PROTOTIPO DE ADMINISTRADOR DE REDES PRIVADAS VIRTUALES USANDO SOFTWARE LIBRE

JOSE ARLEY LOPEZ LARGO
Cod 18617444

MARIA ISABEL GOMEZ ESTRADA
Cod 25173856

UNIVERSIDAD TECNOLOGICA DE PERERIA
INGENIERIA DE SISTEMAS Y COMPUTACION
FACULTAD DE INGENIERÍAS
SEMILLERO DE INVESTIGACIÓN PULPA
DICIEMBRE DE 2006
PEREIRA

TABLA DE CONTENIDO

Pag.

1. PRELIMINARES ***35***

1.1. TITULO DEL PROYECTO **35**

1.2. DEFINICION DEL PROBLEMA **35**

1.2.1. Antecedentes 35

1.2.2. Formulación 36

1.2.3. Descripción del problema 37

1.3. JUSTIFICACIÓN **37**

1.4. OBJETIVOS **38**

1.4.1. Generales 38

1.4.2. Específicos 39

1.5. MARCO TEÓRICO **39**

1.6. DISEÑO METODOLÓGICO **42**

1.7. PERSONAS QUE PARTICIPAN EL EN PROYECTO **43**

2. ANTECEDENTES ***44***

2.1 HISTORIA DE LAS VPN **44**

2.1.1. Frame Relay: Empaquetamiento de la información 45

2.1.2. ATM y convergencia de redes de voz y datos 45

2.1.3. Redes Privadas Virtuales 46

2.2. APLICACIONES DE LAS REDES PRIVADAS VIRTUALES **47**

2.3. CARACTERÍSTICAS DE UNA RED PRIVADA VIRTUAL (VPN) **49**

2.4. IMPLEMENTACIÓN DE LAS REDES PRIVADAS VIRTUALES **50**

2.4.1. Implementación de VPN por Hardware 51

2.4.2. Implementación de VPN por Software 52

2.4.3. Tabla comparativa entre la Implementación de una VPN por Software y Hardware 52

2.5. CARACTERÍSTICAS PRINCIPALES A LA HORA DE MONTAR UNA VPN **55**

2.5.1. La Seguridad de la conexión 55

2.5.2. La Seguridad del servidor 55

2.5.3. Autenticación de Usuarios 56

2.6. PRINCIPALES PROTOCOLOS EMPLEADOS EN LA CONSTRUCCIÓN DE VPNS **56**

2.6.1. IPSec 56

2.6.2. PPTP: 58

2.6.3. L2TP (Layer 2 Tunneling Protocol) 60

2.6.4. SSH 61

2.6.5. SSL/TLS (Secure Socket Layer) (Transport Layer Secure) 62

3. APLICACIONES EXISTENTES *64*

3.1. DESCRIPCIÓN DE LOS PRODUCTOS DE SOFTWARE **64**
3.1.1. FreeS/WAN (Free Secure Wide-Area Networking): 64
3.1.2. StrongSwan: 65
3.1.3. OpenS/WAN: 66
3.1.4. OpenSSH: 67
3.1.5. Stunnel (Universal SSL Wrapper): 67
3.1.6. OpenVPN 68

3.2. ¿QUE TECNOLOGÍA EMPLEAR? **70**
3.2.1. IPSec vs SSL 71
3.2.1.2. SSL 72

3.3. ANÁLISIS COMPARATIVO ENTRE OPENVPN Y APLICACIONES VPN SOBRE IPSEC **73**

3.4. CONCLUSIONES DEL ANALISIS **74**

4. EJEMPLO APLICADO *76*

4.1. CONFIGURACIÓN TRADICIONAL DE OPENVPN **76**
4.1.1. INSTALACIÓN DE LAS HERRAMIENTAS 77
4.1.2. CONFIGURACIÓN DE LA RED 77
4.1.3. PASOS PARA LA CONFIGURACIÓN DE LA VPN 78
4.1.3.1. Creación de los Certificados y Claves RSA 79
4.1.3.2. Creación del Certificado y la Clave para el Servidor 80
4.1.3.3. Creación del Certificado y la Clave para el Cliente 81
4.1.3.4. Creación de la Clave de Diffie-Hellman 81
4.1.3.5. Firmar los Certificados 81
4.1.3.6. Distribuir las Claves y los Certificados 82
4.1.3.7. Archivo de Configuración para el Servidor 82
4.1.3.8. Archivo de Configuración para el Cliente 83
4.1.4. CONFIGURACIÓN DEL FIREWALL 85
4.1.5. ARRANCAR EL SERVIDOR Y LOS CLIENTES 85
4.1.6. REALIZAR PRUEBAS DE CONECTIVIDAD 86

4.2. ANALISIS Y DISEÑO DE LA APLICACION **87**
4.2.1. Diagrama de Clases 88
4.2.2. Diagrama de Casos de Uso 89
4.2.3. Diagramas de Secuencia 98
4.2.4. Diagrama de Secuencia de Ventanas 102
4.2.4.1. Descripción de la Secuencia de Ventanas 103
4.2.5. Diagrama de Distribución 118

4.3. MANUAL **119**

5. CONCLUSIONES *127*

5.1. RECOMENDACIONES **128**

5.2. APORTES **129**

GLOSARIO

3Com/Primary Access Hace parte de el conjunto de empresas para establecer túneles VPNs a través de Internet empleando PPTP

Acceso Remoto Permite a un usuario que se encuentra en un punto geográficamente distante, conectarse a la red por medio de una conexión telefónica. Una vez conectado, puede hacer lo mismo que si estuviera trabajando en un equipo conectado físicamente a la red.

ADSL (Asymmetric Digital Subscriber Line) Línea de Abonado Digital Asimétrica. Es una tecnología de acceso a Internet de banda ancha, lo que implica capacidad para transmitir más datos, lo que, a su vez, se traduce en mayor velocidad. Esto se consigue mediante la utilización de una banda de frecuencias más alta que la utilizada en las conversaciones telefónicas convencionales (300-3.400 Hz) por lo que, para disponer de ADSL, es necesaria la instalación de un filtro (llamado splitter o discriminador) que se encarga de separar la señal telefónica convencional de la que usaremos para conectarnos con ADSL.

AES (Advanced Encryption Standard) Es un esquema de cifrado por bloques adoptado como un estándar de cifrado por el gobierno de los Estados Unidos. Se espera que sea usado en el mundo entero y analizado exhaustivamente, como fue el caso de su predecesor, el Data Encryption Standard (DES).

Agentes Móviles Los agentes móviles son programas de software capaces de viajar por redes de computadoras, como Internet, de interactuar con hosts, pedir información a nombre de un usuario y regresar a su lugar de origen una vez que ha realizado las tareas especificadas por un usuario.

AH (Authentication Header) Cabecera de Autenticación Se trata de una nueva cabecera que se obtiene de la básica IP y que se añade a los resúmenes criptográfios ("hash") de los datos e información de identificación.

Algoritmos de Cifrado Un algoritmo criptográfico es una función matemática que junto con una clave (un número, palabra o frase) permite el cifrado y descifrado de la información.

El concepto de cifrado digital es muy sencillo: dado un mensaje en claro, es decir, mensaje reconocible, si se le aplica un algoritmo de cifrado se generará como resultado un mensaje cifrado que sólo se podrá descifrar por aquellos que conozcan el algoritmo utilizado y la clave correspondiente.

Existen dos tipos de cifrado: el cifrado simétrico (o de clave secreta) y el asimétrico (o de clave pública).

Ancho de Banda Capacidad máxima de transmisión, que se mide por bits por segundo.

ARM Una de las arquitecturas de hardware más comúnmente usadas en la construcción de dispositivos móviles y sistemas embebidos. Se basa principalmente en arquitectura RISC aunque con algunas características CISC y provee bajo consumo de energía combinado con alto desempeño.

Arquitecturas Cliente/Servidor Esta arquitectura consiste básicamente en que un programa, el Cliente informático realiza peticiones a otro programa, el servidor, que le da respuestas.

Aunque esta idea se puede aplicar a programas que se ejecutan sobre una sola computadora es más ventajosa en un sistema multiusuario distribuido a través de una red de computadoras.

En esta arquitectura la capacidad de proceso está repartida entre los clientes y los servidores, aunque son más importantes las ventajas de tipo organizativo debidas a la centralización de la gestión de la información y la separación de responsabilidades, lo que facilita y clarifica el diseño del sistema.

Ataques de REPLAY Un ataque de REPLAY es una forma de ataque de red, en el cual una transmisión de datos válida es maliciosa o fraudulentamente repetida o retardada. Es llevada a cabo por el autor o por un adversario que intercepta la información y la retransmite, posiblemente como parte de un ataque enmascarado.

El ataque de replay pretende capturar información y posteriormente reenviarla con el objetivo de falsificar la identidad de uno de los lados. Es un hecho muy conocido que el intercambio de claves DH de manera primitiva adolece de ser atacado por un ataque de replay, sin embargo, esto puede evitarse con una marca secuencial o una marca de tiempo. Hoy día ninguna aplicación que use el esquema de intercambio de claves DH de manera adecuada se ve afectada por este ataque.

ATM Modo de Transferencia Asíncrono Tecnología multiservicio de banda ancha capaz de soportar datos, voz, video e imágenes sobre la misma infraestructura de red.

Autenticación Proceso mediante el cual el sistema intenta asegurar que la persona que está iniciando sesión es la misma para quien se emitió una cuenta.

Balanceo de Cargas El balance o balanceo de carga es un concepto usado en informática que se refiere a la técnica usada para compartir el trabajo a realizar entre varios procesos, ordenadores, discos u otros recursos. Está íntimamente ligado a los sistemas de multiprocesamiento, o que hacen uso de más de una unidad de procesamiento para realizar labores útiles.

El balance de carga se mantiene gracias a un algoritmo que divide de la manera más equitativa posible el trabajo, para evitar los así denominados cuellos de botella que es el objetivo del multiprocesamiento.

Blowfish Es un codificador de bloques simétricos, diseñado por Bruce Schneier en 1993 e incluido en un gran número de conjuntos de codificadores y productos de cifrado. Es un algoritmo de uso general, intentando reemplazar al antiguo DES y libre de problemas asociados con otros algoritmos. Al mismo tiempo, muchos otros diseños eran propietarios, patentados o los guardaba el gobierno, pero éste no cuenta con patentes y se encuentra a disposición de dominio público, y puede ser usado libremente por cualquiera".

Certificados Digitales El artículo 17-G del Código Fiscal de la Federación describe los certificados digitales de la siguiente manera:

Documento electrónico, mensaje de datos u otro registro que asocia una clave pública con la identidad de su propietario, confirmando el vínculo entre éste y los datos de creación de una Firma Electrónica Avanzada o de un sello digital. Además de la clave pública y la identidad de su propietario.

chroot Un chroot en un sistema operativo Unix es una operación que cambia el directorio raíz, afectando solamente al proceso actual y a sus procesos hijos. "chroot" se refiere a la llamada de sistema chroot(2) o al programa ejecutable chroot(8).

Un programa que se ejecuta en un entorno de directorio raíz cambiado, no puede acceder a archivos fuera de ese directorio. Esto provoca un conveniente entorno seguro para probar programas sospechosos o peligrosos. También es una forma simple de mecanismo de jaula.

Cifrado Técnica que codifica la información de un modo que hace difícil o imposible su lectura, y la decodifica de modo que pueda ser leída nuevamente.

CHAP (Challenge Handshake Authenticacition Protocol) Es un protocolo de autenticación por desafío mutuo. Es un método de autenticación remota o

inalámbrica. Diversos proveedores de servicios emplean CHAP. Este método autentifica a un usuario frente a un ISP, es empleado por servidores accesibles vía PPP. CHAP verifica periódicamente la identidad del cliente remoto usando un intercambio de información de tres etapas. Esto ocurre cuando se establece el enlace inicial y puede pasar de nuevo en cualquier momento de la comunicación. La verificación se basa en un secreto compartido (como una contraseña).

Cliente Remoto La tecnología de clientes remotos facilita que un usuario pueda trabajar en una computadora, a través de su escritorio gráfico, desde otra computadora o Terminal situado en otro lugar, gracias a una red de telecomunicaciones.

Permite la centralización de aquellas aplicaciones que generalmente se ejecutan en entorno de usuario (por ejemplo, procesador de textos o navegador). De esta manera, dicho entorno de usuario se transforma en meros terminales de entrada/salida. Los eventos de pulsación de teclas y movimientos de ratón se transmiten a un servidor central donde la aplicación los procesa como si se tratase de eventos locales. La imagen en pantalla de dicha aplicación es retornada al Terminal cliente cada cierto tiempo. De ahí la idea de “cliente remoto”.

Contraseña (Password) o Clave Una contraseña o clave, es una forma de autenticación que utiliza información secreta para controlar el acceso hacia algún recurso. La contraseña normalmente debe mantenerse en secreto ante aquellos a quien no se les permite el acceso. Aquellos que desean acceder a la información se les solicita una clave; si conocen o no conocen la contraseña, se concede o se niega el acceso a la información según sea el caso.

Cygwin Es una colección de herramientas desarrollada por Cygnus Solutions para proporcionar un comportamiento similar a los sistemas Unix en Windows. Su objetivo es portar software que ejecuta en sistemas POSIX a Windows con una recompilación a partir de sus fuentes. Aunque los programas portados funcionan en todas las versiones de Windows, su comportamiento es mejor en Windows NT, Windows XP y Windows Server 2003.

Dead Peer Detection (DPD) Es un método para detectar un par muerto en el intercambio de llave. El método usa patrones de tráfico IPSec para minimizar el número de mensajes requeridos para confirmar la vida de un par. La muerte por detección se emplea para darse cuenta de la pérdida de recursos en caso que un par sea encontrado muerto.

DES (Data Encryption Standard) Es un algoritmo de cifrado, es decir, un método para cifrar información, escogido como FIPS en los Estados Unidos en 1976, y cuyo uso se ha propagado ampliamente por todo el mundo. El algoritmo fue controvertido al principio, con algunos elementos de diseño clasificados, una longitud de clave relativamente corta, y las continuas sospechas sobre la

existencia de alguna puerta trasera para la National Security Agency (NSA). Posteriormente DES fue sometido a un intenso análisis académico y motivó el concepto moderno del cifrado por bloques y su criptoanálisis.

Demonio Aplicación UNIX la cual está permanentemente en estado de alerta en un servidor Internet con el fin de realizar determinadas tareas como, por ejemplo, enviar un mensaje de correo electrónico o servir una página web.

DHCP (DYNAMIC HOST CONFIGURATION PROTOCOL) Protocolo de configuración dinámica de servidores. Es un protocolo de red en el que un servidor provee los parámetros de configuración a las computadores conectadas a la red informática que los requieran (máscara, puerta de enlace y otros) y también incluye un mecanismo de asignación de direcciones de IP. Este protocolo apareció como un protocolo estándar en octubre de 1993.

Diffie-Hellman El protocolo Diffie-Hellman (debido a Whitfield Diffie y Martin Hellman) permite el intercambio secreto de claves entre dos partes que no han tenido contacto previo, utilizando un canal inseguro, y de manera anónima (no autenticada).

Se emplea generalmente como medio para acordar claves simétricas que serán empleadas para el cifrado de una sesión. Siendo no autenticado, sin embargo provee las bases para varios protocolos autenticados. Su seguridad radica en la extrema dificultad (conjeturada, no demostrada) de calcular logaritmos discretos en un campo finito.

Diseño Modular Es una técnica empleada a la hora de escribir programas de un tamaño y complejidad moderados; se encuentra una gran dificultad para abarcar todo el programa de una sola vez. Para facilitar la tarea de programación, es más práctico dividir un programa en diferentes módulos procedimientos, funciones y otros bloques de código. Está basada en la técnica de resolución humana de problemas: divide y vencerás.

Driver Archivo o archivos que permiten que un sistema operativo entienda y maneje diversos periféricos y hardware que se conectan o forman parte de la computadora. Sistemas operativos como Windows suelen tener una gran base de controladores para poder ser compatibles con diversos hardware, pero muchas veces es necesario instalar otros controladores para poder hacerlos funcionar correctamente.

DSA (Digital Signatura Algorithm) o Fortezza Estándar del Gobierno Federal de los Estados Unidos de América o FIPS para firmas digitales. Fue un Algoritmo propuesto por el Instituto Nacional de Normas y Tecnología de los Estados Unidos para su uso en su Estándar de Firma Digital (DSS), especificado en el FIPS 186 . DSA se hizo público el 30 de agosto de 1991, este algoritmo

como su nombre lo indica, sirve para firmar y para cifrar información. Una desventaja de este algoritmo es que requiere mucho más tiempo de cómputo que RSA.

DMZ (Zona Desmilitarizada) Es un área de una red de computadores que está entre la red de computadores interior de una organización y una red de computadores exterior, generalmente Internet. La zona desmilitarizada permite que servidores interiores provean la red exterior de servicios, mientras protege la red interior de intromisiones.

Eavesdropping Es un tipo de ataque pasivo en el cual un tercero escucha los paquetes enviados entre dos ó más nodos en una red.

ECI Telematics Hace parte de el conjunto de empresas para establecer túneles VPNs a través de Internet empleando PPTP.

Encapsulamiento Proceso de convertir un mensaje en texto cifrado (encriptado) utilizando una clave, de manera que parezca que el mensaje solo contiene basura. Sin embargo, el destinatario designado puede aplicar la clave para descifrado y leerlo.

ESP (Encapsulating Security Payload) Encapsulado de Seguridad Una cabecera y cola de extensión IPv6 que proporciona autenticación del origen de datos, integridad y confidencialidad de datos y servicio anti-repetición para la carga del datagrama encapsulado por la cabecera y cola.

Ethernet Norma o estándar (IEEE 802.3) que determina la forma en que los puestos de la red envían y reciben datos sobre un medio físico compartido que se comporta como un bus lógico, independientemente de su configuración física. Originalmente fue diseñada para enviar datos a 10 Mbps, aunque posteriormente ha sido perfeccionada para trabajar a 100 Mbps, 1 Gbps o 10 Gbps y se habla de versiones futuras de 40 Gbps y 100 Gbps. En sus versiones de hasta 1 Gbps utiliza el protocolo de acceso al medio CSMA/CD (Carrier Sense Multiple Access / Collision Detect - Acceso múltiple con detección de portadora y detección de colisiones). Actualmente Ethernet es el estándar más utilizado en redes locales/LANs.

Exploit Es el nombre con el que se identifica un programa informático malicioso, o parte del programa, que trata de forzar alguna deficiencia o vulnerabilidad de otro programa (llamadas bugs). El fin puede ser la destrucción o inhabilitación del sistema atacado, aunque normalmente se trata de violar las medidas de seguridad para poder acceder al mismo de forma no autorizada y emplearlo en beneficio propio o como origen de otros ataques a terceros. Un "exploit" es usado normalmente para explotar una vulnerabilidad en un sistema OS y acceder a él, lo que es llamado como "rootear".

Failover Es un modo de operación de backup en el cual las funciones de un componente del sistema son asumidas por un segundo componente del sistema cuando el primero no se encuentra disponible debido a un fallo ó un tiempo de parada preestablecido. Es usado para hacer a los sistemas más tolerantes a fallos, y de esta forma hacer el sistema permanentemente disponible.

Firewall (Cortafuego) Combinación de hardware y software la cual separa una red de área local (LAN) en dos o mas partes con propósitos de seguridad. Su objetivo básico es asegurar que todas las comunicaciones entre dicha red e Internet se realicen conforme a las políticas de seguridad de la organización que lo instala. Además, estos sistemas suelen incorporar elementos de privacidad, autentificación, etc.

Firmware o Programación en Firme Es un bloque de instrucciones de programa para propósitos específicos, grabado en una memoria tipo ROM, que establece la lógica de más bajo nivel que controla los circuitos electrónicos de un dispositivo de cualquier tipo. Al estar integrado en la electrónica del dispositivo es en parte hardware, pero también es software, ya que proporciona lógica y se dispone en algún tipo de lenguaje de programación. Funcionalmente, el firmware es el intermediario (interfaz) entre las órdenes externas que recibe el dispositivo y su electrónica, ya que es el encargado de controlar a ésta última para ejecutar correctamente dichas órdenes externas.

Frame Relay Protocolo conmutado de la capa de enlace de datos, de norma industrial, que administra varios circuitos virtuales utilizando un encapsulamiento HDLC entre dispositivos conectados. Frame Relay es más eficiente que X.25, el protocolo para el cual se considera por lo general un reemplazo.

FreeBSD Es un sistema operativo multiusuario, capaz de efectuar multitarea con apropiación, inspirado como ya se dijo, en la variante 4.4 BSD-Lite de UNIX. Aunque FreeBSD no puede ser propiamente llamado UNIX, al no haber adquirido la debida licencia de The Open Group, FreeBSD sí está hecho para ser compatible con la norma POSIX, al igual que varios otros sistemas "clones de UNIX". El sistema FreeBSD incluye el kernel, la estructura de ficheros del sistema, librerías de la API de C, y algunas utilerías básicas. La versión 6.1 trajo importantes mejoras como mayor apoyo para dispositivos Bluetooth y controladores para tarjetas de sonido y red.

FreeS/WAN (Free Secure Wide-Area Networking) Es una implementación de IPSec y posteriores al (Ip security) para sistemas Linux. IPSec provee servicios de encriptación y autenticación sobre la capa de red, permite confiar en una conexión y mantener privados los datos que viajan con ella. Al implementar IPSec, puede ser autenticado y ejecutado por un Server con encriptación y recibido por otro

server en el cual se confie. Es usado habitualmente en VPNsdfd (Virtual Private Network).

FTP (File Transfer Protocol) Protocolo de transferencia de archivos. Se usan programas para FTP como son CuteFTP o LeapFTP para Windows, por ejemplo, que permiten la conexión entre dos computadores, usando por lo general el puerto 21 para conectarse (aunque se pueden usar otros puertos). Por medio del Protocolo de transferencia de archivos se pueden actualizar y descargar archivos entre el cliente y el host.

Gateway El significado técnico se refiere a un hardware o software que traduce dos protocolos distintos o no compatibles. Gateway o pasarela es un dispositivo, con frecuencia un computador, que realiza la conversión de protocolos entre diferentes tipos de redes o aplicaciones. Por ejemplo, un gateway de correo electrónico, o de mensajes, convierte mensajes entre dos diferentes protocolos de mensajes.

GNU (Licencia General Pública) Proyecto creado en 1984 con el fin de desarrollar un sistema operativo tipo Unix según la filosofía del "software libre".

GNU/Linux Nombre por el que se conoce al sistema operativo formado por el conjunto de utilidades de sistema GNU y el núcleo desarrollado por Linus Torvalds y sus colaboradores.

GPL (General Public License) Licencia de regulación de los derechos de autor de los programas de software libre (free software) la cual es promovida por la Free Software Foundation (FSF) en el marco de la iniciativa GNU. Permite la distribución de copias de programas (e incluso cobrar por ello), así como modificar el código fuente de los mismos o utilizarlo en otros programas.

GUI (INTERFAZ GRÁFICA DE USUARIO) Componente de una aplicación informática que el usuario visualiza y a través de la cual opera con ella. Está formada por ventanas, botones, menús e iconos, entre otros elementos.

gzip Es una abreviatura de GNU ZIP, un software libre GNU que reemplaza al programa compress de UNIX. gzip fue creado por Jean-loup Gailly y Mark Adler.

Hacker Es el neologismo utilizado para referirse a un experto (véase Gurú) en varias o alguna rama técnica relacionada con las tecnologías de la información y las telecomunicaciones: programación, redes de computadoras, sistemas operativos, hardware de red/voz, etc. Su entendimiento es más sofisticado y profundo respecto a los sistemas informáticos, ya sea de tipo hardware o software. Se suele llamar hackeo y hackear a las obras propias de un hacker.

Hardware En la Informática se denomina hardware o soporte físico al conjunto de elementos materiales que componen un ordenador. Hardware también son los componentes físicos de una computadora tales como el disco duro, CD-ROM, disquetera (floppy), etc... En dicho conjunto se incluyen los dispositivos electrónicos y electromecánicos, circuitos, cables, tarjetas, armarios o cajas, periféricos de todo tipo y otros elementos físicos.

Hash En computación un hash o función resumen se refiere a una función o método para generar claves o llaves que representen de manera casi unívoca a un documento, registro, archivo, etc. Una función hash puede generar dos claves iguales para objetos diferentes, ya que el rango de posibles claves es mucho menor que el de posibles objetos a resumir (las claves suelen tener en torno al centenar de bits, pero los ficheros no tienen un tamaño límite).

Hilo Un hilo de ejecución, en sistemas operativos, es similar a un proceso en que ambos representan una secuencia simple de instrucciones ejecutada en paralelo con otras secuencias. Los hilos permiten dividir un programa en dos o más tareas que corren simultáneamente, por medio de la multiprogramación. En realidad, este método permite incrementar el rendimiento de un procesador de manera considerable. En todos los sistemas de hoy en día los hilos son utilizados para simplificar la estructura de un programa que lleva a cabo diferentes funciones.

Host Máquina conectada a una red de ordenadores y que tiene un nombre de equipo (en inglés, hostname, es un nombre único que se le da a un dispositivo conectado a una red informática. Puede ser un ordenador, un servidor de ficheros, un dispositivo de almacenamiento por red, una máquina de fax, impresora, etc. Este nombre ayuda al administrador de la red a identificar las máquinas sin tener que memorizar una dirección IP para cada una de ellas.) que lo identifica.

http (HyperText Transfer Protocol) Es el protocolo usado en cada transacción de la Web (WWW). El hipertexto es el contenido de las páginas web, y el protocolo de transferencia es el sistema mediante el cual se envían las peticiones de acceso a una página y la respuesta con el contenido. También sirve el protocolo para enviar información adicional en ambos sentidos, como formularios con campos de texto. HTTP es un protocolo sin estado, es decir, que no guarda ninguna información sobre conexiones anteriores. Al finalizar la transacción todos los datos se pierden.

IDC (Internacional Data Corporation) Principal proveedor global de inteligencia de mercado, servicios de asesoría y eventos para los mercados de tecnologías de la información, telecomunicaciones y tecnología de consumo. IDC ayuda a los profesionales de TI, ejecutivos de negocio y a la comunidad de inversores a tomar decisiones basadas en hechos sobre adquisiciones tecnológicas y estrategias de

negocio. Más de 850 analistas de IDC en 50 países proporcionan su experiencia global, regional y local en tecnologías y oportunidades y tendencias sectoriales.

IDEA (International Data Encryption Algorithm) Es un cifrador por bloques diseñado por Xuejia Lai (?) y James L. Massey de la Escuela Politécnica Federal de Zúrich y descrito por primera vez en 1991. Fue un algoritmo propuesto como reemplazo del DES. IDEA fue una revisión menor de PES (Proposed Encryption Standard, del inglés Estándar de Cifrado Propuesto), un algoritmo de cifrado anterior. Originalmente IDEA había sido llamado IPES (Improved PES, del inglés PES Mejorado).

IETF (Internet Engineering Task Force), Grupo de Trabajo en Ingeniería de Internet Es una organización internacional abierta de normalización, que tiene como objetivos el contribuir a la ingeniería de Internet, actuando en diversas áreas, tales como transporte, encaminamiento, seguridad. Fue creada en EE.UU. en 1986. Es una institución formada básicamente por técnicos en Internet e informática cuya misión es velar porque la arquitectura de la red y los protocolos técnicos que unen a millones de usuarios de todo el mundo funcionen correctamente. Es la organización que se considera con más autoridad para establecer modificaciones de los parámetros técnicos bajo los que funciona la red.

IMAP Es un acrónimo inglés de Internet Message Access Protocol. Protocolo de red de acceso a mensajes electrónicos almacenados en un servidor. Mediante IMAP se puede tener acceso al correo electrónico desde cualquier equipo que tenga una conexión a Internet. Una vez configurada la cuenta IMAP, puede especificar las carpetas que desea mostrar y las que desea ocultar, esta 19 característica lo hace diferente del protocolo POP. Por defecto utiliza el puerto 143.

Internet Es una red mundial de computadoras interconectadas con un conjunto de protocolos, el más destacado, el TCP/IP. Aparece por primera vez en 1969, cuando ARPAnet establece su primera conexión entre tres universidades en California y una en Utah. También se usa el término Internet como sustantivo común y por tanto en minúsculas para designar a cualquier red de redes que use las mismas tecnologías que Internet, independientemente de su extensión o de que sea pública o privada. Cuando se dice red de redes se hace referencia a que es una red formada por la interconexión de otras redes menores.

Interfaz Zona de contacto o conexión entre dos componentes de "hardware"; entre dos aplicaciones; o entre un usuario y una aplicación. Apariencia externa de una aplicación informática.

Interprete de Comandos o shell Es un programa informático lector de líneas de texto que un usuario de un ordenador ha predefinido y este programa lo interpreta para un sistema operativo o lenguaje de programación. Habitualmente la

ejecución de comandos del usuario se realiza por medio de una interfaz de línea de comandos (CLI). Suelen incorporar características tales como control de procesos, redirección de entrada/salida, ficheros, protección, comunicaciones y un lenguaje de órdenes para escribir programas por lotes o (scripts).

Intranet Es una red de ordenadores de una red de área local (LAN) privada empresarial o educativa que proporciona herramientas de Internet, la cual tiene como función principal proveer lógica de negocios para aplicaciones de captura, reportes, consultas, etc. con el fin de auxiliar la producción de dichos grupos de trabajo; es también un importante medio de difusión de información interna a nivel de grupo de trabajo. No necesariamente proporciona Internet a la organización; normalmente, tiene como base el protocolo TCP/IP de Internet y, por ser privada, puede emplear mecanismos de restricción de acceso a nivel de programación como lo son usuarios y contraseñas de acceso o incluso a nivel de hardware como un sistema firewall (cortafuegos) que pueda restringir el acceso a la red organizacional.

IP (INTERNET PROTOCOL) Protocolo de Internet. Conjunto de reglas que regulan la transmisión de paquetes de datos a través de Internet. Se han desarrollado diferentes familias de protocolos para comunicación por red de datos para los sistemas UNIX. El más ampliamente utilizado es el Internet Protocol Suite, comúnmente conocido como TCP / IP. Es un protocolo DARPA que proporciona transmisión fiable de paquetes de datos sobre redes. El nombre TCP / IP proviene de dos protocolos importantes de la familia, el Transmission Control Protocol (TCP) y el Internet Protocol (IP). Todos juntos llegan a ser más de 100 protocolos diferentes. IP es la dirección numérica de un computador en Internet de forma que cada dirección electrónica se asigna a un computador conectado a Internet y por lo tanto es única. La dirección IP esta compuesta de cuatro octetos como por ejemplo, 132.248.53.10.

IP Dinámica Es una IP la cual es asignada mediante un servidor DHCP (Dynamic Host Configuration Protocol) al usuario. La IP que se obtiene tiene una duración máxima determinada. El servidor DHCP provee parámetros de configuración específicos para cada cliente que desee participar en la red IP. Entre estos parámetros se encuentra la dirección IP del cliente.

ISP (Internet Service Provider) Proveedor de Servicios de Internet Es una empresa dedicada a conectar a Internet a los usuarios o las distintas redes que tengan, y dar el mantenimiento necesario para que el acceso funcione correctamente. También ofrecen servicios relacionados, como alojamiento web o registro de dominios entre otros.

IPSec (Internet Protocol security) Es una extensión al protocolo IP que añade cifrado fuerte para permitir servicios de autenticación y, de esta manera, asegurar las comunicaciones a través de dicho protocolo. Inicialmente fue

desarrollado para usarse con el nuevo estándar IPv6, aunque posteriormente se adaptó a IPv4. IPsec actúa a nivel de capa de red, protegiendo y autenticando los paquetes IP entre los equipos participantes en la comunidad IPsec. No está ligado a ningún algoritmo de cifrado o autenticación, tecnología de claves o algoritmos de seguridad específico. Es más, IPsec es un marco de estándares que permite que cualquier nuevo algoritmo sea introducido sin necesitar de cambiar los estándares.

IPtables No es más que un sistema de firewall vinculado al kernel de GNU/Linux el cual hace parte de este Sistema Operativo

IPv4 Es la versión 4 del Protocolo IP (Internet Protocol). Esta fue la primera versión del protocolo que se implementó extensamente, y forma la base de Internet. IPv4 usa direcciones de 32 bits, limitándola a 232 = 4.294.967.296 direcciones únicas, muchas de las cuales están dedicadas a redes locales (LANs). Por el crecimiento enorme que ha tenido del Internet (mucho más de lo que esperaba, cuando se diseñó IPv4), combinado con el hecho de que hay desperdicio de direcciones en muchos casos (ver abajo), ya hace varios años se vio que escaseaban las direcciones IPv4. Esta limitación ayudó a estimular el impulso hacia IPv6, que esta actualmente en las primeras fases de implementación, y se espera que termine reemplazando a IPv4.

IPv6 Es la versión 6 del Protocolo de Internet (Internet Protocol), un estándar del nivel de red encargado de dirigir y encaminar los paquetes a través de una red. Está destinado a sustituir al estándar IPv4, cuyo límite en el número de direcciones de red admisibles está empezando a restringir el crecimiento de Internet y su uso, especialmente en China, India, y otros países asiáticos densamente poblados. Pero el nuevo estándar mejorará el servicio globalmente; por ejemplo, proporcionando a futuras celdas telefónicas y dispositivos móviles con sus direcciones propias y permanentes. Al día de hoy se calcula que las dos terceras partes de las direcciones que ofrece IPv4 ya están asignadas.

Kernel (También conocido como núcleo): es la parte fundamental de un sistema operativo. Es el software responsable de facilitar a los distintos programas acceso seguro al hardware del computador o en forma mas básica, es la encargada de gestionar recursos, a través de servicios de llamada al sistema. Como hay muchos programas y el acceso al hardware es limitado, el núcleo también se encarga de decidir qué programa podrá hacer uso de un dispositivo de hardware y durante cuánto tiempo, lo que se conoce como multiplexado. Acceder al hardware directamente puede ser realmente complejo, por lo que los núcleos suelen implementar una serie de abstracciones del hardware. Esto permite esconder la complejidad, y proporciona una interfaz limpia y uniforme al hardware subyacente, lo que facilita su uso para el programador.

L2TP Layer 2 Tunneling Protocol Diseñado por un grupo de trabajo de IETF como el heredero aparente de los protocolos PPTP y L2F, creado para

corregir las deficiencias de estos protocolos y establecerse como un estándar aprobado por el IETF. L2TP utiliza PPP para proporcionar acceso telefónico que puede ser dirigido a través de un túnel por Internet hasta un punto determinado. L2TP define su propio protocolo de establecimiento de túneles, basado en L2F. El transporte de L2TP está definido para una gran variedad de tipos de paquete, incluyendo X.25, Frame Relay y ATM.

L2F (Layer 2 Forwarding) Se creó en las primeras etapas del desarrollo de las RPV. Como PPTP, L2F fue diseñado por Cisco para establecer túneles de tráfico desde usuarios remotos hasta sus sedes corporativas. La principal diferencia entre PPTP y L2F es que, como el establecimiento de túneles de L2F no depende de IP (Internet Protocol), es capaz de trabajar directamente con otros medios, como Frame Relay o ATM. Como PPTP, L2F utiliza el protocolo PPP para la autenticación del usuario remoto, pero también implementa otros sistemas de autenticación como TACACS+ (Terminal Access Controller Access Control System) y RADIUS (Remote Authentication Dial-In User Service). L2F también difiere de PPTP en que permite que los túneles contengan más de una conexión.

LAN (Local Area Network) Redes de Área Local Red de datos de alta velocidad y bajo nivel de errores que cubre un área geográfica relativamente pequeña (hasta unos pocos miles de metros). Las LAN conectan estaciones de trabajo, periféricos, terminales y otros dispositivos en un solo edificio u otra área geográficamente limitada. Los estándares de LAN especifican el cableado y señalización en las capas físicas y de enlace de datos del modelo OSI. Ethernet, FDDI y Token Ring son tecnologías LAN ampliamente utilizadas. Comparar con MAN y WAN. Ver también VLAN.

LDAP Lightweight Directory Access Protocol Es un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red. LDAP puede considerarse una base de datos (aunque su sistema de almacenamiento puede ser diferente) al que pueden realizarse consultas.

Líneas Alquiladas Conexión permanente entre dos puntos de la red pública para el envío de información el cual es regulado según acuerdos creados por empresas proveedoras de servicios de Telecomunicaciones, mediante unos precios establecidos.

Líneas Punto a Punto Es un servicio orientado a todas aquellas empresas para las cuales Internet es una herramienta crítica de comunicación y/o negocio. A través de Líneas Punto a Punto de gran velocidad, empresas prestadoras de servicios de Internet, integran la red del cliente en Internet ofreciéndole un servicio de gran calidad, máxima fiabilidad y total escalabilidad.

Login En la seguridad de ordenador, es el proceso de intento de verificar la identidad digital del remitente de una comunicación como una petición para conectarse. El remitente siendo autenticado puede ser una persona que usa un ordenador, un ordenador por sí mismo o un programa del ordenador. En un web de confianza, "autenticación" es un modo de asegurar que los usuarios son quién ellos dicen que ellos son - que el usuario que intenta realizar funciones en un sistema es de hecho el usuario que tiene la autorización para hacer así.

MAC (Media Access Control address) Es un identificador hexadecimal de 48 bits que se corresponde de forma única con una tarjeta o interfaz de red. Es individual, cada dispositivo tiene su propia dirección MAC determinada y configurada por el IEEE (los ultimos 24 bits) y el fabricante (los primeros 24 bits). La mayoría de los protocolos que trabajan en la capa 2 del modelo OSI usan una de las tres numeraciones manejadas por el IEEE: MAC-48, EUI-48, y EUI-64 las cuales han sido diseñadas para ser identificadores globalmente únicos. No todos los protocolos de comunicación usan direcciones MAC, y no todos los protocolos requieren identificadores globalmente únicos.

Mac OS (Macintosh Operating System) Es el nombre del primer sistema operativo de Apple para los ordenadores Macintosh. El Mac OS original fue el primer sistema operativo con una interfaz gráfica de usuario en tener éxito.

