UNIVERSIDAD CATOLICA DE SANTIAGO DE GUAYAQUIL

Facultad de Educación Técnica para el Desarrollo
CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

Tesis de Grado

Previo a la obtención del título de

INGENIERO EN TELECOMUNICACIONES

Mención en Gestión Empresarial

Tema:
"DISEÑO E IMPLEMENTACIÓN DE UNA VPN BASADA EN SOFTWARE ENTRE LA UNIVERSIDAD CATÓLICA DE SANTIAGO DE GUAYAQUIL Y LA UNIDAD EDUCATIVA FREIRESTABILE"

Realizado por:

Andy Abraham Rodríguez Aspiazu

David Kléber Reyes Martínez

Christian Dennis Balseca Ramírez

Director de Tesis

Ing. Luis Córdova

Guayaquil **2011** **Ecuador**

TESIS DE GRADO

Título

"DISEÑO E IMPLEMENTACIÓN DE UNA VPN BASADA EN SOFTWARE ENTRE LA UNIVERSIDAD CATÓLICA DE SANTIAGO DE GUAYAQUIL Y LA UNIDAD EDUCATIVA FREIRE STABILE"

Presentada a la Facultad de Educación Técnica para el Desarrollo, Carrera de Ingeniería en Telecomunicaciones de la Universidad Católica de Santiago de Guayaquil.

Realizado por:

Andy Abraham Rodríguez Aspiazu

David Kléber Reyes Martínez

Christian Dennis Balseca Ramírez

Para dar cumplimiento con uno de los requisitos para optar por el Título de:

INGENIERO EN TELECOMUNICACIONES
Mención en Gestión Empresarial

Miembros del Tribunal

Director de Tesis

Ing. Luis Córdova

Ing. Héctor Cedeño
Vocal I

Ing. Carlos Zambrano
Vocal II

Ing. Manuel Romero
Decano de la Facultad

Ing. Luis Córdova
Director de la carrera

INDICE GENERAL

CAPITULO I

CAPITULO II

CAPITULO III

CAPITULO IV

INDICE DE FIGURAS

INDICE DE TABLAS

AGRADECIMIENTO

Nuestro agradecimiento a Dios, por llevarnos a su lado a lo largo de esta vida, siempre llenándonos de fortaleza y dicha y, por dejarnos culminar con éxito nuestros propósitos de ser profesionales.

A nuestros padres, por enseñarnos los valores y toda la fuerza, por el constante apoyo y paciencia.

Igualmente, queremos agradecer cordialmente a nuestro director de Tesis, Ing. Luis Córdova, por su voluntad, esfuerzo, dedicación y apoyo durante la realización de nuestra tesis.

También nos gustaría agradecer los consejos y reflexiones recibidos a lo largo de los últimos años por otros profesores/as de la Facultad Técnica, que de una manera u otra han aportado su apoyo y colaboración a nuestra formación.

DEDICATORIA

Esta tesis está dedicada especialmente a nuestros padres, por su comprensión y ayuda en momentos malos y buenos. Nos han enseñado a encarar las adversidades sin perder nunca la dignidad ni decaer en el intento. Nos han dado todo lo que somos como persona, los valores, principios, perseverancia y empeño, y todo ello con una gran dosis de amor y sin pedir nunca nada a cambio.

Igualmente, este trabajo está dedicado a todos los estudiantes de la Facultad Técnica de la carrera de Telecomunicaciones.

A todos nuestros profesores y autoridades de la Facultad Técnica, por la comprensión, apoyo incondicional y consejos, a todos ellos, está dedicada esta tesis.

GLOSARIO DE TERMINOS

ACL: (Access Control List), es una lista de los servicios disponibles, cada uno con una lista de los host que permitieron usar el servicio.

ARP: (Address Resolution Protocol), protocolo de resolución de dirección. Protocolo usado por una computadora para correlacionar una dirección IP con una dirección de hardware. Las computadoras que llaman el ARP difunden una solicitud a la que responde la computadora objetivo.

Backbone: Línea de transmisión de información de alta velocidad o una serie de conexiones que juntas forman una vía con gran ancho de banda. Un backbone conecta dos puntos o redes distanciados geográficamente, a altas velocidades.

Bridge: Dispositivo que conecta dos o más redes físicas y sirve para transmitir paquetes entre ellas. Puede utilizarse también para filtrar los paquetes que entran o salen, selectivamente. (Similar al router).

Cortafuegos: Mecanismo de seguridad en Internet frente a accesos no autorizados. Básicamente consiste en un filtro que mira la identidad de los paquetes y rechaza todos aquellos que no estén autorizados o correctamente identificados

DHCP: Son las siglas en inglés de Protocolo de configuración dinámica de servidores. Es un protocolo de red en el que un servidor provee los parámetros de

configuración a las computadoras 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.

DNS: (Domain Name System), es un conjunto de protocolos y servicios (base de datos distribuida) que permite a los usuarios utilizar nombres en vez de tener que recordar direcciones IP numéricas.

FTP: Uno de los diversos protocolos de la red Internet, concretamente significa File Transfer Protocol (Protocolo de Transferencia de Archivos) y es el ideal para transferir datos por la red.

Gateway: Dispositivo que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación. Su propósito es traducir la información del protocolo utilizado en una red al protocolo usado en la red de destino.

GNU: Licencia Pública General. Software desarrollado para distribución sin fines de lucro. El proyecto GNU (GNU es un acrónimo recursivo para "Gnu No es Unix") comenzó en 1984 para desarrollar un sistema operativo tipo Unix completo, que fuera Software Libre.

Host: Computador que permite a los usuarios comunicarse con otros sistemas centrales de una red. Los usuarios se comunican utilizando programas de aplicación, tales como correo electrónico, Telnet y FTP.

HSSI: Interface serial que soporta una tasa de transmisión a 52 Mbps, se usa para conectar routers en redes de área local con redes de área ancha (WAN).

HTTP: (HyperText Transmission Protocol), protocolo para transferir archivos o documentos hipertexto a través de la red. Se basa en una arquitectura cliente / servidor.

IP: (Internet Protocol), el protocolo encargado del direccionamiento (identificación del origen y destino).

ISP: (Proveedor de Servicios de Internet), empresa u organización que brinda el servicio de conexión a internet.

Kernel: En Linux parte principal del sistema operativo. Código fuente del propio sistema.

LAN: (Local Area Network). Red de Área Local. Red de datos para dar servicio a un área geográfica máxima de unos pocos kilómetros cuadrados con velocidades de transmisión de hasta 100 Mbps (100 megabits por segundo).

MAC: En redes de computadoras Media Access Control address, es un identificador físico; un número, único en el mundo, de 48 bits almacenado

MAN: (Metropolitan Area Network), que en español significa Red de Área Metropolitana. Es una red de distribución de datos para un área geográfica en el entorno de una ciudad.

NAP: (Network Access Point) Punto de Acceso a la Red. Es una facilidad de intercambio público de red donde los proveedores de acceso a internet (ISP´s,

Internet Service Providers) pueden conectarse entre sí. Los NAP´s son un componente clave del backbone de Internet porque las conexiones dentro de ellos determinan cuánto tráfico puede rutearse. También son los puntos de mayor congestionamiento de internet.

OSI: Modelo para la interconexión de sistemas abiertos (Open Systems Interconnection). Es un modelo teórico de conexión de sistemas, estructurado en 7 capas (física, enlace, red, transporte, sesión, presentación y aplicación).

OSPF: Protocolo de enrutamiento basado en el algoritmo Enlace Estado (LSA - Link State Algorithm), el cual proporciona ciertas ventajas frente a RIP. Las características de OSPF incluyen ruteo a menor costo, ruteo multiruta y balanceo de carga.

Router: Dispositivo hardware o software de interconexión de redes de ordenadores / computadoras que opera en la capa 3 (nivel de red) del modelo OSI. Este dispositivo interconecta segmentos de red o redes enteras. Hacen pasar paquetes de datos entre redes tomando como base la información de la capa de red.

SSH: Nombre de un protocolo y del programa que lo implementa. Este protocolo sirve para acceder a máquinas a través de una red, de forma similar a como se hacía con telnet. La diferencia principal es que SSH usa técnicas de cifrado para que ningún atacante pueda descubrir el usuario y contraseña de la conexión ni lo que se escribe durante toda la sesión.

Switch: Es un dispositivo de interconexión de redes de computadoras que opera en la capa 2 (nivel de enlace de datos) del modelo OSI.

TCP: (Transmission Control Protocol), es uno de los protocolos de comunicaciones sobre los que se basa Internet. Posibilita una comunicación libre de errores entre computadores en internet.

Trama: Conjunto de bits que forman un bloque de datos básico. Generalmente, una trama contiene su propia información de control, en la que se incluye la dirección del dispositivo al que está siendo enviado.

VLAN: Virtual Local Area Network o Virtual LAN. Grupo de dispositivos en una o más LANs que son configurados (utilizando software de administración) de tal manera que se pueden comunicar como si ellos estuvieran conectados al mismo cable, cuando en realidad están localizados en un segmento diferente de LAN. Esto es porque VLAN´s están basadas en las conexiones lógicas en lugar de las físicas y es por eso que son extremadamente flexibles.

WAN: Wide Area Network o Red de Area Amplia. Es una red de computadoras que puede estar localizada en un área geográfica muy extensa y puede contener varios miles de computadoras interconectadas por medio de canales de comunicación de alta velocidad. Utilizadas por organizaciones muy grandes.

RESUMEN

El trabajo presente está compuesto por 4 capítulos, en el primer capítulo se describe el diseño de la investigación, aunque no es científica este trabajo es mas bien de aplicación, se especificó el problema, la justificación y alcance del trabajo, había necesidad de comunicar la UCSG y la unidad educativa Freire Stabille de Playas, se definen los objetivos específicos que llevan a conocer la conceptualización de las VPN´s.

El capítulo dos, trata el marco teórico de las VPN´s, se estudia a las redes privadas virtuales, sus tipos, sus componentes, el proceso de tunelización para el posterior encriptado de la información, esto último es un proceso fundamental para la ejecución o implementación de una VPN.

Se describe las seguridades que deben poseer las VPN´s, se estudian a los protocolos de seguridad y se considera al software Debian versión 6 que es, de los llamados software libre, este es un programa para servidores bajo Linux. El programa para la VPN entre la UCSG y la unidad educativa Freire Stabille es OpenVPN.

El capítulo 3 se describe una breve reseña historia de la institución además de la situación actual de la UEF donde se va a llevar a cabo la implementación del proyecto, se describe

las necesidades tecnológicas así como también la arquitectura y topología de la Red LAN de la UEF existente.

El capítulo 4 es la parte que propone la implementación de la red VPN, con ello se podrán comunicar de manera directa y virtual la unidad educativa Freirestabile, accediendo de esta forma a la información administrativa, financiera entre otros datos mas que genera el portal de la UCSG, que es conocida como el sistema integrado único (SIU).

ABSTRACT

The graduation work is the proposal to implement a Virtual Private Network between UCSG and Freire Stabille educational unit, located in Canton Playas, province of Guayas. The first chapter introduces the problem statement, justification, and proposed specific objectives. In chapter two, is the theoretical framework of the VPN's, we study virtual private networks, their types, their components, the tunneling process for the subsequent encryption of information, the latter is a fundamental process for implementing or implementing a VPN.

Assurances described must have the VPN's, studying security protocols and is considered the Debian software is version 6, so-called free software; this is a program for Linux servers. The program for the VPN between the UCSG and Freire Stabille educational unit is OpenVPN.

Chapter 3 is the part that proposes the implementation of the VPN, they can communicate it directly and virtual with Freire Stabille educational unit, thus access to administrative information, financial and other data generated by the portal over the UCSG, which is known as the single integrated system (SIU).

CAPITULO I

DISEÑO DEL PROYECTO

1.1 Introducción:

Desde el principio de los tiempos, la humanidad ha tenido la necesidad de comunicarse. Paralelamente también ha existido la necesidad de hacerlo de manera privada, es decir que el mensaje solo le llegue a determinados receptores.

En las redes de comunicaciones pasa exactamente lo mismo, en especial el sector corporativo siempre ha requerido la implementación de enlaces privados para transportar de forma segura toda su información confidencial. En el cantón Playas de la provincia del Guayas se halla situada la Unidad Educativa Freirestabile “UEF” con quien se desea diseñar e implementar bajo servidores linux un enlace virtual o una Red Privada Virtual “VPN” con el objetivo de poder tener una conexión segura para la transmisión de datos, actualmente en la unidad educativa laboran funcionarios de la Universidad Católica de Santiago de Guayaquil”UCSG”. El marco teórico se orienta al estudio de las diferentes tecnologías de las VPN que los soportan desde plataforma Windows y bajo Linux, y además el software OpenVPN que es un enlace punto-a-punto, el cual nos permite manejar niveles muy altos de confidencialidad, seguridad y escalabilidad en dicha transmisión de paquetes.

En la implementación el alcance de este proyecto es establecer una conexión directa entre Unidad Educativa con el Sistema Integral Universitario “S.I.U”, este sistema se basa en integrar la información que se genera en la parte académica y administrativa de la UCSG, utilizándola para tomar decisiones de una manera oportuna y eficaz.

1.2 Antecedentes:

La Unidad Educativa Freirestabile es una institución académica perteneciente a la Universidad Católica de Santiago de Guayaquil, está ubicada en la calle Merced y callejón s/n barrio la planta del cantón General Villamil-Playas.

El personal de la UEF de las áreas administrativas, financieras y académicas actualmente no pueden acceder al SIU desde las oficinas de dicho establecimiento y está obligado a viajar desde Playas de Villamil hacia Guayaquil, donde está ubicado el centro de cómputo de la “UCSG” para tener acceso al SIU y de esta manera poder realizar sus labores pertinentes.

El colegio mantiene un servicio de internet permanente con un ancho de banda de 1Mbps con la empresa TELCONET. Consta de un servidor el cual está conectado a una LAN interna de la UEF.

Tanto el software como el hardware del servidor están desactualizados por lo que para la implementación del proyecto es necesario reemplazarlo por un servidor nuevo.

1.3 Planteamiento del problema:

El motivo que llevo a realizar la presente tesis de grado es la dificultad que poseen los funcionarios de la UEF en acceder al SIU de la UCSG, desde en el cantón de General Villamil-Playas.

El problema afecta las áreas administrativas, académicas y financieras de la Unidad Educativa ya que el personal respectivo no tiene acceso directo al S.I.U donde está integrada la información que genera la UCSG.

El personal de las áreas antes mencionadas de la UEF, está obligado a viajar hacia Guayaquil para poder realizar sus labores apropiadas.

Hay que tener presente que el personal que tiene que viajar queda expuesto a tener retrasos en sus labores cotidianas dentro de la UEF, así como también infortunios como robos e inclusive accidentes de tránsito.

1.4 Justificación:

Actualmente las organizaciones e instituciones desean obtener sistemáticamente ventajas comparativas que le permitan alcanzar, sostener y mejorar una determinada posición en el entorno socioeconómico.

La implementación de una VPN basada en software entre la UCSG y la UEF es de suma importancia y relevancia para estas dos instituciones educativas ya que permitirá al personal de las áreas administrativas, académicas y financieras de la Unidad Educativa tener acceso directo al SIU mediante conexión en línea desde sus oficinas sin tener que dirigirse hacia la ciudad de Guayaquil para ingresar la información en la base de datos del sistema.

Tenemos que tener en cuenta que la información con que viaja el personal de la unidad educativa es de suma importancia y por ende no debe seguir siendo expuesta a problemas de seguridad.

1.5 Alcance:

El presente proyecto está estudiado, diseñado y desarrollado para establecer una conexión virtual, económica de forma segura entre la UCSG y la UEF, utilizando el internet como medio de comunicación y servidores VPN con el

software OpenVPN, con la cual se podrá acceder a múltiples servicios que facilitaran la comunicación en línea.

Con la VPN se brindará servicios en línea con acceso directo a nuestras bases de datos SIU, y sobre todo el portal permitirá integrar las distintas soluciones tanto administrativas y financieras de forma segura al estar operativa la VPN.

1.6 Objetivos:

1.6.1 Objetivo General:

Diseñar e implementar una Red Privada Virtual entre la Universidad Católica de Santiago de Guayaquil y la Unidad Educativa FreireStabille del cantón Playas, provincia del Guayas.

1.6.2 Objetivos Específicos:

a. Estudiar y comparar las formas y tipos de VPN
b. Conocer las distribuciones de software con y sin licencia para implementar redes virtuales privadas.
c. Diseñar la Red Virtual Privada (VPN) bajo software libre
d. Implementar una red privada virtual entre la Unidad Educativa FreireStabille y la UCSG para acceder en línea al SIU desde sus oficinas en Playas.

1.7 Hipótesis:

Por medio de la implementación de la VPN, se podrá tener intercomunicadas a las dos instituciones educativas, esto permitirá ampliar sus objetivos estratégicos y sus metas de calidad, con una gestión eficaz, eficiente y dinámica, que contribuya a la adaptación e innovación educativa que incluye: sistemas de información, base de datos (repositorio de información) y un conjunto actualizado de herramientas y equipos informáticos de comunicaciones; que ofrezcan seguridad, confiabilidad y escalabilidad. Los cuales son la base fundamental para el éxito del proyecto y las necesidades de la Unidad educativa y la Universidad.

1.8 Metodología de la Investigación:

Se comenzará haciendo una introducción al desarrollo del tema, y se describirá en forma detallada las especificaciones necesarias que se han considerado en el desarrollo del proyecto. Es más bien una metodología documental, y por ello es un trabajo de titulación aplicada, que es la que se apoya en la solución de problemas específicos para mejor la calidad de vida de las sociedades.

Será adjuntada una pequeña reseña histórica sobre las redes privadas virtuales, y sus tipos de conexión. A demás se incluirá una investigación ampliada sobre las seguridades y protocolos necesarios para tener una VPN segura.

Diseño de la VPN con la propuesta de todo el equipamiento que se necesite cambiar o anexar al ya existente, más los servidores que se utilizaran.

Implementación de la Red Virtual Privada (VPN) basado en la aplicación de servidores con Debian versión 6 utilizando el software OpenVPN.

Se presentaran las conclusiones y recomendaciones finales necesarias obtenidas a la finalización del proyecto.

Finalmente se adjuntarán algunos anexos que contendrán la configuración y los comandos del software liado al proyecto de tesis.

No es un trabajo de orden científico, no se utilizará la experimentación, es decir no habrá grupos de control equivalente y no equivalente, no se procederá a validar el método, se limita a resultado de aplicar software libre para solucionar una necesidad de acceso directo al SIU por parte de la unidad educativa Freire Stabile de Playas.

CAPITULO II

FUNDAMENTOS DE REDES PRIVADAS VIRTUALES

2.1 Introducción:

Una VPN o red privada virtual es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo internet.

Internet es una red de acceso público en todo el mundo, debido a que utiliza IP (Protocolo de internet) su masificación, se ha convertido en una manera atractiva de interconectar sitios remotos. Sin embargo, el hecho de que sea una infraestructura pública conlleva riesgos de seguridad para las empresas y sus redes internas. Favorablemente, la tecnología VPN permite que las organizaciones creen redes privadas en la infraestructura de Internet pública que mantienen la confidencialidad y la seguridad.

2.2 Conceptualización de una VPN:

Es un servicio que ofrece conectividad segura y fiable sobre una infraestructura de la red pública compartida, como internet (Mason, 2002).

Una VPN es un tipo de red que permite utilizar una red WAN[1] como si fuera una red local LAN[2], es decir, se puede considerar una red que está físicamente extendida en una región, como si todas las computadoras integrantes se encontraran en una red local.

El objetivo de crear una VPN es que toda la red pública sea vista desde dentro de la red privada como una conexión lógica que une las dos o más subredes que pertenecen a la red privada.

Con una red privada virtual pueden enviarse datos entre dos computadoras a través de redes públicas o compartidas de forma que simula las propiedades de un enlace punto a punto privado.

Las organizaciones usan las redes privadas virtuales para proporcionar una infraestructura WAN virtual que conecta sucursales, oficinas domésticas, oficinas de socios comerciales y trabajadores a distancia a toda la red corporativa o a parte de ella. Para que permanezca privado, el tráfico está encriptado, en vez de usar una conexión de Capa 2 (modelo OSI) exclusiva, como una línea dedicada punto a punto, la VPN usa conexiones virtuales que se enrutan a través de internet.

---

[1] *Wide Área Network*, Red de área metropolitana

[2] *Local Área Network*, Red de área local.

Dentro de una VPN cada miembro remoto de la red puede comunicarse de manera segura y confiable a través de internet como medio para conectarse a la LAN privada. La VPN puede desarrollarse para alojar más usuarios y ubicaciones diferentes de manera mucho más fácil que una línea dedicada.

Como se mencionó, la escalabilidad es una ventaja principal que tienen las VPN sobre las líneas dedicadas comunes. A diferencia de éstas, donde aumenta el costo en proporción a las distancias en cuestión, las ubicaciones geográficas de cada oficina tienen poca importancia en la implementación de una red privada virtual. Ver figura 2.1.

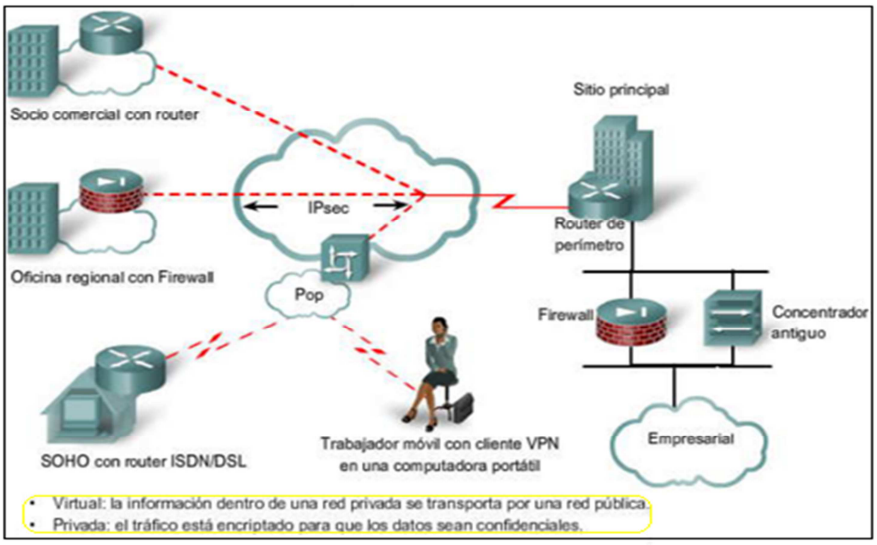


Figura 2.1 Infraestructura general de una red privada virtual

Las organizaciones que usan las VPN se benefician con el aumento en la flexibilidad y la productividad, los sitios remotos y los trabajadores a distancia pueden conectarse de manera segura a la red corporativa desde casi cualquier lugar. Los datos de la VPN están encriptados y ninguna persona que no esté autorizada puede descifrarlos.

Las redes privadas virtuales transfieren a las computadoras o hosts remotos dentro del firewall[3] y les brindan casi los mismos niveles de acceso a los dispositivos de red como si estuvieran en una oficina corporativa.

El firewall puede ser implementado en hardware o software, o una combinación de ambos, estos se utilizan con frecuencia para evitar que los usuarios de internet no autorizados tengan acceso a redes privadas conectadas a internet, todos los mensajes que entren o salgan de la intranet pasan a través del cortafuego, que examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados, véase un esquema de un firewall o cortafuegos en la figura 2.2.

[3] Llamado también “Cortafuegos” es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas

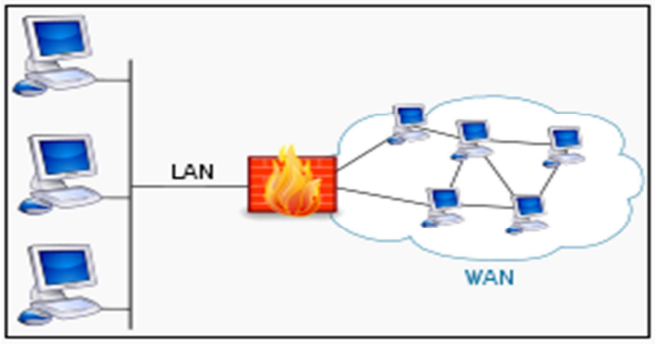


Figura 2.2 Esquema de red que utiliza firewall o cortafuego

Un firewall es un sistema encargado de separar un entorno seguro de uno inseguro. Resumiendo su trabajo se separa en tres tareas principales:

1. Analizar la información que entra o sale de la organización.

2. Decidir, según unas reglas que nosotros establecemos, si dicha información se elimina, se retiene o si se permite el paso.

3. Informar de lo sucedido, ya sea rellenando un registro, enviando un email o activando una alarma.

2.2.1 Beneficios de las VPN

Si se los compara con la opción de líneas dedicadas, las ventajas de la VPN, son ahorro en costos, más seguridad y mayor escalabilidad, se puede analizar la figura 2.3.

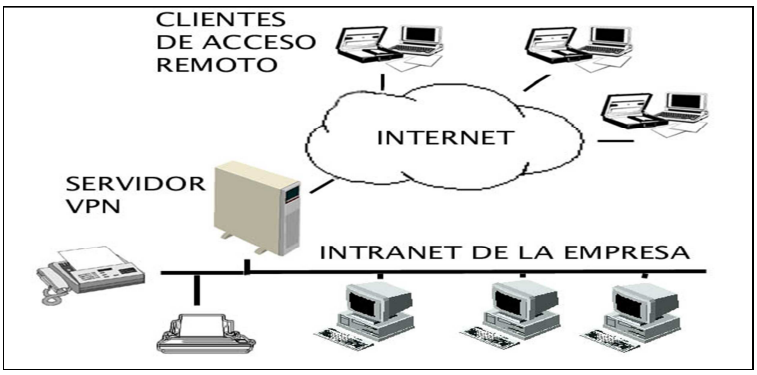


Figura 2.3 Beneficios de la VPN

Para poder realizar una VPN se necesita un servidor (o host) que espera conexiones entrantes, y uno o varios clientes, que se conectan al servidor para formar la red privada.

Una VPN permite establecer conexiones seguras entre otros equipos y acceder a los recursos del otro equipo de forma segura y confidencial, como impresoras, documentos, servidores de base de datos, aplicaciones específicas, etc.

Aparte realiza las siguientes opciones:

Extiende la conectividad geográfica: Una red privada virtual conecta a usuarios remotos a los recursos centrales.

Seguridad Mejorada: Reduce riesgos externos como la falsedad de IP, la pérdida de confidencialidad y la inyección de paquetes en procesos, como por ejemplo, en la transferencia de información.

Crecimiento en productividad de usuarios: Una solución de VPN permite a los usuarios remotos aumentar su productividad haciendo que el tiempo se aproveche al máximo.

Consolidación de recursos escasos: El hecho de tener varias oficinas significa contar con recursos dispersos. Una VPN es un método fácil para consolidar dichos recursos, lo que, en un momento, puede reducir el costo total de propiedad.

Transparencia para los usuarios: Los usuarios no necesitan saber más que una dirección IP asignada por el administrador de la red para poder usar la VPN

Costo reducido: Como las VPN se implementan usando una simple conexión a internet, eliminando la necesidad de líneas dedicadas, de software adicional y de infraestructura de marcación interna.

Mayor seguridad en la conexión: En una conexión de banda ancha a internet existe vulnerabilidad por ataques externos, muchas soluciones de VPN incluyen medidas de seguridad adicional, tales como dispositivos de seguridad

("firewall") y antivirus de chequeo para contrarrestar los diferentes tipos de amenazas a la seguridad de la red.

2.2.2 Desventajas de la VPN

Entre los inconvenientes o desventajas se pueden citar:

Mayor carga en el cliente VPN: Puesto que debe realizar la tarea adicional de encapsular los paquetes de datos una vez más, situación que se agrava cuando además se realiza encriptación de los datos que produce una menor velocidad en la mayoría de las conexiones, sin embargo con procesadores rápidos este problema se puede resolver.

La implementación puede consumir mucho tiempo: La planificación de la configuración, la administración de las claves y la solución de problemas puede convertir fácilmente lo que a simple vista es sencillo en semanas de trabajo.

Disponibilidad de Internet: Aún con todas las ventajas de la VPN, una cosa que no se puede asegurar es la alta disponibilidad. Como las VPN usan internet para el transporte, un servicio VPN puede interrumpirse a veces durante caídas de internet (Kolesnikov & Hatch, 2002)

2.3 Componentes de una VPN

Incluye los siguientes componentes: Conexión VPN, Servidor VPN, Cliente VPN, Túnel y Red de tránsito (infraestructura de internet) como se muestra en la figura 2.4.

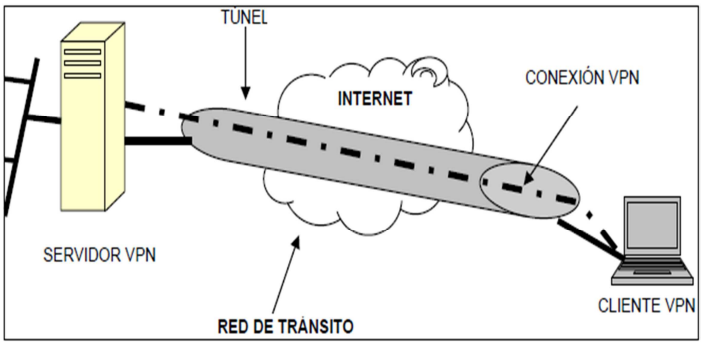


Figura 2.4 Componentes de una red privada virtual

a) Conexión VPN

Es la parte en la cual los datos son encriptados. Para conexiones VPN seguras, los datos son encriptados y encapsulados en la misma sección de la conexión.

Existen dos tipos de conexiones VPN, las cuales son: la conexión VPN de acceso remoto y la conexión VPN de enrutador a enrutador.

b) Conexión de acceso remoto:

Una conexión VPN de acceso remoto la hace un cliente remoto, una computadora personal se conecta con una red privada, el servidor VPN proporciona acceso a los recursos del servidor VPN o a la red completa. Los paquetes enviados desde el cliente remoto a través de la conexión VPN se originan en la computadora cliente de acceso remoto.

El cliente de acceso remoto (el cliente VPN) se autentifica a sí mismo ante el servidor de acceso remoto (el servidor VPN) y para autentificación mutua, el servidor se autentifica a sí mismo ante el cliente.

c) Conexión de enrutador a enrutador:

Una conexión VPN de enrutador a enrutador se lleva a cabo por un dispositivo electrónico llamado ruteador que conecta dos porciones de una red privada. El servidor VPN proporciona una conexión enrutada a la red a la cual el servidor VPN está conectado. En una conexión VPN de enrutador a enrutador, los paquetes enviados desde cualquier enrutador a través de la conexión VPN generalmente no se origina en los ruteadores.

El enrutador que llama (el cliente VPN) se autentifica a sí mismo ante el enrutador que responde (el servidor VPN), y para autentificación mutua, el enrutador que responde se autentifica a sí mismo ante el enrutador que llama.

d) Servidor VPN

Es una computadora que acepta conexiones VPN de clientes VPN la cual debe estar configurada con el software necesario para realizar el túnel, la encriptación, etc. Un servidor VPN puede proporcionar una conexión de acceso remoto VPN o una conexión de enrutador a enrutador.

e) Cliente VPN

Es una computadora que inicia una conexión VPN con un servidor VPN, un cliente VPN o un enrutador tiene una conexión de enrutador a enrutador. La computadora debe estar correctamente configurada para tener comunicación con el servidor VPN.

f) Red de tránsito (infraestructura de internet)

Es la red pública o compartida que es cruzada por los datos encapsulados. La red de tránsito puede ser internet o una intranet IP privada.

g) Datos del túnel

Son los datos enviados a través de un enlace punto a punto

h) Túnel

Los túneles son métodos utilizados para la transferencia de los datos desde una red a otra, los datos que se transfieren se dividen en paquetes. Un protocolo de túnel encapsula cada paquete con una cabecera, que proporciona información de enrutamiento y permite al paquete viajar a través de la red, cuando los paquetes encapsulados llegan a su destino o extremo del túnel, la información se desencapsula y se envía a su destino final.

Todo el proceso de encapsulado, enrutamiento y desencapsulado se denomina túnel (Sanchez, 2002).

Ciertos autores llaman tunneling, en español tunelización a la conceptualización anterior, para realizar el encapsulamiento, enrutamiento y desencapsulamiento existen los protocolos adecuados. La academia Cisco (*Cisco Systems Networking Academy Series*), brinda información fundamental sobre las VPN y es la referencia esencial de este trabajo.

Los protocolos de tunneling[4] criptográficos son para brindar protección contra detectores de paquetes, autenticación de emisores e integración de mensajes. El protocolo del paquete que hace de envoltorio solo es entendido por el emisor y por el receptor, en concreto, por el gateway que lo envía y por el gateway que lo recibe.

Para los usuarios que utilizan esos routers el proceso es transparente ya que el empaquetamiento y el des-empaquetamiento se realiza en el gateway y no, normalmente en el computador.

