Curso de Seguridad Infórmatica

Creada por V. Ana González Hernández

Curso de Seguridad Informática

Módulo 6. Redes Virtuales Privadas

Índice

*Nota de la autora de los 7 primeros temas curso: Escribir un curso de seguridad informática en una semana, es una tarea titánica casi imposible, aún así he decidido enfrentarme a ella para hacer posible este curso. Aunque me encantaría escribir todo con palabras propias, me resulta imposible debido a la falta de tiempo, por lo que copiaré varios textos de los cuales dejaré las referencias para la hacer posible la explicación de todo el contenido que el curso comprende.

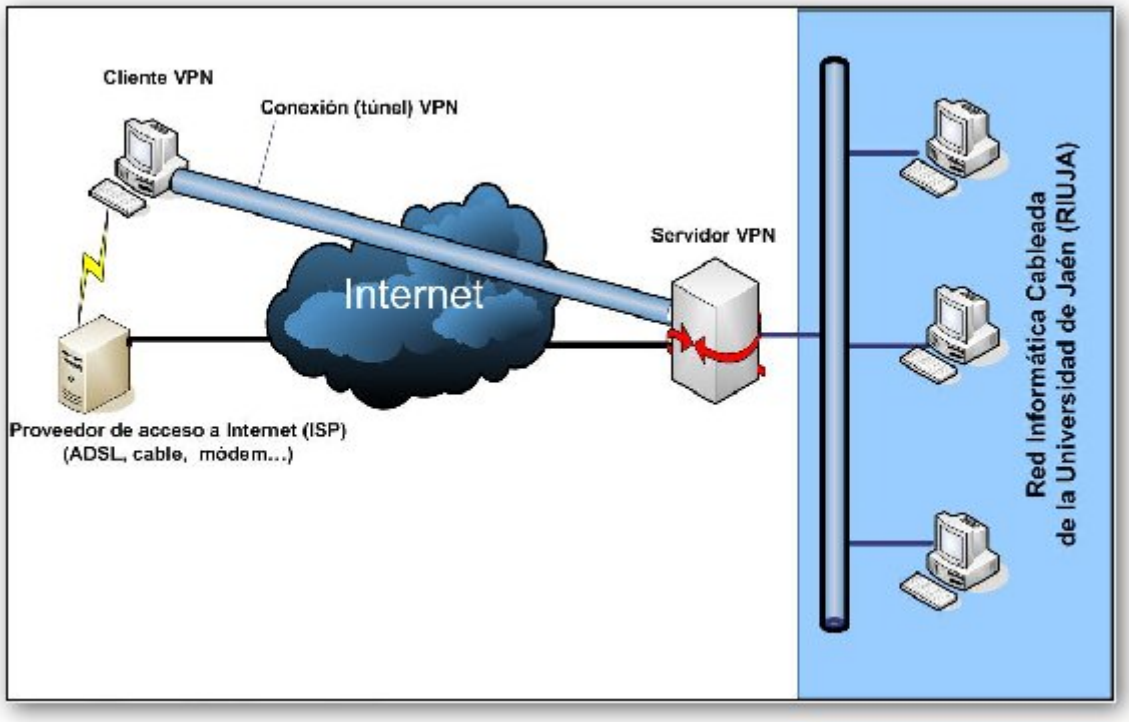
Creada por V. Ana González Hernández

6.1 Introducción a redes virtuales privadas

Los métodos tradicionales de acceso remoto y creación de WAN privadas resultan ser bastante costosos. Puesto que las redes públicas resultan ser mucho más económicas que las privadas, se buscaron maneras de poder establecer una red privada dentro de una red pública.
El resultado fue el surgimiento de las Redes Privadas Virtuales (VPN) las cuales han ofrecido ventajas muy amplias a las corporaciones siendo la principal de ellas la reducción de costos de instalación y mantenimiento de forma muy significativa.

Se puede definir a una VPN de la siguiente manera:
Una Red Privada Virtual (VPN, Virtual Private Network) es una red privada que utiliza la infraestructura de una red pública para poder transmitir información.
Una VPN combina dos conceptos: redes virtuales y redes privadas. En una red virtual, los enlaces de la red son lógicos y no físicos. La topología de esta red es independiente de la topología física de la infraestructura utilizada para soportarla.
Un usuario de una red virtual no será capaz de detectar la red física, el sólo podrá ver la red virtual.

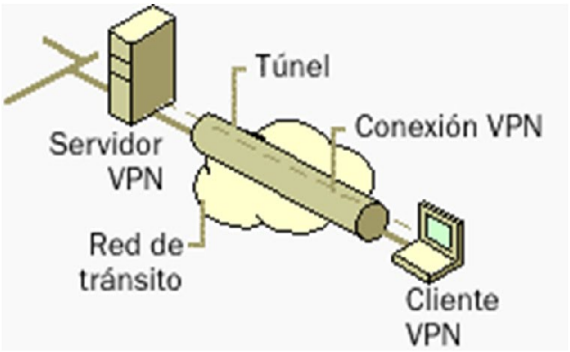
Desde la perspectiva del usuario, la VPN es una conexión punto a punto entre el equipo (el cliente VPN) y el servidor de la organización (el servidor VPN). La infraestructura exacta de la red pública es irrelevante dado que lógicamente parece como si los datos se enviaran a través de un vínculo privado dedicado.



Las redes privadas son definidas como redes que pertenecen a una misma entidad administrativa. Un ejemplo típico de esta clase de red es una intranet corporativa, o la intranet de una universidad, la cual puede ser utilizada sólo por los usuarios autorizados. De los conceptos de red privada y red virtual es como nace el concepto de red privada virtual.

Debido al hecho de ser una red privada que utiliza una red pública, la cuestión de la seguridad en una VPN es muy importante, ya que la información que circula en una red pública puede ser vista por cualquiera si no se toman las debidas precauciones. Y en una red pública como Internet existen muchas personas con diferentes intenciones.
Es por eso que una VPN debe de poseer excelentes mecanismos de autenticación y de encriptación de la información para que ésta viaje segura a través de una red pública

Los componentes básicos de una VPN son:
• Servidor VPN
• Túnel
• Conexión VPN
• Red pública de tránsito
• Cliente VPN



Para emular un vínculo punto a punto en una VPN, los datos se encapsulan o empaquetan con un encabezado que proporciona la información de enrutamiento que permite a los datos recorrer la red pública hasta alcanzar su destino.
Para emular un vínculo privado, los datos se cifran para asegurar la confidencialidad.
Los paquetes interceptados en la red compartida o pública no se pueden descifrar si no se dispone de las claves de cifrado. La parte de la conexión en la cual los datos privados son encapsulados es conocida como túnel. La parte de la conexión en la que se encapsulan y cifran los datos privados se denomina conexión VPN.

Arquitectura de una VPN

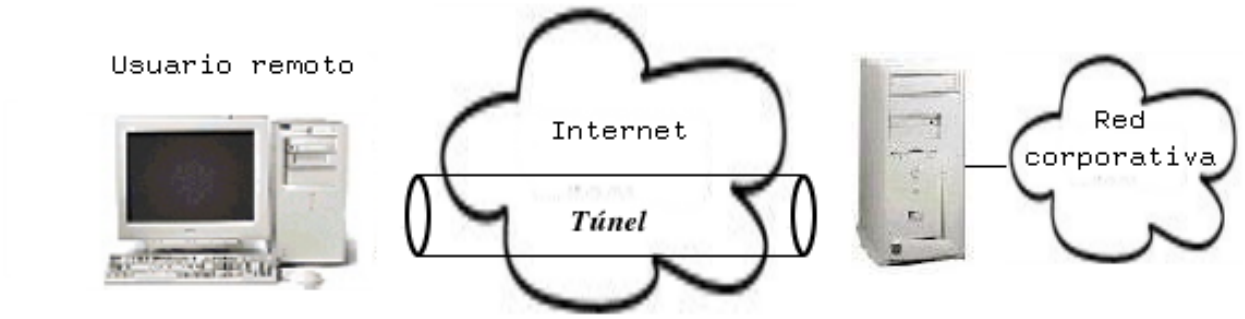
Existen básicamente dos tipos de arquitectura para una VPN. Estos son:

• VPN de acceso remoto
• VPN de sitio a sitio

La VPN de sitio a sitio también puede ser llamada VPN LAN a LAN o VPN POP a POP. Las VPN de sitio a sitio se dividen a su vez en VPN extranet y VPN intranet.
Las VPN de acceso remoto se dividen en VPN Dial-up y VPN directas.

VPN de acceso remoto

Esta VPN proporciona acceso remoto a una intranet o extranet corporativa. Una VPN de acceso remoto permite a los usuarios acceder a los recursos de la compañía siempre que lo requieran. Con el cliente VPN instalado en un dispositivo, el usuario es capaz de conectarse a la red corporativa, no importa
donde se encuentre.



El cliente de acceso remoto inicia una conexión VPN a través de Internet con el servidor VPN de la compañía. Una vez que se ha establecido el enlace, el usuario puede acceder a los recursos de la intranet privada de la empresa.
De acuerdo a la tecnología utilizada para establecer la conexión, las VPN de acceso remoto se puede dividir en VPN dial-up y VPN directas.

VPN dial-up. En esta VPN, el usuario realiza una llamada local al ISP utilizando un módem. El uso de este tipo de VPN se da más entre los usuarios móviles, ya que no en todos los lugares a donde se viaja se pueden tener disponibles conexiones de alta velocidad.

VPN directa. En esta VPN, se utilizan las tecnologías de conexión a Internet de alta velocidad.
Este tipo de VPN se puede encontrar principalmente entre los teletrabajadores. Actualmente se pueden obtener conexiones a Internet desde el hogar utilizando estas tecnologías.

VPN de sitio a sitio
Las VPN de sitio a sitio son utilizadas para conectar sitios geográficamente separados de una corporación. En las redes tradicionales, las distintas oficinas de una corporación son conectadas utilizando tecnologías como T1, E1, ATM o Frame Relay.
Con una VPN, es posible conectar las LAN corporativas utilizando Internet. El envío de información se realiza a través de una conexión VPN. De esta forma, se puede crear una WAN utilizando una VPN. Una empresa puede hacer que sus redes se conecten utilizando un ISP local y establezcan una conexión de sitio a sitio a través de Internet.

Creada por V. Ana González Hernández

6.2 Funcionamiento de las VPNs

Los costos de la comunicación se reducen enormemente porque el cliente sólo paga por el acceso a Internet. Las oficinas remotas se conectan a través de túneles creados sobre Internet. Con el uso de la infraestructura de Internet, una empresa puede desechar la difícil tarea de tener que estar administrando los dispositivos como los que se utilizan en las WAN tradicionales.
En base a lo problemas comerciales que resuelven, las VPN de sitio a sitio pueden subdividirse a su vez en VPN intranet y VPN extranet.

VPN intranet. Las VPN intranet se utilizan para la comunicación interna de una compañía.
Enlazan una oficina central con todas sus sucursales. Se disfrutan de las mismas normas que en cualquier red privada.
Un enrutador realiza una conexión VPN de sitio a sitio que conecta dos partes de una red privada. El servidor VPN proporciona una conexión enrutada a la red a la que está conectado el servidor VPN.

