ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE INGENIERÍA

DISEÑO DE UNA RED DESMILITARIZADA Y BACKUP DE COMUNICACIÓN PARA PETROCOMERCIAL

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO ESPECIALISTA EN INFORMÁTICA MENCIÓN EN REDES

PAULINA ELIZABETH PINO BOADA
JORGE PAÚL YÉPEZ SUBÍA

DIRECTOR: MSC. ING. PABLO RECALDE

Quito, marzo 2006

DECLARACIÓN

Nosotros, Paulina Elizabeth Pino Boada y Jorge Paúl Yépez Subía, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que he hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedemos nuestros derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

Paulina Elizabeth Pino Boada

Jorge Paúl Yépez Subía

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Paulina Elizabeth Pino Boada y Jorge Paúl Yépez Subía, bajo mi supervisión.

MSc. Ing. Pablo Recalde
DIRECTOR DE PROYECTO

AGRADECIMIENTO

Agradecemos a Dios, a nuestros padres y a las personas que colaboraron en la realización de este proyecto.

CONTENIDO

ÍNDICE GENERAL

TEMA **Pág.**

ÍNDICE DE FIGURAS

TEMA **Pág.**

ÍNDICE DE TABLAS

TEMA **Pág.**

RESUMEN

Este trabajo es un estudio que se realizó con la finalidad de satisfacer los requerimientos de implementar mejoras en la administración de la seguridad de acceso y garantizar la comunicación entre Petrocomercial con otras filiales y entidades gubernamentales, así como el brindar una alternativa emergente en las comunicaciones con las sucursales y terminales de la empresa.

En el **Capítulo 1** se realiza un análisis de la situación actual en lo referente a infraestructura, donde se detalla servidores, equipos de seguridad, dispositivos de comunicación, enlaces existentes y seguridad informática estableciéndose de esta forma la necesidad de definir una zona desmilitarizada acertadas políticas de seguridad.

En el **Capítulo 2** se dan a conocer algunas recomendaciones a nivel de seguridad informática y se detallan alternativas de productos y equipos como soluciones de cortafuegos y redes privadas virtuales que garanticen un respaldo en las comunicaciones, aplicables a Petrocomercial, de igual forma se describen los enlaces existentes con otras entidades indicando cuales son las empresas de tecnología que ofrecen los servicios de comunicaciones. Finalmente se realiza un estudio de la viabilidad económica, técnico y logístico de las alternativas planteadas.

En el **Capítulo 3** se refiere a la implementación y administración del firewall utilizado para definir la zona desmilitarizada y las demás reglas de seguridad necesarias para la empresa. Finalmente se plantea el esquema de respaldo de comunicaciones apropiado, detallando su configuración y características.

PRESENTACIÓN

El presente proyecto tiene por objeto cubrir las falencias en los esquemas de seguridad, así como permitir la funcionalidad de los servicios que Petrocomercial puede ofrecer a través de Internet, definiendo un ambiente de servidores e infraestructura seguro que se puede catalogar como zona desmilitarizada y brindando protección a usuarios internos a través de una eficiente barrera de filtrado utilizando una herramienta de software que permita manejar las políticas de acceso con precisión y eficiencia, controlando el tráfico entrante y saliente de la red y ofreciendo una administración sencilla a través de una interfase gráfica amigable para el usuario.

Por otra parte se pretende generar un esquema de respaldo de comunicación basado en redes privadas virtuales, optimizando los recursos disponibles en la empresa en lo referente a los sistemas operativos utilizados, con lo cual se mantendría operativo un enlace emergente y seguro, garantizando la continuidad del servicio.

Adicionalmente se sustentó la necesidad de definir un servidor proxy utilizando un software robusto y confiable con lo que se mejoró la velocidad de acceso y navegación de los usuarios de la red interna hacia el Internet, pudiéndose implementar a futuro filtrado de contenido y controles de acceso.

CAPÍTULO

I

CAPÍTULO I

ESTUDIO DE LA INFRAESTRUCTURA ACTUAL

INTRODUCCIÓN

Dentro de la infraestructura que posee Petrocomercial se puede mencionar dispositivos de red que trabajan a nivel de capa dos y capa tres del modelo OSI a través de los cuales es posible la interconexión de la matriz con sus diferentes terminales y sucursales; así como componentes basados en software tales como: un firewall a través del cual se implementan políticas de acceso y seguridad, el servidor web, el servidor de correo, entre otros.

Sin embargo se ha visto la necesidad de incorporar conceptos tales como: zonas desmilitarizadas, redes privadas virtuales, y optimizar el uso de los recursos ya existentes. De igual forma se pretende mejorar el nivel de protección que ofrece el firewall y sus políticas existentes, buscando nuevas alternativas tanto en el programa como en la definición de las reglas de seguridad, para lo cual se realizará a continuación un análisis de varios conceptos afines.

Se puede entender como una zona desmilitarizada[1] (DMZ), al área exterior de una red destinada a los servidores que son de acceso público tales como: servicios de Web, Correo, DNS y FTP; esta zona se localiza entre el Internet y las líneas de defensa de la red interna, para lo cual en estos servidores, los programas, servicios y protocolos innecesarios son removidos, mientras que los puertos que no están siendo utilizados son deshabilitados.

Generalmente en las organizaciones se utiliza la DMZ para los servicios de Internet sin permitir el acceso no autorizado a la red privada, por lo que en esta zona se debe evitar el compartir servicios de autenticación con servidores importantes dentro de la red; por esta razón es indispensable evaluar los sistemas

[1] Fuente: http://www.microsoft.com/latam/technet/articulos/idc/idc1/default.asp, Agosto 2005

de protección perimetral situados entre la zona desmilitarizada y la red interna de una empresa; obteniendo como resultado de dicha evaluación una visión detallada del estado de la seguridad de la red.

El firewall[2] es una herramienta de seguridad que puede ser implementada en hardware o software, importante para toda organización que accede al Internet como medio de comunicación. Un cortafuegos puede ser una funcionalidad añadida a un ruteador, switch o cualquier otro dispositivo que sirva para detener tráfico desde o hacia partes de la red. La seguridad prestada es en tiempo real y evita que personas no autorizadas tengan acceso a la información privada de la empresa. De igual manera este componente puede actuar como filtro restringiendo el ingreso a determinados sitios en Internet mediante asignación de permisos que se desprenden de las políticas de seguridad propias de la organización.

Otro de los conceptos relevantes en las comunicaciones es el de Redes Privadas Virtuales (VPN), debido a que la continuidad en el servicio es un factor de vital importancia para el normal desarrollo de las actividades en una empresa ya que se debe garantizar la permanente disponibilidad de las comunicaciones y proteger la conexión entre un usuario remoto y la oficina central usando mecanismos de autenticación y técnicas de encriptamiento en ambos extremos, pudiendo utilizarse para este fin, soluciones de software, las cuales tienden a sufrir problemas de procesamiento al existir muchas conexiones simultáneas en una red grande; y soluciones de hardware, siendo su principal desventaja el costo.

Dentro de los dispositivos de mayor importancia para las comunicaciones en una red se puede mencionar a los ruteadores los cuales actúan a nivel de la capa tres del modelo OSI, y a los switchs los cuales trabajan a nivel de capa dos.

Un ruteador[3] es un dispositivo que se coloca entre dos segmentos de red direccionando el tráfico de una red hacia otra y comunicándolas entre si; constituye el elemento fundamental del funcionamiento de Internet ya que

[2] Fuente: http://es.wikipedia.org/wiki/Firewall, Agosto 2005
[3] Fuente: http://www.monografias.com/trabajos13/modosi/modosi.shtml, Agosto 2005

examina el sobre electrónico que envuelve a un paquete a ser enviado, compara direcciones dentro de unas listas las mismas que están almacenadas en tablas de enrutamiento determinando cual debe ser el siguiente ruteador al que se debe enviar el paquete para llegar a su destino basándose en condiciones cambiantes de la red.

Mientras que el switch tiene como función principal el procesar las direcciones físicas en una red LAN sin modificar los contenidos de los paquetes, es decir inspecciona la dirección fuente y destino del paquete para determinar la ruta de conmutación. La tabla de rutas en un switch es dinámica y se actualiza en base a la lectura de las direcciones que ingresan al dispositivo; en caso de que el switch reciba un paquete con una dirección desconocida este aplica la técnica de Inundación (Flooding), es decir emite la dirección a todos los puertos del mismo hasta encontrar su destino.

A continuación, y luego de haber revisado los conceptos más relevantes se va a analizar la infraestructura tanto en servidores, enlaces de comunicación existentes, servicios que se prestan y situación actual en lo referente a seguridad informática en la empresa.

1.1.- PLATAFORMAS, HARDWARE Y SOFTWARE DE SERVIDORES

NOMBRE	MARCA	MODELO	SISTEMA OPERATIVO
Firewall	IBM	RS/6000	Aix 4.5.9
Pcoweb	Compaq	Proliant ML350	Windows 2000 Server SP4
Pcored	Compaq	Proliant ML350	Windows 2000 Server SP 4
Pcored1	IBM	Netfinity 3500	Windows 2000 Server SP 4
Pcored4	IBM	Netfinity 7000 M10	Windows 2000 Server SP 4
Pcored5	IBM	Netvista 8191-83S	Windows 2000 Server SP 4
Pcored6	Compaq	Proliant DL580	Red Hat Linux 7.3 Servidor
Pcored7	Compaq	Proliant ML350	Red Hat Linux 9 Servidor

Tabla 1. Marca y plataforma de los servidores.

En la siguiente tabla se muestra las características de hardware que poseen los mencionados servidores.

NOMBRE	PROCESADORES	VELOCIDAD	MEMORIA	DISCOS	CAPACIDAD
Firewall	1	550 MHz	1 Gb	1	4.2 Gb
Pcoweb	2	795 MHz c/u	1.2Gb	2	8.46 Gb 8.47 Gb
Pcored	1	795 MHz	1.2 Gb	3	8.47 Gb 8.47 Gb 33.9 Gb
Pcored1	2	333 MHz c/u	512 Mb	2	8.47 Gb 8.47 Gb
Pcored4	2	550 MHz c/u	768 Mb	3	8.46 Gb 8.47 Gb 8.47 Gb
Pcored5	1	2 GHz	768 Mb	1	40 Gb
Pcored6	3	700 MHz	1,2 Gb	2	18.2 Gb 36.4 Gb
Pcored7	1	795 MHz	1.2 Gb	2	8.47 Gb 8.47 Gb

Tabla 2. Características de hardware de los servidores.

Con el fin de conocer la funcionalidad de los servidores antes indicados, a continuación se detalla las aplicaciones instaladas en cada uno de ellos:

Firewall:

- SecureWay Firewall versión 4.2; el cual se utiliza para establecer las reglas de filtrado, políticas de seguridad y accesos no autorizados.

- Proxy; el mismo producto SecureWay posee la opción de utilizar al equipo como intermediario, con la finalidad de que todos los usuarios de la red interna puedan acceder a Internet a través de una única conexión física; cabe señalar que este programa no ofrece la utilidad de hacer caché[4].

Pcoweb:

- Internet Information Server (IIS); es un servidor conectado a Internet que puede contener páginas web, servicios de correo electrónico, entre otros; ofrece una serie de servicios tales como: ftp, http, https; para los ordenadores que funcionan con Windows.

  Cabe señalar que este equipo tiene habilitada una conexión ftp con el servidor Pcored4 con el objetivo de mantener actualizada la página web de Petrocomercial.

- Lotus Domino; se utiliza como servidor de correo electrónico externo y permite enviar mensajes de los usuarios internos de la red hacia otros usuarios independientemente de la red que estén usando.

- Symantec System Center; paquete que ofrece protección de antivirus, antispam (correo no deseado) y filtrado de correo externo.

[4] Memoria intermedia utilizada por los navegadores para almacenar las páginas de Internet que ya se han visitado y poder volver a presentarlas sin necesidad de cargarlas de nuevo desde la red. (http://teleenfermeria.iespana.es/teleenfermeria/tecnoglosario.htm; Enero 2006)

Pcored:

- Lotus Domino; utilizado como servidor de correo interno, adicionalmente contiene las aplicaciones de: Ordenes de Pago, Juicios, Viáticos, Help Desk e Inventario de equipos de la empresa.

- Primary Domain Controller, servidor que contiene la base de datos de las cuentas de usuarios; valida las peticiones de ingreso y administra los recursos de la red.

- TSM (Tivoli Storage Managment); paquete que sirve para recopilar, almacenar y respaldar archivos, bases de datos y correos.
  En este equipo se tiene instalado TSM for mail para respaldar correos, TSM Manager Client para permitir respaldar su propia información.

- DNS (Servidor de Nombres de Dominio); sistema que permite traducir los nombres de los ordenadores en direcciones IP numéricas, siendo este proceso transparente para el usuario, con lo que el mismo puede utilizar los recursos de la red conectándose a través de los nombres a los equipos.

- DHCP Server; utilidad que asigna una dirección IP temporal a un ordenador cuando este se conecta a la red, para lo cual usa el protocolo de configuración dinámica de equipos.

Pcored1:

- Aplicaciones utilizadas para la Dirección Nacional de Hidrocarburos (DNH) y el Servicio de Rentas Internas (SRI); las mismas que sirven para el envío de información acerca del movimiento, comercialización y facturación de productos derivados del petróleo.

- Sistema Unificado de Contratistas y Oferentes (SUCO); es una aplicación para la administración de la Base de Datos única de proveedores calificados por Petroecuador y sus filiales.

- Auditoria: aplicación usada por la Unidad de Control de Gestión de Petrocomercial.

- Internet Information Server (Intranet).

- Symantec Web Security; antivirus corporativo de la empresa.

- Java Development Kit; paquete de software que permite escribir, compilar y correr programas y aplicaciones escritas en Java.

Pcored4:

- DataWareHouse; paquete que permite reunir la información generada por todas las unidades de la empresa para que cualquier usuario pueda acceder a esta, es decir es un repositorio de datos.

- Business Object; programa que permite consultar la información almacenada por los usuarios de la red y ayuda a generar informes, reportes, entre otros.

- DB2 UDB; base de datos que recopila la información de los servidores AS/400 y mantiene actualizada la página web del servidor Pcoweb.

- TSM Mananger for DB2; recopila, almacena y respalda la información de la base de datos de DB2.

Pcored5:

- Pruebas con el antivirus OfficeScan.

- DB2UDB; (backup del servidor Pcored4).

Pcored6:

- WebSphere; herramienta para desarrollo de software.

- TSM Server; servidor del Tivoli Storage Managment que permite respaldar la información.

Pcored7:

- Lotus Domino 6.5; utilizado para la implementación de la aplicación de Control Documental.

Finalmente se detalla las plataformas y aplicaciones instaladas en los servidores AS/400.

NOMBRE	S. OPERATIVO	APLICACIONES INSTALADAS
PCO1	OS/400 V5R2	Recursos Humanos, Activos Fijos, Contratos, Maintraker (Control de Bodega)
PCO2	OS/400 V5R2	Contabilidad y presupuesto (CGIFS), Ambiente de Desarrollo de: Comercialización Interna y Movimiento de Productos
PCO8	OS/400 V5R2	Comercialización Interna Movimiento de Productos
PCO9	OS/400 V5R2	Base de Datos del Sistema de Comercialización Interna (Rediseño), Websphere.

Tabla 3. Servidores AS/400.

1.2 TIPOS DE FIREWALLS POR HARDWARE Y SOFTWARE

Con el objetivo de ofrecer protección a la red que posee Petrocomercial, se encuentran implementados esquemas de seguridad utilizando el software SecureWay Firewall 4.2, el mismo que trabaja bajo el Sistema Operativo AIX 4.5.9, y está instalado en un equipo IBM RS/6000.

Las políticas que han sido definidas se detallan a continuación:

Acceso a las Bases de Datos:

- SRI: Esta política administra las autorizaciones de conexión de los equipos de Petrocomercial y otras filiales a la Base de Datos del SRI para realizar los procesos de envío de información.

- Ministerio de Energía: Política que autoriza la conexión de determinados equipos de la empresa y otras filiales hacia el Ministerio con el fin de realizar los procesos de envío de información y conexión con su Base de Datos.

- Petroindustrial, Petroecuador, Oleoducto (SOTE): A través de esta regla se permite a determinados equipos acceder hacia la red interna de Petrocomercial, con el fin de que utilicen el medio de comunicación existente y se enlacen hacia las entidades externas de control como el SRI y el Ministerio de Energía

Correo:

- Servidor Interno: Regla que permite a los servidores de correo tanto de la regional norte como la de la regional sur de la empresa comunicarse con el servidor de correo externo y a su vez a través de Internet enviar mensajes hacia fuera de la red.

- Petroecuador: Esta regla permite la conexión desde el computador de la Presidencia Ejecutiva de Petroecuador hacia el servidor de correo del Ministerio de Energía.

Internet:

- Acceso para todos los equipos de la red de Petrocomercial hacia Internet a través del proxy de la empresa, el cual se encuentra instalado en el mismo equipo donde funciona el firewall.

Acceso telnet:

- Pco8: Permite a ciertos equipos del Ministerio de Energía acceder por sesiones telnet [5] a este servidor, teniendo que autenticarse con su usuario y contraseña para poder realizar consultas en el sistema de movimiento de productos y comercialización interna.

Acceso por ftp:

- Pcoweb – Pcored4: Existe una política que permite la conexión ftp desde el servidor Pcored4 hacia el servidor web, con el fin de actualizar periódicamente la información de la página web en lo referente a existencias, despachos y comercialización de productos.

NAT:

- Pco8: Se tiene implementado una política que permite realizar la traducción de direcciones de red (NAT), con lo que la dirección privada de la red interna del servidor Pco8 es enmascarada con su dirección pública.

[5] Es un protocolo estándar de Internet que permite la conexión a un terminal remoto.

1.3 ENLACES DE COMUNICACIÓN EXISTENTES:

A continuación se detalla los enlaces existentes, los cuales son propiedad de Petrocomercial y sirven para comunicar la matriz con los diferentes terminales y sucursales de la empresa.

PUNTOS DE ENLACE		TIPO DE ENLACE	ANCHO DE BANDA
El Rocío (Matriz)	Pichincha A, Pichincha B	Radio Frecuencia	E1[6]
Pichincha A	Gasolinera, Aeropuerto, Beaterio, Oyambaro, Balao	Radio Frecuencia	E1
Balao	Esmeraldas, Petroindustrial	Radio Frecuencia	E1
Pichincha B	Ambato, Santo Domingo, Condijua, Cerro Azul	Radio Frecuencia	E1
Condijua	Osayacu, Shushufindi, Petroindustrial	Radio Frecuencia	E1
Cerro Azul	Libertad, Guayaquil, Pascuales, Manta, Tres Bocas, Fuel Oil	Radio Frecuencia	E1
El Rocío (Matriz)	Corazón, Chalpi Guayaquil	Radio Frecuencia	64Kbps
El Rocío (Matriz)	Petroindustrial	Radio Frecuencia	E1

Tabla 4. Enlaces de comunicación existentes

El siguiente gráfico muestra el sistema de comunicaciones de Petrocomercial a nivel nacional.

[6] Formato europeo de transmisión digital; la señal E1 lleva datos en una tasa de 2 Mbps y puede contener 32 canales de 64 Kbps (http://es.wikipedia.org/wiki/E1, Enero 2006)

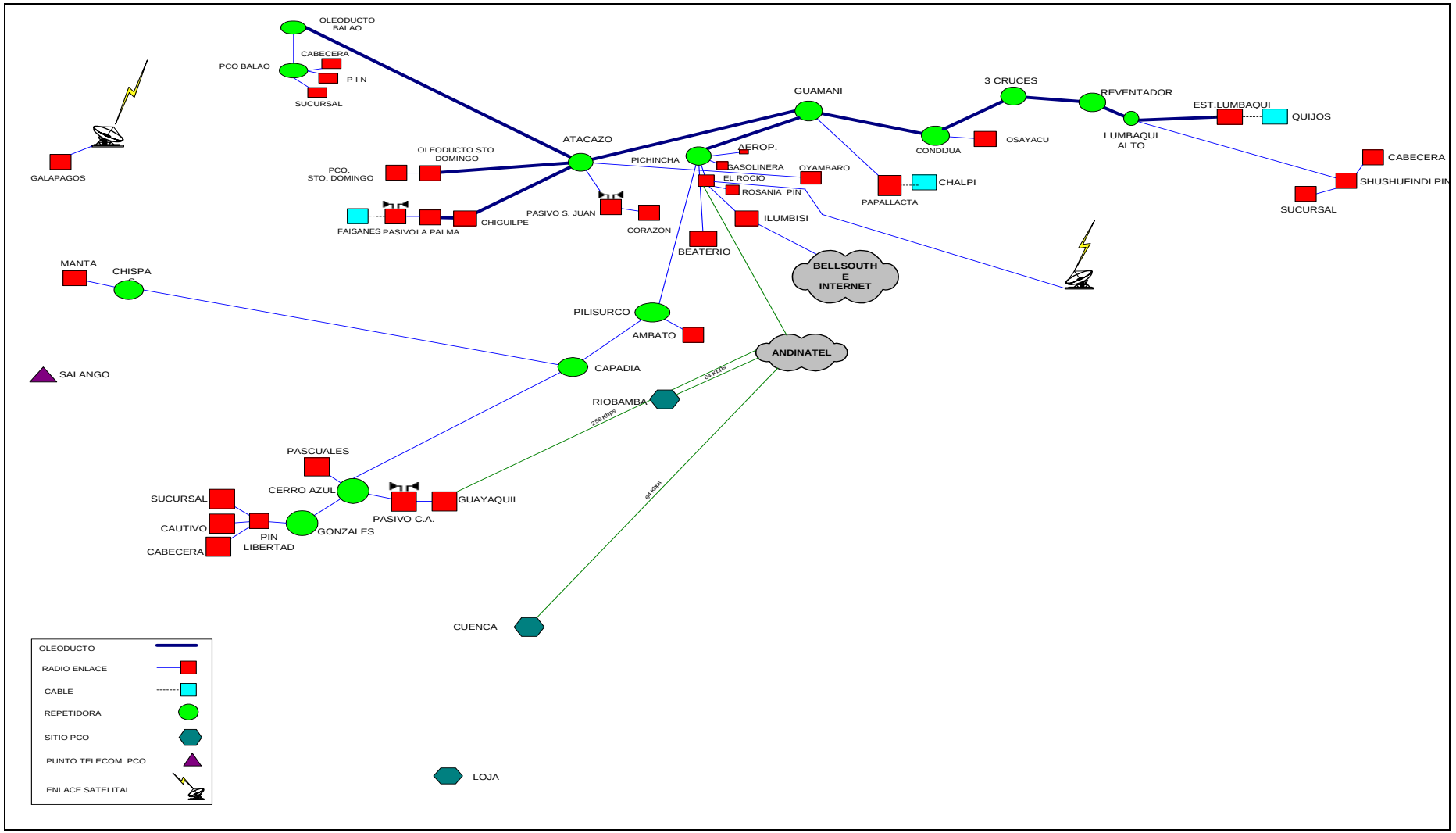


Figura 1. Sistema de comunicaciones de Petrocomercial

En el caso de las comunicaciones con los terminales de Riobamba, Cuenca y el enlace de respaldo existente con Guayaquil, Petrocomercial contrata el servicio con las siguientes empresas:

PUNTOS DE ENLACE		TIPO ENLACE	VELOCIDAD	PROVEEDOR
El Rocío	Guayaquil	Radio Enlace	256 Kbps	Andinadatos
El Rocío	Cuenca	Radio Enlace	64 Kbps	Andinadatos
El Rocío	Riobamba	Radio Enlace	64 Kbps	Andinadatos
El Rocío	Galápagos	Satelital	64 Kbps	Impsat

Tabla 5. Proveedores de enlaces para Petrocomercial

PUNTOS DE ENLACE	ANCHO DE BANDA	PROVEEDOR
El Rocío	256 Kbps	Otecel

Tabla 6. Conexión a Internet

Para solventar la conexión entre la matriz de Petrocomercial con la sucursal de Loja y los bancos tales como: Internacional, Pichincha, Pacífico, Produbanco, Bolivariano, Rumiñahui y Guayaquil se hacen uso de enlaces vía módems los cuales trabajan a una velocidad de 9.6Kbps.

1.3.1 DISPOSITIVOS DE COMUNICACION EXISTENTES

Entre los dispositivos de capa tres utilizados para los enlaces de comunicación en la empresa se describen a continuación los siguientes ruteadores con sus principales funciones y características:

Ruteador Motorola Vanguard 6435/6455:

Utilizado para los enlaces desde la mayoría de sitios remotos hacia la matriz de Petrocomercial, siendo estos equipos de propiedad de la empresa.

El ruteador Vanguard 6435 es diseñado para pequeñas oficinas, provee soporte de hasta 6 puertos seriales o 6 líneas de voz analógicas; trabajan con la versión V6.0.S100 de sistema operativo (IOS).

El equipo Vanguard 6455 es usado para oficinas remotas de mayor tamaño que requieren un grado de funcionalidad superior, con soporte para voz digital, posee dos ranuras de opción y trabajan con la versión V6.4.S10A de sistema operativo.

Los Vanguard 6435 y 6455 incluyen 16MB de SDRAM (memoria dinámica de acceso aleatorio). En su configuración básica poseen un puerto Ethernet 10BaseT [7] y 3 ranuras de expansión.

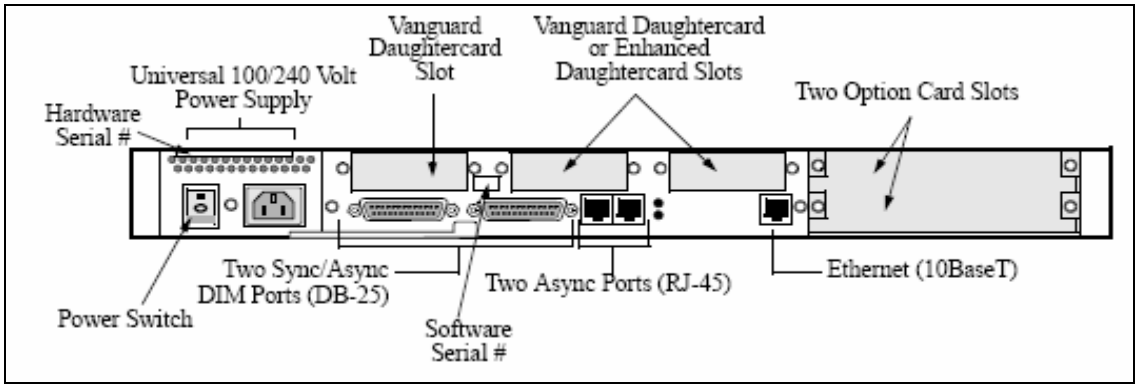


Figura 2. Ruteador Vanguard 6455

[7] Estándar utilizado en redes locales, que utiliza cables de par trenzado (de categoría 3 ó 5) para proveer una velocidad de conexión de 10Mbps. (http://es.wikipedia.org/wiki/10BaseT, Enero 2006)

Ruteador Motorola Vanguard 340:

Utilizado para la comunicación con algunos sitios remotos ya sean estos terminales y sucursales de la empresa, estos equipos son propiedad de Petrocomercial y entre sus características principales cabe resaltar lo siguiente:
Es un dispositivo diseñado para ambientes pequeños y ofrece soluciones para aplicaciones VPN, requiriéndose para esto tarjetas adicionales las cuales no están incluidas en su configuración básica. Adicionalmente tiene dos slots para tarjetas de video, voz y una combinación de tráfico de los dos mencionados anteriormente. El Vanguard 340 posee 16 Mbytes de memoria SDRAM y 4 Mbytes de memoria no volátil que está localizado en la tarjeta madre y es usada para almacenar el software del equipo, trabaja con la versión V5.6R000 de IOS.

Ruteador IBM 2210:

Son equipos propiedad Petrocomercial y utilizados para el acceso a Internet, comunicación con entidades externas y el acceso vía dial up, para lo cual los usuarios se autentifican con su propia contraseña validándose en una lista de control de accesos definida en el ruteador.

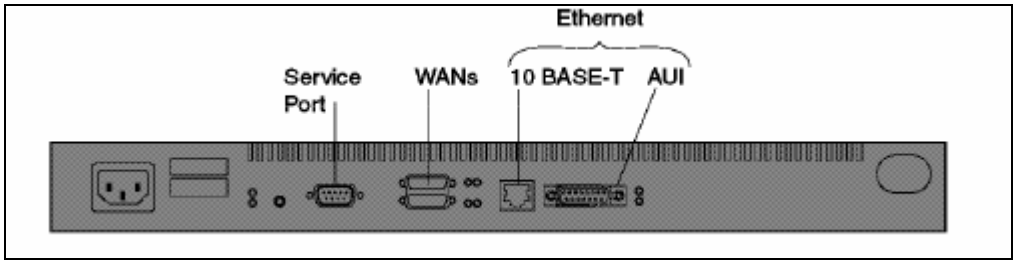


Figura 3. Ruteador IBM 2210-12E

Ofrecen una variedad de servicios como: reservación de ancho de banda, reenrutamientio WAN, marcado sobre demanda, encriptación vía IPSec[8] y pueden trabajar bajo IPv6 [9].

Como parte de su configuración básica poseen: cuatro puertos WAN de alta velocidad, dos puertos Ethernet 10 BaseT, dos puertos Ethernet AUI (Interfase

[8] Es una extensión al protocolo IP que añade cifrado para permitir servicios de autenticación y cifrado y, de esta manera, asegurar las comunicaciones a través de dicho protocolo. (http://es.wikipedia.org/wiki/IPSec, Enero 2006).
[9] IPv6 es la versión 6 del Protocolo IP, que está destinada a sustituir al actual estándar IPv4.

entre el equipo y la LAN), un puerto serial de consola o servicio y memoria DRAM de16 Mb, trabaja con la versión V3.2 de IOS:
Además de estos equipos, los ruteadores que se utilizan para los siguientes enlaces:

Ruteador Cisco 3600 Series:

Propiedad de Petroecuador y sirve para las comunicaciones con las otras filiales de la empresa.

Ruteador Cisco 800 Series:

Propiedad de Andinadatos y sirve para la comunicación con los terminales de Riobamba y Cuenca, así como también se utiliza para un enlace de respaldo con Guayaquil.

En el gráfico del Anexo 1 se puede observar la configuración de la Red LAN y WAN de Petrocomercial con todos los enlaces existentes hacia las diferentes sucursales y terminales de la empresa.

A continuación se detalla en la siguiente tabla la distribución de direcciones IP para los diferentes equipos y dispositivos de red de la matriz; para lo cual se utiliza una red clase B.

RANGO	DETALLE	DESCRIPCION
64.1 – 64.19 Comunicaciones	.2 .3 .4 .5 .6 .9 .11 .12 - .19	Ruteador IBM 2216-400 Ruteador CISCO 800 Series Ruteador IBM 2210 Dial up Impresora IBM Infoprint 1145 (Sistemas) Firewall IBM AIX Impresora IBM Infoprint 1145 (Sistemas) Router Vanguard Motorola RAS
64.20 – 64.29 Servidores y AS/400	.20 .24 .25 .26 .28 .29	Pcored Pcored4 Pco1 Pco2 Pco8 Pco9
64.30 - 64.40		Impresoras de red
64.41 – 64.49 Direcciones para control del Firewall		Equipos: Control de gestión, Seguros y garantías y Coordinación de contratos.
64.50 – 64.69 Servidores	.53 .55 .57	Pcored3 Pcored5 Pcored7
64.70 - 64.99		Impresoras de red
64.101 - 64.232		Switchs Cisco
65.101 - 68.254		Direcciones del DHCP para la red de datos
69.1 - 64.254		Direcciones DHCP para la red de voz
71.9		Pcored6
71.21		Pcored1

Tabla 7. Distribución de direcciones IP de los equipos en la matriz

1.4.- SERVICIOS QUE SE PRESTAN:

Dentro de los servicios que se presta a la Intranet[10], se puede mencionar los siguientes:

- Protección contra de virus para todos los equipos de la red interna utilizando el producto Symantec Web Security, instalado en el servidor Pcored1 que actualiza al Norton Antivirus Corporativo de los computadores de la empresa de forma periódica y realiza una tarea calendarizada de revisión de virus.

- Servicio de correo interno, control documental, ordenes de pago, sistema de viáticos, help desk e inventario de equipos administrado por Lotus Domino que se encuentra instalado en el servidor Pcored.

- Servicio DHCP para asignar direcciones IP dinámicas a los equipos que se conectan a la red interna de la empresa

- Servicio de Nombres de Dominio (DNS) instalado en el servidor Pcored, que realiza la traducción de nombres en direcciones IP y permite la comunicación y utilización de los recursos de la red;

- Internet, para el acceso de todos los usuarios utilizando el proxy que se encuentra instalado en el equipo que funciona como firewall.

- Servidor web para la Intranet usando Internet Information Server, con el propósito de que los usuarios tengan acceso a páginas internas de la empresa.

Servicios que prestan las aplicaciones de Petrocomercial:

- Sistema de administración de oferentes (SUCO) que se encuentra disponible en el servidor Pcored1 para consultas de proveedores y cuya base de datos esta instalada en Petroecuador.

[10] Una intranet es una red local que utiliza herramientas de Internet. Se puede considerar como una Internet privada que funciona dentro de una organización. (http://es.wikipedia.org/wiki/Intranet, Enero 2006)

- Sistema de Comercialización Interna y Movimiento de Productos instalada en un servidor AS/400 denominado PCO8.

- Sistema de Contabilidad (CGIFS) instalado en un servidor AS/400 denominado PCO2.

- Aplicaciones para Recursos Humanos, Activos Fijos, Contratos, Maintraker (Control de Bodega) instalados en un servidor AS/400 denominado PCO1.

- Servicio ftp para actualización de datos del servidor web desde el servidor Interno Pcored4.

Servicios que se presta a la Extranet[11]:

- Servidor web externo utilizando Internet Information Server; donde se aloja la página web de la empresa.

- Servidor de correo externo para lo cual se utiliza Lotus Domino, instalado en el servidor Pcoweb.

- Servicio para la comunicación desde equipos de otras filiales de Petroecuador hacia entidades externas como el SRI y la DNH

1.4.1 SITUACIÓN ACTUAL EN SEGURIDAD INFORMÁTICA

Como parte de la seguridad informática, Petrocomercial posee un instructivo para usuarios de equipos de computación emitido en el mes de noviembre del año 2003 y aprobado por las autoridades de la empresa, dentro del cual se hace referencia a los conceptos básicos para el correcto uso de los recursos informáticos y la responsabilidad legal y administrativa de los funcionarios que tienen a su cargo los equipos.

Dentro de los objetivos específicos planteados en este instructivo se pueden mencionar los siguientes:

[11] Una extranet es una red privada virtual resultante de la interconexión de dos o más intranets que utiliza Internet como medio de transporte de la información entre sus nodos. (http://www.galeon.com/filoesp/glosario/glos_E.htm, Enero 2006)

- Dar a conocer a los usuarios los conceptos generales de hardware, software y cuidados básicos indispensables para el uso de un computador, los diferentes dispositivos que contienen los equipos y unidades de almacenamiento de información.
- Normas para instalación y estandarización en el uso de software aplicativo propiedad de la empresa y software de usuario final, el cual debe contar con las licencias de uso correspondiente y estar justificado como necesario para el óptimo cumplimiento de las actividades. En el caso de uso de software especializado como analizadores de redes, identificadores de vulnerabilidades, entre otros está restringido su utilización a la Unidad de Sistemas y Telecomunicaciones.
- Normas para almacenamiento y denominación de archivos.
- Normas para la utilización adecuada de la red y sus aplicaciones como correo electrónico de Internet e Intranet, restringiendo el enviar indiscriminadamente mensajes que puedan congestionar la red o contener virus. En el caso de realizar pruebas con software sospechoso o contenidos de correo de direcciones desconocidas, es necesario desconectar al equipo de la red.
- Conocimiento, prevención y controles programados de virus informáticos.
- Normas de seguridad en lo referente a claves para los usuarios, siendo estas de uso personal e intransferible pudiendo ser las siguientes:

  Clave de encendido.

  Usuario y clave para acceso a la red local, solicitada a través de un formulario de creación de perfil de usuario y autorizada por el jefe del área.

  Usuario, clave y niveles de acceso a la información de los sistemas de comercialización (AS/400).
- Normas de uso de Internet, el cual debe ser utilizado solo para los siguientes propósitos:

  Comunicación e intercambio de información entre instituciones y personas vinculadas con las labores de la empresa; investigación sobre especificaciones técnicas, proveedores, manuales y documentos relacionados con los recursos que utiliza la empresa.

Como debilidades en lo referente a seguridad informática se puede mencionar:

El personal de la empresa no está conciente de las consecuencias que conlleva la falta de control en el acceso físico y lógico, y demás aspectos relacionados, que son la base de la seguridad corporativa.

La inadecuada documentación de procedimientos como: actualización del portal Web, aplicaciones y bases de datos, cambio de versiones, configuraciones, etc., sumado a su almacenamiento desorganizado, son algunas de las falencias de seguridad.

La descentralización de las actividades de soporte a usuarios provoca la demora en la atención oportuna y el desperdicio de recursos.

El cableado no estructurado sumado a la desactualización de sus diagramas, provocan la demora en la detección de fallas en la comunicación, la pérdida de información y la transmisión de datos insegura.

En Petrocomercial, el implementar planes o estrategias de seguridad de la información se dificulta principalmente por la constante rotación del personal y el cambio de autoridades. Esto puede generar la demora en la implantación de los controles que dichos planes o estrategias sugieran.

Contraseñas débiles, sin tiempo de caducidad, no son personales, repetitivas es decir no se obliga a no ser repetitivas cuando un cambio de estas es realizado.

El uso de recursos e Internet es indiscriminado, existe una sobre utilización en muchos casos para fines ajenos al desempeño de las actividades ingerentes a Petrocomercial.

No hay depuración periódica de la Base de Datos de usuarios que permita inhabilitar usuarios y bloquear equipos de todo personal que haya sido separado de la institución o haya sido removido del área.

