ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

DISEÑO E IMPLEMENTACIÓN DE UNA RED PRIVADA VIRTUAL PARA LA EMPRESA ELÉCTRICA QUITO S.A., MATRIZ LAS CASAS, PARA LA TRANSMISIÓN DE DATOS Y VOZ SOBRE IP

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y REDES DE INFORMACIÓN

PABLO ANDRÉS DÍAZ ALVEAR
pabloandresepnd@yahoo.com

DIRECTOR: ING. PABLO HIDALGO
pablo.hidalgo@epn.edu.ec

Quito, Febrero 2010

DECLARACIÓN

Yo Pablo Andrés Díaz Alvear, declaro que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

La Escuela Politécnica Nacional, puede hacer uso de los derechos correspondientes a este trabajo, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

_____

Pablo Andrés Díaz Alvear

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Pablo Andrés Díaz Alvear, bajo mi supervisión.

_____

Ing. Pablo Hidalgo
DIRECTOR DEL PROYECTO

AGRADECIMIENTOS

Un especial y afectuoso agradecimiento al Ing. Pablo Hidalgo quien además de haber sido uno de mis mejores profesores en la universidad, me ha aportado acertadamente con su valiosa dirección y guía en este proyecto, por lo que ha sido posible ser realizado.

Al Ing. Miguel Araujo quien me ha dado la oportunidad de poner en práctica mis conocimientos al servicio de la Empresa Eléctrica Quito S.A., con lo cual también me ha permitido enriquecerme en el aspecto humano y profesional.

A mi amigo, el Ing. Álvaro Cadena, quien desde las aulas de nuestra querida universidad y desde las oficinas de nuestro trabajo ha sido un gran compañero, y de quien he podido aprender mucho.

A mi querida Escuela Politécnica Nacional le agradezco el haberme acogido en sus aulas con sus profesores que han sido mi guía, y de la cual estoy muy orgulloso de pertenecer.

A mis hermanos Margarita, Fernando y Juanito que siempre me han apoyado en los momentos más difíciles y quienes también han sabido guiarme a lo largo de mi vida estudiantil.

A mis primos y amigos que con su valiosa compañía han sido partícipes anónimos en la realización de éste trabajo.

DEDICATORIA

A Dios todo poderoso que ha sido bondadoso conmigo y mi familia, y me ha dado la dicha de vivir.

A mis padres Margarita y Carlitos, quienes con gran amor y esfuerzo han sabido criar a sus cuatro hijos y que con sabiduría me han entregado las mejores herencias que los padres pueden dejar a sus hijos: valores, principios y el estudio.

A mi gran amor Ruthcita quien ha sido un gran apoyo y a quien le debo mucho.

CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

RESUMEN

Este proyecto contempla una solución para las necesidades más urgentes en el aspecto de comunicación-seguridad, orientadas específicamente a la red de datos de la Empresa Eléctrica Quito S.A. (E.E.Q.S.A.), implementada en su mayoría dentro del modelo de referencia TCP/IP. Además de solucionar las necesidades, se ha planificado también, el proyectar soluciones a las futuras necesidades y aplicaciones que ingresen y sean parte de la red de datos, como por ejemplo las aplicaciones multimedia (VoIP, Telefonía IP, Videoconferencia, etc).

El proyecto se encuentra estructurado de la siguiente manera:

Capítulo 1. Redes Privadas Virtuales y sus Aplicaciones, aquí se revisará la evolución de las VPNs hasta su estado actual, protocolos, sistemas de encripción, y el funcionamiento de éstos. Es una sección teórica donde también se explicará de manera general el avance en sistemas de protección de datos, y también cuáles son las proyecciones y tendencias de las nuevas generaciones de VPNs.

Capítulo 2. Análisis del estado actual de la red de datos de la Empresa Eléctrica Quito S.A., en este capítulo se determinará el número de equipos de usuario, de conectividad y todo aquel dispositivo que genere tráfico dentro de la red interna. Para los enlaces hacia al exterior, se analizará por separado las conexiones con las empresas de intercambio comercial, y el Internet. Esto servirá para establecer de manera adecuada, políticas de seguridad. Además se analizará el funcionamiento del *firewall* que estuvo operativo, las aplicaciones que se ejecutan sobre la red de datos y los métodos de acceso tanto hacia la red como a servidores y a las diferentes aplicaciones que requieran control de acceso.

Capítulo 3. Diseño de la Red Privada Virtual, luego de haber analizado el estado de la red de datos de la E.E.Q.S.A., se podrá establecer los requerimientos, para conocer, qué se debe proteger, y, también, los niveles de seguridad que se deben configurar en aquellos requerimientos. Dentro de los requerimientos obtenidos, se

suman aquellos en que los CARs[1] necesitan acceder a las aplicaciones, para que éstos puedan realizar cobros en línea. Las empresas de intercambio comercial podrán obtener una comunicación telefónica con la E.E.Q.S.A., donde se aplicará VoIP seguro sobre VPN. Estas y otras aplicaciones serán evaluadas para determinar el tráfico que generan, puertos que se necesitan usar, etc. Como resultado de este análisis, se determinarán las características de la solución más adecuada para cubrir con las necesidades del presente y los próximos cinco años en materia de comunicaciones con control de seguridad.

Capítulo 4. Implementación de la Red Privada Virtual, configuración de equipos y pruebas del diseño implementado; con el diseño elaborado y la adquisición de los equipos establecidos en la ingeniería de detalle del diseño propuesto, se empezará a adecuar el lugar dentro del Centro de Cómputo donde se instalarán físicamente los equipos. Se procederá a realizar pruebas de tráfico, y una breve simulación de migración del equipo de seguridad anterior al nuevo. La migración definitiva se realizará, si la prueba de migración es realizada con todo éxito. Una vez con el nuevo equipo, se procederá a configurar los enlaces VPN de prueba, y en lo posterior VoIP seguro. Una vez más, si los resultados de las pruebas de VPN son exitosos, se procederá a implementar estos enlaces, para que se ejecuten en producción.

Capítulo 5. Conclusiones y Recomendaciones, finalizando este trabajo, se analizarán los tráficos generados por los nuevos enlaces, los métodos de acceso aplicados, políticas de seguridad y la nueva topología de la red de la E.E.Q.S.A., para verificar el cumplimiento con los objetivos planteados. Se pondrá a conocimiento de los técnicos y administradores de la red de datos de la E.E.Q.S.A., las capacidades del nuevo equipo y del diseño planteado e implementado; esto con el fin de que se tomen las medidas adecuadas para un buen mantenimiento y evolución de los enlaces VPN y la seguridad de la red de datos.

[1] CARs son las siglas de Centros Autorizados de Recaudación

PRESENTACIÓN

Durante el proceso de modernización continua y actual de los sistemas informáticos, en empresas de nuestro país, los principales parámetros que han determinado esta modernización tecnológica, son: el ancho de banda o capacidad del canal de comunicación, la seguridad y los costos.

Dentro de la seguridad se han ido desarrollando e implementando varios modelos tecnológicos para: accesos, autorizaciones y protocolos. Todos estos desarrollos van enfocados a la protección de redes de datos, en su mayoría privadas. También permiten proteger a las redes de los posibles ataques que lleguen del exterior, aunque existen considerables ataques perpetrados hacia las redes privadas desde su interior y con variedad de métodos.

Analizando los enlaces desde el exterior a la red interna de una empresa o corporación, se puede mencionar que en aquellos enlaces existentes con otras redes, de: empresas asociadas, clientes, entidades estatales e Internet, éstos deberían mantener un control del tráfico, para garantizar disponibilidad, confiabilidad e integridad de los datos, no solo de la empresa o corporación, sino también garantizar que los datos que salen de la red interna sean de confianza.

Es así que, con este antecedente tecnológico, la Empresa Eléctrica Quito S.A., ha estado llevando a cabo un proceso de modernización en su red de datos. Dentro de este proceso, se encuentra el mejorar y mantener en constante evolución los sistemas de seguridad y protección de la red de datos.

También está el poder brindar a los usuarios del servicio eléctrico, más comodidades para los trámites de facturación, recaudación, denuncias y reclamos, creando en conjunto con la empresa privada, Centros Autorizados de Recaudación (CARs). Estos centros físicamente se encuentran creados y operando; sin embargo los procesos de recaudación son todavía poco eficientes, ya que no cuentan con un propio sistema de red de datos.

En vista de estas deficiencias, se ha puesto en marcha, la implementación de equipamiento y alternativas de comunicaciones adecuadas para el transporte de datos, para estos CARs. Como una alternativa para que estos CARs ingresen a la red privada de la E.E.Q.S.A., se ha procedido a realizar el diseño de Redes Privadas Virtuales (VPNs), en la que a través del Internet utilizando infraestructuras de redes públicas como la PSTN, mediante *Dial-Up* o ADSL, puedan abrir sesiones seguras y realizar los cobros en línea y demás operaciones relacionadas con el sistema comercial de la E.E.Q.S.A.

Ésta es solo una de las aplicaciones que se requiere implementar, también existe requerimientos de las empresas asociadas a la E.E.Q.S.A. que justifica el acceso a ciertos sistemas o aplicaciones, la misma que a su vez también necesitan garantizar niveles de seguridad adecuados.

CAPÍTULO 1

REDES PRIVADAS VIRTUALES Y SUS APLICACIONES

1.1 CONCEPTOS Y EVOLUCIÓN DE LAS REDES PRIVADAS VIRTUALES (VPNs – *VIRTUAL PRIVATE NETWORKS*)

1.1.1 INICIOS DE LAS REDES DE DATOS PRIVADAS VIRTUALES

El término de Red Privada Virtual en sus inicios, fue asociado a los servicios prestados a través de la Red de Telefonía Pública (*PSTN*[2]) con líneas dedicadas o *PVCs de los enlaces Frame Relay*[3]. Pero de una manera acertada y bajo las circunstancias modernas de los sistemas de comunicación, este término en la actualidad es asociado a redes de datos, donde el tráfico de bits circula a través de medios físicos de diferente naturaleza; para obtener el título de *privado* utilizan una determinada tecnología, basada en protocolos y algoritmos que aíslan estos datos de los denominados *públicos*.

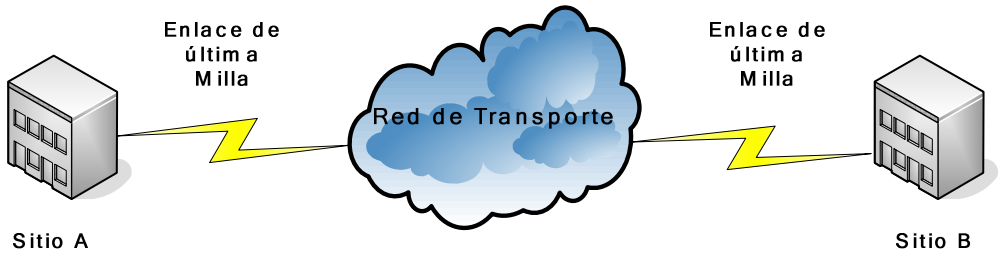


Figura 1.1 Esquema básico de un enlace dedicado

Antes de que este término madurara, las empresas a través de la historia, han tenido la necesidad de extenderse y compartir recursos, mediante enlaces de red privados, hacia lugares remotos, alejados de los centros principales de funcionamiento. Para poder cubrir estas necesidades, se desarrollaron bajo la PSTN, redes de datos de baja velocidad.

---

[2] PSTN son las siglas en inglés de *Public Switching Telephonic Network*

[3] PVCs son las siglas en inglés de *Private Virtual Circuit* en plural, y referidos al concepto que se encuentra dentro de las definiciones del funcionamiento de *Frame Relay*. Ref. Notas de la materia Redes WAN Profesor Rafael Veintimilla.

Los retos que implicaban estas conexiones entre otras, eran las de mejorar la calidad de los enlaces y aumentar las velocidades iniciales; esto implicaba altos costos en sus diseños y sobre todo en las implementaciones.

Las líneas dedicadas y enlaces *ATM*[4] eran soluciones aceptables, pero solo para de empresas con presupuestos económicamente altos. Aquellas empresas que contaban con recursos económicos moderados o de bajo presupuesto, sólo podían conformarse con servicios de conmutación de baja velocidad para la transmisión de datos.

Al llegar el Internet, a ser un servicio comercial, y sobre todo, poseer la capacidad de crecer de manera sorprendente, se llegó a determinar que los enlaces costosos podrían ser reemplazados por accesos a través del Internet, ya que éste es más barato, en relación a los enlaces dedicados. Sin embargo, este costo relativamente bajo para acceder a este servicio, se contrastaba con la poca seguridad que éste ofrecía al comienzo.

Las tecnologías que permiten implementar las VPNs han ido evolucionando, en el aspecto de mejorar la calidad de los enlaces (*bajar overhead*[5]), y sobre todo, la seguridad de los datos que pasan a través de los túneles virtuales.

Hoy en día se cuenta con mejoras en productos para la creación de VPNs, tanto en equipos dedicados a formar VPNs denominados equipos *appliance*[6] para VPNs, así también como en *software*; esto dependerá de los requerimientos de quienes necesiten utilizar este servicio de comunicaciones.

[4] ATM (*Asynchronus Transfer Mode*) Tecnología de comunicaciones para Redes WAN basado en la conmutación de celdas o paquetes fijos de información. Se puede establecer niveles de calidad de servicio.
[5] Reducir la cantidad de bits innecesarios en las cabeceras de los paquetes o tramas utilizados básicamente para el control del enlace.
[6] *Hardware* o *software* que fue diseñado para cumplir funciones específicas de alto rendimiento.

1.1.2 RED PRIVADA VIRTUAL

Una VPN consiste en simular una red privada, sobre una infraestructura de comunicaciones pública, como por ejemplo el Internet, la PSTN, una red *Frame Relay*, etc.