VPN extranet. Estas VPN enlazan clientes, proveedores, socios o comunidades de interés con una intranet corporativa. Se puede implementar una VPN extranet mediante acuerdo entre miembros de distintas organizaciones. Las empresas disfrutan de las mismas normas que las de una red privada. Sin embargo, las amenazas a la seguridad en una extranet son mayores que en una intranet, por lo que una VPN extranet debe ser cuidadosamente diseñada con muchas politicas de control de acceso y acuerdos de seguridad entre los miembros de la extranet.

Tipos de VPN

Existen diferentes formas de que una organización puede implementar una VPN.
Cada fabricante o proveedor ofrece diferentes tipos de soluciones VPN. Cada corporación tendrá que decidir la que más le convenga. Los tipos diferentes de VPN son:

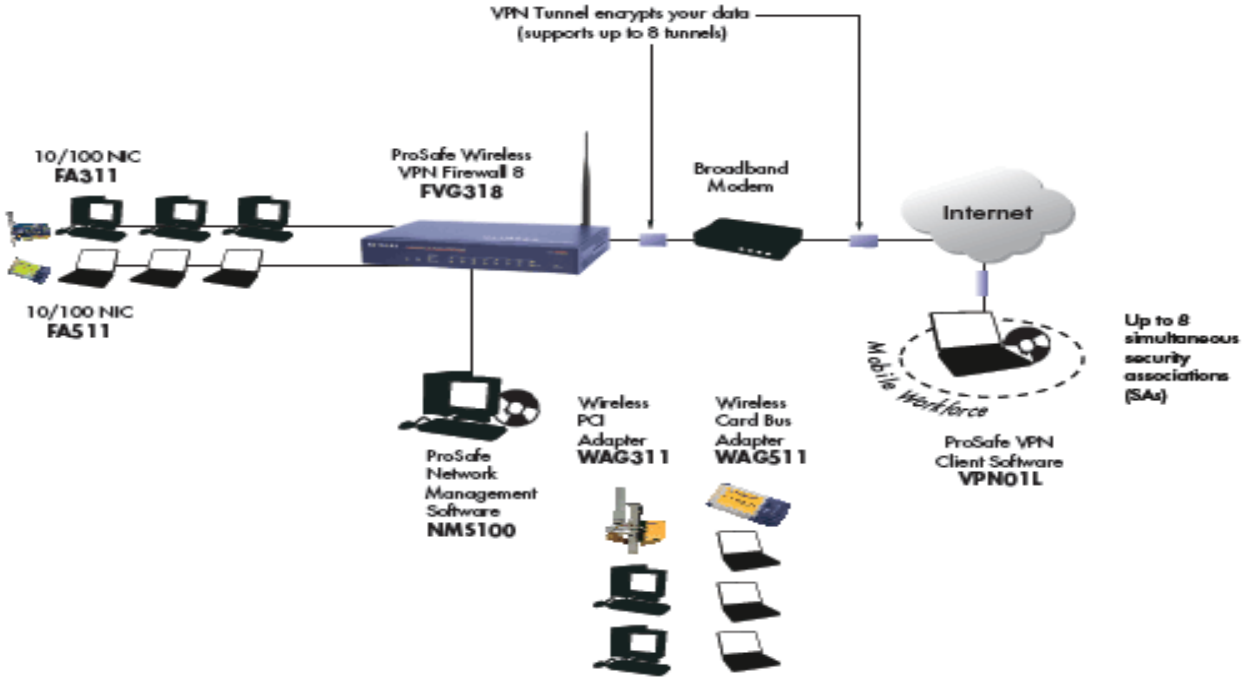
- VPN de firewall
- VPN de router y de concentrador
- VPN de sistema operativo
- VPN de aplicación
- VPN de proveedor de servicios

VPN de firewall

Un firewall (llamado también cortafuegos o servidor de seguridad) es un sistema de seguridad que implanta normas de control de acceso entre dos o más redes.
Se trata de un filtro que controla todas las comunicaciones que pasan de una red a la otra y en función de lo que sean permite o deniega su paso. Para permitir o denegar una comunicación el firewall examina el tipo de servicio al que corresponde, como pueden ser el web, el correo o el IRC. Dependiendo del servicio el firewall decide si lo permite o no. Además, el firewall examina si la comunicación es entrante o saliente y dependiendo de su dirección puede permitirla o no. Un firewall puede ser un dispositivo software o hardware, vamos a hablar detenidamente sobre firewalls más adelante.
Es muy común que se utilice un firewall para proporcionar servicios VPN.
Empresas como Cisco Systems, Nortel Networks y 3Com ofrecen en muchos de sus dispositivos firewall soporte para VPN. Una VPN basada en firewall tiene la ventaja de que simplifica la arquitectura de la red al establecer un único punto de control de seguridad. Además, los ingenieros de redes sólo tienen que hacerse expertos en una tecnología, en lugar de tener que aprender a administrar un firewall y la VPN de forma separada.

Entre los inconvenientes se puede mencionar que tener la VPN en un firewall convierte al dispositivo en algo más complejo, por lo que se debe ser más cuidadoso en su configuración o de lo contrario cualquier intruso podría tener acceso no autorizado a la red.

Otra desventaja ocurre debido a que tener firewall y VPN juntos, se ejerce presión al rendimiento del firewall. Esto ocurre principalmente si se tienen conectados cientos o incluso miles de usuarios.



VPN de sistema operativo

Los sistemas operativos como Windows de Microsoft, Netware de Novell o Linux en sus diferentes distribuciones (Red Hat, Debian,...) ofrecen servicios de VPN ya integrados. La principal ventaja de esta solución es que resulta ser económica ya que en un mismo sistema operativo se pueden contar con una gran variedad de servicios (servidor Web, de nombres de dominio, acceso remoto, VPN) y además mejora los métodos de autenticación y la seguridad del sistema operativo. Tiene la desventaja de que es vulnerable a los problemas de seguridad del propio sistema operativo. Estas VPN se utilizan más para el acceso remoto.

VPN de aplicación

Este tipo de VPN es poco común. Una VPN de aplicación es un programa que añade posibilidades VPN a un sistema operativo. Sin embargo, este programa no queda integrado con el sistema operativo. La ventaja de este tipo de VPN es que la aplicación añade seguridad extra a la que podría ofrecer una VPN integrada al sistema operativo. Un ejemplo de esta VPN es el programa OpenVpn sobre el cual vamso a hacer la práctica.

La desventaja es que estas VPN no soportan una gran cantidad de usuarios y son mucho más lentas que una VPN basada en hardware. Si se utilizan en Internet, son vulnerables a las fallas de seguridad del sistema operativo que contiene a la aplicación.

VPN de proveedor de servicios

Este tipo de VPN es proporcionada por un proveedor de servicios. Al principio las VPN de proveedor de servicios se basaban en tecnologías tales como X.25 y Frame Relay, posteriormente ATM y SMDS y finalmente se ofrecen

redes basadas en IP. El proveedor de servicios es la empresa propietaria de la infraestructura tales como equipos y líneas de transmisión que ofrece líneas dedicadas virtuales a
sus clientes.
El cliente se conecta a la red del proveedor de servicios a través de un dispositivo de equipo terminal del cliente (CPE) como puede ser un router. El CPE se conecta a través de medios de transmisión al equipo del proveedor de servicios, que puede ser X.25, Frame Relay, un conmutador ATM o un router IP. La línea virtual que se le proporciona al cliente mediante el proveedor de servicios se le llama circuito virtual (VC).

El proveedor de servicios puede cargar o una tarifa plana para el servicio VPN, que habitualmente depende del ancho de banda disponible para el cliente, o una tarifa basada en el uso, que puede depender del volumen de datos intercambiados o de la duración del intercambio de datos.

Acuerdos a nivel del servicio (SLA, Service Level Agreements).

Los SLA son contratos negociados entre proveedores VPN y sus abonados en los que se plantean los criterios de servicio que el abonado espera tengan los servicios específicos que reciba. La SLA es el único documento que está a disposición del abonado para asegurar que el proveedor VPN entrega el servicio o servicios con el nivel y calidad acordados. Si se ha de implementar una VPN basada en proveedor de servicios, este documento es de vital importancia para asegurar un buen servicio.

6.3 Requerimientos de una VPN

Una VPN debe de contar con ciertos requerimientos que permitan que valga la pena el uso de esta tecnología. Sin estos requerimientos, las VPN no podrán ofrecer la calidad necesaria que requieren las organizaciones para un desempeño óptimo. Una solución VPN debe ofrecer los siguientes requerimientos:

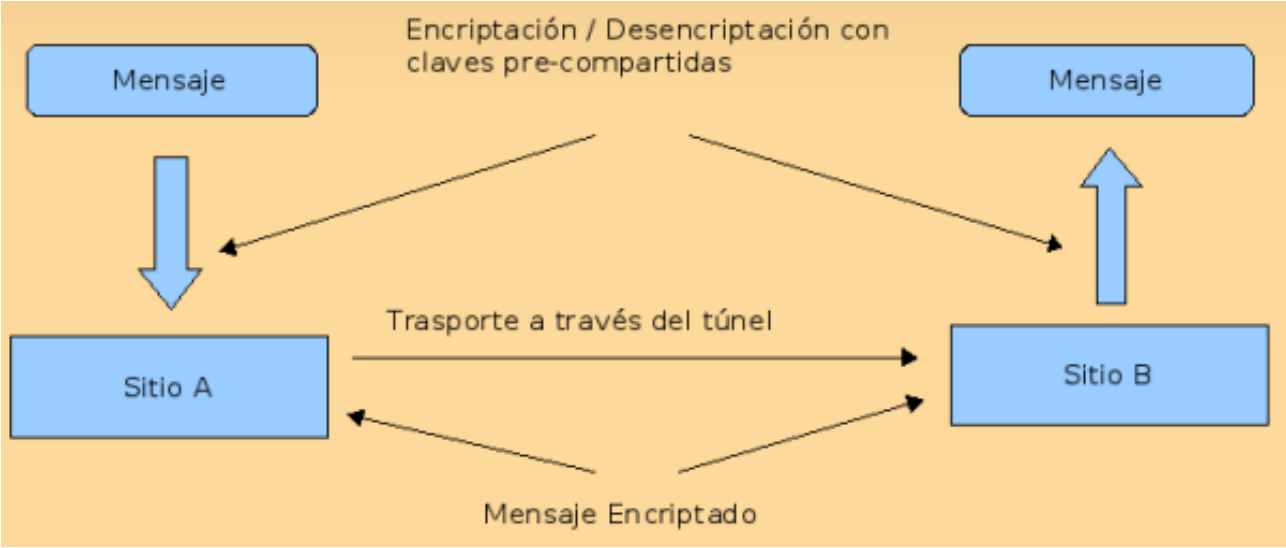
- Autenticación de usuarios
- Control de acceso
- Administración de direcciones
- Cifrado de datos
- Administración de claves
- Soporte a protocolos múltiples
- Ancho de banda

Autenticación de usuarios

La autenticación es uno de los requerimientos más importantes en una VPN. Cada entidad participante en una VPN debe de identificarse a sí misma ante otros y viceversa. La autenticación es el proceso que permite a los diversos integrantes de la VPN verificar las identidades de todos.

