UNIVERSIDAD JOSÉ CARLOS MARIÁTEGUI

VICERRECTORADO DE INVESTIGACIÓN

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

TRABAJO DE SUFICIENCIA PROFESIONAL

IMPLEMENTAR SERVIDOR DE RED PRIVADA (VPN) UTILIZANDO TECNOLOGÍA SATELITAL PARA LA EMPRESA AQUACORP PARA INTERCONECTAR DE FORMA REMOTA LAS ÁREAS Y LA SEGURIDAD INFORMÁTICA

PRESENTADO POR

BACHILLER CARLOS DARIO TICONA APAZA

ASESOR

ING. JULIÁN FLORES MANCHEGO

PARA OPTAR TÍTULO PROFESIONAL DE

INGENIERO DE SISTEMAS E INFORMÁTICA

MOQUEGUA – PERÚ

2017

CONTENIDO

PORTADA **Pág.**

CAPÍTULO IV

CONCLUSIONES Y RECOMENDACIONES

ÍNDICE DE TABLAS

Contenido de tablas **Pág.**

ÍNDICE DE FIGURAS

Contenido de figuras **Pág.**

RESUMEN

La aplicación de software libre está cambiando la informática y software de servidores desde un punto de vista más seguro y confiable la distribución libre para uso en diversos sistemas operativos en las empresas, corporaciones del mercado. El presente trabajo tiene como título implementar servidor de red privada (Vpn) utilizando tecnología satelital para la empresa Aquacorp para interconectar de forma remota las áreas y la seguridad informática. Tiene como finalidad desarrollar un servidor en linux CentOS 6.5 para mejorar la seguridad informática para la empresa Acuacorp además se describen la Vpn sus definiciones, características, funcionalidad, configuraciones de disco, tarjetas de red, comandos en squid y enlace remoto entre computadoras con linux y explicaremos firewall para su protección de virus maliciosos; problemas se pueden presenter en tiempo real en su funcionalidad y los procesos que realiza cada sistema integrado en la Vpn CentOS 6.5. Se obtuvo como resultado la protección del 98% de seguridad informática en eventos peligrosos como es fuerza bruta, bots, malware, errores de configuración , ddos, diagnosticarlos para los futuros daños que pueden ocasionar a los sistemas informáticos dentro de la empresa Acuacorp. Se aplicó estadística descriptiva en los eventos ocurridos en el registro de incidencias de malware durante el año 2016. Finalmente se hará una demostración utilizando la herramienta Sarg (squid analysis report generator), obteniendo un reporte final que nos ayuda analizar, actualizar y monitorear estos eventos ocurridos dentro de nuestra Vpn, nos garantiza la seguridad en los metadatos para su correcto uso dentro y fuera de una red lan.

Palabras clave: Servidor, satelital, seguridad informática.

ABSTRACT

The free software application is changing the computer and server software from a more secure and confinable point of view free distribution for use in various operating systems in companies, market corporations. The present work has the title of implementing private network server (Vpn) using satellite technology for the company Aquacorp to remotely interconnect the areas and computer security. Its purpose is to develop a server in linux CentOS 6.5 to improve the computer security for the company Acuacorp also describe the Vpn definitions, features, functionality, disk configurations, network cards, commands in squid and remote link between computers with linux and we will explain firewall for its protection against malicious viruses; problems can be presented in real time in its functionality and the processes performed by each integrated system in the Vpn CentOS 6.5. The result was the protection of 98% of computer security in dangerous events such as brute force, bots, malware, configuration errors, ddos, diagnose them for future damages that can be caused to computer systems within the company Acuacorp. Descriptive statistics were applied in the occurrences occurred in the register of malware incidents during 2016. Finally, a demonstration will be made using the Sarg (squid analysis report generator) tool, obtaining a final report that helps us analyze, update and monitor these events. within our Vpn, it guarantees the security in the metadata for its correct use inside and outside a LAN network.

Keywords: Server, satellite, computer security.

CAPÍTULO I

INTRODUCCIÓN

En la empresa Aquacorp con muchos ordenadores interconectados a una red de internet satelital, circulan por la red múltiples aplicaciones servicios como: e-mail, compras electrónicas, transacciones de cuentas bancarias, boletas de pagos y devengados financieros en la red se hace muy insegura.

La empresa necesita protección y seguridad informática para sus archivos de envió y acceso a contraseñas y bloqueos de puertos, así controlar el acceso de hacker, malware, spam, virus que alteran su estructura software de manera lógica en librerías, paquetes y registros de sistemas operativos en ejecución de tiempo real.

Nuestros backus siempre serán respaldo seguro, pero si no tenemos un firewall configurado correctamente y bloqueado en accesos corremos el riesgo de perder registros a los sistemas de servidores en las diferentes áreas de trabajo.

La seguridad informática IPSEC (protocolo de seguridad) está dado para mejorar logaritmos de cifrado modo transporte y modo túnel dentro de Linux.

Por ello que el presente trabajo damos a conocer la utilización Linux CentOS en aspectos para la trasferencia de datos, en una plataforma en administración de usuarios y servicios de internet, aplicar ruteo de redes para acceso remoto a datos del servidor.

Aplicaremos servidor como firewall proxy en linux para las Vpn después aplicaremos estadística descriptiva para la representación gráfica en microsoft excel los datos estadísticos.

CAPÍTULO II

OBJETIVOS

2.1. Objetivo general

Identificar y detectar registros de incidencias de virus para mejorar la seguridad en datos con linux aplicado el modelo de una red privada virtual (VPN).

2.2. Objetivos específicos

Realizar la configuración del servidor de red Vpn bajo el sistema Linux CentOS 6.5.

Configurar Squid en Linux sobre una red Vpn en CentOS 6.5.

Aplicar herramientas de modelo segar reportes sobre amenazas en la Vpn.

CAPÍTULO III

DESARROLLO DEL TEMA

3.1 Conceptos generales

3.1.1 Red privada virtual

Red privada virtual es un diseño de controlar lan en un área local de red separada físicamente mediante conexiones de banda ancha, aplicando los protocolos de seguridad para la internet e incrustado de data para la confidencialidad y protección de datos.

Para conectar en forma remota tenemos tres opciones:

- Modem: es un dispositivo que convierte las señales digitales en analógica y en viceversa así nos permite la comunicación entre computadoras ya sean en líneas telefónicas o cable modem.
- Vpn: Como estándar solo es configurar de manera sencilla y aplicaciones con androide 5.5 para encriptar la seguridad en aplicaciones móviles.

3.1.2 Como soporte de VPN

La información privada pasa a ser confidencial perjudicando a empresas, pero esta situación se puede resolver resolviendo el cifrando archivos que se envían y recepcionan la red.

Existen los siguientes protocolos que puedes mencionar:

- **IPsec (Internet Protocolo Security):** Mejora la seguridad a través de diagramas de flujos cifrado con volumen y un sistema de certificación en completo. IPsec tiene dos técnicas para encriptar, modo transporte y modo túnel, soporta encriptado de 56 bit y 168 bit triple DES.
- **PPTP/MPPE:** tecnología fue desarrollada por un consorcio formado por varias empresas. PPTP que soporta varios protocolos VPN con cifrado de 40 bits y 128 bits utilizando el protocolo Microsoft Point To Point Encryption MPPE y PPTP por sí solo no cifra la información de la red.
- **L2TP/IPsec (L2TP sobre IPsec)**: tecnología es eficiente de proveer el nivel de protección de IPsec sobre el protocolo de túnel L2TP, al igual que PPTP, L2TP no desencripta la información por sí mismo.

3.1.3 Seguridad de los datos

La seguridad aplicando VPN podemos elaborar túneles para integrar los paquetes de encriptación entre los clientes y empleados por lo cual, si existe una integridad seguro de los datos, además de ser modificados o alterados durante la transmisión de datos.

3.1.3.1 Tasa de transferencia.

Se envía lo solicitado en datos de información por medio de una red VPN es comprimida y descomprimida en dicheros al servidor el cliente de la VPN realiza la subida o bajada del fichero, esto hace que la VPN se más eficiente con la transferencia de información de datos.

3.1.3.2 Costos.

Elaborar una VPN me permite ahorra en costos de comunicación entre equipos y otros servidores de conexión de red local o intranet lan.

3.1.4 Componentes de una conexión VPN

Según el tipo de VPN necesita implantar algunos componentes para crear la VPN. Estos pasos podrían incluir:

- Cliente de software de escritorio para cada usuario remoto
- Hardware exclusivo como cisco VPN concentrador o un cisco firewall PIX Secure.
- Un servidor VPN exclusivo para los servicios de acceso telefónico.
- Servicios VPN acceso de usuarios remotos.
- Centro con administración de políticas y una red privada.

3.1.5 Elementos de una conexión de VPN

Tabla 1

Observamos los elementos para una conexión VPN para el cual se detalla.

Elementos	Detalles
Servidor	Administra clientes VPN
Cliente	Clientes Remotos
Túnel	Encapsulamiento
Conexión	Encriptación de datos
Protocolos en Túnel	Control de Túneles
Datos de Túnel	Datos que se transmiten
Red de Transito	Red Pública de enlace

Fuente: Pillou,2007

3.1.6 Implementaciones en VPN

3.1.6.1 VPN entre redes locales o intranet.

Una corporación propone red de área local o lan, en ella encontramos características de un uso exclusivo para utilizar HTML y el TCP/IP protocolos que permiten la interacción con la línea de la internet, ello nos permite el acceso a la red remota desde casa o mientras viaja.