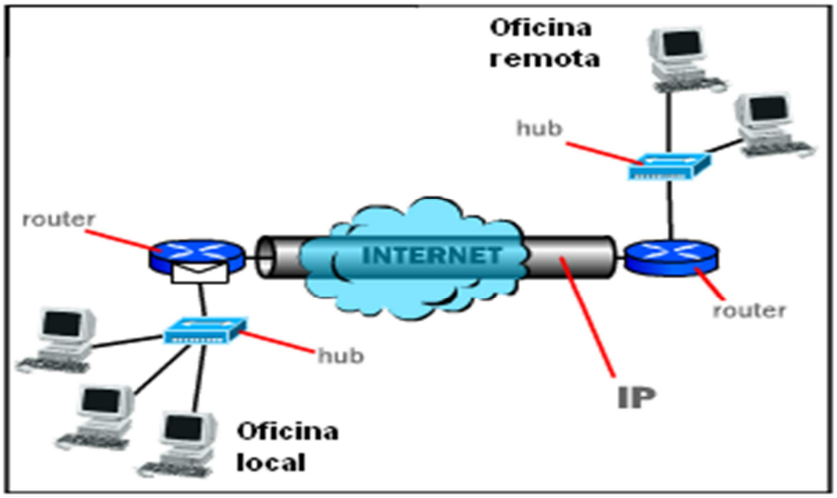


Figura 2.5 Tunelización esquema envió de paquetes encriptados

[4] Es el proceso de colocación de cada paquete de información que se envía dentro de otro paquete que hace de "envoltorio".

2.4 Tipos de VPN

Se distinguen dos tipos de redes privadas virtuales, de sitio a sitio y de acceso remoto (Amato, 2000).

2.4.1 VPN sitio a sitio.- Las organizaciones usan las redes privadas virtuales de sitio a sitio para conectar ubicaciones remotas, tal como se usa una línea dedicada o conexión Frame Relay[5]. Hoy la mayoría de las organizaciones, tiene acceso a internet, es lógico aprovechar los beneficios de VPN de sitio a sitio.

[5] Consiste en una forma simplificada de tecnología de conmutación de paquetes que transmite una variedad de tamaños de tramas o marcos ("*frames*") para datos, perfecto para la transmisión de grandes cantidades de dato

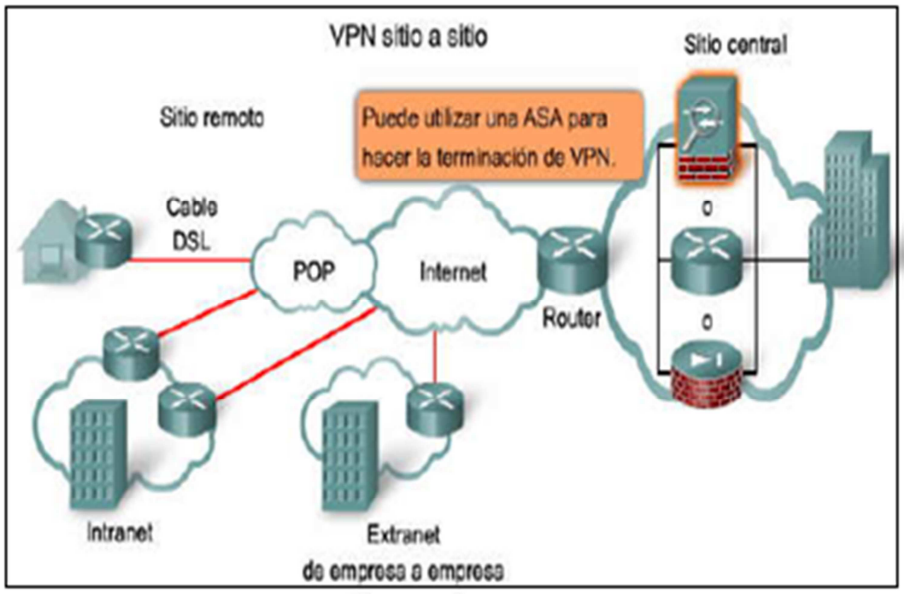


Fig. 2.6 VPN Sitio a Sitio usando ASA

La VPN de sitio a sitio es una extensión de una networking WAN clásica, las VPN de sitio a sitio conectan redes enteras entre ellas. Por ejemplo, pueden conectar la red de una sucursal a la red de la sede central corporativa.

En una VPN de sitio a sitio, los hosts envían y reciben tráfico TCP/IP a través de un gateway VPN, el cual podría ser un router, una aplicación firewall PIX[6] o una aplicación de seguridad adaptable (ASA[7]).

[6] *Private Internet Exchange*, es un modelo de equipos cortafuegos de Cisco, es un firewall completamente hardware: a diferencia de otros sistemas cortafuegos, PIX no se ejecuta en una máquina Unix, sino que incluye un sistema operativo empotrado denominado Finesse, que desde espacio de usuario se asemeja más a un router que a un sistema Unix clásico.

2.4.1.1 Funcionamiento de asa

La filosofía de funcionamiento del Adaptive Security Algorithm, se basa en estas reglas:

Ningún paquete puede atravesar el corta fuegos sin tener conexión y estado.

Cualquier conexión cuyo origen tiene un nivel de seguridad mayor que el destino (outbound[8]) es permitida si no se prohíbe explícitamente mediante listas de acceso.

Cualquier conexión que tiene como origen una interfaz o red de menor seguridad que su destino (inbound[9]) es denegada, si no se permite explícitamente mediante listas de acceso.

Los paquetes ICMP[10] son detenidos a no ser que se habilite su tráfico explícitamente.

---

[7] *Adaptive Security Algorithm.,* El cortafuegos PIX utiliza un algoritmo de protección ASA.

[8] En la operación de un call center se define como la actividad de realización de llamadas de salida

[9] En la operación de un call center se define como la actividad de atención de llamadas recibidas

[10] *Internet Control Message Protocol*, es el sub protocolo de control y notificación de errores del Protocolo de Internet (IP).

Cualquier intento de violación de las reglas anteriores es detenido, y un mensaje de alerta es enviado a syslog[11].

Cuando a una interfaz del cortafuegos llega un paquete proveniente de una red con menor nivel de seguridad que su destino, el firewall le aplica el *Adaptive Security Algorithm* para verificar que se trata de una trama válida, y en caso de que lo sea comprobar si del host origen se ha establecido una conexión con anterioridad; si no había una conexión previa, el firewall PIX crea una nueva entrada en su tabla de estados en la que se incluyen los datos necesarios para identificar a la conexión.

El cortafuego PIX puede resultar muy complejo de gestionar, especialmente a los que provienen del Unix[12], ya que se asemeja más a un router que a un servidor. El gateway VPN es responsable de la encapsulación y encriptación del tráfico saliente para todo el tráfico desde un sitio particular y de su envío a través de un túnel VPN por internet a un gateway VPN par en el sitio objetivo.

[11] Estándar de facto para el envío de mensajes de registro en una red informática IP. Por syslog se conoce tanto al protocolo de red como a la aplicación o biblioteca que envía los mensajes de registro.

[12] Sistema operativo portable, multitarea y multiusuario, de característica abierta, compatible con distintos tipos de hardware; posee algunos comandos similares al DOS.

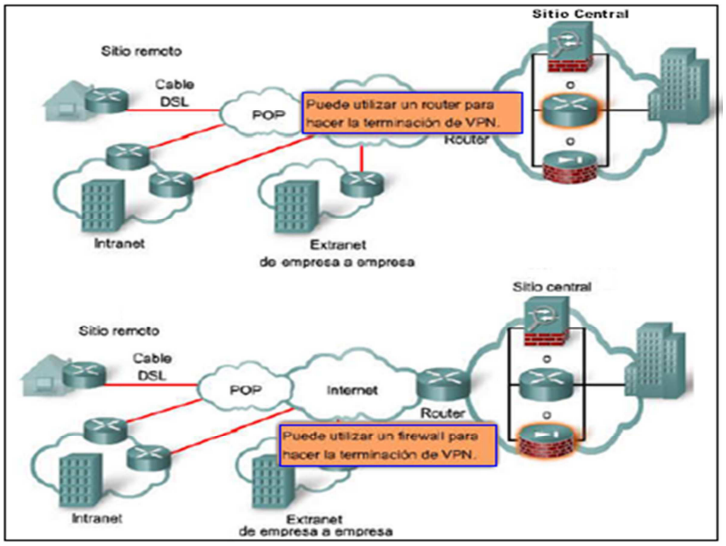


Fig. 2.7 VPN Sitio a Sitio con terminación *router y firewall*

Al recibirlo, el gateway VPN par elimina los encabezados, descifra el contenido y retransmite el paquete hacia el host objetivo dentro de su red privada. Como se aprecia en la figura 2.7 la terminación de una red privada virtual, puede ser mediante router y firewall.

2.4.2 VPN de acceso remoto Permiten a un usuario conectado a internet desde algún punto remoto acceder a una red corporativa y sus servicios asociados. Ver la figura 2.8 un ejemplo de VPN de acceso remoto.

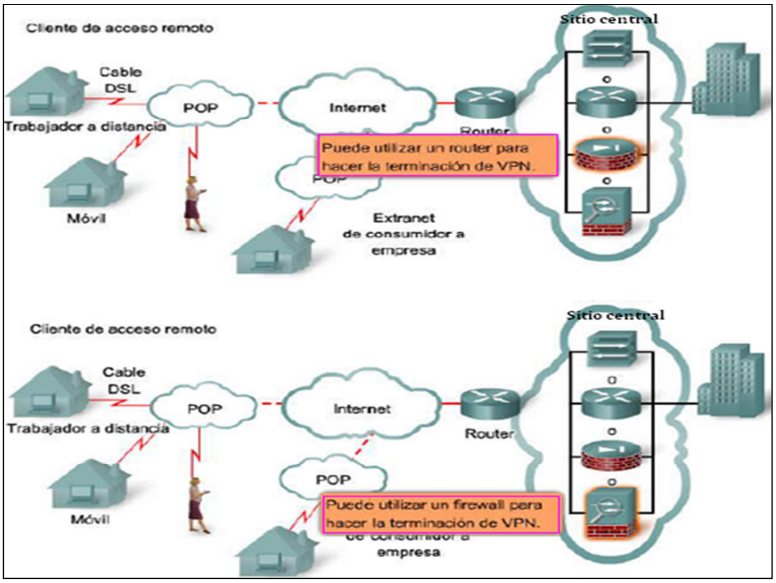


Fig. 2.8 Concepción de VPN con Acceso Remoto

Empleados que realizan su actividad desde su propia casa, pero necesitan acceso a la red de su empresa, y con su propia conexión a internet establecen una red privada virtual que les permite trabajar como si estuviesen físicamente dentro de la red privada.

Entonces usuarios móviles y trabajadores a distancia usan considerablemente las VPN de acceso remoto. En el pasado, las empresas admitían usuarios remotos con

redes dial-up[13], esto implicaba una llamada de larga distancia y los costos correspondientes para lograr el acceso a la empresa.

La mayoría de los trabajadores a distancia ahora tienen acceso a internet desde sus hogares y pueden establecer VPN remotas por medio de las conexiones de banda ancha. De manera similar, un trabajador móvil puede realizar una llamada local a un ISP[14] local para lograr el acceso a la empresa a través de internet.

De hecho, esto marca un avance de evolución en las redes dial-up. Las VPN de acceso remoto pueden admitir las necesidades de los trabajadores a distancia, los usuarios móviles, además de las extranets de consumidores a empresas. Ver figura 2.9.En una VPN de acceso remoto, cada host en general tiene software cliente de VPN.

[13] Conexión por línea conmutada, es una forma barata de acceso a internet en la que el cliente utiliza un módem para llamar a través de la Red Telefónica Conmutada al nodo del ISP.

[14] *Internet Service Provider,* empresa que brinda conexión a Internet a sus clientes. Un ISP conecta a sus usuarios a Internet a través de diferentes tecnologías como DSL, Cable-módem, GSM, Dial-up, Wifi

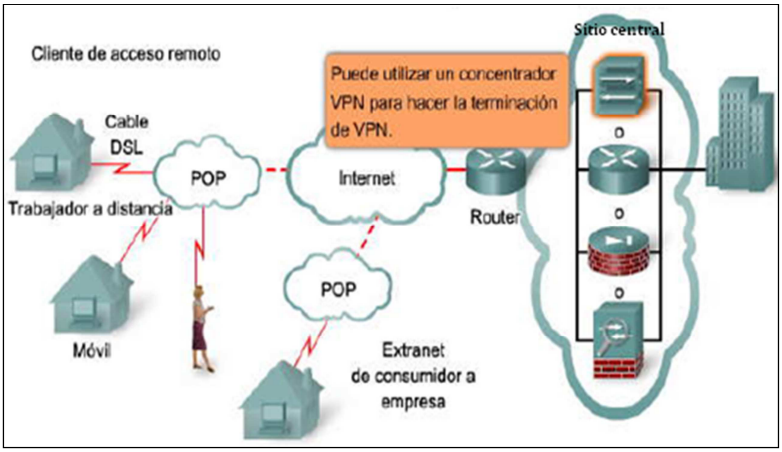


Fig. 2.9 VPN de Acceso Remoto

Cuando el host intenta enviar tráfico, el software cliente de VPN encapsula y encripta ese tráfico antes del envío a través de internet hacia el gateway VPN en el borde de la red objetivo. Al recibirlo, el gateway VPN maneja los datos de la misma manera en que lo haría con los datos de una VPN de sitio a sitio.

2.4.2.1 Características de VPN segura

Las VPN utilizan técnicas de encriptación avanzada y tunneling para permitir que las conexiones de red privadas de extremo a extremo que establezcan las organizaciones a través de Internet sean seguras.

Las bases de una VPN segura son la confidencialidad, la integridad de datos y la autenticación, se conceptualiza los aspectos siguientes:

Confidencialidad de datos: una cuestión de seguridad que suele despertar preocupación es la protección de datos contra personas que puedan ver o escuchar subrepticiamente información confidencial. La confidencialidad de datos, que es una función de diseño, tiene el objetivo de proteger los contenidos de los mensajes contra la intercepción de fuentes no autenticadas o no autorizadas. Las VPN logran esta confidencialidad mediante mecanismos de encapsulación y encriptación.

Integridad de datos: los receptores no tienen control sobre la ruta por la que han viajado los datos y, por lo tanto, no saben si alguien ha visto o ha manejado los datos mientras viajaban por internet. Siempre existe la posibilidad de que los datos hayan sido modificados. La integridad de datos garantiza que no se realicen cambios indebidos ni alteraciones en los datos mientras viajan desde el origen al destino, generalmente, las VPN utilizan hashes para garantizar la integridad de los datos. El hash[15] es como una checksum o un sello (pero más robusto) que garantiza que nadie haya leído el contenido.

Autenticación: la autenticación garantiza que el mensaje provenga de un origen auténtico y se dirija a un destino auténtico. La identificación de usuarios

[15] Se refiere a una función o método para generar claves o llaves que representen de manera casi unívoca a un documento, registro, archivo, etc.

brinda al usuario la seguridad de que la persona con quien se comunica es quien cree que es. Las VPN pueden utilizar contraseñas, certificados digitales, tarjetas inteligentes y biométricas para establecer la identidad de las partes ubicadas en el otro extremo de la red.

2.5 Tunneling VPN

La incorporación de capacidades de confidencialidad de datos adecuadas en una VPN garantiza que sólo los orígenes y los destinos indicados sean capaces de interpretar los contenidos del mensaje original.

El tunneling permite el uso de redes públicas como internet para transportar datos para usuarios, siempre que los usuarios tengan acceso a una red privada. El tunneling encapsula un paquete entero dentro de otro paquete y envía por una red el nuevo paquete compuesto. La figura 2.10 contiene una lista de las tres clases de protocolos que utiliza el tunneling.

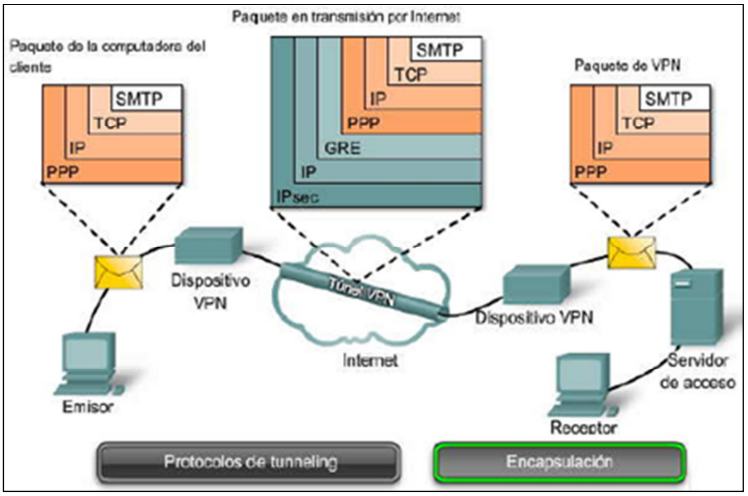


Figura 2.10 Paquetes de encapsulación

Para ilustrar el concepto de tunneling y las clases de protocolos de tunneling, veamos un ejemplo de un envío de una tarjeta por correo tradicional la tarjeta tiene un mensaje adentro. La tarjeta es el protocolo pasajero, el emisor coloca la tarjeta dentro de un sobre (protocolo de encapsulación) y escribe las direcciones correctas. Luego, deposita el sobre en el buzón de correo para que sea entregado.

El sistema postal (protocolo portador) busca y entrega el sobre en el buzón del receptor. Los dos extremos del sistema portador son las "interfaces del túnel", el receptor quita la tarjeta (extrae el protocolo pasajero) y lee el mensaje.

La figura 2.10, muestra un mensaje de correo electrónico que viaja por internet a través de una conexión VPN. PPP[16] transmite el mensaje al dispositivo VPN, donde el mensaje se encapsula dentro de un paquete de encapsulamiento de enrutamiento genérico (GRE)[17].

El GRE es un protocolo de tunneling desarrollado por Cisco Systems[18] que puede encapsular una amplia variedad de tipos de paquetes de protocolo dentro de túneles IP, lo que crea un enlace virtual punto a punto con los routers Cisco en puntos remotos, a través de una internetwork IP.

En la figura 2.10, el direccionamiento del paquete de origen y de destino externo se asigna a "interfaces del túnel" y se hace enrutable a través de la red, una vez que el paquete compuesto llega a la interfaz del túnel de destino, se extrae el paquete interno.

[16] *Point-to-Point Tunneling Protocol*, Protocolo de Tunelado Punto a Punto

[17] *Generic Routing Encapsulation,* es un protocolo para el establecimiento de túneles a través de Internet

[18] Empresa norteamericana, diseña y vende tecnología, ofrece servicios de red como routers (enrutadores), switches (conmutadores), hubs, cortafuegos, productos de telefonía IP, software de gestión de red como CiscoWorks, equipos para Redes de Área de Almacenamiento.

2.6 Integridad de los datos de la VPN

Como se usa internet es necesario poner mucha atención a las cuestiones de seguridad, por esta razón se consideran los esquemas de encriptación. Si por internet pública se transporta texto sin formato, puede ser interceptado y leído.

Para mantener la privacidad de los datos, es necesario encriptarlos, la encriptación VPN encripta los datos y los vuelve ilegibles para los receptores no autorizados. Para que la encriptación funcione, tanto el emisor como el receptor deben conocer las reglas que se utilizan para transformar el mensaje original en la versión codificada, las reglas de encriptación de la VPN incluyen un algoritmo y una clave.

Un algoritmo es una función matemática que combina mensaje, texto, dígitos o los tres con una clave, el resultado es una cadena de cifrado ilegible. El descifrado es extremadamente difícil o imposible sin la clave correcta.

El grado de seguridad que proporciona un algoritmo de encriptación depende de la longitud de la clave, para cualquier longitud de clave, el tiempo que lleva el procesamiento de todas las posibilidades de descifrar texto cifrado es una función de la potencia de cómputo del equipo, por lo tanto, cuanto más corta sea la clave, más fácil será romperla; pero, a su vez, más fácil pasar el mensaje. Ver ilustración de VPN con encriptación.

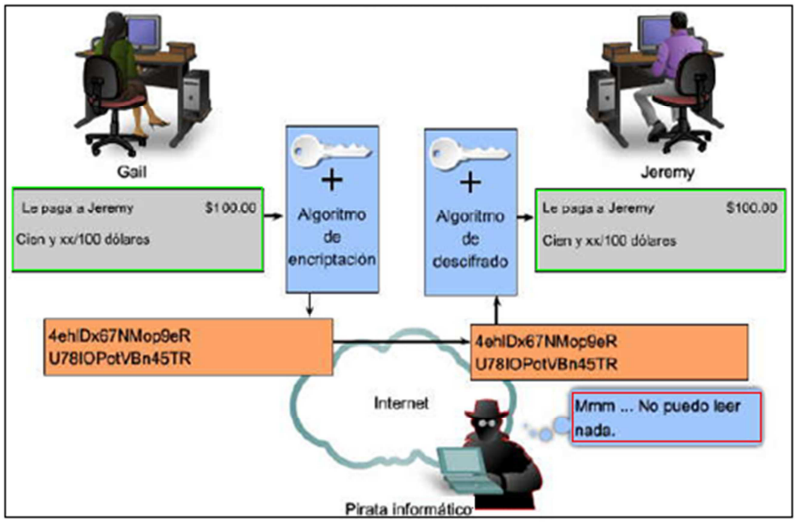


Figura 2. 11 Encriptación de la VPN

En el ejemplo de la figura 2.11, Gail desea enviar un documento de finanzas a Jeremy por internet. Gail y Jeremy han acordado previamente una clave secreta compartida. En el extremo de Gail, el software de cliente de la red privada virtual combina el documento con la clave secreta compartida y lo pasa por un algoritmo de encriptación, el resultado es un texto cifrado indescifrable. El texto cifrado se envía mediante un túnel de la VPN o por internet.

En el otro extremo, el mensaje se vuelve a combinar con la misma clave secreta compartida y se lo procesa con el mismo algoritmo de encriptación, el resultado es el documento de finanzas original, que ahora es legible para Jeremy.

Algunos de los algoritmos de encriptación más comunes y la longitud de claves que se utilizan son los siguientes:

Algoritmo Estándar de cifrado de datos (DES[19]).- Este algoritmo es desarrollado por IBM[20], utiliza una clave de 56 bits para garantizar una encriptación de alto rendimiento. El DES es un sistema de encriptación de clave simétrica. Las claves simétricas y asimétricas se explican más adelante.

Algoritmo Triple DES (3DES).- Una variante más reciente del DES que realiza la encriptación con una clave, descifra con otra clave y realiza la encriptación por última vez con otra clave también diferente, 3DES le proporciona mucha más fuerza al proceso de encriptación.

Estándar de encriptación avanzada (AES[21]).- El Instituto Nacional de Normas y Tecnología (NIST) adoptó el AES para reemplazar la encriptación DES en los dispositivos criptográficos, AES proporciona más seguridad que DES y es más eficaz en cuanto a su cálculo que 3DES. AES ofrece tres tipos de longitudes de clave: claves de 128, 192 y 256 bits.

---

[19] *Data Encryption Standard,* Algoritmo de Encriptación Estándar, desarrollado por IBM

[20]*International Business Machines*, fabrica y comercializa herramientas, programas y servicios relacionados con la informática

[21] *Advanced Encryption Standard*. Algoritmos de cifrado simétrico. Longitud de la clave 128, 192 ó 256 bits

Rivest, Shamir y Adleman (RSA).- Sistema de encriptación de clave asimétrica. Las claves utilizan una longitud de bits de 512, 768, 1024 o superior.

2.6.1 Encriptación simétrica

Los algoritmos de encriptación como DES y 3DES requieren que una clave secreta compartida realice la encriptación y el descifrado, los dos equipos deben conocer la clave para decodificar la información. Con la encriptación de clave simétrica, también llamada encriptación de clave secreta, cada equipo encripta la información antes de enviarla por la red al otro equipo. La encriptación de clave simétrica requiere el conocimiento de los equipos que se comunicarán para poder configurar la misma clave en cada uno.

Por ejemplo, un emisor crea un mensaje codificado en el cual cada letra se sustituye con la letra que se encuentra dos posiciones adelante en el alfabeto; "A" se convierte en "C" y "B" se convierte en "D" y así sucesivamente. En este caso, la palabra SECRETO se convierte en UGETGVQ.

El emisor le ha informado al receptor que la clave secreta es "saltear 2". Cuando el receptor recibe el mensaje UGETGVQ, su equipo decodifica el mensaje al calcular las dos letras anteriores a las del mensaje y llega al código SECRETO. Cualquier otra persona que vea el mensaje sólo verá el mensaje cifrado, que parece una frase sin sentido a menos que la persona conozca la clave secreta.

Se puede utilizar el correo electrónico, un mensajero o un correo de 24 horas para enviar las claves secretas compartidas a los administradores de los dispositivos. Otro método más fácil y más seguro es la encriptación asimétrica.

2.6.2 Encriptación asimétrica

La encriptación asimétrica utiliza diferentes claves para la encriptación y el descifrado. El conocimiento de una de las claves no es suficiente para que un pirata informático deduzca la segunda clave y decodifique la información. Una clave realiza la encriptación del mensaje y otra, el descifrado, no es posible realizar ambos con la misma clave. En la figura 2.12. Hay un esquema de encriptación VPN

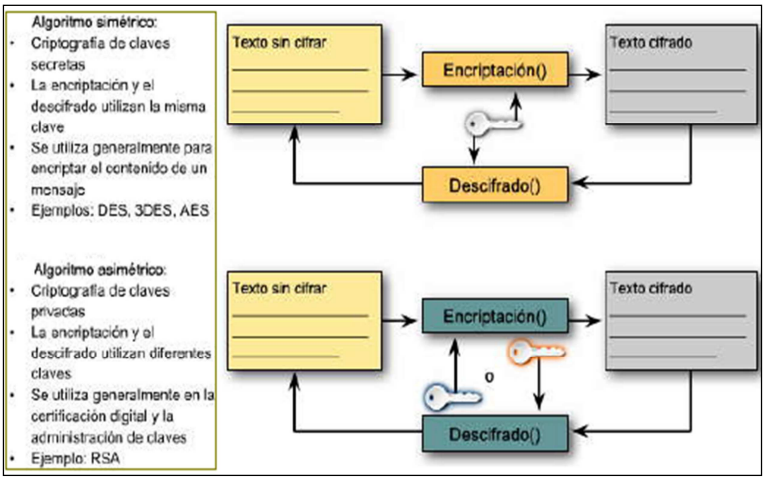


Figura 2.12 Algoritmos de Encriptación de las VPN

La encriptación de clave pública es una variante de la encriptación asimétrica que utiliza una combinación de una clave privada y una pública, el receptor le da una clave pública a cualquier emisor con quien desee comunicarse el receptor, el emisor utiliza una clave privada junto con la clave pública del receptor para encriptar el mensaje.

Además, el emisor debe compartir la clave pública con el receptor, para descifrar un mensaje, el receptor utiliza la clave pública del emisor y su propia clave privada.

Los hashes contribuyen a la autenticación y la integridad de los datos, ya que garantizan que personas no autorizadas no alteren los mensajes transmitidos. Un hash, también denominado message digest, es un número generado a partir de una cadena de texto. Véase la figura 2.13

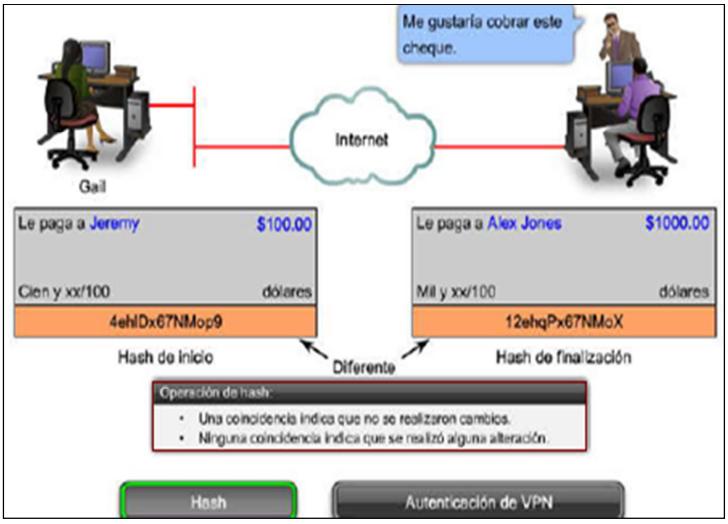


Figura 2. 13 Hashes para integridad de datos

El hash es menor que el texto, se genera mediante una fórmula, de forma tal que es extremadamente improbable que otro texto produzca el mismo valor de hash, el emisor original genera un hash del mensaje y lo envía junto con el mensaje mismo. El receptor descifra el mensaje y el hash, produce otro hash a partir del mensaje recibido y compara los dos hashes, si son iguales, puede estar seguro de que la integridad del mensaje no ha sido afectada.

En la figura 2.13, alguien está intentando enviarle a Jeremy un cheque por 100 dólares. En el extremo remoto, Alex Jones (un ladrón) está intentando cobrar el cheque en efectivo por 1000 dólares, el cheque fue alterado a medida que avanzaba mediante internet. Se cambiaron el receptor y el monto en dólares, en este caso, si se

hubiera utilizado el algoritmo de integridad de datos, los hashes no habrían coincidido y la transacción no habría tenido validez.

Los datos de la VPN se transportan por internet pública, tal como se mostró, hay posibilidades de que estos datos sean interceptados y modificados, como protección frente a esta amenaza, los hosts pueden agregarle un hash al mensaje, si el hash transmitido coincide con el recibido, significa que se ha preservado la integridad del mensaje. Sin embargo, si no coinciden, el mensaje ha sido alterado.

Las VPN utilizan un código de autenticación de mensajes para verificar la integridad y la autenticidad de un mensaje, sin utilizar mecanismos adicionales. Un código de autenticación de mensajes de hash (HMAC[22]) en clave es un algoritmo de integridad de datos que garantiza la integridad del mensaje.

El HMAC tiene dos parámetros: un mensaje de entrada y una clave secreta que sólo conocen el creador del mensaje y los receptores adecuados. El emisor del mensaje utiliza una función HMAC para producir un valor (el código de

[22] *Hash-based Message Authentication Code*, técnica de autenticación de mensajes que incluye una clave secreta. De esta forma se detecta la manipulación del contenido al tiempo que se chequea una clave de autenticación.

autenticación del mensaje) que se forma al condensar la clave secreta y el mensaje de entrada.

El código de autenticación del mensaje se envía junto con el mensaje, el receptor calcula el código de autenticación del mensaje en el mensaje recibido con la misma clave y la misma función HMAC que utilizó el emisor y compara los resultados calculados con el código de autenticación del mensaje. Si los dos valores coinciden, el mensaje se ha recibido correctamente y el receptor está seguro de que el emisor es un miembro de la comunidad de usuarios que comparten la clave.

La fuerza criptográfica de HMAC depende de la fuerza criptográfica de la función hash subyacente en cuanto al tamaño y a la calidad de la clave, y en el tamaño de la longitud del resultado de hash en bits.

Hay dos algoritmos HMAC comunes:

Message Digest 5 (MD5).- utiliza una clave secreta compartida de 128 bits. El mensaje de longitud variable y la clave secreta compartida de 128 bits se combinan y se ejecutan mediante el algoritmo de hash HMAC-MD5. El resultado es un hash de 128 bits. El hash se agrega al mensaje original y se envía al extremo remoto.

Algoritmo de hash seguro 1 (SHA-1).- Utiliza una clave secreta de 160 bits. El mensaje de longitud variable y la clave secreta compartida de 160 bits se combinan y se ejecutan mediante el algoritmo de hash HMAC-SHA-1. El resultado es un hash de 160 bits. El hash se agrega al mensaje original y se envía al extremo remoto.

Cuando se realizan negocios a larga distancia, es necesario saber quién está del otro lado del teléfono, correo electrónico o fax, lo mismo sucede con las redes VPN. Se debe autenticar el dispositivo ubicado en el otro extremo del túnel de la red privada virtual antes de que la ruta de comunicación se considere segura. En la figura 2.14 se muestra un esquema de seguridad en VPN. mediante autenticación.

Hay dos métodos pares de autenticación:

Clave compartida previamente (PSK[23]).- Una clave secreta compartida entre dos partes que utilizan un canal seguro antes de que deba ser utilizado, las PSK utilizan algoritmos criptográficos de clave simétrica. Una PSK se especifica en cada par manualmente y se utiliza para autenticar al par. En cada extremo, la PSK se combina con otra información para formar la clave de autenticación.

[23] *Pre-Shared Key*, clave de acceso de una longitud entre 8 y 63 caracteres, que es la clave compartida

Firma RSA.- Utiliza el intercambio de certificados digitales para autenticar los pares, el dispositivo local deriva un hash y lo encripta con su clave privada. El hash encriptado (firma digital) se adjunta al mensaje y se envía al extremo remoto, en el extremo remoto, el hash encriptado se descifra mediante la clave pública del extremo local. Si el hash descifrado coincide con el hash recalculado, la firma es verdadera.