Existen muchos mecanismos de autenticación pero el más popular de todos ellos es la Infraestructura de Claves Públicas (PKI, Public Key Infraestructure), el cual es un sistema basado en la autenticación por medio de certificados. Cada integrante de una VPN se autentica intercambiando los certificados de cada uno, los cuales

están garantizados por una autoridad de certificación (CA, Certification Authority) en la que todos confían.
El proceso de autenticación también involucra el intercambio de información secreta, como una clave o un desafío ante un Servidor de Acceso a Red (NAS, Network Access Server), el cual consultará a un servidor RADIUS. Un servidor RADIUS administra la autenticación en una red que lo requiere.



Control de acceso

El control de acceso en una red está definido como el conjunto de políticas y técnicas que rigen el acceso a los recursos privados de una red por parte de usuarios autorizados. Una vez que un usuario ha sido autenticado, se debe definir a qué recursos de la red puede tener acceso dicho usuario. Los diferentes tipos de VPN, ya sea de firewalls, sistemas operativos, etc; son responsables de gestionar el estado de la conexión del usuario. La VPN debe administrar el inicio de una sesión, permitir el acceso a ciertos recursos, continuar una sesión, impedir el acceso de recursos y terminar una sesión.
El conjunto de reglas y acciones que definen el control de acceso se denomina politicas de control de acceso. Un servidor RADIUS puede administrar el control de acceso basándose en las politicas. Un ejemplo de una regla de control de acceso sería que el servidor permitiera el acceso sólo los usuarios de acceso remoto que no han rebasado un determinado uso de horas de la red.
El principal propósito de una VPN es permitir acceso seguro y selectivo a los recursos de una red. Con un buen sistema de cifrado y autenticación pero sin control de acceso, la VPN sólo protege la integridad del tráfico transmitido y evita que usuarios no autorizados ingresen a la red, pero los recursos de ésta no
quedan protegidos. Es por eso que el control de acceso es importante.

Administración de direcciones

Un servidor VPN debe de asignar una dirección IP al cliente VPN y asegurarse de que dicha dirección permanezca privada. Está claro que IP no es un protocolo seguro y se puede ver esto en la inseguridad de Internet. Las direcciones deben ser protegidas con fuertes mecanismos de seguridad, esto es, deben usarse
técnicas que permitan la ocultación de la dirección privada dentro de una red pública.

La tecnología más utilizada para ocultar la información es el tunneling. El tunneling es una técnica que encapsula los datos (incluyendo la dirección destino privada) dentro de otro conjunto de datos. Así, el contenido de los paquetes encapsulados se vuelve invisible para una red pública insegura como Internet. Existen muchas tecnologías de tunneling, cada una de ellas con sus ventajas y desventajas. Otra tecnología alterna al tunneling es

MPLS, donde se hace uso de un sistema de etiquetas para transmitir información. MPLS es una tecnología que realizará grandes cambios a los métodos tradicionales de enrutamiento y de la forma de crear túneles.

Cifrado de datos

Cifrar o encriptar los datos es una tarea esencial de una VPN. Aunque se puedan encapsular los datos dentro de un túnel, estos todavía pueden ser leídos si no se implementan fuertes mecanismos de cifrado de la información.
Antes de enviar la información, el servidor VPN cifra la información convirtiéndolo en texto cifrado.
El receptor de la información descifra la información y la convierte en texto nativo.
Al principio los algoritmos de encriptación se mantenían en secreto. Sin embargo, cuando el algoritmo era roto, toda la información protegida con dicho algoritmo se volvía vulnerable. Por consiguiente, actualmente los algoritmos se hacen públicos.
Existen muchos tipos de algoritmos de cifrado muy fuertes utilizados en las VPN entre los que podemos encontrar 3DES, Diffie-Hellman, MD5, RSA y SHA-1 los cuales ya debeis conocer ya que los vimos en el tema anterior.
Puesto que el algoritmo de cifrado es conocido por todos, es necesario implementar técnicas para poder mantener los datos seguros. Esto se logra mediante el uso de claves. Una clave es un código secreto que el algoritmo de encriptación utiliza para crear una única versión de texto cifrado. Mientras la longitud en bits de esta clave sea más grande, más difícil será descifrar una información.

Las VPN requieren del uso de claves con una cierta longitud, de tal manera que resulta prácticamente imposible descifrar los datos (teóricamente tardaría millones de años, a no ser que se posean cientos de procesadores trabajando al mismo tiempo para encontrar la clave y aunque ésta se encontrara, los algoritmos están diseñados de forma que no se garantizaría totalmente el éxito). Aunque de hecho,
el uso de claves muy largas no es recomendable porque se afecta mucho el rendimiento de un procesador. Para eso se utilizan métodos como el uso de claves simétricas y asimétricas.

Con una clave simétrica, se usa la misma clave para cifrar y descifrar la información que viaja por un túnel. Tanto el emisor como el receptor de los datos poseen la misma clave privada. Con una clave asimétrica, la información se cifra con una clave y se descifra con otra diferente. Una de las claves sólo es conocida
por el usuario, la cual es conocida como clave privada. La otra clave es conocida por todos y se le llama clave pública.
Las claves públicas permiten el uso de firmas digitales para autenticar información. Una clave pública es distribuida libremente a cualquiera que requiera enviar información cifrada o firmada. La clave privada debe ser bien resguardada por el usuario y no darla a conocer nunca.

Administración de claves

En una VPN, es importante la administración de claves. Para asegurar la integridad de una clave pública, ésta es publicada junto con un certificado. Un certificado es una estructura de datos firmada digitalmente por una organización conocida como autoridad de certificación (CA) en la cual todos confían. Una CA
firma su certificado con su clave privada. Un usuario que utiliza la clave pública de la CA podrá comprobar que el certificado le pertenece a dicha CA y por lo tanto, la clave pública es válida y confiable.
En una VPN pequeña no es muy necesario establecer una infraestructura de administración de claves. Sin embargo, las grandes compañías obtendrán muchos beneficios si hacen crean una Infraestructura de Claves Públicas (PKI) para poder crear y distribuir certificados. Una corporación puede crear su propia CA o confiar en una CA de terceros. Una PKI es muy útil en aquellas organizaciones que requieren de mucha seguridad y acceso limitado a sus usuarios.

Soporte a protocolos múltiples

Para que una solución VPN sea viable, es necesario también que ésta pueda ofrecer soporte a múltiples protocolos.

Esto incluye el soporte a protocolos de red que no sean IP como pueden ser AppleTalk, IPX y NetBEUI. PPTP soporta varios protocolos de red. IPSec sólo puede ser utilizado en redes basadas en IP, pero siempre es posible encapsular los protocolos no compatibles dentro de un paquete IP, de modo que puedan ser transportados. En cuanto a L2TP, este protocolo VPN no sólo puede ser implementado en redes IP, sino también en ATM y Frame Relay.

Ancho de banda

El ancho de banda es también un requerimiento importante en una VPN. En el mundo de las redes existe un concepto que define la forma de administrar el ancho de banda con el fin de que el tráfico de una red fluya de forma eficiente.
Dicho concepto es la Calidad de Servicio (QoS, Quality of Service). La QoS es una característica muy importante de una VPN. Una solución VPN no estará completa si no proporciona formas para el control y administración del ancho de banda.
La calidad del servicio también se refiere al número de conexiones simultáneas (la cantidad de túneles que pueden ser establecidos entre un sitio remoto y el sitio central) que puede soportar una VPN y la forma cono ésta afecta al rendimiento de la VPN.
Es preciso también asegurarse que una VPN puede cifrar y descifrar los paquetes transmitidos a una velocidad adecuada, ya que algunos algoritmos de cifrado son lentos y si no se tiene un buen procesador el rendimiento se verá afectado. Es importante mencionar que el valor nominal de velocidad de los dispositivos de redes (por ejemplo 100 Mbps) nunca se cumple en la realidad y que eso habrá que tomarse en cuenta a la hora de implementar una VPN.
La calidad de las conexiones a Internet también es importante. Las técnicas de encriptación incrementan el deterioro del rendimiento de la comunicación por las sobrecargas. Las pérdidas de paquetes y la latencia en conexiones a Internet de baja calidad afecta más al rendimiento, que la carga añadida por la encriptación

6.4 Tunneling y VPN

Cuando el uso de túneles se combina con el cifrado de los datos, puede utilizarse para proporcionar servicios de VPN. Las VPN utilizan el tunneling para poder ofrecer mecanismos seguros de transporte de datos. Dentro del contexto de las VPN, el tunneling involucra tres tareas principales:

- Encapsulación
- Protección de direcciones privadas
- Integridad de los datos y confidencialidad de éstos

Para que el proceso del tunneling pueda ser llevado a cabo, existen diversos protocolos llamados protocolos de túnel los cuales se encargan de encapsular y desencapsular los datos que viajan dentro de una red privada virtual. Los protocolos de túnel usados por las VPN como PPTP y L2TP son usados para encapsular tramas de la capa de enlace de datos (PPP). Protocolos de túnel como IP sobre IP e IPSec en modo túnel son utilizados para encapsular paquetes de la capa de red.

Es posible colocar un paquete que utiliza una dirección IP privada dentro de un paquete que usa una dirección IP global única para poder extender una red privada sobre una red pública como Internet. Puesto que los contenidos del paquete entunelado sólo pueden ser interpretados por las interfaces de túnel, las
direcciones IP privadas pueden ser ocultadas completamente de las redes IP públicas.

Los mecanismos de integridad y confidencialidad garantizan que ningún usuario no autorizado pueda alterar los paquetes entunelados durante la transmisión sin que el ataque pueda ser detectado y que los contenidos del paquete permanecen protegidos de acceso no autorizado. Además, el tunneling opcionalmente puede

proteger la integridad de la cabecera del paquete IP externo, mediante técnicas de autenticación. Por ejemplo, si se utiliza IPSec los protocolos AH y ESP pueden proporcionar autenticación de los paquetes transmitidos.

Tres protocolos de túnel son los más usados para la creación de una VPN:
• Protocolo de Túnel punto a punto (PPTP)
• Protocolo de Túnel de Capa 2 (L2TP)
• Protocolo de Seguridad IP

Los protocolos PPTP y L2TP se enfocan principalmente a las VPN de acceso remoto, mientras que IPSec se enfoca mayormente en las soluciones VPN de sitio a sitio.

Los túneles se clasifican de acuerdo a cómo se establece la conexión entre dos hosts. En base a esto, existen dos tipos de túneles. Éstos son:
• Túnel voluntario
• Túnel obligatorio

Túnel voluntario

Un equipo usuario o cliente puede emitir una petición VPN para configurar y crear un túnel voluntario. En este caso, el equipo del usuario es un extremo del túnel que funciona como cliente de túnel. El túnel voluntario se produce cuando una estación de trabajo o un router utilizan software de cliente de túnel para crear una conexión VPN con el servidor de túnel de destino. Para ello, debe instalar el protocolo de túnel correspondiente en el equipo cliente. Un túnel voluntario puede ser creado de dos maneras a través de una conexión dial-up o a través de una lan.

A través de una conexión dial-up:
En este caso, el usuario primero hace una llamada a su ISP para conectarse a Internet y entonces posteriormente podrá ser creado el túnel. Esta suele ser la situación más común. La conexión a Internet es un paso preliminar para crear el túnel pero no forma parte del proceso de creación del túnel.

