Instituto Tecnológico de Costa Rica

Escuela de Ingeniería en Electrónica

Instituto Costarricense de Electricidad

Diseño e implementación de un esquema de seguridad en la red IP para los equipos de las centrales telefónicas

Informe de Proyecto de Graduación para optar por el título de Ingeniero en Electrónica con el grado académico de Licenciatura

Kenneth Serrano Valerín

San José, Noviembre del 2004

INSTITUTO TECNOLOGICO DE COSTA RICA

ESCUELA DE INGENIERIA ELECTRONICA

PROYECTO DE GRADUACIÓN

TRIBUNAL EVALUADOR

Proyecto de Graduación defendido ante el presente Tribunal Evaluador como requisito para optar por el título de Ingeniero en Electrónica con el grado académico de Licenciatura, del Instituto Tecnológico de Costa Rica.

Miembros del Tribunal

Ing. Alfonso Chacón R.

Profesor lector

Ing. William Marín M.

Profesor lector

Ing. Faustino Montes de Oca M.

Profesor asesor

Los miembros de este Tribunal dan fe de que el presente trabajo de graduación ha sido aprobado y cumple con las normas establecidas por la Escuela de Ingeniería Electrónica

Cartago, 28 de enero de 2005

Declaro que el presente Proyecto de Graduación ha sido realizado enteramente por mi persona, utilizando y aplicando literatura referente al tema e introduciendo conocimientos propios.

En los casos en que he utilizado bibliografía, he procedido a indicar las fuentes mediante las respectivas citas bibliográficas.

En consecuencia, asumo la responsabilidad total por el trabajo de graduación realizado y por el contenido del correspondiente informe final.

San José, 12 de noviembre de 2004

Kenneth Serrano Valerín

Céd: *3-381-057*

❖

El presente proyecto está dedicado a mis padres, cuyo apoyo incondicional y sus constantes muestras de aprecio me ayudo a forjarme metas y soñar muy alto.

❖

Agradecimientos

Agradezco a los trabajadores del departamento de Ingeniería de Sistemas de la Unidad Estratégica de Negocios de Gestión de Red y Mantenimiento, y a los ingenieros Luis González Sandoval y el profesor Faustino Montes de Oca por toda la ayuda brindada para la elaboración del presente proyecto.

Además deseo agradecer al Ing. Adolfo Arias Echandi, por permitirme realizar este proyecto en el departamento que el dirige.

Muchas gracias por todas las observaciones realizadas que permitieron llevar este proyecto a su conclusión.

Resumen

En el presente las redes de computadores han llegado a establecerse como un eslabón fundamental en la funcionalidad de una institución o empresa, permitiendo la transferencia de información entre diversas localidades de una forma más eficiente que en la antigüedad. Esto ha permitido que las redes de computadores sean una opción más que viable en la transferencia de información en instituciones como el Instituto Costarricense de Electricidad.

En esta institución se debe realizar transferencias de datos y archivos entre los diversos equipos encargados de llevar a cabo las facturaciones y el funcionamiento de los equipos de telefonía, ya sea móvil o fija, para poder realizar las facturas telefónicas de los usuarios.

Además, los equipos que son adquiridos deben ser administrados por los proveedores por medio de VPN (Virtual Private Networks) desde el país de origen del equipo, esto solamente mientras se está en la fase de pruebas e implementación.

En la solución del presente proyecto se desarrolló firewalls basados en LINUX SuSE 8.2, el cual cuenta con la versión de Kernel 2.4.20. Este sistema operativo permite realizar la escogencia de usuarios por sus direcciones IP y por el tipo de protocolo que utilizan para realizar conexiones remotas.

Como se verá más adelante, la escogencia de LINUX y su paquete IPTABLES como solución corresponde a un análisis de costos y de beneficios en el cual se compara tres tecnologías existentes en el mercado, las cuales pueden satisfacer las necesidades del ICE.

Palabras Claves: Seguridad en redes; IPTABLES; Linux; Telefonía; Listas de acceso; Firewall.

Abstract

Computer networking has become one of the most important fields in the industry, because it allows transferring information between separate geographical sites in a very effective way. For that reason, networking is a very useful option for transfering information troughout Instituto Costarricense de Electricidad (ICE).

In this institution is very important the transfer of data and files between the invoice devices and the switching centrals, because this is the billing method.

Also, new devices must be managed using a VPN from the country of the origin of the equipment. This only for the installation, implementation and the equipment is in test time.

For all these reasons, the firewalls implementation is good solutions to solve the security problems like invalid access to some networks and to avoid invalid users have access to the invoice information and the basic equipment configuration.

For this project, the firewalls equipments are based on LINUX SuSE 8.2, which use the 2.4.20 kernel version, because this operating system can make choosing of users by its IP address and for the used protocols to make the remote connections.

The choosing of LINUX and its IPTABLES packet like solution is based on costs and benefits analysis obtained by compare three different technologies in the market.

Keywords: Network security; IPTABLES; Linux; Access lists; Firewall**.**

INDICE GENERAL

INDICE DE FIGURAS

INDICE DE TABLAS

Capítulo 1 Introducción

1.1 Definición del problema y su importancia

La UEN (Unidad Estratégica de Negocios) de gestión de red y mantenimiento, indica que requiere de un ingeniero en electrónica con conocimientos en redes de computadoras, ya que se cuenta con problemas de seguridad en las redes que tienen los equipos de telefonía que se encargan de realizar los servicios con prepago 110 y 199. Estos equipos están en las localidades de Cartago, Alajuela, Oeste de San José, San Pedro y San José centro.

Esta falta de seguridad afecta de forma significativa el ámbito administrativo, debido a que en estas redes se encuentran los servidores con la información de los cobros, además de otra información que se pretende que no pueda ser alcanzada por cualquier usuario dentro del ICE. Además se pretende evitar que las personas que le dan soporte a estos servidores desde Estados Unidos puedan establecer sesiones en equipos que no sean los suministrados por ellos.

Básicamente, el problema es que la información que se procesa por medio de los equipos de las centrales telefónicas, no se encuentra protegida de posibles accesos indeseados y posibles alteraciones en los datos.

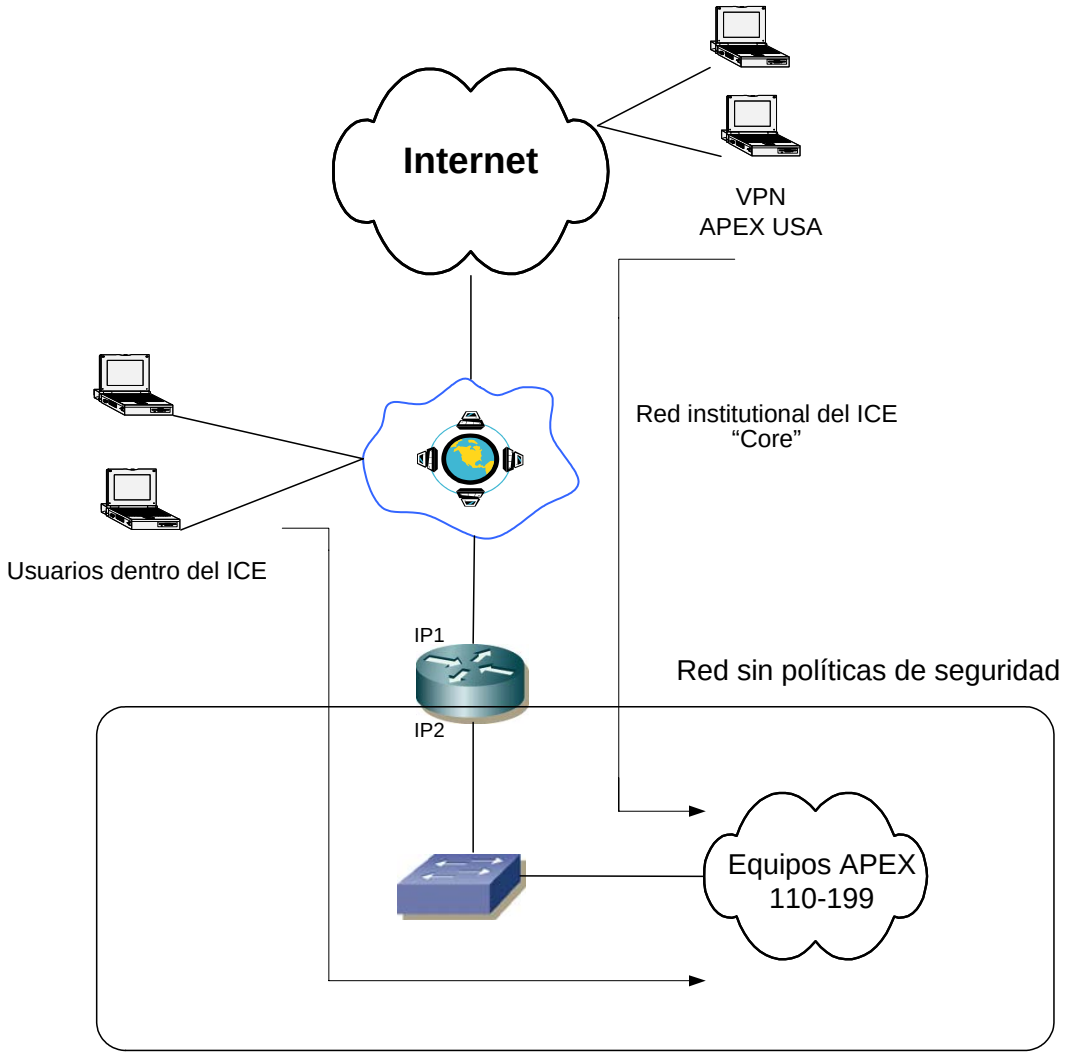

Figura 1 Ubicación de los usuarios que pueden acceder los equipos APEX.

Como se puede observar en la figura 1, actualmente los equipos que permiten los servicios 110 y 199 se encuentran en una red a la cual no se le aplica ninguna política de seguridad, ya que la información solamente se enruta y no se filtra. Por lo tanto, se pretende desarrollar un estándar de seguridad basado en *firewalls* con tecnología LINUX SuSE, ya que ésta fue la tecnología seleccionada para solucionar el problema de entre tres diferentes marcas en el mercado. Este estándar de *firewalls* puede ser implementado en las redes que actualmente cuentan con equipos que procesan información de los servicios telefónicos; sin embargo, para el presente

proyecto se pretende que se pueda implementar este estándar solamente en las redes que cuentan con los equipos APEX.

Llevando este proyecto a término se pretende que se regule el tráfico en la red, impidiendo a los usuarios no deseados el ingreso a los equipos encargados de realizar el manejo y control de los servicios 110 y 199; además impedir que los usuarios del VPN puedan establecer sesiones desde los servidores APEX con algún equipo de las demás redes del ICE, ya que ellos no tienen derechos sobre ningún otro equipo que no sea el que han vendido con ello, se pretende mantener la información resguardada.

Este proyecto pretende solucionar un problema de índole administrativo y de eficiencia, ya que se puede evitar el acceso de usuarios no deseados a información confidencial y además se evita el tráfico de información irrelevante e innecesaria para la funcionalidad de la red; sin embargo se debe aclarar que esta solución cuenta con algunas limitaciones, ya que un plan de seguridad abarca más que la implementación de un *firewall*, como se verá más adelante en las recomendaciones.

La unidad estratégica de negocios de gestión de red y mantenimiento (UEN GRM) pretende que este problema sea resuelto mediante equipos de seguridad en redes, utilizando dispositivos que funcionan con diversos sistemas operativos como lo son LINUX, Windows o los IOS de Cisco. Además, realizar las configuraciones adecuadas de todos estos dispositivos una vez que se haya realizado un análisis completo del tráfico relevante para la funcionalidad de la red.

1.2 Solución seleccionada

El punto de partida para el desarrollo del presente proyecto fue realizar una valoración del mejor método para solucionar la problemática actual basándose en algunas de las tecnologías presentes en el mercado, como lo son: checkpoint, cisco y linux. Con base en el análisis del apartado 3.2.1 se determinó que la mejor solución se puede lograr con linux y iptables, ya que ésta tecnología permite alcanzar los requerimientos del ICE y de esta forma implementar una solución capaz de desarrollar los *firewalls* necesarios y una interfaz entre el administrador y el equipo.

Además linux puede ser utilizado en muchas más aplicaciones del departamento de conmutación. Por lo tanto, la inversión realizada permite solucionar otros problemas con que cuenta este departamento y el precio es bastante razonable.

La empresa presentó una serie de requerimientos que debía cumplir el equipo para solventar la problemática que se ha descrito anteriormente, entre ellos se puede citar:

- Permitir el acceso de usuarios que estén previamente establecidos.
- Denegar el acceso a los usuarios que no cuenten con privilegios para usar los servidores.
- Eliminar los protocolos que no sean necesarios para el funcionamiento normal de los servidores.
- Permitir el acceso a la configuracion del firewall solamente por parte de los administradores de red.
- Cumplir con el cronograma preestablecido.
- Elaborar una interfaz entre el *firewall* y el administrador.
- Elaborar un manual de procedimientos que permita la implementación de los equipos por parte de los técnicos del departamento.

Para poder satisfacer esos requerimientos se utilizó el paquete Netfilter[1] que cuenta con la versión 1.2.11 de iptables, esta herramienta es muy versátil y permite la elaboración de reglas y listas de acceso para poder implementar políticas de seguridad y de filtrado.

El desarrollo del proyecto se basó en los conceptos de redes de computadoras, ethernet como medio físico para la implementación de tecnologías TCP/IP, análisis del tipo de tramas existentes en la red, selección de usuarios por medio de direcciones IP y detección de protocolos utilizados por medio de los puertos de acceso.

[1] Se puede obtener más información en la pagina web http://www.netfilter.org/downloads.html

Capitulo 2 Metas y objetivos

2.1 Meta

- Mejorar los estándares de seguridad de los equipos que permiten los servicios 110 y 199 del Instituto Costarricense de Electricidad.

2.2 Objetivos

2.2.1 Objetivo general

- Diseñar e implementar un esquema de seguridad para los equipos de las centrales telefónicas que funcionan en un entorno IP.

2.2.2 Objetivos específicos

a. Objetivos de software

1. Seleccionar una tecnología capaz de solventar la problemática en seguridad.

2. Diseñar las listas de acceso y las reglas que van a ser implementadas en los *firewalls*.
3. Elaborar la interfaz entre el administrador y el *firewall*.

b. Objetivos de hardware

4. Implementar la topología de las redes seguras con los *firewalls*.

c. Objetivos de implementación

5. Implementar las listas de acceso y las reglas en la solución seleccionada.

d. Objetivos de documentación

6. Realizar un manual de procedimientos de instalación de *firewalls*.

Capitulo 3 Marco Teórico

3.1 Descripción del proceso a mejorar

Los equipos APEX se encuentran distribuidos en cinco puntos del valle central, específicamente en Cartago, Alajuela, Oeste de San José (Pavas), San Pedro y San José centro (Avenida Segunda) , ya que los servicios 110 y 199 son para el uso público y se pretende que puedan ser utilizados por gran parte de la población.

Estos servicios permiten la utilización de líneas telefónicas para realizar llamadas sin portar dinero, debido a que estos servicios son de la modalidad de prepago.

La modalidad de prepago pretende que se pueda llevar a cabo un cobro previo a la realización de la llamada telefónica; específicamente, en el servicio 110 el cargo de la llamada es transferido al usuario que recibe la llamada, antes indicándole que el cobro se va a realizar de este modo. En el servicio 199 se pretende que el usuario adquiera una tarjeta por un monto establecido y cada vez que utiliza el servicio debe marcar el código de la tarjeta que adquirió; por lo tanto el sistema puede descontar de la información que tiene archivada el monto utilizado.

Estos servicios requieren de equipos especiales para su implementación debido a que requieren una interfaz para poder interactuar con las centrales telefónicas y además tener acceso continuo a las bases de datos de los servicios.

Cada equipo APEX se encuentra acoplado a las bases de datos de cada servicio por medio de enlaces E1, los cuales permiten la transferencia de información a velocidades de 2.048 Mbps de forma continua.

Los enlaces ethernet del sistema son para permitir que los funcionarios encargados de dar soporte puedan extraer información útil de los equipos de forma remota, sin tener que desplazarse a cada localidad.

Los servicios de 110 y 199 han sido implementados por el ICE desde hace varios años: sin embargo se ha pensado en mejorarlos para que se pueda atender más personas al mismo tiempo, por lo tanto se adquirió equipo nuevo de la marca APEX.

Este equipo se encuentra en garantía y se requiere que los vendedores puedan realizar las configuraciones necesarias para su implementación. Por lo tanto, la mejor solución para este problema es la implementación de un VPN que permita realizar conexiones con el equipo de forma remota.

Esta necesidad de acoplar el equipo a la red institucional del ICE, genera una problemática de seguridad para los dispositivos y para la integridad de la información de la institución; sin embargo, en la figura 2 se muestra cómo se lleva a cabo la interconexión de los equipos y donde se debe insertar el presente proyecto.

En la figura 2 se ilustra la forma en que se implementan los equipos APEX en las localidades de San Pedro y Alajuela para que estén interconectados al *core* del ICE. Además se muestra como se debe instalar el firewall para poder controlar el tipo de tráfico presente en estas redes y como se debe implementar un enlace redundante para evitar que falle la conectividad entre los servidores de cada localidad y la base de datos localizada en San Pedro, evitando de este modo fallos en el servicios de 110 y 199.

También se ilustra cómo los usuarios del VPN realizan las conexiones con los equipos APEX de cada localidad. En este punto se debe tener claro que la conexión VPN desde Estados Unidos se realiza al *firewall* de internet del departamento de Tecnologías de la Información (TI), y ellos son los encargados de permitir el acceso de los mismos a la red institucional. Una vez dentro de la red, por medio de enrutamiento se alcanzan los equipos APEX. El firewall de cada localidad controla cuáles direcciones del VPN están habilitadas para acceder, además establecen y administran los periodos de tiempo que los suplidores van a tener acceso a los equipos protegidos.

En la figura 2 se indican las soluciones de Alajuela y San Pedro de forma ilustrativa; sin embargo en las demás localidades el proyecto se instaló de la misma

manera, solamente cambiando el direccionamiento y generando las rutas necesarias para enrutar la información de los equipos APEX dependiendo de la localidad.

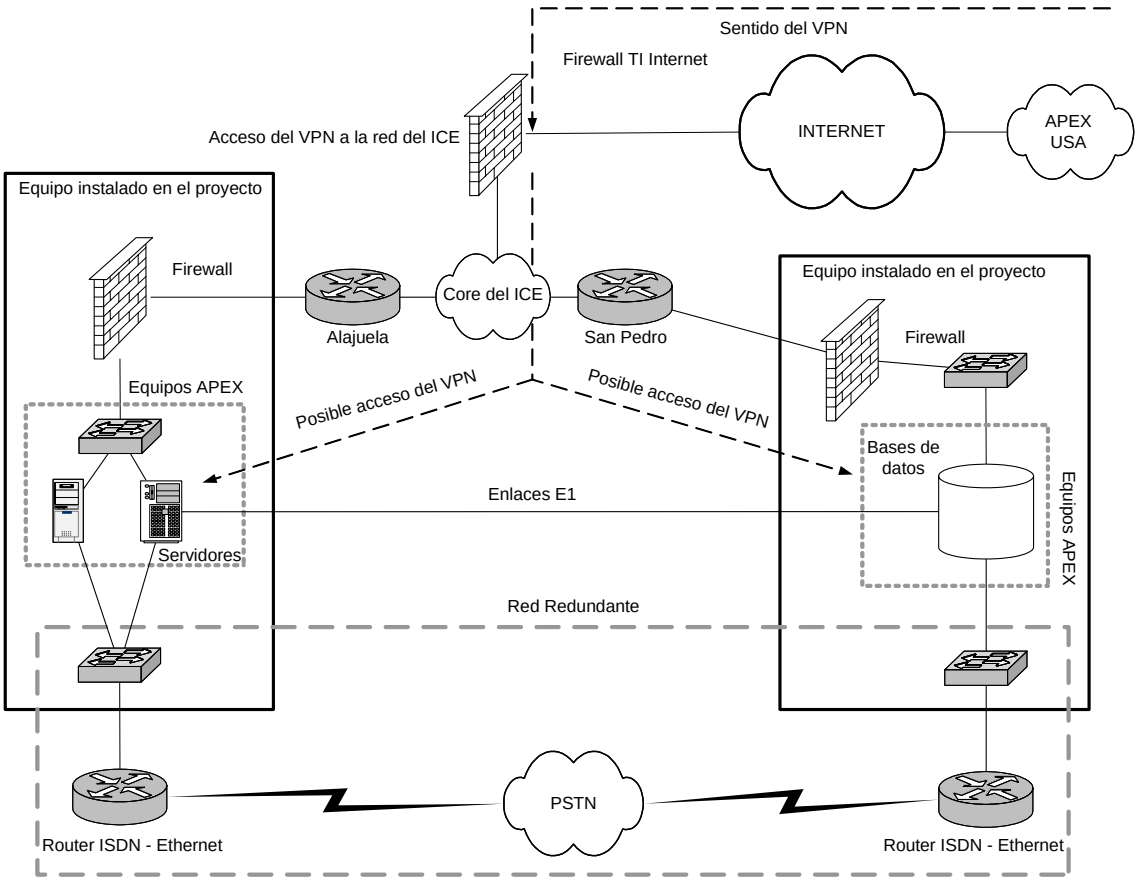

Figura 2 Esquema de la implementación de los equipos APEX en el ICE.

3.2 Antecedentes bibliográficos

3.2.1 Análisis de diversas tecnologías de *firewalls*

En este análisis se pretende realizar un resumen de las principales ventajas y desventajas de Linux, Cisco y Check Point en la implementación de firewalls. Como se verá más adelante, cada tecnología cuenta con ventajas, por ejemplo: Linux es un sistema que permite implementar un firewall de una forma muy sencilla por medio de su módulo de Netfilter; por otro lado los PIX Cisco y FireWall-1 de Check Point son dos de las más reconocidas plataformas de *firewall* en la industria, las cuales cuentan con el respaldo de empresas como Cisco Systems y Check Point.

