

Universidad Luterana Salvadoreña

Cátedra: Redes II

Docente: Ing. Manuel de Jesús Flores

Perfil de Proyecto de fin de ciclo

VPN con GNU/Linux Utilizando PPTP

Estudiante:

Carnet	Apellidos	Nombres	Participación
PR02110097	Piche Ramírez	Fernando Dagoberto	(100%)
AS01121365	Avilés Sánchez	Luis Alfredo	(100%)

Lugar y fecha de Entrega
San Salvador, 14 de noviembre de 2015

INDICE

Introducción	3
Objetivos	
4	
Marco Teórico	5
Descripción del proyecto	5
Tipos de VPN	6
Descripción del proyecto	7,8
Diagrama de RED del proyecto VPN	
9	
Lista de actividades	
10	
Diagrama de Gantt	
11	
Factibilidad Técnica	
12	
Factibilidad Operativa	
13	
Factibilidad Económica	
13	
Viabilidad técnica Económica	
14	
Instalación de paquetes para el vpn	
15, 16,17	
Añadiendo Usuarios	
18	
Configurando iptables	
19,20	
Configuración de Cliente	
21,22	
Conclusión	
23	
Bibliografía	
24	

INTRODUCCION

En el presente trabajo describimos cada una de las actividades, que como grupo hemos realizado en el proyecto de Redes II, el cual consiste en la instalación, configuración e implementación de un servidor VPN con GNU/Linux, en el que integra un conjunto de aplicaciones que proporcionan la capacidad de ejecutar GNU/Linux cómo un servidor VPN desde equipos remotos que tengan acceso a Internet.

También se explican los procedimientos que hacen funcionar el servidor VPN, así como los distintos servicios y protocolos que en su conjunto hacen funcionar un servicio VPN, creando un túnel para el encapsulamiento de protocolos y autenticación de usuarios, logrando mayor seguridad en la conexión.

En este documento se muestra el diagrama de red a utilizar así como también el diagrama de GANT en el que se contempla las actividades realizadas durante el proyecto, y también se muestran las herramientas tangibles e intangibles a utilizar, tales como Hardware y Software.

OBJETIVOS

OBJETIVO GENERAL.

- Presentar la configuración y como se implementa un VPN con GNU/Linux.

OBJETIVOS ESPECIFICOS.

- Mostrar las ventajas en la implementación de un VPN con GNU/Linux.
- Detallar los tipos de VPN y los diferentes protocolos que se pueden implementar.

MARCO TEÓRICO

Red privada virtual.

Una red privada virtual (**RPV**), o **VPN** de las siglas en inglés de **Virtual Private Network**, tecnología de red que permite una extensión segura de la red local (LAN) sobre una red pública o no controlada como Internet. Permite que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada. Esto se realiza estableciendo una conexión virtual punto a punto mediante el uso de conexiones dedicadas, cifrado o la combinación de ambos métodos.

Ejemplos comunes son la posibilidad de conectar dos o más sucursales de una empresa utilizando como vínculo Internet, permitir a los miembros del equipo de soporte técnico la conexión desde su casa al centro de cómputo, o que un usuario pueda acceder a su equipo doméstico desde un sitio remoto, como por ejemplo una empresa que se dedica a la venta de servicios. Todo ello utilizando la infraestructura de Internet.

Características básicas de la seguridad.

Para hacerlo posible de manera segura es necesario proporcionar los medios para garantizar la identificación.

Autenticación y autorización:

- ¿Quién está del otro lado? Usuario/equipo y qué nivel de acceso debe tener.
- Integridad:
- De que los datos enviados no han sido alterados.
- Confidencialidad/Privacidad:

- Dado que sólo puede ser interpretada por los destinatarios de la misma. Se hace uso de algoritmos de cifrado como Data Encryption Standard (DES), Triple DES (3DES) y Advanced Encryption Standard (AES).
- No repudio: es decir, un mensaje tiene que ir firmado, y quien lo firma no puede negar que envió el mensaje.
- Control de acceso: Se trata de asegurar que los participantes autenticados tiene acceso únicamente a los datos a los que están autorizados.
- Auditoría y registro de actividades: Se trata de asegurar el correcto funcionamiento y la capacidad de recuperación.
- Calidad del servicio: Se trata de asegurar un buen rendimiento, que no haya una degradación poco aceptable en la velocidad de transmisión.

Requisitos básicos.

- **Identificación de usuario:** las VPN deben verificar la identidad de los usuarios y restringir su acceso a aquellos que no se encuentren autorizados.
- **Cifrado de datos:** los datos que se van a transmitir a través de la red pública (Internet), antes deben ser cifrados, para que así no puedan ser leídos si son interceptados.

Esta tarea se realiza con algoritmos de cifrado como DESo 3DES que sólo pueden ser leídos por el emisor y receptor.

- **Administración de claves:** las VPN deben actualizar las claves de cifrado para los usuarios.
- Nuevo algoritmo de seguridad SEAL.

TIPOS DE VPN

VPN de acceso remoto.

Es quizás el modelo más usado actualmente, y consiste en usuarios o proveedores que se conectan con la empresa desde sitios remotos (oficinas comerciales, domicilios, hoteles, aviones preparados,

etcétera) utilizando Internet como vínculo de acceso. Una vez autenticados tienen un nivel de acceso muy similar al que tienen en la red local de la empresa. Muchas empresas han reemplazado con esta tecnología su infraestructura dial-up (módems y líneas telefónicas).

VPN punto a punto.

Este esquema se utiliza para conectar oficinas remotas con la sede central de la organización. El servidor VPN, que posee un vínculo permanente a Internet, acepta las conexiones vía Internet provenientes de los sitios y establece el túnel VPN. Los servidores de las sucursales se conectan a Internet utilizando los servicios de su proveedor local de Internet, típicamente mediante conexiones de banda ancha. Esto permite eliminar los costosos vínculos punto a punto tradicionales (realizados comúnmente mediante conexiones de cable físicas entre los nodos), sobre todo en las comunicaciones internacionales. Es más común el siguiente punto, también llamado tecnología de túnel o tunneling.

Tunneling.

La técnica de tunneling consiste en encapsular un protocolo de red sobre otro (protocolo de red encapsulador) creando un túnel dentro de una red de computadoras. El establecimiento de dicho túnel se implementa incluyendo una PDU (unidades de datos de protocolo) determinada dentro de otra PDU con el objetivo de transmitirla desde un extremo al otro del túnel sin que sea necesaria una interpretación intermedia de la PDU encapsulada. De esta manera se encaminan los paquetes de datos sobre nodos intermedios que son incapaces de ver en claro el contenido de dichos paquetes. El túnel queda definido por los puntos extremos y el protocolo de comunicación empleado, que entre otros, podría ser SSH.