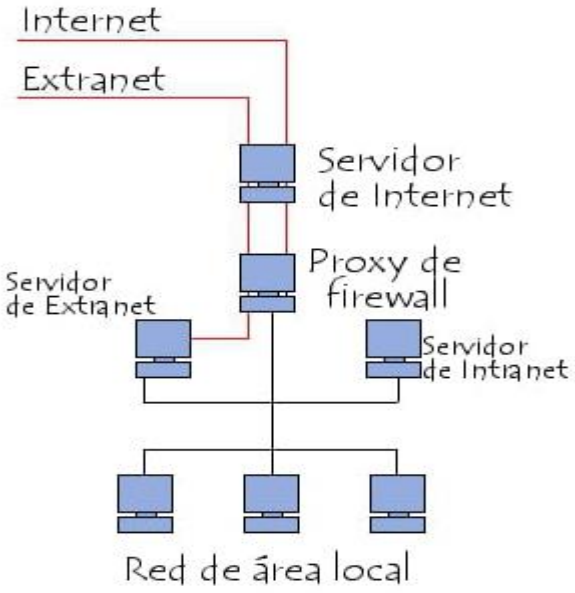

Figura 1. Ver redes locales o intranets

Fuente: Pillou,2007

3.1.6.2 VPN de acceso remoto.

Si nos encontramos en una corporación u empresa quiere acceder red de área local o lan desde un ordenador remoto, puede establecer una VPN de este tipo entre este ordenador y la intranet de la empresa. Ejemplo, una pc que el empleado tiene en su casa, o laptop portátil para el cual se conecta en la red de la empresa cuando está de viaje y para lugares lejanos a la ciudad .

3.1.6.3 VPN extranet.

La extensión de la conectividad a socios corporativos y proveedores es costosa y numerosa en un entorno de red privada, las conexiones dedicadas deben extenderse al socio, y políticas de administración, acceso a la red deben negociarse y mantenerse actualizadas, cuando se utiliza el acceso de mercado, la situación es

igualmente complicada porque deben establecerse y administrarse dominios de mercado separados.

Figura 2. Esquema de conectividad de VPN de Extranet

3.1.6.4 Ipsec (protocolo de seguridad del protocolo de internet Pc).

Se proporciona características de seguridad mejoradas como algoritmos de encriptado y la autenticación más amplia, Ipsec contiene cuatro modos de cifrado para la seguridad:

a. Modo transporte.

- Es el host genera los paquetes
- Se encriptan los datos, la cabecera intacta
- Se añade pocos bytes en las cabeceras
- Permite ver las direcciones de origen y de destino

b. Modo túnel.

- Los extremos de la comunicación es un Gateway enlace.
- Se cifra el paquete IP
- El sistema final es transparente y codificado

c. Atributos de ipsec

- Extensión del protocolo IP

- Servicios criptográficos de seguridad basados en estándares en reglas definidos por el IETF
- Encriptación y autenticación a nivel de red
- Transparente al usuario: no se tienen que modificar los sistemas finales.
- Los paquetes tienen la misma apariencia que un paquete IP contiene
- Combina distintas tecnologías: Diffie Hellman, encriptación clave pública, des, funciones hash, certificados digitales.

d. Formatos de paquetes.

- Tenemos dos nuevas cabeceras: Cabecera autenticación AH : asegura la autenticidad y la integridad de los datos incluyendo campos invariables de cabeceras (direcciones origen y destino, por ejemplo)
- Cabecera de encapsulado de seguridad ESP: protege la autenticidad, confidencialidad e integridad de los datos.
- Diferencia: AH asegura partes de la cabecera IP del paquete.

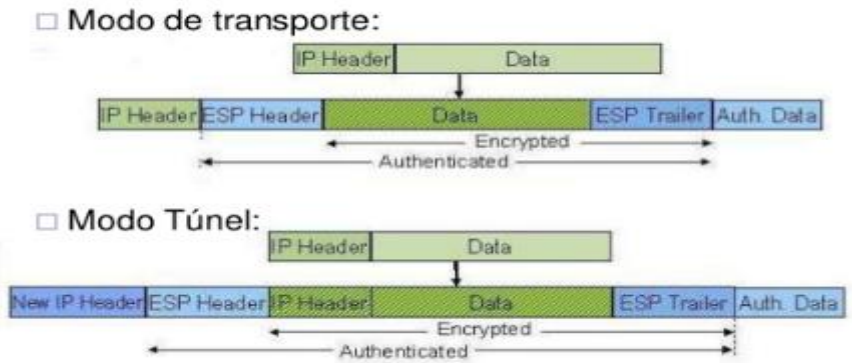

Figura 3. Esquema del IPSEC

Fuente: Nobre, 2013

3.1.6.5. *PPTP/MPPE.*

Point-to-Point Tunneling Protocol fue desarrollado por ingenieros de Ascend Communications, U.S. Robotics, 3Com Corporation, Microsoft, y ECI Telematics para proveer entre usuarios de acceso remoto y servidores de red una red privada virtual VPN.

PPTP fue diseñado para permitir a los participantes puedan conectarse a un servidor desde cualquier punto en internet para tener la misma autenticación, encriptación y los mismos accesos de lan como si se encriptan directamente al servidor. (Adelstein Bill, 2007)

3.1.6.6. *L2TP/IPsec.*

L2TP/IPSec por lo general llamado L2TP sobre IPSec, aporta la seguridad del protocolo Ipsec sobre la tunelización del protocolo tunelización de la capa 2 (L2TP) L2TP es el producto de una asociación entre los miembros del foro PPTP, cisco y el grupo de trabajo de ingeniería en internet (IETF), se utiliza principalmente en las VPN de acceso remoto con sistemas operativos Windows 2000, dado que Windows 2000 proporciona un cliente L2TP e IPSec nativo". (Adelstein Bill, 2007)

3.2 Integridad de datos

Al igual que los ficheros u datos estén cifrados en una Red Pública Local o lan, también es importante verificar que éstos no se hayan cambiado mientras estaban en tránsito. Por ejemplo: Ipsec dispone de un mecanismo que le permite asegurarse de que la parte cifrada del paquete o todo el encabezado y la parte de datos del

paquete, no se haya alterado, si se detecta una alteración, se abandona el paquete, la integridad de los datos también puede implicar una autenticación en remoto.

3.2.1 Autenticación del origen de los datos

Es de gran importancia verificar la identidad del origen de los datos que se envían, esto se debe a la necesidad de protegerse contra los ataques basados en la simulación de la identidad del remitente.

3.2.2 Tunelización de datos/confidencialidad del flujo de tráfico

La tunelización es el proceso que consiste en encapsular un paquete completo dentro de otro paquete y enviarlo por una red, la tunelización de datos es útil en los casos en los que se desea ocultar la identidad del dispositivo de origen del tráfico. Por ejemplo: un único dispositivo que utiliza IPSec encapsula tráfico que pertenece a un determinado número de hosts que tiene detrás y agrega su propio encabezado delante de los paquetes existentes.

3.2.3 Ipsec Protección AH

La AH nos protege los datos u ficheros con un algoritmo de autenticación encriptado. Una ESP protege los datos con un algoritmo de cifrado. ESP puede útil para un mecanismo de autenticación. Si no está atravesando una NAT, puede combinar ESP con AH. Caso contrario se puede usar un algoritmo cifrado con ESP, un algoritmo de modo combinado, como AES-GCM, nos proporciona cifrado y autenticación dentro de un único algoritmo.

El encabezado de autenticación proporciona autenticación de datos, una integridad sólida y protección de repetición para los datagramas IP. AH protege la mayor parte del datagrama IP, como muestra la ilustración siguiente, AH se inserta entre el encabezado IP y el encabezado de transporte.

Figura 4. Encabezado de transporte puede ser TCP, UDP, SCTP o ICMP

Fuente: Grupo de Sistemas Operativos DATSI FI UPM, 2009

Nota : IP Hdr = Datagramas IP ; AH = Cabecera de Autenticación ; TCP Hdr = Encabezado de Transporte .

3.2.4. Des (data encryption standard)

DES (Data Encryption Standard) es un logaritmo en encriptación simétrico desarrollado en 1977 por el Departamento de Comercio y la Oficina Nacional de Estándares de EEUU en colaboración con la empresa IBM, que se creó con objeto de proporcionar al público en general un algoritmo de cifrado normalizado para redes de ordenadores, estaba basado en la aplicación de todas las teorías criptográficas existentes hasta el momento, y fue sometido a las leyes de USA.