En este análisis se pretende comparar entre las características de cada dispositivo para solucionar el problema planteado, así como un análisis de la inversión inicial que se debe realizar al adquirir cada una de estas tecnologías.

Linux *Firewall*

Linux se ha convertido en un una plataforma muy utilizada en la industria ya que permite desarrollar aplicaciones que se pueden acoplar a las tareas de cada empresa, inclusive existen alianzas entre empresas como SuSE[2] y NOVELL, para permitir soluciones más eficientes, además de mejorar el soporte técnico.

Esta tecnología permite desarrollar soluciones funcionales sin realizar una alta inversión inicial en equipo, esto lo ha llevado a que se convierta en una solución ideal para pequeñas y medianas empresas, que cuentan con redes locales y necesitan soluciones que sean funcionales, de fácil manejo y económicas.

Linux es un sistema operativo que ha sido desarrollado para ser una plataforma que pueda estar interconectada a muchos más computadores, esto permite que un equipo Linux pueda ser utilizado para solucionar una amplia gama de

[2] Pagina pricipal de Linux SuSE www.suse.com

problemas de redes. Por ejemplo, implementar servidores web, de correo, servicios de directorio, transferencias de archivos y *firewalls* entre otras funciones.

Linux cuenta con varios módulos para poder realizar el filtraje de la información, algunos de los más importantes son: ipfwadm, ipchains, iptables.

La versión más nueva que ha sido lanzada es iptables-1.2.11. Ésta versión cuenta con una gran gama de funciones de filtrado, como la selección de usuarios por direcciones IP o el tipo de protocolo que se utiliza para abrir conexiones. Inclusive permite determinar el estado actual de una sesión (Connection Tracking[3]).

Inversión inicial para la implementación de Firewalls Linux.

- Una licencia de la versión completa de SUSE LINUX Professional 9.2, tiene un costo $89.95.[4].
- Una PC con procesador pentium II con 128 MB y un disco duro de 4GB tiene un costo aproximado de $170, basándose en los precios actuales de estos equipos en el mercado.
- Cada tarjeta de red ethernet de 10/100 Mbps tienen un costo de $13.
- Por lo tanto, un equipo completo para desarrollar un firewall que cuente con una PC, una licencia completa de SuSE LINUX Professional 9.2 y dos tarjetas de red tiene un valor de $285.95.
- En la solución con Linux no existe límites en el número de usuarios que pueden atravesar el firewall de forma simultanea, es decir, no se debe comprar una licencia extra para mejorar el manejo del *firewall*, ya que el paquete completo de SUSE LINUX Professional 9.2 permite que el diseñador del equipo pueda configurarlo con los requerimientos que él crea conveniente.
- El número máximo de interfaces de red esta limitado a la cantidad de “slots” o puertos I/O para agregar las tarjetas de red en la PC.

[3] Ver Apéndice A.1
[4] Información obtenida en la página de Linux SuSE.

- La licencia que se adquiere puede satisfacer otras necesidades del departamento de conmutación, por ejemplo desarrollar equipos dedicados como bases de datos, realizar interfaces con centrales telefónicas de diferentes tecnologías, implementar servidores web, servidores de directorio como NIS o de transferenicias de archivos como NFS o inclusive mejorar las características de equipos del departamento como los frontales[5].

PIX (Private Internet Exchange) Cisco Firewall

La solución que presenta CISCO para solucionar problemas de seguridad es mediante equipos PIX, los cuales permiten configurar y administrar las características de la red, además de que cuentan con compatibilidad para operar con diversas tecnologías y protocolos de red que existen en el mercado como por ejemplo: encriptación con IPsec o L2TP, protocolos enrutados como IP o IPX. Además, permite enrutamiento multiprotocolo; inclusive puede funcionar como un servidor DHCP. Estos equipos son sistemas desarrollados por Cisco systems, una empresa que cuanta con años de desarrollo en equipos de networking.

Los IOS de los PIX de Cisco proveen una funcionalidad muy robusta para la implementación de *firewalls* y de detección de intrusos en la red[6]. Los PIX de CISCO se encuentran en capacidad de ser mejorados mediante la compra de licencias específicas, las cuales permiten habilitar diferentes tipos de servicios para administrar un mayor número de usuarios o mejorar características de procesamiento de filtrado. Esto se logra definiendo un número máximo de interfaces y la cantidad de memoria que puede soportar cada uno de estos sistemas.

[5] Ver apéndice A.1 Frontal.
[6] Página principal de Cisco Systems http://www.cisco.com/

Inversión inicial en la compra de PIX de CISCO.

Cisco cuenta con una variedad de equipos diseñados para solventar los problemas de seguridad de diversos tipos de redes, desde pequeñas redes (SOHO), hasta equipo para grandes empresas o suplidores de servicios (ISP). Estos son algunos ejemplos que pueden implementarse en el presente proyecto.

Cisco PIX 501: Es una solución para redes SOHO ("Small Office Home Office"), cuenta con las característica básicas de seguridad que requiere una pequeña oficina que cuente con un máximo de 50 usuarios. Este sistema es un equipo de firewall para la inspección de la información en la red. Permite el manejo de VPN por medio de IPsec[7], además de otras tecnologías como L2TP[8]. Está en capacidad de manejar la información del firewall a una velocidad de 10Mbps y los VPN con una velocidad de 3Mbps. Puede controlar un máximo de 5 conexiones simultáneas de VPN. El máximo número de interfaces de red que se le puede acoplar al sistema es dos.

Esta solución es la más económica y tiene un valor que varía entre $435 y $635, dependiendo del tipo de licencia que se adquiera para manejar entre 10 y 50 usuarios o el tipo de cifrado de IPsec que se escoja 56b DES[9] o 168b de 3DES.

La solución más económica es para 10 usuarios y un cifrado de 56b DES y la más costosa es de 50 usuarios con un manejo del VPN de 168b 3DES.

Cisco PIX 506E: Es una solución para sucursales de empresas, en las cuales se requiere una mayor velocidad de procesamiento de la información para afectar con un menor impacto las capacidades de la red.

Este equipo puede procesar la información de filtrado a una velocidad de 20Mbps y permite manejar los VPN a una velocidad de 16Mbps si se trabaja con encriptación 3DES; además, puede manejar 25 conexiones VPN simultáneas.

[7] Ver Apéndice A.1 IPSec.
[8] Ver Apéndice A.1 L2TP.
[9] Ver Apéndice A.1 DES.

Provee protección de más de 55 tipos diferentes de ataques DoS[10] ("Denial of Service").

El costo de este equipo es de $1015

Cisco PIX 515E: Este equipo es una solución de mayor envergadura para empresas de mediano tamaño, por lo cual este sistema se encuentra en tres diferentes versiones, las cuales varían en sus capacidades de procesamiento, cantidad de usuarios y conexiones que pueden manejar. Estas versiones son: restringida (R), No restringida (UR) y fail-over (FO).

Las tres versiones permiten un procesamiento de la información del *firewall* a una velocidad de 188Mbps, y permiten establecer 2000 túneles VPN con IPsec de forma simultánea. Si se le agrega una tarjeta de aceleración de velocidad (VAC) se puede alcanzar un procesamiento de 63Mbps para los VPN.

PIX 515E-R: Este sistema permite el manejo de máximo tres interfaces de red, lo cual permite la implementación de una "zona desmilitarizada" o DMZ para equipos que pueden estar expuestos y de esta forma evitar que se afecte la integridad de los equipos de la red interna, los cuales se encuentran acoplados a otra interfaz de red. Además mejora el procesamiento de la información de filtrado del *firewall*, ya que cuenta con una cantidad de memoria 32MB de RAM.

Este equipo requiere de una inversión inicial de $2495, con todas las características descritas anteriormente. La tercera tarjeta se debe comprar por separado.

PIX 515E-UR: Este modelo mejora las características del PIX 515E-R por medio del software, ya que la licencia "No restringida" permite manejar una memoria RAM de 64MB y permite además manejar una cantidad máxima de 6 interfaces 10/100 Mbps. Además, este equipo cuenta con una tarjeta de aceleración de velocidad (VAC) para mejorar el ancho de banda de los VPN. Este sistema está en capacidad de compartir

[10] Ver Apéndice A.1 DoS attack.

el procesamiento de la información de filtrado para una solución de firewall redundante.

Esta solución cuenta con dos interfaces de red y las demás interfaces deben ser adquiridas por separado, este equipo tiene un valor inicial de $5045.

PIX 515E-FO: Este modelo cuenta con el mismo hardware del equipo PIX 515E-UR, sin embargo cuenta con un software diferente, que permite que este equipo trabaje de forma redundante. Este sistema es una extensión que permite una solución completa si trabaja en conjunto con la versión no restringida de ésta equipo. El PIX 515E-FO opera en un modo de inactividad esperando a ser activado por su contraparte que está siempre activo.

Este equipo tiene la capacidad de manejo de 64 MB de memoria RAM y puede manejar un número máximo de 6 interfaces 10/100 Mbps. Este sistema tiene un costo de $2190.

Existen otros equipos para solucionar los problemas de seguridad por medio de PIX de Cisco, sin embargo estos equipos son para problemas en empresas de gran tamaño o inclusive para suplidores de servicios ISP.

Estos equipos cuentan con procesadores que sobrepasan los 600 MHz y permiten un manejo de la información de *firewall* a velocidades mayores de 370 Mbps, además permiten manejar más de 280.000 conexiones simultáneas. Éstas soluciones son excesivas para solventar el presente proyecto, además de que su valor sobrepasa los $10.400. Ejemplos de estos equipos son los PIX 525 o PIX 535.

Los equipos de CISCO que más se ajustan para solucionar el presente proyecto son los PIX 501 y 506E, ya que las transferencias de información entre los equipos APEX y la red institucional del ICE no requieren de un ancho de banda elevado debido a que el tipo de tráfico va a ser en su totalidad de datos. Por lo tanto la velocidad de procesamiento del firewall de 10Mbps es suficiente para no afectar de forma significativa la velocidad de transmisión de la información. Además el número

de conexiones simultaneas nunca va a sobrepasar las 3500 que puede manejar el PIX 501 o el PIX 506E, esto permite que estas dos soluciones sean suficientes para implementar un firewall adecuado. Además estas soluciones cuentan con soporte técnico por parte Cisco y son dispositivos desarrollados por un proveedor especializado en equipos de redes, por lo tanto el precio de estos equipos es razonable.

Check Point FireWall-1

Check Point[11] es un *firewall* basado en software, lo cual significa que es una aplicación que corre en una plataforma estándar de hardware en conjunto con una gran variedad de sistemas operativos como Windows, Solaris, Linux, AIX, HP UX, Nokia IPSO. Esta solución puede ser implementada en computadores Windows, ya que Check Point altera muchas de las características del mismo (como el kernel) para poder corregir los posibles errores del sistema y volverlo más seguro para la implementación de equipos de seguridad en redes.

Check Point es una tecnología muy popular en el mercado de seguridad en Internet. Debido a que cuenta con diversas soluciones como por ejemplo: FireWall – 1, el cual es una solución escalable que le permite a las empresas desarrollar políticas de filtrado de información en sus redes. Además provee de soluciones como VPN - 1 para el manejo de conexiones VPN.

Check Point cuenta con paquetes de productos establecidos para solventar los requisitos de pequeñas, medianas y grandes empresas con diferentes rangos de precios dependiendo de la aplicación que se pretende implementar.

[11] Página principal de Check Point http://www.checkpoint.com/

FireWall – 1 es un sistema basado en servidores que permiten el manejo de la información generada por los firewalls localizados en los límites de la red, y puede ser controlado por una PC que cuente con el software de Check Point para el manejo de todo el sistema de forma centralizada (“SMARTCENTER”).

Inversión inicial para la implementación de una solución de seguridad con Check Point.

Una solución capaz de solventar el problema de seguridad de los equipos APEX es el paquete de Safe@Office, el cual cuenta con las tecnologías Firewall-1 y VPN-1 que permite tener todas las características de un firewall y de las conexiones VPN.

Estas soluciones se venden con licencias que soportan diferentes números de usuarios concurrentes, es decir, equipos que intenten atravesar el firewall de forma simultánea. Los precios de estas soluciones varían entre los $299 y los $1799, como se puede ver en la tabla 1.

Tabla 1 Valores de licencias Check Point para soluciones en redes pequeñas.

Solución planteada	**Usuarios concurrentes**			
	5	**10**	**25**	**indef.**
Safe@Office	$299	$599	$1099	$1,799

En las redes APEX donde serán aplicados los equipos de seguridad existirá un número máximo de cinco servidores, cuatro servidores APEX (ver figura 10) y una base de datos Linux Red Hat, estos equipos pueden ser accedidos por los usuarios del VPN o por los encargados de dar soporte a los servicios 110 y 199 por parte del

ICE. Por lo tanto con cinco conexiones simultáneas se está comprometiendo mucho la escalabilidad de la red, debido a que se puede evitar que personas habilitadas puedan acceder a los equipos APEX en una hora pico de trabajo. La mejor solución es implementar una licencia de diez usuarios simultáneos para permitir una mayor libertad a la hora de trabajar con las redes protegidas. Por lo tanto es razonable la inversión de $599 para implementar una solución de firewalls y VPN en las redes que se encuentran los equipos APEX.

Análisis de la mejor solución

Todas las soluciones que se plantean permiten la implementación de firewalls con ciertas ventajas y desventajas, inclusive cuentan con características similares, como la inspección de paquetes por medio del estado de la conexión, lo cual permite analizar el tráfico dependido del estado actual de cada sesión y es importante para detectar cuales equipos son los que están abriendo las conexiones.

Cada tecnología que se ha expuesto cuenta con sus fortalezas y debilidades, por ejemplo: Linux permite la implementación de *firewalls* en un sistema operativo muy utilizado, de fácil escalabilidad, pero por otro lado es un software abierto al cual se le puede detectar problemas y atacarlos; Check Point permite desarrollar una solución eficiente que permite a un administrador de red regular todo el tipo de información que se transmite en la red por medio de una interfaz gráfica, sin embargo los montos por las licencias requieren de un fuerte inversión de capital; y Cisco PIX es fácil de instalar cuenta con un gran soporte técnico y sus precios son bastante razonables, pero regula la cantidad máxima de usuarios o las capacidades del equipo como la catidad de memoria.

Tomando la información que se ha expuesto de las diversas tecnologías y analizando las soluciones por el costo de la inversión inicial se obtiene la tabla 2.

Comparando las diversas tecnologías y analizado la posible expansión de la red, esta claro que a medida que se requiera un mayor número de usuarios ingresando a los equipos APEX, se necesitará comprar nuevas licencias que permitan un mayor número de usuarios simultáneos. Por lo tanto, el paquete de linux permite que el diseñador del firewall establezca los requerimientos y criterios que él crea convenientes, sin restricciones y a un menor costo.

Tabla 2 Precios de diversas tecnologías de firewalls.

Equipo	Linux SuSE	Cisco PIX	Check Point
Inversión Inicial (Por equipo)	$285.95	$470	$599
Descripción	Computador completo con dos interfaces de red y una licencia de SuSE Linux Profesional 9.2, No hay restricciones por licencias.	Equipo PIX 501 con una licencia que permite manejar 10 usuarios de forma simultanea.	Paquete Safe@Office que cuenta con Firewall -1 y VPN -1, la licencia permite manejar 10 usuarios de forma simultánea. Se debe agregar el costo de la PC y del sistema operativo.
Inversión inicial en equipos para el proyecto APEX (5 equipos)	$1429.75	$2350	$2995

La implementación de Linux es viable no sólo por que cuenta con el precio menor entre las tecnologías expuestas, si no por que cuenta con muchas de las características de los demás *firewall*, como utilización del estado de la conexión, selección de usuarios por medio de listas de acceso o escogencia de los protocolos permitidos en la red. Además, comprar una licencia de Linux es una buena inversión para el departamento de conmutación, debido a que ese sistema operativo puede ser utilizado para solucionar otros proyectos con que cuenta este departamento.

3.2.2 Implementación de IPTABLES

Para poder implementar la solución se utilizó el sistema operativo Linux SuSE[12] 8.2, el cual cuenta con la versión de Kernel 2.4.20. Este sistema operativo es ampliamente utilizado en todas las centrales telefónicas del ICE, debido a su versatilidad y amplia gama de funciones. Esto permite que se pueda utilizar como herramienta para satisfacer necesidades muy variadas, desde acceder a bases de datos hasta realizar interfaces con centrales telefónicas de diferentes tecnologías. Inclusive este sistema permite realizar muchas acciones relacionadas con la administración y manejo de las redes TCP/IP.

Una de las más útiles es el subsistema de procesamiento de paquetes llamado Netfilter, y el comando iptables es el más utilizado para configurarlo.

Los *firewalls* basados en IPTABLES, pueden llegar a tener varias funciones además del filtrado (filter), esto debido a que se puede cambiar datos de los paquetes como la dirección fuente y dirección destino (NAT "*Network address translation*"), además se puede cambiar información como el tipo de servicio y poner marcas a los paquetes (mangle).

Cada una de estas funciones recibe el nombre de "*table*" o tabla, y estas tablas a su vez cuentan con "*chains*" o cadenas que son las encargadas de realizar funciones específicas dependiendo del destino del paquete.

En el presente documento se trabaja únicamente sobre el filtrado de paquetes, ya que la función principal del *firewall* va a ser evitar el tráfico de información irrelevante para las redes que se pretende proteger.

En la figura 3 se muestra el procesamiento que van a tener los paquetes de información al ingresar al *firewall* por una interfaz de red (Entrada), cuando el *firewall* detecta un paquete verifica la dirección IP destino y procede a enrutarlo (enrutamiento).

[12] Página principal de SuSE http://www.suse.com/us/

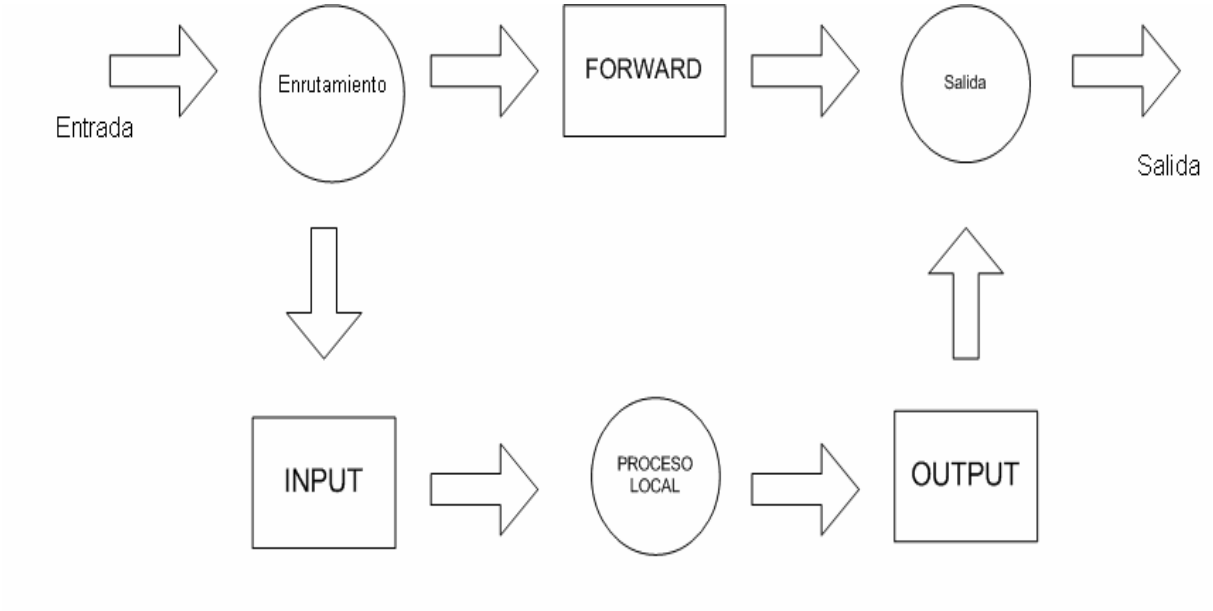

Figura 3 Flujo de paquetes en un firewall con IPTABLES.

Si el paquete va a ser retransmitido por otra interfaz de red, se le aplica las reglas de la cadena de "FORWARD"; ésta cadena es la encargada de descartar la información o de permitir que sea enviada a la interfaz de red necesaria (Salida) para que el paquete siga su rumbo.

Si el paquete tiene como dirección destino una interfaz de red del firewall, se le aplica las reglas de la cadena de entrada o "INPUT"; aquí se decide si se acepta o se rechaza la trama dirigida al firewall. Si se acepta, la información se pasa a los procesos locales del equipo (Proceso Local).

Como se ve en la figura 3, solamente la información que es generada en el firewall (proceso local) será inspeccionada por la cadena de salida "OUTPUT", si las reglas de esta cadena lo permiten, la información alcanzará una interfaz de red (SALIDA) y será transmitida, de lo contrario se descarta.

Estas cadenas pueden llegar a ser configuradas con reglas muy diversas, encargadas de detectar las características que definen que tipo de información está encapsulada en el paquete.

Estas características pueden ser por ejemplo:

- Las direcciones IP fuente y destino.
- El número de puerto para protocolos como TCP o UDP.
- El tipo de paquete en protocolos como ICMP.
- Se pueden definir reglas sobre el estado de la comunicación, es decir, si un paquete está abriendo una sesión (New), si ésta ya se encuentra establecida (Established), inclusive se puede definir si un paquete es producto de una comunicación previa (Related).
- Qué dirección lleva el paquete (Va hacia la red protegida o viene de ella).

Estas son algunas de las características más relevantes que pueden ser detectadas mediante el uso de IPTABLES.

Todas estas reglas que se pueden definir se utilizan para verificar la información encapsulada en el paquete y a su vez ser utiliza para tomar el control sobre el tráfico de la información.