El uso de esta técnica persigue diferentes objetivos, dependiendo del problema que se esté tratando, como por ejemplo la comunicación de islas en escenarios multicast, la redirección de

tráfico, etc.

Uno de los ejemplos más claros de utilización de esta técnica consiste en la redirección de tráfico en escenarios IP Móvil. En escenarios de IP móvil, cuando un nodo-móvil no se encuentra en su red base, necesita que su home-agent realice ciertas funciones en su puesto, entre las que se encuentra la de capturar el tráfico dirigido al nodo-móvil y redirigirlo hacia él. Esa redirección del tráfico se realiza usando un mecanismo de tunneling, ya que es necesario que los paquetes conserven su estructura y contenido originales (dirección IP de origen y destino, puertos, etc.) cuando sean recibidos por el nodo-móvil.

VPN over LAN.

Este esquema es el menos difundido pero uno de los más poderosos para utilizar dentro de la empresa. Es una variante del tipo "acceso remoto" pero, en vez de utilizar Internet como medio de conexión, emplea la misma red de área local (LAN) de la empresa. Sirve para aislar zonas y servicios de la red interna. Esta capacidad lo hace muy conveniente para mejorar las prestaciones de seguridad de las redes inalámbricas (WiFi).

Un ejemplo clásico es un servidor con información sensible, como las nóminas de sueldos, ubicado detrás de un equipo VPN, el cual provee autenticación adicional más el agregado del cifrado, haciendo posible que sólo el personal de recursos humanos habilitado pueda acceder a la información.

Otro ejemplo es la conexión a redes Wi-Fi haciendo uso de túneles cifrados IPSec o SSL que además de pasar por los métodos de autenticación tradicionales (WEP, WPA, direcciones MAC, etc.) agregan las credenciales de seguridad del túnel VPN creado en la LAN interna o externa.

DESCRIPCION DEL PROYECTO

El proyecto de Redes II, consta de la configuración de un servidor VPN, con el cual se pretende acceder remotamente por medio de una red virtual al servidor que se ejecuta en un sistema GNU/Linux,

que será ejecutado por los clientes que tengan acceso a Internet.

Con el Servidor VPN (Virtual Private Network), se puede acceder remotamente desde cualquier parte del mundo con solo tener acceso a Internet y con un nivel de seguridad y autenticación para acceder al servidor VPN.

El proyecto será realizado instalando el servidor VPN utilizando la versión del software libre Debian de GNU/Linux 7.6 wheezy estable, en la que se harán las configuraciones necesarias para el correcto funcionamiento así como también se configurara un Switch para el redireccionamiento y liberación de puertos.

Pasos generales del proyecto:

- Instalación de sistema operativo GNU/Linux.
- Instalación y configuración del servidor PPTPcon GNU/Linux.
- Configuración del Router para el correcto funcionamiento.
- Pruebas y monitoreo.

TIPOS DE CONEXIÓN.

Conexión de acceso remoto Una conexión de acceso remoto es realizada por un cliente o un usuario de una computadora que se conecta a una red privada, los paquetes enviados a través de la conexión VPN son originados al cliente de acceso remoto, y éste se autentifica al servidor de acceso remoto, y el servidor se autentifica ante el cliente.

Conexión VPN router a router.

Una conexión VPN router a router es realizada por un router, y este a su vez se conecta a una red privada. En este tipo de conexión, los paquetes enviados desde cualquier router no se originan en los routers. El router que realiza la llamada se autentifica ante el router que responde y este a su vez se autentifica ante el router que realiza la llamada y también sirve para la intranet.

Conexión VPN firewall a firewall.