A través de una LAN:
En este caso, el cliente ya posee una conexión a la red, por lo que el túnel puede ser creado con cualquier servidor túnel deseado. Este es el caso de un usuario de una LAN que crea un túnel para acceder a otra LAN.

Túnel obligatorio

El túnel obligatorio es la creación de un túnel seguro por parte de otro equipo o dispositivo de red en nombre del equipo cliente. Los túneles obligatorios se configuran y crean automáticamente para los usuarios sin que éstos intervengan ni tengan conocimiento de los mismos. Con un túnel obligatorio, el equipo del usuario no es un extremo del túnel. Lo es otro dispositivo entre el equipo del usuario y el servidor de túnel que actúa como cliente de túnel.
Algunos proveedores que venden servidores de acceso telefónico facilitan la creación de un túnel en nombre de un cliente de acceso telefónico. El dispositivo que proporciona el túnel para el equipo cliente se conoce como procesador cliente (FEP) o PAC en PPTP, concentrador de acceso (LAC) de L2TP en L2TP o puerta de enlace (gateway) de Seguridad IP en IPSec. Para realizar su función, el dispositivo que proporciona el túnel debe tener instalado el protocolo de túnel adecuado y debe ser capaz de establecer el túnel cuando el equipo cliente intenta establecer una conexión.

Esta configuración se conoce como túnel obligatorio debido a que el cliente está obligado a utilizar el túnel creado por el dispositivo que proporciona el túnel. Una vez que se realiza la conexión inicial, todo el tráfico de la red de y hacia el cliente se envía automáticamente a través del túnel. En los túneles obligatorios, la

computadora cliente realiza una conexión única PPP y, cuando un cliente se conecta en el NAS, se crea un túnel y todo el tráfico se enruta automáticamente a través de éste. Se puede configurar un el dispositivo que proporciona el túnel para hacer un túnel a todos los clientes hacia un servidor específico del túnel. De
manera alterna, el dispositivo que proporciona el túnel podría hacer túneles individuales de los clientes basados en el nombre o destino del usuario.
A diferencia de los túneles por separado creados para cada cliente voluntario, un túnel entre el dispositivo que proporciona el túnel y el servidor del túnel puede estar compartido entre varios clientes. Cuando un segundo cliente se conecta al dispositivo que proporciona el túnel para alcanzar un destino para el cual ya existe un túnel, no hay necesidad de crear una nueva instancia del túnel entre el dispositivo que proporciona el túnel y el servidor del túnel. El tráfico de datos para el nuevo cliente se transporta sobre el túnel existente. Ya que puede haber varios clientes en un túnel único, el túnel no se termina hasta que se desconecta el último usuario del túnel.

Una compañía puede contratar a un ISP para que implemente un conjunto de dispositivos que proporcionen túneles por todos los territorios donde existan LAN de la compañía. Estos dispositivos pueden establecer túneles a través de Internet hasta un servidor VPN conectado a la red privada de la organización, consolidando así las llamadas de zonas geográficamente dispersas en una sola conexión a Internet en la red de la organización.

Existen dos formas de crear túneles obligatorios. En la primera forma, el túnel se crea antes de autenticar al cliente de acceso. Una vez creado el túnel, el cliente de acceso se autentica en el servidor de túnel. En la segunda forma, el túnel se crea después de que el dispositivo que proporciona el túnel autentica al cliente de acceso.
La seguridad de una VPN debe ir más allá que simplemente controlar el acceso seguro a los recursos de una red. También debe proveer mecanismos para administrar la implementación de pólizas de seguridad que garanticen el desarrollo exitoso de una VPN. La mejor opción es establecer también, antes de que se
establezca la conexión cifrada con una oficina o LAN remota, unos niveles de seguridad que deben cumplirse. La comprobación de los niveles de seguridad que debe cumplir el equipo remoto que desea conectarse a la red corporativa debe ser lo más amplia posible.

Sin duda, es necesario establecer un sistema de chequeo del status de seguridad de los equipos remotos conectados mediante VPN a la red corporativa. Y el chequeo debe ser percibido por el usuario remoto como una ayuda a la seguridad general, no como una imposición corporativa y además, debe hacerse con
suficiente amplitud como para abarcar productos y sistemas de seguridad no corporativos, sino elegidos por el teletrabajador en su ámbito doméstico.
La autenticación de usuarios y la encriptación de datos son características de seguridad muy fuertes. Y en una VPN la tecnología que podrá ofrecer mejor seguridad será IPSec.

6.5 Seguridad IP (IPSec) y protocolos vpn

Definición de IPSec

La Seguridad del Protocolo de Internet (IPSec, Internet Protocol Security) es un marco de estándares abiertos para lograr comunicaciones privadas seguras a través de redes IP mediante el uso de servicios de seguridad criptográfica. IPSec es la tendencia a largo plazo para las redes seguras. Proporciona una sólida protección contra ataques a redes privadas e Internet mediante la seguridad de extremo a extremo. Los
únicos equipos que deben conocer que existe protección con IPSec son el remitente y el receptor de la comunicación. IPSec tiene dos objetivos:

• Proteger el contenido de los paquetes IP.
• Defender contra los ataques de red mediante el filtrado de paquetes y la exigencia de comunicaciones de confianza.

Ambos objetivos se alcanzan gracias al uso de servicios de protección criptográfica, protocolos de seguridad y administración dinámica de claves. Estos fundamentos proporcionan al mismo tiempo la capacidad y la flexibilidad para proteger las comunicaciones entre equipos de redes privadas, dominios, sitios, sitios remotos, extranets y clientes de acceso telefónico. Incluso pueden utilizarse para bloquear la recepción o la transmisión de determinados tipos de tráfico. IPSec se basa en un modelo de seguridad completo, y establece la confianza y la seguridad desde una dirección IP de origen hasta una dirección IP de destino. La
dirección IP en sí no se considera necesariamente una identidad, sino que el sistema que hay tras la dirección IP tiene una identidad que se valida a través de un proceso de autenticación. Los únicos equipos que deben conocer que el tráfico está protegido son los equipos remitente y receptor.

Cada equipo trata la seguridad en su extremo respectivo y supone que el medio a través del cual tiene lugar la comunicación no es seguro. Los equipos que se limitan a enrutar datos desde el origen hasta el destino no necesitan ser compatibles con IPSec, salvo en el caso de que se filtren paquetes de tipo servidor
de seguridad o se traduzcan direcciones de red entre los dos equipos.

Este modelo permite implementar correctamente IPSec en los siguientes casos:

• Red de área local (LAN): cliente-servidor y entre homólogos
• Red de área extensa (WAN): entre routers y entre puertas de enlace
• Acceso remoto: clientes de acceso telefónico y acceso a Internet desde redes privadas IPSec se basa en los estándares desarrollados por el grupo de trabajo de IPSec del IETF. IPSec se encuentra documentado en diversos RFC de los cuales el principal es el RFC 2401.

IPSec utiliza dos protocolos que proporcionan seguridad en el tráfico. Estos protocolos son:

• Cabecera de autenticación (AH, Authentication Header)
• Carga de Seguridad de Encapsulamiento (ESP, Encapsulating Security
Protocol)

AH proporciona integridad en la conexión, autenticación de los datos de origen y un servicio opcional contra paquetes repetidos. ESP provee confidencialidad de los datos utilizando técnicas de encriptación. Opcionalmente puede proporcionar también autenticación, integridad y protección contra paquetes repetidos. Ambos protocolos son vehículos para el control de acceso, basado en la distribución de
claves criptográficas y la administración de los flujos de tráfico relativos a estos protocolos de seguridad.
Cada protocolo soporta dos modos de uso: modo transporte y modo túnel. En el modo transporte los AH y ESP proveen protección a los protocolos de capas superiores. En el modo túnel AH y ESP son aplicados para entunelar paquetes IP.

También se utiliza un conjunto protocolos necesarios para la gestión de llaves criptográficas. La Asociación de Seguridad (SA), utilizada para llevar a cabo la autenticación, representa una conexión unidireccional para la cual se definen todos los servicios de seguridad que deben ser aplicados al tráfico de red. Las SA
pueden ser creadas tanto automáticamente como manualmente, empleando para ello el protocolo ISAKMP/Oakley.

Protocolos de IPSec

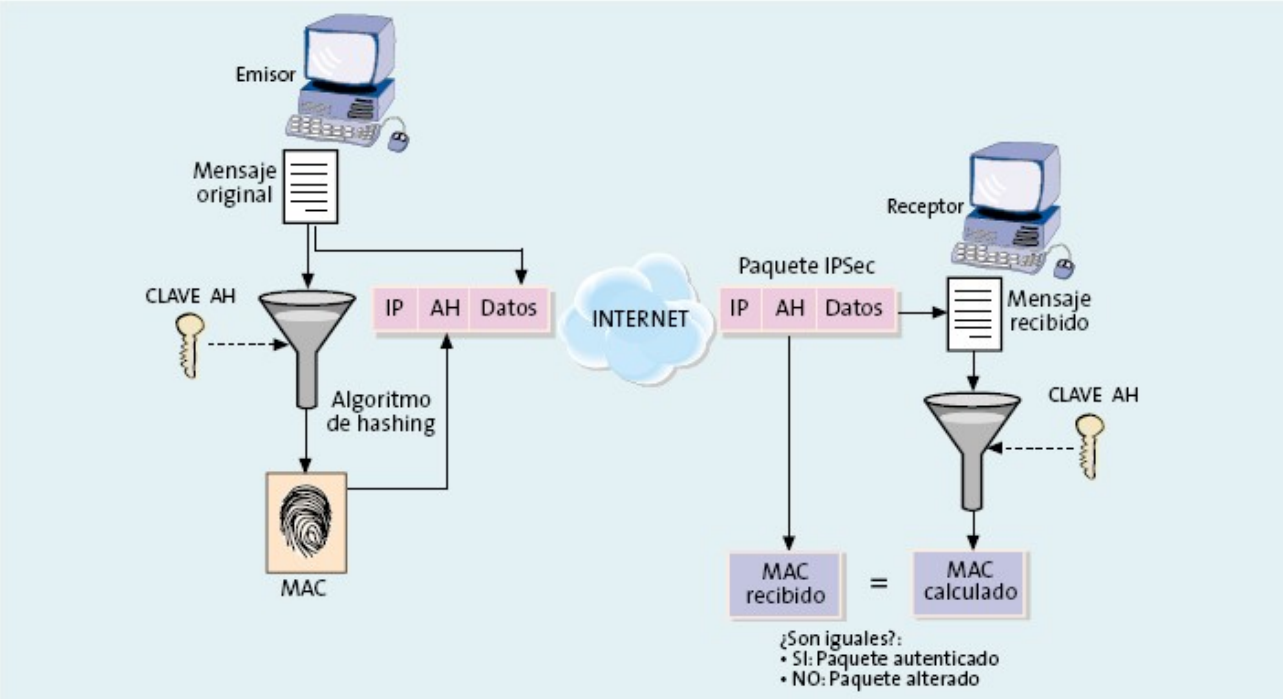
Cabecera de Autenticación (AH)
La cabecera de autenticación (AH, Authentication Header) puede detectar paquetes alterados y puede autenticar la identidad del emisor basándose en el usuario final o en la dirección IP fuente. Las partes que se comunican en

IPSec usando AH pueden utilizar diferentes algoritmos ya sea MD5 o SHA-1 con el fin de crear una firma hash utilizando un componente secreto de la SA, la carga útil del paquete y varias partes de la cabecera del paquete. Contenido del paquete AH. La cabecera AH contiene esencialmente cinco campos

• La cabecera siguiente describe la cabecera de la capa 4 (TCP, UDP, ICMP) para un datagrama IPv4 (8 bits)
• La longitud de la firma hash (8 bits)
• El Índice de Parámetro de Seguridad (SPI) (32 bits)
• El campo de número de secuencia antirepetición, el cual evita los ataques de repetición (32 bits)
• La firma hash propiamente dicha (32 bits)

AH en modo transporte. En el modo transporte, los servicios AH protegen la cabecera IP externa junto con la carga útil de datos. Los servicios AH protegen todos los campos en la cabecera que no cambia durante el transporte.
AH se coloca después de la cabecera IP y antes de la cabecera ESP si está presente, y antes de los protocolos de capas superiores.