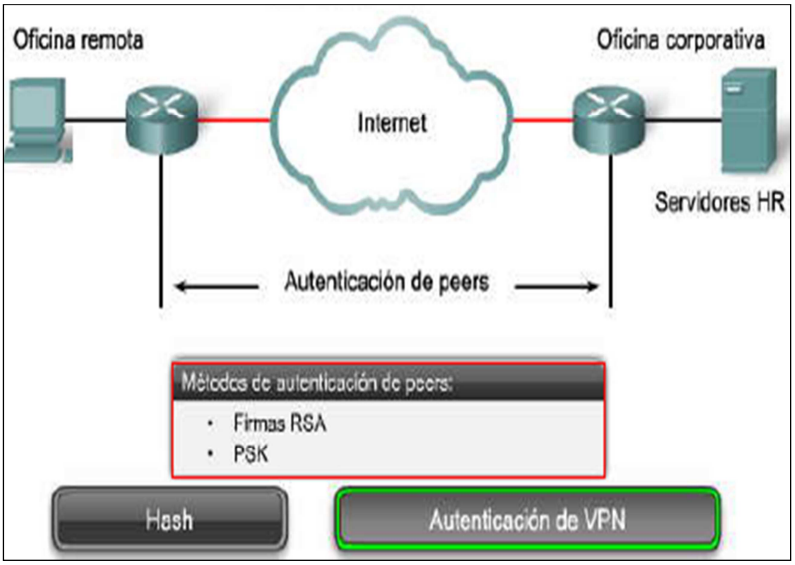


Figura 2.14 Seguridad de las VPN

2.7 Protocolo de seguridad IPSEC

El IPsec[24] es un conjunto de protocolos para la seguridad de las comunicaciones IP que proporciona encriptación, integridad y autenticación.

IPsec ingresa el mensaje necesario para proteger las comunicaciones VPN, pero se basa en algoritmos existentes.

Existen dos protocolos de estructura IPsec:

Encabezado de autenticación (AH).- Se utiliza cuando no se requiere o no se permite la confidencialidad, el encabezado de autenticación proporciona la autenticación y la integridad de datos para paquetes IP intercambiados entre dos sistemas. Verifica que cualquier mensaje intercambiado de R1 a R3 no haya sido modificado en el camino. También verifica que el origen de los datos sea R1 o R2. AH no proporciona la confidencialidad de datos (encriptación) de los paquetes. Si se lo utiliza solo, el protocolo AH proporciona poca protección, por lo tanto, se lo utiliza junto con el protocolo ESP para brindar las funciones de seguridad de la encriptación de los datos y el alerta contra alteraciones.

[24] Es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos.

Contenido de seguridad encapsulado (ESP): proporciona confidencialidad y autenticación mediante la encriptación del paquete IP, la encriptación del paquete IP oculta los datos y las identidades de origen y de destino. ESP autentica el paquete IP interno y el encabezado ESP.

La autenticación proporciona autenticación del origen de datos e integridad de datos. Aunque tanto la encriptación como la autenticación son opcionales en ESP, debe seleccionar una como mínimo.

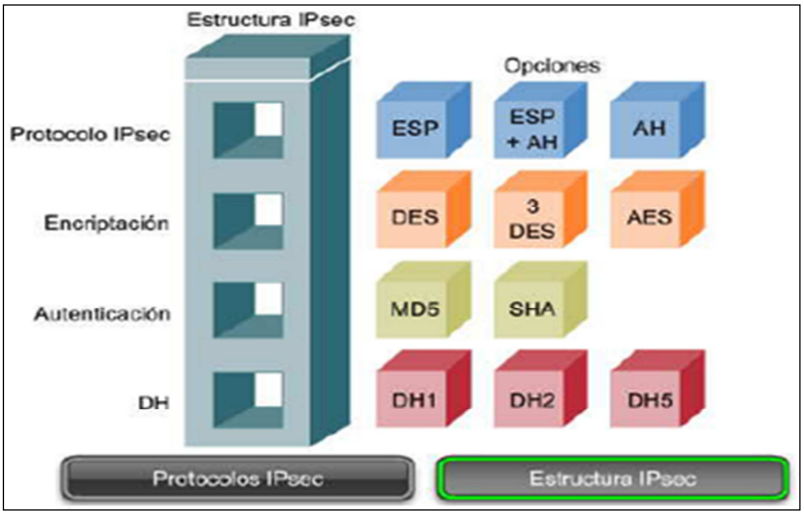


Figura 2.15 Estructura IPsec

IPsec se basa en algoritmos existentes para implementar la encriptación, la autenticación y el intercambio de claves.

Algunos de los algoritmos estándar que utiliza IPsec son:

DES.- Encripta y descifra los datos del paquete.

3DES.- Proporciona una fuerza de encriptación importante superior al DES de 56 bits.

AES.- Proporciona un rendimiento más rápido y una encriptación más fuerte según la longitud de la clave utilizada.

MD5.- Autentica datos de paquetes con una clave secreta compartida de 128 bits.

SHA-1.- Autentica datos de paquetes con una clave secreta compartida de 160 bits.

DH.- Permite que dos partes establezcan una clave secreta compartida mediante la encriptación y los algoritmos de hash, como DES y MD5, sobre un canal de comunicaciones no seguro.

La figura 2.16, muestra cómo se configura IPsec. IP seguridad proporciona la estructura y el administrador elige los algoritmos utilizados para implementar los servicios de seguridad dentro de esa estructura, existen cuatro apartados de estructura IPsec que deben completarse. Cuando configura un gateway de IPsec para proporcionar servicios de seguridad se puede realizar los siguientes pasos:

- Primero se elige un protocolo IPsec.

  Las opciones son ESP o ESP con AH.

- El segundo apartado es un algoritmo de encriptación si IPsec se implementa con ESP.

  Se selecciona el algoritmo de encriptación adecuado para el nivel de seguridad deseado: DES, 3DES o AES.

- El tercer apartado es la autenticación.

  Se selecciona un algoritmo de autenticación para proporcionar la integridad de los datos: MD5 o SHA.

- El último apartado es el grupo de algoritmos Diffie-Hellman (DH).

  Establece que los pares compartan la información de clave. Seleccione el grupo que desea utilizar: DH1 o DH2.

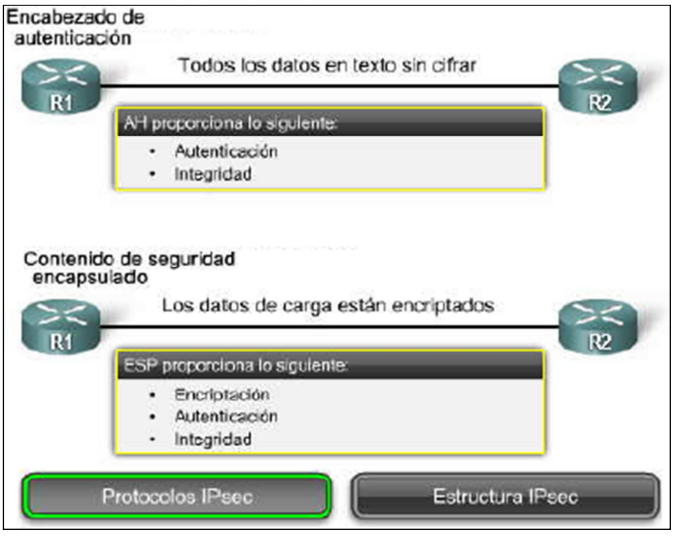


Figura 2.16 Protocolo de seguridad IPSec

En conclusión se pueden distinguir dos modos de funcionamiento de IPSec:

*Modo transporte: La encriptación se realiza extremo a extremo, es decir del host de origen al host de destino. Para la implantación de IPSec en modo transporte es necesario que todos los hosts de las redes origen y destino dispongan de una implementación de IPSec.

*Modo túnel: La encriptación se efectúa únicamente entre los routers de acceso a los hosts y la información viaja no encriptada en la parte de la red local.

Según (Pellejero, Andreu, & Lesta, 2006), el funcionamiento de IPSec en modo túnel permite integrar IPSec en una VPN ya que el mismo dispositivo que realiza el túnel VPN puede realizar las labores correspondientes al túnel IPSec. Ver cabeceras IPSec en la figura 2.17.

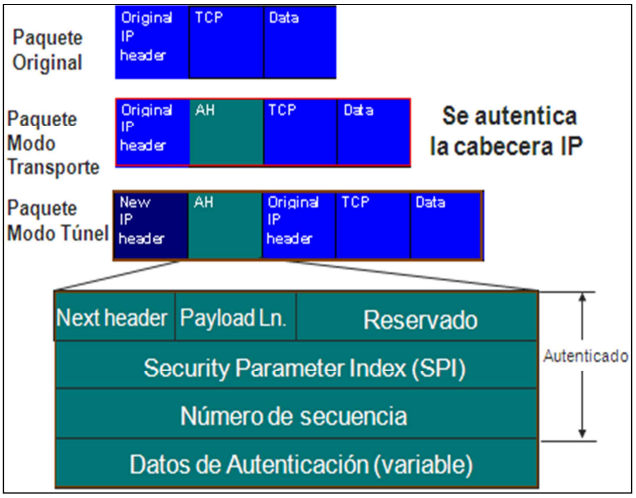


Figura 2.17 Cabeceras para IPSec tanto en modo túnel como modo transporte

El modo transporte es más fiable puesto que ofrece comunicación segura host a host. Sin embargo, el modo túnel tiene la ventaja de permitir incorporar la seguridad sin necesidad de incorporar IPSec en los hosts; aunque la seguridad que se obtiene en este caso no sea tan alta, la sencillez de implantación es mucho mayor y se consiguen la mayor parte de los beneficios ya que se protege la parte más expuesta del trayecto que es la infraestructura pública del operador.

En función de las circunstancias que rodeen cada caso se deberá optar por una u otra, incluso se pueden dar situaciones híbridas en las que determinado tipo de información baste protegerla con el modo túnel mientras que para algún host

concreto, que maneje información de mayor importancia, se deba utilizar el modo transporte.

Uno de los problemas que plantea la encriptación es el consumo intensivo de CPU que puede limitar el rendimiento de las comunicaciones. Esto suele ser un problema especialmente en los routers y servidores de túneles que atienden túneles IPSec con la función ESP activada ya que la función AH no requiere encriptación.

Para evitar este problema muchos servidores de túneles y routers permiten incorporar módulos que realizan los algoritmos de encriptación por hardware.

2.7.1 OSPF

Open Shortest Path First (OSPF), es un protocolo no propietario de routing de estado del enlace basado en un estándar abierto.

OSPF ha sido descrito en varios RFC´s, pero el estándar de OSPF v.2 está descrito en el RFC2328[25].

Los autores (Gil, Pomares, & Candelas, 2010), dicen que existen diferentes protocolos de encaminamiento abiertos, pero para redes de tamaño medio-grande el preferible es OSPF ya que, por ejemplo, no tiene el problema de la limitación de los

[25] *Request for Comments:* 2328. Especifica protocolos de normas para internet en especial la 2º versión del protocolo de enrutamiento de estado OSPF.

15 saltos de RIP[26], los tiempos de convergencia de OSPF son muchísimo mejores en todos los casos y, además, para el cálculo de costes y rutas óptimas tiene en cuenta factores tales como el ancho de banda lo que permite elegir un camino, supuestamente más lento pero con mayor ancho de banda.

Con OSPF no se entrega la tabla de rutas completa, sino el estado de los enlaces para que los routers procesen esta información y generen la base de datos de estado del enlace la cual es esencial para poder dibujar un esquema de quién está conectado con quién.

Todos los routers en una misma área tienen que tener una base de datos del enlace idéntica. Cada router ejecuta independientemente el algoritmo SPF-2[27], también conocido como algoritmo de Dijkstra[28], en la base de datos del enlace con tal de determinar las mejores rutas a los destinos.

[26] *Routing Information Protocol.* Protocolo de Información de Routing.

[27] El algoritmo de ruteo SPF (Primero la Trayectoria Más Corta) es la base de la operación del OSPF. Cuando un ruteador SPF se enciende, inicializa sus estructuras de datos para el protocolo de ruteo y posteriormente las señales de los protocolos de las capas inferiores que indican que sus interfaces están funcionando correctamente.

[28] Edsger Wybe Dijkstra. Es un algoritmo de caminos mínimos, en 1959 describió un algoritmo para la determinación del camino más corto, dado un vértice origen al resto de vértices en un grafo con pesos en cada arista.

El algoritmo SPF añade el costo (el cual está normalmente basado en el ancho de banda) a cada uno de los enlaces entre el router origen y el destino. Entonces el router escoge el camino con coste más bajo y añade el camino a su tabla de encaminamiento, también conocida como base de datos de forwarding[29].

Para simplificar el intercambio de información de encaminamiento sobre varios vecinos en la misma red, los routers que ejecutan OSPF tienen que escoger el Router Designado (DR) y el Router Designado de Backup (BDR) para servir de punto central para la actualización de rutas.

Ya que la proximidad es necesaria para que los routers que utilizan OSPF puedan compartir su información de encaminamiento, un router tiene que ser adyacente con al menos otro router en la red IP a la que esté conectado.

Para iniciar esta adyacencia, cuando un router arranca el proceso de encaminamiento OSPF en una de sus interfaces, envía un paquete 'hello' a la dirección multicast 224.0.0.5, a todos los routers, para asegurar el estado de las adyacencias lo seguirá mandando a intervalos regulares.

[29] Proceso por el cual un puente o conmutador ethernet lee el contenido de un paquete y lo transmite al segmento apropiado. La velocidad de remisión es el tiempo que precisa el dispositivo para ejecutar todos estos pasos.

OSPF utiliza el protocolo Hello para realizar un intercambio inicial con el que se pretende conocer a los vecinos de red; posteriormente, se averiguan las rutas existentes para, por último, elegir las rutas y mantener la información de encaminamiento.

OSPF por defecto según la RFC2328 permite hasta 6 rutas con igual costo hacia un único destino, esto permitiría balanceo de carga en caso que sea necesario.

Capa de transporte

El objetivo de esta capa del modelo OSI, dentro del conjunto de protocolos de TCP/IP, es el de encargarse de la entrega de los paquetes de información que se realiza en texto claro, sin comprobaciones de integridad, sin confidencialidad y no repudio.

Para introducir estas características, se diseñaron los protocolos SSL/TLS[30] y SSH[31] que se introducen entre la capa de transporte y la de aplicación de tal forma que los paquetes se encripta para su transmisión y se desencripta en la recepción de manera transparente para las aplicaciones.

[30] *Secure Sockets Layer / Transport Layer Security*; Ambos son sistemas de cifrado que permite una interacción segura entre un navegador y un servidor web.

[31] *Secure Shell Handler*. Un protocolo de red que permite a un usuario para conectarse a una máquina remota de forma segura

2.7.2 SSL

SSL se introduce en la pila de protocolos de TCP/IP como un protocolo de propósito general que permita al flujo de datos entre una aplicación y el nivel de transporte confiable:

Autenticación y no repudio en el lado del servidor mediante certificados digitales (X.509[32])

Autenticación y no repudio en el lado del cliente mediante certificados digitales (X.509)

Integridad de los datos

Confidencialidad de los datos

Para establecer una comunicación segura utilizando SSL se debe realizar:

Solicitud de seguridad.

Establecer los parámetros que se utilizarán para SSL. Esta parte se conoce como SSL Handshake.

[32] Es un estándar de la UIT para infraestructuras de claves públicas (*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.

Verificaciones periódicas para garantizar que la comunicación sigue siendo segura a medida que se transmiten datos.

Tras completar la transacción, se termina SSL.

Durante el handshake[33] se cumplen varios propósitos, por un lado se realiza la autenticación del servidor y, opcionalmente, la del cliente; se determina qué algoritmos de criptografía serán utilizados y se genera una llave secreta que se utilizará durante el intercambio de mensajes subsiguientes durante la comunicación SSL.

2.7.3 SSH

SSH constituye un conjunto de protocolos para el inicio de sesión remota segura y otros servicios de red como transmisión de ficheros, está compuesto por los siguientes protocolos:

Transporte. Proporciona autenticación del servidor, confidencialidad e integridad de los datos

Autenticación del usuario

[33] Es el protocolo de comienzo de comunicación entre dos máquinas o sistemas

Conexión. Proporciona múltiples canales de datos a través de un único túnel cifrado mediante un código de autenticación de mensajes (MAC)

2.8 Diseño de una VPN

A continuación se describen algunas situaciones en donde se usan los túneles y con ello las VPN, utilizando el protocolo IPSec por ser el que más seguridad y funcionalidad ofrecen en la implementación de las VPN (Corrales, Beltrán, & Guzmán, 2006).

a) De subred a subred

La figura 2.18, muestra el modelo de subred a subred el cual cuenta con 2 redes LAN con conexión a internet por medio de un ruteador para lograr la conexión a internet utilizando una pared de fuego (firewall) y de esta forma proveer seguridad, con dirección de internet (IP) estática.

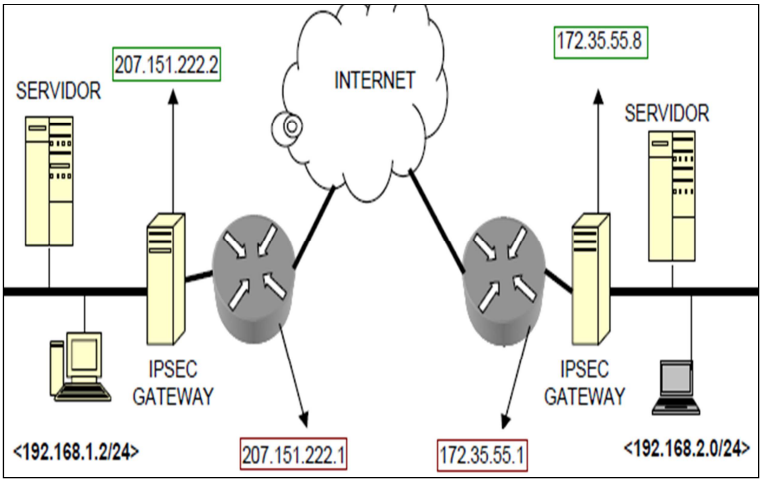


Figura 2.18 Subred a subred

b) Subred a subred utilizando NAT

Es el primer diseño de configuración en donde la puerta de enlace (gateway) está detrás del ruteador/firewall que utiliza NAT[34], el NAT convierte una dirección IP pública en una privada de tal forma que dicha dirección se puede considerar como una IP local.

El NAT también realiza el proceso inverso al descrito anteriormente.

[34] *Network Address Translation.* Traducción de Dirección de Red, es un mecanismo utilizado por routers IP para intercambiar paquetes entre dos redes que se asignan mutuamente direcciones incompatibles.

El proceso de conversión se lleva a cabo con el fin de comunicar a todos los equipos de cómputo de las dos redes y de esta manera lograr la transferencia de información entre cada una de las computadoras que integran la red.

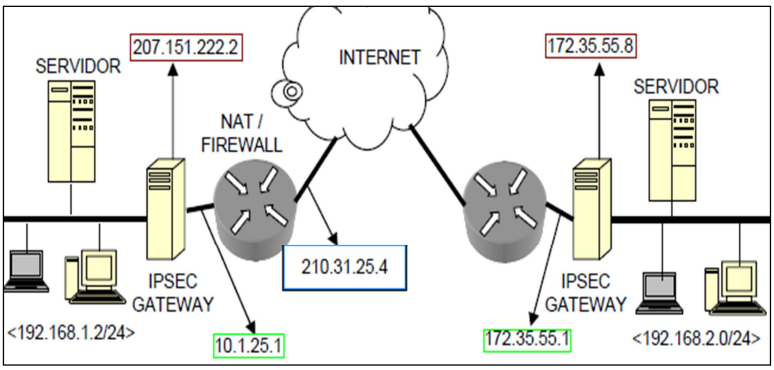


Figura 2.19 Subred a subred aplicando NAT

c) De IPSec a IPSec

Se usa en usuarios con estaciones móviles como laptops que requieren conexión a una red central usando el protocolo IPSec, véase la figura 2.20.

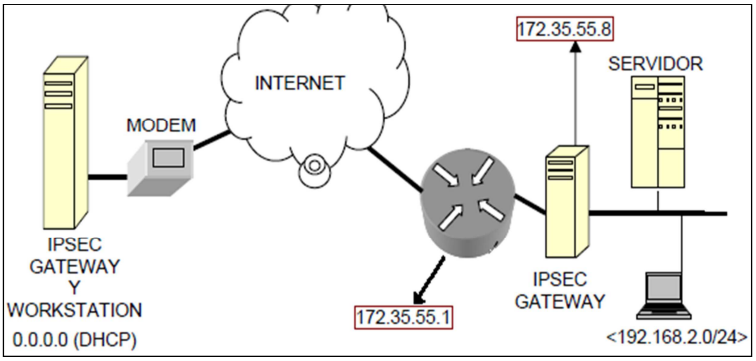


Figura 2.20 Red de IPSec a IPSec

Las dificultades del modelo descrito en la figura 2.20, se generan por la razón de que el túnel está configurado con DHCP (*Dynamic Host Configuración Protocol*, Protocolo de configuración de host dinámico) el cual asigna direcciones IP a las computadoras que se encuentran en una red de forma dinámica, lo que hace que no se tenga un control completo en las conexiones.

Estos son algunos de los diseños posibles para crear una VPN, ya que cada empresa que requiere de VPN normalmente diseña su propia red de acuerdo a sus requerimientos.

Lo que hace que una VPN funcione correctamente para dar solución a los problemas de comunicación es diseñar la configuración óptima.

2.9 Software para el diseño y configuración de la VPN

Como parte del diseño se debe contar con el software especializado para la VPN a implementar, en el caso de esta tesis se lo hará bajo licencia libre. Aunque hay soporte en diferentes sistemas operativos, sea Windows, Macintosh o Linux en la mayoría de sus distribuciones.

A continuación se describen algunas de las características de Linux, por ser el sistema operativo seleccionado para el desarrollo de este proyecto, una de las razones es que la licencia es gratuita se necesita poca memoria en el los servidores y ofrece Estabilidad entre otras cosas.

2.10 Definición de LINUX

Linux es un sistema operativo gratuito, de código abierto, desarrollado mediante cooperación de cientos de programadores dispersos por todo el mundo, parecido a Unix y disponible para casi todas las plataformas de hardware, ofrece un amplio soporte a redes, muchas características de operación con otros sistemas y un gran número de aplicaciones nativas e implementadas (Martin, 2001)).

Es uno de los sistemas operativos más seguros en la actualidad, las ventajas que ofrece son:

- Calidad

- Estabilidad
- Personalización
- Flexibilidad
- Consume pocos recursos
- Ahorro en licencias

Los lugares en los que el sistema operativo Linux ha tenido mayor aceptación son los siguientes:

- Universidades
- Proveedores de servicios de Internet
- Empresas en general

Linux nació en internet y desde entonces se ha venido desarrollando en la red mundial, Linux es realmente el núcleo del sistema operativo completo. El sistema operativo al que se suele llamar Linux es en realidad un conjunto de muchos programas, incluido el núcleo Linux llamado Kernel[35] (Pons, 2009)

[35] Es un software que constituye la parte más importante del sistema operativo Es el principal responsable de facilitar a los distintos programas acceso seguro al hardware de la computadora o en forma más básica, es el encargado de gestionar recursos, a través de servicios de llamada al sistema

Sólo es necesario encontrar un software de creación de VPN compatible con la distribución utilizada y con la versión del Kernel.

Los sitios en internet en los que se pueden descargar algunas distribuciones de Linux se muestran en la tabla 2.1.

DISTRIBUCIÓN	SITIO WEB
REDHAT, FEDORA CORE	http://www.redhat.es/
SUSE	http://www.novell.com/es-es/linux/**suse**/
VECTOR	http://vectorlinux.com/
TURBOLINUX	http://www.turbolinux.com/
LUNAR-LINUX	http://www.lunar-linux.org/
OTROS	http:// www.linux.org

Tabla 2.1 Sitios web para descarga de algunas distribuciones Linux

2.11 Distribuciones de LINUX

Bajo este concepto de libertad surgen las diferentes versiones que comunidades de programadores y empresas de software hacen del sistema operativo GNU/Linux que se denominan Distribuciones, o abreviadamente Diestros.

Para empresas o particulares, para cualquier tipo de uso, surgen en este mundo cientos de distribuciones que al recién llegado, representan una enorme cantidad de opciones a elegir. Se debe elegir aquella que se adapte mejor a las

necesidades presentadas, las hay optimizadas para escritorio, para servidor, para uso empresarial, etc. hay cientos, pero siempre se puede elegir la que mejor convenga.

Las tres primeras Distribuciones GNU[36]/Linux que aparecieron en el mundo del software libre fueron tres: Slackware[37], Debian[38] y Red Hat[39], todas las demás distribuciones posteriores derivan de estas 3, pero como se dijo hoy existen cientos de ellas (Alegre, 2010)

2.12 Software para crear VPN

Los programas que se describen a continuación incluyen todos los elementos necesarios en cuanto a software se refiere, para realizar una conexión VPN, algunos de los elementos más importantes son: protocolo de túnel, archivos de configuración para el servidor y clientes VPN, algoritmos de encriptación y autentificación, entre otros (instalación de Debian GNU/Linux).

[36] Significa "No es Unix" Fue un proyecto iniciado por Richard Stallman en 1984 con el objetivo de crear un sistema operativo tipo Unix completamente libre.

[37] Slackware Linux es la distribución Linux más antigua que tiene vigencia, incluye la versión del núcleo Linux 2.6.33.4 y Glibc 2.11.1

[38] Proyecto Debian, es una comunidad conformada por desarrolladores y usuarios, que mantiene un sistema operativo GNU basado en software libre.

[39] Compañía responsable de la creación y mantenimiento de una distribución del sistema operativo GNU/Linux que lleva el mismo nombre: Red Hat Enterprise Linux, y de otra más, Fedora.

Actualmente el crecimiento en el uso de redes privadas virtuales como medio de comunicación entre computadoras remotas, permite que programadores de todo el mundo pongan su atención en desarrollar programas que permitan tener comunicación entre computadoras por medio de VPN.

En internet existe una gran cantidad de software que ayuda a realizar esta tarea y se puede obtener de forma gratuita así como el propio código fuente para Linux. Algunos ejemplos de estos programas son:

VTUN (VTUN VIRTUAL TUNNEL).- El virtual túnel soporta una variedad de métodos de establecimiento de un enlace y varios algoritmos y como es software libre se puede conseguir gratuitamente en internet

VPND (VIRTUAL PRIVATE NETWORK DAEMON).- El demonio de red privada virtual permite la conexión entre dos redes vía virtual utilizan TCP[40]/IP. Todos los datos transmitidos entre las dos redes son encriptados usando un algoritmo de encriptación

[40] *Transmission Control Protocol*, Protocolo de Control de Transmisión

TINC: Es un paquete ligero que ofrece funcionalidad VPN básica. Actualmente, está disponible para Linux, FreeBSD [41]y Solaris[42] (Ania & Gomez de Silva, 2008).

OpenVPN: El proyecto OpenVPN para mejorar el protocolo SSL tiene algunas características como: proveer el túnel y el encapsulamiento de paquetes necesarios para crear en enlace virtual, utiliza capacidad de encriptación y autentificación de las bibliotecas Open SSL para la seguridad del túnel, las comunicaciones ocurren por un solo puerto TCP o UDP[43], trabaja bajo el modelo cliente servidor y es software libre.

CIPE: Crypto IP Encapsulation. El objetivo de este software es proporcionar una facilidad para la interconexión segura de subredes a lo largo de una red insegura como internet. CIPE encripta los datos a nivel de red, es decir, los paquetes que se envían entre hosts ya están encriptados, este programa se utiliza para hacer túneles, con el fin de hacer VPN, la implementación es simple por consiguiente no muy segura, es software libre (Mathon, 2004).

[41] Sistema operativo libre para computadoras basado en las CPU de arquitectura Intel.

[42] Sistema operativo desarrollado por Sun Microsystems basado y certificado en Unix.

[43] *User Datagram Protocol*, es un protocolo del nivel de transporte basado en el intercambio de datagramas.

FreesWAN (LINUX FREESWAN).- Es un paquete que incluye como protocolo para hacer túneles a IPSec. En la actualidad se puede considerar como la mejor opción puesto que es el que promete mayor interoperabilidad con IPSec.

2.13 Software DEBIAN versión 6

Para el presente tema de tesis se manejará servidores con un sistema operativo libre, se utilizará el Debian 6, se selecciona este software, porque es sostenida por una comunidad de usuarios de todo el mundo, es decir hay soporte por parte de los desarrolladores, es confiable e independiente de los propósitos de mercado que puedan tener empresas patrocinadoras (sea Canonical[44], o Red Hat), es verdaderamente el Sistema Operativo Universal y esto es lo que la diferencia de las demás.

Esta nueva versión de Debian es multiplataforma, disponible en: x86, ARM, 32 y 64 bits, MIPS y otros más, lo que más distingue a Debian de otras distribuciones GNU/Linux es su sistema de gestión de paquetes. Estas herramientas otorgan al administrador de un sistema Debian, total control sobre los paquetes operativos instalados, incluyendo la capacidad de instalar un sólo paquete o actualizar el sistema

[44] Empresa sudafricana para la promoción de proyectos relacionados con software libre.

por completo. También es posible proteger paquetes individualmente de forma que no se actualicen.

A continuación se enumeras otros aspectos:

1- Es el sistema que soporta mayor tipo de arquitecturas de hardware, por ejemplo procesadores de familia Intel, AMD64, Intel Itanium o IA-64, MIPS y MIPSEL, S-390 y Z-Series, también los procesadores ARM, Power PC de IBM y los antiguos Macintosh, procesadores SPARC de Sun Microsistems, hoy Oracle[45]

2- Aunque el núcleo mayoritariamente usado es el núcleo Linux (Debian GNU/Linux), se tiene diferentes versiones de Debian con núcleos diferentes como el Hurd[46] de GNU (Debian GNU/Hurd) y el núcleo de FreeBSD (Debian GNU/KfreeBSD), por lo tanto no es únicamente una distribución Linux

[45] Sistema de gestión de base de datos relacional (o RDBMS Relational Data Base Management System), desarrollado por Oracle Corporation.

[46] Conjunto de programas servidores que simulan un núcleo Unix que establece la base del sistema operativo GNU.

3- En los últimos años, las sucesivas versiones de Debian van generando sistemas cada vez más fáciles de manejar, Debian 6 *Squeeze*[47], es un claro ejemplo de ello.

4- Es más estable y tiene más de 29.000 paquetes de programas mantenidos por la comunidad.

5- El compromiso de la comunidad Debian con el software libre es mucho mayor que en otras Distribuciones comerciales, se descarga con software completamente libre, pero se pueden añadir aplicaciones y librerías propietarias si el usuario lo desea.

6- No hay diferentes ramas de Debian que incomoden al usuario, al instalar una Debian, se elige el tipo de escritorio que se desea utilizar, Gnome[48], KDE[49], Xfce[50], LXDE[51], Enlightenment[52], Fluxbox[53], pero siempre englobados en la misma Distribución.

[47] Debian 6.0 incluye los entornos de escritorio KDE, GNOME, Xfce y LXDE, así como todo tipo de aplicaciones de servidor.

[48] Entorno de escritorio e infraestructura de desarrollo para sistemas operativos Unix y derivados Unix como GNU/Linux, BSD o Solaris.

[49] Proyecto de software libre para la creación de un entorno de escritorio e infraestructura de desarrollo para diversos sistemas operativos como GNU/Linux, Mac OS X, Windows, etc.

[50] Entorno de escritorio ligero para sistemas tipo Unix como Linux, Solaris y derivados.

7- No requiere estar migrando cada poco tiempo a una nueva versión cada 6 meses o cada año, tiene tres versiones:

Stable: Para entornos críticos y de trabajo, muy estable, renueva versión cada 3 años como media, siempre equipada con librerías y programas ampliamente probados y donde prima la seguridad y la estabilidad frente a lo más nuevo.

Testing: O entorno de pruebas de Stable, ideal para computadores de escritorio, tiene programas más nuevos y se actualiza constantemente (concepto Rolling Release[54]), se instala una vez y se actualiza siempre.

Unstable: Entorno de Desarrollo, lleva instalado lo más nuevo, lo último que te puedas encontrar en el mundo de Software Libre, eso sí, no se garantiza nada en lo referente a fallos de funcionamiento, ésta versión se recomienda a los más

[51] Lightweight X11 Desktop Environment, entorno de escritorio libre para Unix y otras plataformas POSIX, como Linux o BSD.

[52] Es un gestor de ventanas ligero para UNIX y GNU/Linux.

[53] Es un gestor de ventanas para el Sistema X Window basado en Blackbox 0.61.1

[54] Una distribución que actualice la paquetería constantemente sin necesidad de instalar o reinstalar la distro para pasarse a una nueva versión.

valientes y amigos de trastear, en todo caso indicaros que muchos paquetes de las últimas versiones de Ubuntu[55] o Linux Mint, salen de esta rama.

