red de origen***. En ***Dirección IP*** se escribirá la dirección IP del servidor VPN o de la interfaz de Internet del enrutador de marcado a petición, y en ***Máscara de subred*** se escribirá ***255.255.255.255***. En ***Protocolo***, se hará clic en ***TCP***. En ***Puerto de origen*** se escribirá ***1723*** y, a continuación, se hará clic en ***Aceptar***.

En el cuadro de diálogo ***Filtros de salida***, se hará clic en ***Agregar***.

En el cuadro de diálogo ***Agregar filtro IP*** se activará la casilla de verificación ***Red de origen***. En ***Dirección IP*** se escribirá la dirección IP del servidor VPN o de la interfaz de Internet del enrutador de marcado a petición, y en ***Máscara de subred*** escribirá ***255.255.255.255***. En ***Protocolo***, se hará clic en ***TCP [establecido]***. En ***Puerto de destino*** se escribirá ***1723*** y, a continuación, se hará clic en ***Aceptar***.

En el cuadro de diálogo ***Filtros de salida***, se hará clic en ***Omitir todos los paquetes que no cumplen el criterio especificado abajo*** y, después, se hará clic en ***Aceptar***.

Se hará clic en ***Aceptar*** para guardar los cambios efectuados en la interfaz.

Agregar filtros de paquetes L2TP

Se hará clic en ***Inicio***, se seleccionará ***Programas***, ***Herramientas administrativas*** y, a continuación, se hará clic en ***Enrutamiento y acceso remoto***.

En el árbol de la consola, se hará doble clic en el servidor para el que desea configurar el filtrado de paquetes L2TP.

Se hará doble clic en ***Enrutamiento IP***.

Se hará clic en ***General***.

En el panel de detalles, se hará clic con el botón secundario del *mouse* en la interfaz que esté conectada a Internet y, a continuación, se hará clic en ***Propiedades***.

En la ficha ***General***, se hará clic en ***Filtros de entrada***.

En el cuadro de diálogo ***Filtros de entrada***, se hará clic en ***Agregar***.

En el cuadro de diálogo ***Agregar filtro IP***, se activará la casilla de verificación ***Red de destino***. En ***Dirección IP*** se escribirá la dirección IP del servidor VPN o de la interfaz de Internet del enrutador de marcado a petición, y en ***Máscara de subred*** se escribirá 255.255.255.255. En ***Protocolo***, se hará clic en ***UDP***. En ***Puerto de origen*** escriba ***500***. En ***Puerto de destino***, se escribirá ***500*** y, a continuación, se hará clic en ***Aceptar***.

En el cuadro de diálogo ***Filtros de entrada***, se hará clic en ***Agregar***.

En el cuadro de diálogo ***Agregar filtro IP***, se activará la casilla de verificación ***Red de destino***. En ***Dirección IP*** se escribirá la dirección IP del servidor VPN o de la interfaz de Internet del enrutador de marcado a petición, y en ***Máscara de subred*** se escribirá ***255.255.255.255***. En ***Protocolo***, se hará clic en ***UDP***. En ***Puerto de origen*** se escribirá ***1701***. En ***Puerto de dest*****no**, se escribirá ***1701*** y, a continuación, se hará clic en ***Aceptar***.

En el cuadro de diálogo ***Filtros de entrada***, se hará clic en ***Omitir todos los paquetes que no cumplen el criterio especificado abajo*** y, después, se hará clic en ***Aceptar***.

En la ficha ***General***, se hará clic en ***Filtros de salida***.

En el cuadro de diálogo ***Filtros de salida***, se hará clic en ***Agregar***.

En el cuadro de diálogo ***Agregar filtro IP*** se activará la casilla de verificación ***Red de origen***. En ***Dirección IP*** se escribirá la dirección IP del servidor VPN o de la interfaz de Internet del enrutador de marcado a petición, y en ***Máscara de subred*** se escribirá ***255.255.255.255***. En ***Protocolo***, se hará clic en ***UDP***. En ***Puerto de origen*** se escribirá ***500***. En ***Puerto de destino***, se escribirá ***500*** y, a continuación, se hará clic en ***Aceptar***.

En el cuadro de diálogo ***Filtros de sa*****lida**, se hará clic en ***Agregar***.

En el cuadro de diálogo ***Agregar filtro IP*** se activará la casilla de verificación ***Red de origen***. En ***Dirección IP*** se escribirá la dirección IP del servidor VPN o de la interfaz de Internet del enrutador de marcado a

petición, y en ***Máscara de subred*** se escribirá ***255.255.255.255***. En ***Protocolo***, se hará clic en ***UDP***. En ***Puerto de origen*** se escribirá ***1701***. En ***Puerto de destino***, se escribirá ***1701*** y, a continuación, se hará clic en ***Aceptar***.