AH en modo túnel. En el modo túnel , la cabecera original entera es autenticada, se construye una cabecera IP nueva y la nueva cabecera IP es protegida de la misma manera que en el modo transporte.



Carga de Seguridad de Encapsulación (ESP)

La Carga de Seguridad de Encapsulamiento (ESP, Encapsulating Security Protocol) puede proporcionar servicios de confidencialidad, autenticidad e integridad. El modo túnel ESP también ofrece confidencialidad en el flujo del tráfico. Las primeras versiones de ESP se enfocaron principalmente en la confidencialidad; sin embargo, el estándar final también incluye una gran funcionalidad como la que proporciona AH. Los estándares ESP soportan principalmente dos métodos de cifrado DES y 3DES.

Contenido del paquete ESP. Al igual que AH, la cabecera ESP contiene lo siguiente,

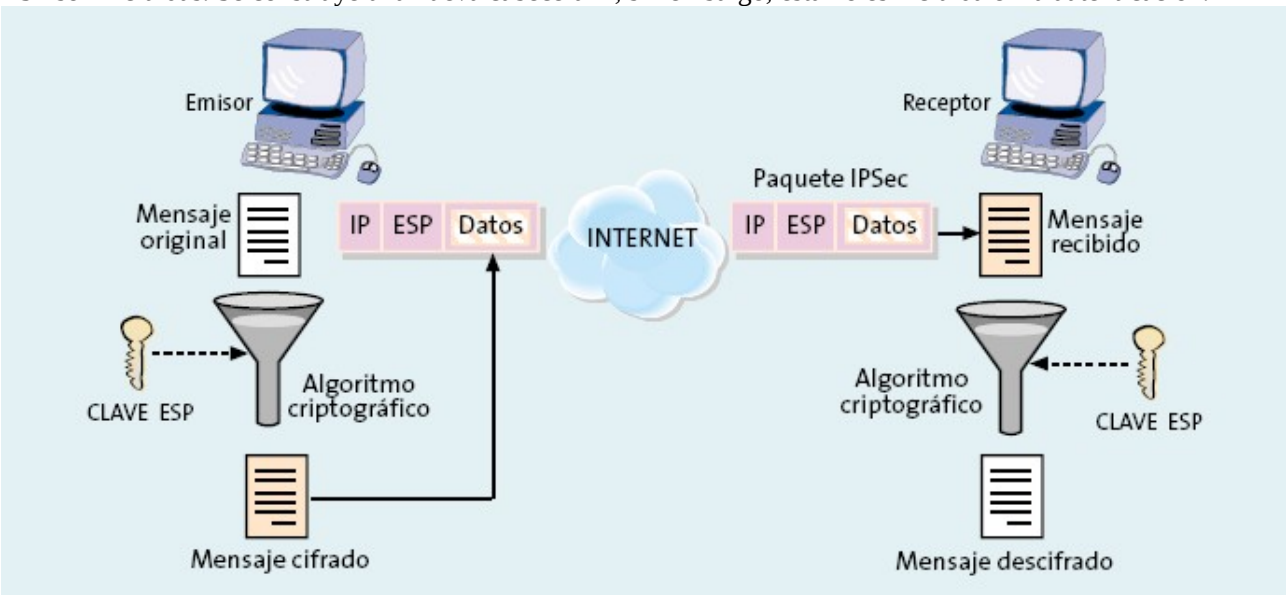
• Índice de Parámetro de Seguridad (SPI) (32 bits)
• El campo de número de secuencia antirepetición (32 bits)
• Longitud de relleno (8 bits)
• Cabecera siguiente (8 bits)
• Relleno (0-255 bits)

A diferencia de AH, ESP también incluye el campo cabecera siguiente como una parte del finalizador del paquete. La carga del paquete debe incluir relleno para que pueda operar el algoritmo de cifrado. El finalizador también debe contener un monto variable de datos de autenticación. ESP en modo transporte. En el modo transporte, la carga IP es cifrada y las cabeceras originales se dejan intactas. La cabecera ESP es insertada después de la cabecera IP y antes de la cabecera del protocolo de capa superior.

Los protocolos de capa superior son cifrados y autenticados utilizando la cabecera ESP. ESP no autentica la cabecera IP. También hay que notar que la información de capas superiores no está disponible debido a que pertenece a la carga cifrada.

ESP en modo túnel.

En el modo túnel, la cabecera IP original se encuentra bien protegida debido a que el datagrama original IP completo se encuentra cifrado. Con el mecanismo de autenticación ESP, el datagrama IP original y la cabecera ESP son incluidas. Se construye una nueva cabecera IP, sin embargo, ésta no es incluida en la autenticación.



Asociaciones de Seguridad (SA)

El concepto de Asociación de Seguridad (SA, Security Association) es fundamental en la arquitectura IPSec. Una SA es una conexión que permite servicios de seguridad para el tráfico transportado por ésta, dicho en otra forma, una SA es un acuerdo entre ambas partes acerca de cómo cifrar y descifrar los datos que se van a transmitir. Los servicios de seguridad son proporcionados a una SA utilizando AH o ESP pero no ambos. Si ambos protocolos son aplicados a influjo de datos determinado, entonces dos o más SA son creadas para dar protección a dicho flujo.

Para asegurar una típica comunicación bidireccional entre dos hosts, o entre dos gateways de seguridad, dos SA (una en cada dirección) son requeridas.
Una SA es identificada de forma única por medio de valores diferentes tales como un Índice de Parámetro de Seguridad (SPI, Security Parameter Index), una dirección IP destino y un identificador del protocolo de seguridad (AH o ESP). Los estándares definen un riguroso mecanismo para asegurar que cada SA es única.
Los dispositivos IPSec almacenan estas SA en una Base de Datos SA (SAD, SA Database).

Administración de claves en IPSec

Los protocolos ISAKMP/Oakley e IKE
Puesto que IPSec es una arquitectura abierta, los protocolos de seguridad (AH y ESP) están diseñados para ser independientes con respecto a la administración de claves cifradas de forma automática. Sin embargo, las implementaciones de IPSec que cumplan con los estándares deben soportar tanto el uso de claves
previamente compartidas como el mecanismo de administración de claves automatizado conocido como Intercambio de claves de Internet (IKE, Internet Key Exchange).

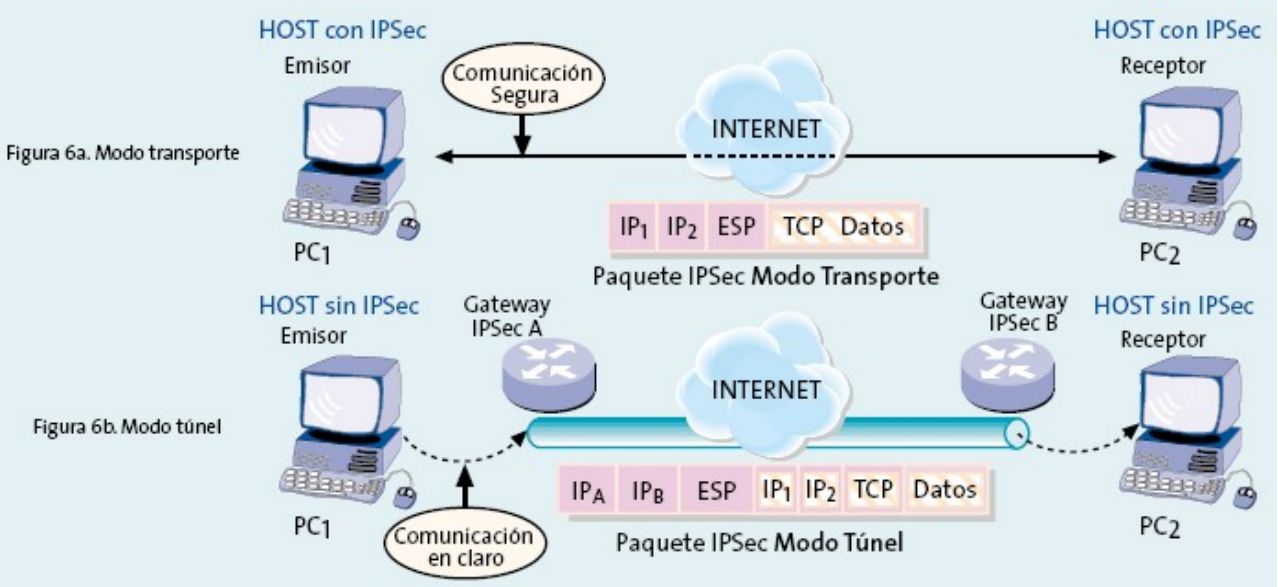
IKE es un diseño específico dentro de un sistema mayor conocido como Protocolo de Administración de Claves y Asociación de Seguridad de Internet (ISAKMP, Internet Security Association and Key Management Protocol). ISAKMP es un sistema de intercambio de claves y autenticación que es independiente de
cualquier tecnología de claves específica. IKE trabaja con otro protocolo llamado Oakley, para el intercambio de claves seguro dentro del modelo ISAKMP.
ISAKMP/Oakley proporciona un mecanismo que permite a servidores VPN separados compartir información de claves de encriptación y hace que IPSec sea práctico en el entorno actual. [16]

Protocolo Oakley

Oakley es un protocolo que utiliza un intercambio de claves Diffie-Hellman para establecer una clave compartida de forma segura entre las dos partes que se comunican. Oakley trabaja dentro del marco ISAKMP para establecer las SA de IPSec. El estándar de determinación de clave Oakley establece una SA de ISAKMP inicial, pero permite un mecanismo más ligero para permitir SA subsecuentes.

Intercambio de Claves de Internet (IKE)

El protocolo de Intercambio de claves de Internet (IKE) pertenece al conjunto ISAKMP/Oakley. Es un protocolo de administración de claves seguro diseñado para establecer las SA de IPSec y para permitir una rápida reasignación de claves para las SA existentes. IKE opera en dos fases, las cuales se describen a
continuación.



Fase 1 de IKE.

El objetivo básico de la fase 1 de IKE es autenticar ambas partes de IPSec. Durante esta fase se llevan a cabo las siguientes funciones:

• Identificar y proteger las identidades de ambas partes de IPSec
• Negociar una póliza SA de ISAKMP entre ambas partes para proteger el intercambio de IKE
• Ejecutar un intercambio Diffie-Hellman autenticado con el resultado final de tener claves secretas compartidas.
• Establecer un túnel seguro para negociar los parámetros de la fase 2 de IKE

Fase 2 de IKE.