8- Debian tiene tres tipos de repositorios oficiales Main, Contrib y Non-Free:

Main: Repositorios creados y mantenidos por la Comunidad de Debian, totalmente libres

Contrib: Resto de Repositorios Libres

Non-Free: No libres, repositorios de código propietario adaptados a Debian (por ejemplo: librerías para mp3, Wav, Zip, Adobe Flash Player)

Repositorios no oficiales como el de Debian-multimedia, para reproducción multimedia

9- Tiene una enorme documentación a tu disposición , para que puedas aprender todo lo necesario para poderla utilizar, aparte de blogs, páginas web y foros, su gestor de paquetes APT[56], es de gran eficiencia y su formato de archivo

[55] Distribución Linux basada en Debian GNU/Linux que proporciona un sistema operativo actualizado y estable para el usuario medio, con un fuerte enfoque en la facilidad de uso y de instalación del sistema

[56] *Advanced Packaging Tool*. Herramienta Avanzada de Empaquetado, es un sistema de gestión de paquetes creado por el proyecto Debian

.deb, uno de los más usados en el software libre, usado en multitud de Distribuciones que derivan de ella.

2.14 OPENVPN

Este software se utilizará para realizar la VPN entre la unidad educativa Freirestabile con la UCSG y se justifica porque OpenVPN provee seguridad, estabilidad y comprobados mecanismos de cifrado sin sufrir la complejidad de otras soluciones VPN, en centro de cómputo de la UCSG también recomienda que se haga con este software.

Se detallan sus principales características:

Túnel de cualquier subred IP virtual o adaptador Ethernet en un único puerto UDP o TCP.

Configuran una solución escalable, con equilibrio de carga de servidores VPN usando una o más máquinas que pueden manejar miles de conexiones dinámicas de los clientes VPN entrantes.

Redes tunneling sobre NAT.

Control de OpenVPN usando GUI en Windows o Mac OS X.

Redes tunneling cuyos extremos sean de red pública, son dinámicos como DHCP o de marcación de los clientes.

Elección entre la estática clave de cifrado basado en convencional o cifrado basado en certificados de clave pública.

Uso estático, claves pre-compartidas o TLS basado en el intercambio de claves dinámicas.

Uso de compresión en tiempo real vínculo de adaptación y de tránsito para gestionar la configuración de la utilización del enlace de ancho de banda.

Redes de túneles pública cuyos extremos son dinámicos como DHCP o de marcación de los clientes.

Este también destaca del resto de software por:

Incluye la portabilidad entre plataformas en la mayor parte del universo informático conocido, una excelente estabilidad, escalabilidad a cientos o miles de clientes, de instalación relativamente fácil, y soporte para direcciones IP dinámicas y NAT.

OpenVPN ofrece una extensible marco de VPN que ha sido diseñado para facilitar específica del sitio de personalización, tales como proporcionar la capacidad

de distribuir un paquete de instalación personalizado a los clientes, o el apoyo a otros métodos de autenticación a través de la interfaz de OpenVPN plugin de módulo (por ejemplo el openvpn-auth-pam módulo permite OpenVPN para autenticar a los clientes utilizando cualquier método de autenticación PAM.

En Windows, OpenVPN puede leer los certificados y claves privadas de las tarjetas inteligentes que soportan el Windows Crypto API.

OpenVPN se construyó para la portabilidad. En el momento de escribir estas líneas, OpenVPN se ejecuta en Linux, Solaris, OpenBSD, FreeBSD, NetBSD, Mac OS X y Windows (2000/XP y versiones posteriores). Debido a que OpenVPN está escrito como un demonio en espacio de usuario en lugar de un módulo del kernel o una compleja modificación a la capa IP, los esfuerzos de portar son considerablemente más simples.

OpenVPN es fácil de usar. En general, un túnel puede ser creado y configurado con un único comando (y sin ningún tipo de archivos de configuración necesarios).

OpenVPN ofrece muchas opciones para controlar los parámetros de seguridad del túnel VPN, sino que también proporciona opciones para proteger la seguridad del propio servidor, por ejemplo - chroot para restringir la parte del sistema de archivos del demonio OpenVPN tiene acceso a, - grupo de descalificación de privilegios tras

el inicio del demonio, y - - usuario y mlock para asegurar que el material y los datos clave del túnel nunca se página en el disco en el que más tarde podrían ser recuperados.

2.14.1 Ventajas y Desventajas de OPENVPN

Ventajas

Además ofrece ventajas que van más allá que cualquier otra solución como son:

Posibilidad de implementar dos modos básicos, en capa 2 o capa 3, con lo que se logran túneles capaces de enviar información en otros protocolos no-IP como IPX o broadcast (NETBIOS).

Protección de los usuarios remotos. Una vez que OpenVPN ha establecido un túnel el firewall de la organización protegerá el laptop remoto aun cuando no es un equipo de la red local. Por otra parte, solo un puerto de red podrá ser abierto hacia la red local por el remoto asegurando protección en ambos sentidos.

Conexiones OpenVPN pueden ser realizadas a través de casi cualquier firewall. Si se posee acceso a Internet y se puede acceder a sitios HTTPS, entonces un túnel OpenVPN debería funcionar sin ningún problema.

Soporte para proxy. Funciona a través de proxy y puede ser configurado para ejecutar como un servicio TCP o UDP y además como servidor (simplemente esperando conexiones entrantes) o como cliente (iniciando conexiones).

Solo un puerto en el firewall debe ser abierto para permitir conexiones, dado que desde OpenVPN 2.0 se permiten múltiples conexiones en el mismo puerto TCP o UDP.

Las interfaces virtuales (tun0, tun1, etc.) permiten la implementación de reglas de firewall muy específicas.

Todos los conceptos de reglas, restricciones, reenvío y NAT10 pueden ser usados en túneles OpenVPN.

Alta flexibilidad y posibilidades de extensión mediante scripting. OpenVPN ofrece numerosos puntos para ejecutar scripts individuales durante su arranque.

Soporte transparente para IP´s dinámicas. Se elimina la necesidad de usar direcciones IP estáticas en ambos lados del túnel.

Ningún problema con NAT. Tanto los clientes como el servidor pueden estar en la red usando solamente IP´s privadas.

Diseño modular. Se basa en un excelente diseño modular con un alto grado de simplicidad tanto en seguridad como red.

Desventajas

No tiene compatibilidad con IPsec que justamente es el estándar actual para soluciones VPN.

Todavía existe poca gente que conoce cómo usar OpenVPN.

Al día de hoy sólo se puede conectar a otras computadoras. Pero ya existen compañías desarrollando dispositivos con clientes OpenVPN integrados.

2.14.2 comparación entre OPENVPN y IPSEC VPN

IPsec	OpenVPN
Estándar de la tecnología VPN	No compatible con IPsec
Plataformas de hardware (dispositivos, aparatos)	Solo en computadoras, pero en todos los sistemas operativos disponibles, ya comienzan a encontrarse dispositivos que cuentan con OpenVPN
Tecnología conocida y probada	Probada y sigue en crecimiento
Muchas interfaces gráficas disponibles	Sin interfaces gráficas profesionales, aunque ya existen algunos proyectos prometedores
Modificación compleja del stack IP	Tecnología sencilla

Necesidad de modificaciones críticas al kernel	Interfaces de red y paquetes estandarizados
Necesidad de permisos de administrador	Ejecuta en el espacio del usuario y puede ser chroot-ed
Diferentes implementaciones de distintos proveedores pueden ser incompatibles entre si	Tecnologías de cifrado estandarizadas
Configuración compleja y tecnología compleja	Facilidad, buena estructuración, tecnología modular y facilidad de configuración
Curva de aprendizaje muy pronunciada	Fácil de aprender y éxito rápido para principiantes
Necesidad de uso de muchos puertos y protocolos en el firewall	Utiliza solo un puerto del firewall
Problemas con direcciones dinámicas en ambas puntas	Trabaja con servidores de nombres dinámicos como DynDNS o No-IP con reconexiones rápidas y transparentes
Problemas de seguridad de las tecnologías IPsec	SSL/TLS como estándar de criptografía
	Control de tráfico (Traffic shaping)
	Velocidad (más de 20 Mbps en máquinas de 1Ghz)
	Compatibilidad con firewall y proxies

Tabla 2.2 Comparación de IPsec vs OpenVPN

En el capítulo siguiente se realiza el proceso para implementar una red privada virtual entre la Unidad Educativa Freire Stabille y la UCSG para acceder directamente al S.I.U. (Sistema Integrado Universitario) desde sus oficinas en Playas.

2.15 IPtables y Firewall

2.15.1 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 debemos verlo como una caja con DOS o más interfaces de red en la que se establecen una reglas de filtrado con las que se decide si una conexión determinada puede establecerse o no. Incluso puede ir más allá y realizar modificaciones sobre las comunicaciones, como el NAT. Esa sería la definición genérica, hoy en día un firewall es un hardware específico con un sistema operativo que filtra el tráfico TCP/UDP/ICMP/../IP y decide si un paquete pasa, se modifica, se convierte o se descarta. Para que un firewall entre redes funcione como tal debe tener al menos dos tarjetas de red. Esta sería la tipología clásica de un firewall:

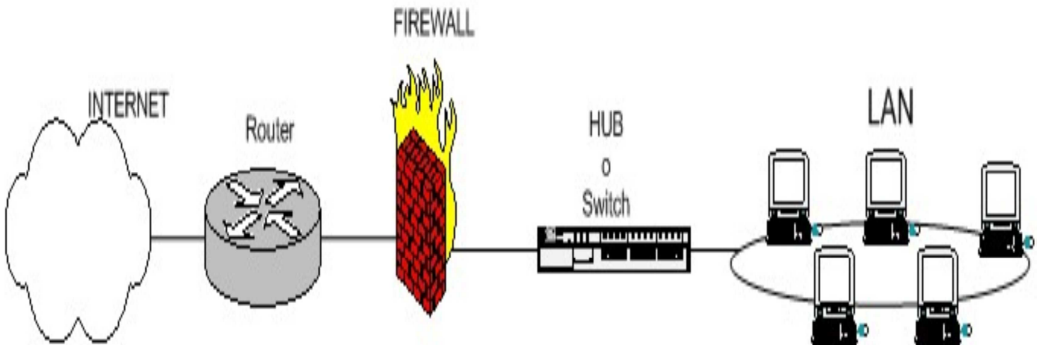


Figura 2.21: Esquema de firewall típico entre red local e internet

Dependiendo de las necesidades de cada red, puede ponerse uno o más firewalls para establecer distintos perímetros de seguridad en torno a un sistema. Es frecuente también que se necesite exponer algún servidor a internet y en esos casos obviamente en principio se debe aceptar cualquier conexión a ellos. Lo que se recomienda en esa situación es situar ese servidor en lugar aparte de la red, el que denominamos DMZ[57] o zona desmilitarizada.

El firewall tiene entonces tres entradas:

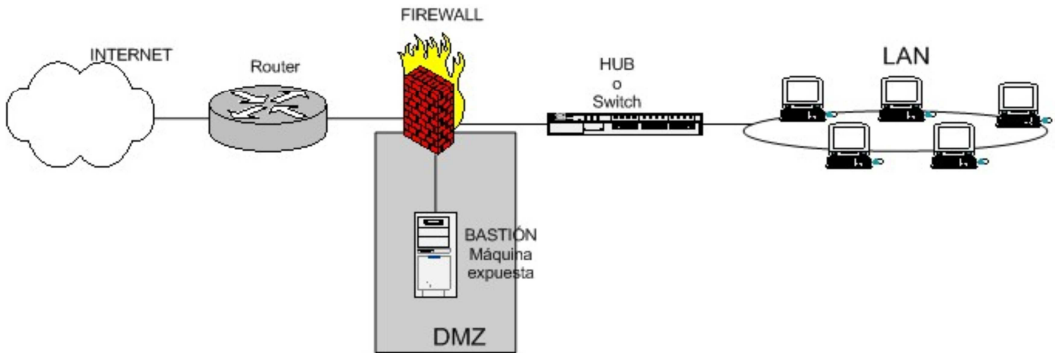


Figura 2.22: esquema de firewall entre red local e internet con zona DMZ para servidores expuestos

[57] DMZ Es una red local que se ubica entre la red interna de una organización y una red externa, generalmente Internet

En la zona desmilitarizada se pueden poner tantos servidores como se necesiten. Con esta arquitectura, permitimos que el servidor sea accesible desde internet de tal forma que si es atacado y se gana acceso a él, la red local sigue protegida por el firewall.

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; esto último se hace con el firewall o frecuentemente con un proxy (que también utilizan reglas, aunque de más alto nivel).

Sea el tipo de firewall que sea, generalmente no tendrá más que un conjunto de reglas en las que se examina el origen y destino de los paquetes del protocolo tcp/ip. En cuanto a protocolos es probable que sean capaces de filtrar muchos tipos de ellos, no solo los tcp, también los udp, los icmp, y otros protocolos vinculados a vpns.

Todo lo que venga de la red local al firewall	ACEPTAR
Todo lo que venga de la ip de mi casa al puerto tcp 22	ACEPTAR
Todo lo que venga de la ip de casa del jefe al puerto tcp 1723	ACEPTAR
Todo lo que venga de hora.rediris.es al puerto udp 123	ACEPTAR
Todo lo que venga de la red local y vaya al exterior	ENMASCARAR
Todo lo que venga del exterior al puerto tcp 1 al 1024	DENEGAR
Todo lo que venga del exterior al puerto tcp 3389	DENEGAR
Todo lo que venga del exterior al puerto udp 1 al 1024	DENEGAR

Tabla 2.3 Políticas de Firewall

En definitiva lo que se hace es:

Habilita el acceso a puertos de administración a determinadas IPs privilegiadas

Enmascara el tráfico de la red local hacia el exterior (NAT[58], una petición de un PC de la LAN sale al exterior con la ip pública), para poder salir a internet

Deniega el acceso desde el exterior a puertos de administración y a todo lo que este entre 1 y 1024.

2.15.2 Iptables

Iptables es el componente más popular construido sobre Netfilter[59] es una herramienta de cortafuegos que permite no solamente filtrar paquetes, sino también realizar traducción de direcciones de red (NAT) para IPv4, permite configurar las tablas proporcionadas por el `kernel Linux firewall` además de las cadenas y reglas que almacena.

[58] **Network Address Translation** es un mecanismo utilizado por enrutadores IP para intercambiar paquetes entre dos redes que se asignan mutuamente direcciones incompatibles

[59] Nombre que recibe el proyecto que se encarga de ofrecer herramientas libres para cortafuegos basados en Linux.

Los diferentes módulos del kernel y los programas se utilizan actualmente para los diferentes protocolos, iptables se aplica a IPv4, IPv6 para ip6tables, arptables [60]de ARP, y ebtables[61] de tramas Ethernet.

2.15.2.1 Características de iptables

Una mejor integración con el kernel de Linux con la capacidad de carga de iptables módulos específicos del núcleo diseñados para mejorar la velocidad y la fiabilidad.

Incorpora (SPI)[62]. Esto significa que el servidor de seguridad realiza un seguimiento de cada conexión que pasa por él y en ciertos casos será ver el contenido de los flujos de datos en un intento de anticipar la siguiente acción de ciertos protocolos. Esta es una característica importante en el apoyo de FTP activo y DNS, así como muchos otros servicios de red.

[60] Herramienta de administrador de la red para el mantenimiento del Address Resolution Protocol (ARP)

[61] El programa ebtables es una herramienta de filtrado de un firewall basado en Linux puente.

[62] Stateful Packet Inspection o la inspección de estado) es un firewall que realiza un seguimiento del estado de las conexiones de red (como TCP arroyos, UDP de comunicación) que viajan a través de ella.

El filtrado de paquetes basado en una dirección MAC y los valores de las banderas en la cabecera TCP. Esto es útil en la prevención de ataques con paquetes mal formados y en restringir el acceso de los servidores conectados localmente a otras redes, a pesar de sus direcciones IP.

Sistema de registro que proporciona la opción de ajustar el nivel de detalle de la presentación de informes.

Mejor traducción de direcciones de red.

Apoyo a la integración transparente con tales programas proxy web como Squid[63].

Una característica de limitación de velocidad que ayuda a iptables bloquear ciertos tipos de denegación de servicio (DoS).

Considerado como una alternativa más rápida y segura a ipchains, iptables se ha convertido en el paquete de servidor de seguridad instalado por defecto en Red Hat Linux, Fedora y Debian.

[63] Es un servidor proxy de alto rendimiento para clientes web

Todos los paquetes inspeccionados por iptables pasan a través de una secuencia de una función de las tablas para su procesamiento. Cada una de estas tablas se dedica a un tipo particular de actividad de paquetes y es controlado por una transformación de paquetes asociados / cadena de filtrado.

Hay tres tablas en total.

Tabla mangle, que es responsable de la alteración de la calidad de los bits de servicio en la cabecera TCP. Esto no se utiliza en un entorno doméstico.

Tabla de filtro que se encarga del filtrado de paquetes. Cuenta con tres cadenas incorporadas en la que puede colocar sus reglas de política de firewall. Estos son:

INPUT -> paquetes entrantes con destino al firewall

FORWARD -> paquetes enrutados con destino a otras máquinas

OUTPUT -> paquetes generados por procesos locales en el firewall

Tabla NAT que es responsable de la traducción de direcciones de red. Tiene dos cadenas internas, que son:

Pre-routing de la cadena: los paquetes NAT o DNAT[64] cuando la dirección de destino del paquete tiene que ser cambiado.

Post-routing de la cadena: los paquetes SNAT[65] cuando la dirección de origen del paquete tiene que ser cambiado.

Tipo de TABLA	Función de la tabla	Paquete de la cadena de transformación en la tabla	Función de la cadena
Filtro	El filtrado de paquetes	FORWARD	Filtros de paquetes a los servidores de acceso de otra tarjeta de red en el firewall.
		INPUT	Filtra paquetes destinados al servidor de seguridad.
		OUTPUT	Filtros de paquetes originados en el firewall

[64] traducción de direcciones de red de destino

[65] traducción de direcciones de red de origen

NAT	Traductor de direcciones de red	PREROUTING	Traducción de direcciones se produce antes de enrutamiento. Facilita la transformación de la dirección IP de destino para que sea compatible con la tabla de enrutamiento del servidor de seguridad. Se utiliza con NAT de la dirección IP de destino, también conocido como **destino NAT** o **DNAT.**
		POSTROUTING	Traducción de direcciones se produce después de enrutamiento. Esto implica que no hubo necesidad de modificar la dirección IP de destino del paquete como en el pre-enrutamiento. Se utiliza con NAT de la dirección IP de origen utilizando de uno a uno o muchos-a-uno, NAT. Esto se conoce como **fuente de NAT,** o **SNAT.**
		OUTPUT	Traducción de direcciones de red para los paquetes generados por el firewall. (Rara vez utilizada en entornos SOHO)
Mangle	Modificación de la cabecera TCP	PREROUTING	Modificación de la calidad de paquetes TCP de bits de servicio antes de enrutamiento se produce. (Rara vez utilizada en entornos SOHO)
		POSTROUTING	
		OUTPUT	
		INPUT	
		FORWARD	

Tabla 2.4 De procesamiento de paquetes encaminados por el firewall

Es necesario especificar la tabla y la cadena para cada regla de firewall que usted cree. Hay una excepción: la mayoría de normas están relacionadas con el filtrado, por lo que iptables asume que cualquier cadena que se define sin una tabla asociada a formar parte de la tabla de filtros. La tabla de filtros por lo tanto el valor por defecto.

Las reglas de firewall están a nivel de kernel por lo tanto lo que hace es dependiendo si el paquete es para la propia maquina o para otra máquina, consultar las reglas de firewall y decidir qué hacer con el paquete según mande el firewall.

Básicamente se mira si el paquete está destinado a la propia maquina o si va a otra. Para los paquetes (o datagramas, según el protocolo) que van a la propia maquina se aplican las reglas INPUT y OUTPUT, y para filtrar paquetes que van a otras redes o maquinas se aplican simplemente reglas FORWARD.

En la figura 2.23 un paquete TCP de Internet llega a la interfaz del firewall [66]en una red para crear una conexión de datos.

[66] Una interfaz para la red protegida (red interna) y una interfaz para la red externa.

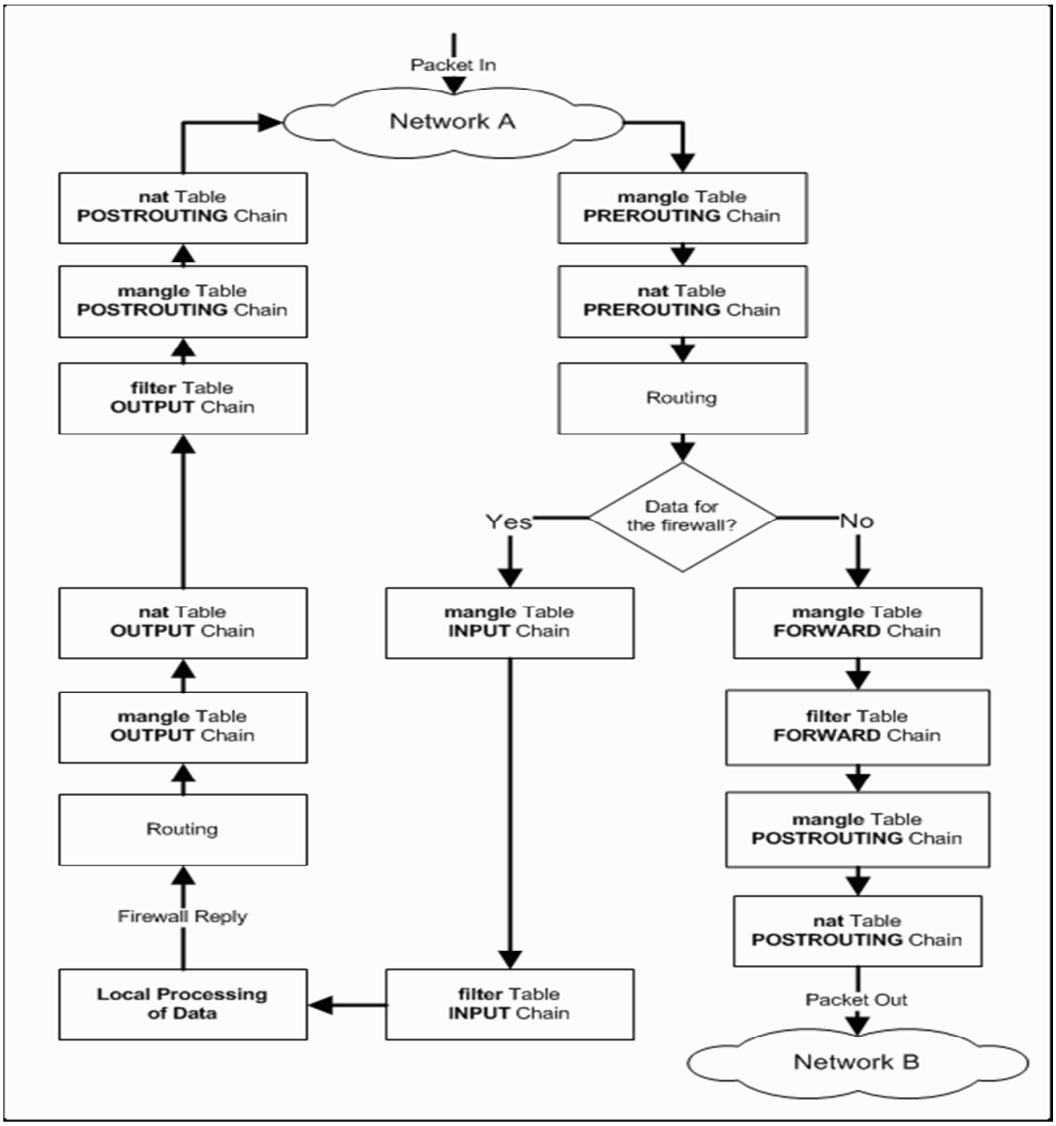


Figura 2.23: Diagrama de flujo de paquetes Iptables

El paquete está en primer lugar por sus reglas en la cadena PREROUTING de la tabla mangle, si lo hubiera. Es entonces inspeccionado por las reglas en la cadena PREROUTING de la tabla NAT para ver si el paquete requiere DNAT. Que se encamina.

Si el paquete está destinado a una red protegida, a continuación, se filtra por las reglas de la cadena FORWARD de la tabla de filtro y, si es necesario, el paquete se somete a SNAT en la cadena POSTROUTING antes de llegar a la red B. Cuando el servidor de destino decide respuesta, el paquete se somete a la misma secuencia de pasos. Tanto el FORWARD y POSTROUTING cadenas se pueden configurar para implementar la calidad de servicio (QoS) en sus tablas de mangle.

Si el paquete está destinado para el cortafuegos, entonces pasa a través de la tabla mangle de la cadena INPUT, si se configura, antes de ser filtrada por las reglas de la cadena INPUT de la tabla de filtros antes. Si supera con éxito estas pruebas, entonces es procesada por la aplicación prevista en el firewall.

En algún momento, el firewall tiene que responder. Esta respuesta se dirige e inspeccionado por las reglas de la cadena de salida de la tabla mangle, en su caso. A continuación, las reglas en la cadena de salida de la tabla nat determinar si se requiere DNAT y las reglas en la cadena de salida de la tabla de filtro son inspeccionados para ayudar a restringir los paquetes no autorizados. Por último, antes

de que el paquete se envíe de nuevo a la Internet, planchado de SNAT y calidad de servicio es realizado por la cadena POSTROUTING

2.16 Squid

Squid es un programa de software libre que implementa un servidor proxy[67] y un *dominio* para caché de páginas web, publicado bajo licencia GPL[68], consta de varias utilidades desde acelerar un servidor web, guardando en caché peticiones repetidas a DNS y otras búsquedas para un grupo de gente que comparte recursos de la red, hasta caché de web, además de añadir seguridad filtrando el tráfico. Está especialmente diseñado para ejecutarse bajo entornos tipo Unix.

Squid ha sido desarrollado durante muchos años y se le considera muy completo y robusto. Aunque orientado principalmente a HTTP y FTP es compatible con otros protocolos como Internet Gopher. Implementa varias modalidades de cifrado como TLS[69], SSL[70], y HTTPS.

[67] Es un programa o dispositivo que realiza una tarea acceso a Internet en lugar de otro ordenador.

[68] La Licencia Pública General GNU (GNU GPL o simplemente GPL) es el más utilizado

[69] Protocolo de seguridad de la capa de transporte

2.16.1 Características

Squid posee las siguientes características:

Proxy y Caché de HTTP, FTP, y otras URL

Squid proporciona un servicio de Proxy que soporta peticiones http, HTTPS y FTP a equipos que necesitan acceder a Internet y a su vez provee la funcionalidad de caché especializado en el cual almacena de forma local las páginas consultadas recientemente por los usuarios. De esta forma, incrementa la rapidez de acceso a los servidores de información Web y FTP que se encuentra fuera de la red interna.

Proxy para SSL

Squid también es compatible con SSL con lo que también acelera las transacciones cifradas, y es capaz de ser configurado con amplios controles de acceso sobre las peticiones de usuarios.

Jerarquías de caché

Squid puede formar parte de una jerarquía de caches. Diversos proxys trabajan conjuntamente sirviendo las peticiones de las páginas. Un navegador solicita

[70] Secure Sockets Layer (SSL; protocolo de capa de conexión segura)

siempre las páginas a un sólo proxy, si este no tiene la página en la caché hace peticiones a sus hermanos, que si tampoco las tienen las hacen a su/s padre/s... Estas peticiones se pueden hacer mediante dos protocolos: HTTP e ICMP[71].

ICP[72], HTCP[73], CARP[74], caché digests[75]

Squid sigue los protocolos ICP, HTCP, CARP y caché digests que tienen como objetivo permitir a un proxy "preguntarle" a otros proxys caché si poseen almacenado un recurso determinado.

Caché transparente

[72] (*i*nternet Control Message Protocol) es el sub protocolo de control y notificación de errores del Protocolo de Internet (IP)

[72] Internet Cache Protocol). HTCP es el sucesor de ICP

[73] HTCP (Hyper Text Caching Protocol) es un protocolo para la consulta, administración y de servidores de caché HTTP

[74] El común de Dirección del protocolo de redundancia o la carpa es un protocolo que permite a varios hosts en la misma red local para compartir un conjunto de direcciones IP

[75] La caché Digest consulta el contenido de la caché de los pares y para la recuperación de los pares.

Squid puede ser configurado para ser usado como proxy transparente de manera que las conexiones son enrutadas dentro del proxy sin configuración por parte del cliente, y habitualmente sin que el propio cliente conozca de su existencia. De modo predefinido Squid utiliza el puerto 3128 para atender peticiones, sin embargo se puede especificar que lo haga en cualquier otro puerto disponible o bien que lo haga en varios puertos disponibles a la vez.

WCCP

A partir de la versión 2.3 Squid implementa `WCCP` (*Web Cache Control Protocol*). Permite interceptar y redirigir el tráfico que recibe un `router` hacia uno o más proxys caché, haciendo control de la conectividad de los mismos. Además permite que uno de los proxys caché designado pueda determinar cómo distribuir el tráfico redirigido a lo largo de todo el array de proxys caché.

Control de acceso

Ofrece la posibilidad de establecer reglas de control de acceso. Esto permite establecer políticas de acceso en forma centralizada, simplificando la administración de una red.

Aceleración de servidores HTTP

Cuando un usuario hace petición hacia un objeto en Internet, este es almacenado en el caché, si otro usuario hace petición hacia el mismo objeto, y este no ha sufrido modificación alguna desde que lo accedió el usuario anterior, Squid mostrará el que ya se encuentra en el caché en lugar de volver a descargarlo desde Internet. Esta función permite navegar rápidamente cuando los objetos ya están en el caché y además optimiza enormemente la utilización del ancho de banda.

SNMP

Squid permite activar el protocolo SNMP, este proporciona un método simple de administración de red, que permite supervisar, analizar y comunicar información de estado entre una gran variedad de máquinas, pudiendo detectar problemas y proporcionar mensajes de estados.

Caché de resolución DNS

Squid está compuesto también por el programa *dnsserver*, que se encarga de la búsqueda de nombres de dominio. Cuando Squid se ejecuta, produce un número configurable de procesos *dnsserver*, y cada uno de ellos realiza su propia búsqueda en DNS. De este modo, se reduce la cantidad de tiempo que la caché debe esperar a estas búsquedas DNS.

Proxy Web

El proxy caché es una manera de guardar los objetos solicitados de Internet (por ejemplo, páginas web) disponibles vía protocolos HTTP, FTP y Gopher en un sistema más cercano al lugar donde se piden. Los navegadores web pueden usar la caché local Squid como un servidor proxy HTTP, reduciendo el tiempo de acceso así como el consumo de ancho de banda. Esto es muchas veces útil para los proveedores de servicios de Internet para incrementar la velocidad de sus consumidores y para las redes de área local que comparten la conexión a Internet.

Debido a que también es un proxy (es decir, se comporta como un cliente en lugar del cliente real), puede proporcionar un cierto grado de anonimato y seguridad. Sin embargo, también puede introducir problemas significativos de privacidad ya que puede registrar mucha información, incluyendo las URL solicitadas junto con otra información adicional como la fecha de la petición, versión del navegador y del sistema operativo, etc.

Un programa cliente (por ejemplo, un navegador) o bien tiene que especificar explícitamente el servidor proxy que quiere utilizar (típico para consumidores de ISP) o bien podría estar usando un proxy sin ninguna configuración extra. A este hecho se le denomina caché transparente, en el cual todas las peticiones HTTP son interceptadas por squid y todas las respuestas guardadas en caché. Esto

último es típico en redes corporativas dentro de una red de acceso local y normalmente incluye los problemas de privacidad mencionados previamente.

Squid tiene algunas características que pueden facilitar establecer conexiones anónimas. Características tales como eliminar o modificar campos determinados de la cabecera de peticiones HTTP de los clientes. Esta política de eliminación y alteración de cabeceras se establece en la configuración de Squid. El usuario que solicita páginas a través de una red que utiliza Squid de forma transparente, normalmente no es consciente de este proceso o del registro de información relacionada con el proceso.

CAPITULO III

DESCRIPCION DE LA UNIDAD EDUCATIVA FREIRESTABILE

3.1 Reseña histórica

La unidad tomada para la realización de tema de tesis es aquella que a partir del 2 de marzo del año 2005, gracias a la donación que hizo el Rvdo. Padre Manuel Freire Heras, la Universidad Católica de Santiago de Guayaquil, es propietaria de la Unidad Educativa FREIRESTABILE ubicada en General Villamil - Playas.

La Unidad cuenta con Pre-primaria, primaria y Secundaria, está última con las especializaciones Físico Matemáticas y Químico Biológicas.

En este complejo educacional también funciona el Sistema de Educación a Distancia de la UCSG Campus Playas.