En el cuadro de diálogo ***Filtros de salida***, se hará clic en ***Omitir todos los paquetes que no cumplen el criterio especificado abajo*** y, después, se hará clic en ***Aceptar***.

Se hará clic en ***Aceptar*** para guardar los cambios efectuados en la interfaz.

ANEXO E. Configurar un número de teléfono en un dispositivo

Se hará clic en ***Inicio***, seleccione ***Programas***, ***Herramientas administrativas*** y, a continuación, se hará clic en ***Enrutamiento y acceso remoto***.

En el árbol de consola, se hará clic en el servidor para el que desea configurar un número de teléfono.

En el panel de detalles, se hará clic con el botón secundario del *mouse* en ***Puertos*** y, a continuación, se hará clic en ***Propiedades***.

En el cuadro de diálogo ***Propiedades de puertos*** se hará clic en el dispositivo que corresponde al equipo VPN o de acceso telefónico y, a continuación, se hará clic en ***Configurar***.

En ***Número de teléfono para este dispositivo*** se escribirá el número de teléfono para el puerto. Para los puertos VPN, se escribirá la dirección IP de la interfaz de Internet del servidor VPN.

Se hará clic en ***Aceptar***.

ANEXO F. Configurar la asignación automática de certificados

Se iniciará la sesión como administrador de dominios.

Se hará clic en ***Inicio***, se seleccionará ***Programas***, ***Herramientas administrativas*** y se hará clic en ***Usuarios y equipos de Active Directory***.

En ***Usuarios y equipos de Active Directory***, se hará clic con el botón secundario del *mouse* en el dominio que contiene la entidad emisora de certificados (CA) y, a continuación, se hará clic en ***Propiedades***.

Se hará clic en la ficha ***Directiva de grupo***, en ***Directiva de dominio predeterminada*** y, después, en ***Modificar***.

En ***Directiva de grupo***, se hará doble clic en ***Configuración del equipo***, en ***Configuración de Windows***, en ***Configuración de seguridad*** y, después, se hará clic en ***Directivas de claves públicas***.

Se hará clic con el botón secundario del *mouse en* ***Configuración de la petición de certificados automática***, se hará clic en ***Nuevo*** y, después, se hará clic en ***Petición de certificados automática***.

En el cuadro de diálogo ***Asistente para instalación de petición automática de certificado***, se hará clic en ***Siguiente***.

En ***Plantillas de certificado***, se hará clic en ***Equipo*** y, después, en ***Siguiente***.

Se seleccionará su entidad emisora de certificados, se hará clic en ***Siguiente*** y, después, en ***Finalizar***.

Se cerrará la consola de ***Directiva de grupo***.

Para obtener un certificado inmediatamente en el servidor VPN mediante inscripción automática, se reiniciará el equipo servidor VPN o bien se escribirá ***secedit /refreshpolicy machine_policy*** en el símbolo del sistema de Windows 2000.

ANEXO G. IPSec (IP Security)

IPSec ofrece los servicios de integridad en las conexiones, garantía de que los datos recibidos por el receptor de la comunicación coinciden con los enviados por el emisor.

Para conseguir estos objetivos IPSec ofrece dos mecanismos de seguridad que pueden usarse por separado o de modo conjunto. La cabecera de autenticación AH (Autentication Header) y la cabecera de encapsulamiento de carga segura ESP (Encapsulating Security Payload). La primera ofrece integridad en las conexiones, autenticación de origen y opcionalmente servicio anti−reenvío. La segunda es más completa y además de los servicios ofrecidos por AH ofrece confidencialidad. Tanto AH como ESP se basan en la existencia de una suite criptográfica previamente negociada para el autenticado y cifrado de los paquetes, tal y como se verá a continuación.

Cada cabecera soporta dos modos de uso: modo transporte y modo túnel. En el primer caso se ofrece seguridad tanto a los protocolos de nivel superior como a las partes de la cabecera del datagrama IP no variables durante el camino del paquete, mientras que en el segundo se ofrece seguridad a todo el datagrama mediante el encapsulamiento de un paquete de nivel de red dentro de otro paquete de nivel de red.

Existen varios modos para implementar IPSec, tanto en un host o equipo final como en un gateway seguro (SG), que se encarga de aplicar los mecanismos de seguridad a los paquetes que deben pasar a través de él. Una posible solución es integrar IPSec en una implementación nativa IP. Para esto es necesario el acceso al código fuente del protocolo de red y es aplicable tanto a host como a gateways seguros. Otra posible solución es la implementación "Bumps−in−the−stack" (BITS), donde IPSec es implementado debajo de una pila IP existente, entre el protocolo IP nativo y el nivel de enlace. No es necesario el acceso al código fuente del protocolo de red. Esta implementación es normalmente empleada en hosts.

