LINEAMIENTOS PARA LA CREACIÓN DE UNA VPN (VIRTUAL PRIVATE NETWORK) RED PRIVADA VIRTUAL

ENEVIS RAFAEL REYES MORENO

Monografía para optar el título de Especialista en Telemática

UNIVERSIDAD DE ANTIOQUIA

FACULTAD DE INGENIERÌA

Departamento de Electrónica

MEDELLÍN 2005

Tabla de contenidos

GLOSARIO

ADSL: línea de abonado digital asimétrica, la cual soporta diferentes tasas de datos para los datos de ida y de vuelta.

AH: autentication Header (Encabezado de Autenticación).

ATM: asynchronous Transfer Mode (Modo de transferencia asíncrono), es una tecnología de red basada en la transferencia de celdas o paquetes de datos de un tamaño fijo.

CRT: comisión de regulación de telecomunicaciones.

CHECKSUM: control de adición.

CHAP: callenge Handsake Authentication Protocol Protocolo de autenticación

DES: data Encryption Standard, norma de cifrado de datos.

ESP: encapsulating Security Payload, La Carga útil de Seguridad encapsulando

ENCRIPTACIÓN: conjunto de técnicas que intentan hacer inaccesible la

información a personas no autorizadas. Por lo general, la encriptación se basa

en una clave, sin la cual la información no puede ser descifrada.

GRE: modo transporte Cubre el encabezado TCP y algunos campos IP.

HASHING: picado

IMAP: internet Message Access Protocol, Protocolo de Acceso de Mensaje en Internet

IPSEC: modo túnel del L2TP

ISP: proveedor de servicios de Internet

LDAP: lightweight Directory Access Protocol, El Protocolo de Acceso de Directorio ligero

LAYER 2: fowarding Protocol L2FP

LLC: tareas de interacción entre la tarjeta de red y el procesador

NAP: punto de acceso a Red

NAT: network Ardes Translation (traducción de direcciones de red) , es un estandar de internet que activa una red de area local LAN para usar un conjunto de direcciones IP para el trafico interno y un conjunto de direcciones para el trafico externo.

NIC: network Interface Card (tarjeta de interfaz de red)

OVERFLOW: buffer Overflow protection, Desbordamiento.

OSI: estructura lógica de siete niveles para facilitar la comunicación entre diversos sistemas de computación.

PAP: password Autenthication protocol, protocolo de autenticacion de contraseña.

POP3 : post Office Protocol 3

PPTP: point to point protocol tunnelling, protocolo de tunnel punto a punto

PGP: pretty Good Privacy utiliza RSA e IDEA

PPP: protocolo punto a punto, un método para conectar un ordenador a internet, el PPP es

estable y proporciona funciones de verificación de errores.

PROTOCOLO: es un formato convenido para transmitir datos entre dos

dispositivos. Y se pueden implementar en software o hardware

RAS: remote Access service. Servicio de acceso remoto a la red

RDSI: red digital de servicios integrados, es un estandar internacional de comunicaciones para transmitir voz videos y datos por línea telefónica digitales o alambres de teléfono normal.

RSA: algoritmo de clave publica iniciales de los nombres de sus inventores, Rivest, Shamir, Adleman

SA: asociación de Seguridad

SSL: secure Sockets Layer (capa de socalos de seguridad

Capa de Socket Segura. Protocolo que ofrece funciones de seguridad a nivel de la capa de transporte para TCP.

SOAP: interoperabilidad

SMTP: simple Mail Transfer Protocol, protocolo de transferencia de correo simple

SNMP: simple Network mangement Protocol, protocolo de administration de red simple

T1: línea de transmisión implementada por AT & T con velocidad de 1.544

Mbps.

VPN: virtual private network

UDP: protocolo de datagrama de usuario

X25: protocolo para red de paquetes conmutados. Generalmente se incluyen los protocolos X.3 y X.28 en estas redes.

Palabras claves.

Red privada virtual, servicio de acceso remoto, Protocolo de internet seguro, protocolo de internet, concentradores, criptografía, encriptación.

INTRODUCCION

Antecedentes

Los estudios de prospectivas en comunicaciones señalan que muchas empresas cuentan con oficinas y sucursales distribuidas en diferentes ubicaciones geográficas; las cuales requieren por lo general poder compartir y acceder libremente a información entre ellas. Por esta razón las VPN jugarán un papel importante en las comunicaciones con accesos a datos y manejo de usuarios remotos que puedan estar en constante movimiento.

La importancia actual del estudio de las VPN no sólo se sustenta desde el punto de vista prospectivo, actualmente se observan aplicaciones y soluciones especiales de las VPN.

Además de la comunicación entre diferentes sucursales, surgió la necesidad de proveer acceso a los usuarios móviles de la empresa. Mediante Remote Access Services(RAS), este tipo de usuario puede conectarse a la red de la empresa y usar los recursos disponibles dentro de la misma.

El gran inconveniente del uso de las líneas telefónicas es su alto costo, ya que se suele cobrar un abono mensual más una tarifa por el uso, en el que se tienen en cuenta la duración de las llamadas y la distancia hacia donde se las hace. Si la empresa tiene sucursales dentro del mismo país pero en distintas áreas telefónicas, y, además, tiene sucursales en otros países, los costos telefónicos pueden llegar a ser prohibitivos. Adicionalmente, si los usuarios móviles deben conectarse a la red corporativa y no se

encuentran dentro del área de la empresa, deben realizar llamadas de larga distancia, con lo que los costos se incrementan.

Las Virtual Private Networks (VPN) son una alternativa a la conexión WAN mediante líneas telefónicas y al servicio RAS, bajando los costos de éstos y brindando los mismos servicios, mediante el uso de la autenticación, encriptación y el uso de túneles para las conexiones.

Cuando se desea enlazar las oficinas centrales con alguna sucursal u oficina remota se tienen cuatro opciones:

Modem: Las desventajas es el costo de la llamada, ya que el costo de esta llamada sería por minuto conectado, además sería una llamada de larga distancia, a parte no contaría con la calidad y velocidad adecuadas.

Línea Privada: Se tendría que conectar un cable ya sea de cobre o fibra óptica de un punto a otro, en esta opción el costo es muy elevado porque si por ejemplo se necesita enlazar una oficina central con una sucursal que se encuentra a 200 Kilómetros de distancia el costo sería por la renta mensual por Kilómetro. Sin importar el uso.

VPN: Los costos son bajos porque solo se realizan llamadas locales, además de tener la posibilidad que los datos viajen encriptados y seguros, con una buena calidad y velocidad.

Frame Relay o ATM

Es una de las mas utilizada y presenta gran desempeño y seguridad, pero su costo de mantenimiento y de servicio es relativamente alto.

En resumen, las VPN tienen un futuro promisorio como solución de comunicación y seguridad de conexiones remotas para las empresas. Dada la creciente importancia de la seguridad en las redes de comunicación y de conexiones más económicas que necesitan las empresas, se pueden mejorar y cubrir con las ventajas y soluciones ofrecidas por las VPN.

En este contexto se escribe la formulación del proyecto “Lineamientos para la creación de VPN ”

Tema

Actualmente las soluciones de comunicaciones a nivel de seguridad no son totalmente rigurosas tanto a nivel de LAN como de WAN, ya que en la LAN se tiene la confianza del personal interno y en la WAN se tiene la confianza al proveedor; la gran mayoría de empresas contratan la transmisión de sus datos con empresas especializadas en ello y por lo general establecen conexiones tipo ATM o Frame Relay que tienen un alto costo y los datos van de manera transparente sin ningún tipo de encriptación. Las empresas se confían porque son líneas privadas, pero un intruso en medio podría determinar la información transmitida y delinquir sobre ella.

Una forma de reducir costos a esta situación es realizar las conexiones remotas a través de internet, ya que estas son supremamente baratas, fáciles de conseguir y funcionan sobre medios básicos como líneas telefónicas, RDSI, ADSL entre otras, pero entra a jugar el factor “seguridad”, ya que la información viaja sin ningún tipo de

encriptación. Aquí es donde se debe pensar en una solución como las VPN.

Debido a la situación económica, la presión en la disminución de costos operativos para incrementar las ganancias, tener comunicaciones eficientes entre las diferentes sucursales, poder contar con fuerza de venta que trabaje remotamente o incluso empleados que operen en modo de tele-trabajo, se hace necesario la implementación de VPN. Pero al momento de su diseño y montaje llegan los siguientes cuestionamientos:

Cual es la mejor tecnología de conexión de acuerdo al abanico de posibilidades que ofrecen los ISP?

Que protocolos se deben utilizar para realizar los túneles?

Que tipo de encriptación se necesita?

Que sistema operativo se necesita para las conexiones?

De acuerdo con la infraestructura perimetral cómo se configura la seguridad para permitir la conexión VPN?

Objetivos

Estudiar la configuración básica de las VPN para plataformas tecnológicas como Windows y Linux.

Analizar los tipos de configuraciones de acuerdo a los diferentes proveedores de telecomunicaciones colombianas para optimizar las conexiones de VPN.

Realizar estudios de los tipos de encripción (Cifrado de información) y niveles de seguridad disponibles para VPN.

Estudiar el manejo de seguridad mediante protocolos como IPSEC utilizando AH (encabezado de autenticación) y ESP como cifrado de datos.

Conocer los diferentes protocolos y su funcionamiento tanto de establecimiento de túneles como de reenvío.

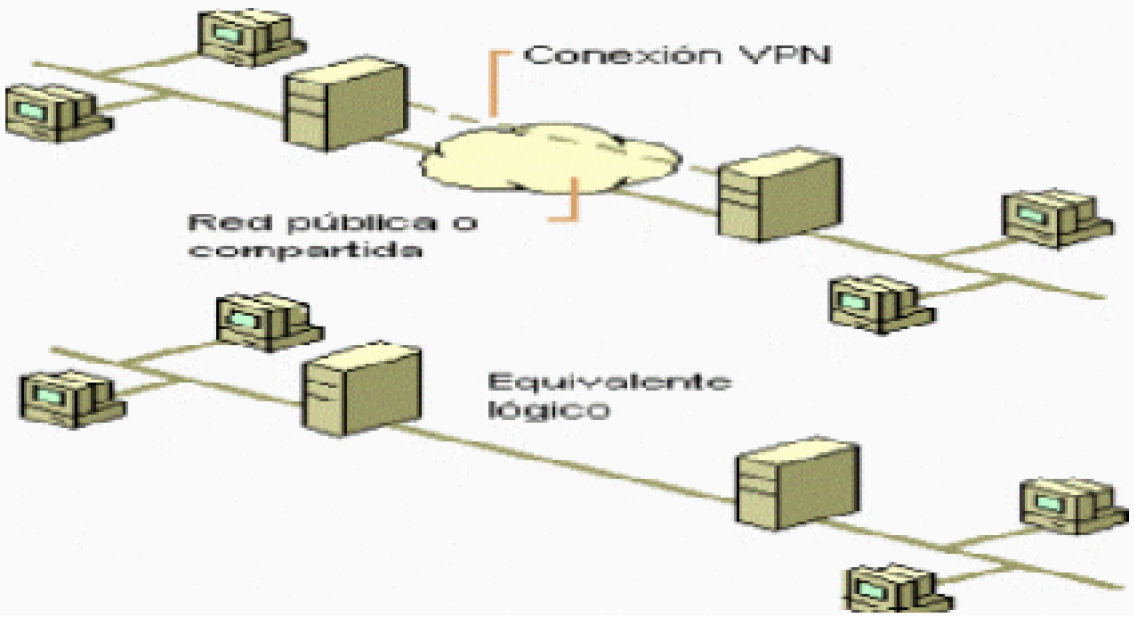
Analizar las diferentes topologías de trabajo sobre VPNs.

Analizar las diferentes formas de realizar el montaje de una VPN como. Basadas en cortafuegos, en caja negra, en enrutador, acceso remoto y basadas en software.

1. FUNDAMENTOS DE VPN

1.1 COMPONENTES Y FUNCIONAMIENTO DE UNA VPN

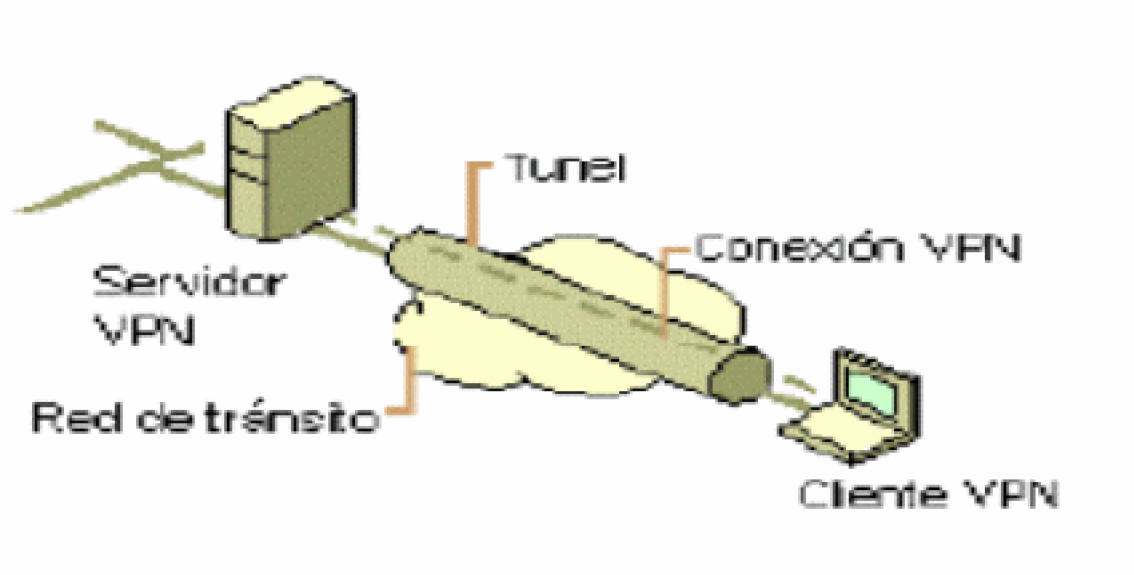
Una Virtual Private Network (VPN) es un sistema para simular una red privada sobre una red pública, por ejemplo Internet. la idea es que la red pública sea "vista" desde dentro de la red privada como un cable lógico que une las dos o más redes que pertenecen a la red privada.



Gráfica 1. Esquema de una VPN.

Las VPNs también permiten la conexión de usuarios móviles a la red privada, tal como si estuvieran en una LAN dentro de una oficina de la empresa donde se implementa la VPN. Esto resulta muy conveniente para personal que no tiene lugar fijo de trabajo dentro de la empresa, como podrían ser vendedores, ejecutivos que viajan, personal que realiza trabajo desde el hogar, etc.

La forma de comunicación entre las partes de la red privada a través de la red pública se hace estableciendo túneles virtuales entre dos puntos para los cuales se negocian esquemas de encriptación y autenticación que aseguran la confidencialidad e integridad de los datos transmitidos utilizando la red pública. Como se usan redes públicas, en general Internet, es necesario prestar debida atención a las cuestiones de seguridad, que se aborda a través de estos esquemas de encriptación y autentificación y que se describirán luego.



Gráfica 2. Componentes de un túnel.

La tecnología de túneles ("Tunneling") es un modo de transferir datos en la que se encapsula un tipo de paquetes de datos dentro del paquete de datos de algún protocolo, no necesariamente diferente al del paquete original. Al llegar al destino, el paquete original es desempaquetado volviendo así a su estado original. En el traslado a través de Internet, los paquetes viajan encriptados.

Las técnicas de autenticación son esenciales en las VPNs, ya que aseguran a los participantes de la misma que están intercambiando información con el usuario o dispositivo correcto. La autenticación en VPNs es conceptualmente parecido al logeo en un sistema como nombre de usuario y contraseña, pero con necesidades mayores de aseguramiento de validación de identidades. La mayoría de los sistemas de autenticación usados en VPN están basados en un sistema de claves compartidas.

La autenticación es llevada a cabo generalmente al inicio de una sesión, y luego aleatoriamente durante el curso de la misma, para asegurar que no haya algún tercer participante que se haya intrometido en la conversación. La autenticación también puede ser usada para asegurar la integridad de los datos. Los datos son procesados con un algoritmo de hashing para derivar un valor incluido en el mensaje como checksum. Cualquier desviación en el checksum indica que los datos fueron corruptos en la transmisión o interceptados y modificados en el camino.

Ejemplos de sistemas de autenticación son Challenge Handshake Authentication Protocol (CHAP) y RSA.

Todas las VPNs tienen algún tipo de tecnología de encriptación, que esencialmente empaqueta los datos en un paquete seguro. La encriptación es considerada tan esencial como la autenticación, ya que protege los datos transportados para no poder ser interpretados durante el viaje de un extremo a otro de la conexión. Existen dos tipos de técnicas de encriptación que se usan en las VPN: encriptación de clave secreta, o privada, y encriptación de clave pública.

En la encriptación de clave secreta, se utiliza una contraseña secreta conocida por todos los participantes que necesitan acceso a la información encriptada. Dicha contraseña se utiliza tanto para encriptar como para desencriptar la información. Este tipo de encriptación posee el problema que, como la contraseña es compartida por todos los participantes y debe mantenerse secreta, al ser revelada, debe ser cambiada y distribuida a los participantes, con lo cual se puede crear de esta manera algún problema de seguridad.

La encriptación de clave pública implica la utilización de dos claves, una pública y una secreta. La primera es enviada a los demás participantes. Al encriptar, se usa la clave privada propia y la clave pública del otro participante de la conversación. Al recibir la información, ésta es desencriptada usando su propia clave privada y la pública del generador de la información. La gran desventaja de este tipo de encriptación es que resulta ser más lenta que la de clave secreta.

En las VPNs, la encriptación debe ser realizada en tiempo real. Por eso, los flujos encriptados a través de una red son encriptados utilizando encriptación de clave secreta

con claves que son solamente buenas para sesiones de flujo.

El protocolo más usado para la encriptación dentro de las VPNs es IPSec, que consiste en un conjunto de propuestas del IETF que delinean un protocolo IP seguro para IPv4 y IPv6. IPSec provee encriptación a nivel de IP.

El método de túneles, como fue descrito anteriormente, es una forma de crear una red privada. Permite encapsular paquetes dentro de paquetes para acomodar protocolos incompatibles. Dentro de los protocolos que se usan para la metodología de túneles se encuentran Point-to-Point Tunneling Protocol (PPTP), Layer-2 Fowarding Protocol (L2FP) y el modo túnel de IPSec.

2. CONFIGURACIÓN BÁSICA DE LAS VPN PARA PLATAFORMAS TECNOLÓGICAS COMO WINDOWS Y LINUX

2.1 PLATAFORMA WINDOWS

Para configurar una VPN bajo Windows se necesita lo siguiente:

Conexión a Internet tanto para el servidor local de NT como para las máquinas remotas.

Una dirección IP estática para el servidor NT.

Proxy que se ejecute en el servidor NT, para evitar el acceso desautorizado al sistema.

Direcciones IP para los recursos a compartir.

Adaptador virtual de la red instalado en la máquina remota o cliente.

La secuencia de pasos es:

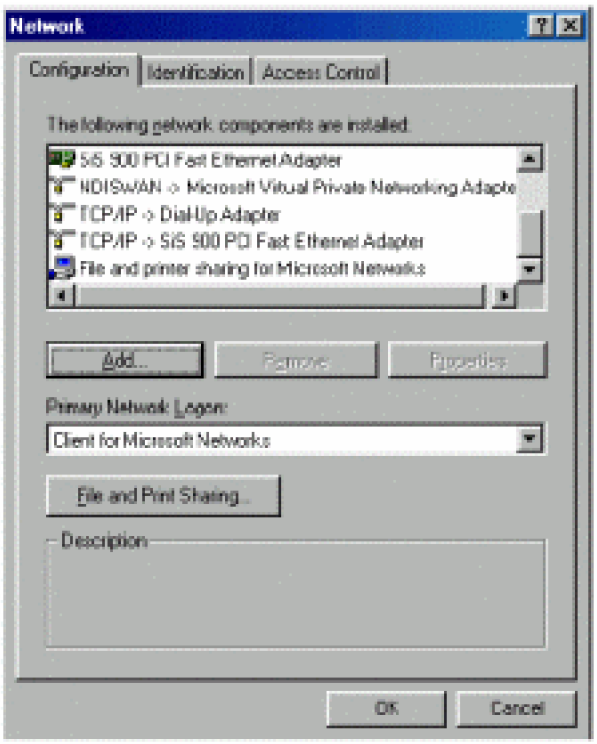
Hacer una lista de las direcciones IP de los recursos que serán compartidos a través de Internet.

Instalación y ejecución del proxy.

En el servidor NT, se deben configurar los archivos del usuario NT para que pueda llamar y conectarse al servidor, garantizando su acceso al sistema con los permisos de la VPN.

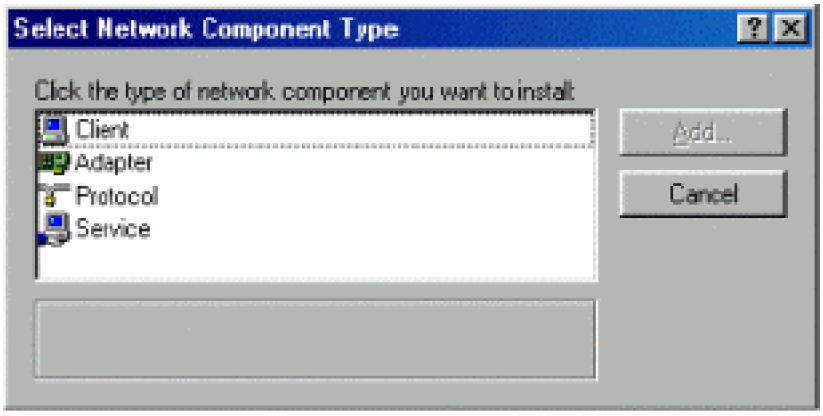
Luego de estos pasos, se deberá instalar el adaptador privado de la red en la máquina cliente, como se indica:

Dentro del Diálogo de Red, que se muestra debajo, y al cual se accede a través de la opción Propiedades del icono Entorno de Red, se presiona el botón Add.



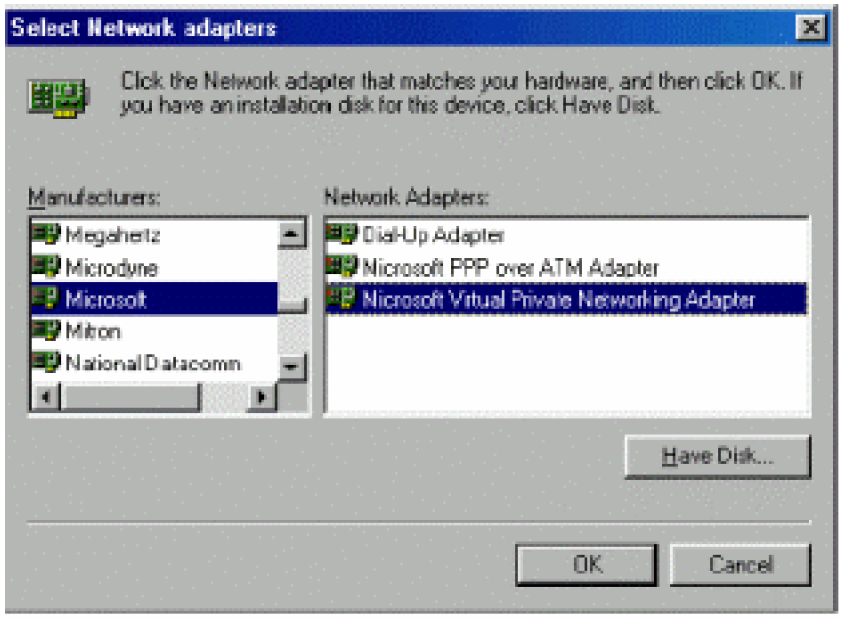
Gráfica 3. Diálogo de Red.

Aparecerá la siguiente pantalla, se deberá seleccionar Adapter y luego presionar el botón Add.



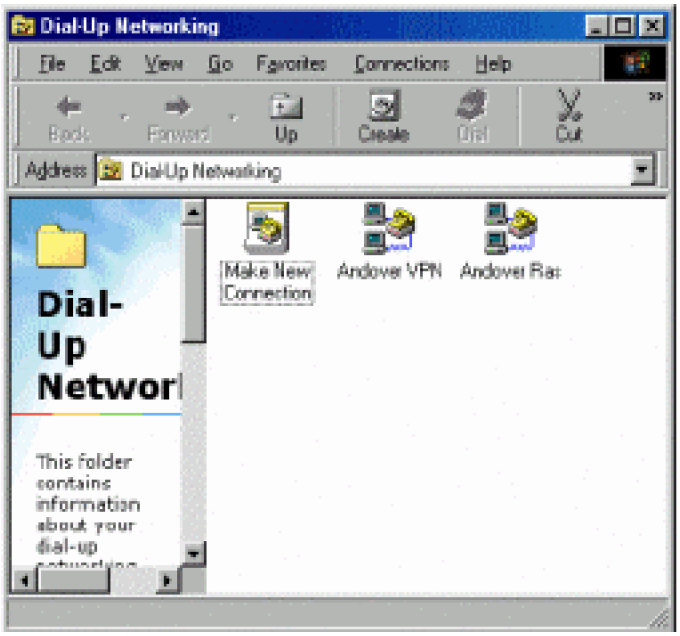
Gráfica 4. Pantalla de selección de componente.