FACTOR DE RIESGO	CONSECUENCIAS	TIPO DE PROTECCIÓN	NIVEL DE EFECTIVIDAD
Acceso físico no autorizado	Pérdida física de equipos, robo de información, daño de equipos, pérdidas en el negocio.	Guardias, tarjetas magnéticas, cámaras al ingresar	Bajo
Acceso lógico no autorizado	Alteración, pérdida y robo de información, pérdida de confidencialidad e integridad de los datos	Contraseñas, perfiles de usuario, roles o tipos de acceso	Medio
Contraseñas débiles	Vulneración de seguridades, pérdida de confidencialidad y daños en la integridad de la información	Administradores de red y Bases de Datos	Bajo
Divulgación de contraseñas	Fácil acceso a información e infiltración de terceros.	Instructivo para usuarios de equipos de computación	Bajo
El hardware no corresponde a las necesidades del software	Bajo rendimiento y lentitud en las aplicaciones	Implementación de equipos que solventen los requerimientos de respuesta	Bajo
Daño y mal funcionamiento de equipos	Pérdida parcial o total de la información, paralización en las actividades del negocio	Soporte técnico, contratos de mantenimiento, equipamiento asegurado	Medio
Cambio de configuraciones, instalación de software malicioso	Violación de seguridades, ingreso de virus, daños en equipos y aplicaciones, paralización en las actividades del negocio.	Perfiles de usuarios, logs del sistema, respaldos y backups.	Medio
Mal uso de privilegios de usuario	Eliminación o robo de información instalación de software no autorizado, accesos no autorizados	Asignación de contraseñas, logs del sistema, establecimiento de privilegios a nivel de usuarios	Bajo
Errores y descuidos del personal	Daños en el equipo o aplicaciones, pérdidas de información, paralización en las actividades del negocio.	Instructivo para usuarios de equipos de computación, reglamento interno de la empresa	Bajo

Tabla 8. Identificación de riesgos.

Luego de realizado el análisis de las falencias, se determina que muchas de estas afectan directamente a los servidores AS/400, por lo que es conveniente identificarlas y además señalar su impacto puesto que cada uno de ellos tiene sus aplicaciones específicas.

PCO8.- Paralización del negocio con pérdidas económicas, pues los sistemas de Comercialización Interna quedan inutilizados, por lo que los registros de despachos de combustible y su facturación deben ser realizados manualmente, sin poderse verificar que los controles de garantía se cumplan. De igual manera no se garantizaría el abastecimiento de combustible para la región por la inaccesibilidad al Sistema de Movimiento de Productos.

PCO9.- Interrupción del negocio debido a que no se puede utilizar la Base de Datos del Sistema de Comercialización Interna, por tanto no se puede manejar el Sistema de Comercialización, causando un impacto similar al causado por la falla en PCO8.

PCO2.- Retraso en el normal desempeño de las diligencias del negocio, ya que produciría fallas del sistema de contabilidad y presupuesto (CGIFS), es decir se paralizaría la contabilidad, el registro de los asientos contables de los movimientos financieros de la filial, por ende demora en la entrega financiera a Petroecuador.

PCO1.-Demora en las actividades relacionadas con Recusos Humanos como es la generación de nóminas mensuales de remuneraciones. Retraso en las actividades del sistema contable. Información no disponible de los procesos de compra y contratación; imposibilidad de realizar un control de bodegas, las compras locales e importaciones.

Adicionalmente la falta de control al ingreso de zonas sensibles como centro de computo y cuarto de servidores permite que visitantes ajenos al departamento e incluso ajenos a la organización, transiten indiscriminadamente por cada una de las áreas, corriendo el peligro de hurto de equipos así como manipulación no controlada de la información, pudiendo manejarla en forma peligrosa o incluso añadir código malicioso, o instalar software de riesgo.

Con respecto a los demás servidores se ha realizado una tabla con los niveles de riesgo relacionados a antigüedad, uso y sometimiento.

NOMBRE	ANTIGÜEDAD	USO	SOMETIMIENTO
Firewall	8 años	Alto	Alto
Pcoweb	5 años	Medio	Alto
Pcored	5 años	Alto	Alto
Pcored1	6 años	Alto	Medio
Pcored4	5 años	Medio	Alto
Pcored5	3 años	Bajo	Bajo
Pcored6	3 años	Medio	Medio
Pcored7	5 años	Bajo	Medio

Tabla 9. Parámetros de riesgo en los servidores

A partir del análisis realizado en este cuadro se puede observar que los equipos en su mayoría tiene mas de cinco años de servicio y considerando que en muchos de ellos el uso y sometimiento es elevado debido a la cantidad de usuarios que acceden a los mismos, se puede concluir que el riesgo de operatividad es alto por lo que se recomienda la renovación en los servidores: Firewall, Pcoweb, Pcored y Pcored1.

CAPÍTULO

II

CAPÍTULO II

ANÁLISIS DE LOS POSIBLES MEDIOS DE SEGURIDAD APLICABLES A LA EMPRESA

INTRODUCCIÓN

Luego del análisis de la situación actual en Petrocomercial, y como propuesta dentro de un plan de seguridad informática se recomienda la aplicación de las siguientes políticas:

Dirección de las responsabilidades: Crear un manual de procedimientos para en casos de alguna eventualidad se informe oportunamente a los responsables que hayan sido señalados mediante una política de la Institución, estableciendo tiempos máximos de respuesta para el restablecimiento normal de las actividades luego de haber puesto en marcha el plan de contingencia oportuno según el caso.

Instalación y mantenimiento de equipos: Todo equipo de computación propiedad de la empresa debe estar registrado dentro del inventario de hardware que maneja la Unidad de Sistemas y Telecomunicaciones de Petrocomercial.

Los equipos que sean de propósito específico y tengan una misión crítica asignada requieren estar ubicados en áreas que cumplan con los requerimientos de: seguridad física, condiciones ambientales, alimentación eléctrica y su acceso debe ser únicamente para personal autorizado.

Los equipos de computación deben someterse a mantenimientos preventivos y correctivos periódicos con el fin de garantizar su funcionamiento y conservación de su instalación, verificación de la seguridad física.

Actualización de los equipos: En todos los equipos de computación debe procurarse que esté actualizado, tendiendo a conservar su desempeño e incrementar la calidad del servicio que presta.

Control de accesos: En las áreas críticas donde se encuentre equipos cuyo propósito reúna características de imprescindible, solo personal autorizado deberá tener acceso, además de llevar un registro de tráfico de personal.

Utilización de cuentas de usuarios: Los usuarios deben tener sólo los permisos necesarios para realizar sus tareas habituales, es importante revisar las aplicaciones para que no se requiera manejar permisos administrativos.

Es recomendable la utilización de contraseñas complejas y el cambio periódico de las mismas para lo cual es necesario auditar las contraseñas evitando repetir por lo menos las dos anteriores ya utilizadas.

Acceso a sistemas administrativos: El manejo de información administrativa que se considere de uso restringido deberá ser cifrado con el objeto de garantizar su integridad.

El control de acceso a software aplicativo de la empresa será regularizado e informado para el control y supervisión de la Unidad de Sistemas.

Crear una política para la “Administración de la continuidad del negocio” la misma que debe generar, luego del análisis, un diseño de una conexión alterna para posibles enlaces paralelos, o rutas de acceso y conectividad alternativas a ser implementadas.

Acceso a Internet: Los accesos a las páginas Web a través de los navegadores deben sujetarse a los sitios autorizados y restricciones normadas por la empresa.

Utilización de recursos de red: Los recursos disponibles a través de la red serán de uso exclusivo para asuntos relacionados con actividades de la empresa, siendo responsabilidad de la Unidad de Sistemas administrar, mantener y actualizar la infraestructura de la red.

Instalación de software: En los equipos de computación, de telecomunicaciones y en dispositivos basados en sistemas de cómputo, únicamente se permitirá la instalación de software con licenciamiento respectivo.

Con el propósito de proteger la integridad de los sistemas informáticos y de telecomunicaciones, es imprescindible que todos y cada uno de los equipos involucrados dispongan de software de seguridad (antivirus, vacunas, privilegios de acceso).

Para la implantación y cumplimiento de los objetivos de las políticas de seguridad de la Información, se debería formar equipos de trabajo por cada área o unidad los cuales identifiquen los activos a proteger y sus vulnerabilidades, dichos equipos deben actuar permanentemente en tareas de prevención, detección y reacción frente a incidentes.

Se debe documentar todos los procesos y actividades para que se tenga claramente definidas las funciones y responsabilidades, tomando en cuenta el elevado nivel de rotación de empleados que la filial posee. El éxito en la implantación de las políticas de seguridad depende del compromiso de altos directivos y personal de la empresa.

Debido a que el campo de la seguridad informática es muy extenso, en el presente proyecto nos centraremos en la definición e implementación de las políticas de seguridad a nivel del firewall con su zona desmilitarizada bien definida, así como también en el análisis de una alternativa de enlace para mantener operativo las comunicaciones entre la matriz con los diferentes sitios remotos de la empresa.

En lo referente a las definiciones de las interfases del firewall existente en Petrocomercial no se tiene definido una zona desmilitarizada (DMZ), y por otra parte ya que el producto y equipo instalado como cortafuegos no presenta facilidades para su administración e implementación de mejoras a nivel de seguridades en los accesos hacia la red, se ha visto la necesidad de considerar nuevas soluciones poniendo a consideración los siguientes tipos de firewall para que después de un análisis de requerimientos en la empresa se pueda escoger el más apropiado:

Firewall por Software[12].- Son los más comunes debido a que su costo es inferior a una implementación por hardware, adicionalmente su instalación y actualización es más sencilla aunque pueden presentar problemas debido al consumo de recursos del ordenador y ocasionar errores de compatibilidad con otro software instalado, de igual forma para su configuración se necesita poseer conocimientos en redes y saber los puertos necesarios para las aplicaciones utilizadas. Sin embargo varios sistemas operativos traen incorporados firewalls internos, como es el caso de Windows XP y Linux.

Firewall por Hardware.- Son dispositivos que trabajan independientemente del computador y no consumen recursos del mismo. Normalmente se colocan entre el servidor y la conexión física al Internet. Una de sus desventajas es el mantenimiento ya que son más complicados de actualizar y configurar correctamente.

Generalmente en todos los tipos de firewalls es recomendable bloquear todos los servicios basados en datagramas que no hagan uso de autentificación, es decir todos los basados en UDP (protocolo no orientado a conexión) no cifrados, y todos los servicios basados en TCP (protocolo orientado a conexión) que no se consideren estrictamente necesarios.

A continuación se puede listar servicios accesibles desde Internet o puertos considerados poco seguros con su descripción y posibles problemas que podría ocasionar el tener abierto estos agujeros de seguridad

- echo (7/tcp, udp): utilizado para depuración; un atacante podría realizar labores de depuración creando bucles en la red a partir de este puerto.
- systat (19/tcp, udp): muestra información del equipo como usuarios conectados, carga del sistema, procesos en funcionamiento, etc.
- telnet (23/tcp, udp): vulnerable a toma de sesiones, es preferible usar en su lugar soluciones seguras como SSH[13] (Secure Shell) que utiliza cifrado para el envío de la información por la red.

[12] Fuente: http://www.dric.com.mx/seguridad/firewall/firewall1.php?scat=4, Enero 2006

[13] SSH es el nombre de un protocolo y del programa, sirve para acceder a máquinas a través de una red, de forma similar a telnet. La diferencia es que SSH usa técnicas de cifrado. (http://es.wikipedia.org/wiki/SSH, Enero 2006).

- smtp (25/tcp, udp): es un protocolo usado para la transferencia de correo electrónico, la mayoría de ataques a equipos han surgido a través de este puerto; es aconsejable tener la última versión estable conocida de cualquier programa de correo.
- nameserver (42/tcp, udp): si se dispone de una red privada, se debe instalar un servidor de nombres, por lo que hay que bloquear el acceso a este servidor desde el exterior utilizando la última versión de BIND para resolver nombres.
- tftp (69/tcp, udp): protocolo para transferencia de archivos que no posee autenticación; es aconsejable bloquear si no se tiene algún equipo con arranque remoto.
- private dialout (75/tcp, udp): utilizado para escanear puertos de un equipo.
- finger (79/tcp, udp): sirve para obtener información acerca de usuarios concretos lo cual puede utilizarse para adivinar claves de acceso.
- npp (92/tcp, udp): puerto usado para enviar impresiones en red.
- ntp (123/tcp, udp): puerto para sincronizar los relojes de las máquinas de una red, se puede usar este para distorsionar los registros (logs) de los equipos.
- netbios (137,138,139/tcp, udp): es el sistema básico de entrada y salida de una red; no dispone de suficiente autenticación.
- snmp (161/tcp, udp): protocolo de administración y monitoreo de redes a través del cual se puede obtener mucha información de conexiones y recursos de una red, por lo que es aconsejable bloquear este puerto.
- exec (512/tcp): ejecuta órdenes en estaciones remotas, su autenticación es basada en dirección IP y usuario remoto.
- biff (512/udp): notifica la llegada de correo, suele ser usado para ataques que provocan desbordamiento de buffer.
- who (513/udp): muestra quien utiliza el equipo remoto, tiempo de funcionamiento, carga de la máquina.
- syslog (514/udp): usado para corromper los registros del sistema con entradas falsas.
- ingreslock (1524/tcp): en los equipos Unix se puede encontrar esta entrada, es un puerto no privilegiado utilizado para habilitar puertas traseras.

2.1.- EMPRESAS DE TECNOLOGÍA Y PROVEEDORES DE SERVICIOS DE COMUNICACIONES PARA PETROCOMERCIAL

Para los diferentes enlaces dentro de la empresa y con otras entidades se utilizan dispositivos de comunicación propios y en otros casos se contrata los servicios con empresas externas como se detalla a continuación:

- Para las conexiones: de la red WAN se utilizan ruteadores Motorola Vanguard los cuales son de propiedad de la empresa.

- En las comunicaciones con Petroecuador y las demás filiales como Petroindustrial y Petroproducción se utiliza un ruteador Cisco 3600 Series. Con Petroecuador se comparten aplicaciones de Sistemas de Oferentes, Auditoria y Seguros, así como también se utiliza la conexión que tiene Petrocomercial con el Ministerio de Energía y Minas para acceso de las otras filiales.

- Para comunicarse con las estaciones de Corazón y Chalpi se utiliza un ruteador IBM 2216 en la matriz, mientras que en estos sitios se tiene ruteadores IBM 2210, con una velocidad de 64 Kbps por cada enlace, siendo estos equipos de propiedad de Petrocomercial.

- En el acceso remoto vía dial up se utiliza un ruteador IBM 2210, el cual soporta hasta ocho conexiones simultáneas con una velocidad máxima total de 64 Kbps; este mismo equipo es utilizado para la conexión con los bancos.

- Los enlaces con las sucursales de Guayaquil, Riobamba y Cuenca provee Andinadatos y utiliza un ruteador Cisco 800 Series. El enlace con Guayaquil de 256 Kbps es considerado como respaldo del enlace principal el cual utiliza los ruteadores Motorola Vanguard y provee un ancho de banda de un E1, mientras que la comunicación con el Depósito Riobamba y la Sucursal Cuenca son de 64 Kbps cada uno.

- En lo referente al servicio de Internet (ISP) el proveedor es Movistar (Otecel); con un ancho de banda contratado de 256 Kbps y para esta conexión se usa un ruteador IBM 2210 propiedad de Petrocomercial; este mismo equipo sirve para la comunicación con el SRI y el Ministerio de Energía.

- Se tiene contratado un enlace satelital para las estaciones en las Islas Galápagos, este servicio es proporcionado por Impsat, para lo cual desde la matriz de Petrocomercial se tiene un enlace de 128 Kbps hasta el Telepuerto desde donde esta empresa provee los dos canales de comunicación de 64 Kbps cada uno hasta Baltra y Puerto Ayora.

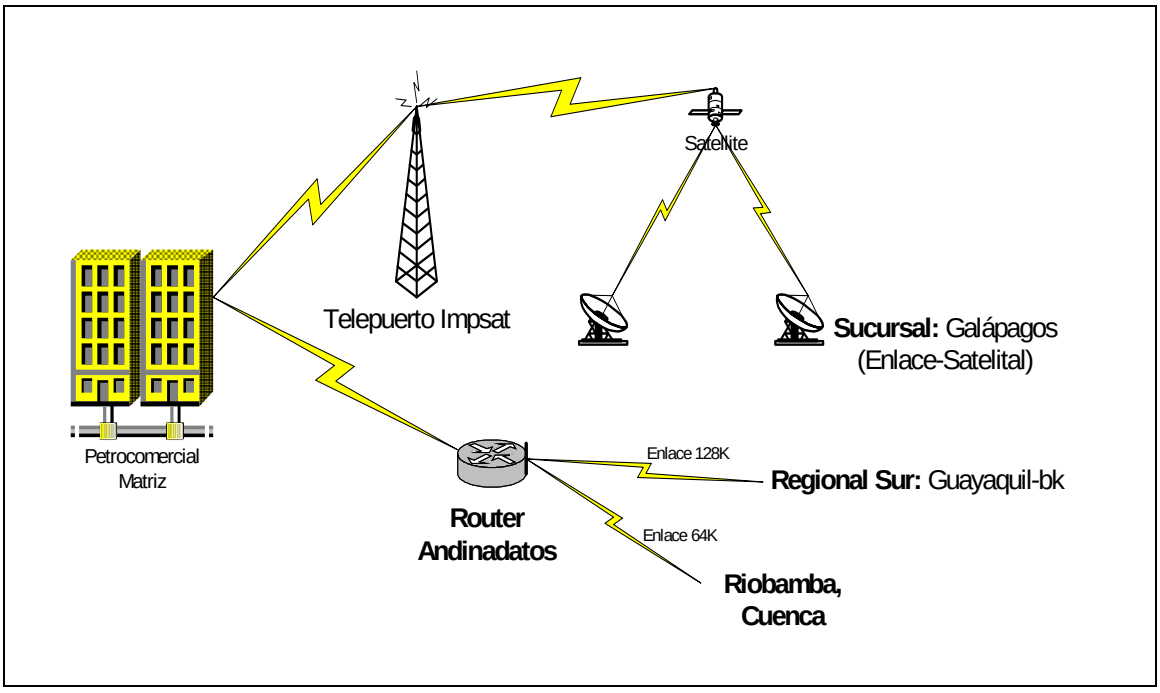


Figura 4. Enlace satelital con las Islas Galápagos

Dentro de los servicios que ofrecen estas empresas de tecnología en lo referente a transmisión de datos se puede mencionar a continuación una breve descripción:

ANDINADATOS[14]

Es la unidad de telecomunicaciones avanzadas de Andinatel, implementada con el fin de ofrecer soluciones integrales en la transmisión de datos. Esta empresa cuenta con un backbone ATM[15] que va sobre un sistema de transporte SDH[16] en anillos de fibra óptica a nivel regional con redundancia por microonda. Los puntos de acceso tienen diferentes servicios, TDM (Multiplexación por División de Tiempo) y xDSL (línea digital de abonado) a nivel regional los cuales se detallan a continuación.

TDM (Clear Channel)**.-** Andinatel a través de su red TDM entrega servicios transparentes para enlaces, en los cuales los clientes necesitan solamente el envío de datos a través de la red WAN. Ofrece el transporte de la información a velocidad constante. Andinadatos instala los módems punto a punto para la transmisión de datos y el cliente instala y programa sus equipos (ruteadores) que le permiten tener diferentes protocolos y aplicaciones a través de la red TDM.

Frame Relay**.-** Este servicio de conmutación Frame Relay ofrece una velocidad contratada mínima, que es una tasa de información confiable y además una velocidad que se puede utilizar en el caso de no existir congestión; este servicio va dirigido a clientes que necesitan enlaces de comunicación más económicos que los enlaces TDM o que quieren tener una conexión punto-multipunto entre una matriz y varios sitios remotos. Andinadatos instala los módems de punto a punto y el cliente instala y configura los ruteadores conectados a los módems.

Dependiendo del tipo de enlace para estos dos servicios, Andinadatos puede rentar los ruteadores o entregar un equipo que haga las veces de módem y ruteador.

xDSL Digita.- Es un servicio punto-multipunto que consta de dos diferenciaciones, ADSL y G.SHDSL. El ADSL ó DSL asimétrico, proporciona a la transmisión de

---

[14] Fuente: http://www.andinadatos.com.ec

[15] Tecnología de transmisión de datos en forma de paquetes. La información se divide en pequeñas células que se transmiten individualmente y se procesan de manera asíncrona. (http://www.red.es/glosario/glosario.html, Enero 2006)

[16] Es un formato de transmisión digital usado en circuitos de microondas, que sirve de soporte para banda ancha. El estándar de la tasa de transmisión para SDH es el STM-1, que establece una velocidad de operación de 155 Mbps. (http://www.genesisbci.com/genesis/glosario/conceptos.asp, Enero 2006)

datos la velocidad de 8 Mbps como tráfico entrante al cliente y hasta 1,5 Mbps como saliente, siendo útil para la transmisión de Internet. Mediante ADSL y por medio de un divisor la voz y los datos se separan, de manera que se puede hablar por teléfono aunque el computador esté conectado a Internet al mismo tiempo. El G.SHDSL, o DSL simétrico permite la conexión de hasta 2Mbps de entrada y salida en forma simétrica donde el cliente puede tener transmisión de datos sobre la red ATM a cualquier sitio que desee, desde Internet hasta conexiones entre agencias.

ISDN.- Red digital de servicios integrados que permite integrar voz, datos, video en forma conmutada utilizando la infraestructura telefónica existente de una forma totalmente digital.

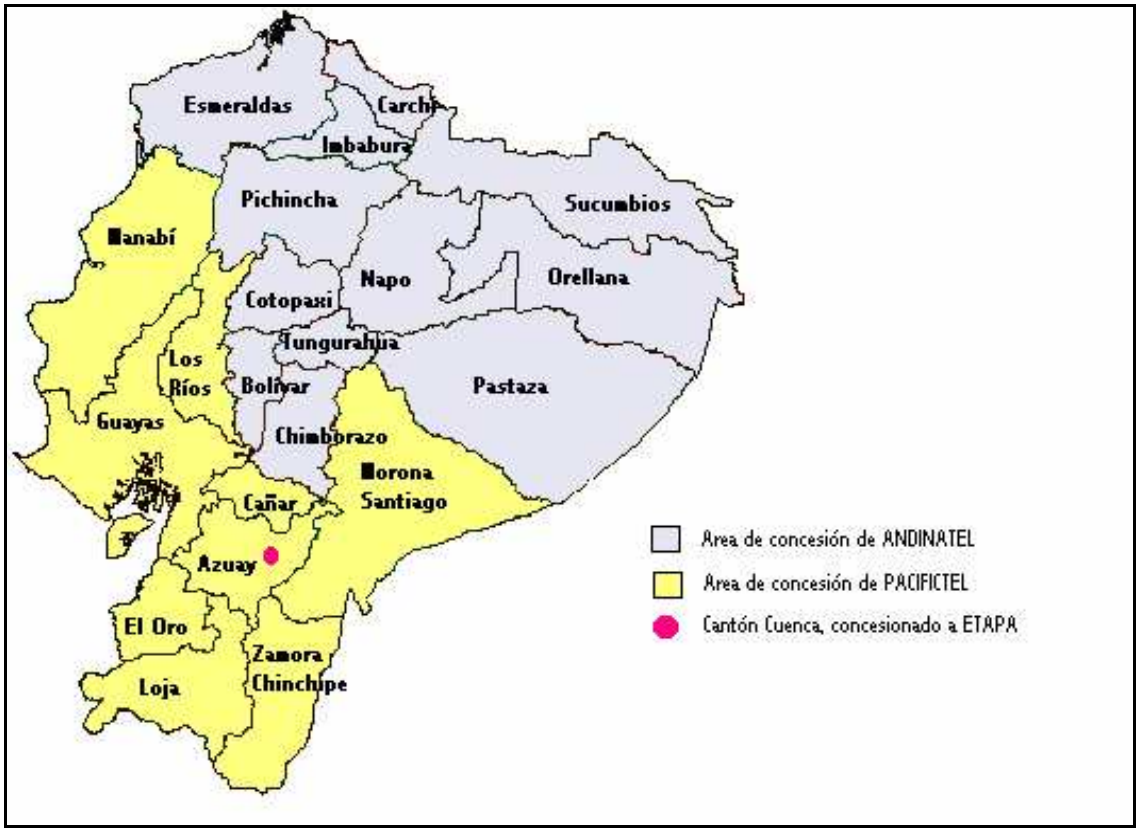


Figura 5. Cobertura nacional de Andinadatos

IMPSAT[17]

Es una empresa que brinda el servicio de transmisión de datos a nivel urbano, interurbano e internacional en las principales ciudades de Latinoamérica, cuenta con una red de fibra óptica de gran capacidad y velocidad. El servicio comprende: redes IP, Frame Relay, ATM y conexiones LAN a LAN. Posee cobertura en 17 ciudades a nivel nacional y soporte técnico permanente; dentro de los principales servicios que ofrece se puede nombrar los siguientes:

Interplus.- Es un paquete de servicios satelitales de transmisión de voz, datos, fax y video punto a punto que opera a diversas velocidades; como beneficios se puede mencionar el acceso rápido a lugares distantes con alta demanda de tráfico permanente permitiendo transferir archivos, voz y videoconferencia entre oficinas dispersas geográficamente.

Vsat.- Es una solución satelital integrada de conectividad y equipamiento para redes, destinada a interconexiones entre oficinas centrales y la posibilidad de ofrecer un gran número de puntos remotos. Resulta un sistema económico que tiene cobertura geográfica ilimitada, alta flexibilidad y homogeneidad de red brindando seguridad en la información transmitida. Como aplicaciones de esta solución se tiene la instalación de aplicaciones corporativas criticas donde es importante la confiabilidad del enlace y los buenos tiempos de respuesta, interconexión de redes LAN y complementación o respaldo de redes terrestres.

Dataplus.- Servicio de conectividad vía satélite que permite establecer enlaces punto a punto digitales bidireccionales de alto tráfico y transparente al protocolo, con tiempos de respuesta mínimos y constantes y un ancho de banda asignado en forma permanente. Como aplicaciones de este servicio se puede citar: interconexión de equipos de telecomunicaciones con oficinas dispersas geográficamente, complementar redes terrestres para acceder rápidamente a lugares geográficamente distantes y con alta demanda de tráfico.

[17] Fuente: http://200.55.6.163/?c=544|545|&seccion=545&idioma=1&pais=17

MOVISTAR

Esta empresa presta el servicio de Internet dedicado a través de circuitos de ancho de banda fijos y con conexiones redundantes al backbone internacional de Internet a través de fibra óptica; como servicios adicionales ofrece: cuentas dial up, estadísticas vía web, DNS primario o secundario, Web hosting[18], cuentas de correo, filtros de correo entre otros.

A continuación se muestra la estructura de conexión

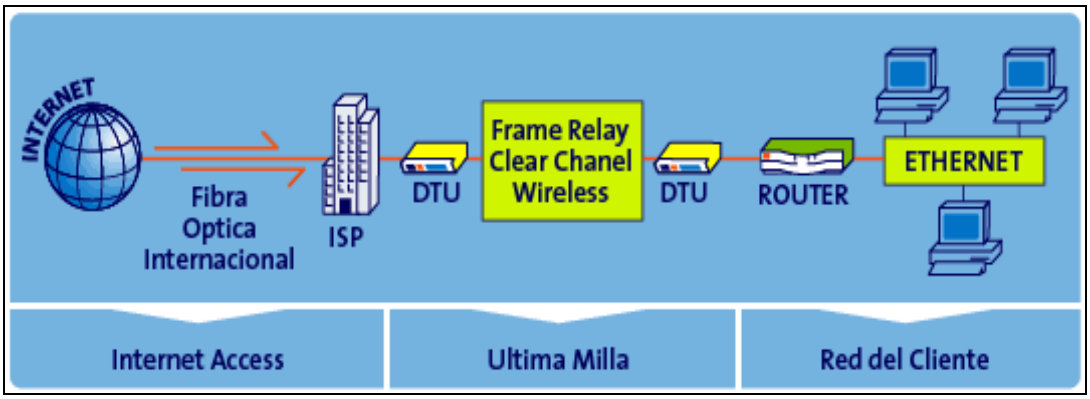


Figura 6. Estructura de la conexión con el proveedor del servicio de Internet

2.2.- ESQUEMAS DE BACKUP DE COMUNICACIONES:

Existe un solo esquema considerado como respaldo de comunicación que cubre el enlace con Guayaquil con un ancho de banda de 256 Kbps, siendo este contratado a Andinadatos.

Por esta razón se podría implementar redes privadas virtuales (VPN), lo cual permitiría crear un túnel de comunicación seguro, cifrando los datos que viajan a través de Internet para conectarse con los sitios o usuarios que utilizan aplicaciones críticas o acceden a los sistemas de despacho y facturación en los terminales y sucursales de la empresa.

[18] Servicio que permite a un sitio web estar conectado a Internet a alta velocidad a través de un servidor web para que la información pueda ser vista en todo el mundo a través de un navegador (http://www.sindicacion.net/diccionario_glosario/diccionario_w.htm, Enero 2006)

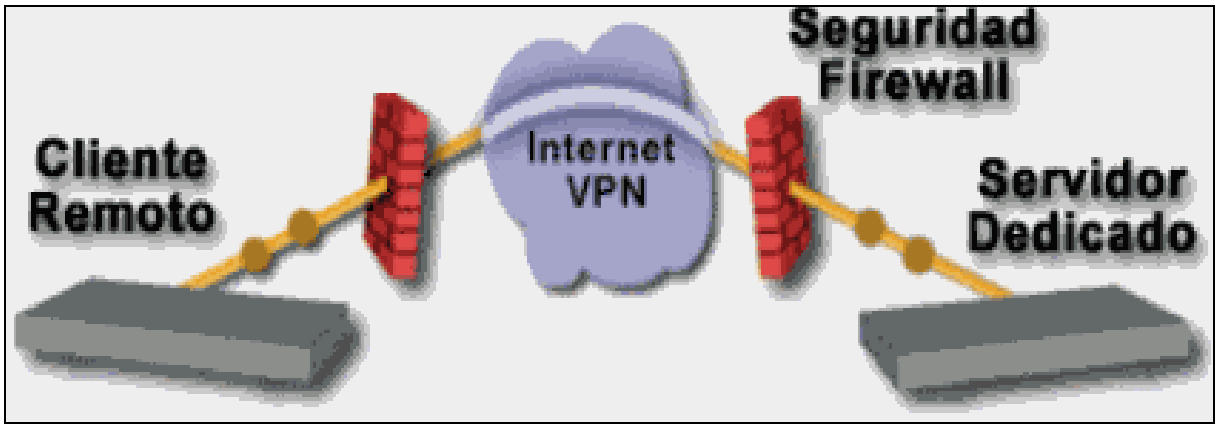


Figura 7. Esquema de una conexión VPN

Generalmente cuando se desea implantar una VPN hay que asegurarse que esta proporcione: identificación de usuario y restringir el acceso a aquellos no autorizados, administración de direcciones, codificación de datos, administración de claves, es decir renovar las claves de codificación para el cliente y servidor, y soporte a protocolos múltiples que usa la red pública.

En el mercado existen varias alternativas para poder realizar conexiones de red privadas y seguras a través de Internet por lo que a continuación nombraremos las siguientes:

CHECK POINT[19]: Presenta algunas soluciones como:

VPN-1 Net la cual es una solución de red privada virtual dedicada, que proporciona conectividad sencilla, rápida y segura, está diseñada para interconectar múltiples oficinas y usuarios basándose en una tecnología de control de accesos patentada por la misma empresa y denominada inspección completa del estado de conexión (statefull inspection).

VPN-1 Pro es una solución de software combinada de cortafuegos y VPN que permite gestionar políticas de seguridad e integra funciones de control de acceso, autenticación, cifrado avanzado (AES) y el algoritmo de encriptación 3DES para

[19] Fuente: http://www.solucionesseguras.com/productos/checkpoint/enterprise.asp

garantizar las conexiones de red. Con la utilidad VPN One Click que ofrece Check Point pueden crearse conexiones VPN de gran escala, solamente con definir todos los puntos finales de VPN-1 para que estas se activen automáticamente.

Los requerimientos del sistema para este producto son: Windows 2000 Server/Advanced Server, Windows NT 4.0, Red Hat Linux 7.0, 7.2, 7.3; espacio en disco duro de 40Mb y memoria RAM 128Mb.

Adicionalmente Check Point ofrece una plataforma de servicios de seguridad denominada Safeoffice que consiste en un dispositivo de fácil instalación cuya finalidad es la de proteger la conexión a Internet, proteger la privacidad de los datos, mantener la integridad de los equipos y de la red, filtrar contenidos inapropiados (URL[20]) y asegurar la vía de acceso a cualquier red corporativa.

CISCO[21]: Esta empresa ofrece con sus equipos la capacidad de conexión segura utilizando redes privadas virtuales que pueden dividirse en: VPN de ubicación a ubicación, y VPN de acceso remoto. Las VPN de ubicación a ubicación se construyen con ruteadores optimizados: Cisco 800, 1700, 2600, 3600, 7100 y 7200, los cuales incluyen encriptación mediante IPSec y 3DES, mientras que para las VPN de acceso remoto se utiliza el equipo Cisco VPN 3000 concentrator

Con la utilidad Easy VPN el servidor acepta conexiones de los clientes Cisco y elimina las configuraciones complejas en los sitios remotos en donde los clientes pueden utilizar plataformas Win9x, NT, 2000, XP, Linux o Solaris; una vez que el perfil está definido solo se necesita importar a las maquinas remotas con lo que casi no se necesita la intervención del usuario final.

[20] Es el término técnico que se utiliza para referirse a una dirección de Internet. Cada URL es único y está formado por varias partes.
[21] Fuente: http://www.adatel.es/interconexion_cisco.htm

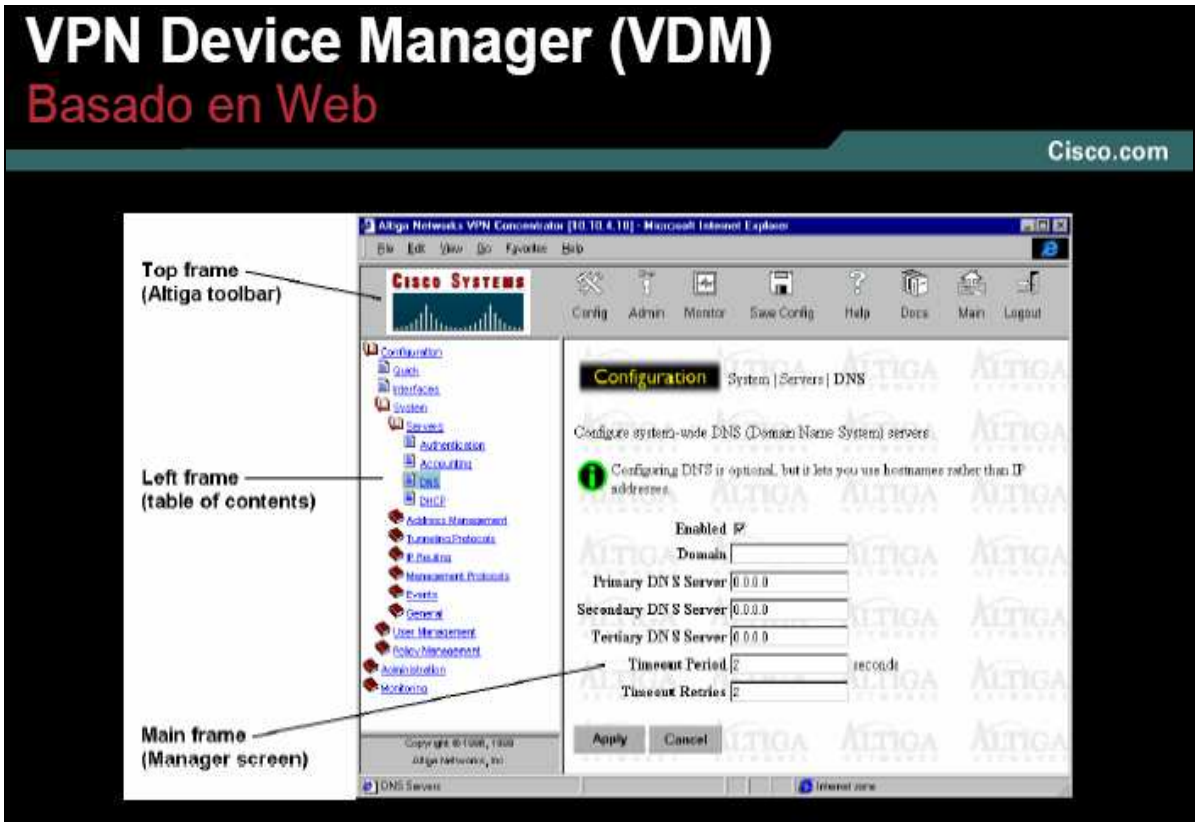


Figura 8. Interfase gráfica de VPN Device Manager de Cisco

Como principales características de los dispositivos Cisco utilizados para conexiones VPN podemos citar las siguientes:

Cisco VPN 3000.- Concentrador disponible para acceso remoto cuyos clientes utilizan un dispositivo de hardware denominado VPN 3002, posee la capacidad de realizar actualizaciones y es independiente de una plataforma de hardware, pueden trabajar con todos los sistemas operativos sin interferir en las operaciones del PC. Esta aplicación es de gran efectividad e ideal para organizaciones con usuarios remotos.

Cisco 800 Series.- Ruteadores ideales para oficinas de hasta 20 usuarios que permiten usar servicios de red gestionados, redes virtuales y acceso seguro a Internet.

Cisco 1700.- Es un producto modular para el acceso a Internet, Intranet y Extranet, proporciona una solución a medida de acceso para pequeñas y medianas empresas, permite gran flexibilidad para adaptarse al continuo cambio

de los requerimientos y al crecimiento de las tecnologías WAN. Dentro de esta serie está el Cisco 1750 y 1760 siendo los equipos más pequeños que pueden implementar voz sobre IP (VoIP).

Cisco 3600.- Esta familia de ruteadores constituyen una plataforma multifunción que permiten utilizar aplicaciones de acceso telefónico, LAN to LAN o de enrutamiento, además permite incorporar capacidades de integración multiservicio de voz y datos con lo que se ahorra costos de llamadas entre oficinas.

SYMANTEC[22]: Como solución VPN ofrece un ruteador denominado Nexland Pro 800 turbo que posee una funcionalidad de conexiones privadas virtuales avanzada; dispone de dos entradas de ancho de banda de Internet, es decir, se puede conectar al mismo dos líneas ADSL o del tipo que sean y sumar los anchos de banda, o se puede mezclar tipos de conexión y proveedores; hace un balance de carga de ambas conexiones a Internet con el fin de asegurar las máximas prestaciones en cualquier circunstancia.