Asociaciones de Seguridad

Una SA (Security Association) o Asociación de Seguridad es una relación unidireccional que proporciona servicios de seguridad al tráfico mantenido por ella. Estos servicios son ofrecidos por una SA mediante el uso de las cabeceras AH o ESP, pero no ambos. Si tanto AH como ESP son requeridos entonces dos o más Asociaciones de Seguridad deberán ser creadas. Al ser una conexión unidireccional, en una comunicación típica entre dos host o dos gateways seguros se requieren dos SAs, una para cada dirección de la comunicación.

En concreto una SA es una estructura de datos que describe qué transformaciones serán aplicadas a un datagrama y cómo, especificando como parámetros el algoritmo de autenticación para las cabeceras AH y ESP, el algoritmo de cifrado para ESP, las claves de autenticación y cifrado, el tiempo de vida de estas, el tiempo de vida de la SA, número de secuencia para la prevención anti−reenvío, etc.

Cada Asociación de Seguridad es identificada unívocamente por una tripleta consistente en:

SPI (Security Parameter Index). Índice para identificación de SAs. Son datos de 32 bits de longitud, que o bien pueden ser creados de modo aleatorio al establecerse la SA o bien pueden ser dados por al sistema.

Dirección IP destino. Normalmente es una dirección unicast, aunque también puede ser una dirección

broadcast o una dirección de grupo multicast.

Identificador de la cabecera de seguridad (AH o ESP).

Según los modos de uso de las cabeceras vistas anteriormente se pueden definir dos tipos de Asociaciones de Seguridad, modo túnel y modo transporte. Una SA en modo transporte aplica los mecanismos de seguridad tanto a la carga de los datagramas de la comunicación como a la propia cabecera de este, teniendo en cuenta los valores variables, mientras que una SA en modo túnel aplica estos mecanismos al datagrama completo encapsulado. Un host debe soportar tanto modo transporte como modo túnel, mientras que un gateway seguro solo se requiere que soporte el modo túnel.

El conjunto de servicios de seguridad ofrecidos por una SA depende de la cabecera de seguridad seleccionada (AH o ESP), el modo de la comunicación (transporte o túnel), los puntos finales de la SA y la selección de servicios opcionales dentro del protocolo. Por ejemplo, AH proporciona autenticación de origen e integridad en la conexión, pero la precisión del servicio de autenticación está en función de la granularidad de la SA en la que AH es empleado, es decir, de los tipos de algoritmos seleccionados, de la longitud de la clave, las restricciones de acceso, etc.

Combinaciones de Asociaciones de Seguridad

A continuación se muestran cuatro ejemplos de las combinaciones mínimas de SAs que deben ser soportados por todo host o gateway seguro. La línea punteada indica información protegida, y un asterisco indica que el equipo conoce IPSec.

Caso 1: Proveer protección a la comunicación entre dos equipos a través de Internet. Tanto el modo transporte como el modo túnel pueden ser seleccionados por los hosts. En la ilustración 1 se muestran diferentes combinaciones de las cabeceras AH y ESP. Cuando las dos cabeceras están presentes la cabecera de autenticación siempre debe ser la primera como se verá más adelante. Para la comunicación entre dos hosts la combinación AH+ESP para el modo túnel no es requerida.

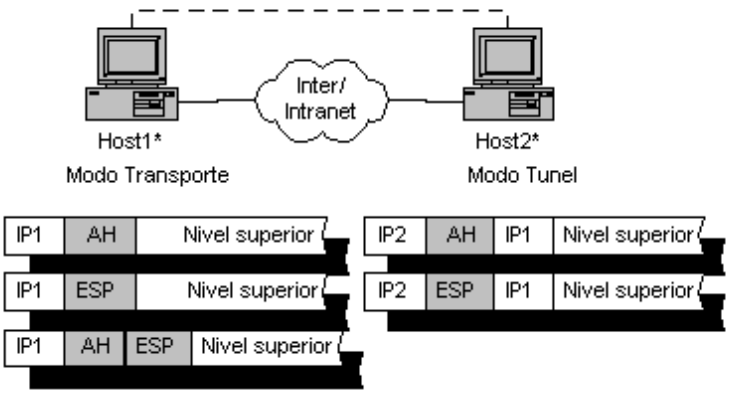


Ilustración 1. Conexión host−to−host mediante IPSec.