Posteriormente se sacó una versión de DES implementada por hardware, que entró a formar parte de los estándares de la ISO con el nombre de DEA. Se basa en un sistema mono alfabético, con un algoritmo de cifrado consistente en la aplicación sucesiva de varias permutaciones y sustituciones. Inicialmente el texto en claro a cifrar se somete a una permutación, con bloque de entrada de 64 bits (o múltiplo de 64), para posteriormente ser sometido a la acción de dos funciones principales, una función de permutación con entrada de 8 bits y otra de sustitución

con entrada de 5 bits, en un proceso que consta de 16 etapas de cifrado (University of Malaga, 2014)

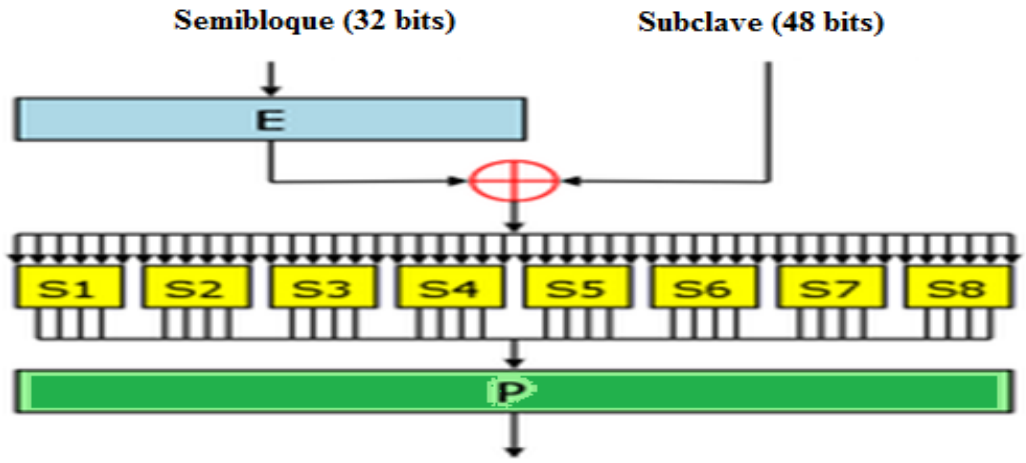

Figura 5. Criptografía Esquema
Fuente: Universidad Tribhuvan de Katmandú ,2016

3.3 Firewall

Es también llamado cortafuego para proteger nuestro sistema pc o red lan, wifi de nuestra empresa, además es un dispositivo que filtra el tráfico entre redes, ya que circulan muchos virus que bloquean nuestros puertos y comunicaciones, se trata de un software instalado dentro de un computador capaz de controlar todo evento dentro de nuestras redes.

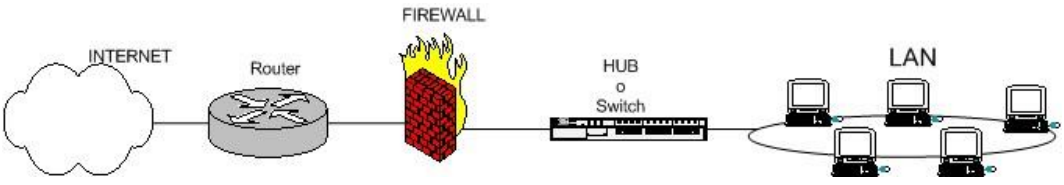

Figura 6. Esquema de Firewall típico entre red local e internet.
Fuente: Goncalvez,2002

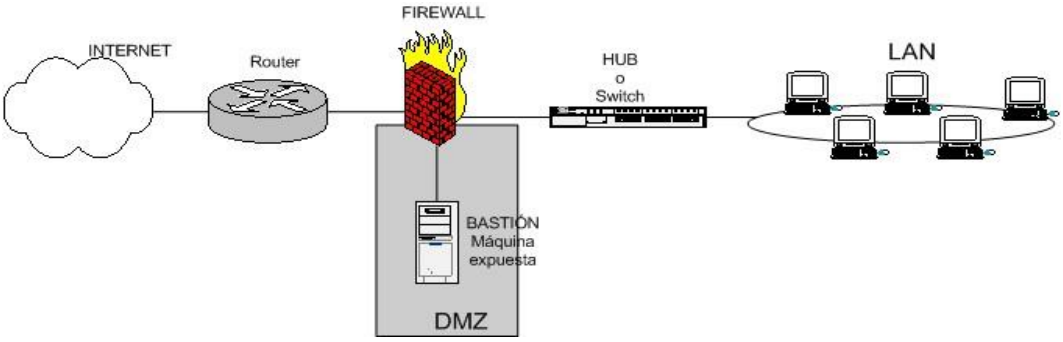

Figura 7. Esquema de Firewall típico entre red local e internet con zona DMZ para servidores
Fuente: Goncalvez,2002

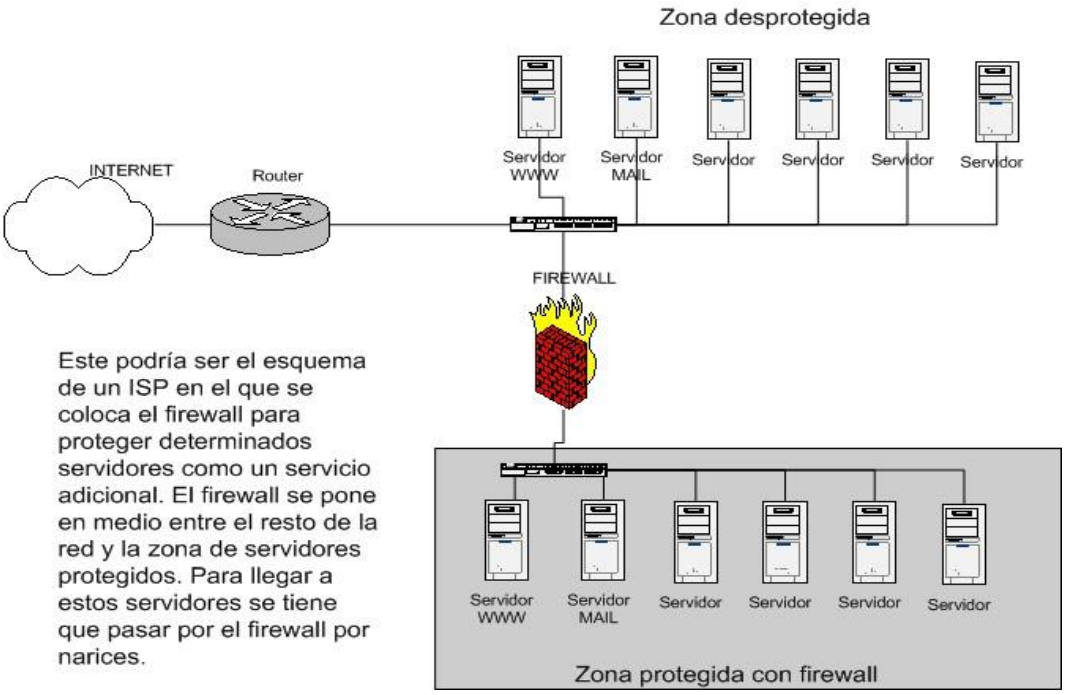

Figura 8. Esquema de firewall típico entre redes, en las que solo se filtran y no se hacen NAT
Fuente: Goncalvez,2002

3.4 Iptables

Se conoce como herramienta de cortafuegos que me permite filtrar los paquetes de entrada y salida dentro del CentOS 6.5, realizar traducción de direcciones de red (NAT) o mantener registros de log, puertos de internet, se pueden realizar operaciones de cadenas:

- Se elabora una nueva cadena (-N).

- Se Borra enlace a Vacío (-X).
- Se puede cambiar la política de un enlace de uso céntrico (-P).
- Visualizan las normas de un enlace (-L).
- Visualizan las normas un enlace (-F).
- Iniciar en 0 para los contadores de paquetes y bytes del total las reglas de un enlace (-Z).

3.4.1. Qué verá cuando el ordenador arranque

Bueno iniciar la orden de iptables, habrá normas de reglas en ninguna de las cadenas de uso interno («INPUT», «FORWARD» y «OUTPUT»), todas las reglas contendrán la política de ACCEPTAR. Se puede alterar la política por defecto de FORWARD proporcionando la opción «forward=0» al módulo iptable_filter.

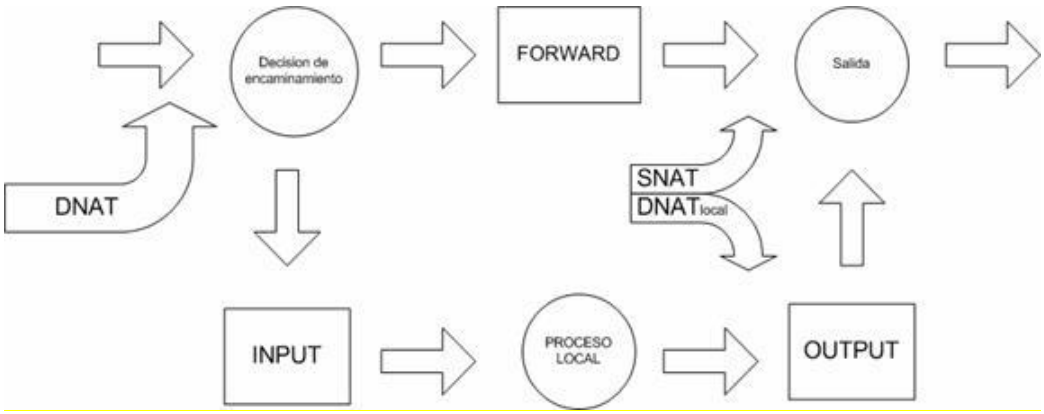

Figura 9. La comunicación que llegan al kernel para la iptables entrada y salida.

Fuente: García,1995

3.5 Desarrollo de la solución

3.5.1 Instalado servidor VPN Linux

Para CentOS 6.5 tener una infraestructura es compartida, se puede dar conectividad a menor costo con redes locales en una VPN.