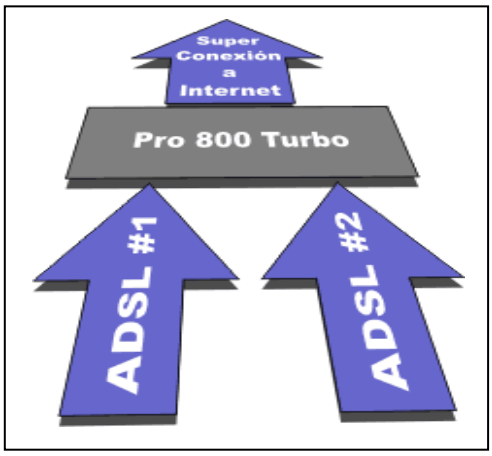


Figura 9. Esquema de conexión Nexland pro 800 turbo de Symantrec

Con este equipo se puede establecer conexiones VPN punto a punto, ofreciendo alta seguridad IPSec, y gracias a su capacidad de unir anchos de banda se puede tener conexiones privadas virtuales equilibradas; adicionalmente este dispositivo tiene incluido un switch de ocho puertos integrado el cual ahorra costos en redes pequeñas.

[22] Fuente: http://www.adslnet.ws/modules.php?name=News&file=article&sid=1414

OPENVPN [23]: Es una solución de conectividad basada en software SSL[24], ofrece conectividad punto-a-punto con validación jerárquica de usuarios y equipos conectados remotamente, y soporta una amplia configuración entre ellas balanceo de cargas entre otras. Está publicado bajo licencia de código libre.

Esta aplicación usa todas las características de encriptación, autenticación y certificación de la librería OpenSSL para tunelizar en forma segura redes IP sobre un solo puerto TCP/UDP.

Con OpenVPN se puede enlazar dos nodos de forma que parezca que están conectados a la misma LAN; un nodo A conectado a una red privada y a Internet y un nodo B en cualquier parte del mundo conectado a Internet; para la autenticación se utilizan certificados RSA (sistema criptográfico de clave pública) de forma que solo los equipos autorizados puedan acceder a la red virtual.

2.3.- ESQUEMAS DE COMUNICACIÓN SEGUROS ENTRE PETROCOMERCIAL Y OTRAS ENTIDADES.

Para garantizar la seguridad dentro la red y la confiabilidad en la comunicación con entidades externas se tiene instalado el producto IBM Firewall SecureWay, el cual se encuentra bajo el sistema operativo AIX; sus requerimientos en hardware son los siguientes:

1GB en disco duro.
Mínimo 64 Mb de memoria
Por lo menos 2 interfases de red: Una conexión segura y una no segura con direcciones IP estáticas asignadas para cada una.
Sistema operativo AIX versión 4.3.2 o mayores; no soporta versiones anteriores.
Recomendable instalar en un equipo IBM Risc System / 6000; y poseer un servidor de nombres de dominio (DNS) interno y otro externo.

[23] Fuente: http://laurel.datsi.fi.upm.es/~rpons/openvpn_como/
[24] Protocolo que sirve para asegurar los datos enviados por el navegador mediante encriptación o cifrado

Adicionalmente dentro del producto se tiene una aplicación a nivel de proxy llamado IBM Firewall Secure Mail Proxy el cual no realiza caché y actúa como intermediario entre el servidor de correo original y el receptor.
Si se desea usar SNMP para monitorear el firewall se requiere instalar el sistema View Agent para AIX.

En la comunicación con otras entidades se tiene definido esquemas de seguridad mencionados anteriormente y que se detallan a continuación:

SRI:
En la comunicación con esta entidad, el enlace sirve para enviar información acerca de la facturación en despacho de combustible a nivel nacional. Para esto se tiene definido una política con la dirección IP del equipo a través del cual Petrocomercial se comunica con el SRI esperando de retorno una respuesta indicando que esta ha sido recibida correctamente.

DNH:
La comunicación con esta institución se realiza utilizando un medio físico directo (par de cobre), con lo que conseguimos comunicación privada entre el Ministerio de Energía y Minas y Petrocomercial, de igual forma se tiene definido políticas en las que se describe las direcciones IP de los equipos a los cuales se envía información hacia la base de datos en la DNH; así como computadores que se comunican a través de sesiones telnet con el servidor PCO8 de Petrocomercial con el fin de utilizar las aplicaciones de comercialización interna y movimientos de productos de la empresa, para lo cual se autentifica con su propio usuario y contraseña.

Petroecuador:
Existe un enlace directo de fibra óptica que comunica a la empresa con Petroecuador utilizando el ruteador Cisco 3600 ubicado en la matriz, con lo que mediante la definición de políticas en el firewall se puede acceder desde determinados equipos de Petrocomercial a las aplicaciones de los sistemas de oferentes, auditoria y control de gestión; los cuales se encuentran instaladas en servidores de Petroecuador.

Filiales:
En estas reglas de seguridad se describen los equipos que se pueden conectar desde las filiales de Petroecuador como son: Petroindustrial y Petroproducción hacia el SRI y la DNH aprovechando el enlace de comunicación existente desde Petrocomercial, de igual forma se permite la comunicación entre ciertos servidores de Petrocomercial con equipos de las demás filiales para solventar determinados requerimientos.

Luego de este análisis y debido a que SecureWay Firewall es un software cerrado cuyo propietario es IBM y adicionalmente viene funcionando desde hace 7 años, sin tener definido una zona desmilitarizada; se consideró la posibilidad de reemplazarlo por un producto cuya administración sea más amigable y en un equipo en el cual se pueda añadir una interfase de red adicional para implementar la DMZ, y poder depurar las políticas de seguridad que en algunos casos están mal definidas o simplemente se deben eliminar ya que estas crean agujeros de seguridad que ponen en riesgo el acceso hacia los equipos de la red interna de la empresa.

Es importante considerar que al dejar de utilizar SecureWAy Firewall se debe configurar un servidor proxy el cual debe tener la capacidad de hacer caché para mejorar la velocidad de acceso hacia el Internet por parte de los usuarios.

Por esta razón se menciona a continuación productos con sus principales características, los cuales pueden ser utilizados como cortafuegos para la empresa:

ASTARO: Ofrece su producto Astaro Security Linux V5, el cual provee de una completa solución de seguridad de red que proporciona seis aplicaciones críticas: firewall, VPN, antivirus, antispam (correo electrónico no deseado), detección de intrusos y filtrado de contenido.
En lo referente al firewall provee de una completa inspección de paquetes y proxy de aplicaciones para proteger el tráfico de las comunicaciones de Internet en la organización, protección de ataques de negación de servicio y escaneo de puertos.

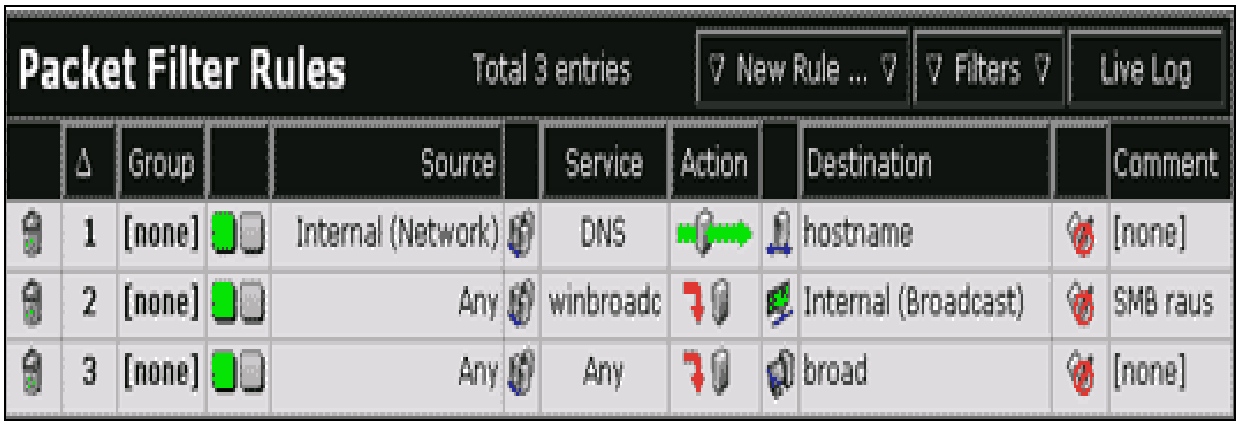


Figura 10. Interfase gráfica del firewall de Astaro

Posee una herramienta administrativa vía remota usando Webadmin que permite el manejo del sistema vía Web mediante un enlace encriptado, con lo que cambios a usuarios o grupos, políticas de seguridad y configuraciones del sistema pueden ser realizados de forma rápida y sencilla a través de pantallas intuitivas.
Astaro Security Linux está disponible como software para ser instalado en una PC o preinstalado en equipos dedicados, el cual está basado en proyectos de código abierto y ha sido puesta en práctica y probada con más de 10000 instalaciones en varios países.
Entre sus características se puede instalar hasta 20 tarjetas de red PCI Ethernet y soporta 40000 LAN virtuales.

FOTIGATE[25]: Fortigate Antivirus Firewall es una gama de aplicaciones desarrollada por Fortinet para la protección de redes en tiempo real, son plataformas que combinan hardware y software para ofrecer antivirus, filtrado de contenidos web y de correo, cortafuegos de inspección detallada, VPN con IPSec, detección y prevención de intrusos, detección y eliminación de intrusos que provienen de los contenidos de correos y tráfico de la web en tiempo real sin reducir el rendimiento de la red.

Las plataformas desarrolladas por Fortinet se basan en una tecnología denominada ASIC (Application-Specific Integrated Circuit) con lo que tienen la

[25] Fuente: http://www.afina.es/productos/Fortinet/fortinet_n.htm

capacidad de procesar gran cantidad de datos y analizar los contenidos de la red en tiempo real.

Dentro de las aplicaciones existe la solución para seguridad de host remoto Forticlient diseñada para proveer de acceso seguro desde sitios remotos hacia los recursos de la red, este software con capacidad IPSec es fácil de usar e incluye un firewall personal, NAT, administración de políticas centralizada, encriptación robusta y la mayoría de sistemas operativos Windows están soportados de forma nativa.

Para la administración y monitoreo se utiliza la herramienta denominada Fortimanager la cual permite implementar, monitorear, y mantener el rango completo de servicios provistos por estos dispositivos dando soporte a las necesidades de seguridad de la empresa.

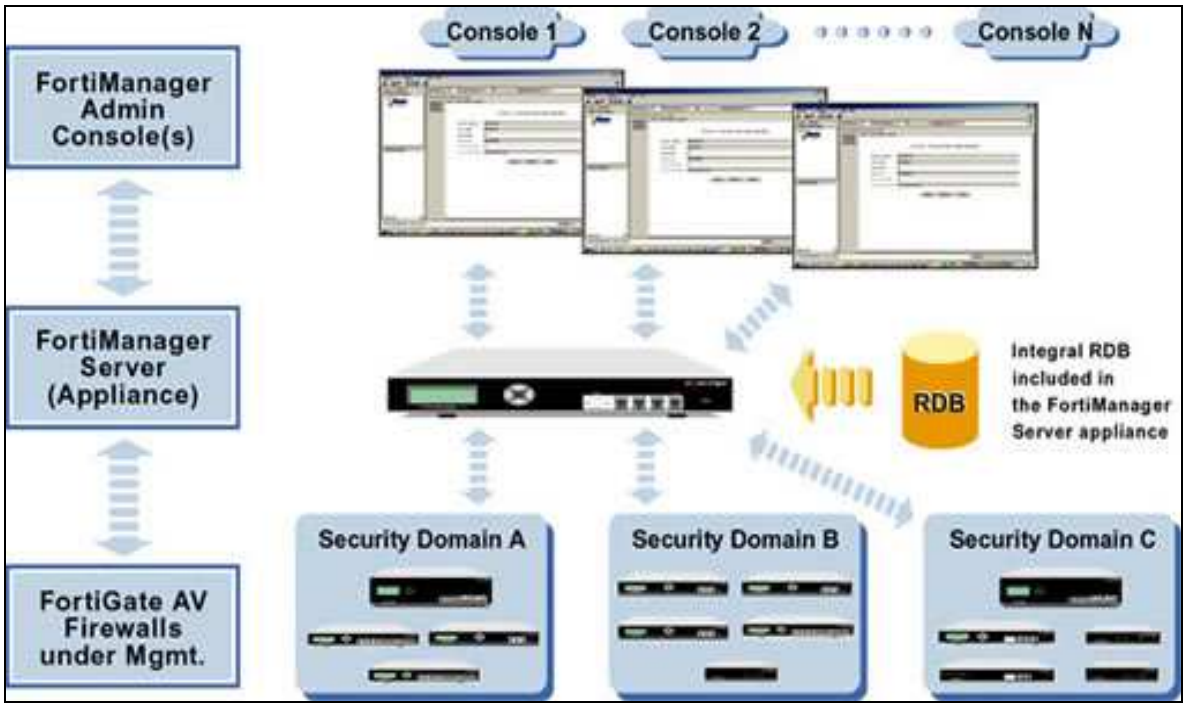


Figura 11. Esquema de seguridad de Fortigate

SYMANTEC[26]: En lo referente a soluciones de firewall esta empresa ofrece Symantec Gateway Security 5400 que es un dispositivo de que integra tecnología de inspección completa de paquetes con inteligencia de prevención de intrusos en el gateway entre Internet y la red corporativa o entre segmentos de red. Esto permite a los administradores configurar políticas granulares para obtener control completo de la información que entra y sale de la red, en el caso de existir sesiones VPN activas la tecnología de red privada virtual desencripta el paquete y lo integra en el flujo de datos. La tecnología de detección y prevención de intrusos bloquean paquetes que contienen amenazas y notifican al firewall la existencia de sesiones maliciosas de direcciones IP específicas.

Adicionalmente el firewall abre y examina los paquetes de protocolo de capa de aplicación; si estos están basados en http, la tecnología de filtrado de contenidos compara la fuente IP con una lista de sitios web prohibidos interrumpiendo y registrando estos paquetes; si los mismos están basados en http, ftp o smtp, los archivos anexos se envían al analizador de virus para que se reparen o elimine si es el caso; luego de todas estas comprobaciones el paquete puede entrar o salir de la red.

En lo referente a la administración de la configuración de políticas se lo hace a través de una interfaz segura basada en la red SSL, se integra fácilmente en la consola de administración de Symantec y permite generar alertas informes centralizados y una visión en tiempo real del tráfico en la red.

CISCO: Pone a disposición los dispositivos de seguridad ASA (Adaptive security appliance) de la familia 5500 los cuales permiten detener ataques antes que se difundan a la red corporativa, controla el tráfico en aplicaciones y redes y ofrece conectividad VPN flexible. Esta familia de dispositivos incluye productos como el Cisco ASA 5510, 5520 y 5540, los cuales son diseñados para abarcar requerimientos de empresas pequeñas hasta grandes corporaciones consiguiendo un alto rendimiento y la posibilidad de operar múltiples servicios de seguridad de forma simultánea.

[26] Fuente: http://www.symantec.com/region/mx/product/integrated/gateway/DS00086-SL_SGS_5400_Series.pdf

Cisco ofrece defensa Anti-X basada en la web contra gusanos y virus, protección de spyware[27] y adware[28], micro inspección de tráfico en red corporativa y prevención ante intrusos, hakers y ataques de negación de servicio.

Estos dispositivos se instalan en el extremo de la red corporativa para asegurar los flujos de paquetes entrantes y salientes y el tráfico VPN, de igual forma se pueden desplegar en el centro de datos o en segmentos de la LAN a fin de restringir los accesos a ciertos equipos de la red y monitorizar el tráfico interno ya que incluyen capacidades de inspección de capa dos a cuatro.

El Cisco ASA 5510 es destinado a empresas con conexiones remotas y es usado como una solución fácil de instalar, gestionar y monitorizar con una aplicación basada en la web, este modelo incluye funciones de firewall de alto rendimiento con opción DMZ, servicio VPN y prevención de intrusos.

El Cisco ASA 5520 aporta una amplia gama de servicios de seguridad y conectividad Gigabit Ethernet para medianas empresas, posee capacidad IPSec y SSL VPN para soportar un gran número de conexiones remotas pudiendo duplicar su capacidad VPN instalando una actualización de la licencia.

El Cisco ASA 5540 es una solución de alto rendimiento y conectividad Gigabit Ethernet para grandes y medianas empresas y proveedores de servicios. Su aplicación de defensa anti-x puede ser extendida utilizando un módulo de servicios de seguridad, así como su capacidad IPSec y SSL VPN para un mayor número de conexiones remotas.

En lo referente a la administración el Cisco ASA de la serie 5500 utiliza Adaptive Security Device Manager para un solo dispositivo y Cisco Security Managment Suite para múltiples dispositivos, estos están basados en la web y ofrecen configuración a todos los servicios de dispositivo VPN y de seguridad; entrega el estado del equipos, monitoreo y reporte de servicio.

---

[27] Software espía. Suelen ser programas que incluyen un pequeño código para lograr subir a una página web o correo electrónico determinado datos del usuario sin el conocimiento ni el consentimiento del mismo. (http://webs.ono.com/usr016/Agika/4diccionario/diccioP_U.htm, Enero 2006)

[28] Software que durante su funcionamiento despliega publicidad de distintos productos o servicios. Estas aplicaciones incluyen código adicional que muestra la publicidad en ventanas emergentes o en barras que aparece en la pantalla. (http://es.wikipedia.org/wiki/Adware, Enero 2006)

2.4.- ESTUDIO DE VIABILIDAD ECONÓMICO, TÉCNICO Y LOGÍSTICO.

Dentro de los rubros que Petrocomercial mensualmente asume como gastos de comunicaciones contratados a empresas se tiene los siguientes:

- Depósito de Riobamba, 800 dólares mensuales por un canal de 64 Kbps contratado a Andinadatos.
- Terminal de Cuenca, 1500 dólares mensuales por un canal de 64 Kbps contratado a Andinadatos.
- Sucursal Guayaquil, 2000 dólares mensuales por el enlace de respaldo de 256 Kbps contratado a Andinadatos.
- Enlace satelital, dos canales de 64 Kbps cada uno hacia Baltra y Puerto Ayora actualmente contratado con Impsat por tres meses el cual tiene un costo total de 16000 dólares.

Debido a que estos valores representan gastos operativos, se puede pensar en optimizar las comunicaciones hacia estos lugares implementando soluciones VPN con equipos especializados como las citados anteriormente o desarrollar soluciones emergentes para el acceso remoto de equipos o usuarios críticos desde los diferentes terminales y sucursales de la empresa hacia la matriz garantizando la operatividad en despacho y atención a clientes.

Los costos de soluciones de redes privadas virtuales se detallan a continuación:

Checkpoint: Conectividad para 25 usuarios $ 2.300
Conectividad para 100 usuarios $ 7.000

Cisco: Conectividad de acceso remoto Cisco VPN 3000 v 4.1 $ 2.200
Conectividad VPN de ubicación a ubicación con ruteadores optimizados:
Cisco 800 series: entre 500 y 700 dólares dependiendo del modelo.
Cisco 2600 series: entre 1500 y 2600 dólares dependiendo del modelo.
Cisco 3600 series: entre 3000 y 5200 dólares dependiendo del modelo

Symantec:

Nexland Pro 800 Turbo: ADSL, ruteador y VPN, tiene un costo de 5000 dólares.

A continuación se realiza un análisis comparativo de las soluciones de seguridad citadas

Soluciones de Seguridad								
Detalle	Astaro Opc.1		Astaro Opc.2		Cisco		Cisco	
	Modelo 420		Servidor Dell		ASA 5520		ASA 5540	
		Costo		Costo		Costo		Costo
Appliance propietario	Si	$ 11.775			Si	$ 19.995	Si	$ 28.996
Servidor Dell			Si	$5.000	No		No	
Licencia Base	Si		Si	$7.590				
Licencia 500 usuarios					*		*	
Licencia 1000 usuarios		X			*		*	
Ilimitado				X	*		*	
Base de S. Operativo		Linux		Linux				
APLICACIONES DE SEGURIDAD								
Firewall	Si		Si		Si		Si	
VPN	Si		Si		Si		Si	
Protección de Intrusos	Si		Si		Si		Si	
Antivirus para correo	Si	$ 2.898	Si	$5.450	*		*	
Antivirus para web	Si	$4.055	Si	$6.100	*		*	
Filtrado anti-spam	Si		Si		No		No	
Filtrado URL	Si		Si		No		No	
Actualización automática de software	Si		Si		*		*	
Ventajas	Licencia para web y correo menor que opc.2		Licencia Base + correo + web usuarios ilimitados					
Desventajas LB: Licencia Base u: usuarios	LB 1000 usuarios LB + correo 750 LB + web 600 LB + coreo + web 500		El costo de licenciamiento de correo y web es mayor		Baja el rendimiento a un 70% con IPS activo		Baja el rendimiento a un 70% con IPS activo	
Instalación	Si	$ 2.000	Si	$2.000		*		*
Total sin IVA	$20.728		$26.140		$ 19.995		$ 28.996	

Tabla 10. Cuadro comparativo 1 de soluciones de seguridad

Soluciones de Seguridad								
Detalle	Fortigate		Symantec		Symantec		FirewallBuilder	
	1000		Gateway Security 5400		Gateway Securuty 5400		VPN Windows	
		Costo		Costo		Costo		Costo
Appliance propietario	Si	$ 12.995	Si	$37.300	Si	$ 24.000	No	
Servidor Dell	No		No		No		No	
Licencia Base								
Licencia 500 usuarios	*			X		X		
Licencia 1000 usuarios	*							
Ilimitado	*							X
Base de S. Operativo				Linux		Linux		Linux
APLICACIONES DE SEGURIDAD								
Firewall	Si	$9.369	Si		Si		Si	
VPN	Si		Si		Si		Si	
Protección de Intrusos	Si		Si		No			
Antivirus para correo	Si		Si		No			
Antivirus para web	Si		Si		No			
Filtrado anti-spam	Si		Si		No			
Filtrado URL	Si		Si		No		Si	
Actualización automática de software	Si		Si		No			Internet
Ventajas							Costo	
Desventajas LB: Licencia Base u: usuarios	Baja el rendimiento un 40% con IPS y el antivirus activo		Licenciamiento solo para 500 usuarios		Licenciamiento solo para 500 usuarios		No se tiene protección de antivirus, anti-spam y otros.	
Instalación		*		*		*		*
Total sin IVA	$22.364		$37.300		$ 24.000		$ 0	

* No se tiene información

Tabla 11. Cuadro comparativo 2 de soluciones de seguridad

Con estos antecedentes la factibilidad técnica y logística de implementar alguna de las soluciones expuestas depende de las aplicaciones, nivel de seguridad y número de usuarios que actualmente a nivel nacional son entre 600 y 700 entre la regional norte y sur de la empresa.

En lo referente a la viabilidad económica no existe actualmente la disponibilidad de recursos para la adquisición de equipos por lo que los procesos de compra pueden demorar varios meses; pero debido a la necesidad de atender de forma prioritaria los requerimientos de cambio de firewall y por ende de proxy, así como también el diseñar un respaldo en las comunicaciones que de forma emergente pueda mantener operativo las aplicaciones y atención en los terminales y sucursales de la empresa; se deberá utilizar herramientas sin licenciamiento o software libre que en el caso del firewall y del proxy pueden ser instaladas y configuradas sobre una plataforma Linux que posee algunas ventajas como las siguientes:

- Es un sistema operativo gratuito.
- No necesita un equipo con mayores requerimientos de hardware.
- Ofrece alta fiabilidad ya que Linux presenta gran estabilidad.
- Sobre este sistema operativo se puede montar múltiples servicios como servidor proxy http y ftp con caché de disco para acelerar la navegación por Internet y bloqueo opcional para los sitios web.
- Conversión de direcciones IP (NAT).

CAPÍTULO III

CAPÍTULO III

DISEÑO A NIVEL DE IMPLEMENTACIÓN DE LOS SISTEMAS DE SEGURIDAD Y BACKUP SOBRE LA INFRAESTRUCTURA ACTUAL DE LA EMPRESA

INTRODUCCIÓN

Para la definición de la zona desmilitarizada se necesita utilizar un firewall por software que trabaje sobre Linux y soporte el manejo de cuatro interfases ya que el producto anterior IBM Secure Way tenía definido solo tres y no se contemplaba la DMZ, de igual forma debe ser un producto flexible que permita administrar las políticas de seguridad con precisión, para ofrecer un confiable acceso a la red y proteger los recursos e información de la misma. Por esta razón se ha elegido la utilización de Firewall Builder como cortafuegos para controlar el tráfico de entrada y salida de la red así como para definir el área desmilitarizada.

En el caso del proxy se usará la herramienta propia de Linux denominada Squid con lo que se aprovechará la propiedad de hacer caché para mejorar el funcionamiento y acelerar la velocidad de acceso hacia el Internet ya que se agilita la navegación en las páginas de uso mas frecuente por parte de los usuarios, tomando en cuenta que el producto de Secure Way no ofrecía esta característica.

Con respecto al respaldo de comunicación emergente se puede utilizar la herramienta de VPN propio de Windows debido a que en la empresa el 90% de los equipos funcionan con los sistemas operativos Windows 2000 y XP, de esta forma la comunicación será más transparente para el usuario sin necesidad de utilizar programas o equipos adicionales y tener un acceso seguro desde medios como el Internet.

3.1.- ESQUEMAS Y DEFINICIÓN DE POLÍTICAS DE SEGURIDAD A DESARROLLARSE.

Para la instalación del cortafuegos se utilizó el sistema operativo Linux CentOS 4.0 ya que debido a la discontinuidad de Red Hat y la aparición de las licencias comerciales para Enterprise Linux, las cuales oscilan entre 500 a 1500 dólares se debe buscar alternativas libres y gratuitas como: Lineox Enterprise, Tao Linux, White Box Enterprise y CentOS; los cuales han sido construidos a partir de las mismas fuentes de RHEL (Red Hat Enterprise Linux).

Como principales características del sistema operativo Linux CentOS (Community Enterprise Operating System), se puede mencionar que es un clon a nivel binario de la distribución de RHEL compilado por voluntarios a partir del código fuente.

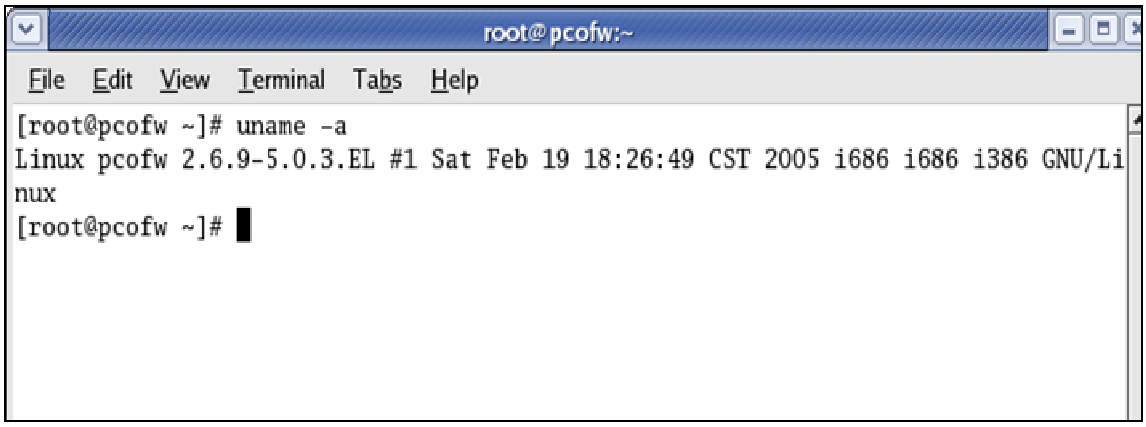


Figura 12. Versión del Kernel de Linux CentOS 4.0

Los requerimientos del sistema son los siguientes:
Memoria RAM: 192 MB (Mínimo).
Espacio en Disco Duro: 850 MB (Mínimo) - 2 GB (Recomendado).
Procesador: Intel Pentium I/II/III/IV/Celeron, AMD K6/II/III, AMD Duron, AMD Athlon/XP/MP.

El equipo utilizado para la instalación en Petrocomercial de Linux CentOS 4.0 y Firewall Builder es un servidor Compaq Proliant ML350 el cual posee las siguientes características: Procesador Pentium III de 800MHz, Memoria RAM de 1,2 Gb y dos discos duros de 8,5 Gb cada uno, con lo cual se solventa los requerimientos garantizando un correcto funcionamiento.

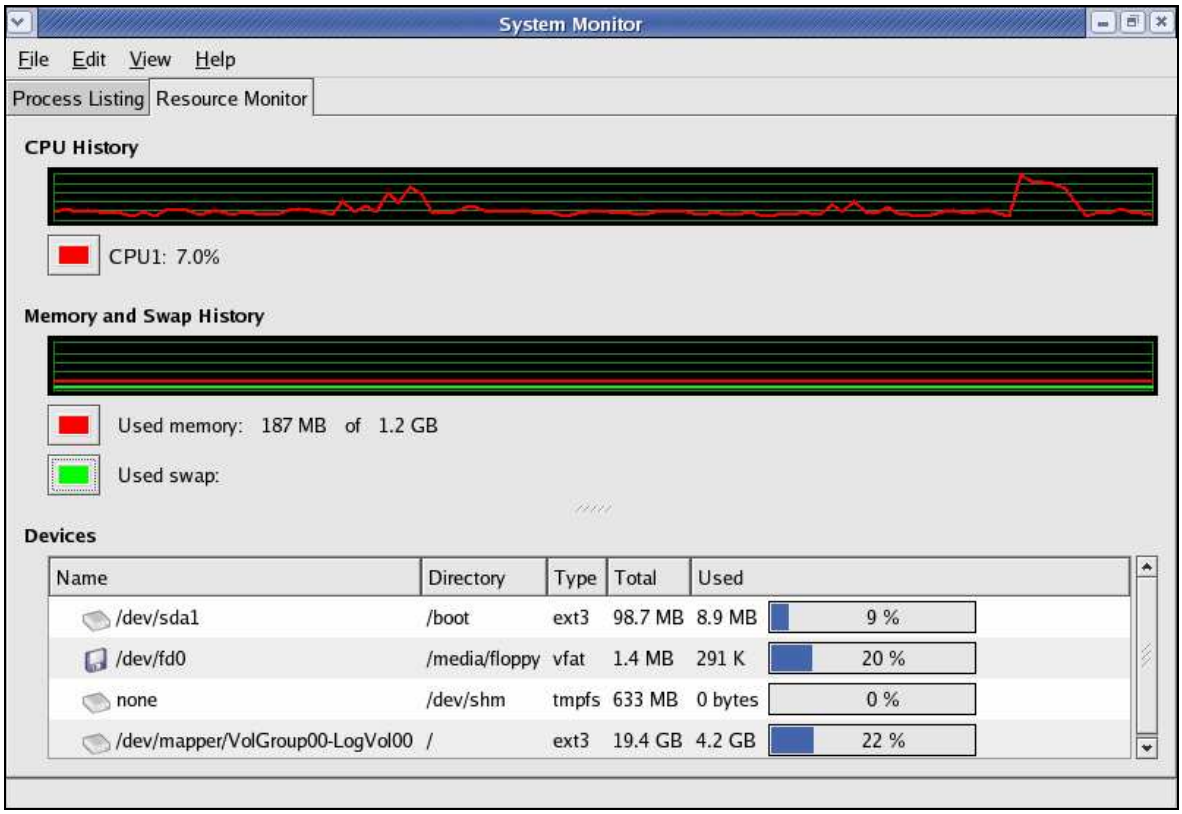


Figura 13. Características del servidor firewall

Al realizar la partición del disco duro se usaron los espacios en el orden y tamaño recomendado por CentOS, como se observa en la Figura 13, excepto en la partición Swap, ya que en un servidor que va a trabajar como firewall se tiene altas demandas de peticiones de usuarios y servicios por lo que es recomendable tener una memoria virtual bastante grande y en este caso se definió el doble del tamaño de la memoria RAM es decir 2Gb dividida en tres partes iguales en los dos discos.

En las configuraciones de red se definió cuatro interfases denominadas de la siguiente manera y con sus direcciones IP:

Nombre del servidor: Pcofw

No segura Eth0: IP: X.X.212.22
Máscara: 255.255.255.248

Segura Eth1: IP: X.X.64.6
Máscara: 255.255.248.0

Petroecuador:	IP: X.X.230.12
	Máscara: 255.255.255.0
DMZ:	IP: X.X.10.1
	Máscara: 255.255.255.0

La configuración del DNS son las direcciones del servidor de nombres de dominio del proveedor del servicio de Internet:

DNS Primario: X.X.208.1

DNS Secundario: X.X.208.2

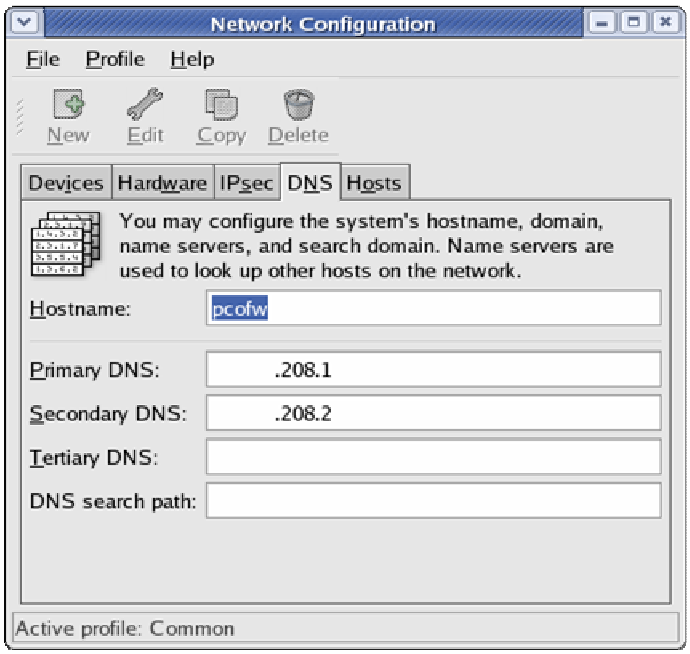


Figura 14. Configuración del DNS en el servidor Pcofw

Finalmente se selecciona las aplicaciones y paquetes tales como una interfase gráfica de usuario que en este caso es Gnome y otras funciones necesarias, cabe mencionar que se realizó la instalación mínima es decir solo con los paquetes indispensables para que el sistema funcione, así como también en la definición del firewall en el sistema operativo se mantienen cerrados todos los servicios para abrir solamente los puertos estrictamente necesario con la aplicación Firewall Builder.

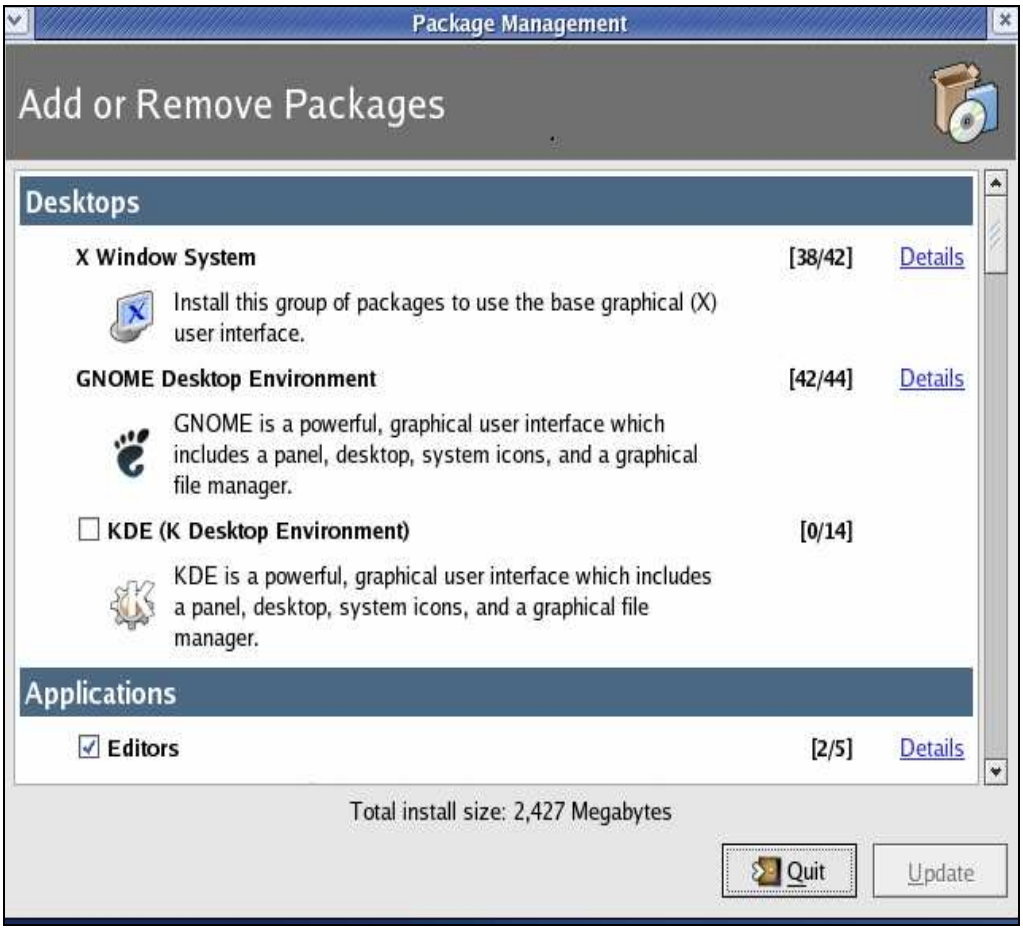


Figura 15. Instalación de paquetes en Linux CentOS 4.0

Firewall Builder:

Firewall Builder versión 2.0.6 es una herramienta Open Source (Código Abierto) escogida para configurar el cortafuegos cuya fortaleza está en poder manejar las políticas de seguridad con precisión y eficiencia sin estar asociado a líneas de comando como lo hacen otros productos disponibles en el mercado y prestando la facilidad de poder administrarlo a través de su interfase gráfica.