Mac OS X Es el actual sistema operativo de la familia de ordenadores Macintosh.

Mainframe u Ordenador Central Es un ordenador grande, potente y costoso usado principalmente por una gran compañía para el procesamiento de una gran cantidad de datos; por ejemplo, para el procesamiento de transacciones bancarias.

man in the middle attack (Ataque por interceptación) Estrategia de ataque en la que el atacante intercepta una comunicación entre dos partes, substituyendo el tráfico entre ambas a voluntad y controlando la comunicación.

MD5 (Message-Digest Algorithm 5) Algoritmo de Resumen del Mensaje 5, Es un algoritmo de reducción criptográfico de 128 bits ampliamente usado. El código MD5 fue diseñado por Ronald Rivest en 1991 cuando un análisis indicó que el algoritmo MD4 era inseguro, se decidió a programar el MD5 para sustituirlo en 1991. Las debilidades en MD4 fueron descubiertas por Hans Dobbertin.. Durante el año 2004 fueron divulgados ciertos defectos de seguridad, lo que hará que en un futuro cercano se cambie de este sistema a otro más seguro.

Microsoft Acrónimo de Microcomputer Software, es una empresa de Estados Unidos, fundada por Bill Gates y Paul Allen, los cuales siguen siendo sus principales accionistas. Dueña y productora de los sistemas operativos: Microsoft

DOS y Microsoft Windows, que se utilizan en la mayoría de las computadoras del planeta.

MIPS Acrónimo de "millones de instrucciones por segundo". Es una forma de medir la potencia de los procesadores. Sin embargo, esta medida sólo es útil para comparar procesadores con el mismo juego de instrucciones y usando benchmarks que fueron compilados por el mismo compilador y con el mismo nivel de optimización. Esto es debido a que la misma tarea puede necesitar un número de instrucciones diferentes si los juegos de instrucciones también lo son; y por motivos similares en las otras dos situaciones descritas. En las comparativas, usualmente se representan los valores de pico, por lo que la medida no es del todo realista. La forma en que funciona la memoria que usa el procesador también es un factor clave para la potencia de un procesador, algo que no suele considerarse en los cálculos con MIPS. Debido a estos problemas, los investigadores han creado pruebas estandardizadas tales como SpecInt para medir el funcionamiento real, y las MIPS han caído en desuso.

Modelo OSI El modelo de referencia de Interconexión de Sistemas Abiertos (OSI, Open System Interconection) lanzado en 1984 fue el modelo de red descriptivo creado por ISO. Proporcionó a los fabricantes un conjunto de estándares que aseguraron una mayor compatibilidad e interoperabilidad entre los distintos tipos de tecnología de red producidos por las empresas a nivel mundial.

MPLS Multiprotocol Label Switching Es un mecanismo de transporte de datos estándar creado por la IETF y definido en el RFC 3031. Opera entre la capa de enlace de datos y la capa de red del modelo OSI. Fue diseñado para unificar el servicio de transporte de datos para las redes basadas en circuitos y las basadas en paquetes. Puede ser utilizado para transportar diferentes tipos de tráfico, incluyendo tráfico de voz y de paquetes IP.

Multiplataforma Término utilizado frecuentemente en informática para indicar la capacidad o características de poder funcionar o mantener una interoperabilidad de forma similar en diferentes sistemas operativos o plataformas. Por ejemplo la posibilidad de utilizar un programa o software determinado en sistemas Windows y Linux.

Multiplexación Combinación de dos o más canales de información en un solo medio de transmisión usando un dispositivo llamado multiplexor. El proceso inverso se conoce como demultiplexación.

Existen muchas formas de multiplexación según el sistema de comunicación, los más utilizados son la multiplexación por división de tiempo o TDM (Time division multiplexing), la multiplexación por división de frecuencia o FDM (Frequency-division multiplexing) y la multiplexación por división en código o CDM (Code division multiplexing).

NAT (TRADUCCIÓN DE DIRECCIONES DE RED) Mecanismo que reduce la necesidad de tener direcciones IP exclusivas globales. NAT permite que las organizaciones cuyas direcciones no son globalmente exclusivas se conecten a la Internet transformando esas direcciones en espacio de direccionamiento enrutable global. También denominado traductor de dirección de red.

NETBIOS Protocolo de red originalmente creado para redes locales de computadores IBM PC. NetBIOS fue la API del producto llamado "PC Network", desarrollado por Sytec, empresa contratada por IBM. "PC Network" soportaba menos de 80 nodos y era bastante simple, pero en aquella época era más apropiado para los computadores personales que su pariente más viejo y complejo para mainframes de IBM, el SNA. NetBIOS engloba un conjunto de protocolos de nivel de sesión, que proveen 3 tipos de servicios: servicio de nombres servicio de paquetes servicio de sesión. El servicio de nombres permite el registro de nombres de computador, aplicaciones y otros identificadores en general en la red. Un programa puede, a través de este servicio, determinar qué computador en la red corresponde un determinado nombre. El servicio de paquetes (en inglés, datagram) es análogo al protocolo UDP y posibilita el envío y recibimiento de paquetes en la red, punto a punto o por difusión. El servicio de sesión permite el establecimiento de conexiones entre dos puntos en la red y es análogo al protocolo TCP. NetBIOS es utilizado por protocolos de nivel más alto como SMB.

NetBSD Sistema operativo de la familia Unix, open source y libre, y, a noviembre de 2006, disponible para más de 50 plataformas hardware. Su diseño y sus características avanzadas lo hacen ideal para multitud de aplicaciones. NetBSD ha surgido como resultado del esfuerzo de un gran número de personas que tienen como meta producir un sistema operativo tipo Unix accesible y libremente distribuibleq.

Netscape Es una empresa de software. Fue una de las primeras compañías en trabajar con la naciente World Wide Web. Lanzó un navegador llamado Mosaic Netscape 0.9 el 13 de octubre de 1994. Este navegador fue posteriormente renombrado como Netscape Navigator por el cual es famosa

OpenBSD Sistema operativo libre tipo Unix, multiplataforma, basado en 4.4BSD. Es un descendiente de NetBSD, con un foco especial en la seguridad y la criptografía. Este sistema operativo, se concentra en la portabilidad, cumplimiento de normas y regulaciones, corrección, seguridad proactiva y criptografía integrada. OpenBSD incluye emulación de binarios para la mayoría de los programas de los sistemas SVR4 (Solaris), FreeBSD, GNU/Linux, BSD/OS, SunOS y HP-UX.

OpenSSH (Open Secure Shell) Conjunto de aplicaciones que permiten realizar comunicaciones encriptadas a través de una red, usando el protocolo SSH, es una

versión de SSH escrita a principios de 1999 que se convirtió en la implementación libre por excelencia para OpenBSD.

OpenSSH Portability Team Equipo que se responsabiliza de añadir el código necesario para portar el software a todas las plataformas posibles.

OpenSSL Es un proyecto de software desarrollado por los miembros de la comunidad Open Source para libre descarga y está basado en SSLeay desarrollado por Eric Young y Tim Hudson. Consiste en un robusto paquete de herramientas de administración y librerías relacionadas con la criptografía, que suministran funciones criptográficas a otros paquetes como OpenSSH y navegadores web (para acceso seguro a sitios HTTPS). Estas herramientas ayudan al sistema a implementar el Secure Sockets Layer (SSL), así como otros protocolos relacionados con la seguridad, como el Transport Layer Security (TLS). Este paquete de software es importante para cualquiera que esté planeando usar cierto nivel de seguridad en su máquina Linux. OpenSSL también nos permite crear certificados digitales que podremos aplicar a nuestro servidor, por ejemplo Apache.

OpenS/WAN Es una implementación de IPsec para GNU/Linux. Este soporta kernels 2.0, 2.2, 2.4 y 2.6, y corre en muchas plataformas diferentes, incluye x86, x86_64, ia64, MIPS y ARM.

OpenVPN Es una solución de conectividad basada en software: SSL (Secure Sockets Layer) VPN Virtual Private Network (red virtual privada), OpenVPN ofrece conectividad punto-a-punto con validación, jerárquica de usuarios y host conectados remotamente, resulta una muy buena opción en tecnologías Wi-Fi (redes inalámbricas EEI 802.11) y soporta una amplia configuración, entre ellas balanceo de cargas entre otras. Está publicado bajo la licencia GPL, de código abierto.

PAP Protocolo de autenticación de password. Cuando se establece la conexión entre el servidor y el cliente este último envía el par formado por el nombre de usuario y la contraseña, luego se verificará la identidad del usuario y se autentificara o rechazará la petición con lo cual la conexión será finalizada.

Paquete Un paquete de datos es una unidad fundamental de transporte de información en todas las redes de computadores modernas. El término datagrama es usado a veces como sinónimo.

Password Contraseña o clave, Es una forma de autenticación que utiliza información secreta para controlar el acceso hacia algún recurso. La contraseña normalmente debe mantenerse en secreto ante aquellos a quienes no se les permite el acceso. Aquellos que desean acceder a la información se les solicita

una clave; si conocen o no conocen la contraseña, se concede o se niega el acceso a la información según sea el caso.

PKI (Public Key Infrastructure) Infraestructura de Clave Pública Es una combinación de hardware y software, políticas y procedimientos de seguridad que permiten la ejecución con garantías de operaciones criptográficas como el cifrado, la firma digital o el no repudio de transacciones electrónicas. El término PKI se utiliza para referirse tanto a la autoridad de certificación y al resto de componentes, como para referirse, de manera más amplia y a veces confusa, al uso de algoritmos de clave pública en comunicaciones electrónicas. Este último significado es incorrecto, ya que no se requieren métodos específicos de PKI para usar algoritmos de clave pública.

PocketPC Es un ordenador de bolsillo, también llamado PDA (Personal Digital Assistant). Se trata de un pequeño ordenador, diseñado para ocupar el mínimo espacio y ser fácilmente transportable que ejecuta el sistema operativo Windows CE de Microsoft entre otros, el cual le proporciona capacidades similares a los PCs de escritorio.

POP Post Office Protocol Al contrario de otros protocolos creados con anterioridad como el SMTP el POP no necesita una conexión permanente a Internet, puesto que es en el momento de la conexión cuando solicita al servidor el envío de la correspondencia almacenada en el servidor para dicho usuario. Si se está permanentemente conectado a Internet pueden configurarse los programas cliente de correo de tal forma que la petición al servidor de correo se efectúe automáticamente cada cierto tiempo y de esta forma avise al usuario de que tiene correo pendiente de recibir.

Poptop Poptop es una aplicación de código abierto del servidor PPTP. Corriendo en arquitecturas x86 o en arquitecturas embebidas de Motorola ColdFire, Poptop provee completa interoperabilidad con los clientes VPN con Microsoft PPTP.

PPP (PROTOCOLO PUNTO A PUNTO) Implementación del protocolo TCP/IP por líneas seriales (como en el caso del módem). Es más reciente y complejo que SLIP.

PPTP (Point to Point Tunneling Protocol) Es un protocolo desarrollado por Microsoft, U.S. Robotics, Ascend Communications, 3Com/Primary Access, ECI Telematics conocidas colectivamente como PPTP Forum, para implementar redes privadas virtuales o VPN.

Protocolo Descripción formal de formatos de mensaje y de reglas que dos computadores deben seguir para intercambiar dichos mensajes.

Protocolos de Handshake Es el encargado de intercambiar las claves que se usarán para crear un canal seguro de comunicación. Podemos decir que es el núcleo del protocolo SSL porque también es el encargado de coordinar los estados de los extremos de la comunicación.

Proxy El término proxy hace referencia a un programa o dispositivo que realiza una acción en representación de otro. La finalidad más habitual es la del servidor proxy, que sirve para permitir el acceso a Internet a todos los equipos de una organización cuando sólo se puede disponer de un único equipo conectado, esto es, una única dirección IP.

PVC Circuitos Virtuales Permanentes Conexiones establecidas en forma permanente, que se utilizan en transferencia de datos frecuentes y constantes entre dispositivos DTE a través de la red Frame Relay. La comunicación a través de un PVC no requiere los estados de establecimiento de llamada y finalización que se utilizan con los SVCs (Circuitos Virtuales Conmutados).

QoS Calidad del Servicio Garantiza que se transmitirá cierta cantidad de datos en un tiempo dado (throughput). Una de las grandes ventajas de ATM (Asynchronous Transfer Mode – Modo de Transferencia Asíncrona) respecto de técnicas como el Frame Relay y Fast Ethernet, es que admite niveles de QoS. Esto permite que los proveedores de servicios ATM garanticen a sus clientes que el retardo de extremo a extremo no excederá un nivel específico de tiempo. Además que en los servicios satelitales da una nueva perspectiva en la utilización del ancho de banda, dando prioridades a las aplicaciones de extremo a extremo con una serie de reglas.

RC2 es un algoritmo que, debido a un fallo de concepto, resulta especialmente vulnerable a un ataque de fuerza bruta (donde se prueban todas las posibles combinaciones de claves) si el tamaño de la clave lo permite. Bruce Schneier, de Counterpane Systems, ha creado un programa para romper claves RC2 de 40 bits, y que funciona como ...!un salvapantallas!

RC4 Sistema de cifrado de flujo Stream cipher más utilizado y se usa en algunos de los protocolos más populares como Transport Layer Security (TLS/SSL) (para proteger el tráfico de Internet) y Wired Equivalent Privacy (WEP) (para añadir seguridad en las redes inalámbricas). RC4 fue excluido en seguida de los estándares de alta seguridad por los criptógrafos y algunos modos de usar el algoritmo de criptografía RC4 lo han llevado a ser un sistema de criptografía muy inseguro, incluyendo su uso WEP. No está recomendado su uso en los nuevos sistemas, sin embargo, algunos sistemas basados en RC4 son lo suficientemente seguros para un uso común.

rlogin (Remote Login) El Rlogin comienza una sesión de terminal remoto sobre el anfitrión especificado como host. El anfitrión remoto debe hacer funcionar

un servicio de Rlogind (o demonio) para que el Rlogin conecte con el anfitrión; además utiliza un mecanismo estándar de autorización de los Rhosts. Cuando no se especifica ningún nombre de usuario ni con la opción -l ni con la opción username@, Rlogin conecta como el usuario actualmente loggeado.

Road Warriors (Teletrabajador) Es aquella persona que utiliza la telemática para la realización de su profesión. Esta actividad se realiza fuera del establecimiento empresarial. El aspecto principal del teletrabajador es tener mayor independencia en la realización del trabajo, sin embargo, debido a la evolución de la tecnología, el teletrabajar puede llegar a estar más fiscalizado que los trabajadores que prestan sus servicios dentro de la empresa.

Router (ENRUTADOR O ENCAMINADOR) Es un dispositivo hardware o software de interconexión de redes de computadores/computadores que opera en la capa 3 (nivel de red) del modelo osi. Este dispositivo interconecta segmentos de red o redes enteras. Hace pasar paquetes de datos entre redes tomando como base la información de la capa de red.

RSA El sistema criptográfico con clave pública RSA es un algoritmo asimétrico cifrador de bloques, que utiliza una clave pública, la cual se distribuye (en forma autenticada preferentemente), y otra privada, la cual es guardada en secreto por su propietario. Los mensajes enviados usando el algoritmo RSA se representan mediante números y el funcionamiento se basa en el producto de dos números primos grandes (mayores que 10100) elegidos al azar para conformar la clave de descifrado. La seguridad de este algoritmo radica en que no hay maneras rápidas conocidas de factorizar un número grande en sus factores primos utilizando computadoras tradicionales.

Script Secuencia de comandos que se le dan a un módem con el propósito de configurarlo (velocidad, compresión de datos, etc) o para realizar tareas específicas (llamar al proveedor, colgar, etc). A veces es necesario modificar un script o cadena de inicio la cual establece las condiciones iniciales del módem (por ejemplo cambiar ATDT que establece una línea telefónica por tonos a ATDP que indica una línea telefónico por pulsos, etc.).

Serpent Algoritmo de cifrado simétrico de bloques que quedó finalista en el concurso Advanced Encryption Standard del NIST, tras Rijndael. Serpent fue diseñado por Ross Anderson, Eli Biham y Lars Knudsen. Como otros participantes del AES Serpent usa un tamaño de bloque de 128 bits y soporta tamaños de clave de 128, 192 y 256 bits de longitud. El cifrado consiste en 32 rondas de substitución-permutación operando sobre cuatro bloques de 32 bits. Cada ronda usa 32 copias de la misma S-Box de 4-bit a 4-bit. Serpent se diseñó para que las operaciones se realizasen en paralelo, usando 32 desplazamientos de 1 bit.

Servidor de la LAN Es aquel o aquellos ordenadores que van a compartir sus recursos hardware y software con los demás equipos de la red. Sus características son potencia de cálculo, importancia de la información que almacena y conexión con recursos que se desean compartir.

Servidor X El sistema de ventanas X fue desarrollado a mediados de los años 1980 en el MIT para dotar de una interfaz gráfica a los sistemas Unix. Este protocolo permite la interacción gráfica en red entre un usuario y una o más computadoras haciendo transparente la red para éste. X es el encargado de mostrar la información gráfica y es totalmente independiente del sistema operativo. El sistema de ventanas X distribuye el procesamiento de aplicaciones especificando enlaces cliente-servidor. El servidor provee servicios para acceder a la pantalla, teclado y ratón, mientras que los clientes son las aplicaciones que utilizan estos recursos para interactuar con el usuario. De este modo mientras el servidor se ejecuta de manera local, las aplicaciones pueden ejecutarse remotamente desde otras máquinas, proporcionando así el concepto de transparencia de red.

Sesión FTP Es un tipo de sesión en el cual un usuario puede transferir ficheros desde o hacia un host remoto, una sesión puede utilizar dos tipos de conexiones TCP, una para control y otra para datos. La conexión de control se utiliza para emitir datos de control entre los dos equipos. La conexión de datos es la que se establece para transmitir el fichero, si se han de transmitir varios ficheros se deberán establecer varias conexiones TCP, una por fichero como mínimo.

Shell Intérprete de comandos. Interpreta y activa los comandos o utilidades introducidos por el usuario. Es un programa ordinario (ejecutable) cuya particularidad es que sirve de interface entre el Kernel y el usuario. Es también un lenguaje de programación (similar al C), y como tal permite el usar variables, estructuras sintácticas, entradas/salidas etc.

Sistema Operativo Es un conjunto de programas destinados a permitir la comunicación del usuario con un ordenador y gestionar sus recursos de manera eficiente. Comienza a trabajar cuando se enciende el ordenador, y gestiona el hardware de la máquina desde los niveles más básicos. Un sistema operativo se puede encontrar normalmente en la mayoría de los aparatos electrónicos que podamos utilizar sin necesidad de estar conectados a un ordenador y que utilicen microprocesadores para funcionar, ya que gracias a estos podemos entender la máquina y que ésta cumpla con sus funciones (teléfonos móviles, reproductores de DVD, autoradios... y computadoras).

Sistema X Window Fue desarrollado a mediados de los años 80 en el MIT para dotar de una interfaz gráfica a los sistemas Unix. Este protocolo permite la interacción gráfica en red entre un usuario y una o más computadores haciendo transparente la red para éste. Generalmente se refiere a la versión 11 de este

protocolo, X11, el que está en uso actualmente. X es el encargado de visualizar la información gráfica y es totalmente independiente del sistema operativo. El sistema X Window distribuye el procesamiento de aplicaciones especificando enlaces cliente-servidor. El servidor provee servicios para acceder a la pantalla, teclado y ratón, mientras que los clientes son las aplicaciones que utilizan estos recursos para interacción con el usuario. De este modo mientras el servidor se ejecuta de manera local, las aplicaciones pueden ejecutarse remotamente desde otras máquinas, proporcionando así el concepto de transparencia de red.

Smartcard (Tarjeta Inteligente) Tarjeta como una de crédito que tiene anexado un microchip (EEPROM o microprocesador) que tiene la utilidad de almacenar información y procesarla.

SMTP (Simple Mail Transport Protocol) Protocolo simple de transferencia de correo electrónico. Protocolo de red basado en texto utilizado para el intercambio de mensajes de correo electrónico entre computadoras o distintos dispositivos (PDA's, teléfonos móviles, etc.). SMTP se basa en el modelo cliente-servidor, donde un cliente envía un mensaje a uno o varios receptores. En el conjunto de protocolos TCP/IP, el SMTP va por encima del TCP, usando normalmente el puerto 25 en el servidor para establecer la conexión.

Socket Designa un concepto abstracto por el cual dos programas (posiblemente situados en computadoras distintas) pueden intercambiarse cualquier flujo de datos, generalmente de manera fiable y ordenada. Un socket queda definido por una dirección IP, un protocolo y un número de puerto.

Software Se denomina software, programática, equipamiento lógico o soporte lógico a todos los componentes intangibles de un ordenador o computadora, es decir, al conjunto de programas y procedimientos necesarios para hacer posible la realización de una tarea específica, en contraposición a los componentes físicos del sistema (hardware). Esto incluye aplicaciones informáticas tales como un procesador de textos, que permite al usuario realizar una tarea, y software de sistema como un sistema operativo, que permite al resto de programas funcionar adecuadamente, facilitando la interacción con los componentes físicos y el resto de aplicaciones.

Software Libre Es el software que, una vez obtenido, puede ser usado, copiado, estudiado, modificado y redistribuido libremente. El software libre suele estar disponible gratuitamente en Internet, o a precio del costo de la distribución a través de otros medios; sin embargo no es obligatorio que sea así y, aunque conserve su carácter de libre, puede ser vendido comercialmente. Análogamente, el software gratuito (denominado usualmente Freeware) incluye en algunas ocasiones el código fuente; sin embargo, este tipo de software no es libre en el mismo sentido que el software libre, al menos que se garanticen los derechos de modificación y redistribución de dichas versiones modificadas del programa.

SOFTWARE NO LIBRE (También llamado software propietario, software privativo, software privado y software con propietario) se refiera a cualquier programa informático en el que los usuarios tienen limitadas las posibilidades de usarlo, modificarlo y/o redistribuirlo (con o sin modificaciones), o que su código fuente no está disponible o el acceso a éste se encuentra restringido.

Software de VPN Opción disponible en la actualidad para la creación de una Red Privada Virtual, en la actualidad además de esta categoría existen otras dos modalidades, por hardware y por cortafuego. Este tipo de solución es considerado el mas flexible debido a todas sus posibles configuraciones y son ideales cuando surgen problemas de interoperatividad en los otros modelos. Obviamente el rendimiento es menor y la configuración más delicada, porque se suma el sistema operativo y la seguridad del equipo en general

Solaris Es un sistema operativo desarrollado por Sun Microsystems. Es un sistema certificado como una versión de UNIX. Aunque Solaris en sí mismo aún es software propietario, la parte principal del sistema operativo se ha liberado como un proyecto de software libre denominado Opensolaris.

Soporte Multiprotocolo Tecnología que soporta diversos protocolos existentes.

SSH (Secure SHell) Es el nombre de un protocolo y del programa que lo implementa. Este protocolo sirve para acceder a máquinas remotas a través de una red, de forma similar a como se hace con telnet. La diferencia principal es que SSH usa técnicas de cifrado que hacen que la información que viaja por el medio de comunicación vaya de manera no legible y ningúna tercera persona pueda descubrir el usuario y contraseña de la conexión ni lo que se escribe durante toda la sesión; aunque es posible atacar este tipo de sistemas por medio de ataques de REPLAY y manipular así la información entre destinos. Al igual que telnet, sólo permite conexiones tipo terminal de texto, aunque puede redirigir el tráfico de X para poder ejecutar programas gráficos si tenemos un Servidor X arrancado.

SSH Communications Security Compañía que ofrecía el protocolo SSH gratuitamente para uso doméstico y académico, pero exigía el pago a otras empresas.

SSL/TLS Es un protocolo diseñado por la empresa Netscape Communications, que permite cifrar la conexión, incluso garantiza la autenticación. Se basa en la criptografía asimétrica y en el concepto de los certificados. La versión estandarizada por el IETF se conoce como TLS. Su mayor ventaja es que funciona entre la capa TCP y la capa de aplicación, por esto es muy fácil usarlo para proteger los protocolos de la capa de aplicación (por ejemplo FTP, gopher, HTTP...) sin tener que realizar cambios importantes en los mismos.

StrongSwan Solución VPN de código libre para Linux Basada en IPSec.

Stunnel (Universal SSL Wrapper) El paquete Stunnel contiene un programa que permite encriptar conexiones TCP arbitrarias dentro de SSL (Secure Sockets Layer) para poder comunicarse fácilmente con clientes sobre canales seguros. Stunnel puede usarse para añadir funcionalidad SSL a los demonios comúnmente usados bajo Inetd como los servidores POP-2, POP-3, y IMAP, a servidores independientes como NNTP, SMTP y HTTP, y para hacer un túnel PPP sobre conectores de red sin hacer cambios en el código fuente del paquete del servidor.

Switch Es un dispositivo electrónico de interconexión de redes de computadoras que opera en la capa 2 (nivel de enlace de datos) del modelo OSI (Open Systems Interconection). Un switch interconecta dos o más segmentos de red, funcionando de manera similar a los puentes (bridges), pasando datos de un segmento a otro, de acuerdo con la dirección MAC de destino de los datagramas en la red. Los switches se utilizan cuando se desea conectar múltiples redes, fusionándolas en una sola. Al igual que los bridges, dado que funcionan como un filtro en la red, mejoran el rendimiento y la seguridad de las LANs (Local Area Network- Red de Área Local).

TCP (Transmission Control Protocolo) Protocolo de Control de Transmisión. Es uno de los protocolos fundamentales en Internet. Muchos programas dentro de una red de computadores pueden usar TCP para crear conexiones entre ellos a través de las cuales enviarse datos. El protocolo garantiza que los datos serán entregados en su destino sin errores y en el mismo orden en que se transmitieron. También proporciona un mecanismo para distinguir distintas aplicaciones dentro de una misma máquina, a través del concepto de puerto. TCP soporta muchas de las aplicaciones más populares de Internet, incluidas HTTP, SMTP y SSH.

TCP/IP (TRANSMISSION CONTROL PROTOCOL/INTERNET PROTOCOL) Sistema de protocolos en los que se basa en buena parte Internet. El primero se encarga de dividir la información en paquetes en origen, para luego recomponerla en el destino. El segundo la dirige adecuadamente a través de la red.

Tcpwrappers Es una herramienta simple que sirve para monitorear y controlar el tráfico que llega por la red. Esta herramienta ha sido utilizada exitosamente en la protección de sistemas y la detección de actividades ilícitas. Fue desarrollada por Wietze Zweitze Venema y esta basada en el concepto de Wrapper; es una herramienta de seguridad libre y muy útil.

Telnet Es el protocolo estándar de Internet que permite la conexión a una terminal remota.

Terminal Server Los servicios de terminal (o terminal services) son un componente de los sistemas operativos windows que permite a un usuario acceder a las aplicaciones y datos almacenados en otro ordenador mediante un acceso por red. Basado en el protocolo de escritorio remoto (Remote Desktop Protocol (RDP)) aparece por primera vez en Windows NT 4.0 (Terminal Server Edition).

Trafic shaping (Control de tráfico) El Traffic Shaping es un intento para controlar el tráfico de una red de ordenadores para optimizar o garantizar su funcionamiento, las bajas latencias, etc... Así, proporciona un mecanismo para controlar el volumen de tráfico que es enviado en una red así como su frecuencia. Aunque es un método para mejorar los protocolos de red, puede ser utilizado para limitar cierto tipo de paquetes o tráfico desde un punto a otro.

Tramas Es una unidad de envío de datos. Viene a ser sinónimo de paquete de datos o Paquete de red, aunque se aplica principalmente en los niveles OSI más bajos, especialmente en el Nivel de enlace de datos. Normalmente una trama constará de cabecera, datos y cola. En la cola suele estar algún chequeo de errores. En la cabecera habrá campos de control de protocolo. La parte de datos es la que quiera transmitir en nivel de comunicación superior, típicamente el Nivel de red.

Triple DES Así se llama al algoritmo que hace triple cifrado del DES. También es conocido como TDES, fue desarrollado por IBM en 1978. No llega a ser un cifrado múltiple, porque no son independientes todas las subclases. Este hecho se basa en que DES tiene la característica matemática de no ser un grupo, lo que implica que si se cifra el mismo bloque dos veces con dos llaves diferentes se aumenta el tamaño efectivo de la llave.

Túnel Virtual Túnel que se establece cada vez que se conectan los equipos a través de la Red Privada Virtual.

UDP (USER DATAGRAM PROTOCOL) Protocolo del nivel de transporte basado en el intercambio de datagramas. Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera. Se utiliza cuando se necesita transmitir voz o vídeo y resulta más importante transmitir con velocidad que garantizar el hecho de que lleguen absolutamente todos los bytes.

UNIX Sistema operativo especializado en capacidades de multiusuario y multitarea. Fue la base inicial de Internet. Entre sus características más importantes se encuentran: Redireccionamiento de Entrada/Salida, alta portabilidad al estar escrito en lenguaje C, lo que lo hace independiente del hardware. Interface simple e interactivo con el usuario Sus componentes básicos

son: Programas, shell, shell scripts (comandos y sentencias interpretadas por una shell)

Usuarios Remotos Usuarios que deben acceder a la red interna de la empresa o a sus recursos desde diferentes sitios geográficos, haciendo uso de Internet, empleando equipos normales o ya sea por medio de dispositivos móviles, permitiéndoles trabajar como si se encontraran dentro de la empresa.

U.S. Robotics, Ascend Communications Hace parte de el conjunto de empresas para establecer túneles VPNs a través de Internet empleando PPTP

VPN (Virtual Private Network) Red Privada Virtual. Es una red privada que se extiende, mediante un proceso de encapsulamiento y cifrado de paquetes de datos a distintos puntos remotos mediante el uso de unas infraestructuras públicas de transporte (como la Internet), pero garantizando que la información que se transmite solo pueda ser accedida por los entes involucrados en la comunicación.

VPN Interna Redes separadas y seguras a través de la misma Intranet

VPN sitio-a-sitio Conexión permanente entre oficinas mediante Internet.

VPN de acceso remoto Conexiones aleatorias de los agentes móviles con su oficina mediante Internet.

WAN Una red de área amplia, con frecuencia denominada WAN, acrónimo de la expresión en idioma inglés Wide Area Network, es un tipo de red de computadoras capaz de cubrir distancias desde unos 100 hasta unos 1000 km, proveyendo de servicio a un país o un continente. Un ejemplo de este tipo de redes sería RedIRIS, Internet o cualquier red en la cual no estén en un mismo edificio todos sus miembros (sobre la distancia hay discusión posible). Muchas WAN son construidas por y para una organización o empresa particular y son de uso privado, otras son construidas por los proveedores de internet (ISP) para proveer de conexión a sus clientes.

Windows 95/98/Me/NT/2000/XP Conjunto de sistemas operativos gráficos para computadoras personales cuyo propietario es la empresa Microsoft. Existen diferentes versiones de Windows, las mencionadas anteriormente son las mas modernas antes de que fuera lanzado la mercado la última versión, denominada Windows Vista. Este sistema operativo es de los más conocidos en todo el mundo.

Wi-Fi Es un conjunto de estándares para redes inalámbricas basados en las especificaciones IEEE 802.11. Wi-Fi se creó para ser utilizada en redes locales inalámbricas, pero es frecuente que en la actualidad también se utilice para acceder a Internet.

Wireless (Conexiones Inalámbricas) Se aplica el término inalámbrico al tipo de comunicación en la que no se utiliza un medio de propagación físico, sino se utiliza la modulación de ondas electromagnéticas, las cuales se propagan por el espacio sin un medio físico que comunique cada uno de los extremos de la transmisión. En general, la tecnología inalámbrica utiliza ondas de radiofrecuencia de baja potencia y una banda específica, de uso libre para transmitir, entre dispositivos. Estas condiciones de libertad de utilización, sin necesidad de licencia, han propiciado que el número de equipos, especialmente computadoras, que utilizan las ondas para conectarse, a través de redes inalámbricas haya crecido notablemente.

WPA (Wi-Fi Protected Access) Acceso Protegido Wi-Fi Es un sistema para proteger las redes inalámbricas (Wi-Fi); creado para corregir las deficiencias del sistema previo WEP (Wired Equivalent Privacy - Privacidad Equivalente a Cableado). Los investigadores han encontrado varias debilidades en el algoritmo WEP (tales como la reutilización del vector de inicialización (IV), del cual se derivan ataques estadísticos que permiten recuperar la clave WEP, entre otros). WPA implementa la mayoría del estándar IEEE 802.11i, y fue creado como una medida intermedia para ocupar el lugar de WEP mientras 802.11i era finalizado.

WEP (Wired Equivalent Privacy) Privacidad Equivalente a Cableado Es el sistema de cifrado incluido en el estándar IEEE 802.11 como protocolo para redes Wireless que permite cifrar la información que se transmite. Proporciona cifrado a nivel 2. Está basado en el algoritmo de cifrado RC4, y utiliza claves de 64 bits (40 bits más 24 bits del vector de inicialización IV) o de 128 bits (104 bits más 24 bits del IV).

Wikipedia Es una enciclopedia libre plurilingüe basada en la tecnología wiki. Wikipedia se escribe de forma colaborativa por voluntarios, permitiendo que la gran mayoría de los artículos sean modificados por cualquier persona con acceso mediante un navegador web. El proyecto comenzó el 15 de enero de 2001, fundada por Jimbo Wales y Larry Sanger como complemento de la enciclopedia escrita por expertos Nupedia. Ahora depende de la fundación sin ánimo de lucro Wikimedia Foundation.

X11 El sistema de ventanas X fue desarrollado a mediados de los años 1980 en el MIT para dotar de una interfaz gráfica a los sistemas Unix. Este protocolo permite la interacción gráfica en red entre un usuario y una o más computadoras haciendo transparente la red para éste. Generalmente se refiere a la versión 11 de este protocolo, X11, el que está en uso actualmente.

X.25 Norma X.25 Red de conmutación de paquetes basada en el protocolo HDLC proveniente de IBM. Establece mecanismos de direccionamiento entre usuarios, negociación de características de comunicación, técnicas de recuperación de errores. Los servicios públicos de conmutación de paquetes

admiten numerosos tipos de estaciones de distintos fabricantes. Por lo tanto, es de la mayor importancia definir la interfaz entre el equipo del usuario final y la red.

X.509 Es un estándar UIT-T para infraestructuras de claves públicas (en inglés, Public Key Infrastructure o PKI). X.509 especifica, entre otras cosas, formatos estándar para certificados de claves públicas y un algoritmo de validación de la ruta de certificación. En el sistema X.509, una autoridad certificante (AC) emite un certificado asociando una clave pública a un Nombre Distinguido particular en la tradición de X.500 o a un Nombre Alternativo tal como una dirección de correo electrónico o una entrada de DNS.

X WINDOW Fue desarrollado a mediados de los años 80 en el MIT para dotar de una interfaz gráfica a los sistemas Unix. Este protocolo permite la interacción gráfica en red entre un usuario y una o más computadores haciendo transparente la red para éste. Generalmente se refiere a la versión 11 de este protocolo, X11, el que está en uso actualmente.

RESUMEN

En este documento se pretende hacer una presentación sobre el proyecto denominado “Prototipo de Administrador de Redes Privadas Virtuales usando Software Libre”; este proyecto trae consigo grandes beneficios debido a que podrá brindar a muchas pymes la oportunidad de crear redes entre sus sucursales a bajo costo y de manera segura, además de permitirles generar la configuración de dichas redes por si mismos sin mayores contratiempos, para esto se desarrolla la herramienta denominada CygnusVPN la cual permite de manera muy amigable por medio de sus interfaces y su manual operativo, la configuración de una Red Privada Virtual a usuarios con pocos conocimientos técnicos.

Otro beneficio que presenta, dado a que el desarrollo de CygnusVPN está basado en librerías que se rigen bajo la normatividad del software libre es que los usuarios pueden acceder a esta herramienta sin tener que pagar por utilizarla, pero deben tener en cuenta que por ahora el prototipo solamente se podrá emplear con equipos que cuenten con cualquier distribución de GNU/Linux como Sistema Operativo.

INTRODUCCION

Sin duda alguna, los servicios informáticos han dado un cambio radical al estilo de vida y a la forma de realizar labores, tanto a nivel empresarial como del hogar; de esta manera gracias a estos avances tecnológicos se ha logrado ser más competitivo a nivel empresarial al punto que el avance de las compañías se debe en gran medida al buen trato que se le dé a la información y al uso eficiente que hagan de la misma.

De esta forma, para muchas pymes, resulta de vital importancia la integración de sus diferentes departamentos; como es sabido muchas de estas poseen sus diferentes áreas en lugares distantes de la empresa o también presentan la necesidad de la comunicación con empleados que permanentemente están fuera de ella, y requieren de manera indispensable la creación de redes que puedan soportar el trafico de información de manera segura.

Por consiguiente las empresas se ven avocadas a invertir grandes sumas de dinero en mejorar sus plataformas tecnológicas, para permitir un buen flujo de información entre cada uno de los entes que conforman la compañía, garantizando un progreso firme y sin contratiempos para cada una de ellas. No obstante, existen muchas empresas las cuales debido a que no poseen grandes capitales de dinero, se ven avocadas a postergar a un segundo plano las ayudas tecnológicas que podrían tener para la integración de sus sucursales, teletrabajo entre otras

Ahora bien, la necesidad de integrar cada uno de los entes de las empresas mediante redes existe, pero muchas de estas se ven obligadas a retrasar esta integración, esto debido a que las soluciones que brinda el mercado son bastante costosas y otras alternativas bastante económicas ofrecidas, no cuentan con requerimientos importantes como lo es la seguridad.

En el documento que se presenta a continuación, se ilustra las formas en que se ha tratado de dar solución a este tipo de necesidad, para de esta manera crear un criterio serio de la necesidad que se posee de tener redes seguras y a bajo costo; se muestran las diferentes implementaciones que se han hecho a lo largo de los años y se hace un estudio de las ventajas y desventajas que presentan estas tecnologías.