El propósito de la fase 2 de IKE es negociar las SA de IPSec para establecer el túnel IPSec. La fase 2 de IKE lleva a cabo las siguientes funciones

• Negociar los parámetros SA de IPSec protegidos por una SA de ISAKMP existente.
• Establece SA de IPSec
• Periódicamente renegocia las SA de IPSec para garantizar la seguridad
• Ejecuta opcionalmente un intercambio Diffie-Hellman adicional

Funcionamiento de IPSec

IPSec es una tecnología que envuelve muchos componentes tecnológicos y métodos de encriptación. Así pues, la operación de IPSec se puede descomponer en cinco pasos principales que se explican a continuación

1. En este primer paso se determina el tráfico inicial IPSec. Determinar este tráfico inicial es parte de la formulación de una póliza de seguridad para usar en una VPN. Esta póliza es implementada en ambas partes que se comunican.

2. El segundo paso consiste en ejecutar la Fase 1 de IKE, donde se autentican ambos extremos.

3. El tercer paso consiste en ejecutar la Fase 2 de IKE, donde se establecen las SA para crear el túnel.

4. El cuarto paso es donde se lleva acabo la transferencia de datos por el túnel IPSec. Los paquetes son cifrados y descifrados de acuerdo con el método especificado en la SA de Ipsec.

5. El último paso consiste en la terminación del túnel IPSec, donde las SA expiran y se deben negociar nuevas SA para continuar transmitiendo datos. Entonces se regresa a la Fase 2 o a la Fase 1. Esto resulta en nuevas SA y nuevas claves.

6.6 VPN SSL/TLS y VPN IPSec

En este punto de la memoria se hará una comparación entre las dos tecnologías más utilizadas en Internet para la implementación de VPN: SSL/TLS e IPSec.

Para ello se describirán las ventajas y desventajas que se pueden obtener utilizando una implementación u otra en nuestra VPN, destacando sobre todo las ventajas que ofrecen respecto a seguridad y como evitan ciertos ataques. Además, se describirán posibles aplicaciones específicas que ofrece una y otra tecnología y como se pueden compensar las debilidades de IPSec con las ventajas de SSL/TLS y viceversa.

Sin embargo, actualmente, la mayoría de los expertos y también de suministradores, tienden a considerar que IPSec y SSL, más que de tecnologías en competencia, se trata de propuestas complementarias. De hecho, según argumentan los que adoptan esta actitud conciliadora, la creciente popularidad de las VPN SSL tendría como motivo su capacidad para cubrir de una forma sencilla y económica una necesidad que IPSec nunca ha podido satisfacer adecuadamente: el acceso remoto, específicamente en el área de las aplicaciones extranet. Según reconocen los expertos, a la hora de brindar este acceso universal, el protocolo IPSec, tradicionalmente utilizado en las conexiones LAN to LAN vía VPN, presentaba importantes inconvenientes.

La principal ventaja de las SSL VPN es el hecho de que, a diferencia de las implementaciones IPSec VPN, no exigen el despliegue de agentes software permanente sobre los dispositivos a los que se facilita acceso a las aplicaciones corporativas. De esta forma, se reduce significativamente la carga de soporte asociada a las implementaciones IPSec, simplificando la gestión y el mantenimiento, y reduciendo al mismo tiempo el coste de la solución. También se hace posible extender el acceso remoto a través de Internet a un número mucho mayor de usuarios, dado que soporta la conexión a los recursos corporativos desde cualquier sistema dotado de navegador Web, incluido en la práctica totalidad de los dispositivos de usuario. Los agentes VPN SSL son descargados a los PC remotos, sean estos cuales sean y estén ubicados donde estén, una vez que el usuario se haya autenticado en una aplicación SSL, instalada de forma similar a un proxy entre Internet y la red corporativa. El acceso se independiza así de un determinado dispositivo o ubicación, pasando a estar vinculado al usuario.

Con SSL, el acceso puede distribuirse, de una forma tremendamente sencilla, a más personas, lugares, y dispositivos que con IPSec, reduciendo al mismo tiempo los costes de despliegue y soporte. Una solución mágica para muchas empresas. Además, según han subrayado repetidamente los promotores de SSL VPN, al trabajar a nivel de aplicación, esta alternativa permite un control más preciso de los recursos a los que un determinado usuario está autorizado a acceder, proporcionándole a través del proxy SSL, los privilegios corporativos según su perfil.

Frente a toda esta sencillez, el acceso remoto IPSec resulta, en el mejor de los casos, difícil de desplegar cuando existen grandes cantidades de usuarios o si hay múltiples empresas y gateways implicados, algo inevitable en entornos extranet. No obstante, IPSec, cuyo funcionamiento se produce en el nivel de red, presenta importantes ventajas cuando de lo que se trata es de realizar conexiones LAN to LAN a este nivel, permitiendo que la

experiencia del usuario sea la misma que si estuviera ubicado en la propia LAN a la que accede. Además, sus restricciones respecto de los dispositivos cliente soportados, un inconveniente para proporcionar un acceso remoto más abierto, supone una ventaja en determinados aplicaciones, al elevar en cierto modo la seguridad del acceso.

Así, el hecho de que sobre los dispositivos sea necesario desplegar un agente específico de forma permanente, limita los accesos a aquellos sistemas gestionados corporativamente, evitando de antemano potenciales brechas en la seguridad de la red corporativa, que pueden abrirse, por ejemplo, cuando los usuarios trabajan desde estaciones de uso público.

Entre las ventajas de IPSec también se encuentra su capacidad de trabajar con todo tipo de aplicaciones y recursos de la empresa, incluidos los heredados, sin necesidad de instalar soluciones adicionales. SSL VPN, por sí mismo, sólo brinda acceso a aquellos dotados de soporte Web, aunque puede extenderse a cualquier recurso a través de productos software añadidos. Tampoco permite el acceso a estaciones de trabajo, ni soporta tráfico de voz ni streaming. Teniendo en cuenta estas limitaciones de SSL, IPSec, debido a su capacidad de distribuir conectividad completa a nivel de red, se convierte, según los expertos, en la mejor alternativa para conectar múltiples redes privadas. Resulta también especialmente indicada cuando se trata de programas que requieren una comunicación automatizada en ambos sentidos.

Como se ha dicho, existe ya un cierto consenso en conceder a cada alternativa un hueco en la empresa por derecho propio, dejando en manos de las IPSec VPN las conexiones sitio a sitio y en las de SSL VPN el acceso remoto a través de Internet. Zanjando de alguna forma la polémica, dada la influencia de sus acciones, marcas importantes como Cisco han asumido enfoques estratégicos que demuestran su coincidencia con la idea de que en la empresa existe un espacio para cada una de estas tecnologías incorporando ambas alternativas en su oferta.

Resumiendo este apartado, se van a mostrar las principales ventajas y desventajas que ofrecen IPSec y SSL/TLS, así como sus aplicaciones y uso en otras tecnologías en la actualidad:

− Ventajas de SSL/TLS:

• Ofrece confidencialidad (cifrado simétrico), autenticación del servidor y del cliente (este último opcional) e integridad de los mensajes brindando unos niveles de seguridad excelentes que permiten el establecimiento de extranets con confianza y tranquilidad

• SSL constituye la solución de seguridad implantada en la mayoría de los servidores Web que ofrecen servicios de comercio electrónico ya que ofrece un canal seguro para el envío de números de tarjeta de crédito.

• Bajos costes de mantenimiento y no requiere mantenimiento en los clientes además de tener una buena interoperabilidad

• Se pueden encontrar en Internet numerosas implementaciones de libre distribución para implementar redes privadas virtuales basadas en SSL/TLS.

• Muchas implementaciones de VPN basadas en SSL/TLS ofrecen mecanismos para defenderse frente a ataques del tipo “man in the middle” y ataques de denegación de servicio (DoS)

− Desventajas de SSL/TLS:

• Protección parcial, ya que garantiza la integridad y confidencialidad de los datos únicamente durante el tránsito de los mismos, pero no los protege una vez recibidos por el servidor. Por tanto, un hacker podría manipular tranquilamente un servidor por lo expuesto anteriormente.

• No es una solución totalmente transparente para el usuario final.

• En transacciones electrónicas SSL/TLS garantiza la confidencialidad extremo a extremo pero una vez finalizada

la conexión, el vendedor posee todos los datos del comprador, así como su número de tarjeta de crédito. El vendedor podría almacenar esos datos y el cliente estaría expuesto a cualquier tipo de fraude por parte de toda persona que tuviera acceso a dicha información..

• En transacciones electrónicas SSL/TLS no garantiza la integridad de la información una vez finalizada la conexión, por lo que el vendedor podría modificar esos datos, por ejemplo, cobrando más al cliente.

• En ciertas transacciones electrónicas SSL/TLS el cliente no necesita autenticarse, por lo que una persona con acceso a números de tarjeta de crédito robados podría realizar cualquier tipo de compra por Internet. Este es precisamente el tipo de fraude más común y que causa mayores pérdidas a las compañías de crédito.

• En transacciones electrónicas del tipo SSL/TLS, una vez finalizada la compra, no existe ningún tipo de comprobante de compra por lo que cualquier protesta posterior carecerá de medios para su confirmación.

Tampoco existe ningún documento firmado por lo que tanto el cliente como el vendedor o el banco podrían negar su participación en la compra sin que existiera la posibilidad de probar lo contrario.

• Tiene problemas con algunos protocolos de la capa de transporte y con ciertas aplicaciones, sobre todo con protocolos no orientados a conexión.

• Interceptando los mensajes de “Client_Hello” y “Server_Hello”, es relativamente sencillo interceptar los primeros mensajes intercambiados en el mecanismo de Handshake y manipularlos para lograr que la sesión SSL se establezca en condiciones óptimas para su posterior escucha, haciendo creer al cliente que, por ejemplo, el servidor sólo soporta la versión 2.0 del protocolo, longitudes de clave de 40 bits o que el único algoritmo común es el DES.

• No soporta tráfico de voz ni streaming.

• No soporta multicast

− Aplicaciones en la Actualidad de SSL/TLS:

• Se usa en la mayoría de los casos junto a HTTP para formar HTTPS. HTTPS es usado para asegurar páginas Web para aplicaciones de comercio electrónico, utilizando certificados de clave pública para verificar la identidad de los extremos.

• La mayoría de las aplicaciones son versiones seguras de programas que emplean protocolos que no lo son. Hay versiones seguras de servidores y clientes de protocolos como el http, nntp, ldap, imap, pop3.

• SSL/TLS se puede utilizar en aplicaciones como: Applets de Java, controles ActiveX, Microsoft FrontPage o Adobe PageMill, o FileMaker Pro de Claris...

• Librerías multiplataforma como OpenSSL.

− Ventajas de IPSec:

• IPSec ofrece confidencialidad (cifrado), autenticación e integridad.

• Basado en estándares y muy adecuado para tráficos totalmente IP.

• IPSec está debajo de la capa de transporte, por lo que resulta transparente para las aplicaciones.

• IPSec puede ser transparente a los usuarios finales.

• Compatible con la infraestructura de claves públicas.

• Provee un alto grado de encriptación a bajo nivel.