Caso 2: Muestra una solución simple para redes privadas virtuales, ilustración 2. En esta situación sólo se requiere el modo túnel entre los equipos que actúan de gateway seguro. En estos casos los hosts de las intranets suelen tener direcciones no enrutables y los gateways seguros actúan como firewalls y proxys estableciendo restricciones de entrada y salida a los paquetes que tienen que viajar de una red a otra. Como se puede ver la combinación AH+ESP tampoco es obligatoria en este caso.

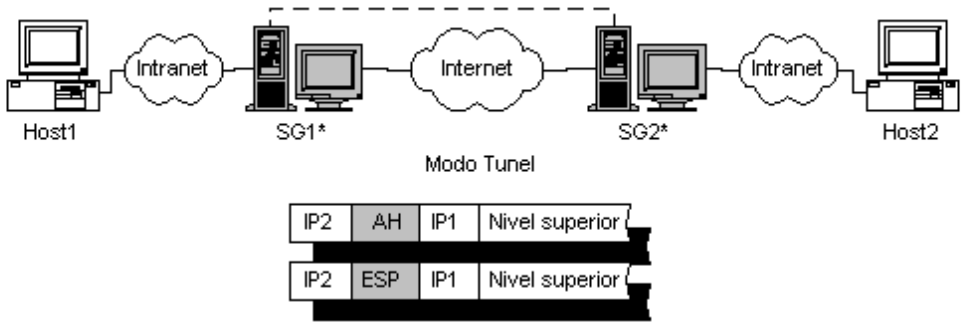


Ilustración 2. Conexión SG−SG mediante IPSec.

Caso 3: Se combinan los casos 1 y 2, ilustración 3, proporcionando seguridad extremo a extremo entre los hosts emisor y receptor. Este ejemplo proporciona mayor seguridad que el anterior, a costa de tener que instalar en todos los equipos IPSec. Solo se requiere que los hosts puedan utilizar el modo transporte, mientras que los SG's deben de permitir tanto el modo transporte como el modo túnel. Lo normal es que en los extremos se utilice la cabecera de cifrado ESP, mientras que en los SG's se autentique la información mediante AH. Las combinaciones soportadas son las vistas para los dos casos anteriores.

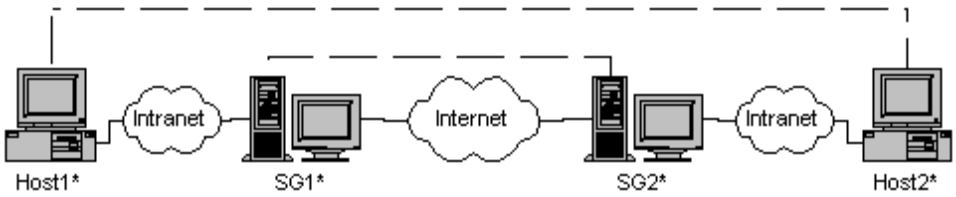


Ilustración 3. Conexión host−to−host con SGs.

Caso 4: Muestra la situación en la que un host remoto quiere establecer una comunicación con un equipo de una organización que está protegido por un SG, los tres equipos soportan IPSec. Los dos modos, transporte y túnel, que se muestran en la ilustración 4 se pueden aplicar al mismo tiempo siendo una situación similar a la del caso 3. Entre Host1 y SG solo es requerido el modo túnel.

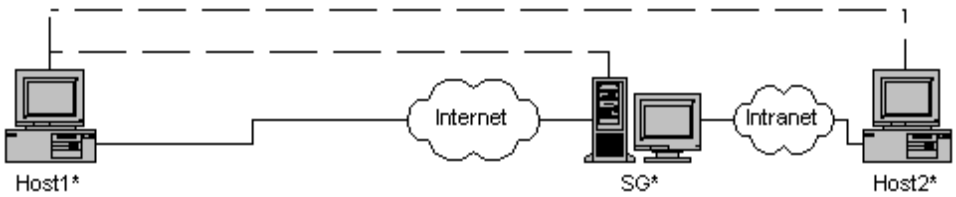


Ilustración 4. Conexión host−SG.

Técnicas criptográficas

A continuación se explicarán brevemente cuales son las principales técnicas criptográficas que son utilizadas por los mecanismos de seguridad a nivel de red. Aunque el protocolo ESP no está orientado hacia ningún tipo de algoritmo criptográfico en concreto, se están imponiendo como estándar los algoritmos en modo CBC (Cipher Block Chaining) principalmente 3DES−CBC.

DES es un algoritmo de cifrado de bloque que utiliza bloques de 64 bits y realiza permutaciones al inicio y al final, junto con intercambios, transformaciones y operaciones lógicas intermedias para obtener bloques cifrados. Actualmente DES ha sido comprometido y se utiliza una combinación de sucesivas etapas cifrado y descrifrado para formar 3DES, algoritmo que es seguro. El modo CBC requiere un vector de inicialización (IV) del mismo tamaño del bloque empleado. Dado el primer bloque del texto en claro se le hace un XOR con el IV antes de que sea cifrado. Para los sucesivos bloques del texto, el anterior bloque cifrado se usa como IV.