Una conexión VPN firewall a firewall es realizada por uno de

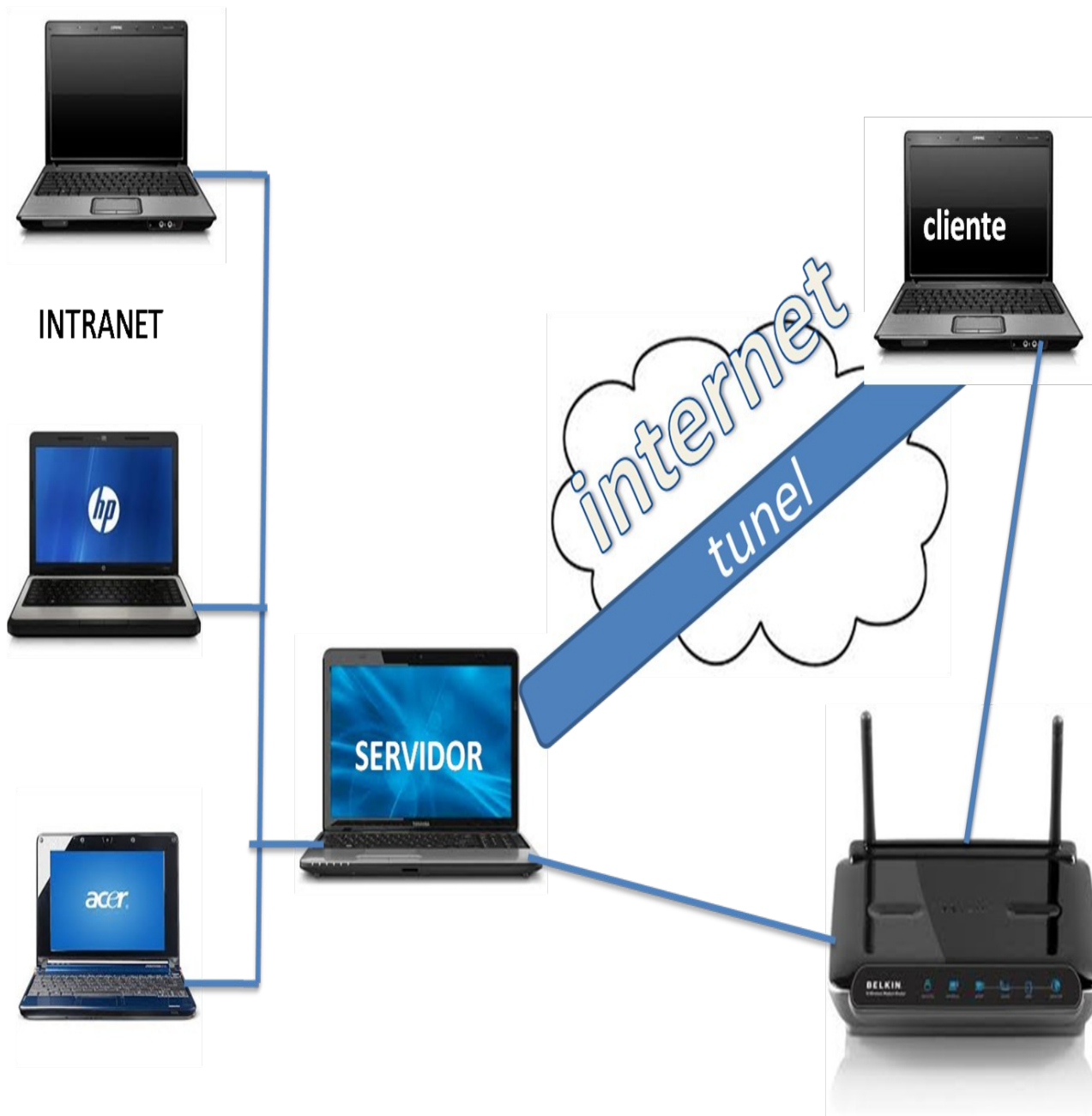
ellos, y éste a su vez

se conecta a una red privada. En este tipo de conexión, los paquetes son enviados

desde cualquier usuario en Internet. El firewall que realiza la llamada se autentifica

ante el que responde y éste a su vez se autentifica ante el llamante.

DIAGRAMA DE RED DEL PROYECTO VPN



Lista de actividades

- 1-) Recopilación de información necesaria para instalar y configurar un VPN.
- 2-) Redactar y presentar el perfil del proyecto VPN.
- 3-) Instalación de debían en la computadora.
- 4-) Instalación del PPTP, que nos servirá para hacer las conexiones, identificaciones,
 encapsula miento y asignara las ip a los clientes.
- 5-) Configuración de la computadora que utilizaremos como servidor VPN.

nos servira para hacer las conexiones, identificaciones, encapsulamiento y asignara las ip a los clientes.																		
Configuración de la computadora que utilizaremos como servidor VPN.																		
Configuración de las computadoras que se utilizaran como clientes que tendra el servicio VPN.																		
Pruebas hacia el pptp																		
Corrección de errores del proyecto.																		

FACTIBILIDAD DEL PROYECTO.

Analizaremos la disponibilidad de los recursos necesarios para llevar a cabo los objetivos y metas señalados. A raíz del tipo de proyecto que estamos presentando hemos determinado las siguientes factibilidades.

FACTIBILIDAD TÉCNICA.

Al hacer la investigación sobre las tecnologías existentes sobre Redes Privadas Virtuales o VPN, se hizo la recolección de la información sobre los componentes y equipos tecnológicos necesarios para llevar a cabo el proyecto de VPN con GNU/Linux.

De acuerdo con los componentes necesarios para la implementación del servidor VPN, se hizo la evaluación con respecto a dos enfoques (Hardware y software).

En cuanto al hardware, los componentes necesarios para la implementación del servidor VPN son los siguientes:

Servidor:

Procesador Pentium 4 de 2.0 GHZ o superior.

Tarjeta madre.

RAM

2GB o Más.

Disco Duro 320 o más.

Tarjeta de red integrada o PCI Ethernet 10/100 Mbps. O superior.

Monitor, Teclado y Mouse.

Clientes.

- Puerto para conexión de teclado
- Puerto para conexión de mouse
- Puerto de red Ethernet 10/100 Mbps
- Puerto para conexión de monitor
- Dos puertos USB 2.0.
- Tarjeta madre.
- Monitor.
- Teclado.
- Mouse.

Tomando en cuenta los requerimientos y habiendo evaluado el hardware con el que se dispone, es factible técnicamente la implementación del proyecto.

En cuanto al software:

Se pretende utilizar un sistema operativo GNU/Linux, como por ejemplo Debian o una distribución derivada de la misma ya sea Ubuntu o Linux min, etc.

Como resultado del estudio técnico realizado, se determinó que se cuenta con los requerimientos básicos en cuanto al hardware y software necesarios para la implementación del servidor VPN.

FACTIBILIDAD OPERATIVA.

Según el estudio de factibilidad operativa y el análisis realizado podemos determinar que se cuenta con los conocimientos necesarios y básicos para poder implementar el proyecto de VPN con GNU/Linux. Además es necesario el apoyo de otros recursos como bibliográficos, digitales y la web, entre otros, para poder implementar el proyecto y así lograr determinar que la implementación es factible operativamente.

FACTIBILIDAD ECONÓMICA.

Según el estudio de factibilidad económica y el análisis realizado podemos determina económicamente con los recursos con los que se cuenta y con los que se necesitan para poder desarrollar el proyecto de Redes Privadas Virtuales o VPN:

Recursos disponibles:

- Una computadora con sistema operativo GNU/Linux utilizado como servidor VPN.
- Dos computadoras que servirán como clientes con acceso a Internet.
- Servicio de Internet.

Viabilidad técnica y económica.

RECURSOS NECESARIOS DE ADQUIRIR		
RECURSOS	COSTO	CANTIDAD
Cable UTP categoría 5e 0 superior	\$0.50 yarda	2 de tres yardas
Conector RJ45	\$0.15	5
Crimpadora	\$12.00	1