Las VPNs pueden formarse según los requerimientos de los usuarios, aplicaciones y ubicación de los dos anteriores. Tomando en cuenta estos factores las VPNs toman las siguientes topologías o tipos: *LAN – LAN, LAN – WAN y Acceso Remoto a intranets o extranets*[7]. [1]

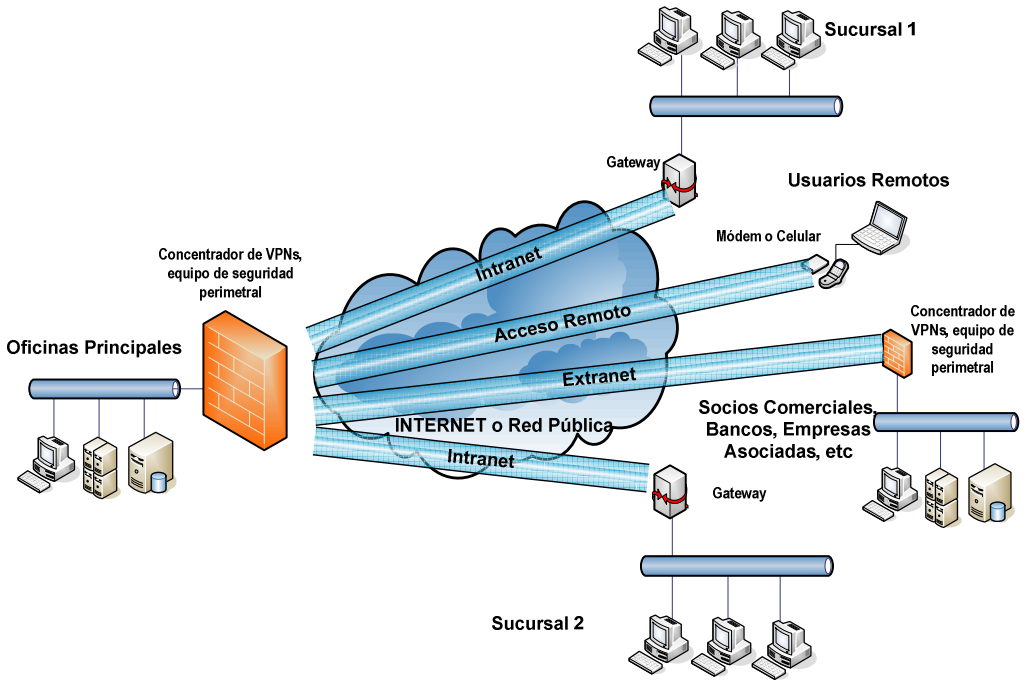


Figura 1.2 Diferentes esquemas para la formación de VPNs

Para establecer una VPN se han desarrollado varias tecnologías, muchas de ellas han sido establecidas como estándares y otras, han sido soluciones de propietarios para sus propios productos fabricados, o también denominados Estándares de Facto.

[7] Clasificación tomada del *paper IPSec Virtual Private Networks Conformance and Performance Testing* y Wikipedia: Redes Privadas Virtuales.

Las tecnologías que han llegado a ser aceptadas para la implementación de las VPNs, deben cumplir básicamente con los siguientes requerimientos:

***Seguridad**,* para cumplir con este requerimiento, es necesario brindar a la conexión, los siguientes elementos:

- ***Privacidad***, la cual se realiza a través dos métodos, que son la encripción y el encapsulamiento. Dentro de la encripción sólo se encripta los datos y no el *header*. Los algoritmos más utilizados para la encripción son DES (*Data Encryption Standard*)[8], 3DES (*Triple* DES)[9], AES (*Advanced Encryption Standard*)[10], RSA[11], IDEA (*International Data Encryption Algorithm*) [12]. El método de encapsulamiento encripta los datos y el *header*, luego coloca un nuevo *header*; para este propósito se emplean protocolos como *IPSec y L2TP*[13].*[2]*

- ***Integridad**,* para garantizar que los datos no han sido modificados, se usan algoritmos de *hashing* como SHA (*Secure Hash Algorithm*)[14], MD4 (*Message-Digest Algorithm* 4)[15], MD5 (*Message-Digest Algorithm* 5)[16], entre los más utilizados.

- ***Autenticación**,* para garantizar que quien desea ingresar, es realmente quien dice ser. Esto se logra mediante esquemas como *user/password*, *token cards*, *smartcards*, certificados X.509. Cada uno de estos esquemas tiene diferentes niveles de fiabilidad.

---

[8] DES es un algoritmo de cifrado. También es conocido como DEA (*Data Encryption Algorithm*).
[9] 3DES es el algoritmo que hace triple cifrado del DES. También es conocido como TDES o 3DES, fue desarrollado por IBM en 1978.
[10] AES es un moderno algoritmo de encripción que utiliza un tamaño de bloque de 128 bits y una clave de longitud de al menos 128 bits. Técnicamente es mejor que 3DES.
[11] RSA es un algoritmo asimétrico cifrador de bloques, que utiliza una clave pública. El algoritmo fue descrito en 1977 por Ron **R**ivest, Adi **S**hamir y Len **A**dleman; las letras RSA son las iniciales de sus apellidos.
[12] IDEA es un cifrador por bloques. Fue un algoritmo propuesto como reemplazo del DES.
[13] Tecnologías para la formación de Redes Privadas Virtuales
[14] SHA es un sistema de funciones *hash* criptográficas relacionadas y publicadas por el *National Institute of Standards and Technology* (NIST).
[15] MD4 es un algoritmo de resumen del mensaje (el cuarto en la serie). Implementa una función criptográfica de *hash* para el uso en comprobaciones de integridad de mensajes.
[16] MD5 es un algoritmo de reducción criptográfico de 128 bits ampliamente usado.

- ***Autorización**,* para los usuarios que han ingresado se les posibilita el acceso, solo a aquellos recursos o información permitida por los administradores del sistema informático y personal administrativo. Esto se consigue asignando perfiles de usuario y, niveles de autorización y acceso.

- ***Contabilidad,*** o también conocido con su término en inglés *Accounting*, permite que se registre la actividad del usuario. [2]

Desempeño, este requerimiento sugiere que, a más del sistema de seguridad de la red creada, los tiempos de respuesta sean adecuados y comparables con los de redes inseguras. Esto implica que se deba cumplir factores tales como: Calidad de Servicio (QoS), Acuerdos de niveles de servicio SLA (*Service Level Agreement*)[17], soporte de múltiples protocolos y confiabilidad.

Facilidad de Administración, este requerimiento indica que quienes gestionen este tipo de redes, lo realicen de manera rápida y efectiva. Con ello se ofrece un mejor desempeño en el monitoreo, mejorando la toma de decisiones y medidas adecuadas y necesarias en caso de encontrar anormalidades. Esto se puede lograr teniendo un sistema de administración centralizada, manejo de direcciones, manejo de *logs* de eventos, auditoría y reportes, entre las más recomendadas

Cumplimiento con estándares e interoperabilidad, las tecnologías que han llegado a ser estándares para la creación de VPNs son IPSec para encripción, MD5 para integridad, SOCKSv5 como servidor Proxy, autenticación con CHAP, intercambio de llaves a través de IKE, SKIP, Diffie-Hellman, firmas digitales con X.509. A más de éstos, se pueden utilizar estándares de facto y ampliamente difundidos como L2F, PPTP

[17] SLA o Acuerdo de Nivel de Servicio es un contrato escrito entre un proveedor de servicio y su cliente con objeto de fijar el nivel acordado para la calidad del servicio.

para la creación de túneles en sistemas Microsoft o también autenticación como RADIUS y TACACS+.

1.1.3 TECNOLOGÍAS PARA LA CREACIÓN DE VPNs

Las técnicas y tecnologías utilizadas para la creación y establecimiento de VPNs, varían dependiendo del nivel, que cada uno haya adoptado en los requerimientos antes señalados. En esta sección se revisará y analizará de manera breve las tecnologías más utilizadas en el ambiente de VPNs.

La *figura 1.3* permite visualizar los principales protocolos y su ubicación en el modelo de referencia OSI.

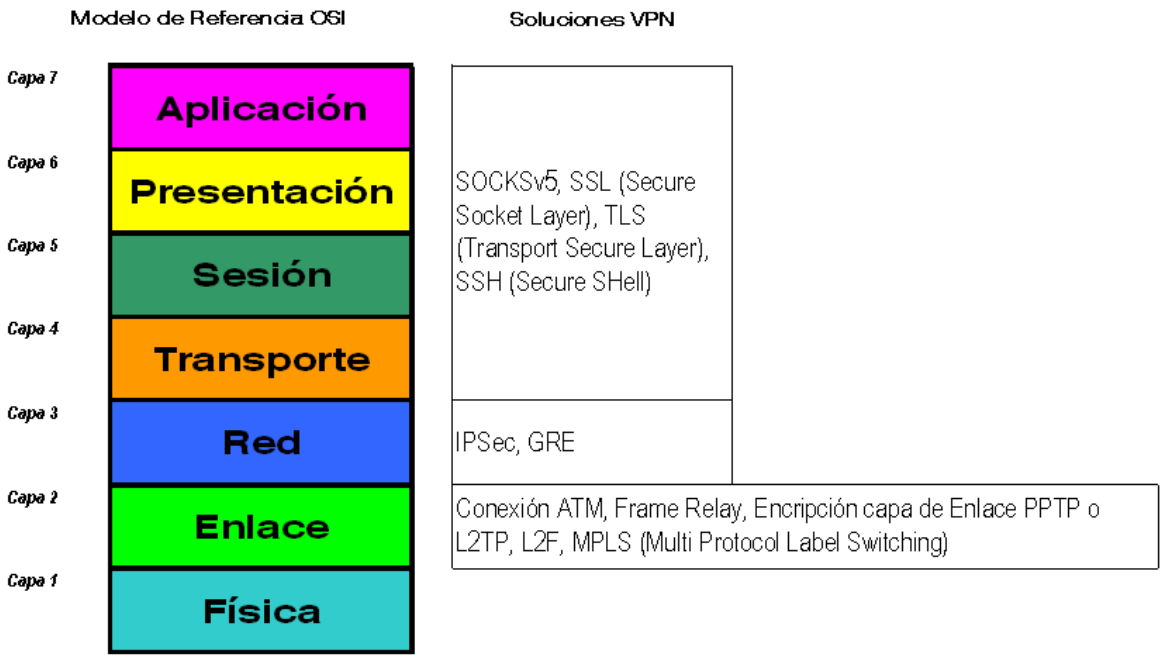


Figura 1.3 Ubicación de las soluciones VPN en el modelo de referencia OSI [2]

1.1.3.1 PPTP (*Point to Point Tunneling Protocol*)

Este protocolo se sitúa en la capa 2 del modelo de referencia OSI. Básicamente lo que hace, es utilizar el protocolo PPP *(Point to Point Protocol*) para encapsularlo en un datagrama IP usando el protocolo GREv2 (*Generic Routing Encapsulation Tunnels* versión 2).

Este protocolo fue propuesto por Microsoft y es ampliamente utilizado por fabricantes de equipos de conectividad y concentradores de VPNs.

El modo de operación, consiste en la apertura de dos canales. El primero permite el establecimiento, gestión y liberación del canal de datos. El segundo es un canal de datos, en donde se realiza la encapsulación de la información detallado en la *figura 1.4*.

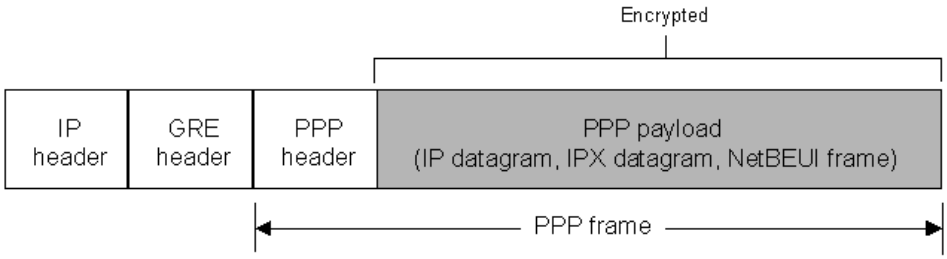


Figura 1.4 Esquema de encapsulamiento en PPTP [3]

PPTP como tal, no provee encripción, lo hace RC4 y MS-CHAP que utiliza MD4 como algoritmo de *hashing*. Un servidor PPTP abre el puerto TCP 1723, mientras que el cliente abre un puerto dinámico.

1.1.3.2 L2TP (*Layer 2 Tunneling Protocol*)

Esta mecanismo de formación de VPNs, fue propuesto por el IETF y combina PPTP y L2F en un solo estándar.

Las mejoras respecto a PPTP son:

- El *header* se comprime de 6 bytes a 4 bytes
- Se permite autenticación de usuarios
- Se pueden abrir más de un túnel entre dos sistemas, dando como resultado, que se pueda ofrecer diferente QoS.

Este protocolo está ampliamente difundido, especialmente en ruteadores CISCO y soportado en los sistemas Windows 2000 y XP.

El esquema de encapsulamiento en L2TP es similar a PPTP, con las respectivas variantes, que se presenta en la *figura 1.5*.

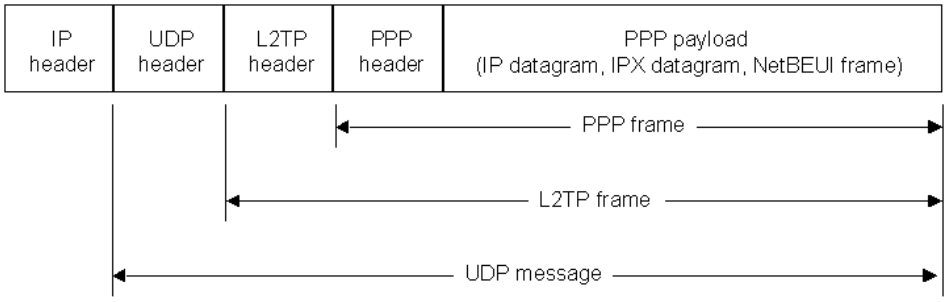


Figura 1.5 Esquema de encapsulamiento en L2TP [3]

1.1.3.3 IPSec (IP *Security extension*)

IPSec es un conjunto de protocolos diseñados para proveer seguridad basada en criptografía robusta para IPv4 e IPv6; de hecho IPSec está incluido en IPv6.

Su operación se fundamenta en las siguientes partes con sus respectivas descripciones:

> ***Protocolos de seguridad***, que desempeñan la función de proteger los datos contenidos en paquetes IP. Para este efecto se utilizan dos protocolos que son: *Authentication Header* (AH) y *Encapsulating Security Payload* (ESP).
>
> AH es un protocolo que provee autenticación del origen de los datos, así como verifica la integridad de éstos. MD5 o SHA son utilizados para garantizar la integridad de los paquetes.
>
> ESP provee de confidencialidad al tráfico de datos. Con este protocolo a más de encriptar el *payload*, también se encripta el *header*. La encripción se la realiza con cualquier esquema de encripción simétrica como DES y 3DES.

Manejo de llaves, proporciona un nivel más de seguridad, y para IPSec se pueden emplear diferentes tipos de sistemas de manejos de llaves. *Internet Key Exchange* (IKE) es por defecto, el sistema que tiene el manejo de llaves, aunque su principal función es el establecimiento y mantenimiento de asociaciones de seguridad. El manejo de llaves también realiza ISAKMP, OAKLEY. La combinación de estas últimas es el resultado de IKE.