Algoritmo	Tamaño Clave (bits)	Tamaño popular	Por defecto
CAST−128	40−128	40, 64, 80, 128	128
RC5	40−2040	40, 128,160	128
IDEA	128	128	128
Blowfish	40−448	128	128
3DES	192	192	192

Algoritmos de cifrado soportados por IPSec.

Para realizar la autenticación AH se utilizan los algoritmos de firma digital HMAC−MD5−96 o HMAC−SHA1−96. Estos se basan en la aplicación de algoritmos de cálculo de resumen digital, como MD5 (Message Digest 5) o SHA1 (Secure Hash Algorithm 1). Un "Keyed Hash" será la aplicación de un algoritmo de resumen digital a un texto en claro junto con una clave de sesión.

Un resumen digital se define como una función hash de un solo sentido, es decir, una función *f* que cumple la condición de que para cualquier valor *y* es muy difícil encontrar el valor *x* tal que *f(x)=y*. Se dan por tanto las siguientes características: A partir de un resumen digital no se puede hallar el mensaje en claro, pues es una función de un solo sentido. El resumen es de longitud fija y mucho más corto que cualquier mensaje típico. Es casi imposible encontrar dos mensajes que produzcan el mismo resumen digital y cualquier alteración del mensaje original, por pequeña que sea, genera un resumen totalmente distinto.

Existen muchos algoritmos para calcular resúmenes digitales. Los principales son SHA, algoritmo publicado por el gobierno estadounidense que transforma un mensaje de longitud variable a un valor de 160 bits, y MD5, desarrollado por RSA Data Security, Inc. transforma un mensaje de longitud variable a un valor de 128 bits. Son ampliamente utilizados y se consideran razonablemente seguros.

Linares 28 de Mayo del 2001, proyecto realizado por los ingenieros técnicos de telecomunicación:

Fº José Manuel González Prieto Nºcolegiado 1457 Fº Susana García Carrión Nºcolegiado 1458

Fº Mª Carmen Esteban Díaz Nºcolegiado 1459 Fº Oscar Gómez Morillo Nºcolegiado 1460

3. PLANOS

Linares 19 de Mayo del 2001, proyecto realizado por los ingenieros técnicos de telecomunicación:

Fº José Manuel González Prieto Nºcolegiado 1457 Fº Susana García Carrión Nºcolegiado 1458

Fº Mª del Carmen Esteban Díaz Nºcolegiado 1459 Fº Oscar Gómez Morillo Nºcolegiado 1460

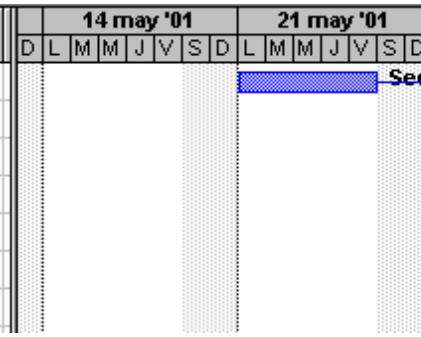
4. PLIEGO DE CONDICIONES

4.1. PLIEGO DE CONDICIONES GENERALES

Para la ejecución del proyecto se establece un máximo de catorce días hábiles, la planificación se desarrollará de la forma que a continuación se expone:

El gráfico de Gantt de la planificación inicial es el de la siguiente figura:

	Nombre de tarea	Duración	Comienzo	Fin
1	Busqueda de proveedores de materiales y de PSI	5d	lun 21/05/01	vie 25/05/01
2	Instalación HW del servidor	1d	lun 28/05/01	lun 28/05/01
3	Instalación HW de los clientes	2d	lun 28/05/01	mar 29/05/01
4	Instalación SW del servidor	1d	mar 29/05/01	mar 29/05/01
5	Instalación SW de los clientes	4d	mié 30/05/01	lun 04/06/01
6	Pruebas de funcioalidad	1d	mar 05/06/01	mar 05/06/01
7	Curso a los empleados	1d	mié 06/06/01	mié 06/06/01



El grafico de Pert de la planificación inicial es el siguiente:

Actividades:

A;B;C;D;E;F;G

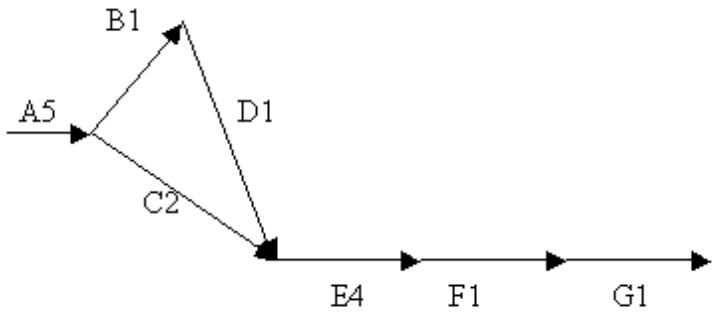
Restricciones:

A<B,C B<D C,D<E E<F F<G

Duraciones:

A=5 B=1 C=2 D=1 E=4 F=1 G=1

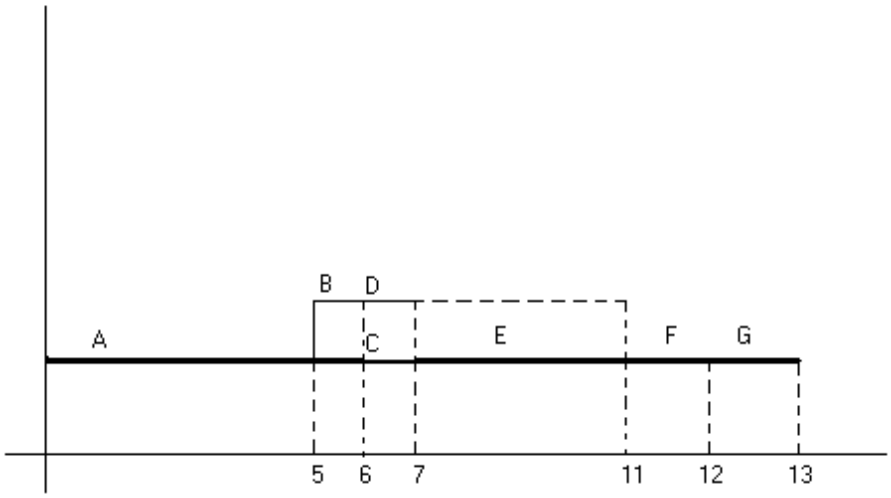
Grafo:



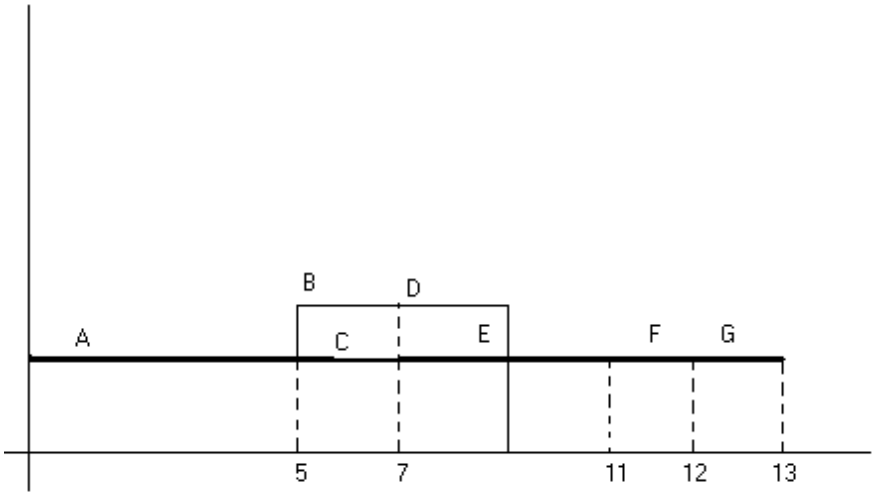
Minimización de costes:

	Tmin	Cmin	Tnor	Cnor	Tace	Cace
A	7	35.700	5	52.500	2	130.000
B	2	8.000	1	17.500	1	17.500
C	4	15.500	2	70.000	1	70.000

D	2	12.000	1	24.500	1	24.500
E	6	102.000	4	196.000	2	413.500
F	3	21.000	1	67.900	1	67.900
G	2	30.300	1	67.900	1	67.900



Alargando D y B una unidad de tiempo minimizamos los costes reduciéndolos 22.000ptas.



4.2. PLIEGO DE CONDICIONES TÉCNICAS

Los equipos necesarios para la realización del proyecto tienen que cumplir como mínimo las especificaciones y características técnicas mencionadas.