Aparece el cuadro Select Network adapters, donde se deberá elegir el fabricante y el adaptador como se muestra en la siguiente figura:



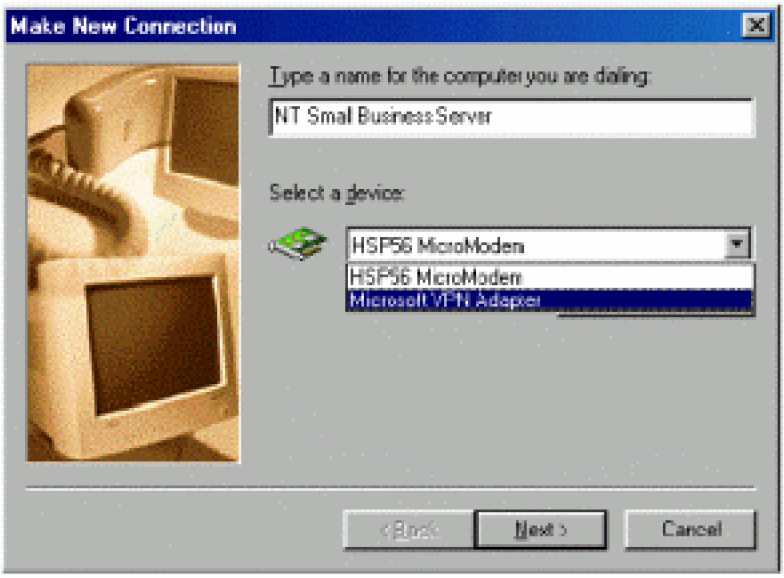
Gráfica 5. Pantalla de selección de fabricante y el adaptador.

Posteriormente, para instalar la conexión a la LAN, se deberá acceder al Acceso Remoto a Redes



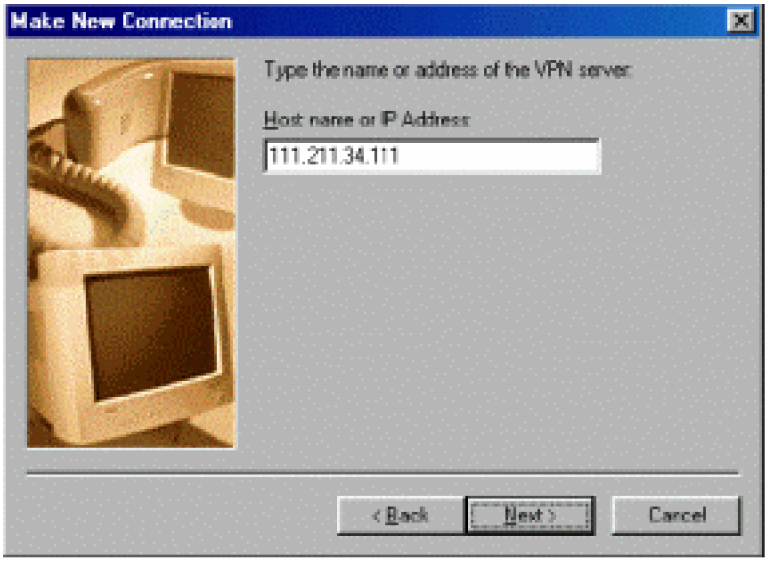
Gráfica 6. Pantalla de Acceso Remoto a Redes.

Se selecciona Make a New Connection, apareciendo la siguiente pantalla, donde se podrá elegir el adaptador de VPN:



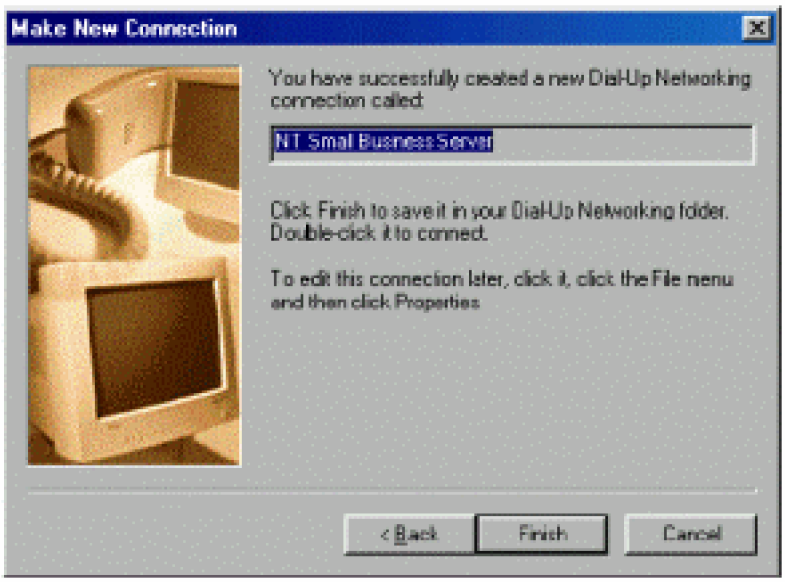
Gráfica 7.Pantalla de adaptadores.

Luego de presionar el botón Next, se deberá introducir la dirección IP del servidor VPN en la siguiente pantalla:



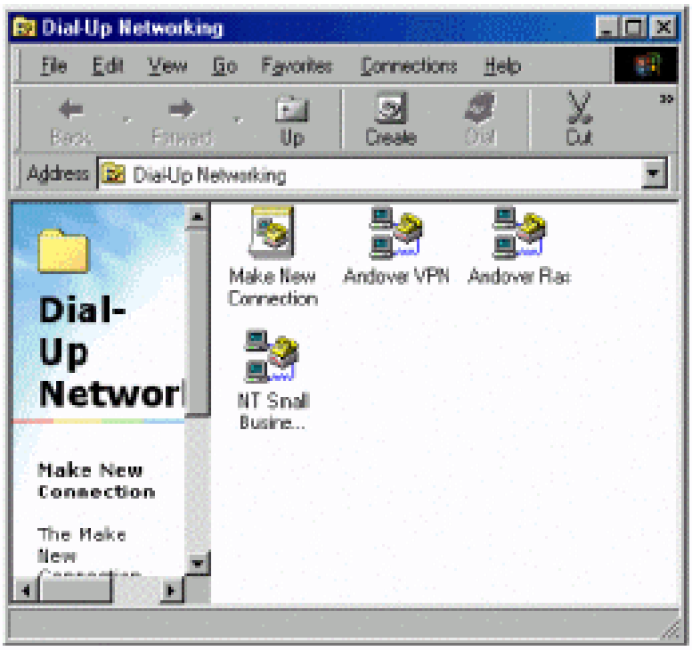
Gráfica 8. Pantalla de captura de IP.

Así se finaliza la creación de la nueva conexión:



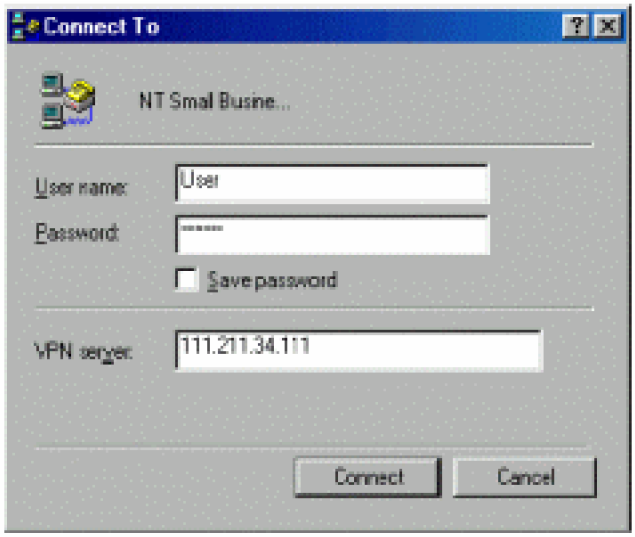
Gráfica 9. Pantalla de finalización de conexión.

Para acceder al servidor NT, se abre el Acceso Remoto a Redes:



Gráfica. 10. Pantalla de acceso remoto a redes

Al hacer doble-click en el icono de la conexión VPN, aparecerá la siguiente pantalla, donde se debe introducir el nombre de usuario, la contraseña y la dirección IP del servidor NT:

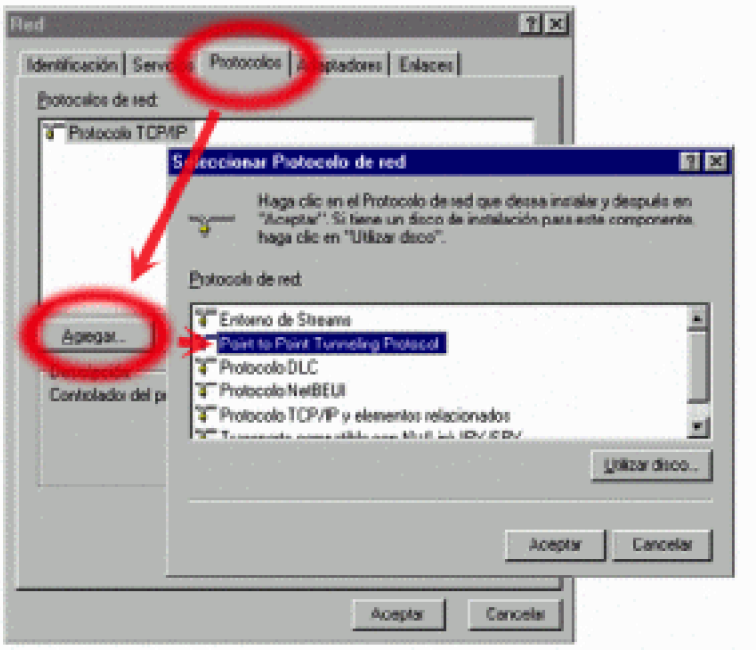


Gráfica 11. Pantalla para realizar conexión

Para configurar el servidor VPN, se deberá configurar PPTP, activar el filtro PPTP y activar el soporte PPTP en los clientes.

Para configurar PPTP en el servidor RAS y en los clientes que vayan a utilizarlo, se deberán realizar los siguientes pasos:

Dentro de Red en el Panel de Control, seleccionando Protocolos, se deberá presionar el botón Agregar:

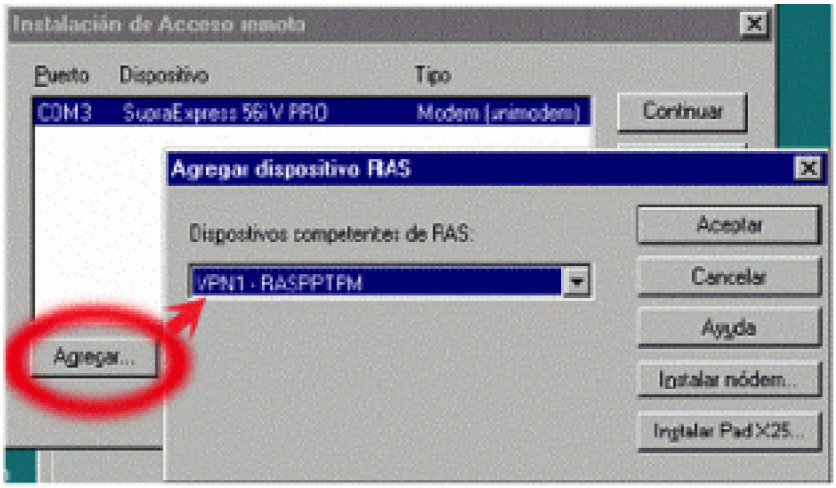


Gráfica 12. Pantalla de selección de Protocolos.

Se selecciona Point to Point Tunneling Protocol, y, luego de copiados los archivos, aparecerá el cuadro de diálogo Configuración de PPTP. El campo Número de redes privadas virtuales indica el número de conexiones PPTP admitidas. En el ejemplo, se establecen 2 VPN:

Gráfica 13. Pantalla de conexiones PPTP admitidas.

Luego, se inicia la herramienta de configuración RAS, donde se deben añadir los puertos virtuales que darán servicio a las redes privadas virtuales que se deseen establecer. Al presionar el botón Agregar, se accede al dialogo Agregar dispositivo RAS:



Gráfica 14. Pantalla de herramienta de configuración RAS.

Después de ingresadas las entradas, se presiona Aceptar. Luego se podrá seleccionar cada entrada del diálogo Instalación de Acceso Remoto, para configurar el uso del puerto. Las opciones son: Sólo recibir llamadas o Hacer y recibir llamadas.

Después de añadir todos los dispositivos virtuales, se podrá cerrar este diálogo para volver a la ficha Protocolos. Al reiniciar la computadora, ya estará configurado el server.

Para la activación del filtro PPTP, se debe seleccionar la solapa Protocolos de Panel de Configuración / Red. Dentro de esta pantalla, se elige Protocolo TCP/IP, luego Propiedades. En la solapa Dirección IP, se selecciona el adaptador de red sobre el que se aplicará el filtro. Luego de presionar el botón Avanzadas, se marca la casilla Activar filtro PPTP y, por último, se reinicia la máquina para activar la configuración.

Cuando un cliente se conecta a Internet, el procedimiento para establecer un túnel VPN consta de dos pasos:

Establecimiento por parte del cliente mediante una conexión de acceso telefónico a través de un ISP.

Establecimiento de una conexión PPTP con el servidor RAS.

Cuando un cliente se conecta directamente a Internet, no es necesario establecer una conexión de acceso telefónico. Sin embargo, el procedimiento para iniciar la conexión PPTP con el servidor RAS es idéntico. Para establecer una conexión PPTP es necesario crear una entrada especial en la guía telefónica. Esta entrada se distingue por dos características:

El campo Marcar utilizado tiene uno de los dispositivos virtuales VPN añadidos a la configuración RAS al instalar PPTP. Esta lista sólo muestra los VPN configurados para hacer llamadas.

El campo Presentación preliminar de número telefónico contiene el nombre DNS o la dirección IP del servidor PPTP.

La creación de una conexión PPTP implica también dos pasos:

Se abre la aplicación Acceso telefónico a redes, utilizando la guía telefónica que permite acceder al ISP a través de un número de teléfono y un modem.

Establecida la conexión, se debe abrir la entrada de la guía telefónica que se conecta al túnel PPTP mediante un nombre DNS o una dirección IP.

Si el cliente está conectado directamente a Internet, sólo es necesario el segundo paso.

2.2 PLATAFORMA LINUX

2.2.1. Configuración de una VPN bajo LINUX.

En este apartado se explica la configuración del demonio de VPN (VPND) sobre Debian, pero no deberá traer ningún problema al configurarlo en otra distribución de Linux.

Linux trabaja bajo un esquema multitarea y multiusuario, cuenta con herramientas de desarrollo y por su estructura permite a los desarrolladores tener acceso al hardware y a las redes que a este se conectan. La siguiente tabla ilustra cual es la presencia de Linux en el mundo de las telecomunicaciones y la informática

VPND permite crear enlaces seguros sobre TCP/IP con claves de hasta 512 bits y algoritmo de encriptación BLOWFISH, montando una interfaz virtual serie que proporciona la posibilidad de enrutamiento de IP entre redes. Los pasos a seguir son:

Dar soporte SLIP en el kernel LINUX, recompilándolo y probando que funcione.

Instalación del paquete vnpd, que, en Debian, se puede hacer con ‘apt-get install vpnd’.

Creación de una clave de sesión, utilizando ‘vpnd –m /etc/vnpd/vpnd.key’, que debe ser pasada al otro extremo de la VPN mediante un medio seguro, ya que es la clave que ambos extremos de la VPN comparten.

Configuración de los extremos de la VPN, siguiendo la estructura Cliente/Servidor. A continuación, se muestran el contenido de los archivos vpnd.conf de configuración para el servidor y el cliente.

Archivo /etc/vpn/vpnd.conf para el servidor:

mode server

Direccion IP y puerto del servidor

server a.b.c.d 2001

Direccion IP y puerto del cliente

client w.x.y.z 2001

Direccion IP privada del servidor

local a.b.c.d

Direccion IP privada del cliente

remote w.x.y.z

Opciones generales

autoroute

Keepalive 10

noanswer 3

keyfile /etc/vnpd/vnpd.key

pidfile /var/run/vpnd.pid

keyttl 120

ramdomdev /dev/urandom

mtu 1600

Archivo /etc/vpn/vpnd.conf para el cliente:

mode client

Direccion IP y puerto del servidor

client w.x.y.z 2001

Direccion IP y puerto del cliente

server a.b.c.d 2001

Direccion IP privada del servidor

local w.x.y.z

Direccion IP privada del cliente

remote a.b.c.d

Opciones generales

autoroute

Keepalive 10

noanswer 3

keyfile /etc/vnpd/vnpd.key

pidfile /var/run/vpnd.pid

keyttl 120

ramdomdev /dev/urandom

mtu 1600

Una vez creados estos archivos, se podrá levantar la VPN, iniciando los demonios con '/etc/init.d/vpnd start'. Para comprobar el correcto funcionamiento, se puede hacer pings a las direcciones privada y del otro extremo y verificar con 'ifconfig –a' que exista una nueva interfaz como la siguiente:

sl0 Link encap: VJ Serial Line IP

Inet addr: 10.0.0.1 P-t-P: 10.0.0.2 Mask : 255.255.255

UP POINTOPOINT RUNNING NOARP MULTICAST MTU: 1600 Metric: 1

Rx packets:0 errors: 0 dropped:0 overruns: 0 frame: 0

Compressed: 0

Tx packets:0 errors: 0 dropped:0 overruns: 0 carrier: 0

Collisions: 0 compressed: 0 txqueuelen: 10

RX bytes: 0 (0.0 b) TX bytes; 0 (0.0 b)

3. TIPOS DE ENCRIPCIÓN (CIFRADO DE INFORMACIÓN) Y NIVELES DE SEGURIDAD DISPONIBLES PARA VPN

La criptografía es el arte de resolver problemas difíciles, ya que la tecnología VPN depende de las funciones criptográficas y la seguridad de las VPN depende de la solidez criptográfica del algoritmo de cifrado.

El cifrado es tomar un mensaje, por ejemplo “ llegaré tarde “ y convertirlo en algo como “2retr5556%6^*t6tgyhu06”. El otro extremo de este proceso se llama descifrado y es el reverso del cifrado ejemplo el tomar “2retr5556%6^*t6tgyhu06” y convertirlo a “llegaré tarde “.

Todos los algoritmos de cifrado dependen de las funciones criptográficas. (La criptografía es una de las ramas de las matemáticas aplicadas y que está relacionada con operaciones matemáticas en números finitos.

3.1 CRIPTOGRAFÍA SIMÉTRICA

La criptografía simétrica se refiere al conjunto de métodos que permiten tener

comunicación segura entre las partes siempre y cuando anteriormente se hayan intercambiado la clave correspondiente que llamaremos clave simétrica. La simetría se refiere a que las partes tienen la misma llave tanto para cifrar como para descifrar.

Este tipo de criptografía se conoce también como criptografía de clave privada o criptografía de llave privada. Existe una clasificación de este tipo de criptografía en tres familias, la criptografía simétrica de bloques (block cipher), la criptografía simétrica de lluvia (stream cipher) y la criptografía simétrica de resumen (hash functions). Aunque con ligeras modificaciones un sistema de criptografía simétrica de bloques puede modificarse para convertirse en alguna de las otras dos formas, sin embargo es importante verlas por separado dado que se usan en diferentes aplicaciones.

La criptografía simétrica ha sido la más usada en toda la historia, esta ha podido ser implementada en diferente dispositivos, manuales, mecánicos, eléctricos, hasta los algoritmos actuales que son programables en cualquier computadora. La idea general es aplicar diferentes funciones al mensaje que se quiere cifrar de tal modo que solo conociendo una clave pueda aplicarse de forma inversa para poder así descifrar.

Aunque no existe un tipo de diseño estándar, quizá el más popular es el de Fiestel, que consiste esencialmente en aplicar un número finito de interacciones de cierta forma, que finalmente da como resultado el mensaje cifrado. Este es el caso del sistema criptográfico simétrico más conocido, DES.

3.1.1 Sistema DES.

Es un sistema criptográfico que toma como entrada un bloque de 64 bits del mensaje y este se somete a 16 interacciones, una clave de 56 bits, en la práctica el bloque de la clave tiene 64 bits, ya que a cada conjunto de 7 bits se le agrega un bit que puede ser usada como de paridad. Dependiendo de la naturaleza de la aplicación DES tiene 4 modos de operación para poder implementarse: ECB (Electronic Codebook Mode) para mensajes cortos, de menos de 64 bits, CBC (Cipher Block Chaining Mode) para mensajes largos, CFB (Cipher Block Feedback) para cifrar bit por bit ó byte por byte y el OFB (Output Feedback Mode) el mismo uso pero evitando propagación de error.

En la actualidad no se ha podido romper el sistema DES desde la perspectiva de poder deducir la clave simétrica a partir de la información interceptada, sin embargo con un método a fuerza bruta, es decir probando alrededor de 256 posibles claves, se pudo romper DES en Enero de 1999. Lo anterior quiere decir que, es posible obtener la clave del sistema DES en un tiempo relativamente corto, por lo que lo hace inseguro para propósitos de alta seguridad. La opción que se ha tomado para poder suplantar a DES ha sido usar lo que se conoce como cifrado múltiple, es decir aplicar varias veces el mismo algoritmo para fortalecer la longitud de la clave, esto ha tomado la forma de un nuevo sistema de cifrado que se conoce actualmente como triple-DES o 3DES.

3.1.2 Sistema 3DES.

3DES El funcionamiento de 3DES consiste en aplicar 3 veces DES de la siguiente

manera: la primera vez se usa una clave K1(azul) junto con el bloque B0, de forma ordinaria E (de Encription), obteniendo el bloque B1. La segunda vez se toma a B1 con la clave K2 (roja), diferente a K1 de forma inversa, llamada D (de Descencriptión) y la tercera vez a B2 con una clave K3 (verde) diferente a K1 y K2, de forma ordinaria E (de Encription), es decir, aplica de la interacción 1 a la 16 a B0 con la clave K1, después aplica de la 16 a la 1, a B1 con la clave K2, finalmente aplica una vez mas de la 1 a la 16 a B2 usando la clave K3, obteniendo

finalmente a B3. En cada una de estas tres veces aplica el modo de operación más adecuado.

3.2 CRIPTOGRAFÍA ASIMÉTRICA

La criptografía asimétrica es por definición aquella que utiliza dos claves diferentes

para cada usuario, una para cifrar que se le llama clave pública y otra para descifrar que es la clave privada. El nacimiento de la criptografía asimétrica se dio al estar buscando un modo más práctico de intercambiar las llaves simétricas. Diffie y Hellman, proponen una forma para hacer esto, sin embargo solo hasta que el popular método de Rivest Shamir y Adleman RSA publicado en 1978, cuando toma forma la criptografía asimétrica, su funcionamiento está basado en la imposibilidad computacional de factorizar números enteros grandes. Actualmente la Criptografía asimétrica es muy usada; sus dos principales aplicaciones son el intercambio de claves privadas y la firma digital. Una firma digital se puede definir como una cadena de caracteres que se agrega a un archivo digital que hace el mismo papel que la firma convencional que se escribe en un documento de papel ordinario. Los fundamentos de la criptografía asimétrica pertenecen a la teoría de números, en la actualidad la criptografía asimétrica o de clave pública se divide en tres familias según el problema matemático en el cual basan su seguridad. La primera familia es la que basa su seguridad en el Problema de Factorización Entera FE, los sistemas que pertenecen a esta familia son, el sistema RSA, y el de Rabin Williams RW. La segunda familia es la que basa su seguridad en el Problema del Logaritmo Discreto PLD, a esta familia pertenece el sistema de Diffie Hellman DH de intercambio de claves y el sistema DSA de firma digital. La tercera familia es la que basa su seguridad en el Problema del Logaritmo Discreto Elíptico PLDE, en este caso hay varios esquemas tanto de intercambio de claves como de firma digital que existen como el DHE (Diffie Hellman Elíptico), DSAE, (Nyberg-Rueppel) NRE, (Menezes, Qu, Vanstone) MQV, etcétera. Criptografía para principiantes.

Aunque a las familias anteriores pertenecen los sistemas asimétricos más conocidos, existen otro tipo de sistemas que basan su seguridad en problemas diferentes como por ejemplo, en el Problema del Logaritmo Discreto Hiperelíptico, sobre problemas de retículas y sobre subconjuntos de clases de campos numéricos reales y complejos.

3.2.1 Sistema RSA.

RSA, en el caso de RSA el problema matemático es el de la factorización de un número entero n grande (1024 bits, que equivale a un número de 308 dígitos), este número entero se sabe es producto de dos números primos p,q de la misma longitud, entonces la clave pública es el número n y la privada es p,q. El razonamiento del funcionamiento de RSA es el siguiente:

a) a cada usuario se le asigna un número entero n, que funciona como su clave pública

b) solo el usuario respectivo conoce la factorización de n (o sea p,q), que mantiene en secreto y es la clave privada

c) existe un directorio de claves públicas

d) si alguien quiere mandar un mensaje m a algún usuario entonces elige su clave pública n y con información adicional también pública puede mandar el mensaje cifrado c, que solo podrá descifrar el usuario correspondiente, el mensaje m convertido a número (codificación) se somete a la siguiente operación (donde e es constante y público)

Uso: este esquema se usa principalmente para cifrar claves de sistemas simétricos (claves de 128 bits aprox.)

1) Se toma el mensaje M (por ejemplo una clave simétrica de 128 bits (38 dígitos), como en la practica actual es recomendable usar arreglos de longitud de 1024 bits (308 dígitos), los complementa esos 128 bits con una serie de técnicas para obtener un arreglo de 1024 bits, después se aplica un proceso de codificación para que la computadora entienda al mensaje como un número entero m.