Cuando se detecta algún paquete con la información que se ha definido en las reglas preestablecidas, se procede a realizar una acción como ACCEPT, DROP, LOG o inclusive saltar a otra cadena[13] para seguir con otro grupo de reglas más específicas.

[13] Se puede definir cadenas personalizadas además de las predefinidas ("INPUT", "OUTPUT", "FORWARD"). Ver Bibliografía, entrada 1.

Comandos aplicables a las cadenas.

Tabla 3 Comandos aplicables a las cadenas de reglas.

Comando	**-A –append**
Ejemplo	**iptables INPUT -A…**
Explicación	Agrega una regla al final de la cadena
Comando	**-D –delete**
Ejemplo	**iptables -D INPUT --dport 80 -j DROP, iptables -D INPUT 1**
Explicación	Elimina la regla especificada
Comando	**-I –insert**
Ejemplo	**iptables -I INPUT 1 --dport 80 -j ACCEPT**
Explicación	Inserta una regla en la posición especificada
Comando	**-F**, **--flush**
Ejemplo	**iptables -F FORWARD**
Explicación	Elimina todas las reglas que se han agregado a la cadena especificada.
Comando	**-Z**, **--zero**
Ejemplo	**iptables -Z OUTPUT**
Explicación	Pone todos los contadores de paquetes y bytes de la cadena especificada en cero.
Comando	**-N**, **--new-chain**
Ejemplo	**iptables -N allowed**
Explicación	Crea una nueva cadena a la cual se le puede agregar reglas y se pueden acceder con una acción de “JUMP“.
Comando	**-P**, **--policy**
Ejemplo	**iptables -P INPUT DROP**
Explicación	Establece la política por defecto en alguna cadena, es decir que se hace cuando un paquete no cumple con ninguna regla.

En la tabla 3 se tiene un resumen de los comandos necesarios para controlar las reglas de cada cadena, estos comandos permiten generar o eliminar reglas, reiniciar los contadores, generar nuevas cadenas o establecer la política por defecto de las mismas.

Verificaciones generales

Tabla 4 Verificaciones generales en los paquetes.

Comando	**-p**, **--protocol**
Ejemplo	**iptables -A INPUT -p tcp**
Explicación	Revisa el protocolo del paquete TCP, UDP e ICMP, también se puede usar la forma **--protocol ! tcp.**
Comando	**-s**, **--src**, **--source**
Ejemplo	**iptables -A INPUT -s 192.168.1.1**
Explicación	Revisa la dirección fuente del paquete. Se puede usar la forma **--source ! 192.168.0.0/24** La cual indica que el paquete no proviene de la red 192.168.0.0/24
Comando	**-d**, **--dst**, **--destination**
Ejemplo	**iptables -A INPUT -d 192.168.1.1**
Explicación	Revisa la dirección destino del paquete. Se puede usar la forma **--destination ! 192.168.0.0/24** La cual indica que el paquete no va hacia la red 192.168.0.0/24
Comando	**-i**, **--in-interface**
Ejemplo	**iptables -A INPUT -i eth0**
Explicación	Revisa por cual interfaz entro el paquete, se puede usar **-i ! eth0**, la cual indica que el paquete no entró por la eth0
Comando	**-o**, **--out-interface**
Ejemplo	**iptables -A FORWARD -o eth0**
Explicación	Revisa por cual interfaz va a salir el paquete, se puede usar **-o ! eth0**, la cual indica que el paquete no sale por la eth0

En la tabla 4 se muestra los principales comandos para generar las especificaciones de cada regla, es decir, se ilustra cómo se deben establecer las reglas necesarias para detectar paquetes por dirección IP fuente o destino, por protocolo, e inclusive detectar por cuál interfaz de red se envía o recibe un dato.

Verificaciones implícitas

Tabla 5 Verificaciones implícitas TCP

Comando	**--sport**, **--source-port**
Ejemplo	**iptables -A INPUT -p tcp --sport 22**
Explicación	Verifica cual es el puerto fuente del protocolo TCP del paquete. Se puede usar **--source-port 22:80** y **-source-port ! 22**
Comando	**--dport**, **--destination-port**
Ejemplo	**iptables -A INPUT -p tcp --dport 22**
Explicación	Verifica cual es el puerto destino del protocolo TCP del paquete.
Comando	**--tcp-flags**
Ejemplo	**iptables -p tcp --tcp-flags SYN,FIN,ACK SYN**
Explicación	Verifica el estado de las banderas del paquete, en este ejemplo verifica las banderas SYN, FIN y ACK; de las cuales SYN debe estar activada, por otro lado FIN y ACK no deben estarlo.
Comando	**--syn**
Ejemplo	**iptables -p tcp –syn**
Explicación	Verifica que el paquete tenga solamente activa la bandera SYN y todas las demas esten inactivas.

Tabla 6 Verificaciones implícitas UDP

Comando	**--sport**, **--source-port**
Ejemplo	**iptables -A INPUT -p udp --sport 22**
Explicación	Verifica cual es el puerto fuente del protocolo UDP del paquete. Se puede usar **--source-port 22:80** y **-source-port ! 22**
Comando	**--dport**, **--destination-port**
Ejemplo	**iptables -A INPUT -p udp --dport 22**
Explicación	Verifica cual es el puerto destino del protocolo UDP del paquete.

Tabla 7 Verificaciones implícitas ICMP

Comando	**--icmp-type**
Ejemplo	**iptables -A INPUT -p icmp --icmp-type 8**
Explicación	Verifica cual es el tipo de mensaje ICMP encapsulado en el paquete.

En las tablas 5, 6 y 7 se muestran cuales son los comandos aplicables para cada uno de los protocolos IP, por ejemplo, detectar los puertos fuente o destino de una comunicación TCP o UDP, detectar el tipo de de información contenida en los mensajes ICMP o detectar el orden de las banderas de un paquete TCP, entre otros.

La tabla 8 muestra cuales son las tres principales acciones que se puede realizar cuando se detecta que un paquete ha coincidido con alguna regla, entre ellos podemos citar: “ACCEPT”, “DROP” o “LOG”.

“*Targets/Jumps*” (Blancos/Saltos)

Sirven para realizar la acción una vez que se ha encontrado un paquete que cumple con alguna regla.

Tabla 8 Blancos/Saltos (“Targets/Jumps”)

Comando	**-j ACCEPT**
Ejemplo	**iptables -A -p tcp -d 15.45.23.67 -j ACCEPT**
Explicación	Acepta el paquete y permite que siga con su recorrido.
Comando	**-j DROP**
Ejemplo	**iptables -A -p tcp -d 15.45.23.67 -j DROP**
Explicación	Descarta el paquete.
Comando	**-j DROP**
Comando	**-j LOG --log-prefix "Su mensaje"**
Ejemplo	**iptables -A INPUT -p tcp -j LOG –log-prefix "INPUT"**
Explicación	Crea un mensaje en /var/log/messages, el paquete no se acepta ni se descarta, sigue con la próxima regla.
Comando	**-j JUMP**
Ejemplo	**iptables -A INPUT -p tcp -j JUMP Valid_IO**
Explicación	Salta a una cadena establecida por el administrador. En este ejemplo se denomina a esa cadena “Valid_IO”.

Capítulo 4 Antecedentes

4.1 Estudio del problema a resolver

El presente proyecto pretende desarrollar un equipo que esté en la capacidad de controlar el tipo de tráfico, los protocolos y a su vez establecer cuales puertos pueden estar abiertos y a cuales direcciones, además de realizar un control bien establecido y estructurado de las direcciones fuente y de destino de los paquetes que circulan por la red.

Desarrollando e implementando este equipo se pretende que se evite el acceso a equipos que se encuentran en redes que actualmente son de dominio público y de libre acceso, de este modo mejorar los estándares de seguridad y por lo tanto mantener segura la información que es de suma importancia para el ICE.

Como solución a este problema se pretende instalar un firewall, que esté en capacidad de desarrollar las tareas antes mencionadas para poder solventar estos problemas de seguridad, por lo tanto se implementará un equipo con sistema operativo Linux, que esté en capacidad de realizar esta función por medio de IPTABLES, ya que ésta fue la mejor opción entre las tres tecnologías que se plantearon como posibles soluciones (ver apartado 3.2.1).

4.2 Principales problemas que se deben enfrentar

Se debe realizar un análisis de la situación actual de la red, es decir se debe revisar cuales protocolos están actualmente operando y sobre cuales puertos están siendo utilizados.

Esto es de suma importancia, ya que si se dejan puertos abiertos o protocolos que no se utilizan, se puede dar paso a que la red sea atacada, y de este modo comprometer la información que se pretende mantener segura. Por lo tanto, se desea implementar un firewall, que cuente con una política de desechar por defecto, es decir que si un paquete no es aceptado en ninguna de las reglas preestablecidas el dispositivo lo desecha y de este modo se evita el tráfico de información innecesaria e irrelevante para los efectos de operación de la red, además de desechar todo lo que puede llegar a ser potencialmente peligroso.

Otro problema es la implementación de una nueva red para que opere el firewall, esto debido a que se debe tener cuando menos dos tarjetas de red y cada una de ellas debe estar en un segmento de red diferente.

Como se ejemplifica en las figura 4, debe existir una red entre el router y el firewall, la cual puede llegar a tener incluso solo dos direcciones válidas y se encargaría de enlazar estos dos equipos (IP2), y otra red que sería la encargada de tener los equipos y servidores, la cual va estar protegida por el firewall (IP3).

Como se puede ver en la figura 4, esta solución corresponde a la de cualquier localidad, el resto de redes con equipos APEX también va a estar unido al core de la red institucional. En la figura 2 se muestra un ejemplo de cómo se encuentran instaladas las soluciones de Alajuela y San Pedro, ambas en la misma figura.

El Switch 2 que se muestra en la figura 4, es para dar redundancia por medio de un enlace ISDN, como se puede observar en la figura 2, sin embargo el establecimiento de este enlace no es un objetivo del presente proyecto.

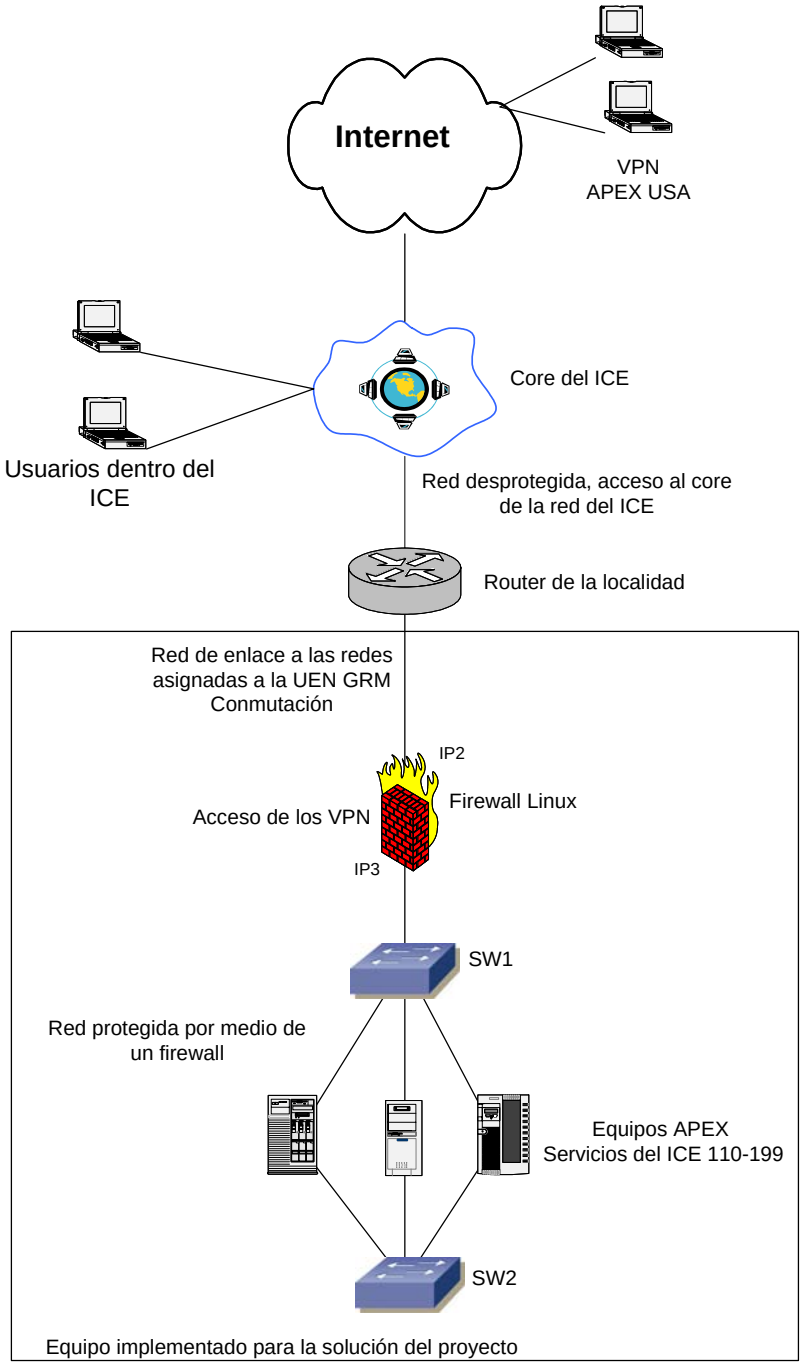

Figura 4 Diagrama de la instalación del firewall en una red existente.

4.3 Requerimientos de la empresa

Para el departamento de conmutación de la UEN de gestión de red y mantenimiento, es indispensable que el firewall tenga la capacidad de enrutar los paquetes provenientes de los usuarios del VPN hacia los equipos APEX, esto para permitir a los proveedores acceder a los equipos remotamente. Sin embargo, este acceso no va a ser constante, sino que va a estar regulado.

Con base en lo anterior, un requerimiento de la empresa es que los firewalls puedan ser configurados para establecer el tiempo de acceso a los servidores APEX, según se acuerde en el departamento de conmutación.

Ésta configuración permite asignar un tiempo establecido a las conexiones de los usuarios del VPN, por lo tanto, si este tiempo se vence la sesión se cierra y se debe solicitar otro periodo de operación, esto es debido a que el departamento de conmutación debe supervisar todas las acciones que se realicen en los equipos APEX comprados.

Además, para el departamento de conmutación en la UEN GRM, es indispensable que la solución planteada sea lo suficientemente efectiva para permitir el acceso a los equipos en las redes protegidas y evitar que los usuarios de los VPN puedan salir a la red institucional del ICE.

Con base en lo anterior, el requerimiento principal de la empresa es separar las plataformas 110 y 199 de la red Institucional ICE y asegurar que sólo clientes autorizados y utilizando protocolos establecidos puedan utilizar los servidores y servicios.

Además es importante el establecimiento de una aplicación capaz de interactuar con el firewall, permitiendo la configuración del equipo de una forma sencilla.

4.4 Solución propuesta

En las localidades de Cartago, Alajuela, Oeste de San José (Pavas), San Pedro y San José centro (Avenida Segunda), existen centrales telefónicas del ICE, en éstas, existe equipo para el manejo de las llamadas con prepago, a estos servicios se les conoce como “110” y “199”.

Estos equipos se encuentran interconectados a la red institucional del ICE por medio de enlaces ethernet, que permiten que los funcionarios del ICE puedan accederlos, sin importar donde se encuentren.

Para la implementación de la solución se procedió de la siguiente forma. Primero, se realizó un análisis de la red y de los equipos a los que se pretende proteger, esto para establecer su funcionamiento y como se intercomunican con los demás equipos de su localidad y de las otras centrales, de esta forma se tiene claro desde el principio los requerimientos del firewall. Ya que es de suma importancia establecer el tipo de tráfico que se presenta en cada red, las direcciones de los usuarios y los puertos que se permite acceder en los equipos de la red protegida.

Por lo tanto, se debe realizar un análisis del software que se utiliza en cada una de estas centrales y de este modo establecer las comunicaciones que se deben permitir y que son de vital importancia para el correcto funcionamiento de los equipos.

Fue importante también, establecer reuniones con los operadores de los equipos, para poder explicar como les va afectar la puesta en marcha de la nueva red, además poder obtener información adicional del modo de operación de estos equipos de telefonía.

Aunque existe una serie de tecnologías que cuentan con las características necesarias para poder implementar un firewall, específicamente los PIX de cisco, el paquete de Netfilter de Linux y licencias de software de Check Point, se desarrolló la implementación de la solución con Linux debido al análisis del apartado 3.2.1, el cual permitió escoger a Linux como la mejor alternativa para este proyecto. Por lo tanto se

procedió a realizar una investigación de las principales características y herramientas de Linux, como herramienta para alcanzar los requerimientos planteados por el departamento de conmutación.

Se propuso como solución la creación de cinco nuevas redes en coordinación con el departamento de tecnologías de la información, el cual, es el encargado de la administración de los servicios de la Intranet, del manejo de toda la red institucional, asignación de redes para tareas específicas, controlar el acceso a Internet, entre otras tareas.

Para la implementación de estas redes se utilizó un enrutador con sistema operativo Linux, en el cual se implementó el estándar de firewall diseñado. Con estos firewalls se controla el tráfico de los equipos APEX, además de que permiten llevar una bitácora de los accesos a los equipos por dirección IP y por protocolo TCP.

Capítulo 5 Procedimiento metodológico

Para alcanzar cado objetivo específico se desarrolló un paso metodológico, así como una serie de tareas necesarias para llevar cada paso a su correcta conclusión.

A continuación se enumeran los pasos metodológicos y sus respectivas tares.

5.1 Seleccionar una tecnología capaz de solventar la problemática en seguridad.

5.1.1 Analizar los principales problemas de seguridad de la red.

5.1.2 Investigar las tecnologías actuales para la implementación en la red.

5.1.3 Analizar las principales plataformas en que se puede desarrollar el proyecto.

5.2 Diseñar las políticas de seguridad que van a ser implementados en los *firewalls*.

5.2.1 Establecer que puertos se pretende mantener cerrados y cuales se podrán abrir.

5.2.2 Establecer que política será utilizada en los *firewalls*.

5.2.3 Realizar con base a la información recolectada el diseño de las listas de acceso.

5.2.4 Diseñar las listas de reglas que van a ser implementadas en la plataforma seleccionada.

5.3 Implementar la topología de las redes seguras con los *firewalls*.

5.3.1 Elaborar el direccionamiento de las redes en conjunto con el departamento de tecnologías de la información.

5.3.2 Establecer cuales deben ser las características físicas de los equipos que se utilizaron como *firewalls*.

5.4 Implementar en los firewalls las reglas diseñadas.

5.4.1 Implementar en cada localidad los *firewalls* necesarios para la solución del proyecto.

5.4.2 Implementar en los equipos las condiciones que se han diseñado para mejorar la seguridad.

5.4.3 Conectar los equipos a la red.

5.5 Elaborar la interfaz entre el administrador y el firewall.

5.5.1 Elaborar la aplicación que genera y elimina usuarios y administradores.

5.5.2 Elaborar una aplicación que permita guardar la información más relevante del equipo en forma de bitácora.

5.5.3 Implementar un sistema capaz de detectar las conexiones con los equipos en la red protegida.

5.5.4 Elaborar un control para los VPN de forma temporizada.

5.6 Realizar un manual de procedimientos de instalación de firewalls.

5.6.1 Consultar con el personal del departamento el formato necesario para el desarrollo del procedimiento.

5.6.2 Elaborar una lista de las principales tareas y responsabilidades que deben tener los técnicos a la hora de implementar un *firewall*.

5.6.3 Elaborar el procedimiento en conjunto con la ingeniera industrial del departamento.

5.1 Reconocimiento y definición del problema

Para poder reconocer el problema y poder definir bien la problemática real que se vivía en la empresa, se necesitaron varios días de consultas y reuniones con el asesor de la empresa, así como entrevistas con los ingenieros del departamento de conmutación de la UEN GRM.

Como se puede ver en las tareas necesarias para realizar el paso metodológico 5.1, se recopiló información acerca de soluciones de problemas anteriores similares a los que se estaba teniendo en ese momento, esto con el fin de verificar cuáles eran las posibles causas de los problemas y cómo poder enfrentarlos.

Una vez que se tuvo planteado el problema claramente, se procedió a elaborar la posible solución a este, basándose en las restricciones que puso la empresa y en las observaciones técnicas que se realizaron, además se seleccionaron las posibles tecnologías que podían solventar la problemática y dar una solución.

5.2 Obtención y análisis de información

Basándose en los pasos metodológicos 5.1 y 5.2 se comenzó una búsqueda de materiales bibliográficos y en Internet, acerca de los principales tópicos del proyecto, es decir, se realizó una búsqueda de teoría de *firewalling*.

Con base en la información recopilada se elaboró un informe comparativo que permite ilustrar el desempeño entre diversas tecnologías presentes en el mercado para la implementación de *firewalls* (ver apartado 3.2.1); luego de analizar la información que se generó y basándose en los criterios propios se seleccionó la implementación de Linux como plataforma para la solución de este problema.

Se escogió Linux debido a:

- Es muy escalable, permite realizarle modificaciones radicales al sistema sin que se afecte la funcionalidad de la red.
- Usa Connection Tracking[14] al igual que los PIX de Cisco y Check Point permite trabajar con el estado de la conexión.
- Su implementación es la más económica como se puede ver en la tabla 2, además Linux puede ser utilizado para solventar más proyectos con que cuenta el departamento.

5.3 Implementación de la solución

Los pasos metodológicos 5.2, 5.3, 5.4 y 5.5 tratan del diseño y la implementación de la solución del proyecto.

Para solucionar el problema planteado se implementó un ambiente de desarrollo, en el cual se contaba con el equipo necesario para poder simular de forma real las características que iba a tener el sistema cuando estuviera en funcionamiento. Entre el equipo utilizado se puede citar un enrutador Cisco, equipos con el sistema operativo Linux SuSE 8.2 y varias PC que actuaban como servidores y clientes.