Switch Fas Ethernet	\$20.00	1
---------------------	---------	---

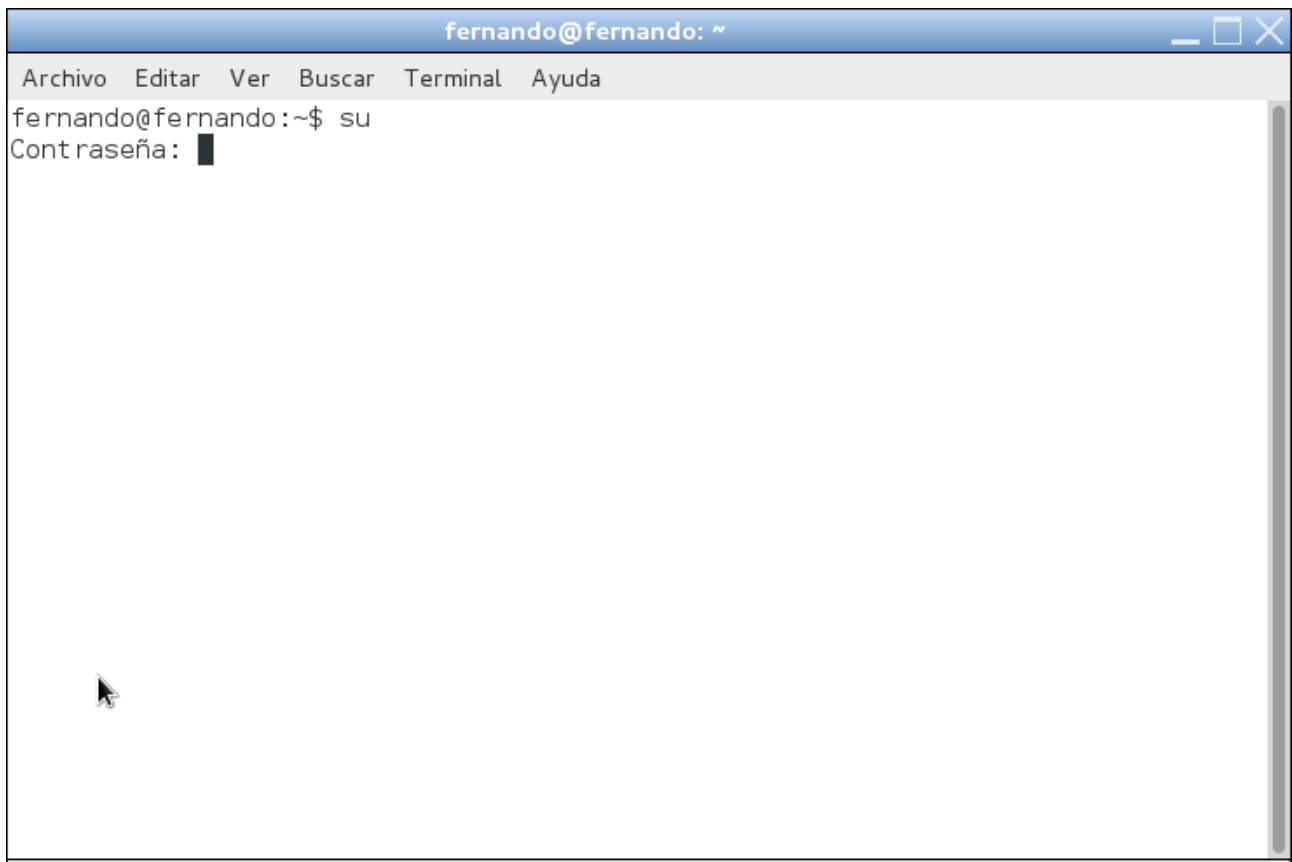
Configuración del servidor

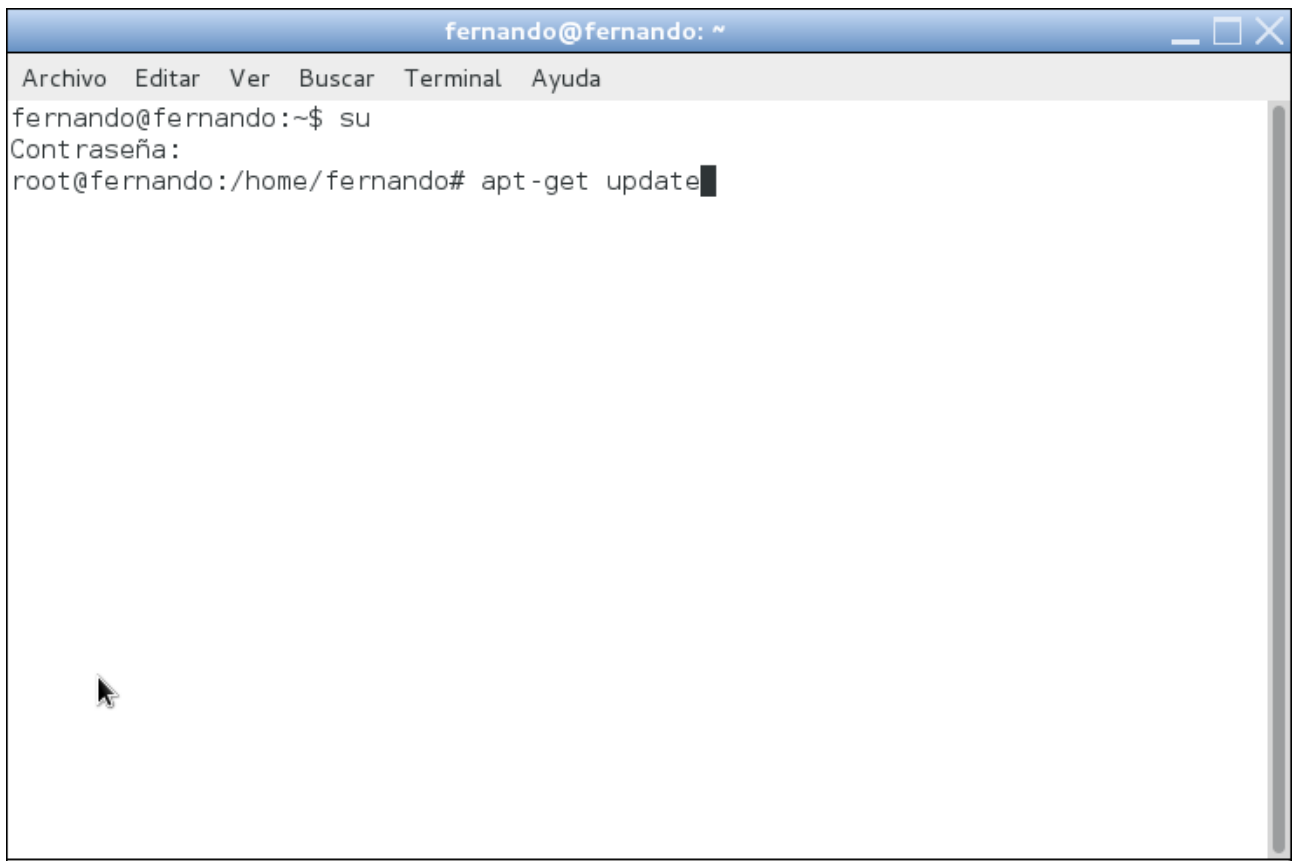
- Tener una dirección estática
- Router debe tener puerto PPTP(1723 TCP) abierto
- Iniciamos una terminal

Instalar los paquetes

En el terminal tecleamos la siguiente orden:

```
sudo aptget install pptpd
```



A terminal window titled "fernando@fernando: ~" with a menu bar containing "Archivo", "Editar", "Ver", "Buscar", "Terminal", and "Ayuda". The terminal content shows the user switching to root with "su", entering a password, and then running "apt-get update" as root. A mouse cursor is visible in the lower-left area of the terminal.

```
fernando@fernando: ~  
Archivo  Editar  Ver  Buscar  Terminal  Ayuda  
fernando@fernando:~$ su  
Contraseña:  
root@fernando:/home/fernando# apt-get update
```