Figura 10. Insertando disco DVD de instalación de CentOS-6.5-i386-LiveDVD

Figura 11. Ventana de instalador CentOS-6.5

3.5.2 Descripción de almacenamiento básicos disco físico

Figura 12. Dispositivo de almacenamiento básico

Unidad de almacenamiento libre: 20473

Figura 13. Creando diseño personalizado de particiones del disco

Añadiendo particiones

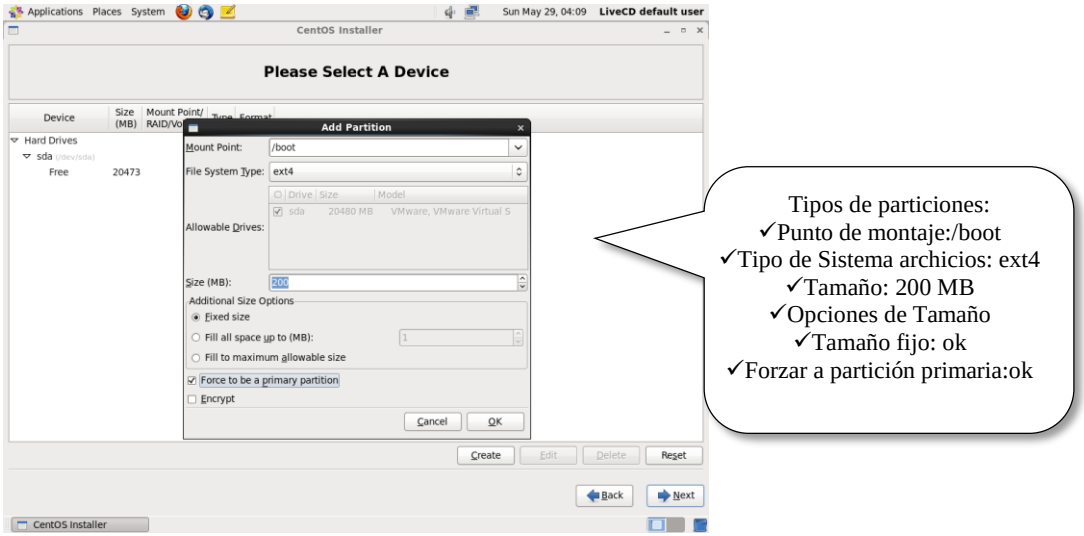

Figura 14. Añadiendo partición /boot

3.5.3 Particiones a configurar básicas

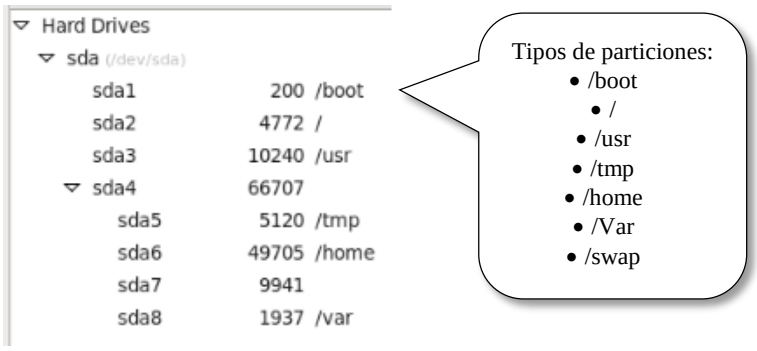

Figura 15. Añadiendo particiones principales

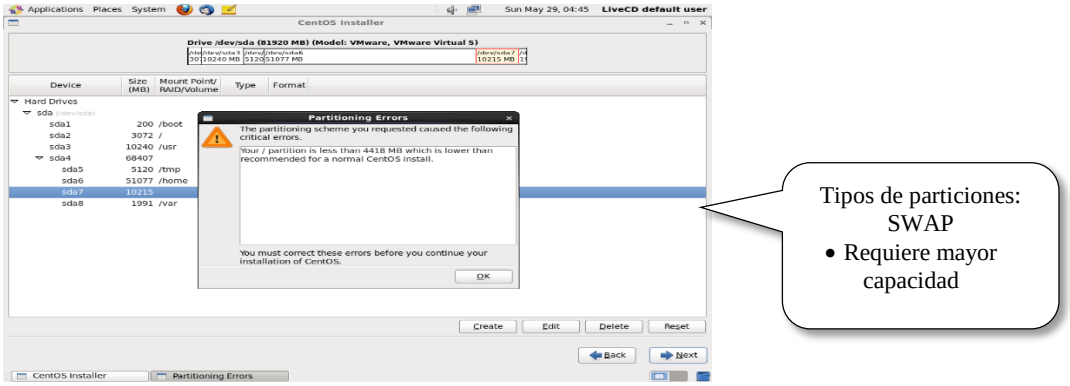

Figura 16. Tamaño de partición de memoria intercambio SWAP es bajo 4418

Configurando contraseña Linux hdd

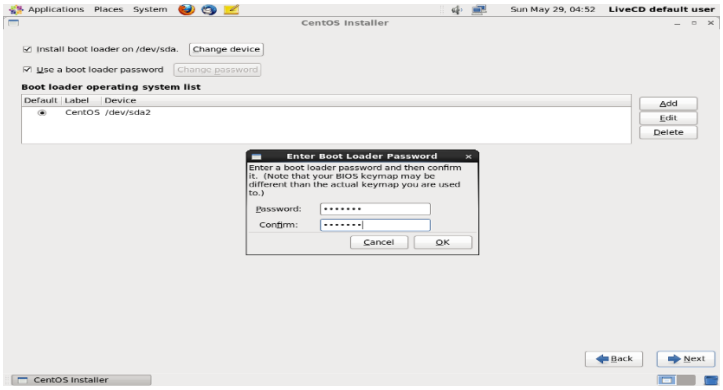

Figura 17. Usar contraseña /boot

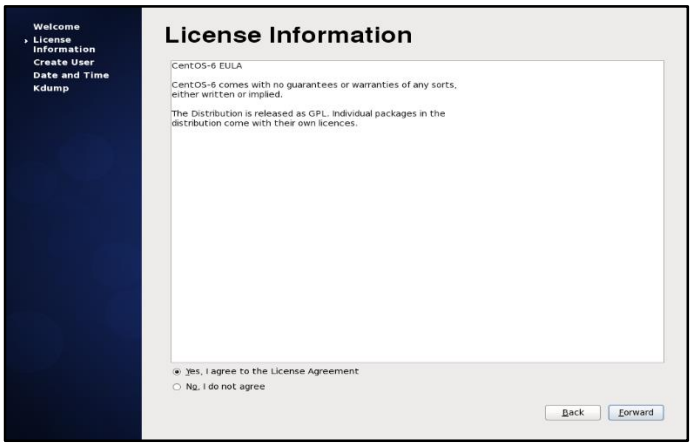

Figura 18. Licencia de distribución CENTOS 6 y Versión de Kdump

Figura 19. Kdump

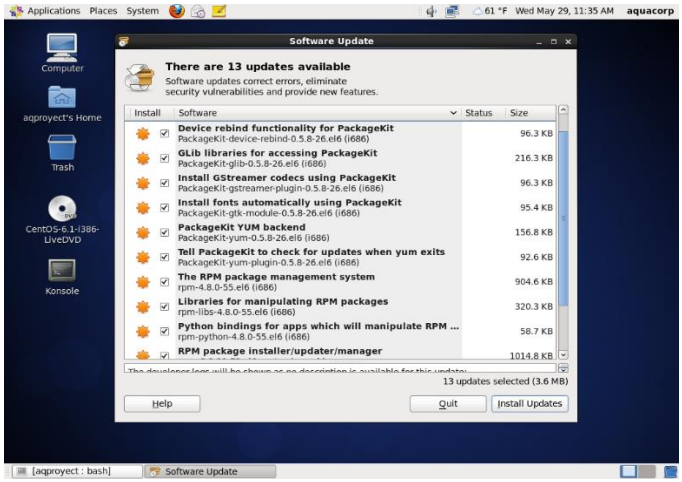

Figura 20. Packge por instalar y actualizaciones

CentOS 6 ingresando a usuario aquacorp Empresa

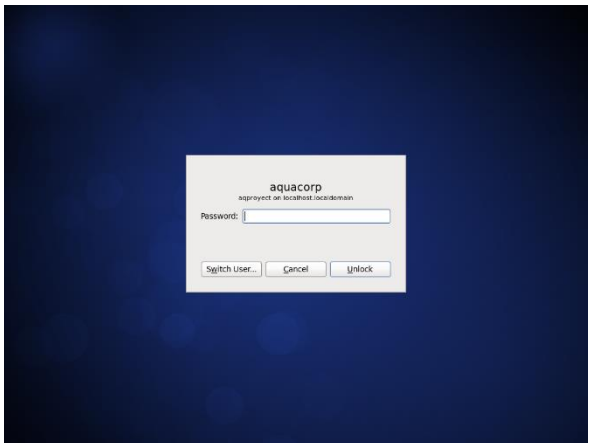

Figura 21. Ingreso como usuario y password

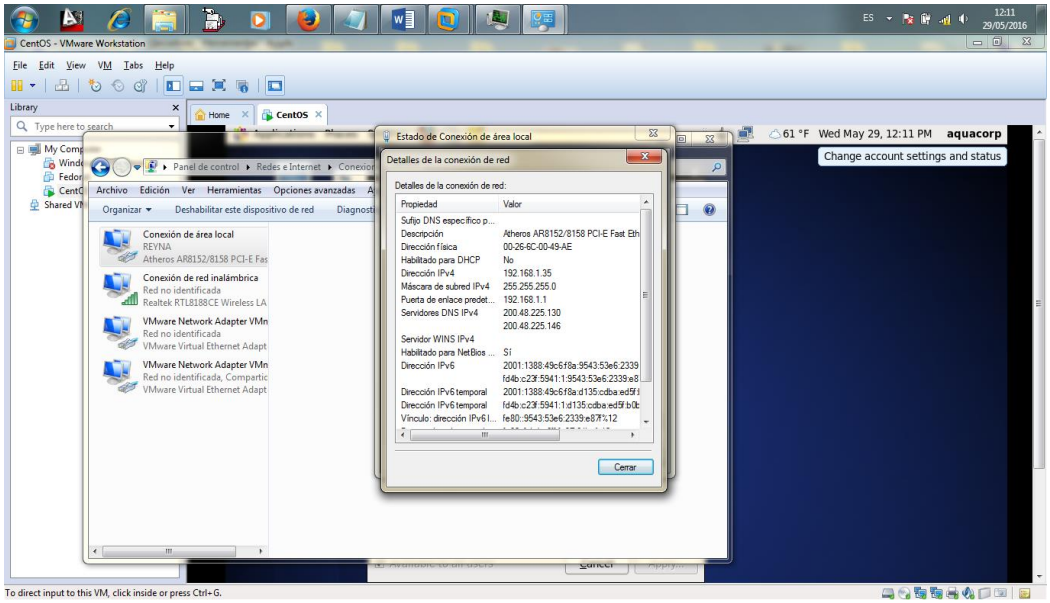

Figura 22. Configurando ip del cliente en Windows 7

3.5.4. Install dhcp

[root@localhost -] #rpm –q dhcp si existe fichero

[root@localhost -] # Yum install -y dhcp * instalando

[root@localhost -] # Yum install –y bind*

[root@localhost -] # yum install -y bind bind-choot bind-libs bind-utils caching-nameserver