En la primera fase del diseño se elaboró una serie de diagramas de flujo, los cuales se pueden observar en las figuras 6 y 7; estos diagramas permiten vislumbrar el orden correcto en que se debe revisar las tramas de información que se transmitían por las redes ethernet.

Una vez implementadas estas reglas con base en los diagramas, se procedió a simular las principales formas en que se espera que se intenten abrir conexiones con los equipos protegidos y de este modo observar cómo el sistema responde a esas conexiones.

[14] Ver apéndice A.1

Una vez que se obtuvieron los primeros datos (ver apartado 8.1) se pudo comparar entre el desempeño obtenido con las pruebas y el desempeño esperado, el cual corresponde a los requerimientos de la empresa y el alcance de los objetivos específicos. Una vez que se tuvo información para ver los resultados se pudo ir mejorando el sistema y acercarse cada vez más a la solución esperada.

Cuando se tuvo una solución satisfactoria, que cumpliera con los requisitos del departamento de conmutación, se procedió a implementar un manual de procedimiento para la puesta en marcha de los firewalls adicionales por parte de los técnicos del departamento de conmutación. Este procediendo fue revisado por la ingeniera industrial del departamento de conmutación.

El punto 5.6 permite desarrollar un manual de procedimientos que permite implemetar *firewalls* por parte de los tecnicos del departamento de conmutacion del ICE.

5.4 Reevaluación y rediseño

Como se explicó en capítulos anteriores, una solución completa de seguridad en redes no abarca solamente la implementación de un *firewall* como mecanismo de filtrado. Se debe tener claro que para proteger la integridad de los equipos que están dentro de una red se debe tener toda una política de seguridad bien establecida.

Basándose en modelos como el "Modelo OSI" o el "Modelo TCP/IP" (ver figura 5)[15] se puede realizar un análisis por capas, y de este modo visualizar los principales problemas que se presentan en una red y así mejorar la seguridad de forma modular, se debe poner especial atención a las capas 2 y 3 del modelo OSI.

El modelo OSI es el más utilizado ya que se encuentra mejor distribuido en capas independientes unas de otras, esto permite analizar de un modo más sistemático los posibles puntos de falla, este modelo se va a utilizar para exponer las posibles mejoras al proyecto.

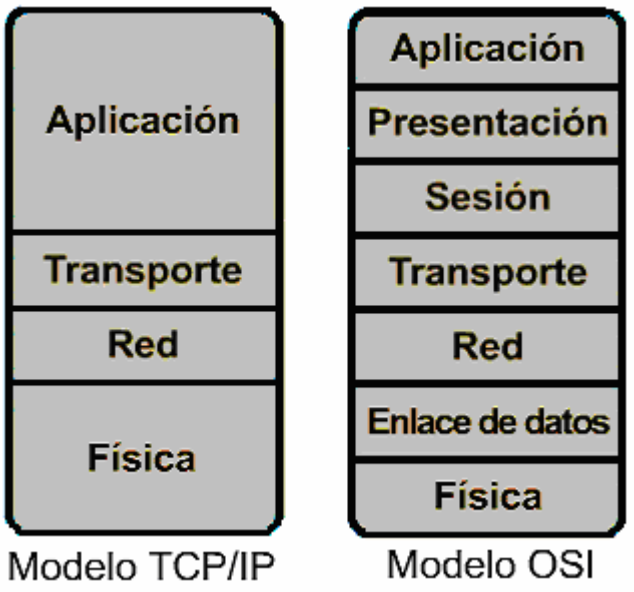

Figura 5 Modelos de referencia para la transferencia de información

[15] Referencias a los modelos OSI y TCP/IP http://www.uwsg.iu.edu/usail/network/nfs/network_layers.html
http://www2.rad.com/networks/1994/osi/layers.htm

La primera forma en que se puede mejorar este proyecto es basándose en la capa 3 del modelo OSI, la cual tiene que ver con el direccionamiento IP.

En este punto se recomienda un reacomodo de los usuarios, los administradores y los equipos, es decir realizar un mejor direccionamiento IP en la red actual. Para lo cual, se podría implementar subredes, en las cuales se tenga bien definida la finalidad de las mismas.

Logrando esta separación se puede tratar a los usuarios como un conjunto de direcciones o una subred a la cual se le puede aplicar reglas específicas, y los equipos se pueden tratar como otras subredes y no como direcciones IP únicas. Esto permite que el flujo de información por las reglas del *firewall* sea más eficiente, ya que se puede verificar por conjuntos de usuarios y no por dirección IP individuales, de este modo reducir el número de reglas con que cuenta el equipo y por lo tanto mejorar el tiempo de procesamiento del *firewal*l.

Otra forma de mejorar el proyecto es realizando una política de seguridad de capa 2, es decir, configurar los *switches* para controlar el acceso de usuarios a la red institucional del ICE.

Esto se puede lograr asignado las direcciones MAC de los equipos a puertos específicos de los *switches* y realizar una acción correctiva cuando un dispositivo con una dirección MAC diferente a la configurada es conectado a un puerto, como por ejemplo, bloquear el trafico de información, o generar una alarma. Esto es de suma importancia ya que en la actualidad cualquier persona que ingresa a la institución puede conectarse a un *switch* y acceder a todos los recursos de la red, solamente conociendo una dirección IP.

La mejor forma de proceder en la solución de esta problemática es generar las subredes donde se separe en usuarios, administradores y equipos, y una vez que se tiene esta distinción se puede proceder a configurar los *switches* para limitar el acceso de usuarios inválidos a la red institucional, de este modo evitar que los cambios de direcciones IP en los equipos puedan afectar las reglas del *firewall*.

Basándose en lo anterior, una mejor solución de seguridad afecta muchos aspectos como el direccionamiento y la configuración apropiada de los equipos de

red, por lo tanto se debe tener claro que para mejorar una red de tan grandes dimensiones como la que tiene el ICE se debe hacer un rediseño de la red, en el cual se tome en cuenta el direccionamiento de los equipos y los usuarios, y de esta forma solucionar un problema que puede ser muy peligroso.

Otra forma en que se puede mejorar el presente proyecto es implementar un servidor que permita el manejo de forma centralizada de todos los *firewalls,* de este modo, solamente se debe cambiar la información de un usuario o un protocolo en un único equipo y esta información va a tener validez en todos los equipos de seguridad, ya que se puede elaborar una rutina que actualice la información de cada *firewall* si se da un cambio en los datos del servidor. Esta solución evita que el administrador de red deba cambiar el perfil de un usuario en cada *firewall* existente y de este modo se elimina trabajo innecesario y posibles incongruencias en la información de cada *firewall*.

Capítulo 6 Descripción del hardware del sistema

El hardware de cada firewall consiste de un equipo de computación, el cual debe estar en capacidad de controlar más de una tarjeta de red (por lo general dos), además de soportar el sistema operativo Linux SuSE 8.2 y un disco duro con suficiente espacio libre para poder almacenar la información que genera el equipo durante su operación normal.

Otro punto que se debe tomar en cuenta es que el procesador debe estar en capacidad de manipular la información del enrutamiento, el filtrado y la información que se guarda de las sesiones que se establecen y de las que son descartadas.

Las tarjetas de red deben permitir la operación a 10/100 Mbps, ya que estas son las velocidades normales de operación de la red del ICE; sin embargo se puede tomar en cuenta que el *core* del ICE es de 1Gbps, esto si se desea escalabilidad en la solución. Otro punto relevante es que las tarjetas deben permitir la transmisión de información por medio de Ethernet.

Es importante tomar en cuenta que con una computadora se puede procesar cantidades considerables de información si se tiene los recursos necesarios como lo expone check point[16], ya que la solución que plantea, indica que si una computadora cuenta con 1 GB de memoria y se utiliza Linux con un procesador Dual Xeon 2.2 GHz se puede soportar 1.500.000 conexiones de firewall concurrentes, también con esa cantidad de memoria se puede manejar hasta 40.000 tuneles VPN.

Sin embargo realizando un pequeño análisis se muestra que esos números son teóricos y no pueden ser alcanzados con los anchos de banda de los enlaces normales ethernet, ya que estos se verán limitados antes de alcanzar un número tan grande de conexiones simultaneas. Por ejemplo si un túnel requiere 10kbps para

[16] VPN-1/FireWall-1 **Resumen de desempeño. (“Performance brief”)** **www.checkpoint.com**

funcionar, 10.000 túneles necesitarán 100Mbps del ancho de banda de la red, consumiendo de este modo todos los recursos de un enlace ethernet IEEE 802.3.

Aunque estos números no pueden ser alcanzados, sirven para indicar que mientras mejor sea las capacidades de los equipos en que se instalan los *firewall* Linux, también se verá mejorada la velocidad de procesamiento, disminuyendo de este modo la latencia que puede inducir el firewall a la hora de procesar información.

Capítulo 7 Descripción del software del sistema

Se comenzó con la configuración del kernel versión 2.4.20 para que la PC pueda realizar funciones de *firewall* y enrutador al mismo tiempo. Por este motivo se necesito cargar los módulos de operación necesarios para el correcto funcionamiento de los IPTABLES, así mismo habilitar el IP Forwarding, el cual permite que la computadora pueda realizar el enrutamiento de paquetes entre sus interfaces de red.

Para la implementación de la solución fue de gran utilidad el uso de "scripts" en BASH shell, el cual es un interprete del sistema operativo que configura el kernel vía comandos y realiza la manipulación del hardware del sistema, además de permitir la implementación de aplicaciones capaces de detectar el tipo de tráfico presente en la red y poder tomar control sobre el mismo. En este proyecto todos los archivos implementados están basados en BASH Shell.

Se generó un archivo ejecutable (rc.fire)[17], que permite implementar el enrutador y el *firewall*, además, en éste se encuentran las reglas (IPTABLES) básicas para que se pueda inicializar el *firewall*.

En este archivo, sólo existe habilitada una dirección de administración del *firewall*. Esta es la dirección del primer administrador, el cual puede crear los demás usuarios y administradores por medio de otro archivo ejecutable (fireManager)[18].

Este archivo ejecutable es una interfaz entre el administrador y el archivo que contiene la información de las reglas (rc.fire), ya que al administrador solamente debe utilizar la aplicación "fireManager" para poder ingresar reglas que habilitan o deshabilitan a los usuarios y a los protocolos, el "fireManager" puede ser analizado en el desarrollo del apartado 8.1.1.

Cuando el equipo está en funcionamiento se crea otro archivo de lectura (firewall.log), éste permite guardar la información de cuales usuarios han tratado de

[17] El listado de reglas se encuentra en el Apéndice A.3.
[18] El análisis del sistema fireManager se encuentra en el apartado 8.1.1.

ingresar a la red protegida, por cuales puertos trataron de hacerlo y cuando terminó la conexión.

El sistema puede ser accesado de forma remota, sin embargo él protege todos sus archivos de posibles alteraciones estableciendo sólo una pocas direcciones IP como administradores; además cada administrador solamente puede utilizar SSH para configurar el firewall. Este protocolo permite establecer contraseñas encriptadas para mejorar la seguridad en el equipo.

7.1 Explicación del diseño

7.1.1 Inicialización del sistema

Primero se debe cargar el módulo de iptables, el cual es el más importante, ya que sin éste, no se puede realizar ningún tipo de filtrado, NAT o mangle.

- /sbin/modprobe ip_tables

En este proyecto se utiliza ampliamente el análisis del estado de la comunicación, es decir, se verifica si los paquetes que pasan por el equipo están abriendo comunicaciones, o estas ya están establecidas, para lo cual, se requiere el módulo de connection tracking.

- /sbin/modprobe ip_conntrack

Como se explicó antes, en el *firewall* se utiliza el análisis del estado de la comunicación, por lo tanto al usar FTP se presenta un problema con el módulo de connection tracking, ya que FTP funciona pasando información por dos puertos distintos, el 20 y el 21, por lo tanto se requiere implementar un nuevo estado denominado RELATED, el cual permite el flujo de paquetes que son producto de

comunicaciones ya establecidas. Para implementar esto se requiere el módulo de connection tracking para FTP.

- /sbin/modprobe ip_conntrack_ftp

Para poder generar las reglas que van a ser aplicadas en la tabla de filtrado se debe implementar el módulo de iptables_filter, el cual permite que se pueda implementar reglas para cada cadena (ENTRADA,SALIDA y FORWARD), habilitando este módulo la máquina funciona como un firewall.

- /sbin/modprobe iptable_filter

Otra característica interesante y muy útil es la capacidad de poder crear logs cuando un paquete coincide con una regla. Esto permite que se pueda estar analizando en tiempo real, cuando un paquete entra o sale del equipo, además de su información más relevante, para esto se carga el módulo ipt_LOG.

- /sbin/modprobe ipt_LOG

Para poder crear un enrutador con el *firewall*, se debe permitir que éste tenga la capacidad de enrutar los paquetes entre sus interfaces de red, para lo cual se debe habilitar el IP FORWARDING, por este motivo se debe variar la información contenida en el archivo ip_forward, con la siguiente instrucción.

- echo "1" > /proc/sys/net/ipv4/ip_forward

7.1.2 Diseño de las reglas de filtrado

A la hora de diseñar un equipo de filtrado como un firewall, se debe realizar un análisis de la información que no cumple ninguna de las reglas.

Existen dos formas para proceder, la primera es ir cerrando los puertos uno a uno y eliminando direcciones, el resto de paquetes que no cumplen caen en un aceptar por defecto.

La otra forma de proceder es a la inversa, ir aceptando los usuarios permitidos y los puertos validos, y todo lo demás se debe desechar, es decir un desechar por defecto.

En este proyecto se escogió la segunda opción, la cual permite mayor seguridad, sin embargo es más difícil de implementar, ya que si las reglas no están bien definidas el sistema no funcionará correctamente, eliminando información importante y útil. Por lo tanto para proceder con la solución se realizaron diagramas de flujo[19] para plantear de una forma clara el orden de las reglas que permiten el tráfico de la información relevante para la operación normal de los equipos.

Para proceder a crear las reglas se debe conocer cual es la ruta que los paquetes van a seguir en la red, es decir se debe saber cuál es la dirección de origen y cual es la dirección destino de los mismos, esto para saber si los paquetes van dirigidos al firewall, son generados por éste o van de una red a otra.

[19] Ver figuras 6 y 7

Esto permite implementar reglas en las tres cadenas básicas de la tabla de filtrado. Ver apartado 3.2.2.

Entrada: Los paquetes llevan como dirección de destino alguna de las interfaces de red del firewall.

Salida: El firewall establece comunicaciones con otros equipos.

Forward: Los paquetes van a pasar por el firewall de una interfaz de red a otra.

Para la implementación de cada cadena se utilizaron los diagramas de flujo de las figuras 6 y 7 para visualizar la ruta que van a seguir los paquetes cuando están siendo revisados.

.

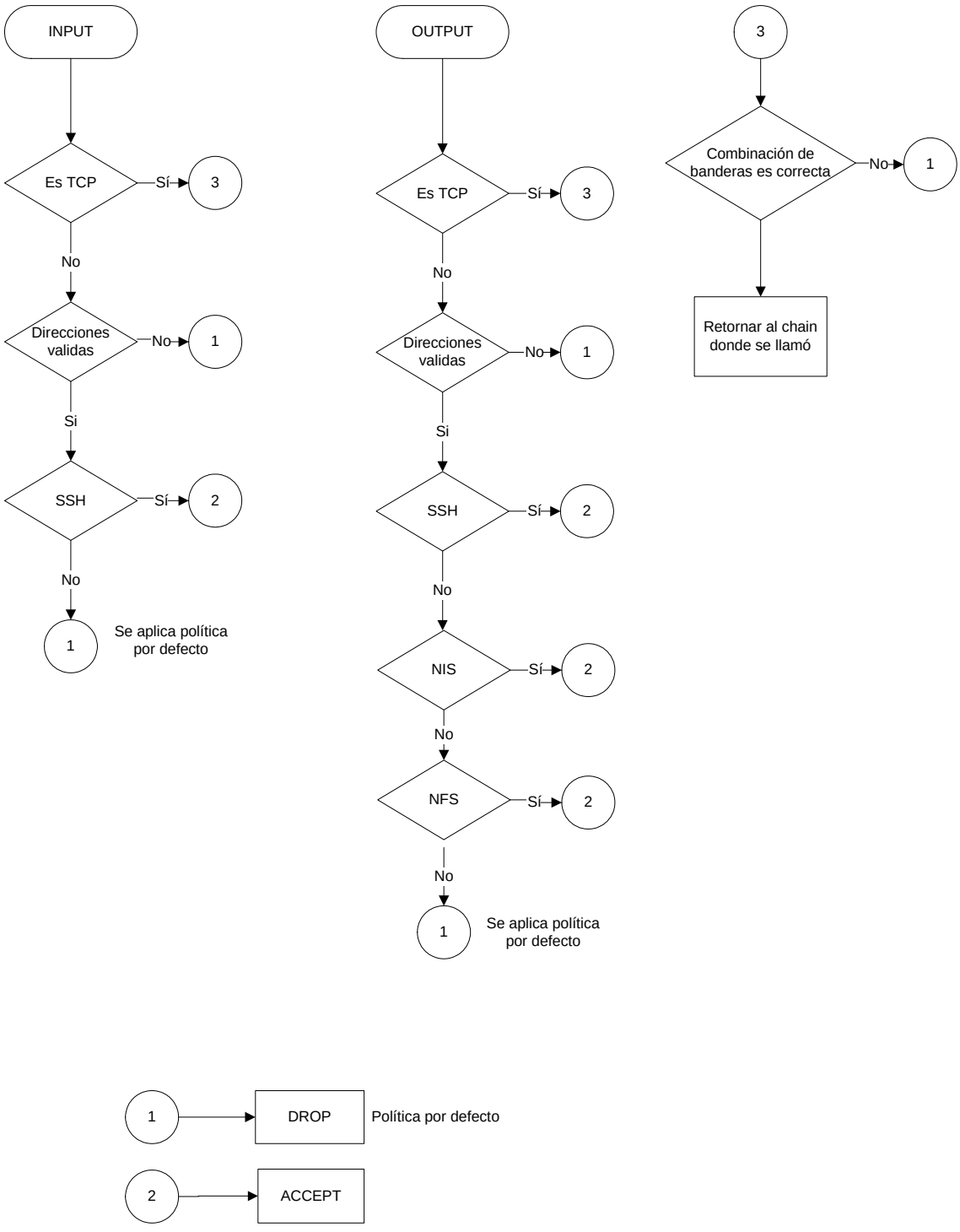

Figura 6 Diagrama de flujo de las cadenas de entrada y salida.

En la figura 6 se puede observar el orden en que se aplican las reglas de filtrado a los paquetes que ingresan al firewall o salen de él. Primeramente se verifica en ambas cadenas si los paquetes son TCP. Si lo son, serán verificados para corroborar que el orden de sus banderas es el correcto y de este modo poder eliminar paquetes que puedan causar problemas de ataques al firewall. Cualquier otro protocolo IP será desechado (UDP, ICMP) ya que este equipo solamente se podrá acceder por medio de SSH, el cual funciona sobre TCP en el puerto 22.

El sistema requiere de protección para evitar que usuarios no deseados puedan acceder al equipo para tratar de administrarlo, por lo tanto para evitar que cualquier usuario pueda ingresar al *firewall* se elaboró una lista de acceso (ver figura 6, direcciones validas), la cual verifica la dirección fuente de los paquetes TCP que le llegan y compara para verificar si es una dirección válida; de lo contrario el paquete es descartado y no se le envía ningún tipo de respuesta, como se puede ver en la cadena de salida “OUTPUT”, en la figura 6.

En la cadena de salida se pretende que cada firewall solamente se pueda comunicar con otros firewall que protegen equipos APEX, para lo cual se desarrollaron otras listas de acceso (direcciones validas) que solamente afectan esta cadena, las cuales permiten que cuando una dirección es válida se le habiliten protocolos para que pueda acceder a estos otros firewall o servidores NIS o NFS.

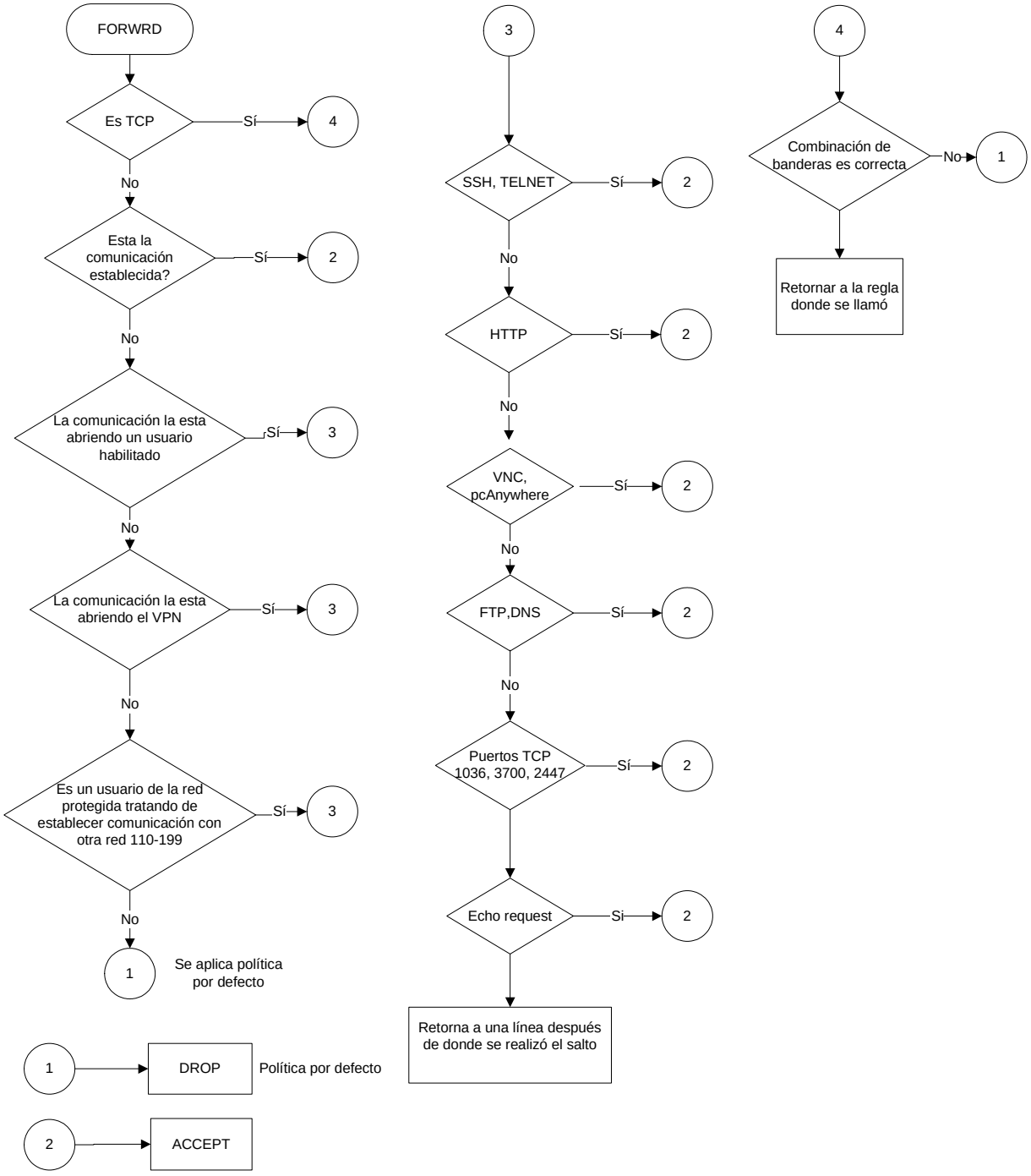

Figura 7 Diagrama de flujo de la cadena de forward

El diagrama de la figura 7 representa el flujo de los paquetes a través del firewall cuando van a ser enrutados por este equipo. Este diagrama es el más importante ya que permite a los usuarios establecidos comunicarse con la red segura y además establecer cuales protocolos van a ser los habilitados para hacerlo.