Este producto trabaja a nivel de capa de aplicación por lo que no permiten el tráfico directamente entre dos redes, sino que realiza un seguimiento detallado del trafico que pasa por él; maneja la pila de protocolos TCP/IP (http, ftp,telnet) e intercepta todos los paquetes que llegan salen de una aplicación, evitando que algún agente externo indeseado alcance las máquinas protegidas.

Estos firewalls de capa siete pueden ser usados como traductores de direcciones de red; es decir según pasa el tráfico de un lado a otro, enmascara la dirección de origen, lo que dificulta observar la topología de la red desde el exterior.

MODELO OSI	
Nivel de aplicación	DNS, FTP, HTTP, IMAP, IRC, NFS, NNTP, NTP, POP3, SMB/CIFS, SMTP, SNMP, SSH, Telnet, SIP
Nivel de presentación	ASN.1, MIME, SSL/TLS, XML,
Nivel de sesión	NetBIOS,
Nivel de transporte	SCTP, SPX, TCP, UDP,
Nivel de red	AppleTalk, IP, IPX, NetBEUI, X.25
Nivel de enlace	ATM, Ethernet, Frame Relay, HDLC, PPP, Token Ring, Wi-Fi,
Nivel físico	Cable coaxial, Cable de fibra óptica, Cable de par trenzado, Microondas, Radio, RS-232

Tabla 12. Tecnologías y protocolos de red del Modelo OSI

Al utilizar Firewall Builder, la configuración de las políticas no va asociado a términos de números de puertos o interfases del firewall, obligando a escoger la regla acertada para la interfase dada, por el contrario se puede crear un conjunto de objetos que describen al firewall, servidores, subredes y luego implementar las políticas por inclusión de objetos dentro de las reglas de la política. Con este producto se tiene la ventaja de escoger dentro de una amplia lista de objetos predefinidos que describen varios protocolos y servicios estándar; una vez que una política es construida en la interfase gráfica del usuario solo basta con compilarla e instalarla en la máquina del firewall.

Ventajas:

- Este producto posee 100 objetos predefinidos para los más populares y ampliamente usados servicios y protocolos.
- Tiene la capacidad para crear objetos describiendo servicios conocidos, IP, ICMP, TCP y UDP; así como para equipos, redes y rangos de direcciones.
- Posee plantillas para poder implementar las reglas del firewall utilizando políticas estándar para redes típicas las cuales pueden ser extendidas y

editadas de acuerdo a las demandas de crecimiento y complejidad que la red tenga.

- Se maneja una misma base de datos para los objetos de tal manera que cualquier cambio realizado a uno de ellos se verá reflejado en todas las reglas y políticas donde se lo haya incluido.
- Ofrece facilidad para cambiar una política en el archivo de configuración y luego instalarla esta en el firewall.
- Tiene una interfase gráfica amigable para el usuario que permite realizar operaciones como: copiar y pegar con el fin de poder editar las políticas de una manera más ágil.
- Soporta múltiples plataformas, incluyendo Cisco PIX y firewalls de código abierto iptables, ipfilter.
- Tiene la posibilidad de imprimir desde un solo objeto, una política del firewall, la jerarquía completa y exportar este a un archivo de texto, a un texto plano o a formato html.

Para la instalación de este producto debemos bajar los archivos de instalación de la siguiente dirección en Internet: www.fwbuilder.org/archives/cat_downloads.html

fwbuilder-2.0.6-1.rh90.i386.rpm; instalador de la aplicación.
libfwbuilder-2.0.6-1.rh90.i386.rpm; librerías de firewall builder.
Paquetes necesarios para el funcionamiento del programa:
fwbuilder-ipt-2.0.6-1.rh90.i386.rpm;
fwbuilder-pf-2.0.6-1.rh90.i386.rpm;
fwbuilder-ipfw-2.0.6-1.rh90.i386.rpm;
fwbuilder-ipf-2.0.6-1.rh90.i386.rpm;

Estos son instalados con el siguiente comando:
rpm –Uvh fwbuilder-2.0.6.1.rh90.i386.rpm
rpm –Uvh libfwbuilder-2.0.6.1.rh90.i386.rpm
rpm –Uvh fwbuildeript-2.0.6.1.rh90.i386.rpm
rpm –Uvh fwbuilderpf-2.0.6.1.rh90.i386.rpm
rpm –Uvh fwbuilderipf-2.0.6.1.rh90.i386.rpm
rpm –Uvh fwbuilderipfw-2.0.6.1.rh90.i386.rpm

Para abrir el programa se ejecuta el comando fwbuilder y se crea un nuevo firewall, en este caso denominado pcofw.

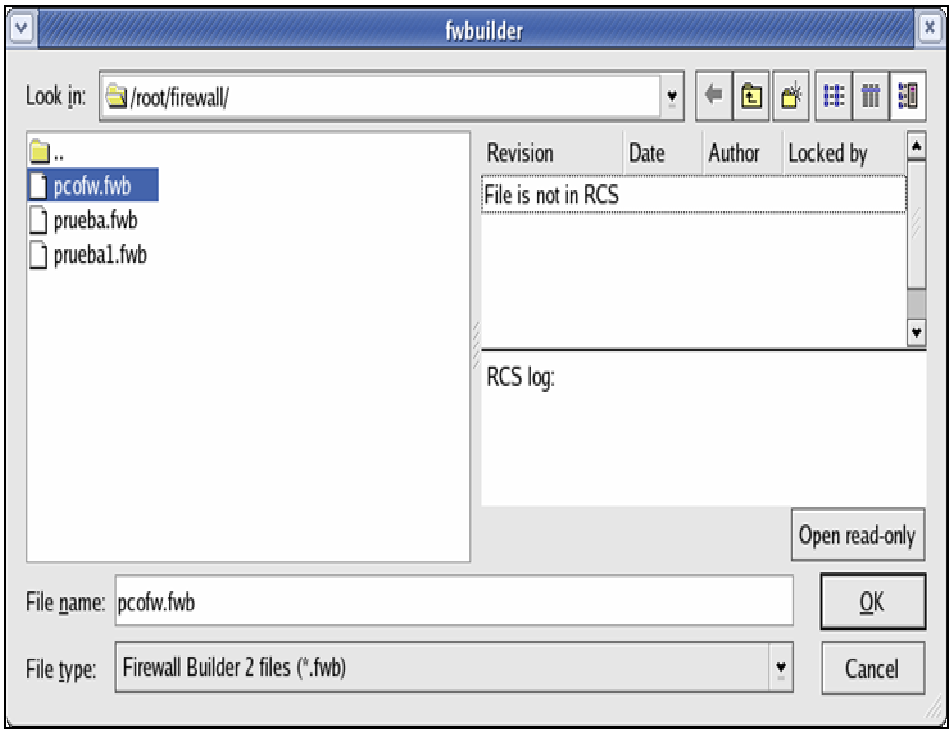


Figura 16. Creación del firewall Pcofw

Con el fin de poder establecer las políticas de seguridad e implementarlas es necesario crear las interfases del firewall y objetos dentro de los cuales se va a definir: direcciones, rangos de direcciones, redes, grupos y servicios utilizados en Petrocomercial.

Para la creación de las cuatro interfases se debe ir añadiendo una a una simplemente con un click derecho sobre el firewall creado y editando su dirección y máscara. Cabe señalar que al instalar las reglas, el producto realiza la validación de las interfases creadas para asociarlas con las que están configuradas a nivel del sistema operativo y verificar la coherencia entre sus direcciones IP y nombre de los dispositivos de red usados como se muestra en la Figura 17.

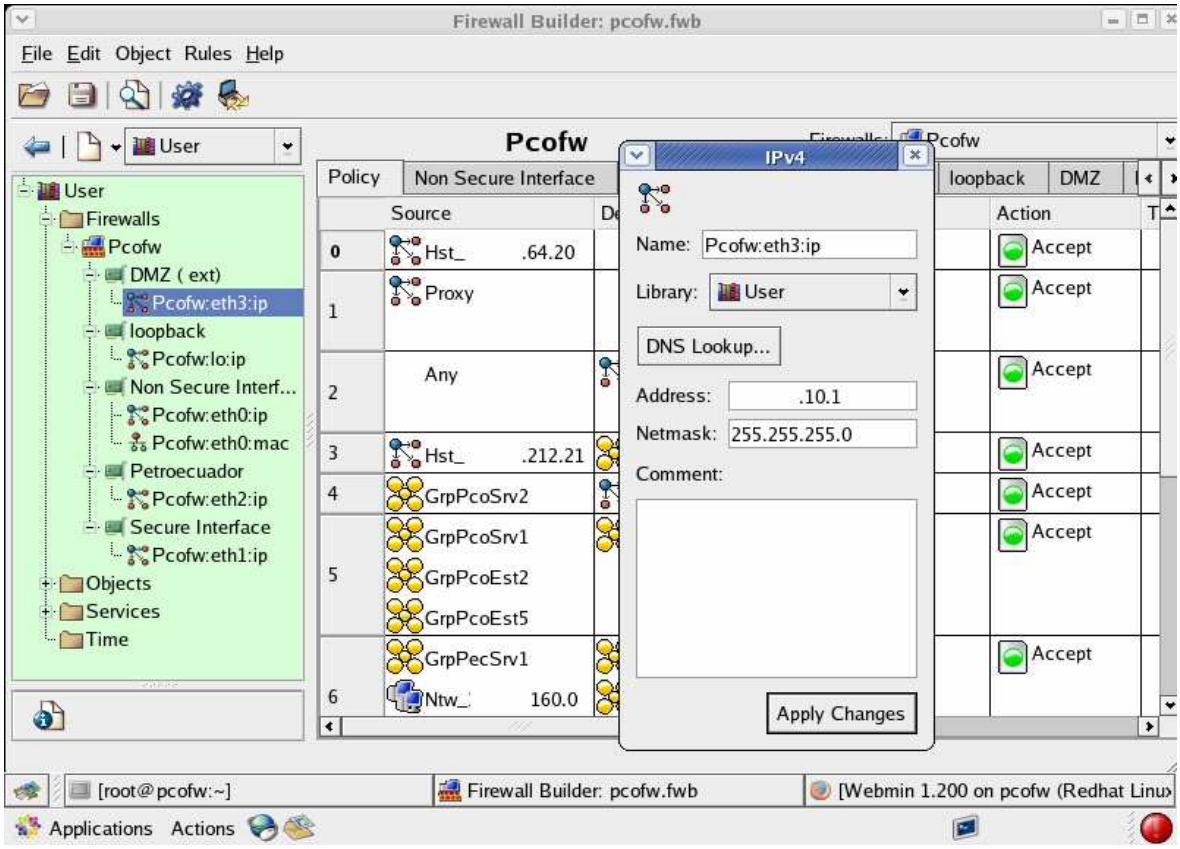


Figura 17. Interfases creadas en el firewall

Interfases del firewall

NonSecure Interface:	Nombre:	Pcofw:eth0:ip
	Dirección:	X.X.212.22
	Máscara:	255.255.255.248
Secure Interface	Nombre:	Pcofw:eth1:ip
	Dirección:	X.X.64.6
	Máscara:	255.255.248.0
Petroecuador:	Nombre:	Pcofw:eth2:ip
	Dirección:	X.X.230.12
	Máscara:	255.255.255.0
DMZ	Nombre:	Pcofw:eth3:ip
	Dirección:	X.X.10.1
	Máscara:	255.255.255.0

En la creación de objetos se tiene las opciones de: direcciones, rangos de direcciones, grupos, equipos y redes; se crea primero las direcciones una a una con sus respectivas direcciones IP, luego se puede crear grupos y a estos anexar direcciones solamente copiando y pegando en cada uno de ellos. De igual forma los rangos y redes se los definen con subdirecciones y máscaras como se detalla a continuación:

Direcciones:

Equipos y servidores de Petroecuador:

Hst_X.X.10.1	Hst_X.X.10.15	Hst_X.X.10.25
Hst_X.X.10.3	Hst_X.X.10.4	Hst_ X.X.144.231
Hst_ X.X.144.245	Hst_ X.X.145.182	Hst_ X.X.208.84
Hst_ X.X.226.11	Hst_ X.X.226.16	Hst_ X.X.226.17
Hst_ X.X.226.19	Hst_ X.X.226.21	Hst_ X.X.226.22
Hst_ X.X.226.4	Hst_ X.X.226.5	Hst_ X.X.226.6

Firewall Symantec Gateway Security de Petroecuador.

Hst_X.X.12.1

Equipos servidores del SRI

Hst_X.X.7.10 Hst_X.X.7.8

Equipos y servidores del Ministerio de Energía y Minas

Hst_X.X.1.20	Hst_X.X.1.207	Hst_X.X.1.5
Hst_X.X.1.8	Hst_X.X.1.9	

Equipos y servidores AS/400 de Petroindustrial

Hst_X.X.20.12	Hst_X.X.24.103	Hst_X.X.24.11
Hst_X.X.24.44	Hst_X.X.24.74	Hst_X.X.28.11

Equipos de Petrocomercial Regional Sur

Hst_X.X.170.145 Hst_X.X.170.146

Equipos y servidores de Petrocomercial matriz

Hst_X.X.64.100	Hst_X.X.64.15	Hst_X.X.64.20
Hst_X.X.64.24	Hst_X.X.64.25	Hst_X.X.64.26
Hst_X.X.64.28	Hst_X.X.64.29	Hst_X.X.64.59
Hst_X.X.64.65	Hst_X.X.64.66	Hst_X.X.64.8
Hst_X.X.71.21	Hst_X.X.71.25	Hst_X.X.71.5
Hst_X.X.71.6	Hst_X.X.71.7	

Equipos de Petrocomercial Guayaquil

Hst_X.X.97.11	Hst_X.X.97.110	Hst_X.X.97.131
Hst_X.X.97.173	Hst_X.X.97.20	Hst_X.X.97.48
Hst_X.X.97.57	Hst_X.X.97.88	

Equipos (DMZ)

Hst_ X.X.10.10	Hst_X.X.10.20

Equipos del SOTE

Hst_X.X.10.126	Hst_X.X.10.57

Equipos con direcciones públicas de Petrocomercial

Rt_X.X.212.17	Hst_X.X.212.18	Hst_X.X.212.19
Hst_X.X.212.20	Hst_X.X.212.21	

Servidor proxy de Petrocomercial: Proxy

Redes:

Ntw_X.16.0.0	Máscara:	255.255.0.0	Ministerio de Energía
Ntw_X.17.28.0	Máscara:	255.255.255.0	Petroindustrial
Ntw_X.17.33.0	Máscara:	255.255.255.0	Petroindustrial
Ntw_X.19.160.0	Máscara:	255.255.240.0	Petroecuador

Redes de Sucursales y Terminales de Petrocomercial:

Ntw_X.X.129.0	Ntw_X.X.130.0	Ntw_X.X.131.0
Ntw_X.X.132.0	Ntw_X.X.134.0	Ntw_X.X.136.0

Ntw_X.X.137.0	Ntw_X.X.138.0	Ntw_X.X.139.0
Ntw_X.X.161.0	Ntw_X.X.162.0	Ntw_X.X.163.0
Ntw_X.X.164.0	Ntw_X.X.165.0	Ntw_X.X.167.0
Ntw_X.X.169.0	Ntw_X.X.170.0	Ntw_X.X.75.0
Ntw_X.X.76.0	Ntw_X.X.77.0	Ntw_X.X.97.0

Todas con Máscara : 255.255.255.0

Ntw_X.20.64.0 Máscara: 255.255.248.0 Petrocomercial Matriz

World Dirección: 0.0.0.0. Máscara: 0.0.0.0

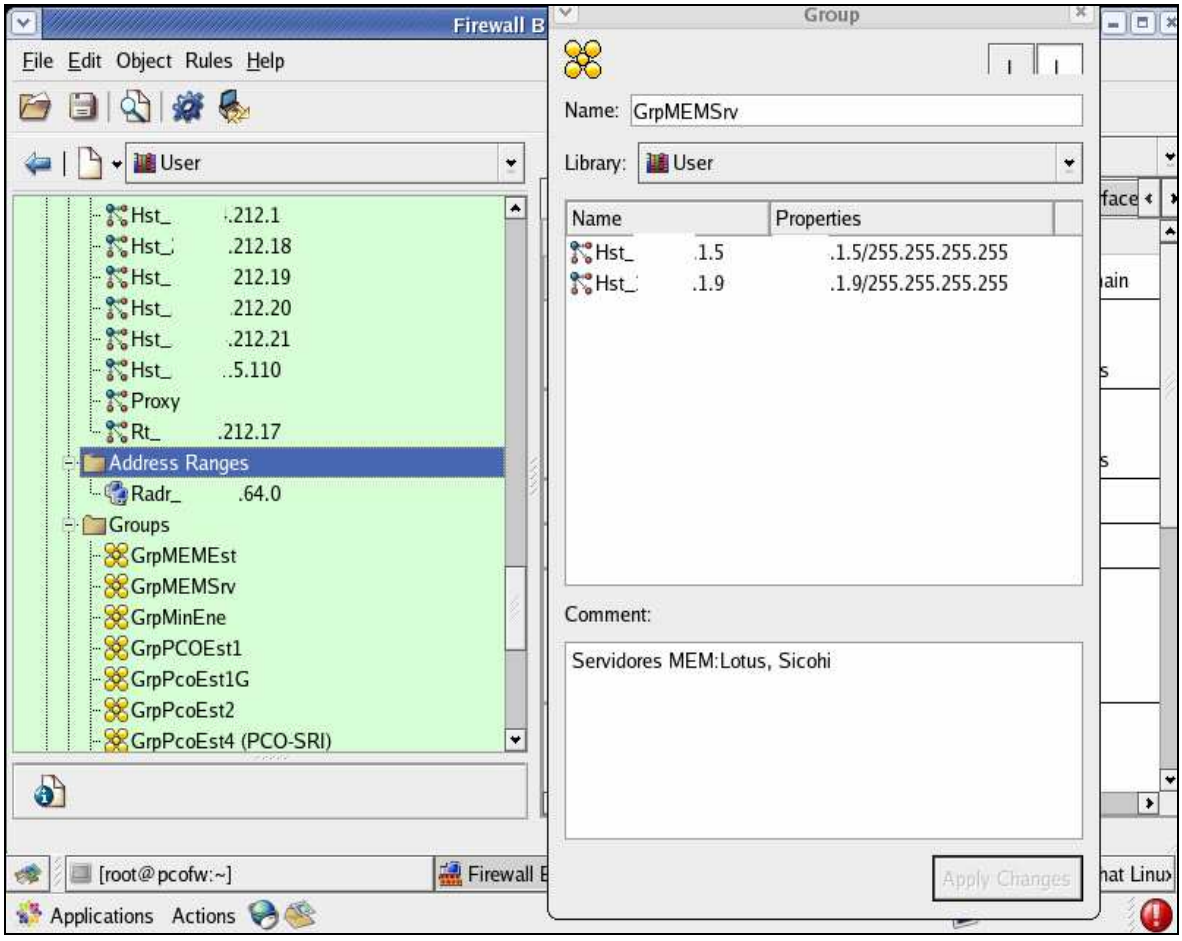


Figura 18. Creación de objetos en Firewall Builder

Rangos de direcciones:

Radr_X.X.64.0 Rango: X.X.64.30 hasta X.X.64.53

Grupos:

GrpMEMEst: (Estaciones del Ministerio de Energía)

Hst_X.X.1.20 Hst_X.X.1.207 Hst_X.X.1.8

GrpMEMSrv: (Servidores del MEM: Lotus y Sicohi)

Hst_X.X.15 Hst_X.X.1.9

GrpPCOEst1: (Redes de Petrocomercial y Petroindustrial)

Ntw_X.X.28.0	Ntw_X.X.33.0	Ntw:_X.X.129.0
Ntw_X.X.130.0	Ntw_X.X.131.0	Ntw_X.X.132.0
Ntw_X.X.134.0	Ntw_X.X.136.0	Ntw_X.X.137.0
Ntw_X.X.138.0	Ntw_X.X.139.0	Ntw_X.X.161.0
Ntw_X.X.162.0	Ntw_X.X.163.0	Ntw_X.X.164.0
Ntw_X.X.165.0	Ntw_X.X.167.0	Ntw_X.X.169.0
Ntw_X.X.170.0	Ntw_X.X.64.0	Ntw_X.X.75.0
Ntw_X.X.76.0	Ntw_X.X.77.0	Ntw_X.X.97.0

GrpPCOEst1G: (Equipos de Guayaquil que se conectan a servidores de Petroecuador)

Hst_X.X.170.145 Hst_X.X.170.146

GrpPcoEst2: (Equipos que utilizan la aplicación SUCO de Petroecuador)

Hst_X.X.64.20	Hst_X.X.97.11	Hst_X.X.97.110
Hst_X.X.97.20	Hst_X.X.97.48	Hst_X.X.97.57

Radr_X.X.64.0

GrpPcoEst4 (PCO-SRI): (Servidor y equipo que conectan al SRI)

Hst_X.X.71.21 Hst_X.X.71.5

GrpPcoEst5: (Equipos de Petrocomercial Sistemas)

Hst_X.X.71.5 Hst_X.X.71.6

GrpPcoEst6 (PCO-MEM): (Servidor y equipos que se conectan al MEM)

Hst_X.X.71.21 Hst_X.X.71.5 Hst_172.0.71.7

GrpPcoSrv1: (Servidores AS/400)

Hst_X.X.64.25 Hst_X.X.64.26 Hst_X.X.64.28

Hst_X.X.64.8

GrpPcoSrv2: (Equipos y servidores de correo de Quito y Guayaquil)

Hst_X.X.64.20 Hst_X.X.97.20 Hst_X.X.64.100

Hst_X.X.64.15

GrpPecSrv1: (Servidores y equipos de Petroecuador)

Hst_X.X.10.1 Hst_X.X.10.15 Hst_X.X.10.25

Hst_X.X.10.3 Hst_X.X.10.4 Hst_X.X.144.231

Hst_X.X.144.245 Hst_X.X.145.182 Hst_X.X.226.11

Hst_X.X.226.16 Hst_X.X.226.17 Hst_X.X.226.19

Hst_X.X.226.21 Hst_X.X.226.22 Hst_X.X.226.4

Hst_X.X.226.5 Hst_172.29.226.6

GrpPecUCont: (Servidor de la Unidad de Contratos de Petroecuador)

Hst_X.X.208.84 Hst_X.X.71.5

GrpPin: (Estaciones de Petroindustrial que se conectan al MEM)

Hst_X.X.24.103 Hst_X.X.24.44 Hst_X.X.24.74

GrpPinAS400: (Servidores AS/400 de Petroindustrial)

Hst_X.X.20.12 Hst_X.X.24.11 Hst_X.X.28.11

GrpSoteSrv: (Servidor del SOTE que se conecta al MEM)

Hst_X.X.10.126

GrpSriEst: (Servidores del SRI)

Hst_X.X.7.8 Hst_X.X.7.10

Servicios:

Se crearon los siguientes servicios adicionales a los predefinidos por el producto necesarios para la definición de las políticas de seguridad.

HtttpXX	puerto: XX	para conexión con websphere.
HttpProxyout 2/2	puerto: XX	para conexión con Internet.
MEM Oracle	puerto: XX	conexión con el servidor Oracle del MEM
Notes	puerto: XX	conexión con el servidor de correo
SRI Oracle	puerto: XX	conexión con el servidor Oracle del SRI

Dentro de los servicios definidos como objetos en el producto Firewall Builder y utilizados para la definición de reglas están:

Udp domain	puerto: 53
http	puerto: 80
https	puerto: 443
ftp	puerto: 21
ftpdata	puerto de origen: 20
	puerto de destino: 1024 a 65535
ftpdatapassive	puerto: 20
telnet	puerto: 23
pop3	puerto: 110
smtp	puerto: 25
ICMP ping reply	
ICMP ping request	

Existe la opción de poder definir como objetos a rangos de tiempo dentro de los cuales se va a aplicar las reglas definidas, pero en este caso no se llegó a utilizar esta utilidad.

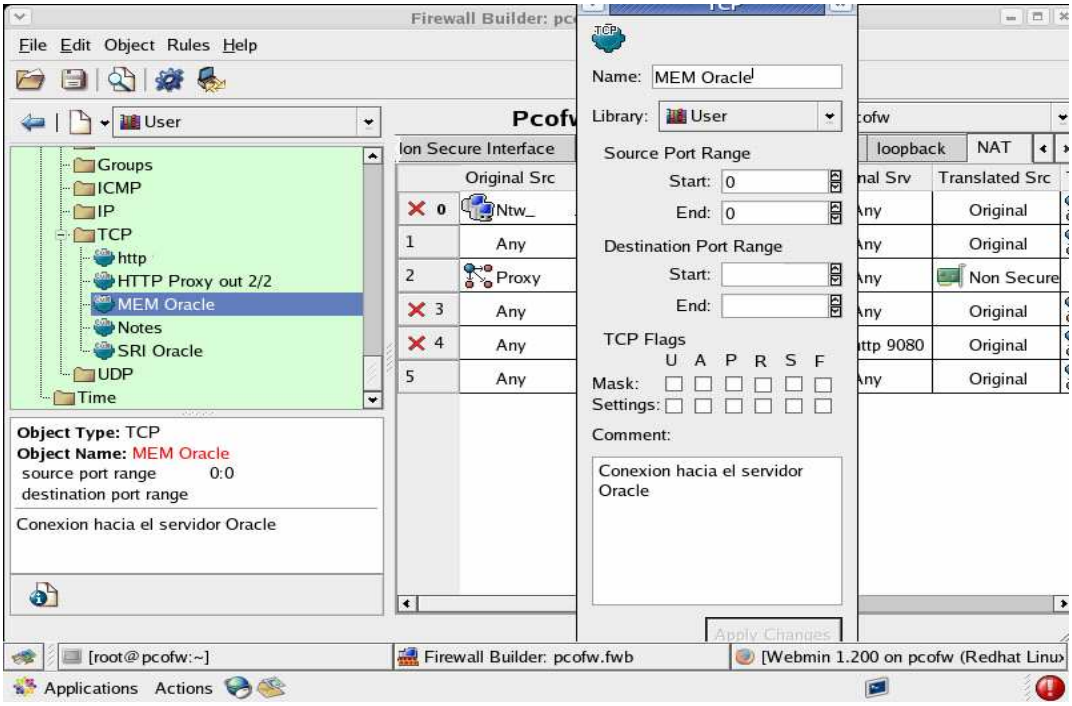


Figura 19. Definición de servicios en Firewall Builder

Políticas de Seguridad Implementadas:

El firewall Pcofw tiene implementadas cuatro interfases de red en cada una de las cuales se van definiendo las reglas necesarias, adicionalmente existen políticas para NAT (Traducción de direcciones de red) utilizadas para las conexiones desde fuera hacia servidores de la red interna.

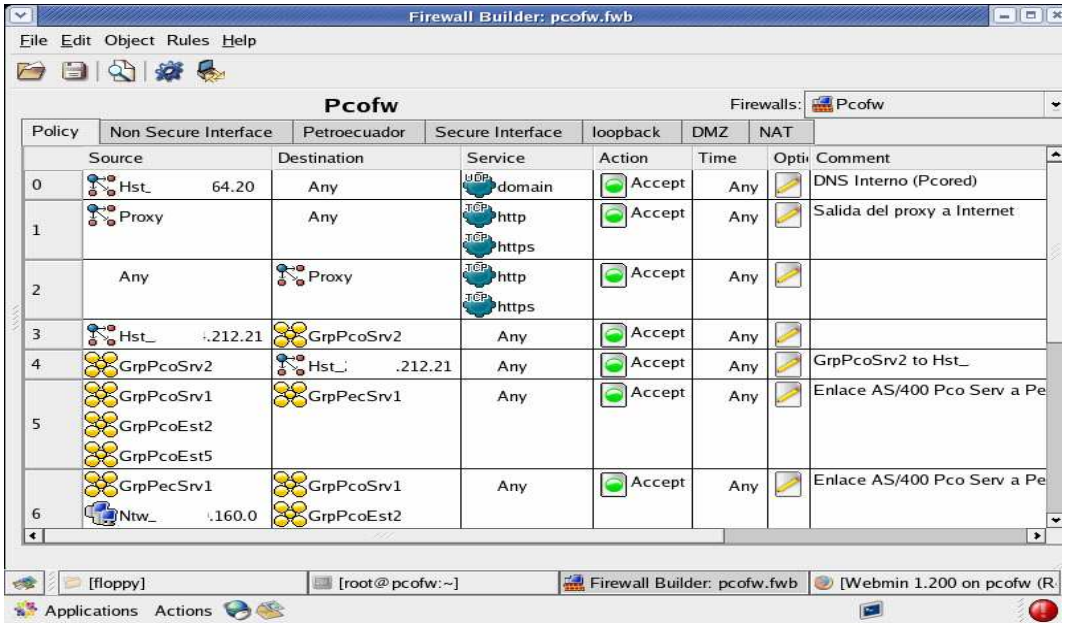


Figura 20. Definición de políticas de seguridad

Primero se definen las políticas generales y luego las reglas de cada una de las interfases mencionadas.

POLICY				
SOURCE	DESTINATION	SERVICE	ACTION	COMMENT
Hst_X.X.64.20	Any	UDP(domain)	Accept	DNS interno (Pcored)
Proxy	Any	TCP (http) TCP (https)	Accept	Salida del proxy a Internet
Any	Proxy	TCP (http) TCP (https)	Accept	
Hst_X.X.212.21	GrpPcoSrv2	Any	Accept	Conexión de los servidores de correo al servidor web externo
GrpPcoSrv2	Hst_X.X.212.21	Any	Accept	
GrpPcoSrv1 GrpPcoEst2 GrpPcoEst5	GrpPecSrv1	Any	Accept	Conexión servidores AS/400 *PCO–*PEC y equipos que usan aplicaciones de PEC.
GrpPecSrv1 Ntw_X.X.160.0	GrpPcoSrv1 GrpPcoEst2 GrpPcoEst5	Any	Accept	Conexión servidores AS/400 PEC-PCO, equipos de PEC que acceden a PCO
Hst_X.X.64.24	Hst_X.X.212.21	Any	Accept	Conexión Pcored4 a Pcoweb para actualización de la página web
Hst_X.X.212.21	Hst_X.X.64.24	Any	Accept	
Hst_X.X.64.59	Any	ftp ftpdata ftpdatpassive	Accept	Equipo utilizado para transferencia de archivos vía ftp
Any	Hst_X.X.64.59	ftp ftpdata ftpdatpassive	Accept	
Any	Any	Any	Deny	Regla para rechazar cualquier conexión que no especificada anteriormente

Tabla 13. Políticas de seguridad globales.

*PCO: Petrocomercial
*PEC: Petroecuador

NON SECURE INTERFACE				
SOURCE	DESTINATION	SERVICE	DIRECTION	COMMENT
Ntw_X.16.0.0	Hst_X.X.64.28	TCP (tel net)	Inbound (entrada)	Sesiones Telnet de *MEM a PCO.
Any	Hst_X.X.64.25	TCP (telnet)	Inbound	Acceso telnet al servidor Pco1
Non Secure Interface	Any	TCP (http) TCP (HTTP proxyout2/2)	Both (bidireccional)	Interfase no segura al mundo (Internet)
Ntw_X.16.0.0	GrpPinAS400	TCP (telnet)	Inbound	Sesiones Telnet de MEM a *PIN.
GrpMEMEst	GrpPcoEst6	Any	Both	Conexión de las estaciones de PCO a MEM

Tabla 14. Políticas de seguridad de la interfase no segura

*MEM: Ministerio de Energía y Minas
*PIN: Petroindustrial

En la Figura 21 se muestra la interfase gráfica de configuración de las políticas en la interfase no segura del firewall Pcofw.

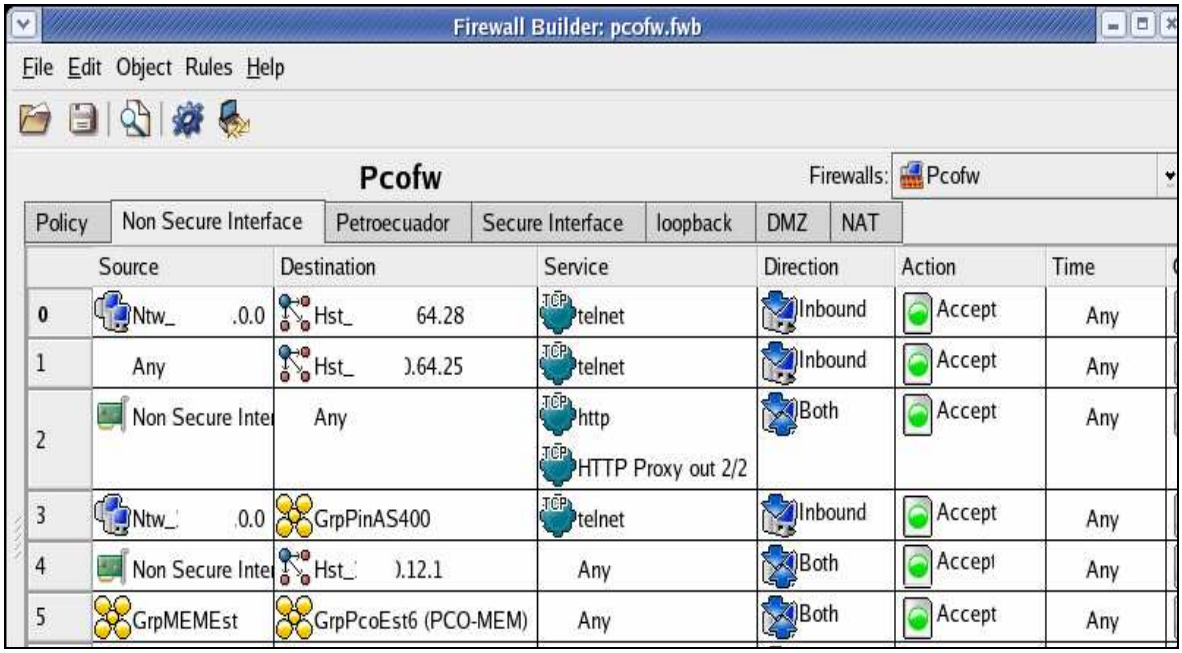


Figura 21. Políticas de seguridad en la interfase no segura

PETROECUADOR				
SOURCE	DESTINATION	SERVICE	DIRECTION	COMMENT
GrpPin Hst_X.X.71.6	GrpMEMSrv	TCP (pop3) TCP (Notes) TCP (smtp) ICMP ping reply, request	Both	Acceso a aplicaciones desde equipos PIN a MEM.
Hst_X.X.48.80	Hst_X.X.1.5	TCP (Notes)	Both	Acceso desde el equipo de la Presidencia Ejecutiva de PEC a MEM
GrpSoteSrv	GrpMEMEst	Any	Both	Conexión de SOTE-MEM
GrpPecUCont	GrpMEMSrv	TCP(Notes) TCP(smtp) TCP(MEM Oracle)	Both	Conexión equipos de Contratos de PEC a aplicaciones de MEM
GrpPin	GrpMEMSrv	TCP(MEM Oracle)	Both	Conexión equipos PIN a aplicaciones de MEM

Tabla 15. Políticas de seguridad de la interfase de Petroecuador

SECURE INTERFACE				
SOURCE	DESTINATION	SERVICE	DIRECTION	COMMENT
GrpPcoEst5 Hst_X.X.64.24	Rt_X.X.212.17	Any	Both	Administración del ruteador
GrpPcoEst5	HstX.X.10.57	Any	Both	Conexión de equipos PCO al Serv. Domino del SOTE
GrpPcoEst6 (Pco-MEM)	GrpMemEst	Any	Both	Conexión de equipos de PCO a MEM interfase segura
GrpPcoEst1G	GrpPecSrv1	Any	Both	Equipos de Guayaquil que acceden a servidores de PEC
GrpPcoEst5	Secure interface	Any	Both	Equipos para administración del firewall
GrpPcoEst4(Pco-Sri)	GrpSriEst	TCP(SRI Oracle)	Both	Conexión de equipos de PCO al SRI
Ntw_X.X.28.0 Ntw_X.X.33.0	GrpPecSrv1	TCP(http) TCP(https)	Both	Servicio de Internet PEC a PIN
GrpPcoEst1	Proxy	Any	Both	Conexión de equipos de PCO al proxy para salida a Internet

Tabla 16. Políticas de seguridad de la interfase segura

Al realizar la configuración del firewall se crea un dispositivo de red loopback el cual es una interfase virtual que representa al propio dispositivo independiente de la dirección IP asignada y cuyo valor es 127.0.0.1 por lo que se define la regla de permitir todo en el mismo equipo.

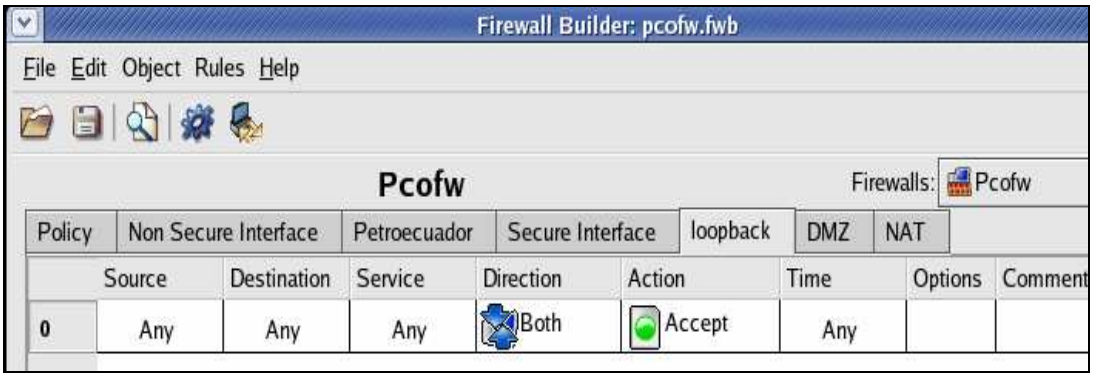


Figura 22. Política de la interfase loopback

DMZ				
SOURCE	DESTINATION	SERVICE	DIRECTION	COMMENT
Any	Hst_X.X.1.10	TCP(http) TCP(https)	Both	Conexión hacia el servidor web
Any	Hst_X.X.1.20	Any	Both	Conexión a equipo de servicios web

Tabla 17. Políticas de la interfase DMZ

En la definición de reglas en la zona desmilitarizada se puede añadir servidores de acceso público tales como: correo, servidor de nombres de dominio, ftp; lo cual puede ser implementado posteriormente con el fin de alojar servicios sin permitir el acceso no autorizado a la red privada de la empresa.