2) Se le aplica la formula de cifrado de RSA al entero m

3) Se envía el número entero c

4) Al recibir este número se aplica la formula de descifrado al entero c para obtener el entero m

5) Se decodifica m para obtener el mensaje M

Ejemplo simple

Generación de parámetros

1) p = 3, q = 5 (se eligen dos números primos como clave privada)

2) n = 15 (se calcula el producto, es la clave pública)

3) (n)=(3-1)(5-1)=8

4) Sea e=3, entonces d=3, ya que e*d = 3*3 =9 mod 8 =1 (como este caso solo es para mostrar el funcionamiento no importa que d sea igual a e, sin embargo en la práctica e es pequeño y d es muy grande)

5) Si el mensaje es m=2

Proceso de cifrado

6) El mensaje cifrado es c= me mod n, es decir, c=23 mod 15, o sea c=8

Proceso de descifrado

7) Para descifrar el mensaje m=83 mod 15, es decir, m=512 mod 15, asi m=2

(ya que 512/15=2 mod 15 = m)

Por lo tanto es correcto el funcionamiento.

4. MANEJO DE SEGURIDAD MEDIANTE PROTOCOLOS COMO IPSEC UTILIZANDO AH (ENCABEZADO DE AUTENTICACIÓN) Y ESP COMO CIFRADO DE DATOS.

Como el nombre indica, IPSec proporciona seguridad para datagramas IP. Teniendo en cuenta que la mayoría de las redes no son seguras, por lo que requieren componentes adicionales para proteger los datos durante su transmisión a través de una conexión, IPSec proporciona autenticación de origen, comprobación de integridad y confidencialidad del contenido.

La protección de los datos no es nada nuevo; hay diferentes formas de proporcionar esa seguridad. Algunas aplicaciones proporcionan servicios de seguridad a nivel de aplicación que incluye Nivel de socket seguro (SSL) o Seguridad de nivel de transporte (TLS). En el caso de estos protocolos, la aplicación realiza las llamadas al proveedor de seguridad subyacente para proporcionar estos servicios. Aunque la mayoría de los detalles de la implementación puedan extraerse (por ejemplo, en Windows 2000, la Interfaz del Proveedor de seguridad, o SSPI, proporciona una interfaz común para que las aplicaciones tengan acceso a los componentes de seguridad subyacentes), la aplicación

necesita como mínimo estar "preparada para la seguridad". IPSec elimina este requisito bajando la seguridad al nivel de red. Esto permite a las aplicaciones permanecer independientes de la infraestructura de seguridad subyacente. Los datagramas IP se protegen sin tener en cuenta la aplicación que inicialmente generó el tráfico. En otras palabras, las aplicaciones no son compatibles con IPSec. Las reglas de seguridad las define el administrador sin tener en cuenta qué aplicación se ejecuta; IPSec es transparente para las aplicaciones. Las implicaciones que esto conlleva son importantes; IPSec proporciona la capacidad de autenticar, proteger y opcionalmente cifrar los datos que van por la red IP, que incluye Internet. IPSec proporciona seguridad de extremo a extremo entre equipos y redes.

4.1 FUNCIONAMIENTO DE IPSEC

IPSec proporciona seguridad de datagramas IP. Es de extremo a extremo, lo que implica que sólo el remitente y el destinatario necesitan ser conscientes de los detalles acerca de la seguridad. Los dispositivos entre las dos partes no necesitan preocuparse acerca del cifrado, las claves secretas y otros aspectos, para reenviar todos los datos. Esto es significativo para un cliente como un Banco por dos razones. Primero, la conexión por la que se transmiten los datos puede no ser segura. Esto significa que en muchos casos, la infraestructura de la red subyacente no necesita ser modificada. Segundo, la implementación es relativamente sencilla. Sólo los hosts que necesitan comunicarse tienen que entender IPSec. Los dispositivos intermediarios como los enrutadores no necesitan ser compatibles con IPSec. Para los clientes esto significa que puede implementarse un alto nivel de seguridad sin grandes costos o un cambio significativo para la infraestructura de su red. Es, sin embargo, importante tener en cuenta que los servidores de seguridad y otros dispositivos que bloquean tipos específicos de tráfico necesitan una consideración especial y se explicarán más adelante.

La implementación de IPSec de Windows 2000 está basada en los estándares del sector que desarrolla el grupo de trabajo IETF que trabaja en IPSec, funciona identificando el tráfico que necesita ser protegido y, a continuación, aplicando el nivel definido de seguridad. Así, por ejemplo, el Banco podría identificar el tráfico que reúne ciertos criterios, como la dirección IP de origen o el nombre de host, y elegir un nivel apropiado de seguridad basado en esa identificación.

Utilizando IPSec, los datos se pueden proteger entre hosts, enrutadores de red, o servidores de seguridad específicos, o entre hosts y enrutadores o servidores de seguridad. Utilizando algoritmos de autenticación y de cifrado estándar en la industria, IPSec aprovecha las tecnologías existentes y ofrece un método completo para proteger el tráfico de la red. La protección de datagramas IP es proporcionada por dos protocolos, Encabezado de autenticación (AH) y Carga de seguridad de encapsulación (ESP). AH se utiliza para garantizar la integridad de los datos, proporciona protección antirreproducción y protege la autenticación del host. ESP proporciona una funcionalidad parecida a AH; sin embargo, ESP también incluye la confidencialidad de los datos opcional. Es importante

tener en cuenta que ni AH ni ESP proporcionan los algoritmos criptográficos reales para implementar las características especificadas anteriormente, pero en cambio AH y ESP aprovechan la existencia de algoritmos criptográficos y de autenticación.

IPSec consta de cuatro componentes principales en Windows 2000:

Protocolos IPSec

Asociaciones de seguridad

Directiva de seguridad

Controlador IPSec

4.2 PROTOCOLOS IPSEC

Dos protocolos, AH y ESP, funcionan para proporcionar autenticación, integridad y confidencialidad. Estos protocolos pueden configurarse para proteger toda la carga IP, o simplemente los protocolos de nivel superior de la carga IP. Utilizando los protocolos de forma individual, o en combinación, el Banco puede utilizar la autenticación simple y la comprobación de la integridad, así como el cifrado de los datos que se transmiten a través de una conexión.

4.3 ENCABEZADO DE AUTENTICACIÓN

AH, como se define en RFC 2402, proporciona integridad de los datos trasmitidos a través de claves hash. Actualmente los algoritmos de hash compatibles incluyen HMAC MD5 y HMAC SHA. (HMAC o Código de autenticación de mensajes basado en hash es un algoritmo de clave secreta que crea una firma digital de los datos que pueden comprobarse por el destinatario. MD5 da como resultado un valor de 128 bits, mientras SHA da un valor de 160 bits. Normalmente SHA es más seguro, pero no tan rápido como MD5.) Tenga en cuenta que AH incluye los valores hash de la carga y el encabezado IP, pero no incluye las partes del datagrama que se asume que van a cambiar, como el recuento de saltos. Debido a que tanto el encabezado como la carga se incluyen en valores de hash, AH puede comprobar la información de la dirección y garantizar que los datos IP no han sido manipulados.

Los servicios de antirreproducción también son una función de AH. Los números de secuencia incrementales de forma consecutiva y una ventana de recepción deslizante proporcionan garantías de antirreproducción tanto para AH como para ESP.

AH no proporciona confidencialidad en forma de cifrado de datos; esa es una función de ESP.

4.4 CARGA DE SEGURIDAD DE ENCAPSULACIÓN

ESP es un protocolo de Internet definido en RFC 2406. Utilizado sólo o en combinación con AH, ESP proporciona integridad de datos y cifrado. Los algoritmos de cifrado compatibles con ESP incluyen DES-CBC, DES de 56 bits y 3DES. ESP proporciona también comprobación de la integridad mediante HMAC MD5 y HMAC SHA. Los servicios de antirreproducción se implementan de la misma forma que AH.

Tenga en cuenta que la autenticación, la integridad y los algoritmos de cifrado están determinados como parte de la negociación de seguridad entre los extremos de la comunicación IPSec. Este proceso se conoce como una asociación de seguridad y se explicará en las secciones siguientes.

Pueden usarse ambos protocolos en dos modos diferentes, denominados modo de transporte y modo de túnel. Las operaciones subyacentes de AH y ESP no cambian basadas en el modo de operaciones; lo único que cambia es que los datos se firman para propósitos de integridad. El modo de transporte se usa para proteger paquetes donde el extremo de las comunicaciones es también el extremo criptográfico. En el modo de túnel, el extremo criptográfico es una puerta de enlace de seguridad que proporciona seguridad en nombre de otra red. En este caso, el paquete IPSec se autentica, se comprueba y posiblemente se descifra antes de reenviarse al extremo de las comunicaciones. El modo de túnel podría usarse en un escenario para crear una VPN de enrutador a enrutador. (Para obtener más información acerca de VPN y el enrutamiento, En el modo de transporte, un encabezado se posiciona entre la parte IP del datagrama y los encabezados de la capa superior, mientras que en el modo de túnel, todo el paquete IP se encapsula en otro datagrama IP y un encabezado IPSec se sitúa entre los dos encabezados IP.

Los problemas más significativos actualmente son la interoperabilidad con las implementaciones de proveedores diferentes y la incapacidad para enviar por túnel el tráfico de multidifusión y de difusión. El último obstaculiza la habilidad de crear conexiones VPN de enrutador a enrutador utilizando el modo de túnel de IPSec. Por ahora, la solución es usar L2TP/IPSec para la creación de túneles para las conexiones de acceso remoto. La implementación de L2TP e IPSec se explicarán más adelante.

Debido a la forma en la que IPSec se implementa en Windows 2000, el Banco puede optar por aplicar niveles diferentes de IPSec en áreas con requisitos específicos. Esto proporciona flexibilidad para definir áreas que requieren una seguridad baja, media y alta, y aplicar por lo tanto IPSec. Por ejemplo, el Banco puede haber determinado que la autenticación y la integridad se requieren en todas las áreas, pero que la confidencialidad sólo es necesaria en ciertos entornos de alta seguridad. En este caso, la aplicación sería de la siguiente forma:

Para las áreas que requieren confidencialidad, se requiere tanto ESP como AH. Tenga en cuenta que el cifrado de los datos es caro desde el punto de vista de los

recursos informáticos. Tenga esto en consideración en todos los planes en los que utilice las características de cifrado de ESP.

Para las áreas que no requieren confidencialidad, AH es suficiente para proporcionar autenticación e integridad.

Asociaciones de seguridad

Antes de que dos hosts puedan comunicarse usando IPSec, deben establecer primero las directrices para esa sesión (por ejemplo, el método de la autenticación y el algoritmo de cifrado). Tenga en cuenta la asociación de seguridad (SA) como el acuerdo entre las dos partes referente a los valores de configuración de la seguridad que se van a emplear. Por ejemplo, si el Host A desea comunicarse con el Host B, deben estar de acuerdo en ciertos valores de configuración. Utilizarán AH o ESP para la integridad, Kerberos o certificados para la autenticación, etc.

Las asociaciones de seguridad son unidireccionales, lo que significa que las asociaciones de seguridad independientes deben establecerse para definir los parámetros de seguridad para el tráfico entrante y saliente. Además, las asociaciones múltiples existirán si un host está comunicándose con uno o más hosts IPSec simultáneamente. Las asociaciones de seguridad se almacenan en una base de datos en cada equipo IPSec. En la base de datos, cada SA se identifica por un Índice de parámetros de seguridad (SPI) que se incluye en cada AH o encabezado ESP. El destinatario usa este SPI para decidir qué SA utilizar para procesar los paquetes entrantes.

IETF ha definido el marco para el establecimiento de asociaciones de seguridad para el intercambio de claves asociadas. El Intercambio de claves de Internet (IKE) administra la creación de asociaciones de seguridad y genera las claves utilizadas para proteger la información. IKE utiliza Diffie-Hellman para generar y administrar claves. La técnica de Diffie-Hellman proporciona la capacidad de generar las claves simétricas que se usarán tanto para cifrar como para descifrar los datos. La criptografía simétrica requiere un canal seguro para intercambiar las claves e IKE proporciona este canal.

Nota: Si una asociación de seguridad no puede establecerse, la directiva IPSec puede configurarse aunque se bloqueen las comunicaciones o se envíen datos sin requerir la negociación de la SA.

Gráfica 15. Asociación de seguridad.

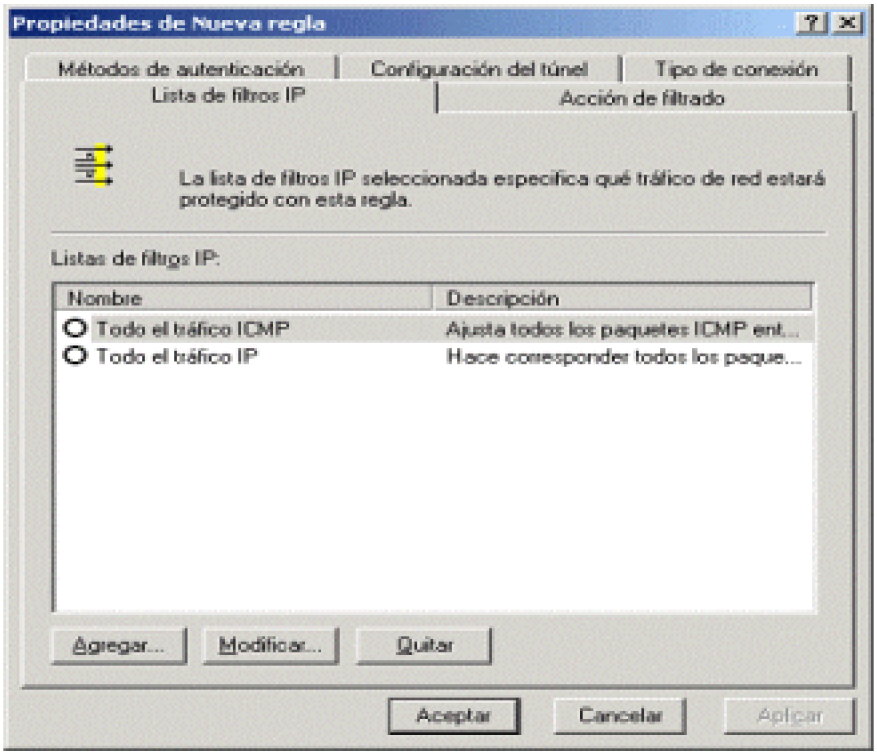
Directiva de seguridad

La base de la seguridad IP es identificar los tipos específicos de tráfico y asegurarse de que ese tráfico es seguro. Al Banco le gustaría proteger el tráfico entre las sucursales y la red corporativa mediante una conexión VPN. La seguridad en el contexto de IPSec podría significar autenticación, no modificable y posiblemente con cifrado. Determinar qué

tráfico proteger y el nivel de seguridad que se va a implementar se define en la directiva de seguridad. Windows 2000 proporciona administración basada en directivas en la cual las directivas IPSec pueden asociarse con equipos, sitios, dominios o unidades organizativas. Las directivas deben definirse teniendo en cuenta la seguridad requerida o deseada de la organización.

La implementación de la directiva IPSec se controla a través del uso de reglas. Las reglas rigen cómo y cuándo la directiva IPSec se invoca teniendo en cuenta el origen, destino y tipo de tráfico IP. Las reglas contienen filtros que permiten identificar un tipo específico de tráfico y aplicar las acciones de seguridad cuando existe una coincidencia.

Las propiedades de una regla son las siguientes:



Gráfica 16. Propiedades de una regla.

La Lista de filtros IP define qué tráfico se protegerá con esta regla.

La Acción de filtrado enumera las acciones de seguridad que tendrán lugar en una lista de filtros IP coincidentes.

Los Métodos de autenticación especifican si utilizar Kerberos, certificados o recursos secretos compartidos para autenticar cada equipo.

La Configuración del túnel especifica si se aplica la regla para un túnel.

El Tipo de conexión permite al administrador especificar a qué conexiones se aplica esta regla. Las tres opciones son Todas las conexiones de red, LAN o Acceso remoto.

Todas las conexiones de red requiere que el host al que se le aplica la directiva examine todo el tráfico (entrante o saliente). Por ejemplo, el configurar esta directiva en un servidor SQL que mantiene una base de datos financiera significa que todas las

conexiones a y desde el servidor requieren un examen para determinar las acciones de seguridad específicas que se emprenderán.

LAN requiere que se examine todo el tráfico LAN a este host.

Finalmente, Acceso remoto examina todas las comunicaciones con el servidor a través de conexiones de acceso remoto.

Windows 2000 contiene automáticamente una regla de respuesta predeterminada. Esto asegura que el equipo responderá a las solicitudes de comunicaciones seguras aunque una regla no esté definida para un equipo que solicite comunicaciones seguras. Por ejemplo, si el Host B solicita comunicaciones seguras al Host A, pero el Host A no tiene un filtro entrante definido para el Host B, la regla de respuesta predeterminada se invocará y la seguridad se negociará entre el Host A y el Host B. La regla se designa para todas las directivas definidas, pero no tiene que estar activa.

4.5 CONTROLADOR IPSEC

El controlador IPSec está cargado al inicio si se ha definido una directiva IP. Es responsable de supervisar todo el tráfico IP y proteger los paquetes basados en los requisitos de la directiva IPSec. El controlador IPSec es responsable de:

Revisar cada paquete IP que entra o sale si coincide con un filtro de directiva IP específico.

Solicitar asociaciones de seguridad para las conexiones nuevas.

Implementar la directiva que especifica un método de autenticación (Kerberos o certificados, por ejemplo).

Actualizar y eliminar asociaciones de seguridad.

Gráfica 17. Pasos para proteger un datagrama.

Introducción al proceso

El proceso de seguridad IP es el siguiente:

Un paquete IP coincide con un filtro IP que forma parte de una directiva de seguridad IP. Por ejemplo, un filtro de salida especifica que debe protegerse todo el trafico TCP dirigido al puerto 23 (telnet).

IKE negocia una asociación de seguridad que se almacena en su base de datos.

Como el controlador IPSec recibe los paquetes de salida, se aplican los métodos de seguridad definidos.

Requisitos de la empresa

Ahora que se entienden los fundamentos de IPSec, se puede evaluar como una solución para un Banco. Esto necesitará incluir un examen del entorno actual del cliente y los problemas específicos de interoperabilidad, rendimiento e integración de las tecnologías en la infraestructura existente. De esta forma, se puede determinar cómo IPSec puede proporcionar las soluciones de seguridad deseadas.

Además, una vez que se han establecido las ventajas, es necesario ver los requisitos de la empresa; qué áreas necesitan protegerse y qué nivel de seguridad se requiere.

Como se explicó anteriormente, el Banco tiene varios requisitos de seguridad. El primer requisito del Banco es garantizar que la información confidencial a la que se tiene acceso en servidores específicos y que se actualiza a través de la red sea auténtica, no sujeta a rechazo y confidencial. Esto incluye la habilidad de autenticar los host de origen y de destino, garantizar la integridad de los datos que se transmiten y proporcionar servicios de cifrado.

Segundo, hay sucursales en Oficina1 y Oficina2 que se conectan a la oficina central corporativa mediante Internet. Esto permite al Banco proporcionar conectividad ampliada entre las sucursales sin tener que proporcionar vínculos punto a punto entre cada sucursal y la oficina central corporativa. Todo lo que se requiere en ambos extremos es una conexión a Internet y la red local. Sin embargo, Internet es una red pública que proporciona poca seguridad inherente. ¿Cómo puede aprovechar el Banco la comodidad de usar Internet para conectar sitios remotos con la oficina central corporativa, al tiempo que se mantienen los niveles de seguridad más altos?

Estos dos requisitos pueden cumplirse utilizando las tecnologías proporcionadas por IPSec y Windows 2000. En la sección siguiente, se examinara cómo el Banco puede usar IPSec y Windows 2000 para alcanzar estos objetivos.

En general, las directivas IPSec pueden implementarse para que cumplan los requisitos de seguridad del equipo, dominio o unidad organizativa. Determinar los requisitos de seguridad del Banco permitirá comprender en qué nivel se puede aplicar la directiva IPSec. El escenario que se a identificado para el Banco es con el deseo de autenticar a todos los hosts que se comunican con los servidores seguros que alojan los datos financieros de la oficina central corporativa. Estos datos residen en servidores físicamente seguros que se han asignado a direcciones IP estáticas. Una infraestructura

de clave pública (PKI) ya se ha implementado internamente para las comunicaciones de la intranet, por lo que el Banco desearía proporcionar autenticación de host IPSec que utilice certificados x.509. Estos datos también necesitan ser protegidos usando los servicios de cifrado proporcionados por IPSec. Dado que todas las comunicaciones de los Bancos están dentro de los límites de la ciudad, el cifrado 3DES proporciona los algoritmos más fuertes. Además, ¿recuerda las sucursales de Oficina1 y Oficina2? Están usando actualmente las conexiones VPN de enrutador a enrutador para la oficina central corporativa mediante PPTP. Basado en los riesgos de seguridad inherentes de usar una red pública como Internet como red troncal para esta conectividad y la incapacidad de PPTP para proporcionar autenticación de host, el Banco ha elegido implementar el Protocolo de túnel de nivel 2 (L2TP) con IPSec para la autenticación, integridad y confidencialidad. Explicaremos los detalles específicos y las ventajas de L2TP en una sección posterior.

En este momento, se han identificado las necesidades del Banco y se esta preparado para la implementación. Windows 2000 proporciona la interfaz para crear y administrar la implementación de IPSec localmente o como parte de la implementación de la Directiva de grupo en Active Directory.

4.6 DIRECTIVAS PREDEFINIDAS

En este momento es obvio que el Banco tiene ciertos requisitos de seguridad que pueden ser compatibles mediante IPSec y las tecnologías asociadas. Sin embargo, el desarrollo de una estrategia de implementación de IPSec implica más que las tecnologías en sí mismas. Antes de distribuir IPSec, el arquitecto también necesita considerar las características que se desea incluir así como el tiempo, esfuerzo y costos que implican la creación de la tecnología más apropiada para el cliente. Otras cuestiones que se deben tener en cuenta:

¿Qué repercusión tendrá en el rendimiento? La implementación de IPSec aumentará la utilización del procesador, el tráfico IP y el tamaño del paquete IP.

¿Qué efecto tendrá en la red existente? Para el Banco, la eficacia del proceso adicional en los pocos equipos que realmente usarán IPSec y la carga en la red prevalecieron sobre los intereses de seguridad. Esto no quiere decir que sea el caso de cada entorno. Se requiere una consideración cuidadosa de todos los hechos para una implementación correcta. Si el rendimiento se convierte en un problema, las tarjetas de red dedicadas pueden ser una solución apropiada.

4.7 CREAR LA DIRECTIVA PARA EL DOMINIO

Hasta ahora, se evaluaron las necesidades comerciales del Banco y solo identificado las

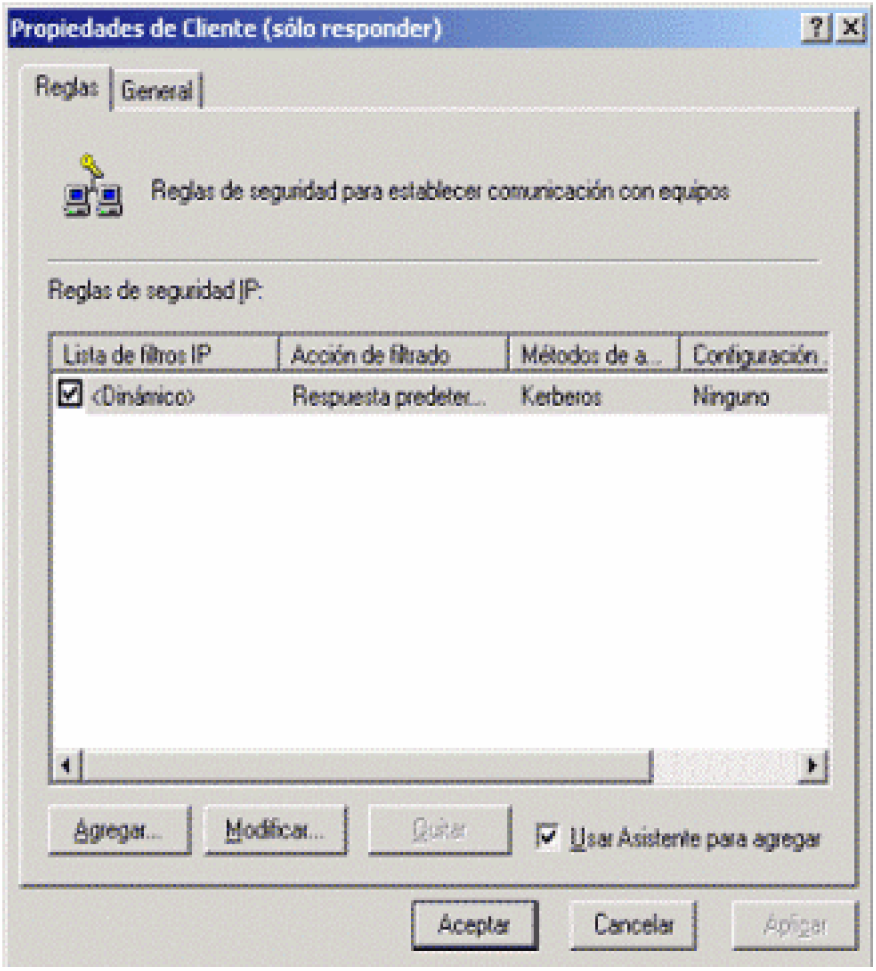
tecnologías pertinentes, y ahora se esta preparado para llevar a cabo la implementación. El Banco desea garantizar que todo el tráfico entre los servidores seguros que alojan información confidencial y los hosts que tienen acceso a dicha información es auténtico, sin modificaciones y cifrado. La autenticación aprovechará un PKI existente que utilice certificados x.509. La comprobación de la integridad se proporcionará utilizando HMAC-MD5 y el cifrado de los datos se implementará utilizando 3DES. Esto puede hacerse mediante la característica Directiva de grupo de Windows 2000 para difundir la regla IPSec. Recuerde que la directiva IPSec puede implementarse en el equipo, dominio o nivel de unidad organizativa local. Dado que la directiva que está implementando el Banco sólo es aplicable a unos pocos servidores, es conveniente colocar esos servidores en una unidad organizativa. Después, la directiva puede aplicarse a la unidad organizativa, y para los servidores se aplicará la directiva según residan en la unidad organizativa en particular. Esto eliminará los procesos innecesarios en el resto de equipos cliente.