Servidor:

Tipo de procesador: Pentium III 800MHz
Número de procesadores (est./máx.): ½
Caché L2: 256 KB / 256 KB

Memoria − estándar / máxima: 512MB/4096MB
Subsistema de disco: Integrated Dual Channel Ultra2 SCSI LVD, ServeRAID−4L Ultra160 SCSI Adapter, 54,6GB instalado
Tipo de disco duro: Ultra160 SCSI
Maximum storage capacity: 218,4GB
Ranuras y bahías (totales/disponibles):PCI 5(4) x 10(5)
CD−ROM: 40X máx. − 17X mín.
Interfaz de red: Ethernet integrada

Monitor 19".

Ordenador Portátil:

Características
Tipo de procesador: PIII 750MHz
Memoria − estándar / máxima: 128 MB / 512 MB
Capacidad del disco: 10GB
Monitor 13,3" 1024x768 −− TFT − matriz activa
Soporte para PCMCIA: 2 Tipo I/II ó 1 Tipo III
CD−ROM: 24Xmax−10Xmin
Audio: Crystal Semiconductor CS4624/CS4297a
Velocidad del fax/módem: 56K V.90 Integrado con Ethernet 10/100 (Intel)
Interfaz de red: Ethernet integrada
Sistema operativo instalado:Microsoft Windows 98 Second Edition

Teléfono Móvil:

Dimensiones/mm:	98·60·28		
Dual Band:	900/1800		
Tarjeta SIM:	Plug−in	Modem:	☑
Autonomía en llamada:	4h 30m	W@P:	☑
Autonomía en stand−by:	145h	GPRS:	☑
Batería:	Li 800mAh	T9:	☑
Peso:	155g	Juegos:	☑
Recepción/Envío de SMS:	☑	Agenda electrónica:	☑
Aviso de llamada en espera:	☑	Alarma:	☑
Llamada múltiple:	☑	Grabación de voz:	☑
Identificación de llamada:	☑	GPS:	☑
	☑	Calculadora:	☑

Rechazo de identificación:			
Indicación de gasto de llamada:	☑	Datos/fax:	☑
EFR (Enhanced Full Rate):	☑	VibraCall:	☑
Voice Dial:	☑	IrDA (infrarrojos):	☑

Modem 56K Analogico Externo:

CARACTERISTICAS	
Sistema Operativo	Modem compatible con Windows NT 4.0/5.0, Windows 98, Windows 95, Windows 3.x, Windows 2000, Windows ME DOS, Macintosh, UNIX, Linux, y otros sistemas que soporten un puerto serie RS−232 y comandos AT.
Factor de forma	Externo con interfaz serie RS−232.
Estándares y Protocolos Soportados	Hasta 56 Kbps con ITU v.90 ITU V.34 a 33.6 Kbps o 28.8 Kbps V.32 terbo a 19.2 Kbps ITU V.32 bis a 14.4 Kbps HST a 16.8 Kbps Compatible con la mayoría ITU y Bell estándares hasta los 300 bps EIA/TIA Clase 1 y 2.0, Group III
Control de Errores	ITU−T V.42 MNP 2−4
Compresión de Datos	ITU−T V.42 bis MNP 5
Paquete de Accesorios	Cable de teléfono RJ−11C, adaptador universal a toma de tensión, cable serie RS−232, Paquete de Documentación.
Compatibilidad de Fax	ITU−T V.17 a 14.4 Kbps ITU−T V.29 a 9600 bps ITU−T V.27 ter a7200 bps

Accesorios telf. Movil:

Cable de extensión de datos para la conexión entre el ordenador portátil y el teléfono o un PDA.

Tarjetas PCMCIA.

Software:

Windows 2000 Server.

Windows 2000.

Software para el cable de extensión de datos.

Nota: El software a utilizar será original, nunca copia ilegal, siendo por lo tanto obligatoria la adquisición de las licencias pertinentes.

4.3. PLIEGO DE CONDICIONES FACULTATIVAS

La empresa SkyTEL S.A. se responsabiliza y compromete en el plazo especificado a llevar a cabo el proyecto encargado por Sr. Sánchez Navarro, este plazo acordado por las dos partes comprende un periodo de catorce días, con una demora máxima para la ejecución de dicho proyecto de una semana. La parte contratista entrega al contratante todos los manuales y certificados de garantía del material, así como todos los certificados, para que surtan efecto ante el servicio técnico oficial pertinente.

En caso de incumplimiento de contrato por parte del contratista deberá devolver por duplicado de acuerdo a ley la cantidad apercibida por el contratante, quedando el contratante eximido de ninguna obligación de mantener dicho contrato y condiciones con el contratista quedando libre para la contratación con cualquier otra empresa.

4.4. PLIEGO DE CONDICIONES ECONÓMICAS

Las dos partes reunidas el día 21 de Mayo del 2001 en las oficinas de la empresa SkyTEL S.A. firman el contrato que especifica y determina todos los aspectos y condiciones del proyecto a llevar a cabo por la parte contratante.