Una vez finalizado el proceso se iniciará el servidor PPTP automáticamente, pero aún no está configurado, para lo cual ejecutaremos:

```
sudo nano /etc/pptpd.conf
```

```
fernando@fernando: ~
Archivo Editar Ver Buscar Terminal Ayuda
GNU nano 2.2.6 Fichero: /etc/pptpd.conf
#      4. If you give a single localIP, that's ok - all local IPs will
#      be set to the given one. You MUST still give at least one remote
#      IP for each simultaneous client.
#
# (Recommended)
localip 192.168.0.115
remoteip 192.168.0.10-238,192.168.0.245
# or
#localip 192.168.0.10-238,192.168.0.245
#remoteip 192.168.1.234-238,192.168.1.245
#or
#localip 10.0.0.1
#remoteip 10.0.0.10-60
█

^G Ver ayuda  ^O Guardar   ^R Leer Fich ^Y Pág Ant   ^K CortarTxt ^C Pos actual
^X Salir      ^J Justificar ^W Buscar    ^V Pág Sig   ^U PegarTxt  ^T Ortografía
```

Tras ejecutarlo aparecerá en la misma ventana del terminal el editor nano. Usando los cursores bajamos hasta el final del todo e insertamos, como si se tratara del bloc de notas, las líneas (en la captura la hemos seleccionado para distinguirlas del resto del texto):

```
localip 192.168.0.115
remoteip 192.168.0.10-238,192.168.0.245
```

Explicación:

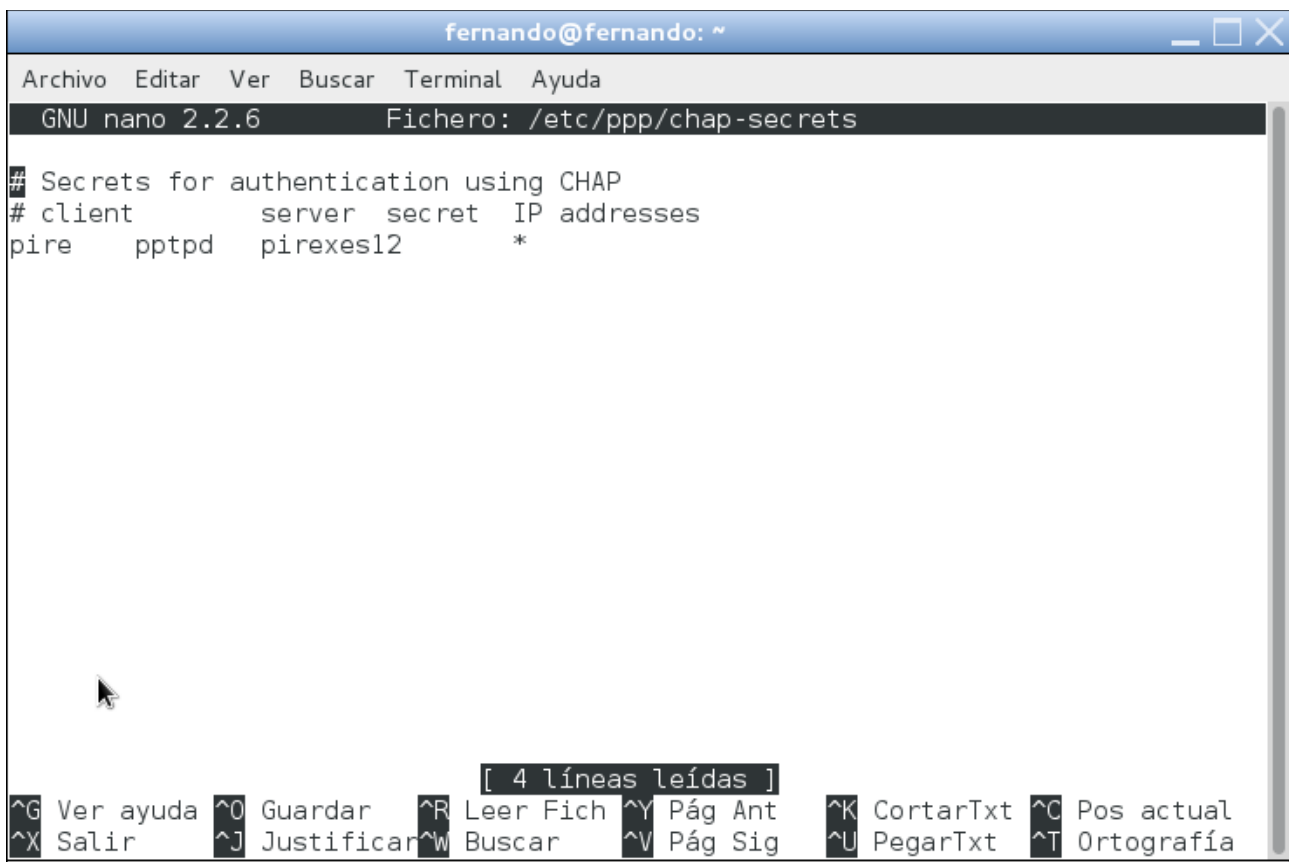
- Primera línea: Especificamos cuál será la dirección IP de nuestro servidor dentro de la VPN. Para que no haya conflicto con las direcciones IP "domésticas", hemos seleccionado un rango de direcciones distinto.
- Segunda línea: Especifica el rango de direcciones que usaremos para asignar a los clientes. En la parte anterior a la "," (coma) hemos especificado un rango y detrás una dirección simple. Con esto hemos querido mostraros las dos posibles formas de especificar las direcciones de los clientes, es decir, que se puede especificar simplemente un rango.

Para guardar los cambios presionamos "Control + O" y para salir "Control + X".

Añadiendo usuarios

Ahora vamos a añadir usuarios a nuestra VPN. Para hacerlo modificaremos el archivo chapsecrets:

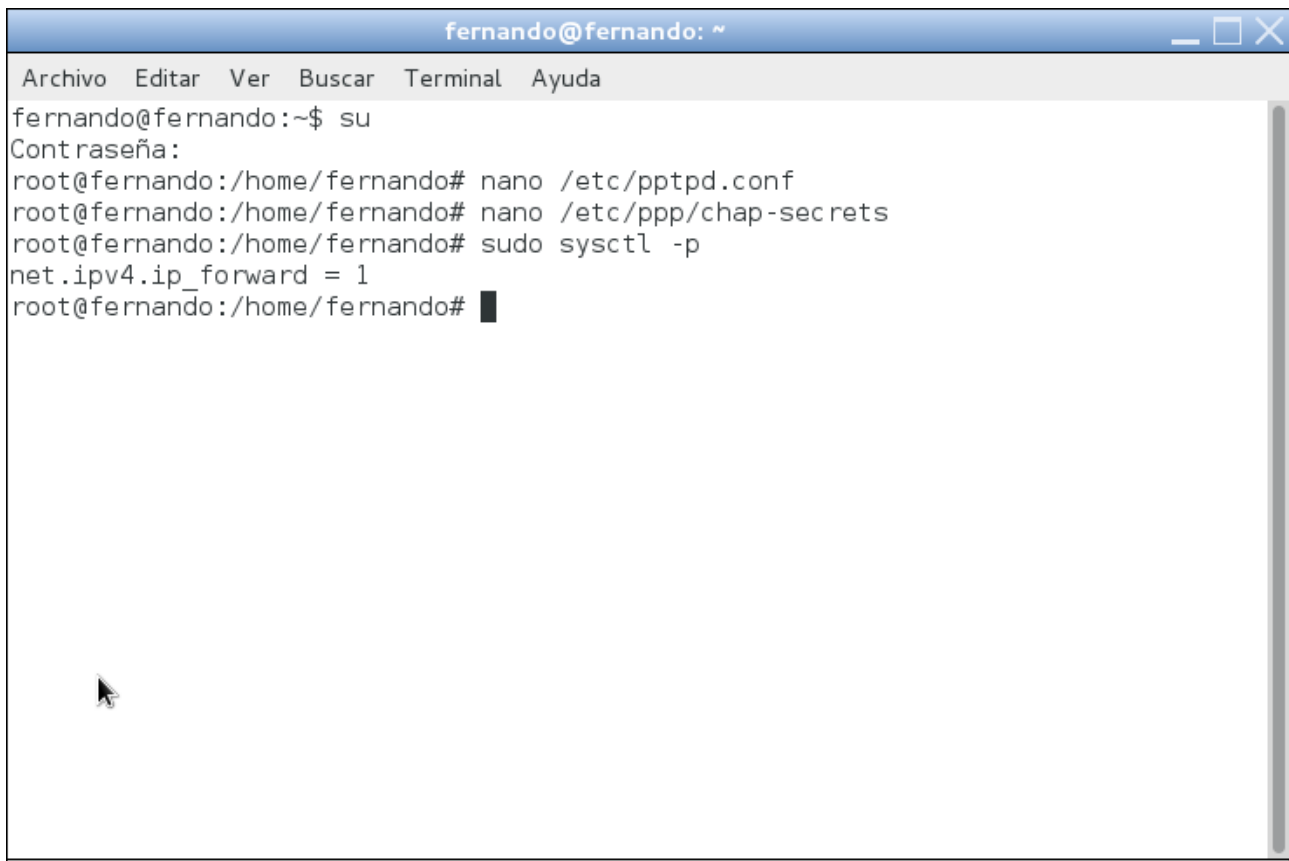
```
sudo nano /etc/ppp/chapsecrets
```



```
fernando@fernando: ~
Archivo Editar Ver Buscar Terminal Ayuda
GNU nano 2.2.6 Fichero: /etc/ppp/chap-secrets
# Secrets for authentication using CHAP
# client      server  secret  IP addresses
pire  pptpd  pirexes12  *
```

[4 líneas leídas]

^G Ver ayuda	^O Guardar	^R Leer Fich	^Y Pág Ant	^K CortarTxt	^C Pos actual
^X Salir	^J Justificar	^W Buscar	^V Pág Sig	^U PegarTxt	^T Ortografía

A terminal window titled 'fernando@fernando: ~' with a menu bar containing 'Archivo', 'Editar', 'Ver', 'Buscar', 'Terminal', and 'Ayuda'. The terminal shows the following commands and output:

```
fernando@fernando:~$ su
Contraseña:
root@fernando:/home/fernando# nano /etc/pptpd.conf
root@fernando:/home/fernando# nano /etc/ppp/chap-secrets
root@fernando:/home/fernando# sudo sysctl -p
net.ipv4.ip_forward = 1
root@fernando:/home/fernando# █
```