La Universidad consciente de su responsabilidad social y con el objetivo de brindar un servicio a los amantes de la naturaleza, decidió crear en la parte posterior de la edificaciones, el PARQUE ECOLÓGICO Y DEPORTIVO "SENDEROS DE LA ARMONÍA", como un sitio de sana recreación para todos los turistas nacionales y extranjeros que visitan General Villamil - Playas.

Sistema de Educación a Distancia de la UCSG (Campus Playas)	
CARRERAS	TITULACIÓN
Derecho	Abogado de los Tribunales y juzgados de la República
Administración	Ingeniero Comercial
Ingeniería en Marketing	Ingeniero en Marketing
Ingeniería en Contabilidad y Auditoria	Ingeniero en Contabilidad y Auditoría
Ingeniería en Administración de Empresas Turísticas y Hoteleras	Ingeniero en Administración de Empresas Turísticas y Hoteleras
Licenciatura en Educación Básica Bilingue	Licenciado en Educación Básica Bilingüe

TABLA 3.1 Sistema de Educación a Distancia de la UCSG (Campus Playas)

3.2 Infraestructura de la red

3.2.1. Red LAN

Local Área Network (LAN), es la red de comunicaciones de la UEF instalada dentro del campus, lo cual permite a los usuarios compartir información y recursos como: acceder al correo y acceso al internet. Para tener un mejor panorama se describe a continuación los elementos de la red LAN.

3.2.1.1. Arquitectura

La arquitectura de la red LAN de la UEF o también conocida como IEEE 802.2, en este caso la computadora escucha el cable de la red y espera hasta un periodo de silencio para poder mandar un mensaje que choca con el transito con otros mensajes. Si se pasa del 1% de colisiones o 15% de utilización de cable, se dice que la red esta saturada. La Ethernet vigente en la UEF es de 802.3 a 100Mbps.

3.2.1.2. Topología de la Red

La topología de la red LAN de la UEF es de tipo estrella en este caso todos los mensajes pasan a través de un dispositivo central como concentrador de cableado, que es un SWITCH el cual controla el flujo d datos.

3.2.1.3. Diagrama de la red LAN existente en la UEF

En la figura 3.1 se muestra la red LAN en la matriz, donde se puede apreciar las conexiones entre el SWITCH Central y el SWITCH del Laboratorio de computación.

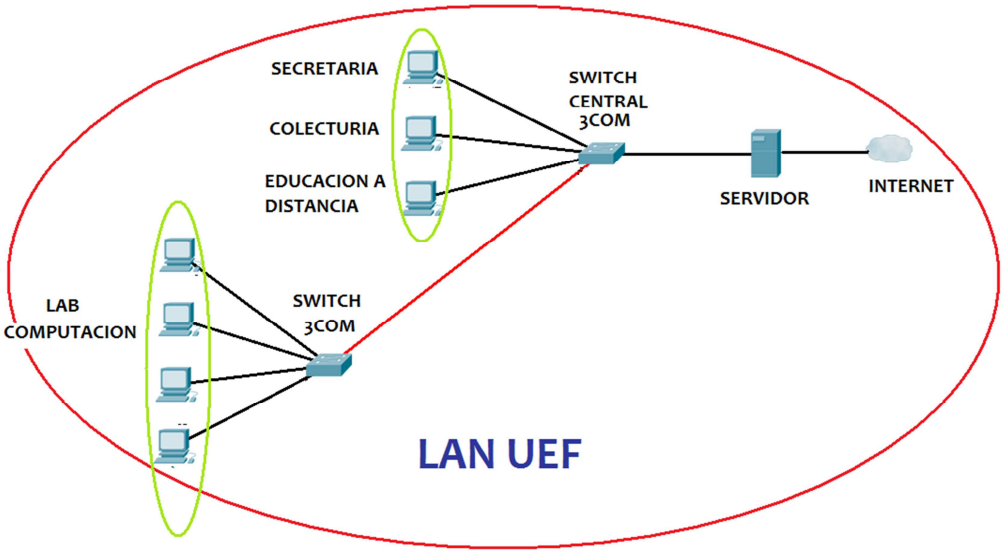


Figura 3.1 Diagrama de la red LAN existente en la UEF

3.2.1.4. Estaciones de trabajo

Cada computadora conectada a la red conserva la capacidad de funcionar de manera independiente, realizando sus propios procesos. Generalmente se la utiliza para acceder al correo electrónico e internet. Se tienen 15 estaciones de trabajo en la UEF.

3.2.1.5. Servidor

EL servidor dentro de la red de la UEF sirve para compartir recursos de internet a todos los usuarios. Existe solo 1 servidor dentro de la institución.

3.3 Infraestructura de telecomunicaciones

Para poder interconectar los host con el servidor la UEF cuenta con medios de transmisión de tecnología que utiliza la UEF para tener una comunicación global y oportuna.

3.3.1 Conexión a internet

Para acceder al servicio de internet, la institución mantiene una conexión permanente de banda ancha de 1/0,5 Mbps con la empresa TELCONET.

Esta conexión es aprovechada por todas las maquinas conectadas a la red LAN

3.4 Plataforma de software y hardware

3.4.1 Sistema operativo de red

Es el sistema (SOFTWARE) que se encarga de administrar y controlar en forma general la red, para esto tiene que ser un sistema operativo multiusuario.

El sistema operativo d red que utiliza la UEF es Microsoft Windows, el esquema de la red Microsoft trabaja e modo de dominio, soporta el protocolo TCP/IP y proporciona una interfaz amigable al administrador de la red.

3.4.2 Estaciones de trabajo

Para las estaciones de trabajo se emplea el sistema operativo de Windows XP, además de presentar una interfaz de fácil manejo a los usuarios, proporciona a estos el soporte para ejecutar el conjunto de aplicaciones que cumplen con los requerimientos de información y trabajos que se manejan en la UEF.

3.4.3 Hardware de la red

Son aquellos dispositivos que se utilizan para interconectar a los componentes de la red, serian básicamente las tarjetas y el cableado entre servidores y estaciones de trabajo, así como los cables para conectar los periféricos.

3.4.3.1 Tarjeta de interfaz de la red

Para pertenecer a la red Ethernet, cada computadora tiene instalada una tarjeta de interfaz de red (network interface card,NIC) y el software adecuado para que la tarjeta funcione. Normalmente las tarjetas deben enviar y recibir las tramas.

Los controladores de 10Mbps en poca cantidad y de 100Mbps en su gran mayoría.

3.4.3.2 Cableado

La institución dispone de cableado estructurado, capaz de interconectar los equipos que forman la red, para interconectar las estaciones de trabajo con el switch central se tiene cable de par trenzado UTP categoría 5e.

3.5 Requerimientos y necesidades de la UEF

A continuación las principales necesidades de la UEF que actualmente presenta y se deberían ser atendidas oportunamente.

3.5.1 Renovación Tecnológica.

La evolución de la tecnología, particularmente de la electrónica, los sistemas informáticos y las telecomunicaciones ha obligado a las empresas a estar actualizadas constantemente, en la UEF se podría tomar en cuenta lo siguiente:

- Es necesario actualizar el servidor que cuentan con procesador Pentium II, por la escases de repuestos no resulta conveniente mantenerlos, además sus características han perdido terreno frente al avance de los sistemas operativos y aplicaciones.
- Reemplazar el switch 3com de 8 puertos por uno de mayores puertos ya que así permitiría una ampliación de la red LAN.
- Incremento de firewall en el servidor para brindar mayor seguridad a la información, debido a que tienen datos igual de importantes y

además pueden ser utilizados como pasarela hacia la re LAN en caso de un ataque informático.

- Estudiar nuevas tecnologías de conectividad como por ejemplo las VPN que signifiquen un ahorro significativo para la UEF

3.5.2 Intranet

La UEF al ser parte de la UCSG y al carecer de un acceso directo al SIU, surge la necesidad de implementar una tecnología que permita una conexión segura y de costos económicos.

CAPITULO IV

DISEÑO E IMPLEMENTACION DE LA VPN

4.1. Planeación

El objetivo de este capítulo es diseñar e implementar una red privada virtual entre la UEF con la UCSG, de tal manera que permita establecer una conexión directa y segura entre ambas instituciones.

Para el diseño e implementación de la red VPN se consideraron los requerimientos tecnológicos de la UEF descritos en el capítulo anterior, tomando en cuenta factores de legitimación, seguridad, económicos, factibilidad.

Partiendo de la infraestructura tecnológica y física de la UEF, el escenario a implementar es una **Red Privada Virtual (VPN) punto a punto** (servidor Linux-servidor Linux) con el software OPENVPN, el cual cubre con las necesidades de seguridad de la red VPN, además ya es fácil de instalar y configurar.

A continuación el detalle del escenario a ser implementado.

4.1.1 Descripción del Escenario a implementar (Red VPN Punto a Punto)

La VPN de punto a punto es una extensión de una networking WAN clásica, las VPN de punto a punto conectan redes enteras entre ellas. Por ejemplo, pueden conectar la red de una sucursal a la red de la sede central corporativa.

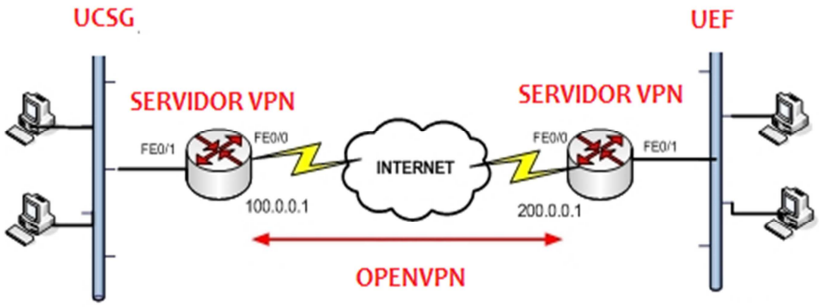


Figura 4.1 Diagrama de una conexión VPN Punto a Punto

4.1.2 Requerimientos

- La red VPN estará formada por los siguientes componentes:
- **Topología:** LAN-to-LAN
- **Tecnología de túnel:** PPTP
- **Plataforma:** por software , usando servidores linux y el paquete de OPEN VPN 2.2.1
- **Equipos utilizados:**

- Un computador Dell inter Core Duo 2,5 GHz,2 MB RAM,160 GB, actuando como Servidor y Gateway , con Debian 6.02 Squezee estable.
- Un computador Dell inter Core Duo 2,5 GHz,2 MB RAM,160 GB, actuando como Servidor y Gateway , con Debian 6.02 Squezee estable.

❖ Conexión a internet

4.1.3 Escenario de la red VPN montada entre la UCSG y la UEF

Se diseña en software Packet Tracer un esquema básico de conexión de una red privada virtual entre la UCSG y la UEF del cantón Playas.

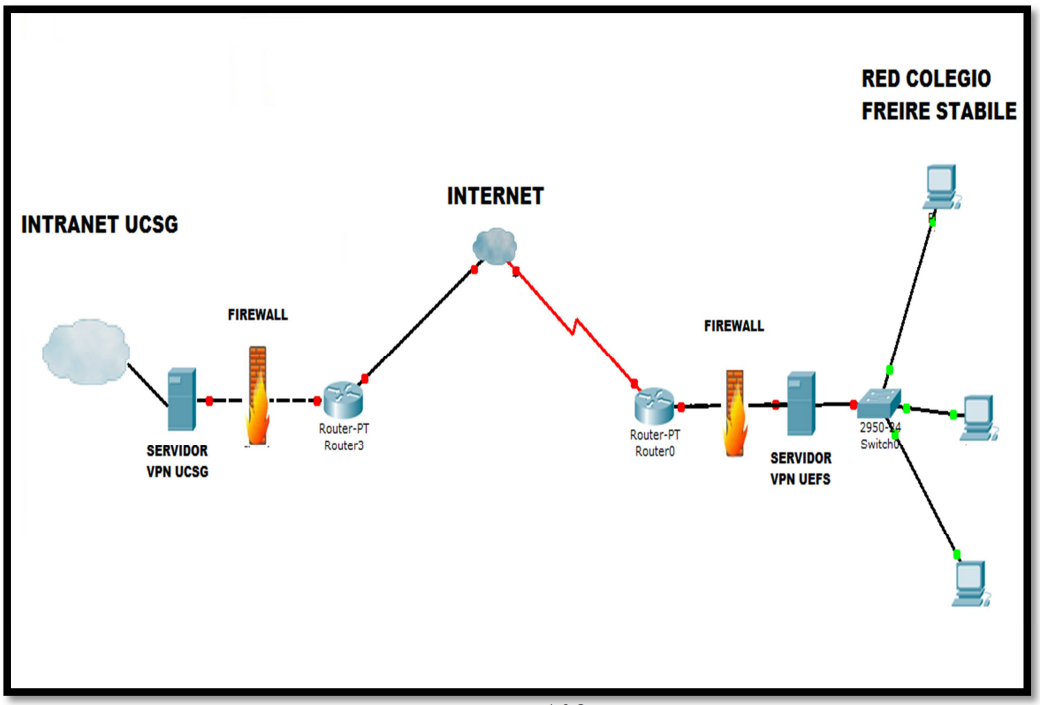


Figura 4.2 Topología de la red VPN en la Unidad Educativa Freirestabile

Según el esquema de la figura 4.2 se aprecia la conexión VPN entre el servidor de la UCSG y el servidor de UEF, permitiendo el acceso al SUI a las estaciones de trabajo de la UEF de forma segura y remota, el punto intermedio se conoce como el proveedor de internet o ISP, en este caso es Telconet, y la velocidad que ofrece a la unidad educativa es de 1 mega bit por segundo, en otras palabras se tiene un considerable ancho de banda en la unidad mencionada.

Los servidores son colocados uno en cada institución los mismos que también hacen las veces de routers, Gateway`s y firewall.

Se remplazó el switch existente por uno de 48 puertos marca TP Link administrable, al cual se interconectan tres estaciones de trabajo:

- Secretaría
- Colecturía
- Educación a distancia.

Por el momento solo 3 máquinas podrán acceder al SIU, pero si las autoridades de la unidad educativa desean podrán expandir aún más la red de la VPN. Solo se deberá hacer las configuraciones de Host, IP, Gateway, proxy e instalar

J2RE[76] a las maquinas que se encuentran conectadas a la LAN de la Unidad Educativa.

4.2 Instalación y Configuración de la red VPN

Los pasos de Instalación y configuración de los servidores VPN de la UCSG y la UEFS son:

- Instalación Debian 6.02 Squezee
- Configuración de tarjetas de red
- Levantar tarjetas de red y servicios del sistema
- Instalar OpenVPN 2.2.1
- Configurar túnel VPN con red 10.10.10.0/30
- Instalar cbq 0.7
- Inicializar cbq con políticas
- Configurar firewall
- Configurar squid
- Configuración de las estaciones de trabajo conectadas a LAN de la UEF

[76] **Java Runtime Environment** es un conjunto de utilidades que permite ejecutar las aplicaciones desarrolladas en lenguaje Java

❖ Pruebas de funcionamiento y resultados

4.2.1 instalación de DEBIAN 6 en los servidores VPN de la UCSG y la UEF

El proceso de instalación comienza con la descarga desde internet, podemos descargar las imágenes de CD en formatos isos desde el sitio web oficial (http://www.debian.org/distrib/index.en.html). El asistente de instalación de Debian nos ofrece opciones que ningún otro instalador nos brinda de forma sencilla, como por ejemplo instalar un entorno de escritorio o servidores con diferentes tipos de servicios. Pero además, Debian soporta diversos tipos de arquitectura y plataformas (i386, i686, PowerPC, Mips, kFreeBSD..etc).

En resumen, si Ud quiere tener control de su sistema, instalar solo lo que necesita haciendo uso de una potente herramienta como dpkg y apt, Debian es su mejor opción.

En el subcapítulo 2.13 se describió este software y en el Anexo 2 muestra los pasos de instalación completa de Debian en los servidores que estarán en cada una de las instituciones.

Figura 4.3 Instalando Debian versión 6.0 el servidor UEF

4.2.2 Configuración de tarjetas de red

Aquí se detalla los siguientes pasos: Conexiones de puerto, asignación de dirección IP asignados por centro de cómputo (UCSG), claves, estatus.

Antes de procedes a configurar las interfaces de red instaladas en los servidores vamos a asignar las direcciones IP para cada uno de los servidores. Las direcciones IP fueron dadas por el centro de cómputo de la UCSG

4.2.2.1 Asignación de direcciones IP en los servidores

Servidor UCSG

IP Publica (eth0)

192.188.52.170/24

GW -> 192.188.52.1

DNS -> 200.93.192.148

DNS -> 200.93.192.1161

IP privada (eth1)

172.16.1.170/24

VPN

10.10.10.2/32 (tun0)

Servidor Playas UEF

PUBLICA (eth0)

186.3.39.130 /30

GW - 186.3.39.129

PRIVADA (eth1)

192.17.1.1/24

GW -> 192.17.1.1

VPN

10.10.10.1/32 (tun0)

4.2.2.2 Configuración de las interfaces de red en el servidor VPN de la UCSG.

Para realizar la configuración de las interfaz de red físicas de cada uno de los servidores se realiza los siguientes pasos:

- Primero conectamos y definimos los puertos del servidor UCSG, como eth0 (publica) eth1 (privada)
- Entrar al terminal (Ctrl+Alt+F1) de Debian como súperusuario
- comando: cd /etc/network/,
- comando: etc/network/nano interfaces , sirve para editar los valores en las tarjetas de red existentes en el servidor
- configuramos las tarjetas con las direcciones asignadas anteriormente por el centro de cómputo.
- comando: ifconfig, para ver las configuraciones de las tarjetas de red
- comando: : etc/network/ service networking start, sirve para levantar las interfaces de red existentes en el servidor.

Ahora desde Centro Computo (UCSG) en Guayaquil, se realiza la configuración de las tarjetas de red Ver fig4.2, se ubica en el rak de cómputo el switch que tenga el puerto asignado por ellos.

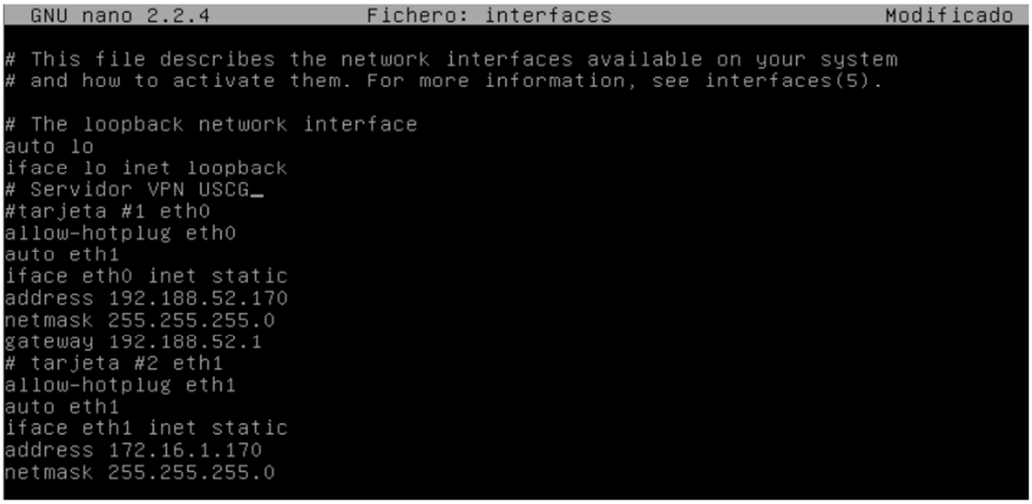


Figura 4.4 Configuración de las tarjetas de red en el servidor UCSG

4.2.2.3 Configuraciones de las interfaces de red en el servidor VPN de la UEF.

Ahora se realiza la configuración de las tarjetas de red del servidor UEF desde la unidad educativa Freire Stabille, tomando en cuenta puerto, dirección IP dado por centro computo, velocidad, clave. Ver figure 4.5

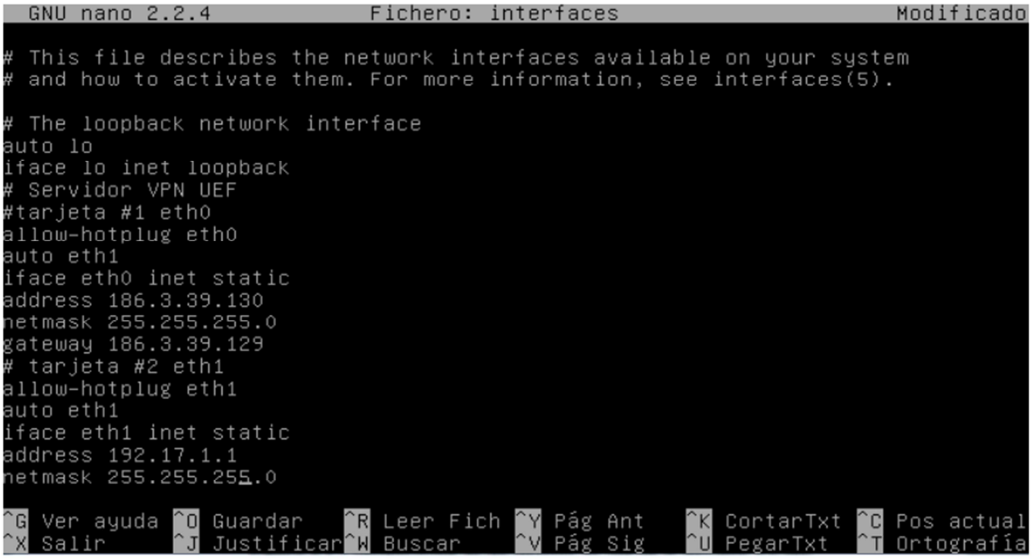


Figura 4.5 Configuración de las tarjetas de red en el servidor UEF

4.2.3 Configuración de OPEN VPN

Como el usuario **root**, desde una terminal, crear el fichero **/etc/openvpn/tun0.conf**, utilizando cualquier editor de texto. En el siguiente ejemplo se utiliza **nano**.

Procedimientos.

- Commando para descargar open vpn : Apt-get install openvpn
- Commando para rear fichero :touch /etc/openvpn/tun0.conf
- Comando para editar fichero : nano /etc/openvpn/tun0.conf

Cambiarse al directorio, desde la terminal, ejecutar lo siguiente para cambiarse al directorio **/etc/openvpn**:

```
cd /etc/openvpn/
```

NOTA: Todos los procedimientos necesarios para configurar un servidor con **OpenVPN** se realizan sin salir de **/etc/openvpn/**. Por favor, **evite cambiar de directorio** hasta haber finalizado los procedimientos descritos en este documento.

A fin de facilitar los procedimientos, se copiarán dentro del directorio **/etc/openvpn/** los ficheros **openssl.cnf**, **whichopensslcnf**, **pkitool** y **vars**, que se localizan en **/etc/openvpn/easy-rsa/2.0/**:

```
cp /usr/share/openvpn/easy-rsa/2.0/openssl.cnf ./
cp /usr/share/openvpn/easy-rsa/2.0/whichopensslcnf ./
cp /usr/share/openvpn/easy-rsa/2.0/pkitool ./
cp /usr/share/openvpn/easy-rsa/2.0/vars ./
```

Utilizar el editor de texto y abrir el fichero **/etc/openvpn/vars**:

```
nano /etc/openvpn/vars
```

De este fichero, solamente editar las últimas líneas, que corresponden a lo siguiente:

```
export KEY_COUNTRY="US"
export KEY_PROVINCE="XX"
export KEY_CITY="XXXXXX"
export KEY_ORG="XXXXX"
export KEY_EMAIL="XX@XXX.com"
```

Reemplazar por valores reales, como los del siguiente ejemplo:

```
export KEY_COUNTRY="EC"
export KEY_PROVINCE="GY"
export KEY_CITY="GYQ"
export KEY_ORG="servidor.mi-dominio.com"
export KEY_EMAIL=" "
```

Se requiere ejecutar del siguiente modo el fichero **/etc/openvpn/vars** a fin de que carguen las variables de entorno que se acaban de configurar.

```
source /etc/openvpn/./vars
```

Cada vez que se vayan a generar nuevos certificados, debe ejecutarse el mandato anterior a fin de que carguen las variables de entorno definidas.

Se ejecuta el fichero **/usr/share/openvpn/easy-rsa/2.0/clean-all** a fin de limpiar cualquier firma digital que accidentalmente estuviera presente.

```
sh /usr/share/openvpn/easy-rsa/2.0/clean-all
```

Lo anterior realiza un **rm -fr** (eliminación recursiva) sobre el directorio **/etc/openvpn/keys**, por lo que se eliminarán todas los certificados y firmas digitales que hubieran existido con anterioridad.

A fin de crear el certificado del servidor, se crea un certificado:

```
sh /usr/share/openvpn/easy-rsa/2.0/build-ca
```

Se crea el fichero dh1024.pem, el cual contendrá los parámetros del protocolo **D**iffie-**H**ellman, de 1024 bits:

```
sh /usr/share/openvpn/easy-rsa/2.0/build-dh
```

El protocolo **D**iffie-**H**ellman permite el intercambio secreto de claves entre dos partes que sin que éstas hayan tenido contacto previo, utilizando un canal inseguro, y de manera anónima (sin autenticar). Se emplea generalmente como medio para acordar claves simétricas que serán empleadas para el cifrado de una sesión, como es el caso de una conexión VPN.

Para generar la firma digital, se utilizan el siguiente mandato:

```
sh /usr/share/openvpn/easy-rsa/2.0/build-key-server server
```

Finalmente se crean los certificados para los clientes. En el siguiente3 ejemplo se crean los certificados para **cliente1**, **cliente2**, **cliente3**, **cliente4**, **cliente5**, y **cliente6**:

```
sh /usr/share/openvpn/easy-rsa/2.0/build-key cliente1
sh /usr/share/openvpn/easy-rsa/2.0/build-key cliente2
sh /usr/share/openvpn/easy-rsa/2.0/build-key cliente3
```

```
sh                  /usr/share/openvpn/easy-rsa/2.0/build-key          cliente4
sh                  /usr/share/openvpn/easy-rsa/2.0/build-key          cliente5
sh /usr/share/openvpn/easy-rsa/2.0/build-key cliente6
```

A fin de utilizar los certificados y que se configure el sistema, se crea con el editor de texto el fichero **/etc/openvpn/servidorvpn-udp-1194.conf**, donde *servidorvpn* se reemplaza por el nombre de anfitrión del sistema:

```
vi /etc/openvpn/servidorvpn-udp-1194.conf
```

Para la **VPN** se recomienda utilizar una red privada que sea poco usual, a fin de poder permitir a los clientes conectarse sin conflictos de red.

4.2.3.1 Configuración del túnel VPN de UCSG y la UEF

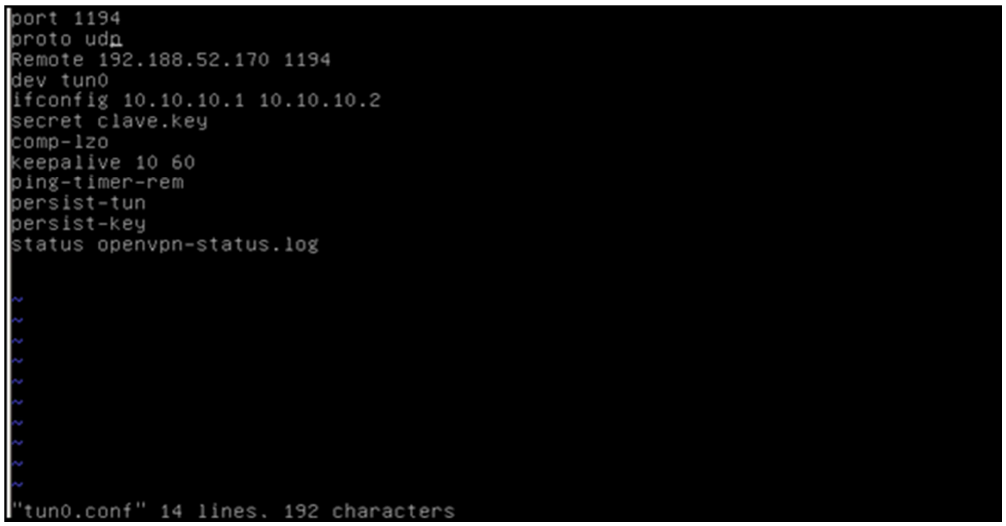


Figura 4.6 Configuración del túnel en el servidor UEF

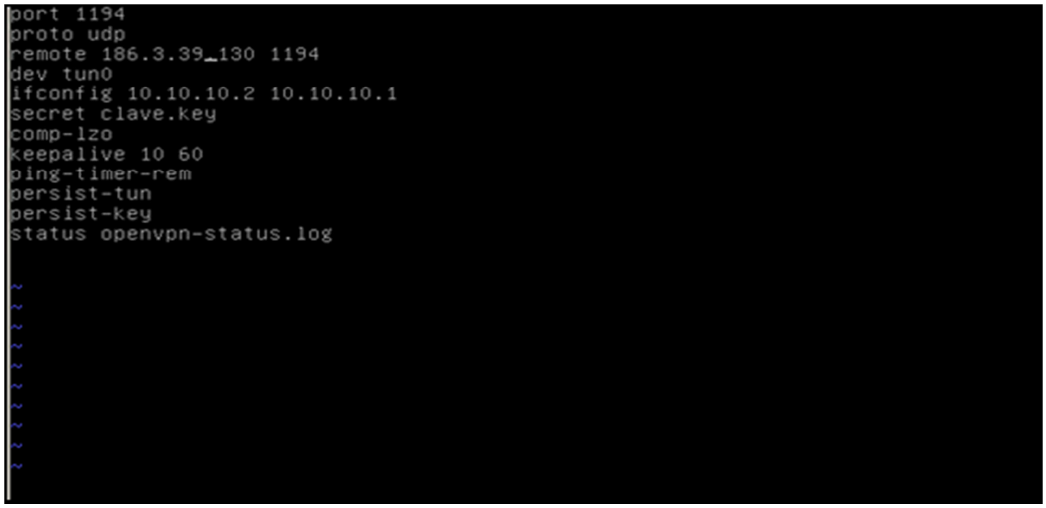


Figura 4.7 Configuración del túnel en el servidor UCSG

Ahora necesitamos insertar el módulo [***tun0]*** para controlar los interfaces */dev/net/tunX* que se necesiten en le sistema para el servicio OpenVPN:

Se crean los ficheros **ipp.txt** y **openvpn-status-servidorvpn-udp-1194.log**:

```
cd /etc/openvpn/
touch ipp.txt
touch openvpn-status-servidorvpn-udp-1194.log
```

Para iniciar el servicio, se utiliza el mandato **service** del siguiente modo:

```
service openvpn start
```

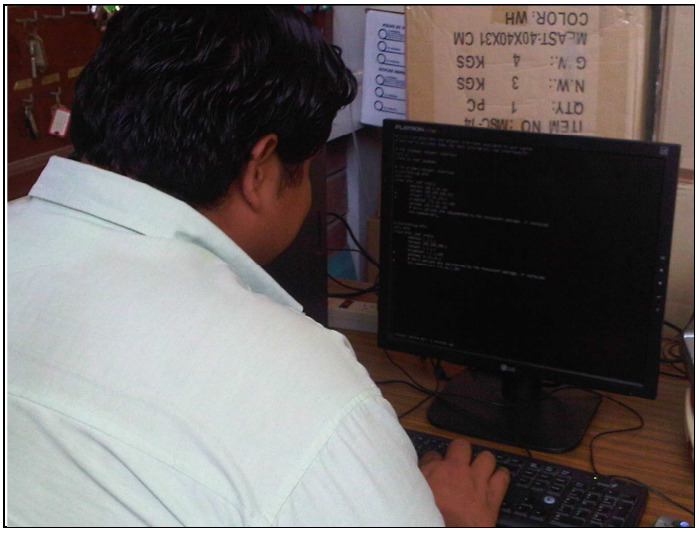


Figura 4.8 Instalación de túnel en Playas, servidor

4.2.4 Configuración del FIREWALL

Este proceso es para la seguridad y encriptación de la información que tendrán los dos puntos, en el subcapítulo 2.2 en lo que respecta a conceptualización de una VPN, se describió el concepto de firewall o cortafuegos, disponer de un firewall nos asegura tener un determinado control de accesos. Es algo similar al control de entrada y salida de la información a nuestra red.