Hay un elemento adicional que se debe tener en cuenta: los equipos cliente. De forma predeterminada, las directivas que no son IPSec se aplican a los hosts en un entorno Windows 2000. Sin embargo, para que los clientes respondan de forma apropiada cuando los servidores seguros soliciten seguridad, se debe aplicar una directiva que proporcione esas instrucciones. Los equipos host necesitan poder responder a las solicitudes de autenticación que usan certificados y negociar el cifrado deseado. Esto puede llevarse a cabo modificando la directiva del dominio predeterminada para que sea compatible con los certificados y asignando la directiva de cliente al nivel del dominio.

Asignar y modificar la directiva de cliente predeterminada para permitir la autenticación basada en certificados

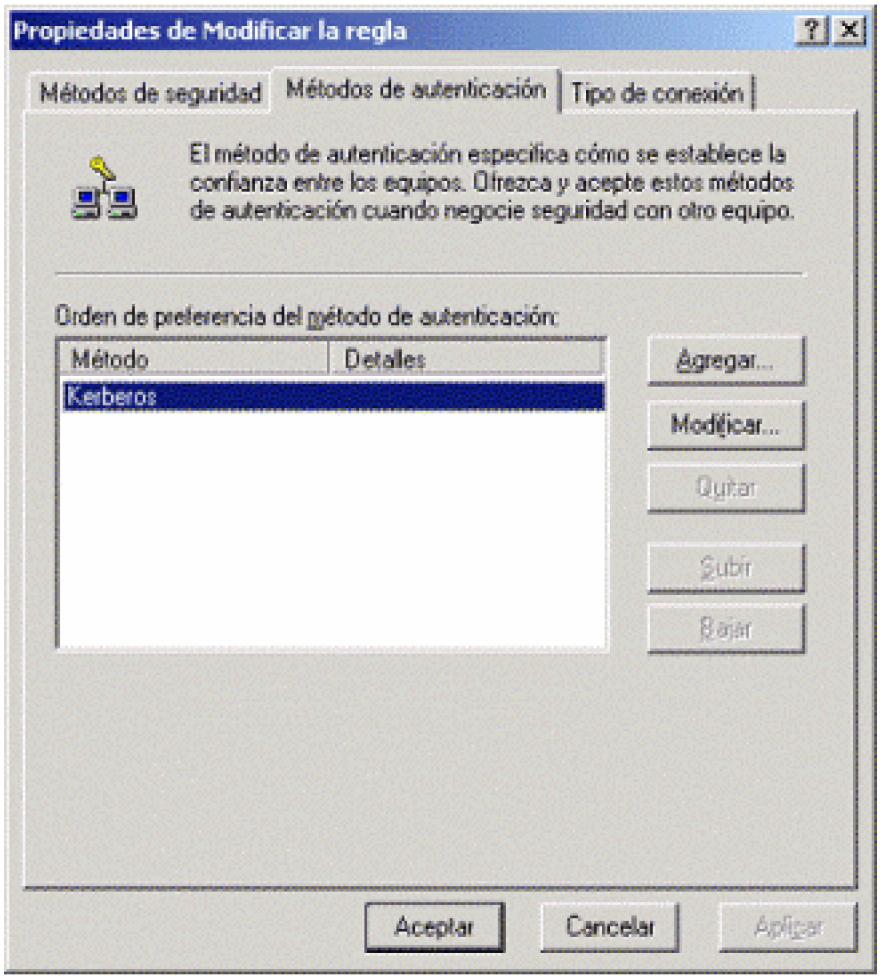
El Banco ha implementado una entidad emisora de certificados (CA) interna que es responsable de emitir y mantener todos los certificados de cliente. La directiva puede cambiarse modificando la regla de respuesta predeterminada para especificar la entidad emisora de certificados.

En la ficha Reglas de la hoja Propiedades de Cliente (sólo responder), seleccione la acción de filtro Respuesta predeterminada y, a continuación, haga clic en Modificar



Gráfica 18. Propiedades de Cliente.

En la ficha Métodos de autenticación de la hoja de propiedades Modificar regla, haga clic en Agregar.

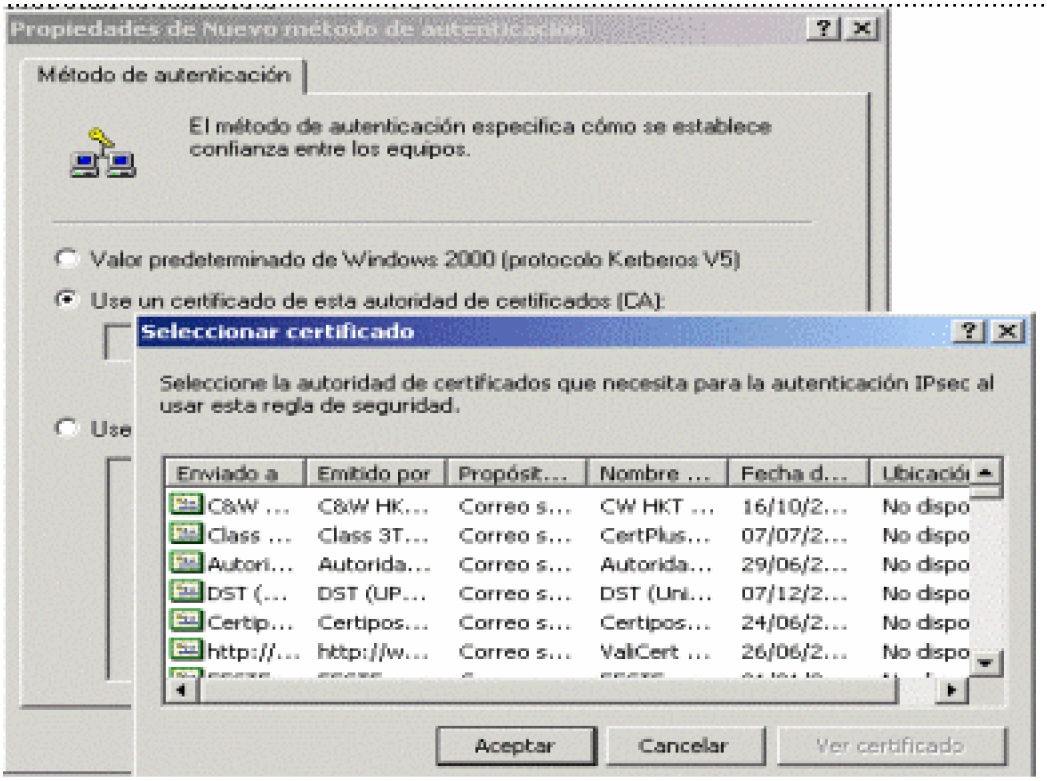


Gráfica 19. Pantalla Métodos de autenticación.

En la hoja de propiedades Nuevo método de autenticación, seleccione Usar un certificado de esta entidad emisora de certificados (CA) y haga clic en Examinar.

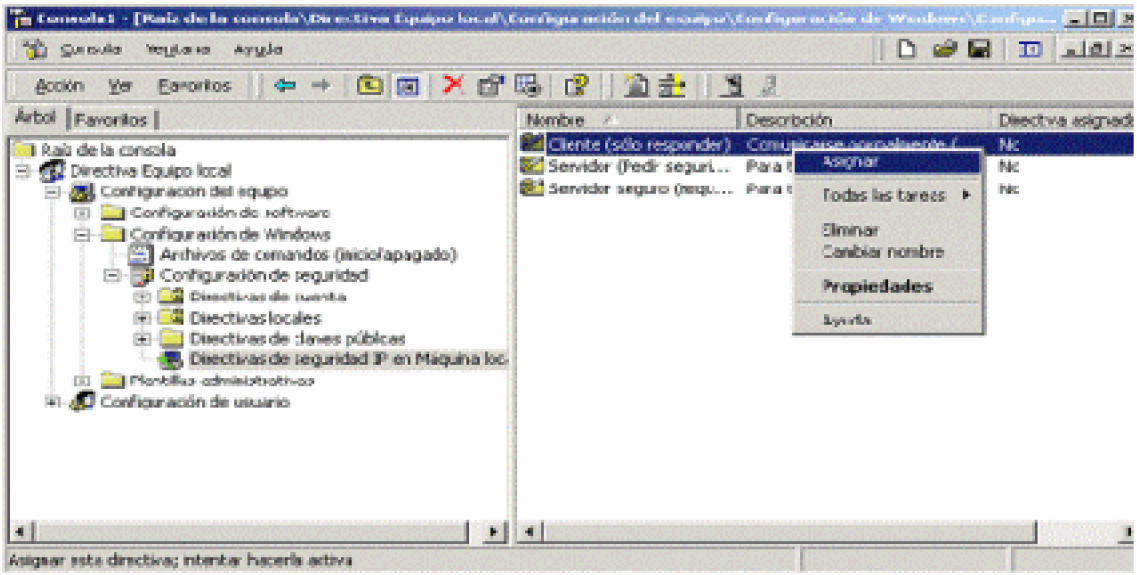
Seleccione la entidad emisora de certificados que desee y haga clic en Aceptar.

Nota: Una vez que la entidad emisora de certificados se haya agregado, asegúrese de que se muestra en la lista antes que la autenticación Kerberos para eliminar los intentos de validación innecesarios.



Gráfica 20. Lista de autenticación.

En el panel de detalles, haga clic con el botón secundario del mouse (ratón) en la directiva Cliente (sólo responder) y, a continuación, haga clic en Asignar.



Gráfica 21. Consola.

Los equipos host que procesan esta directiva responderán a las solicitudes para proteger las comunicaciones y negociarán la asociación de seguridad, pero el mismo host no utilizará comunicaciones seguras si el cliente no las solicita.

4.8 CONFIGURAR SERVIDORES SEGUROS PARA REQUERIR IPSEC

El siguiente paso es configurar una directiva para los servidores que requieran autenticación basada en certificados, integridad y cifrado. Además, la directiva no permite comunicaciones no IPSec. Esto garantiza que sólo se les permitirá el acceso a las partes de confianza que se han especificado en la directiva.

La configuración requiere tres pasos.

Primero, debe modificarse la directiva IPSec del Servidor seguro para requerir certificados válidos para la autenticación.

Segundo, debe definirse un filtro que especifique el tráfico que llega desde cualquier origen a los servidores seguros. Este paso se simplifica utilizando el Asistente para agregar filtros. Esto permite especificar el tráfico desde "cualquier dirección IP" a "mi dirección IP" según determina esta directiva. El hecho de que la directiva sólo se aplicará a los equipos de la unidad organizativa SecureServers asegurará que todo el tráfico hacia y desde esos equipos será auténtico, sin modificaciones y cifrado.

Tercero, el Banco ha elegido adicionalmente implementar 3DES como algoritmo de cifrado predeterminado. Esta modificación también puede hacerse a través de la directiva.

Nota: De forma predeterminada, todos los filtros son "reflejados". Esto especifica que los paquetes con direcciones de origen y de destino invertidas también coincidirán con el filtro.

Implementar IPSec como una solución VPN

El segundo requisito para el Banco era implementar IPSec como parte de una estrategia VPN general para proteger los datos entre las sucursales y la oficina central corporativa. Como se advirtió anteriormente, IPSec puede usarse con el Protocolo de túnel de nivel 2 (L2TP) para proteger el tráfico entre los hosts así como entre los enrutadores o las puertas de enlace.

Los datos transmitidos a través de VPN se encapsulan con un encabezado que le permite enrutarse a través de la red pública. Una vez que el servidor VPN recibe el paquete, se elimina el encabezado y el paquete se reenvía a su destino dentro de la red privada. La red pública proporciona la infraestructura para enviar los datos. El establecimiento de VPN es controlado por varios protocolos de túnel, por ejemplo, Protocolo de túnel punto a punto (PPTP) o Protocolo de túnel de nivel 2 (L2TP).

El cifrado de datos encapsulados se proporciona a través de protocolos individuales como IPSec. Esto asegura que los datos interceptados durante la transmisión sean ininteligibles. Tenga en cuenta que las conexiones L2TP se pueden realizar sin IPSec; sin embargo, esto no se considera una VPN sin la privacidad de los datos garantizada proporcionada por IPSec. Además, IPSec se puede utilizar para crear un túnel sin L2TP,

pero ello tiene varias implicaciones que están más allá del alcance de nuestra discusión. Cuando el controlador IPSec recibe un paquete L2TP, se comprueba para ver si el paquete está incluido en una directiva IPSec. De acuerdo con la configuración de la directiva, IPSec encapsula el mensaje utilizando los encabezados y finalizadores ESP adecuados.

La autenticación del equipo de L2TP a través de IPSec requiere que se instale un certificado tanto en el cliente VPN como en el servidor VPN. En los casos donde no sea conveniente, se puede configurar una clave compartida para que proporcione la autenticación del cliente y del servidor VPN.

Nota: Esto no es tan seguro como los certificados del equipo, pero proporciona una alternativa para organizaciones más pequeñas que aún no cuentan con una infraestructura de certificados.

4.9 USO DE IPSEC Y L2TP PARA PROTEGER EL TRÁFICO DE LA SUCURSAL

De forma predeterminada, todos los equipos y usuarios de un dominio Windows 2000 se autentican utilizando el protocolo Kerberos V5. IPSec utiliza los servicios de seguridad de Windows 2000 para proporcionar la autenticación de la conexión de los hosts. Sin embargo, el uso de certificados de claves públicas es un método alternativo en situaciones que incluyen el acceso a Internet, las comunicaciones con equipos que no son compatibles con Kerberos V5 o cualquier acceso remoto basado en L2TP. De hecho, la implementación de Windows 2000 de L2TP/IPSec requiere la autenticación basada en certificados para los hosts participantes. El uso de certificados para la autenticación del equipo requiere al menos una entidad emisora de certificados (CA) de confianza. El Banco ha implementado una entidad emisora de certificados raíz independiente para proporcionar certificados a equipos cliente. Tenga también en cuenta que Windows 2000 es compatible con la mayoría de las entidades emisoras de certificados estándar de la industria, como VeriSign y Entrust.

El Banco está actualmente proporcionando compatibilidad PPTP de Windows 2000 para la conectividad entre las sucursales y la oficina central corporativa. El enrutador de la sucursal se conecta a Internet y, a continuación, utiliza PPTP para tener acceso al servidor VPN y a la red corporativa. Debido a la inseguridad inherente de Internet, el administrador de la red desearía implementar el protocolo de túnel utilizando L2TP e IPSec. El Banco tiene conexiones permanentes (T1) a Internet a través de los enrutadores de la sucursal y de la oficina central corporativa. La conexión a la LAN es un adaptador instalado en el enrutador de Windows 2000.

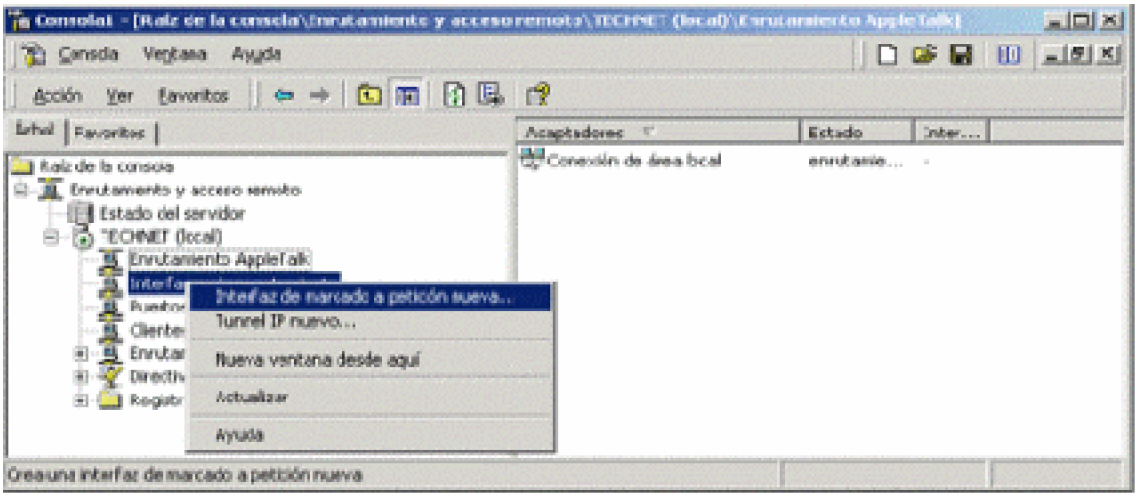
Gráfica 22. Protocolo de túnel utilizando L2TP.

La implementación. Para utilizar L2TP a través de una conexión IPSec, tanto el servidor como el cliente VPN deben tener certificados de equipo para autenticarse. Tenga en cuenta que esto se configuró en el primer escenario como parte de la directiva predeterminada para el Banco. El Servicio de enrutamiento y acceso remoto de Windows 2000 proporciona compatibilidad tanto para túneles L2TP como para PPTP.

En el enrutador de la sucursal, es necesario configurar la conexión que se utilizará para tener acceso al enrutador de la oficina central corporativa. Ésta sería la interfaz conectada a Internet. Al configurar esta interfaz para el Banco se incluyó la especificación del extremo del túnel. Tenga en cuenta que dado que se utiliza esta conexión para una conexión de enrutador a enrutador, los valores de configuración deben reflejarse en ambos lados del túnel. El proceso empleado para el Banco se detalla a continuación. La mayoría del proceso se realiza con la ayuda de un asistente y puede invocarse desde los Servicios de enrutamiento y acceso remoto. Para obtener más información, consulte la Ayuda en pantalla para la configuración de VPN de enrutador a enrutador basada en L2TP.

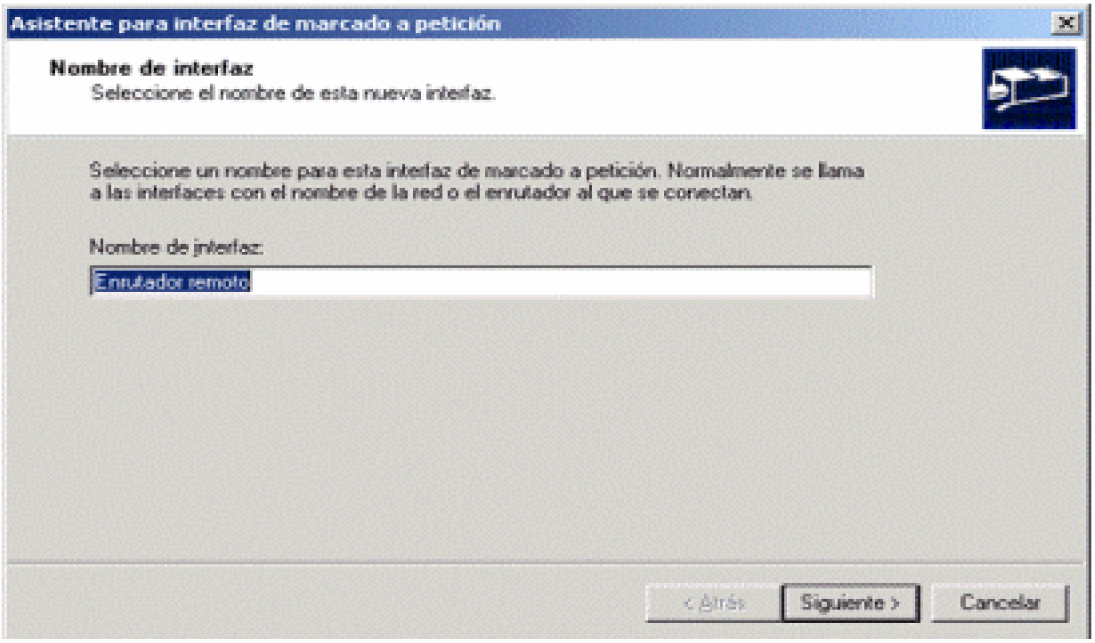
Para configurar una solución VPN de enrutador a enrutador utilizando L2TP/IPSec

En el panel del árbol del complemento Servicios de enrutamiento y acceso remoto, haga clic con el botón secundario del mouse (ratón) en Interfaces de enrutamiento y, a continuación, haga clic en Nueva interfaz de marcado a petición. Aparecerá el Asistente para Interfaz de marcado a petición nueva.



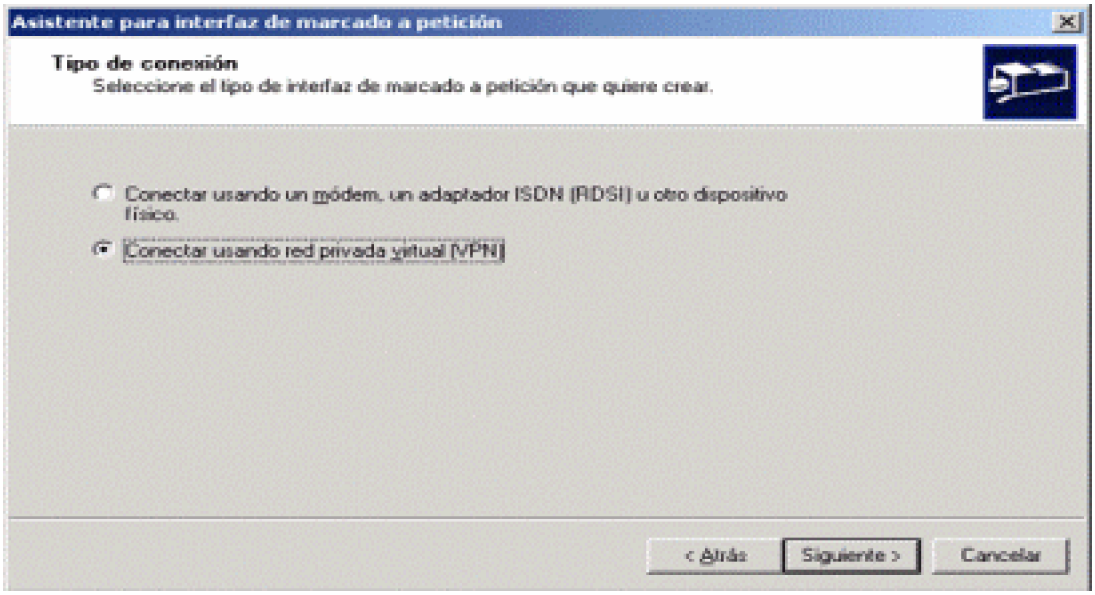
Gráfica 23. Consola enrutamiento y acceso remoto.

Escriba el nombre de la nueva interfaz y haga clic en Siguiente.



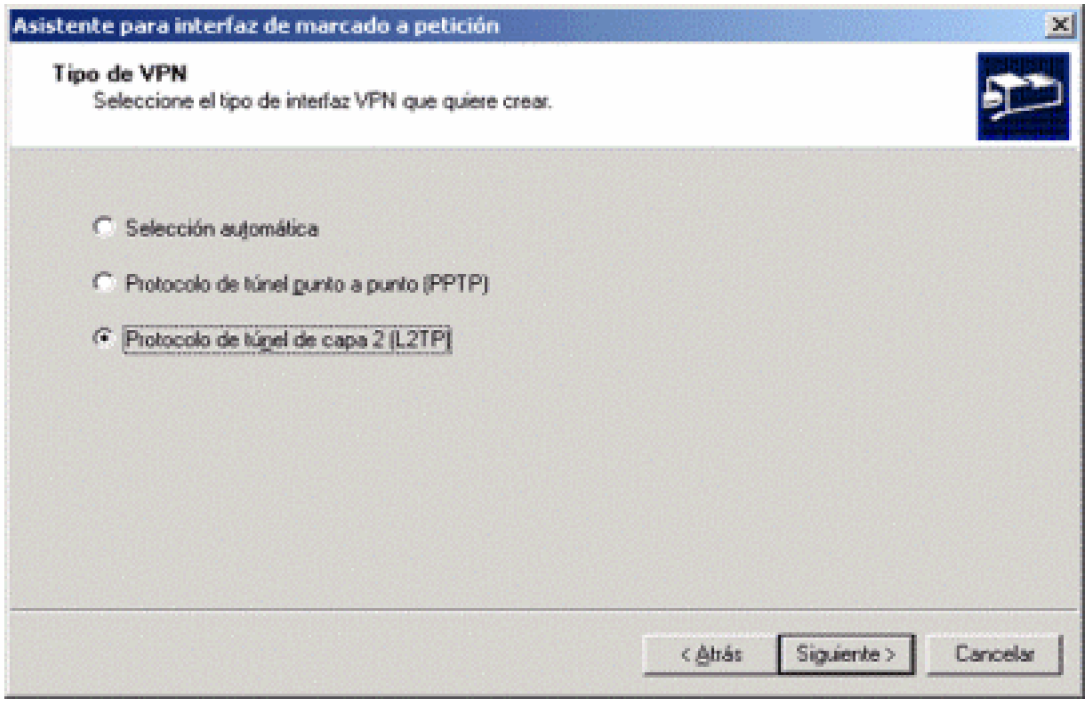
Gráfica 24. Asistente de interfaz.