En la cadena de *forward* se estableció la inspección de los paquetes para revisar las direcciones fuentes y las direcciones destino, de este modo verificar si los paquetes vienen de usuarios habilitados o no.

Por lo tanto, se permite a los usuarios cuya dirección IP ha sido validada, utilizar los protocolos preestablecidos para poder tener acceso a los servidores APEX del servicio 110-199.

Además se verifica si la dirección corresponde a la de usuarios habilitados para ingresar por medio del VPN y poder tomar acciones que se les aplica solamente a éstos, como el control por tiempo, guardar todas las acciones que realizan y verificar el tipo de protocolos que están utilizando. Esto se puede realizar por medio de la opción de generar mensajes con IPTABLES y del CRON[20] que permite realizar tareas programadas y cronometradas.

7.1.3 Administración del f*irewall*

Una vez que se tuvo establecido cuales eran las reglas que debían ser implementadas para poder eliminar el tráfico innecesario y peligroso en la red protegida y en el *firewall* mismo, se elaboró una aplicación que estuviera en capacidad de controlar las reglas del *firewall*, esto con el fin de que las personas encargadas de la administración de la red no deban conocer a fondo la teoría de la solución y solo puedan utilizarla.

Esta aplicación que se elaboró se basó en la generación y eliminación de reglas, además se encarga de colocarlas en el lugar justo para que no interfiera con el flujo normal de la revisión de los paquetes.

[20] Ver apéndice A.1

Además, se elaboró un detector de conexiones en tiempo real para las comunicaciones sobre TCP (no se aceptan comunicaciones sobre UDP ni ICMP), el cual requiere de la utilización de la teoría de "*Three way handshake*" (ver figura 8), y que funciona de la siguiente manera:

Primeramente, cuando se detecta un paquete con la bandera de SYN activa se guarda la información de los puertos TCP y las direcciones IP y se establece la conexión como en proceso de conexión.

Seguidamente, cuando se recibe un paquete ACK SYN por parte del servidor, se compara la información de éste con las conexiones establecidas como en proceso de conexión del paso previo, si los datos calzan se guarda los datos y se establece la conexión como en proceso de establecimiento.

Finalmente, cuando se recibe un paquete ACK por parte del equipo que intenta abrir la conexión, se comparan los datos TCP e IP para verificar si corresponden a alguna conexión en estado de establecimiento, de ser así se establece la conexión como abierta, y se procede a desplegar en pantalla la información relevante de las capas de red y de transporte de la conexión, respectivamente las direcciones IP que intervienen y los puertos relacionados en la comunicación.

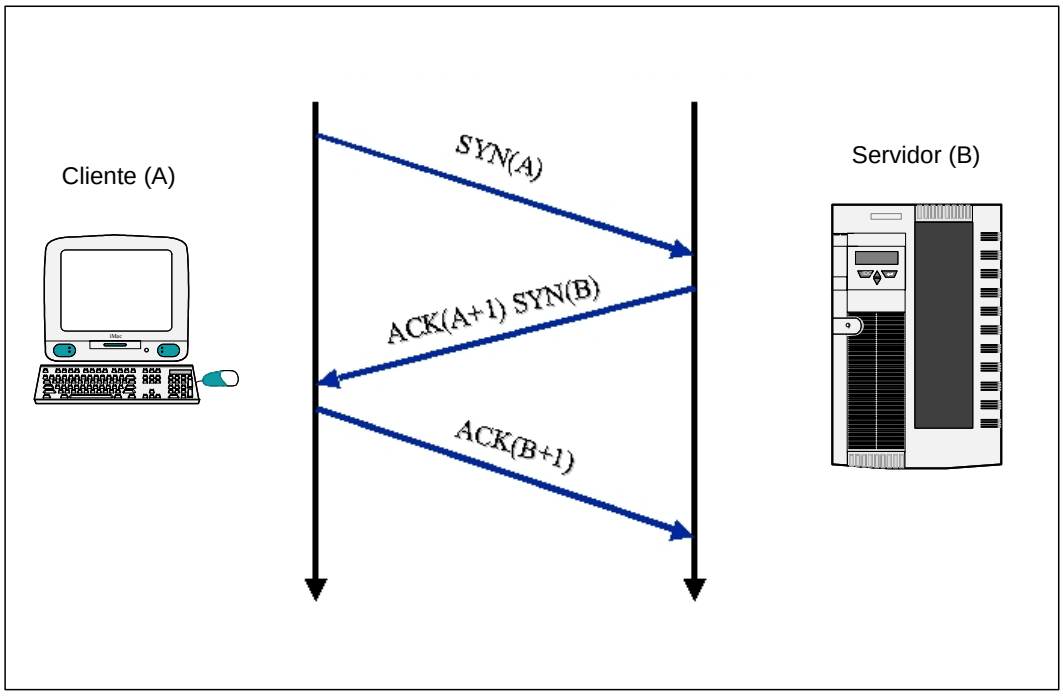

Figura 8 Forma en que se abre una conexión TCP (Three way Handshake).

Posteriormente, se procedió a implementar las reglas que registran los paquetes encargados de terminar las conexiones, para lo cual se buscó en la información que enruta el firewall los paquetes que lleven una combinación de banderas RST ACK y FIN ACK, ya que estos son los dos métodos que usa TCP para dar por finalizada una conexión. La primera es por *reset* y se produce cuando el servidor necesita cerrar la comunicación de forma inmediata y la segunda es porque el usuario terminó de forma correcta la sesión.

Estas dos formas de terminar las sesiones funcionan como el “three way handshake”, ya que se establece un intercambio de información entre el cliente y el servidor para poder terminar la sesión. Por lo tanto, con la generación de mensajes de tipo “LOG” se pudo analizar cuando una sesión se cierra de igual forma que como se implementó para detectar cuando se abre una conexión.

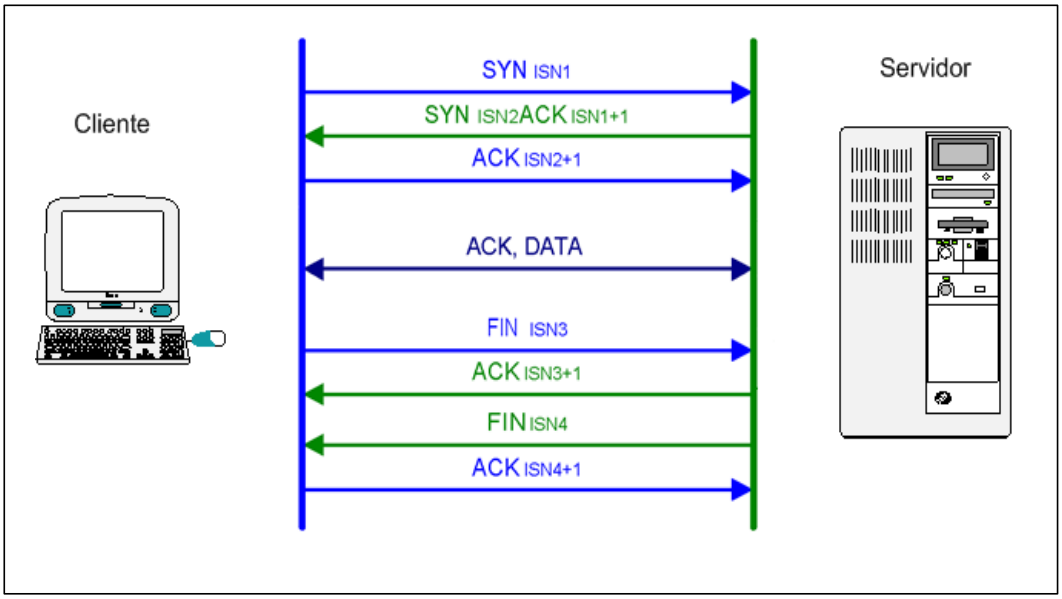

Figura 9 Comunicación por TCP (Inicio, transferencia y finalización)

Como se puede observar en la figura 9, existe un intercambio de información entre el cliente y el servidor para cerrar una sesión, en la figura se muestra la transferencia con la bandera de FIN, pero es igual para RST.

Con toda esta información se puede definir cuales usuarios están estableciendo conexiones y sobre cuales puertos lo están haciendo, permitiéndole al administrador un mejor control del tráfico en la red protegida; además puede ver en que momento se están realizando conexiones por medio del VPN.

Capítulo 8 Análisis y resultados

Nota importante:

En este punto se debe realizar una aclaración para la utilización de los datos de las redes protegidas y de los equipos de los servicios 110 y 199.

Muchas figuras contienen información que solamente es de uso específico del Instituto Costarricense de Electricidad, por lo tanto algunos de los datos de las figuras han sido eliminados o alterados para que no puedan ser vistos o relacionados con la realidad por el lector del presente proyecto, esto debido a la confidencialidad de la información. Entre los datos que han sido suprimidos se encuentra el direccionamiento IP de los usuarios, el nombre de los funcionarios y las dependencias para las que laboran.

Por lo tanto se solicita discreción por parte del lector.

8.1 Análisis y resultados

El Instituto Costarricense de Electricidad tiene un desarrollo enorme en el área de las telecomunicaciones, este crecimiento ha sido tan esporádico que no se ha tratado de analizar los cambios que se pretenden realizar y diseñar una solución a largo plazo para la situación de la institución.

Con base en lo anterior, el departamento de conmutación planteo el problema de la carencia de protección en los equipos que esta dependencia maneja, así como un problema de falta de orden en las redes que controlan los equipos. Éste fue el problema inicial que se encontró al momento de iniciar el proyecto.

Una vez que se pudo iniciar con el proyecto se propuso desde el inicio la implementación de cinco nuevas redes que fueran completamente independientes de las que ya existían y pudieran estar protegidas con el *firewall* como se observa en la figura 10.

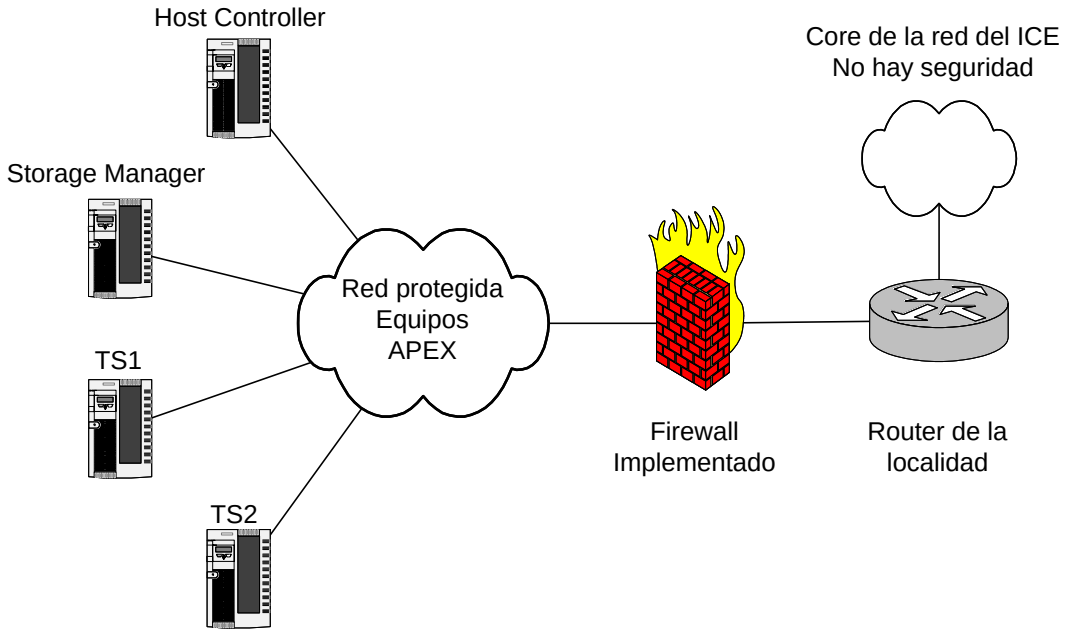

Figura 10 Situación actual de las redes APEX de los servicios 110 y 199.

Cuando se planteó el proyecto se realizó un análisis de los problemas en la red, para lo cual se obtuvieron los datos de un servidor NIS y NFS en una red insegura, los cuales pueden observarse en las figuras 11 y 12. Las gráficas de problemas presentes en la red fueron tomadas por medio del software NESSUS, que es un software de inspección de puertos y problemas de redes en sistemas operativos.

Es importante destacar que en la figura 11 solamente están especificados los problemas más graves; pero existen más problemas de menor peligrosidad que se puede ver en la figura 12.

En la figura 11 se ilustra la cantidad de problemas por tipo de protocolo que afectar la funcionalidad del sistema.

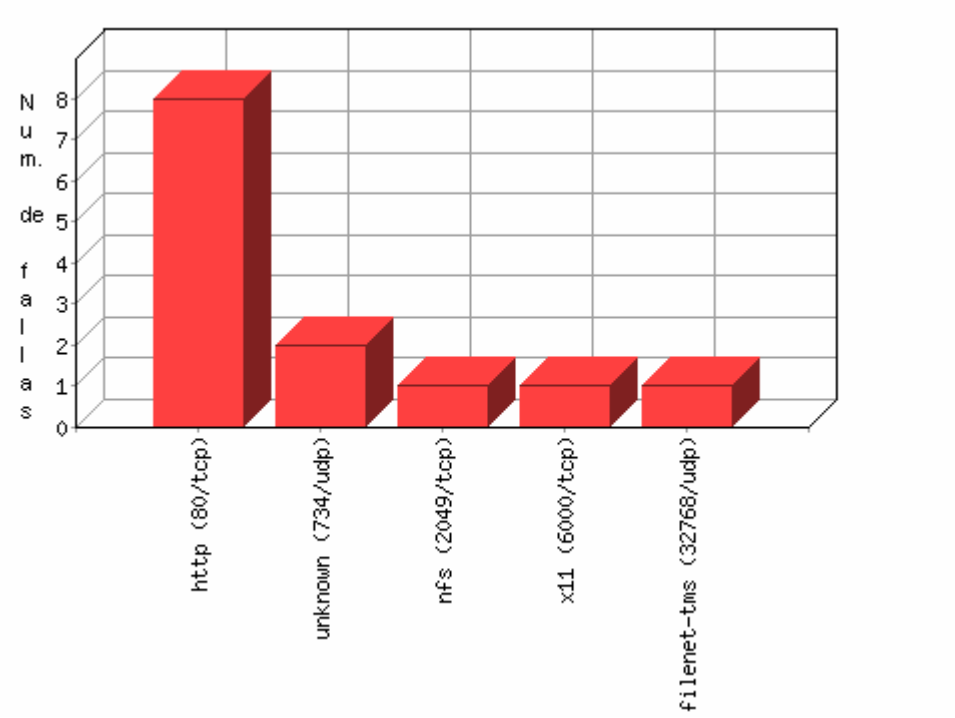

Figura 11 Diagrama de los problemas peligrosos por puerto en un servidor NIS.

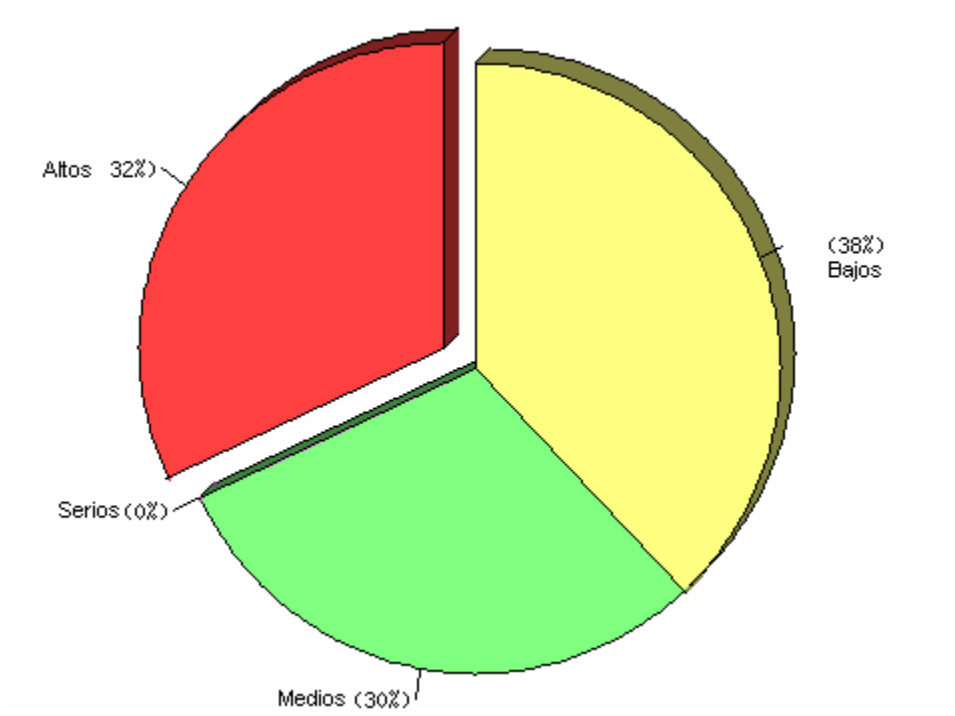

Figura 12 Nivel de problemas de seguridad de un servidor NIS.

En la figura 11 se puede observar como al analizar un equipo, se descubre la situación actual de éste y además averiguar cuales son las posibles debilidades que se puede atacar, en este caso se pueden enumerar los puertos 80 (http), 734, 2049 (NFS), 6000 (X11), 32768 (filenet) entre otros.

Inclusive con NetworkView[21] se puede obtener información del sistema de una forma muy simple, simplemente realizando pruebas con SNMP se puede tener información como el sistema operativo, la dirección MAC, la dirección IP y datos de los NetBIOS entre otros. Como se puede apreciar en la figura 13 la red inspeccionada no se encuentra protegida.

Realizando una inspección desde un equipo habilitado a una red segura se pudo obtener la figura 14, en la cual se puede observar como los equipos protegidos pueden ser detectados, sin embargo no se puede averiguar la información de los sistemas, ya que existe un bloqueo en el *firewall* del puerto en que opera SNMP.

Al colocar los sistemas que deben tener puertos abiertos para transferir información detrás de un *firewall* se evita totalmente los accesos indeseados al equipo, inclusive se pudo evitar que el software NESSUS pudiera analizar los equipos protegidos si se aplica desde una dirección no habilitada, ya que al no poder detectar los equipos en la red, asume que el equipo no existe y no realiza un análisis.

Esto es el resultado que se pretendía obtener al principio del proyecto, poder seleccionar entre los usuarios habilitados y los que no lo eran.

[21] Ver apéndice A.1 “Software utilizado”

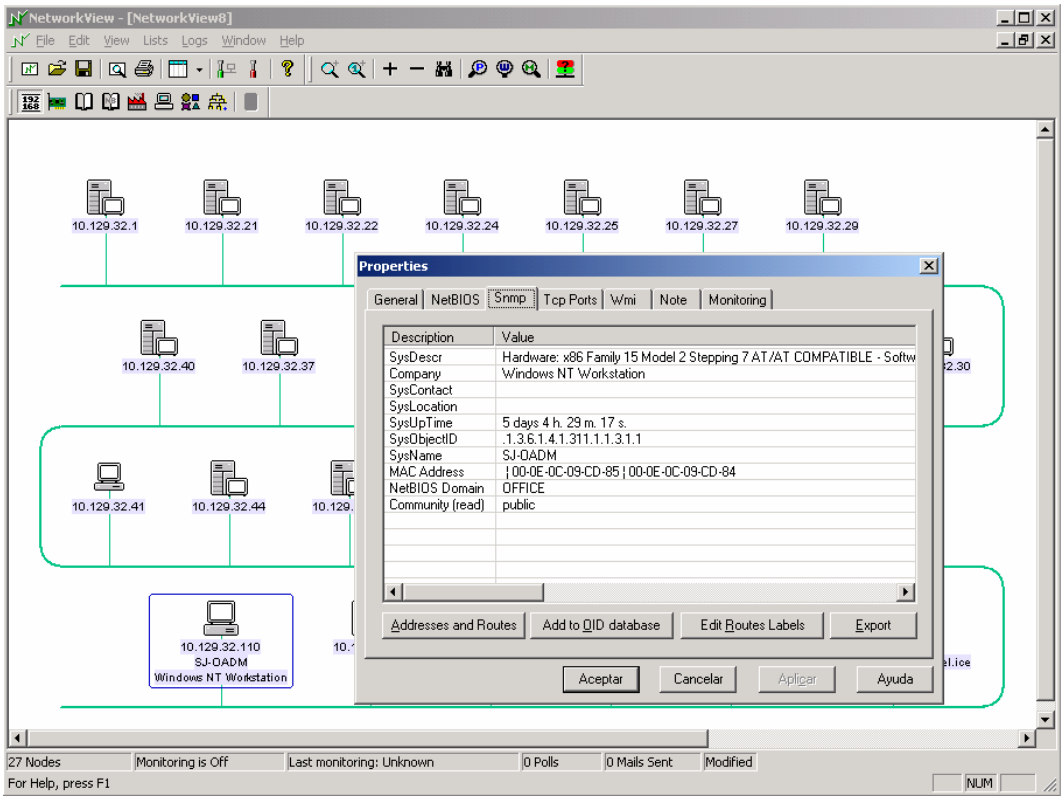

Figura 13 Inspección de red desprotegida con NetworkView.