Es como el cerramiento perimetral, más la barrera de accesos, más el servicio de vigilancia, todo en uno. Se procede a poner los siguientes comandos: , y direcciones aceptadas a la red; la configuración completa del firewall lo podrán ver en el anexo 3.

```
root@tesisplayasUEF:~# cd /etc/init.d/
root@tesisplayasUEF:/etc/init.d# nano firewall.sh
```

```
# squid server IP
SQUID_SERVER="192.17.1.1"
#RED
PRIVATE="192.17.1.1"
PUBLIC="186.3.39.130"
LOOP="127.0.0.1"
```

```
iptables -A INPUT -i tun+ -j ACCEPT
iptables -A FORWARD -i tun+ -j ACCEPT
iptables -A INPUT -i tap+ -j ACCEPT
iptables -A FORWARD -i tap+ -j ACCEPT
```

```
# Interface connected to Internet
INTERNET="eth0"
# Interface connected to LAN
LAN_IN="eth1"
# Squid port
SQUID_PORT="3128"
```

```
# Permitir pings entrantes (pueden desabilitarse)
iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT

# Permitir servicios tales como www y ssh (pueden desabilitarse)
iptables -A INPUT -p tcp --dport http -j ACCEPT
iptables -A INPUT -p tcp --dport ssh -j ACCEPT

# Puertos abiertos 80(web), 3128(proxy), 22 (SSH)
iptables -A INPUT -p tcp --dport 80 -j ACCEPT
iptables -A INPUT -p tcp --dport 3128 -j ACCEPT
iptables -A INPUT -p tcp --dport 22 -j ACCEPT
iptables -A INPUT -p tcp --dport 20:21 -j ACCEPT
```

```
## Establecemos politica por defecto
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -t nat -P PREROUTING ACCEPT
iptables -t nat -P POSTROUTING ACCEPT
```

```
# Abriendo el localhost (ejemplo conexiones locales a mysql)
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT

# Evitar que los paquetes externos usen la dirección de loopback
iptables -A INPUT -i $INTERNET -s $LOOP -j DROP
iptables -A FORWARD -i $INTERNET -s $LOOP -j DROP
iptables -A INPUT -i $INTERNET -d $LOOP -j DROP
iptables -A FORWARD -i $INTERNET -d $LOOP -j DROP

# A nuestra IP le dejamos todo
iptables -A INPUT -s $SQUID_SERVER -j ACCEPT

# Allow UDP, DNS and Passive FTP
iptables -A INPUT -i $INTERNET -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Figura4.9 Políticas de seguridad firewall en el servidor UEF

4.2.5 Instalación de Squid

Squid puede ser descargar como una fuente de calamar del archivo histórico en forma de bolas de alquitrán gzip (eg.squid-*- src.tar.gz) disponible en http://www.squid-cache.org/ o de ftp://www.squid-cache. org / pub calamares también se puede descargar como un archivo binario de http://www.squid-cache.org/binaries.html

comandos:

```
root@tesisplayasUEF:~# cd /etc/squid/
root@tesisplayasUEF:/etc/squid# ls
squid.conf
root@tesisplayasUEF:/etc/squid# nano squid.conf
```

Luego de abrir el fichero se procede a insertar las reglas para definir el proxy.

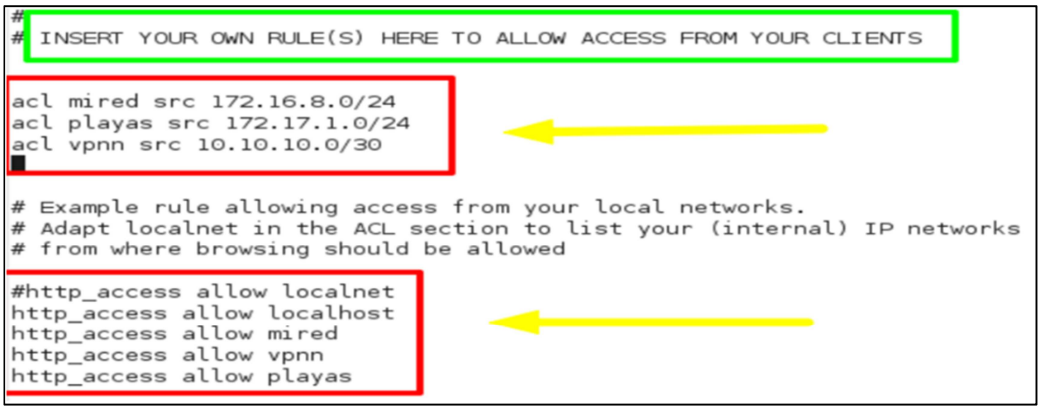


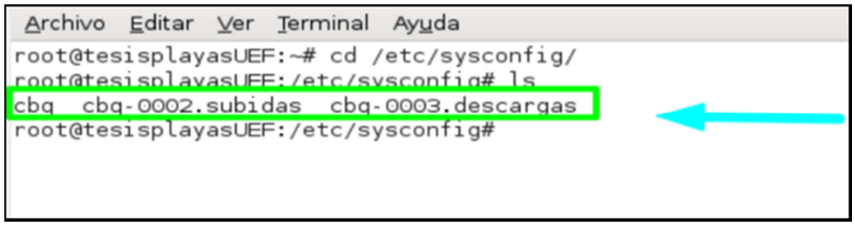
Figura 4.10 configuración del proxy

4.2.6 Configuración del CBQ

El uso de este limitador de ancho de banda, permite darle un límite de uso de conexión a cada computadora en la VPN, según corresponda. Si se necesita navegar y descargar archivos multimedia en los laboratorios de la unidad educativa lo más probable es que se necesite unos 512KB de velocidad de conexión. Mientras que otra computadora ejecuta una aplicación o un buscador web (firefox) solo necesitaría de

unos 128KB o menos para funcionar bien. De esta forma podremos tener operativa la red sin saltos de latencia.

Para la configuración del CBQ se utilizan la siguiente línea de comandos:



REGLAS DE SUBIDA

```
DEVICE=eth1,1Mbit
RATE=1024Kbit
WEIGHT=100Kbit
RULE=192.17.1.2,
RULE=192.17.1.3,
RULE=192.17.1.4,
```

REGLAS DE BAJADA

```
DEVICE=eth2,1Mbit
RATE=1024Kbit
WEIGHT=100Kbit
RULE=,192.17.1.2
RULE=,192.17.1.3
RULE=,192.17.1.4
```

4.2.7 Configuración de la red LAN de la UEF.

Para configurar las estaciones de trabajo primero hay que conectarlas a la red LAN de la UEF los detalles en la figura 4.12, 4.13

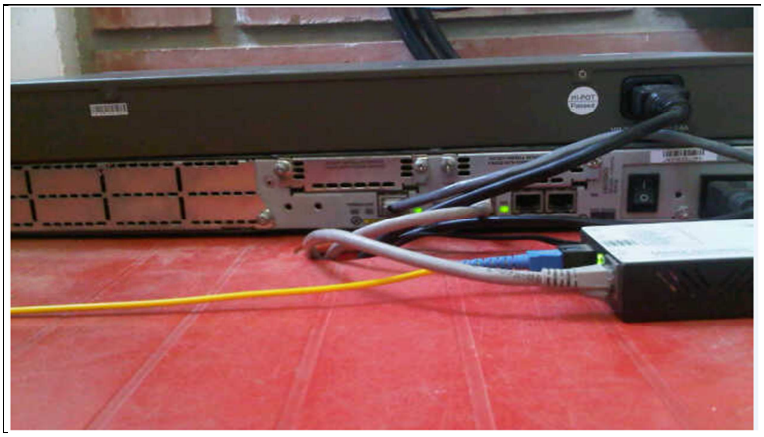


Figura 4.11 Convertidor óptico/eléctrico conectado al switch

Figura 4.12 Conexión del switch a las computadoras

Según la figura 4.14 se muestra la conexión inicial de puertos son 3 computadoras que estarán conectadas al SIU y aunque se conecte 4 computadoras solo las 3 tendrán acceso al SIU de la UCSG, después se hará el adecuado ordenamiento y fijación de un lugar seguro para el switch.

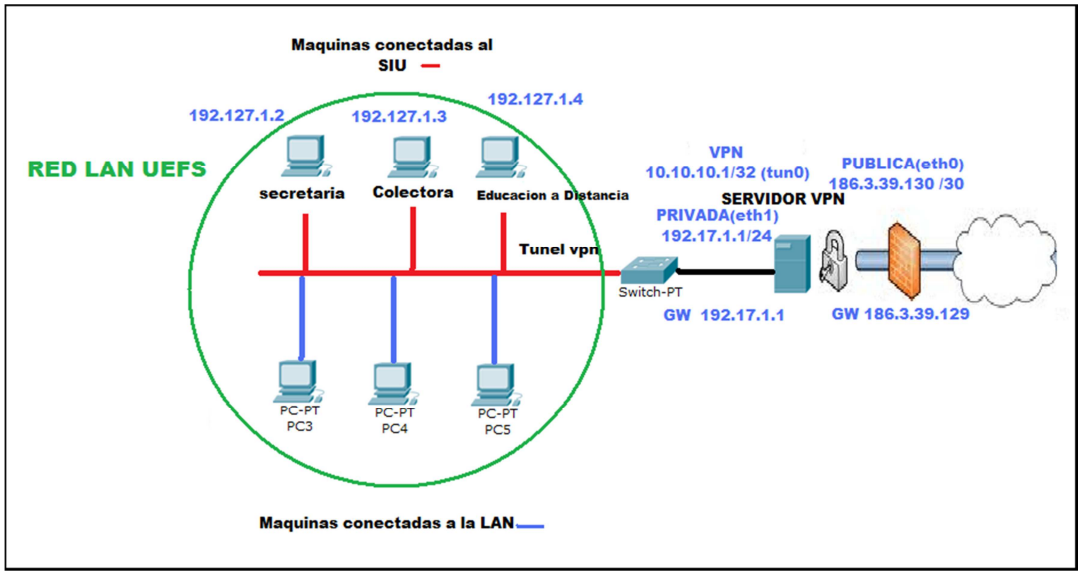


Figura 4.13Topología de la red VPN en la UEF

4.2.7.1 Configuraciones de las estaciones de trabajo

Para configurar las estaciones de trabajo que van a ingresar a la intranet (SIU) se realiza los siguientes pasos:

- Configuración de las direcciones IP
- Configuración de la red LAN (proxy)
- Se añaden las nuevas rutas en el HOST
- Se descarga el J2RE y se lo ejecuta como administrador.
- Se inicia el SIU con el nombre de usuario y password

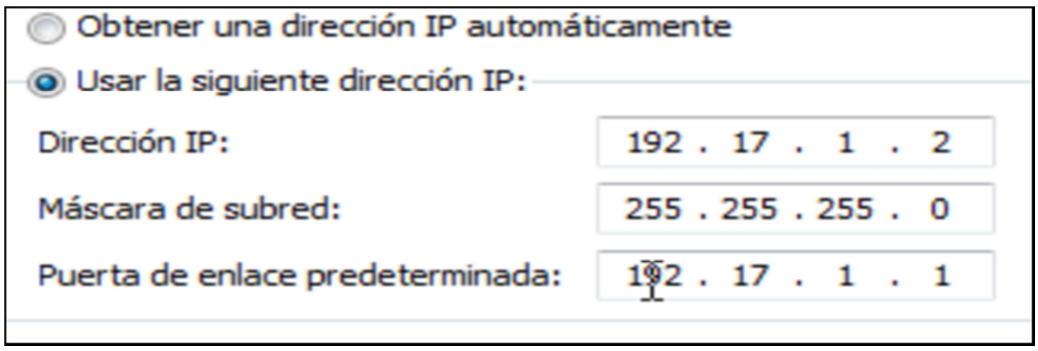


Figura 4.14 configuración de las direcciones IP asignadas a las estaciones de trabajo

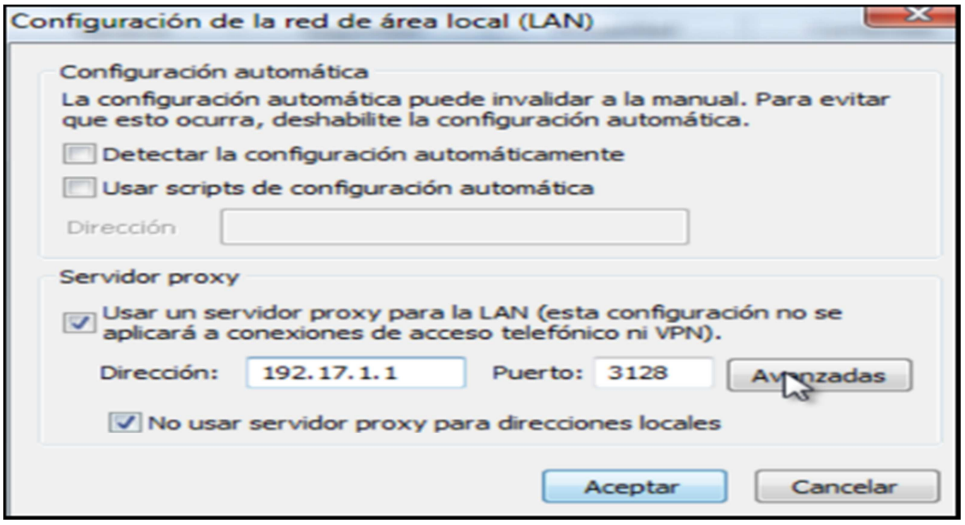


Figura 4.15 Configuración de la estación de trabajo a la LAN

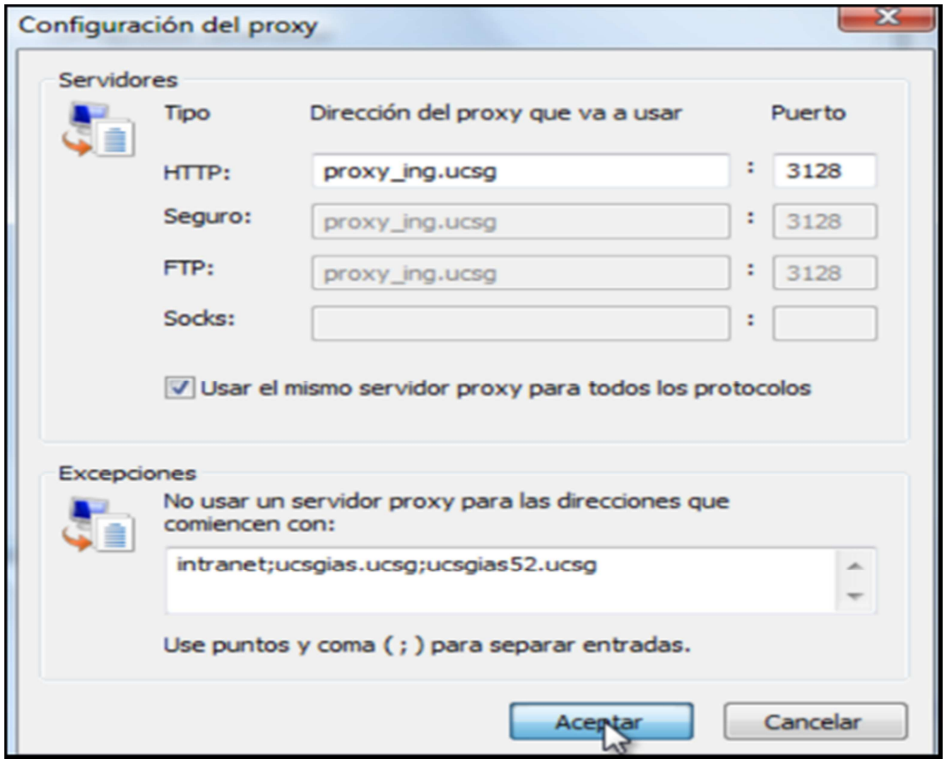


Figura 4.16 configuración del proxy de la estación de trabajo

Figura 4.17 ruta para abrir el archivo HOSTS