Al tener un estudio detallado de los pro y contras de cada una de las tecnologías se emprende la labor de dar solución a esta necesidad; dando paso a la creación de las Redes Privadas Virtuales utilizando software libre, pasando por etapas de análisis y diseño donde se modelará una herramienta que permita una fácil configuración de una VPN. Finalmente y gracias a las etapas anteriormente mencionadas, se creará la aplicación denominada CygnusVPN que junto con su manual de usuario permitirá satisfacer los objetivos de este proyecto.

1. PRELIMINARES

Cuando se quiere dar solución a un problema es preciso conocer tanto el problema como las principales características del entorno que lo rodea. De esta manera resulta de vital importancia tener ciertos fundamentos generales que permitan vislumbrar la magnitud de la tarea a realizar, construyendo de esta manera una perspectiva clara que permita generar buenas soluciones a inconvenientes venideros en etapas futuras.

En este primer capitulo se especifican algunos conceptos importantes para la gestación del proyecto, comenzando por la definición del problema al cual se le quiere dar solución, analizando la forma mediante la cual se ha tratado de resolver dicho problema a través del tiempo permitiendo así apreciar de alguna manera las principales fallas que se han tenido en éstas soluciones; todo este análisis permitirá presentar unos objetivos, que serán definidos a lo largo de este capítulo y que además se utilizarán como pilares fundamentales para el desarrollo del proyecto, de esta forma se llegará al final del capítulo con buenas bases teóricas en lo que concierne a temas relacionados.

1.1. TITULO DEL PROYECTO

Prototipo de administrador de redes privadas virtuales usando software libre

1.2. DEFINICION DEL PROBLEMA

1.2.1. Antecedentes

A lo largo del desarrollo de las redes privadas, han existido dos alternativas a emplear:

Tener una red dedicada entre sucursales, la cual nos puede brindar beneficios como seguridad, confiabilidad, eficiencia, velocidad, en términos generales información de buena calidad, que es vital para el buen funcionamiento de las organizaciones. Sin embargo, el montaje de una red dedicada implica la inversión de grandes cantidades de dinero, lo cual no resulta viable para la mayoría de las organizaciones.

La otra alternativa consiste en emplear una red pública como Internet para la comunicación, teniendo esto como resultado bajos costos pero sacrificando la seguridad de la información.

Debido a que ninguna de las anteriores soluciones satisface totalmente a los usuarios, nacen las Redes Privadas Virtuales (VPN), las cuales no son más que unas configuraciones de software y/o hardware que hacen que la comunicación por medio de una red pública sea confiable gracias al empleo de mecanismos de cifrado y autenticación de usuarios en la red.

En la actualidad existen un sin número de herramientas para la implementación de VPN'S divididas en dos grandes categorías, las propietarias y las libres. De las herramientas propietarias se puede decir que el costo es un gran impedimento para la mayoría de usuarios cuando desean adquirirlas, sin embargo este mismo factor es considerado como ventaja para las herramientas libres además que brindan la oportunidad de tener acceso a los códigos fuentes para así crear aplicaciones derivadas adecuadas a beneficios particulares; a pesar de esto, presentan una desventaja y es que no existe un producto final que contenga todas las herramientas en un mismo ente garantizando la compatibilidad de las mismas y a su vez con la debida documentación para una mejor manipulación del producto.

1.2.2. Formulación

Es posible simplificar el proceso del montaje de una red privada virtual usando software libre haciéndolo accesible para personas con conocimientos técnicos medios.

1.2.3. Descripción del problema

Muchas empresas de la región, se han visto inmersas en un sin número de factores como:

- El crecimiento que han tenido en los últimos años.
- La necesidad de satisfacer unas necesidades cada vez más exigentes.
- Abarcar nuevos mercados.
- Competir por un mercado que se amplia cada vez mas.

Que de una u otra manera las ha hecho pensar en nuevas alternativas para satisfacer estos nuevos requerimientos como:

- Ampliar sus establecimientos.
- Crear nuevas sucursales.
- Crear nuevos puntos de venta claves en zonas apartadas.

Por consiguiente también se ven obligados a mejorar sus procesos, a tener siempre a mano una muy buena tecnología que les sirva de ayuda para sus tareas diarias, y permita una comunicación optima entre sucursales, que les permita siempre tener una información de excelente calidad que les ayude en la toma de buenas decisiones. Dando esto lugar a verse inmersas en un mar de dudas, a la hora de escoger una tecnología que les sirva de apoyo en la comunicación de dichas sucursales. Ya que se ven obligados a pagar costos muy altos por productos que existen en el mercado, debilitando esto sus finanzas, o contemplar la estrategia de optar por herramientas de software libre, pero muchas veces con la duda, ya que se encuentran pocos profesionales que tengan los conocimientos suficientes como para llevar a feliz termino una tarea como esta.

Lo anterior permite detectar una falencia en este aspecto, ya que no existen herramientas que integren todo el software especializado para la construcción de este tipo de redes, y que además ofrezcan una muy buena documentación para consultar cualquier inquietud que se pueda tener.

1.3. JUSTIFICACIÓN

En un mundo enmarcado por la competencia, donde las empresas no se pueden dar el lujo de dar ventaja a sus competidores, donde la administración de la información resulta primordial para el buen desarrollo de la empresa en el terreno

al cual hace parte, donde las empresas necesitan estar a toda hora comunicadas para poder compartir la información necesaria que les ayude a realizar mejor sus tareas y permitir que se tomen excelentes decisiones, y en el cual los costos que se tengan para la administración de la misma no se pueden ver muy dilatados, resulta de gran ayuda la construcción de redes privadas virtuales para la comunicación de estas empresas, y mas aún cuando se tienen en cuenta herramientas de software libre para la construcción de estas redes, pues de esta manera se reducen los costos de manera significativa y con la ayuda de una buena administración se puede llegar a tener excelentes resultados.

La herramienta que se propone como solución al problema de la falta de documentación e integración del software libre disponible para estos casos tiene las siguientes razones de justificación para llevarlo a cabo.

1. Elimina la ausencia de integración de herramientas para la creación de redes privadas virtuales, ofreciendo además una muy buena documentación.
2. Las personas que utilicen esta herramienta, se verán beneficiadas de gran forma, ya que no tendrán que preocuparse por una grande inversión en cuanto a hardware y licencias de software privado.
3. Brindará un beneficio social debido a que muchas personas y pequeñas empresas se verán beneficiadas debido a que podrán acceder a una aplicación de bajo costo.
4. Las personas no tendrán que conseguir las diferentes herramientas por separado para la creación de VPN'S, gracias a que éstas se encontrarán integradas en un solo producto para mayor comodidad de los usuarios además de garantizarles compatibilidad entre las herramientas.
5. Los usuarios podrán contar con una muy buena documentación, la cual les brindará toda la información necesaria para el manejo de las herramientas, ayudándoles a configurar de manera sencilla una Red Privada Virtual.

1.4. OBJETIVOS

1.4.1. Generales

Desarrollar una herramienta que integre herramientas de desarrollo libre para la implementación de Redes Privadas Virtuales VPN'S

1.4.2. Específicos

Reunir la documentación de las herramientas que formarán parte del producto y crear la documentación de la integración de las herramientas.

Consultar las opciones de software y/o hardware óptimas para el desarrollo del proyecto.

Aprender los conceptos necesarios para administrar el software de firewall seleccionado.

Aprender los conceptos necesarios para administrar el software de VPN seleccionado.

Integrar un grupo de herramientas de desarrollo libre para la creación de VPN'S en un solo producto final, el cuál se distribuirá en un medio magnético (CD o DVD).

Generar un manual de uso de la herramienta elaborada.

Presentar ejemplos de uso de la herramienta construida con casos específicos.

1.5. MARCO TEÓRICO

A medida que los computadores fueron adquiriendo mayor auge, y debido a las grandes ventajas que estos presentaban frente a la solución de problemas, surge la necesidad de crear redes que permitieran comunicar varios de estos equipos para poder compartir la información, es así como a mediados de los años setenta nacen la primeras redes privadas que permitieron a las empresas comunicar su principales sedes haciendo así que la información no tuviera que estar relegada a la maquina en la cual residía sino permitirle ser compartida garantizando de esta manera mayores niveles de eficiencia.

Las primeras redes creadas eran conectadas mediante líneas alquiladas independientes para voz y datos con anchos de bandas fijos.

A partir de este momento no se ha parado de crear nuevas tecnologías que permitan la trasmisión de información de manera más eficiente. Pasando así por

tecnologías como X.25, Frame Relay, ATM, que en su momento solucionaron los problemas existentes en cuanto a la transmisión de la información,

Sin embargo en un mundo enmarcado por el cambio y el rápido avance de la tecnología, surgen cada día nuevas necesidades que se deben solucionar, de esta manera se ha pasado por necesitar grandes niveles de procesamiento, a necesitar anchos de banda enormes para la transmisión de la información y en la actualidad con el auge que han tenido las comunicaciones bussines-to-bussines, las transacciones vía Internet, los trabajadores móviles, poder garantizar altos niveles de seguridad en la información transmitida.

Debido a las soluciones que se deben implementar para este tipo de necesidades surgen las Redes Privadas Virtuales, las cuales brindan seguridad en la comunicación por medio de mecanismos de autenticación, cifrado y encapsulamiento de la información mediante la creación de túneles virtuales, debido a que este proyecto se interesa en la implementación de Redes Privadas Virtuales deben dejarse muy claros ciertos conceptos fundamentales, los cuales se presentan a continuación.

Qué es una VPN

Es una red privada que se extiende, mediante un proceso de encapsulamiento y cifrado de paquetes de datos a distintos puntos remotos mediante el uso de unas infraestructuras públicas de transporte (como la Internet).

Los paquetes de datos de la red privada viajan por medio de un "túnel" definido en la red pública.

Anterior a la difusión de Internet, especialmente de la Web, las compañías que querían que las redes LAN trascendieran más allá del ámbito de la oficina e incluyeran a los trabajadores y centros de información de otros edificios, ciudades, estados o incluso otros países, tenían que invertir en hardware y servicios de telecomunicaciones costosos para crear redes amplias de servicio, WAN. Sin embargo, con Internet, las compañías tienen la posibilidad de crear una red privada virtual que demanda una inversión relativamente pequeña de hardware y utiliza el Internet global para la conexión entre los puntos de la red.

Las LAN tradicionales son redes esencialmente restringidas, por lo cual se puede intercambiar información entre las computadoras usualmente sin pensar en la seguridad de la información o preocuparse mucho por ella. Sin embargo, con las VPN la situación es preocupante porque el Internet público es intrínsecamente abierto e inseguro. Por lo tanto, las VPN se implementan usando protocolos especiales que le permitan al remitente cifrar los paquetes de información y permitir únicamente al receptor autorizado descifrar la información que esté

sellada con un identificador único que además comprueba que la transmisión se hace desde una fuente confiable.

Cuando un empleado se conecta a Internet, la configuración de las VPN les permite acceder a la red privada de la compañía y navegar en la red como si estuvieran en la oficina.

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 esta bien definido pueden existir serias consecuencias.

Para el correcto funcionamiento de una VPN existen varios aspectos importantes que se deben conocer como es el caso del cifrado, el encapsulamiento, y la autenticación.

Cifrado

Las redes privadas virtuales garantizan la privacidad y la confidencialidad de la información haciendo uso del cifrado. En un muy breve resumen, el cifrado es una técnica que codifica la información de modo que hace difícil o imposible su lectura, y la decodifica (con ayuda de una clave secreta) de modo que pueda ser leída nuevamente. A la información codificada se la llama “texto cifrado” y a la información sin codificar, “texto nativo”.

Cuando en una VPN se transmite información de un punto a otro, el Gateway de la VPN del punto de origen cifra la información en texto cifrado antes de enviarla. En el otro punto, el Gateway receptor descifra la información, es decir la vuelve texto nativo, y luego la envía a la LAN.

Autenticación

Una vez clara la definición de la tecnología de cifrado, la cual garantiza la privacidad de la información al atravesar la red pública se puede dar una definición de autenticación:

La autenticación es el proceso mediante el cual el sistema intenta asegurar que la persona que está iniciando sesión es la misma para quien se emitió una cuenta. El único medio de autenticación en la mayoría de las redes es la solicitud de una contraseña, aun cuando se sabe que este método de autenticación tiene serias fallas en la seguridad.

Por lo tanto se puede concluir que la tecnología de autenticación garantiza:

- La identidad de los participantes de la VPN (los *gateways* y clientes son quienes dicen ser)
- La integridad de la información recibida (no ha sido alterada en el camino)

Encapsulamiento

El encapsulamiento es el proceso por el cual los datos que se deben enviar a través de una red se deben colocar en paquetes que se puedan administrar y rastrear. El encapsulado consiste pues en ocultar los detalles de implementación de un objeto, pero a la vez se provee una interfaz pública por medio de sus operaciones permitidas. Considerando lo anterior también se puede definir como el proceso de convertir un mensaje en texto cifrado (encriptado) utilizando una clave, de manera que parezca que el mensaje solo contiene basura. Sin embargo, el destinatario designado puede aplicar la clave para descifrado y leerlo.

Qué es un Firewall

Un firewall es un dispositivo que filtra el tráfico entre redes (como mínimo dos). El firewall puede ser un dispositivo físico o un software sobre un sistema operativo. En general se debe ver como una caja con dos o mas interfaces de red en la que se establecen reglas de filtrado con las que se decide si una conexión determinada puede establecerse o no.

Los firewalls se pueden usar en cualquier red. Es habitual tenerlos como protección de Internet en las empresas, aunque ahí también suelen tener una doble función: controlar los accesos externos hacia dentro y también los internos hacia el exterior.

Generalmente, en un firewall no se tendrá más que un conjunto de reglas en las que se examina el origen y destino de los paquetes del protocolo entrante. Una excelente manera de implementar un firewall y hacer que se vayan ejecutando este conjunto de reglas es **Iptables**, el cual no es más que un sistema de firewall vinculado al kernel de Linux el cual hace parte de este Sistema Operativo.

1.6. DISEÑO METODOLÓGICO

Inicialmente se realizará un levantamiento de información actual respecto a la implementación de Redes Privadas Virtuales y Firewalls para poder determinar que aplicaciones existen, bajo que tipo de protocolos trabajan, cuales son sus

ventajas frente a las demás soluciones, bajo que tipo de licenciamiento están sujetas, como garantizan la seguridad, bajo que plataformas trabajan, cuales son sus principales problemas, que tipo de soporte tienen y determinar las especificaciones técnicas, entre otros, para llevar a feliz termino el montaje de la red.

Se realizará un estudio exhaustivo de las herramientas en cuanto a su instalación, funcionamiento, administración y rendimiento, el cual nos permitirá apropiarnos de unos fundamentos claves que van a permitir una adecuada manipulación de las herramientas para poder garantizar un buen uso de estas.

Una vez reunida toda la información necesaria en cuanto a aplicaciones existentes y las ventajas que ofrecen, se podrá realizar una integración de las herramientas que se consideren mejores para satisfacer los requerimientos que se deben cumplir. Procediendo con la elaboración de un manual, el cual contendrá la documentación necesaria para la creación, configuración y administración de una red privada virtual, en base a las herramientas escogidas.

La solución resultante debe ser implantada, probada y puesta en funcionamiento para tener algún caso específico de prueba que nos permita demostrar que se puede brindar una solución óptima en la implementación de Redes Privadas Virtuales haciendo uso de herramientas libres.

1.7. PERSONAS QUE PARTICIPAN EL EN PROYECTO

Asesor:

John Alexis Guerra Gómez
Ingeniero de Sistemas y Computación

Ejecutores:

Maria Isabel Gómez Estrada
Estudiante

Jose Arley López Largo
Estudiante

2. ANTECEDENTES

En este capitulo se presentará un breve resumen acerca de la evolución de las redes de computadores a través del tiempo, así mismo, se mencionarán cuales han sido las más importantes tecnologías empleadas y porque la necesidad de implementar una tecnología en particular.

Además se presentarán los fundamentos que se deben tener en cuenta respecto a las Redes Privadas Virtuales, los cuales se pueden resumir en definición de VPN, escenarios de aplicación, principales características, beneficios, tipos de implementaciones y algunos conceptos que se deben tener en cuenta si se desea llegar a implementar algún tipo de VPN.

2.1 HISTORIA DE LAS VPN

Los años setenta fueron testigos del surgimiento de las redes privadas, estos tipos de redes permitían a las empresas interconectar sus sedes principales mediante líneas alquiladas independientes para voz y datos, empleando anchos de banda fijos. Sin embargo, la demanda de transmisión de datos a mayores velocidades y rendimientos tan sólo surgió en la década de los 80, ésta fue iniciada gracias al cambio del modelo informático basado en mainframe hacia arquitecturas cliente/servidor, así como el desarrollo de nuevas aplicaciones para estos nuevos entornos.

Es así como comenzaron a aparecer nuevos patrones de tráfico, donde el ancho de banda podía permanecer ocioso durante prolongados períodos de tiempo. De igual manera se comenzó a detectar la necesidad de interconectar las distintas redes de área local (LAN) que empezaban a surgir en las organizaciones.

2.1.1. Frame Relay: Empaquetamiento de la información

Finalizando la década de los 80 y comenzando los 90's, Frame Relay comenzó a ganar mayor aceptación, ya que ofrecía una más elevada capacidad de procesamiento de datos que X.25, su tecnología predecesora. Todas las mejoras fueron adquiridas mediante la implementación de un sistema de procesamiento de paquetes simplificado que se encargaba de dividir la información en tramas, cada una de las cuales se encargaba de transportar una dirección, la cual era utilizada por los conmutadores para determinar su destino final. La eficiencia del sistema se incrementaba cada vez más gracias a la utilización de los recursos brindados por la nueva tecnología, dado que ésta permitía fragmentar el tráfico en ráfagas permitiendo así aprovechar el ancho de banda que antes permanecía ocioso, y generando una reducción significativa de los costos de transmisión frente a los de las líneas alquiladas.

A mediados de los noventa, se presentó un incremento en la dependencia de las empresas respecto de sus redes debido a la alta demanda en la utilización del correo electrónico y la implantación de aplicaciones que consumían grandes anchos de banda.

2.1.2. ATM y convergencia de redes de voz y datos

Esta expansión, unido a la aparición del concepto de convergencia de las redes de voz y datos en una sola plataforma de networking, fue la que condujo al desarrollo de ATM (Modo de Transferencia Asíncrono), la cual fue concebida como una tecnología multiservicio de banda ancha capaz de soportar datos, voz, video e imágenes sobre la misma infraestructura de red.

ATM se diferencia de Frame Relay debido a que en la segunda se empleaba un tamaño de paquetes variable, en cambio ATM se basa en conmutación de celdas de tamaño fijo. Esta característica permitía aprovechar todas las ventajas de la multiplexación estadística ofreciendo así un rendimiento determinístico. Los enlaces ATM están basadas en circuitos virtuales permanentes (PVC) con Calidad de Servicio (QoS), las cuales son capaces de proporcionar transmisiones de extremo a extremo garantizadas y fiables.

Poco después, la Red vuelve a actuar como elemento central frente a un nuevo cambio. Gracias a la gran demanda en el uso de Internet para las comunicaciones business-to-business (negocio a negocio), surgió la necesidad de garantizar

mayores niveles de seguridad sobre esta infraestructura, ya que por ser de carácter público carece completamente de regulación. De esta forma, nacieron diferentes tecnologías, las cuales permiten la creación de túneles a través de Internet, surgiendo así las Redes Privadas Virtuales las cuales serán mencionadas a continuación de una manera más formal.

2.1.3. Redes Privadas Virtuales

Se puede decir que son redes que permiten realizar una comunicación entre dos puntos, sin importar su ubicación geográfica, a través de una red pública, pero garantizando que la información que se transmite solo pueda ser accedida por los entes involucrados en la comunicación.

En conclusión, las definiciones de red privada virtual (VPN) que pueden ser encontradas en el medio son múltiples, pero según lo investigado a través de Internet, todas convergen en lo siguiente.

"Una red privada virtual es una implementación o sistema que habilita una comunicación segura a través de un medio inseguro, siendo transparente para el usuario u aplicación que realiza y recibe la comunicación."[1].

Debido a que toda la información encontrada en Internet se acerca a la definición anteriormente citada, se puede considerar como válida, sin embargo se puede ampliar y se puede decir que siempre que se desee asegurar una comunicación entre dos puntos, se podrá utilizar una red privada virtual, independientemente del potencial de privacidad que se tenga en la comunicación, si la información ha de ser preservada de terceros por su importancia.

En algunas ocasiones las redes privadas virtuales han sido denominas como túneles, ya que transportan la información a través de un canal público, pero aislando la información del resto y consecuentemente creando así túneles virtuales que separan la información de la del resto que viaja a través de la red.

La separación de la información se logra mediante el cifrado de la misma, haciendo así que el sistema sea más seguro, el nivel de seguridad lo suministra el sistema criptográfico seleccionado.

A continuación se mostrará como la evolución de la informática ha sido de gran ayuda para la aparición de las Redes Privadas Virtuales por medio de la creación

---

[1] http://reina.usal.es/pub/fernandez2006redes.pdf Fecha Consulta 15122006

de varios escenarios, en los cuales pueden ser aplicadas dichas redes para facilitar las labores de seguridad.

2.2. APLICACIONES DE LAS REDES PRIVADAS VIRTUALES

En base a consultas realizadas en Internet[2], se encontró que a la hora de crear Redes Privadas Virtuales, pueden presentarse varios escenarios de aplicación y también se puede apreciar como estos escenarios fueron apareciendo a medida que la informática evolucionó.

La informática surgió debido a la necesidad de realizar cálculos y procesar grandes volúmenes de información en tiempos muy cortos, pero a comienzos de esta tecnología, las necesidades en cuanto a seguridad eran mínimas.

A medida que la informática fue evolucionando, se pudo notar como no es suficiente el hecho de simplemente procesar la información, sino que en muchas situaciones es necesario compartirla entre distintos equipos, de igual manera con los recursos existentes que en muchos casos pueden ser muy costosos se puede satisfacer dicha necesidad, estos hechos dieron el nacimiento a la Red de Area Local (LAN - Local Area Network). En este punto ya se tiene conectada toda una red de equipos, pero ¿que pasa cuando se tiene que compartir información confidencial entre dos equipos particulares?, la solución sería interconectando entre si los equipos que comparten la información confidencial separándolos físicamente de la red general.

En este momento se pueden presentar varios problemas, el primero es la duplicación de los recursos que se necesitan dentro de la red debido a que se deben montar y mantener dos redes. El segundo problema es que aunque se cuente con dos redes, no hay manera de considerar segura la confidencialidad ya que ésta viene de la mano de la separación física de las dos redes, pero en ningún momento se están empleando mecanismos que impidan que en algún punto de la red alguien se pueda conectar y así obtener la información que se está tratando de proteger. La forma de solucionar este problema es emplear la misma red para enviar la información confidencial, junto con la información general haciendo así surgir el primer escenario de aplicación de las Redes Privadas Virtuales, donde en una Intranet se separarán las personas, equipos o departamentos que no deben tener acceso a cierta información de los que si lo pueden tener.

El anterior panorama le permitió a la informática dar un siguiente paso, pero esta vez es a nivel empresarial, en donde los empresarios ven la necesidad de

---

[2] http://reina.usal.es/pub/fernandez2006redes.pdf Fecha Consulta 15122006

extender sus negocios mediante varios edificios pero permitiéndoles estar interconectadas todas sus oficinas. Para este tipo de arquitecturas se emplearon las líneas punto a punto, X25, Frame Relay, etc. Las cuales son más conocidas como Redes de Área Extensa (WAN – Wide Area Network). Este sistema es considerado seguro hasta cierto punto, ya que para acceder a este tipo de líneas no es tan fácil pues se requiere de conocimientos técnicos avanzados, además se requiere equipo especializado que no se encuentra al alcance de cualquier persona. Este tipo de sistema era el preferido por bancos, el ejercito, oficinas del estado entre otras hasta hace poco tiempo.

En realidad no es muy necesaria la utilización de las Redes Privadas Virtuales en este tipo de conexiones. Sin embargo el crecimiento empresarial y la globalización en general, nos presentan un nuevo escenario, en el cual las empresas están creciendo mediante la adquisición de oficinas y sucursales en diferentes ciudades e incluso en otros países. Además cuentan con empleados móviles (trabajadores que deben movilizarse geográficamente, para realizar sus actividades laborales) que necesitan acceder a toda la información de la empresa sin importar el sitio en el que se encuentren. Para realizar este tipo de comunicaciones fue creado Internet, que es conocido como la Red de Redes, en donde se puede encontrar una gran cantidad de computadores conectados entre si a través de todo el mundo.

Debido a que Internet es de carácter público, parece lógico pensar que es el sistema más inseguro que se puede encontrar, y en realidad es así, la información que circula por la misma está al alcance de cualquiera, por lo tanto es muy factible encontrar personal altamente calificado en cuanto a la interceptación de información. Sin embargo, las empresas están decididas a emplear este medio a pesar de este alto riesgo debido a varias razones:

Los costos de las comunicaciones dentro de las empresas representan un costo importante a considerar. Ya que Internet es un servicio que suele estar implantado en la mayoría de ellas, el hecho de poderla emplear para transmitir información, haría que se redujeran los costos de manera considerable, ya que las conexiones a Internet tienen unos costos relativamente bajos.

Gracias a la penetración de Internet en los distintos países del planeta es muy posible encontrar en la mayoría de ellos un Proveedor de Servicios (IPS - Internet Service Provider), que permita la conexión de los trabajadores móviles con la oficina principal.

Internet garantiza una ruta segura desde un punto de la red a otro. Si por alguna circunstancia, la comunicación es cortada entre los dos puntos de la comunicación, los nodos de la red de Internet están preparados para buscar caminos alternativos con el objetivo que la información llegue a su destino, claro

que esto es válido si el punto afectado no es uno de los nodos por los que se está tratando de acceder a la red.

Como conclusión de la aparición de las comunicaciones a larga distancia entre oficinas, sucursales y agentes móviles mediante el uso de Internet, se puede definir el segundo escenario en el que se pueden aplicar las Redes Privadas Virtuales, ya que el cifrado de la información hace imposible la lectura y/o modificación de la misma.

Como último escenario donde se puede encontrar la utilización de las VPNs es mediante las conexiones inalámbricas (wireless) el cual es considerado un entorno relativamente reciente, debido a que estas conexiones están expuestas a ser interceptadas por cualquiera que se encuentre dentro del alcance de ésta y aunque existen routers especiales para realizar conexiones wireless los cuales emplean algún algoritmo de cifrado WPA (Wi-Fi Protected Access - Acceso Protegido Wi-Fi) y WEP (Wired Equivalent Privacy - Privacidad Equivalente a Cableado); donde este último sistema es mucho menos seguro que el primero. Aun así, la información es realmente vulnerable haciendo que estos dos sistemas de cifrado sean insuficientes haciendo recurrir en este instante a las VPNs.

En resumen, los cuatro posibles escenarios que se pueden presentar son:

1. **VPN Interna** red separada y segura a través de una misma Intranet.
2. **VPN sitio-a-sitio** conexión permanente entre oficinas a través de una red pública como Internet.
3. **VPN de acceso remoto** conexiones aleatorias de teletrabajadores con sus oficinas a través de Internet.
4. **VPN Interna** conexión de equipos mediante dispositivos Wireless.

A continuación serán mencionadas algunas características y beneficios de las Redes Privadas Virtuales, que gracias a información recopilada de varias páginas de Internet se puede concluir que son consideradas como las más importantes.

2.3. CARACTERÍSTICAS DE UNA RED PRIVADA VIRTUAL (VPN)

Confidencialidad o privacidad La información que viaja a través de la red debe estar disponible sólo para las personas autorizadas.

Confiabilidad o integridad La información que viaja a través de la red no se debe poder cambiar entre el remitente y el receptor.

Disponibilidad La información que viaja a través de la red debe estar disponible cuando sea necesaria.

No Repudio para impedir que una vez firmado un documento se retracte el remitente o niegue haberlo redactado.

Para que las condiciones anteriormente mencionadas se cumplan, se deben realizar ciertos pasos a los paquetes IP que se desean enviar:

- Se cifran para garantizar la confidencialidad.
- Se firman para garantizar la autenticidad, integridad y no repudio.
- El paquete resultante se encapsula en un nuevo paquete IP y se envía a través de Internet al otro extremo de la VPN.

Beneficios

- Ahorro de costos directos
- Reducción del tiempo de aprendizaje
- Reducción en la cantidad de equipos
- Reducción en el soporte técnico necesario
- Aumento de flexibilidad
- Escalabilidad: extiende la red WAN a más usuarios remotos
- Soporta más conexiones y ancho de banda
- Se encuentran basadas en fiabilidad de conexión, rendimiento, cantidad de información y no en distancia y en tiempo de conexión.

La implementación de las Redes Privadas Virtuales además de poder presentarse en diferentes escenarios, pueden ser realizadas en formas diferentes, siendo las más importantes las VPN basadas en hardware y software, estos tipos de implementación de VPN serán explicados a continuación con ayuda del modelo OSI.

2.4. IMPLEMENTACIÓN DE LAS REDES PRIVADAS VIRTUALES

No está de más resaltar que las VPNs deben operar de forma transparente tanto para los usuarios como para las aplicaciones que las utilizan. ¿Cómo puede ser implementada una VPN?.

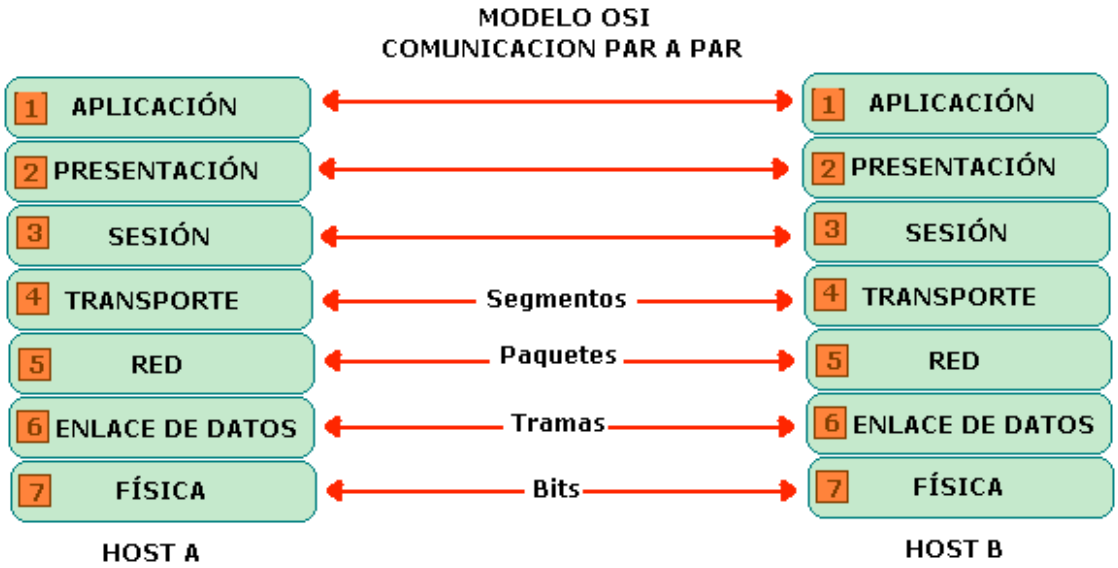


Figura 1. Modelo OSI

El proceso de cifrado y descifrado de la información puede ser realizado en cualquier punto en el que se encuentre el flujo de la información, la única restricción existente, es que el descifrado solo se puede realizar en el destino en la capa equivalente a la que se realizo el cifrado en el origen.

En base a lo anterior y teniendo en cuenta al modelo OSI, se pueden resaltar dos zonas importantes: Hardware y Software. Cuando se habla de Hardware se está refiriendo al sistema de interconexión física que se establece entre los dos equipos (capa física del modelo OSI), pero al hablar de Software se están teniendo en cuenta las seis capas restantes del modelo OSI. Y como se decía anteriormente, gracias a que el cifrado y descifrado puede ser realizado en cualquier punto, siempre y cuando sean capas equivalentes, entonces se pueden definir dos tipos de VPN:

- VPN por Hardware
- VPN por Software

2.4.1. Implementación de VPN por Hardware

El proceso de cifrado y descifrado se realiza a nivel físico en los puntos inmediatamente anterior e inmediatamente posterior al comienzo de la línea de comunicación. Por realizarse a nivel físico, se requieren unos equipos que permitan realizar este tipo de tarea de forma transparente. Por lo general los

equipos empleados son routers que traen software para VPN incorporado. Estos dispositivos llevan incorporado un procesador y algoritmos de cifrado y descifrado. La ventaja de éste tipo de dispositivos es que el fabricante entrega el equipo completamente listo para trabajar, además la instalación y uso de los mismos es extremadamente fácil, ya que lo único que hay que realizar es intercalar los routers en los puntos de salida y entrada de la línea de comunicación, activarles el cifrado y descifrado, configurar la contraseña, y el mecanismo de certificación o medio que servirá para el cifrado y descifrado de la información.

La gran desventaja que presentan las VPN implementadas por hardware, es en cuanto al sistema de cifrado, pues éste viene impuesto por el fabricante, y depende del mismo para las actualizaciones.

2.4.2. Implementación de VPN por Software

Gracias a la documentación encontrada en diferentes páginas de Internet y la consulta realizada en algunas empresas de la región se logró establecer que en la medida que ha transcurrido el tiempo, el uso de las Redes Privadas Virtuales por software se ha hecho más popular, debido a que las pequeñas y medianas empresas han encontrado la necesidad de implementar mecanismos de seguridad para comunicar sus redes. Debido a que este tipo de sistema tiende a crecer rápidamente, es más favorable la implementación de una Red Privada Virtual por software que por hardware.

2.4.3. Tabla comparativa entre la Implementación de una VPN por Software y Hardware

Como se mencionó anteriormente las soluciones VPN pueden ser realizadas mediante hardware, es decir empleando equipos dedicados para este fin, de igual manera pueden ser realizadas por medio de software. A continuación se presenta una tabla que reúne las principales ventajas y desventajas de estos dos tipos de implementaciones.

VPN por Software	**VPN por Hardware**
VENTAJAS	**DESVENTAJAS**

VPN por Software	VPN por Hardware
Existen una gran cantidad de soluciones desarrolladas tanto comerciales como libres.	Al realizar una VPN mediante hardware, se obliga a utilizar el software que el proveedor ofrece.
Mayor número de usuarios debido a los bajos costos de implementación, por tanto se encuentra mayor documentación.	Relegadas a grandes compañías debido a sus altos costos.
Brindan cobertura tanto a redes internas como externas.	En la actualidad solo brindan cobertura interna o externa, pero no las dos opciones al mismo tiempo.
La seguridad de la información puede garantizarse desde la salida del equipo emisor hasta el equipo destino.	La seguridad se garantiza únicamente entre los extremos de la VPN, es decir de gateway a gateway.
No requiere un equipo dedicado si la carga de transacciones es baja	Requiere un dispositivo dedicado (router) para realizar la Red Privada Virtual.
Se puede tener conocimiento de su funcionamiento y ajustarlo a necesidades particulares.	Se depende de una tecnología externa por lo tanto no se tiene conocimiento de su operación.
Existe la libertad de realizar actualizaciones del software cada vez que se liberan nuevas versiones.	Se depende del fabricante para poder realizar cualquier tipo de actualización al firmware.
Se pueden emplear diferentes librerías que permiten la implementación de distintos mecanismos de cifrado.	Los sistemas de cifrado usados por los fabricantes son cerrados y por lo general estos sólo utilizan un único tipo.
Pueden emplearse computadores diferentes en los extremos de la VPN en cuanto a lo que concierne a características físicas como la memoria, el procesador, etc. y lógicas como el S.O. y las versiones de las aplicaciones.	Requiere de equipos iguales o del mismo fabricante en los extremos de la VPN para garantizar compatibilidad.
DESVENTAJAS	**VENTAJAS**
Para algunas aplicaciones VPN, la configuración puede necesitar conocimientos avanzados.	Permite una instalación y configuración relativamente sencillas.
Requiere de personal especializado para su mantenimiento.	No requiere de personal especializado y el mantenimiento que requiere es mínimo.
El sistema si depende de las máquinas que se encuentran conectadas a la red, debido a que todo el tráfico de las redes	El sistema no depende de las máquinas que se encuentren conectadas a la red.

VPN por Software	VPN por Hardware
que se están tratando de conectar, debe pasar a través de los equipos que están operando como gateways.	
Ya que el software debe instalarse en una máquina, si la carga de transacciones es alta, debe dedicarse una máquina exclusiva para este fin.	Al emplearse un equipo dedicado, no tiene que compartir recursos con ningún otro tipo de aplicación.
El sistema de claves y certificados están en máquinas potencialmente inseguras, que pueden ser atacadas.	El mecanismo de autenticación se encuentra integrado dentro del router el cual cuenta con mecanismos de seguridad para protegerse de ataques.
Al operar mediante aplicaciones de libre distribución, puede existir la posibilidad de haber sido dejadas puertas traseras.	Los distribuidores de estos dispositivos VPN, integran el software dentro de los equipos.

Tabla 1. Diferencias en la implementación de VPNs por Hardware y Software

Después de realizar este análisis comparativo se pueden concluir varios puntos importantes para definir el rumbo de este proyecto; se puede apreciar como las soluciones basadas en Hardware brindan seguridad, comodidad y un buen servicio a los clientes que se deciden por este tipo de solución, sin embargo, no deja de ser una solución costosa y que además viene ligada a ciertas restricciones por parte del fabricante en cuanto a configuración y uso del dispositivo lo que la hace perder puntos frente a la solución basada en Software que mediante la combinación con unos buenos mecanismos de seguridad, puede ser muy segura y además permite una configuración flexible para los usuarios, además por ser herramientas basadas en Software Libre, los costos de implementación de una Red Privada Virtual se verían potencialmente reducidos, siendo este un factor clave a la hora de montar una red como estas.

Es cierto que la tarea de configuración de una VPN basada en Software hasta ahora ha sido algo compleja, pero precisamente lo que se busca mediante la elaboración de este proyecto es hacer que la configuración de estas redes pueda ser realizada de una manera amigable, tanto para usuarios con altos conocimientos técnicos como para los que aún no los poseen.