Para Tipo de conexión, seleccione Conectar usando red privada virtual (VPN) y, a continuación, haga clic en Siguiente.



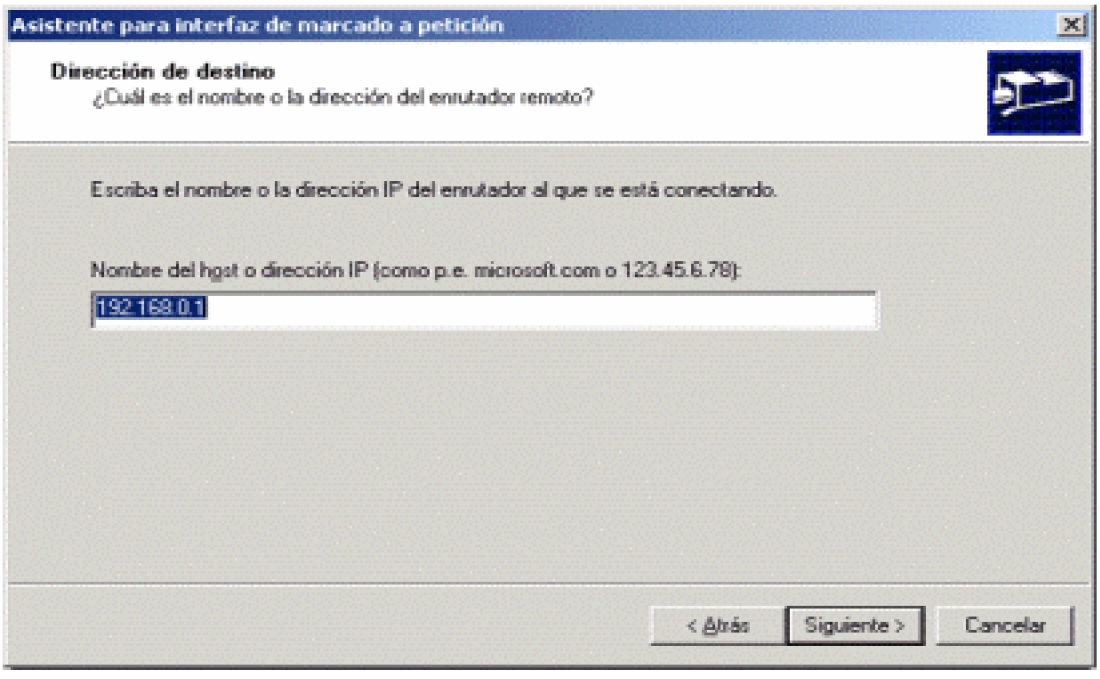
Gráfica 25. Asistente de interfaz paso 2.

Para Tipo de VPN, seleccione Protocolo de túnel de capa 2 (L2TP) y, a continuación, haga clic en Siguiente.



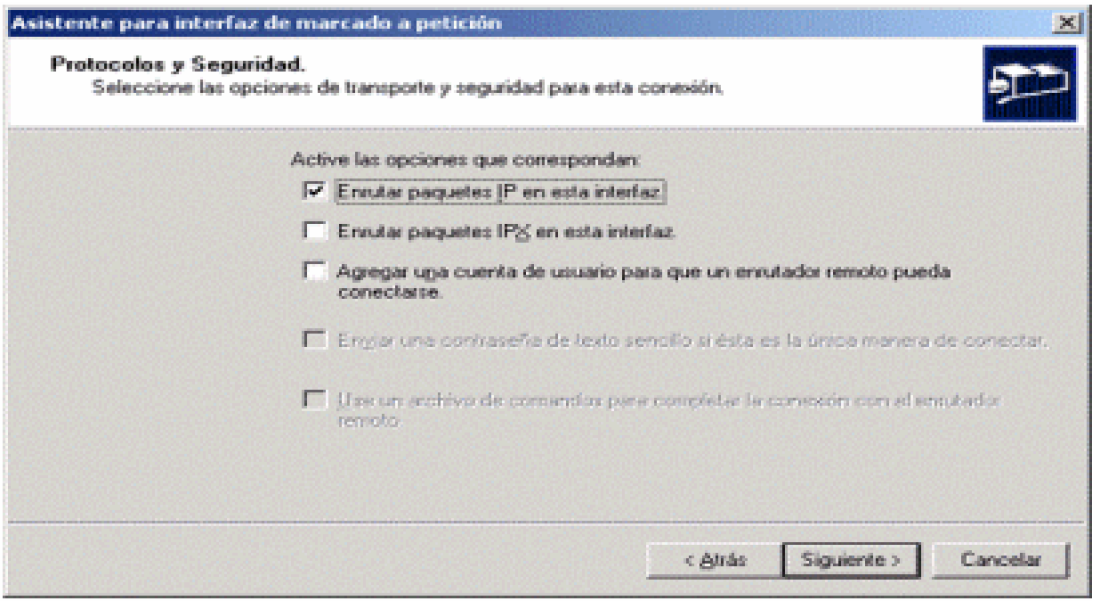
Gráfica 26. Asistente de interfaz paso 3.

Para Dirección de destino, escriba el nombre de host o la dirección IP y, a continuación, haga clic en Siguiente.



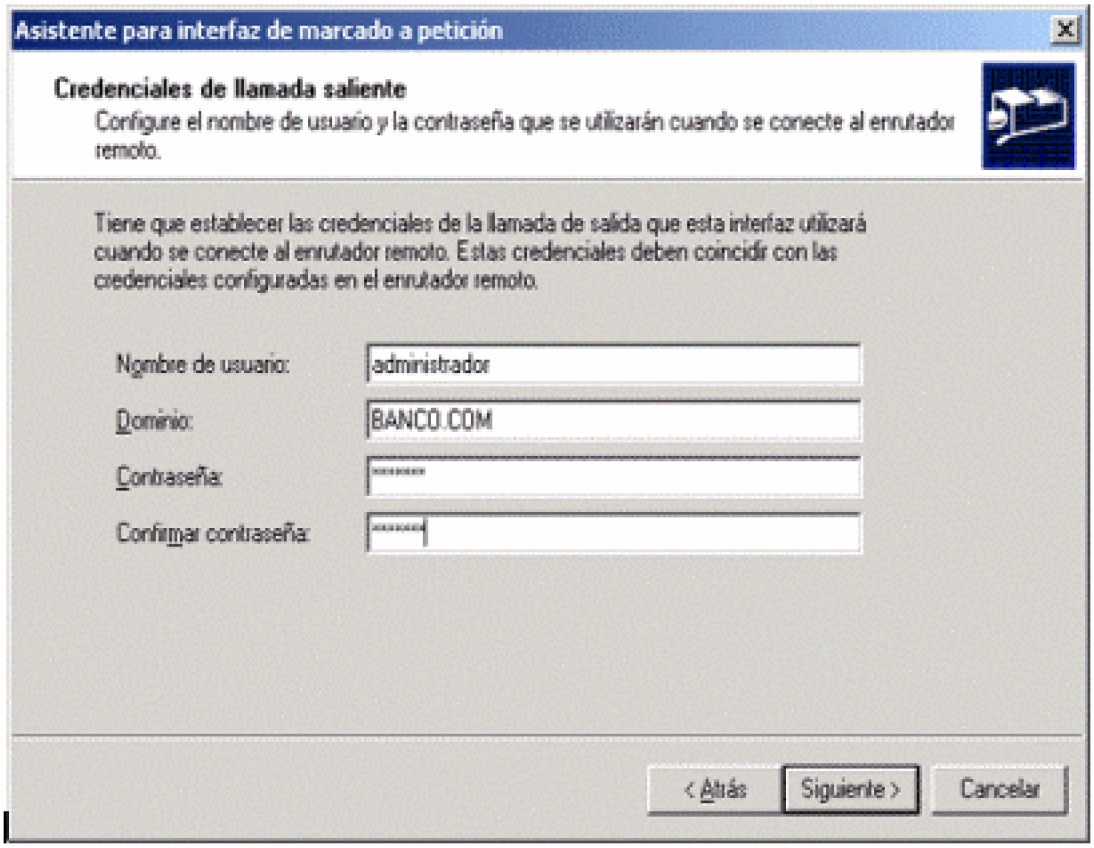
Gráfica. 27. Asistente de interfaz paso 4.

Para Protocolos y seguridad, active la casilla de verificación Enrutar paquetes IP en esta interfaz y, a continuación, haga clic en Siguiente.



Gráfica 28. Asistente de interfaz paso 5.

Para Credenciales de llamada saliente, escriba el nombre de usuario, dominio y contraseña; confirme la contraseña y, a continuación, haga clic en Siguiente.

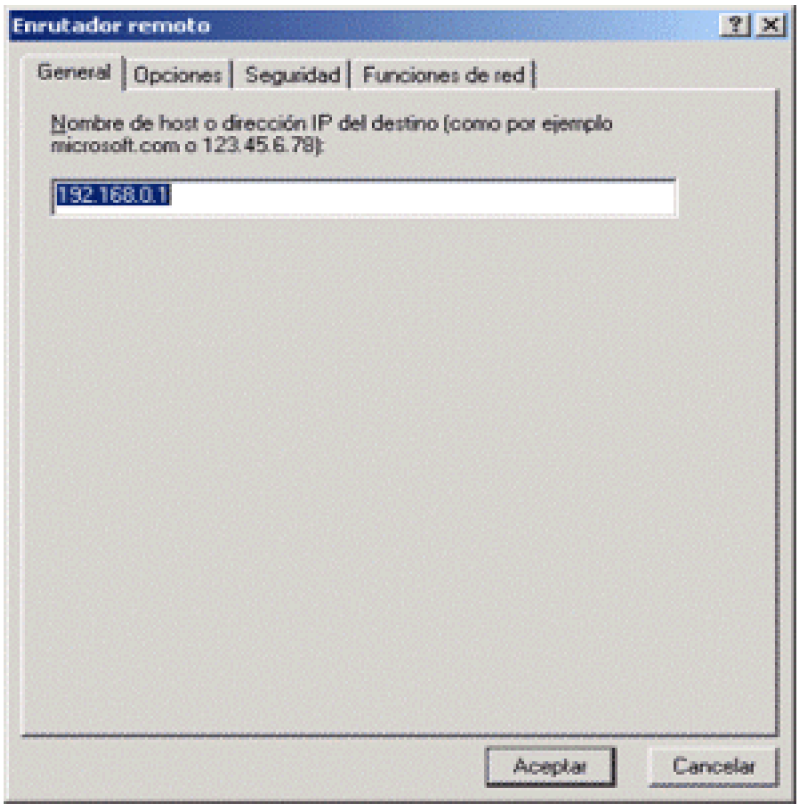


Gráfica 29. Asistente de interfaz paso 6.

Haga clic en Finalizar para terminar el proceso de configuración.

Cualquiera de las opciones adicionales que necesitan configurarse para la conexión,

como la dirección IP para la interfaz, la seguridad, etc., pueden configurarse en la hoja de propiedades para la interfaz.



Gráfica 30. Enrutador remoto.

Los servidores VPN que proporcionan un punto de acceso desde el exterior a la red corporativa pueden requerir filtros especiales para asegurarse que los paquetes IPSec no son rechazados en el servidor VPN. Para evitar el tráfico distinto de L2TP/IPSec desde el que se enruta a la red corporativa, el servidor VPN debe configurarse usando el complemento Servicios de enrutamiento y acceso remoto de la manera siguiente:

Los puertos 50 y 51 de TCP para el tráfico IPSec AH y ESP entrante y saliente.

El puerto 500 UDP, entrante y saliente, para el tráfico de negociación IKE.

Tenga en cuenta que estos pasos necesitan realizarse en ambos lados de la conexión para que el VPN de enrutador a enrutador funcione correctamente.

El diseño de una implementación de IPSec requiere una comprensión de las tecnologías subyacentes así como el conocimiento acerca de su implementación y administración en Windows 2000. Windows 2000 proporciona una distribución integrada y una infraestructura de administración para simplificar la distribución de IPSec.

Para que la implementación de IPSec se complete correctamente, debe tener en cuenta varias cosas. Primero, evalúe la naturaleza y el tipo de información que se envía por la red y la necesidad de proteger esos datos. ¿Se trata de información propietaria confidencial? Algunas áreas de su red pueden requerir niveles superiores de seguridad mientras que otras áreas pueden estar bien como están. Una clasificación de las áreas

que requieren seguridad alta, seguridad media y seguridad baja puede ser útil a la hora de documentar un plan de proyecto. Un plan correcto conlleva evaluar los riesgos de ataques y la susceptibilidad a los mismos, así como determinar una estrategia basada en la información recopilada.

Además, debe identificar cómo los datos se transmiten a través de la red, cómo están enrutándose. ¿Se tiene acceso a los mismos desde fuera de la red corporativa (mediante conexiones VPN)? Un plan correcto equilibrará las necesidades de seguridad de su entorno con la implementación y la administración de un plan de seguridad. Windows 2000 proporciona una arquitectura integrada a través de la compatibilidad con IPSec, L2TP, Directiva de grupo, Kerberos y certificados para simplificar la implementación de seguridad en su entorno tanto como sea posible.

1 Si la sobrecarga de cálculo de IPSec es suficientemente alta, considere la posibilidad de implementar una solución de hardware. La descarga de las tarjetas de interfaz de red (NIC) permite la descarga de muchos de los procesos de IPSec al NIC. 3Com e Intel admiten actualmente las capacidades de descarga en varios NIC. Las pruebas de rendimiento realizadas por Intel indican un gran aumento del rendimiento cuando se descargan los procesos al NIC. Póngase en contacto con los proveedores específicos para obtener más información.

2 EAP significa Protocolo de autenticación extensible, y permite la negociación entre el cliente y el servidor de acceso remoto en relación con el método de autenticación que se debe utilizar. Los ejemplos serían extensiones para dispositivos biométricos, tarjetas de identificación, etc.

3 Más especialmente, el modo de túnel IPSec es principalmente una conexión basada en unidifusión entre subredes. La interoperabilidad para protocolos de multidifusión, difusión y enrutamiento no queda bien definida. Además, la mayoría de las soluciones de modo de túnel IPSec son implementaciones propietarias difíciles de integrar con soluciones de un proveedor independiente. Por estas razones, L2TP/IPsec parece ser la mejor solución por ahora.

La implementación de IPSec en Windows 2000 proporciona la capacidad de autenticar equipos durante el IKE mediante certificados. Todas las validaciones de certificados las lleva a cabo la API de cifrado (CAPI). El IKE solamente sirve para negociar los certificados a utilizar y proporciona seguridad para el intercambio de credenciales de certificados. La directiva IPSec especifica la entidad emisora (CA) raíz que se utilizará, no el certificado específico que se utilizará. Ambos extremos deben tener una CA raíz común en la configuración de sus directivas IPSec.

He aquí los requisitos del certificado que se utilizará en IPSec:

Certificado almacenado en la cuenta del equipo (almacén del equipo)

El certificado contiene una clave pública RSA que tiene su correspondiente clave privada RSA que se puede utilizar para firmas RSA.

Se utiliza durante un determinado período de validez

Se confía en la entidad emisora raíz

Se puede construir una cadena válida de entidades emisoras mediante el módulo CAPI

Estos requisitos son muy elementales. IPSec no requiere que el certificado de la máquina sea del tipo IPSec, ya que las entidades emisoras existentes puede que no emitan este tipo de certificados.

Obtener un certificado de Microsoft para pruebas

Primero debe obtener un certificado válido de un servidor de certificados. Incluso si tiene otro servidor de certificados que desee utilizar, obtenga primero un certificado de Microsoft para las pruebas. Puede utilizarse cualquier certificado de equipo válido. No se utilizan certificados basados en usuarios. Se ha comprobado la compatibilidad con varios sistemas de certificados, como los de Microsoft, Entrust, VeriSign y Netscape.

Nota: No todos los servidores de certificados inscriben automáticamente el equipo con un certificado. El certificado debe aparecer en la cuenta de equipo local bajo los certificados personales y debe tener el certificado de CA raíz en el almacén Entidades emisoras raíz de confianza.

4.10 PASOS PARA OBTENER UN CERTIFICADO

Abra Internet Explorer y diríjase al sitio de la entidad emisora de certificados. Si no conoce ningún otro sitio del cual recibir certificados, utilice:

http://sectestca1.rte.microsoft.com/

Este sitio proporciona acceso a cuatro entidades emisoras de certificados. En aras de la simplicidad, este procedimiento utiliza un certificado emitido por la CA raíz independiente, sectestca3.

Seleccione Standalone Root (RSA 2048).

Seleccione Request a Certificate y haga clic en Next.

Seleccione Advanced Request y haga clic en Next.

Seleccione Submit a Certificate Request Using a Form.

En el formulario Advanced Certificate Request, escriba las siguientes respuestas:

Identifying Information (información de identificación): a discreción.

Intended Purpose (fines): “Client Authentication” o “Server Authentication”.

Este campo establece el campo extended key usage (uso extendido de claves) del certificado. También existe un campo IPSec Certificate para que cumpla con la especificación, que todavía están desarrollando los grupos de estándares. Se puede utilizar este tipo de certificado si desea interoperar con otras implementaciones de IPSec que lo requieran. Sin embargo, la autenticación de certificados IPSec de Windows 2000 utiliza cualquier certificado válido de la cuenta del equipo, lo que significa que resulta aceptable cualquier configuración de uso de claves extendidas. Las directivas IPSec no

ofrecen ninguna posibilidad de limitar la utilización exclusivamente a certificados IPSec. Si existen varios certificados de equipo en la carpeta de certificados personales del equipo local, sólo se elegirá uno de ellos. El certificado elegido será el primero encontrado que tenga una ruta de confianza de vuelta a esa entidad emisora raíz, comenzando por la primera entidad emisora raíz del Método de autenticación de la regla.

Proveedor de servicios de cifrado: Microsoft Base Cryptographic Provider v1.0

Uso de claves: Firma.

Tamaño de la clave: 1024

Si selecciona Microsoft Enhanced Cryptographic Provider, puede elegir un tamaño de clave mayor. Sin embargo, es posible que se produzca un error en la petición de inscripción debido a que la versión de Windows 2000 no tiene instalado el Strong Cryptography Pack. Si se utiliza este certificado para interoperar con otras implementaciones de IPSec, asegúrese de comprobar si el producto IPSec de la otra empresa puede procesar una firma con un tamaño de clave superior a 1024. Algunos productos de otras empresas también pueden imponer limitaciones a la directiva IPSec en lo tocante al tamaño de la clave utilizada.

Nota: Esta configuración determina si la clave privada puede utilizarse para el cifrado de datos o solamente para firmas. La implementación actual del IKE utiliza claves privadas certificadas únicamente para las firmas. Por lo tanto, un certificado emitido con el uso limitado al intercambio para cifrado de datos no funcionará. Los certificados con ambos usos sí funcionarán.

Crear un nuevo conjunto de claves: habilitado

Usar el almacén de equipo local: habilitado

Opciones adicionales: cumplimente a su gusto

Algoritmo hash: SHA1/RSA

Enviar la petición. Recibirá un mensaje en el que se indica que se ha emitido un certificado para usted.

Haga clic en Instalar este certificado.

Aparecerá un mensaje en el que se indica que el certificado se ha instalado correctamente. Cierre Internet Explorer.

Abra la consola MMC de administración de IPSec en la que agregó un complemento para administrar Certificados (Equipo local).

Compruebe que la inscripción del certificado se ha llevado a cabo correctamente

La carpeta Certificados personales debe contener el nombre de certificado de equipo que seleccionó para la prueba de IPSec de su nombre.

Haga clic en el símbolo + que se encuentra junto a Certificados (Equipo local) para expandirlo. Expanda la carpeta Personal y haga clic en la carpeta Certificados. En el panel derecho deberá ver un certificado emitido para el Administrador o para el nombre de usuario con el que inició la sesión.

Haga doble clic en este certificado del panel derecho. Deberá contener el mensaje Tiene una clave privada correspondiente a este certificado. Observe el nombre de la CA donde aparece Emitido por: (en el ejemplo es SectestCA3). Haga clic en Aceptar.

Nota: Si en las propiedades del certificado del equipo aparece “No tiene una clave privada correspondiente a este certificado”, la suscripción ha sufrido un error y el certificado no servirá para la autenticación IKE de IPSec. Es necesario obtener correctamente una clave privada que corresponda a la clave pública del certificado del equipo.

Expanda Entidades emisoras raíz de confianza y haga clic en la carpeta Certificados. Desplácese hacia abajo y busque un certificado en este almacén con el nombre de la entidad emisora que aparece en Emitido por.

Repita todos los pasos de este procedimiento para recuperar un certificado en la otra máquina de pruebas.

Nota: Si se obtuvo un certificado emitido desde el Servidor de certificados de Microsoft con la opción establecida como Protección segura de claves privadas, el usuario deberá escribir un número de identificación secreto (PIN) para tener acceso a la clave privada cada vez que se utilice para firmar datos en la negociación IKE. Dado que la negociación IKE se lleva a cabo en segundo plano mediante un servicio del sistema, no existe ninguna ventana con la que solicitar información al usuario. Por lo tanto, los certificados obtenidos con esta opción no funcionarán con la autenticación IKE.

Configurar la autenticación del certificado para una regla

Si va a crear una nueva regla, puede buscar la entidad emisora que se utilizará. Se trata de una lista de certificados de entidades emisoras que se encuentran en la carpeta Entidades emisoras raíz de confianza, no una lista de los certificados personales de su equipo. Esta especificación de CA en una regla IPSec tiene dos finalidades. En primer lugar, proporciona IKE con una CA raíz en la que confía. IKE en su equipo enviará una petición de un certificado válido a esta CA raíz para el otro equipo. En segundo lugar, la especificación de la CA proporciona el nombre de la CA raíz que utilizará el equipo para buscar su propio certificado personal en respuesta a una petición del interlocutor.

Precaución Debe seleccionar al menos la entidad emisora raíz de la que depende el certificado del equipo, esto es, la CA de nivel superior en la ruta de certificación del certificado de equipo que se encuentra en el almacén personal del equipo.

Vuelva a la carpeta Directivas de seguridad IP en la MMC.

Haga doble clic en la directiva Compañero en el panel derecho.

Asegúrese de que la opción Filtro del compañero está seleccionada y haga clic en Modificar.

Seleccione el botón de radio para Todo el tráfico IP.

Haga clic en Modificar.

Asegúrese de que la casilla de verificación Asistente para regla nueva está activada y haga clic en Aceptar.

Haga clic en la ficha Métodos de autenticación.

Seleccione la Clave previamente compartida con los detalles ABC123 y haga clic en Modificar.

Seleccione la opción Usar un certificado de esta entidad emisora de certificados (CA) y haga clic en Examinar. Haga clic para seleccionar la CA utilizada anteriormente: en este ejemplo se trata de SecTestCA3.

Haga clic en Aceptar.

El editor de Reglas IPSec permite crear una lista ordenada de entidades emisoras de certificados que el equipo enviará a petición del equipo interlocutor durante la negociación IKE. Para que la autenticación tenga éxito, el equipo interlocutor debe tener un certificado personal emitido por una de las entidades emisoras raíz de la lista.

Puede continuar agregando y organizando entidades emisoras de certificados cuanto desee.

Haga clic en Aceptar dos veces y, a continuación, haga clic en Cerrar.

Repita el procedimiento completo en la otra máquina. Ahora intente hacer ping desde cada uno de los equipos al otro.

Puede pedir la lista de métodos de autenticación para especificar certificados en primer lugar y, a continuación, Kerberos o clave previamente compartida. Sin embargo, no se puede fragmentar la lista de certificados incluyendo en medio un

método sin certificados.

Al agregar CA raíz adicionales, se puede crear una lista de CA raíz en las que confíe, que es mayor que la lista de entidades que han emitido un certificado para su equipo. Esto resulta necesario para la interoperabilidad en muchos escenarios empresariales.

Es importante entender que el equipo puede recibir peticiones de certificado de un interlocutor destinatario que puede incluir o no una CA raíz en la lista de entidades emisoras de certificados especificada en directiva IPSec. Es necesaria la coordinación con el administrador del destino para acordar la CA raíz que utilizará cada extremo.

Si la petición del destino incluye una entidad emisora de certificados en esta lista, IKE comprobará si su equipo tiene un certificado personal válido que dependa de esta CA raíz. Si lo hace, elegirá el primer certificado personal de equipo válido que encuentre y lo enviará como la identidad del equipo.

Si su equipo recibe una petición de certificado de una CA raíz que no estaba especificada en esta regla de directiva IPSec, enviará el primer certificado que encuentre y que dependa del nombre de CA raíz especificado en su propia regla de directiva IPSec. Dado que las peticiones de certificados son opcionales en el estándar RFC 2409, una vez que su equipo acepte la autenticación por certificado debe enviar un certificado incluso aunque no reciba una petición de certificado IKE, o si la petición de certificado no coincide con los nombres de CA raíz de la directiva de su equipo. En este caso, es probable que la negociación IKE produzca un error, ya que los dos equipos no pudieron ponerse de acuerdo en una CA raíz común. Si la petición del destino no incluye una de las entidades emisoras de certificados, se producirá un error en la negociación IKE.

4.11 COMPROBACIÓN DE LA LISTA DE REVOCACIÓN DE CERTIFICADOS

La mayoría de los servidores de certificados emiten certificados que contienen un Punto de distribución de lista de revocación de certificados (CRL), abreviado a veces todo ello como CDP. Para que un equipo pueda validar totalmente un certificado, debe comprobar que dicho certificado no haya sido revocado por el emisor. Dado que el estándar para realizar esta comprobación ha evolucionado y que existen varios servidores de certificados y sistemas PKI en uso, no todos los sistemas de certificados admiten el mismo método y la funcionalidad de la comprobación de CRL. Por lo tanto, la comprobación de CRL está inhabilitada de manera predeterminada. Antes de habilitar la comprobación de CRL, asegúrese de que la autenticación mediante certificados se lleva a cabo con éxito y que ha examinado el archivo de rastreo Oakley.log para ver cómo aparece este éxito en el registro. (El paso 3 muestra la ubicación de este archivo.)