• Estándar abierto del sector. IPSec proporciona una alternativa de estándar industrial abierto ante las tecnologías de cifrado IP patentadas. Los administradores de la red aprovechan la interoperabilidad resultante.

− Desventajas de IPSec:

• En la mayoría de los casos, su implementación necesita modificaciones críticas al kernell.

• IPSec no es seguro si el sistema no lo es. Los gateways de seguridad deben estar en perfectas condiciones para poder confiar en el buen funcionamiento de IPSec

• Puede ser vulnerable a ataques del tipo “man in the middle” y de denegación de servicio (DoS).

• Es un protocolo complejo de entender, su configuración es complicada y además requiere una configuración minuciosa en el cliente. Su administración suele ser lenta y complicada.

• Tiene un alto coste de implementación y de mantenimiento.

• IPSec autentica máquinas, no usuarios: el concepto de identificación y contraseña de usuarios no es entendido por IPSec, si lo que se necesita es limitar el acceso a recursos dependiendo del usuario que quiere ingresar, entonces habrá que utilizar otros mecanismos de autenticación en combinación con IPSec.

• Problemas con traducción de direcciones NAT (Network Address Translation).

• Diferentes implementaciones incompatibles entre si.

• Necesita del uso de muchos puertos y protocolos en el sistema hardware que lo implemente (router, firewall,...).

de distintos proveedores pueden ser

− Aplicaciones en la Actualidad de IPSec:

• Desarrolla y depura aplicaciones web ASP.NET en Delphi 2005 mediante Cassini, Delphi, JBuilder 2006, Beta Visual Studio 2006 Desarrollo de aplicaciones Web y Windows con Visual Basic 2005.

• Comercio electrónico de negocio a negocio pero con menos influencia que SSL/TLS.

• El proyecto FreeS/WAN es la primera implementación completa y de código abierto de IPsec para Linux.

• En las redes IPv6 será obligatoria la implementación de IPSec.

6.7 Parte Práctica

Esta parte es relativa a OPENVPN, no es obligatoria y quizás no todos podáis hacerla, está incluida para quienes cuenten con los medios y recursos para ello.
Podéis intentarlo creando dos maquinas virtuales distintas

Instalamos open vpn:
sudo aptitude install openvpn

Túnel sin seguridad mediante OpenVPN:
*En A: openvpn --remote ippubB --dev tun0 --ifconfig ipvirtualA ipvirtualB [--verb 9]
*En B: openvpn --remote ippubA --dev tun0 --ifconfig ipvirtualB ipvirtualA [--verb 9]
*Probar: ping ipvirtualB (en A); ping ipvirtualA (en B)

La comunicación entre A y B ocurre por defecto en el puerto 1194 UDP. Se use en vez de TCP porque UDP es más fuerte frente ataques DoS y escaneos de puertos (UDP es no conectivo, no fiable, no orientado a conexión). En vez de “ippubX”, se podría poner el nombre DNS correspondiente.Para servidores caseros en los cuales la ip es dinámica,se puede utilizar un servicio gratuito de DNS dinámico,como http://www.dyndns.com ó

http://www.no-ip.com
Normalmente, las ips virtuales se eligen del rango 10.0.0.0/8, ya que las LANs reales suelen tener el 192.168.0.0/16

Túnel cifrado con claves estáticas mediante OpenVPN:
*Generate a static key (en A o B, da igual): openvpn --genkey --secret static.key
*Copy the static key to both A and B, over a pre-existing secure channel (ssh, for example).
*En A: openvpn --remote ippubB --dev tun0 --ifconfig ipvirtualA ipvirtualB --secret static.key
*En B: openvpn --remote ippubA --dev tun0 --ifconfig ipvirtualB ipvirtualA --secret static.key
*Asegurarse que el puerto Udp 1194 del servidor esté abierto,y que la interfaz tunX no sea bloqueada en ambo
*Probar el túnel. Por ejemplo, en A se puede hacer un ping: ping ipvirtualB (y viceversa en B)

La configuración de claves estáticas es la configuración segura más simple, y es ideal para VPNs punto a punto. No obstante, tiene varios inconvenientes:

*Sólo permite conexiones punto a punto: un cliente, un servidor.
*La clave secreta ha de existir en forma de texto plano en cada extremo VPN
*La clave secreta debe ser intercambiada usando un canal seguro preexistente
*El hackeo de la clave permite el descifrado de no sólo las sesiones futuras sino las pasadas

También se podrían haber utilizado ficheros de configuración (con el parámetro –config /ruta/arxiu de openvpn ...o incluso escribiendo /ruta/arxiu a secas -si no se especifica ningún parámetro más-). Una vez creada y copiada la clave (pasos 1 y 2), hacer:

*Fichero configuración A:
dev tun0
remote ippubB
ifconfig ipvirtualA ipvirtualB
secret static.key
#comp-lzo (para usar compresión)
*Fichero configuración B:
dev tun0
remote ippubA
ifconfig ipvirtualB ipvirtualA
secret static.key
#comp-lzo (para usar compresión)
*Probar el túnel de la misma manera.

Teoría de certificados:
Un certificado digital es un documento digital mediante el cual un tercero confiable (una autoridad de certificación) garantiza la vinculación entre la identidad de un sujeto o entidad y su clave pública. Puede ser usado, por ejemplo, para verificar la firma digital de dicha entidad.

Un certificado contiene usualmente, entre otros datos:

*Nombre y datos burocráticos identificativos de la entidad certificada
*Número de serie

*Fecha de expiración
*Copia de la clave pública de la entidad certificada (utilizada para verificar su firma digital)
*Firma digital de la autoridad certificadora (de forma que el receptor pueda verificar que esta última ha establecido realmente la asociación)

En caso particular, por ejemplo, de un servidor web, el certificado que ofrece a los navegadores cuando un usuario visita su web garantiza que, durante la comunicación encriptada que realice el navegador gracias a la clave pública obtenida de este servidor web, dicho servidor es realmente la que dice ser (siempre y cuando dicho certificado venga firmado por una autoridad de certificación confiable por el cliente). Los navegadores ya vienen de serie con una lista de firmas reconocidas de varias autoridades de certificación confiables (los llamados "certificados raíz")...por eso en muchas páginas seguras no salta ningún popup extraño: porque su certificado fue firmado por una autoridad reconocida por el navegador. De hecho, el navegador comprueba varias cosas para dar por válida la conexión y comenzar la comunicación encriptada:

-El certificado obtenido no haya expirado ya
-El certificado obtenido ha sido creado por el mismo servidor web al que se está accediendo
-El certificado está firmado por alguien en el que se confía

El formato más extendido para certificados digitales es el estándar UIT-T X.509 (son los ficheros con extensión .crt).

Túnel con certificados mediante OpenVPN:
Los pasos básicos serán:
1.-Convertirnos en nuestra propia CA (generando los ficheros ca.crt y ca.key, certificado y clave RSA privada de la CA, respectivamente)

2.-Crear el par certificado/clave privada para el servidor VPN (se crearán los ficheros miserver.crt y miserver.key). Ahora sí que hablamos de servidor porque éste aceptará múltiples conexiones de diferentes clientes, a diferencia de los casos anteriores, donde sólo se podían hacer conexiones punto a punto.

3.-Crear el par certificado/clave privada para todos los clientes que se autorizarán a conectarse al servidor (se crearán los ficheros cliente1.crt y cliente1.key, cliente2.crt y cliente2.key y así)

4.-Copiar a cada cliente su par certificado/clave privada correspondiente, más el fichero ca.crt, por un medio seguro, como Ssh.

5.-Configurar el servidor y los clientes de la forma adecuada

En vez de usar OpenSSL directamente para realizar los pasos anteriores (que se podría hacer perfectamente), OpenVPN provee de unos comandos wrappers que facilitan el proceso. Los comandos concretos (realizados todos como root) a ejecutar en el servidor VPN son:

*Copiamos todos los scripts necesarios a una ubicación estándar,como puede ser /etc/openvpn, y nos situamos:
cp -r /usr/share/openvpn/easy-rsa/2.0 /etc/openvpn
cd /etc/openvpn/easy-rsa

*Inicializamos las variables de entorno necesarias para realizar el proceso sin problemas:
source ./vars

En realidad, el fichero vars no es más que un script que se puede editar sin problemas. Por ejemplo, se pueden establecer las respuestas por defecto a las preguntas que realizarán los comandos posteriores, si se editan las entradas KEY_* del final del fichero, tales como KEY_COUNTRY, KEY_ORG, KEY_EMAIL, que serán utilizadas para crear los pares OpenSSL. También es interesante el valor KEY_SIZE, y de KEY_DIR...

*Borramos los posibles certificados y claves viejas que pudieran existir de procesos anteriores:
./clean-all
*Nos convertimos en CA, creando un par certificado/clave_privada válido para 10 años por defecto:
./build-ca
Obtendremos los ficheros ca.crt y ca.key (certificado y clave privada de la CA, respectivamente) dentro de la subcarpeta “keys”. Un comando alternativo al anterior es ./pkitool --initca
*Generamos el par certificado/clave para nuestro servidor VPN:
./build-key-server miserver

Aparecerán una serie de preguntas, que podemos responder con lo que deseemos o conformarnos con los valores por defecto. Obtendremos los ficheros miserver.crt y miserver.key (certificado y clave privada del servidor VPN, respec).
Un comando alternativo al anterior es ./pkitool --server miser. El fichero miserver.crt está firmado por la CA que es el propio servidor. No obstante, si se desea firmar el certificado del servidor por otra CA, el comando anterior también genera el fichero miserver.csr, el cual es una petición de firma de certificado que se deberá enviar a la CA elegida para que ésta la firme y devuelva el correspondiente server.crt

*Generamos los pares certificado/clave para cada uno de los clientes VPN a los que deseamos dar acceso:
./build-key cliente1
./build-key cliente2

Obtenemos los ficheros cliente1.crt (certificado firmado por la CA del propio servidor) y cliente1.key, su clave privada. Un comando alternativo al anterior es ./pkitool cliente1. Si deseáramos generar más certificados de clientes en otro momento, deberemos ejecutar antes de ./build-key el comando source ./vars. Si se desea que los pares generados estén protegidos por contraseña, se puede utilizar el comando ./build-key-pass cliente1

*Generamos además los parámetros Diffie-Hellman para el servidor,necesarios para que el intercambio secreto de claves entre dos partes que no han tenido contacto previo se realice correctamente
./build-dh
Obtendremos el fichero dh1024.pem

*Copiar los ficheros miserver.crt, miserver.key, ca.crt y dh1024.pem a la carpeta /etc/openvpn local
cp keys/ca.crt /etc/openvpn
cp keys/server.{key,crt} /etc/openvpn
cp keys/dh1024.pem /etc/openvpn
*Copiar (mover) los ficheros cliente1.crt, cliente1.key y ca.crt a la carpeta /etc/openvpn de “cliente1” por un canal seguro (como Ssh, un lápiz Usb, etc). Hacer lo propio con los demás clientes.
*Crear el fichero de configuración del servidor:
local ippubServidor (el servidor sólo será funcional en la interfaz real asociada a dicha ip)
dev tun0
ca ca.crt (la ruta absoluta no es necesaria ponerla si está en la misma carpeta)
cert miserver.crt
key miserver.key #este fichero debería guardarse en secreto!