Debido a que actualmente el servidor Pcoweb y el equipo para pruebas de servicios web tienen direcciones públicas es necesario realizar la traducción de direcciones para tener acceso a estos.

NAT				
Original source	Original destiny	Translated src	Translated dst	Comment
Ntw_X.16.0.0	Hst_X.X.212.20	Original	Hst_X.X.64.28	NAT de MEM al servidor Pco8
Proxy	Any	NonSecureInt.	Original	NAT desde proxy a interfase no segura. Salida a Internet
Any	Hst_X.X.212.21	Original	Hst_X.X.1.10	NAT para acceso a servidor Pcoweb
Any	Hst_X.X.212.19	Original	Hst_X.X.1.20	NAT para acceso a equipo de servicios web de prueba.

Tabla 18. Políticas de NAT

Luego de crear todas las reglas es necesario compilar el firewall con el fin de validar la correcta aplicación de las reglas, proceso en el cual el programa verifica el orden jerárquico de las políticas y comprueba que ninguna regla contradiga a otra o exista duplicación en las mismas.

Finalmente para instalar el firewall creado, el programa pide que el usuario se autentique como root y las políticas entran a funcionar.

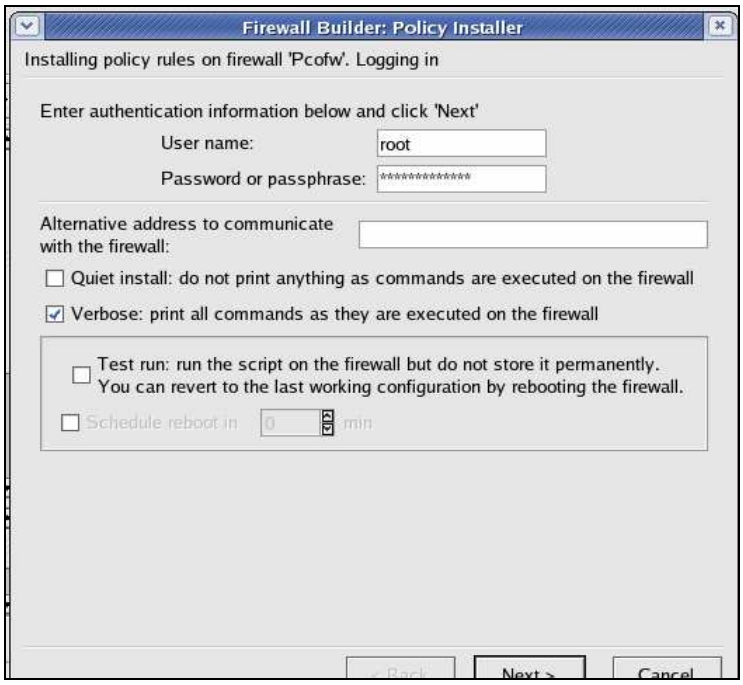


Figura 23. Instalación de políticas con autenticación de usuario

Como resultado de este proceso el programa crea un archivo Pcofw.fw en el cual se detalla la configuración de las reglas aplicada en el equipo y cuyo contenido se puede observar en el Anexo 2.

Para evitar el abrir el programa y realizar la compilación e instalación cada vez que se reinicie el equipo se configuró el arranque automático del firewall editando el archivo: /etc/rc.d/rc.local; y añadiendo la siguiente línea de comando:

sh /root/firewall/Pcofw.fw

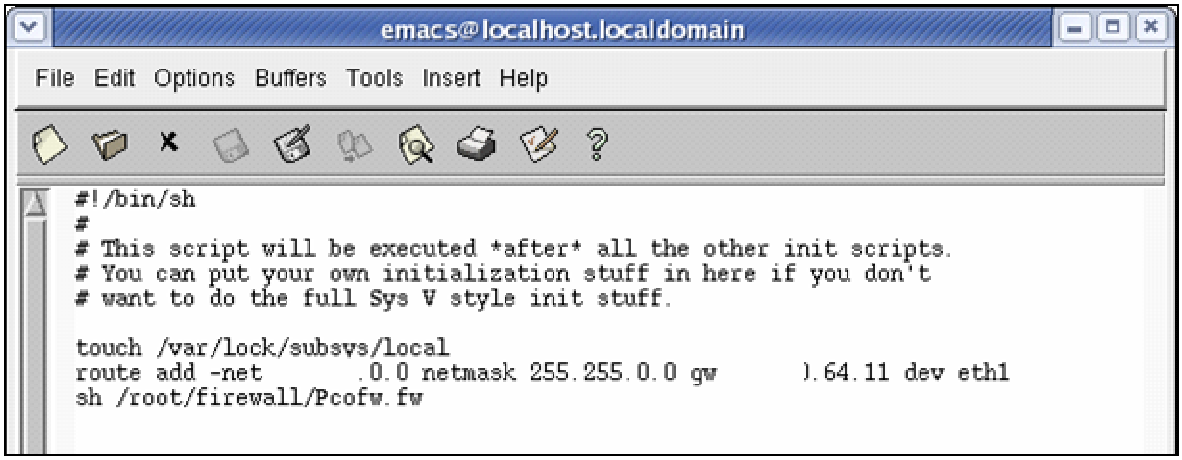


Figura 24. Arranque automático de las políticas del firewall

En el sistema operativo se definió las rutas por defecto de las interfases de red que se muestran a continuación; para desplegar estas rutas se usa el comando route –n

Destino	Gateway	Máscara	Interfase
X.X.10. 0	X.X.230.11	255.255.255.0	eth2 Petroecuador
X.X.0.0	X.X.230.11	255.255.0.0	eth2 Petroecuador
X.X.0.0	X.X.230.11	255.255.0.0	eth2 Petroecuador
X.X.0.0	X.X.64.11	255.255.0.0	eth1 Petrocomercial
0.0.0.0	X.X.212.17	0.0.0.0	eth0 (ruta por defecto)

Para añadir o eliminar rutas se usa el comando:
route add –net X.X.0.0 gw X.X.64.11 netmask 255.255.0.0 dev eth1
route del –net X.X.0.0 gw X.X.64.11 netmask 255.255.0.0 dev eth1

Servidor Proxy

Con el cambio de firewall fue necesaria la creación de un servidor proxy, para lo cual se utilizó un equipo Compaq Proliant ML350 con las mismas características que el anterior, de igual forma se instaló el sistema operativo Linux CentOS 4.0 y a este equipo se lo configuró de la siguiente manera:

Nombre del equipo: pcoproxy
Dirección IP: X.X.64.7
Máscara: 255.255.248.0
Gateway: X.X.64.11

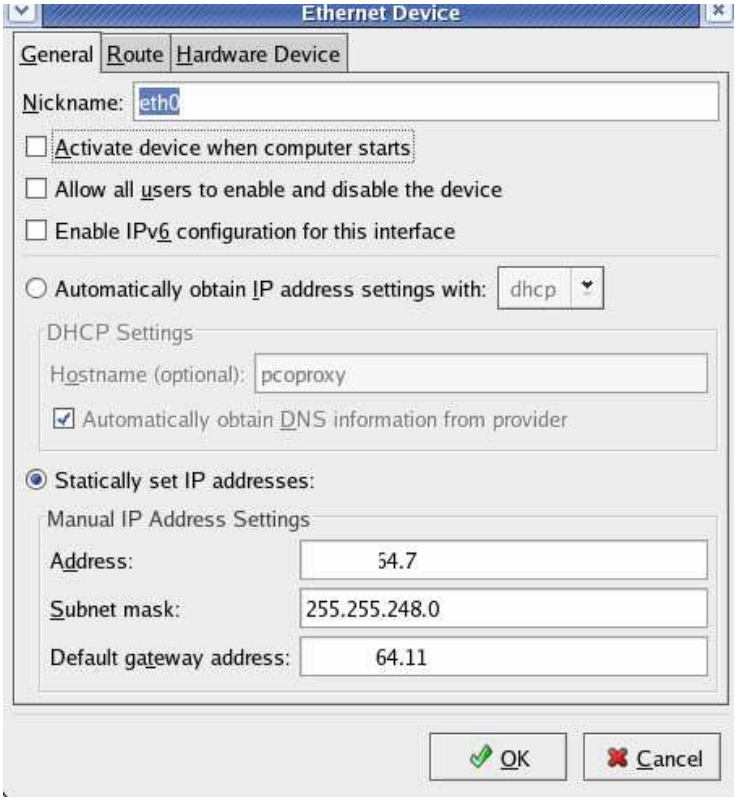


Figura 25. Configuración del servidor proxy

El programa que se utilizó para este propósito es Squid el cual es un software libre y puede hacer proxy y caché con los protocolos HTTP, FTP, Gopher[29] y WAIS[30], pero no funciona para servicios como: SMTP, POP3[31], Telnet, SSH.

Squid utiliza el fichero de configuración localizado en /etc/squid/squid.conf; para lo cual con un editor de texto se puede configurar el archivo de la siguiente forma:

Por defecto squid usa el puerto 3128 para atender peticiones pero en este caso se usó el puerto 8080 y adicionalmente se habilitó el puerto 8082.

#Default:
http_port 8080
http_port 8082

[29] Servicio de Internet consistente en el acceso a la información a través de menús. Antiguo sistema para la localización de información en Internet. (http://es.wikipedia.org/wiki/Gopher, Enero 2006)
[30] Un método para buscar y recuperar información de bases de datos disponibles en Internet, hoy en día en desuso.
[31] Es un esquema de protocolo de Internet utilizado para que clientes locales recuperen su correo electrónico de un servidor remoto a través de Internet. La mayoría de las cuentas de correo electrónico son accedidas a través de POP3. (http://www.cpsr-peru.org/seguridad/ongs/parte4, Enero 2006)

En el parámetro cache_mem se establece la cantidad de memoria para: objetos en tránsito, objetos hot y objetos negativamente almacenados en caché, estos datos se almacenan en bloques de 4 Kb, el cache_mem especifica un límite máximo en el tamaño total de bloques acomodados donde los objetos en tránsito tienen mayor prioridad y los otros pueden usar la memoria hasta que esta no sea requerida; por defecto este valor se establece en 8 MB pero en este caso se ha establecido un valor de 150 Mb ya que el equipo tiene disponibilidad de 1,2 GB en memoria RAM.

#Default:
#cache_mem 8MB
cache_mem 150MB

La definición del valor de cahe_dir depende del tamaño que se desee almacenar en disco duro de las páginas accedidas por los usuarios al Internet, por defecto squid usa 100 MB aunque este valor se puede incrementar con la finalidad de que se almacenen más objetos y reducir el uso de ancho de anda.

#Default:
#cache_dir ufs /var/spool/squid 100 16 256
cache_dir ufs /var/spool/squid 500 16 256

En este caso se configuró en 500 MB, y los números 16 y 256 significan que el directorio del caché contendrá 16 subdirectorios con 256 niveles cada uno; no se debe exceder el espacio real disponible en disco ya que en este caso Squid se bloqueará.

En las listas de control de acceso se especifica la red que va a tener acceso al Squid de la siguiente forma: acl (nombre de la lista) src (ip de la red y máscara)

acl Mi.Red.Local src 172.20.0.0/16

Para las reglas de control de acceso no se editó ninguna salvo la siguiente que permite el acceso http al propio equipo y a la red local denegando cualquier otro acceso.

http_access allow localhost
http_access allow MI.Red.Local
http_access deny all

De esta forma se finaliza la configuración del Proxy.
De igual manera se edita el archivo etc/rc.d/rc.local; añadiendo la siguiente línea de comando: sh /etc/squid/squid.conf; para que squid arranque junto con el sistema operativo.

3.2.- BACKUP DE COMUNICACIONES A DESARROLLARSE.

Debido a que en su configuración básica los ruteadotres Vanguard 6455 y 6435 utilizados por Petrocomercial no integran las tarjetas de opción para compresión y cifrado basada en hardware necesaria para ofrecer el soporte de VPN y en razón de que la mayoría de equipos en la empresa funcionan con sistemas operativos Windows 2000 o XP se decidió montar conexiones VPN para definir el diseño del backup de comunicaciones emergente con la utilidad propia de Windows, la cual está disponible y es muy poco explotada. Anteriormente Microsoft no proporcionaba la capacidad necesaria para conectar dos equipos sobre una VPN por lo que se requería agregar el protocolo de túnel punto a punto (PPTP) en Windows NT 4.0; actualmente Windows 2000 y XP habilitan una conexión VPN con el protocolo de Internet (IP) instalado; siendo la siguiente la estructura del enlace

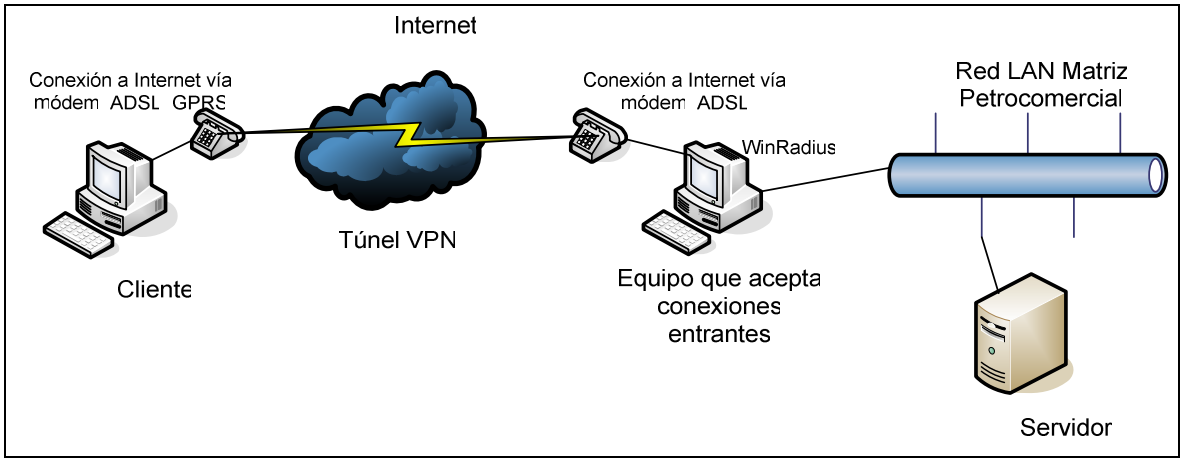


Figura 26. Esquema de conexión del backup de comunicaciones

En el caso de definir conexiones entrantes en un servidor de acceso remoto es necesario habilitar el puerto a través del cual los clientes se van a conectar, en este caso puertos para conexiones VPN; si el servidor es miembro de un dominio se usa la herramienta: enrutamiento y acceso remoto para configurar conexiones entrantes así como las directivas de acceso, autenticación y opciones de cifrado.

Los equipos que van a establecer un túnel por una red privada virtual deben estar conectados a Internet ya sea utilizando un módem, un equipo de vínculo permanente como una línea digital asimétrica de abonado (ADSL), o tecnología digital de telefonía móvil (GPRS); y en el extremo donde se va a aceptar las conexiones entrantes de los clientes remotos podría instalarse WinRadius el cual es un estándar de autenticación y autorización de acceso usado para conexiones inalámbricas.

Los sistemas operativos Windows 2000 y XP incluyen soporte para redes privadas virtuales utilizando PTPP (Protocolo de túnel punto a punto), Layer 2 Tunneling Protocol e IPSec.

El protocolo IPSec proporciona servicios de protección de integridad, autenticación y opcionalmente protección contra reproducción y privacidad para el tráfico IP, siendo los paquetes IPSec de dos tipos: Protocolo IP 50 denominado formato de carga de seguridad de encapsulación (ESP) que ofrece privacidad, autenticidad e integridad y el Protocolo IP 51 denominado formato de encabezado de autenticación (AH) que solo proporciona integridad y autenticidad para paquetes pero no ofrece privacidad.

L2TP es un protocolo que encapsula las tramas del protocolo punto a punto (PPP, Point-to-Point Protocol) que van a enviarse a través de redes IP. Cuando está configurado para utilizar IP como su transporte, L2TP se puede utilizar como protocolo de túnel VPN en Internet.

PPTP es un protocolo que se diseñó para proporcionar comunicaciones autenticadas y cifradas, (sin necesitar una infraestructura de clave pública) utilizando una identificación de usuario y contraseña. El objetivo de su diseño fue la simplicidad, compatibilidad multiprotocolo y capacidad de cruzar una amplia

gama de redes IP. El protocolo de túnel punto a punto utiliza una conexión TCP para el mantenimiento del túnel y tramas PPP encapsuladas para los datos del túnel. El uso de PPP proporciona la capacidad de negociar los servicios de autenticación, cifrado y asignación de dirección IP.

En el Anexo 3 se explica más a detalle los protocolos IPSec y L2TP.

3.3.- IMPLEMENTACION DE PROTOTIPOS PARA LOS BACKUP DE COMUNICACIONES

Para realizar la conexión VPN entre dos equipos se utilizó el sistema operativo Windows XP, para lo cual se habilita la conexión de entrada en el computador que se encuentra formando parte de la red LAN en la matriz de Petrocomercial siguiendo los siguientes pasos:

– En conexiones de red se realiza una nueva conexión para iniciar el asistente; en el cuadro de diálogo tipo de conexiones de red se escoge la opción configurar una conexión avanzada.

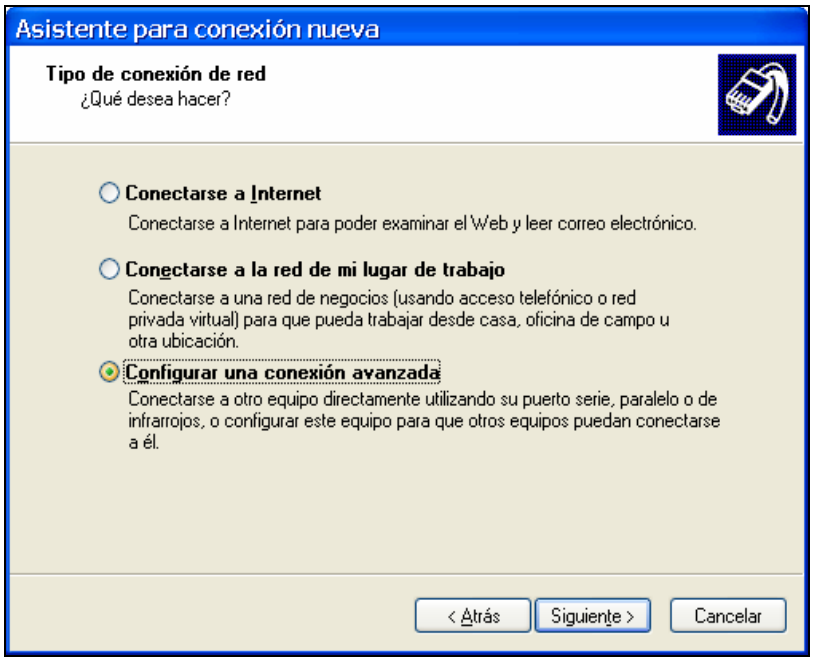


Figura 27. Asistente para conexión nueva

- A continuación se selecciona aceptar conexiones entrantes y en dispositivos de conexiones entrantes no se selecciona ninguno; en el siguiente cuadro de diálogo de conexión de red privada virtual entrante se secciona la opción permitir conexiones privadas virtuales con lo cual el sistema modifica la configuración del firewall de Windows para permitir que el equipo envíe y reciba paquetes de VPN.
- Dentro de permisos de usuarios se selecciona o agrega todos los usuarios para los que se desee habilitar el acceso y estas cuentas deben existir en ambos equipos implicados en el establecimiento de la conexión VPN. Para este caso se creó dos usuarios: jyepez y pyepez con sus respectivas contraseñas.

Figura 28. Permisos para usuarios de la conexión VPN

- Posteriormente en la opción software de red debe estar activado los componentes de red siguientes: Protocolo Internet (TCP/IP), compartir archivos e impresoras para redes Microsoft y cliente para redes Microsoft. Estos dos últimos componentes permiten que otros equipos tengan acceso a los recursos de la red.

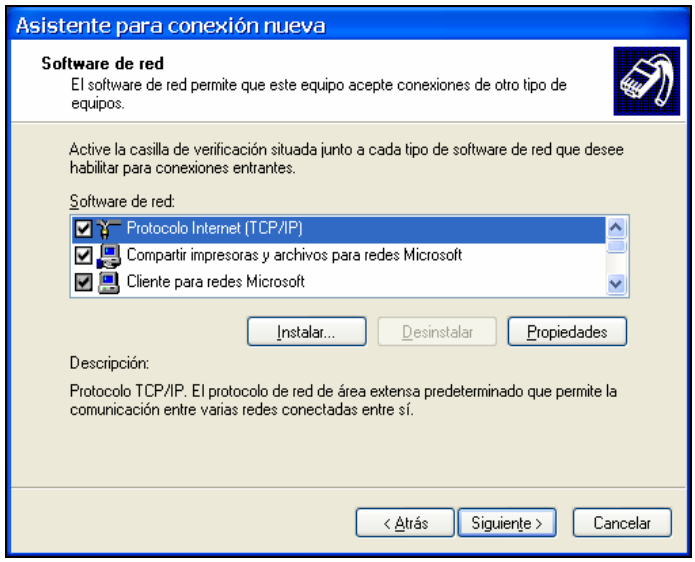


Figura 29. Software de red instalado para habilitar recursos compartidos

– Finalmente queda habilitado la opción de conexiones entrantes en el equipo para poder establecer una conexión VPN con el cliente.

A continuación en el cliente se configura se configura la conexión VPN de la siguiente forma:

– Se realiza una nueva conexión de red y se escoge la opción conectarse a la red de mi lugar de trabajo. En el cuadro de diálogo conexión de red se escoge la opción conexión de red privada virtual a través de Internet.

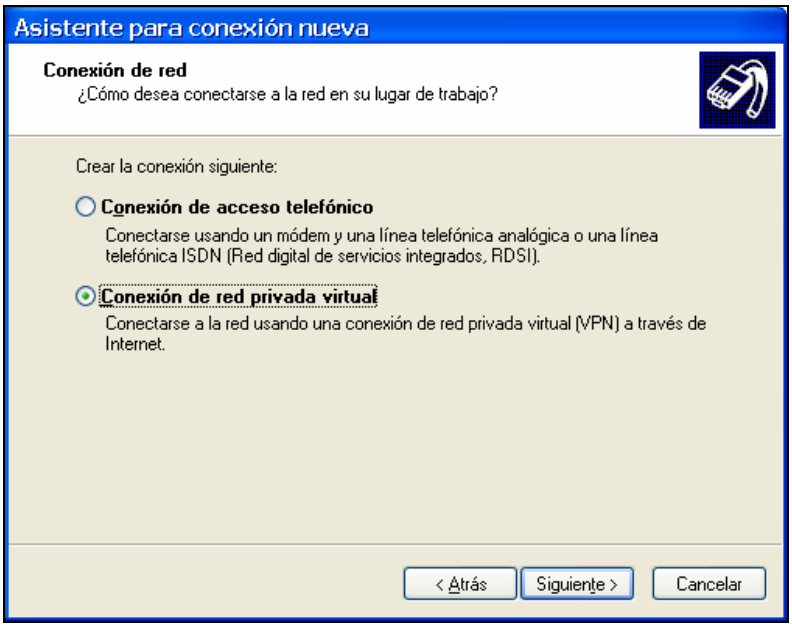


Figura 30. Conexión nueva para cliente VPN

- Seguidamente se especifica un nombre para la conexión que en este caso es VPN PCO. En el cuadro de diálogo red pública existe la opción de marcar automáticamente un proveedor de servicios de Internet; a continuación se selecciona el servidor VPN que es la dirección pública del equipo al cual se va a realizar la conexión, en el caso de VPN PCO es la dirección 64.76.63.214 que es el equipo que se encuentra habilitado las conexiones entrantes y forma parte de la red LAN de la matriz de Petrocomercial.
-

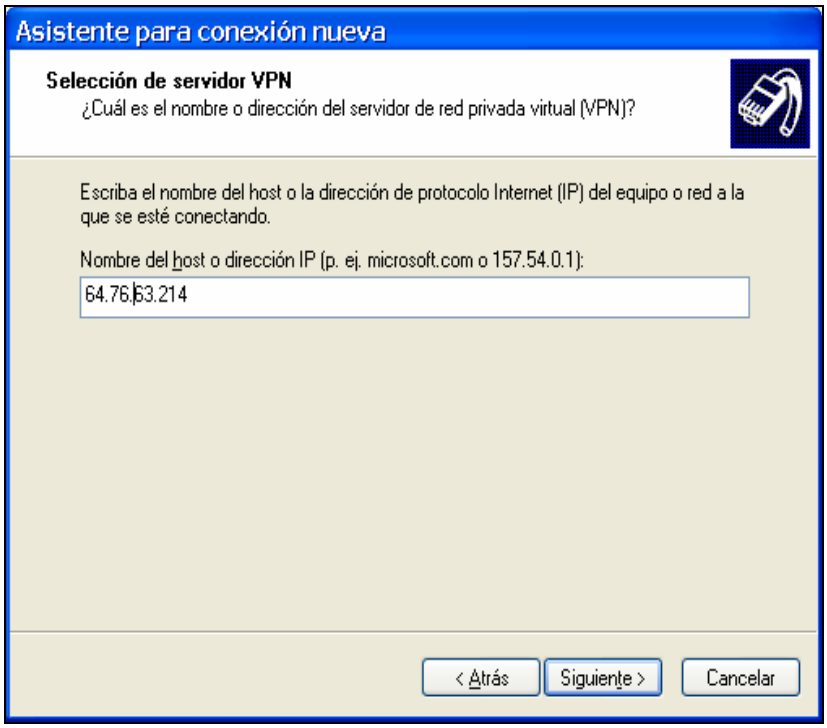


Figura 31. Selección del servidor VPN en el cliente

- En cuadro de disponibilidad de conexión se escoge la opción de todos los usuarios para que tengan acceso a esta conexión; finalmente se completa el asistente para la conexión de red.
- Para realizar la conexión desde el cliente es necesario ingresar la clave y contraseña para la conexión VPN PCO.

Figura 32. Autenticación para la conexión VPN PCO

Realizada la conexión, el servidor asigna una dirección IP al cliente permitiéndole a este acceder a la red e indicando las propiedades a través de las cuales se define la conexión VPN.

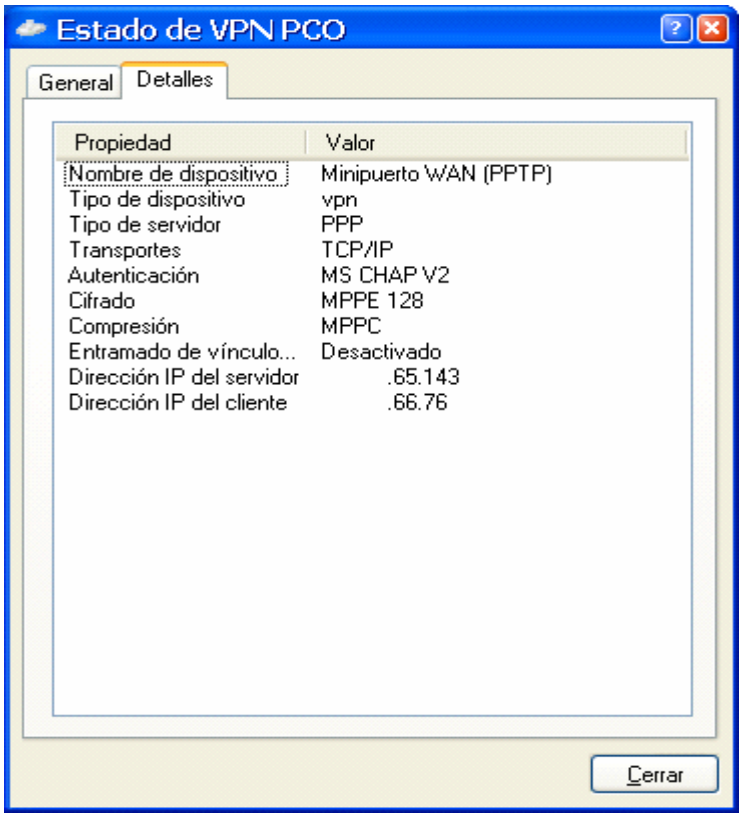


Figura 33. Estado de la conexión VPN PCO

En el cliente se puede observar la dirección IP asignada por el servidor así como la dirección del DNS de la red en el adaptador PPP VPN PCO, siendo este proceso transparente para el usuario con lo que el cliente puede trabajar como si estuviese conectado físicamente a la red y usar los recursos, servicios y aplicaciones en el caso de que el enlace principal no este operativo.

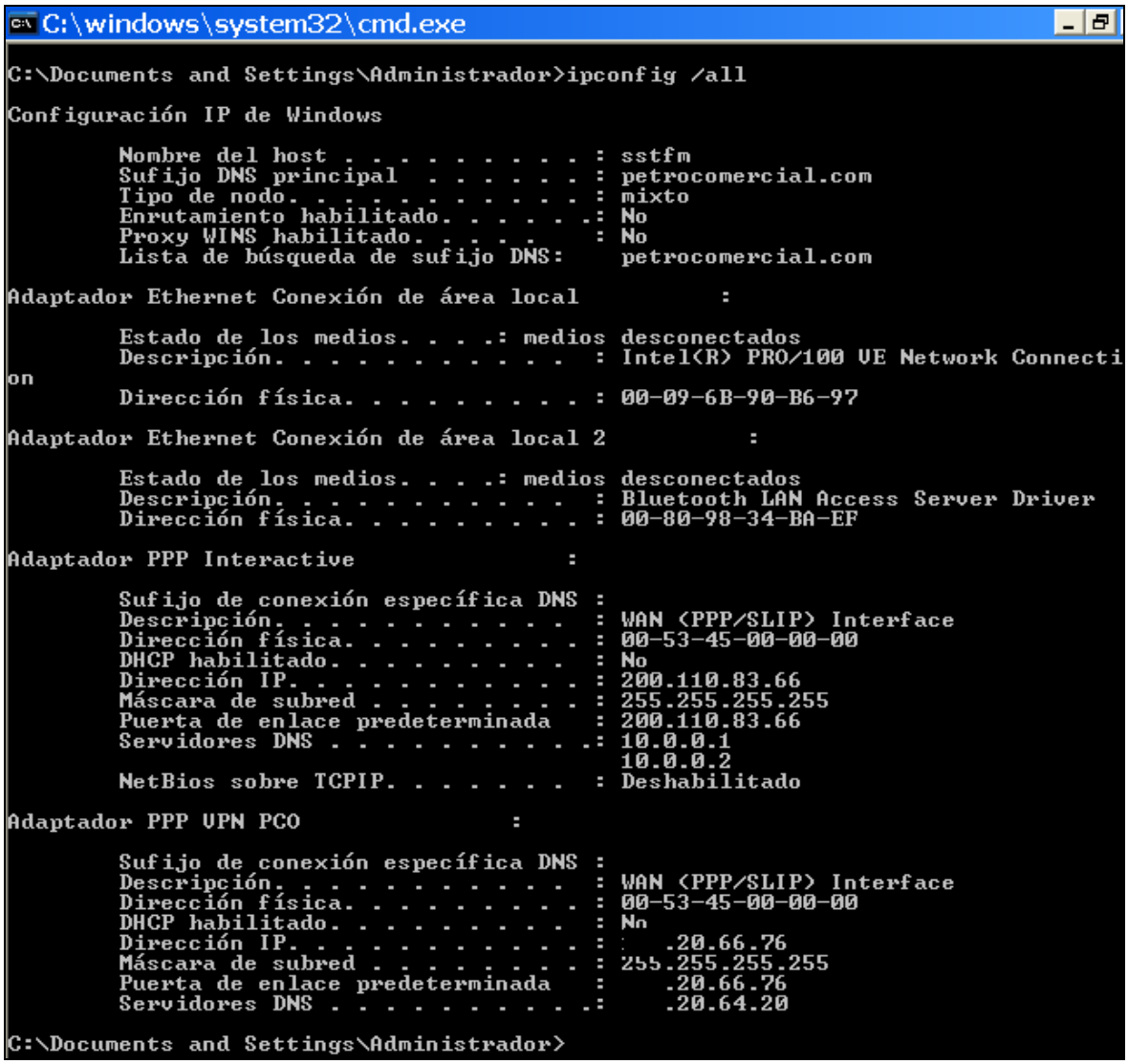


Figura 34. Configuración IP del cliente

De igual forma en el servidor se puede observar el estado de las conexiones con el comando netstat –n donde se observa la comunicación establecida con el cliente que posee la dirección pública 200.110.83.66 conectado hacia el equipo servidor a través del puerto 172

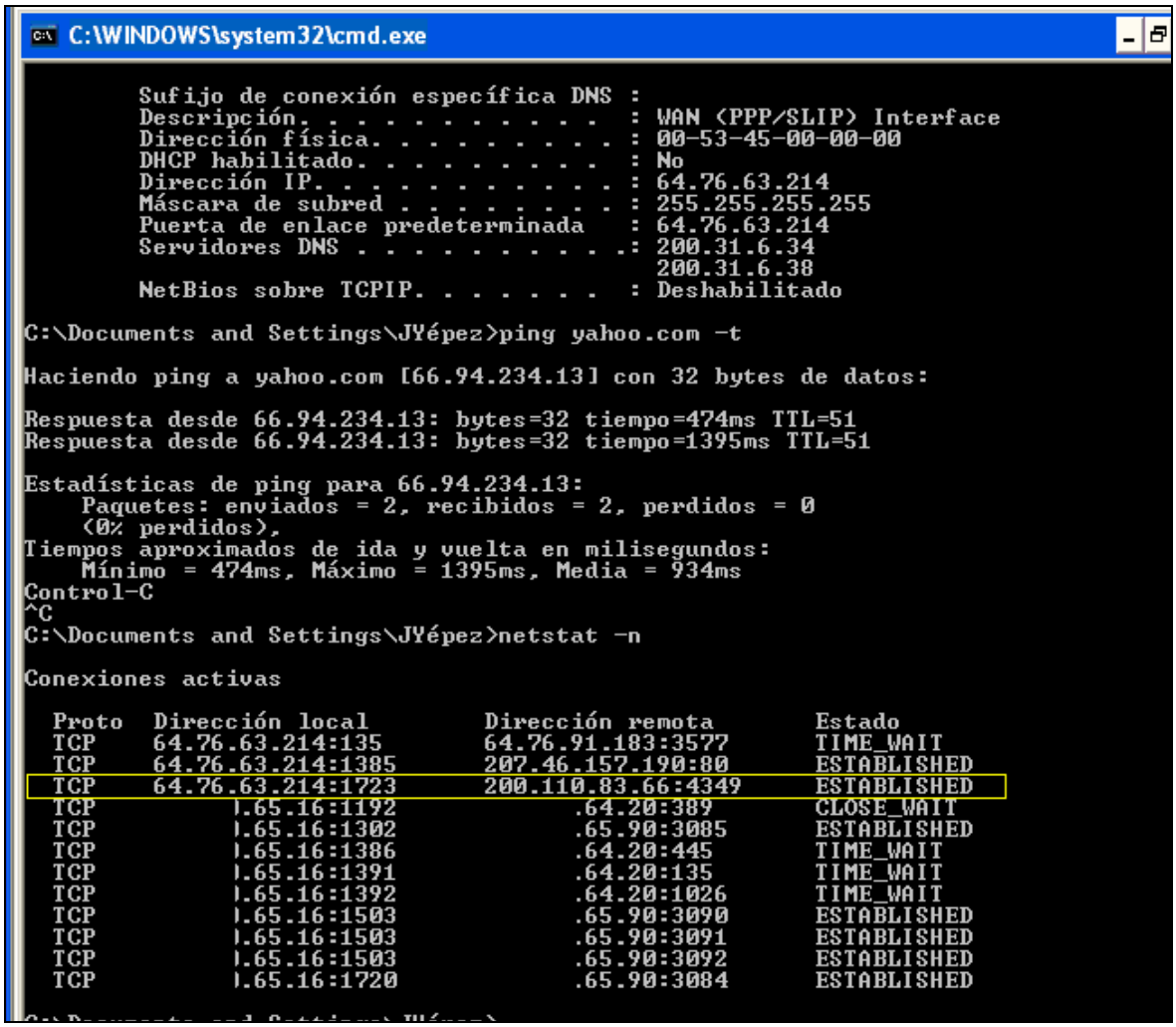


Figura 35. Estado de las conexiones en el servidor VPN

En el caso de un servidor VPN con el sistema operativo Windows 2000 Server o 2003 Server que forma parte de un dominio se habilita las conexiones entrantes con la opción de enrutamiento y acceso remoto dentro del menú de herramientas administrativas.

Sobre el nombre del servidor se selecciona configurar y habilitar el enrutamiento y acceso remoto, a continuación se completa el asistente y se define las directivas de acceso, autenticación y opciones de cifrado.