Instalando : bind-libs.i686 9.8

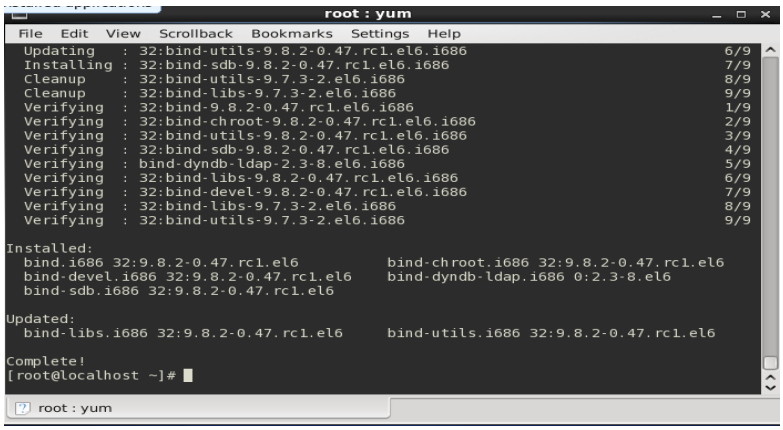

Figura 23. Instalando complementos.

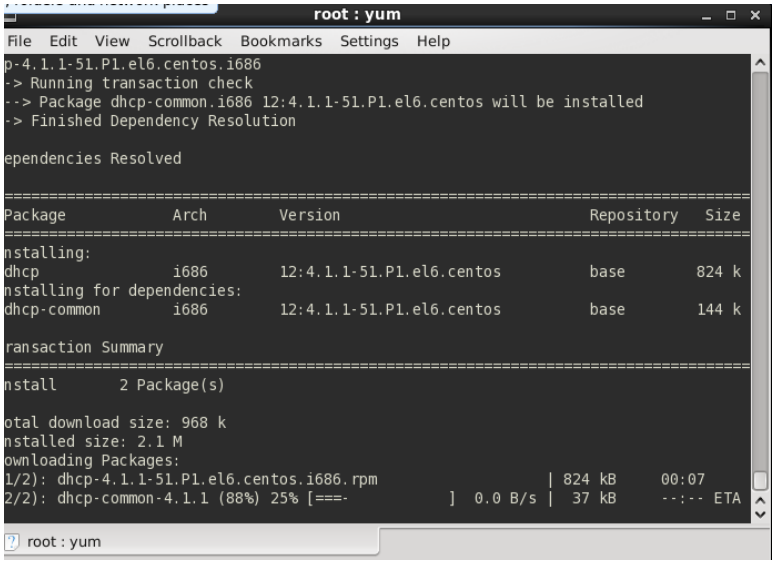

Figura 24. Install Dhcp.

3.5.4.1. Configurando tarjeta de red : eth0.

[root@localhost -] # /etc/sysconfig/network-scripts/ifcfg-eth0

Interfaces

Static IP Address:

DEVICE=eth0

ONBOOT=yes

BOOTPROTO=static

IPADDR=192.168.1.30

NETMASK=255.255.255.0

GATEWAY=192.168.1.1

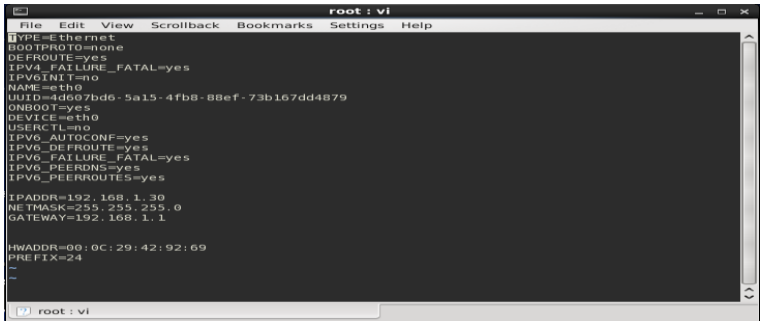

Figura 25. Configurando eth0

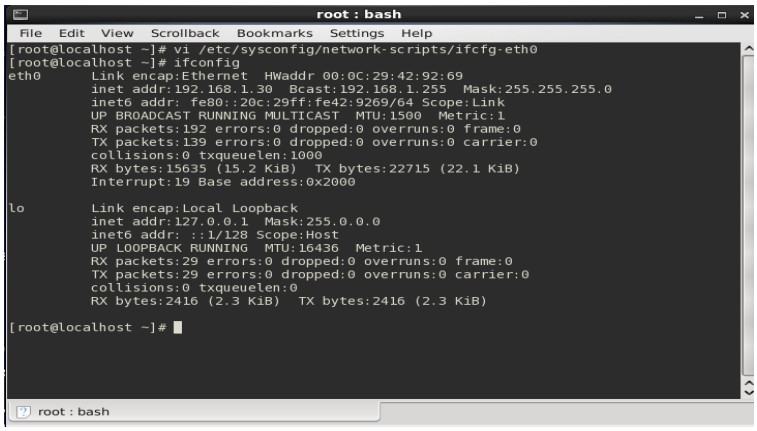

Figura 26. Configurando ifconfig comando

[root@localhost -] # yun install Squid 3.1

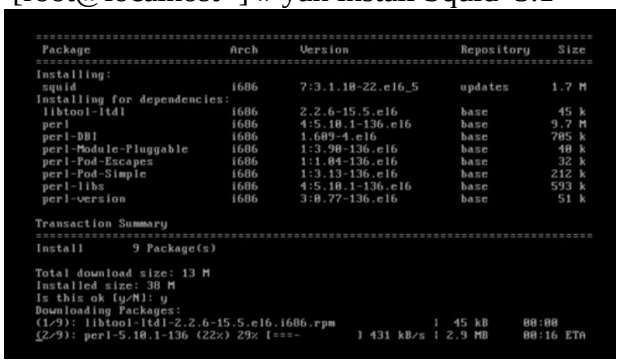

Figura 27. Install Squid 3.1

Fuente: Txaber Guereta, 2017

3.5.4.2. Configurando Squid.

[root@localhost -] # vi /etc/Squid/ Squid.conf

Esta lista que define el método:

acl password proxy_auth REQUIRED

#Listas de control de acceso por defecto para cualquiera pc:

acl all src 0.0.0.0/0.0.0.0 acl localhost src 127.0.0.1/255.255.255.255

Listas que definen grupo de redlocal src "/etc/Squid/redlocal"

acl privilegiados src "/etc/Squid/privilegiados"

acl restringidos src "/etc/Squid/restringidos"

acl administrador src 192.168.1.254

Listas que definen palabras contenidas en un URL acl porno, paginas prohibidas para menores de edad url_regex "/etc/Squid/porno"

Contenido:

sex

porn

girl

celebrit

extasis

drug

playboy

hustler

Listas que definen tipos de extensiones

Se define lista estricta de extensiones prohibidas acl multimedia sonido y video urlpath_regex "/etc/Squid/multimedia"

Contenido:

\.mp3$ # \.avi$ # \.mov$ # \.mpg$ # \.bat$ # \.pif$ # \.sys$ # \.lnk$ # \.scr$ # \.exe$

Define una lista en extensiones prohibidas acl peligrosos u sospechosas para virus urlpath_regex "/etc/Squid/peligrosos"