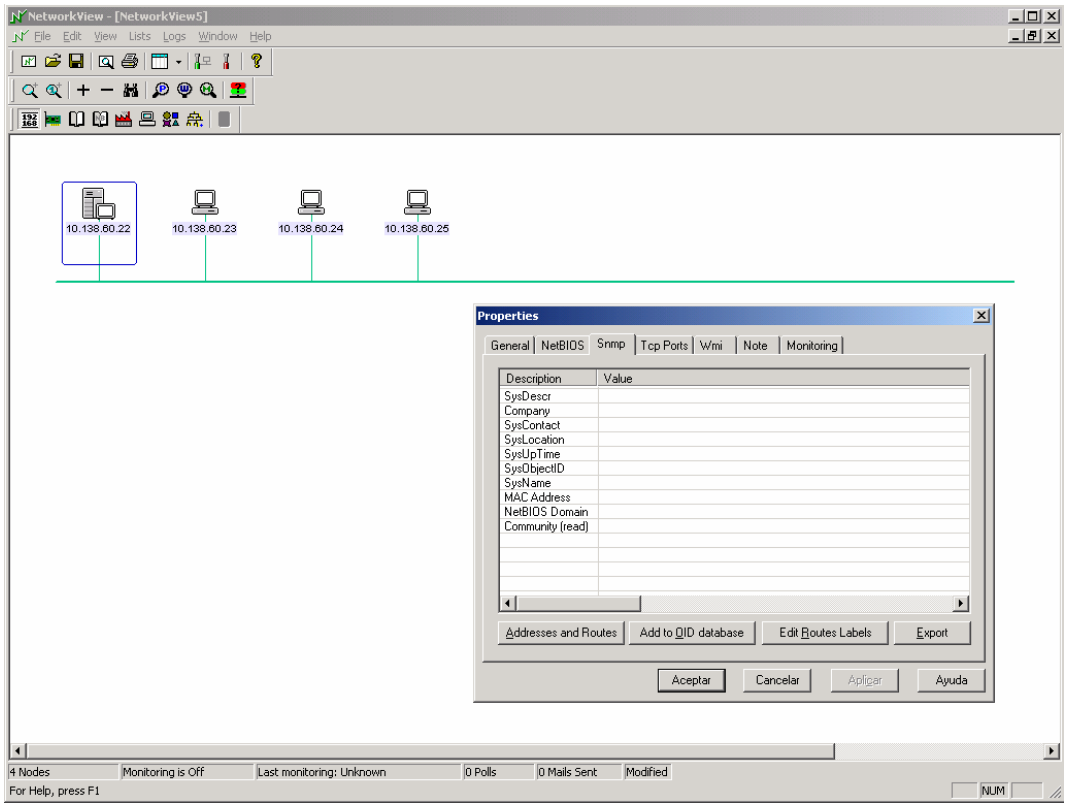

Figura 14 Inspección de red segura con NetworkView.

La solución que se planteó inicialmente permite seleccionar equipos por direcciones IP fuente, lo cual, permite separarlos en grupos de administradores (utilizan el *firewall*), usuarios (pasan a través del *firewall*), usuarios no válidos (no puedan utilizar ningún recurso de la red). Esta división le asigna diferentes características o perfiles a cada uno, por ejemplo un administrador no puede ver la red protegida, pero tiene libre acceso al *firewall* por medio de SSH, el usuario válido puede usar los recursos de la red protegida que el administrador desee, y el resto de las direcciones no pueden ni siquiera detectar la red protegida, ni el equipo de protección. El *firewall* se protege de posibles revisiones de la red no respondiendo a ninguna petición de ICMP, por lo cual no se puede detectar el direccionamiento del equipo.

Por ejemplo, la figura 15 muestra como un usuario habilitado que utiliza el NetworkView para revisar una red segura puede detectar los equipos que se

encuentran en la misma, pero no puede detectar el *firewall*, esto se logró mediante la implementación de reglas que impiden el acceso por medio del protocolo ICMP y además cerrando todos los puertos de UDP y TCP al equipo para direcciones diferentes a la de un administrador.

Esto es de suma importancia, ya que si no se realiza de este modo, cualquier usuario malicioso podría detectar el equipo y tratar de acceder al mismo para eliminar la seguridad y permitir el acceso a cualquier dirección, lo cual se pretende que no sea posible, inclusive al realizar un análisis con “tracert” no se puede obtener la información del equipo como se puede observar en la figura 16.

En la prueba con “tracert” se pudo observar como todos los equipos que enrutan la información para que esta llegue al equipo 10.149.36.22 responden con su dirección IP; sin embargo el *firewall* no responde a la prueba, lo cual es un resultado satisfactorio para el proyecto ya que se mantiene el equipo oculto para cualquier tipo de usuario. En la figura 17 se puede observar como el *firewall* no permite las conexiones a un equipo protegido cuando la dirección fuente no es valida.

Los resultados que se obtuvo con NESSUS son bastante satisfactorios ya que se pudo demostrar que el sistema es capaz de sobreponerse a una revisión que cuanta con ataques como DoS[22] o ping of death, entre muchos más. El sistema es capaz de mantenerse completamente oculto si la dirección fuente no es de un administrador.

[22] Ver Apéndice A.1

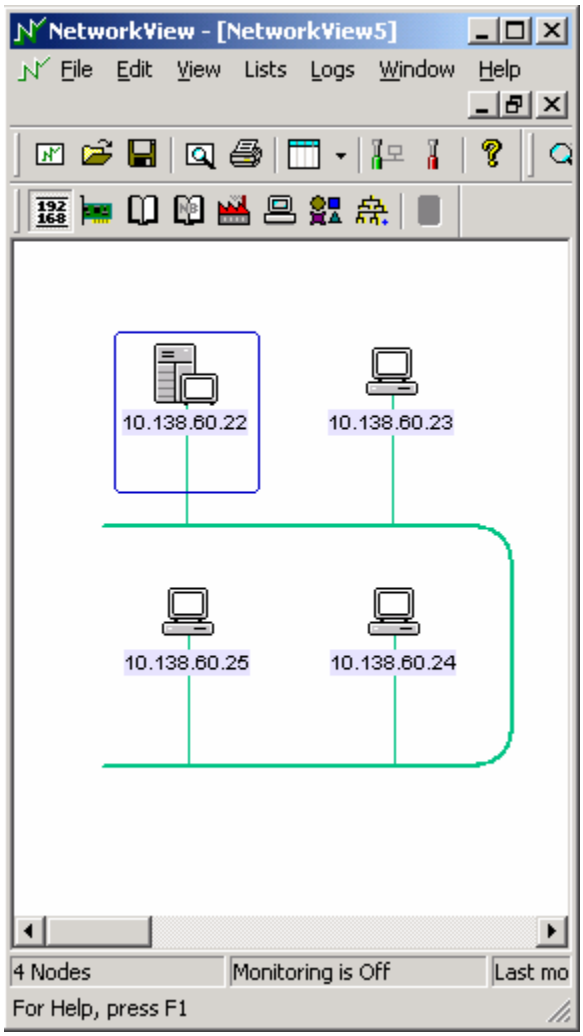

Figura 15 Usuario válido revisando una red protegida.

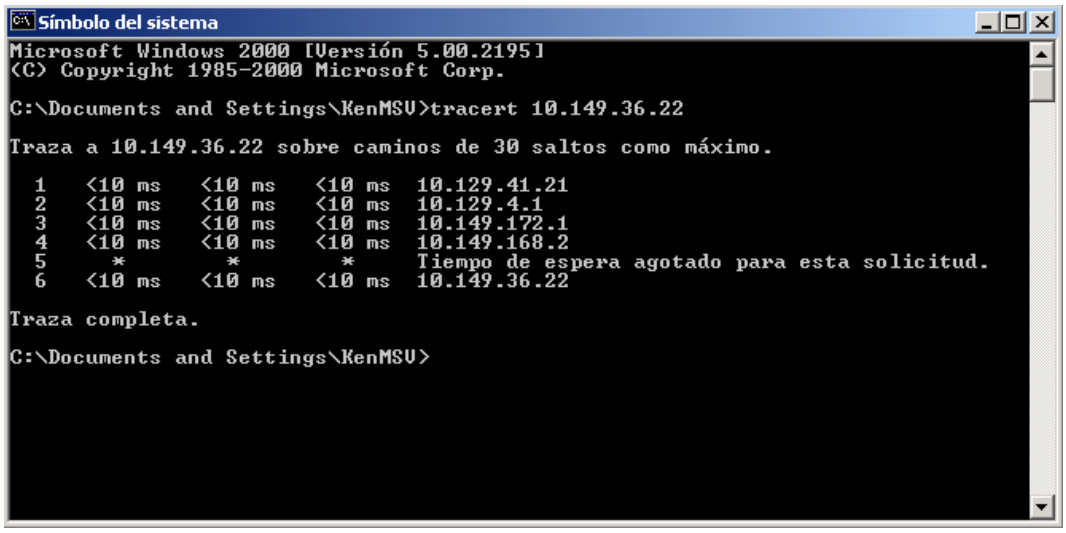

Figura 16 Usuario válido probando el sistema con “TRACERT”.

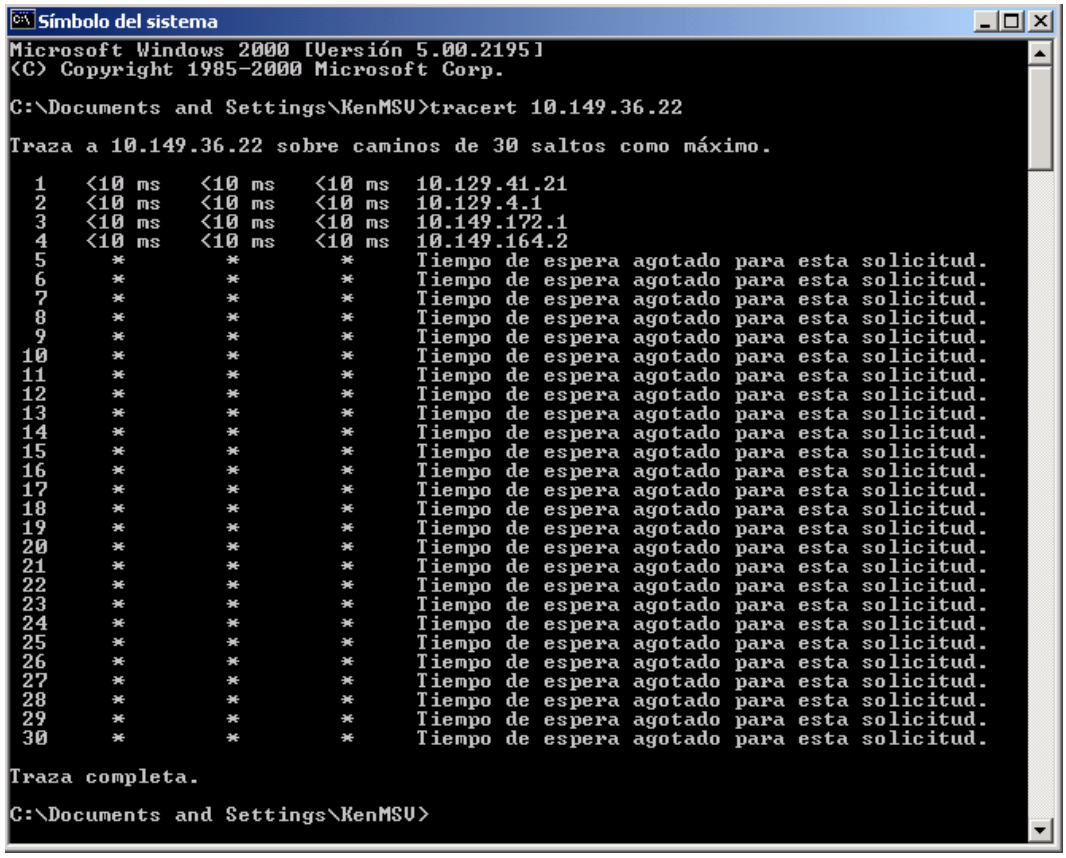

Figura 17 Usuario no válido probando el sistema con “TRACERT”.

8.1.1 Sistema funcional

La parte principal de la administración del equipo de firewall y de sus reglas es una aplicación desarrollada en Bash Shell que se denomina fireManager, la cual permite una mejor operabilidad del equipo ya que fue desarrollada para permitir la administración de forma más amigable y sencilla.

En la figura 18 se puede observar la interfaz entre el administrador y el firewall de San Pedro, la cual se encarga de agregar y eliminar usuarios, ingresar o eliminar protocolos, visualizar los últimos cambios que se le hizo al sistema, desplegar la información actual del sistema, habilitar el acceso de usuarios por medio de un VPN (suplidores de los equipos APEX), mostrar la información más relevante de los accesos recientes y desplegar el estado de las ultimas conexiones.

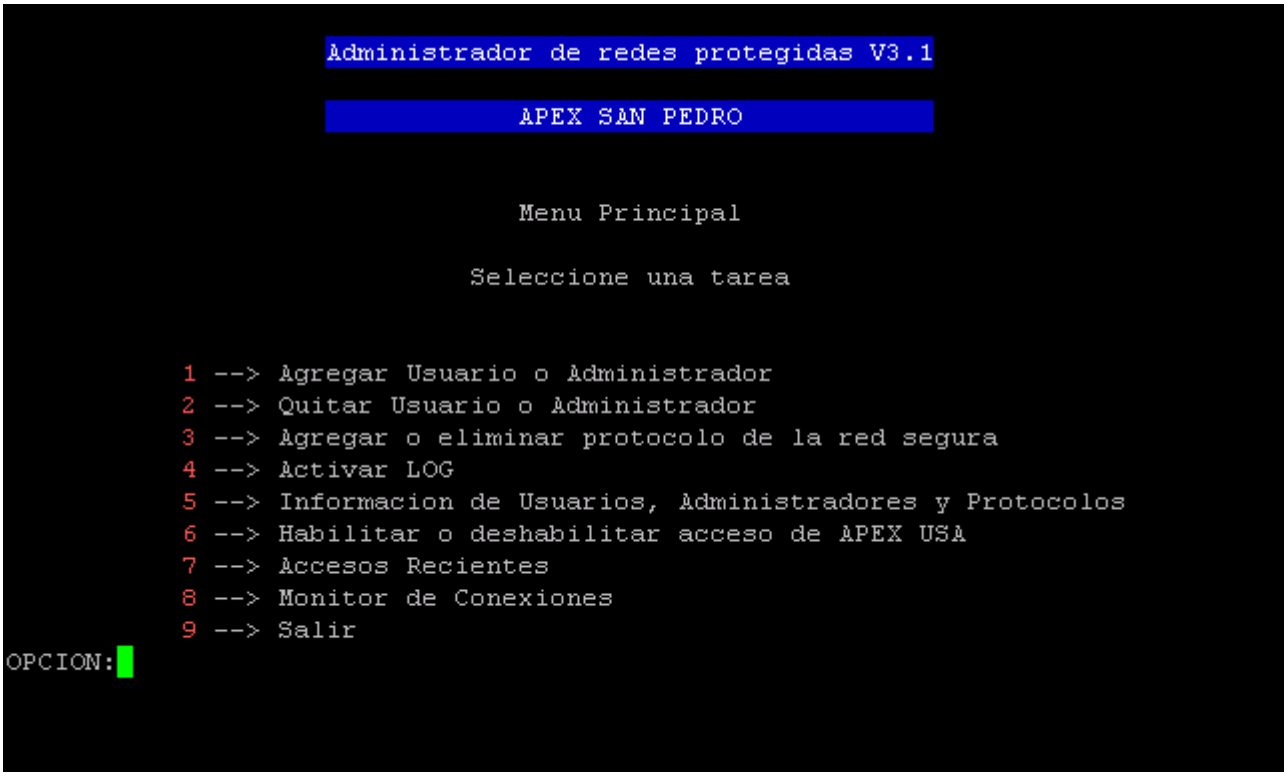

Figura 18 Interfaz entre el administrador y el firewall

Con esta interfaz se pretende que el administrador de red no requiera de conocimientos acerca de la teoría de filtrado de paquetes para poder manipular el *firewall*, solamente debe saber utilizar la aplicación.

Opción 1: Creación de usuarios o administradores.

Esta opción permite que se pueda implementar nuevas reglas en el sistema, las cuales van a estar definidas en diferentes cadenas de IPTABLES.

Para la creación de usuarios se van a crear nuevas reglas en la cadena de FORWARD, ya que se les debe permitir el uso de la red protegida. Para la creación de administradores se van agregar reglas en la cadena de ENTRADA, ya que aplican para la configuración del *firewall*.

Estas reglas van a ser aplicadas de inmediato al sistema y además van a ser guardadas en el archivo rc.fire, debido a que el sistema debe estar en capacidad de activar todos los cambios que se han realizado cuando el sistema se reinicia.

La forma en que se debe ingresar la información al sistema se ilustra en la figura 19, en la cual, se puede observar como el sistema solicita la dirección IP del usuario a ser validado. Luego el sistema pedirá información acerca del perfil del usuario como el nombre y la dependencia para la que labora; con esta información la aplicación actualiza los perfiles y luego despliega los datos.

En la figura 19 se puede observar los datos de cada usuario habilitado configurado en el sistema antes de agregar uno nuevo, esto con el fin de evitar que se agreguen perfiles que ya estaban definidos.

La forma en que se solicita la información al agregar un nuevo administrador es similar a la que se ilustra en la figura 19, con la diferencia de que el sistema despliega la información de los administradores en vez de los datos de los usuarios.

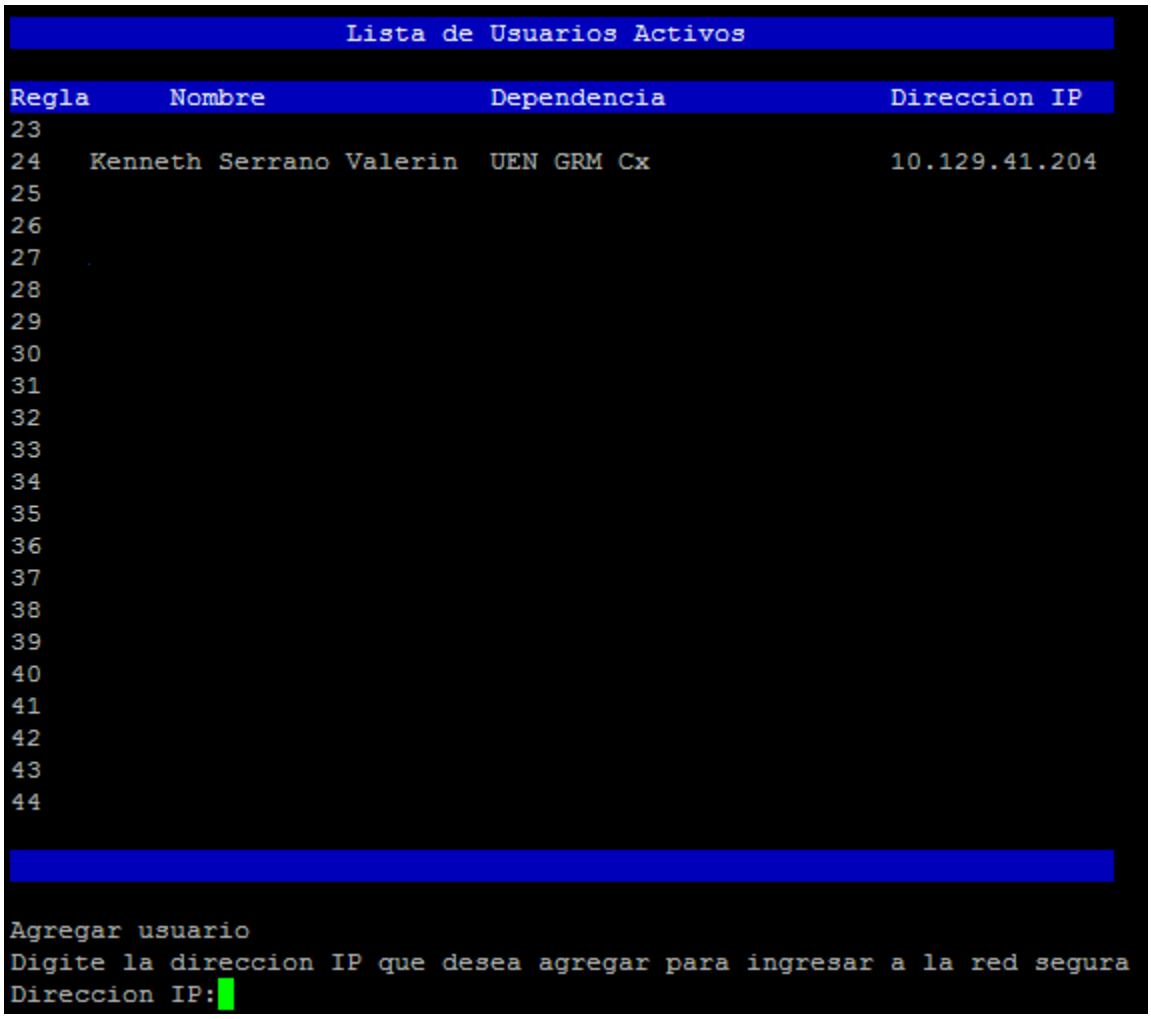

Figura 19 Implementación de nuevos usuarios

Opción 2: Eliminación de usuarios o administradores.