Asociaciones de seguridad, es el primer paso antes de establecer una sesión segura entre dispositivos que soportan IPSec. Estas asociaciones comprenden la negociación de parámetros de seguridad como: funcionalidad de encripción, dirección IP de origen, algoritmos de encripción y *hashing*, llaves usadas para encripción y algoritmos de *hashing*, nombre o identificador de la entidad involucrada, protocolo de transporte, puertos de origen y destino. Esta negociación es unidireccional y perfectamente identificada por medio del SPI (*Security Parameters Index*)[18]. Está claro que si se requiere una negociación bidireccional, se necesitará una asociación de seguridad en cada sentido, en total dos. [2]

1.1.3.4 SSL (*Secure Sockets Layer*)

Es una tecnología de VPN que se ubica en la capa sesión del modelo de referencia OSI. Desarrollado por Netscape, provee seguridad en conexiones TCP utilizando de manera predeterminada el puerto TCP 443.

Las entidades participantes son: un servidor y un cliente web (cualquier navegador que soporte SSL). El resultado es la formación de un túnel seguro entre el navegador y el *Web Server*, ya que la integridad de la información se garantiza con algoritmos de *hash* y la confidencialidad se garantiza con algoritmos de encripción.

[18] En español Indice de Parámetros de Seguridad, es uno de los parámetros que identifican a las asociaciones de seguridad. Este índice es transportado en las cabecesar AH y ESP.

Cuando se inicia una sesión SSL, se realiza una encripción asimétrica para poder establecer el túnel seguro. Esto se garantiza con la participación de una tercera entidad, que es la Autoridad Certificadora.

Cuando se ha establecido el túnel seguro, la encripción pasa a ser simétrica, por cuestiones de optimización de recursos computacionales y de red.

Ésta fue una breve revisión de los aspectos teóricos más relevantes sobre VPNs. Se debe señalar que dentro de esta sección teórica no se ha incluido la tecnología MPLS, porque será objeto de revisión en el ítem *1.4 Futuro de las VPNs*.

1.2 SISTEMAS ACTUALES DE SEGURIDAD EN LAS REDES DE DATOS

En esta sección se tratará de analizar las diferentes actualizaciones y evolución que han tenido los sistemas de seguridad. Pero antes de continuar se debe indicar que estos sistemas de seguridad, sólo podrán ser lo bastante efectivos si se programan y planifican con adecuadas políticas de seguridad, lo cual incluye una modernización en la cultura de cada uno de los administradores y usuarios, de todos los niveles que componen una red corporativa.

Mencionado este aspecto, es preciso indicar que en esta sección se expondrá sobre las mejoras en los tradicionales sistemas de seguridad y los avances más relevantes y de rápida aceptación dentro del mercado.

1.2.1 SISTEMAS TRADICIONALES DE SEGURIDAD PARA LAS REDES Y EQUIPOS COMPUTACIONALES

Los sistemas de seguridad para las redes de datos, se han ido desarrollando para protegerse de las diferentes amenazas, a las que están expuestos los datos y recursos computacionales a través de la red de datos. El grado de avance y mejora dependerá de la gran habilidad de los creadores de nuevos y mejoradas

armas para penetrar sobre los sistemas informáticos, ya sean desde simples PCs hasta grandes sistemas de seguridad planificada.

El estar bien informado sobre las amenazas que circulan sobre las redes, permite, que las medidas a tomar para mitigar estos peligros, sean apropiadas, y mientras más se conozca sobre los peligros que existen en la red, será cada vez mejor la prevención y la respuesta.

Dentro de las amenazas más comunes se tienen:

- Anexos a mensajes enviados por correo electrónico infectados con virus.
- El intercambio de códigos de virus.
- *Firewalls* mal configurados.
- Ataques a la disponibilidad de los recursos de información existentes en la red (bancos de datos o *software* disponibles para ser descargados por los usuarios).
- Alteración de páginas *web*.
- El "repudio" y las estafas asociadas al comercio electrónico.
- Las vulnerabilidades de los sistemas operativos y la desactualización de los "parches" concernientes a su seguridad.
- Rotura de contraseñas.
- Suplantación de identidades.
- Acceso a páginas pornográficas, terroristas, etc.
- Robo y la destrucción de información.
- Pérdida de tiempo durante el acceso a sitios ajenos a la razón social de la entidad.
- El hecho de que herramientas de *hacking* y *cracking* se ofrezcan como *freeware*.

Ante todas estas amenazas, se ha desarrollado *software* que permite eliminar o reducir de manera puntual ciertas amenazas, como los virus, gusanos, troyanos y espías. Sin embargo al utilizar determinada herramienta de protección, el desempeño de los sistemas se reducen significativamente, tanto en recursos

computacionales locales (CPU, memoria, espacio en disco, etc), como también en el recurso de comunicaciones (ancho de banda, tráfico sobre la red y prioridades).

Cuando se tiene que proteger a una gran cantidad de usuarios, se hace necesario que los sistemas informáticos, no se vean afectados al tener que ejecutar este tipo de herramientas que permiten la protección. Es así que los sistemas convencionales de servicios anti-x (antivirus, antiespias, etc), no residan cada uno, en diferentes localidades físicas.

1.2.2 NUEVA GENERACIÓN DE SISTEMAS DE PROTECCIÓN PARA REDES DE DATOS

La nueva generación de sistemas de protección para redes de datos, se fundamenta, en que las soluciones más comunes de protección: *Firewalls*, VPNs, Antivirus e IPS[19], se ejecuten a nivel de *hardware*, administrado por un sistema operativo robusto y actualizable. Claro que esto dependerá de cada caso, ya que existen soluciones basadas en *software* que también realizan el mismo trabajo, y hasta un poco más, por ejemplo en el campo de la gestión y administración de la red.

Las soluciones para proteger las redes de datos, van desde aplicaciones de escritorio, pasando por servidores y equipos dedicados a la protección, hasta grandes sistemas de prevención y mitigación de amenazas, los cuales varían según la empresa fabricante de equipos y soluciones.

Empresas como CISCO, Fortinet, 3COM Tipping Point, Juniper, Astaro, IBM, Symantec, aplicaciones sobre sistemas Linux y UNIX, entre las más importantes, son las que han llegado con sus productos y soluciones de seguridad, a cubrir el mercado de protección de redes de datos, básicamente sobre redes IP.

[19] IPS (*Intrusion Prevention System*) es un dispositivo que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques.

1.2.2.1 Casos de estudio de sistemas de seguridad para redes de datos

Se analizarán tres ejemplos muy claros de protección, donde intervienen los nuevos métodos para protección, prevención, y respuesta ante amenazas y ataques. Se revisarán soluciones propuestas y comercializadas por las empresas CISCO, Fortinet y Astaro; estas tres propuestas buscan un mismo fin pero con variantes en sus metodologías y tecnologías aplicadas.

1.2.2.1.1 La Red de Autodefensa de CISCO: El Sistema de Defensa de Ataques [4]

Este sistema de seguridad, se basa principalmente, en concebir a la red de datos como un factor crítico dentro de los negocios, y que las empresas a su vez se ven en la obligación de enfrentar retos muy específicos de seguridad, que ponen en peligro su productividad y rentabilidad.

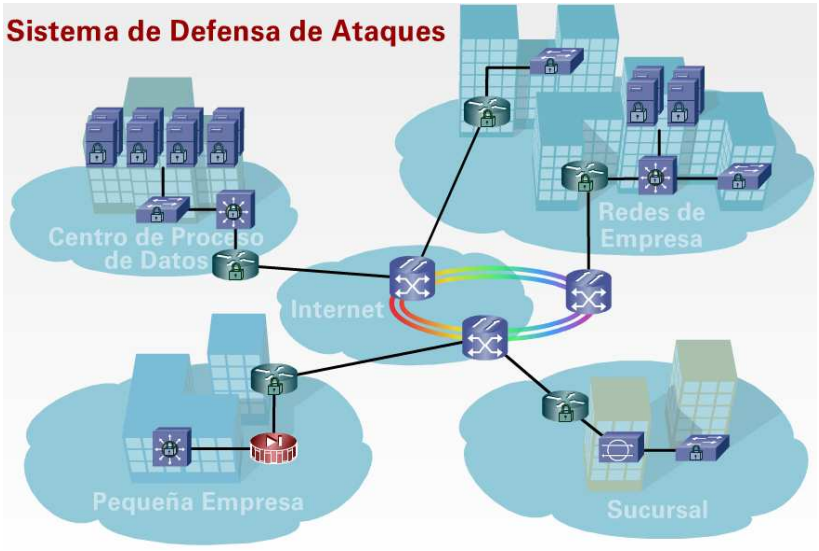


Figura 1.6 Esquema de red corporativa a ser protegida por el TDS [4]

Realizando un análisis de los ataques producidos por los llamados “Ataques de Día 0”, Denegación de Servicio (DoS) y Robo interno de información confidencial, se señala que le tomaría considerables cantidades de tiempo y dinero en recuperarse a una empresa, poniendo en peligro la estabilidad de la misma.

Ante esto, los negocios deben desplegar soluciones de seguridad más proactivas y autodefensivas con el objeto de identificar, prevenir y mitigar estas crecientes y costosas amenazas.

La solución que propone CISCO es el denominado Sistema de Defensa de Ataques (TDS – *Threat Defense System*), como parte de redes de autodefensa, mitiga e incluso previene que estas amenazas puedan afectar el normal funcionamiento de determinada empresa.

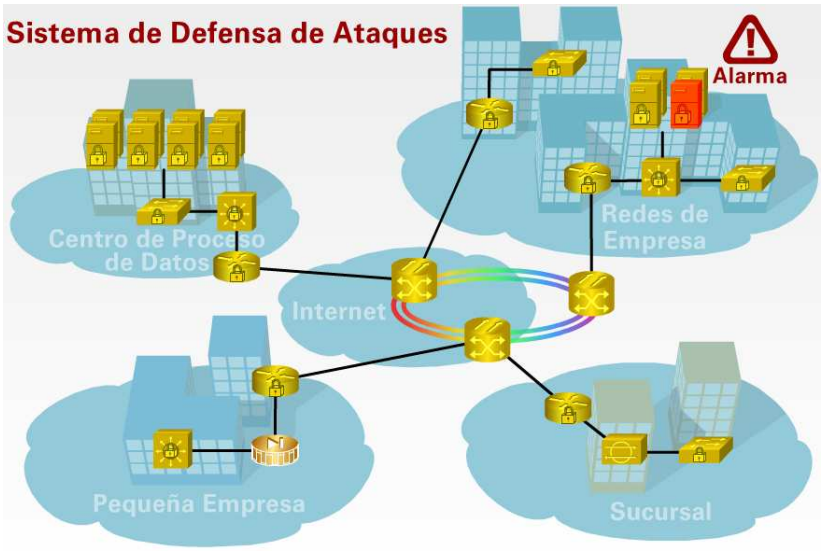


Figura 1.7 Todas las entidades principales conocen sobre un peligro inminente en ejecución sobre la red [4]

Este sistema protege a toda la red a través de la combinación de tecnologías avanzadas de seguridad, con inteligencia de redes IP, extendida por toda la infraestructura de red

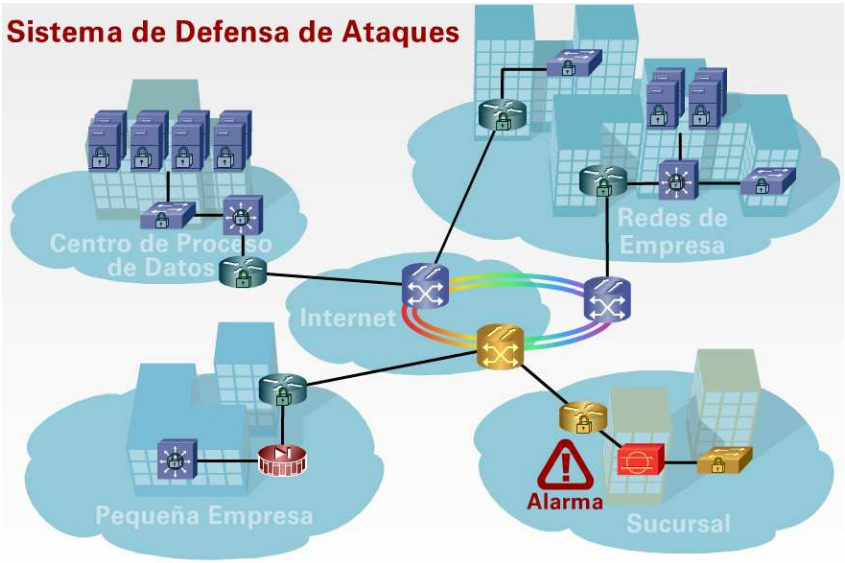


Figura 1.8 Los dispositivos más cercanos al peligro toman medidas inmediatas para mitigar tal peligro [4]

El TDS es una solución completa basada solamente en productos CISCO; sin embargo los criterios de defensa son aplicables entre diferentes fabricantes, siempre y cuando exista un estudio de ingeniería adecuado.

Este sistema integra seguridad, con el único fin de proteger y salvaguardar los bienes expuestos y que son dependientes de la red de datos. Para garantizar esta seguridad, la solución presentada consta de los siguientes elementos:

- *Seguridad en los clientes y servidores para proteger de ataques conocidos o Día 0*. En el *figura 1.9* se muestra que equipos finales como: servidores y de usuario, cuentan con la seguridad de tipo cliente proporcionada por el CSA[20].

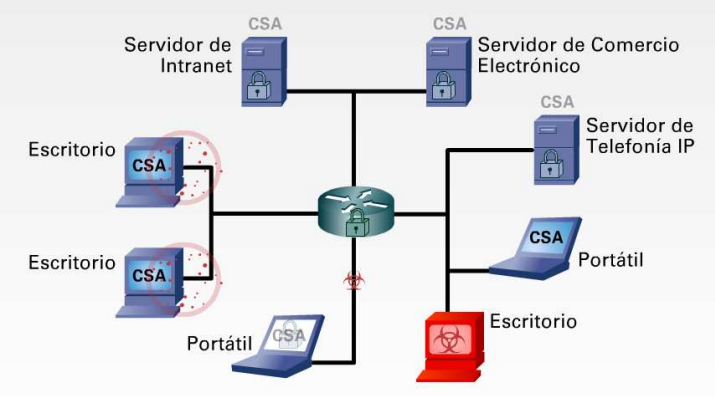


Figura 1.9 Seguridad en los equipos finales [4]

- *Tecnologías que están basadas en Firewalls para la seguridad perimetral*. Pueden tener varios segmentos de red conectados a un *Firewall,* lo que permite aislar la red interna de la red insegura como Internet; un ejemplo de un *Firewall* como equipo perimetral se observa en la *figura 1.10*.

[20] CSA (*Cisco Security Agent*) Es una aplicación de seguridad desarrollado por Cisco Systems para equipos servidores y de usuario.