Después de tener bien fundamentados todos los argumentos para definir que tipo de solución emplear, se ha decidido que este proyecto se enfocará en los tipos de solución basados en Software Libre.

2.5. CARACTERÍSTICAS PRINCIPALES A LA HORA DE MONTAR UNA VPN

Una vez definidos los principales factores para realizar el montaje de una VPN, es importante considerar los diferentes riesgos de seguridad que se pueden llegar a presentar, por lo tanto el primer paso para el montaje de una VPN es considerar la seguridad.

2.5.1. La Seguridad de la conexión

El tráfico OpenVPN que fluye a través de la Internet es protegido por TLS. La configuración aquí usa intercambio de llave pública; la autenticación del computador es realizada por medio de intercambio de llaves públicas y privadas basado en RSA (las llaves públicas también son llamadas certificados). En esta configuración se debe crear un certificado principal propio para así tener una red confiable. Además se debe crear un servidor de llaves pares y pares de llaves para clientes múltiples. La configuración es la criptografía básica de diseño de OpenVPN.

2.5.2. La Seguridad del servidor

El servidor OpenVPN, puede ser víctima de ataques. Este riesgo puede ser minimizado mediante estos consejos:

- Usando llaves compartidas con la opción de autenticación TLS antes de que ocurra el intercambio de llaves públicas. Haciendo esto, impide que las personas se aprovechen de la configuración SSL, si es que esto es posible.
- Configurando las opciones del usuario y de grupo como: nobody. Esto garantiza que el servidor no corra como root.
- Usando un espacio separado en una DMZ (Zona Desmilitarizada). De esta manera un hacker habilidoso es frenado por la protección interna que proporciona el firewall de la DMZ. Las conexiones extrañas serán notificadas en el login del firewall.
- Empleando las reglas de firewall iptables en el servidor OpenVPN para prevenir que el tráfico que viaja a través del túnel desde los hosts entre al

servidor, así como todo el tráfico de Internet a excepción del tráfico UDP necesario.

2.5.3. Autenticación de Usuarios

La configuración segura de los computadores de los clientes es crítica. Si los teletrabajadores pueden acceder la red de la compañía por medio de sus computadores, la información puede volverse pública en un futuro. No importa que tan bueno sea el cifrado SSL, éste es un riesgo separado. Si una computadora puede conectarse a través de un túnel de una OpenVPN directamente con la red de la compañía, se tiene un problema. Para evitar que esto suceda, se necesita establecer autenticación de los usuarios a la computadora o a las llaves SSL.

2.6. PRINCIPALES PROTOCOLOS EMPLEADOS EN LA CONSTRUCCIÓN DE VPNS

Existen varias tecnologías desarrolladas que permiten la creación de Redes Privadas Virtuales. Dadas las ventajas de la implementación de éste tipo de redes por medio de soluciones basadas en Software frente a sus homólogas realizadas por hardware, se decidió que éste tipo de redes serán la base para el desarrollo de los siguientes capítulos de éste documento, por lo tanto se hará una descripción de los protocolos más reconocidos en el medio para llevar a cabo tareas que permitan implementar Redes Privadas Virtuales; según información recopilada a través de Internet los protocolos que permiten la creación de redes con estas características son los siguientes:

- IPSec
- PPTP
- L2TP
- SSH
- SSL/TLS

2.6.1. IPSec

Según información obtenida en Wikipedia[3], se puede definir IPsec (la abreviatura de Internet Protocol Security) como una extensión al protocolo IP que añade cifrado fuerte para permitir servicios de autenticación y cifrado y, de esta manera, asegurar las comunicaciones a través de dicho protocolo. Inicialmente fue desarrollado para usarse con el nuevo estándar IPv6, aunque posteriormente se adaptó a IPv4.

IPsec actúa a nivel de capa de red, protegiendo y autenticando los paquetes IP entre los equipos participantes en la comunidad, no está ligado a ningún algoritmo de cifrado o autenticación, tecnología de claves o algoritmos de seguridad específico. IPSec es un marco de estándares que permite que cualquier nuevo algoritmo sea introducido sin la necesidad de cambiar los estándares.

IPsec proporciona: Confidencialidad, integridad y autenticación. Por sus características y por el uso que se le ha venido dando es el protocolo estándar para la construcción de Redes Privadas Virtuales.

IPSec hace posible la creación de “túneles” seguros entre dos gateways –típicamente un router, cortafuegos o, incluso, software sobre un PC conectado a la red privada del usuario– a través de redes públicas. Los túneles IPSec son establecidos dinámicamente y liberados cuando no están en uso. Para establecer un túnel, los dos gateways IPSec han de autenticarse entre sí y definir cuáles serán los algoritmos de seguridad y las claves que utilizarán. Así, IPSec proporciona comunicaciones seguras y la separación lógica entre los flujos del tráfico de la Red Privada Virtual (VPN) frente al resto de las transmisiones que cursan la red IP compartida.

IPSec cuenta con dos protocolos diferentes, de esta manera, se emplea uno u otro de acuerdo a lo que se interese proteger y el modo en que se realice la comunicación. Estos protocolos son los siguientes:

Cabecera de Autenticación (Authentication Header, AH). Se trata de una nueva cabecera que se obtiene de la básica IP y que se añade a los resúmenes criptográficos ("hash") de los datos e información de identificación.

Encapsulado de Seguridad (Encapsulating Security Payload, ESP).
Permite reescribir los datos en modo cifrado. No considera los campos de la cabecera IP por lo que sólo garantiza la integridad de los datos.

Ambos protocolos controlan el acceso y distribuyen las claves criptográficas. No pueden ser aplicados los dos a la vez. Lo que sí se permite es aplicarlos uno

[3] http://es.wikipedia.org/wiki/IPsec Fecha Consulta 15122026

después de otro, es decir, a un datagrama IP aplicarle un protocolo y al paquete resultante aplicarle otro. Cada uno de estos protocolos puede funcionar en dos modos distintos:

Modo transporte es el que usa un anfitrión que genera paquetes. En modo transporte, las cabeceras de seguridad se añaden antes que las cabeceras de la capa de transporte (TCP, UDP), y antes de que la cabecera IP sea añadida al paquete.

Modo Túnel se usa cuando la cabecera IP extremo-a-extremo ya ha sido adjuntada al paquete, y uno de los extremos de la conexión segura es solamente una pasarela.

Según la información recopilada, se encontraron algunas ventajas y desventajas que pueden traer la implementación de un protocolo como es el IPSec, las cuales se describen a continuación.

Ventajas

- Tecnología estándar de VPN.
- Plataformas de hardware (dispositivos, aplicaciones).
- Tecnología bien conocida.
- Existen muchos GUIs para su administración.

Desventajas

- Los equipos que hacen posible la creación de la VPN, deben estar conectados directamente a Internet, por tanto no pueden estar detrás de una NAT.
- Según la experiencia de muchos usuarios, su configuración puede ser muy complicada debido a que se deben editar un sin número de archivos de configuración.
- No es posible emplear IPs dinámicas. Además no es posible consultar dominios mediante este protocolo.
- Al tener que modificar una gran cantidad de archivos de configuración, para su puesta en marcha, el costo de su mantenimiento es más significativo.
- En ocasiones implementaciones hechas por diferentes fabricantes, resultan incompatibles entre si.
- Para lograr la comunicación se requieren varios puertos, además de la utilización de diferentes protocolos en el cortafuego.

2.6.2. PPTP:

PPTP (Point to Point Tunneling Protocol). Fue desarrollado por Microsoft, U.S. Robotics, Ascend Communications, 3Com/Primary Access, ECI Telematics conocidas colectivamente como PPTP Forum y fue usado para establecer túneles VPNs a través de Internet. Este protocolo les permite a los usuarios remotos acceder a la red corporativa desde cualquier punto en Internet.

PPTP usa un modelo cliente-servidor para establecer las conexiones VPN. La mayoría de los sistemas operativos de Microsoft navegan con un cliente PPTP, por eso no se necesita comprar un software para el cliente.

Para poder conectar clientes PPTP a servidores GNU/Linux, es necesario emplear el servidor Poptop.

Usando Poptop, los servidores GNU/Linux pueden funcionar de manera similar en un ambiente VPN bajo PPTP. Esto permite a los administradores emplear los beneficios de ambos sistemas operativos (GNU/Linux y Microsoft).

La versión actual soporta clientes GNU/Linux PPTP y clientes Windows 95/98/Me/NT/2000/XP PPTP.

Desventajas

- Se encontró en algunos foros en la red, que debido a errores de implementación la información que ha sido cifrada puede ser leída por personas no autorizadas.
- Los algoritmos que emplea para resumir los passwords (hashing) son débiles y permiten que atacantes puedan descubrir las claves de los usuarios.
- El uso de passwords comunes producen llaves vulnerables, aun si se está empleando cifrado de 128-bit.
- Mensajes no autenticados permiten a los atacantes tumbar servidores PPTP.
- La seguridad de PPTP ha sido completamente rota.
- Los ataques a PPTP no pueden ser detectados por el cliente o el servidor porque el exploit es pasivo.
- Tiene fallas por tener errores de diseño en la criptografía en los protocolos de saludo (handshake) y por las limitaciones de la longitud de la clave.
- La actualización de PPTP para las plataformas Microsoft viene por parte de L2TP o IPsec.

2.6.3. L2TP (Layer 2 Tunneling Protocol)

De acuerdo a consultas realizadas en Wikipedia[4], el protocolo L2TP fue diseñado por un grupo de trabajo de IETF como el heredero aparente de los protocolos PPTP y L2F (Layer 2 Forwarding), creado para corregir las deficiencias de estos protocolos y establecerse como un estándar aprobado por el IETF. L2TP utiliza PPP para proporcionar acceso telefónico que puede ser dirigido a través de un túnel por Internet hasta un punto determinado. L2TP define su propio protocolo de establecimiento de túneles, basado en L2F. El transporte de L2TP está definido para una gran variedad de tipos de paquete, incluyendo X.25, Frame Relay y ATM.

Al utilizar PPP para el establecimiento telefónico de enlaces, L2TP incluye los mecanismos de autenticación de PPP, PAP y CHAP. De forma similar a PPTP, soporta la utilización de estos protocolos de autenticación, como RADIUS.

A pesar de que L2TP ofrece un acceso económico, con soporte multiprotocolo y acceso a redes de área local remotas, no presenta unas características criptográficas especialmente robustas.

A causa de ciertas desventajas que presenta este protocolo, el grupo del IETF que trabaja en el desarrollo de PPP consideró la forma de solventarlos. Ante la opción de crear un nuevo conjunto de protocolos para L2TP del mismo estilo de los que se están realizando para IPSec, y dado la duplicación del trabajo respecto al propio grupo de desarrollo de IPSec que supondría, se tomó la decisión de utilizar los propios protocolos IPSec para proteger los datos que viajan por un túnel L2TP.

Desventajas

- Sólo realiza la operación de autenticación entre los puntos finales del túnel, pero no para cada uno de los paquetes que viajan por él. Esto puede dar lugar a suplantaciones de identidad en algún punto interior al túnel.
- Sin comprobación de la integridad de cada paquete, es posible realizar un ataque de denegación del servicio por medio de mensajes falsos de control que den por acabado el túnel L2TP o la conexión PPP subyacente.
- L2TP no cifra en principio el tráfico de datos de usuario, lo cual puede dar problemas cuando sea importante mantener la confidencialidad de los mismos.
- A pesar que la información contenida en los paquetes PPP puede ser cifrada, este protocolo no dispone de mecanismos para generación automática de claves, o refresco automático de claves. Esto puede hacer

[4] http://es.wikipedia.org/wiki/L2TP Fecha Consulta 10122026

que alguien que escuche en la red y descubra una única clave tenga acceso a todos los datos transmitidos.

2.6.4. SSH

En base a consultas en Wikipedia[5], se obtuvo que SSH (Secure SHell) es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red. Permite manejar por completo el ordenador mediante un intérprete de comandos, y también puede redirigir el tráfico de X (servidor que permite dotar de una interfaz gráfica los entornos Unix) para poder ejecutar programas gráficos en el caso de tener un Servidor X arrancado.

Además de la conexión a otras máquinas, SSH permite copiar datos de forma segura (tanto ficheros sueltos como simular sesiones FTP cifradas), gestionar claves RSA para no escribir claves al conectar a las máquinas y pasar los datos de cualquier otra aplicación por un canal seguro de SSH.

En cuanto a seguridad, se puede decir que SSH trabaja de forma similar a como se hace con telnet. La diferencia principal es que SSH usa técnicas de cifrado que hacen que la información que viaja por el medio de comunicación vaya de manera no legible y ninguna tercera persona pueda descubrir el usuario y contraseña de la conexión ni lo que se escribe durante toda la sesión; aunque es posible atacar este tipo de sistemas por medio de ataques de replay y manipular así la información entre destinos.

En un principio sólo existían los r-commands, que eran los basados en el programa rlogin, el cual funciona de una forma similar a telnet.

La primera versión del protocolo y el programa eran libres y los creó un sueco llamado Tatu Ylönen, pero su licencia fue cambiando y terminó apareciendo la compañía `SSH Communications Security', que lo ofrecía gratuitamente para uso doméstico y académico, pero exigía el pago a empresas. En el año 1997 (dos años después de que se creara la primera versión) se propuso como borrador en la IETF.

A principios de 1999 se empezó a escribir una versión que se convertiría en la implementación libre por excelencia, la de OpenBSD, llamada OpenSSH.

Ventajas:

[5] http://es.wikipedia.org/wiki/Secure_Shell#Manejo_de_SSH Fecha Consulta 10122026

- Crea un túnel de forma nativa y transparente conexiones X11.
- Comprime con gzip.
- Instalado en la mayoría de los equipos Unix.
- Ideal para hacer túneles para resolver problemas puntuales.
- Soportado bajo Windows con cygwin.

Desventajas

- Su objetivo principal no es hacer túneles.
- Hay que tener mucho cuidado al configurarlo. No se deben dar privilegios al usuario que crea el túnel.
- El cliente del túnel no corre como demonio, es necesario hacer scripts para verificar que no muera, iniciarlo automáticamente, etc.
- No soporta UDP.
- Crea el túnel sobre TCP.

2.6.5. SSL/TLS (Secure Socket Layer) (Transport Layer Secure)

Gracias a Daniel Sepúlveda y Tejedores del Web por su artículo en Internet[6], se puede concluir que el protocolo SSL fue desarrollado por Netscape para permitir confidencialidad y autenticación en Internet. SSL se encuentra una capa por debajo de HTTP y tal como lo indica su nombre está a nivel de socket por lo que permite ser usado no sólo para proteger documentos de hipertexto sino también servicios como FTP (File Transfer Protocol), SMTP (Simple Mail Transport Protocol), TELNET entre otros.

La idea que persigue SSL es cifrar la comunicación entre servidor y cliente mediante el uso de llaves y algoritmos de cifrado.

Habitualmente, sólo el servidor es autentificado (es decir, se garantiza su identidad) mientras que el cliente se mantiene sin autentificar; la autenticación mutua requiere un despliegue de infraestructura de claves públicas (o PKI) para los clientes. Los protocolos permiten a las aplicaciones cliente-servidor comunicarse de una forma diseñada para prevenir escuchas (eavesdropping), la falsificación de la identidad del remitente y mantener la integridad del mensaje.

SSL implica una serie de fases básicas:

---

6 http://www.tejedoresdelweb.com/307/article-5670.html Fecha Consulta 10122026

- Negociar entre las partes el algoritmo que se usará en la comunicación.
- Intercambio de claves públicas y autenticación basada en certificados digitales.
- Cifrado del tráfico basado en cifrado simétrico.

Durante la primera fase, el cliente y el servidor negocian qué algoritmos criptográficos se van a emplear. Las implementaciones actuales proporcionan las siguientes opciones:

- Para criptografía de clave pública: RSA, Difie-Hellman, DSA (Digital Signatura Algorithm) o Fortezza.
- Para cifrado simétrico: RC2, RC4, IDEA (International Data Encryption Algorithm), DES (Data Encryption Standard), Triple DES o AES (Advanced Encryption Standard).
- Con funciones hash: MD5 o de la familia SHA.

SSL/TLS poseen una variedad de medidas de seguridad:

- Numerando todos los registros y usando el número de secuencia en la MAC.
- Usando un resumen de mensaje mejorado con una clave (de forma que solo con dicha clave se pueda comprobar la MAC).
- Protección contra varios ataques conocidos (incluidos ataques man in the middle), como los que implican un degradado del protocolo a versiones previas (por tanto, menos seguras), o conjuntos de cifrados más débiles.
- El mensaje que finaliza el protocolo handshake (Finished) envía un hash de todos los datos intercambiados y vistos por ambas partes.
- La función seudo aleatoria divide los datos de entrada en 2 mitades y las procesa con algoritmos hash diferentes (MD5 y SHA), después realiza sobre ellos una operación XOR. De esta forma se protege a sí mismo de la eventualidad de que alguno de estos algoritmos se revelen vulnerables en el futuro.

Es importante señalar que ambos protocolos se ejecutan sobre una capa de transporte definida, pero no determinada. Esto indica que pueden ser utilizados para cualquier tipo de comunicaciones. La capa de transporte más usada es TCP sobre la cual pueden implementar seguridad en HTTP (HyperText Transfer Protocol).

SSL también puede ser usado para hacer pasar por un túnel a una red completa y crear una red privada virtual (VPN), como en el caso de OpenVPN.

3. APLICACIONES EXISTENTES

Existe una amplia gama de implementaciones de Redes Privadas Virtuales basadas en Software, entre las cuales se encuentran aplicaciones tanto de tipo comercial como de libre distribución; para efectos de este documento no es fundamental el estudio de aplicaciones propietarias ya que estas no permiten el estudio de su código y además resultan mucho más costosas que las aplicaciones libres, por lo tanto, en adelante sólo se mencionarán las aplicaciones de tipo libre. En este orden de ideas se describirán las herramientas más utilizadas con sus ventajas e inconvenientes, para finalmente elegir aquella que brinde mejores características en cuanto a seguridad, fiabilidad, desempeño entre otras, frente a las demás herramientas expuestas.

3.1. DESCRIPCIÓN DE LOS PRODUCTOS DE SOFTWARE

A continuación serán descritas las aplicaciones que permiten la implementación de Redes Privadas Virtuales más reconocidas en el medio:

- FreeS/WAN
- StrongSwan
- OpenS/WAN
- OpenSSH
- Stunnel
- OpenVPN

3.1.1. FreeS/WAN (Free Secure Wide-Area Networking):

Es una implementación de IPSec & IKE para GNU/Linux y otros sistemas operativos como Unix. El objetivo de éste proyecto de cifrado universal del tráfico de Internet no fue realizado, aunque contribuyó al cifrado general de Internet.

La última versión 2.06 de FreeS/WAN fue liberada el 22 de abril de 2003. La versión anterior 2.04 fue empleada para formar parte de dos proyectos, Openswan y strongSwan.

3.1.2. StrongSwan:

Gracias a un articulo publicado por Andreas Steffen del Instituto de Tecnologías y Aplicaciones en Internet[7], se obtuvo información suficiente para concluir que StrongSwan es una implementación de código abierto de IPSec para los sistemas operativos GNU/Linux. Está basado en el proyecto ya descontinuado de FreeS/WAN y el certificado de autenticación X.509 el cuál ha sido desarrollado durante los últimos tres años. En busca de obtener una plataforma IPSec estable para poder basar futuras extensiones sobre la capacidad del certificado X.509, por lo tanto se decidió lanzar el proyecto strongSwan.

El proyecto se enfoca en:

- Simplicidad en la configuración
- Métodos de autenticación y cifrado fuerte
- Fuertes políticas de IPSec soportando complejas redes VPNs.
- Jerarquías de certificados o membresías de grupos definidas por el certificado X.509.
- Revocación de certificados basados en protocolos de certificado de estado en línea.
- Asignación de direcciones IP virtuales.
- Soporte de smartcard.
- Dead Peer Detection.

El desarrollador del proyecto strongSwan es Andreas Steffen, el cuál es un profesor de seguridad en comunicaciones y cabeza del “Instituto para Tecnologías y Aplicaciones en Internet” en la Universidad de Ciencias Aplicadas Rapperswil en Suiza y presidente de la firma de consultoría strongSec GmbH.

---

7 http://www.strongswan.org/docs/LinuxTag2005-strongSwan.pdf Fecha Consulta 20122006

La distribución de strongSwan revela todo un ambiente basado en certificados de infraestructura de llave pública, haciendo uso del manejo de llaves privadas por medio de tarjetas inteligentes.

Una característica única de strongSwan es la posibilidad de definir políticas de IPSec basadas en un grupo de atributos que pueden ser desplegados de manera segura poniéndolos en los atributos de los certificados X.509.

Características

- Corre en los kernels de GNU/Linux 2.4 y 2.6.
- Inicio de conexión y periodos de actualización rápidos, empleando el iniciador de IPsec.
- Borrado e inserción automática de las políticas de IPSec basado en reglas del firewall.
- Cifrado fuerte 3DES, AES, Serpent o Blowfish.
- Soporta NAT vía encapsulamiento UDP.
- IPs estáticas y virtuales e intercambio de llaves (IKE).
- Muerte por detección.
- Autenticación basada en el certificado X.509 o llaves precompartidas.
- Generación de un certificado por defecto durante el primer inicio de strongSwan.
- Recuperación y captura local de listas de certificados de revocación a través de HTTP o LDAP.
- Soporte completo del protocolo de estado de certificados en línea.
- Almacenamiento opcional de llaves privadas RSA y certificados en tarjetas inteligentes.
- Acceso de tarjetas inteligentes a través de interfaces estandarizadas.

3.1.3. OpenS/WAN:

Openswan es una implementación de IPsec para GNU/Linux. Este soporta kernels 2.0, 2.2, 2.4 y 2.6, y corre en muchas plataformas diferentes, incluye x86, x86_64, ia64, MIPS y ARM, además de esto opera entre diferentes Sistemas Operativos e incluso con implementaciones de routers IPSec.

Ventajas:
La seguridad, ya que el protocolo IPSec es robusto, poderoso y bien diseñado.
La Interoperabilidad, madurez y flexibilidad.

Desventajas:
La Complejidad de la herramienta.

3.1.4. OpenSSH:

Gracias a los aportes de Wikipedia[8], se puede concluir que (Open Secure Shell) es un conjunto de aplicaciones que permiten realizar comunicaciones cifradas a través de una red, usando el protocolo SSH. Fue creado como una alternativa libre y abierta al programa Secure Shell, que es software propietario. El proyecto está liderado por Theo de Raadt, de Calgary.

Sus desarrolladores aseguran que OpenSSH es más seguro que el original, lo cual es debido a la conocida reputación de los desarrolladores de OpenBSD por crear código limpio y perfectamente auditado, lo que contribuye a que sea más seguro. Su seguridad también es atribuible al hecho de que su código fuente se distribuya libremente con una licencia BSD. Aunque todo el código fuente del SSH original también está disponible, existen restricciones con respecto a su uso y distribución, lo que convierte a OpenSSH en un proyecto mucho más atractivo a la hora de atraer nuevos desarrolladores.

Portabilidad
Como OpenSSH es una aplicación de comunicación entre ordenadores, debe funcionar en la mayor cantidad de sistemas operativos posibles, para lo que existe un equipo, llamado OpenSSH Portability Team que se responsabiliza de añadir el código necesario para portar el software a todas las plataformas posibles.

3.1.5. Stunnel (Universal SSL Wrapper):

Stunnel es un programa que permite cifrar arbitrariamente conexiones TCP sobre SSL (Secure Sockets Layer) disponible en Unix y Windows. Stunnel también le permite asegurar demonios y protocolos no-SSL como (POP, IMAP, LDAP, etc.) empleando un Stunnel se provee cifrado sin requerir cambios en el código de los demonios.

---

8 http://es.wikipedia.org/wiki/OpenSSH Fecha Consulta 20122026

El código fuente de Stunnel no es un producto completo, todavía se requieren librerías SSL como OpenSSL o SSLeay para compilar Stunnel. Esto quiere decir que Stunnel soporta sólo lo que la librería SSL pueda soportar sin tener que hacerle ningún cambio al código de Stunnel.

El código fuente de Stunnel es disponible bajo la licencia general pública (GNU), lo que significa que puede emplearse para aplicaciones comerciales y no comerciales siempre y cuando se entregue el código fuente con todas sus modificaciones.

Interoperatibilidad:
Depende solo de openssl y tcpwrappers.
Compila en todos los Unix, FreeBSD, GNU/linux.
Compila bajo Win NT/2000/XP.
Algoritmos usados: Autenticación X 509, y todos los algoritmos soportados por OpenSSL.

Ventajas:
Permite dar soporte SSL a servidores que no tienen SSL de manera nativa. (imaps, https, etc.)
Una sola instancia del demonio puede atender varios túneles.
Soporta chroot en forma nativa.

Inconvenientes:
Un hilo por conexión, usar solo con kernel 2.6
No soporta UDP.
Crea los túneles sobre TCP (usar opción TCP_NODELAY=1).

3.1.6. OpenVPN

En base a la página principal de OpenVPN[9], se pudo obtener la siguiente información:

OpenVPN es una solución de conectividad basada en software: SSL (Secure Sockets Layer) VPN Virtual Private Network (Red Privada Virtual), OpenVPN ofrece conectividad punto-a-punto con validación, jerárquica de usuarios y host conectados remotamente, resulta una muy buena opción en tecnologías Wi-Fi (redes inalámbricas EEI 802.11) y soporta una amplia configuración, entre ellas balanceo de cargas. Está publicado bajo licencia de código-abierto GPL.

[9] http://openvpn.net/ Fecha Consulta 03122006

Algunas de sus ventajas son:

Implementación de la VPN en la capa 2 y la capa 3 del modelo OSI: OpenVPN ofrece dos modos básicos, de funcionamiento como la capa 2 o capa 3. Así los túneles de OpenVPN pueden también transportar tramas de Ethernet, los paquetes del IPX, y los paquetes del navegador de la red de Windows (NETBIOS), que son un problema en la mayoría de las otras soluciones de VPN.

Protección de sesión con el cortafuego interno: Una sesión conectada con la oficina central de una compañía con un túnel VPN puede cambiar la configuración (setup) de la red en un ordenador portátil, para enviar todo el tráfico de la red a través del túnel. Una vez que OpenVPN haya establecido un túnel, el cortafuego central en la oficina central de la compañía puede proteger el ordenador portátil, aún cuando él no sea una máquina local. Solamente un puerto de la red se debe abrir en local para trabajar la sesión. El cortafuego central protege al empleado siempre que la persona esté conectada a través de la VPN.

Las conexiones de OpenVPN pueden ser establecidas a través de casi cualquier cortafuego: Si se tiene acceso a Internet y si se puede tener acceso a la Web, los túneles de OpenVPN deben de trabajar.

Soporte de Proxy y configuraciones: OpenVPN tiene soporte de Proxy y se puede configurar para funcionar como un servicio de TCP o de UDP, y como servidor o cliente. Como servidor, OpenVPN espera simplemente hasta que un cliente solicita una conexión, mientras que como cliente, intenta establecer una conexión según su configuración.

Apertura de un solo puerto en el cortafuego para permitir conexiones entrantes: Desde OpenVPN 2.0, el modo especial del servidor permite conexiones entrantes múltiples en el mismo puerto del TCP o del UDP, mientras que todavía usa diversas configuraciones para cada conexión.

Las interfaces virtuales permiten reglas muy específicas del establecimiento de una red y del cortafuego: Todas las reglas, restricciones, mecanismos de la expedición, y conceptos como NAT se pueden utilizar con los túneles de OpenVPN.

Alta flexibilidad con posibilidades extensas de lenguaje interpretado (scripting): OpenVPN ofrece numerosos puntos durante la conexión para la ejecución de los scripts individuales. Estos scripts se pueden utilizar para una gran variedad de propósitos como la autenticación, recuperación en caso de fallos (failover) entre otros.

Soporte transparente y alto rendimiento para IPs dinámicas: Si se usa OpenVPN, no hay necesidad de utilizar más IPs estáticas de cualquier lado del túnel. Ambas puntos finales del túnel pueden tener acceso barato de ADSL con las IPs dinámicas y los usuarios no notarán un cambio de IP de cualquier lado. Las sesiones del Terminal Server de Windows y las sesiones seguras de Shell (SSH) parecerán congeladas solamente por algunos segundos, pero no terminarán y continuarán con la acción solicitada después de una corta pausa.

Ningún problema con NAT: El servidor y los clientes de OpenVPN pueden estar dentro de una red usando solamente direcciones privadas IP. Cada cortafuego se puede utilizar para enviar el tráfico del túnel al otro punto final del túnel.

Instalación simple en cualquier plataforma: La instalación y el uso son increíblemente simples. Especialmente, si ha intentado instalar IPsec con diversas configuraciones, se apreciará la facilidad de instalación de OpenVPN.

Diseño modular: El diseño modular con un alto grado de simplicidad en seguridad y establecimiento de una red es excepcional. Ninguna otra solución de VPN puede ofrecer la misma gama de posibilidades a este nivel de seguridad.

Además con la versión 2.0 se incorporaron las siguientes mejoras:

Soporte Multi-cliente: OpenVPN ofrece un modo de conexión especial, donde proporciona a los clientes TLS-autenticados al estilo DHCP de IPs en el establecimiento de la red (túnel). De esta manera, varios túneles (hasta 128) pueden comunicarse sobre el mismo puerto del TCP o UDP. Obviamente, es necesario activar un switch para activar el modo servidor.

Opciones de Envío/Recepción: La configuración de la red de clientes puede ser controlada por el servidor. Después de la configuración correcta del túnel, el servidor puede decir al cliente (Windows y Linux) que utilice una configuración diferente de red instantáneamente.

Interfaz de control (Telnet): Se ha añadido una interfaz de control vía Telnet.

El driver y el software de Windows se han mejorado extensamente.

3.2. ¿QUE TECNOLOGÍA EMPLEAR?

Gracias a toda la información recopilada de tecnologías existentes para la implementación de VPNs mencionada en los puntos anteriores de éste capítulo,

se decidió realizar un análisis comparativo entre las herramientas líderes en el medio, las cuales son: IPsec por ser el estándar empleado en la mayoría de las VPN implementadas hasta ahora y SSL por ser el protocolo que está adquiriendo cada vez más, mayor aceptación en el campo de las VPNs.

3.2.1. IPSec vs SSL

Con la información anteriormente obtenida, se pueden mencionar las características más relevantes de cada una de estas herramientas las cuales se presentan a continuación y de esta manara permitir conocer cual puede ofrecer mejores ventajas para así asegurar una buena elección del tipo de tecnología a emplear.

Simplicidad vs. Versatilidad

SSL permite una configuración simple, pero parte de esta simplicidad exige renunciar a algunas de las prestaciones típicas que aporta IPSec; por ejemplo, las VPN basadas en SSL no soportan las aplicaciones cliente/servidor heredadas. Pero las soluciones están en camino y, además, pueden tratar la mayor parte del tráfico que el resto de redes privadas virtuales. Y, al final, como siempre, todo dependerá de las funciones específicas de cada organización.

El protocolo SSL –utilizado en las transacciones financieras por Internet– está presente en una gran mayoría de los PC corporativos dotados de navegadores Web. Para que estas máquinas remotas trabajen con VPN SSL no requieren ni software adicional ni mantenimiento. Además, SSL ofrece cifrado de 168 bits, igual al cifrado Triple-Des utilizado por IPSec.

Las nuevas firmas basan sus soluciones en la instalación de servidores entre los PCs remotos y el servidor de la LAN corporativa. Este servidor intermediario establece una conexión SSL en la máquina remota, dando a ese enlace Web un enlace al servidor de datos, haciendo accesible la red de la empresa desde Internet. El tráfico Web seguro llega a través del cortafuego corporativo por un único puerto SSL que puede ser configurado para que sólo permita acceder al servidor intermediario.

Por el contrario, el acceso remoto IPSec requiere instalar y mantener un cliente remoto configurado con los parámetros de seguridad correctos. Estos clientes remotos y el gateway VPN han de ser integrados con el cortafuego, complicando la tarea del personal técnico.

Esta ventaja de una mayor simplicidad juega a favor de las soluciones SSL. No en vano, según IDC (Internacional Data Corporation), alrededor de un 14% de los usuarios que no utilizan todavía VPN IP dicen no estar considerando las Redes Privadas Virtuales por su falta de madurez y un 13% por su excesiva complejidad.

3.2.1.1. IPSec

Ventajas: Muy seguro, basado en estándares y muy adecuado para tráficos totalmente IP. Es un protocolo muy probado y es bien soportado por muchos enrutadores comerciales. Asegura de manera fácil que puede y que no puede ir a través de un túnel a nivel del kernel sin tener que realizar configuraciones adicionales a las reglas del firewall. Es muy flexible para la configuración de subredes.

Desventajas: Interoperatividad incompleta, costos de mantenimiento y falta de ubicuidad. Puede ser complicada la configuración y la puesta en marcha. Además no trabaja con algunos gateways NAT.

3.2.1.2. SSL

Ventajas: Bajos costos de mantenimiento (ya presente en los navegadores), no requiere mantenimiento en los clientes y buena interoperatividad. Fácil configuración, solo necesita un puerto TCP o UDP. Es un protocolo muy maduro. Disponible para la mayoría de sistemas operativos incluido Windows. Opciones de configuración flexibles.

Desventajas: No soporta aplicaciones en tiempo real y no permite compartir ficheros. Requiere mayor configuración del firewall que IPSec para controlar el acceso a los recursos internos. No es soportada en los concentradores VPN más comerciales.

Después de haber realizado la anterior exposición acerca de las ventajas y desventajas de las tecnologías OpenVPN e IPSec, en el siguiente punto de este capítulo, se presentará una tabla que las resume para poder ser apreciadas de una mejor manera.

3.3. ANÁLISIS COMPARATIVO ENTRE OPENVPN Y APLICACIONES VPN SOBRE IPSEC

A continuación se presenta un análisis comparativo entre las dos tecnologías para de esta manera tener los argumentos suficientes para determinar cual de ellas es mas apropiada.

Aplicaciones VPN sobre IPsec	**OpenVPN**
VENTAJAS	**DESVENTAJAS**
Reconocida como la tecnología estándar de VPN	Considerado como una tecnología relativamente nueva (todavía creciendo y en aumento) no compatible con IPsec.
Embebido en un gran número de dispositivos Hardware.	Exclusivo para computadores, pero opera en todos los S.O.
Para su administración se encuentra una gran variedad de GUIs.	Las GUIs todavía se encuentran en desarrollo, pero dentro de proyectos prometedores.
DESVENTAJAS	**VENTAJAS**
Se requiere realizar una modificación compleja a la pila IP y al núcleo de GNU/Linux.	Es una tecnología simple, fácil de configurar, además funciona en el espacio del usuario, por lo tanto puede ser chroot-ed.
Para su operación se requieren privilegios de administración.	Por medio de la ayuda de comandos puede operar como usuario normal tanto como un usuario con privilegios de administración
Diversas implementaciones de Ipsec de diversos fabricantes pueden ser incompatibles	Usa tecnologías estandarizadas de cifrado
Configuración compleja, tecnología compleja	Tecnología fácil, bien estructurada, modular, configuración fácil
Curva grande de aprendizaje para los novatos	Fácil de aprender, éxito rápido para los novatos
Son necesarios varios puertos y protocolos en el cortafuego	Solamente es necesario un puerto en el cortafuego
Problemas con direcciones dinámicas	DynDNS trabaja enteramente, vuelve a

Aplicaciones VPN sobre IPsec	OpenVPN
en ambos lados	conectar más rápidamente
Problemas de seguridad con las tecnologías de IPsec	SSL/TLS como capa criptográfica estándar industrial
	Trafic shaping (Control de tráfico)
	Velocidad (hasta 20 Mbps en una máquina de un 1Ghz)
	Compatibilidad con los cortafuegos y los proxys
	Ningun problema al realizar NAT (ambos lados pueden estar en las redes NAT)
	Permite brindarle acceso a nodos viajantes, es decir que se desplazan físicamente (road warriors)

Tabla Open VPN Versus IPSec

3.4. CONCLUSIONES DEL ANALISIS

De los dos tipos de redes privadas virtuales analizadas cabe resaltar que IPsec se considera un estándar dentro de la industria y está ampliamente difundida e instalada, en cuanto a OpenVPN, se puede decir que es una herramienta que ha tenido críticas favorables en la documentación consultada. De estas dos herramientas, se ha decidido seleccionar la segunda opción, siendo las razones desfavorables de más peso de la primera las siguientes:

- Proceso de instalación y configuración muy complicado.
- Es necesaria la recompilación del núcleo en el caso de GNU/Linux.
- Una mala configuración puede dar problemas de seguridad (una excepción en la ejecución abre un shell con privilegios de root).

En el caso de la OpenVPN las razones que han hecho que sea la herramienta seleccionada son las siguientes:

- Fácil instalación y configuración.
- Está publicado bajo la licencia GPL, de código abierto.
- El sistema de criptografía se basa en OpenSSL.

- Es multiplataforma corriendo en los sistemas: GNU/Linux, Windows 2000/XP y superiores, OpenBSD, FreeBSD, NetBSD, Mac OS X, Solaris y OpenVPN PocketPC port esta en desarrollo.

Por todo lo anteriormente mencionado, la opción elegida es OpenVPN.

4. EJEMPLO APLICADO

A lo largo de este capítulo se tratarán temas más enfocados en la aplicación a implementar, se mencionará la manera como se han venido configurando las Redes Privadas Virtuales hasta ahora de manera detallada, esto como fundamento para dar paso a una ilustración del diseño de la interfaz la cual permitirá crear la configuración de dicha red, esta ilustración trae consigo la Ingeniería de Software apropiada para el tipo de aplicación, un ejemplo con un caso práctico y pruebas funcionales de la aplicación.