Contenido: # \.bat$ # \.pif$ # \.sys$ # \.lnk$ # \.scr$ # \.exe$

Define una sola extensión acl realmedia urlpath_regex \.rm$

Reglas de control de acceso

Regla por defecto:

http_access allow localhost

Las reglas de control de acceso para ususarios en la red

http_access allow restringidos password !porno !multimedia

http_access allow redlocal password !porno !peligrosos

http_access allow privilegiados password !peligrosos

http_access allow administrador

http_access allow noporno all

Regla por defecto para sus efectos aplicamos resetear CentOS 6.5:

http_access deny all

[root@localhost -] #service Squid restart

3.5.4.3. Configuramos navegador puerto al navegador web: 3128.

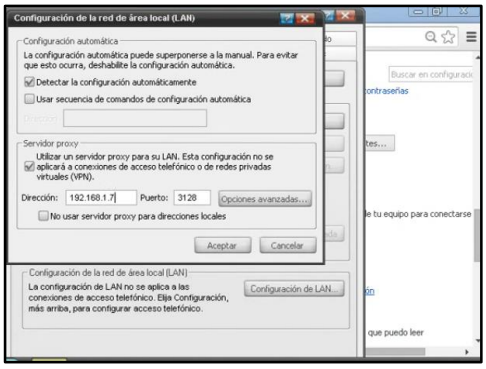

Figura 28. Configurando proxy

Primera prueba de error acceso denegado por/root

Figura 29. Realizando pruebas

[root@localhost -] # service iptables start

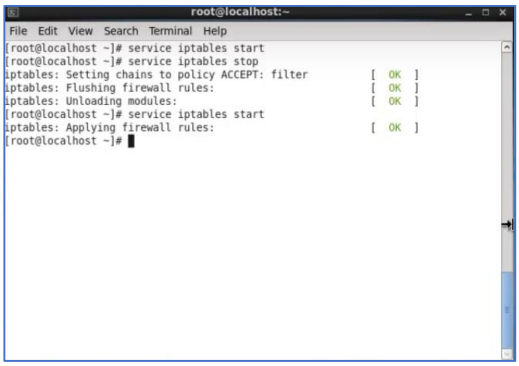

Figura 30. Servicio de iptables

[root@localhost -] #service iptables stop

[root@localhost -] #service iptables status

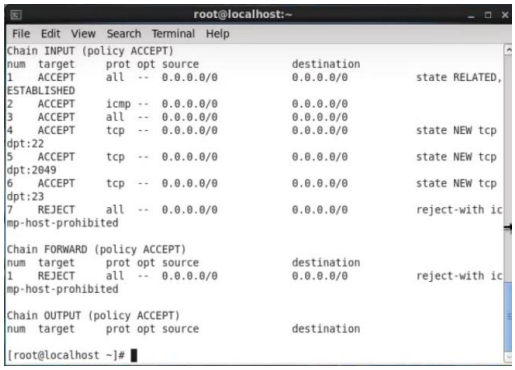

Figura 31. Configurando iptables

[root@localhost -] vi /etc/sysconfig/iptables

Figura 32. Configurando iptables modo reglas

3.5.4.4. Script de reglas iptables.

iptables -f input

iptables -f forward

iptables -f output

iptables -f -t nat

iptables -a forward -i eth1 -o eth0 -j ACCEPT

iptables -a forward -i eth0 -o eth1 -m state --state ESTABLISHED, RELATED -j ACCEPT

iptables -a input-i eth0 -m state --state ESTABLISHED, RELATED -j ACCEPT

iptables -a input-i eth1 -s 0/0 -d 0/0 -j ACCEPT iptables -A INPUT -i lo -s 0/0 -d 0/0 -j ACCEPT

iptables -a POSTROUTING -t nat -s 170.10.10.1/24 -o eth0 -j SNAT --to-source x.y.z.c.

iptables -a input -i eth0 -s 170.10.10.1/32 -j DROP

iptables -a input -i eth0 -s 170.10.10.10/24 -j DROP

iptables -a input -i eth0 -s 127.0.0.0/8 -j DROP

iptables -a input -p tcp -s 0/0 -d 0/0 --destination-port 25 --syn -j ACCEPT iptables -a input -p tcp -s 0/0 -d 0/0 --destination-port 80 --syn -j ACCEPT iptables -a input -p tcp -s 0/0 -d 0/0 --destination-port 443 --syn -j ACCEPT iptables -a input -p tcp -s 0/0 -d 0/0 --destination-port 22 --syn -j ACCEPT

iptables -a input -p tcp -s 0/0 -d 170.10.10.15/32 --destination-port 25 --syn -j ACCEPT

iptables -a input -p tcp -s 0/0 -d 0/0 --destination-port 110 --syn -j ACCEPT iptables -a input -p tcp -s 0/0 -d 0/0 --destination-port 995 --syn -j ACCEPT iptables -a input -p tcp -s 0/0 -d 0/0 --destination-port 143 --syn -j ACCEPT iptables -a input -p tcp -s 0/0 -d 0/0 --destination-port 993 --syn -j ACCEPT

iptables -a input -i eth1 -p tcp --sport 68 --dport 67 -j ACCEPT iptables -a input -i eth1 -p udp --sport 68 --dport 67 -j ACCEPT

iptables -a input -p udp -s 170.10.10.2/32 --source-port 53 -d 0/0 -j ACCEPT

3.5.4.5. Acceso remoto CentOS 6 con interfaz gráfica.

Instalar modo gráfico Gnome.

Configurar los repositorios EPEL y Linux.

```
bash# rpm -Uvh https://dl.fedoraproject.org/pub/epel/7/x86_64/e/epel-release-7-8.noarch.rpm
```

```
rpm -Uvh http://li.nux.ro/download/nux/dextop/el7/x86_64/nux-dextop-release-0-1.el7.nux.noarch.rpm
```

Crear repositorios locales en CentOS 6, Crear nuestro archivo de repositorio, para ello abrimos un editor de texto y creamos un archivo con el nombre xrdp.repo.

```
bash# nano /etc/yum.repos.d/xrdp.repo.
```

Copiamos el siguiente contenido en el archivo.

```
[xrdp]
name=xrdp
baseurl=http://li.nux.ro/download/nux/dextop/el7/x86_64/
enabled=1
gpgcheck=0
```

Instalamos xrdp desde los repositorios.

```
bash# yum -y install xrdp tigervnc-server
```

Una vez instalado iniciamos el servicio.

```
bash# systemctl start xrdp.service
```

Verificamos el puerto de escucha, por defecto es el puerto 3389.

```
bash# netstat -antup | grep xrdp
tcp   0   0   0.0.0.0:3389       0.0.0.0:*   LISTEN   1508/xrdp
tcp   0   0   127.0.0.1:3350   0.0.0.0:*   LISTEN   1507/xrdp-sesman
```

Si queremos habilitar el servicio para que inicie con el sistema.

```
bash# systemctl enable xrdp.service
```

A continuación, hay que crear una regla para que el firewall permita la conexión RDP desde las máquinas externas, el siguiente comando añadirá la excepción para el puerto TCP (3389).

```
bash# firewall-cmd --permanent --zone=public --add-port=3389/tcp
bash# firewall-cmd --reload
```

Cambiamos el contexto de seguridad SELinux.

```
bash# chcon --type=bin_t /usr/sbin/xrdp
bash# chcon --type=bin_t /usr/sbin/xrdp-sesman
```

Para realizar un test de conexión remota desde Windows nos dirigimos al buscador de Windows, y escribimos “Conexión a escritorio remoto” aparecerá una ventana como la siguiente (Server World, 2007)

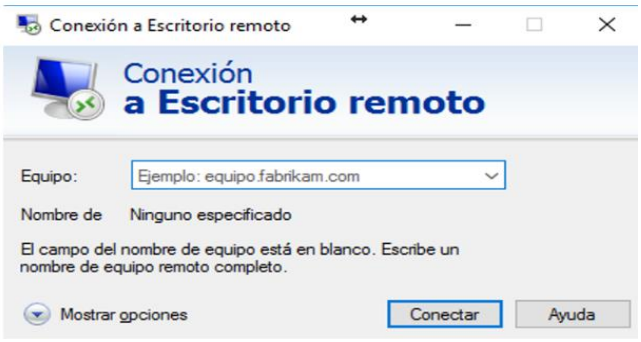

Figura 33. Conexión remota

Fuente: Server World,2007

3.6 Caso práctico

3.6.1 Causas incidentes de la Empresa Acuacorp

Los empleados ingresan a páginas institucionales del estado en línea, por ello en la red se incrustar maliciosos malware a base de datos en Oracle en sistema financiero y logístico, correos con adjuntos .exe, páginas web de dudosa reputación, redes de datos con poca seguridad en ejecución de servicios y puertos abiertos.

Para ello es necesario aplicar seguridad informática que faciliten la notificación a los administradores y/o responsables de la seguridad de la información a fin de responder oportunamente a estas amenazas, se implanta utilizar VPN en Linux para respaldar la seguridad.

3.6.2 Consecuencias el servidor proxy es vulnerable a un ataque de denegación de servicios al manejar conexiones SSL/TLS

La primera medida es deshabilitar por completo el protocolo https, de esta forma al no poder conectarse un cliente a una web que utilice este protocolo.

```
1 acl HTTPS proto HTTPS
2 http_access deny HTTPS
```

Figura 34. Servidor Proxy

Fuente: Sanz ,2010

La segunda medida es la de retransmitir el tráfico https a través de un servidor proxy no vulnerable, de esta manera todas las peticiones se podrán realizar sin tener el problema de seguridad.

La tercera medida que podemos tomar es la de bloquear todos los puertos de las conexiones https menos el 443 (el típico para este tipo de conexiones), de esta forma evitaremos ataques simples que podrían provocar el fallo del servicio.

3.6.3 Aplicando Sarg

Utilizando Sarg (Squid analysis report generator), como herramienta desarrollada para realizar reportes, pudiendo saber qué usuarios accedieron a qué sitios, a qué horas cuantos bytes han sido descargados, relación de sitios accedidos denegados, errores de autentificación entre otros, la flexibilidad que puede obtener con sarg

muy alta, principalmente para las empresas que quieren tener un control de accesos y ancho de banda de acceso a internet y otros (Ravi Saive, 2014)

3.6.4 Estadística de Sarg

Nos dirigimos a estadística de los reportes realizados durante 2016 que es una base datos del aplicativo sarg, allí analizaremos los virus, maliciosos y otros que se encuentran en nuestra red VPN.

Se presenta una tabla de incidentes que fueron detectados en la empresa Aquacorp durante el año 2016, en la primera gráfica se muestran la cantidad de eventos detectados agrupado por trimestres.