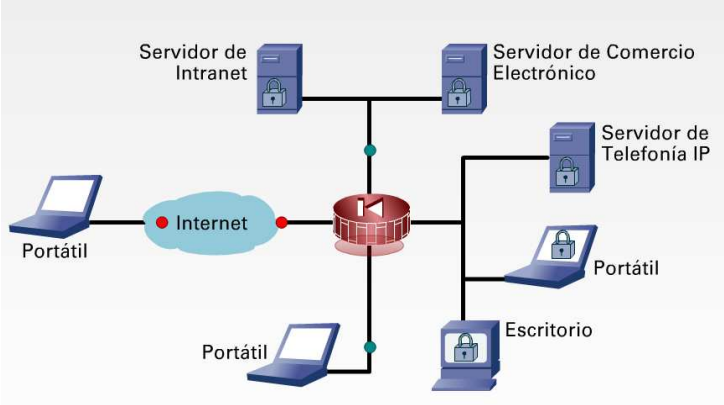


Figura 1.10 Tecnología de Firewalls [4]

– *Sistemas de prevención de intrusos (IPS), para detectar ataques maliciosos*. El IPS mostrado en la *figura 1.11* grafica el control de acceso de los datos de un segmento de red a otro.

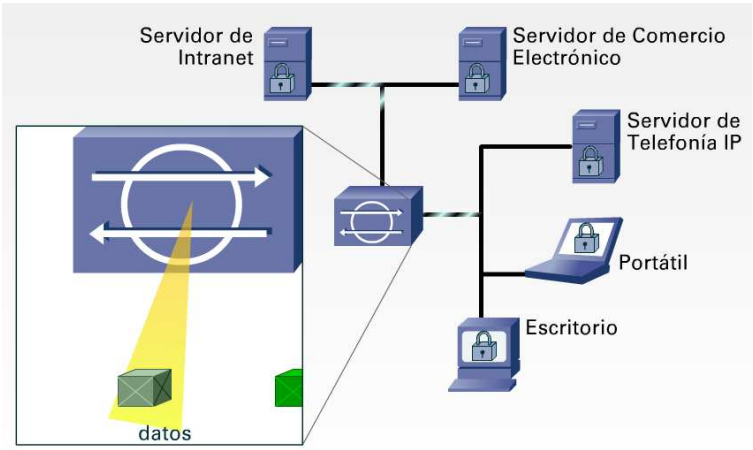


Figura 1.11 Sistemas de Prevención de Intrusos [4]

– *La mitigación de ataques distribuidos de Denegación de Servicio, para garantizar la disponibilidad de la red*. Los objetivos buscados para denegar el servicio, son servidores corporativos; éstos deben ser protegidos cuando se ha detectado la anomalía y las peticiones falsas de servicio deben ser rechazadas por el sistema de protección; esta acción de seguridad se la muestra en la *figura 1.12*.

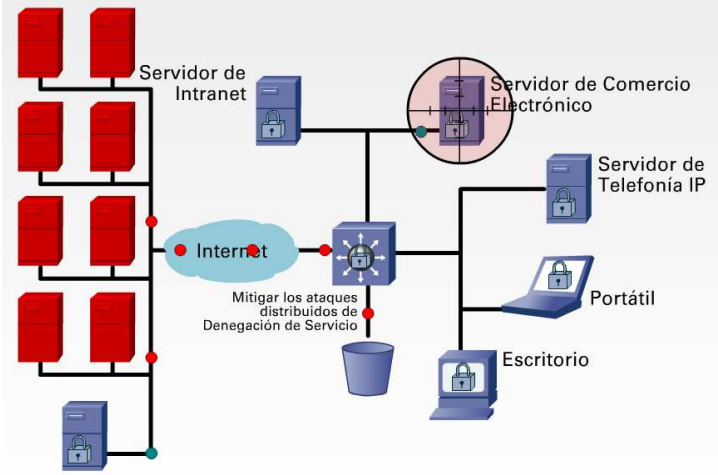


Figura 1.12 Mitigar los ataques distribuidos de Denegación de Servicio [4]

– *Seguridad de los contenidos para comprobar y proteger las aplicaciones WEB y servicios*. Mucha información no deseada o sin autorización puede ingresar a los equipos finales; por lo que es necesario contar con un dispositivo que verifique el contenido autorizado y que es accedido a través de los navegadores *WEB* de los equipos de usuario o servidores; el dispositivo de control de contenido o Seguridad de Contenido está entre el equipo final y la red no segura como el Internet (Ver *figura 1.13)*.

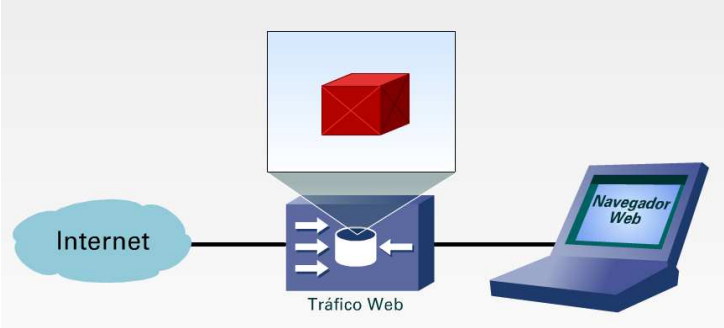


Figura 1.13 Gráfica del control en la Seguridad de Contenidos [4]

– *Mecanismos inteligentes de routing para priorizar y clasificar tráfico de red*. Optimizar el tráfico permite mejorar la disponibilidad de la red; así en la *figura 1.14* se grafica la intervención de un *router* con priorización y clasificación de tráfico.

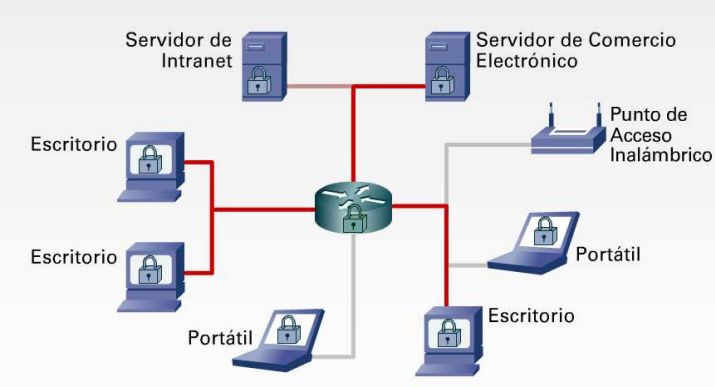


Figura 1.14 Inteligencia en Routing [4]

– *Tecnologías de conmutación, para la defensa de ataques internos*. En la *figura 1.15* se observa que un equipo que no es parte de la red corporativa quiere ingresar a la red, esta acción es controlada y rechazada por el *switch*. Se debe realizar este tipo de acciones ya que el permitir ingresar libremente a una red puede ser muy riesgoso para los intereses de la corporación.

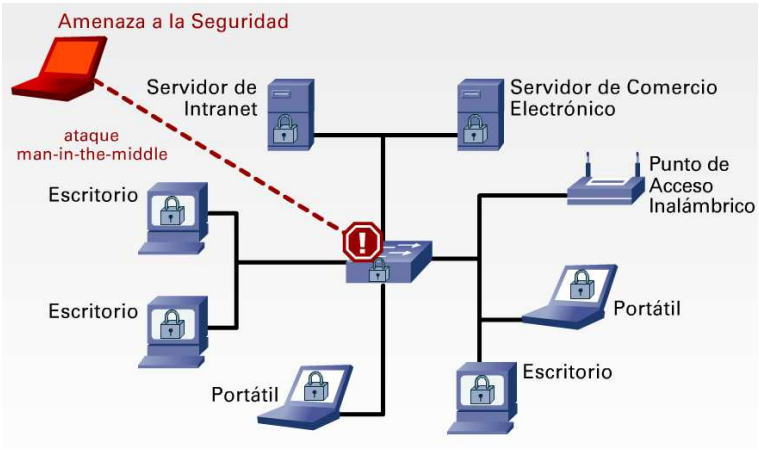


Figura 1.15 Tecnología de Conmutación [4]

Todos estos elementos son administrados y monitorizados por un sistema central de gestión escalable; en la *figura 1.16* se muestra el sistema de seguridad completo y se indica que está gestionado por una consola.

Debido a la gran gama de equipos que produce y distribuye CISCO alrededor del mundo, es lógico que pueda presentar una solución basada en cada uno de los elementos que compone el TDS.

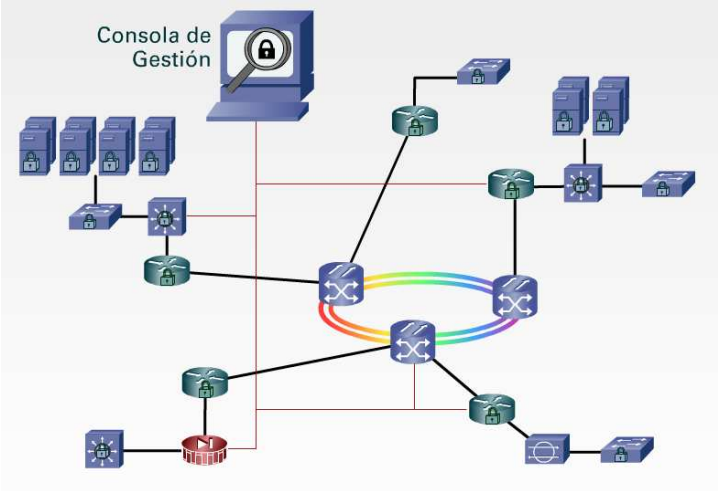


Figura 1.16 Monitorización y Gestión Centralizada [4]

La propuesta presentada cubre en gran parte, las amenazas a las que están expuestas las empresas a través de sus redes corporativas. Para una empresa que trabaje sobre sistemas CISCO le conviene adoptar este tipo de solución, ya que tendría que complementar la seguridad con los elementos faltantes. Pero para una empresa que no tiene un sistema homogéneo, en equipos de conectividad, adoptar desde cero un sistema como éste, es digno de analizar, evaluar y decidir si es adecuado, ya que el factor económico, en última instancia, tiene una gran influencia a la hora de implementar cualquier sistema informático.

1.2.2.1.2 Nueva generación de dispositivos de seguridad en tiempo real Unified Threat Management (UTM) o Gestión Unificada de Amenazas. Caso Fortinet con sus equipos FortiGate

Dado que en muchos casos, los sistemas de redes datos son heterogéneos, y el factor interoperabilidad es muy débil, aparecen soluciones integrales de seguridad, basadas en equipos que pueden mitigar las amenazas de seguridad de manera casi independiente. Éste es el caso de las soluciones presentadas por Fortinet con su gama de equipos FortiGate. Estos equipos se basan en el principio de detener en tiempo real los ataques de contenido, del tráfico que entra y sale de los accesos principales de una red corporativa.

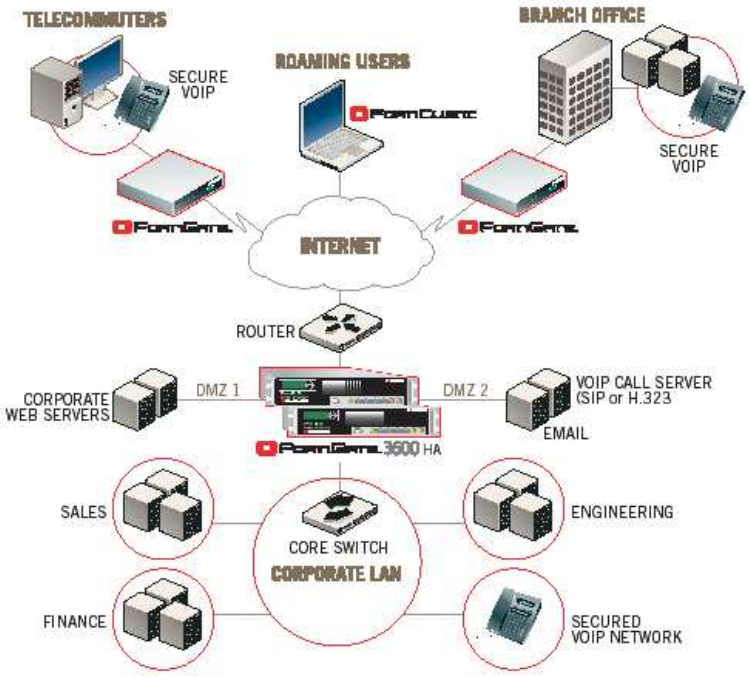


Figura 1.17 Ambiente de red corporativa con seguridad basada en Fortinet [5]

La *figura 1.17* muestra que, a diferencia de la solución de TDS de CISCO, Fortinet basa su seguridad en un sistema centralizado, donde el equipo ocupa la parte perimetral de la red. Dependiendo de las posibilidades económicas de las empresas, éstas pueden adoptar sistemas de alta disponibilidad, es decir, más de un equipo de seguridad perimetral, en línea.

Al interior de los equipos FortiGate, se maneja una compleja solución basada en *hardware*, donde se provee de los siguientes servicios: Antivirus, *Firewall*, IPS e IPSec-VPN.

Cada uno de estos servicios de seguridad es ejecutado en tiempo real, ya que el procesamiento es directo en *hardware* y gestionados a través de un sistema operativo que permite la configuración de cada uno de los parámetros que implican los servicios antes mencionados.

El obtener certificación internacional por la ICSA Labs, en los servicios de Antivirus, *Firewall*, IPS e IPSec VPN, indica que cumple con normas a nivel

internacional, lo que garantiza tanto los servicios como la compatibilidad con otros fabricantes.

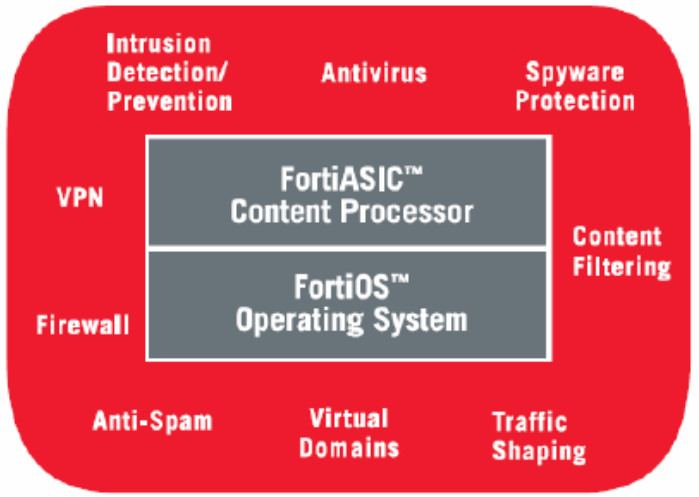


Figura 1.18 Arquitectura de ASIC acelerado [5]

A más de ofrecer estos servicios en un solo equipo, el sistema operativo cuenta con la capacidad de configurar y ejecutar otro tipo de servicios como Anti-*Spyware*, *Traffic Shapping* (QoS), *Anti-Spam*, Dominios Virtuales, Filtrado de Contenido, entre lo más destacado en protección, e innovación en manejo de tráfico; en la *figura 1.18* se muestra la arquitectura en la que se basa el funcionamiento de las unidades de seguridad Fortigate.