4.1. CONFIGURACIÓN TRADICIONAL DE OPENVPN

A continuación se mostrará el procedimiento para la implementación de una Red Privada Virtual, por tanto se describirá la configuración requerida tanto en el equipo servidor como en el cliente. La configuración de este tipo de redes puede hacerse de varias maneras gracias a la flexibilidad que ofrece la herramienta seleccionada para el montaje; para la configuración de la red, se empleará la generación de certificados de seguridad.

A grandes rasgos el escenario que se va a presentar es el siguiente: Se va a simular un usuario que pertenece a una red en su casa y necesita conectarse de forma remota con la red de la oficina por medio de Internet.

El montaje de la red se hará en equipos con distribuciones Debian de GNU/Linux instaladas; las herramientas requeridas para el montaje son las siguientes:

- OpenVPN
- OpenSSL
- Librería LZO
- Modulo Tun/Tap (para kernel menor a 2.4.7)

4.1.1. INSTALACIÓN DE LAS HERRAMIENTAS

Las distribuciones Debian ofrecen una gran ventaja y es una herramienta que trae incorporada para la instalación de aplicaciones denominada **apt-get**. Sin embargo los paquetes pueden ser instalados directamente con sus fuentes las cuales se encuentran en las páginas oficiales de cada una de las herramientas. A continuación se presentará la instalación de los paquetes por medio de la aplicación apt-get.

Lo primero que hay que hacer es asegurarse de tener la lista de fuentes actualizadas, esto se realiza mediante el comando

apt-get update.

Se puede buscar el paquete a instalar para ver que lanzamientos hay disponibles y así poder decidir que versión instalar. Lo anterior se realiza por medio del comando:

apt-cache search *nombre_paquete.*

Una vez obtenida la lista, se selecciona el paquete apropiado (una versión estable) y se procede a su instalación de la siguiente manera:

apt-get install *nombre_paquete.*

La ventaja al utilizar *apt-get* es que esto resolverá todos los problemas con las dependencias de otros paquetes que se necesiten e informará si se tiene algún problema con algún paquete no encontrado.

Para este caso la instalación de los paquetes se realizo de la siguiente manera:

apt-get update
apt-cache search openvpn
apt-get install openvpn
apt-cache search lzo
apt-get install liblzo1

Debido a que el paquete openssl ya se encuentra dentro de la versión de GNU/Linux instalada, no hubo necesidad de instalarlo, pero de haber sido necesario se habría realizado el mismo proceso que con los otros paquetes.

4.1.2. CONFIGURACIÓN DE LA RED

Como se menciono anteriormente la idea es poder conectar un equipo de una red domestica con la red de la compañía a través de Internet, de esta manera se presentara a continuación la configuración de las interfaces de red para los equipos.

En el servidor:

eth1 (IP / Hostname)	190.65.68.227		
eth0 (Red Interna)	192.168.5.1	Máscara	255.255.255.0
interfáz Tun/Tap	10.8.1.0	Máscara	255.255.255.0
Puerto	1194		

En el cliente:

eth0	201.236.216.4	255.255.255.0	Interfaz que sale a Internet
eth1	192.168.4.1	255.255.255.0	Red Interna
Puerto		1194	

Nota: Si el servidor OpenVPN no es el gateway por defecto hay que habilitar el ruteo para que los paquetes puedan pasar de una interfaz a la otra. Lo cual se hace por medio del siguiente comando:

echo 1 > /proa/sys/net/ipv4/ip_forward

4.1.3. PASOS PARA LA CONFIGURACIÓN DE LA VPN

Anteriormente se definió que la red se va implementar mediante la generación de los certificados de seguridad. Básicamente existen dos formas de implementar seguridad, la primera es basada en SSL/TLS mediante certificados y claves RSA y el otro es por medio de claves estáticas pre-compartidas.

Se decidió usar un sistema de seguridad empleando SSL-TLS ya que es más seguro que por medio de claves estáticas.

Para poder generar certificados se necesita una entidad certificadora. Para este caso se va a crear una CA (Autoridad Certificadora) propia.

A continuación se enumerarán los pasos a seguir a la hora de configurar una VPN creando una CA, los cuales serán descritos de manera detallada a lo largo de este capítulo:

1. Crear el certificado de la CA para en base a el poder firmar y revocar certificados de los clientes.
2. Crear un certificado y una clave pública para el servidor.
3. Crear un certificado y una clave pública para cada cliente.
4. Crear la clave de Diffie-Hellman.
5. Firmar los certificados usando el certificado de la CA.
6. Distribuir la clave y certificados a los clientes empleando un medio seguro.
7. Configurar el script del servidor.
8. Configurar los scripts de los clientes.

4.1.3.1. Creación de los Certificados y Claves RSA

Una vez instalado el OpenVPN, junto con los otros paquetes necesarios para la operación de la VPN, se debe copiar el directorio **easy-rsa** en una ruta que se va a utilizar como directorio de trabajo antes de comenzar con cualquier tipo de configuración; éste directorio se encuentra en la ruta **/usr/share/doc/openvpn/examples/.** Se debe crear una copia de este directorio para que con cualquier tipo de actualización de OpenVPN no sobrescriba las modificaciones realizadas a la configuración de la red. Esto se realiza de la siguiente manera:

mkdir /etc/openvpn
cp /usr/share/doc/openvpn/examples/easy-rsa /etc/openvpn
cd /etc/openvpn/ easy-rsa

Luego de tener el directorio copiado, se debe correr el siguiente archivo batch **init-config** para crear los archivos de configuración en el nuevo directorio, este comando sobrescribe los archivos vars.bat y openss.cnf si existían.

Inmediatamente hay una información que es solicitada para completar la configuración de la Entidad Certificadora (a este proceso se le conoce como "establecimiento del archivo vars"), por lo tanto los campos requeridos deben asignarse de la siguiente manera:

export KEY_COUNTRY=CO
export KEY_PROVINCE=RDA
export KEY_CITY=SantaRosa
export KEY_ORG=IsNET
export KEY_EMAIL="prueba@isnet.midominio"

Cabe resaltar que esta información no tiene que especificarse exactamente como se ha venido indicando, la información sugerida es sólo la que se empleo en el momento de realizar la configuración y con el objetivo de obtener una buena

documentación del proceso es que se recomienda seguir estos pasos como se están indicando. Una vez terminado este paso se debe inicializar el PKI mediante la ejecución de los siguientes comandos:

. ./vars
./clean-all
./build-ca

El último de los anteriores comandos, es el que construye la Autoridad Certificadora (certificado y clave).

Cabe notar que muchos de los parámetros que salen en la secuencia para crear la Entidad Certificadora son los mismos que se pusieron cuando fue establecido el archivo vars, por lo tanto se pueden dejar con su valor por defecto ya especificado, el único parámetro, que debe ser explícitamente digitado es el **Common Name.** Se debe poner **OpenVPN-CA** para especificar que es la Autoridad Certificadora.

Al crearse los certificados, son creados unos archivos en el subdirectorio keys en este paso son *ca.crt* y *ca.key*

4.1.3.2. Creación del Certificado y la Clave para el Servidor

Para la generación del certificado y la llave para el servidor se ejecuta el siguiente comando:

./build-key-server server

Al igual que con la entidad certificadora, unos parámetros son requeridos, pero el que es realmente importante es el **Common Name** debido a que es el mismo que será utilizado “textualmente” en la configuración de los clientes. Se debe poner el mismo nombre que se haya puesto al construir la clave es decir **server.**

Nota: Los nombres escogidos para el servidor, la entidad certificadora y los clientes no tienen que ser los que se especifican en este documento, estos nombres fueron escogidos por ser tan específicos de acuerdo al uso que se les dará.

Luego, aparecen dos preguntas a las que se responde afirmativamente.

Los archivos creados en el subdirectorio keys en este paso son:

server.crt, server.key y *server.csr.*

4.1.3.3. Creación del Certificado y la Clave para el Cliente

Para la creación del certificado y la llave para cada cliente se realiza por medio de la ejecución del siguiente comando:

./build-key cliente1

Los pasos a seguir son muy similares a los del paso anterior, ahora el **Common Name** es: **cliente1** (los nombres escogidos para los clientes, deben ser diferentes).

Los archivos creados en el subdirectorio keys en este paso son:

cliente1.crt, cliente1.key y *cliente1.csr.*

4.1.3.4. Creación de la Clave de Diffie-Hellman

Se realiza por medio del script **build-dh** que se encuentra dentro de la carpeta easy-rsa, este proceso toma unos cuantos minutos.

El archivo que se crea en el subdirectorio keys es dh1024.pem

4.1.3.5. Firmar los Certificados

Para que los certificados sean válidos, tanto el del servidor como el de cada cliente, deben ser firmados por la CA obteniendo así un archivo .crt que es el que se envía a cada máquina junto con el archivo **.key** que ya existe, Para poder hacerlo hay que ejecutar el siguiente script:

./sign-req *nombre*

Para la labor de firmar los certificados se debe tener una máquina, en este caso se empleo el servidor, lo importante es que la máquina escogida para realizar esta tarea es la única que debe tener el archivo **ca.key** que fue creado cuando se creó la entidad certificadora.

4.1.3.6. Distribuir las Claves y los Certificados

Una vez creadas y firmadas todas las claves necesarias para la operación de la VPN, se deben distribuir los archivos generados. Esta distribución debe hacerse de la siguiente manera:

Archivo	Descripción	Ubicación	Secreto
dh1024.pem	Parámetros Diffie Hellman	servidor	-
ca.crt	Certificado raíz CA	servidor y todos los clientes	No
ca.key	Clave raíz CA	únicamente la máquina encargada de firmar	Si
server.crt	Certificado del servidor	servidor	No
server.key	Clave del servidor	servidor	Si
client1.crt	Certificado del cliente	cliente	No
client1.key	Clave del cliente	cliente	Si

Nota: Es muy importante tener en cuenta que el canal por el cual se van a enviar estas claves debe ser totalmente seguro, porque de otro modo, de nada servirá todo el trabajo que se está realizando para garantizar la seguridad de la red.

4.1.3.7. Archivo de Configuración para el Servidor

Dentro de la carpeta de ejemplos de configuración del OpenVPN se encuentra un archivo que puede ser empleado como base para realizar la configuración del servidor; debido a que el archivo se encuentra comprimido, hay que descomprimirlo en una carpeta dentro del directorio de trabajo de la VPN, de la siguiente manera:

cd /etc/openvpn
mkdir ccd
gzip –d /usr/share/doc/openvpn/examples/sample-config-files/server.conf.gz

Una vez obtenido el archivo server.conf, se le debe hacer varias modificaciones con el objetivo de adoptarlo a las necesidades de la VPN.

Los valores mas importantes a tener en cuenta dentro de la configuración del archivo son los siguientes:

Variable	Valor	Comentario
port	1194 (puerto por defecto)	Puede ser cualquier otro, pero los clientes deben saber dicho valor para saber a donde conectarse
proto	udp	También pude ser tcp, el cliente debe configurarse de la misma forma
dev	tun	tun Si se desea crear un túnel IP tap Si se desea crear un túnel ethernet, se emplea para configuraciones más sencillas de clave simétrica pre-compartida.
ca	ca.crt	El certificado CA generado.
cert	server.crt	El certificado generado para el servidor
key	server.key	Clave privada generada para el servidor
dh	dh1024.pem	Parámetros Diffie – Hellman
server	10.8.1.0 255.255.255.0	Red virtual a utilizar. Cada cliente debe poder alcanzar dicha red
keepalive	10 120	Produce mensajes ping cada 10 seg para que el otro lado de la VPN sepa que la conexión sigue activa.
tls-aut	ta.key 0	El servidor y cada cliente, deben tener una copia de esta llave. El segundo parámetro debe ser 0 en el servidor y 1 en los clientes.
comp-lzo		Habilita la compresión en el enlace VPN. Si se habilita en el servidor, también debe habilitarse en el cliente.
status	openvpn-status.log	Crea un archivo de estado mostrando las conexiones actuales y las creadas cada minuto.
verb	3	Establezca el nivel apropiado de verbosidad: 0 silencio 4 razonable 5, 6 para hacer debug 9 muchisima información

4.1.3.8. Archivo de Configuración para el Cliente

Al igual que con el archivo de configuración para el servidor, en la carpeta de ejemplos de configuración del openvpn se encuentra un archivo base para la configuración del cliente, así que solamente hay que copiarlo al directorio de trabajo de la VPN, para poderlo modificar

cd /etc/openvpn
cp /usr/share/doc/openvpn/examples/sample-config-files/client.conf

Una vez copiado el archivo **client.conf**, también se le deben hacer varias modificaciones con el objetivo de adoptarlo a las necesidades de la VPN.

Variable	Valor	Comentario
client		Indica que es la configuración de un cliente
proto	udp	También pude ser tcp, se debe configurar igual que el servidor.
dev	tun	tun Si se desea crear un túnel IP tap Si se desea crear un túnel ethernet, se emplea para configuraciones más sencillas de clave simétrica pre-compartida.
ca	ca.crt	El certificado CA generado
remote	190.65.68.227 1194	IP de la interfaz pública del servidor de la oficina y puerto en el que está escuchando el OpenVPN instalado allí
cert	cliente1.crt	El certificado que generamos en el servidor y copiamos en el cliente por algún método “seguro”
key	cliente1.key	La clave privada que nos generaron en el servidor
comp-lzo		Habilita la compresión en el enlace VPN. Si se habilita en el servidor, también debe habilitarse en el cliente.
tls-aut	ta.key 1	El servidor y cada cliente, deben tener una copia de esta llave. El segundo parámetro debe ser 0 en el servidor y 1 en los clientes.
verb	3	Establezca el nivel apropiado de verbosidad: 0 silencio 4 razonable 5, 6 para hacer debug 9 muchisima información

En el servidor:

En cada cliente se debe crear un archivo en el mismo directorio en el que se tiene el archivo de configuración, este archivo debe tener el mismo nombre con el que se creo su certificado, por ejemplo para este caso sería de la siguiente manera:

echo "iroute 192.168.1.0 255.255.255.0" > /etc/openvpn/ccd/client1

La dirección que se puso es la de la red interna de la empresa de manera que el cliente pueda acceder a los equipos de dicha red.

4.1.4. CONFIGURACIÓN DEL FIREWALL

Cuando se tiene un firewall en el servidor hay que tener en cuenta que se deben agregar reglas que permitan el tráfico por el nuevo túnel creado. Al establecerse el túnel, se crean interfaces virtuales "tunX", que pueden ser usados mediante reglas de iptables para filtrar la información que viaja a través de ellas. Esto garantiza mayor seguridad, ya que el túnel solo permitirá tráfico desde los puntos autorizados así que se puede permitir sin ningún problema todo el tráfico entre dichas interfaces. Las siguientes reglas fueron las que se implementaron en el servidor:

iptables -A INPUT -i tun0 -j ACCEPT
iptables -A FORWARD -i tun0 -j ACCEPT
iptables -A OUTPUT -o tun0 -j ACCEPT
iptables -A FORWARD -o tun0 -j ACCEPT

4.1.5. ARRANCAR EL SERVIDOR Y LOS CLIENTES

Después de tener toda la configuración anteriormente detallada, se procede a arrancar el servidor mediante el siguiente script:

cd /etc/openvpn/
openvpn server.conf

Un arranque normal del servidor debe lucir más o menos de la siguiente manera:

```
Sun Feb  6 20:46:38 2005 OpenVPN 2.0_rc12 i686-suse-linux
[SSL] [LZO] [EPOLL] built on Feb  5 2005
```

```
Sun Feb  6 20:46:38 2005 Diffie-Hellman initialized with 1024
bit key
Sun Feb  6 20:46:38 2005 TLS-Auth MTU parms [ L:1542 D:138
EF:38 EB:0 ET:0 EL:0 ]
Sun Feb  6 20:46:38 2005 TUN/TAP device tun1 opened
Sun Feb  6 20:46:38 2005 /sbin/ifconfig tun1 10.8.0.1
pointopoint 10.8.0.2 mtu 1500
Sun Feb  6 20:46:38 2005 /sbin/route add -net 10.8.0.0
netmask 255.255.255.0 gw 10.8.0.2
Sun Feb  6 20:46:38 2005 Data Channel MTU parms [ L:1542
D:1450 EF:42 EB:23 ET:0 EL:0 AF:3/1 ]
Sun Feb  6 20:46:38 2005 UDPv4 link local (bound):
[undef]:1194
Sun Feb  6 20:46:38 2005 UDPv4 link remote: [undef]
Sun Feb  6 20:46:38 2005 MULTI: multi_init called, r=256
v=256
Sun Feb  6 20:46:38 2005 IFCONFIG POOL: base=10.8.0.4 size=62
Sun Feb  6 20:46:38 2005 IFCONFIG POOL LIST
Sun Feb  6 20:46:38 2005 Initialization Sequence Completed
```

Una vez el servidor está corriendo, los clientes pueden empezar a conectarse al servidor mediante el siguiente comando:

cd /etc/openvpn/
openvpn client.conf

Un arranque normal del cliente, debe lucir más o menos de la misma forma que el servidor

4.1.6. REALIZAR PRUEBAS DE CONECTIVIDAD

Lo único que queda faltando es realizar las pruebas para verificar que la red está operando bien, así que por medio de una Terminal se hace ping entre los equipos conectados dentro de la Red Privada Virtual:

ping 10.8.0.1
ping 190.65.68.227
ping 192.168.15.1

Si todos los ping son exitosos, Excelente, La VPN está funcionando correctamente.

4.2. ANALISIS Y DISEÑO DE LA APLICACION

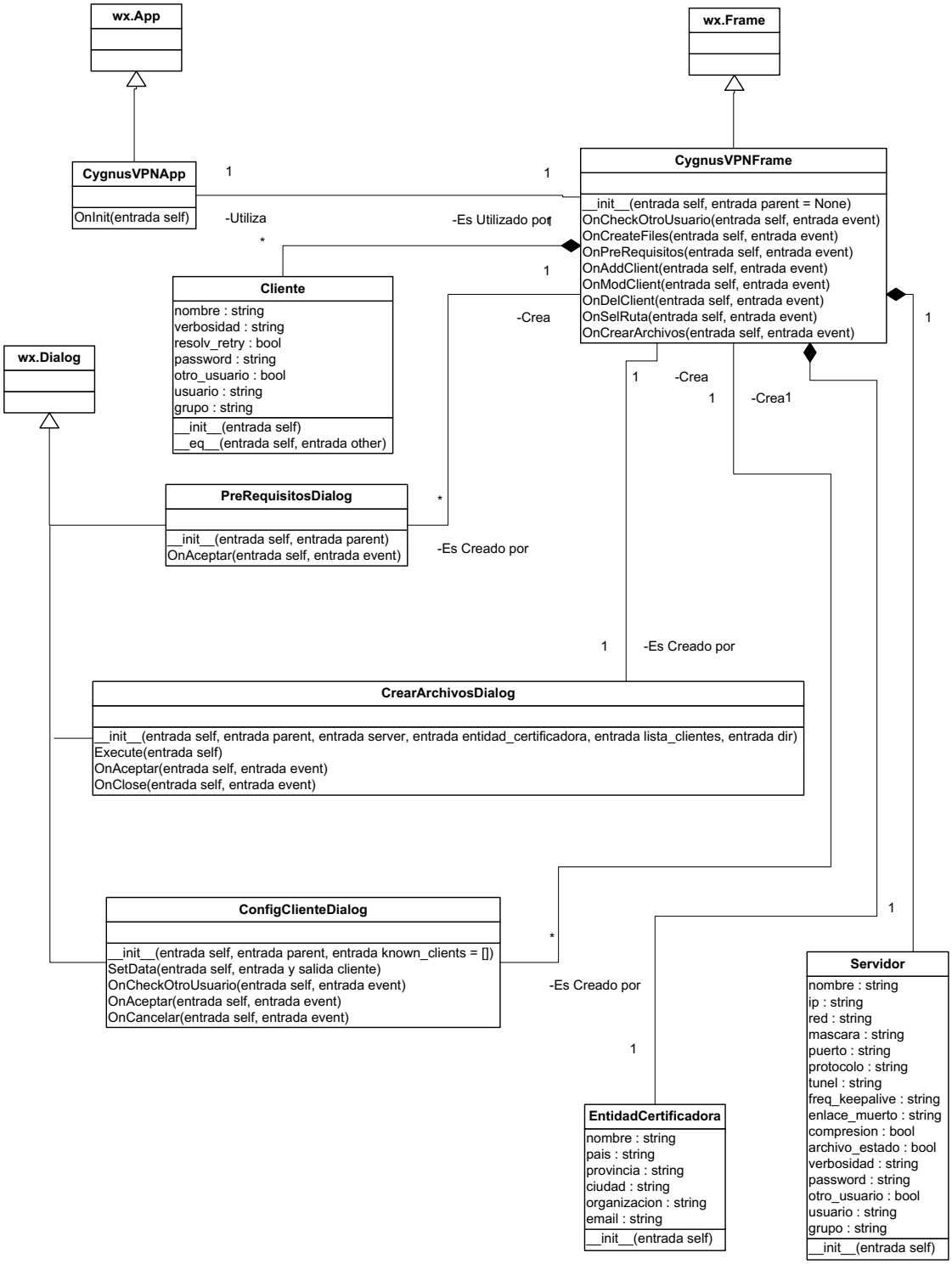
En cualquier proyecto de ingeniería, desde el más simple hasta el más complejo, se requieren etapas de modelamiento, que permitan experimentar y visualizar el sistema. Para este caso en particular, al implementarse una metodología orientada a objetos en el desarrollo de la aplicación, se utilizó el Lenguaje de Modelado Unificado UML para realizar el tipo de modelamiento requerido.

El UML esta compuesto por varios diagramas que permiten en conjunto dar una mejor interpretación y explicación del proyecto. Estos diagramas modelan diferentes aspectos del sistema, desde el comportamiento lógico y físico hasta los aspectos dinámicos, estáticos y funcionales del mismo. Sin embargo debido a que el tamaño de la aplicación que se desea implementar es muy pequeño, se decidió que no se utilizara UML de manera pura, sino una modificación de este lenguaje el cual consiste en un conjunto de diagramas suficientes para modelar el sistema, esto es debido a que muchos de los diagramas serían redundantes y no aportarían mayor información para dicho fin. Por lo tanto se reitera que no se va a seguir al pie de la letra ninguna metodología de desarrollo debido al tamaño del proyecto.

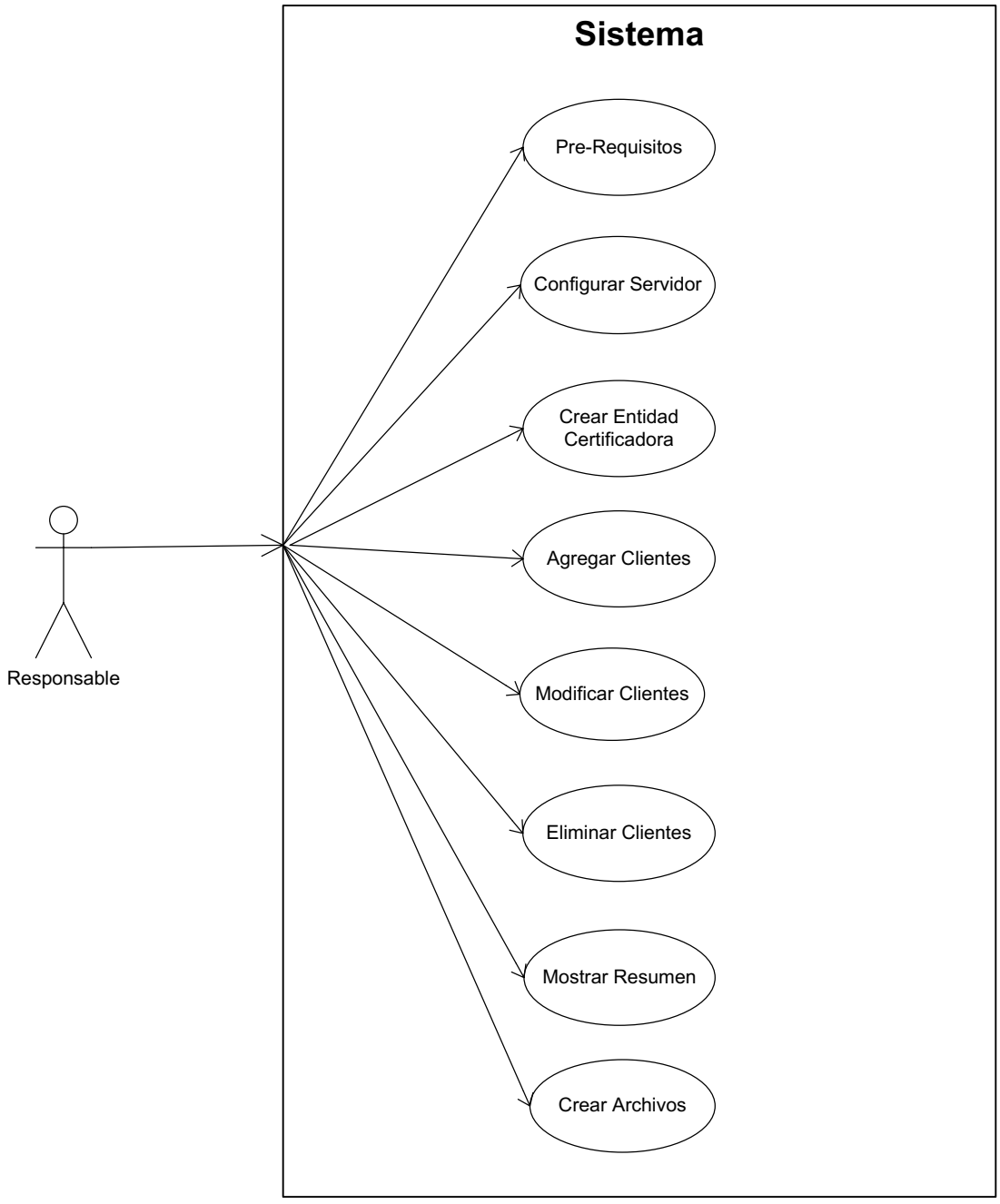
Después de analizar detenidamente el problema se decidió que los diagramas que se van a emplear son los siguientes:

- Diagrama de Clases
- Diagrama de Casos de Uso
- Diagramas de Secuencia
- Diseño de Secuencia de Ventanas
- Diagrama de Componentes

4.2.1. Diagrama de Clases



4.2.2. Diagrama de Casos de Uso



DESCRIPCIÓN CASOS DE USO

CASO DE USO		**PRE-REQUISITOS**
ACTORES		Responsable_Red
PROPOSITO		Dar Información al usuario
RESUMEN		El responsable de red debe asegurarse que las herramientas requeridas para el funcionamiento de la aplicación estén instaladas en el equipo.
TIPO		Principal
REFERENCIAS CRUZADAS		
SECCION PRINCIPAL		
Curso normal de los eventos	**ACCION DE LOS ACTORES**	**RESPUESTA DEL SISTEMA**
	1. Este caso de uso comienza cuando el responsable de red hace clic en el botón Pre-requisitos. 3. Hace clic en el botón Aceptar.	2. El Sistema despliega una ventana informativa. 4. La ventana se cierra.
Cursos Alternos		

<table>
<tr><td colspan="2">CASO DE USO</td><td>CONFIGURAR SERVIDOR</td></tr>
<tr><td colspan="2">ACTORES</td><td>Responsable_Red</td></tr>
<tr><td colspan="2">PROPOSITO</td><td>Ingresar toda la información necesaria para la configuración del servidor.</td></tr>
<tr><td colspan="2">RESUMEN</td><td>El responsable de red debe ingresar toda la información referente a la configuración del servidor.</td></tr>
<tr><td colspan="2">TIPO</td><td>Principal</td></tr>
<tr><td colspan="2">REFERENCIAS CRUZADAS</td><td></td></tr>
<tr><td colspan="3">SECCION PRINCIPAL</td></tr>
<tr><td rowspan="2">Curso normal de los eventos</td><td>ACCION DE LOS ACTORES</td><td>RESPUESTA DEL SISTEMA</td></tr>
<tr><td>1. Este caso de uso comienza cuando el responsable hace clic en el icono Servidor.

3. Ingresa información requerida.</td><td>2. Muestra Formulario.

4. Realiza operaciones internas.</td></tr>
<tr><td>Cursos Alternos</td><td colspan="2"></td></tr>
</table>

CASO DE USO		CREAR ENTIDAD CERTIFICADORA
ACTORES		Responsable_Red
PROPOSITO		Ingresar toda la información necesaria para la creación de la entidad certificadora.
RESUMEN		El responsable de red debe ingresar toda la información referente a la entidad certificadora.
TIPO		Principal
REFERENCIAS CRUZADAS		
SECCION PRINCIPAL		
Curso normal de los eventos	ACCION DE LOS ACTORES	RESPUESTA DEL SISTEMA
	1. Este caso de uso comienza cuando el responsable hace clic en el icono Certificados . 3. Ingresa información requerida.	2. Muestra Formulario. 4. Realiza operaciones internas.
Cursos Alternos		

<table>
<tr><td colspan="2">CASO DE USO</td><td>AGREGAR CLIENTES</td></tr>
<tr><td colspan="2">ACTORES</td><td>Responsable_Red</td></tr>
<tr><td colspan="2">PROPOSITO</td><td>Agregar clientes a la red.</td></tr>
<tr><td colspan="2">RESUMEN</td><td>El responsable de red debe ingresar toda la información referente a la configuración de los clientes que vayan a hacer parte de la red.</td></tr>
<tr><td colspan="2">TIPO</td><td>Principal</td></tr>
<tr><td colspan="2">REFERENCIAS CRUZADAS</td><td></td></tr>
<tr><td colspan="3">SECCION PRINCIPAL</td></tr>
<tr><td rowspan="2">Curso normal de los eventos</td><td>ACCION DE LOS ACTORES</td><td>RESPUESTA DEL SISTEMA</td></tr>
<tr><td>1. Este caso de uso comienza cuando el responsable hace clic en el icono Clientes.

3. El responsable hace clic en el botón Adicionar Cliente.

5. Ingresa información requerida.
6. Hace clic en el botón Aceptar.</td><td>2. Muestra matriz de clientes y botones con opciones.

4. Despliega ventana para agregar cliente.

7. Realiza operaciones internas.
8. Cierra la ventana.
9. Muestra matriz actualizada con la información del nuevo cliente.</td></tr>
<tr><td>Cursos Alternos</td><td colspan="2">Línea 6. Hace clic en el botón cancelar -> Se cierra la ventana y no se crea el cliente.</td></tr>
</table>

CASO DE USO	MODIFICAR CLIENTES
ACTORES	Responsable_Red
PROPOSITO	Modificar la información de los clientes.
RESUMEN	El responsable de red debe seleccionar el cliente al cual desea modificarle la información y luego hacer clic en el botón Modificar Cliente para finalmente cambiar la información necesaria y almacenarla.
TIPO	Principal
REFERENCIAS CRUZADAS	

SECCION PRINCIPAL		
	ACCION DE LOS ACTORES	RESPUESTA DEL SISTEMA
Curso normal de los eventos	1. Este caso de uso comienza cuando el responsable hace clic en el icono Clientes.	
		2. Muestra matriz de clientes y botones con opciones.
	3. El responsable hace clic en el botón Modificar Cliente.	
		4. Despliega ventana con la información del cliente seleccionado para modificar.
	5. Modifica la información necesaria.	
	6. Hace clic en el botón Aceptar.	
		7. Realiza operaciones internas.
		8. Cierra la ventana.
		9. Muestra matriz con la información actualizada.
Cursos Alternos	**Línea 6. Hace clic en el botón cancelar -> Se cierra la ventana y no se modifica el cliente.**	

<table>
<tr><td colspan="2">CASO DE USO</td><td>ELIMINAR CLIENTES</td></tr>
<tr><td colspan="2">ACTORES</td><td>Responsable_Red</td></tr>
<tr><td colspan="2">PROPOSITO</td><td>Eliminar un cliente</td></tr>
<tr><td colspan="2">RESUMEN</td><td>El responsable debe seleccionar el cliente que desea eliminar y confirmar la acción.</td></tr>
<tr><td colspan="2">TIPO</td><td>Principal</td></tr>
<tr><td colspan="2">REFERENCIAS CRUZADAS</td><td></td></tr>
<tr><td colspan="3">SECCION PRINCIPAL</td></tr>
<tr><td rowspan="2">Curso normal de los eventos</td><td>ACCION DE LOS ACTORES</td><td>RESPUESTA DEL SISTEMA</td></tr>
<tr><td>1. Este caso de uso comienza cuando el responsable hace clic en el icono Clientes.

3. El responsable hace clic en el botón Eliminar Cliente.

5. Hace clic en el botón aceptar.</td><td>2. Muestra matriz de clientes y botones con opciones.

4. Muestra mensaje de confirmación.

6. Realiza operaciones internas.
7. Cierra la ventana.
8. Muestra matriz con la información actualizada.</td></tr>
<tr><td>Cursos Alternos</td><td colspan="2">Línea 5. Hace clic en el botón cancelar -> No se elimina el cliente.</td></tr>
</table>

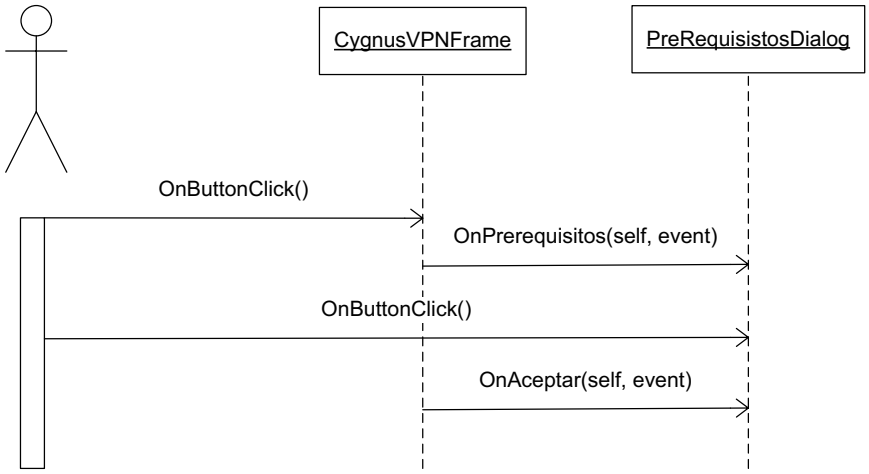
CASO DE USO		MOSTRAR RESUMEN
ACTORES		Responsable_Red
PROPOSITO		Mostrar un resumen al usuario con la información que suministró en los formularios para que éstos sean verificados.
RESUMEN		El Responsable ingresa a la opción Crear Archivos e inmediatamente se despliega el resumen. Si hay errores de configuración también hacen parte de este resumen.
TIPO		Principal
REFERENCIAS CRUZADAS		
SECCION PRINCIPAL		
Curso normal de los eventos	ACCION DE LOS ACTORES	RESPUESTA DEL SISTEMA
	1. Este caso de uso comienza cuando el responsable hace clic en el icono Crear Archivos.	2. Muestra Información.
Cursos Alternos		

CASO DE USO		CREAR ARCHIVOS
ACTORES		Responsable_Red
PROPOSITO		Crear los archivos necesarios para poner a funcionar la VPN.
RESUMEN		El responsable debe seleccionar la ruta en la que los archivos van a quedar almacenados, luego debe seleccionar crear los archivos los cuales son almacenados en esta ruta. Si la aplicación no detecta la carpeta que contiene instalado el OpenVPN, el responsable debe ingresar esta ruta, normalmente se encuentra en: /usr/share/doc/packages/openvpn/examples/easy-rsa.
TIPO		Principal
REFERENCIAS CRUZADAS		
SECCION PRINCIPAL		
Curso normal de los eventos	ACCION DE LOS ACTORES	RESPUESTA DEL SISTEMA
	1. Este caso de uso comienza cuando el responsable hace clic en el icono Crear Archivos.	
		2. Muestra Información.
	3. El responsable hace clic en el botón Crear Archivos ubicado en la parte inferior de la ventana	
		4. Despliega una ventana.
		5. Solicita ruta de archivo
	6. Ingresa ruta y hace clic en el botón aceptar.	
		7. Realiza operaciones.
		8. Muestra Información al usuario.
	9. El responsable hace clic en el botón aceptar.	
		10. Cierra la ventana.