dh dh1024.pem
user nobody (el servidor se ejecutará con privilegios del usuario y grupo “nobody”...)
group nogroup (...esto se hace por seguridad, ya que “nobody” es un usuario casi sin permisos)
server 10.8.0.0 255.255.255.0 (permite asignar a los clientes que se conencten una ip dentro del rango de red especificado -a modo de rudimentario servidor Dhcp- , dentro del cual el propio servidor automáticamente se asignará siempre la primera ip -”10.8.0.1” en el ejemplo-. Si se utilizan dispositivos Tap en vez de Tun, la directiva es server-bridge)
ifconfig-pool-persist ficheroips.txt (contiene la lista de ips virtuales asignadas a los distintos clientes. El formato de las líneas del fichero es “commonname,ip” y se regenera automáticamente en el arranque y parada del servicio, y también cada 10 minutos -esto se puede cambiar añadiendo un segundo parámetro a esta directíva indicando el número de segundos. Si se indica 0 segundos, el fichero será tratado como de sólo lectura)
persist-key (no se vuelven a leer las claves en un reinicio del servidor -aumenta resistencia del link-)
persist-tun (no cierra y reabre el dispositivo tun en un reinicio del servidor - “ “ “ “)
client-to-client
(permite que los clientes conectados al servidor se puedan ver entre sí)
keepalive 10 120 (emite un ping al cliente a los 10s de inactividad, y si a los 120s se continúa sin recibir nada, se reabre la conexión. Esta opción incluye las opciones “ping” y “ping-restart”, respectivamente. También está “ping-exit”)

*Iniciar el servidor:
service openvpn start
Este script buscará todos los ficheros *.conf que haya en /etc/openvpn y lanzará un servidor por cada uno de ellos. Si existiera en esa carpeta algún fichero *.sh, se ejecutaría antes. La opción “reload” lanza una señal SIGHUP y la señal “reopen” lanza una señal SIGUSR1.
*Crear el fichero de configuración del cliente:
remote ippubServidor 1194
dev tun0
ca ca.crt
cert cliente1.crt
key cliente1.key
client (equivalente a tls-client más pull)
persist-key
persist-tun

*Probar de la manera usual (interesante probar el “traceroute”)
*Si se deseara quitar el acceso a un cliente concreto, lo que se puede hacer es (como root):
source ./vars
./revoke-full cliente1

*De forma opcional, se puede aumentar todavía más la seguridad creando una llave TLS-AUTH adicional para todas las negociaciones SSL/TLS para la verificación de la integridad, haciendo que cualquier paquete UDP que no posea dicha clave sea bloqueado. De esta manera nos protegeremos de ataques DoS, escaneo de puertos...y ahorramos trabajo al servidor porque si esto falla al intentar la autenticación, corta la conexión. Por defecto esta clave estará encriptada mediante AES-256bits-CBC

openvpn –genkey –secret ta.key

En la configuración del servidor deberemos escribir la línea tls-auth ta.key 0 (0 de incoming) y en el cliente la

línea tls-auth ta.key 1 (1 de outcoming)

*Si se tiene activado el firewall, vigilar de tener abierto el puerto 1194/udp (o el que se utilice) y de habilitar todo el tráfico que vaya dirigido a o desde la interfaz tunX, así:

iptables -A INPUT -p udp –dport 1194 -j ACCEPT
iptables -A INPUT -i tun+ -j ACCEPT
iptables -A OUTPUT -o tun+ -j ACCEPT
iptables -A FORWARD -i tun+ -j ACCEPT (si se quiere acceder a la LAN de detrás -caso siguiente-)
iptables -A FORWARD -o tun+ -j ACCEPT (si se quiere acceder a la LAN de detrás -caso siguiente-)

*Permitir el acceso a la LAN del servidor VPN:
Supongamos que tenemos esta configuración de red (se supone que 89.09.87.66 y 12.34.56.78 son ips públicas otorgadas por un ISP):

Cliente VPN
eth0=89.09.87.65
tun0=10.0.0.2
Servidor VPN
eth0=12.34.56.78/DynDns
tun0=10.0.0.1
eth1=192.168.0.1
3r Ordenador
eth0=192.168.0.2

Para permitir al cliente acceder a la red LAN del servidor , hay que hacer tres cosas:

1.-En el servidor (y en el cliente también si se deseara acceder también a su LAN si tuviera alguna por detrás, para conseguir enlazar LAN con LAN) hay que activar el IP Fowarding para que las peticiones que le lleguen por la interfaz tunX (asociada a la interfaz externa, en este caso, eth0) le pasen internamente a la interfaz interna (en este caso, eth1) y de allí al ordenador de su LAN deseado (es decir, que funcione como un router normal y corriente):
echo 1 > /proc/sys/net/ipv4/ip_forward (o bien sysctl -w net.ipv4.ip_forward=1)
En ambos casos esta configuración es temporal hasta que la máquina servidora se reinicie. Si se desea hacer el forward permanente, hay que escribir la siguiente línea en el archivo /etc/sysctl.conf: net.ipv4.ip_forward=1 y activar dicho cambio haciendo sysctl -p /etc/sysctl.conf (o reiniciando la máquina)

2.-Configurar el cliente añadiendo una ruta a su tabla de rutas que diga que todos los paquetes que vayan a parar a la red interna 192.168.0.0 tengan que pasar por el servidor VPN
ip route add 192.168.0.0/24 via 10.0.0.1
Esto mismo se podría haber hecho de forma automática si se añade al archivo de configuración del cliente la línea route 192.168.0.0 255.255.255.0
Si detrás del cliente también hubiera una LAN a la que se desea acceder (es decir, que el cliente también hiciera de servidor de su propia LAN), se debería de hacer un paso similar en el servidor (que estaría haciendo de cliente, en este caso). Es decir, , la directiva “route xxx” se debería escribir en el fichero de configuración del servidor, especificando la ip de la red privada del cliente.
Otra forma alternativa de hacer lo mismo es, en vez de modificar el fichero de configuración del cliente (que a veces puede ser inaccesible), modificar el fichero de configuración del servidor de manera que éste sea capaz de indicar determinados valores que se desean transmitir a los clientes, como por ejemplo el especificado con

la directiva “route”. De esta manera, no hace falta escribir explícitamente en el fichero del cliente la directiva que se desea sino que desde el propio servidor se le puede indicar (no sirve para todas, no obstante). En concreto, para indicar el ruteo de los clientes se podría establecer en el el archivo de configuración del servidor lo siguiente:
push “route 192.168.0.0 255.255.255.0”
3.-Habiendo hecho los dos primeros pasos, ya tenemos el tráfico tunelado que va desde el cliente hasta el “3r ordenador” (se puede observar esto si se ejecuta un analizador de tráfico en este 3r ordenador), pero la comunicación todavía no es completa porque este 3r ordenador no es capaz de saber a dónde tiene que enviar las respuestas. Faltaría añadirle al 3r ordenador (de hecho, a cada uno de los ordenadores de la LAN interna del servidor) una ruta dentro de su tabla de rutas que diga que todos los paquetes que vayan a parar al cliente VPN tengan que pasar por el servidor:
ip route add 10.0.0.2/32 via 192.168.0.1
O más general, para cualquier cliente VPN posible que se pudiera conectar:
ip route add 10.0.0.0/24 via 192.168.0.1
Las rutas establecidas de esta manera (con el comando “ip route”, tanto en el punto 2 como en éste) son temporales. Para hacer que aparezcan fijas en el ordenador, existen varios métodos, pero tal vez el más sencillo es utilizar la directiva up de los ficheros de configuración de OpenVPN, la cual sirve para indicar un shell script que se ejecutará en el momento de activar la interfaz tunX, con lo que en este shell script podríamos escribir dicho comando “ip route”
Lo más probable es que nos encontremos con que nuestro servidor VPN no está conectado directamente a la red Internet (es decir, él no tiene ip pública propiamente), ni tan siquiera tenga dos tarjetas de red: lo más habitual es tener un router, de esta manera:
Cliente VPN
eth0=89.09.87.65
tun0=10.0.0.2
Router
eth0=12.34.56.78/DynDns
eth1=192.168.0.1
Servidor VPN
eth0=192.168.0.123
tun0=10.0.0.1
3r Ordenador
eth0=192.168.0.2
En este caso, la configuración sería muy similar a la explicada, pero además deberíamos configurar el router para que hiciera un “port forwarding” del puerto 1194. Es decir, indicarle que todas las peticiones dirigidas a ese puerto las redireccionara al servidor VPN, en este caso, con la ip 192.168.0.123, de forma que el router sea en este caso un mero transmisor “correveydile”. Esto se hace de forma muy sencilla mediante el panel de control via web de que dispone el router (si es que dispone de esta opción, claro...depende del modelo).

También existe la posibilidad de que el propio router ya incorpore dentro de sí mismo un servidor VPN, con lo que nos podríamos ahorrar la instalación y configuración del servidor OpenVPN en un PC, excepto para generar los certificados y claves, los cuales se deberán copiar en la configuración del router.

*Más parámetros de OpenVPN:
Consultar el manual para más información: man openvpn
--port 1194 : el puerto a usar por OpenVPN
--proto udp : el protocolo a usar por OpenVPN (la otra opción es poner en un extremo tcp-server y en el otro tcp-client)
--show-ciphers : muestra los algoritmos de cifrado que puede utilizarse en el túnel. Por defecto se usa

128-Blowfish.
--cipher BF-CBC : sirve para especificar el algoritmo de cifrado deseado (se ha de poner en ambos extremos)
--shaper 10000 : establece el máximo ancho de banda en bytes/s para el túnel
--max-clients 30 : establece el máximo de clientes concurrentes que un servidor acceptará
--up /ruta/shell/script/a/ejecutar/al/crear/el/tunel
--down /ruta/shell/script/a/ejecutar/al/destruir/el/tunel

Biografía y agradecimientos

De Cuaderno Red de Cátedras Telefónica ->Sistemas Biométricos creado por: Carlos Manuel Travieso González
Marcos del Pozo Baños
Jaime Roberto Ticay Rivas
Antonio Villalon Huerta http://www.rediris.es/cert/doc/unixsec/node14.html
BY MICHAEL SCHWARTZKOPFF WWW.LINUX- MAGAZINE.ES
http://dns.bdat.net/seguridad_en_redes_inalambricas/x80.html María Dolores Cano Baños
http://karenmarce.blogspot.es/1307915040/ Natalio López Martínez
http://es.tldp.org/Manuales-LuCAS/GARL2/garl2/x-087-2-ppp.authentication.html
http://dominiohacker.com/autentificacion-en-redes-wifi-ii-eap-ttls-peap-eap-fast-327/
http://dtoapanta-no-shura.blogspot.com.es/
Wikipedia

Agradecerles a estos autores sus contribuciones, la autoría de sus textos les pertenece completamente y me permito hacerles un guiño a mis amigos, a los viejos que siempre estuvieron ahí y a los nuevos, (ellos saben quienes son (Malka, Kalambre,Red,Uka,Mari,Fanta,Joker,Epsylon,), por leer mis temas, animarme en mis locuras, apoyarme y compartir conmigo conversaciones que no tienen muchos adeptos, pero sobretodo por acompañarme en el solitario camino hacia el conocimiento.