La solución que ofrece Fortinet a los clientes, se amplia con clientes basados en *software*, para aquellos usuarios remotos que necesiten integrarse a un ambiente con este sistema de seguridad, con el único propósito de mejorar el nivel de seguridad.

Esta solución permite visualizar el avance que ha tenido las seguridades en las redes de datos. Cabe señalar que no es la mejor ni la peor de las opciones, esto es muy relativo, y estos equipos serán óptimos en su funcionamiento, siempre y cuando técnicos calificados en seguridades en redes de datos puedan dominar el manejo de este equipo. Caso contrario cualquier solución por más sofisticada que sea, sin un adecuado manejo y administración, será tanto o más deficiente como los primeros sistemas de seguridad para redes de datos.

1.2.2.1.3 Soluciones de seguridad para redes de datos basadas en sistemas Operativos. Caso distribuciones LINUX: ASTARO SECURITY GATEWAY[6]

La solución de seguridad que ofrece ASTARO, al mercado de la redes de datos, está basada en *software*, y usa la idea de los sistemas de seguridad perimetral. Se trata de un sistema robusto, ya que entre sus características ofrece la mayoría de los servicios proporcionados por Fortinet, pero con la gran diferencia, que el motor principal de estos servicios es *software* y no *hardware*.

La diferencia radica, en que al ejecutar aplicaciones como por ejemplo IPSec-VPN en *hardware*, la transacción es más rápida, mientras que en un Sistema Operativo (SO), el procesamiento principal lo hace a través de *software* y luego de esto lo pasa a *hardware*, para que circule por la red.

No con esto, se quiere decir que esta solución es mala o deficiente, lo que se trata de indicar, es que este sistema propuesto es adecuado para redes de datos con un cierto límite de usuarios, y de carga de tráfico, por debajo de los sistemas de seguridad basados en *hardware*.

Las ventajas que este sistema trae consigo, es el de poder gestionar aspectos como, utilización del ancho de banda, usuarios conectados a los servicios que involucran este equipo, ataques, auditoria, etc., ya que se trata de un equipo de propósito general, donde se le pueden agregar más servicios.

1.3 APLICACIONES MULTIMEDIA SOBRE VPNs

Una vez revisado algunos métodos para enviar información entre sitios de red privados, a través de redes no seguras, es conveniente analizar la prioridad que tienen ciertas aplicaciones, como aquellas que necesitan enviarse en tiempo real.

Cuando se transfiere información, ésta puede ser de diferente naturaleza, y por su manejo debe ser diferente, básicamente empleando priorización de tráfico.

Es así que la información de tipo multimedia como voz y video, tienen un trato especial sobre la red de datos. La información de voz y video, son aplicaciones que necesitan llegar en tiempo real a su destino.

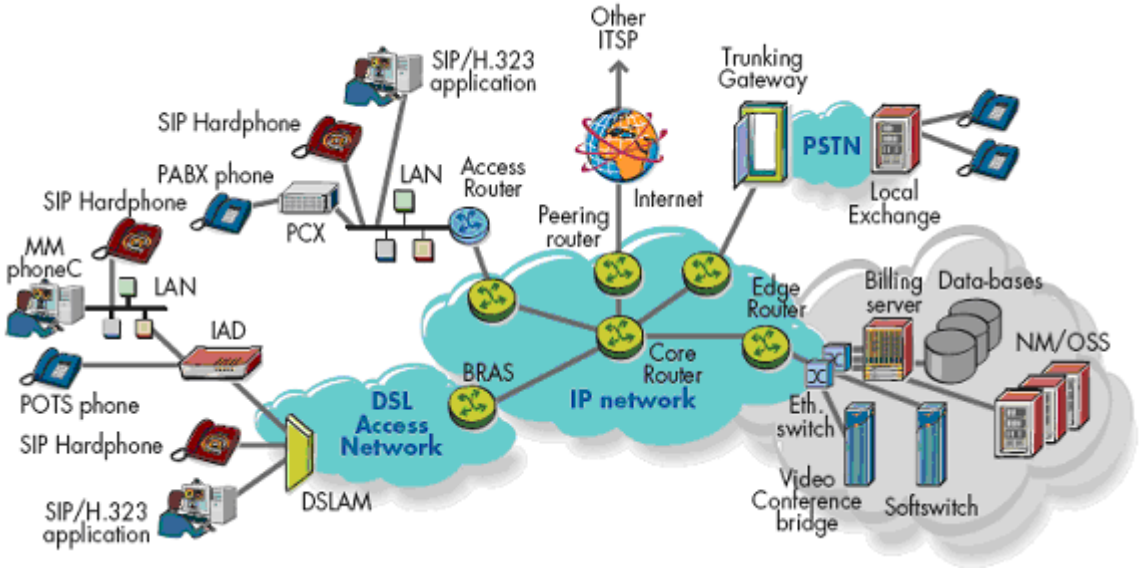


Figura 1.19 Arquitectura de redes de próxima generación (NGN) [7]

Para aplicaciones en tiempo real, el retardo es un factor importante, ya que éste mide la factibilidad de ser implementado sobre una red de datos. Otro aspecto es el consumo de ancho de banda de los enlaces, necesario para transportar el tráfico en tiempo real. Un enlace saturado degradará la calidad de voz o imagen, por lo cual, se hace necesario emplear mecanismos para aplicar Calidad de Servicio (QoS) sobre los enlaces.

Cuando este tipo de aplicaciones se ejecutan sobre enlaces sin seguridad, son relativamente rápidos, pero no confiables y de un alto riesgo. No se puede poner en riesgo cierta información confidencial ante las amenazas existentes en las redes y sistemas informáticos.

En la *figura 1.19* se puede observar que la tendencia de las nuevas redes de datos es, transportar tráfico de información de diferente naturaleza, es así que los nodos principales de comunicación como son *routers*, *gateways*, *switches* necesitan manejar priorización de tráfico, de tal manera que se pueda optimizar el

uso de la capacidad de canal de comunicaciones y brindar servicio agregado de seguridad.

La circulación de este tipo de tráfico por enlaces VPNs, tiene un retardo mayor comparado con enlaces no-VPN de iguales condiciones, pero son confiables, dependiendo del tipo de tecnología aplicada, para formar enlaces VPN. Para compensar este retardo las NGNs son aplicadas principalmente sobre enlaces que van desde los 10 Mbps hasta 1 Gbps, lo cual hace que estos retardos no sean un problema.

Cuando los enlaces de alta velocidad son del tipo Ethernet, cubriendo grandes zonas y con los equipos adecuados, estas redes se transforman en metro - Ethernet.

La causa del retardo se debe a que al transitar información por un túnel VPN, cualquiera que ésta sea, implica mayor *overhead* en los paquetes creados, procesamiento de encripción (sitio fuente), y desencripción (sitio remoto). Son procesamientos inherentes de la comunicación, que son tolerables para el paso de información de tipo, archivo binario, texto, tráfico http, *e-mail*, etc. Pero para voz y video en tiempo real, es muy considerable el retardo, por lo que se recomienda obtener accesos de alta capacidad, a Internet o a cualquier otra red pública.

Una vez entendido que las aplicaciones en tiempo real necesitan un trato diferente, se analizarán estas aplicaciones y algunos conceptos importantes, que son tomados en cuenta para poder generar tráfico en tiempo real sobre VPNs

1.3.1 APLICACIONES DE VOZ SOBRE VPNs

Las aplicaciones de voz, en la actualidad, son las aplicaciones multimedia, más comunes sobre las redes de datos y las de mayor antigüedad. Sin embargo, el transporte de este tipo de aplicaciones sobre enlaces VPN no es muy común, ya

que no hay mucha experiencia para aplicaciones multimedia sobre este tipo de enlaces, donde no se garantiza niveles de calidad en la transmisión.

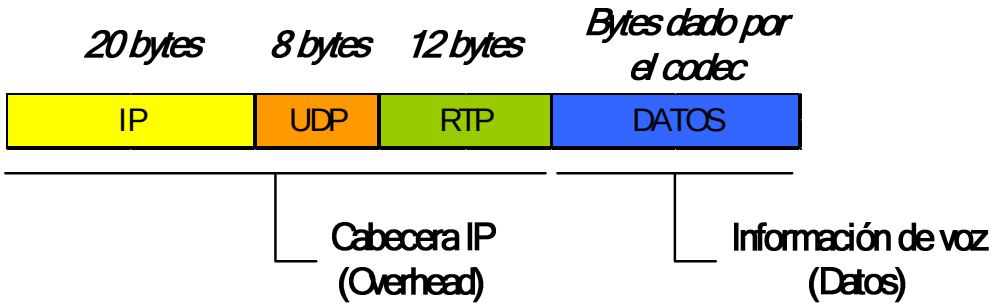


Figura 1.20 Formato de un paquete IP que encapsula un segmento que contiene información de voz

En la actualidad, existen nuevos equipos de comunicaciones que permiten que el tráfico que contiene voz, o cualquier otra aplicación de naturaleza multimedia, atraviese y llegue a su destino, utilizando mecanismos de priorización de tráfico.

Códec	Bandwidth[21] (kbps)	Periodo de muestro (ms)	Tamaño de la Trama (bytes)	Tramas / Paquete	Ethernet Bandwidth (kbps)
G.711 (PCM)	64.0	20.0	160	1	95.2
G.723.1A (ACELP)	5.3	30.0	20	1	26.1
G.723.1A (MP-MLQ)	6.4	30.0	24	1	27.2
G.726 (ADPCM)	32.0	20.0	80	1	63.2
G.728 (LD-CELP)	16.0	2.5	5	4	78.4
G.729A (CS-CELP)	8.0	10.0	10	2	39.2
AMR (ACELP)	4.8	20.0	12	1	36.0
AMR (ACELP)	7.4	20.0	19	1	38.8
AMR (ACELP)	12.2	20.0	31	1	43.6
AMR-WB/G.722.2 (ACELP)	6.6	20.0	17	1	38.0

Tabla 1.1 Códecs para voz con la cantidad de bytes generados y ancho de banda necesario para ser transportados dentro de una red Ethernet [8]

Para poder transmitir en idénticos niveles de calidad, al igual que sobre enlaces no seguros, las aplicaciones de telefonía IP y en general Voz sobre IP, necesitan utilizar códecs que permitan adecuar la información original digitalizada, en forma

[21] El término Ancho de Banda (*Bandwidth*) es un parámetro de ocupación del canal que es medido en *hertzios,* sin embargo a lo largo de este proyecto se referirá a la capacidad de transmisión medida en bps, kbps, Mbps o Gbps.

de voz sobre un canal de datos, eliminar la ausencia de voz y aumentar el ancho de banda por donde circulará el tráfico que contiene la voz.
Para visualizar de mejor manera de cómo estaría conformada la información de voz encapsulada por la cabecera IP, se puede observar la *figura 1.20*:

En la *figura 1.20* se puede apreciar que la información de naturaleza de voz, es encapsulada por el tipo de aplicación (protocolo RTP), asociado por el servicio de UDP y que al final es completado por información del protocolo IP.

Como se conoce, este tipo de aplicaciones de tiempo real, son tolerables a errores en los paquetes (hasta determinado número de fallos), pero no al retardo, es así que UDP se convierte en el protocolo ideal para su transporte de extremo a extremo.

Dependiendo del códec utilizado, el tamaño del paquete variará, y esto determinará si es aplicable en determinado tipo de enlace.

La *tabla 1.1* muestra la cantidad de ancho de banda necesario para determinado códec, dentro de una red Ethernet.

Entre IP, UDP y RTP, la cabecera del paquete tendrá al menos 40 octetos o bytes fijos, y que serán agregados a los datos según el orden de encapsulamiento.

Con la utilización de VPN, el tráfico de voz se verá modificado, ya que la cabecera del paquete se incrementará según la tecnología utilizada para formar VPNs.

1.3.2 APLICACIONES DE VIDEO SOBRE VPNs

Las aplicaciones de video que utilizan como medio de transporte una red de datos, ya sea ésta de cobre, fibra óptica, o medios inalámbricos, están basadas en el mismo principio de prioridad que necesitarían las aplicaciones de voz, ya antes mencionadas.

En síntesis el destino de las redes privadas virtuales en conjunto con aplicaciones multimedia, tienen un amplio campo en el desarrollo.

En la *figura 1.21* se presenta un esquema de las nuevas redes donde se prioriza la seguridad, manejando *backbones* MPLS, y un acceso al Internet con un nivel adecuado de seguridad.

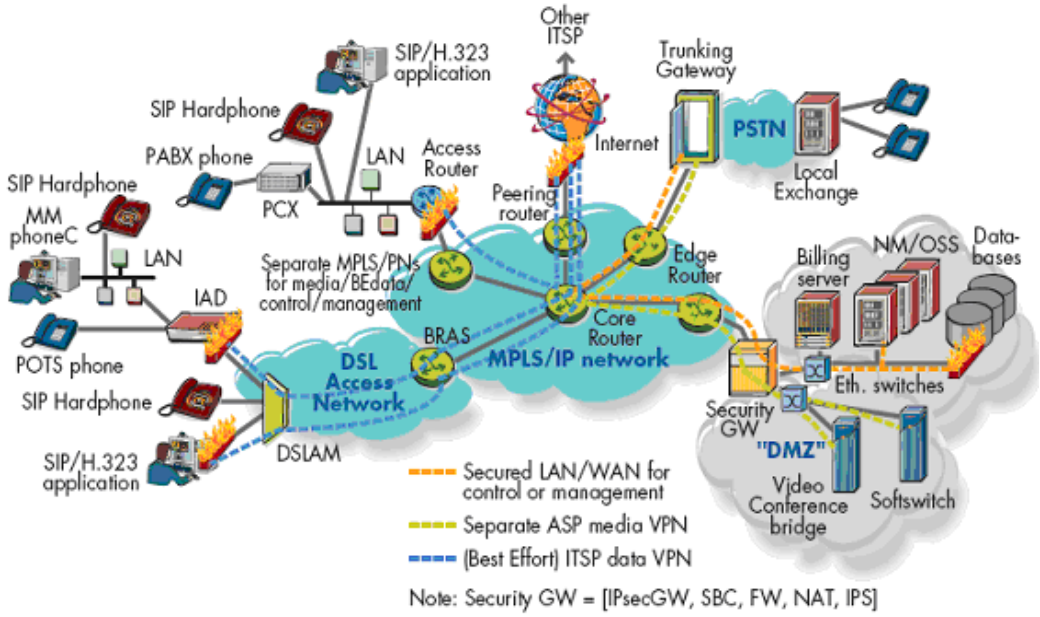


Figura 1.21 Arquitectura de redes de próxima generación (NGN) con MPLS como red núcleo y sistemas de seguridad [7]

1.4 FUTURO DE LAS VPNs

Las VPNs desde su creación han ido evolucionando, y desde su concepción han demostrado ser muy flexibles y escalables. Las actuales tecnologías que se utilizan para formar VPNs, pueden evolucionar a versiones avanzadas, donde se pueda agregar o mejorar servicios para el intercambio de información, de manera segura y confiable.