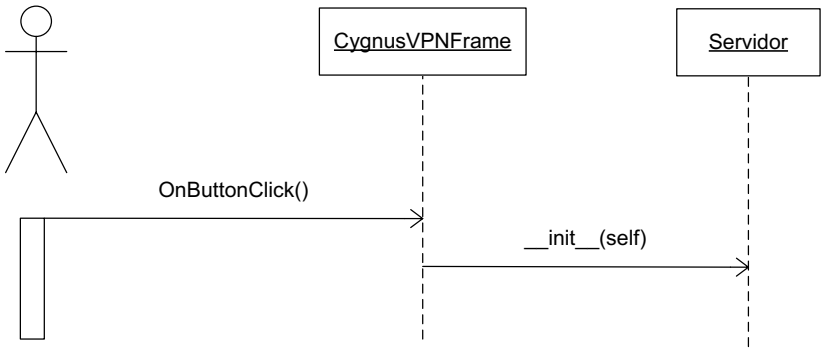
Cursos Alternos	**Línea 6. Ingresa una ruta inválida -> Regresa a la línea 3.**

4.2.3. Diagramas de Secuencia

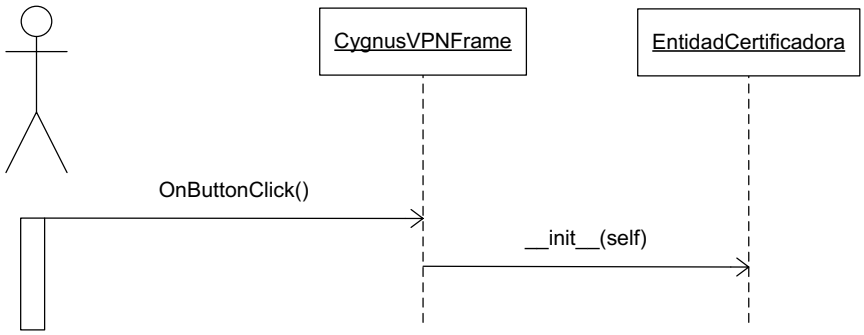
Caso de Uso Pre-Requisitos



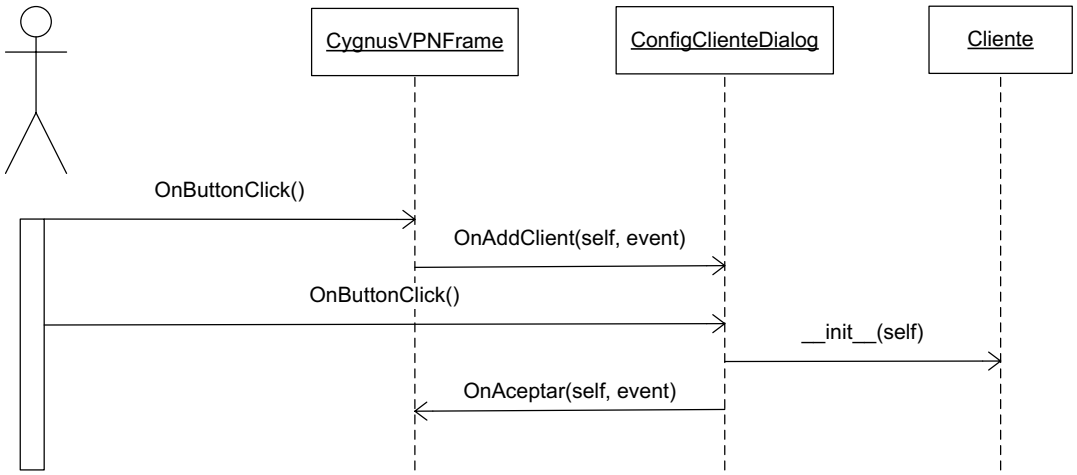
Caso de Uso Configurar Servidor



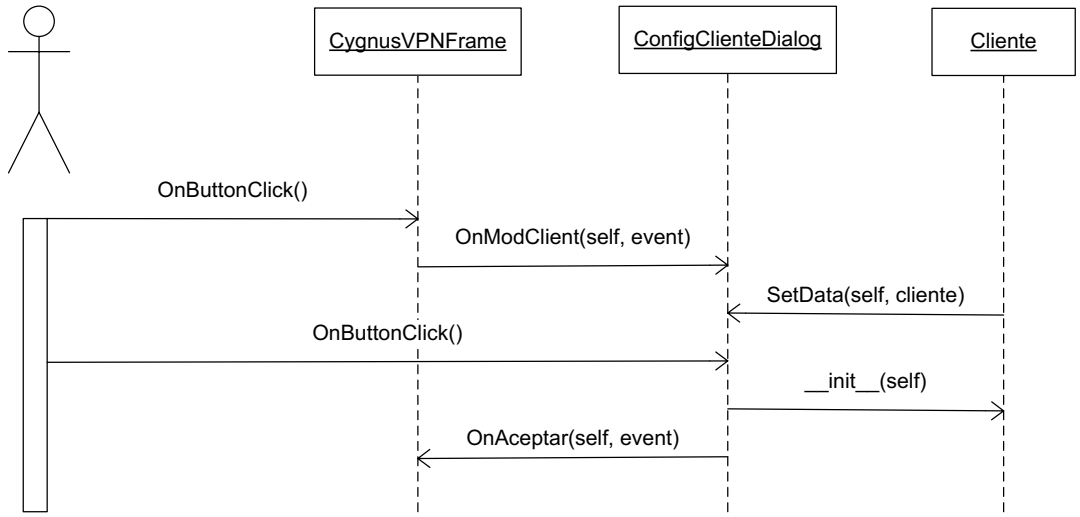
Caso de Uso Crear Entidad Certificadora



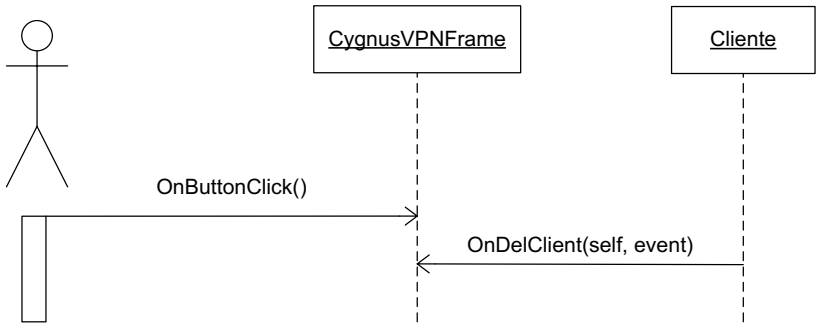
Caso de Uso Agregar Clientes



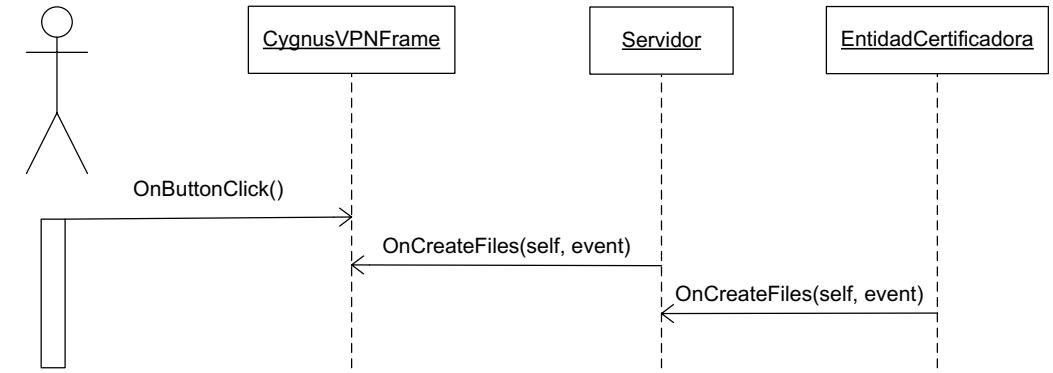
Caso de Uso Modificar Clientes



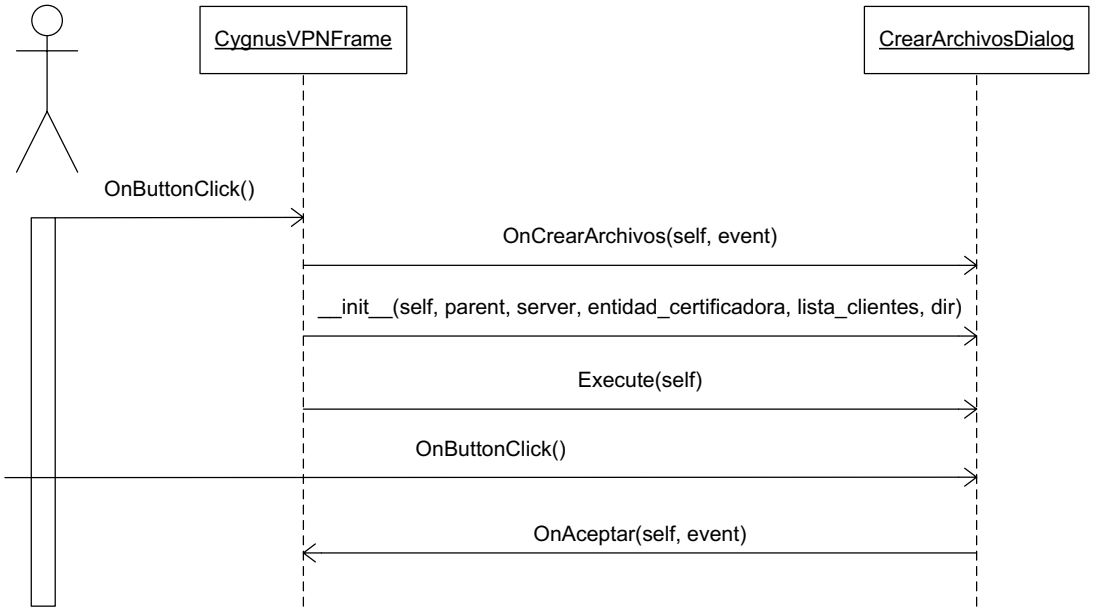
Caso de Uso Eliminar Clientes



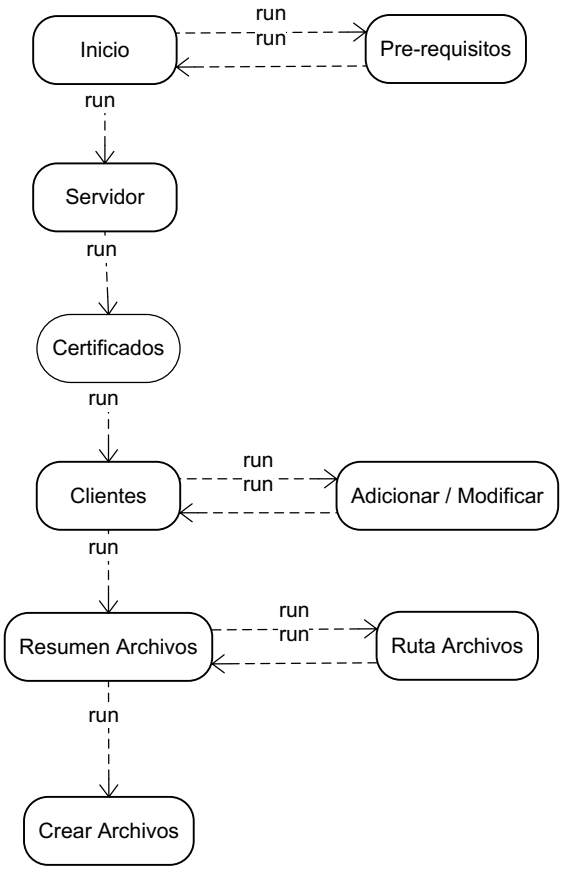
Caso de Uso Mostrar Resumen



Caso de Uso Crear Archivos



4.2.4. Diagrama de Secuencia de Ventanas



4.2.4.1. Descripción de la Secuencia de Ventanas

a. INICIO

La interfaz diseñada para la configuración de la aplicación CygnusVPN es bastante amigable ya que le permite al usuario configurar una Red Privada Virtual de manera fácil.

En el panel izquierdo se cuenta con un conjunto de íconos que le permitirán al usuario navegar por diferentes ventanas de configuración para agregar la información requerida en la creación de la VPN.

En la parte inferior del panel principal de esta ventana se encuentra un botón que al seleccionarlo, brinda información acerca de las herramientas que deben estar instaladas, después de realizar esto se puede acceder a cualquier ventana a través de los iconos del panel izquierdo e ingresar la información requerida allí, sin embargo se recomienda continuar con el icono Servidor con el fin de mantener un orden de configuración mas apropiado.

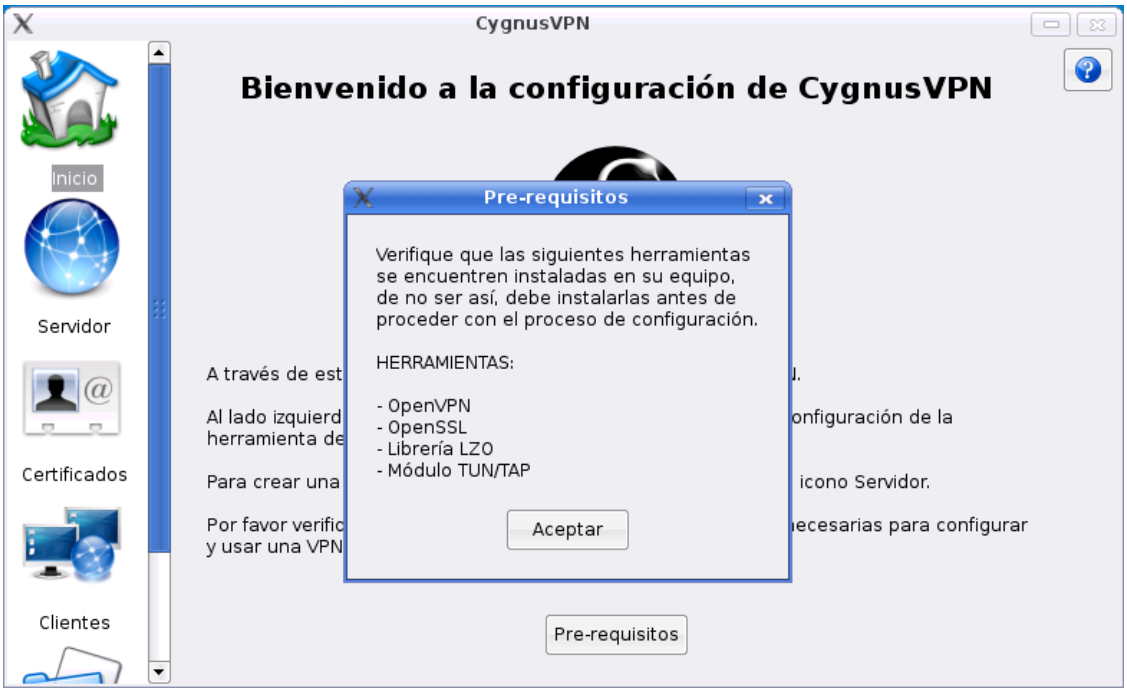
En la parte superior derecha de la ventana principal se encuentra un botón que le permitirá al usuario al hacer clic en él, desplegar una ventana con el manual el cual brinda información para el uso de la aplicación CygnusVPN. Al hacer clic en este botón la ventana de ayuda se abrirá y mostrará información correspondiente a la ventana en la que se encuentre el usuario, sin embargo esta ventana le

permitirá al usuario desplazarse por los diferentes temas de ayuda; en caso de ya estar abierta esta ventana, desplegará la información correspondiente a la ventana en la que se volvió a solicitar la ayuda.

b. PRE-REQUISITOS DE CONFIGURACIÓN

Es importante aclarar que todas las herramientas son indispensables para el funcionamiento de la VPN. Queda bajo la responsabilidad del usuario que todas las herramientas requeridas sean instaladas, ya que es la única manera de garantizar que la aplicación CygnusVPN funcione.

Después de tener conocimiento de estos requerimientos el usuario debe hacer clic en el botón Aceptar que se encuentra en la parte inferior de la ventana para así regresar a la ventana principal y continuar con el proceso de configuración.



c. CONFIGURACIÓN DEL SERVIDOR

En esta ventana se debe ingresar la información correspondiente al servidor. Una vez hecho esto, se recomienda continuar el proceso de configuración seleccionando el icono Certificados que se encuentra en el panel izquierdo, sin embargo se reitera que el orden sugerido es simplemente por mantener un orden más apropiado, pero el usuario puede acceder a cualquier ventana a través de los iconos del panel izquierdo en cualquier momento, ya sea para modificar algún dato o para ingresar la información requerida en esa ventana sin que esto afecte el proceso de configuración.

Se recuerda que en la parte superior derecha de la ventana principal se encuentra un botón que le permitirá al usuario al hacer clic en él, desplegar una ventana con el manual el cual brinda información para el uso de la aplicación CygnusVPN.

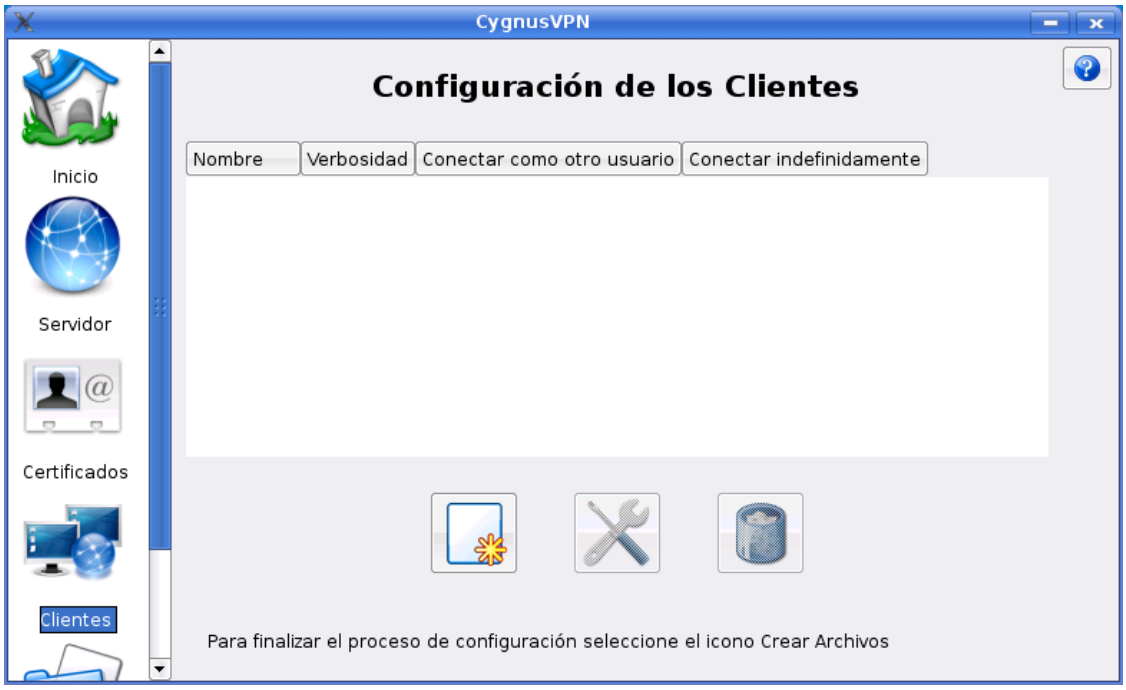
d. CREACIÓN DE LA ENTIDAD CERTIFICADORA

Aquí, se debe ingresar la información necesaria para crear la entidad certificadora. Una vez hecho esto, se recomienda continuar el proceso de configuración seleccionando el icono Clientes que se encuentra en el panel izquierdo.

Se recuerda que en la parte superior derecha de la ventana principal se encuentra un botón que le permitirá al usuario al hacer clic en él, desplegar una ventana con el manual el cual brinda información para el uso de la aplicación CygnusVPN.

e. CONFIGURACIÓN DE LOS CLIENTES

En esta ventana se cuenta con varios elementos. En la parte superior de la ventana se puede apreciar una matriz en la que se van a adicionar los clientes a medida que se van creando y en la parte inferior se cuenta con tres botones que permitirán adicionar, modificar y borrar la configuración de los clientes. Es importante saber que al pasar el Mouse por encima de los botones aparecerá un mensaje informativo indicando la funcionalidad de cada botón.



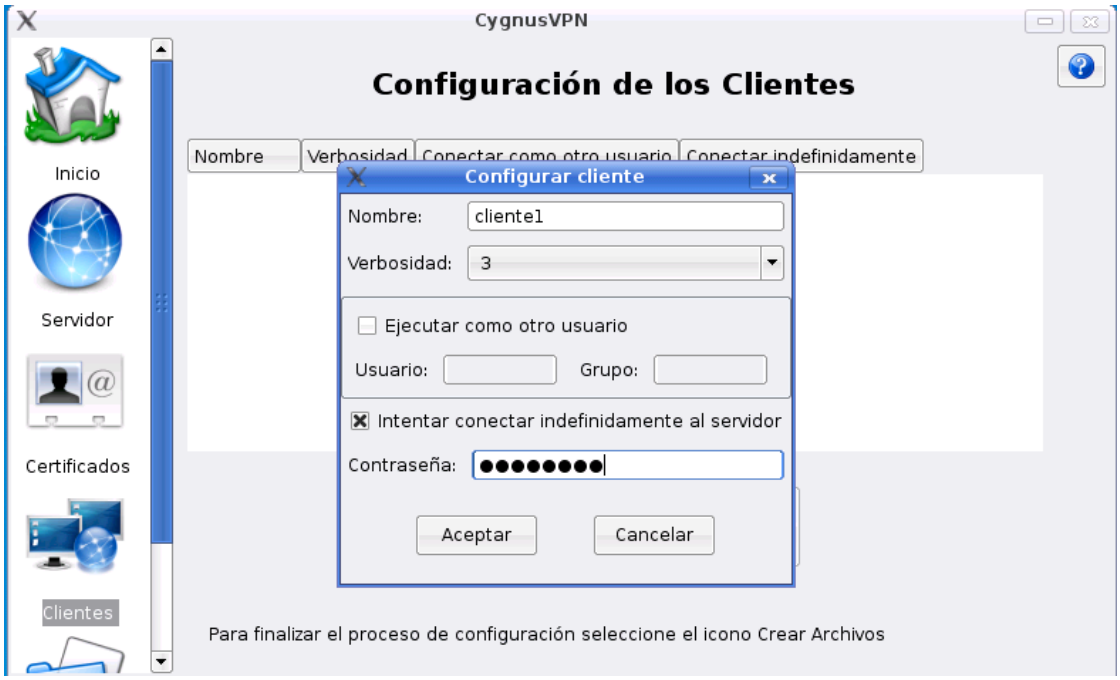
Se recuerda que en la parte superior derecha de la ventana principal se encuentra un botón que le permitirá al usuario al hacer clic en él, desplegar una ventana con el manual el cual brinda información para el uso de la aplicación CygnusVPN.

Una vez se tiene la configuración de todos los clientes realizada, se recomienda continuar el proceso de configuración seleccionando el icono Crear Archivos que se encuentra en el panel izquierdo.

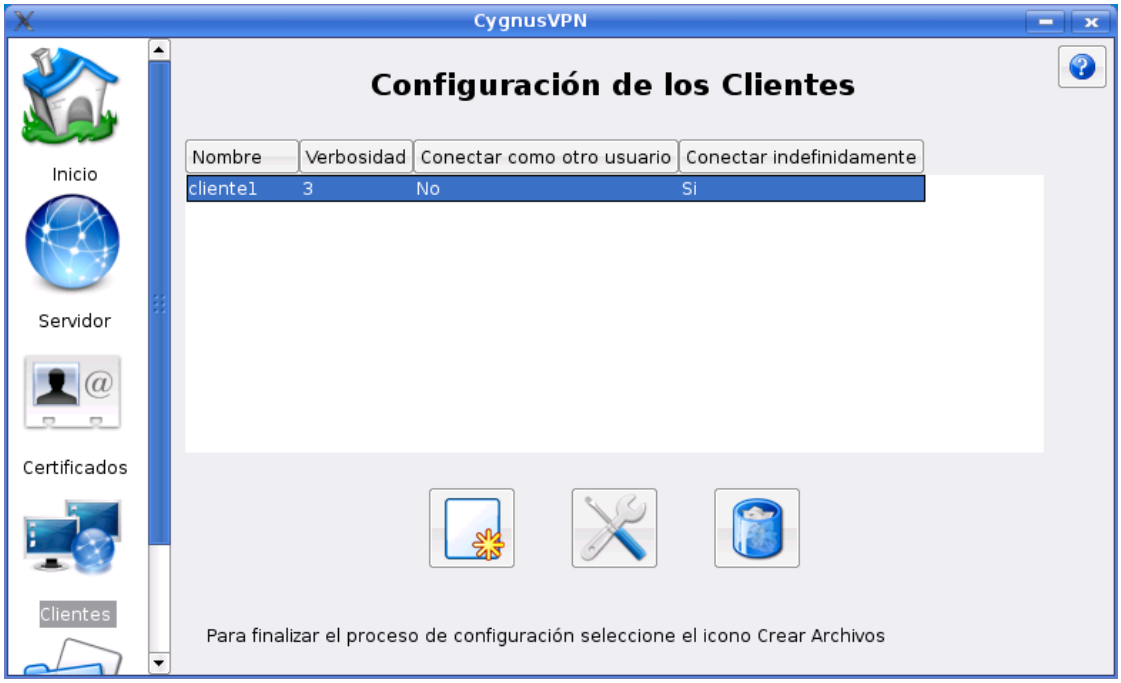
Adicionar un Cliente:

Se debe hacer clic en el primer botón que se encuentra en la parte inferior de la ventana, esto desplegará otra ventana que permitirá ingresar la información de un cliente.

Para confirmar que la información del cliente es la deseada, se debe hacer clic en el botón Aceptar, en caso que ya no se desee adicionar el cliente se debe hacer clic en el botón Cancelar.



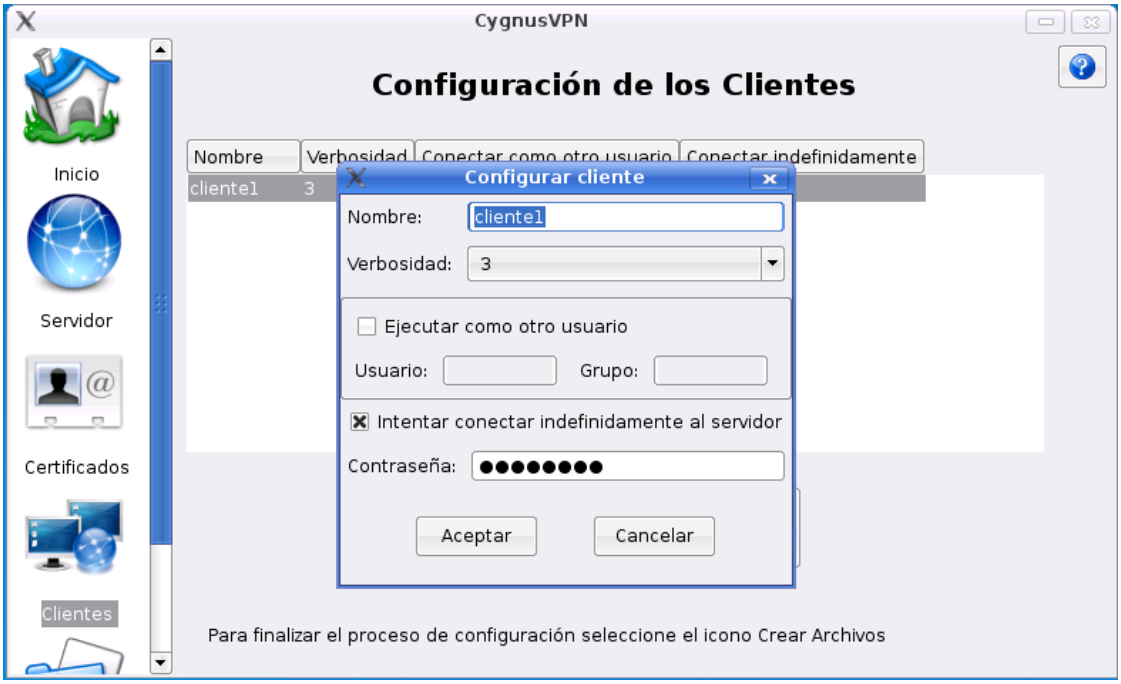
Inmediatamente después que la ventana se cierre aparecerá en la matriz la información del cliente creado a no ser que se haya cancelado el proceso de creación del mismo. Una vez se haya aceptado la configuración del primer cliente, se habilitarán los botones para modificar y eliminar clientes ubicados en la ventana principal.



Modificar un Cliente:

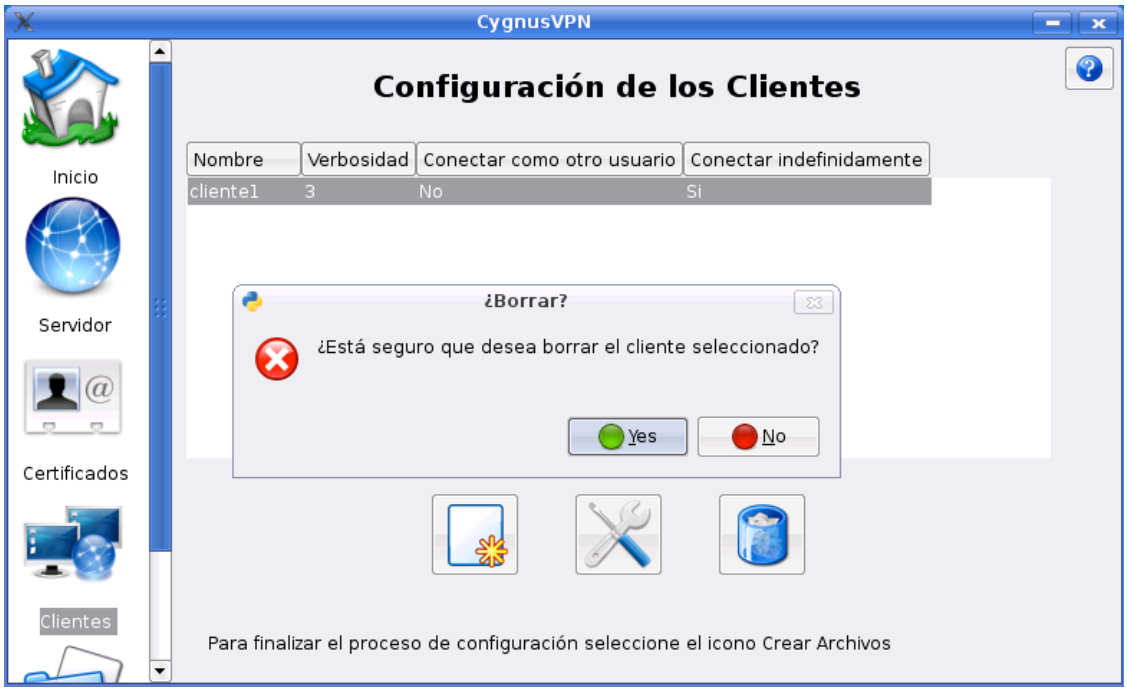
Se debe seleccionar en la matriz el cliente que se desea modificar y enseguida hacer clic en el segundo botón denominado Modificar Cliente el cual se encuentra en la parte inferior de la ventana. Es importante aclarar que la interfaz sólo permitirá seleccionar un cliente a la vez. Este evento desplegará una ventana que mostrará la información del cliente que se había ingresado.

Una vez modificada la información necesaria se debe hacer clic en el botón Aceptar para almacenar los cambios, en caso de no desear hacer algún tipo de modificación, se debe hacer clic en el botón Cancelar. Inmediatamente los cambios se verán reflejados en la matriz de clientes en la ventana principal.


CygnusVPN
Configuración de los Clientes
Inicio
Servidor
Certificados
Clientes
Nombre
Verbosidad
Conectar como otro usuario
Conectar indefinidamente
cliente1 3
Configurar cliente
Nombre: cliente1
Verbosidad: 3
Ejecutar como otro usuario
Usuario:
Grupo:
Intentar conectar indefinidamente al servidor
Contraseña:
Aceptar
Cancelar
Para finalizar el proceso de configuración seleccione el icono Crear Archivos

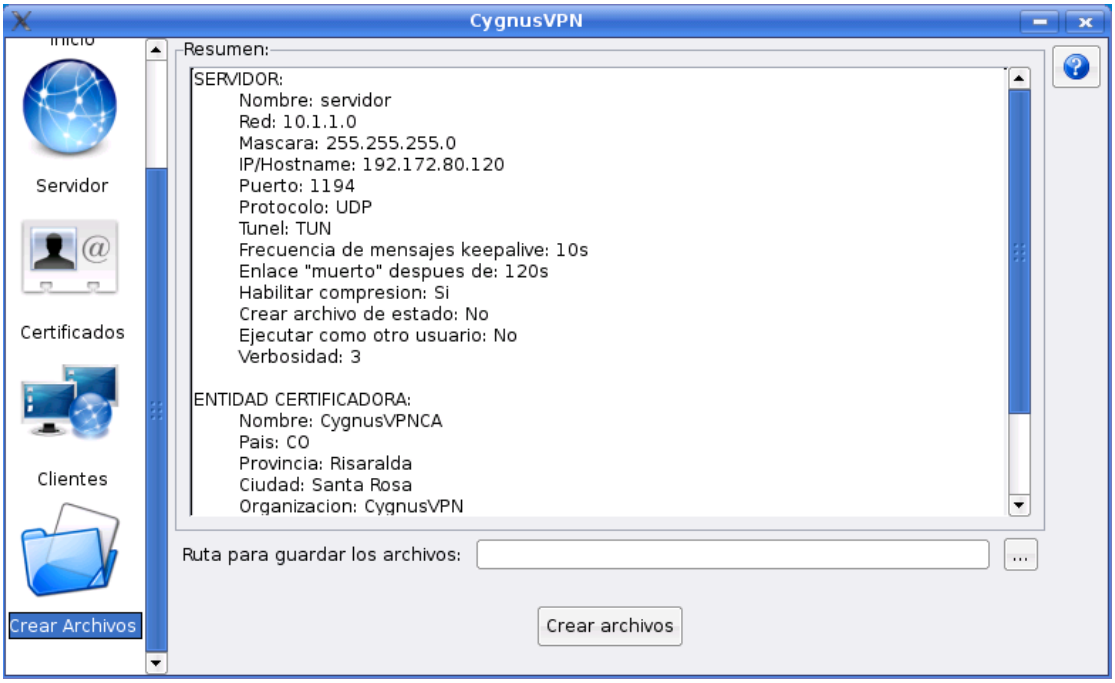
Eliminar un Cliente:

Se debe seleccionar en la matriz el cliente que se desea borrar y después se debe hacer clic en el último botón que se encuentra en la parte inferior de la ventana, inmediatamente se desplegará un mensaje de confirmación para la eliminación del cliente, si se desea eliminar el cliente debe hacer clic en si, de lo contrario debe hacer clic en no.



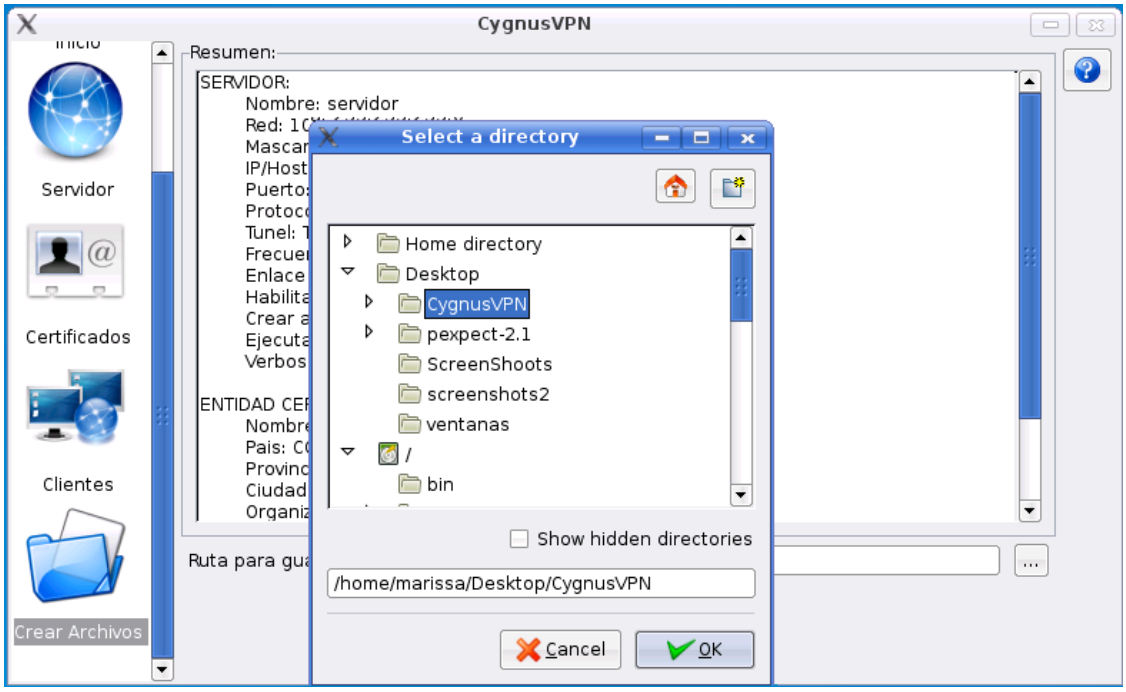
f. RESUMEN DE CONFIGURACIÓN

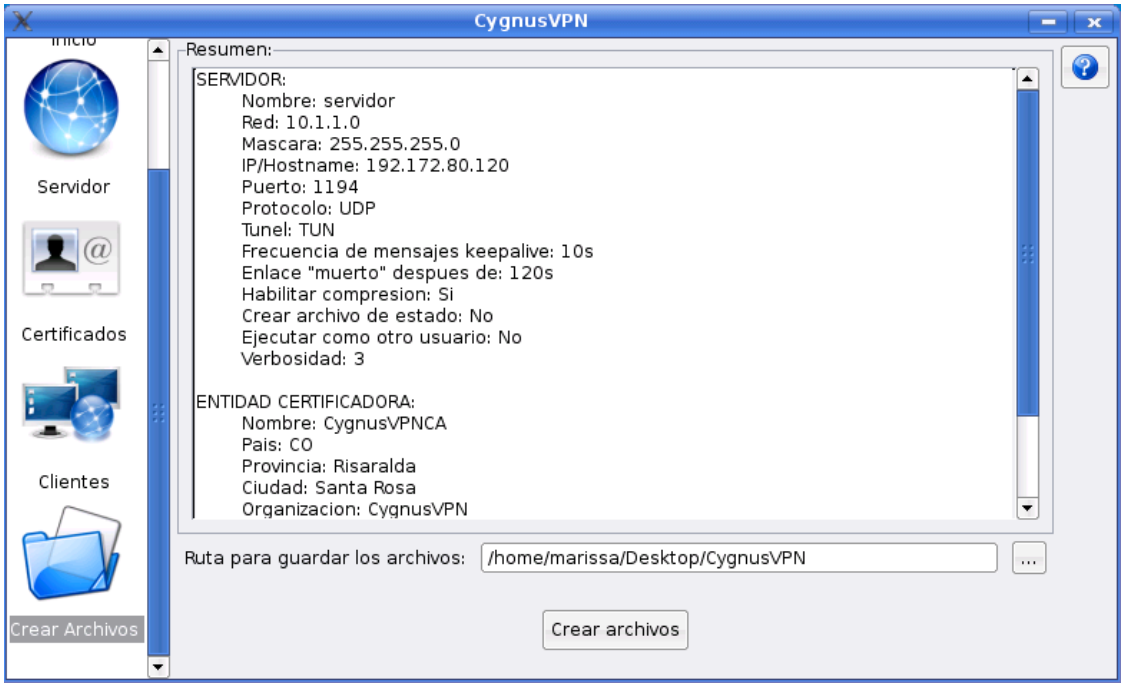
Al hacer clic en el último icono del panel izquierdo denominado Crear Archivos se despliega un reporte con toda la información que se ingreso a través de las otras ventanas, si ese reporte es satisfactorio el botón Crear Archivos que se encuentra ubicado en la parte inferior de la ventana principal estará habilitado, de no ser así es porque se encontró por lo menos un error de configuración el cual se puede detallar en el resumen y por lo tanto hay que corregirlo para que el botón se habilite y así poder crear los archivos.



g. SELECCIÓN DE LA RUTA PARA GENERACIÓN DE ARCHIVOS DE CONFIGURACIÓN

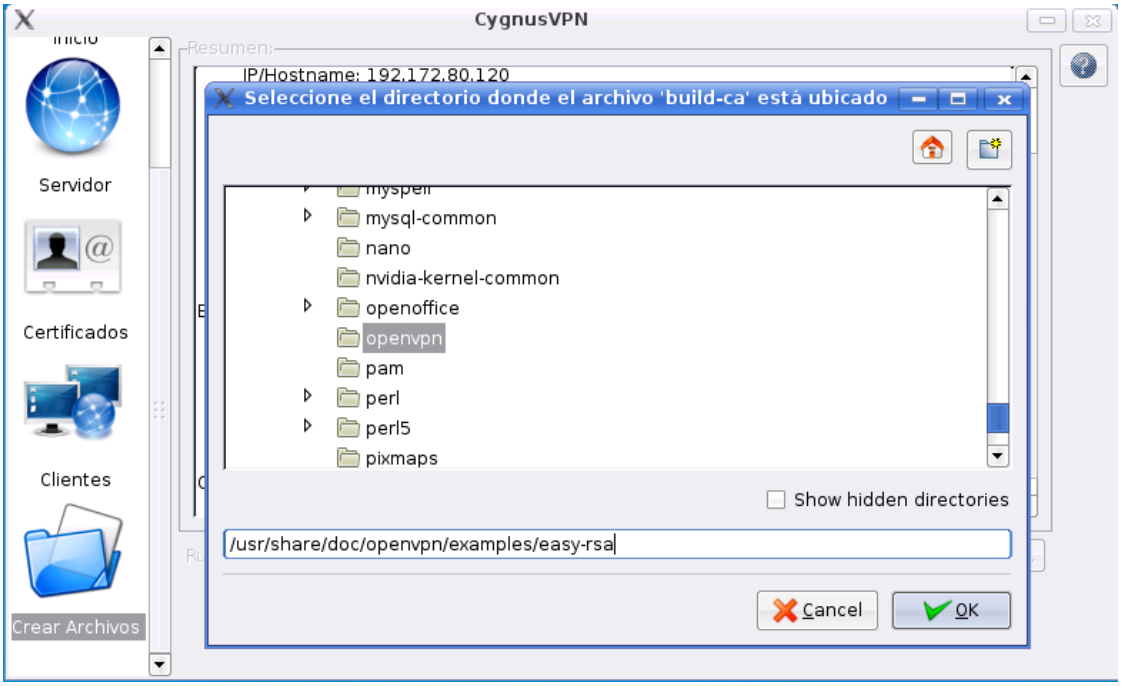
Antes de proceder a la creación de los archivos se debe hacer clic en el botón para la selección de la ruta donde serán almacenados, inmediatamente se despliega una ventana que le permite hacer dicha tarea y una vez seleccionada debe hacer clic en el botón Ok, para que la ruta sea establecida.