Configurando iptables

Hasta este punto ya tenemos todo lo referente a nuestra VPN configurado, tan sólo queda configurar el cortafuegos de Ubuntu para que permita el acceso a las conexiones entrantes y redirija el tráfico. Para que la configuración se mantenga con cada reinicio modificaremos el script rc.local:

```
sudo nano /etc/rc.local
```

```
fernando@fernando: ~
Archivo Editar Ver Buscar Terminal Ayuda
GNU nano 2.2.6 Fichero: /etc/rc.local

#!/bin/sh -e
#
# rc.local
#
# This script is executed at the end of each multiuser runlevel.
# Make sure that the script will "exit 0" on success or any other
# value on error.
#
# In order to enable or disable this script just change the execution
# bits.
#
# By default this script does nothing.
#/etc/ppp/vpnconfig.sh
iptables -t nat -A POSTROUTING -s 192.168.0.0/24 -o eth0 -j MASQUERADE
exit 0

[ 15 líneas leídas ]
^G Ver ayuda ^O Guardar ^R Leer Fich ^Y Pág Ant ^K CortarTxt ^C Pos actual
^X Salir ^J Justificar ^W Buscar ^V Pág Sig ^U PegarTxt ^T Ortografía
```

```
fernando@fernando: ~
Archivo Editar Ver Buscar Terminal Ayuda
GNU nano 2.2.6 Fichero: /etc/ppp/pptpd-options

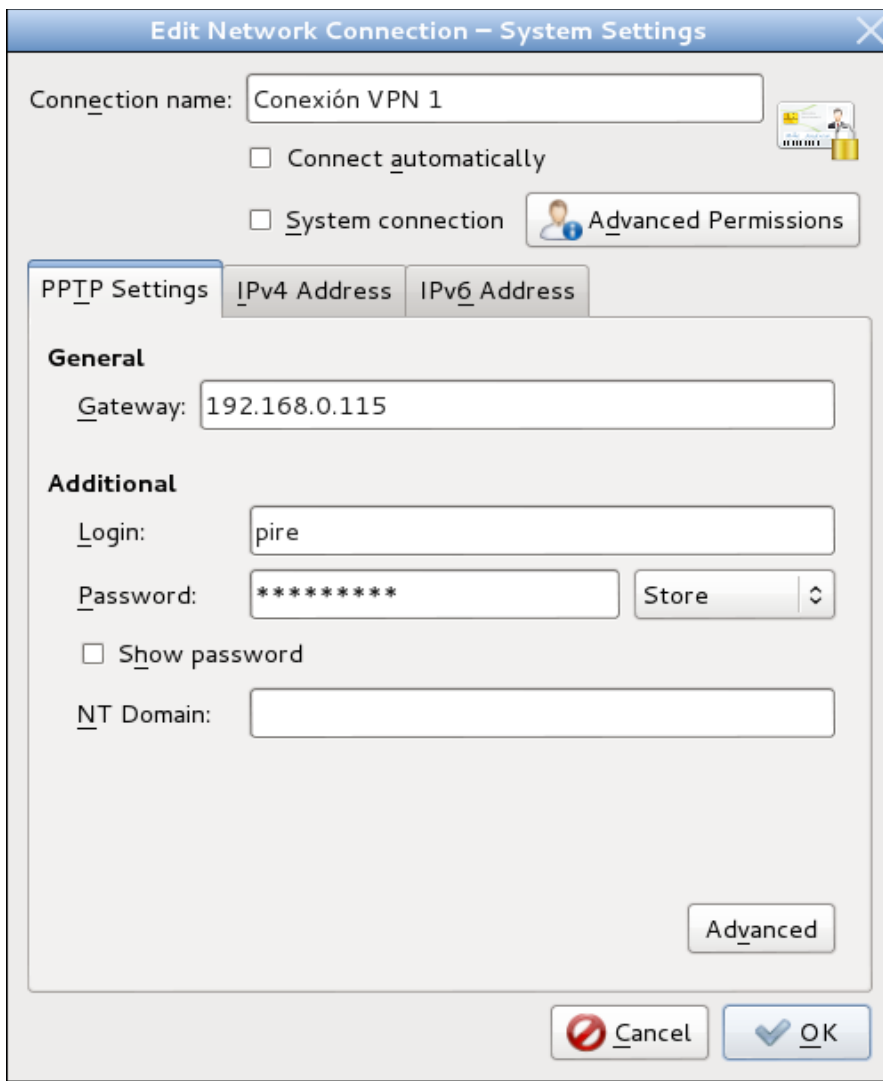
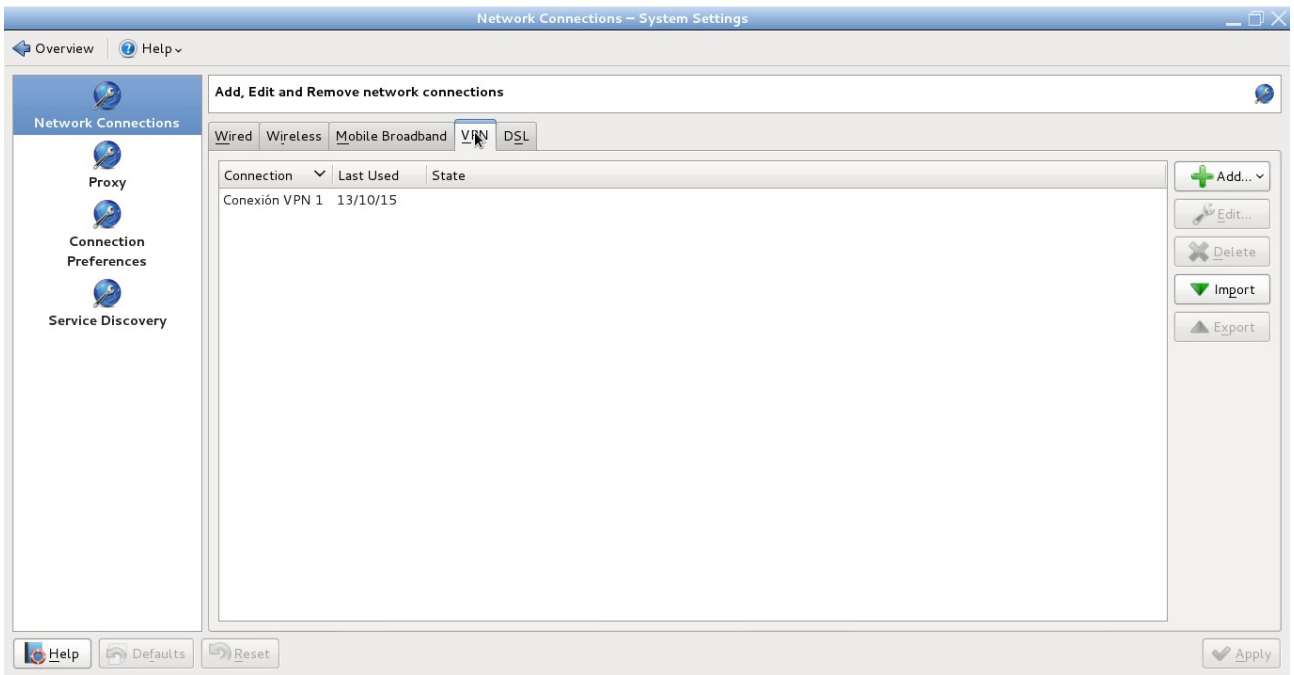
# specifies the primary DNS address; the second instance (if given)
# specifies the secondary DNS address.
# Attention! This information may not be taken into account by a Windows
# client. See KB311218 in Microsoft's knowledge base for more information.
#ms-dns 10.0.0.1
#ms-dns 10.0.0.2
ms-dns 8.8.8.8
ms-dns 8.8.4.4

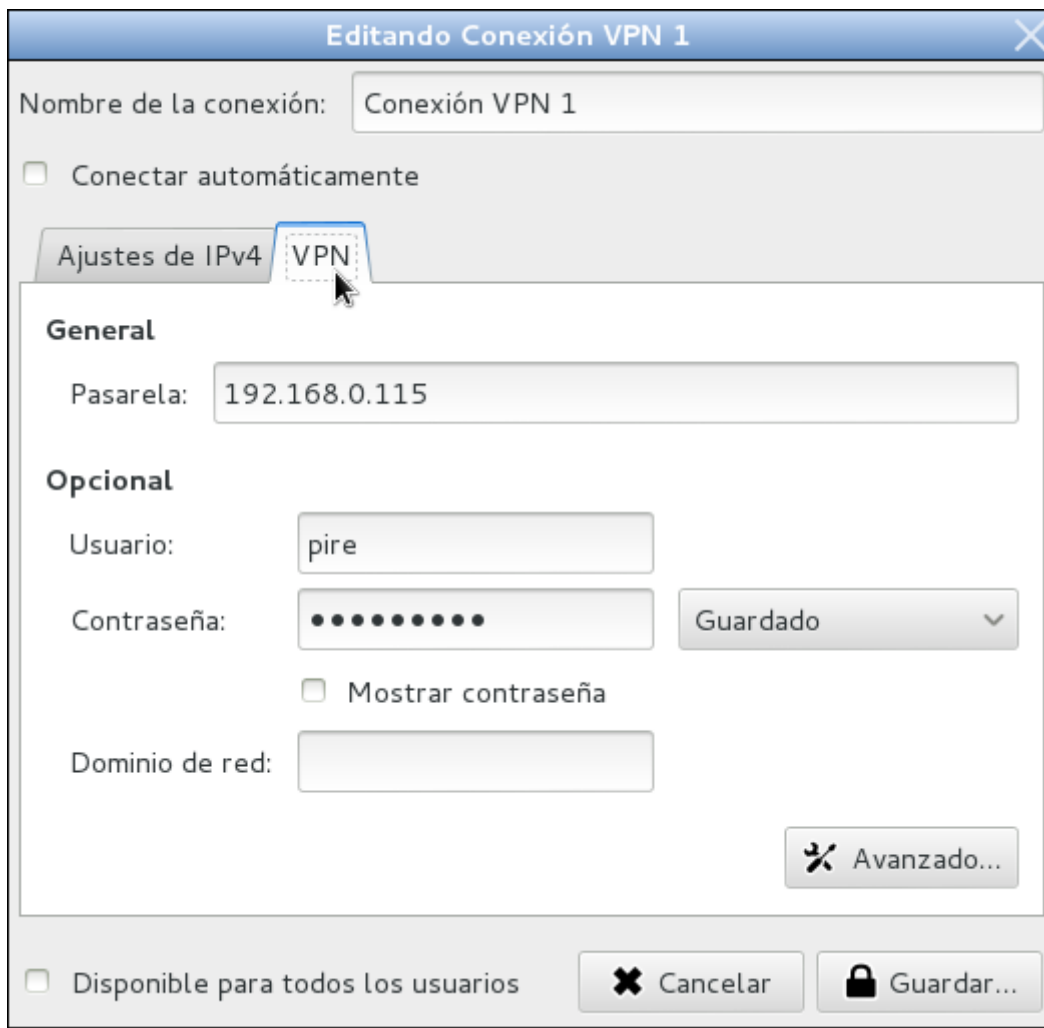
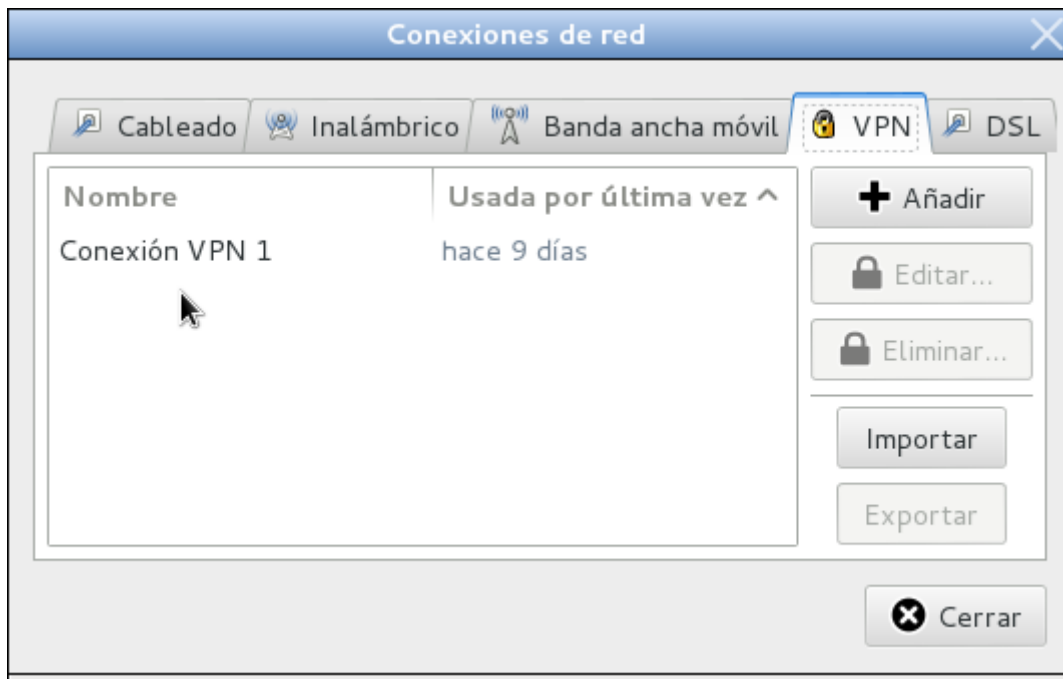
# If pptpd is acting as a server for Microsoft Windows or "Samba"
# clients, this option allows pptpd to supply one or two WINS (Windows
# Internet Name Services) server addresses to the clients. The first
# instance of this option specifies the primary WINS address; the
# second instance (if given) specifies the secondary WINS address.
#ms-wins 10.0.0.3
#ms-wins 10.0.0.4

# Add an entry to this system's ARP [Address Resolution Protocol]
# table with the IP address of the peer and the Ethernet address of this

^G Ver ayuda ^O Guardar ^R Leer Fich ^Y Pág Ant ^K CortarTxt ^C Pos actual
^X Salir ^J Justificar ^W Buscar ^V Pág Sig ^U PegarTxt ^T Ortografía
```