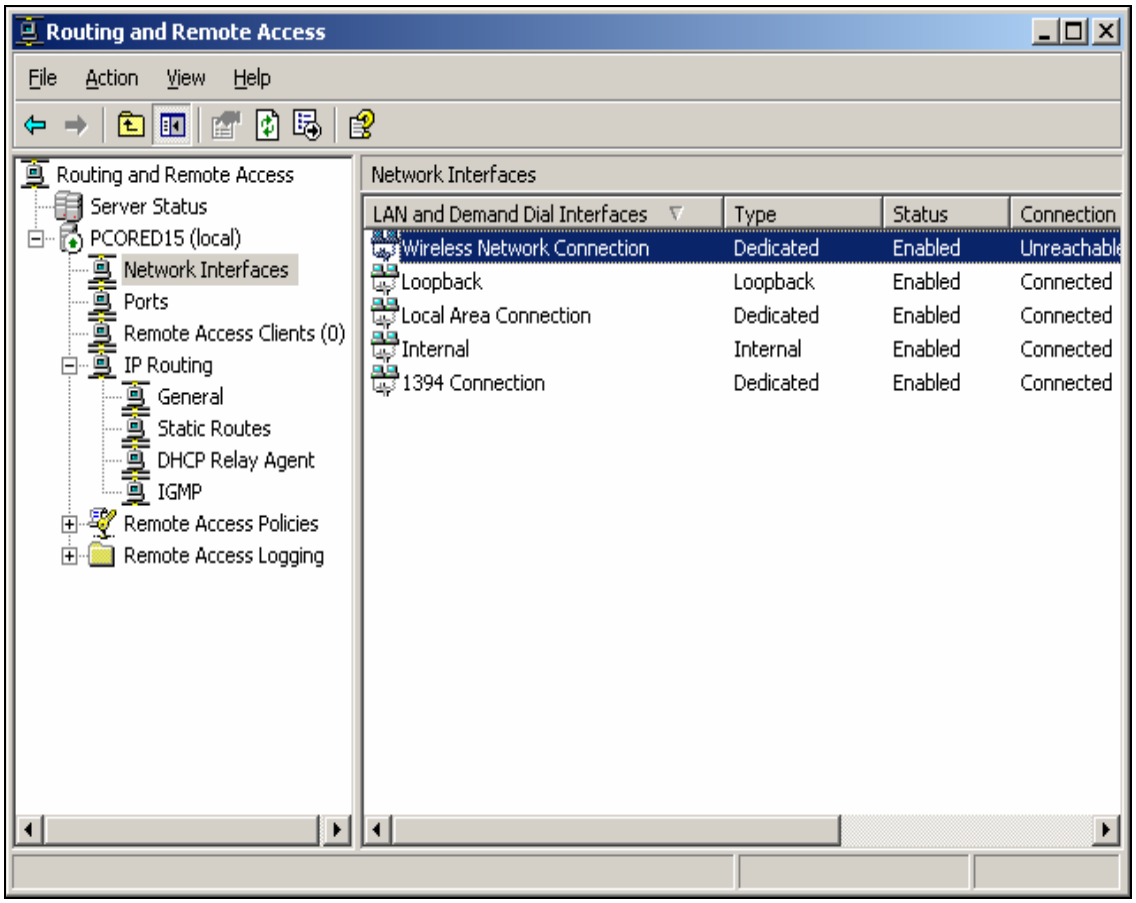


Figura 36. Enrutamiento y acceso remoto en Windows 2003 Server

La primera vez que se inicia un servidor VPN con Windows Server crea automáticamente 128 puertos PPTP y 128 puertos L2TP. El número de puertos virtuales disponibles para un servidor VPN no está limitado por el hardware físico de la máquina y puede ser aumentado o reducido al número apropiado para el ancho de banda disponible en el servidor.

Para habilitar los puertos VPN se selecciona un dispositivo Minipuerto WAN (PPTP) y Minipuerto WAN (L2TP) en las propiedades de puertos.

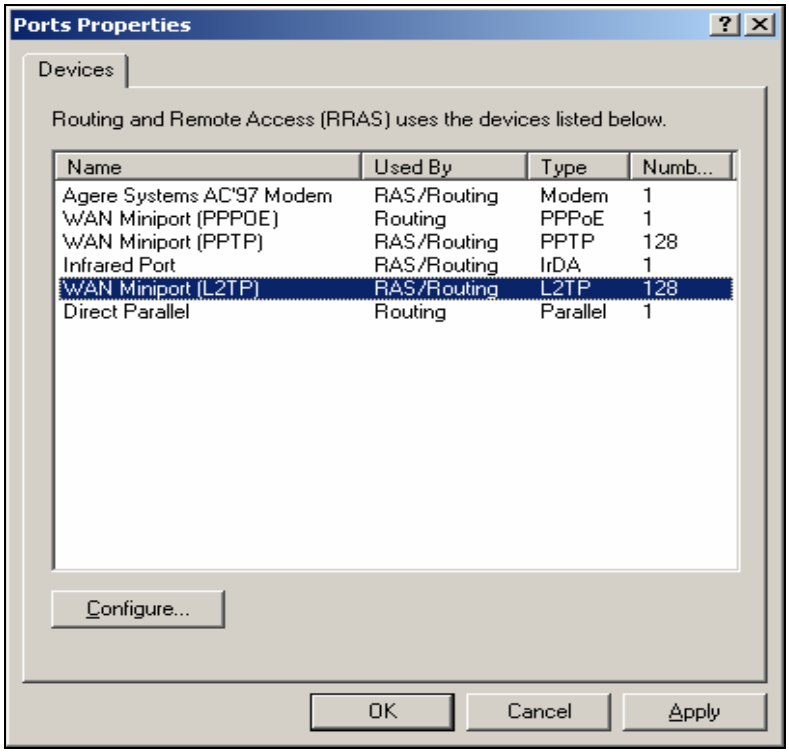


Figura 37. Propiedades de puertos VPN

Finalmente en la opción configurar se activa la casilla de verificación: Conexiones de acceso remoto (solo entrada).

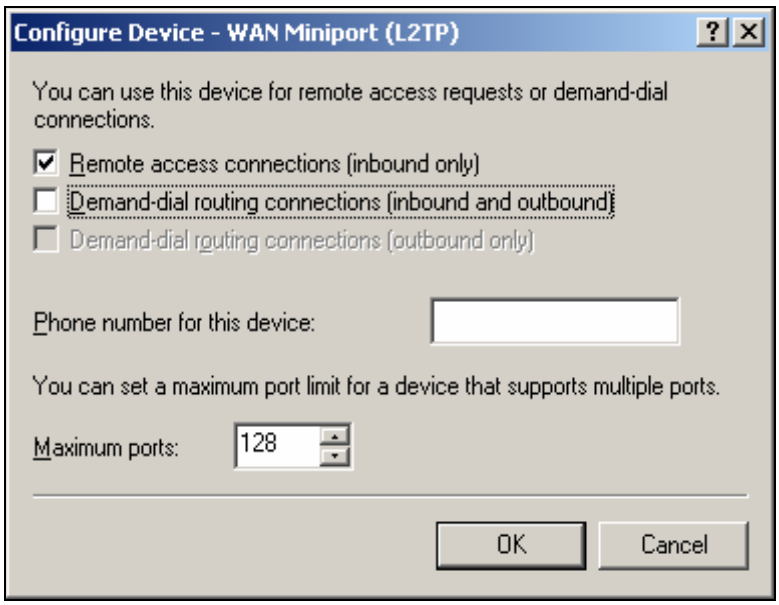


Figura 38. Conexiones de acceso remoto

Para la configuración de los clientes remotos se realiza el mismo procedimiento que en el caso anterior.

OpenVPN

Como segunda opción para realizar conexiones a través de la implementación de redes privadas virtuales es la utilización de OpenVPN que es una solución de conectividad basada en software: SSL (Secure Sockets Layer). Esta aplicación como ya se mencionó anteriormente usa todas las características de encriptación, autenticación y certificación de la librería OpenSSL para tunelizar en forma segura redes IP sobre un solo puerto TCP/UDP. De esta forma dos equipos se pueden enlazar de manera que parezca que están conectados a la misma red de área local, utilizando para la autenticación un sistema criptográfico de clave pública con lo cual se asegura que solo usuarios autorizados accedan a la red virtual.

Este software de código abierto y trabaja bajo los sistemas operativos Linux, Windows 2000/XP, Mac OS X, y Solaris.
A continuación se detalla una descripción breve de los pasos para poder conseguir que una VPN funcione bajo Linux:

- Se instala el paquete openvpn:
  #apt-get install openvpn.
- Se instala el paquete lzop para comprimir los datos:
  #apt –get install liblzol lzop.
- Se genera la clave para la VPN:
  # openvpn –genkey --secret clave.key
- Esta clave la ponemos en:
  /etc/openvpn/
- Se traslada este archivo al equipo2 para lo cual se puede usar el programa scp con el fin de encriptar la información enviada:
  # scp /etc/openvpn/clave.key
  root_at_ip_segundo_nodo:/etc/openvpn/clave_dot_key
- Para evitar que genere un error al copiar se debe crear la ubicación:
  /etc/openvpn y luego ejecutar el comando. El archivo clave.key viene a ser la contraseña para la VPN por lo que debe ser enviado por un medio seguro.
- Se carga el módulo tun (Universal TUN/TAP device driver support)
  #modprobe tun

- Se comprueba que exista el directorio: /dev/net/tun, en el caso de no existir, se procede a crearlo:
  # mknod /dev/net/tun c 10 200
- A continuación se crea el archivo de configuración para la VPN que debe ser de la siguiente forma:

```
local [ip local]
remote [ip remota]
dev tun0
port 5000 [puerto elegido, se lo puede cambiar]
comp-lzo
user nobody
ping 15
ifconfig [ip del tunel local] [ip del tunel remoto]
secret /etc/openvpn/clave.ke
```

En la ip local se coloca la dirección de la interfaz que tiene salida a Internet y en ip remota la dirección a la cual nos queremos conectar. En la sección ip del tunel local se crea las propias IP (privadas) para la VPN, en local se define la ip del equipo 1, y en remota la del equipo 2.

Es decir si por ejemplo el equipo 1 tiene la siguiente dirección en eth0: 192.168.0.5 se llama equipo1.ath.cx por ejemplo, en el equipo 2 se tiene la dirección: 192.168.0.10 y el dominio es equipo2.ath.cx.

Las direcciones privadas para la VPN pueden ser, para el equipo 1: 10.0.0.1 y para el equipo 2: 10.0.0.2, tendiendo esta información se crea los archivos de configuración.

En el equipo 1 se define lo siguiente en el archivo /etc/openvpn/tunel.conf

```
local 192.168.0.5
remote equipo2.ath.cx
dev tun0
port 5000
```

```
comp-lzo
user nobody
ping 15
ifconfig 10.0.0.1 10.0.0.2
secret /etc/openvpn/clave.ke
```

En el equipo 2 se define lo siguiente en el archivo /etc/openvpn/tunel.conf

```
local 192.168.0.10
remote equipo1.ath.cx
dev tun0
port 5000
comp-lzo
user nobody
ping 15
ifconfig 10.0.0.2 10.0.0.1
secret /etc/openvpn/clave.ke
```

- Luego se ejecuta el siguiente comando en los 2 equipos:

```
#openvpn  --verb 5 –config /etc/openvpn/tunel.conf
```

El parámetro --verb permite ver la información que despliega el programa openvpn; si muestra un mensaje:
Peer Connectoin Initiated with [ip remota]:[puerto]
Significa que está funcionando. Se debe crear el archivo en rc.d o init.d llamado openvpn para agregar al proceso de arranque con lo que la conexión VPN estará completa y funcionando.

CAPÍTULO

IV

CAPÍTULO IV

CONCLUSIONES Y RECOMEDACIONES

Una vez finalizado el desarrollo de los diferentes temas de todos los capítulos contemplados en este proyecto, se tiene las siguientes conclusiones y recomendaciones**.**

CONCLUSIONES:

- El uso de sistemas operativos así como productos de código abierto y software libre ayudan a realizar implementaciones en este caso de seguridad optimizando costos a la empresa, tomando en cuenta que de la correcta instalación y configuración de los mismos dependerá su adecuado funcionamiento. Por otra parte también es importante la permanentemente actualización de versiones, parches y revisión de vulnerabilidades ya que las amenazas de seguridad se incrementan constantemente.

- En algunos casos no fue posible llegar a un mayor grado de precisión en la definición de las políticas del firewall ya que los constantes cambios tanto de usuarios como de equipos en la empresa y en las otras entidades con las cuales se mantiene comunicación no lo han permitido.

- El uso de Linux como sistema operativo, así como la herramienta Firewall Builder, ayudó a facilitar la administración de las reglas y permitió mejorar el nivel de seguridad ya que se definió una zona desmilitarizada en la cual la empresa podrá alojar sus servicios de acceso público protegiendo la red interna; sí como también se independizó los servidores de firewall y proxy dando la opción de implementar la utilización de filtrado de contenido y acelerando el acceso a Internet por parte de los usuarios de la red.

- En lo referente a las VPN, este tipo de conexiones representan una buena alternativa de solución para la empresa debido a que a más de servir de respaldo en las comunicaciones, puede reemplazar a los enlaces contratados garantizando seguridad, confidencialidad, e integridad de los datos y disminuyendo los costos que Petrocomercial destina para mantener los enlaces con los sitios remotos.

- Una de las desventajas de utilizar DSL o cable módem para mantener una conexión siempre activa, como sería el caso de un servidor para conexiones VPN, es que este equipo sería vulnerable a ataques debido a que no es un objetivo móvil, ya que permanece con una conexión de red estática y siempre disponible para recibir peticiones de conexión.

RECOMENDACIONES:

- Actualmente para los servidores y equipos de comunicación que han cumplido su ciclo de funcionamiento se debe considerar su renovación tecnológica ya que corren el riesgo de sufrir algún desperfecto sin tener al momento una posibilidad de reemplazo.

- En la zona desmilitarizada se debe colocar los servicios de Web, Correo, DNS y FTP, para lo cual es necesario independizar estos servidores ya que estos se encuentran funcionando con aplicaciones y servicios de autenticación de la red interna.

- Se recomienda a futuro implementar una solución de seguridad integral la cual ofrezca los servicios de: firewall antivirus, anti-spam, detección de intrusos, filtrado de contenido; pudiendo utilizarse la implementación de Firewall Builder detrás del primer cortafuegos y delimitando el acceso a la zona desmilitarizada.

- Con el propósito de solventar una solución VPN global, es necesario dedicar un servidor o adquirir un dispositivo apropiado para realizar conexiones privadas virtuales con sitios remotos para lo cual se debe contratar una conexión a Internet con la suficiente velocidad para reemplazar incluso a los enlaces contratados a empresas externas sin denigrar la velocidad del enlace.

- No es aconsejable el uso del sistema operativo con perfiles de súper usuarios (root) ya que estos tienen el permiso para modificar o instalar cualquier configuración o aplicación poniendo en riesgo el funcionamiento de los equipos.

- Se podría utilizar el programa de Linux, Webmin para administrar a través del navegador de Internet y de forma remota la configuración de los servidores tanto del firewall como del proxy, definiendo solamente ciertos equipos y usuarios para este propósito.

REFERENCIAS BIBLIOGRAFICAS

a) GARCIA Jesús, Redes para Procesos Distribuidos, Tercera Edición. Editorial Alfa-Omega, 2001.

b) JAMES Senn, Análisis y Diseño de Sistemas de Información, Segunda Edición, Mc Graw Hill, 1992.

c) TANENBAU, Redes de Computadores, Tercera Edición, Prentice Hall, 1997.

d) http://www.securityfocus.com (Septiembre 2005) "IDS, firewalls, código malicioso"

e) http://www.insecure.org/nmap (Agosto 2005) "Soluciones de seguridad en ambientes de red"

f) http://www.vanguardms.com/support/documentation/vanguard/index.html (Agosto 2005) "Ruteadores Vangurad"

g) http://www.redbooks.ibm.com/abstracts/sg244446.html?Open (Octubre 2005) "Ruteadores IBM"

h) http://www.precidia.com/support/glossary.html (Enero 2006) "Diccionario de términos"

i) http:// alumno.ucol.mx/al962223/public_html/puerto.html (Octubre 2005) "Puertos TCP/UDP"

j) http://www. movistar.com.ec/datos/index.asp?framesuperior=1 (Enero 2006) "Servicios Movistar"

k) http://www.solucionesseguras.com/productos/checkpoint/enterprise.asp (Octubre 2005) "Solución de seguridad Check Point"

l) http://publib.boulder.ibm.com/tividd/td/SW_FS/sbsup/es_ES/PDF/ct6rzes.pdf (Agosto 2005) "Secure Way Firewall"

m) http://www.microsistemas.net/Astaro%20Data_Sheet_es.pd (Octubre 2005) “Solución de seguridad Astaro”

n) http://www.rigg.cl/Productos/seguridad/noticias/3.act (Octubre 2005) “Firewall de Symantec”

o) http://www.ciscoredaccionvirtual.com/redaccion/comunicados/ver_comunicados.asp?Id=1055 (Octubre 2005) “Soluciones Cisco ASA”

p) http://www.fwbuilder.org (Enero 2006) “Firewall Builder”

q) http://www.openvpn.net (Septiembre 2005) “OpenVPN”

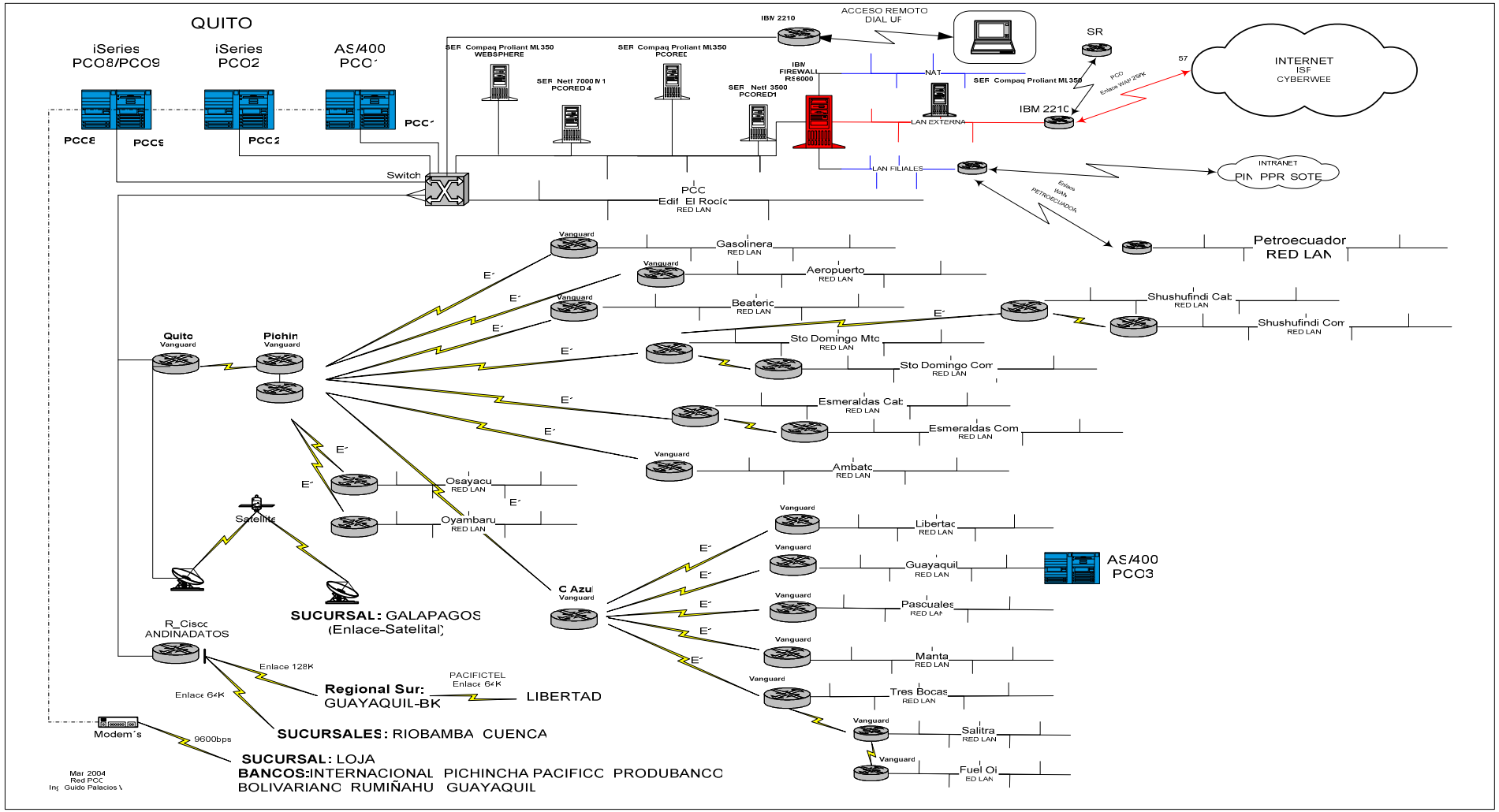
r) http://www.oviedos.com.mx/index.php?gadget=Blog&action=SingleView&id=7 (Septiembre 2005) “Configuración de OpenVPN”

s) http:// es.wikipedia.org/wiki/CentOS#V.C3.A9ase_tambi.C3.A9n (Enero 2006) “Linux CentOS”