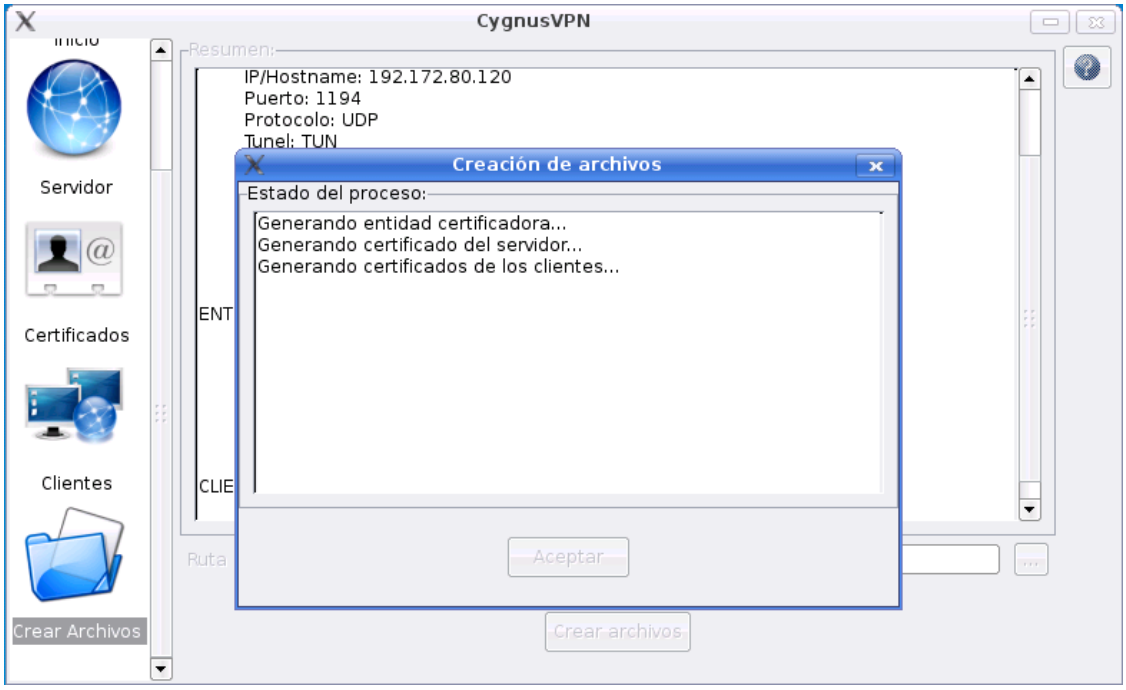

CygnusVPN
Inicio
Servidor
Certificados
Clientes
Crear Archivos
Resumen:
SERVIDOR:
Nombre: servidor
Red: 10.1.1.0
Mascara: 255.255.255.0
IP/Hostname: 192.172.80.120
Puerto: 1194
Protocolo: UDP
Tunel: TUN
Frecuencia de mensajes keepalive: 10s
Enlace "muerto" despues de: 120s
Habilitar compresion: Si
Crear archivo de estado: No
Ejecutar como otro usuario: No
Verbosidad: 3
ENTIDAD CERTIFICADORA:
Nombre: CygnusVPNCA
Pais: CO
Provincia: Risaralda
Ciudad: Santa Rosa
Organizacion: CygnusVPN
Ruta para guardar los archivos:
/home/marissa/Desktop/CygnusVPN
...
Crear archivos

h. GENERACIÓN DE ARCHIVOS DE CONFIGURACIÓN

Al hacer clic en el botón Crear Archivos, la aplicación solicitará la ruta en la que se encuentra instalada la herramienta OpenVPN, la ruta que aparece en la imagen es usualmente la ruta en la que se encuentra instalada, una vez el usuario identifica la ubicación de la carpeta easy-rsa, debe hacer clic en el botón ok.

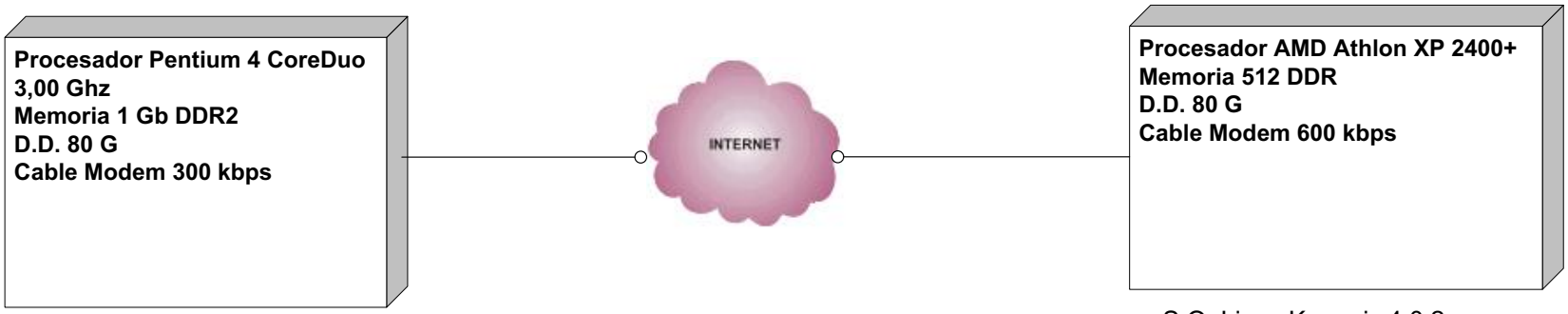


Después de hacer clic en el botón Crear Archivos se despliega una ventana la cual tiene un botón deshabilitado en la parte inferior denominado Aceptar el cual se habilitará cuando el proceso de creación de archivos termine.



Una vez se haga clic en el botón Aceptar el proceso de configuración de la VPN habrá terminado y se podrá cerrar la aplicación CygnusVPN.

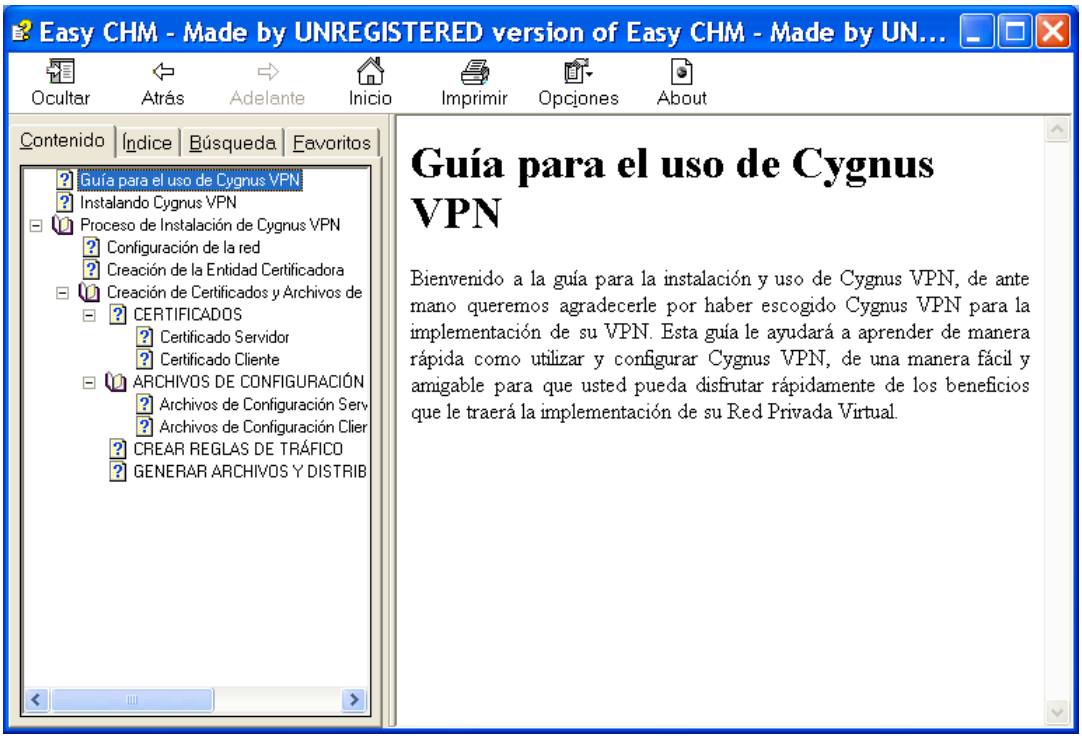
4.2.5. Diagrama de Distribución

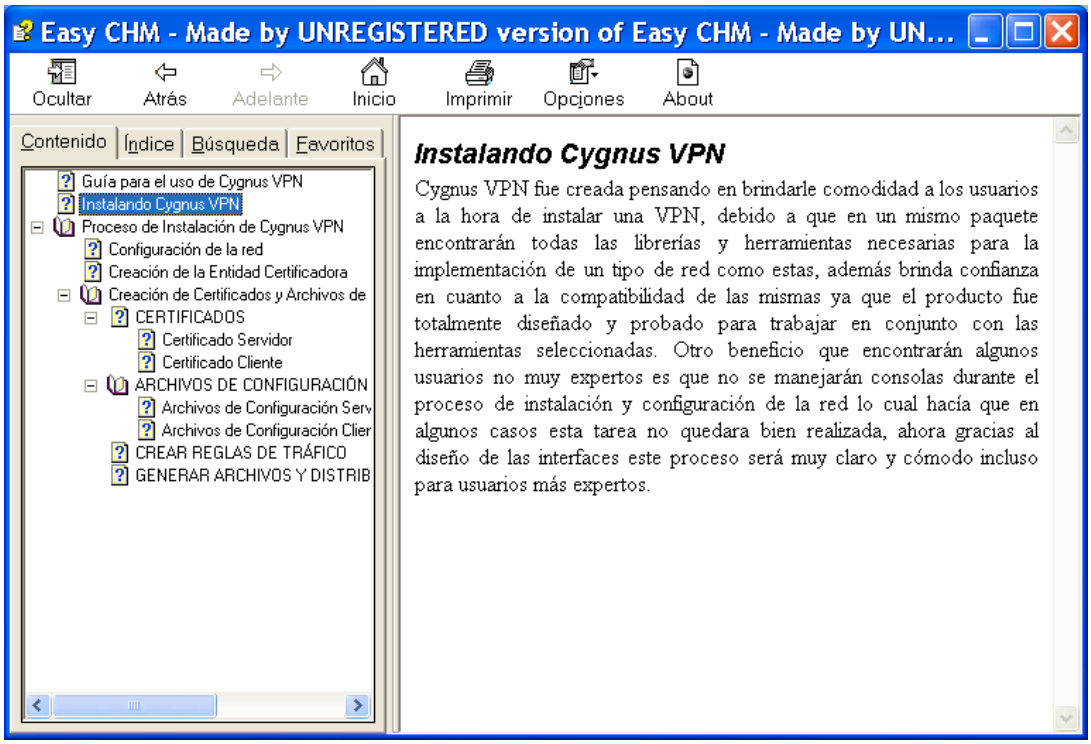


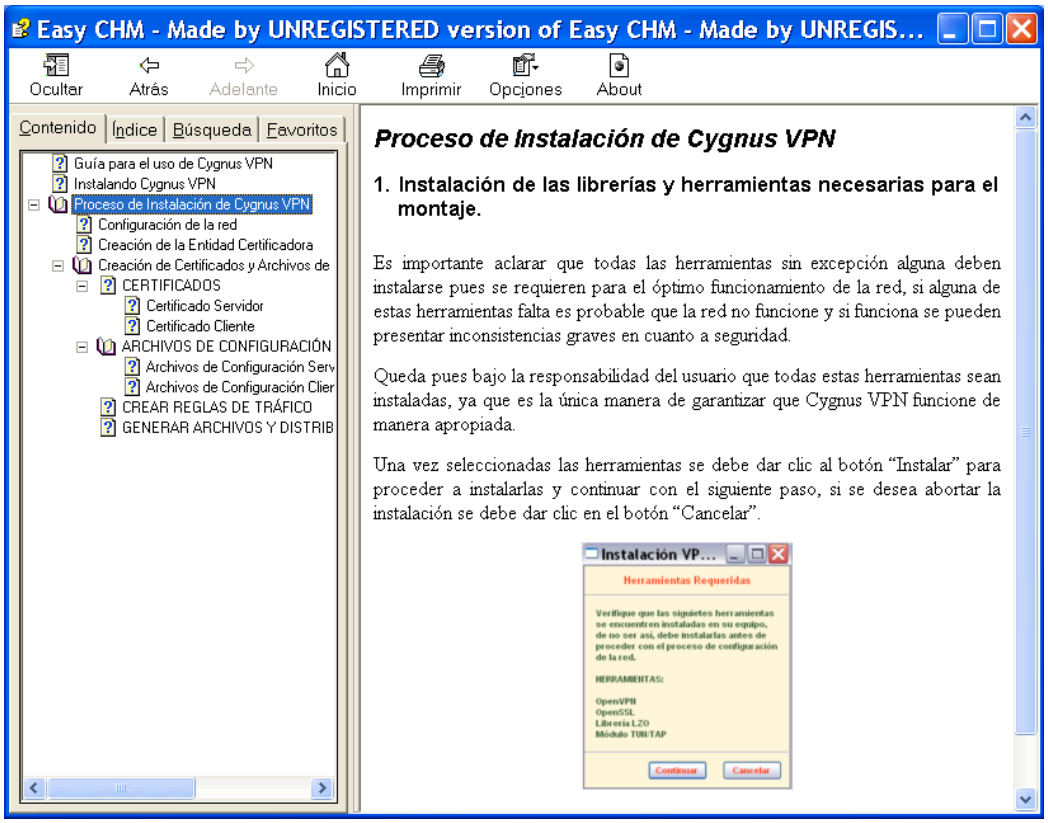
S.O. Linux Knoppix 4.0.2
Python v2.5
WxPython v2.8
WxGlade v0.5
OpenVPN v
OpenSSL v
liblzo1

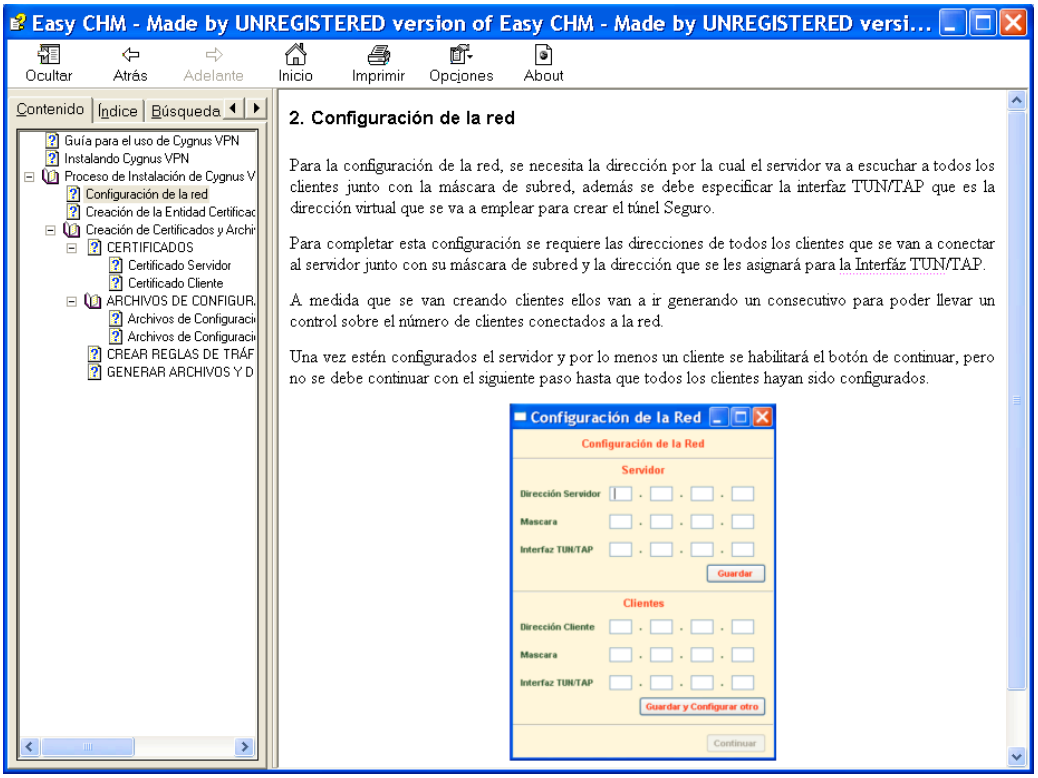
S.O. Linux Knoppix 4.0.2
Python v2.5
WxPython v2.8
WxGlade v0.5
OpenVPN v
OpenSSL v
liblzo1

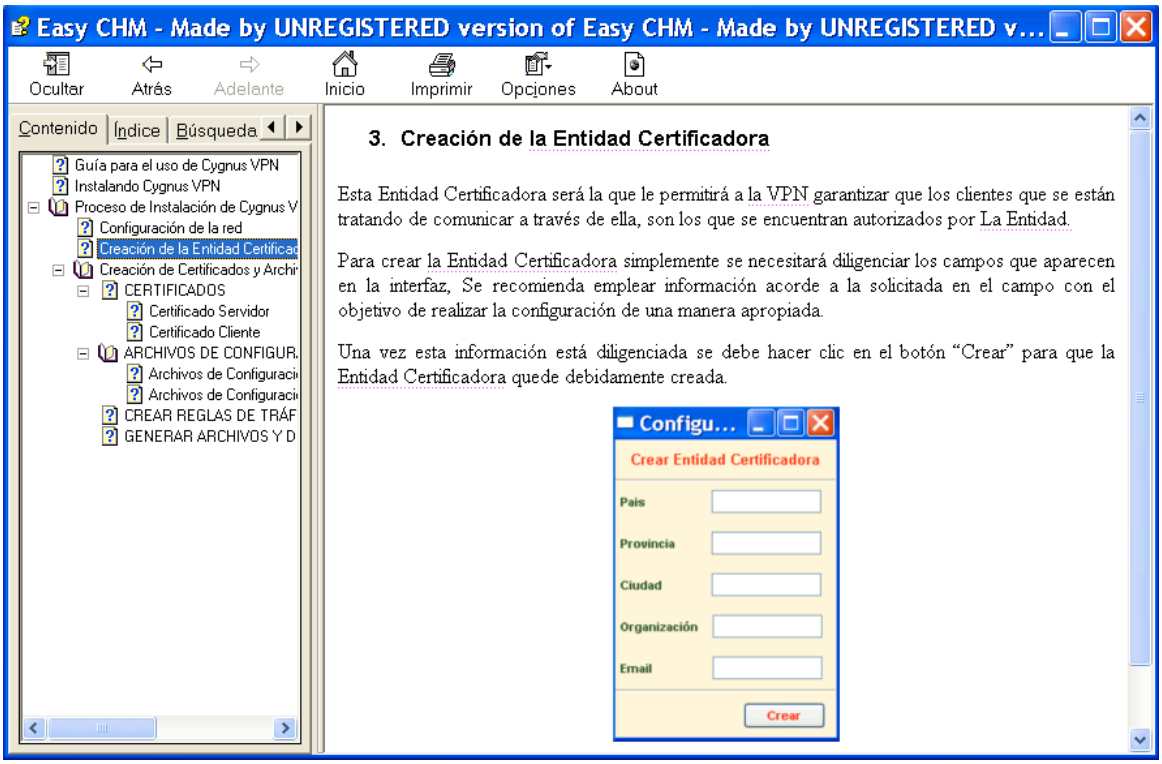
4.3. MANUAL

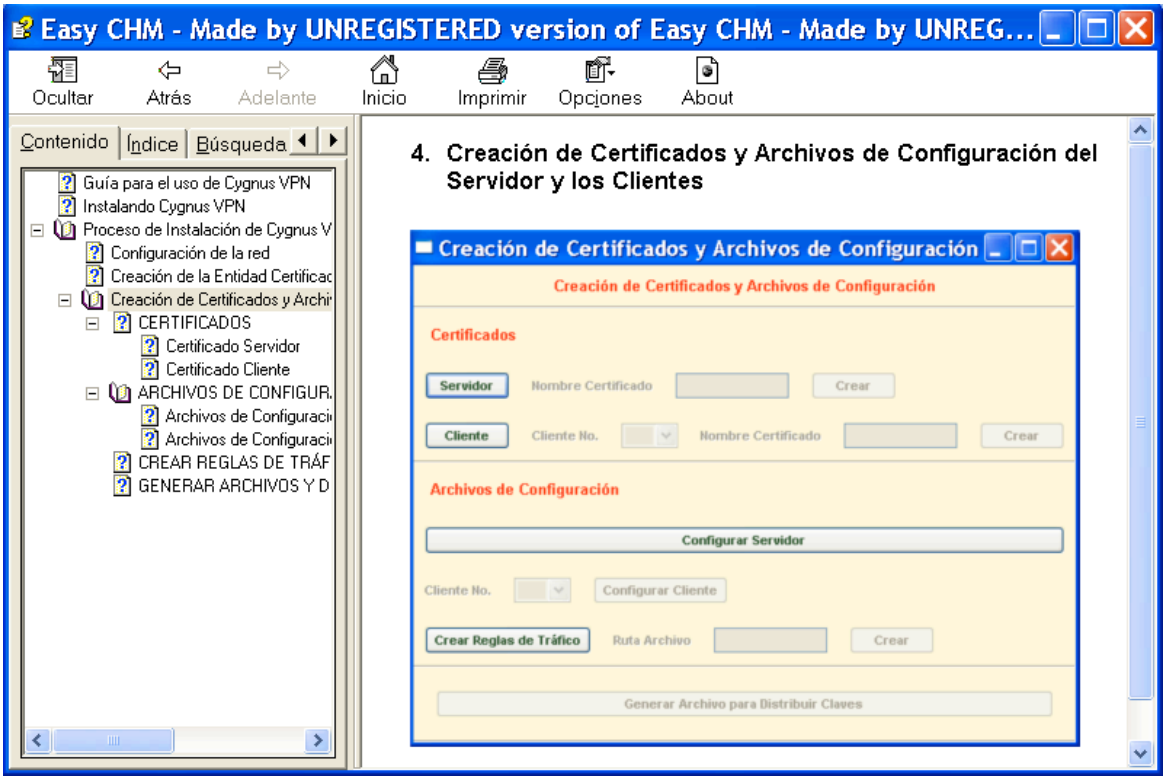

Easy CHM - Made by UNREGISTERED version of Easy CHM - Made by UN...
Ocultar
Atrás
Adelante
Inicio
Imprimir
Opciones
About
Contenido
Índice
Búsqueda
Favoritos
Guía para el uso de Cygnus VPN
Instalando Cygnus VPN
Proceso de Instalación de Cygnus VPN
Configuración de la red
Creación de la Entidad Certificadora
Creación de Certificados y Archivos de
CERTIFICADOS
Certificado Servidor
Certificado Cliente
ARCHIVOS DE CONFIGURACIÓN
Archivos de Configuración Serv
Archivos de Configuración Clier
CREAR REGLAS DE TRÁFICO
GENERAR ARCHIVOS Y DISTRIB
Guía para el uso de Cygnus VPN
Bienvenido a la guía para la instalación y uso de Cygnus VPN, de ante mano queremos agradecerle por haber escogido Cygnus VPN para la implementación de su VPN. Esta guía le ayudará a aprender de manera rápida como utilizar y configurar Cygnus VPN, de una manera fácil y amigable para que usted pueda disfrutar rápidamente de los beneficios que le traerá la implementación de su Red Privada Virtual.

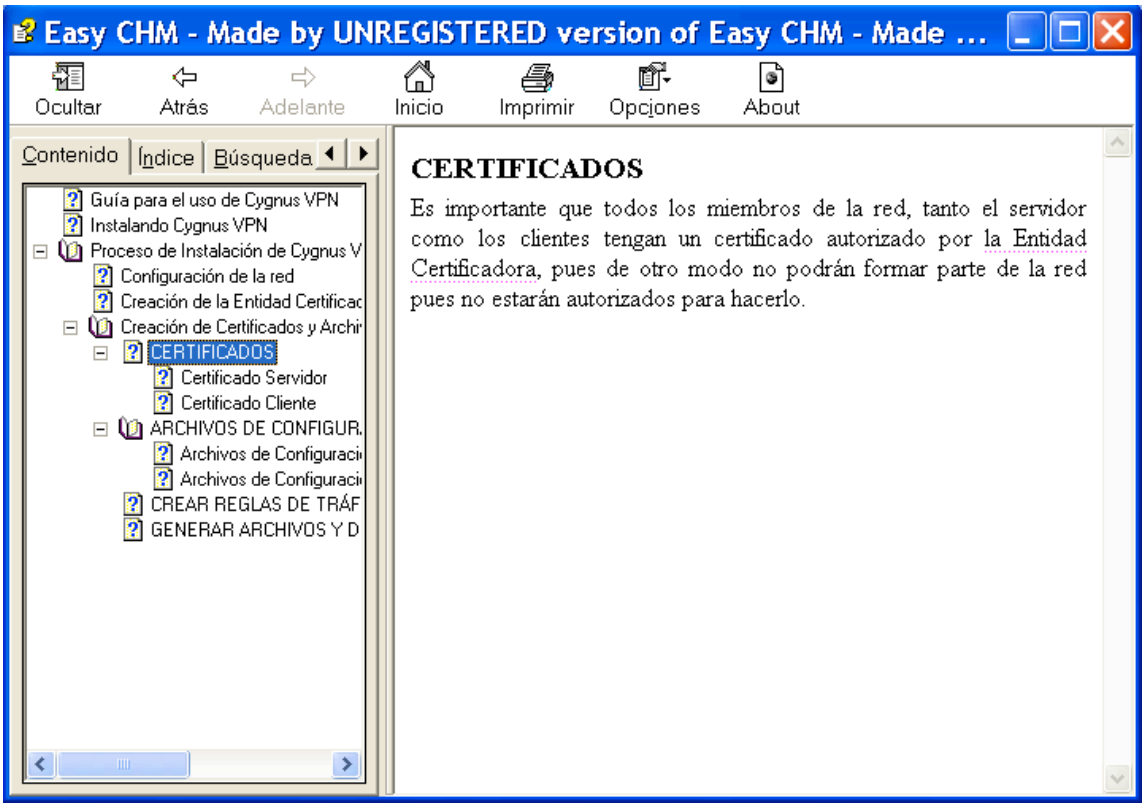

Easy CHM - Made by UNREGISTERED version of Easy CHM - Made by UN...
Ocultar
Atrás
Adelante
Inicio
Imprimir
Opciones
About
Contenido
Índice
Búsqueda
Favoritos
Guía para el uso de Cygnus VPN
Instalando Cygnus VPN
Proceso de Instalación de Cygnus VPN
Configuración de la red
Creación de la Entidad Certificadora
Creación de Certificados y Archivos de
CERTIFICADOS
Certificado Servidor
Certificado Cliente
ARCHIVOS DE CONFIGURACIÓN
Archivos de Configuración Serv
Archivos de Configuración Clier
CREAR REGLAS DE TRÁFICO
GENERAR ARCHIVOS Y DISTRIB
Instalando Cygnus VPN
Cygnus VPN fue creada pensando en brindarle comodidad a los usuarios a la hora de instalar una VPN, debido a que en un mismo paquete encontrarán todas las librerías y herramientas necesarias para la implementación de un tipo de red como estas, además brinda confianza en cuanto a la compatibilidad de las mismas ya que el producto fue totalmente diseñado y probado para trabajar en conjunto con las herramientas seleccionadas. Otro beneficio que encontrarán algunos usuarios no muy expertos es que no se manejarán consolas durante el proceso de instalación y configuración de la red lo cual hacía que en algunos casos esta tarea no quedara bien realizada, ahora gracias al diseño de las interfaces este proceso será muy claro y cómodo incluso para usuarios más expertos.

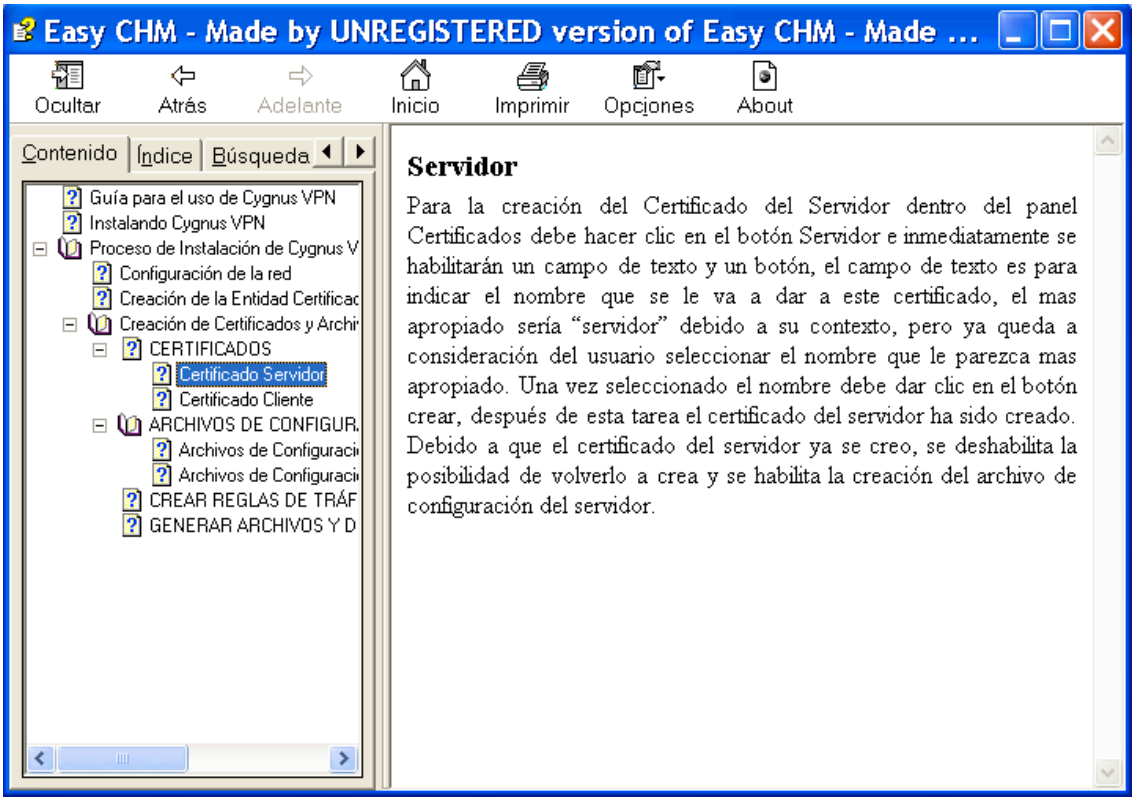

Easy CHM - Made by UNREGISTERED version of Easy CHM - Made by UNREGIS...
Ocultar
Atrás
Adelante
Inicio
Imprimir
Opciones
About
Contenido
Índice
Búsqueda
Favoritos
Guía para el uso de Cygnus VPN
Instalando Cygnus VPN
Proceso de Instalación de Cygnus VPN
Configuración de la red
Creación de la Entidad Certificadora
Creación de Certificados y Archivos de
CERTIFICADOS
Certificado Servidor
Certificado Cliente
ARCHIVOS DE CONFIGURACIÓN
Archivos de Configuración Serv
Archivos de Configuración Clier
CREAR REGLAS DE TRÁFICO
GENERAR ARCHIVOS Y DISTRIB
Proceso de Instalación de Cygnus VPN
1. Instalación de las librerías y herramientas necesarias para el montaje.
Es importante aclarar que todas las herramientas sin excepción alguna deben instalarse pues se requieren para el óptimo funcionamiento de la red, si alguna de estas herramientas falta es probable que la red no funcione y si funciona se pueden presentar inconsistencias graves en cuanto a seguridad.
Queda pues bajo la responsabilidad del usuario que todas estas herramientas sean instaladas, ya que es la única manera de garantizar que Cygnus VPN funcione de manera apropiada.
Una vez seleccionadas las herramientas se debe dar clic al botón "Instalar" para proceder a instalarlas y continuar con el siguiente paso, si se desea abortar la instalación se debe dar clic en el botón "Cancelar".
Instalación VP...
Herramientas Requeridas
Verifique que las siguietes herramientas se encuentren instaladas en su equipo, de no ser así, debe instalarlas antes de proceder con el proceso de configuración de la red.
HERRAMIENTAS:
OpenVPN
OpenSSL
Librería LZO
Módulo TUN/TAP
Continuar
Cancelar