El cliente se hará cargo de los gasto suplidos que especifica a continuación:

−Derechos de visado.

−Seguro de responsabilidad civil.

−Gastos de administración.

En caso de incumplimiento de contrato por parte del contratante, éste no tendrá derecho a reclamación alguna de tipo monetario, perdiendo en su totalidad las cantidades entregadas por anticipado a modo de señal y a cuenta.

Del pago anticipado que efectúa Sr. Sánchez Navarro por valor del 40% del valor total de la obra, dicho anticipo a modo de señal y pago a cuenta se realiza en las oficinas de SkyTEL S.A. el día de la entrega del proyecto, mediante un talón nominativo con fecha efectiva al día posterior a la reunión. Y el resto será entregado el día después de finalización de la obra, que será ingresado en la cuenta de SkyTEL S.A. Nº1236.14.2589.000 de CajaMar Crt. Cabo de Gata Nº125. Linares (Jaén).

Linares 28 de Mayo del 2001, proyecto realizado por los ingenieros técnicos de telecomunicación:

Fº José Manuel González Prieto Nºcolegiado 1457 Fº Susana García Carrión Nºcolegiado 1458

Fº Mª Del Carmen Esteban Díaz Nºcolegiado 1459 Fº Oscar Gómez Morillo Nºcolegiado 1460

5. PRESUPUESTO

Total de material o ejecución

Concepto	cantidad	precio unitario(Ptas)	total	
			Ptas	Euros
Servidor	1	1.383.000	1.383.000	8.312,00
Monitor	1	87.100	87.100	523,48
Ordenador Portátil	25	425.000	10.625.000	63.857,5
Teléfono Móvil	25	75.000	1.875.000	11.295,18
Accesorios telf. Móvil	25	10.000	250.000	1.506,02
MODEM 56K	1	45.000	45.000	270,4
Tarjeta PCMIA	25	15.000	375.000	2250.09
Precio (paquete de SOFTWARE completo)	1		250.000	1.506,02

Honorarios

	empleados	Pta/H	Euros/H	pta/70 H	euros/70 H	c(0.9)
Empresa (Ing.Tec.Telemática)	4	9.700	58,43	2.176.000	163641,44	1.958.4000

Gastos generales

	empleados	Pta/H	Euros/H	Total pta	Total euros/ H
Secretario/a	1	1.500	9,03	52.500	315,12
Instalador técnico	2	2.500	15,06	105.000	630,25
Programador	2	3.500	21,08	245.000	1.470,58
I.T. Telemática	1	9.700	58.43	135.800	581,12

	DIAS	PTA/DIAS	EUROS/DIAS	PTA/10DIAS	EUROS/10DIAS
Costes indirectos fijos	10	20.000	120,48	200.000	1204,81

Total de ejecución material.

Concepto	**Subtotal**	
	Ptas	**Euros**
Total de material o ejecución	14.890.100	89.344,174

Honorarios	1.958.400	14.727,73
Gastos generales	674.300	4.047,41

El total asciende a 15.504.400 ptas sin IVA .

El total con el 16% de IVA será 18.054.704 ptas

Con los Gastos suplidos(otros gastos) más honorarios.

El presupuesto asciende a 20.107.982 ptas.

El total de ejecución del material asciende a la cantidad de veinte millones ciento siete mil, novecientas ochenta y dos pesetas, que son ciento veinte mil seiscientas noventa y seis euros y diecisiete céntimos de euros .

5.1. OTROS GASTOS

Costes de explotación:

Producto / Servicio	**Precio unidad pts**	***Cantidad***	**Total pts**
Cuota mensual tarifa plana RTB	10.000	***1***	10.000
Registro de un nuevo dominio	20.000	***1***	20.000
Mantenimiento anual del Dominio,ftp, e−mail,WEB	10.500	***1***	10.500
Cuota anual por dirección IP fija asignada a una conexión	25.000	***1***	25.000

Gastos Suplidos.

Derecho de visado.

Se obtiene de la formula D.V=(0.007P)Coef.

D.V=(0.007*18.054.704) 0.7=88.468,05 ptas

Seguro de responsabilidad civil.

SRC=5000ptas.

Gastos de administración.

Tramitación Normal =1.410 ptas

Linares 28 de Mayo del 2001, proyecto realizado por los ingenieros técnicos de telecomunicación:

Fº José Manuel González Prieto Nºcolegiado 1457

Fº Susana García Carrión Nºcolegiado 1458

Fº Mª Del Carmen Esteban Díaz Nºcolegiado 1459

Fº Oscar Gómez Morillo Nºcolegiado 1460

47

Plano general de la Oficina Central de la empresa

Escala 1:170