```
##ruta
#route -p add 172.16.1.0 mask 255.255.255.0 10.10.10.1
#
# Copyright (c) 1993-2006 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host
name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host
# route -p add  172.16.1.0 mask 255.255.255.0 10.10.10.1
127.0.0.1       localhost
172.16.1.18     intranet
172.16.1.130    ucsgias1.ucsg
172.16.1.128    ucsgias2.ucsg
::1             localhost
```

Figura 4.20 configuración de la ruta de encaminamiento.

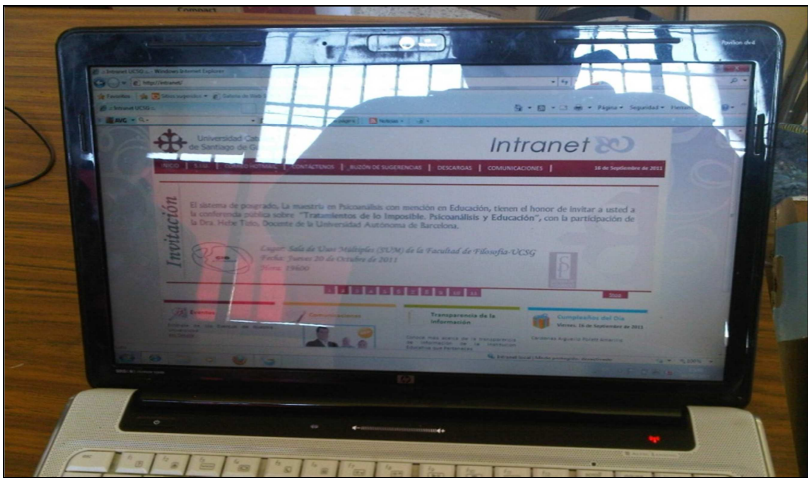


Figura 4.10 Instalación de Intranet UCSG en la UEF

Figura 4.20 página de inicio para acceder al SIU

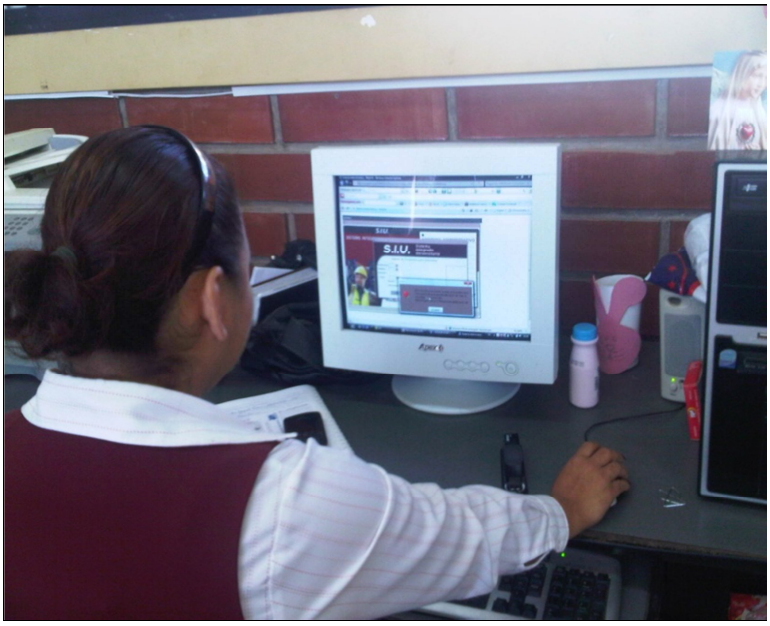


Figura 4.21 Instalación del SIU en computador de Secretaria- UEF

CONCLUSIONES:

Existen dos formas típicas de implementar una red privada virtual, basadas en hardwar*e* y en software respectivamente. En el fondo ambas soluciones implementan los mismos protocolos y soluciones típicas para construir redes privadas virtuales, aunque en distintos niveles.

Una solución práctica para comunicar directamente la UCSG y Freire Stabille en Playas fue utilizando una VPN, ya que la información administrativa y financiera es competencia solo de, los empleados de la UCSG. Otras soluciones serian de proveer de un enlace de internet sea satelital, vía microondas, vía fibra óptica desde la UCSG y Freire Stabille y eso es muy costoso y demanda estudios de propagación amplios.

Una vez establecida la conexión de la red privada virtual entre la UCSG y Freire Stabille los datos viajan encriptados de forma que sólo el emisor y el receptor son capaces de leerlos.

La velocidad de comunicación entre la UCSG y Freire Stabille es óptima y confiable gracias a la robustez de OpenVPN y en cuanto al ancho de banda por medio de la aplicación sharper se puede asignar diferentes velocidades a las computadoras de la unidad educativa Freire Stabille.

RECOMENDACIONES

La operatividad de la conexión al S.I.U desde la UCSG, hasta la unidad educativa Freire Stabille debe ser monitoreada desde el centro de cómputo de la UCSG, para así garantizar el servicio permanente libre de suspensiones en el servicio.

La red privada virtual debe ser supervisada por profesionales idóneos con formación telecomunicaciones, analistas de sistemas, de programación; de ellos depende que la implementación siempre brinde la conectividad del SIU en la unidad educativa Freire Stabille.

Esta plataforma tecnológica incluye: sistemas de información, base de datos relacional (repositorio de información) y un conjunto actualizado de equipos informáticos; que solo debe ser operado por parte de personal administrativo de la UCSG que labore en la unidad educativa.

Es posible instalar más computadoras al SIU desde la unidad educativa Freire Stabille, siempre y cuando deben hacerlo saber a centro de cómputo de la UCSG, quienes tienen la autoridad para realizarlo.

BIBLIOGRAFIA:

Amato, Vito: Academia de Networking de Cisco Systems: Guía del primer año. Ed. Cisco Press, 2000. ISBN 1-57870-218-6

Amato, Vito: Programa de la Academia de Networking de Cisco: Guía del segundo año. Ed. Cisco Press, 2001. ISBN 1-578713-002-5

Alegre, M. (2010). *Sistemas operativos monopuestos* . Madrid: Paraninfo.

Ania, I., & Gomez de Silva, A. (2008). *Introducción a la computación.* Mexico: Cengage Learning.

Corrales, A., Beltrán, M., & Guzmán, A. (2006). *Diseño e implantación de arquitecturas informáticas seguras: Una aproximacion practica.* Madrid: Dykinson.

Gil, P., Pomares, J., & Candelas, F. (2010). *Redes Y Transmision De Datos.* Alicante: Publicaciones de la Universidad de Alicante.

Kolesnikov, O., & Hatch, B. (2002). *Building Linux Virtual Private Networks (VPNs).* New York: New Rider Publishing.

Martin, M. (2001). *De Windows a Linux: para distribuciones Red Hat y SuSE* . Barcelona: Marcombo.

Mason, A. (2002). *Cisco secure virtual private networks.* Michigan: Cisco Press.

Mathon, P. (2004). *Windows Server 2003: servicios de Red TCP/IP* . Barcelona: Ediciones Eni .

Pellejero, I., Andreu, F., & Lesta, A. (2006). *Fundamentos y aplicaciones de seguridad en redes WLAN.* Barcelona: Marcombo.

Pons, N. (2009). *Linux:Principio básico del uso del sistema.* Barcelona: Ediciones Eni.

Sanchez, A. (2002). *Windows Xp Avanzado* . Málaga: Antakira Grafic.

REFERENCIA EN LA WEB

*http://diversistemas.com/2011/08/06/distribuciones-gnu-linux-principales-debian-gnu-linux-hurd-o-kfreebsd/ recuperado: 27 de Septiembre del 2011

*http://www.lugro.org.ar/biblioteca/articulos/introvpn.pdf Recuperado: 27 de Septiembre del 2011

*http://tuxjm.net/docs/Creacion_de_Redes_Privadas_Virtuales_en_GNU_Linux_con_OpenVPN/html-onechunk/#id536375 Recuperado: 28 Septiembre del 2011

*http://www.debian.org/devel/debian-installer/ Recuperado: 28 septiembre del 2011

ANEXOS

ANEXO 2: Instalación completa Debian 6

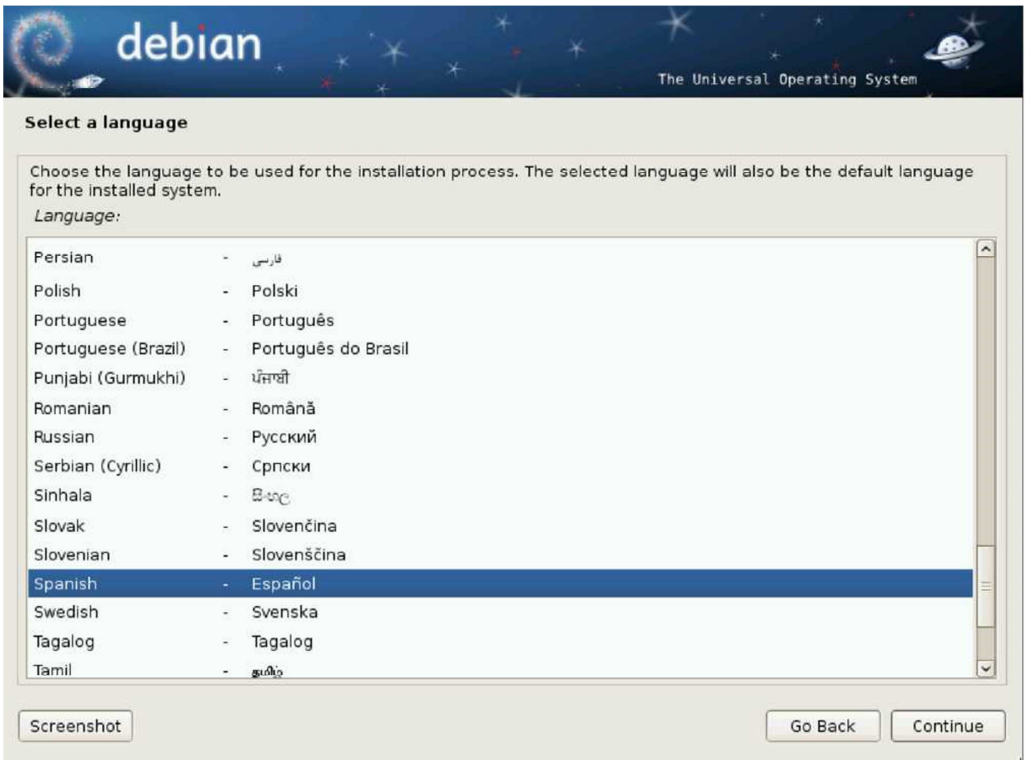
Aquí podemos escoger entre varias opciones:

- Install (Inicia el asistente de instalación sin gráficos, digamos que a modo de consola).
- Graphical install (Es el que vamos a utilizar, iniciar el asistente de instalación con gráfico).
- Advanced Options (Para realizar instalaciones avanzadas).
- Help (Ayuda sobre el asistente de instalación y otras opciones).

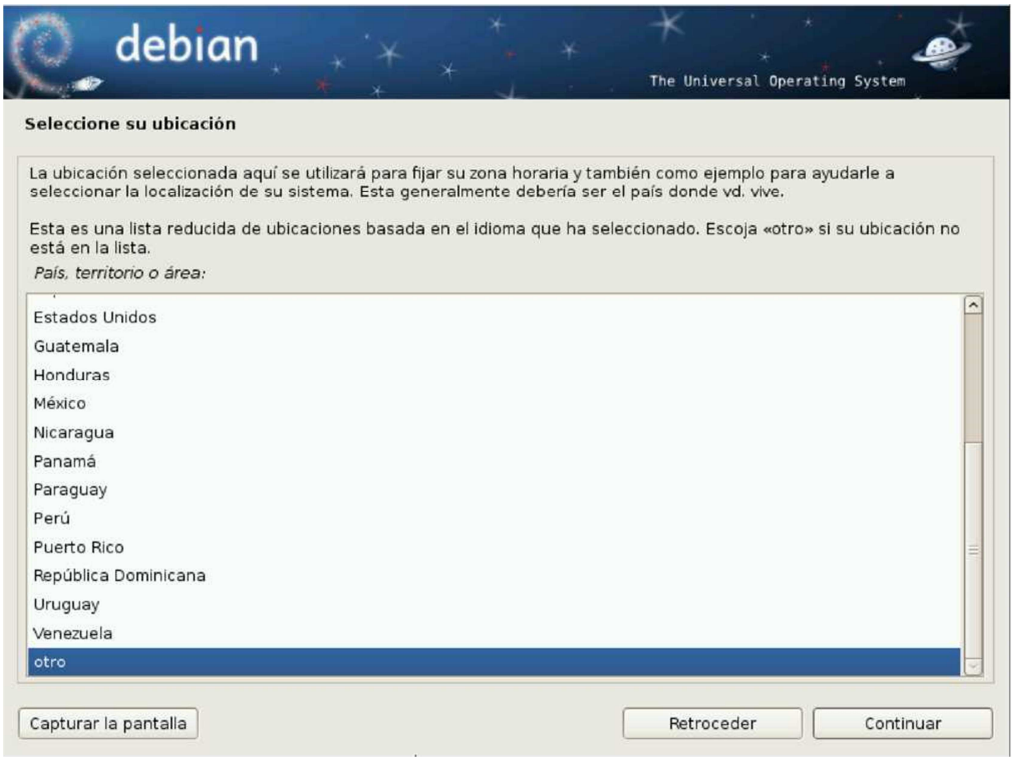
Escogemos la opción Graphical install como les dije anteriormente y nos disponemos a instalar nuestro sistema. Si nuestro equipo es de recursos limitados, podemos utilizar la opción Install que es lo mismo, pero no carga gráfico alguno, ni tampoco el cursor.

Seleccionando el idioma.

El primer paso es seleccionar nuestro idioma ya que por defecto se instalará en inglés. En este proceso no hay mucho que aclarar. Voy a realizar la instalación en Español para que el asistente muestre su ayuda y al propio asistente en este idioma. Seleccionamos Spanish y hacemos clic en Continue.

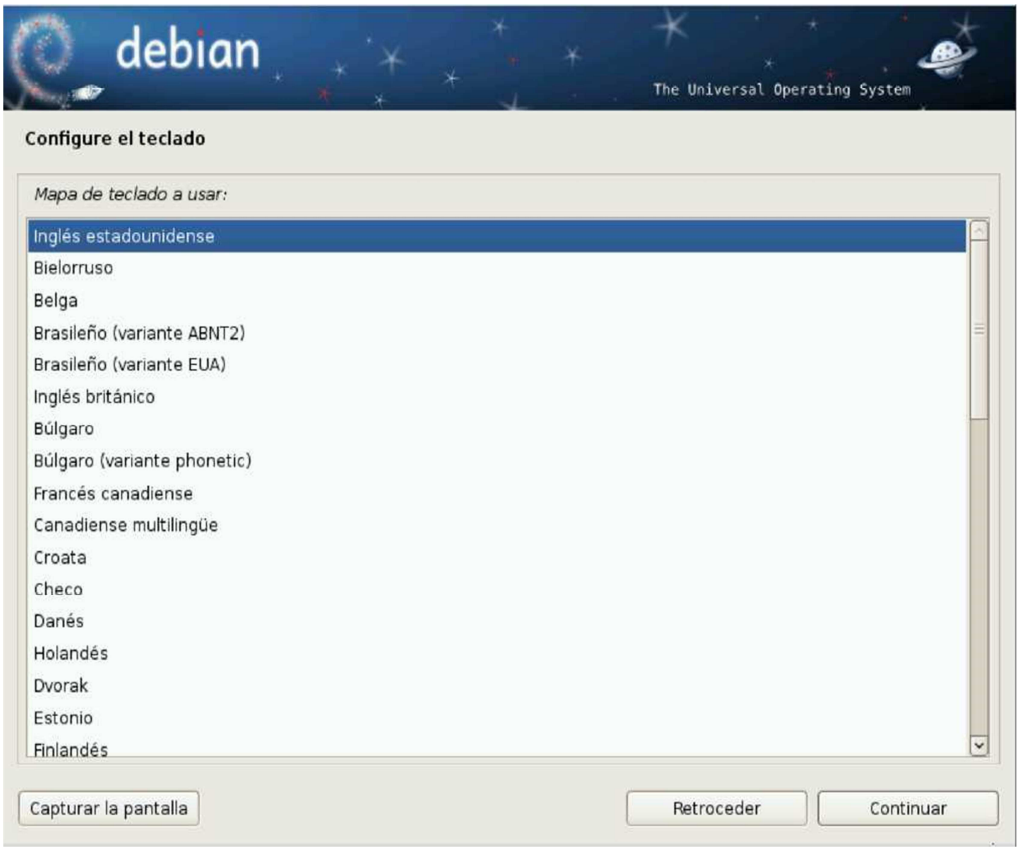


Las siguientes diapositivas nos pide seleccionar el área o región donde vivimos.



Luego el asistente nos pide que seleccionemos una localización para el idioma. En este caso como la instalación es en español, selecciono España. Esto es para los locales es_ES.utf8 del sistema.

Seleccionamos la configuración de nuestro teclado, en mi caso el mío está en Inglés. Aunque el instalador no nos brinda escoger una variante de teclado :(Por ejemplo, yo uso el teclado en Inglés con teclas muertas, así de esta forma puedo tener la letra Ñ con el atajo de teclado Alt Gr + N.

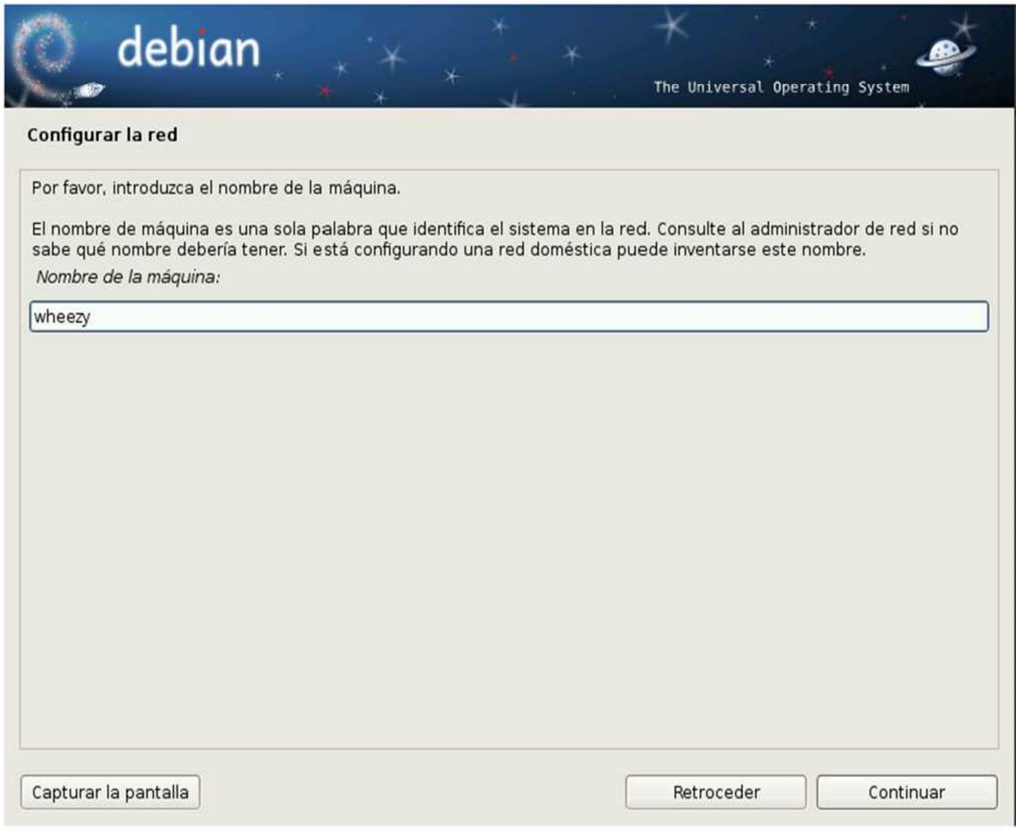


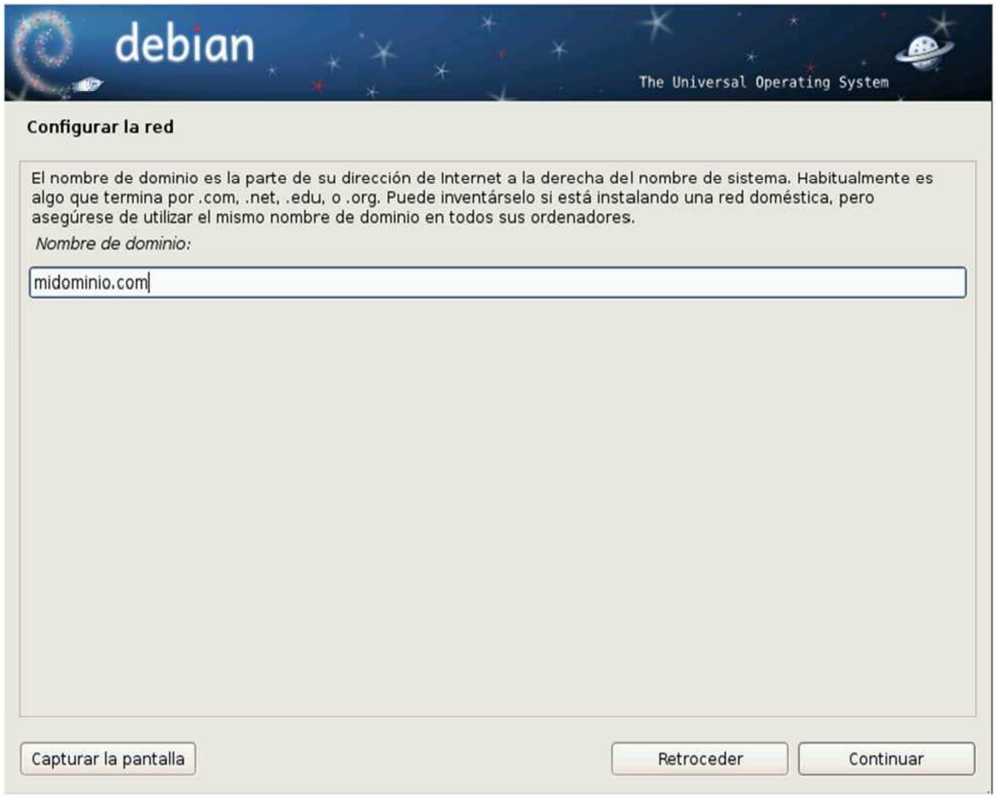
Luego nos toca configurar la red. Con VirtualBox por defecto nos toma nuestra PC (anfitrión) como servidor DHCP. Como es lógico esto se puede establecer manualmente, aunque por lo general, este proceso no es necesario en las demás partes del mundo.

Si cancelamos esta parte y establecemos los datos manualmente, tendremos que poner nuestra IP, la máscara de red, el gateway y el servidor DNS de nuestra preferencia.

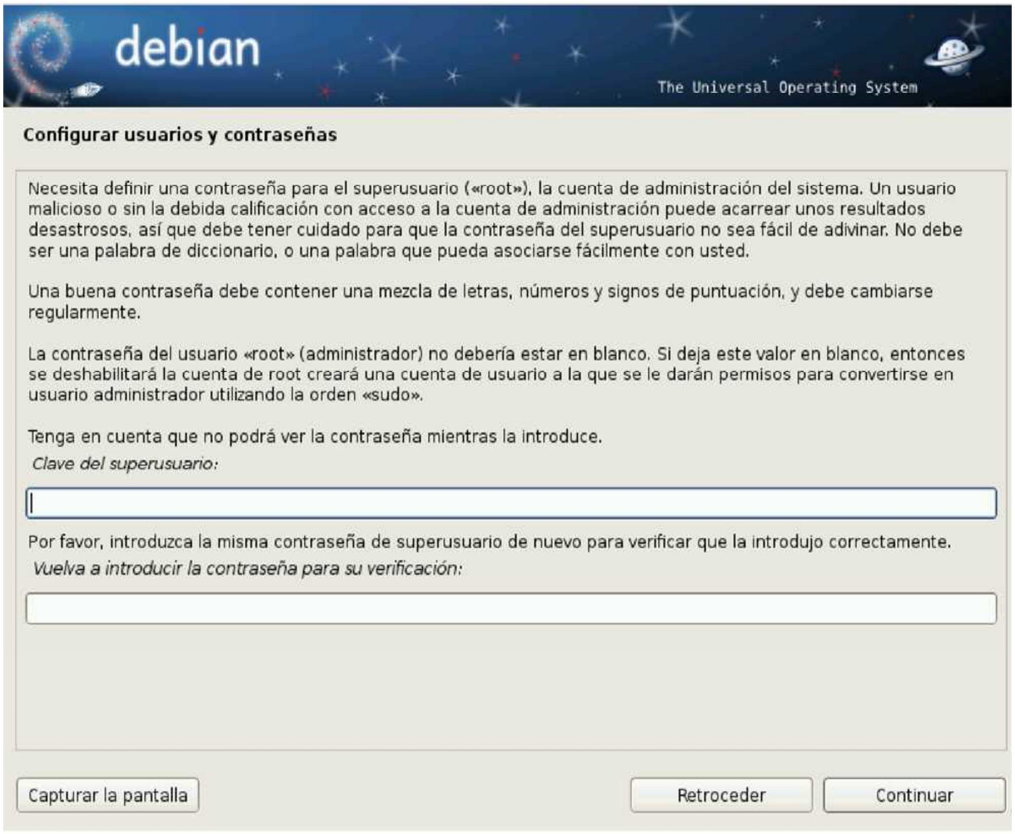
Terminando este proceso lo que nos toca es configurar el nombre de nuestra PC (Host), la contraseña de root, nuestro nombre de usuario y el dominio al que pertenecemos (en caso de estar dentro de uno).

El asistente explica bastante bien para que es cada cosa, de ahí mi criterio de que Debian es muy fácil de instalar. Pueden tomar como ejemplo la imagen posterior, donde se explica muy bien que cosa es el nombre de la máquina (host).
Establecemos el nombre de nuestra PC y el dominio al que pertenecemos.





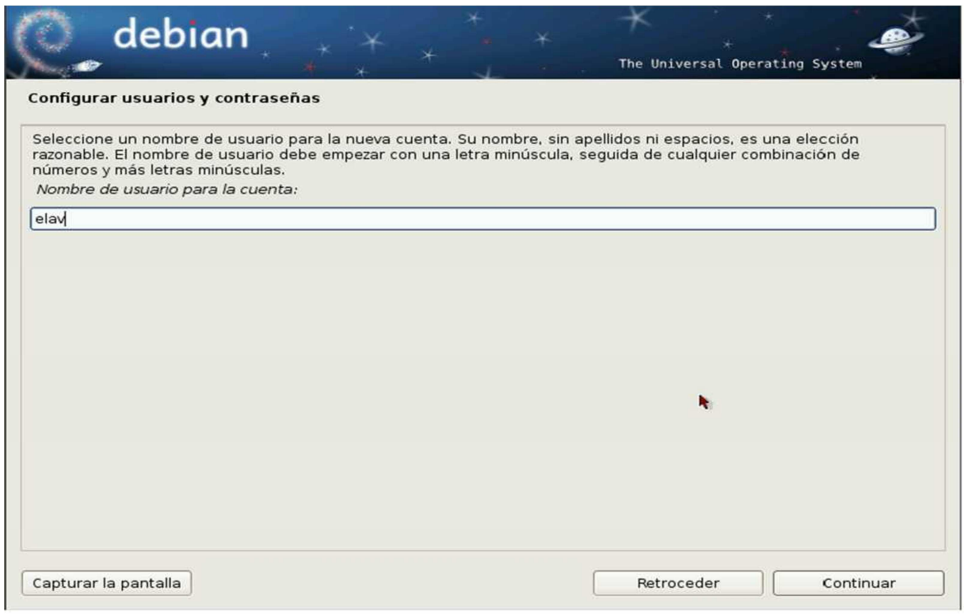
Ahora nos toca poner la clave de root. Es importante que esta clave sea segura y que no la olvidemos ya que sin ella no podremos realizar ninguna tarea administrativa, además por cuestiones de seguridad debe ser una clave fuerte, por lo que es recomendable hacer uso de símbolos, espacios y letras en mayúsculas y minúsculas.
También, como indica la ayuda del asistente, tenemos la opción de dejarla en blanco, por lo que usaremos nuestro usuario con privilegios administrativos como en Ubuntu, usando "sudo".

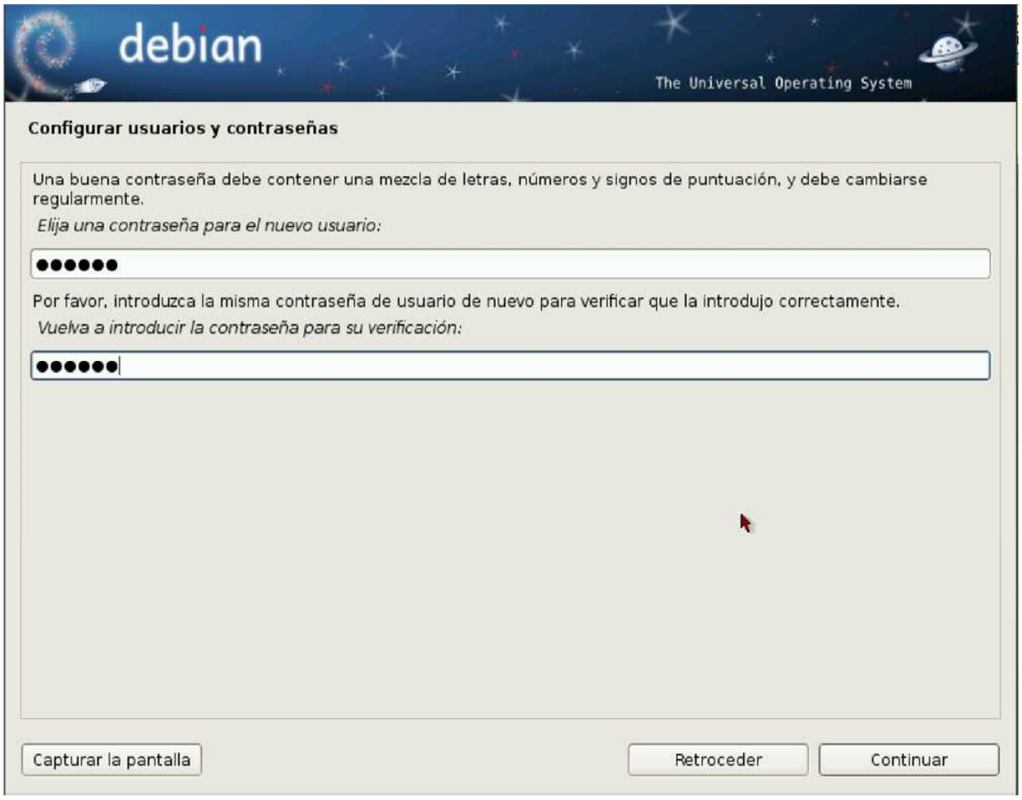


Posteriormente introducimos nuestro nombre real completo, el cual usará el sistema como nombre predeterminado a la hora de configurar nuestras cuentas de correo o de mensajería.. El nombre completo nada tiene que ver con el usuario.

El nombre de usuario, será el nombre de nuestra carpeta en nuestro /home. En este caso mi usuario tendré mis configuraciones en /home/elav/. Si alguna vez tenemos que formatear nuestro PC, a la hora de configurar nuestro usuario, si queremos tener las mismas configuraciones, debemos poner el mismo usuario aunque el nombre completo sea diferente.


debian
The Universal Operating System
Configurar usuarios y contraseñas
Se creará una cuenta de usuario para que la use en vez de la cuenta de superusuario en sus tareas que no sean administrativas.
Por favor, introduzca el nombre real de este usuario. Esta información se usará, por ejemplo, como el origen predeterminado para los correos enviados por el usuario o como fuente de información para los programas que muestren el nombre real del usuario. Su nombre completo es una elección razonable.
Nombre completo para el nuevo usuario:
Ernesto Acosta
Capturar la pantalla
Retroceder
Continuar


debian
The Universal Operating System
Configurar usuarios y contraseñas
Seleccione un nombre de usuario para la nueva cuenta. Su nombre, sin apellidos ni espacios, es una elección razonable. El nombre de usuario debe empezar con una letra minúscula, seguida de cualquier combinación de números y más letras minúsculas.
Nombre de usuario para la cuenta:
elav
Capturar la pantalla
Retroceder
Continuar



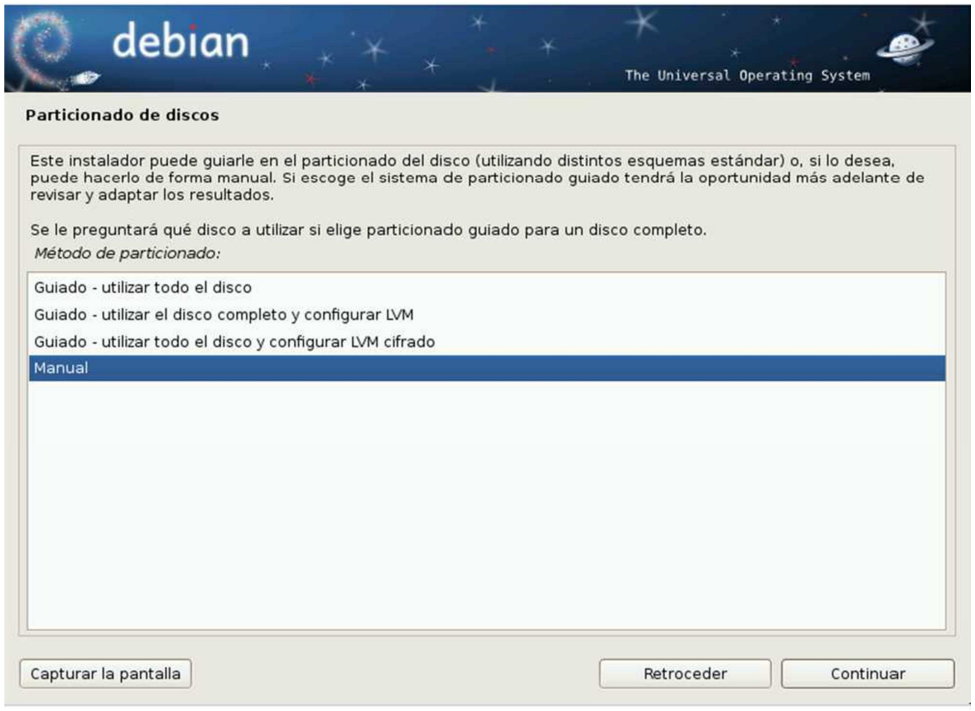
Establecemos nuestra contraseña de usuario. Si no establecemos un password para root, entonces esta contraseña será la misma que utilizaremos para administrar nuestro sistema, recordando siempre hacer uso del "sudo", aunque en Debian esto no es muy común.

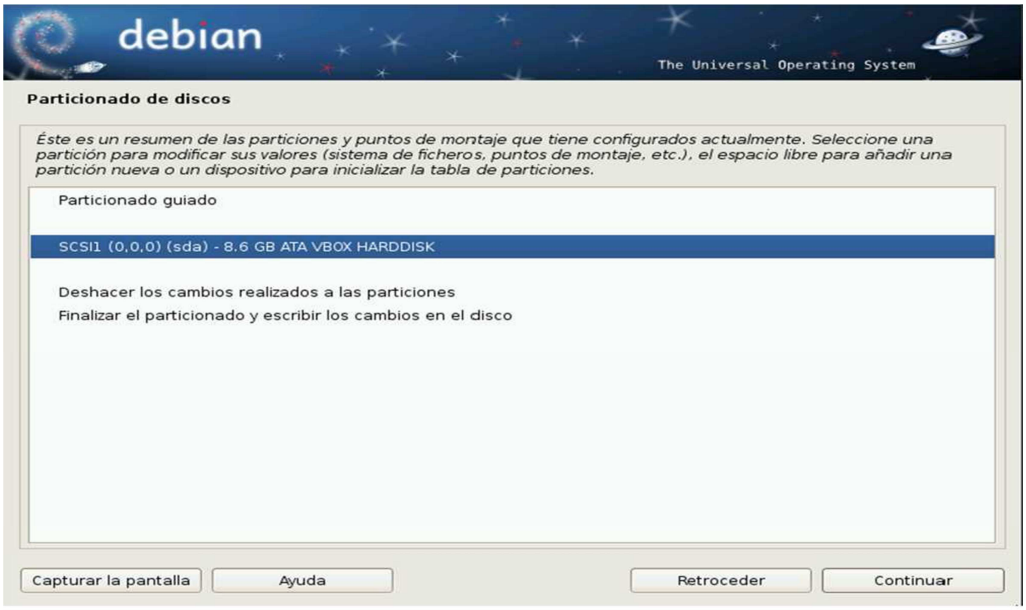
Terminado esta parte nos toca ahora particionar nuestro disco duro. Para este ejemplo como es lógico usé VirtualBox, donde cree un disco de 8Gb para la instalación del sistema completo. La partición se puede realizar de diversas formas. Yo siempre creo 3 particiones:

# de Partición	Punto de Montaje	Tipo de Partición	Orden de Partición
1	/	Primaria	Principio
2	/home	Lógica	Principio
3	swap	Lógica	Principio o Final

Así lo hago yo. Pero puede hacerlo como desee, dejando de separar la partición /home o incluso no estableciendo swap, pero siempre tiene que declarar la partición /. También sería bueno leer estas recomendaciones para tener una mejor idea del proceso de particionado.

Llegamos al proceso de particionado y veremos algo como en la imagen posterior. Si hacemos una instalación sobre otra instalación, ya tendremos nuestras particiones creadas, pero en el caso de VirtualBox como instalo desde cero, tengo que crearlas manualmente.





Seleccionamos la opción Manual. Sería más fácil para un usuario normal utilizar el Particionamiento Guiado, el cual le creará automáticamente sus particiones, incluso les separa la partición /home para que no pierda sus datos, pero hay que tener cuidado con esa opción, porque si no estamos seguros de lo que hacemos, podemos borrar otras particiones creadas.

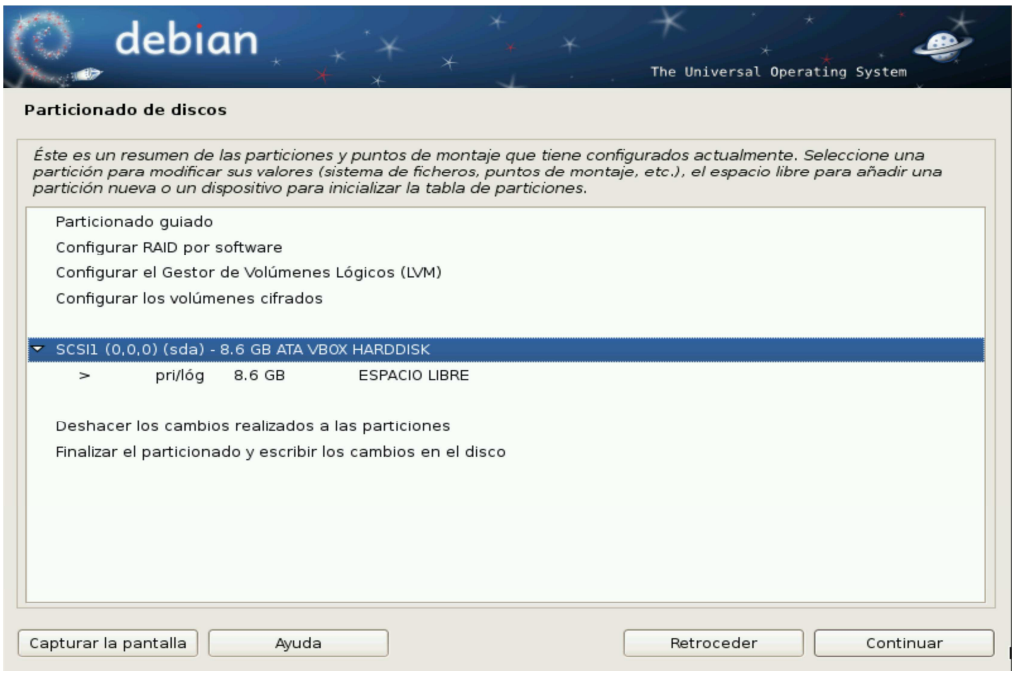
Si se fijan en la imagen anterior, como nuestro disco es virgen no tiene creada una tabla de particiones válida, por lo que tenemos que hacerla. Es muy sencillo, solo nos paramos (en mi caso) sobre:

SCSI1 (0,0,0) (sda) - 8.6 GB ATA VBOX HARDDISK

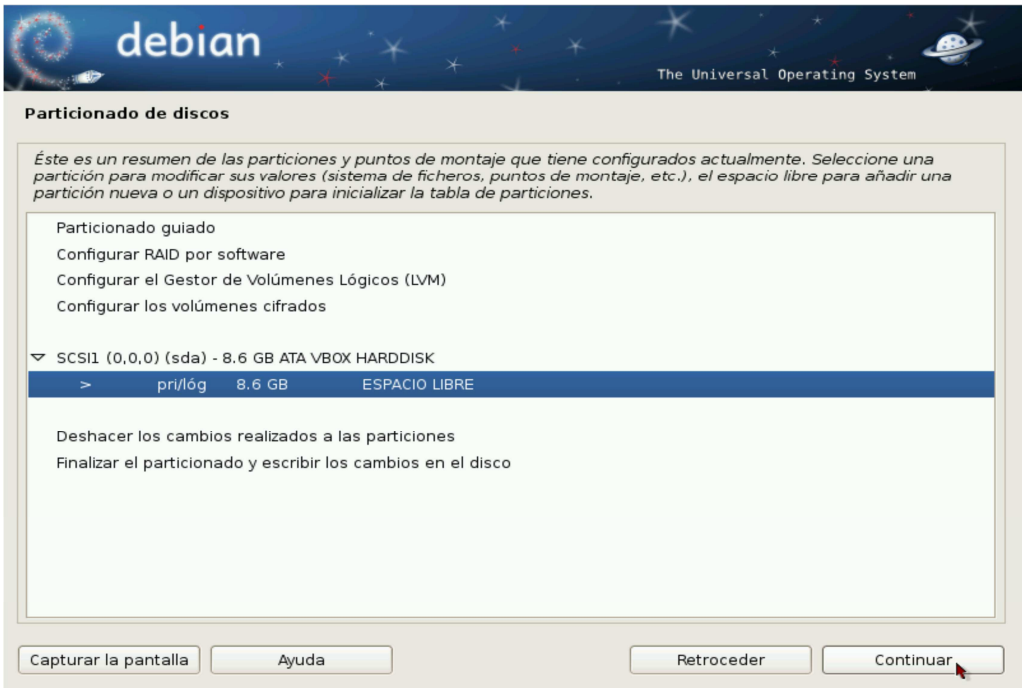
Y le damos al botón de continuar.

No pregunta si queremos crear una nueva tabla de particiones en el dispositivo seleccionado y seleccionamos la opción "Si".

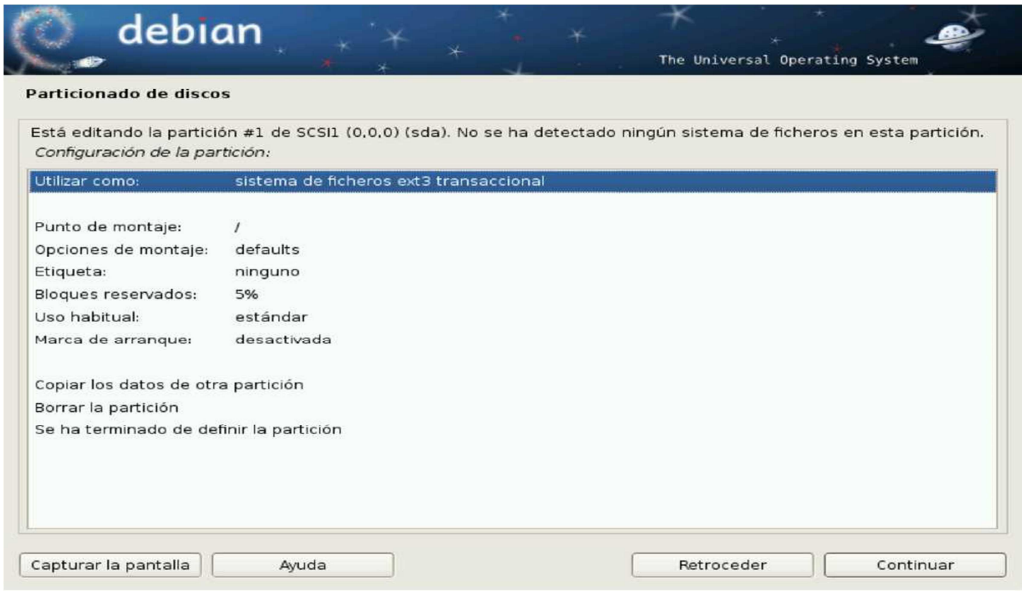
Le damos clic al botón de Continuar y nos debe mostrar el disco de la siguiente forma:

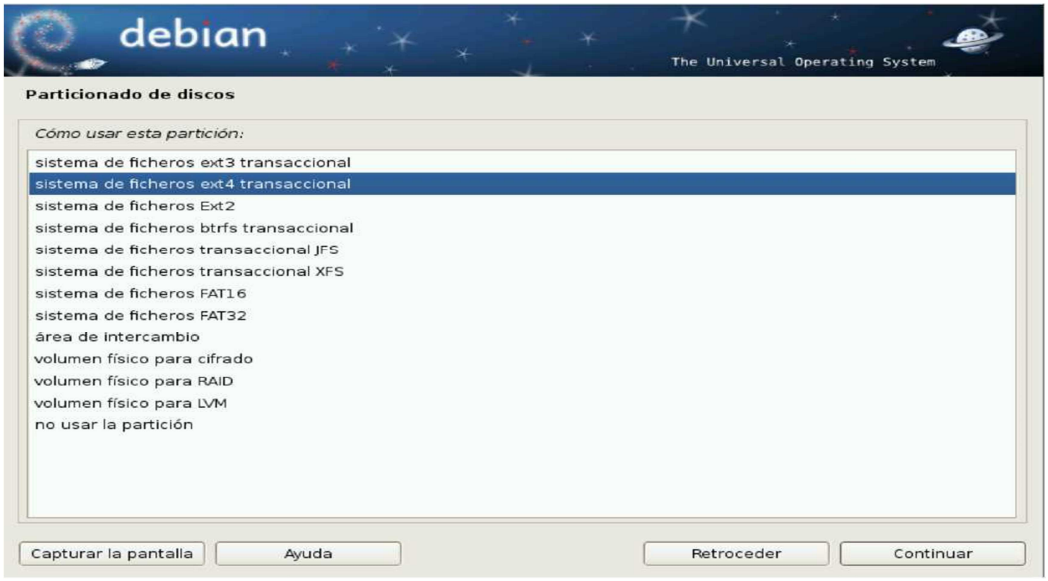


Ahora la primera partición la crearemos sobre el ESPACIO LIBRE.

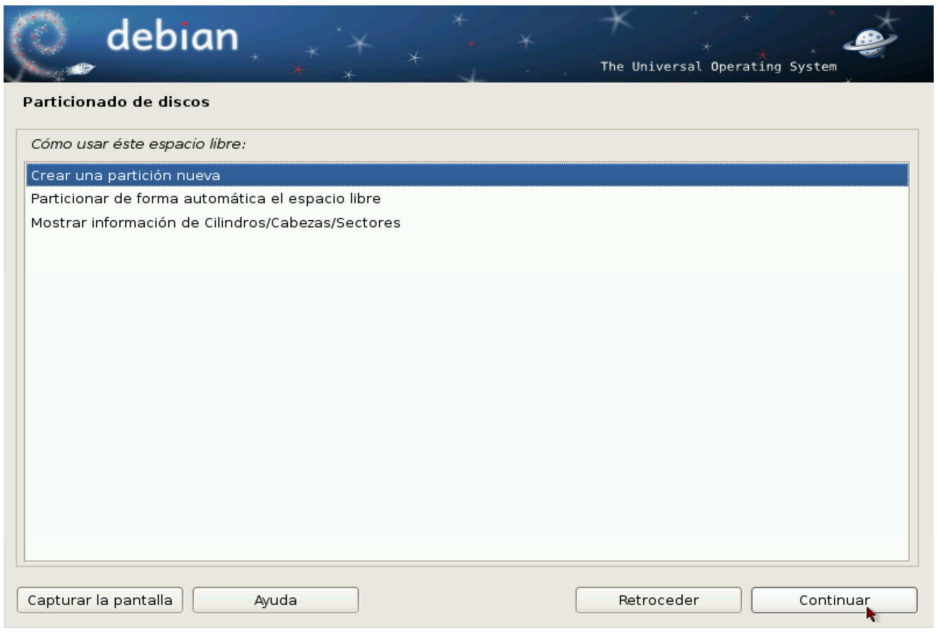


Ahora un paso importante. Por defecto Debian nos crea la partición en Ext3, pero podemos hacer uso de Ext4 que es mucho mejor. Sencillamente seleccionamos la opción Utilizar como y hacemos clic en Continuar para escoger Ext4.





La primera partición es la /. Hacemos clic en Siguiente y seguimos los pasos como se muestran en las imágenes a continuación.Creamos



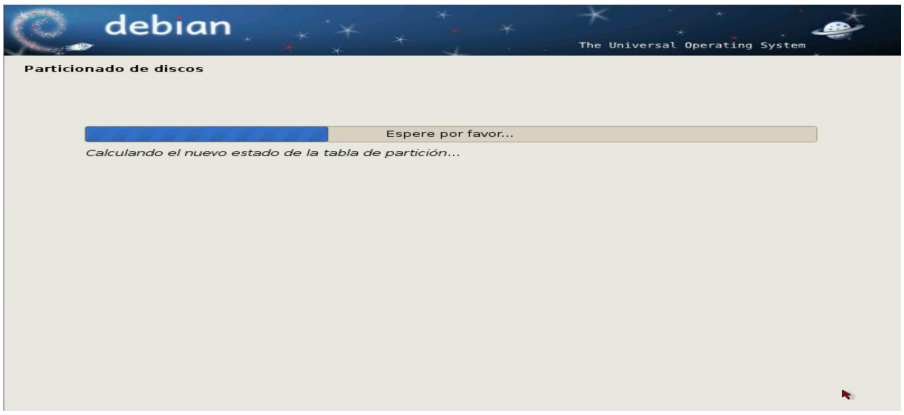
Creamos una partición automática.

El instalador de Debian nos permite mover las particiones por el disco mientras las vamos creando.

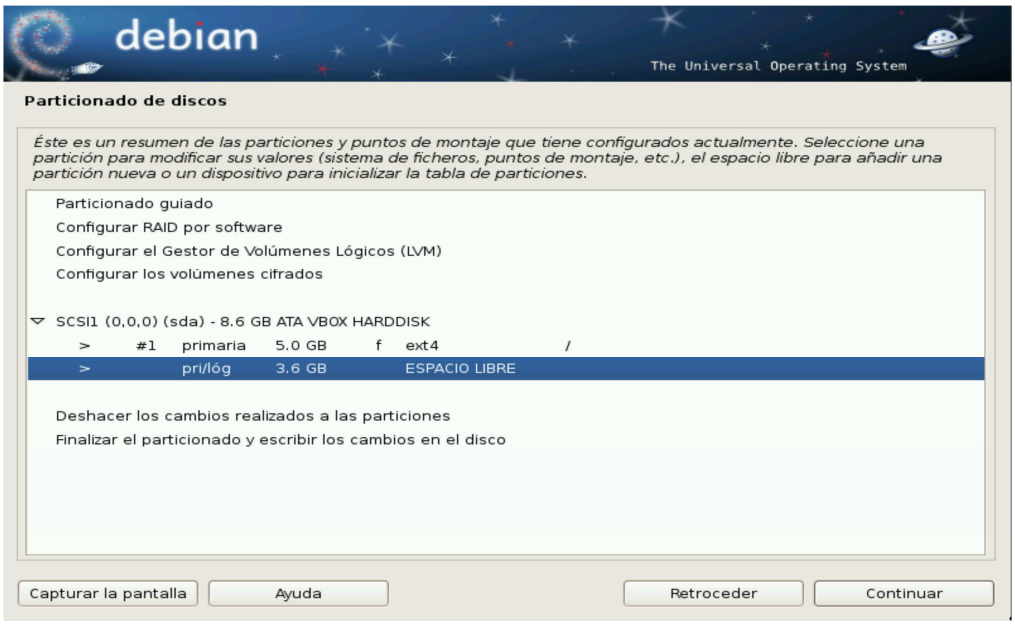
Ud puede, por ejemplo, crear la partición /home, swap, /usr o /var y ponerla al final del disco (final) o a continuación de la última partición creada (principio).

Esto es bueno saberlo sobre todo a la hora de distribuir la capacidad de cada partición. Yo por ejemplo, si tengo duda en el espacio que me quedará para la Swap o la partición /home después de creada la partición /, primero creo la Swap con 1Gb digamos, y la muevo al final, así el espacio restante queda para el /home y se coloca a continuación de la /.

Esto es algo que con el tiempo van aprendiendo los nuevos usuarios. Así que no es necesario entenderlo a la primera.



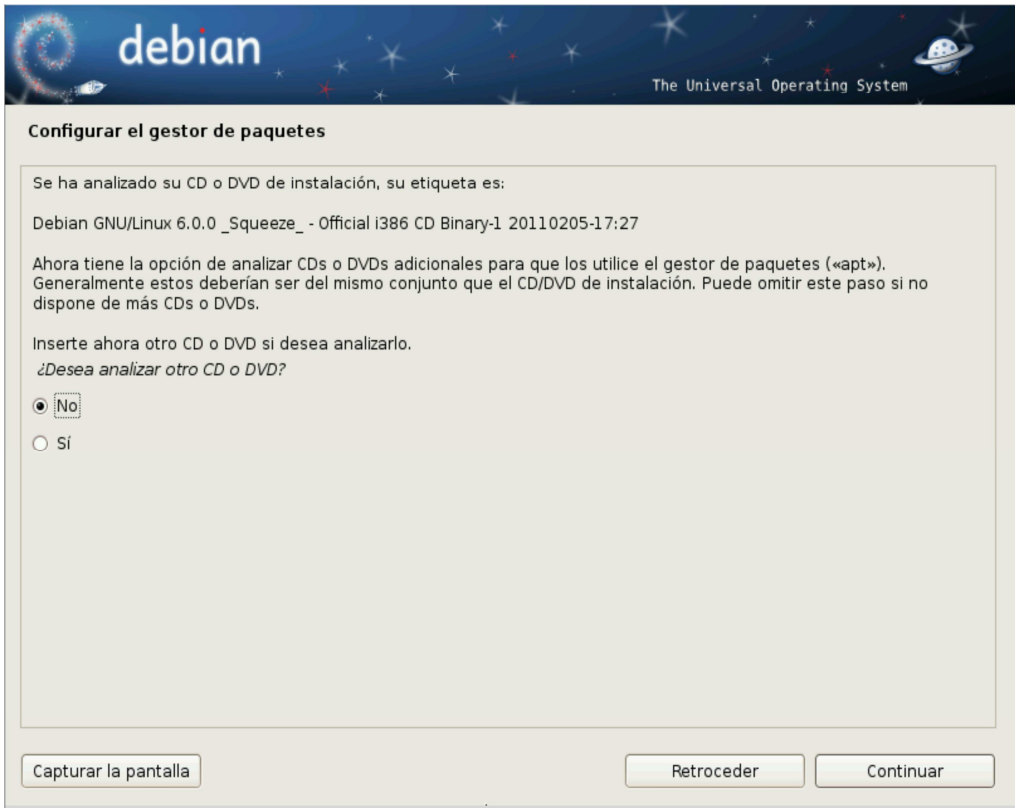
Nos quedaría de la siguiente forma:



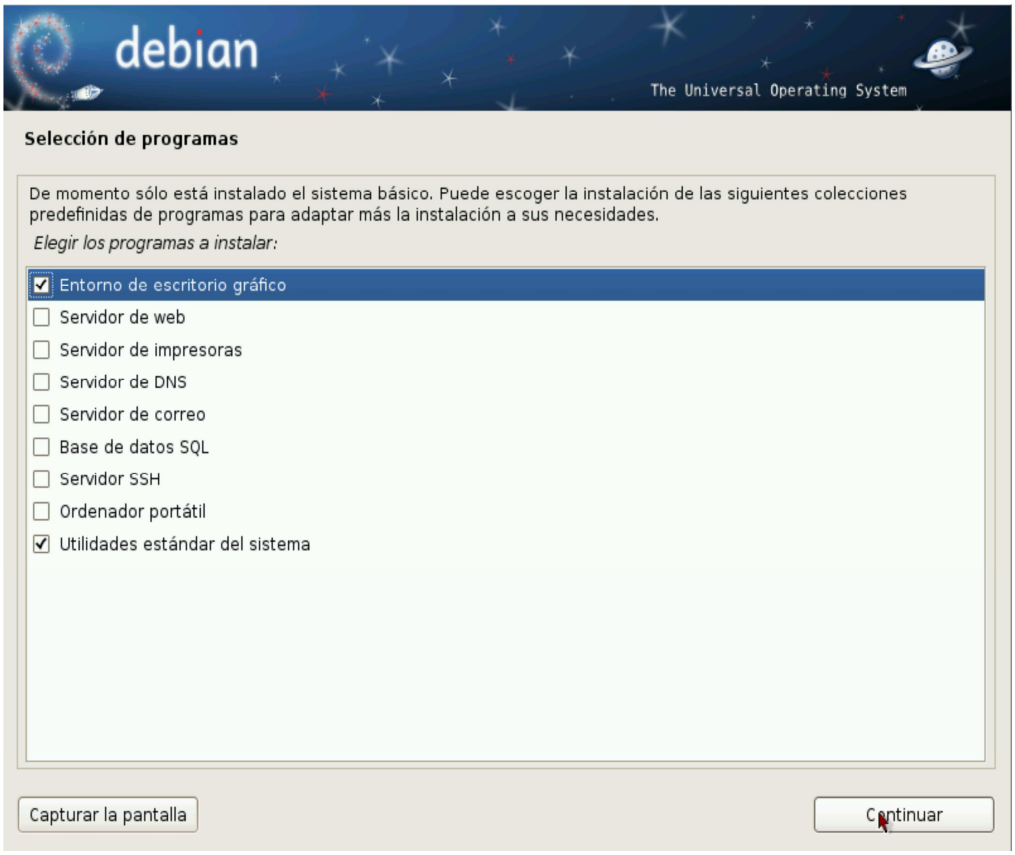
En el momento que aceptamos, el instalador formatea el disco duro con nuestras preferencias y comienza a preparar el sistema para la instalación. Luego nos pregunta

si queremos instalar desde otro CD o DVD (en este caso no) y si queremos usar una réplica de red (en este caso no). También podremos escoger si queremos enviar estadísticas semanales sobre los paquetes que más usamos.

Todo esto (que mostraré en las imágenes a continuación) hasta llegar a la opción de lo que queremos instalar ya sea una PC de escritorio o un servidor.



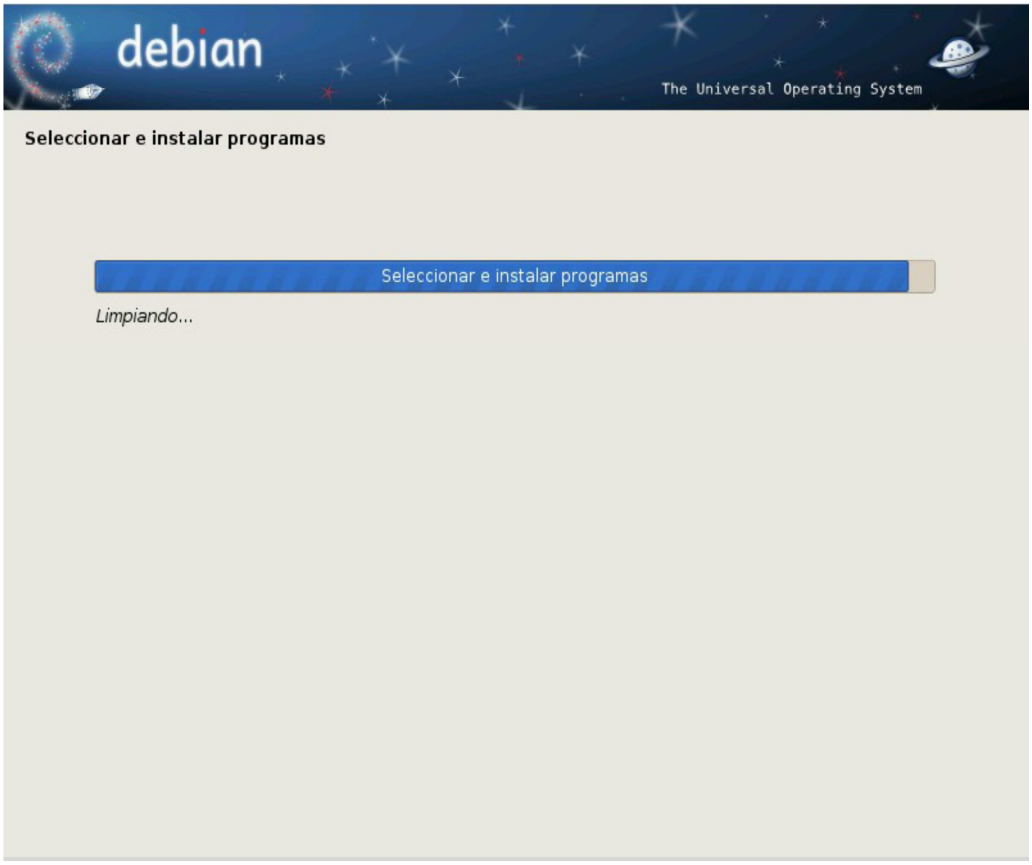
Ahora llegaremos a esta pantalla:



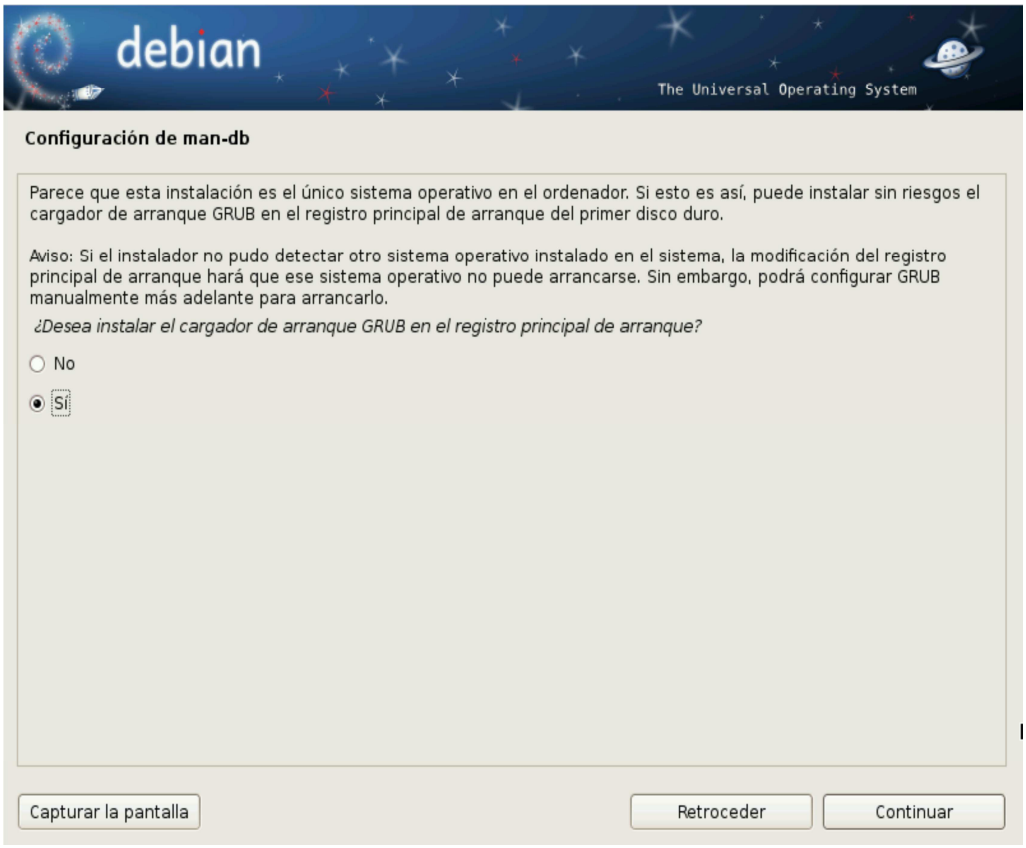
Por defecto Debian instalará el entorno de escritorio Gnome (en este caso) con algunas utilidades estándart del sistema. Si tenemos experiencia con la instalación de Debian podemos desmarcar la primera opción, para posteriormente instalar lo que querramos. Si eres nuevo, es recomendable que lo dejes por defecto.

También podemos apreciar las opciones para instalar servidores con diferentes servicios e incluso, los paquetes necesarios si nuestro equipo es un portátil. Hacemos clic en Continuar y el sistema se empieza a instalar. Esto toma un poco de tiempo, así

que le recomiendo que aproveche para tomarse un café, ir al baño o responder los mensajes del móvil

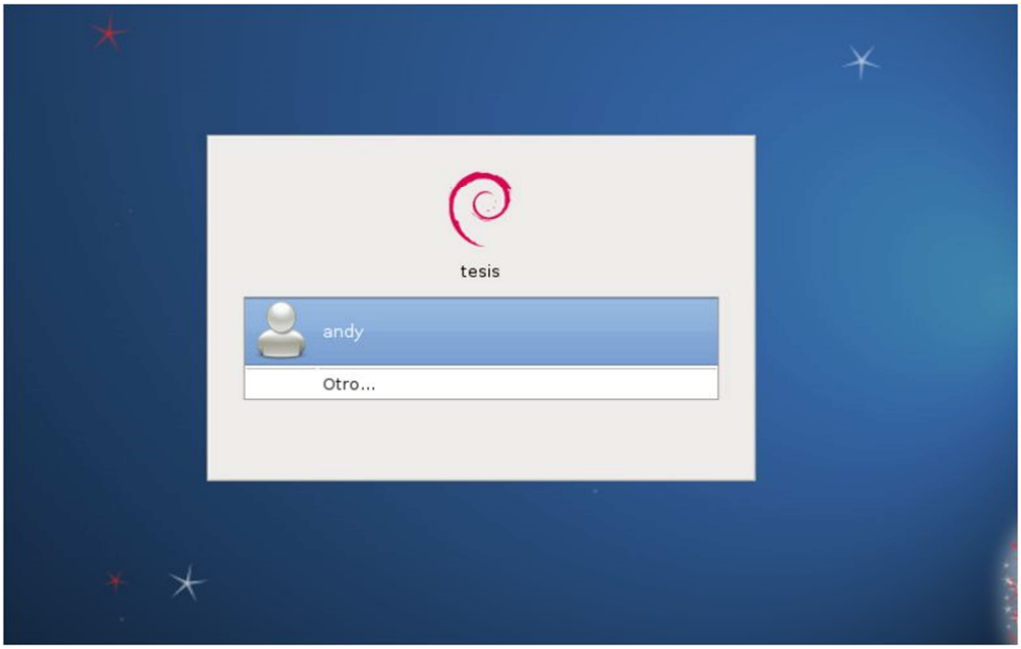


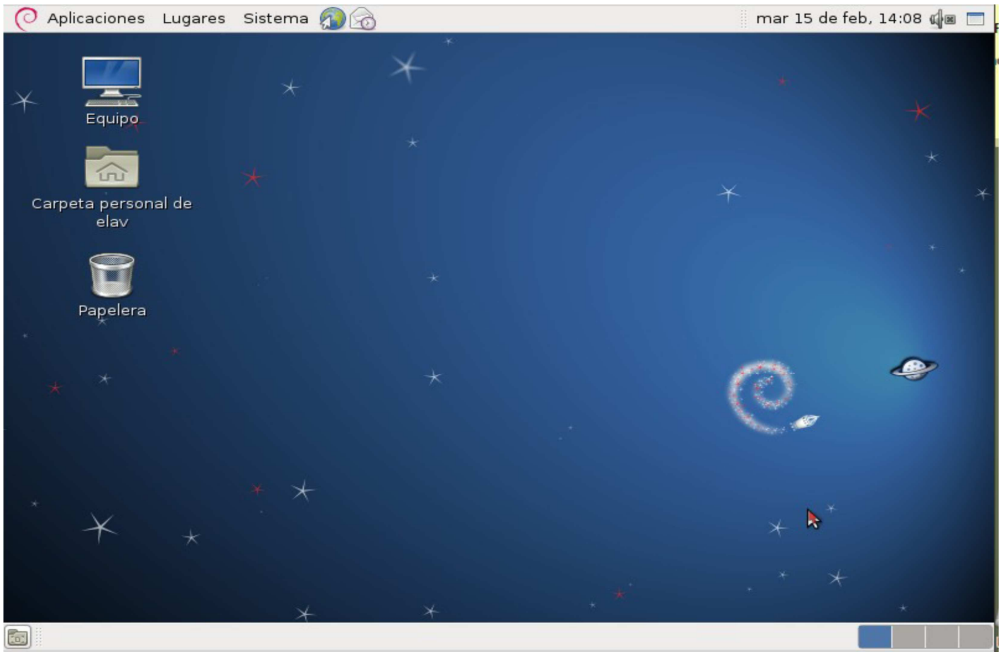
Una vez que termine de instalar nos pedirá instalar GRUB y de esta forma terminará la instalación.



Reiniciamos la PC y si todo sale bien nos saldrá algo como esto:

Luego nos aparecerá nuestra pantalla de Login y finalmente usando nuestro usuario y contraseña, accedemos a Gnome. De por si, solo instalamos un sistema básico con programas para realizar tareas básicas como navegar por Internet o revisar el correo.


tesis
andy
Otro...


Aplicaciones
Lugares
Sistema
mar 15 de feb, 14:08
Equipo
Carpeta personal de elav
Papelera

ANEXO 3

Configuracion de firewall