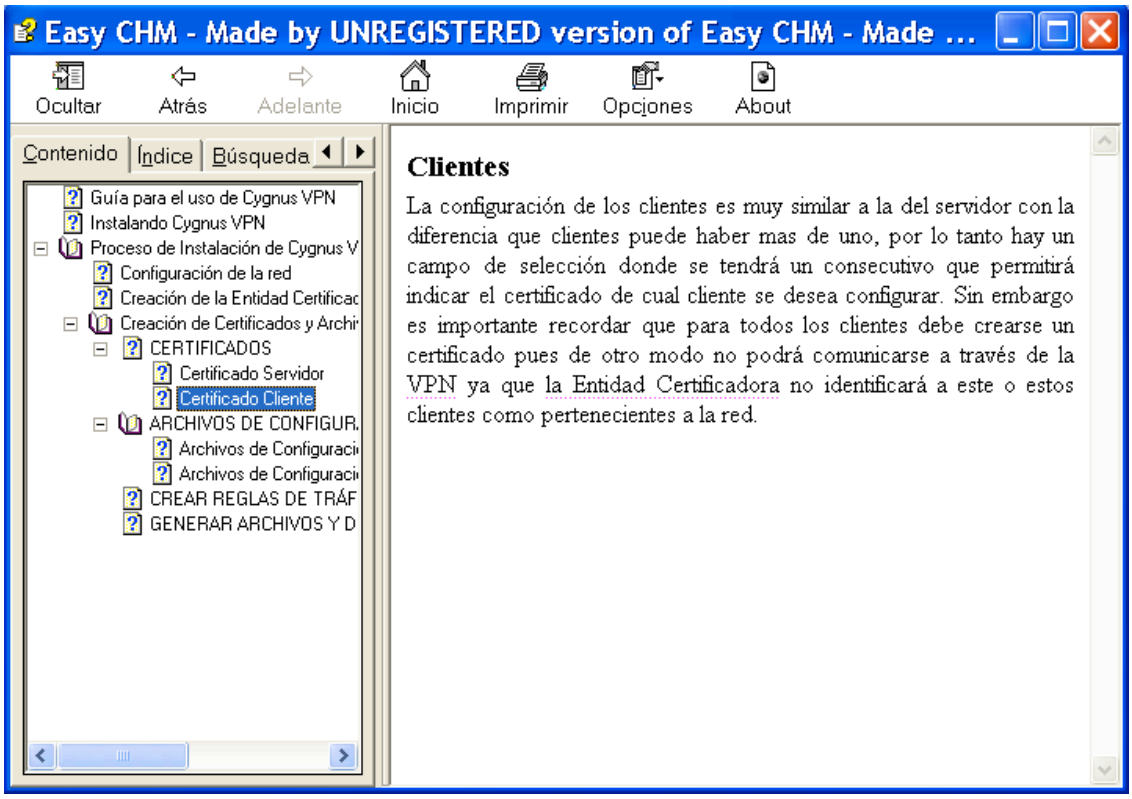

Easy CHM - Made by UNREGISTERED version of Easy CHM - Made by UNREGISTERED versi...
Ocultar
Atrás
Adelante
Inicio
Imprimir
Opciones
About
Contenido
Índice
Búsqueda
Guía para el uso de Cygnus VPN
Instalando Cygnus VPN
Proceso de Instalación de Cygnus V
Configuración de la red
Creación de la Entidad Certificac
Creación de Certificados y Archi
CERTIFICADOS
Certificado Servidor
Certificado Cliente
ARCHIVOS DE CONFIGUR.
Archivos de Configuraci
Archivos de Configuraci
CREAR REGLAS DE TRÁF
GENERAR ARCHIVOS Y D
2. Configuración de la red
Para la configuración de la red, se necesita la dirección por la cual el servidor va a escuchar a todos los clientes junto con la máscara de subred, además se debe especificar la interfaz TUN/TAP que es la dirección virtual que se va a emplear para crear el túnel Seguro.
Para completar esta configuración se requiere las direcciones de todos los clientes que se van a conectar al servidor junto con su máscara de subred y la dirección que se les asignará para la Interfáz TUN/TAP.
A medida que se van creando clientes ellos van a ir generando un consecutivo para poder llevar un control sobre el número de clientes conectados a la red.
Una vez estén configurados el servidor y por lo menos un cliente se habilitará el botón de continuar, pero no se debe continuar con el siguiente paso hasta que todos los clientes hayan sido configurados.
Configuración de la Red
Configuración de la Red
Servidor
Dirección Servidor
Mascara
Interfaz TUN/TAP
Guardar
Clientes
Dirección Cliente
Mascara
Interfaz TUN/TAP
Guardar y Configurar otro
Continuar

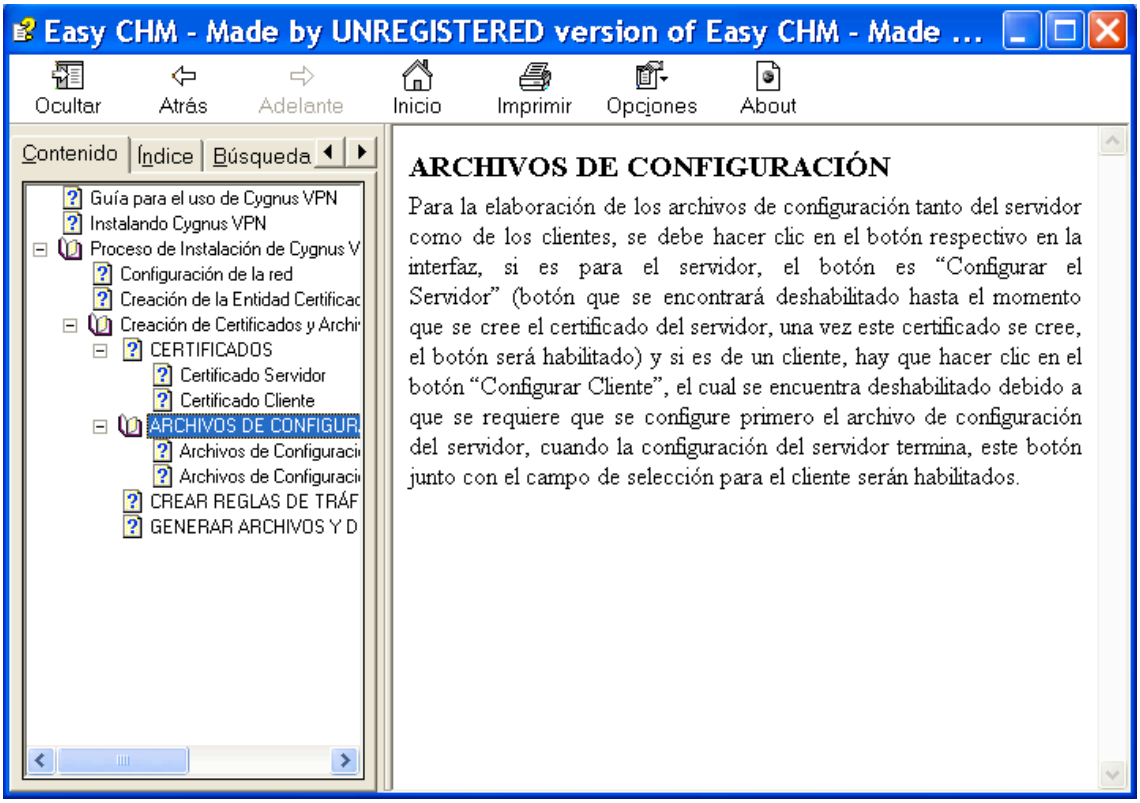

Easy CHM - Made by UNREGISTERED version of Easy CHM - Made by UNREGISTERED v...
Ocultar
Atrás
Adelante
Inicio
Imprimir
Opciones
About
Contenido
Índice
Búsqueda
Guía para el uso de Cygnus VPN
Instalando Cygnus VPN
Proceso de Instalación de Cygnus V
Configuración de la red
Creación de la Entidad Certificac
Creación de Certificados y Archi
CERTIFICADOS
Certificado Servidor
Certificado Cliente
ARCHIVOS DE CONFIGUR.
Archivos de Configuraci
Archivos de Configuraci
CREAR REGLAS DE TRÁF
GENERAR ARCHIVOS Y D
3. Creación de la Entidad Certificadora
Esta Entidad Certificadora será la que le permitirá a la VPN garantizar que los clientes que se están tratando de comunicar a través de ella, son los que se encuentran autorizados por La Entidad.
Para crear la Entidad Certificadora simplemente se necesitará diligenciar los campos que aparecen en la interfaz, Se recomienda emplear información acorde a la solicitada en el campo con el objetivo de realizar la configuración de una manera apropiada.
Una vez esta información está diligenciada se debe hacer clic en el botón "Crear" para que la Entidad Certificadora quede debidamente creada.
Configu...
Crear Entidad Certificadora
Pais
Provincia
Ciudad
Organización
Email
Crear

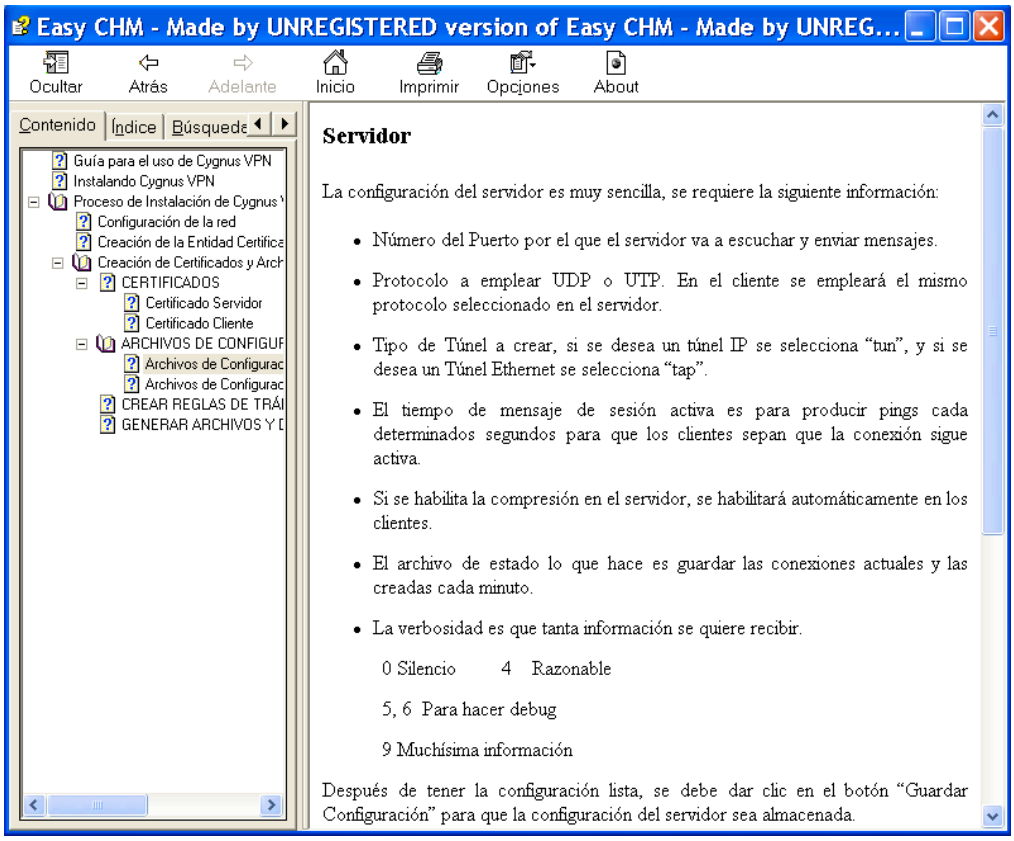

Easy CHM - Made by UNREGISTERED version of Easy CHM - Made by UNREG...
Ocultar
Atrás
Adelante
Inicio
Imprimir
Opciones
About
Contenido
Índice
Búsqueda
Guía para el uso de Cygnus VPN
Instalando Cygnus VPN
Proceso de Instalación de Cygnus V
Configuración de la red
Creación de la Entidad Certificac
Creación de Certificados y Archi
CERTIFICADOS
Certificado Servidor
Certificado Cliente
ARCHIVOS DE CONFIGUR.
Archivos de Configuraci
Archivos de Configuraci
CREAR REGLAS DE TRÁF
GENERAR ARCHIVOS Y D
4. Creación de Certificados y Archivos de Configuración del Servidor y los Clientes
Creación de Certificados y Archivos de Configuración
Creación de Certificados y Archivos de Configuración
Certificados
Servidor
Nombre Certificado
Crear
Cliente
Cliente No.
Nombre Certificado
Crear
Archivos de Configuración
Configurar Servidor
Cliente No.
Configurar Cliente
Crear Reglas de Tráfico
Ruta Archivo
Crear
Generar Archivo para Distribuir Claves

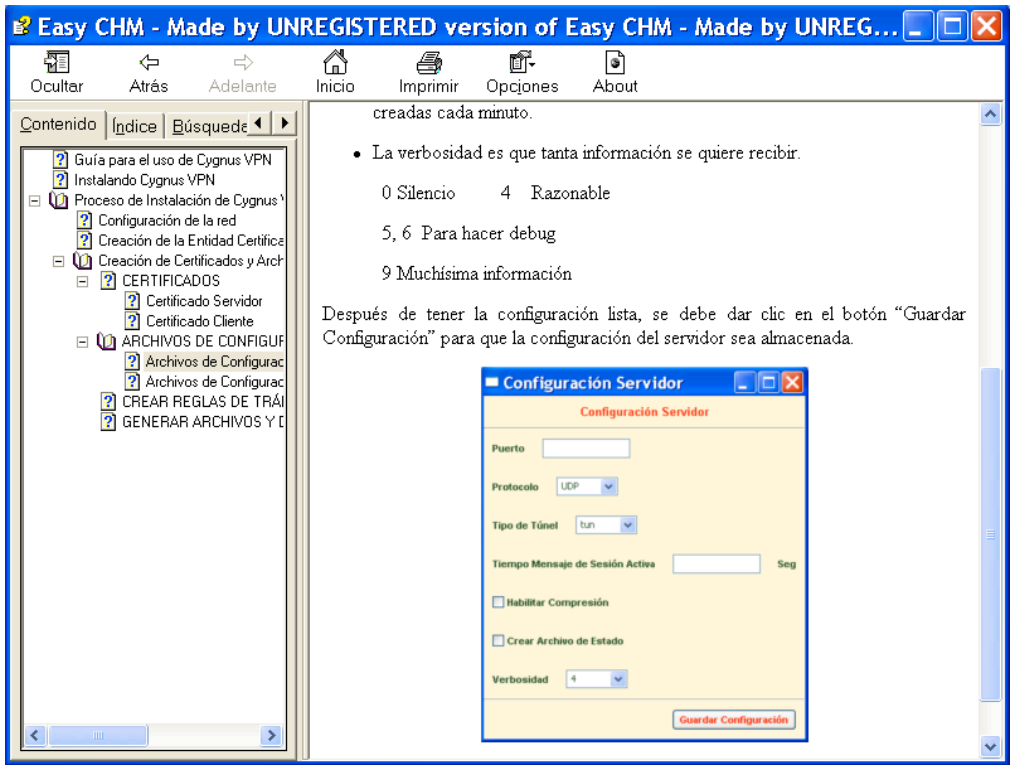

Easy CHM - Made by UNREGISTERED version of Easy CHM - Made ...
Ocultar
Atrás
Adelante
Inicio
Imprimir
Opciones
About
Contenido
Índice
Búsqueda
Guía para el uso de Cygnus VPN
Instalando Cygnus VPN
Proceso de Instalación de Cygnus V
Configuración de la red
Creación de la Entidad Certificac
Creación de Certificados y Archi
CERTIFICADOS
Certificado Servidor
Certificado Cliente
ARCHIVOS DE CONFIGUR.
Archivos de Configuraci
Archivos de Configuraci
CREAR REGLAS DE TRÁF
GENERAR ARCHIVOS Y D
CERTIFICADOS
Es importante que todos los miembros de la red, tanto el servidor como los clientes tengan un certificado autorizado por la Entidad Certificadora, pues de otro modo no podrán formar parte de la red pues no estarán autorizados para hacerlo.

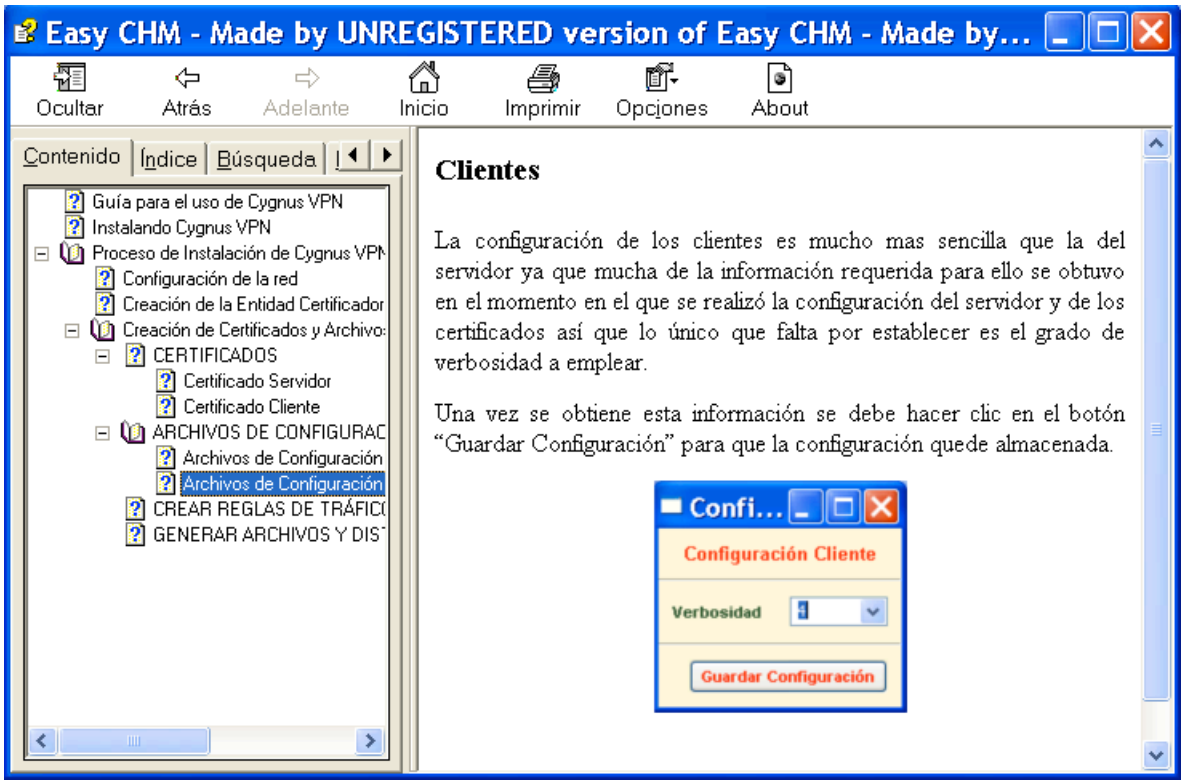

Easy CHM - Made by UNREGISTERED version of Easy CHM - Made ...
Ocultar
Atrás
Adelante
Inicio
Imprimir
Opciones
About
Contenido
Índice
Búsqueda
Guía para el uso de Cygnus VPN
Instalando Cygnus VPN
Proceso de Instalación de Cygnus V
Configuración de la red
Creación de la Entidad Certificac
Creación de Certificados y Archi
CERTIFICADOS
Certificado Servidor
Certificado Cliente
ARCHIVOS DE CONFIGUR.
Archivos de Configuraci
Archivos de Configuraci
CREAR REGLAS DE TRÁF
GENERAR ARCHIVOS Y D
Servidor
Para la creación del Certificado del Servidor dentro del panel Certificados debe hacer clic en el botón Servidor e inmediatamente se habilitarán un campo de texto y un botón, el campo de texto es para indicar el nombre que se le va a dar a este certificado, el mas apropiado sería "servidor" debido a su contexto, pero ya queda a consideración del usuario seleccionar el nombre que le parezca mas apropiado. Una vez seleccionado el nombre debe dar clic en el botón crear, después de esta tarea el certificado del servidor ha sido creado. Debido a que el certificado del servidor ya se creo, se deshabilita la posibilidad de volverlo a crea y se habilita la creación del archivo de configuración del servidor.

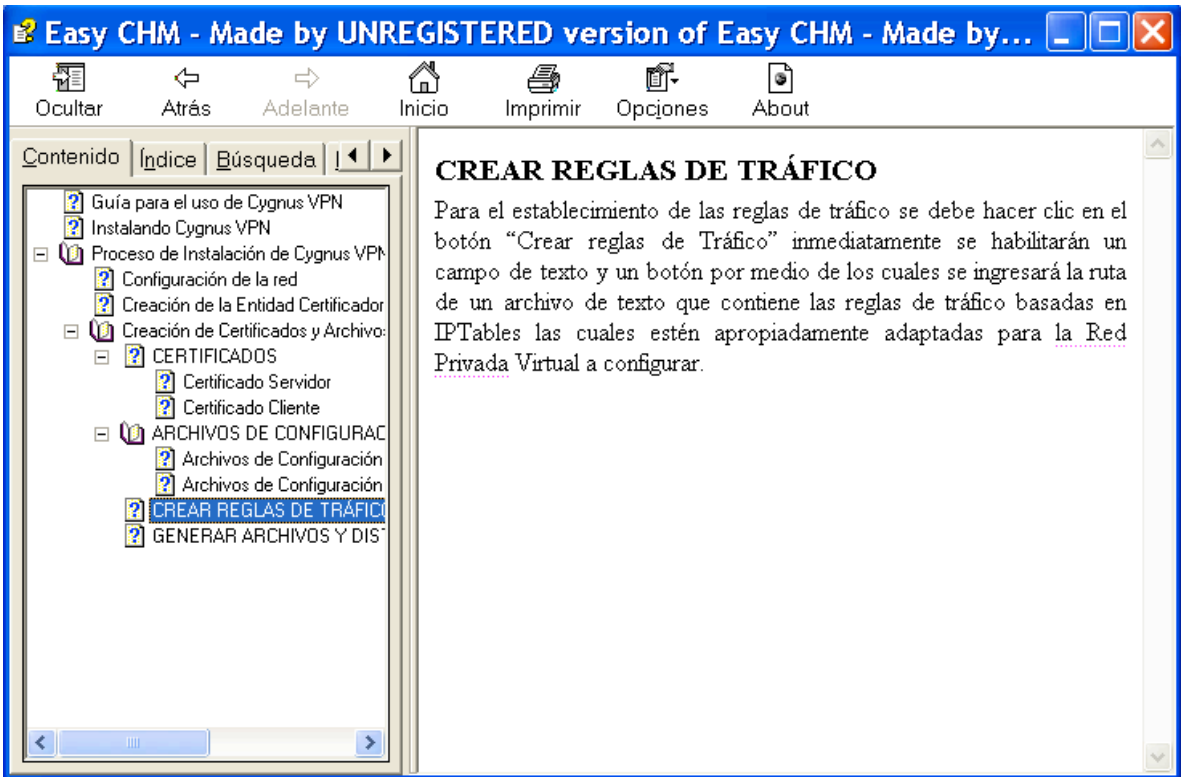

Easy CHM - Made by UNREGISTERED version of Easy CHM - Made ...
Ocultar
Atrás
Adelante
Inicio
Imprimir
Opciones
About
Contenido
Índice
Búsqueda
Guía para el uso de Cygnus VPN
Instalando Cygnus VPN
Proceso de Instalación de Cygnus V
Configuración de la red
Creación de la Entidad Certificac
Creación de Certificados y Archi
CERTIFICADOS
Certificado Servidor
Certificado Cliente
ARCHIVOS DE CONFIGUR
Archivos de Configuraci
Archivos de Configuraci
CREAR REGLAS DE TRÁF
GENERAR ARCHIVOS Y D
Clientes
La configuración de los clientes es muy similar a la del servidor con la diferencia que clientes puede haber mas de uno, por lo tanto hay un campo de selección donde se tendrá un consecutivo que permitirá indicar el certificado de cual cliente se desea configurar. Sin embargo es importante recordar que para todos los clientes debe crearse un certificado pues de otro modo no podrá comunicarse a través de la VPN ya que la Entidad Certificadora no identificará a este o estos clientes como pertenecientes a la red.

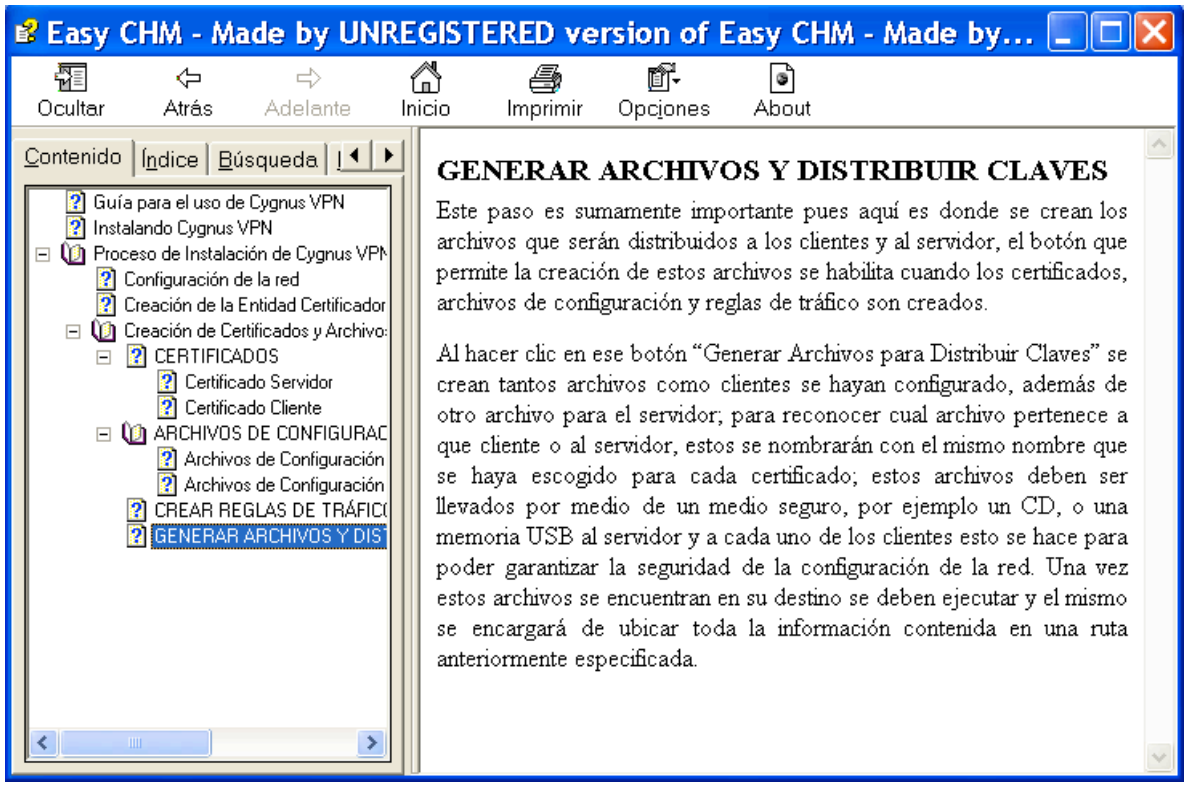

Easy CHM - Made by UNREGISTERED version of Easy CHM - Made ...
Ocultar
Atrás
Adelante
Inicio
Imprimir
Opciones
About
Contenido
Índice
Búsqueda
Guía para el uso de Cygnus VPN
Instalando Cygnus VPN
Proceso de Instalación de Cygnus V
Configuración de la red
Creación de la Entidad Certificac
Creación de Certificados y Archi
CERTIFICADOS
Certificado Servidor
Certificado Cliente
ARCHIVOS DE CONFIGUR
Archivos de Configuraci
Archivos de Configuraci
CREAR REGLAS DE TRÁF
GENERAR ARCHIVOS Y D
ARCHIVOS DE CONFIGURACIÓN
Para la elaboración de los archivos de configuración tanto del servidor como de los clientes, se debe hacer clic en el botón respectivo en la interfaz, si es para el servidor, el botón es "Configurar el Servidor" (botón que se encontrará deshabilitado hasta el momento que se cree el certificado del servidor, una vez este certificado se cree, el botón será habilitado) y si es de un cliente, hay que hacer clic en el botón "Configurar Cliente", el cual se encuentra deshabilitado debido a que se requiere que se configure primero el archivo de configuración del servidor, cuando la configuración del servidor termina, este botón junto con el campo de selección para el cliente serán habilitados.


Easy CHM - Made by UNREGISTERED version of Easy CHM - Made by UNREG...
Ocultar
Atrás
Adelante
Inicio
Imprimir
Opciones
About
Contenido
Índice
Búsqueda
Guía para el uso de Cygnus VPN
Instalando Cygnus VPN
Proceso de Instalación de Cygnus
Configuración de la red
Creación de la Entidad Certifica
Creación de Certificados y Arch
CERTIFICADOS
Certificado Servidor
Certificado Cliente
ARCHIVOS DE CONFIGUR
Archivos de Configurac
Archivos de Configurac
CREAR REGLAS DE TRÁ
GENERAR ARCHIVOS Y
Servidor
La configuración del servidor es muy sencilla, se requiere la siguiente información:
Número del Puerto por el que el servidor va a escuchar y enviar mensajes.
Protocolo a emplear UDP o UTP. En el cliente se empleará el mismo protocolo seleccionado en el servidor.
Tipo de Túnel a crear, si se desea un túnel IP se selecciona "tun", y si se desea un Túnel Ethernet se selecciona "tap".
El tiempo de mensaje de sesión activa es para producir pings cada determinados segundos para que los clientes sepan que la conexión sigue activa.
Si se habilita la compresión en el servidor, se habilitará automáticamente en los clientes.
El archivo de estado lo que hace es guardar las conexiones actuales y las creadas cada minuto.
La verbosidad es que tanta información se quiere recibir.
0 Silencio 4 Razonable
5, 6 Para hacer debug
9 Muchísima información
Después de tener la configuración lista, se debe dar clic en el botón "Guardar Configuración" para que la configuración del servidor sea almacenada.


Easy CHM - Made by UNREGISTERED version of Easy CHM - Made by UNREG...
Ocultar
Atrás
Adelante
Inicio
Imprimir
Opciones
About
Contenido
Índice
Búsqueda
creadas cada minuto.
La verbosidad es que tanta información se quiere recibir.
0 Silencio 4 Razonable
5, 6 Para hacer debug
9 Muchísima información
Después de tener la configuración lista, se debe dar clic en el botón "Guardar Configuración" para que la configuración del servidor sea almacenada.
Configuración Servidor
Configuración Servidor
Puerto
Protocolo
UDP
Tipo de Túnel
tun
Tiempo Mensaje de Sesión Activa
Seg
Habilitar Compresión
Crear Archivo de Estado
Verbosidad
4
Guardar Configuración


Easy CHM - Made by UNREGISTERED version of Easy CHM - Made by...
Ocultar
Atrás
Adelante
Inicio
Imprimir
Opciones
About
Contenido
Índice
Búsqueda
Guía para el uso de Cygnus VPN
Instalando Cygnus VPN
Proceso de Instalación de Cygnus VPN
Configuración de la red
Creación de la Entidad Certificador
Creación de Certificados y Archivo:
CERTIFICADOS
Certificado Servidor
Certificado Cliente
ARCHIVOS DE CONFIGURAC
Archivos de Configuración
Archivos de Configuración
CREAR REGLAS DE TRÁFIC
GENERAR ARCHIVOS Y DIS
Clientes
La configuración de los clientes es mucho mas sencilla que la del servidor ya que mucha de la información requerida para ello se obtuvo en el momento en el que se realizó la configuración del servidor y de los certificados así que lo único que falta por establecer es el grado de verbosidad a emplear.
Una vez se obtiene esta información se debe hacer clic en el botón "Guardar Configuración" para que la configuración quede almacenada.
Confi...
Configuración Cliente
Verbosidad
3
Guardar Configuración


Easy CHM - Made by UNREGISTERED version of Easy CHM - Made by...
Ocultar
Atrás
Adelante
Inicio
Imprimir
Opciones
About
Contenido
Índice
Búsqueda
Guía para el uso de Cygnus VPN
Instalando Cygnus VPN
Proceso de Instalación de Cygnus VPN
Configuración de la red
Creación de la Entidad Certificador
Creación de Certificados y Archivo:
CERTIFICADOS
Certificado Servidor
Certificado Cliente
ARCHIVOS DE CONFIGURAC
Archivos de Configuración
Archivos de Configuración
CREAR REGLAS DE TRÁFIC
GENERAR ARCHIVOS Y DIS
CREAR REGLAS DE TRÁFICO
Para el establecimiento de las reglas de tráfico se debe hacer clic en el botón "Crear reglas de Tráfico" inmediatamente se habilitarán un campo de texto y un botón por medio de los cuales se ingresará la ruta de un archivo de texto que contiene las reglas de tráfico basadas en IPTables las cuales estén apropiadamente adaptadas para la Red Privada Virtual a configurar.


Easy CHM - Made by UNREGISTERED version of Easy CHM - Made by...
Ocultar
Atrás
Adelante
Inicio
Imprimir
Opciones
About
Contenido
Índice
Búsqueda
Guía para el uso de Cygnus VPN
Instalando Cygnus VPN
Proceso de Instalación de Cygnus VPN
Configuración de la red
Creación de la Entidad Certificador
Creación de Certificados y Archivo:
CERTIFICADOS
Certificado Servidor
Certificado Cliente
ARCHIVOS DE CONFIGURAC
Archivos de Configuración
Archivos de Configuración
CREAR REGLAS DE TRÁFIC
GENERAR ARCHIVOS Y DIS
GENERAR ARCHIVOS Y DISTRIBUIR CLAVES
Este paso es sumamente importante pues aquí es donde se crean los archivos que serán distribuidos a los clientes y al servidor, el botón que permite la creación de estos archivos se habilita cuando los certificados, archivos de configuración y reglas de tráfico son creados.
Al hacer clic en ese botón "Generar Archivos para Distribuir Claves" se crean tantos archivos como clientes se hayan configurado, además de otro archivo para el servidor; para reconocer cual archivo pertenece a que cliente o al servidor, estos se nombrarán con el mismo nombre que se haya escogido para cada certificado; estos archivos deben ser llevados por medio de un medio seguro, por ejemplo un CD, o una memoria USB al servidor y a cada uno de los clientes esto se hace para poder garantizar la seguridad de la configuración de la red. Una vez estos archivos se encuentran en su destino se deben ejecutar y el mismo se encargará de ubicar toda la información contenida en una ruta anteriormente especificada.

5. CONCLUSIONES

Se pudo concluir que una red privada virtual es una implementación o sistema que habilita una comunicación segura a través de un medio inseguro, siendo transparente para el usuario u aplicación que realiza y recibe la comunicación.

Gracias a documentación recopilada de Internet, se pudieron conocer las principales características de las diferentes herramientas libres existentes en el mercado para la creación de Redes Privadas Virtuales; logrando de esta manera relacionar mediante un análisis de cuadros comparativos las principales ventajas y desventajas de cada una de ellas; este análisis brindó argumentos que permitieron escoger la mejor herramienta según los resultados obtenidos.

Luego de realizar análisis comparativos entre las soluciones para configurar VPNs basadas en software y hardware se decidió que este proyecto se base en los tipos de soluciones basados en software libre ya que mediante la combinación de ciertos factores, brinda mayores beneficios tanto en seguridad y desempeño como en costos a los usuarios.

Después de indagar en el mercado se encontraron varias aplicaciones reconocidas para realizar la configuración de una Red Privada Virtual, con el fin de determinar que herramienta es mas apropiada para la realización de este proyecto se realizó un análisis comparativo entre las herramientas mas reconocidas, siendo estas: IPSec por ser considerado como estándar dentro de la industria y OpenVPN por ser una herramienta nueva pero que ha tenido críticas favorables en la documentación consultada, además de estar ganando terreno en el mercado de manera rápida. Una vez realizado el análisis, se decidió seleccionar la segunda opción ya que permite realizar el proceso de instalación y configuración de una VPN de una manera más fácil, está publicado bajo la licencia GPL, de código abierto, y es multiplataforma.

Actualmente las herramientas utilizadas para la creación de Redes Privadas Virtuales, aunque ofrecen un buen desempeño, a veces es difícil llegar a éste debido a que exige muy buenos conocimientos técnicos en la configuración, haciendo de esta una tarea complicada incluso para personas con altos conocimientos en el tema. Gracias a las interfaces que trae CygnusVPN, una Red

Privada Virtual puede ser configurada por usuarios con pocos conocimientos técnicos de manera rápida y fácil.

Se obtuvieron conocimientos fuertes en cuanto a la configuración de Redes Privadas Virtuales ya que se estudiaron a fondo cada una de las etapas de configuración.

Se adquirieron fundamentos necesarios para el uso de las herramientas empleadas en la fase de desarrollo de la aplicación CygnusVPN como son:

- Python
- wxPython
- wxWidgets
- wxFormBuilder

5.1. RECOMENDACIONES

Para garantizar un correcto funcionamiento de la VPN, creada a través de CygnusVPN es importante considerar que al momento de instalar las herramientas para la configuración de la red, se deben emplear mecanismos que permitan garantizar la compatibilidad de las mismas, por ejemplo en el caso de las distribuciones Debian las cuales cuentan con una herramienta incorporada para la instalación de aplicaciones denominada **apt-get.** La ventaja de emplear este tipo de herramientas, es que así se resolverán todos los problemas de dependencias de otros paquetes que se puedan necesitar y de igual manera informar si hay problemas por paquetes no encontrados o incompatibilidades. Esto es importante pues el buen funcionamiento de la aplicación CygnusVPN puede verse afectado por no instalar las herramientas apropiadas.

CygnusVPN al considerarse un prototipo de configuración de Redes Privadas Virtuales, por ahora solo es disponible para diferentes distribuciones de GNU/Linux, sin embargo a futuro se puede hacer que la aplicación CygnusVPN sea aplicable en diferentes plataformas existentes en el mercado ya que la herramienta empleada OpenVPN lo permite.

En un principio se pretendía que la aplicación CygnusVPN efectuara todos los pasos necesarios para la creación de la VPN incluyendo la instalación de los paquetes requeridos para garantizar el buen funcionamiento de la red, al existir

diferentes distribuciones de GNU/Linux en el mercado y en aras de garantizar compatibilidad entre las diferentes versiones se omitió este paso. Sin embargo, esto da pie a pensar en la creación de modificaciones de la aplicación CygnusVPN las cuales permitan realizar la instalación de las herramientas pero garantizando la compatibilidad entre las diferentes versiones de GNU/Linux.

Este trabajo sirve como punto de partida para posteriores proyectos que quieran profundizar más en cuanto a la configuración de Redes Privadas Virtuales, pensando en abarcar comunicaciones entre diferentes plataformas de desarrollo.

5.2. APORTES

Indagando sobre la evolución de las redes en Internet, se pudo crear un documento en español el cual brinda todo un panorama que permite ver las ventajas que puede proporcionar la adaptación de una Red Privada Virtual en un entorno apropiado. Además se mencionan temas como las herramientas existentes actualmente junto con sus ventajas y desventajas y la configuración de una VPN de manera tradicional.

Gracias a la experiencia obtenida en el uso de CygnusVPN se pudo apreciar que no se requiere hardware muy poderoso en las máquinas para la implementación la red.

Para un mejor entendimiento del funcionamiento de la aplicación CygnusVPN, se elaboró y se entrega al usuario un manual en español con un lenguaje sencillo, de fácil comprensión para cualquier tipo de usuario, el cual le permitirá configurar una VPN.

Las herramientas empleadas para la elaboración de CygnusVPN están cobijadas bajo la filosofía del software libre, para que de esta manera la aplicación CygnusVPN final pueda ser estudiada y utilizada por cualquier tipo de persona sin ningún tipo de contratiempo.

Se entrega evidencia sobre la realización de pruebas satisfactorias comprobando el buen funcionamiento de CygnusVPN en una red conformada por cuatro equipos; teniendo dos conexiones a Internet en donde se ensayaron diferentes tipos de conexión como lo son:

- servidor a servidor

- cliente a servidor
- cliente a cliente