Configuración Cliente





CONCLUSION

En conclusión se muestra el proceso para desarrollar la

implementación de un Servidor pptp con GNU/Linux, que consiste en el uso de redes virtuales privadas a través de protocolos para hacer un túnel entre ellos y así hacer un acceso remoto a través de Internet.

Como grupo se llegó a la conclusión, que el perfil que se muestra contiene las generalidades básicas para la instalación y configuración de una VPN, así como también la utilización de la misma en el que se muestra los objetivos del proyecto, los cuales se cumplieron y se ponen en manifiesto en la culminación del mismo. El cual es de suma importancia porque en él se puede plasmar las ideas principales realizadas en el proyecto e identificar si el mismo es viable o factible y así desarrollar la configuración de pptp en GNU/Linux.

SITIOGRAFÍA

REFERENCIA 1.

Autor: Wikipedia.

Título: Red Privada Virtual.

URL: http://es.wikipedia.org/wiki/Red_privada_virtual

Fecha de Consulta: 20/08/2014.

REFERENCIA 2.

Autor: Web Adicto.

Título: ¿Qué es una Red Privada Virtual VPN? - Ventajas, Desventajas y

Herramientas

URL:[http://webadicto.net/post/Redes-Privadas-Virtuales-VPN-Ventajas-](http://webadicto.net/post/Redes-Privadas-Virtuales-VPN-Ventajas-Desventajas-y-Herramientas)

[Desventajas-y-Herramientas](http://webadicto.net/post/Redes-Privadas-Virtuales-VPN-Ventajas-Desventajas-y-Herramientas)

Fecha de Consulta: 22/08/2014.

REFERENCIA 3.

Título: Conexiones VPN con PPTP bajo Linux

<http://www.redes-linux.com/manuales/vpn/pptp.pdf>