Tabla 2

Muestra de datos obtenidos en la Empresa Aquacorp se describen a continuación:

		enero	febrero	marzo	abril	mayo	junio	julio	agosto	septiembre	octubre	noviembre	diciembre
1	Fuerza bruta	252	2917	289	800	6027	15833	6852	7332	3348	932	1135	186
2	Bots	4	26	1	38	91	61	4	54	25	4	0	0
3	Malware	3	11	0	3	19	142	25	114	42	4	2	0
4	Error de configuración	1	1	9	0	0	1	0	3	11	10	1	3
5	Ddos	1	2	0	2	1	0	12	27	0	0	0	0
6	Spam	1	1	3	2	15	5	3	14	14	10	5	7
7	Otros	0	1	2	4	1	5	0	3	6	1	1	2
	Totales	262	2959	304	849	6154	16047	6896	7547	3446	961	1144	198

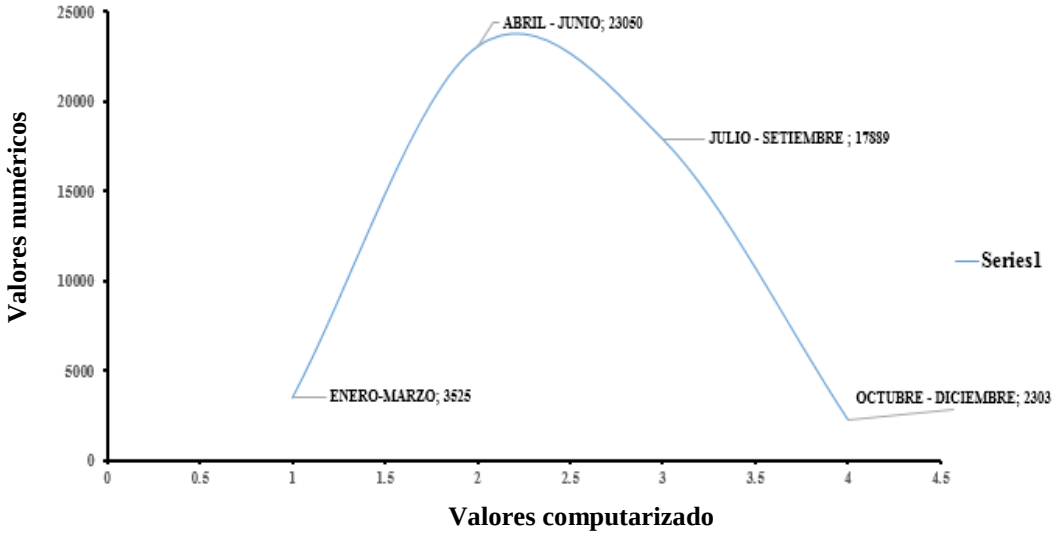

Figura 35. Incidencia detectados empresa Aquacorp

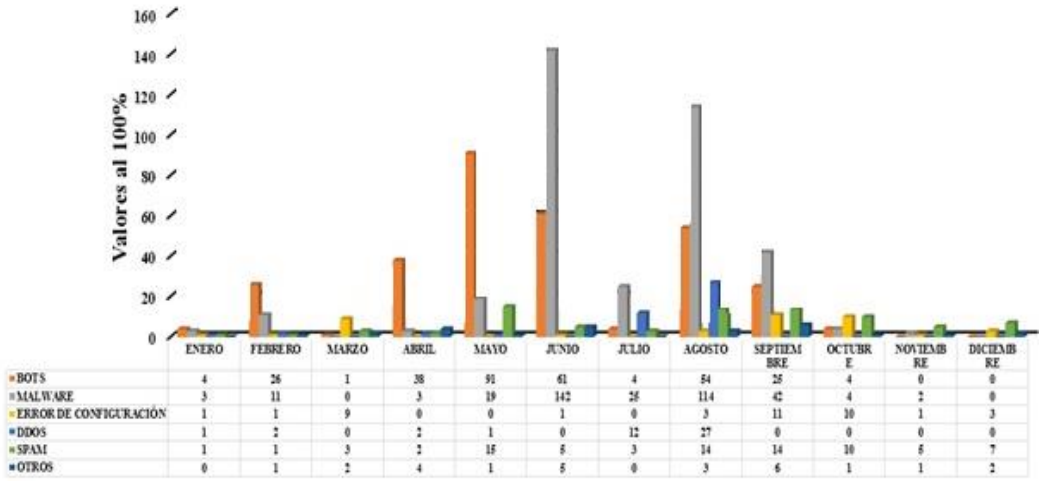

Figura 36. Tipos de Incidencias 2016

Nota: En la categoría otros se agrupan los incidentes que por su baja ocurrencia no se desglosan de manera individual. Entre estos incidentes se encuentran: redireccionamientos, XSS, SQLi, phishing y Web Shell.

3.6.5 Evolución de los principales incidentes en 2016

La presente evolución de incidentes que son tres con máximo número de eventos detectados por el año 2016 se observan ataques de fuerza bruta, malware y bots. Podemos reconocer los ataques de fuerza bruta siguieron siendo creciente a lo largo

del año y aumentaron cantidades de igual que malware, que se muestra como el tercer tipo de incidente con mayor número de registros.

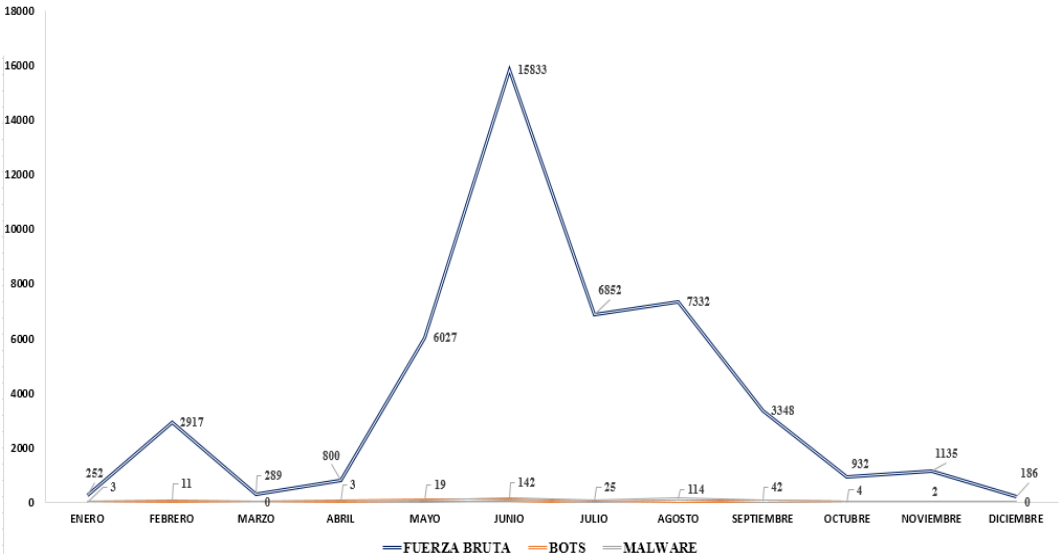

Figura 37. Evolución de los principales incidentes en 2016.

3.6.6 Ataques malware

El tipo incidente más sobresaliente por la cantidad de reportes que se generaron durante los meses de junio, julio y setiembre, es sin duda malware se presenta una gráfica que se ilustran el alza de eventos detectados durante los meses más activos.

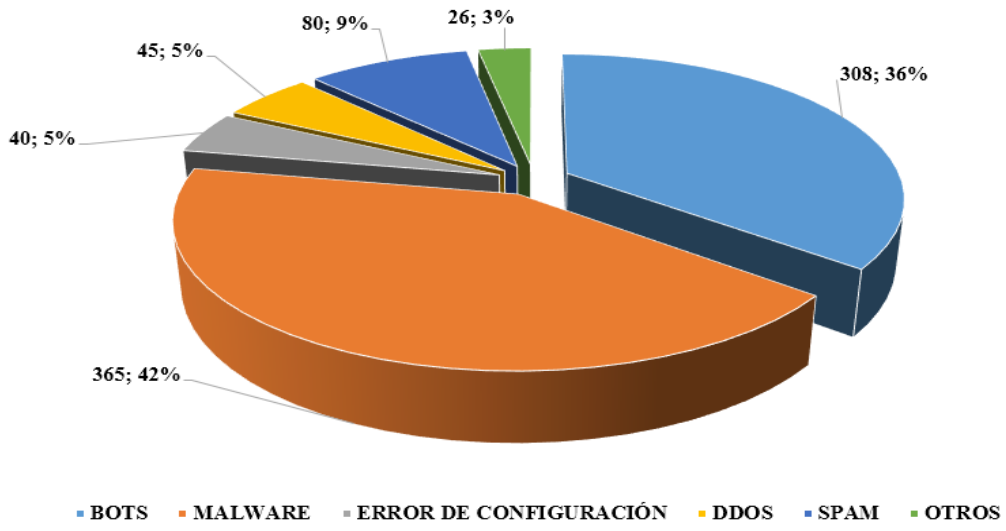

Figura 38. Registro de Evolución II

Tabla 3

Muestra la estadística por los trimestre dentro de un año.

	Trimestre 1	Trimestre 2	Trimestre 3	Trimestre 4
No. de reportes	3525	23050	17889	2303

3.6.7 Herramienta de modelado Sarg

El modelado, clasificación, recopilación de la información en tiempo real.