```
#!/bin/sh
# SCRIPT de IPTABLES
# MICRO Firewall
echo FIREWALL-INITIALIZER
#VARS
# squid server IP
SQUID_SERVER="192.17.1.1"
#RED
PRIVATE="192.17.1.1"
PUBLIC="186.3.39.130"
LOOP="127.0.0.1"

# Interface connected to Internet
INTERNET="eth0"
# Interface connected to LAN
LAN_IN="eth2"
# Squid port
SQUID_PORT="3128"
## Borrado de reglas
Iptables -F
Iptables -X
Iptables -Z
iptables -t nat -F
```

```
iptables -t nat -X
iptables -t mangle -F
iptables -t mangle -X

# Load IPTABLES modules for NAT and IP conntrack support
modprobe ip_conntrack
modprobe tun
modprobe ip_conntrack_ftp
#modprobe ip_nat_ftp
echo 1 > /proc/sys/net/ipv4/ip_forward

## Establecemos politica por defecto
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT
#iptables -P INPUT DROP
#iptables -P FORWARD DROP
iptables -t nat -P PREROUTING ACCEPT
iptables -t nat -P POSTROUTING ACCEPT

## Empezamos a filtrar

# Abriendo el local host (ejemplo conexiones locales a mysql)
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT

# Evitar que los paquetes externos usen la dirección de loopback
```

```
iptables -A INPUT -i $INTERNET -s $LOOP -j DROP
iptables -A FORWARD -i $INTERNET -s $LOOP -j DROP
iptables -A INPUT -i $INTERNET -d $LOOP -j DROP
iptables -A FORWARD -i $INTERNET -d $LOOP -j DROP

# A nuestra IP le dejamos todo
iptables -A INPUT -s $SQUID_SERVER -j ACCEPT

# Allow UDP, DNS and Passive FTP
iptables -A INPUT -i $INTERNET -m state --state
ESTABLISHED,RELATED -j ACCEPT

# DNAT port 80 request comming from LAN systems to squid 3128
($SQUID_PORT) aka transparent proxy
iptables -t nat -A PREROUTING -i $LAN_IN -p tcp --dport 80 -j DNAT --to
$SQUID_SERVER:$SQUID_PORT
# if it is same system
iptables -t nat -A PREROUTING -i $INTERNET -p tcp --dport 80 -j
REDIRECT --to-port $SQUID_PORT

# Permitir pings entrantes (pueden desabilitarse)
iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT

#Permitir la VPN
iptables -A INPUT -s 10.10.10.0/24 -p tcp --dport http -j ACCEPT
iptables -A FORWARD -s 10.10.10.0/24 -p tcp --dport http -j ACCEPT
iptables -A INPUT -s 172.16.1.0/24 -p tcp --dport http -j ACCEPT
```

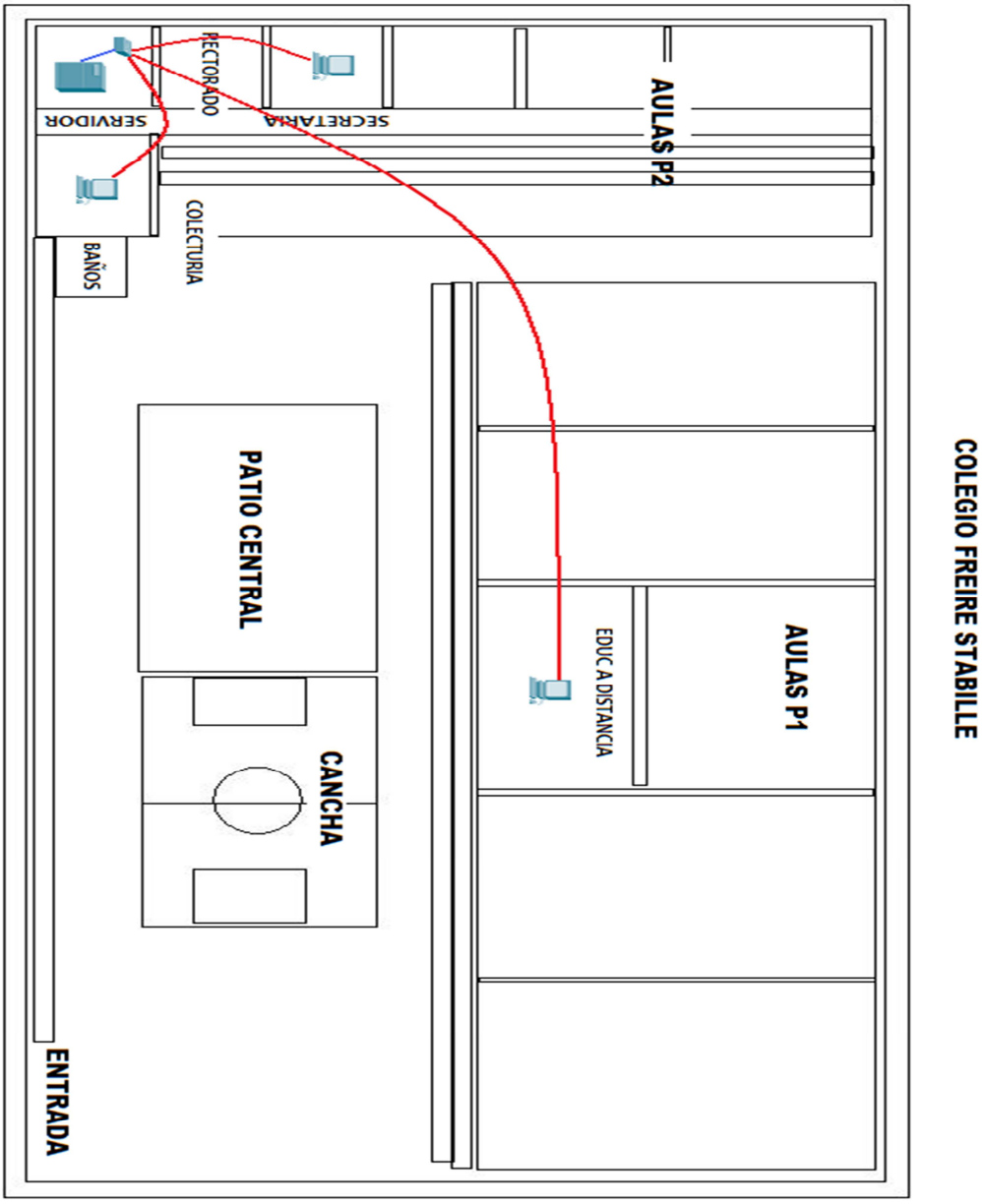
```
iptables -A FORWARD -s 172.16.1.0/24 -p tcp --dport http -j ACCEPT
iptables -A INPUT -s 192.17.1.0/24 -p tcp --dport http -j ACCEPT
iptables -A FORWARD -s 192.17.1.0/24 -p tcp --dport http -j ACCEPT

# Permitir servicios tales como www y ssh (pueden desabilitarse)
iptables -A INPUT -p tcp --dport 80 -j ACCEPT
iptables -A INPUT -p tcp --dport 8080 -j ACCEPT
iptables -A INPUT -p tcp --dport ssh -j ACCEPT

# Puertos abiertos 80(web), 3128(proxy), 22 (SSH)
iptables -A INPUT -p tcp --dport 80 -j ACCEPT
iptables -A INPUT -p tcp --dport 3128 -j ACCEPT
iptables -A FORWARD -p tcp --dport 3128 -j ACCEPT
iptables -A INPUT -p tcp --dport 22 -j ACCEPT
iptables -A INPUT -p tcp --dport 20:21 -j ACCEPT

# unlimited access to LAN
iptables -A INPUT -i $LAN_IN -j ACCEPT
iptables -A OUTPUT -o $LAN_IN -j ACCEPT

# Permitir paquetes entrantes a OpenVPN
# Duplicar la línea inferior por cada
# túnel OpenVPN, cambiando --dport n
# para que encaje con el puerto UDP de OpenVPN.
# En OpenVPN, el número de puerto se
# control con la opción --port n.
# Si pone esta opción en el fichero de configuración,
```

```
# puede eliminar los caracteres iniciales '--'
# Si está usando el firewall con estado
# (consulte el OpenVPN COMO),
# entonces comente la línea de abajo.
iptables -A INPUT -p udp --dport 1194 -j ACCEPT
# Permitir paquete del dispositivo TUN/TAP.
# Cuando OpenVPN está ejecutando en modo seguro,
# autenticará los paquetes previos a
# su llegada en el interfaz
# tun o tap.  Por lo tanto, no es
# necesario añadir ningun filtro aqui,
# a menos que quiera restringir el
# tipo de paquete que puedan circular por
# el túnel.
iptables -A INPUT -i tun+ -j ACCEPT
iptables -A FORWARD -i tun+ -j ACCEPT
iptables -A INPUT -i tap+ -j ACCEPT
iptables -A FORWARD -i tap+ -j ACCEPT
# Permitir paquetes de subredes privadas
iptables -A INPUT -i $LAN_IN -j ACCEPT
iptables -A FORWARD -i $LAN_IN -j ACCEPT
# Mantener el estado de las conexiones locales y las subredes privadas
iptables -A OUTPUT -m state --state NEW -o $INTERNET -j ACCEPT
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -m state --state NEW -o $INTERNET -j ACCEPT
iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j
ACCEPT
```

```
# Enmascarar la subred local
#iptables -t nat -A POSTROUTING -s $PRIVATE -o $INTERNET -j
MASQUERADE
# Cualquer cosa que venga de Internet debería tener una dirección de Internet
real
#iptables -A FORWARD -i $INTERNET -s 192.168.0.0/16 -j DROP
#iptables -A FORWARD -i $INTERNET -s 172.16.0.0/12 -j DROP
#iptables -A FORWARD -i $INTERNET -s 10.0.0.0/8 -j DROP
#iptables -A INPUT -i $INTERNET -s 192.168.0.0/16 -j DROP
#iptables -A INPUT -i $INTERNET -s 172.16.0.0/12 -j DROP
#iptables -A INPUT -i $INTERNET -s 10.0.0.0/8 -j DROP
# Bloquear paquetes NetBios salientes (si tiene máquinas windows en
# la subred privada).  Ésto no afecta al tráfico NetBios
# que circula por el túnel VPN, pero detendrá a las maquinas
# windows locales de mandar mensajes de broadcast
# a Internet.
#iptables -A FORWARD -p tcp --sport 137:139 -o $INTERNET -j DROP
#iptables -A FORWARD -p udp --sport 137:139 -o $INTERNET -j DROP
#iptables -A OUTPUT -p tcp --sport 137:139 -o $INTERNET -j DROP
#iptables -A OUTPUT -p udp --sport 137:139 -o $INTERNET -j DROP
# Politicas por defecto
## Y ahora cerramos los accesos indeseados del exterior:
# Nota: 0.0.0.0/0 significa: cualquier red
# Cerramos el rango de puerto bien conocido
#iptables -A INPUT -p tcp --dport 20:21 -j DROP
#iptables -A INPUT -p tcp --dport 22 -j DROP
iptables -A INPUT -p tcp --dport 3306 -j DROP
```

```
        # Cerramos el rango de puerto bien conocido
        iptables -A INPUT -s 0.0.0.0/0 -i $INTERNET -p tcp --dport 1:1024 -j DROP
        iptables -A INPUT -s 0.0.0.0/0 -i $INTERNET -p udp --dport 1:1024 -j
DROP
        #iptables -A INPUT -s 0.0.0.0/0 -p tcp --dport 1:1024 -j DROP
        #iptables -A INPUT -s 0.0.0.0/0 -p udp --dport 1:1024 -j DROP
        # Cerramos un puerto de gestión: webmin
        iptables -A INPUT -s 0.0.0.0/0 -i $INTERNET -p tcp --dport 10000 -j DROP
        #iptables -A INPUT -p tcp --dport 10000 -j DROP
        iptables -A INPUT -j LOG
        echo "FIREWALL-ON"
```

ANEXO 4. Diagrama de conexión de las unidades instaladas en la Unidad Educativa FreireStabile.



ANEXO 1 CRONOGRAMA DE TRABAJO

Actividades	9 al 15 de Mayo	16 al 22 de Mayo	23 al 29 de Mayo	30 de Mayo al 5 de Junio	6 al 12 de Junio	13 al 19 de Junio	20 al 26 de Junio	27 de Junio al 3 de Julio	4 al 10 de Julio	11 al 17 de Julio	18 al 24 de Julio	25 al 31 de Julio	1 al 7 de Agosto	22al 27 de agosto	29 al 2 de octubre	5 al 9 de octubre
Recopilación de información sobre Redes Virtuales Privadas																
Anàlisis y Estudio de la red del centro de computo de la UCSG.																
Análisis y Estudio de la red de la Unidad Educativa Freirestabile																
Adecuación de la red y los equipos del centro de computo, para la instalación de la VPN.																
Instalación de los servidores VPN con el respectivo software y las pruebas de funcionamiento dentro de la UCSG.																
Segunda prueba de los servidores VPN dentro de la UCSG.																
Instalación definitiva del primer servidor VPN con su respectivo software en el centro de computo.																
Selección del punto para ubicar la VPN, Análisis, estudio de la red existente en la Unidad Educativa Freirestabile.																
Adecuación de la red y los equipos del punto elegido en la Unidad Educativa Freirestabile.																
Instalaciòn del segundo servidor VPN con su respectivo software en la Unidad Educativa Freirestabile.																
Primeras pruebas del software y sistema completo en la Unidad Educativa Freirestabile.																
Pruebas finales del sistema completo en la Unidad Educativa Freirestabile.																
Prueba general del sistema completo en el centro de computo de la UCSG																