Para la eliminación de un usuario o un administrador el sistema despliega la información que se puede observar en la figura 20.

En esa figura se puede observar como el sistema le indica al administrador cual regla desea eliminar, en la primera columna se enumeran las reglas activas que tiene el sistema, esta numeración es correspondiente a los perfiles de los usuarios activos.

Al seleccionar un número se elimina el perfil especificado, esto se logra eliminando las reglas del sistema y del archivo rc.fire que le brindaban características a un funcionario de usuario o administrador.

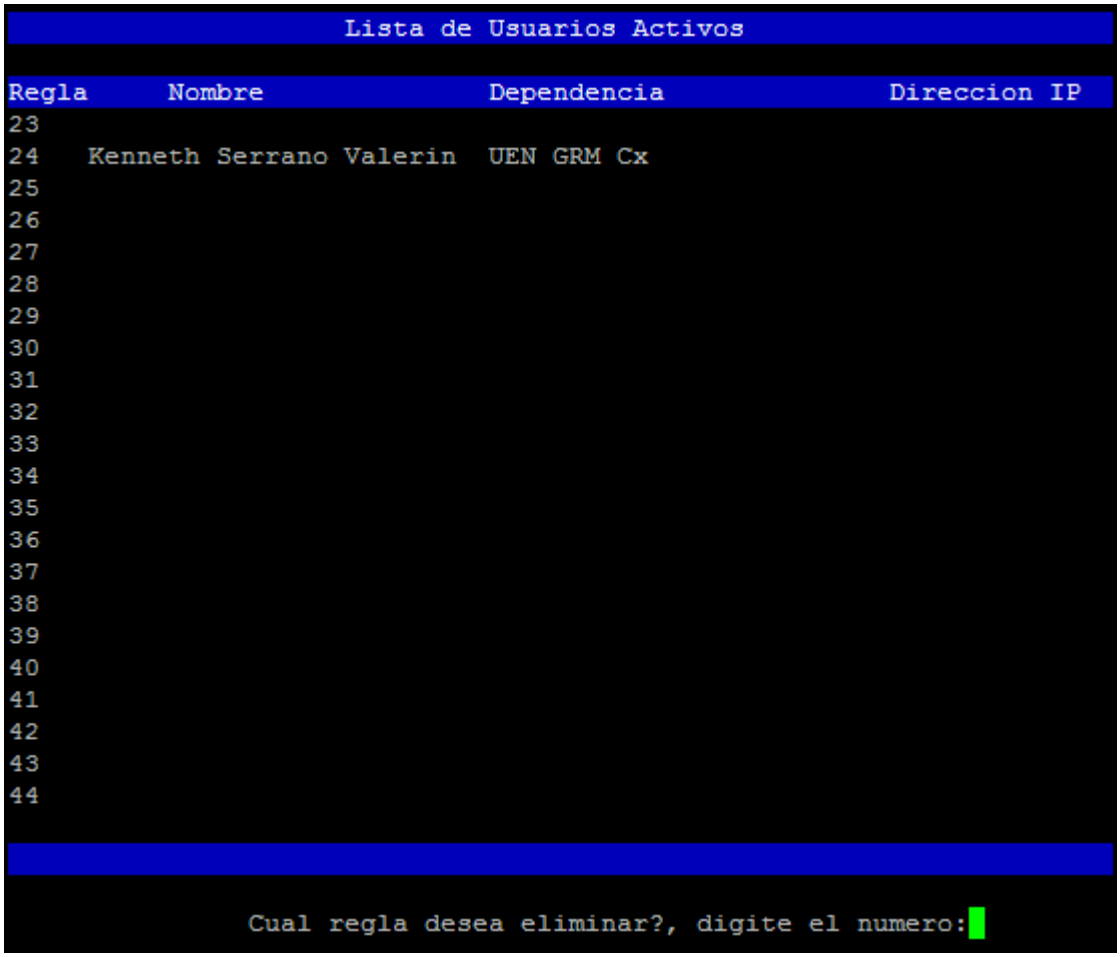

Figura 20 Eliminación de usuarios del sistema

Opción 3: Agregando o eliminando protocolos de la red segura.

Esta aplicación permite que el administrador del equipo pueda generar reglas que permitan abrir nuevos puertos en el firewall, esto con la finalidad de poder utilizar más aplicaciones para interactuar con la red protegida; sin embargo, esto se realiza de forma muy esporádica, ya que los puertos con que se va a trabajar en la red segura ya están establecidos.

En la figura 21 se ilustra la lista de protocolos habilitados para interactuar con la red protegida.

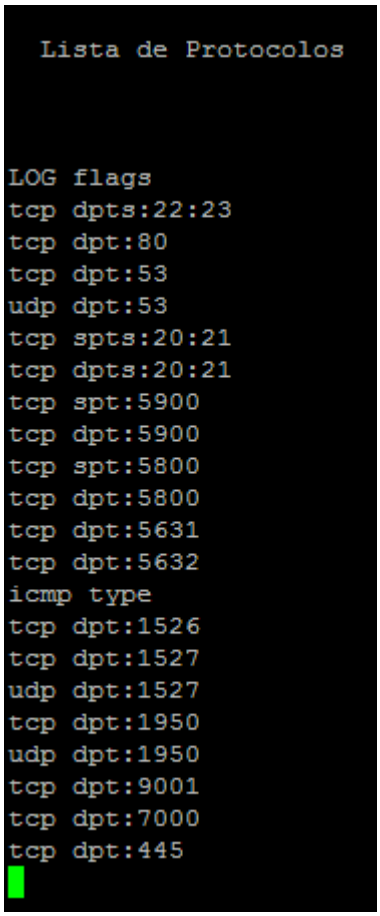

Figura 21 Lista de puertos permitidos para interactuar con la red protegida.

Opción 4: Activar los “LOGS”.

Esta opción permite que el administrador del *firewall* pueda observar las ultimas 20 líneas de la bitácora del sistema, cuyos datos se guardan en un archivo llamado firewall.log.

Esta bitácora es actualizada cada vez que un administrador del equipo realice algún cambio que altere los datos actuales del sistema de *firewall*, además permite guardar la información de la fecha y la hora en que se habilita el acceso a algún usuario del VPN.

Esta bitácora es de suma importancia para el manejo de los cambios que se han realizado al sistema y para poder verificar las fechas en que se han realizado.

Esta opción permite solamente ver una parte de la bitácora, sin embargo el archivo completo está a disposición del administrador del equipo.

No se puede mostrar una figura de la bitácora debido a que contiene la información de los usuarios que se han ingresado o eliminado del sistema.

Opción 5: Información general del sistema.

Esta opción es de suma importancia para el administrador, ya que le permite analizar el estado actual del sistema. Con esta opción se puede observar los datos actuales de los usuarios y los administradores, así como los protocolos establecidos. Esta opción es solamente de verificación y no realiza ningún cambio sobre el sistema.

Esta aplicación se genera por medio de los comandos que permiten devolver a los usuarios información de las reglas establecidas, esta información es procesada y luego se despliega de forma que el administrador la pueda entender.

Los datos que devuelve el sistema se pueden observar en las figuras 21, 22 y 23.

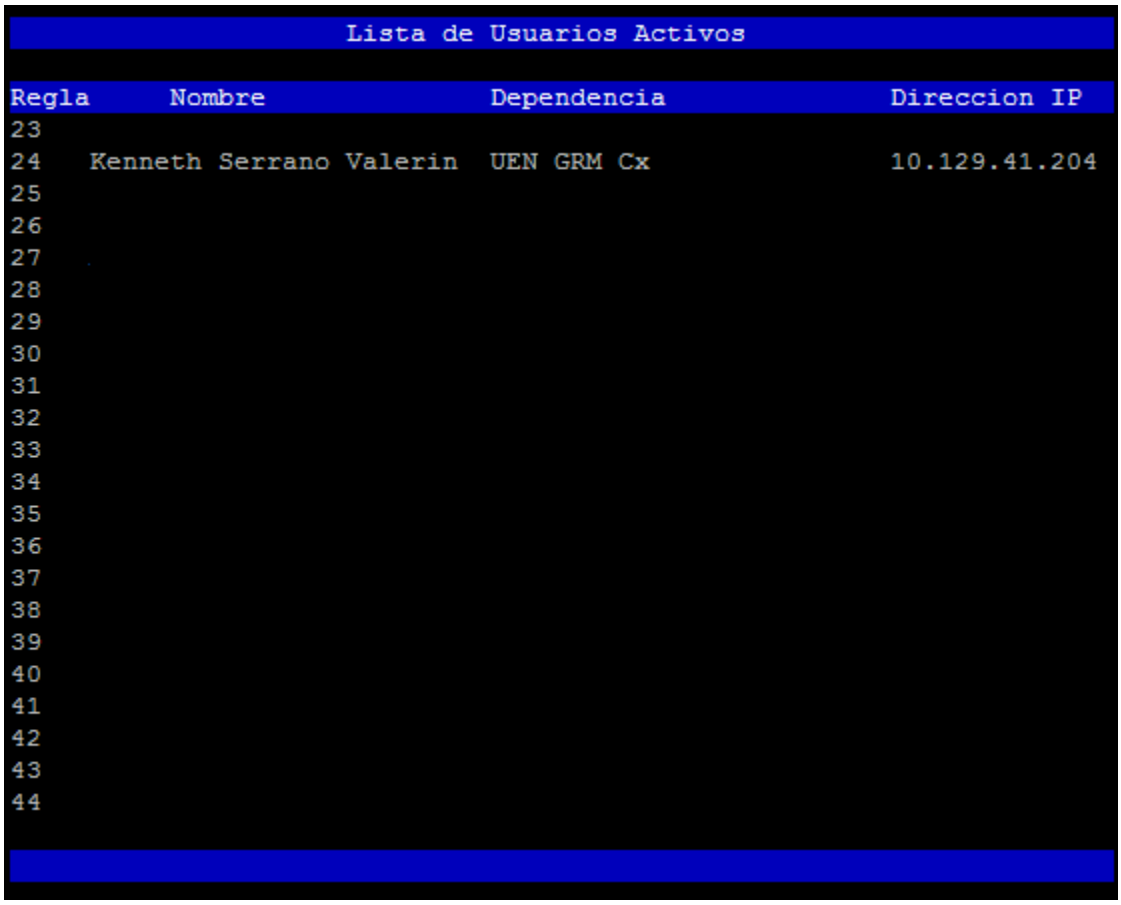

Figura 22 Información de usuarios activos

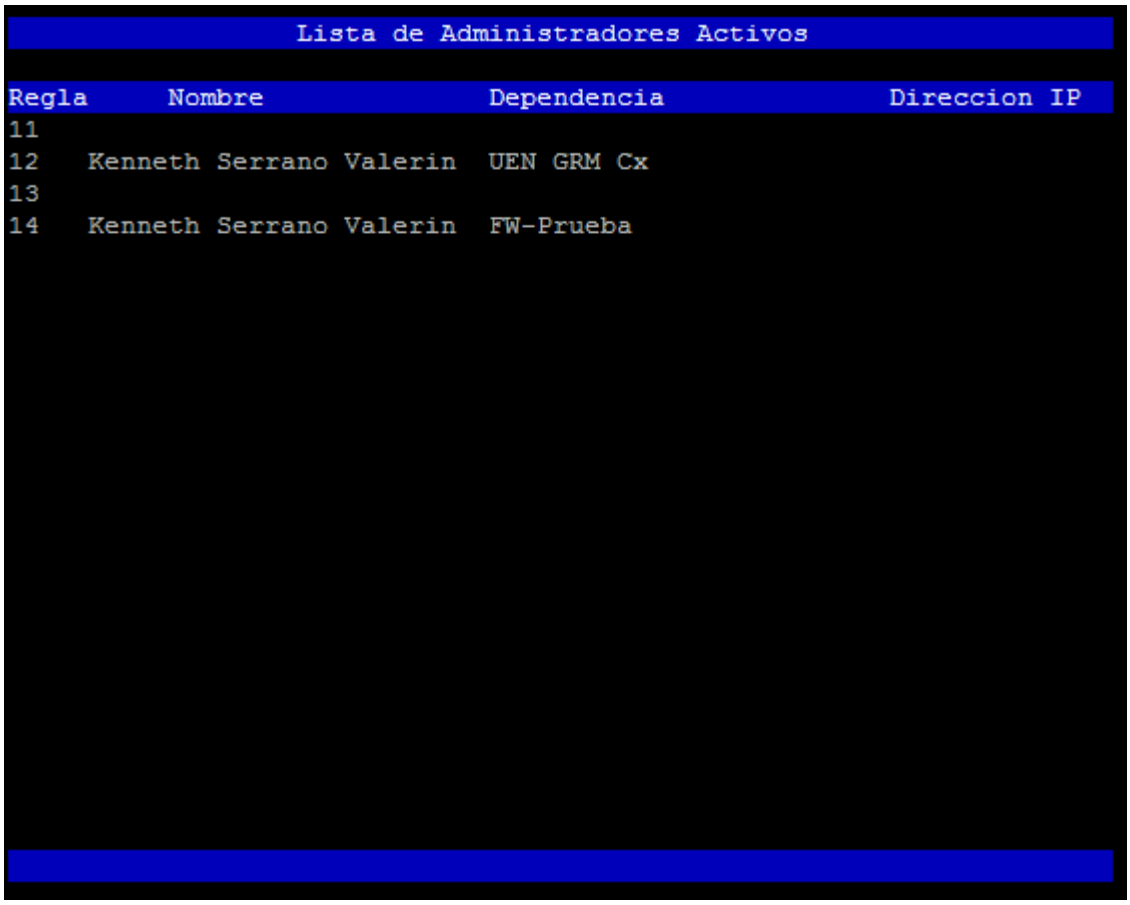

Figura 23 Información de los administradores activos.

Opción 6: Generación de ventanas de tiempo para el acceso por VPN.

Esta opción es de suma importancia para el departamento de conmutación debido a que permite el manejo del VPN de forma desatendida, es decir, esta función permite que el administrador establezca fechas y horas para permitir y denegar el acceso de los usuarios del VPN, sin necesidad de que el encargado esté al tanto del tiempo. Esta función fue generada utilizando el demonio CRON, el cual es una aplicación con que cuenta el sistema operativo para poder realizar trabajos programados. La configuración del sistema de forma desatendida se ilustra en la figura 24.

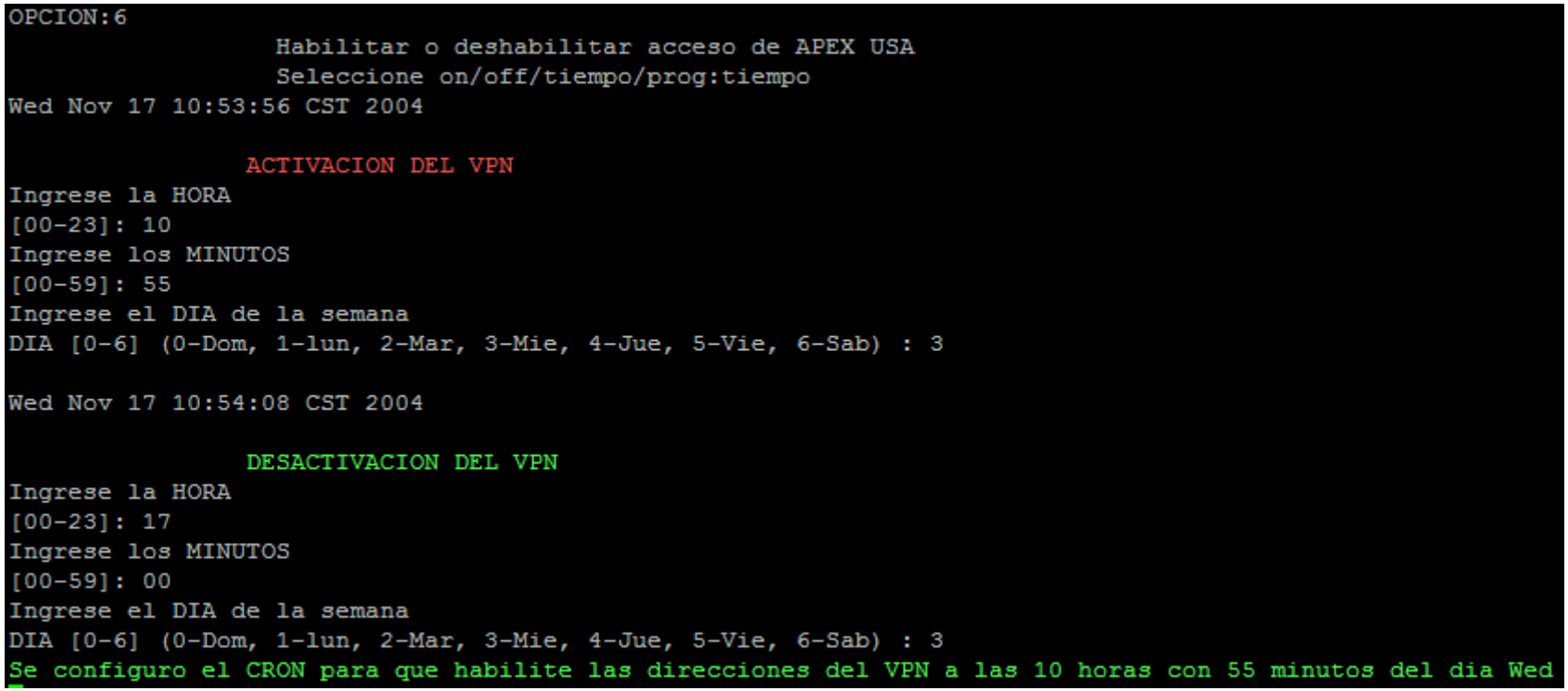

Figura 24 Configuración de acceso programado para el VPN.

Opción 7: Últimos intentos de conexión con la red segura.

Para la implementación de este punto se desarrolló una aplicación que permite generar mensajes cada vez que un usuario válido o un usuario del VPN trata de establecer una conexión con los equipos de la red segura. Esta información es guardada por el sistema en un archivo y se despliega cuando se selecciona esta opción. El sistema es capaz de actualizar la información en tiempo real.

En la figura 25 se ilustra la forma en que se despliega la información. En estas figuras se eliminó las direcciones IP que tienen que ver con las conexiones detectadas.

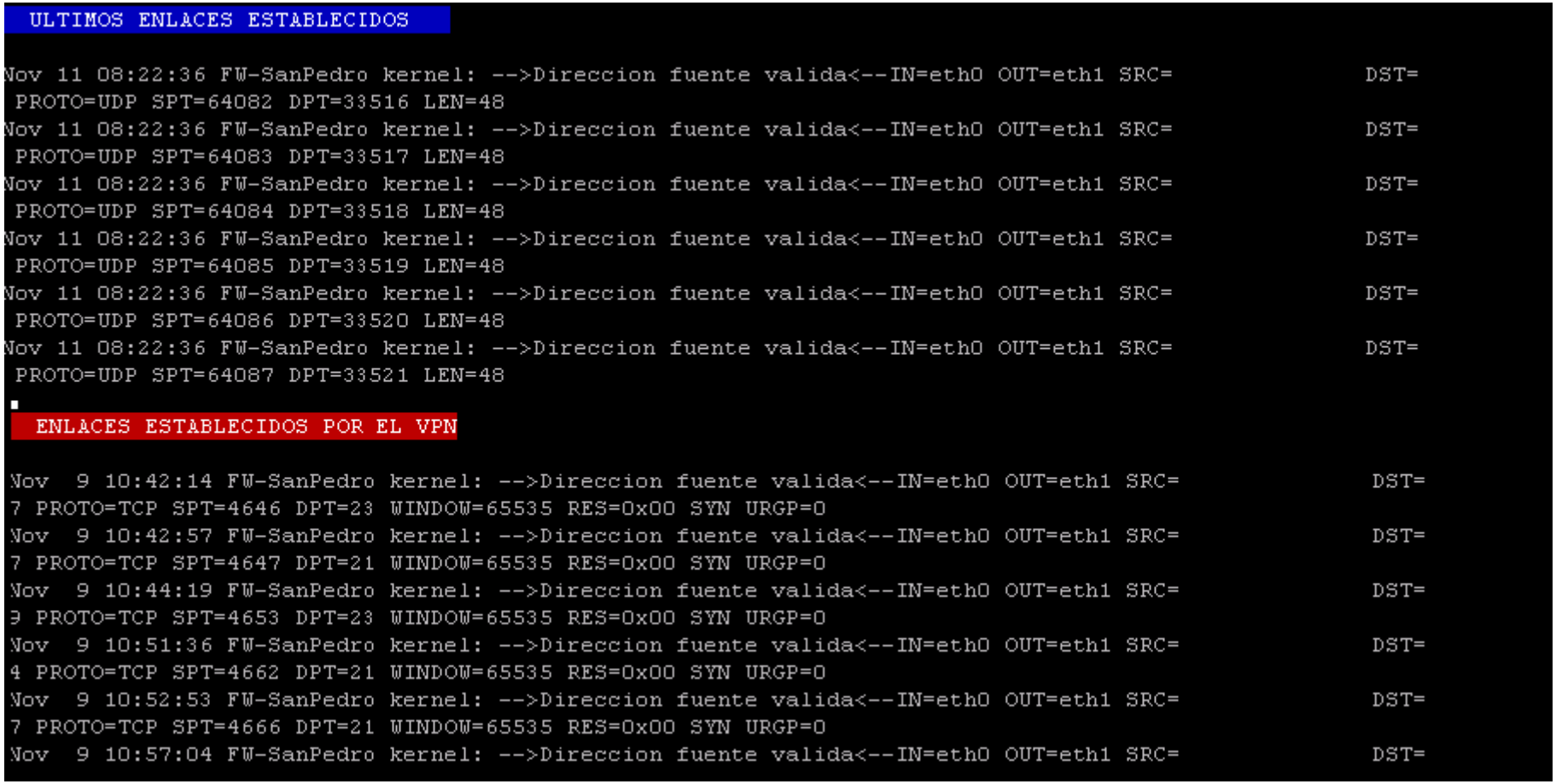

Figura 25 Últimos intentos de enlace con equipos en la red protegida.