De acuerdo con el avance de nuevas aplicaciones, y nuevos requerimientos administrativos en las empresas, las VPNs pueden llegar a satisfacer todas estas necesidades. Es el caso de los empleados "*teleworkers*", que han crecido de manera considerable en varios países de Europa, Asia y América del Norte. América Latina no está lejos de este tipo de requerimientos, ya que los espacios

en oficinas y edificios, parqueaderos, el tráfico formado en las autopistas, es un problema de las grandes ciudades del mundo.

Al implementar VPNs con tecnología robusta, como por ejemplo MPLS, se podrá disponer de mejores resultados en la transmisión de datos y QoS para aquellas aplicaciones de misión crítica según la empresa o negocio.

Al mejorar el medio de transporte para los datos, las empresas designarán aquellos empleados que están asociados a actividades en las cuales su presencia dentro de la edificación, oficina o lugar de trabajo, no es necesaria, y que desde sus hogares puedan realizar las tareas cotidianas de una manera segura y confiable; valga la aclaración todo esto concerniente a transporte de la información por el sistema de comunicaciones.

Para hablar del futuro de las VPNs se puede referir a los casos de alto grado de evolución como lo son las tecnologías de SSL y MPLS. Dentro de estas tecnologías se ve un gran avance en las aplicaciones que ya pueden circular bajo sus tecnologías.

Para describir estos avances, a continuación se detallan las mejoras incluidas tanto en SSL como en MPLS, no sin antes hacer una explicación de cómo funcionan estas tecnologías en su esencia.

1.4.1 SSL-VPN

SSL es una tecnología que desde su creación, fue la solución para aplicaciones que necesitaban cierto nivel de seguridad, sencillo uso y configuración rápida, como por ejemplo, sitios *Web*, conexión vía Telnet y FTP. SSL contempla una configuración de cliente basada sobre un navegador de Internet, el cual posea capacidades de establecer sesiones seguras y soporte de cifrado de hasta 128 bits.

Los retos para SSL fueron creciendo, en el hecho de que por su facilidad de realizar una sesión segura, se requería ampliar el conjunto aplicaciones; es así que surge una nueva tendencia para la formación de túneles VPN, denominados SSL-VPN.

1.4.1.1 Formas de Conexión SSL

Para el establecimiento de enlaces VPN, SSL presenta tres modos para establecer el acceso:

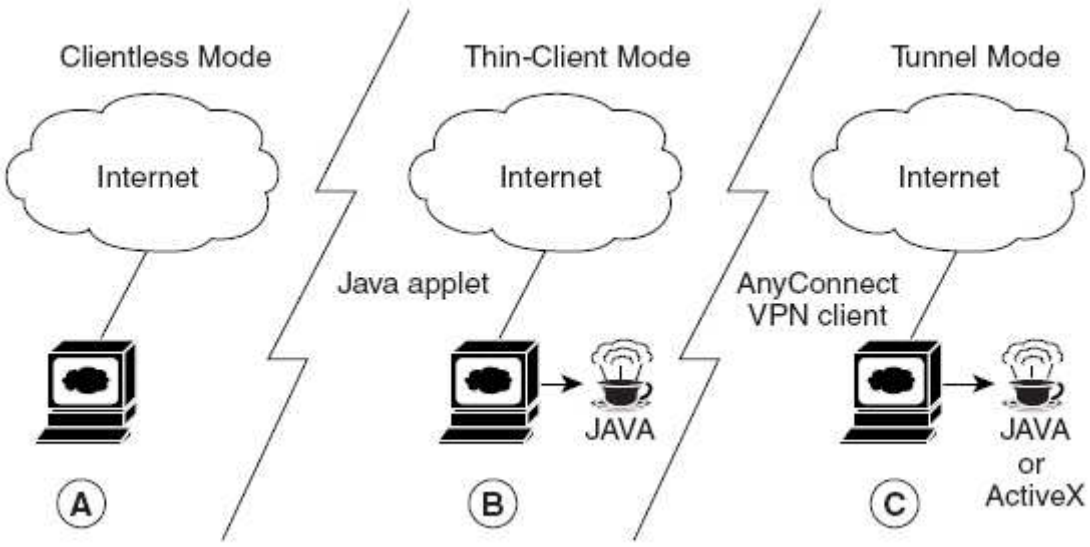


Figura 1.22 Tipos de Clientes para el acceso a través de VPN –SSL [9]

- ***Clientless*.** Provee un acceso seguro a recursos *web* privados. Este modo es muy usado ya que se accede a través de un *web browser*, como Internet Explorer, Mozilla, etc., a sistemas de bases de datos, y otras herramientas que contengan una interfaz *web* de usuario.[9]

- ***Thin Client* (Puerto de envío basado en un Java Applet)**. *Thin Client* extiende la capacidad de las funciones criptográficas del *web browser* para permitir el acceso remoto a aplicaciones basadas en TCP como *Post Office Protocol* versión 3 (POP3), *Simple Mail Transfer Protocol* (SMTP), *Internet Message Access Protocol* (IMAP), Telnet, y *Secure Shell* (SSH). [9]

- ***Modo Túnel***. El modo Túnel de Cliente ofrece un soporte considerable de aplicación a través de su cliente de próxima generación SSL-VPN (un *software* JAVA o control ActiveX). Este modo entrega una configuración ligera de SSL-VPN, centralmente configurado y con apoyo fácil en el establecimiento de un túnel para el cliente. Además proporciona el acceso de capa de red a prácticamente cualquier aplicación.[9]

La accesibilidad de aplicación de SSL-VPN es algo limitado con relación a VPNs basadas en IPSEC; sin embargo, las VPNs basadas en SSL proporcionan el acceso a un crecimiento de aplicaciones de *software* comunes, incluído el acceso de página *web*, servicios habilitados por la *web*, como acceso de archivos, *e-mail*, y aplicaciones basadas en TCP (por vía de un *applet ThinClient*). VPN basado en SSL requiere cambios leves en el volumen de trabajo de usuario porque algunas aplicaciones son presentadas por una interfaz de navegador *web*, no por su GUI natal. La ventaja para SSL-VPN viene de la accesibilidad de casi cualquier sistema conectado por Internet sin tener que instalarse software de escritorio adicional.

En la *figura 1.22* se pueden apreciar los tres modos de acceso SSL-VPN.

SSL-VPN aprovecha las facilidades de SSL para poder formar VPNs sin muchas dificultades.

Esto lleva a otros tipos de problemas, como por ejemplo, el cumplimiento de las horas de trabajo, la presencia, etc., aspectos que antes de implementarse deberán ser analizados, tanto por los departamentos o áreas correspondientes a la administración del personal y por supuesto a los responsables de la tecnología aplicada.

El futuro de las VPNs, más allá de crecer tecnológicamente, será un tema de contenido social, en el que mientras se desarrollen mejoras en las tecnologías para la formación de VPNs, las costumbres de las personas irán cambiando y adaptándose.

1.4.2 VPNs BASADAS EN LA TECNOLOGÍA MPLS

La tecnología MPLS es un claro ejemplo de adaptabilidad y escalabilidad para el desarrollo de VPNs actuales y futuras.

Este tipo de VPNs se puede describir como, la combinación de la inteligencia de enrutamiento con el desempeño de *switching* o conmutación, lo que provee significantes beneficios a los proveedores de servicio que cuentan con arquitecturas IP nativas existentes, arquitecturas nativas IP con ATM existentes, o una mezcla de otras tecnologías de capa 2. Las VPNs de capa 3 basadas en MPLS conforman un modelo *peer-to-peer* que usa BGP (*Border Gateway Protocol*), para distribuir información VPN relacionada. Todo esto está basado en la recomendación RFC 2547bis especificación para BGP de la IETF, la cual define una solución VPN que usa MPLS para enviar tráfico al cliente usando etiquetas por cliente. BGP distribuye información de ruta a través del *backbone* de la red del proveedor, así que el proveedor participa dentro y gestiona la información de enrutamiento del cliente.

Una ventaja primaria con la que cuenta MPLS es el de proveer escalabilidad al soportar el despliegue de VPNs tanto pequeñas y de muy grande escala; se puede mencionar en el orden de diez mil VPNs sobre la misma arquitectura de red principal.

Adicional a la escalabilidad, este beneficio incluye calidad de servicio de extremo a extremo, una corrección rápida de enlace y falla de nodo, protección de ancho de banda, y una función para despliegue adicional de servicios de valor agregado.

La tecnología MPLS también simplifica la configuración, gestión, y disponibilidad, ayudando al proveedor de servicio a una entrega altamente escalable, diferenciada, en servicios basados en IP de extremo a extremo. Por ejemplo, el proveedor de servicio puede ofrecer SLAs para permitir ingeniería en el tráfico MPLS y capacidad de rutas rápidas en el corazón de la red. Junto con el servicio ofrecido por la VPN-MPLS, el proveedor de servicio también puede ofrecer

servicio de *multicast*, con replicación de paquetes desde un solo origen a destinos múltiples, permitiendo *broadcasts* de voz y video, por ejemplo.

La tecnología MPLS (conmutación por etiquetas multiprotocolo) aparece a finales de los años 90, y con ésta aparecen diferentes tipos de VPNs. La clasificación puede ser de diferentes formas; una de las más comunes, está basada en el servicio que se está ofreciendo al cliente. Este servicio es multipunto o punto a punto de capa 2 o capa 3, y con esto se generan los siguientes tipos de VPN:

- ***VPN multipunto de capa 3 o VPNs IP***. Se denominan normalmente como VPRN (Redes Enrutadas Privadas Virtuales). [10]
- ***VPNs punto a punto de capa 2***. Estas consisten básicamente en una colección de VLLs (Líneas alquiladas virtuales) distintas o PWs (*Pseudowires*).[10]
- ***VPNs multipunto de capa 2***, o VPLS (Servicios LAN Privados Virtuales).[10]

Las VPNs IP basadas en MPLS, introducidas hace algunos años, disfrutan actualmente de un crecimiento saludable. Los dos puntos fuertes de este servicio VPN son su naturaleza multipunto y su soporte de IP. Las VLLs, introducidas más recientemente, ofrecen una clara migración de las tradicionales VPNs de FR/ATM (*frame relay*/modo de transferencia asíncrona) a la red MPLS convergente sin sustituir equipo en las instalaciones del cliente y sin afectar a la experiencia de servicio del cliente.

Como las VPNs IP basadas en MPLS, el VPLS es un servicio multipunto, pero a diferencia de las VPNs IP éste puede transportar tráfico no-IP; también se beneficia de las bien conocidas ventajas de Ethernet. VPLS también se utiliza dentro de una red de proveedores de servicios para agregar servicios a suministrar a clientes de empresas y residenciales.

1.4.2.1 VPN multipunto de capa 3 o VPNs IP [10]

Dentro de las clasificaciones de VPNs está claro que existen dos grupos bien definidos, y que son las VPNs de capa 2 y las VPNs de capa 3; en la *figura 1.23* se muestra la clasificación de las VPNs. Las VPNs de capa 3 como IPSec tienen un concepto diferente respecto a las basadas en MPLS. Es por eso que se analizará lo más relevante de las VPNs de capa 3 basadas en PE (*Provider Equipment* o equipo de proveedor).

Las VPNs de capa 3 basadas en el PE conectan varios sitios, permitiéndoles hacer comunicaciones basadas en direcciones IP. Los *routers* PE son responsables del mantenimiento de contextos IP diferentes para cada VPN y del aislamiento del tráfico de distintas VPNs. En consecuencia, los dispositivos CE (*Customer Equipment* o equipo de cliente) no requieren ningún cambio, ni de ninguna funcionalidad adicional para conectarse a una VPN en lugar de a una red privada clásica.

La solución de VPN de BGP (protocolo de pasarela de frontera)/MPLS IP es el método más popular de VPN basada en PE. No sólo es el único adoptado como estándar propuesto por el IETF (Grupo de Tareas sobre Ingeniería de Internet), sino que también está soportado por los principales fabricantes de *routers* IP.

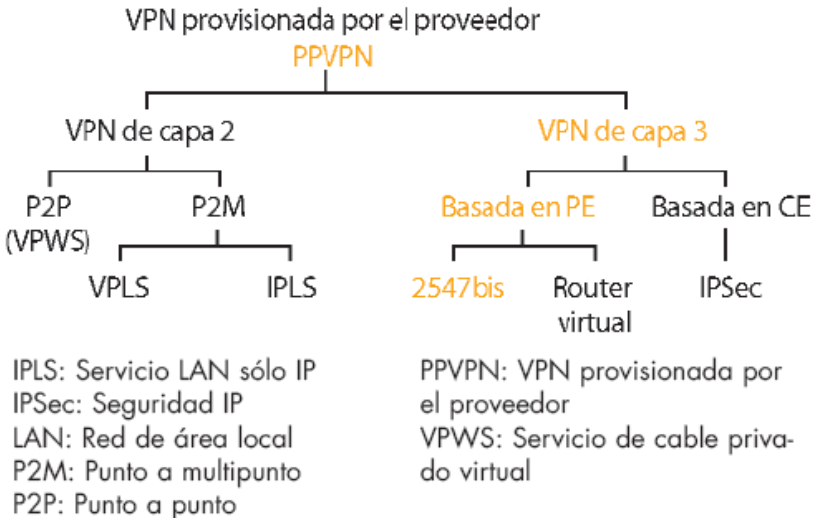


Figura 1.23 Clasificación de VPNs [10]

En el método BGP/MPLS, el proveedor de servicios usa BGP para distribuir información de alcance IP entre sitios que pertenecen a la misma VPN. A continuación se detallan algunos de los aspectos generales de VPN BGP/MPLS IP.

1.4.2.1.1 Tablas de encaminamiento y de envío virtual múltiples en el PE [10]

Si dos VPNs no tienen sitios comunes, pueden tener solapamiento de los espacios de direccionamiento; es decir, dos sistemas en dos VPNs distintas pueden usar la misma dirección IP. Es una situación común cuando cada una de las VPNs utiliza un espacio de direccionamiento privado. Naturalmente, cada dirección sigue siendo única dentro de cada VPN.

Como se ilustra en la *figura 1.24*, cada *router* PE mantiene un número de tablas diferentes de envío. Una es la tabla de envío por defecto, mientras que las otras son tablas VRF (VPN *Routing and Forwarding*). En cada PE, el operador necesitará configurar un VRF por cada VPN a la que está conectado el PE considerado. Cada interfaz PE-CE se asocia, mediante configuración, con un VRF. Cuando se recibe por el PE un paquete IP sobre una interfaz de entrada determinada, se busca su dirección IP de destino en la VRF asociada para determinar cómo hay que encaminar el paquete a través del *backbone*. Una VRF se distribuye con rutas aprendidas del dispositivo CE asociado.