IKE especifica a CAPI la manera de tratar la comprobación de CRL cuando solicita que se valide un certificado. Para habilitar la comprobación de CRL, el administrador del equipo debe cambiar el valor de la clave de registro que se muestra más abajo. El administrador de directivas IPSec y el administrador del servidor de certificados deben determinar la configuración adecuada de este valor.

Para habilitar que IKE compruebe la CRL

En el menú Inicio, haga clic en Ejecutar y escriba regedt32. Haga clic en OK. Esto iniciará el Editor del Registro.

Diríjase a HKEY_LOCAL_MACHINE en la máquina local.

Diríjase a la siguiente ubicación: System\CurrentControlSet\Services\Rdr\Parameters

Haga doble clic en PolicyAgent.

En el menú Edición, haga clic en Agregar clave.

Escriba el Nombe de clave (distingue entre mayúsculas y minúsculas): Oakley.

Deje Clase en blanco y haga clic en Aceptar.

Seleccione la nueva clave, Oakley.

En el menú Edición, haga clic en Agregar valor.

Escriba el Nombe de valor (distingue entre mayúsculas y minúsculas): StrongCrlCheck.

Seleccione el Tipo de dato: REG_DWORD y haga clic en Aceptar.

Escriba un valor, bien 1 ó 2, según el comportamiento que desee habilitar:

Utilice 1 para dar un error en la validación del certificado sólo si la comprobación de CRL contesta que el certificado se ha revocado (modo normal de comprobación de CRL).

Utilice 2 para dar un error en la validación del certificado ante cualquier error de comprobación de CRL. Ésta es la forma más restrictiva y se utiliza cuando se debe tener acceso a través de la red al punto de distribución de CRL y no debe indicar que nunca se emitió el certificado o cualquier otro error. En realidad, un certificado supera este nivel de comprobación únicamente si el proceso de la CRL afirma claramente que el certificado no se ha revocado.

Haga clic en Hexa como la Base. Haga clic en Aceptar

Salga del Editor del Registro.

En la ventana de línea de comandos de Windows 2000, escriba net stop policyagent y, a continuación, escriba net start policyagent para reiniciar los servicios relacionados con IPSec.

Nota: Si su sistema está configurado como un servidor de VPN para L2TP/IPSec, debe reiniciar Windows 2000.

Para inhabilitar la comprobación de CRL, simplemente suprima el valor StrongCRLCheck que se encuentra en la clave Oakley y reinicie el servicio o Windows 2000, según sea necesario.

Comprender la negociación IKE (usuarios avanzados)

Esta sección está destinada a aquellos que desean aprender más cerca de los detalles del comportamiento de la negociación IKE. No resulta necesaria para completar los pasos de esta guía. La Ayuda en pantalla de las versiones Server y Professional de Windows 2000 contiene explicaciones detalladas acerca de IPSec, IKE y otros aspectos de la implementación. (El contenido de la Ayuda es el mismo en las versiones Professional y Server, aunque se utiliza una tabla de contenido diferente). Simplemente inicie el complemento Administración de directivas IPSec y elija Ayuda).

En el registro de seguridad se auditan los Aciertos y Errores de IKE, junto con un motivo del error. El procedimiento para habilitar la auditoría se explica al principio de esta guía. Si el servidor utiliza la directiva integrada Servidor (pedir seguridad), o en realidad cualquier directiva personalizada que tenga una regla que utilice la acción de filtrado integrada Pedir seguridad (opcional), la negociación puede retroceder a texto sin formato para los destinos que no contesten a la petición de IKE. Para llevar a cabo el seguimiento de esta acción se audita un suceso de lo que se denomina una asociación de seguridad de software. Esto aparece en el supervisor de IPSec como un valor <ninguna> en la columna Seguridad. Si el servidor utiliza Servidor seguro y desiste de intentar alcanzar un destino que no envía una respuesta IKE, en el registro de seguridad aparecerá un suceso de auditoría de errores con el motivo sin respuesta del interlocutor.

Utilice la directiva Servidor (pedir seguridad) y el registro de auditoría de un servidor para descubrir y rastrear los destinos con los que se comunica normalmente el servidor a lo largo del tiempo. De esta manera, se puede obtener una mejor comprensión acerca de la manera de crear una directiva personalizada que proteja los destinos correctos y permita que otras comunicaciones de mantenimiento e infraestructura se envíen sin proteger.

Modo principal de IKE (fase 1)

La forma larga inicial de la negociación IKE (modo principal o fase 1) lleva a cabo la autenticación y establece una asociación de seguridad (SA) IKE entre las máquinas, lo que implica generar el material de clave maestra. Al resultado se le conoce como una asociación de seguridad IKE. Las reglas de directiva IPSec controlan el modo principal de IKE utilizando solamente las direcciones de origen y de destino obtenidas de los filtros de las reglas. Una vez establecida con éxito, la configuración predeterminada de las directivas predeterminadas mantendrán activa la SA IKE durante ocho horas (consulte Intercambio de claves en la ficha General de la directiva). Si al final de las ocho horas se sigue transmitiendo datos de manera activa, la asociación de seguridad del modo principal se volverá a negociar de manera automática. La asociación de seguridad del modo principal de IKE no resulta visible en la herramienta de supervisión de IPSec. Sin embargo, el administrador local puede mostrarla mediante la línea de comandos netdiag.exe /test:ipsec /v. Netdiag.exe es una herramienta de soporte que se encuentra en la carpeta \Support del CD de Windows 2000 Professional y Windows 2000 Server.

Modo rápido de IKE (fase 2)

La versión más corta de la negociación de IKE (modo rápido) se produce después de que el modo principal establezca una asociación IPSec para proteger el tráfico particular de acuerdo con partes de dirección de origen y de destino, y de protocolo y de puerto, si existen, de los filtros de paquetes de las reglas de la directiva. La negociación de la SA IPSec implica elegir algoritmos, generar claves de sesión y determinar los números de índice de parámetro de seguridad (SPI) utilizados en los paquetes. Se establecen dos asociaciones de seguridad IPSec, cada una de ellas con su propio SPI (la etiqueta del paquete): uno para el tráfico entrante y otro para el tráfico saliente. El supervisor de IPSec muestra únicamente la asociación de seguridad saliente. Tras cinco minutos de inactividad en la SA entrante se eliminan ambas SA IPSec, lo que provoca que la SA saliente desaparezca de la presentación del supervisor de IPSec. Si se vuelve a enviar tráfico que requiera seguridad IPSec, se producirá una negociación del modo rápido para volver a establecer dos nuevas asociaciones de seguridad IPSec, que utilizarán nuevas claves y SPI. Los valores predeterminados establecidos en los métodos de seguridad predeterminados requieren nuevas asociaciones de seguridad IPSec cada hora (3.600 segundos) o tras 100 megabytes transferidos. Si se han transferido datos de manera activa durante los cinco minutos anteriores, las asociaciones de seguridad IPSec se volverán a negociar automáticamente antes de que caduquen. El extremo que ha transmitido más datos o que ha iniciado el método rápido anterior iniciará el nuevo modo rápido.

Solución de problemas

Solución de problemas en la configuración de directivas

Esta guía pretende abarcar únicamente las directivas IPSec de equipo local que utilizan el transporte IPSec y no el túnel para proteger el tráfico entre un equipo de origen y un equipo de destino. No incluye la utilización de Directivas de grupo en Active Directory para distribuir directivas IPSec. La configuración de directivas IPSec es muy flexible y eficaz, aunque la configuración adecuada requiere la comprensión de los protocolos IKE e IPSec. Existen varios aspectos de la configuración de la seguridad que deberá tener en

cuenta. Consulte la Ayuda en pantalla y busque artículos relacionados con IPSec en Microsoft Knowledge Base. Seguidamente, lea las notas adicionales que aparecen a continuación para que le ayuden a entender las incompatibilidades intrínsecas de la configuración de directivas. Si no puede hacer funcionar la comunicación IPSec, siga los pasos que se detallan más adelante para crear la directiva más sencilla y utilizarla para pruebas.

Sólo un método de autenticación entre dos sistemas

La directiva IPSec está diseñada de manera que sólo pueda utilizarse un método de autenticación entre dos sistemas, sin tener en cuenta el número de métodos configurados. Si tiene varias reglas que se aplican al mismo par de equipos, teniendo en cuenta únicamente las direcciones IP de origen y de destino, debe asegurarse de que dichas reglas permiten que los dos equipos utilicen el mismo método de autenticación. También debe asegurarse de que la credencial utilizada para dicho método de autenticación es válida. Por ejemplo, el complemento IPSec permite configurar una regla que utilice Kerberos para autenticar sólo los datos TCP entre dos direcciones IP de equipo y crear una segunda regla con las mismas direcciones pero que especifique que los datos UDP utilicen certificados para la autenticación. Esta directiva no funcionará correctamente, ya que al coincidir el UDP del protocolo y no sólo las direcciones, el tráfico de datos saliente puede seleccionar una regla más específicamente que la negociación IKE en el equipo de destino cuando se intenta encontrar una regla coincidente en la directiva para que responda en el modo principal, que sólo puede utilizar la dirección IP de origen del paquete IKE. Por lo tanto, esta configuración de directiva utiliza dos métodos de autenticación diferentes entre un mismo par de direcciones IP o equipos. Para evitar este problema, no utilice filtros específicos del protocolo o del puerto para negociar la seguridad del tráfico. En su lugar, utilice filtros específicos del puerto y del protocolo principalmente para acciones de permiso y de bloqueo.

No se permite la protección IPSec unidireccional del tráfico

La directiva IPSec no está diseñada para permitir la protección unidireccional del tráfico mediante IPSec. Si crea una regla para proteger el tráfico entre las direcciones IP de los equipos A y B, debe especificar tanto el tráfico entre A y B como el tráfico entre B y A en la misma lista de filtros. Esto puede llevarse a cabo creado dos filtros en la misma lista de filtros. Alternativamente, puede dirigirse al cuadro de diálogo Propiedades de la especificación de filtro del complemento IPSec y activar la casilla de verificación Reflejado. Esta opción está seleccionada de manera predeterminada, ya que la protección debe negociarse en ambas direcciones incluso si el tráfico de datos sólo fluye en una dirección la mayor parte del tiempo.

Puede crear filtros unidireccionales para bloquear o permitir el tráfico, pero no para protegerlo. Para proteger el tráfico, debe especificar manualmente el reflejo de filtro, o bien utilizar la casilla de verificación de reflejo para que el sistema lo genere automáticamente por usted.

Los certificados de equipo deben tener una clave privada

Los certificados obtenidos de manera incorrecta pueden provocar una situación en la que el certificado existe y se utiliza para la autenticación IKE, pero no puede funcionar

porque la clave privada correspondiente a la clave pública del certificado no está presente en el equipo local.

Para comprobar que el certificado tiene una clave privada

En el menú Inicio, haga clic en Ejecutar y escriba mmc en el cuadro de texto. Haga clic en OK.

En el menú Consola, haga clic en Agregar o quitar complemento y, a continuación, haga clic en Agregar.

En la lista Complemento, haga doble clic en Certificados. Haga clic en Cerrar y, a continuación, haga clic en Aceptar.

Expanda Certificados-Usuario (equipo local) y, a continuación, expanda Personal.

Haga clic en la carpeta Certificados.

En el panel de la derecha, haga doble clic en el certificado que desea comprobar.

En la ficha General deberá ver el texto Tiene una clave privada correspondiente a este certificado. Si no aparece este mensaje, el sistema no utilizará este certificado correctamente en IPSec.

Según cómo se haya solicitado el certificado y colocado en el almacén local de certificados del equipo, este valor de clave privada puede no existir o no estar disponible para su uso durante la negociación IKE. Si el certificado de la carpeta personal no tiene una clave privada correspondiente, se ha producido un error en la suscripción de certificado. Si se obtuvo un certificado del Servidor de certificados de Microsoft con la opción establecida como Protección segura de claves privadas, el usuario debe escribir un número de identificación personal (PIN) para tener acceso a la clave privada cada vez que se utilice dicha clave para firmar datos en la negociación IKE. Dado que la negociación IKE se lleva cabo en segundo plano mediante un servicio del sistema, no existe ninguna ventana con la que solicitar información al usuario. Por lo tanto, los certificados obtenidos con esta opción no son válidos para la autenticación IKE.

Crear y probar la directiva de extremo a extremo más sencilla

La mayoría de los problemas, sobre todo los problemas de interoperabilidad, pueden resolverse mediante la creación de la directiva más simple, en lugar de utilizar las directivas predeterminadas. Cuando cree un nueva directiva, no habilite un túnel IPSec ni la regla de respuesta predeterminada. Modifique la directiva en la ficha General; modifique el intercambio de claves para que tenga una sola opción que aceptará el destinatario. Por ejemplo, utilice las opciones necesarias DES, SHA1, con el grupo 1 (bajo) de Diffie Hellman, de RFC 2049. Cree una lista de filtros con un filtro reflejado que especifique el origen Mi dirección IP y el destino de la dirección IP con la que intenta comunicar de manera segura. Se recomienda llevar a cabo las pruebas creando un filtro que contenga sólo direcciones IP. Cree su propia acción de filtrado para negociar la seguridad mediante un único método de seguridad. Si desea ver el tráfico en paquetes con formato IPSec mediante un husmeador, utilice Seguridad media (formato AH). De lo contrario, seleccione personalizada y cree un único método de seguridad. Por ejemplo, utilice el conjunto necesario de parámetros RFC 2049, como el formato ESP mediante

DES con SHA1, sin especificar vigencias y sin Confidencialidad directa perfecta (PFS). Asegúrese de desactivar ambas casillas de verificación en el método de seguridad para que requiera IPSec para el destino, no se comunique con equipos que no admitan IPSec, y no acepte comunicaciones no seguras. Utilice un método de autenticación de claves previamente compartidas para la regla y asegúrese de que la cadena de caracteres no contiene espacios en blanco. El destino debe utilizar exactamente la misma clave previamente compartida.

Nota: El destino debe estar configurado de la misma manera, sólo debe cambiarse la dirección IP de origen por la de destino y viceversa.

Debe asignar esta directiva a un equipo e intentar hacer ping al destino desde ese equipo. El ping debe mostrar Negociando la seguridad. Esto indica que se está haciendo coincidir el filtro de la directiva y que IKE debe intentar negociar la seguridad con el destino del paquete ping. Si continúa recibiendo Negociando la seguridad IP tras hacer ping varias veces al destino, probablemente no existe un problema de directiva, sino de IKE. Consulte la sección Solución de problemas en la negociación IKE, que aparece a continuación.

Solución de problemas en la negociación IKE

El servicio IKE se ejecuta como parte del servicio Agente de directiva IPSec. Asegúrese de que el servicio está en ejecución.

Asegúrese de que se ha habilitado la auditoría del éxito o del error del atributo de auditoría Auditar sucesos de inicio de sesión. El servicio IKE realizará entradas de auditoría en el registro de seguridad y proporcionará una explicación acerca del motivo del error en la negociación.

Borrar el estado de IKE: Reiniciar el servicio Agente de directiva IPSec

Para borrar completamente el estado de la negociación IKE, es necesario iniciar y detener el servicio de agente de directiva mediante los siguientes comandos desde la línea de comandos, una vez iniciada una sesión como administrador local:

net stop policyagent

net start policyagent

Vuelva a intentar los pasos para proteger el tráfico.

Precaución Cuando detenga el servicio Agente de directiva IPSec, se desactivarán las protecciones de filtro IPSec. Los túneles VPN activos ya no estarán protegidos por IPSec. si piensa utilizar también los servicios de Enrutamiento o Acceso remoto, o si ha habilitado las conexiones de VPN entrantes, debe detener y reiniciar el servicio de acceso remoto, net start remoteaccess, una vez reiniciado el servicio Agente de directiva IPSec.

Utilizar el registro de seguridad para ver los errores de IKE

Cuando falla una negociación IKE, el registro de seguridad anota los motivos de error. Utilice estos mensajes para detectar si una negociación ha fallado y por qué. Es necesario que habilite la auditoría mediante el procedimiento descrito al principio de esta guía.

Utilizando un husmeador

Si ninguna de las indicaciones anteriores ha servido de ayuda y si todavía no ha leído la sección Comprender la negociación IKE, hágalo ahora.

Para investigar de manera más detallada utilice un husmeador, como Microsoft Network Monitor, para capturar los paquetes intercambiados. Recuerde que la mayoría del contenido de los paquetes utilizados en la negociación IKE está cifrado y no se puede interpretar mediante un husmeador. Aun así, merece la pena husmear todo el tráfico entrante y saliente del equipo para comprobar que es tal como se esperaba. Windows 2000 Server incluye una versión limitada de Microsoft Network Monitor. El programa no se instala de manera predeterminada, así que debe dirigirse al Panel de control, Agregar o quitar componentes de Windows, Herramientas de administración y supervisión, seleccionar Herramientas de monitor de red y seguir los pasos que se requieran.

Utilizar el seguimiento de depuración IKE (usuarios expertos)

El registro de seguridad es el mejor lugar para determinar la causa del error en una negociación IKE. Sin embargo, los expertos en la negociación del protocolo IKE pueden habilitar la opción de seguimiento de depuración mediante una clave del registro. El registro está deshabilitado de forma predeterminada. Para habilitar el registro de depuración, debe detener e iniciar el servicio Agente de directiva IPSec.

Para habilitar el registro de depuración de IKE

En el escritorio de Windows, haga clic en Inicio, haga clic en Ejecutar y escriba regedt32 en el cuadro de texto. Haga clic en OK. Esto iniciará el Editor del registro.

Diríjase a HKEY_LOCAL_MACHINE en la máquina local.

Diríjase a la siguiente ubicación: System\CurrentControlSet\Services\PolicyAgent.

Haga doble clic en PolicyAgent.

Si la clave Oakley no existe, haga clic en Agregar clave en el menú Edición.

Escriba el Nombre de clave (distingue entre mayúsculas y minúsculas): Oakley.

Deje Clase en blanco y haga clic en Aceptar.

Seleccione la nueva clave, Oakley.

En el menú Edición, haga clic en Agregar valor.

Escriba el Nombe de Valor (distingue entre mayúsculas y minúsculas): EnableLogging

Seleccione el Tipo de dato: REG_DWORD y haga clic en Aceptar.

Escriba el valor 1

Haga clic en Hexa como la Base. Haga clic en Aceptar

Salga del Editor del Registro.

En la ventana de línea de comandos de Windows 2000, escriba net stop policyagent y, a continuación, escriba net start policyagent para reiniciar los servicios relacionados con IPSec.

El archivo se escribirá de manera predeterminada en directorio de windows\debug\oakley.log y el archivo oakley.log.sav es la versión anterior del archivo de registro una vez reiniciado el servicio de agente de directiva.

El archivo de registro está limitado a 50.000 entradas, lo que limita normalmente el tamaño del archivo a menos de seis megabytes.

5. CONOCER LOS DIFERENTES PROTOCOLOS Y SU FUNCIONAMIENTO TANTO DE ESTABLECIMIENTO DE TÚNELES COMO DE REENVÍO

5.1 PROTOCOLOS

IPSec, (Protocolo de seguridad en Internet) trata de remediar algunas falencias de IP, tales como protección de los datos transferidos y garantía de que el emisor del paquete sea el que dice el paquete IP. Si bien estos servicios son distintos, IPSec da soporte a ambos de una manera uniforme.

IPSec provee confidencialidad, integridad, autenticidad y protección a repeticiones mediante dos protocolos, que son Authentication Protocol (AH) y Encapsulated Security Payload (ESP).

Por confidencialidad se entiende que los datos transferidos sean sólo entendidos por los participantes de la sesión.

Por integridad se entiende que los datos no sean modificados en el trayecto de la comunicación.

Por autenticidad se entiende por la validación de remitente de los datos.

Por protección a repeticiones se entiende que una sesión no pueda ser grabada y repetida salvo que se tenga autorización para hacerlo.

AH provee autenticación, integridad y protección a repeticiones pero no así confidencialidad. La diferencia más importante con ESP es que AH protege partes del header IP, como las direcciones de origen y destino.

ESP provee autenticación, integridad, protección a repeticiones y confidencialidad de los datos, protegiendo el paquete entero que sigue al header.

AH sigue al header IP y contiene diseminaciones criptográficas tanto en los datos como en la información de identificación. Las diseminaciones pueden también cubrir las partes invariantes del header IP.

El header de ESP permite rescribir la carga en una forma encriptada. Como no considera los campos del header IP, no garantiza nada sobre el mismo, sólo la carga.

Una división de la funcionalidad de IPSec es aplicada dependiendo de dónde se realiza la encapsulación de los datos, si es la fuente original o un gateway:

El modo de transporte es utilizado por el host que genera los paquetes. En este modo, los headers de seguridad son antepuestos a los de la capa de transporte, antes de que el header IP sea incorporado al paquete. En otras palabras, AH cubre el header TCP y algunos campos IP, mientras que ESP cubre la encriptación del header TCP y los datos, pero no incluye ningún campo del header IP.

El modo de túnel es usado cuando el header IP entre extremos está ya incluido en el paquete, y uno de los extremos de la conexión segura es un gateway. En este modo, tanto AH como ESP cubren el paquete entero, incluyendo el header IP entre los extremos, agregando al paquete un header IP que cubre solamente el salto al otro extremo de la conexión segura, que, por supuesto, puede estar a varios saltos del gateway.

Los enlaces seguros de IPSec son definidos en función de Security Associations (SA). Cada SA está definido para un flujo unidireccional de datos y generalmente de un punto único a otro, cubriendo tráfico distinguible por un selector único. Todo el tráfico que fluye a través de un SA es tratado de la misma manera. Partes del tráfico puede estar sujeto a varios SA, cada uno de los cuales aplica cierta transformación. Grupos de SA son denominados SA Bundles. Paquetes entrantes pueden ser asignados a un SA específico por los tres campos definitorios: la dirección IP de destino, el índice del parámetro de seguridad y el protocolo de seguridad. El SPI puede ser considerado una cookie que es repartido por el receptor del SA cuando los parámetros de la conexión son negociados. El protocolo de seguridad debe ser AH o ESP. Como la dirección IP de destino es parte de la tripleta antes mencionada, se garantiza que este valor sea único.

Un ejemplo de paquete AH en modo túnel es:

Gráfica 31. Paquete AH en modo túnel.

Un ejemplo de paquete AH en modo transporte es:

Gráfica. 32. Paquete AH en modo transporte

Como ESP no puede autentificar el header IP más exterior, es muy útil combinar un header AH y ESP para obtener lo siguiente:

Gráfica 33. Combinación de encabezado AH y ESP.

Este tipo de paquete se denomina Transport Adjacency.

La versión de entunelamiento sería:

Gráfica 34. Versión de entunelamiento.

Sin embargo, no es mencionado en las RFC que definen estos protocolos. Como en Transport Adjacency, esto autenticaría el paquete completo salvo algunos pocos campos del header IP y también encriptaría la carga. Cuando un header AH y ESP son directamente aplicados como en esta manera, el orden de los header debe ser el indicado. Es posible, en el modo de túnel, hacer una encapsulación arbitrariamente recursiva para que el orden no sea el especificado.

En el Intercambio de claves de Internet IKE, el principal componente de los procesos de seguridad seguirán siendo las claves. Ya sea que estén disponibles gratuitamente en un servidor público o en el disco duro de algún servidor inseguro, las claves pueden comprometer a todo el sistema. La generación, la distribución y el manejo de estas claves caen dentro de lo que se conoce como administración de claves. Uno de los problemas de IPSec es la carencia de un sistema de administración de claves. La administración el intercambio y el mantenimiento de estas claves criptográficas no existen en IPSec, sin embargo el protocolo de intercambio de claves de internet IKE es una norma de un protocolo de administración de claves usado por IPSec y que aun se encuentra en desarrollo. IKE es un protocolo híbrido que implementa los intercambios de claves Oakley dentro de una asociación de seguridad de internet y el protocolo de administración de claves ISAKMP. El sistema de IKE permite que IPSec ofrezca funciones tales como:

Especificar un tiempo de vida útil para la asociación de seguridad IPSec.

Permitir que se utilicen las claves cifradas durante las sesiones

Permitir que IPSec proporciones servicios contra repeticiones

Permitir el soporte de la autoridad emisora de certificados.

ISAKMP

La asociación de seguridad de internet y el protocolo de administración de claves ISAKMP que especifica el RFC-2408 define el proceso y los formatos de los paquetes para configurar, negociar, modificar y eliminar las asociaciones de seguridad. La asociación de seguridad contiene información que se requiere en los servicios de seguridad de la red, como la autenticación y el encapsulamiento de la carga. ISAKMP define la carga para intercambiar la generación de claves y la autenticación de los datos. Sin embargo, no está ligado a ningún algoritmo criptográfico, técnica de generación de claves o mecanismo de seguridad. Mientras que AH y ESP salvaguardan los datos, ISAKMP podría estar abierto a un ataque de intermediario; por lo tanto las firmas digitales son obligatorias. Además, aunque ISAKMP, IKE especifica que se debe emplear el intercambio de claves Oakley.

ISAKMP utiliza distintas funciones de seguridad para su protección. Emplea un cookie o una señal contra obstrucciones (ACT), para protegerse contra ataques de denegación del servicio. En ISAKMP se elimina la intrusión en sesiones al vincular la autenticación, el intercambio de claves y los intercambios de asociación de seguridad.