ANEXOS

ANEXOS

ANEXO 1: Red LAN y WAN de Petrocomercial



ANEXO 2. Pcofw.fw Archivo de configuración de las reglas del firewall

```
#!/bin/sh
#
#  This is automatically generated file. DO NOT MODIFY !
#
#  Firewall Builder  fwb_ipt v2.0.6-1
#
#  Generated Mon Mar  6 17:48:37 x6 ECT by root
#
# files: * Pcofw.fw

PATH="/sbin:/usr/sbin:/bin:/usr/bin:${PATH}"
export PATH

# Prolog script

# End of prolog script

log() {
  echo "$1"
  test -x "$LOGGER" && $LOGGER -p info "$1"
}

va_num=1
add_addr() {
  addr=$1
  nm=$2
  dev=$3

  type=""
  aadd=""

  L=`$IP -4 link ls $dev | head -n1`
  if test -n "$L"; then
    OIFS=$IFS
    IFS=" /:,<"
    set $L
    type=$4
    IFS=$OIFS

    L=`$IP -4 addr ls $dev to $addr | egrep "$dev\$"`
    if test -n "$L"; then
      OIFS=$IFS
      IFS=" /"
      set $L
      aadd=$2
      IFS=$OIFS
    fi
  fi
  if test -z "$aadd"; then
    if test "$type" = "POINTOPOINT"; then
      $IP -4 addr add $addr dev $dev scope global label $dev:FWB${va_num}
      va_num=`expr $va_num + 1`
    fi
    if test "$type" = "BROADCAST"; then
```

```
      $IP -4 addr add $addr/$nm dev $dev brd + scope global label $dev:FWB${va_num}
      va_num=`expr $va_num + 1`
    fi
  fi
}

getInterfaceVarName() {
  echo $1 | sed 's/\./_/'
}

getaddr() {
  dev=$1
  name=$2
  L=`$IP -4 addr show dev $dev | egrep "$dev\$"`
  test -z "$L" && {
    eval "$name=""
    return
  }
  OIFS=$IFS
  IFS=" /"
  set $L
  eval "$name=$2"
  IFS=$OIFS
}

getinterfaces() {
  NAME=$1
  $IP link show | egrep "$NAME[^ ]*: "| while read L; do
    OIFS=$IFS
    IFS=" :"
    set $L
    IFS=$OIFS
    echo $2
  done
}

LSMOD="/sbin/lsmod"
MODPROBE="/sbin/modprobe"
IPTABLES="/sbin/iptables"
IPTABLES_RESTORE="/sbin/iptables-restore"
IP="/sbin/ip"
LOGGER="/usr/bin/logger"

if $IP link ls >/dev/null 2>&1; then
  echo;
else
  echo "iproute not found"
  exit 1
fi

INTERFACES="eth0 eth2 eth1 lo DMZ "
for i in $INTERFACES ; do
  $IP link show "$i" > /dev/null 2>&1 || {
    log "Interface $i does not exist"
    exit 1
  }
done

$IP -4 neigh flush dev eth0 >/dev/null 2>&1
```

```
$IP -4 addr flush dev eth0 secondary label "eth0:FWB*" >/dev/null 2>&1
$IP -4 neigh flush dev eth2 >/dev/null 2>&1
$IP -4 addr flush dev eth2 secondary label "eth2:FWB*" >/dev/null 2>&1
$IP -4 neigh flush dev eth1 >/dev/null 2>&1
$IP -4 addr flush dev eth1 secondary label "eth1:FWB*" >/dev/null 2>&1
$IP -4 neigh flush dev DMZ >/dev/null 2>&1
$IP -4 addr flush dev DMZ secondary label "DMZ:FWB*" >/dev/null 2>&1

add_addr x.x.212.22 29 eth0
$IP link set eth0 up
add_addr x.x.230.12 24 eth2
$IP link set eth2 up
add_addr x.x.64.6 21 eth1
$IP link set eth1 up
add_addr 127.0.0.1 8 lo
$IP link set lo up
add_addr x.x.10.1 24 DMZ
$IP link set DMZ up

MODULE_DIR="/lib/modules/`uname -r`/kernel/net/ipv4/netfilter/"
MODULES=`(cd $MODULE_DIR; ls *_conntrack_* *_nat_* | sed -n -e 's/\.ko$//p' -e 's/\.o$//p' -e
's/\.ko\.gz$//p' -e 's/\.o\.gz$//p')`
for module in $MODULES; do
  if $LSMOD | grep ${module} >/dev/null; then continue; fi
  $MODPROBE ${module} ||  exit 1
done

add_addr x.x.212.20 29 eth0
add_addr x.x.212.21 29 eth0
add_addr x.x.212.19 29 eth0

log "Activating firewall script generated Mon Mar  6 17:48:37 x6 ECT by root"

$IPTABLES -P OUTPUT  DROP
$IPTABLES -P INPUT   DROP
$IPTABLES -P FORWARD DROP

cat /proc/net/ip_tables_names | while read table; do
  test "X$table" = "Xmangle" && continue
  $IPTABLES -t $table -L -n | while read c chain rest; do
      if test "X$c" = "XChain" ; then
        $IPTABLES -t $table -F $chain
      fi
  done
  $IPTABLES -t $table -X
done

$IPTABLES -A INPUT   -m state --state ESTABLISHED,RELATED -j ACCEPT
$IPTABLES -A OUTPUT  -m state --state ESTABLISHED,RELATED -j ACCEPT
$IPTABLES -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT

 # Rule 0 (NAT)

echo "Rule 0 (NAT)"
#
# NAT Ministerio
$IPTABLES -t nat -A PREROUTING   -s x.16.0.0/16 -d x.x.212.20 -j DNAT --to-destination x.x.64.28
#
# Rule 1 (NAT)
```

```
#
echo "Rule 1 (NAT)"
#
# Enmascaramiento
$IPTABLES -t nat -A POSTROUTING -o eth0  -s x.20.64.7 -j SNAT --to-source x.x.212.22
#
# Rule 2 (NAT)
#
echo "Rule 2 (NAT)"
#
# NAT Servidor web
$IPTABLES -t nat -A PREROUTING   -d x.x.212.21 -j DNAT --to-destination x.x.1.10
#
# Rule 3 (NAT)
#
echo "Rule 3 (NAT)"
#
# NAT WEB Services
$IPTABLES -t nat -A PREROUTING   -d x.x.212.19 -j DNAT --to-destination x.x.1.20
#
# Rule 0 (eth0)
#
echo "Rule 0 (eth0)"
#
# Telnet MEM to PCO
#
$IPTABLES -N eth0_In_RULE_0
$IPTABLES -A FORWARD  -i eth0 -p tcp -m tcp  -s x.16.0.0/16  -d x.20.64.28  --dport 23  -m state --state
NEW  -j eth0_In_RULE_0
$IPTABLES -A eth0_In_RULE_0   -j LOG  --log-level info --log-prefix "RULE 0 -- ACCEPT "
$IPTABLES -A eth0_In_RULE_0   -j ACCEPT
#
# Rule 1 (eth0)
#
echo "Rule 1 (eth0)"
#
# NonSecInt to World    (Proxy)  Servicios Internet 2
#
$IPTABLES -N Cid440CDF20.0
$IPTABLES -A INPUT  -i eth0  -s x.24.212.22  -m state --state NEW  -j Cid440CDF20.0
$IPTABLES -N eth0_In_RULE_1
$IPTABLES -A Cid440CDF20.0  -p tcp -m tcp  -m multiport  --dports 80,3x0  -j eth0_In_RULE_1
$IPTABLES -N Cid440CDF20.1
$IPTABLES -A FORWARD  -i eth0  -s x.24.212.22  -m state --state NEW  -j Cid440CDF20.1
$IPTABLES -A Cid440CDF20.1  -p tcp -m tcp  -m multiport  --dports 80,3x0  -j eth0_In_RULE_1
$IPTABLES -A eth0_In_RULE_1   -j LOG  --log-level info --log-prefix "RULE 1 -- ACCEPT "
$IPTABLES -A eth0_In_RULE_1   -j ACCEPT
$IPTABLES -N Cid440CDF20.2
$IPTABLES -A OUTPUT  -o eth0  -s x.24.212.22  -m state --state NEW  -j Cid440CDF20.2
$IPTABLES -N eth0_Out_RULE_1
$IPTABLES -A Cid440CDF20.2  -p tcp -m tcp  -m multiport  --dports 80,3x0  -j eth0_Out_RULE_1
$IPTABLES -A eth0_Out_RULE_1   -j LOG  --log-level info --log-prefix "RULE 1 -- ACCEPT "
$IPTABLES -A eth0_Out_RULE_1   -j ACCEPT
#
# Rule 2 (eth0)
#
echo "Rule 2 (eth0)"
#
# MEM to PIN AS/400    Telnet direct
```

```
#
$IPTABLES -N Cid440CDF2B.0
$IPTABLES -A FORWARD  -i eth0 -p tcp -m tcp  -s x.16.0.0/16  --dport 23  -m state --state NEW  -j
Cid440CDF2B.0
$IPTABLES -N eth0_In_RULE_2
$IPTABLES -A Cid440CDF2B.0   -d x.17.20.12  -j eth0_In_RULE_2
$IPTABLES -A Cid440CDF2B.0   -d x.17.28.11  -j eth0_In_RULE_2
$IPTABLES -A Cid440CDF2B.0   -d x.17.24.11  -j eth0_In_RULE_2
$IPTABLES -A eth0_In_RULE_2   -j LOG  --log-level info --log-prefix "RULE 2 -- ACCEPT "
$IPTABLES -A eth0_In_RULE_2   -j ACCEPT
#
# Rule 3 (eth0)
#
echo "Rule 3 (eth0)"
#
#
#
$IPTABLES -N eth0_In_RULE_3
$IPTABLES -A FORWARD  -i eth0  -s x.24.212.22  -d x.x.12.1  -j eth0_In_RULE_3
$IPTABLES -A eth0_In_RULE_3   -j LOG  --log-level info --log-prefix "RULE 3 -- DENY "
$IPTABLES -A eth0_In_RULE_3   -j DROP
$IPTABLES -N eth0_Out_RULE_3
$IPTABLES -A OUTPUT  -o eth0  -s x.24.212.22  -d x.x.12.1  -j eth0_Out_RULE_3
$IPTABLES -A eth0_Out_RULE_3   -j LOG  --log-level info --log-prefix "RULE 3 -- DENY "
$IPTABLES -A eth0_Out_RULE_3   -j DROP
#
# Rule 4 (eth0)
#
echo "Rule 4 (eth0)"
#
# PcoEst to MEM (Oracle)
#
$IPTABLES -N Cid440CDF3F.0
$IPTABLES -A FORWARD  -i eth0  -s x.16.1.20  -m state --state NEW  -j Cid440CDF3F.0
$IPTABLES -A FORWARD  -i eth0  -s x.16.1.207  -m state --state NEW  -j Cid440CDF3F.0
$IPTABLES -A FORWARD  -i eth0  -s x.16.1.8  -m state --state NEW  -j Cid440CDF3F.0
$IPTABLES -N eth0_In_RULE_4
$IPTABLES -A Cid440CDF3F.0   -d x.20.71.21  -j eth0_In_RULE_4
$IPTABLES -A Cid440CDF3F.0   -d x.20.71.5  -j eth0_In_RULE_4
$IPTABLES -A Cid440CDF3F.0   -d x.20.71.7  -j eth0_In_RULE_4
$IPTABLES -A eth0_In_RULE_4   -j LOG  --log-level info --log-prefix "RULE 4 -- ACCEPT "
$IPTABLES -A eth0_In_RULE_4   -j ACCEPT
$IPTABLES -N Cid440CDF3F.1
$IPTABLES -A FORWARD  -o eth0  -s x.16.1.20  -m state --state NEW  -j Cid440CDF3F.1
$IPTABLES -A FORWARD  -o eth0  -s x.16.1.207  -m state --state NEW  -j Cid440CDF3F.1
$IPTABLES -A FORWARD  -o eth0  -s x.16.1.8  -m state --state NEW  -j Cid440CDF3F.1
$IPTABLES -N eth0_Out_RULE_4
$IPTABLES -A Cid440CDF3F.1   -d x.20.71.21  -j eth0_Out_RULE_4
$IPTABLES -A Cid440CDF3F.1   -d x.20.71.5  -j eth0_Out_RULE_4
$IPTABLES -A Cid440CDF3F.1   -d x.20.71.7  -j eth0_Out_RULE_4
$IPTABLES -A eth0_Out_RULE_4   -j LOG  --log-level info --log-prefix "RULE 4 -- ACCEPT "
$IPTABLES -A eth0_Out_RULE_4   -j ACCEPT
#
# Rule 5 (eth0)
#
echo "Rule 5 (eth0)"
#
# Prueba WEB Services
#
```

```
$IPTABLES -N eth0_In_RULE_5
$IPTABLES -A FORWARD  -i eth0  -d x.20.71.5  -m state --state NEW  -j eth0_In_RULE_5
$IPTABLES -A eth0_In_RULE_5   -j LOG  --log-level info --log-prefix "RULE 5 -- ACCEPT "
$IPTABLES -A eth0_In_RULE_5   -j ACCEPT
#
# Rule 0 (eth2)
#
echo "Rule 0 (eth2)"
#
# PIN to MEM     Acceso a las aplicaciones desde PIN Shushufindi a MEM: Lotus y Pop3
#
$IPTABLES -N Cid440CDF92.0
$IPTABLES -A FORWARD  -i eth2  -d x.16.1.5  -m state --state NEW  -j Cid440CDF92.0
$IPTABLES -A FORWARD  -i eth2  -d x.16.1.9  -m state --state NEW  -j Cid440CDF92.0
$IPTABLES -N Cid440CDF92.1
$IPTABLES -A Cid440CDF92.0   -s x.17.24.44  -j Cid440CDF92.1
$IPTABLES -A Cid440CDF92.0   -s x.17.24.74  -j Cid440CDF92.1
$IPTABLES -A Cid440CDF92.0   -s x.17.24.103  -j Cid440CDF92.1
$IPTABLES -A Cid440CDF92.0   -s x.20.71.6  -j Cid440CDF92.1
$IPTABLES -N eth2_In_RULE_0
$IPTABLES -A Cid440CDF92.1  -p icmp  -m icmp  --icmp-type 0/0   -j eth2_In_RULE_0
$IPTABLES -A Cid440CDF92.1  -p icmp  -m icmp  --icmp-type 8/0   -j eth2_In_RULE_0
$IPTABLES -A Cid440CDF92.1  -p tcp -m tcp  -m multiport  --dports 110,25,1352  -j eth2_In_RULE_0
$IPTABLES -A eth2_In_RULE_0   -j LOG  --log-level info --log-prefix "RULE 0 -- ACCEPT "
$IPTABLES -A eth2_In_RULE_0   -j ACCEPT
$IPTABLES -N Cid440CDF92.2
$IPTABLES -A FORWARD  -o eth2  -d x.16.1.5  -m state --state NEW  -j Cid440CDF92.2
$IPTABLES -A FORWARD  -o eth2  -d x.16.1.9  -m state --state NEW  -j Cid440CDF92.2
$IPTABLES -N Cid440CDF92.3
$IPTABLES -A Cid440CDF92.2   -s x.17.24.44  -j Cid440CDF92.3
$IPTABLES -A Cid440CDF92.2   -s x.17.24.74  -j Cid440CDF92.3
$IPTABLES -A Cid440CDF92.2   -s x.17.24.103  -j Cid440CDF92.3
$IPTABLES -A Cid440CDF92.2   -s x.20.71.6  -j Cid440CDF92.3
$IPTABLES -N eth2_Out_RULE_0
$IPTABLES -A Cid440CDF92.3  -p icmp  -m icmp  --icmp-type 0/0   -j eth2_Out_RULE_0
$IPTABLES -A Cid440CDF92.3  -p icmp  -m icmp  --icmp-type 8/0   -j eth2_Out_RULE_0
$IPTABLES -A Cid440CDF92.3  -p tcp -m tcp  -m multiport  --dports 110,25,1352  -j eth2_Out_RULE_0
$IPTABLES -A eth2_Out_RULE_0   -j LOG  --log-level info --log-prefix "RULE 0 -- ACCEPT "
$IPTABLES -A eth2_Out_RULE_0   -j ACCEPT
#
# Rule 1 (eth2)
#
echo "Rule 1 (eth2)"
#
# Hst_x.19.48.80 to Srv_x.16.1.5     Acceso desde Host de la Presidencia Ejecutiva de PEC al Servidor
Domino de MEM
#
$IPTABLES -N eth2_In_RULE_1
$IPTABLES -A FORWARD  -i eth2 -p tcp -m tcp  -s x.19.48.80  -d x.16.1.5  --dport 1352  -m state --state
NEW  -j eth2_In_RULE_1
$IPTABLES -A eth2_In_RULE_1   -j LOG  --log-level info --log-prefix "RULE 1 -- ACCEPT "
$IPTABLES -A eth2_In_RULE_1   -j ACCEPT
$IPTABLES -N eth2_Out_RULE_1
$IPTABLES -A FORWARD  -o eth2 -p tcp -m tcp  -s x.19.48.80  -d x.16.1.5  --dport 1352  -m state --state
NEW  -j eth2_Out_RULE_1
$IPTABLES -A eth2_Out_RULE_1   -j LOG  --log-level info --log-prefix "RULE 1 -- ACCEPT "
$IPTABLES -A eth2_Out_RULE_1   -j ACCEPT
#
# Rule 2 (eth2)
```

```
#
echo "Rule 2 (eth2)"
#
# SOTE to MEM
#
$IPTABLES -N Cid440CDFAB.0
$IPTABLES -A FORWARD  -i eth2  -s x.190.10.126  -m state --state NEW  -j Cid440CDFAB.0
$IPTABLES -N eth2_In_RULE_2
$IPTABLES -A Cid440CDFAB.0   -d x.16.1.20  -j eth2_In_RULE_2
$IPTABLES -A Cid440CDFAB.0   -d x.16.1.207  -j eth2_In_RULE_2
$IPTABLES -A Cid440CDFAB.0   -d x.16.1.8  -j eth2_In_RULE_2
$IPTABLES -A eth2_In_RULE_2   -j LOG  --log-level info --log-prefix "RULE 2 -- ACCEPT "
$IPTABLES -A eth2_In_RULE_2   -j ACCEPT
$IPTABLES -N Cid440CDFAB.1
$IPTABLES -A FORWARD  -o eth2  -s x.190.10.126  -m state --state NEW  -j Cid440CDFAB.1
$IPTABLES -N eth2_Out_RULE_2
$IPTABLES -A Cid440CDFAB.1   -d x.16.1.20  -j eth2_Out_RULE_2
$IPTABLES -A Cid440CDFAB.1   -d x.16.1.207  -j eth2_Out_RULE_2
$IPTABLES -A Cid440CDFAB.1   -d x.16.1.8  -j eth2_Out_RULE_2
$IPTABLES -A eth2_Out_RULE_2   -j LOG  --log-level info --log-prefix "RULE 2 -- ACCEPT "
$IPTABLES -A eth2_Out_RULE_2   -j ACCEPT
#
# Rule 3 (eth2)
#
echo "Rule 3 (eth2)"
#
# PECUniCont to MEM  (Oracle)
#
$IPTABLES -N Cid440CDFB5.0
$IPTABLES -A FORWARD  -i eth2  -s x.19.208.84  -m state --state NEW  -j Cid440CDFB5.0
$IPTABLES -A FORWARD  -i eth2  -s x.20.71.5  -m state --state NEW  -j Cid440CDFB5.0
$IPTABLES -N Cid440CDFB5.1
$IPTABLES -A Cid440CDFB5.0   -d x.16.1.5  -j Cid440CDFB5.1
$IPTABLES -A Cid440CDFB5.0   -d x.16.1.9  -j Cid440CDFB5.1
$IPTABLES -N eth2_In_RULE_3
$IPTABLES -A Cid440CDFB5.1  -p tcp -m tcp  -m multiport  --dports 1352,25,1521  -j eth2_In_RULE_3
$IPTABLES -A eth2_In_RULE_3   -j LOG  --log-level info --log-prefix "RULE 3 -- ACCEPT "
$IPTABLES -A eth2_In_RULE_3   -j ACCEPT
$IPTABLES -N Cid440CDFB5.2
$IPTABLES -A FORWARD  -o eth2  -s x.19.208.84  -m state --state NEW  -j Cid440CDFB5.2
$IPTABLES -A FORWARD  -o eth2  -s x.20.71.5  -m state --state NEW  -j Cid440CDFB5.2
$IPTABLES -N Cid440CDFB5.3
$IPTABLES -A Cid440CDFB5.2   -d x.16.1.5  -j Cid440CDFB5.3
$IPTABLES -A Cid440CDFB5.2   -d x.16.1.9  -j Cid440CDFB5.3
$IPTABLES -N eth2_Out_RULE_3
$IPTABLES -A Cid440CDFB5.3  -p tcp -m tcp  -m multiport  --dports 1352,25,1521  -j eth2_Out_RULE_3
$IPTABLES -A eth2_Out_RULE_3   -j LOG  --log-level info --log-prefix "RULE 3 -- ACCEPT "
$IPTABLES -A eth2_Out_RULE_3   -j ACCEPT
#
# Rule 4 (eth2)
#
echo "Rule 4 (eth2)"
#
# PIN Est (Shushufindi) to MEM Oracle
#
$IPTABLES -N Cid440CDFC1.0
$IPTABLES -A FORWARD  -i eth2 -p tcp -m tcp  --dport 1521  -m state --state NEW  -j Cid440CDFC1.0
$IPTABLES -N Cid440CDFC1.1
$IPTABLES -A Cid440CDFC1.0   -d x.16.1.5  -j Cid440CDFC1.1
```

```
$IPTABLES -A Cid440CDFC1.0   -d x.16.1.9  -j Cid440CDFC1.1
$IPTABLES -N eth2_In_RULE_4
$IPTABLES -A Cid440CDFC1.1   -s x.17.24.44  -j eth2_In_RULE_4
$IPTABLES -A Cid440CDFC1.1   -s x.17.24.74  -j eth2_In_RULE_4
$IPTABLES -A Cid440CDFC1.1   -s x.17.24.103  -j eth2_In_RULE_4
$IPTABLES -A eth2_In_RULE_4   -j LOG  --log-level info --log-prefix "RULE 4 -- ACCEPT "
$IPTABLES -A eth2_In_RULE_4   -j ACCEPT
$IPTABLES -N Cid440CDFC1.2
$IPTABLES -A FORWARD  -o eth2 -p tcp -m tcp  --dport 1521  -m state --state NEW  -j Cid440CDFC1.2
$IPTABLES -N Cid440CDFC1.3
$IPTABLES -A Cid440CDFC1.2   -d x.16.1.5  -j Cid440CDFC1.3
$IPTABLES -A Cid440CDFC1.2   -d x.16.1.9  -j Cid440CDFC1.3
$IPTABLES -N eth2_Out_RULE_4
$IPTABLES -A Cid440CDFC1.3   -s x.17.24.44  -j eth2_Out_RULE_4
$IPTABLES -A Cid440CDFC1.3   -s x.17.24.74  -j eth2_Out_RULE_4
$IPTABLES -A Cid440CDFC1.3   -s x.17.24.103  -j eth2_Out_RULE_4
$IPTABLES -A eth2_Out_RULE_4   -j LOG  --log-level info --log-prefix "RULE 4 -- ACCEPT "
$IPTABLES -A eth2_Out_RULE_4   -j ACCEPT
#
# Rule 0 (eth1)
#
echo "Rule 0 (eth1)"
#
# Prueba 1   Administracion
#
$IPTABLES -N Cid440CE022.0
$IPTABLES -A FORWARD  -i eth1  -d x.24.212.17  -m state --state NEW  -j Cid440CE022.0
$IPTABLES -N eth1_In_RULE_0
$IPTABLES -A Cid440CE022.0   -s x.20.71.5  -j eth1_In_RULE_0
$IPTABLES -A Cid440CE022.0   -s x.20.71.6  -j eth1_In_RULE_0
$IPTABLES -A Cid440CE022.0   -s x.20.64.99  -j eth1_In_RULE_0
$IPTABLES -A Cid440CE022.0   -s x.20.64.24  -j eth1_In_RULE_0
$IPTABLES -A eth1_In_RULE_0   -j LOG  --log-level info --log-prefix "RULE 0 -- ACCEPT "
$IPTABLES -A eth1_In_RULE_0   -j ACCEPT
$IPTABLES -N Cid440CE022.1
$IPTABLES -A FORWARD  -o eth1  -d x.24.212.17  -m state --state NEW  -j Cid440CE022.1
$IPTABLES -N eth1_Out_RULE_0
$IPTABLES -A Cid440CE022.1   -s x.20.71.5  -j eth1_Out_RULE_0
$IPTABLES -A Cid440CE022.1   -s x.20.71.6  -j eth1_Out_RULE_0
$IPTABLES -A Cid440CE022.1   -s x.20.64.99  -j eth1_Out_RULE_0
$IPTABLES -A Cid440CE022.1   -s x.20.64.24  -j eth1_Out_RULE_0
$IPTABLES -A eth1_Out_RULE_0   -j LOG  --log-level info --log-prefix "RULE 0 -- ACCEPT "
$IPTABLES -A eth1_Out_RULE_0   -j ACCEPT
#
# Rule 1 (eth1)
#
echo "Rule 1 (eth1)"
#
# PcoEst to SOTE   PCO al Serv Domino de Oleoducto
#
$IPTABLES -N Cid440CE02D.0
$IPTABLES -A FORWARD  -i eth1  -d x.190.10.57  -m state --state NEW  -j Cid440CE02D.0
$IPTABLES -N eth1_In_RULE_1
$IPTABLES -A Cid440CE02D.0   -s x.20.71.5  -j eth1_In_RULE_1
$IPTABLES -A Cid440CE02D.0   -s x.20.71.6  -j eth1_In_RULE_1
$IPTABLES -A Cid440CE02D.0   -s x.20.64.99  -j eth1_In_RULE_1
$IPTABLES -A eth1_In_RULE_1   -j LOG  --log-level info --log-prefix "RULE 1 -- ACCEPT "
$IPTABLES -A eth1_In_RULE_1   -j ACCEPT
$IPTABLES -N Cid440CE02D.1
```

```
$IPTABLES -A FORWARD  -o eth1  -d x.190.10.57  -m state --state NEW  -j Cid440CE02D.1
$IPTABLES -N eth1_Out_RULE_1
$IPTABLES -A Cid440CE02D.1   -s x.20.71.5  -j eth1_Out_RULE_1
$IPTABLES -A Cid440CE02D.1   -s x.20.71.6  -j eth1_Out_RULE_1
$IPTABLES -A Cid440CE02D.1   -s x.20.64.99  -j eth1_Out_RULE_1
$IPTABLES -A eth1_Out_RULE_1   -j LOG  --log-level info --log-prefix "RULE 1 -- ACCEPT "
$IPTABLES -A eth1_Out_RULE_1   -j ACCEPT
#
# Rule 2 (eth1)
#
echo "Rule 2 (eth1)"
#
# PcoEst to MEM (Oracle)
#
$IPTABLES -N Cid440CE037.0
$IPTABLES -A FORWARD  -i eth1  -s x.20.71.21  -m state --state NEW  -j Cid440CE037.0
$IPTABLES -A FORWARD  -i eth1  -s x.20.71.5  -m state --state NEW  -j Cid440CE037.0
$IPTABLES -A FORWARD  -i eth1  -s x.20.71.7  -m state --state NEW  -j Cid440CE037.0
$IPTABLES -N eth1_In_RULE_2
$IPTABLES -A Cid440CE037.0   -d x.16.1.20  -j eth1_In_RULE_2
$IPTABLES -A Cid440CE037.0   -d x.16.1.207  -j eth1_In_RULE_2
$IPTABLES -A Cid440CE037.0   -d x.16.1.8  -j eth1_In_RULE_2
$IPTABLES -A eth1_In_RULE_2   -j LOG  --log-level info --log-prefix "RULE 2 -- ACCEPT "
$IPTABLES -A eth1_In_RULE_2   -j ACCEPT
$IPTABLES -N Cid440CE037.1
$IPTABLES -A FORWARD  -o eth1  -s x.20.71.21  -m state --state NEW  -j Cid440CE037.1
$IPTABLES -A FORWARD  -o eth1  -s x.20.71.5  -m state --state NEW  -j Cid440CE037.1
$IPTABLES -A FORWARD  -o eth1  -s x.20.71.7  -m state --state NEW  -j Cid440CE037.1
$IPTABLES -N eth1_Out_RULE_2
$IPTABLES -A Cid440CE037.1   -d x.16.1.20  -j eth1_Out_RULE_2
$IPTABLES -A Cid440CE037.1   -d x.16.1.207  -j eth1_Out_RULE_2
$IPTABLES -A Cid440CE037.1   -d x.16.1.8  -j eth1_Out_RULE_2
$IPTABLES -A eth1_Out_RULE_2   -j LOG  --log-level info --log-prefix "RULE 2 -- ACCEPT "
$IPTABLES -A eth1_Out_RULE_2   -j ACCEPT
#
# Rule 3 (eth1)
#
echo "Rule 3 (eth1)"
#
# PcoEst to PecSrv1     Gye-Uio     Maquinas de PEC con dir. IP de Pco.
#
$IPTABLES -N Cid440CE041.0
$IPTABLES -A FORWARD  -i eth1  -s x.20.170.145  -m state --state NEW  -j Cid440CE041.0
$IPTABLES -A FORWARD  -i eth1  -s x.20.170.146  -m state --state NEW  -j Cid440CE041.0
$IPTABLES -N eth1_In_RULE_3
$IPTABLES -A Cid440CE041.0   -d x.19.144.245  -j eth1_In_RULE_3
$IPTABLES -A Cid440CE041.0   -d x.19.145.182  -j eth1_In_RULE_3
$IPTABLES -A Cid440CE041.0   -d x.19.226.19  -j eth1_In_RULE_3
$IPTABLES -A Cid440CE041.0   -d x.19.226.4  -j eth1_In_RULE_3
$IPTABLES -A Cid440CE041.0   -d x.x.10.15  -j eth1_In_RULE_3
$IPTABLES -A Cid440CE041.0   -d x.x.10.1  -j eth1_In_RULE_3
$IPTABLES -A Cid440CE041.0   -d x.x.10.3  -j eth1_In_RULE_3
$IPTABLES -A Cid440CE041.0   -d x.x.10.25  -j eth1_In_RULE_3
$IPTABLES -A Cid440CE041.0   -d x.x.10.4  -j eth1_In_RULE_3
$IPTABLES -A Cid440CE041.0   -d x.19.144.231  -j eth1_In_RULE_3
$IPTABLES -A Cid440CE041.0   -d x.19.226.11  -j eth1_In_RULE_3
$IPTABLES -A Cid440CE041.0   -d x.19.226.21  -j eth1_In_RULE_3
$IPTABLES -A Cid440CE041.0   -d x.19.226.16  -j eth1_In_RULE_3
$IPTABLES -A Cid440CE041.0   -d x.19.226.17  -j eth1_In_RULE_3
```

```
$IPTABLES -A Cid440CE041.0   -d x.19.226.5  -j eth1_In_RULE_3
$IPTABLES -A Cid440CE041.0   -d x.19.226.6  -j eth1_In_RULE_3
$IPTABLES -A Cid440CE041.0   -d x.19.226.22  -j eth1_In_RULE_3
$IPTABLES -A eth1_In_RULE_3   -j LOG  --log-level info --log-prefix "RULE 3 -- ACCEPT "
$IPTABLES -A eth1_In_RULE_3   -j ACCEPT
$IPTABLES -N Cid440CE041.1
$IPTABLES -A FORWARD  -o eth1  -s x.20.170.145  -m state --state NEW  -j Cid440CE041.1
$IPTABLES -A FORWARD  -o eth1  -s x.20.170.146  -m state --state NEW  -j Cid440CE041.1
$IPTABLES -N eth1_Out_RULE_3
$IPTABLES -A Cid440CE041.1   -d x.19.144.245  -j eth1_Out_RULE_3
$IPTABLES -A Cid440CE041.1   -d x.19.145.182  -j eth1_Out_RULE_3
$IPTABLES -A Cid440CE041.1   -d x.19.226.19  -j eth1_Out_RULE_3
$IPTABLES -A Cid440CE041.1   -d x.19.226.4  -j eth1_Out_RULE_3
$IPTABLES -A Cid440CE041.1   -d x.x.10.15  -j eth1_Out_RULE_3
$IPTABLES -A Cid440CE041.1   -d x.x.10.1  -j eth1_Out_RULE_3
$IPTABLES -A Cid440CE041.1   -d x.x.10.3  -j eth1_Out_RULE_3
$IPTABLES -A Cid440CE041.1   -d x.x.10.25  -j eth1_Out_RULE_3
$IPTABLES -A Cid440CE041.1   -d x.x.10.4  -j eth1_Out_RULE_3
$IPTABLES -A Cid440CE041.1   -d x.19.144.231  -j eth1_Out_RULE_3
$IPTABLES -A Cid440CE041.1   -d x.19.226.11  -j eth1_Out_RULE_3
$IPTABLES -A Cid440CE041.1   -d x.19.226.21  -j eth1_Out_RULE_3
$IPTABLES -A Cid440CE041.1   -d x.19.226.16  -j eth1_Out_RULE_3
$IPTABLES -A Cid440CE041.1   -d x.19.226.17  -j eth1_Out_RULE_3
$IPTABLES -A Cid440CE041.1   -d x.19.226.5  -j eth1_Out_RULE_3
$IPTABLES -A Cid440CE041.1   -d x.19.226.6  -j eth1_Out_RULE_3
$IPTABLES -A Cid440CE041.1   -d x.19.226.22  -j eth1_Out_RULE_3
$IPTABLES -A eth1_Out_RULE_3   -j LOG  --log-level info --log-prefix "RULE 3 -- ACCEPT "
$IPTABLES -A eth1_Out_RULE_3   -j ACCEPT
#
# Rule 4 (eth1)
#
echo "Rule 4 (eth1)"
#
# GrpPcoEst5 to SecInt   Administracion del Firewall
#
$IPTABLES -N Cid440CE04B.0
$IPTABLES -A INPUT  -i eth1  -d x.20.64.6  -m state --state NEW  -j Cid440CE04B.0
$IPTABLES -N eth1_In_RULE_4
$IPTABLES -A Cid440CE04B.0   -s x.20.71.5  -j eth1_In_RULE_4
$IPTABLES -A Cid440CE04B.0   -s x.20.71.6  -j eth1_In_RULE_4
$IPTABLES -A Cid440CE04B.0   -s x.20.64.99  -j eth1_In_RULE_4
$IPTABLES -A eth1_In_RULE_4   -j LOG  --log-level info --log-prefix "RULE 4 -- ACCEPT "
$IPTABLES -A eth1_In_RULE_4   -j ACCEPT
$IPTABLES -N Cid440CE04B.1
$IPTABLES -A FORWARD  -o eth1  -d x.20.64.6  -m state --state NEW  -j Cid440CE04B.1
$IPTABLES -N eth1_Out_RULE_4
$IPTABLES -A Cid440CE04B.1   -s x.20.71.5  -j eth1_Out_RULE_4
$IPTABLES -A Cid440CE04B.1   -s x.20.71.6  -j eth1_Out_RULE_4
$IPTABLES -A Cid440CE04B.1   -s x.20.64.99  -j eth1_Out_RULE_4
$IPTABLES -A eth1_Out_RULE_4   -j LOG  --log-level info --log-prefix "RULE 4 -- ACCEPT "
$IPTABLES -A eth1_Out_RULE_4   -j ACCEPT
#
# Rule 5 (eth1)
#
echo "Rule 5 (eth1)"
#
# PcoEst to SRI
#
$IPTABLES -N Cid440CE055.0
```

```
$IPTABLES -A FORWARD  -i eth1 -p tcp -m tcp  --dport 1521  -m state --state NEW  -j Cid440CE055.0
$IPTABLES -N Cid440CE055.1
$IPTABLES -A Cid440CE055.0   -s x.20.71.21  -j Cid440CE055.1
$IPTABLES -A Cid440CE055.0   -s x.20.71.5  -j Cid440CE055.1
$IPTABLES -N eth1_In_RULE_5
$IPTABLES -A Cid440CE055.1   -d 10.1.7.10  -j eth1_In_RULE_5
$IPTABLES -A Cid440CE055.1   -d 10.1.7.8  -j eth1_In_RULE_5
$IPTABLES -A eth1_In_RULE_5   -j LOG  --log-level info --log-prefix "RULE 5 -- ACCEPT "
$IPTABLES -A eth1_In_RULE_5   -j ACCEPT
$IPTABLES -N Cid440CE055.2
$IPTABLES -A FORWARD  -o eth1 -p tcp -m tcp  --dport 1521  -m state --state NEW  -j Cid440CE055.2
$IPTABLES -N Cid440CE055.3
$IPTABLES -A Cid440CE055.2   -s x.20.71.21  -j Cid440CE055.3
$IPTABLES -A Cid440CE055.2   -s x.20.71.5  -j Cid440CE055.3
$IPTABLES -N eth1_Out_RULE_5
$IPTABLES -A Cid440CE055.3   -d 10.1.7.10  -j eth1_Out_RULE_5
$IPTABLES -A Cid440CE055.3   -d 10.1.7.8  -j eth1_Out_RULE_5
$IPTABLES -A eth1_Out_RULE_5   -j LOG  --log-level info --log-prefix "RULE 5 -- ACCEPT "
$IPTABLES -A eth1_Out_RULE_5   -j ACCEPT
#
# Rule 6 (eth1)
#
echo "Rule 6 (eth1)"
#
# GrpPcoEst1 to PEC : Servicios Internet PEC
#
$IPTABLES -N Cid440CE05F.0
$IPTABLES -A FORWARD  -i eth1 -p tcp -m tcp  -m multiport  --dports 80,443  -m state --state NEW  -j
Cid440CE05F.0
$IPTABLES -N Cid440CE05F.1
$IPTABLES -A Cid440CE05F.0   -d x.19.144.245  -j Cid440CE05F.1
$IPTABLES -A Cid440CE05F.0   -d x.19.145.182  -j Cid440CE05F.1
$IPTABLES -A Cid440CE05F.0   -d x.19.226.19  -j Cid440CE05F.1
$IPTABLES -A Cid440CE05F.0   -d x.19.226.4  -j Cid440CE05F.1
$IPTABLES -A Cid440CE05F.0   -d x.x.10.15  -j Cid440CE05F.1
$IPTABLES -A Cid440CE05F.0   -d x.x.10.1  -j Cid440CE05F.1
$IPTABLES -A Cid440CE05F.0   -d x.x.10.3  -j Cid440CE05F.1
$IPTABLES -A Cid440CE05F.0   -d x.x.10.25  -j Cid440CE05F.1
$IPTABLES -A Cid440CE05F.0   -d x.x.10.4  -j Cid440CE05F.1
$IPTABLES -A Cid440CE05F.0   -d x.19.144.231  -j Cid440CE05F.1
$IPTABLES -A Cid440CE05F.0   -d x.19.226.11  -j Cid440CE05F.1
$IPTABLES -A Cid440CE05F.0   -d x.19.226.21  -j Cid440CE05F.1
$IPTABLES -A Cid440CE05F.0   -d x.19.226.16  -j Cid440CE05F.1
$IPTABLES -A Cid440CE05F.0   -d x.19.226.17  -j Cid440CE05F.1
$IPTABLES -A Cid440CE05F.0   -d x.19.226.5  -j Cid440CE05F.1
$IPTABLES -A Cid440CE05F.0   -d x.19.226.6  -j Cid440CE05F.1
$IPTABLES -A Cid440CE05F.0   -d x.19.226.22  -j Cid440CE05F.1
$IPTABLES -N eth1_In_RULE_6
$IPTABLES -A Cid440CE05F.1   -s x.20.129.0/24  -j eth1_In_RULE_6
$IPTABLES -A Cid440CE05F.1   -s x.20.130.0/24  -j eth1_In_RULE_6
$IPTABLES -A Cid440CE05F.1   -s x.20.134.0/24  -j eth1_In_RULE_6
$IPTABLES -A Cid440CE05F.1   -s x.20.136.0/24  -j eth1_In_RULE_6
$IPTABLES -A Cid440CE05F.1   -s x.20.137.0/24  -j eth1_In_RULE_6
$IPTABLES -A Cid440CE05F.1   -s x.20.138.0/24  -j eth1_In_RULE_6
$IPTABLES -A Cid440CE05F.1   -s x.20.161.0/24  -j eth1_In_RULE_6
$IPTABLES -A Cid440CE05F.1   -s x.20.162.0/24  -j eth1_In_RULE_6
$IPTABLES -A Cid440CE05F.1   -s x.20.164.0/24  -j eth1_In_RULE_6
$IPTABLES -A Cid440CE05F.1   -s x.20.163.0/24  -j eth1_In_RULE_6
$IPTABLES -A Cid440CE05F.1   -s x.20.167.0/22  -j eth1_In_RULE_6
```

```
$IPTABLES -A Cid440CE05F.1   -s x.20.169.0/22  -j eth1_In_RULE_6
$IPTABLES -A Cid440CE05F.1   -s x.20.170.0/24  -j eth1_In_RULE_6
$IPTABLES -A Cid440CE05F.1   -s x.20.64.0/21  -j eth1_In_RULE_6
$IPTABLES -A Cid440CE05F.1   -s x.20.75.0/24  -j eth1_In_RULE_6
$IPTABLES -A Cid440CE05F.1   -s x.20.76.0/24  -j eth1_In_RULE_6
$IPTABLES -A Cid440CE05F.1   -s x.20.97.0/24  -j eth1_In_RULE_6
$IPTABLES -A Cid440CE05F.1   -s x.20.165.0/24  -j eth1_In_RULE_6
$IPTABLES -A Cid440CE05F.1   -s x.20.132.0/24  -j eth1_In_RULE_6
$IPTABLES -A Cid440CE05F.1   -s x.20.131.0/24  -j eth1_In_RULE_6
$IPTABLES -A Cid440CE05F.1   -s x.20.77.0/24  -j eth1_In_RULE_6
$IPTABLES -A Cid440CE05F.1   -s x.20.139.0/24  -j eth1_In_RULE_6
$IPTABLES -A Cid440CE05F.1   -s x.17.28.0/24  -j eth1_In_RULE_6
$IPTABLES -A Cid440CE05F.1   -s x.17.33.0/24  -j eth1_In_RULE_6
$IPTABLES -A eth1_In_RULE_6   -j LOG  --log-level info --log-prefix "RULE 6 -- ACCEPT "
$IPTABLES -A eth1_In_RULE_6   -j ACCEPT
$IPTABLES -N Cid440CE05F.2
$IPTABLES -A OUTPUT  -o eth1 -p tcp -m tcp  -m multiport  --dports 80,443  -m state --state NEW  -j
Cid440CE05F.2
$IPTABLES -N Cid440CE05F.3
$IPTABLES -A Cid440CE05F.2   -d x.19.144.245  -j Cid440CE05F.3
$IPTABLES -A Cid440CE05F.2   -d x.19.145.182  -j Cid440CE05F.3
$IPTABLES -A Cid440CE05F.2   -d x.19.226.19  -j Cid440CE05F.3
$IPTABLES -A Cid440CE05F.2   -d x.19.226.4  -j Cid440CE05F.3
$IPTABLES -A Cid440CE05F.2   -d x.x.10.15  -j Cid440CE05F.3
$IPTABLES -A Cid440CE05F.2   -d x.x.10.1  -j Cid440CE05F.3
$IPTABLES -A Cid440CE05F.2   -d x.x.10.3  -j Cid440CE05F.3
$IPTABLES -A Cid440CE05F.2   -d x.x.10.25  -j Cid440CE05F.3
$IPTABLES -A Cid440CE05F.2   -d x.x.10.4  -j Cid440CE05F.3
$IPTABLES -A Cid440CE05F.2   -d x.19.144.231  -j Cid440CE05F.3
$IPTABLES -A Cid440CE05F.2   -d x.19.226.11  -j Cid440CE05F.3
$IPTABLES -A Cid440CE05F.2   -d x.19.226.21  -j Cid440CE05F.3
$IPTABLES -A Cid440CE05F.2   -d x.19.226.16  -j Cid440CE05F.3
$IPTABLES -A Cid440CE05F.2   -d x.19.226.17  -j Cid440CE05F.3
$IPTABLES -A Cid440CE05F.2   -d x.19.226.5  -j Cid440CE05F.3
$IPTABLES -A Cid440CE05F.2   -d x.19.226.6  -j Cid440CE05F.3
$IPTABLES -A Cid440CE05F.2   -d x.19.226.22  -j Cid440CE05F.3
$IPTABLES -N eth1_Out_RULE_6
$IPTABLES -A Cid440CE05F.3   -s x.20.129.0/24  -j eth1_Out_RULE_6
$IPTABLES -A Cid440CE05F.3   -s x.20.130.0/24  -j eth1_Out_RULE_6
$IPTABLES -A Cid440CE05F.3   -s x.20.134.0/24  -j eth1_Out_RULE_6
$IPTABLES -A Cid440CE05F.3   -s x.20.136.0/24  -j eth1_Out_RULE_6
$IPTABLES -A Cid440CE05F.3   -s x.20.137.0/24  -j eth1_Out_RULE_6
$IPTABLES -A Cid440CE05F.3   -s x.20.138.0/24  -j eth1_Out_RULE_6
$IPTABLES -A Cid440CE05F.3   -s x.20.161.0/24  -j eth1_Out_RULE_6
$IPTABLES -A Cid440CE05F.3   -s x.20.162.0/24  -j eth1_Out_RULE_6
$IPTABLES -A Cid440CE05F.3   -s x.20.164.0/24  -j eth1_Out_RULE_6
$IPTABLES -A Cid440CE05F.3   -s x.20.163.0/24  -j eth1_Out_RULE_6
$IPTABLES -A Cid440CE05F.3   -s x.20.167.0/22  -j eth1_Out_RULE_6
$IPTABLES -A Cid440CE05F.3   -s x.20.169.0/22  -j eth1_Out_RULE_6
$IPTABLES -A Cid440CE05F.3   -s x.20.170.0/24  -j eth1_Out_RULE_6
$IPTABLES -A Cid440CE05F.3   -s x.20.64.0/21  -j eth1_Out_RULE_6
$IPTABLES -A Cid440CE05F.3   -s x.20.75.0/24  -j eth1_Out_RULE_6
$IPTABLES -A Cid440CE05F.3   -s x.20.76.0/24  -j eth1_Out_RULE_6
$IPTABLES -A Cid440CE05F.3   -s x.20.97.0/24  -j eth1_Out_RULE_6
$IPTABLES -A Cid440CE05F.3   -s x.20.165.0/24  -j eth1_Out_RULE_6
$IPTABLES -A Cid440CE05F.3   -s x.20.132.0/24  -j eth1_Out_RULE_6
$IPTABLES -A Cid440CE05F.3   -s x.20.131.0/24  -j eth1_Out_RULE_6
$IPTABLES -A Cid440CE05F.3   -s x.20.77.0/24  -j eth1_Out_RULE_6
$IPTABLES -A Cid440CE05F.3   -s x.20.139.0/24  -j eth1_Out_RULE_6
```

```
$IPTABLES -A Cid440CE05F.3   -s x.17.28.0/24  -j eth1_Out_RULE_6
$IPTABLES -A Cid440CE05F.3   -s x.17.33.0/24  -j eth1_Out_RULE_6
$IPTABLES -N Cid440CE05F.4
$IPTABLES -A FORWARD  -o eth1 -p tcp -m tcp  -m multiport  --dports 80,443  -m state --state NEW  -j
Cid440CE05F.4
$IPTABLES -N Cid440CE05F.5
$IPTABLES -A Cid440CE05F.4   -d x.19.144.245  -j Cid440CE05F.5
$IPTABLES -A Cid440CE05F.4   -d x.19.145.182  -j Cid440CE05F.5
$IPTABLES -A Cid440CE05F.4   -d x.19.226.19  -j Cid440CE05F.5
$IPTABLES -A Cid440CE05F.4   -d x.19.226.4  -j Cid440CE05F.5
$IPTABLES -A Cid440CE05F.4   -d x.x.10.15  -j Cid440CE05F.5
$IPTABLES -A Cid440CE05F.4   -d x.x.10.1  -j Cid440CE05F.5
$IPTABLES -A Cid440CE05F.4   -d x.x.10.3  -j Cid440CE05F.5
$IPTABLES -A Cid440CE05F.4   -d x.x.10.25  -j Cid440CE05F.5
$IPTABLES -A Cid440CE05F.4   -d x.x.10.4  -j Cid440CE05F.5
$IPTABLES -A Cid440CE05F.4   -d x.19.144.231  -j Cid440CE05F.5
$IPTABLES -A Cid440CE05F.4   -d x.19.226.11  -j Cid440CE05F.5
$IPTABLES -A Cid440CE05F.4   -d x.19.226.21  -j Cid440CE05F.5
$IPTABLES -A Cid440CE05F.4   -d x.19.226.16  -j Cid440CE05F.5
$IPTABLES -A Cid440CE05F.4   -d x.19.226.17  -j Cid440CE05F.5
$IPTABLES -A Cid440CE05F.4   -d x.19.226.5  -j Cid440CE05F.5
$IPTABLES -A Cid440CE05F.4   -d x.19.226.6  -j Cid440CE05F.5
$IPTABLES -A Cid440CE05F.4   -d x.19.226.22  -j Cid440CE05F.5
$IPTABLES -A Cid440CE05F.5   -s x.20.129.0/24  -j eth1_Out_RULE_6
$IPTABLES -A Cid440CE05F.5   -s x.20.130.0/24  -j eth1_Out_RULE_6
$IPTABLES -A Cid440CE05F.5   -s x.20.134.0/24  -j eth1_Out_RULE_6
$IPTABLES -A Cid440CE05F.5   -s x.20.136.0/24  -j eth1_Out_RULE_6
$IPTABLES -A Cid440CE05F.5   -s x.20.137.0/24  -j eth1_Out_RULE_6
$IPTABLES -A Cid440CE05F.5   -s x.20.138.0/24  -j eth1_Out_RULE_6
$IPTABLES -A Cid440CE05F.5   -s x.20.161.0/24  -j eth1_Out_RULE_6
$IPTABLES -A Cid440CE05F.5   -s x.20.162.0/24  -j eth1_Out_RULE_6
$IPTABLES -A Cid440CE05F.5   -s x.20.164.0/24  -j eth1_Out_RULE_6
$IPTABLES -A Cid440CE05F.5   -s x.20.163.0/24  -j eth1_Out_RULE_6
$IPTABLES -A Cid440CE05F.5   -s x.20.167.0/22  -j eth1_Out_RULE_6
$IPTABLES -A Cid440CE05F.5   -s x.20.169.0/22  -j eth1_Out_RULE_6
$IPTABLES -A Cid440CE05F.5   -s x.20.170.0/24  -j eth1_Out_RULE_6
$IPTABLES -A Cid440CE05F.5   -s x.20.64.0/21  -j eth1_Out_RULE_6
$IPTABLES -A Cid440CE05F.5   -s x.20.75.0/24  -j eth1_Out_RULE_6
$IPTABLES -A Cid440CE05F.5   -s x.20.76.0/24  -j eth1_Out_RULE_6
$IPTABLES -A Cid440CE05F.5   -s x.20.97.0/24  -j eth1_Out_RULE_6
$IPTABLES -A Cid440CE05F.5   -s x.20.165.0/24  -j eth1_Out_RULE_6
$IPTABLES -A Cid440CE05F.5   -s x.20.132.0/24  -j eth1_Out_RULE_6
$IPTABLES -A Cid440CE05F.5   -s x.20.131.0/24  -j eth1_Out_RULE_6
$IPTABLES -A Cid440CE05F.5   -s x.20.77.0/24  -j eth1_Out_RULE_6
$IPTABLES -A Cid440CE05F.5   -s x.20.139.0/24  -j eth1_Out_RULE_6
$IPTABLES -A Cid440CE05F.5   -s x.17.28.0/24  -j eth1_Out_RULE_6
$IPTABLES -A Cid440CE05F.5   -s x.17.33.0/24  -j eth1_Out_RULE_6
$IPTABLES -A eth1_Out_RULE_6   -j LOG  --log-level info --log-prefix "RULE 6 -- ACCEPT "
$IPTABLES -A eth1_Out_RULE_6   -j ACCEPT
#
# Rule 7 (eth1)
#
echo "Rule 7 (eth1)"
#
# Grupo IP a proxy
#
$IPTABLES -N Cid440CE06A.0
$IPTABLES -A FORWARD  -i eth1  -d x.20.64.7  -m state --state NEW  -j Cid440CE06A.0
$IPTABLES -N eth1_In_RULE_7
```

```
$IPTABLES -A Cid440CE06A.0   -s x.20.129.0/24  -j eth1_In_RULE_7
$IPTABLES -A Cid440CE06A.0   -s x.20.130.0/24  -j eth1_In_RULE_7
$IPTABLES -A Cid440CE06A.0   -s x.20.134.0/24  -j eth1_In_RULE_7
$IPTABLES -A Cid440CE06A.0   -s x.20.136.0/24  -j eth1_In_RULE_7
$IPTABLES -A Cid440CE06A.0   -s x.20.137.0/24  -j eth1_In_RULE_7
$IPTABLES -A Cid440CE06A.0   -s x.20.138.0/24  -j eth1_In_RULE_7
$IPTABLES -A Cid440CE06A.0   -s x.20.161.0/24  -j eth1_In_RULE_7
$IPTABLES -A Cid440CE06A.0   -s x.20.162.0/24  -j eth1_In_RULE_7
$IPTABLES -A Cid440CE06A.0   -s x.20.164.0/24  -j eth1_In_RULE_7
$IPTABLES -A Cid440CE06A.0   -s x.20.163.0/24  -j eth1_In_RULE_7
$IPTABLES -A Cid440CE06A.0   -s x.20.167.0/22  -j eth1_In_RULE_7
$IPTABLES -A Cid440CE06A.0   -s x.20.169.0/22  -j eth1_In_RULE_7
$IPTABLES -A Cid440CE06A.0   -s x.20.170.0/24  -j eth1_In_RULE_7
$IPTABLES -A Cid440CE06A.0   -s x.20.64.0/21  -j eth1_In_RULE_7
$IPTABLES -A Cid440CE06A.0   -s x.20.75.0/24  -j eth1_In_RULE_7
$IPTABLES -A Cid440CE06A.0   -s x.20.76.0/24  -j eth1_In_RULE_7
$IPTABLES -A Cid440CE06A.0   -s x.20.97.0/24  -j eth1_In_RULE_7
$IPTABLES -A Cid440CE06A.0   -s x.20.165.0/24  -j eth1_In_RULE_7
$IPTABLES -A Cid440CE06A.0   -s x.20.132.0/24  -j eth1_In_RULE_7
$IPTABLES -A Cid440CE06A.0   -s x.20.131.0/24  -j eth1_In_RULE_7
$IPTABLES -A Cid440CE06A.0   -s x.20.77.0/24  -j eth1_In_RULE_7
$IPTABLES -A Cid440CE06A.0   -s x.20.139.0/24  -j eth1_In_RULE_7
$IPTABLES -A Cid440CE06A.0   -s x.17.28.0/24  -j eth1_In_RULE_7
$IPTABLES -A Cid440CE06A.0   -s x.17.33.0/24  -j eth1_In_RULE_7
$IPTABLES -A eth1_In_RULE_7   -j LOG  --log-level info --log-prefix "RULE 7 -- ACCEPT "
$IPTABLES -A eth1_In_RULE_7   -j ACCEPT
$IPTABLES -N Cid440CE06A.1
$IPTABLES -A OUTPUT  -o eth1  -d x.20.64.7  -m state --state NEW  -j Cid440CE06A.1
$IPTABLES -N eth1_Out_RULE_7
$IPTABLES -A Cid440CE06A.1   -s x.20.129.0/24  -j eth1_Out_RULE_7
$IPTABLES -A Cid440CE06A.1   -s x.20.130.0/24  -j eth1_Out_RULE_7
$IPTABLES -A Cid440CE06A.1   -s x.20.134.0/24  -j eth1_Out_RULE_7
$IPTABLES -A Cid440CE06A.1   -s x.20.136.0/24  -j eth1_Out_RULE_7
$IPTABLES -A Cid440CE06A.1   -s x.20.137.0/24  -j eth1_Out_RULE_7
$IPTABLES -A Cid440CE06A.1   -s x.20.138.0/24  -j eth1_Out_RULE_7
$IPTABLES -A Cid440CE06A.1   -s x.20.161.0/24  -j eth1_Out_RULE_7
$IPTABLES -A Cid440CE06A.1   -s x.20.162.0/24  -j eth1_Out_RULE_7
$IPTABLES -A Cid440CE06A.1   -s x.20.164.0/24  -j eth1_Out_RULE_7
$IPTABLES -A Cid440CE06A.1   -s x.20.163.0/24  -j eth1_Out_RULE_7
$IPTABLES -A Cid440CE06A.1   -s x.20.167.0/22  -j eth1_Out_RULE_7
$IPTABLES -A Cid440CE06A.1   -s x.20.169.0/22  -j eth1_Out_RULE_7
$IPTABLES -A Cid440CE06A.1   -s x.20.170.0/24  -j eth1_Out_RULE_7
$IPTABLES -A Cid440CE06A.1   -s x.20.64.0/21  -j eth1_Out_RULE_7
$IPTABLES -A Cid440CE06A.1   -s x.20.75.0/24  -j eth1_Out_RULE_7
$IPTABLES -A Cid440CE06A.1   -s x.20.76.0/24  -j eth1_Out_RULE_7
$IPTABLES -A Cid440CE06A.1   -s x.20.97.0/24  -j eth1_Out_RULE_7
$IPTABLES -A Cid440CE06A.1   -s x.20.165.0/24  -j eth1_Out_RULE_7
$IPTABLES -A Cid440CE06A.1   -s x.20.132.0/24  -j eth1_Out_RULE_7
$IPTABLES -A Cid440CE06A.1   -s x.20.131.0/24  -j eth1_Out_RULE_7
$IPTABLES -A Cid440CE06A.1   -s x.20.77.0/24  -j eth1_Out_RULE_7
$IPTABLES -A Cid440CE06A.1   -s x.20.139.0/24  -j eth1_Out_RULE_7
$IPTABLES -A Cid440CE06A.1   -s x.17.28.0/24  -j eth1_Out_RULE_7
$IPTABLES -A Cid440CE06A.1   -s x.17.33.0/24  -j eth1_Out_RULE_7
$IPTABLES -N Cid440CE06A.2
$IPTABLES -A FORWARD  -o eth1  -d x.20.64.7  -m state --state NEW  -j Cid440CE06A.2
$IPTABLES -A Cid440CE06A.2   -s x.20.129.0/24  -j eth1_Out_RULE_7
$IPTABLES -A Cid440CE06A.2   -s x.20.130.0/24  -j eth1_Out_RULE_7
$IPTABLES -A Cid440CE06A.2   -s x.20.134.0/24  -j eth1_Out_RULE_7
$IPTABLES -A Cid440CE06A.2   -s x.20.136.0/24  -j eth1_Out_RULE_7
```

```
$IPTABLES -A Cid440CE06A.2   -s x.20.137.0/24  -j eth1_Out_RULE_7
$IPTABLES -A Cid440CE06A.2   -s x.20.138.0/24  -j eth1_Out_RULE_7
$IPTABLES -A Cid440CE06A.2   -s x.20.161.0/24  -j eth1_Out_RULE_7
$IPTABLES -A Cid440CE06A.2   -s x.20.162.0/24  -j eth1_Out_RULE_7
$IPTABLES -A Cid440CE06A.2   -s x.20.164.0/24  -j eth1_Out_RULE_7
$IPTABLES -A Cid440CE06A.2   -s x.20.163.0/24  -j eth1_Out_RULE_7
$IPTABLES -A Cid440CE06A.2   -s x.20.167.0/22  -j eth1_Out_RULE_7
$IPTABLES -A Cid440CE06A.2   -s x.20.169.0/22  -j eth1_Out_RULE_7
$IPTABLES -A Cid440CE06A.2   -s x.20.170.0/24  -j eth1_Out_RULE_7
$IPTABLES -A Cid440CE06A.2   -s x.20.64.0/21  -j eth1_Out_RULE_7
$IPTABLES -A Cid440CE06A.2   -s x.20.75.0/24  -j eth1_Out_RULE_7
$IPTABLES -A Cid440CE06A.2   -s x.20.76.0/24  -j eth1_Out_RULE_7
$IPTABLES -A Cid440CE06A.2   -s x.20.97.0/24  -j eth1_Out_RULE_7
$IPTABLES -A Cid440CE06A.2   -s x.20.165.0/24  -j eth1_Out_RULE_7
$IPTABLES -A Cid440CE06A.2   -s x.20.132.0/24  -j eth1_Out_RULE_7
$IPTABLES -A Cid440CE06A.2   -s x.20.131.0/24  -j eth1_Out_RULE_7
$IPTABLES -A Cid440CE06A.2   -s x.20.77.0/24  -j eth1_Out_RULE_7
$IPTABLES -A Cid440CE06A.2   -s x.20.139.0/24  -j eth1_Out_RULE_7
$IPTABLES -A Cid440CE06A.2   -s x.17.28.0/24  -j eth1_Out_RULE_7
$IPTABLES -A Cid440CE06A.2   -s x.17.33.0/24  -j eth1_Out_RULE_7
$IPTABLES -A eth1_Out_RULE_7   -j LOG  --log-level info --log-prefix "RULE 7 -- ACCEPT "
$IPTABLES -A eth1_Out_RULE_7   -j ACCEPT
#
# Rule 0 (lo)
#
echo "Rule 0 (lo)"
#
$IPTABLES -A INPUT  -i lo  -m state --state NEW  -j ACCEPT
$IPTABLES -A OUTPUT  -o lo  -m state --state NEW  -j ACCEPT
#
# Rule 0 (DMZ)
#
echo "Rule 0 (DMZ)"
#
$IPTABLES -N Cid440CE0A1.0
$IPTABLES -A FORWARD  -i DMZ  -d x.168.1.10  -m state --state NEW  -j Cid440CE0A1.0
$IPTABLES -N DMZ_In_RULE_0
$IPTABLES -A Cid440CE0A1.0  -p tcp -m tcp  -m multiport  --dports 80,443  -j DMZ_In_RULE_0
$IPTABLES -A DMZ_In_RULE_0   -j LOG  --log-level info --log-prefix "RULE 0 -- ACCEPT "
$IPTABLES -A DMZ_In_RULE_0   -j ACCEPT
$IPTABLES -N Cid440CE0A1.1
$IPTABLES -A OUTPUT  -o DMZ  -d x.168.1.10  -m state --state NEW  -j Cid440CE0A1.1
$IPTABLES -N DMZ_Out_RULE_0
$IPTABLES -A Cid440CE0A1.1  -p tcp -m tcp  -m multiport  --dports 80,443  -j DMZ_Out_RULE_0
$IPTABLES -N Cid440CE0A1.2
$IPTABLES -A FORWARD  -o DMZ  -d x.168.1.10  -m state --state NEW  -j Cid440CE0A1.2
$IPTABLES -A Cid440CE0A1.2  -p tcp -m tcp  -m multiport  --dports 80,443  -j DMZ_Out_RULE_0
$IPTABLES -A DMZ_Out_RULE_0   -j LOG  --log-level info --log-prefix "RULE 0 -- ACCEPT "
$IPTABLES -A DMZ_Out_RULE_0   -j ACCEPT
#
# Rule 1 (DMZ)
#
echo "Rule 1 (DMZ)"
#
$IPTABLES -N DMZ_In_RULE_1
$IPTABLES -A FORWARD  -i DMZ  -d x.168.1.20  -m state --state NEW  -j DMZ_In_RULE_1
$IPTABLES -A DMZ_In_RULE_1   -j LOG  --log-level info --log-prefix "RULE 1 -- ACCEPT "
$IPTABLES -A DMZ_In_RULE_1   -j ACCEPT
$IPTABLES -N DMZ_Out_RULE_1
```

```
$IPTABLES -A OUTPUT  -o DMZ  -d x.168.1.20  -m state --state NEW  -j DMZ_Out_RULE_1
$IPTABLES -A FORWARD  -o DMZ  -d x.168.1.20  -m state --state NEW  -j DMZ_Out_RULE_1
$IPTABLES -A DMZ_Out_RULE_1   -j LOG  --log-level info --log-prefix "RULE 1 -- ACCEPT "
$IPTABLES -A DMZ_Out_RULE_1   -j ACCEPT
#
# Rule 0 (global)
#
echo "Rule 0 (global)"
# DNS Interno (Pcored)
#
$IPTABLES -N RULE_0
$IPTABLES -A INPUT -p udp -m udp  -s x.20.64.20  --dport 53  -m state --state NEW  -j RULE_0
$IPTABLES -A FORWARD -p udp -m udp  -s x.20.64.20  --dport 53  -m state --state NEW  -j RULE_0
$IPTABLES -A RULE_0  -j LOG  --log-level info --log-prefix "RULE 0 -- ACCEPT "
$IPTABLES -A RULE_0  -j ACCEPT
#
# Rule 1 (global)
#
echo "Rule 1 (global)"
#
# Salida del proxy a Internet
#
$IPTABLES -N Cid440CDE14.0
$IPTABLES -A INPUT  -s x.20.64.7  -m state --state NEW  -j Cid440CDE14.0
$IPTABLES -N RULE_1
$IPTABLES -A Cid440CDE14.0 -p tcp -m tcp  -m multiport  --dports 80,443  -j RULE_1
$IPTABLES -N Cid440CDE14.1
$IPTABLES -A FORWARD  -s x.20.64.7  -m state --state NEW  -j Cid440CDE14.1
$IPTABLES -A Cid440CDE14.1 -p tcp -m tcp  -m multiport  --dports 80,443  -j RULE_1
$IPTABLES -A RULE_1  -j LOG  --log-level info --log-prefix "RULE 1 -- ACCEPT "
$IPTABLES -A RULE_1  -j ACCEPT
#
# Rule 2 (global)
#
echo "Rule 2 (global)"
#
$IPTABLES -N Cid440CDE1F.0
$IPTABLES -A OUTPUT  -d x.20.64.7  -m state --state NEW  -j Cid440CDE1F.0
$IPTABLES -N RULE_2
$IPTABLES -A Cid440CDE1F.0 -p tcp -m tcp  -m multiport  --dports 80,443  -j RULE_2
$IPTABLES -N Cid440CDE1F.1
$IPTABLES -A FORWARD  -d x.20.64.7  -m state --state NEW  -j Cid440CDE1F.1
$IPTABLES -A Cid440CDE1F.1 -p tcp -m tcp  -m multiport  --dports 80,443  -j RULE_2
$IPTABLES -A RULE_2  -j LOG  --log-level info --log-prefix "RULE 2 -- ACCEPT "
$IPTABLES -A RULE_2  -j ACCEPT
#
# Rule 3 (global)
#
echo "Rule 3 (global)"
#
$IPTABLES -N Cid440CDE2A.0
$IPTABLES -A FORWARD  -s x.24.212.21  -m state --state NEW  -j Cid440CDE2A.0
$IPTABLES -N RULE_3
$IPTABLES -A Cid440CDE2A.0  -d x.20.64.20  -j RULE_3
$IPTABLES -A Cid440CDE2A.0  -d x.20.97.20  -j RULE_3
$IPTABLES -A Cid440CDE2A.0  -d x.20.64.100  -j RULE_3
$IPTABLES -A Cid440CDE2A.0  -d x.20.64.15  -j RULE_3
$IPTABLES -A RULE_3  -j LOG  --log-level info --log-prefix "RULE 3 -- ACCEPT "
$IPTABLES -A RULE_3  -j ACCEPT
```

```
#
# Rule 4 (global)
#
echo "Rule 4 (global)"
#
# GrpPcoSrv2 to Hst_x.24.212.21  Servidores mail Quito y Guayaquil hacia fuera
#
$IPTABLES -N Cid440CDE34.0
$IPTABLES -A FORWARD  -d x.24.212.21  -m state --state NEW  -j Cid440CDE34.0
$IPTABLES -N RULE_4
$IPTABLES -A Cid440CDE34.0  -s x.20.64.20  -j RULE_4
$IPTABLES -A Cid440CDE34.0  -s x.20.97.20  -j RULE_4
$IPTABLES -A Cid440CDE34.0  -s x.20.64.100  -j RULE_4
$IPTABLES -A Cid440CDE34.0  -s x.20.64.15  -j RULE_4
$IPTABLES -A RULE_4  -j LOG  --log-level info --log-prefix "RULE 4 -- ACCEPT "
$IPTABLES -A RULE_4  -j ACCEPT
#
# Rule 5 (global)
#
echo "Rule 5 (global)"
#
# Enlace AS/400 Pco Serv a Pec Serv
#
$IPTABLES -N Cid440CDE3E.0
$IPTABLES -A OUTPUT  -d x.19.144.245  -m state --state NEW  -j Cid440CDE3E.0
$IPTABLES -A OUTPUT  -d x.19.145.182  -m state --state NEW  -j Cid440CDE3E.0
$IPTABLES -A OUTPUT  -d x.19.226.19  -m state --state NEW  -j Cid440CDE3E.0
$IPTABLES -A OUTPUT  -d x.19.226.4  -m state --state NEW  -j Cid440CDE3E.0
$IPTABLES -A OUTPUT  -d x.x.10.15  -m state --state NEW  -j Cid440CDE3E.0
$IPTABLES -A OUTPUT  -d x.x.10.1  -m state --state NEW  -j Cid440CDE3E.0
$IPTABLES -A OUTPUT  -d x.x.10.3  -m state --state NEW  -j Cid440CDE3E.0
$IPTABLES -A OUTPUT  -d x.x.10.25  -m state --state NEW  -j Cid440CDE3E.0
$IPTABLES -A OUTPUT  -d x.x.10.4  -m state --state NEW  -j Cid440CDE3E.0
$IPTABLES -A OUTPUT  -d x.19.144.231  -m state --state NEW  -j Cid440CDE3E.0
$IPTABLES -A OUTPUT  -d x.19.226.11  -m state --state NEW  -j Cid440CDE3E.0
$IPTABLES -A OUTPUT  -d x.19.226.21  -m state --state NEW  -j Cid440CDE3E.0
$IPTABLES -A OUTPUT  -d x.19.226.16  -m state --state NEW  -j Cid440CDE3E.0
$IPTABLES -A OUTPUT  -d x.19.226.17  -m state --state NEW  -j Cid440CDE3E.0
$IPTABLES -A OUTPUT  -d x.19.226.5  -m state --state NEW  -j Cid440CDE3E.0
$IPTABLES -A OUTPUT  -d x.19.226.6  -m state --state NEW  -j Cid440CDE3E.0
$IPTABLES -A OUTPUT  -d x.19.226.22  -m state --state NEW  -j Cid440CDE3E.0
$IPTABLES -N RULE_5
$IPTABLES -A Cid440CDE3E.0  -s x.20.64.25  -j RULE_5
$IPTABLES -A Cid440CDE3E.0  -s x.20.64.28  -j RULE_5
$IPTABLES -A Cid440CDE3E.0  -s x.20.64.26  -j RULE_5
$IPTABLES -A Cid440CDE3E.0  -s x.20.64.8  -j RULE_5
$IPTABLES -A Cid440CDE3E.0  -s x.20.64.20  -j RULE_5
$IPTABLES -A Cid440CDE3E.0  -s x.20.97.11  -j RULE_5
$IPTABLES -A Cid440CDE3E.0  -s x.20.97.48  -j RULE_5
$IPTABLES -A Cid440CDE3E.0  -s x.20.97.20  -j RULE_5
$IPTABLES -A Cid440CDE3E.0  -s x.20.97.57  -j RULE_5
$IPTABLES -A Cid440CDE3E.0  -s x.20.64.32/28  -j RULE_5
$IPTABLES -A Cid440CDE3E.0  -s x.20.64.30  -j RULE_5
$IPTABLES -A Cid440CDE3E.0  -s x.20.64.31  -j RULE_5
$IPTABLES -A Cid440CDE3E.0  -s x.20.64.48/30  -j RULE_5
$IPTABLES -A Cid440CDE3E.0  -s x.20.64.52  -j RULE_5
$IPTABLES -A Cid440CDE3E.0  -s x.20.64.53  -j RULE_5
$IPTABLES -A Cid440CDE3E.0  -s x.20.97.110  -j RULE_5
$IPTABLES -A Cid440CDE3E.0  -s x.20.71.21  -j RULE_5
```

```
$IPTABLES -A Cid440CDE3E.0  -s x.20.64.29  -j RULE_5
$IPTABLES -A Cid440CDE3E.0  -s x.20.97.88  -j RULE_5
$IPTABLES -A Cid440CDE3E.0  -s x.20.97.131  -j RULE_5
$IPTABLES -A Cid440CDE3E.0  -s x.20.64.65  -j RULE_5
$IPTABLES -A Cid440CDE3E.0  -s x.20.64.66  -j RULE_5
$IPTABLES -A Cid440CDE3E.0  -s x.20.97.173  -j RULE_5
$IPTABLES -A Cid440CDE3E.0  -s x.20.71.5  -j RULE_5
$IPTABLES -A Cid440CDE3E.0  -s x.20.71.6  -j RULE_5
$IPTABLES -A Cid440CDE3E.0  -s x.20.64.99  -j RULE_5
$IPTABLES -N Cid440CDE3E.1
$IPTABLES -A FORWARD  -d x.19.144.245  -m state --state NEW  -j Cid440CDE3E.1
$IPTABLES -A FORWARD  -d x.19.145.182  -m state --state NEW  -j Cid440CDE3E.1
$IPTABLES -A FORWARD  -d x.19.226.19  -m state --state NEW  -j Cid440CDE3E.1
$IPTABLES -A FORWARD  -d x.19.226.4  -m state --state NEW  -j Cid440CDE3E.1
$IPTABLES -A FORWARD  -d x.x.10.15  -m state --state NEW  -j Cid440CDE3E.1
$IPTABLES -A FORWARD  -d x.x.10.1  -m state --state NEW  -j Cid440CDE3E.1
$IPTABLES -A FORWARD  -d x.x.10.3  -m state --state NEW  -j Cid440CDE3E.1
$IPTABLES -A FORWARD  -d x.x.10.25  -m state --state NEW  -j Cid440CDE3E.1
$IPTABLES -A FORWARD  -d x.x.10.4  -m state --state NEW  -j Cid440CDE3E.1
$IPTABLES -A FORWARD  -d x.19.144.231  -m state --state NEW  -j Cid440CDE3E.1
$IPTABLES -A FORWARD  -d x.19.226.11  -m state --state NEW  -j Cid440CDE3E.1
$IPTABLES -A FORWARD  -d x.19.226.21  -m state --state NEW  -j Cid440CDE3E.1
$IPTABLES -A FORWARD  -d x.19.226.16  -m state --state NEW  -j Cid440CDE3E.1
$IPTABLES -A FORWARD  -d x.19.226.17  -m state --state NEW  -j Cid440CDE3E.1
$IPTABLES -A FORWARD  -d x.19.226.5  -m state --state NEW  -j Cid440CDE3E.1
$IPTABLES -A FORWARD  -d x.19.226.6  -m state --state NEW  -j Cid440CDE3E.1
$IPTABLES -A FORWARD  -d x.19.226.22  -m state --state NEW  -j Cid440CDE3E.1
$IPTABLES -A Cid440CDE3E.1  -s x.20.64.25  -j RULE_5
$IPTABLES -A Cid440CDE3E.1  -s x.20.64.28  -j RULE_5
$IPTABLES -A Cid440CDE3E.1  -s x.20.64.26  -j RULE_5
$IPTABLES -A Cid440CDE3E.1  -s x.20.64.8  -j RULE_5
$IPTABLES -A Cid440CDE3E.1  -s x.20.64.20  -j RULE_5
$IPTABLES -A Cid440CDE3E.1  -s x.20.97.11  -j RULE_5
$IPTABLES -A Cid440CDE3E.1  -s x.20.97.48  -j RULE_5
$IPTABLES -A Cid440CDE3E.1  -s x.20.97.20  -j RULE_5
$IPTABLES -A Cid440CDE3E.1  -s x.20.97.57  -j RULE_5
$IPTABLES -A Cid440CDE3E.1  -s x.20.64.32/28  -j RULE_5
$IPTABLES -A Cid440CDE3E.1  -s x.20.64.30  -j RULE_5
$IPTABLES -A Cid440CDE3E.1  -s x.20.64.31  -j RULE_5
$IPTABLES -A Cid440CDE3E.1  -s x.20.64.48/30  -j RULE_5
$IPTABLES -A Cid440CDE3E.1  -s x.20.64.52  -j RULE_5
$IPTABLES -A Cid440CDE3E.1  -s x.20.64.53  -j RULE_5
$IPTABLES -A Cid440CDE3E.1  -s x.20.97.110  -j RULE_5
$IPTABLES -A Cid440CDE3E.1  -s x.20.71.21  -j RULE_5
$IPTABLES -A Cid440CDE3E.1  -s x.20.64.29  -j RULE_5
$IPTABLES -A Cid440CDE3E.1  -s x.20.97.88  -j RULE_5
$IPTABLES -A Cid440CDE3E.1  -s x.20.97.131  -j RULE_5
$IPTABLES -A Cid440CDE3E.1  -s x.20.64.65  -j RULE_5
$IPTABLES -A Cid440CDE3E.1  -s x.20.64.66  -j RULE_5
$IPTABLES -A Cid440CDE3E.1  -s x.20.97.173  -j RULE_5
$IPTABLES -A Cid440CDE3E.1  -s x.20.71.5  -j RULE_5
$IPTABLES -A Cid440CDE3E.1  -s x.20.71.6  -j RULE_5
$IPTABLES -A Cid440CDE3E.1  -s x.20.64.99  -j RULE_5
$IPTABLES -A RULE_5  -j LOG  --log-level info --log-prefix "RULE 5 -- ACCEPT "
$IPTABLES -A RULE_5  -j ACCEPT
#
# Rule 6 (global)
#
echo "Rule 6 (global)"
```

```
#
# Enlace AS/400 Pco Serv a Pec Serv
#
$IPTABLES -N Cid440CDE4A.0
$IPTABLES -A INPUT  -s x.19.144.245  -m state --state NEW  -j Cid440CDE4A.0
$IPTABLES -A INPUT  -s x.19.145.182  -m state --state NEW  -j Cid440CDE4A.0
$IPTABLES -A INPUT  -s x.19.226.19  -m state --state NEW  -j Cid440CDE4A.0
$IPTABLES -A INPUT  -s x.19.226.4  -m state --state NEW  -j Cid440CDE4A.0
$IPTABLES -A INPUT  -s x.x.10.15  -m state --state NEW  -j Cid440CDE4A.0
$IPTABLES -A INPUT  -s x.x.10.1  -m state --state NEW  -j Cid440CDE4A.0
$IPTABLES -A INPUT  -s x.x.10.3  -m state --state NEW  -j Cid440CDE4A.0
$IPTABLES -A INPUT  -s x.x.10.25  -m state --state NEW  -j Cid440CDE4A.0
$IPTABLES -A INPUT  -s x.x.10.4  -m state --state NEW  -j Cid440CDE4A.0
$IPTABLES -A INPUT  -s x.19.144.231  -m state --state NEW  -j Cid440CDE4A.0
$IPTABLES -A INPUT  -s x.19.226.11  -m state --state NEW  -j Cid440CDE4A.0
$IPTABLES -A INPUT  -s x.19.226.21  -m state --state NEW  -j Cid440CDE4A.0
$IPTABLES -A INPUT  -s x.19.226.16  -m state --state NEW  -j Cid440CDE4A.0
$IPTABLES -A INPUT  -s x.19.226.17  -m state --state NEW  -j Cid440CDE4A.0
$IPTABLES -A INPUT  -s x.19.226.5  -m state --state NEW  -j Cid440CDE4A.0
$IPTABLES -A INPUT  -s x.19.226.6  -m state --state NEW  -j Cid440CDE4A.0
$IPTABLES -A INPUT  -s x.19.226.22  -m state --state NEW  -j Cid440CDE4A.0
$IPTABLES -A INPUT  -s x.19.160.0/20  -m state --state NEW  -j Cid440CDE4A.0
$IPTABLES -N RULE_6
$IPTABLES -A Cid440CDE4A.0  -d x.20.64.25  -j RULE_6
$IPTABLES -A Cid440CDE4A.0  -d x.20.64.28  -j RULE_6
$IPTABLES -A Cid440CDE4A.0  -d x.20.64.26  -j RULE_6
$IPTABLES -A Cid440CDE4A.0  -d x.20.64.8  -j RULE_6
$IPTABLES -A Cid440CDE4A.0  -d x.20.64.20  -j RULE_6
$IPTABLES -A Cid440CDE4A.0  -d x.20.97.11  -j RULE_6
$IPTABLES -A Cid440CDE4A.0  -d x.20.97.48  -j RULE_6
$IPTABLES -A Cid440CDE4A.0  -d x.20.97.20  -j RULE_6
$IPTABLES -A Cid440CDE4A.0  -d x.20.97.57  -j RULE_6
$IPTABLES -A Cid440CDE4A.0  -d x.20.64.32/28  -j RULE_6
$IPTABLES -A Cid440CDE4A.0  -d x.20.64.30  -j RULE_6
$IPTABLES -A Cid440CDE4A.0  -d x.20.64.31  -j RULE_6
$IPTABLES -A Cid440CDE4A.0  -d x.20.64.48/30  -j RULE_6
$IPTABLES -A Cid440CDE4A.0  -d x.20.64.52  -j RULE_6
$IPTABLES -A Cid440CDE4A.0  -d x.20.64.53  -j RULE_6
$IPTABLES -A Cid440CDE4A.0  -d x.20.97.110  -j RULE_6
$IPTABLES -A Cid440CDE4A.0  -d x.20.71.21  -j RULE_6
$IPTABLES -A Cid440CDE4A.0  -d x.20.64.29  -j RULE_6
$IPTABLES -A Cid440CDE4A.0  -d x.20.97.88  -j RULE_6
$IPTABLES -A Cid440CDE4A.0  -d x.20.97.131  -j RULE_6
$IPTABLES -A Cid440CDE4A.0  -d x.20.64.65  -j RULE_6
$IPTABLES -A Cid440CDE4A.0  -d x.20.64.66  -j RULE_6
$IPTABLES -A Cid440CDE4A.0  -d x.20.97.173  -j RULE_6
$IPTABLES -A Cid440CDE4A.0  -d x.20.71.5  -j RULE_6
$IPTABLES -A Cid440CDE4A.0  -d x.20.71.6  -j RULE_6
$IPTABLES -A Cid440CDE4A.0  -d x.20.64.99  -j RULE_6
$IPTABLES -N Cid440CDE4A.1
$IPTABLES -A FORWARD  -s x.19.144.245  -m state --state NEW  -j Cid440CDE4A.1
$IPTABLES -A FORWARD  -s x.19.145.182  -m state --state NEW  -j Cid440CDE4A.1
$IPTABLES -A FORWARD  -s x.19.226.19  -m state --state NEW  -j Cid440CDE4A.1
$IPTABLES -A FORWARD  -s x.19.226.4  -m state --state NEW  -j Cid440CDE4A.1
$IPTABLES -A FORWARD  -s x.x.10.15  -m state --state NEW  -j Cid440CDE4A.1
$IPTABLES -A FORWARD  -s x.x.10.1  -m state --state NEW  -j Cid440CDE4A.1
$IPTABLES -A FORWARD  -s x.x.10.3  -m state --state NEW  -j Cid440CDE4A.1
$IPTABLES -A FORWARD  -s x.x.10.25  -m state --state NEW  -j Cid440CDE4A.1
$IPTABLES -A FORWARD  -s x.x.10.4  -m state --state NEW  -j Cid440CDE4A.1
```

```
$IPTABLES -A FORWARD  -s x.19.144.231  -m state --state NEW  -j Cid440CDE4A.1
$IPTABLES -A FORWARD  -s x.19.226.11  -m state --state NEW  -j Cid440CDE4A.1
$IPTABLES -A FORWARD  -s x.19.226.21  -m state --state NEW  -j Cid440CDE4A.1
$IPTABLES -A FORWARD  -s x.19.226.16  -m state --state NEW  -j Cid440CDE4A.1
$IPTABLES -A FORWARD  -s x.19.226.17  -m state --state NEW  -j Cid440CDE4A.1
$IPTABLES -A FORWARD  -s x.19.226.5  -m state --state NEW  -j Cid440CDE4A.1
$IPTABLES -A FORWARD  -s x.19.226.6  -m state --state NEW  -j Cid440CDE4A.1
$IPTABLES -A FORWARD  -s x.19.226.22  -m state --state NEW  -j Cid440CDE4A.1
$IPTABLES -A FORWARD  -s x.19.160.0/20  -m state --state NEW  -j Cid440CDE4A.1
$IPTABLES -A Cid440CDE4A.1  -d x.20.64.25  -j RULE_6
$IPTABLES -A Cid440CDE4A.1  -d x.20.64.28  -j RULE_6
$IPTABLES -A Cid440CDE4A.1  -d x.20.64.26  -j RULE_6
$IPTABLES -A Cid440CDE4A.1  -d x.20.64.8  -j RULE_6
$IPTABLES -A Cid440CDE4A.1  -d x.20.64.20  -j RULE_6
$IPTABLES -A Cid440CDE4A.1  -d x.20.97.11  -j RULE_6
$IPTABLES -A Cid440CDE4A.1  -d x.20.97.48  -j RULE_6
$IPTABLES -A Cid440CDE4A.1  -d x.20.97.20  -j RULE_6
$IPTABLES -A Cid440CDE4A.1  -d x.20.97.57  -j RULE_6
$IPTABLES -A Cid440CDE4A.1  -d x.20.64.32/28  -j RULE_6
$IPTABLES -A Cid440CDE4A.1  -d x.20.64.30  -j RULE_6
$IPTABLES -A Cid440CDE4A.1  -d x.20.64.31  -j RULE_6
$IPTABLES -A Cid440CDE4A.1  -d x.20.64.48/30  -j RULE_6
$IPTABLES -A Cid440CDE4A.1  -d x.20.64.52  -j RULE_6
$IPTABLES -A Cid440CDE4A.1  -d x.20.64.53  -j RULE_6
$IPTABLES -A Cid440CDE4A.1  -d x.20.97.110  -j RULE_6
$IPTABLES -A Cid440CDE4A.1  -d x.20.71.21  -j RULE_6
$IPTABLES -A Cid440CDE4A.1  -d x.20.64.29  -j RULE_6
$IPTABLES -A Cid440CDE4A.1  -d x.20.97.88  -j RULE_6
$IPTABLES -A Cid440CDE4A.1  -d x.20.97.131  -j RULE_6
$IPTABLES -A Cid440CDE4A.1  -d x.20.64.65  -j RULE_6
$IPTABLES -A Cid440CDE4A.1  -d x.20.64.66  -j RULE_6
$IPTABLES -A Cid440CDE4A.1  -d x.20.97.173  -j RULE_6
$IPTABLES -A Cid440CDE4A.1  -d x.20.71.5  -j RULE_6
$IPTABLES -A Cid440CDE4A.1  -d x.20.71.6  -j RULE_6
$IPTABLES -A Cid440CDE4A.1  -d x.20.64.99  -j RULE_6
$IPTABLES -A RULE_6  -j LOG  --log-level info --log-prefix "RULE 6 -- ACCEPT "
$IPTABLES -A RULE_6  -j ACCEPT
#
# Rule 7 (global)
#
echo "Rule 7 (global)"
#
# Pcored4 a Pcoweb Hst_x.20.64.24 to Hst_x.24.212.21
#
$IPTABLES -N RULE_7
$IPTABLES -A FORWARD  -s x.20.64.24  -d x.24.212.21  -m state --state NEW  -j RULE_7
$IPTABLES -A RULE_7  -j LOG  --log-level info --log-prefix "RULE 7 -- ACCEPT "
$IPTABLES -A RULE_7  -j ACCEPT
#
# Rule 8 (global)
#
echo "Rule 8 (global)"
#
# Pcored4 a Pcoweb Hst_x.20.64.24 to Hst_x.24.212.21
#
$IPTABLES -N RULE_8
$IPTABLES -A FORWARD  -s x.24.212.21  -d x.20.64.24  -m state --state NEW  -j RULE_8
$IPTABLES -A RULE_8  -j LOG  --log-level info --log-prefix "RULE 8 -- ACCEPT "
$IPTABLES -A RULE_8  -j ACCEPT
```

```
#
# Rule 9 (global)
#
echo "Rule 9 (global)"
#
$IPTABLES -N Cid440CDE6B.0
$IPTABLES -A INPUT  -s x.20.64.59  -m state --state NEW  -j Cid440CDE6B.0
$IPTABLES -N RULE_9
$IPTABLES -A Cid440CDE6B.0 -p tcp -m tcp  --sport 20  --dport 1024:65535  -j RULE_9
$IPTABLES -A Cid440CDE6B.0 -p tcp -m tcp  -m multiport  --dports 21,20  -j RULE_9
$IPTABLES -N Cid440CDE6B.1
$IPTABLES -A FORWARD  -s x.20.64.59  -m state --state NEW  -j Cid440CDE6B.1
$IPTABLES -A Cid440CDE6B.1 -p tcp -m tcp  --sport 20  --dport 1024:65535  -j RULE_9
$IPTABLES -A Cid440CDE6B.1 -p tcp -m tcp  -m multiport  --dports 21,20  -j RULE_9
$IPTABLES -A RULE_9  -j LOG  --log-level info --log-prefix "RULE 9 -- ACCEPT "
$IPTABLES -A RULE_9  -j ACCEPT
#
# Rule 10 (global)
#
echo "Rule 10 (global)"
#
$IPTABLES -N Cid440CDE77.0
$IPTABLES -A OUTPUT  -d x.20.64.59  -m state --state NEW  -j Cid440CDE77.0
$IPTABLES -N RULE_10
$IPTABLES -A Cid440CDE77.0 -p tcp -m tcp  --sport 20  --dport 1024:65535  -j RULE_10
$IPTABLES -A Cid440CDE77.0 -p tcp -m tcp  -m multiport  --dports 21,20  -j RULE_10
$IPTABLES -N Cid440CDE77.1
$IPTABLES -A FORWARD  -d x.20.64.59  -m state --state NEW  -j Cid440CDE77.1
$IPTABLES -A Cid440CDE77.1 -p tcp -m tcp  --sport 20  --dport 1024:65535  -j RULE_10
$IPTABLES -A Cid440CDE77.1 -p tcp -m tcp  -m multiport  --dports 21,20  -j RULE_10
$IPTABLES -A RULE_10  -j LOG  --log-level info --log-prefix "RULE 10 -- ACCEPT "
$IPTABLES -A RULE_10  -j ACCEPT
#
# Rule 11 (global)
#
echo "Rule 11 (global)"
#
$IPTABLES -N RULE_11
$IPTABLES -A OUTPUT  -j RULE_11
$IPTABLES -A INPUT  -j RULE_11
$IPTABLES -A FORWARD  -j RULE_11
$IPTABLES -A RULE_11  -j LOG  --log-level info --log-prefix "RULE 11 -- DENY "
$IPTABLES -A RULE_11  -j DROP
#
#
echo 1 > /proc/sys/net/ipv4/ip_forward
#
# Epilog script
#
# End of epilog script
#
```