Opción 8: Monitor de Conexiones.

Esta aplicación requirió del conocimiento del modo de operar de algunos protocolos de comunicaciones en redes de computadoras.

Primeramente se basó en el análisis establecido en el apartado 7.1.3, en el cual se analiza el orden en que se envían las tramas entre los equipos que intentan establecer comunicaciones; por tal motivo se requirió de análisis muy específicos en los paquetes de cada protocolo.

Fue necesario revisar el estado de bits específicos en las banderas de los paquetes TCP, y de este modo se pudo establecer algunos criterios para poder saber en que punto se encuentra la comunicación.

En la figura 26 se ilustra como el sistema es capaz de detectar en tiempo real si una comunicación está establecida (Sesión Abierta) o si ésta ya fue cerrada (Sesión Cerrada). Inclusive el sistema es capaz de detectar si la comunicación fue cerrada de forma correcta (→ FIN) o se debió cerrar por algún error (→ RST).

En la información que se despliega se establece los puertos que tienen que ver con la comunicación y las direcciones IP de los equipos que se encuentran interconectados (datos suprimidos en la figura 26).

Como se ha expuesto con los resultados obtenidos, el fireManager, que fue una aplicación desarrollada enteramente para el presente proyecto, está en capacidad de controlar de manera efectiva el firewall elaborado mediante las condiciones que fueron desarrolladas en el apartado 7.1.2.

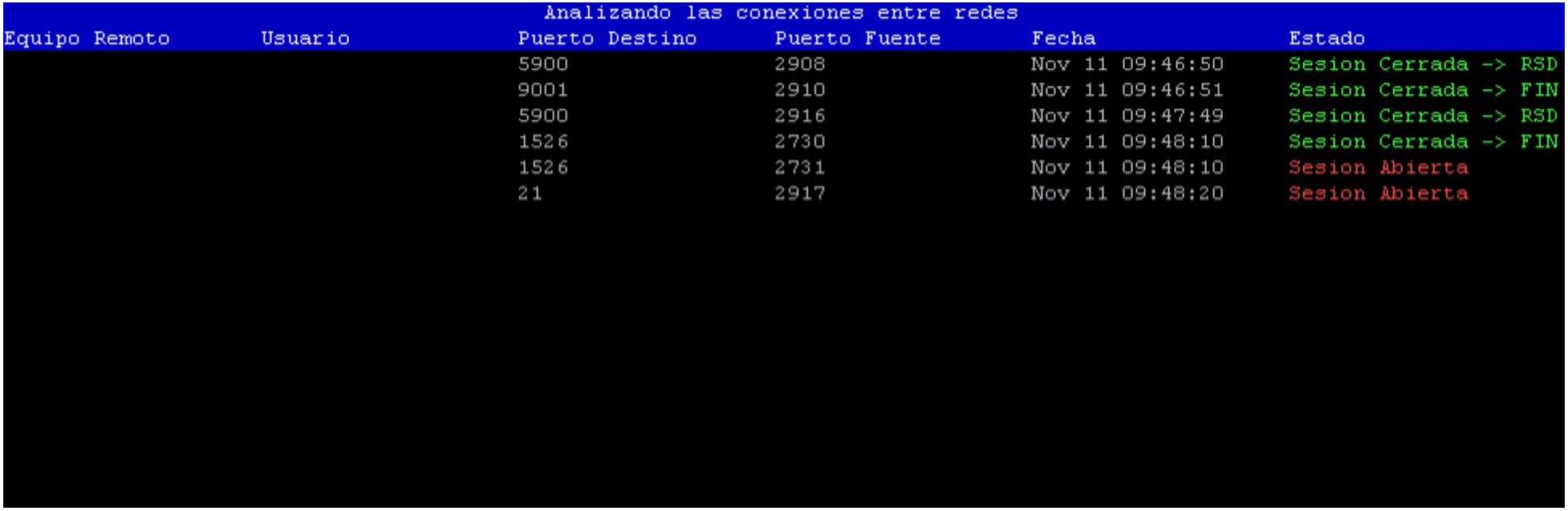

Figura 26 Monitor de las conexiones establecidas con la red protegida

.

8.2 Alcances y limitaciones

Este proyecto es una solución eficaz al problema planteado, es decir, permite a un administrador de red establecer reglas que permiten clasificar los usuarios y los protocolos que están permitidos en la red protegida. De este modo se pueden definir claramente las listas de usuarios a los que se les permite el acceso a la información que brindan los equipos APEX de los servicios 110 y 199, y por ende eliminar usuarios que no tienen que ver con el correcto funcionamiento de los equipos.

Además, permite al administrador de red agregar y eliminar protocolos para que los usuarios habilitados pueden utilizar y de este modo evitar que se pueda tener acceso a los servicios de 110 y 199 por puertos que pueden ser peligrosos para el equipo; esto permite un control del tráfico de la red protegida, ya que se puede estar seguro de que tipo de información se está utilizando.

Otro punto importante es la implementación de una bitácora con la información relevante que se maneja en la red protegida, ya que se tienen archivos en el firewall que guardan la información de cuando se abren las sesiones y cuando se cierran y de esta forma se puede visualizar que usuarios pueden estar tratando de realizar operaciones indebidas con el equipo protegido.

Este proyecto cuenta con una interfaz entre el administrador y el equipo de *firewall* que es fácil de entender, además permite un fácil manejo, y no se requiere de una explicación acerca de la teoría que está detrás del funcionamiento del *firewall*, es decir, que no se requiere que el administrador deba saber toda la teoría de IPTABLES y configuración de Linux. Solamente basta con saber en que puerto corre dado protocolo, y que dirección IP tiene asignada cierto usuario.

Además se pudo implementar una forma en que el sistema al reiniciar pueda cargar las aplicaciones y de este modo no se necesite atender el equipo si existe un fallo en la energía eléctrica.

Sin embargo existen ciertas limitantes que puede tener el proyecto, las cuales permiten que se pueda alterar el correcto funcionamiento del equipo.

Cualquier usuario habilitado que permita acceso a su máquina, está poniendo en peligro la información que se encuentra protegida por el firewall, ya que esto habilita al intruso a usar la dirección habilitada del usuario como puente para ingresar a los equipos protegidos. Debido a que el firewall no está en capacidad de detectar esta forma de entrar a la red, se creó una bitácora de accesos, la cual permite guardar la información del usuario que ingreso, y por cuales puertos lo hizo, de esta forma se puede tomar mediadas correctivas.

Otra limitante del proyecto es que cada firewall es específico para cada localidad, esto implica que cuando sea necesario instalar un nuevo equipo se debe cambiar cierta información que solamente la conoce un administrador de la red, como por ejemplo las direcciones IP de las interfaces, la dirección de la red protegida y la dirección de la red de enlace para entrar a la red del ICE (estas direcciones ya están establecidas, pero se deben configurar cuando se implemente el equipo)[23].

El firewall tiene una limitante grave que no se puede satisfacer con la situación actual de la red del ICE, esto es debido a que cada usuario cuenta con su dirección IP y la pueda cambiar sin ninguna restricción, esto permite que un usuario mal intencionado pueda tomar la dirección IP de un administrador o de un equipo y de esta forma analizar el tráfico en la red y poder realizar acciones indebidas. Esto se podría solucionar separando el equipo, los administradores y los usuarios en segmentos bien definidos, lo cual se logra realizando subredes de forma objetiva y sistemática y realizando políticas de seguridad de capa dos (Modelo OSI), es decir configurar los switches para que los puertos verifiquen las direcciones MACde los equipos (ver apartado 5.4 y apartado 9.2). Solamente de esta forma se podría tener una solución estructurada y efectiva para el problema de seguridad.

Sin embargo esta problemática está fuera de los alcances del presente proyecto, por lo tanto se trata de esto en las recomendaciones.

[23] Ver Procedimiento de instalación de firewalls en el Apéndice A.3

Capítulo 9 Conclusiones y recomendaciones

9.1 Conclusiones

1. Al elaborar un análisis comparativo entre diversas tecnologías se debe establecer parámetros de comparación como inversión inicial, características físicas, eficiencia de la posible solución o posibles beneficios a la hora de realizar la implementación, de este modo se puede realizar una escogencia más objetiva y por lo tanto una mejor selección.

2. Linux es una solución efectiva en la implementación de firewalls ya que permite realizar funciones como las propuestas por Check Point o Cisco y no existe un límite establecido para las capacidades de los firewall, como número de usuarios simultáneos o tamaño máximo de memoria a utilizar.

3. Implementar reglas en el *firewall* que afecten a subredes es más eficiente que manipular direcciones IP individuales, debido a que se disminuye el número de reglas a verificar, de este modo se mejora el tiempo de procesamiento del firewall y se reduce la latencia generada por el equipo.

4. Para poder mantener un *firewall* oculto en la red y eliminar los posible blancos de ataque, este equipo debe interactuar con la red con el menor número de puertos TCP/UDP posibles y debe existir un control de los mensajes ICMP que envía o recibe el *firewall,* reduciendo así las posibles debilidades en seguridad del equipo.

5. Implementar una política de desechar por defecto en un conjunto de reglas de un *firewall* brinda mayor seguridad debido a que todos los paquetes que no están contemplados en las reglas preestablecidas serán descartados, de este modo se evita que usuarios no validados puedan acceder a la red segura o al *firewall,* además se descartan todos los protocolos que no hayan sido predefinidos para utilizar en la red protegida.

6. Implementar una bitácora que permita registrar los accesos a los equipos de la red protegida permite controlar de una forma cronológica las conexiones realizadas por los usuarios, así como las acciones realizadas por los mismos, de esta forma se puede detectar si una persona intenta realizar actividades indebidas con el equipo protegido.

7. Utilizar cadenas personalizadas en IPTABLES permite una mayor flexibilidad y un mejor manejo de las reglas del *firewall*, debido a que se puede aplicar reglas específicas solo a los paquetes que lo requieran, evitando de este modo que todos los paquetes sean verificados por todas las reglas, mejorando así la eficiencia del equipo.

8. Registrar en tiempo real las conexiones que se realizan en la red protegida es indispensable para poder tomar acciones correctivas de una forma pronta y oportuna y de este modo evitar ataques al equipo protegido.

9. Implementar un *firewall* que no pueda ser descubierto en la red por ningún usuario permite un mejor nivel de seguridad, debido a que se impide que el direccionamiento del equipo pueda ser detectado y de este modo evitar ataques al firewall.

10. Implementar una interfaz en el *firewall* que permita generar reglas para la creación de usuarios o seleccionar entre protocolos validos para utilizar en la red segura, mejora la administración de este equipo sin necesidad de que el administrador deba conocer a fondo la teoría de funcionamiento del sistema.

11. Configurar el firewall para que permita a los usuarios del VPN acceder a la red segura solamente durante horas preestablecidas, ayuda al administrador de red a monitorear las acciones realizadas por este tipo de usuarios, permitiendo así, un control más efectivo sobre los equipos protegidos.

9.2 Recomendaciones

1. Se debe realizar un análisis de la topología actual del edificio de San Pedro, en especial las redes asignadas al departamento de Conmutación, esto con el fin de documentar todos los enlaces, la ubicación de equipos y direccionamiento asignado en la red interna. Esto permite trabajar de una forma más eficiente en la solución de problemas e implementación de nuevas aplicaciones.

2. Es de suma importancia separar en redes independientes a los funcionarios de áreas administrativas o de áreas que no requieren la utilización de los equipos que están conectados a la red interna, de forma que los administradores puedan estar en redes separadas y se pueda aplicar políticas de seguridad dependiendo de las actividades asignadas a cada tipo de funcionario del ICE.

3. Es indispensable que los equipos funcionales (servidores, bases de datos, centrales telefónicas, etc.) estén localizados en subredes independientes destinadas solamente a funciones específicas, esto permite un mayor orden a la hora de localizar un equipo y permite la implementación de reglas específicas a cada subred.

4. Configurar los switches de cada red, para evitar que usuarios ajenos a éstas, puedan tener acceso a la red institucional y de este modo adquieran características de usuarios válidos, administradores o equipos, esto se puede realizar asignando direcciones MAC establecidas a puertos específicos de los switches, los cuales se encargan de revisar la dirección MAC de la información que reciben y con base en esta información se puede tomar acciones, como bloquear el puerto, permitir el flujo normal de información o generar una alarma.

5. Implementar un servidor centralizado, en el cual se mantenga la información de los perfiles de usuarios y de los protocolos habilitados, de este modo se evita que el administrador deba configurar cada equipo de forma individual y se evita incongruencias en los datos de cada firewall. Para lo cual, se puede generar una base de datos con toda la información que considere necesaria el administrador y la implementación de una aplicación que actualice los demás equipos en caso de que se produzca un cambio en los datos del servidor.

Bibliografía

- Andreasson, Oskar. **"Iptables Tutorial 1.1.19"**. 2001-2003. http://www.jollycom.ca/iptables-tutorial/iptables-tutorial.html

- Check Point. **“Home Page”.** 2004 www.checkpoint.com

- Linux SuSE. **“Home Page”**. 2004 www.suse.com

- Cisco Systems **“Home Page**”. 2004. http://www.cisco.com/

- Purdy, Gregor. **"Linux iptables pocket reference"**, First Edition. O’ Reilly. USA , 2004

- Sandoval, Luis. **“Procedimiento de instalación de frontales para centrales”**. 2004. ICE

- Ziegler, Robert. **"Linux Firewalls"**, Second Edition. New Riders. Indiana, 2001

Apéndices y anexos

Apéndice A.1 Glosario

Connection Tracking: Forma en que se inspecciona la información que es filtrada por medio de un firewall para poder establecer cual es el estado actual de una sesión, una aplicación muy importante es detectar si las conexiones son abiertas por usuarios en la red segura o provienen del exterior.

Chain (Cadena): Grupo de reglas que se pueden aplicar a cada tabla de IPTABLES.

CRON: Es un “demonio” del sistema Linux, permite trabajar con la hora y fecha del sistema operativo. Es muy utilizado para correr aplicaciones que se ejecutan automáticamente en fechas preestablecidas.

DES (Data encryption standard): Es un protocolo de encriptamiento usado por IPsec para poder transmitir información sobre redes IP de forma segura.

Demonios: Aplicaciones del sistema operativo linux que es encuentran esperando la acción que los pone a funcionar para realizar tareas específicas. Por ejemplo: SSHD detecta las peticiones de conexión por SSH, CRON corre aplicaciones configuradas cuando se cumple alguna fecha fijada. Es muy similar a lo que se conoce en Windows como servicios.

DNAT: Cambio de la dirección destino del paquete.

DoS attack: Tipo de ataque sobre un red que satura la misma con información inútil, impidiendo el tráfico de los datos importantes, se elaboran utilizando las limitaciones de TCP/IP.

Ethernet: Es la tecnología de red de área local más extendida en la actualidad. Fue diseñado originalmente por Digital, Intel y Xerox por lo cual, la especificación original se conoce como Ethernet DIX. Posteriormente en 1.983, fue formalizada por el IEEE como el estándar Ethernet 802.3. La velocidad de transmisión de datos en Ethernet es de 10Mbits/s y 100Mbits/s en las configuraciones habituales pudiendo llegar a ser de más de 1Gbits/s en las especificaciones Fast Ethernet.

FTP: Protocolo de transferencia de archivos (puertos TCP 20 y 21)

Firewall: Equipo con dos o más interfaces de red que permite el enrutamiento y además se le establecen reglas de filtrado con las que se decide si una conexión determinada puede establecerse o no. Incluso puede ir más allá y realizar modificaciones sobre las comunicaciones, como el NAT o manipular conexiones de tipo VPN.

IPsec (IP security): Es una tecnología propia de CISCO, la cual permite manejar información IP de forma segura.

IPTABLES: Comando más importante de Netfilter que permite realizarle reglas de filtrado a los paquetes TCP/IP.

L2TP (Layer 2 tunneling protocol): Es una tecnología abierta (no propietaria), cuya implementación permite implementar túneles entre redes.

Linux: Sistema operativo desarrollado por Linus Torvalds. Linux es el nombre del sistema operativo kernel, el cual es la parte central del sistema operativo, incluye utilidades, editores y compiladores además de componentes de red.

Netfilter: Paquete de linux que cuenta con todas las capacidades de networking del sistema operativo para implementar IPTABLES.

NIS: Es un servicio de Directorio Centralizado (puerto TCP 111)

Modelo OSI: En 1984, la Organización Internacional de Estandarización (ISO) desarrolló un modelo llamado OSI(Open Systems Interconection, Interconexión de sistemas abiertos). El cual es usado para describir el uso de datos entre la conexión física de la red y la aplicación del usuario final. Este modelo es el mejor conocido y el más usado para describir los entornos de red. Esta basado en 7 capas. (Física, enlace de datos, red, transporte, sesión, presentación, aplicación).

Modelo TCP/IP: Este modelo define solamente tres capas que funcionarán en los niveles superiores a las capas físicas y de enlace para hacerlo así un modelo independiente del hardware en el que se implemente.

Ping of death: Ataque DoS que permite tomar ventaja de debilidades de ICMP, se envía una petición con un tamaño mayor a 65.536 bytes el máximo permitido por IP, de este modo el equipo que lo recibe tiene un desbordamiento en su buffer de transmisión y el sistema operativo cae.

Table (Tabla): Funciones generales del IPTABLES. Filtrar, NAT, cambiar características como TOS (type of service) o TTL (time to live), existen tres tipos diferentes de tablas: “Filter”, “Mangle”, “NAT”.

TELNET: Protocolo de acceso remoto (puerto TCP 23)

TRACERT: Prueba que permite conocer los saltos que realizan los paquete en los enrutadores antes de llegar a su destino.

Shell: Compilador de Linux, permite la interacción del usuario con el kernel vía comandos, existen varios como el bash, el korn y otros.

SNAT: Cambio de la dirección fuente del paquete.

SSH: Protocolo de acceso remoto, permite la encriptación de la información y permite muchas más funciones que TELNET, como transferir archivos (puerto TCP 22).

SuSE: Establecido en 1992, SUSE LINUX es uno de los abastecedores principales del mundo del software y de los servicios de Linux. Con el equipo dedicado más grande de investigación y de desarrollo de Linux, SUSE entrega software a las empresas listo para utilizar, por otro lado cada entrega de Linux SuSE cuenta con el código abierto para que sea de utilidad para la comunidad.

VNC: Software especializado para control remoto gráfico (puerto TCP 5900).

Protocolos más importantes del Internet Protocol (IP)

ICMP: (Internet Control Message Protocol) Protocolo que permite controlar el flujo de informarción por medio de mensajes de error u otros tipos de información.

TCP: (Transmission Control Protocol) Protocolo orientado a la conexión, el cual permite una transferencia de información confiable.

Three way handshake: Protocolo que permite que se establezca una conexión por medio de TCP.

UDP: (User Datagram Protocol) Protocolo no orientado a la conexión, permite el intercambio de información pero no lo hace de una forma confiable.

Terminología del ICE

APEX: Compañía norteamericana que provee de equipo telefónico al ICE.

Frontal: Equipo encargado de realizar una interfaz con las centrales telefónicas de diversas tecnologías, además de procesar la información obtenida para que sea entendible y utilizable por el departamento de conmutación

GRM: Gestión de Red y Mantenimiento.

TI: Tecnologías de la Información.

UEN: Unidad Estratégica de Negocios.

Software utilizado en el proyecto

NESSUS: Software capaz de detectar una gran cantidad de problemas en los equipos de red, inclusive puede detectar fallas de red en los sistemas operativos de los equipos.

NetworkView: Software de inspección de redes, capaz de detectar equipos y realizarle pruebas básicas a puertos TCP específicos, además puede detectar la información del sistema, para este proyecto se utilizó un free trial.

Segmento de la licencia de NetworkView : “You may try out the unregistered version of NetworkView without any charge for the period of one month. After that period, you have to register it with the author or completely remove it from your computer or floppy disk, even if the software contains no "time bombs", i.e. that it will not stop functioning after one month.”

Apéndice A.2 Información de la institución

La empresa para la que se pretende desarrollar el proyecto de graduación es el instituto costarricense de electricidad, esta institución está separada en dos sectores, los cuales tienen sus respectivas misiones:

La Misión del ICE energía es la siguiente:

Suministrar servicios de electricidad que satisfagan sus las necesidades de sus clientes y agreguen valor a su calidad de vida y a sus procesos productivos, bajo condiciones de competitividad en precio, calidad y oportunidad en clase internacional.

La Misión del ICE Telecomunicaciones es la siguiente:

Ofrecer los servicios de telecomunicaciones que los clientes requieran con calidad, oportunidad y tarifas competitivas, mediante el uso óptimo de la tecnología y el aporte del recurso humano motivado y calificado.

Recursos Humanos:

En los dos Sectores: Energía y Telecomunicaciones, a noviembre de 1995: 9.385 funcionarios, distribuidos de la siguiente forma:

Ejecutivos	13
Profesionales	1.258
Técnicos	6.332
Servicios y obreros	1.782
Total	**9.385**

El ICE fue creado mediante el Decreto Ley Nº 449 del 8 de abril de 1949.