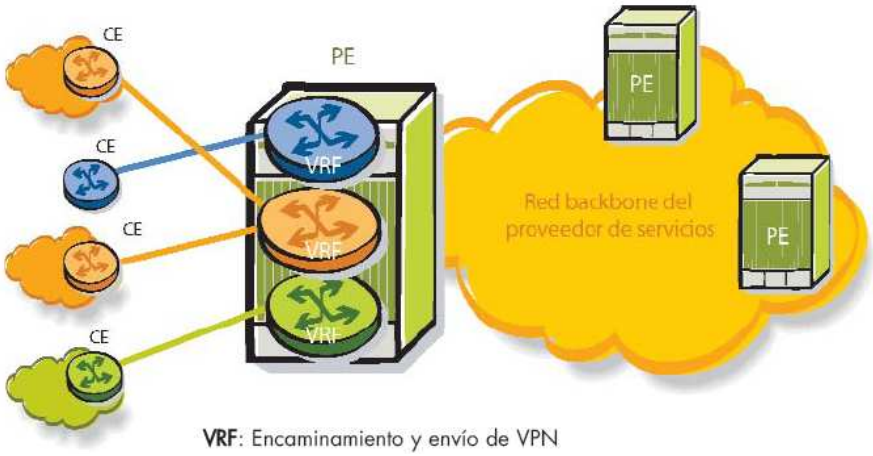


Figura 1.24 Ejemplos de tablas VRF en el PE [10]

El método BGP/MPLS no presupone ninguna técnica particular de aprendizaje: PE podrá aprender rutas usando un protocolo de encaminamiento dinámico, como BGP u OSPF (primer trayecto más corto abierto), o mediante configuración local (encaminamiento estático). Los *routers* PE también necesitan aprender las rutas de otros PEs en la misma VPN.

1.4.2.1.2 Distribución de rutas en la VPN utilizando BGP[10]

Como los *routers* PE utilizan un único proceso de BGP para distribuir las rutas de diferentes VPNs, se debe mejorar el protocolo BGP para soportar potencialmente las direcciones de solapamiento. Aparte de eso, el tratamiento de BGP podría instalar sólo una de ellas, haciéndola inalcanzable para los otros sistemas. La técnica VPN BGP/MPLS logra esto utilizando una nueva familia de direcciones y controlando la distribución de rutas.

1.4.2.1.3 Familia de direcciones VPN-IPv4 [10]

Las ampliaciones MPBGP (multiprotocolo BGP) existentes permiten a BGP transportar rutas de múltiples familias de direcciones. La técnica BGP/MPLS introduce la noción de familia de direcciones VPN-IPv4: una dirección VPN-IPv4 es un campo de 12 bytes, empezando con 8 bytes para el RD (distinguidor de ruta) y acabando con 4 bytes para la dirección IPv4 clásica. Si varias VPNs utilizan el mismo prefijo de dirección IPv4, los PEs pueden traducirlo en varios prefijos de dirección VPN-IPv4 únicos. Una vez que el *router* PE ha aprendido una ruta IPv4 clásica de un *router* CE, convierte la ruta en una única ruta VPN, la cual después se exporta al BGP que la distribuye a todos los demás PEs que necesitan conocerla. Si la ruta de la VPN se selecciona por el proceso de decisión del BGP, se convierte hacia atrás en una ruta IPv4 y se importa en la VRF correcta en el *router* PE remoto. Por último, cualquier ruta instalada en una VRF en un PE remoto se puede distribuir a los *routers* CE asociados. Hay que hacer notar que las direcciones VPN-IPv6 se definen de forma similar, permitiendo a un proveedor de servicios ofrecer VPNs IPv6 utilizando la misma infraestructura de *backbone* y el mismo entorno operacional que se utiliza para ofrecer servicios VPN IPv4.

1.4.2.1.4 Etiqueta MPLS VPN [10]

Cuando un *router* PE distribuye una ruta VPN a través del BGP a otros *routers* PE, también asigna y distribuye una etiqueta MPLS, llamada etiqueta VPN. Cuando los otros *routers* PE envían paquetes de datos de cliente al destino identificado por la ruta BGP recibida, añaden esta etiqueta VPN del MPLS a la cabecera de encapsulado del paquete y abren un túnel al *router* PE del siguiente tramo, que originó la ruta BGP. En este PE, la etiqueta identifica localmente el contexto VPN IP (encaminamiento y envío hacia delante virtual) en el que se debe tratar el paquete etiquetado. La *figura 1.25* muestra un ejemplo de actualización de encaminamiento BGP en el *backbone* del proveedor de servicios.

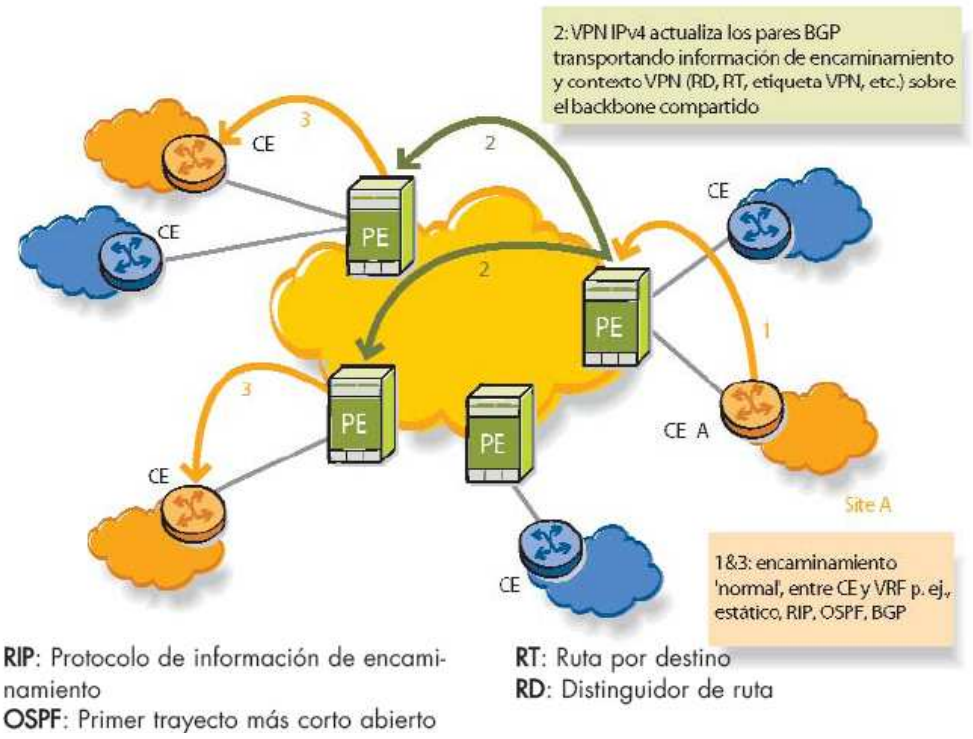


Figura 1.25 Tabla de contactos para distribución de información de alcance [10]

El mensaje contiene rutas VPN-IPv4, cada una de las cuales se asocia con su objetivo de ruta a exportar y con su etiqueta VPN.

1.4.2.1.5 Envío hacia delante [10]

En primer lugar, cuando un *router* PE recibe un paquete IP desde un dispositivo CE, elige una VRF particular en donde busca la dirección de destino del paquete, dependiendo de la interfaz de ingreso del paquete. En segundo lugar, el paquete debe viajar a través del *backbone* hasta un PE remoto, que es el siguiente tramo del BGP, como se estableció en la VRF particular. Para este fin, el paquete IP se convierte en un paquete MPLS con la etiqueta VPN añadida a la pila de etiquetas. Después el paquete se va por el túnel al siguiente tramo del BGP. Por último, en el PE remoto, cuando el paquete sale del túnel, se examina la etiqueta VPN del MPLS; el PE remoto deduce a partir de esta etiqueta o la VRF en la que tiene que procesar a continuación el paquete o la interfaz sobre la que debería transmitirse el dispositivo CE correcto. El encapsulado para los paquetes IP con etiqueta VPN a través del *backbone* posibilita mantener todas las rutas de la VPN fuera de los *routers* de proveedor central. Es crucial para asegurar la escalabilidad del mecanismo. El *backbone* no necesita tener rutas a los CEs, sólo para los PEs. Si el *backbone* soporta MPLS como tecnología de túnel, PE añade otra etiqueta MPLS (asociada con la dirección IP del PE remoto) a la pila de etiquetas del paquete y el paquete se conmuta a través del *backbone* al PE remoto.

1.4.2.1.6 Estado de encaminamiento adicional en la infraestructura de encaminamiento del proveedor de servicios [10]

Para ofrecer un servicio VPN de capa 3 basado en PE, el proveedor de servicios almacena la información de alcance del cliente en su sistema BGP. Esto da lugar a un mayor número de peticiones a los *routers* BGP (frecuentemente conocidos como “BGP *speakers*”), a actualizaciones más frecuentes de memoria/*router*, a un esquema modificado del crecimiento del estado de encaminamiento, a un gasto mayor de ancho de banda para control del tráfico, a más tiempo para volver a iniciar, a rutas del cliente compitiendo por los recursos en el plano de control del proveedor, a medidas específicas para evitar el crecimiento incontrolado, etc. La carga del *router* PE se limita en función de número de rutas y VPNs.

En general, un determinado PE puede soportar tantas VPNs como interfaces (incluyendo subinterfaces), pero se limita el número total de rutas que puede manejar. No obstante, el número de VPNs soportados por un único *router* PE se puede limitar por el número de casos de encaminamiento que el PE puede soportar. Dependiendo de las técnicas usadas para intercambiar información sobre el enlace PE-CE, el número de casos de encaminamiento en el PE puede ser diferente. En el caso de BGP ó encaminamiento estático, un único sistema puede soportar el encaminamiento con todos los CEs. No obstante, cuando se utiliza OSPF, PE debe mantener una instancia OSPF por VRF.

Los proveedores de servicios deberían tomar medidas para evitar que los usuarios inyecten demasiadas rutas en la infraestructura de encaminamiento de su *backbone*. Para ello, el SLA (acuerdo de nivel de servicio) de la VPN con el cliente debería especificar claramente el número máximo de rutas de cliente a distribuir. El proveedor de servicios puede ayudar al cliente en el diseño de su topología de red privada y arquitectura de direccionamiento para que haga frente a estas limitaciones.

Finalmente, el proveedor de servicios puede utilizar medidas dinámicas que avisen al usuario cuando se ha alcanzado el límite acordado de rutas inyectadas y para que deje de aceptar rutas de cliente por encima de un umbral adicional.

1.4.2.1.7 Estabilidad del encaminamiento del proveedor de servicios [10]

Más allá del mantenimiento de la propia información de encaminamiento, la escalabilidad también está afectada por la dinámica del protocolo PE-CE. Esto significa que la velocidad a la que se advierten los cambios de ruta entre CE y PE afecta a la dinámica del sistema BGP del proveedor de servicios, ya que los cambios reportados por un CE a su PE asociado se podrían propagar a otros PEs. De ahí que la estabilidad del encaminamiento no dependa únicamente de las propiedades del *backbone* y del número limitado de conexiones con operadores de pares, sino que también depende de las inestabilidades dentro del gran número de redes de cliente.

El impacto de las inestabilidades de la red de cliente depende de cómo se desacoplan los protocolos PE-CE del BGP *backbone* del proveedor de servicios en la instalación. El uso de BGP externo como protocolo de encaminamiento PE-CE es el caso peor, ya que generalmente BGP se instala como un proceso único en un PE.

También se tiene la dinámica inherente del cliente; de hecho, el método BGP/MPLS implica muchos planos independientes de control de clientes proyectados en uno del proveedor. Si, por ejemplo, varias VPNs comparten una interfaz de cliente, un solo fallo del enlace provocará múltiples oscilaciones de rutas en el *backbone*.

Es importante hacer notar que la velocidad máxima de cambios de la información de encaminamiento debería incluirse en el SLA. Además, el proveedor de servicios puede ayudar a sus clientes en el diseño de la red para optimizar la dinámica de encaminamiento.

1.4.2.1.8 El uso de VPN BGP afecta al uso de BGP Internet [10]

Ya que, desde una perspectiva del PE, se podría considerar Internet como una VPN BGP/MPLS especial, las interferencias entre VPN BGP y BGP Internet son similares a las interferencias entre VPNs. Esto conduce a los mismos problemas de escalabilidad. En consecuencia, el despliegue creciente de VPNs BGP/MPLS de proveedor entre servicios puede desestabilizar potencialmente el encaminamiento Internet.

Así como una red que soporta encaminamiento VPN también necesitará, de alguna manera, soportar el encaminamiento Internet (por ejemplo, para proporcionar conectividad Internet a usuarios VPN y no VPN), se debe tener cuidado para asegurar que el encaminamiento VPN no afecte al encaminamiento tradicional Internet, y viceversa. Además, cuando un único sistema da soporte tanto a encaminamiento Internet como VPN, es posible que los problemas e inestabilidades en un sistema de encaminamiento pudieran afectar a otro sistema.

Para prevenir esto, las instalaciones deberían permitir que los recursos empleados por el encaminamiento Internet y por el encaminamiento VPN estuviesen divididos en un *router* PE. Una forma de lograr esto es dividir los recursos disponibles del PE entre familias de direcciones diferentes, y permitir a un operador asignar prioridades cuando haya escasez de recursos PE.

Hay que destacar que estas consideraciones tienen gran dependencia de las capacidades del *router*, del despliegue y de la instalación del método VPN.

1.4.2.2 VPNs punto a punto de capa 2

Las VPNs punto a punto de capa 2 se las puede identificar también como un tipo de Servicio de Línea Ethernet, y básicamente consiste en una conexión virtual Ethernet o EVC (*Ethernet Virtual Connection*) entre dos UNIs. El servicio *E-Line* es usado para conectividad Ethernet punto a punto. En la *figura 1.26* se puede observar los elementos de un *E-Line*.

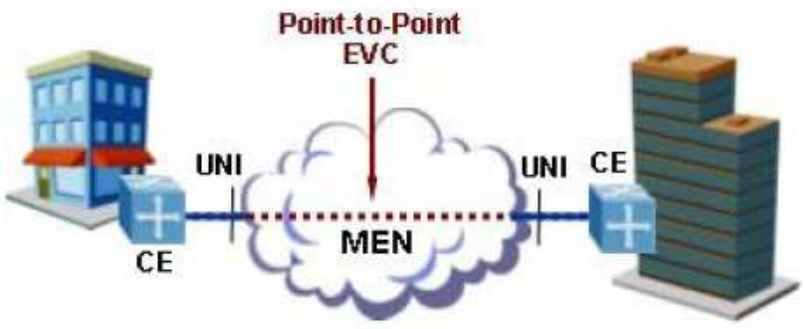


Figura 1.26 Servicio E-Line utilizando un EVC punto a punto [11]

En una simple forma el servicio *E-Line* puede proveer anchos de banda simétricos para el envío de datos en cualquiera de las dos direcciones sin afectar el desempeño; por ejemplo un servicio puede estar dado entre dos UNIs a 10 Mbps. En otras formas más sofisticadas el servicio *E-Line* puede proveer un CIR (*Committed Burst Size*), EIR (*Excess Information Rate*) y asociado EBS (*Excess Burst Size*) y retardo, *jitter*, y pérdida en el desempeño de seguridad entre dos diferentes velocidades de UNIs.