De acuerdo con el RFC, está vinculación impide que se permita la autenticación de un agresor para que complete, y después salte y haga pasar por distintas entidades durante el intercambio de claves y el intercambio de asociación de seguridad. Los ataques de intermediarios se eliminan con los requisitos de autenticación de ISAKMP que evita que se establezca una asociación de seguridad con cualquiera que no sea la parte involucrada.

Protocolo de envío de nivel 2 (L2F)

En 1996 Cysco System desarrolló un protocolo que iba a emplearse en combinación con el protocolo PPTP de Microsoft. Con el crecimiento de los servicios de marcación y la disponibilidad de muchos protocolos diferentes se necesitaba crear un escenario de marcación virtual donde cualquiera de los protocolos que no fuera IP pudiera disfrutar de los beneficios de internet. Cysco definió el concepto de establecimiento de túneles, como el encapsulamiento de paquetes no IP; es decir los usuarios hacen una conexión PPP o SLIP a un proveedor PSI de marcación y con el uso de L2F, se conectan a las máquinas de sus compañías. Estos túneles se encuentran en los extremos de la conexión a internet, en los enrutadores con software para el establecimiento de túneles, el envió de nivel 2 ofrece muchos beneficios como:

Independencia de protocolo (IPX, SNA)

Autenticación (PPP, CHAP, TACACS)

Administración de direcciones (asignadas por destino)

Túneles dinámicos y seguros

Apertura de cuentas

Independencia de medios, por ejemplo sobre LF (ATM, X.25, Tramas)

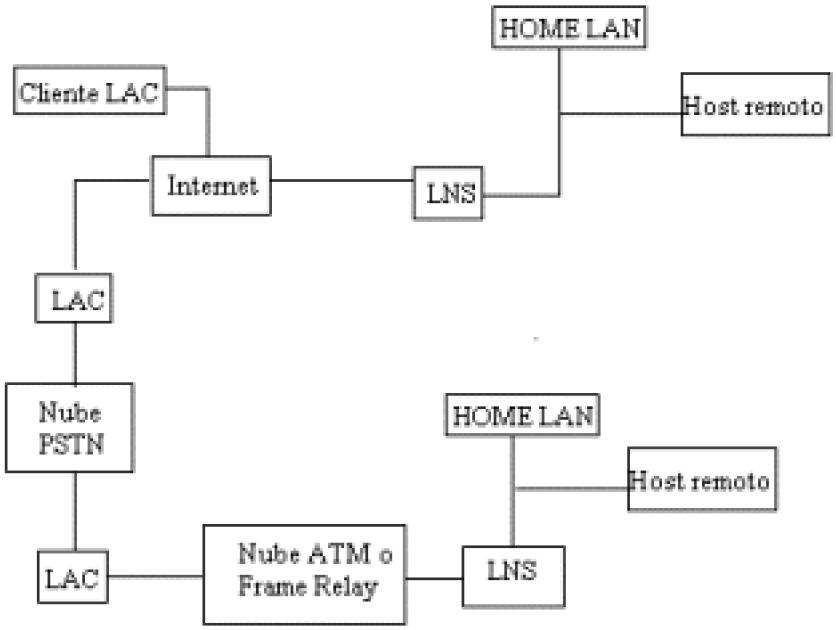
En la configuración básica el usuario realiza una conexión PPP o una conexión similar al PSI local. Con la solicitud del usuario, el NAS, mediante el software LF, inicia un túnel al destino del usuario. El destino pide la contraseña al usuario y un a vez autorizado,

le asigna una dirección IP al usuario, igual que un dispositivo de acceso por marcación típica. El punto terminal (enrutador corporativo que ejecuta L2F) quita el encabezado del túnel, registra el tráfico y permite que haya comunicación.

L2F es una de los protocolos de transporte utilizados en las redes privadas de actualidad.

Layer-2 Tunneling Protocol (L2TP) facilita el entunelamiento de paquetes PPP a través de una red de manera tal que sea lo más transparente posible a los usuarios de ambos extremos del túnel y para las aplicaciones que éstos corran.

El escenario típico L2TP, cuyo objetivo es la creación de entunelar tramas PPP entre el sistema remoto o cliente LAC y un LNS ubicado en una LAN local, es el que se muestra en la siguiente figura:



Gráfica 35. Mapa de seguimiento en la LAN

Un L2TP Access Concentrator (LAC) es un nodo que actúa como un extremo de un túnel L2TP y es el par de un LNS. Un LAC se sitúa entre un LNS y un sistema remoto y manda paquetes entre ambos. Los paquetes entre el LAC y el LNS son enviados a través del túnel L2TP y los paquetes entre el LAC y el sistema remoto es local o es una conexión PPP.

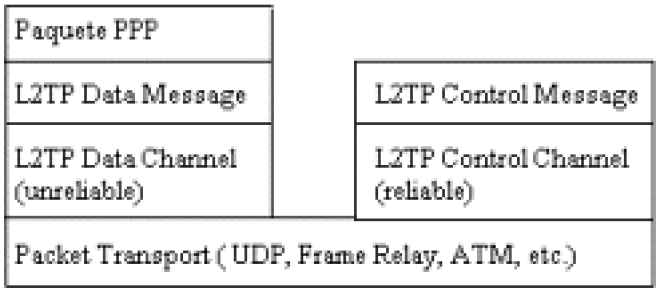
Un L2TP Network Server (LNS) actúa como el otro extremo de la conexión L2TP y es el otro par del LAC. El LNS es la terminación lógica de una sesión PPP que está siendo puesta en un túnel desde el sistema remoto por el LAC.

Un cliente LAC, una máquina que corre nativamente L2TP, puede participar también en el túnel, sin usar un LAC separado. En este caso, estará conectado directamente a Internet.

El direccionamiento, la autenticación, la autorización y el servicio de cuentas son proveídos por el Home LAN's Management Domain.

L2TP utiliza dos tipos de mensajes: de control y de datos. Los mensajes de control son usados para el establecimiento, el mantenimiento y el borrado de los túneles y las llamadas. Utilizan un canal de control confiable dentro de L2TP para garantizar el envío. Los mensajes de datos encapsulan los marcos PPP y son enviados a través del túnel.

La siguiente figura muestra la relación entre las tramas PPP y los mensajes de control a través de los canales de control y datos de L2TP.



Gráfica 36. Relación entre los marcos PPP y los mensajes de control.

Las tramas PPP son enviados a través de un canal de datos no confiable, encapsulado primero por un encabezado L2TP y luego por un transporte de paquetes como UDP, Frame Relay o ATM. Los mensajes de control son enviados a través de un canal de control L2TP confiable que transmite los paquetes sobre el mismo transporte de paquete.

Se requiere que haya números de secuencia en los paquetes de control, que son usados para proveer el envío confiable en el canal de control. Los mensajes de datos pueden usar los números de secuencia para reordenar paquetes y detectar paquetes perdidos.

Al correr sobre UDP/IP, L2TP utiliza el puerto 1701. El paquete entero de L2TP, incluyendo la parte de datos y el encabezado, viaja en un datagrama UDP. El que inicia un túnel L2TP toma un puerto UDP de origen que esté disponible, pudiendo ser o no el 1701 y envía a la dirección de destino sobre el puerto 1701. Este extremo toma un puerto libre, que puede ser o no el 1701, y envía la respuesta a la dirección de origen, sobre el mismo puerto iniciador. Luego de establecida la conexión, los puertos quedan estáticos por el resto de la vida del túnel.

En la autenticación de L2TP, tanto el LAC como el LNS comparten un secreto único. Cada extremo usa este mismo secreto al actuar tanto como autenticado como autenticador.

Sobre la seguridad del paquete L2TP, se requiere que el protocolo de transporte de L2TP tenga la posibilidad de brindar servicios de encriptación, autenticación e integridad para el paquete L2TP en su totalidad. Como tal, L2TP sólo se preocupa por la confidencialidad, autenticidad e integridad de los paquetes L2TP entre los puntos extremos del túnel, no entre los extremos físicos de la conexión.

Protocolo para establecimiento de túneles punto a punto (PPTP)

Point-to-Point Tunneling Protocol fue desarrollado por ingenieros de Ascend Communications, U.S. Robotics, 3Com Corporation, Microsoft, y ECI Telematics para

proveer entre usuarios de acceso remoto y servidores de red una red privada virtual.

Como protocolo de túnel, PPTP encapsula datagramas de cualquier protocolo de red en datagramas IP, que luego son tratados como cualquier otro paquete IP. La gran ventaja de este tipo de encapsulamiento es que cualquier protocolo puede ser ruteado a través de una red IP, como Internet.

PPTP fue diseñado para permitir a los usuarios conectarse a un servidor RAS desde cualquier punto en Internet para tener la misma autenticación, encriptación y los mismos accesos de LAN como si discaran directamente al servidor. En vez de discar a un modem conectado al servidor RAS, los usuarios se conectan a su proveedor y luego "llaman" al servidor RAS a través de Internet utilizando PPTP.

Existen dos escenarios comunes para este tipo de VPN:

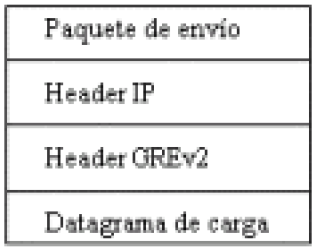
el usuario remoto se conecta a un ISP que provee el servicio de PPTP hacia el servidor RAS.

el usuario remoto se conecta a un ISP que no provee el servicio de PPTP hacia el servidor RAS y, por lo tanto, debe iniciar la conexión PPTP desde su propia máquina cliente.

Para el primero de los escenarios, el usuario remoto estable una conexión PPP con el ISP, que luego establece la conexión PPTP con el servidor RAS. Para el segundo escenario, el usuario remoto se conecta al ISP mediante PPP y luego "llama" al servidor RAS mediante PPTP. Luego de establecida la conexión PPTP, para cualquiera de los dos casos, el usuario remoto tendrá acceso a la red corporativa como si estuviera conectado directamente a la misma.

La técnica de encapsulamiento de PPTP se basa en el protocolo Generic Routing Encapsulation (GRE), que puede ser usado para realizar túneles para protocolos a través de Internet. La versión PPTP, denominada GREv2, añade extensiones para temas específicos como Call Id y velocidad de conexión.

El paquete PPTP está compuesto por un header de envío, un header Ip, un header GREv2 y el paquete de carga. El header de envío es el protocolo enmarcador para cualquiera de los medios a través de los cuales el paquete viaja, ya sea Ethernet, frame relay, PPP. El header IP contiene información relativa al paquete IP, como ser, direcciones de origen y destino, longitud del datagrama enviado, etc. El header GREv2 contiene información sobre el tipo de paquete encapsulado y datos específicos de PPTP concernientes a la conexión entre el cliente y servidor. Por último, el paquete de carga es el paquete encapsulado, que, en el caso de PPP, el datagrama es el original de la sesión PPP que viaja del cliente al servidor y que puede ser un paquete IP, IPX, NetBEUI, entre otros. La siguiente figura ilustra las capas del encapsulamiento PPTP.



Gráfica 37. Capas del encapsulamiento.

Para la autenticación, PPTP tiene tres opciones de uso: CHAP, MS-CHAP y aceptar cualquier tipo, inclusive texto plano. Si se utiliza CHAP, standard en el que se intercambia un "secreto" y se comprueba ambos extremos de la conexión coincidan en el mismo, se utiliza la contraseña de Windows NT, en el caso de usar este sistema operativo, como secreto. MS-CHAP es un standard propietario de Microsoft y resulta ser una ampliación de CHAP. Para la tercer opción, el servidor RAS aceptará CHAP, MS-CHAP o PAP (Password Autenthication Protocol), que no encripta las contraseñas.

Para la encriptación, PPTP utiliza el sistema RC4 de RSA, con una clave de sesión de 40 bits.

5.2 TOPOLOGÍAS DE TRABAJO SOBRE VPNS.

Para la configuración de una VPN en su mayoría los dispositivos son internos, lo que significa que pueden dejar que pasen los paquetes cifrados a la red sin que sean modificados por un enrutador o por un cortafuego (siempre que el permiso este garantizado). Las VPN también pueden situarse en casos donde incorporan las funciones de un cortafuego y manejan los procesos de cifrado y descifrado.

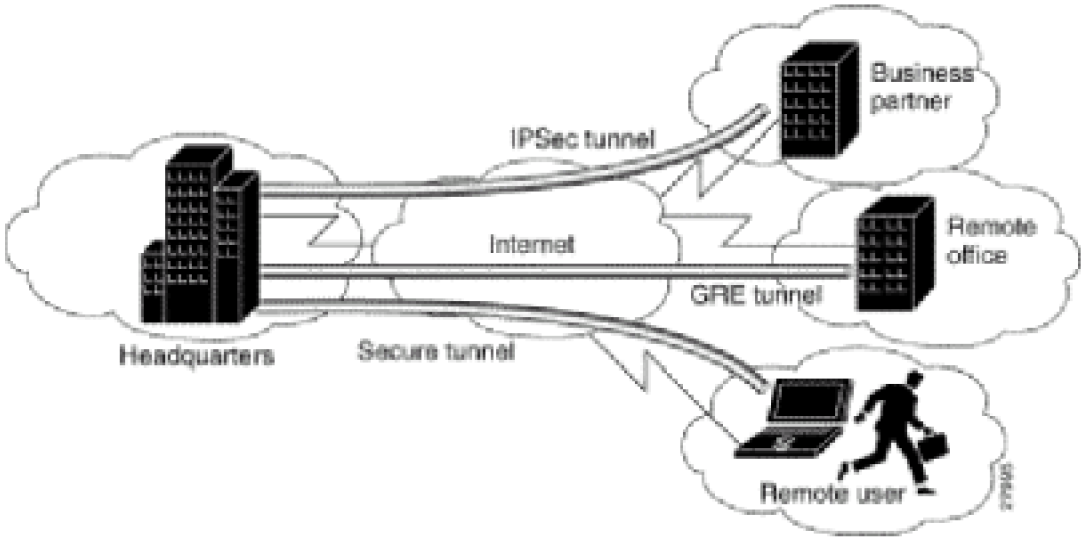
Entre las topologías mas comunes se encuentran, VPN de cortafuego a equipo portátil, VPN de LAN a LAN, topologías anidadas y topologías de túneles.

Antes de definir que topología implementar primero se debe observar la topología de la red y la conexión a internet. Después examinar las oficinas remotas que tendrán su propia conexión a internet y los puntos de creación de túneles.

Topología de cortafuego / VPN a cliente

Esta topología será el punto de partida por ser una de las más comunes y que prácticamente todas las organizaciones que implementan una VPN utilizaran este tipo de configuración. Esto no implica que se trate de la mejor topología, sin embargo, es la mas común y posiblemente la mas fácil de configurar para los que no tienen un cortafuego colocado y solo desean la funcionalidad de la VPN.

En la figura se observa que un usuario en su equipo portátil remoto necesita el acceso a un servidor que se encuentra dentro de la red de la compañía, detrás de un cortafuego / VPN. El usuario desea conectarse al servidor de la compañía y obtener un reporte confidencial.



Gráfica 38. Esquema de conexión.

En la grafica hay dos componentes que deben habilitarse para establecer la comunicación.

El dispositivo de cortafuego/ VPN debe ejecutarse algún tipo de código VPN. Existen muchas formas de realizar este proceso, algunos cortafuegos tienen incluido en su código la capacidad de crear una VPN, así que las reglas deberían agregarse al cortafuego. Con algunos fabricantes será necesario agregar mas software si utiliza un cortafuego antiguo que no incluya el cifrado.

El equipo portátil tiene una pila de VPN instalada. Se trata de una pila de VPN puesto que una aplicación de VPN implicaría que el código corriera en el nivel 7 (aplicación) del modelo OSI. La pila de VPN en realidad se encuentra entre los niveles 2 (enlace de datos) y 3 (red)

Los siguientes pasos describen el proceso de comunicación entre el equipo portátil y el servidor una vez que se han completado las configuraciones.

El usuario con equipo portátil marca a su PSI local y establece una conexión PPP.

El equipo portátil solicita las claves del dispositivo del cortafuego/VPN. Este puede ser un paso manual realizado por el usuario o un paso automático configurado por el software.

El cortafuego/VPN responde con la clave apropiada.

El software de VPN instalado en el equipo portátil espera a que el usuario intente tener acceso al servidor (conocido como la dirección IP de destino. Si el usuario visita cualquier sitio distinto al de la red corporativa no pasa nada. Ahora el usuario quiere hacer una conexión con el servidor de la empresa. El software que ejecuta en el equipo portátil ve la solicitud (de nuevo conocida como dirección IP), cifra el paquete y lo envía a la dirección IP pública de la combinación cortafuego/VPN.

El dispositivo cortafuego/VPN le quita la dirección IP, descifra el paquete y lo envía al

servidor dentro de la LAN local.

El servidor interno responde la solicitud y envía el documento de regreso.

El cortafuego/VPN examina el tráfico y por su tabla sabe que es una configuración de túnel de VPN. Así que toma el paquete lo cifra y lo envía al equipo portátil.

La pila de VPN en el equipo portátil ve el flujo de datos, sabe que viene del dispositivo cortafuego/VPN , descifra el paquete y lo maneja en aplicaciones de niveles superiores.

Topología de VPN / LAN a LAN

Este tipo de topologías es la segunda mas utilizada. Por lo general se ha utilizado la topología de cortafuegos /VPN a cliente y ahora quieren extenderla a distintas oficinas remotas. Esta topología también se utiliza entre oficinas y distintos clientes/fabricantes, creando un túnel VPN entre los dos sitios.

Dos oficinas que cada una tiene su cortafuego propio, una es una máquina basada en NT y la otra es una máquina basada en UNIX. Ambas ejecutan software de VPN de distintos fabricantes y el algoritmo de cifrado utilizado en los productos de VPN de los fabricantes es DES.

El ejemplo presenta a un usuario de la oficina remota que necesita conectarse al servidor de la otra oficina y hacer una transferencia FTP para transferir un archivo.

Los componentes que deben habilitarse son los siguientes:

El administrador de cada sitio con el software de VPN y con el manejo de cifrado DES crea una clave única.

Si se trata de un producto cortafuegos/VPN, el administrador de cada sitio establece una regla, por ejemplo, que todo el tráfico destinado a la otra terminal debe cifrarse.

El usuario final debe utilizar una aplicación FTP en su escritorio para poder conectarse al servidor.

El paquete abandona el escritorio en texto sencillo y llega al dispositivo de cortafuego/VPN.

El paquete es cifrado y se envía a la dirección IP pública del dispositivo de cortafuego/VPN

El cortafuego/VPN acepta y descifra el paquete y lo reenvía a su destino final.

El servidor recibe el paquete y responde

Envía un paquete en texto sencillo a su dispositivo de cortafuego/VPN local.

Después, el cortafuego/VPN lo cifra y lo envía al otro cortafuego/VPN.

El cortafuego/VPN lo descifra y finalmente lo envía de regreso al usuario final.

Topología de VPN / cortafuego a Intranet/Extranet

En la topología VPN estos servicios de intranets y extranets no han cambiado, pero ahora tienen un nivel adicional de cifrado. Normalmente las intranets se utilizaban internamente por los empleados, y las extranets externamente por los clientes. La

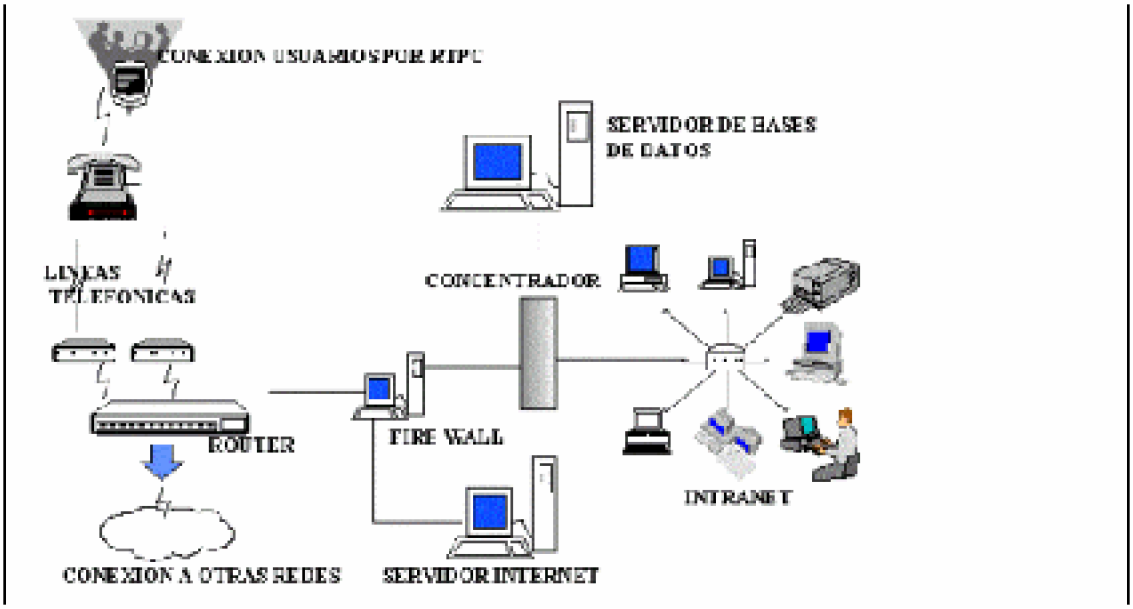
principal diferencia radicaba en la dirección en la que se tenía acceso a ellas. Ahora con la tecnología VPN, se puede tener acceso internamente o externamente a cualquier servicio. Esto tiene dos condiciones. Primero se cuenta con flexibilidad para que una máquina se encargue de ambos y por lo tanto se reduce la redundancia. La segunda condición es la seguridad, ahora existe una forma para que los usuarios tengan acceso a estos servidores.

En el futuro, comenzará a desaparecer la diferencia entre intranet y extranet.

Los clientes y los proveedores tienen permiso para conectarse al servidor de la extranet. El servidor web es para tráfico web normal y esta disponible para todos. La intranet se ubica detrás del dispositivo VPN y solo los usuarios internos que llegan de internet la usan.

Ahora al colocar la extranet en la misma zona que el servidor web. El servidor web tiene una seguridad mínima; el servidor de la extranet por lo general tiene más seguridad. Este es un riesgo de seguridad. Así que se necesita restringir el acceso a la extranet.

Ubicación apropiada de una extranet.



Gráfica 39. Ubicación apropiada de una extranet.

El servidor web se mantiene en una pared poco confiable, permitiendo que todos tengan acceso a este enlace de red. No importa que el dispositivo del cortafuego o de la VPN permita que los paquetes fluyan al servidor web sin modificación.

La extranet se coloca en su propia red por separado. La seguridad que puede implementar aquí consiste en permitir que solo aquellas direcciones de origen que considere necesarias pasen al dispositivo de cortafuego/VPN.

Su extranet se estableció entre ciertas compañías y fabricantes; así que lo más probable es que lleguen desde sus propias redes internas. Por lo tanto puede restringir el acceso solo a esas redes. Desde luego, alguien puede burlar las direcciones de origen, pero cuando se estableció la comunicación, se creo utilizando una VPN. Desde el

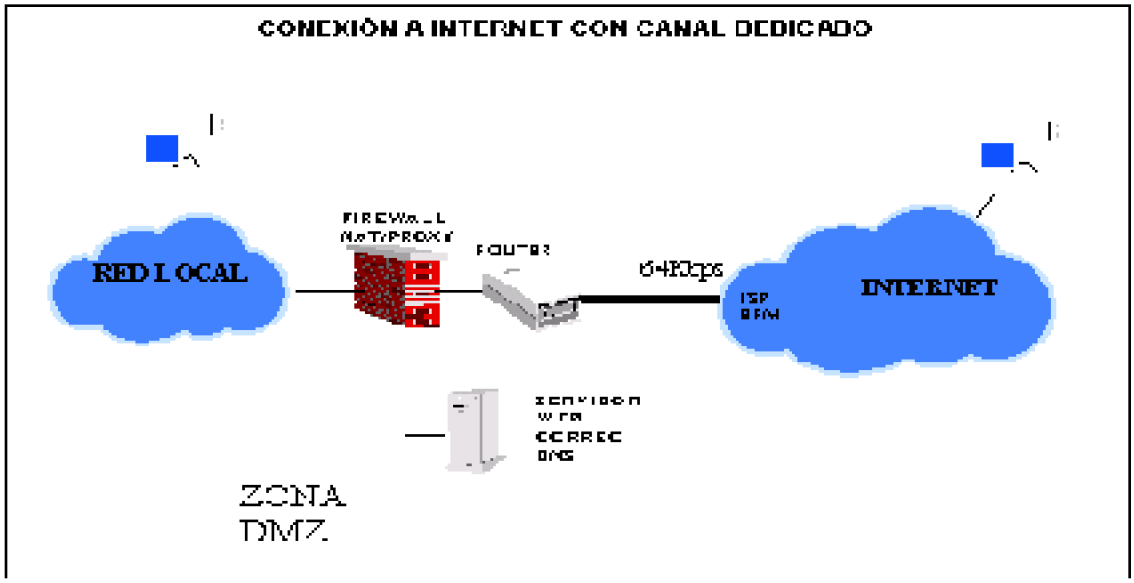
principio se cifraron todos los datos, y solo se esta agregando una restricción adicional.

Para tener en cuenta en seguridad: La única diferencia entre las intranets/Extranet VPN y no VPN es el punto donde se efectúa el proceso de cifrado. Si es en la máquina piense en la seguridad web como un servidor web típico.