ANEXO 3. Protocolos IPSec y L2TP

IPSec se puede utilizar en dos modos: modo de transporte que asegura un paquete IP existente desde el origen al destino y *modo de túnel* que coloca un paquete IP existente dentro de un nuevo paquete IP que se envía a un extremo del túnel con formato IPSec. Ambos modos, transporte y túnel, se pueden encapsular en encabezados ESP o AH.

El modo de transporte IPSec se diseñó para proporcionar seguridad para tráfico IP extremo a extremo entre dos sistemas de comunicación, por ejemplo, para hacer segura una conexión TCP o un datagrama UDP. El modo de túnel IPSec se diseñó principalmente para puntos intermedios, enrutadores o puertas de enlace para asegurar otro tipo de tráfico IP dentro de un túnel IPSec que conecta una red IP privada a otra red IP privada en una red IP pública o que no es de confianza (por ejemplo, Internet). En ambos casos, se realiza una negociación de seguridad compleja entre los dos equipos a través del protocolo de intercambio de claves de Internet (IKE, Internet Key Exchange), normalmente mediante certificados PKI para una autenticación mutua.

L2TP sobre IP utiliza el puerto UDP 1701 e incluye una serie de mensajes de control L2TP para el mantenimiento del túnel. Este protocolo también utiliza UDP para enviar tramas PPP encapsuladas en L2TP como datos del túnel. Las tramas PPP encapsuladas se pueden cifrar o comprimir. Cuando los túneles L2TP aparecen como paquetes IP, aprovechan la seguridad IPSec estándar mediante el modo de transporte IPSec para obtener una fuerte protección de integridad, reproducción, autenticidad y privacidad. L2TP se diseñó específicamente para conexiones cliente a servidores de acceso a redes, así como para conexiones puerta de enlace a puerta de enlace. L2TP/IPSec, por lo tanto, proporciona túneles bien definidos e interoperables, con la seguridad de alto nivel e interoperabilidad de IPSec. Es una buena solución para conexiones seguras de acceso remoto.

ABREVIATURAS

OSI:	Open System Interconection
DMZ:	Demilitarized zone
DNS:	Domain Name Server
FTP:	File Transfer Protocol
LAN:	Local Area Network
VPN:	Virtual Private Network
Gb:	Gigabytes (10^9 bytes)
MHz:	Megahertz (10^6 hertz)
GHz:	Gigahertz (10^9 hertz)
HTTP:	Hyper Text Transfer Protocol
HTTPS:	Hyper Text Transfer Protocol Secure
DHCP:	Dynamic Host Configuration Protocol
NAT:	Network Address Translation
Kbps:	Kilo bits por segundo
Mbps:	Mega bits por segundo
WAN:	Wide Area Network
IOS:	Internetwork Operating System
SDRAM:	Synchronous Dynamic Random Access Memory
AUI:	Attachment Unit Interface
IPSec:	Internet Protocol security
TCP:	Transmission Control Protocol
UDP:	User Datagram Protocol
SSH:	Secure Shell
ATM:	Asynchronous Transfer Mode
SDH:	Synchronous Digital Hierarchy
TDM :	Time Division Multiplexer
xDSL :	Digital Subscriber Line (x: variable)
CIR:	Commited Information Rate
ADSL:	Asymmetric Digital Subscriber Line
SHDSL:	Single-pair high-speed digital subscriber line
ISDN:	Integrated Services Digital Network
IP:	Internet Protocol

ISP: Internet Service Provider
DTU: Digital Transmission Unit
AES: Advanced Encryption Standard
DES: Data Encryption Standard
URL: Uniform Resource Locator
SSL: Secure Socket Layer
RSA: Rivest, Shamir y Adleman (Inventores)
SNMP: Simple Network Management Protocol
SMTP: Simple Mail Transfer Protocol
WAIS: Wide Area Information Server
POP3: Post Office Protocol 3
GPRS: General Packet Radio Service
L2TP: Layer 2 Tunneling Protocol
PPTP: Point to Point Tunneling Protocol