SITIO ACCEDIDO	CONEXIÓN	BYTES	%BYTES	ENTRADA - CACHE	SALIDA	TIEMPO UTILIZADO
www.yotube.com	44	7.34M	10.50%	0.56%	99.60%	0:03:45
ds.serving-sys.com	23	4.34M	6.50%	0.56%	100.00%	0:01:45
www.aprendemosphp.com	2.7K	3.34M	12.50%	7.56%	99.60%	0:03:45
lax-triple.com	2	3.34M	2.50%	0.56%	100.00%	0:03:45
www.comercio.com.pe	3.3	3.34M	1.50%	0.56%	87.60%	0:12:45
www.videosboysfood.com.pe	1	3.34M	1.50%	2.56%	99.60%	0:03:45
www.adultos.com.pe	79	3.34M	4.50%	0.00%	99.60%	0:03:45
www.diseñograficos.com	19	5.34M	3.50%	0.00%	100.00%	0:11:45

Figura 39. Squid analysis report generator - user

3.6.8 Glosario de términos

- VPN. Una red privada virtual en inglés: virtual private network (VPN) es una tecnología de red de computadoras que permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como internet.
- Dhcp. (Dynamic Host Configuración Protocolo), en español es conocido como "protocolo de configuración dinámica de host", es un servidor que usa protocolo de red de tipo cliente/servidor .
- IPsec. (abreviatura de internet protocolo security) 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.
- Sarg. Generador de informes de análisis de calamares y herramienta de monitoreo de ancho de banda de internet.

- Kdump se define como mecanismo para kernel en Linux a la comunicación sobre el descenso del sistema, crea una imagen de la memoria (vmcore) que pueda ayudar a determinar las causas del problema.
- Kernel. El kernel Linux es el componente central de un sistema operativo GNU/Linux como opensuse, un kernel se encarga de manejar los recursos hardware como la cpu, la memoria, los discos duros, y proporciona abstracciones que le dan a las aplicaciones una visión consistente de esos recursos.
- Boot partición de arranque (/boot): en esta partición va en el núcleo del sistema aquí Linux y el kernel.
- Servidor proxy. Es un servidor programa o dispositivo, que hace de intermediario en las peticiones de recursos que realiza de un cliente (A) a otro servidor (C).
- Proxy local. La dirección el servidor proxy es una puerto utilizado por defecto 8080. Acceso para servidores IR, mediante la dirección IP realiza conexión internet.
- Internet satelital. Es un método de conexión vía área a internet utiliza un medio de enlace un satélite.
- Modo túnel. Es lo que permite a las VPN funcionar como lo hacen permite a un usuario conectarse de forma remota a una red, entre otras cosas, con una dirección Ip que no es parte de la red local.
- Latencia. Es el tiempo que lleva que los datos desde su dispositivo lleguen a la ubicación del servidor VPN, medido en milisegundos (ms).
- Firewall. Es un dispositivo que filtra el tráfico entre redes, como mínimo dos.

- Acceso Remoto. Es una solución de conectividad remota una red global increíblemente rápida y segura con cimentamos el camino hacia un espacio de trabajo tiempo real.

3.7. Representación de resultados

Aplicando CentOS 6.5 sea configurando e instalado como se detalla:

- Sea configurado particiones: /boot, /, /usr, /home,/var,/ swap en un Hard Disck.
- Sea creado usuario contraseña para root.
- Se acepto la licencia libre de Kdump.
- Sea instaló dhcp.
- Configuraciones de tarjetas: Eth0 y Eth1.
- Sea configurado el Squid 3.1.
- Sea realizado la prueba en navegador web proxy.
- Aplicando la herramienta de sarg, se pudo aplicar estadística se detalla:
- Partimos de datos estadística de bots, malware, error de configuración, ddos y Spam se pretende realizar el análisis de gráficos de tablas.
- Análisis de los datos por trimestre de tipo de incidencia: Fuerza bruta tiene más alto nivel.
- De menor cantidad de incidencia encontramos: Error de configuración, se relacionan los datos de administradores de redes
- La totalidad de incidencia se muestra en tabla 1.2. se muestran en trimestre la cantidad de 46,767.00 incidencias.

CAPÍTULO IV

CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

Primera. Este trabajo final concluye exitosamente en la implantación de CentOS 6.5, sistema basado en linux se ha logrado mejorar la seguridad de 98 % en la VPN y la seguridad informática en los sistemas financiero y logística para la empresa Acuacorp.

Segunda. Se aplicó políticas de red en eth0 y eth1 para bloquear puertos, páginas web y dominios en el puerto 8080, se mejoró la optimización de la seguridad informática en un servidor VPN.

Tercera. Se configuró Squid en Linux sobre un VPN para mejorar la administrar los usuarios, accesos remotos, unidades lógicas e ingresos a los sistemas lógicos con reglas.

Cuarta. Aplicar sarg herramienta para reportes estadística en tiempo real permite detectar un registro de incidencias de virus, malware, bloqueos de claves y Span, nos da una visión específica del cálculo estadístico y un modelo a seguir aplicando en futuros servidores en las VPN.

4.2 Recomendaciones

Primera. Tener actualizado linux y sus componentes para así actualizar paquetes de ERP en nuestras políticas de red, bloqueos puertos y páginas web.

Segunda. Se pide realizar actualizaciones de iptables y squid.

Tercera. Monitorizar y/o detectar intrusos en nuestra VPN es posible una de ellas es tomando como referencia modelo de Sarg para así predecir posibles ataques en nuestro entorno de trabajo lan, wan.

Cuarta. Este trabajo está enfocado hacia los administradores de servidores windows y linux ya que es diario supervisar, detectar las posibles incidencias dentro de una VPN o estaciones de trabajo.

REFERENCIAS BIBLIOGRÁFICAS

Adelstein Bill. (2007). *Administración de Sistemas Linux*. Madrid : Ediciones Anaya Multimedia (Grupo Anaya, Sa) 2007 0-338 pág.

Alcancelibre.Org. (1999). *Ajustes Posteriores a la Instalación de CentOS 6.5.* Recuperado de http://www.alcancelibre.org/staticpages/index.php/ajustes-posteriores-CentOS6-instalar

Chamillard, G. (2010). A*dministración de un sistema Linux.* Recuperado de https://www.ediciones-eni.com/open/mediabook.aspx?idR=149cfb5ae21f7adb6e54a7d1b39ea87b

Jimenez,J. (2009). *Servidor proxy squid*. Recuperado de https://rooteando.com/entry/servidor-proxy-squid-sarg-y-dansguardian

Jorba, J. y Suppi, R.(2004). A*dministración de Linux Avanzada*. 08035 Barcelona: Primera Edición. 472 pág.

García, M. (1995). *Uso de iptables*. Recuperado de https://netfilter.org/documentation/HOWTO/es/packet-filtering-HOWTO-7.html

Goncalvez, M. (2002). *Manuales de Firewalls.* Ciudad de México, editorial MCCGRAW-HILL/ Pág. 1-700

Goujon, A. (2012). *¿Qué es y cómo funciona una VPN para la privacidad de la información?* Recuperado de https://www.welivesecurity.com/la-es/2012/09/10/Vpn-funcionamiento-privacidad-informacion/

Grupo de Sistemas Operativos DATSI FI UPM. (2009). *Protocolo Ipsec*. Recuperado de http://laurel.datsi.fi.upm.es/proyectos/teldatsi/teldatsi/protocolos_de_comunicaciones/protocolo_ipsec

Nettix Perú. (2014). *Manual de instalación y configuración.* Recuperado de: http://www.nettix.com.pe/documentacion/manual-de-instalacion-de-un-servidor-CentOS-7

Nobre, A. (2013). Ipsec. Recuperado de https://pt.slideshare.net/andredrops/protocolo-ipsec

Orovengua, J. (2012). *Configurar servidor VPN en linux para clientes windows y linux.* Recuperado de http://www.linux-party.com/index.php/57-seguridad/6834-configurar-servidor-Vpn-en-linux-para-clientes-windows-linux

Pillou, J. (2007). *Intranet y extranet.* Recuperado de https://es.ccm.net/contents/213-intranet-y-extranet

Rioja Telecom. (2008). *Entender las redes privadas virtuales*. Recuperado de http://www.riojatelecom.com/servicios_3_3.html

Ravi Saive. (2014) SARG – *Squid Analysis Report Generator and Internet Bandwidth Monitoring Too. l* Recuperado de https://www.tecmint.com/sarg-Squid-analysis-report-generator-and-internet-bandwidth-monitoring-tool/

Rohaut, S. (2015). *Preparación a la certificación LPIC-1 Linux.* Lugar: México. Editorial ENI Pág. 35 - 45

Sanz, J. (2010). *Iptables configuración del firewall en linux con iptables.* Recuperado de https://www.redeszone.net/gnu-linux/iptables-configuracion-del-firewall-en-linux-con-iptables/

Server World. (2007). *Configuraciones de servidores Linux CentOS.* Recuperado de http://www.server-world.info/query?os=CentOS_7&p=download

Sojo, J. (2014). *Firewall*. Recuperado de http://elservidorsc.blogspot.com/2014/07/firewall.html

Txaber Guereta. (2017) *Descubre algunos de los comandos de linux que no conocías.* Recuperado de https://rootear.com/categoria/ubuntu-linux

University of Malaga. (2014). *Herramientas web para la enseñanza de protocolos de comunicación*. Recuperado de http://neo.lcc.uma.es/evirtual/cdd/tutorial/presentacion/des.html

Universidad Tribhuvan de Katmandú. (2016). *Data Encryption Standard.* Recuperado de https://www.docsity.com/en/data-encryption-standard-2/797564/