Coloque los servidores de red de acuerdo con la función. Si esta permitido el acceso público, colóquelos en una DMZ pública. Si hay clientes y proveedores externos, colóquelos en su propia DMZ; si hay empleados, de nuevo colóquelos en su propia DMZ. Con máquinas bien instaladas puede tener varias zonas DMZ. Algunos fabricantes de cortafuegos/VPN soportan hasta 32 DMZ.

Para implementar una seguridad adicional al enlace DMZ1 del servidor web, solo permita que pase el tráfico http del dispositivo VPN al servidor web, denegando los otros tipos de tráfico.

5.2.1 Basadas en cortafuegos.



Gráfica 40. VPN Basada en cortafuegos canal dedicado.

Esta forma de implementación es probablemente la más común hoy en día, y muchos proveedores ofrecen este tipo de configuración, no significa que sean superiores a otras formas de VPN.

Debido a que muchas organizaciones ya están conectadas a internet, todo lo que se necesitaría es añadir software de cifrado.

Un aspecto importante de seguridad es el sistema operativo subyacente. Saber en que plataforma se está ejecutando el cortafuego, si en un NT, UNIX LINUX o algún otro sistema conociendo los puntos vulnerables de cada uno.

Si el dispositivo de VPN no es 100 % seguro, se necesita asegurar de que el sistema operativo subyacente sea seguro.

Las VPN deberían ubicarse en los niveles más bajos de la pila OSI. Entre mas arriba se encuentren en la pila, se presentaran mayores oportunidades de que ocurran intrusiones en la seguridad de las capas inferiores de las que depende.

También se debe decidir que tipo de norma VPN desea utilizar, por ejemplo PPTP, L2TP o IPSec.

Hasta el momento existen tres tipos de implementaciones de cortafuegos para elegir: inspección de estado, Proxy y filtrado de paquetes. Cuando se añada una tecnología VPN a un cortafuego se refiere a añadir tecnología VPN únicamente a un cortafuego de inspección de estado. De la misma forma que la tecnología VPN en si misma se ejecuta en los niveles mas bajos de la pila de OSI, el cortafuego debe hacerlo o puede caer en problemas de desempeño importantes. Un servidor proxy se ejecuta en la capa 7 la capa de aplicaciones del modelo OSI. Un cortafuego de inspección de estados se ejecuta en los niveles 2 y 3.

5.2.2 VPN basadas en caja negra.

Se trata básicamente de un dispositivo cargado con software de cifrado para crear un túnel de VPN. Algunas cajas negras vienen con software que se ejecuta en un equipo cliente para ayudar en la administración. Se cree que estos dispositivos de cifrado de hardware son más veloces que los tipos de software, ya que crean túneles más rápidos bajo demanda y ejecutan el proceso de cifrado con mayor rapidez. También se requiere otro servidor si se quiere llevar a cabo la autenticación, aunque algunos dispositivos permiten añadir usuarios si se desea y permite configurar el dispositivo para su autenticación contra el servidor que se instaló.

Con la mayoría de las instalaciones de caja negra es posible que se requiera un cortafuego independiente, aunque algunos proveedores están incorporando VPN de caja negra con capacidad de cortafuego.

El dispositivo VPN de caja negra se ubica detrás del cortafuego, aunque también puede situarse a un lado del mismo. El cortafuego proporciona seguridad a la organización, pero no provee seguridad para los datos. Asimismo el dispositivo VPN brindará seguridad a los datos pero no a la organización.

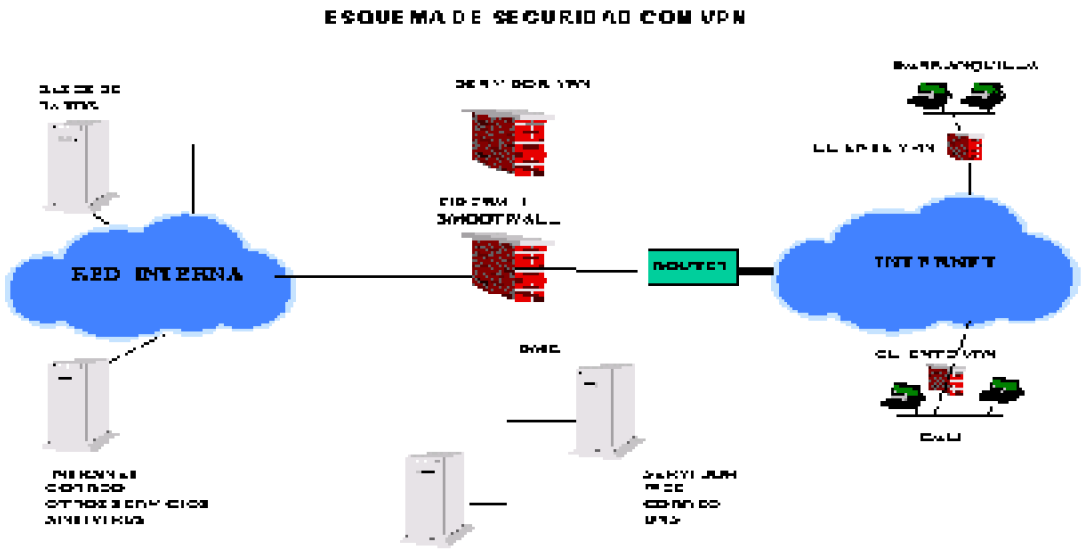
Nótese que el cortafuego estará enfrente del dispositivo VPN y si tiene políticas basadas en reglas se debe asegurar de pasar aquellos paquetes cifrados. El cortafuego como mecanismo de protección si está filtrando en los puertos TCP, tratara de examinar los paquetes y al ver que no puede hacerlo lo soltará, por consiguiente se deben establecer las reglas para pasar esos paquetes.

5.2.3 VPN Basada en Enrutador.

La VPN basadas en enrrutador son adecuados para la organización que ha hecho una gran inversión en sus enrutadores y cuyo personal tiene experiencia en ellos.

Existen dos tipos de VPN basados en enrutadores. En uno de ellos el software se

añade al enrutador para permitir que el proceso de cifrado ocurra. En el segundo método se inserta una tarjeta externa de otro proveedor en el mismo chasis del enrutador, este método está diseñado para endosar el proceso de cifrado del CPU del enrutador a la tarjeta adicional.



Gráfica 41. Esquema de seguridad.

Se debe tener en cuenta que el desempeño puede ser un problema con las VPN basadas en enrutador. Debido a la adición de un proceso de cifrado al proceso de enrutamiento, se puede agregar una carga mas pesada al enrutador, especialmente si este esta manejando una gran cantidad de rutas o implementando un algoritmo de enrutamiento intensivo.

5.2.4 VPN basadas en software.

Una VPN basada en software básicamente es un programa para establecer túneles o cifrado a otro anfitrión. Por lo general se utiliza desde un cliente a un servidor. Por ejemplo una VPN de PPTP, el software cargado en el cliente se conecta al software cargado en el servidor y establece una sesión de VPN.

Al seleccionar este tipo de VPN necesitará tener procesos de administración de claves adecuadas posiblemente una autoridad emisora de certificación en su oficina.

Orto tipo de VPN, de cortafuego a cortafuego solo necesita claves de VPN a VPN y el tráfico en la red interna se descifra, pero el caso de utilizar cliente servidor cada estación posiblemente podría tener su propio par de claves privada/publica.

6. CONCLUSIONES

Cuando una aplicación esté expuesta en la Intranet de la organización o Internet, no se puede garantizar que sea 100% segura. Se puede hablar de ciertos niveles de seguridad, pero no se puede hablar de que sea 100% infalible contra ataques.

Cuando se trata de seguridad y de ataques o de accesos fraudulentos a una aplicación o a un sistema, dicen las estadísticas que el mayor porcentaje de estos, proviene de usuarios que están dentro de la organización y solo un pequeño porcentaje son efectuados desde afuera. Muchos de estos accesos son planeados y malintencionados, pero también se da el caso de accesos que son accidentales.

Según lo anterior, se hace necesario proteger los sistemas, tanto contra accesos fraudulentos internos, como externos, y se debe proteger tanto los sistemas que están en la Intranet como los que están expuestos en Internet.

Las VPN representan una gran solución para las empresas en cuanto a seguridad, confidencialidad e integridad de los datos y prácticamente se ha vuelto un tema importante en las organizaciones, debido a que reduce significativamente el costo de la transferencia de datos de un lugar a otro, el único inconveniente que pudieran tener las VPN es que primero se deben establecer correctamente las políticas de seguridad y de acceso porque si esto no está bien definido pueden existir consecuencias serias.

BIBLIOGRAFÍA

BROWN, Steven. Implementación de redes privadas virtuales RPV. México D.F: McGraw-Gill, 2000. P. 61

DOAK, Wilson y Peter, Creating and Implementing VIRTUAL PRIVATE NETWORKS, CASEY, United States of America : the Coriolis Group, 2000. . P. 158.

GUTIÉRREZ GONZÁLEZ, Maria Nieves. Estudio sobre las VPN, http://www.infor.uva.es/~jvegas/docencia/ar/seminarios/VPN.pdf. p. 195

HARRIS, Nick et al. Linux Handbook, A Guide to IBM Linux Solutions and Resources. Redbooks, 2003. <http://ibm.com/redbooks/sg247000> p. 1,9

MICROSOFT NETWORK. Foro de Windows NT Server: 2004,

http://www.microsoft.com/spain/windows2000/ p. 110.

McDYSAN, David. VPN Aplications Guide: Real Solutions for Enterprice Networks, E. United State of America: 2000. John Wiley & Sons Inc. p. 150.

OPENBSD: http://www.openbsd.org/faq/faq13.html

SCOTT, Charly. Virtual Private Networks. O'Reilly & Associates, 2° edition, 1999. p. 75-78.

SCHNEIER, Bruce, Applied Cryptography. United States of America: Secon Edition, 1996. p. 154.

SEGURIDAD Y VPN, http://www.entarasys.com/la

http://www.cisco.com/warp/public/44/solutions/network/vpn.shtml

SECURITY, http://www.microsoft.com/technet/win2000/

SHAUGHNESSY, Tom, Manual de cisco, España, 2000, McGraw –Hill.

UNIVERSIDAD DE VALENCIA: http://www.uv.es/ciuv/cas/vpn/

VALENCIA, A., Townsley, W., Rubens, A., Pall, G., Zorn, G., Palter, B.: RFC 1999. p. 98.

Lineamientos para la creación de una VPN

Anexo

Enevis Rafael Reyes Moreno

Facultad de Ingeniería

Especialización en Ciencias Electrónicas e Informática

Universidad de Antioquia UDEA

e-mail: (enevisr@gmail.com)

Abstract

Traditional network security focuses on establishing

a perimeter to keep outsiders at bay and on limiting

access through password protection, smart cards, or

biometrics. Emerging Virtual Private Networks (VPNs) focus on secure site interconnection and remote access over the Wide Area Network (WAN).

But a recent research confirms what security experts knew for years: most security breaches occur within the corporate network, over a Local Area Network (LAN).

According to the information mentioned before, it is necessary to protect the system against internal and external fraudulent accesses and it can protect the system in the Intranet , like those that are exposed in Internet.

The virtual private network represents a great solution for the companies and for security, confidentiality and data integrity, and as a matter of fact, it becomes an important

topic into the organizations, the only disadvantage of the VPN is that they should have right policies, if they do not serious consequences can exist.

Palabras claves.

Red privada virtual, servicio de acceso remoto, Protocolo de internet seguro, protocolo de internet, concentradores, criptografía, encriptación.

Introducción

Los estudios de prospectivas en comunicaciones señalan que muchas empresas cuentan con oficinas y sucursales distribuidas en diferentes ubicaciones geográficas; las cuales requieren por lo general poder compartir y acceder libremente a información entre ellas. Por esta razón las VPN jugarán un papel importante en las comunicaciones con accesos a datos y manejo de usuarios remotos que puedan estar en constante movimiento.[1]

Además de la comunicación entre diferentes sucursales, surgió la necesidad de proveer acceso a los usuarios móviles de la empresa. Mediante (RAS) Servicio de acceso remoto, este tipo de usuario puede conectarse a la red de la empresa y usar los recursos disponibles dentro de la misma.[2]

Cuando se desea enlazar las oficinas centrales con alguna sucursal u oficina remota se tienen cuatro opciones:

Modem: este tipo de solución presente la desventaja en el costo de la llamada, ya que el costo de esta llamada sería por minuto conectado, además sería una llamada de larga distancia y no contaría con la calidad y velocidad adecuadas.

Línea Privada: se tendría que conectar un cable ya sea de cobre o fibra óptica de un punto a otro, en esta opción el costo es muy elevado. Sin importar el uso.

VPN: los costos son bajos porque solo se realizan llamadas locales, además de tener la posibilidad que los datos viajen encriptados y seguros, con una buena calidad y velocidad.

Frame Relay o ATM: es la más utilizada, presenta gran desempeño y seguridad, pero su costo de mantenimiento y de servicio es relativamente alto.

En resumen, las VPN tienen un futuro promisorio como solución de comunicación y seguridad de conexiones remotas para las empresas. Dada la creciente importancia de la seguridad en las redes de comunicación y de conexiones más económicas que necesitan las empresas, se pueden mejorar y cubrir con las ventajas y soluciones ofrecidas por las VPN.

Una forma de reducir costos a esta situación es realizar las conexiones remotas a través de internet, ya que estas son supremamente baratas, fáciles de conseguir y funcionan sobre medios básicos como líneas telefónicas, red digital de servicios integrados, Línea servicio de abonado digital entre otras, pero entra a jugar el factor “seguridad”, ya que la información viaja sin ningún tipo de encriptación. Aquí es donde se debe pensar en una solución como las VPN.

Debido a la situación económica, la presión en la disminución de costos operativos para incrementar las ganancias, tener comunicaciones eficientes entre las diferentes

sucursales, poder contar con fuerza de venta que trabaje remotamente o incluso empleados que operen en modo de tele-trabajo, se hace necesario la implementación de VPN. Pero al momento de su diseño y montaje llegan los siguientes cuestionamientos:

Cual es la mejor tecnología de conexión de acuerdo al abanico de posibilidades que ofrecen los proveedores de servicios de internet?

Que protocolos se deben utilizar para realizar los túneles?

Que tipo de encriptación se necesita?

Que sistema operativo se necesita para las conexiones?

De acuerdo con la infraestructura perimetral cómo se configura la seguridad para permitir la conexión VPN?

FUNDAMENTOS DE VPN, COMPONENTES Y FUNCIONAMIENTO.

Una Virtual Private Network (VPN) es un sistema para simular una red privada sobre una red pública, por ejemplo Internet. la idea es que la red pública sea "vista" desde dentro de la red privada como un cable lógico que une las dos o más redes que pertenecen a la red privada.

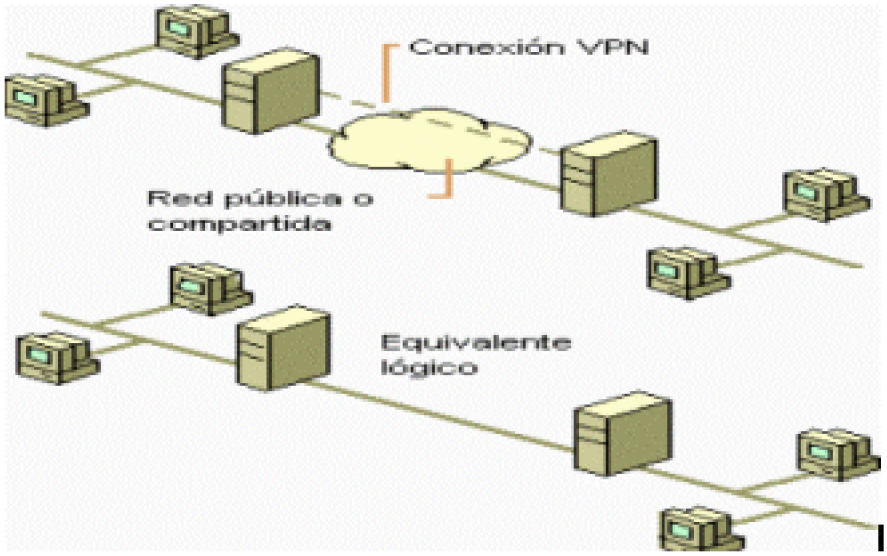


Fig. 1. Esquema de una VPN, Creating and Implementing VIRTUAL PRIVATE NETWORKS. CASEY.

Como se usan redes públicas, en general Internet, es necesario prestar debida atención a las cuestiones de seguridad, que se aborda a través de estos esquemas de encriptación y autentificación y que se describirán luego.[3]

Fig. 2. Componentes de un túnel, . VPN Aplications Guide: Real Solutions for Enterprice Networks, E. United State of America.

fig043.gif

El método de túneles, es una forma de crear una red privada. Permite encapsular paquetes dentro de paquetes para acomodar protocolos incompatibles. Dentro de los protocolos que se usan para la metodología de túneles se encuentran Point-to-Point

Tunneling Protocol (PPTP), Layer-2 Fowarding Protocol (L2FP) y el modo túnel de IPSec[4]

CRIPTOGRAFÍA SIMÉTRICA

La criptografía simétrica se refiere al conjunto de métodos que permiten tener comunicación segura entre las partes siempre y cuando anteriormente se hayan intercambiado la clave correspondiente que llamaremos clave simétrica. La simetría se refiere a que las partes tienen la misma llave tanto para cifrar como para descifrar.

CRIPTOGRAFÍA ASIMÉTRICA

La criptografía asimétrica es por definición aquella que utiliza dos claves diferentes

para cada usuario, una para cifrar que se le llama clave pública y otra para descifrar que es la clave privada. El nacimiento de la criptografía asimétrica se dio al estar buscando un modo más práctico de intercambiar las llaves simétricas.

FUNCIONAMIENTO DE IPSEC

El protocolo de intertnet seguro proporciona seguridad de datagramas IP. Es de extremo a extremo, lo que implica que sólo el remitente y el destinatario necesitan ser conscientes de los detalles acerca de la seguridad. Los dispositivos entre las dos partes no necesitan preocuparse acerca del cifrado, las claves secretas y otros aspectos, para reenviar todos los datos. Esto es significativo para un cliente como un Banco por dos razones. Primero, la conexión por la que se transmiten los datos puede no ser segura. Esto significa que en muchos casos, la infraestructura de la red subyacente no necesita ser modificada. Segundo, la implementación es relativamente sencilla. Sólo los concentradores que necesitan comunicarse tienen que entender IPSec. Los dispositivos intermediarios como los enrutadores no necesitan ser compatibles con IPSec. Para los clientes esto significa que puede implementarse un alto nivel de seguridad sin grandes costos o un cambio significativo para la infraestructura de su red. Es, sin embargo, importante tener en cuenta que los servidores de seguridad y otros dispositivos que bloquean tipos específicos de tráfico necesitan una consideración especial

PROTOCOLOS

IPSec, (Protocolo de seguridad en Internet) trata de remediar algunas falencias de IP, tales como protección de los datos transferidos y garantía de que el emisor del paquete sea el que dice el paquete IP. Si bien estos servicios son distintos, IPSec da soporte a ambos de una manera uniforme.

Protocolo de internet seguro provee confidencialidad, integridad, autenticidad y protección a repeticiones mediante dos protocolos, que son Authentication Protocol (AH) y Encapsulated Security Payload (ESP).

Por confidencialidad se entiende que los datos transferidos sean sólo entendidos por los participantes de la sesión.

Por integridad se entiende que los datos no sean modificados en el trayecto de la comunicación.

Por autenticidad se entiende por la validación de remitente de los datos.

Por protección a repeticiones se entiende que una sesión no pueda ser grabada y repetida salvo que se tenga autorización para hacerlo.

AH provee autenticación, integridad y protección a repeticiones pero no así confidencialidad. La diferencia más importante con ESP es que AH protege partes del encabezado IP, como las direcciones de origen y destino.

ESP provee autenticación, integridad, protección a repeticiones y confidencialidad de los datos, protegiendo el paquete entero que sigue al header.

AH sigue al header IP y contiene diseminaciones criptográficas tanto en los datos como en la información de identificación. Las diseminaciones pueden también cubrir las partes invariantes del header IP.

El header de ESP permite rescribir la carga en una forma encriptada. Como no considera los campos del header IP, no garantiza nada sobre el mismo, sólo la carga.

Una división de la funcionalidad de IPSec es aplicada dependiendo de dónde se realiza la encapsulación de los datos, si es la fuente original o un gateway:

El modo de transporte es utilizado por el host que genera los paquetes. En este modo, los headers de seguridad son antepuestos a los de la capa de transporte, antes de que el header IP sea incorporado al paquete. En otras palabras, AH cubre el header TCP y algunos campos IP, mientras que ESP cubre la encriptación del header TCP y los datos, pero no incluye ningún campo del header IP.

El modo de túnel es usado cuando el header IP entre extremos está ya incluido en el paquete, y uno de los extremos de la conexión segura es un gateway. En este modo, tanto AH como ESP cubren el paquete entero, incluyendo el header IP entre los extremos, agregando al paquete un header IP que cubre solamente el salto al otro extremo de la conexión segura, que, por supuesto, puede estar a varios saltos del gateway.

Los enlaces seguros de IPSec son definidos en función de Security Associations (SA). Cada SA está definido para un flujo unidireccional de datos y generalmente de un punto único a otro, cubriendo tráfico distinguible por un selector único. Todo el tráfico que fluye a través de un SA es tratado de la misma manera.

Sin embargo, no es mencionado en las RFC que definen estos protocolos. Como en Transport Adjacency, esto autenticaría el paquete completo salvo algunos pocos campos del header IP y también encriptaría la carga. Cuando un header AH y ESP son directamente aplicados como en esta manera, el orden de los header debe ser el indicado. Es posible, en el modo de túnel, hacer una encapsulación arbitrariamente recursiva para que el orden no sea el especificado[5]

Glosario

ADSL: línea de abonado digital asimétrica, la cual soporta diferentes tasas de datos para los datos de ida y de vuelta.

AH: autentication Header (Encabezado de Autenticación).

ATM: asynchronous Transfer Mode (Modo de transferencia asíncrono), es una tecnología de red basada en la transferencia de celdas o paquetes de datos de un

tamaño fijo.

CRT: comisión de regulación de telecomunicaciones.

CHAP: callenge Handsake Authentication Protocol Protocolo de autenticación

DES: data Encryption Standard, norma de cifrado de datos.

ESP: encapsulating Security Payload, La Carga útil de Seguridad encapsulando

ENCRIPTACIÓN: conjunto de técnicas que intentan hacer inaccesible la información a personas no autorizadas. Por lo general, la encriptación se basa

en una clave, sin la cual la información no puede ser descifrada.

GRE: modo transporte Cubre el encabezado TCP y algunos campos IP.

HASHING: picado

IMAP: internet Message Access Protocol, Protocolo de Acceso de Mensaje en Internet

IPSEC: modo túnel del L2TP

ISP: proveedor de servicios de Internet

LDAP: lightweight Directory Access Protocol, El Protocolo de Acceso de Directorio ligero

LAYER 2: fowarding Protocol L2FP

LLC: tareas de interacción entre la tarjeta de red y el procesador

NAP: punto de acceso a Red

NAT: network Ardes Translation (traducción de direcciones de red) , es un estandar de internet que activa una red de area local LAN para usar un conjunto de direcciones IP para el trafico interno y un conjunto de direcciones para el trafico externo.

NIC: network Interface Card (tarjeta de interfaz de red)

OVERFLOW: buffer Overflow protection, Desbordamiento.

OSI: estructura lógica de siete niveles para facilitar la comunicación entre diversos sistemas de computación.

PAP: password Autenthication protocol, protocolo de autenticacion de contraseña.

POP3 : post Office Protocol 3

PPTP: point to point protocol tunnelling, protocolo de tunnel punto a punto

PPP: protocolo punto a punto, un método para conectar un ordenador a internet, el PPP es estable y proporciona funciones de verificación de errores.

PROTOCOLO: es un formato convenido para transmitir datos entre dos dispositivos. Y se pueden implementar en software o hardware.

RAS: remote Access service. Servicio de acceso remoto a la red

RDSI: red digital de servicios integrados, es un estandar internacional de comunicaciones para transmitir voz videos y datos por línea telefónica digitales o

alambres de teléfono normal.

RSA: algoritmo de clave publica iniciales de los nombres de sus inventores, Rivest, Shamir, Adleman

SA: asociación de Seguridad

SSL: secure Sockets Layer (capa de socalos de seguridad

Capa de Socket Segura. Protocolo que ofrece funciones de seguridad a nivel de la capa de transporte para TCP.

SOAP: interoperabilidad

SMTP: simple Mail Transfer Protocol, protocolo de transferencia de correo simple

SNMP: simple Network mangement Protocol, protocolo de administration de red simple

T1: línea de transmisión implementada por AT & T con velocidad de 1.544

Mbps.

VPN: virtual private network

UDP: protocolo de datagrama de usuario

X25: protocolo para red de paquetes conmutados. Generalmente se incluyen los protocolos X.3 y X.28 en estas redes.

Referencias

[1] SCOTT, Charly. Virtual Private Networks. O'Reilly & Associates, 2° edition, 1999. p. 78.

[2] BROWN, Steven. Implementación de redes privadas virtuales RPV. México D.F: McGraw-Gill, 2000.

[3] McDYSAN, David. VPN Aplications Guide: Real Solutions for Enterprice Networks, E. United State of America: 2000. John Wiley & Sons Inc.

[4] DOAK, Wilson y Peter, Creating and Implementing VIRTUAL PRIVATE NETWORKS. CASEY, United States of America : the Coriolis Group, 2000. .

[5] HARRIS, Nick et al. Linux Handbook, A Guide to IBM Linux Solutions and Resources. Redbooks,2003. http://ibm.com/redbooks/sg247000