Puede ocurrir un servicio de multiplexación de más de un EVC, es decir que más de un *E-Line* puede estar dentro de un mismo puerto físico a uno de los UNIs.

Estos conceptos que provienen de las redes Metro Ethernet (MEN), son aplicados a redes existentes como *Frame Relay*, ATM y MPLS, ya que al construir y usar un EVC, lo que se está formando es un Línea Privada de Capa 2 o una Red privada Virtual (VPN).

1.4.2.3 VPNs multipunto de capa 2, o VPLS (Servicios LAN Privados Virtuales) [12]

VPLS, también conocido como TLS (servicio de LAN transparente) o servicio E-LAN, es una VPN multipunto de capa 2 que permite conectar múltiples sitios en un único dominio puenteado sobre una red MPLS/IP gestionada por el proveedor. Todos los sitios del cliente en un caso de VPLS (es decir, un VPLS para una empresa particular) parecen estar en la misma LAN (red de área local), sin tener en cuenta sus localizaciones. VPLS utiliza una interfaz Ethernet con el cliente, simplificando la frontera LAN/WAN y permitiendo un aprovisionamiento rápido y flexible del servicio.

Una red con VPLS consta de CEs (equipos de cliente), PEs (equipos de proveedor) y de una red central MPLS:

- ***El dispositivo CE*** es un *router* o conmutador situado en las instalaciones del cliente; puede pertenecer y gestionarse por el cliente o por el proveedor de servicios. Se conecta al PE mediante un AC (circuito de conexión). En el caso de VPLS, se asume que Ethernet es la interfaz entre CE y PE.

- ***El dispositivo PE*** es donde reside toda la inteligencia de VPN, donde el VPLS comienza y termina y donde se establecen todos los túneles necesarios para conectar con todos los otros PEs. Ya que el VPLS es un servicio Ethernet de capa 2, el PE debe ser capaz de conocer, puentear y replicar el MAC (control de acceso a los medios) en base a VPLSs.

- ***La red central MPLS/IP*** interconecta los PEs; no participa realmente en la funcionalidad de VPN. El tráfico se conmuta simplemente basándose en etiquetas MPLS.

La base de cualquier servicio VPN multipunto (VPN IP o VPLS) es una malla completa de túneles MPLS (LSPs – trayectos conmutados por etiquetas, también llamados túneles externos) que se establecen entre todos los PEs que participan en el servicio VPN. LDP (protocolo de distribución de etiqueta) se utiliza para establecer estos túneles; alternativamente se puede utilizar RSVP-TE (protocolo de reserva de recurso – ingeniería de tráfico) o una combinación de LDP y RSVP-TE. Las VPNs multipunto pueden crearse encima de esta malla completa, ocultando la complejidad de la VPN desde los *routers* centrales.

Para cada instancia VPLS se crea una malla completa de túneles internos (llamados *pseudowires*) entre todos los PEs que participan en la instancia VPLS. Un mecanismo de auto-detección localiza todos los PEs que participan en la instancia VPLS. Este mecanismo no se ha incluido en las especificaciones previas, de esta forma el proveedor de servicio puede configurar el PE con las identidades de todos los otros PEs en un VPLS concreto, o puede seleccionar el mecanismo de auto-detección que prefiera, por ejemplo, RADIUS (servicio de autenticación remota de marcación de entrada de usuario).

La tecnología *pseudowire* está normalizada por el IETF (grupo de tareas sobre ingeniería de Internet) PWE3 (*Pseudo Wire Emulation Edge to Edge*) *Working Group* [5]. Los PWs son conocidos históricamente como “túneles Martini”, y a las extensiones al protocolo LDP para permitir la señalización de PWs se las denomina frecuentemente “señalización Martini”.

Un PW consta de un par de LSPs unidireccionales punto-a-punto de un solo salto en direcciones opuestas, cada uno identificado por una etiqueta PW, también llamada VC (conexión virtual). Las etiquetas PW se intercambian entre un par de PEs usando el mencionado protocolo de señalización LDP. El identificador VPLS se intercambia con las etiquetas; así ambos PWs pueden enlazarse y asociarse a

una instancia VPLS particular. Se debe observar que este intercambio de etiquetas PW tiene que darse entre cada pareja de PEs participantes en una instancia VPLS concreta, y que las etiquetas PW tienen solamente un significado local entre cada una de esas parejas. La creación de PWs con una pareja de LSPs permite a un PE participar en el aprendizaje del MAC: cuando PE recibe una trama Ethernet con una dirección de fuente MAC desconocida, PE sabe en qué VC se envió.

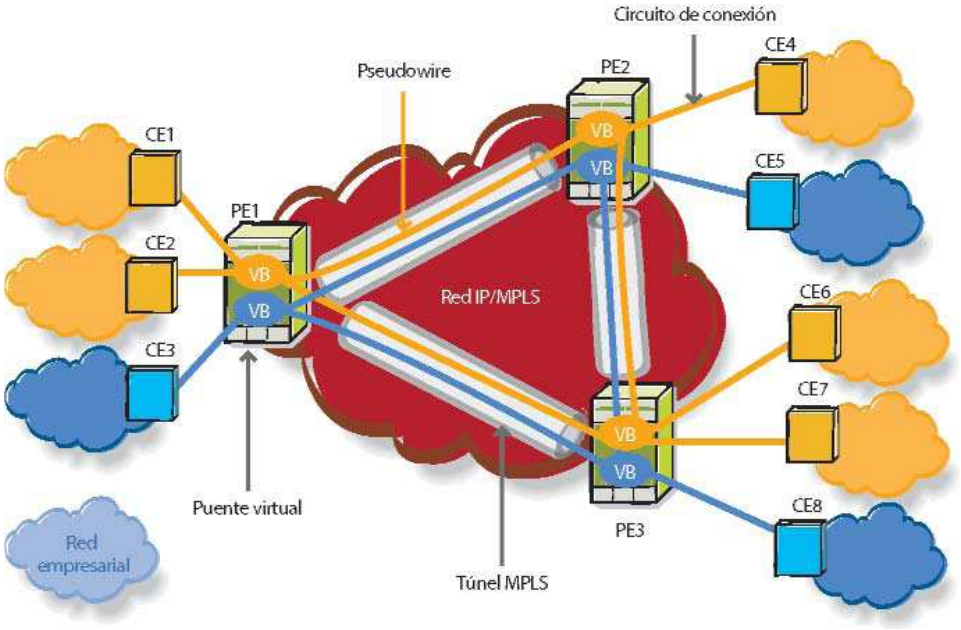


Figura 1.27 Modelo de referencia VPLS [12]

Los *routers* PE deben soportar todas las prestaciones “clásicas” Ethernet, como aprendizaje MAC, replicación y envío de paquetes. Conocen las direcciones MAC de la fuente MAC del tráfico que llega a sus puertos de acceso y de red. Desde un punto de vista funcional, esto significa que los PEs deben implementar un puente por cada instancia VPLS, al que se le suele llamar VB (puente virtual), como se muestra en la *figura 1.27*. La funcionalidad VB se lleva a cabo en el PE mediante una FIB (retransmisión de base de información) para cada supuesto de VPLS; esta FIB se propaga con todas las direcciones MAC aprendidas. Todo el tráfico se conmuta en base a las direcciones MAC y se reenvía entre todos los *routers* PE participantes, usando túneles LSP. Los paquetes desconocidos (es decir, las direcciones de destino MAC que no han sido aprendidas) se replican y reenvían en todos los LSPs a todos los *routers* PE que participan en ese servicio hasta que

responde la estación de destino y la dirección MAC es aprendida por los *routers* PE asociados con dicho servicio.

Para evitar bucles de reenvío se usa la regla llamada “*Split Horizon* (horizonte dividido)”. En el contexto VPLS, esta regla implica básicamente que un PE nunca debe enviar un paquete a un PW si ese paquete se ha recibido de un PW. Esto asegura que el tráfico no pueda formar un bucle sobre la red de *backbone* usando PWs. El hecho de que haya siempre una malla completa de PWs entre los dispositivos PE asegura que cada paquete emitido alcanzará su destino dentro del VPLS.

CAPÍTULO 2

ANÁLISIS DEL ESTADO ACTUAL DE LA RED DE DATOS DE LA EMPRESA ELÉCTRICA QUITO S.A.

2.1 BREVE ANÁLISIS DE USUARIOS Y APLICACIONES QUE UTILIZAN LA RED DE DATOS DE LA E.E.Q.S.A.

Los usuarios y aplicaciones que utilizan la red de datos de la E.E.Q.S.A.[22] para comunicarse, son diversos, por lo que se ha optado por realizar una clasificación tanto de usuarios como de aplicaciones.

2.1.1 CLASIFICACIÓN DE USUARIOS

La clasificación obedece a un criterio de importancia, entorno a la administración de la infraestructura informática y a la ubicación geográfica de los usuarios, ya que esto determinará los requerimientos en cuanto a enlaces y configuraciones de comunicación, así como a niveles de acceso.

2.1.1.1 Usuarios de la División de Tecnología de la Información y Comunicaciones

Estos usuarios corresponden a los administradores, que son responsables de los diferentes sistemas informáticos, los mismos que son utilizados por los usuarios de la E.E.Q.S.A. Aquí se pueden distinguir tres grandes grupos de administradores que corresponden a:

- *Administración de Sistemas Informáticos y Bases de Datos.* Tienen acceso total a la mayoría de los sistemas informáticos y bases de datos. Se ocupan de la gestión de usuarios, mantenimiento en óptimas condiciones de todos los servidores, actualizaciones y cambios en la configuración de las aplicaciones que llegan al usuario final, entre sus funciones más importantes.

[22] E.E.Q.S.A. (Empresa Eléctrica Quito Sociedad Anónima).

- *Administración de Comunicaciones y Redes.* En cuanto a la gestión de los equipos de comunicación, el Departamento Comunicaciones y Soporte, administra tanto los enlaces de datos como los equipos computacionales que conforman la red corporativa. Para tal objetivo existen dos grupos de trabajo. El primer grupo se encarga del soporte y mantenimiento de equipos finales como PCs de escritorio, equipos portátiles, impresoras, escaners, fax, etc.; el segundo grupo está encargado del monitoreo, soporte y mantenimiento de los enlaces y equipos de conectividad, así como de la elaboración de proyectos de nuevas instalaciones y redes informáticas. Todo esto implica acceso a los equipos de comunicación y computacionales con la mayoría de privilegios de gestión.

- *Desarrolladores de Sistemas.* Estos usuarios diseñan y desarrollan sistemas, brindan soporte y mantenimiento a la mayoría de las aplicaciones que los usuarios, tanto internos como externos de la E.E.Q.S.A. utilizan. Para tal motivo necesitan acceder a los servidores de aplicaciones y de bases de datos. Los privilegios para este grupo de usuarios es menor al de los dos anteriores por razones de seguridad, refiriéndose básicamente al manejo de los datos alojados en los servidores de producción.

2.1.1.2 Usuarios Locales (Red Corporativa)

Los usuarios que se analizará son aquellos que cuentan con acceso de alta velocidad[23] en ambiente LAN[24] a la red corporativa de la E.E.Q.S.A. La ubicación de estos usuarios corresponde a las instalaciones del Edificio Matriz “Las Casas”, Edificio Comercial “Mariana de Jesús”, Edificio Técnico “Alvarez Cañizares”, Centro de Operaciones “El Dorado”, Subestaciones y Centrales de Generación (a través de fibra óptica). Estas edificaciones cuentan con enlaces de fibra óptica para poder ingresar al centro de cómputo de la E.E.Q.S.A. ubicado en el Edificio Matriz. Las velocidades de transmisión son de 100 Mbps (*Fast-Ethernet*) y 1 Gbps

[23] Mayor o igual a 100 Mbps
[24] LAN (*Local Area Network* – Red de Área Local).

(*Gigabit-Ethernet*). A estos usuarios se los puede identificar en un grupo que se lo denominará Usuarios Administrativos y de Operación.

- *Usuarios Administrativos y de Operación.* En este grupo se encuentra a una gran variedad de personal que tiene acceso a una PC de escritorio o computador portátil, como Ejecutivos, Jefes de las diferentes áreas, Secretarias, Oficinistas, Profesionales, etc. Todos ellos tienen en común un grupo de aplicaciones y sistemas informáticos que utilizan, aunque entre ellos pueden variar de una aplicación a otra. Básicamente ellos ejecutarán aplicaciones que residen en el portal de la Intranet, Correo Electrónico y Aplicaciones CITRIX[25].

2.1.1.3 Usuarios Remotos

En esta clasificación se encuentran dos grupos bien definidos de usuarios: internos y externos.

- *Usuarios Internos.* Compuesto por todos aquellos que se encuentran fuera del alcance de los enlaces de alta velocidad, ya sea por la ubicación o por la forma en cómo acceden a las aplicaciones y servicios de la E.E.Q.S.A. como son las Agencias de Recaudación y Atención al Cliente, Subestaciones de Transmisión Eléctrica y Centrales de Generación. Dentro de estas dependencias existen usuarios de tipo administrativos y de operación, que en conjunto van a compartir un solo canal de comunicaciones hacia el centro de cómputo ubicado en el edificio Matriz, ya sea por medio de enlaces dedicados con Andinadatos o Telconet o vía repetidores inalámbricos con tecnología OFDM[26] o *Spread Spectrum*.

- *Usuarios Externos.* Una gran variedad de usuarios son los que en la actualidad necesitan ingresar a los servicios informáticos que presta la

[25] Citrix Systems, o *Citrix*, es una empresa de Estados Unidos, con sede central en la ciudad de *Fort Lauderdale*, en el estado de Florida. Es una compañía dedicada principalmente al desarrollo de *software*[1]. Al mencionar CITRIX se refiere al Sistema que comprende los servidores donde reside las aplicaciones y el cliente.
[26] OFDM (*Orthogonal Frequency Division Multiplexing*)

E.E.Q.S.A., y que no necesariamente están dentro de las instalaciones locales o remotas de esta empresa. Existen centros autorizados de recaudación, empresas con convenios de cooperación interinstitucional y comercial, personal autorizado y contratistas, y en general usuarios de los servicios que presta el sitio *Web* de la E.E.Q.S.A. La mayoría de esta variedad de usuarios tienen como puerta de entrada el Internet. La E.E.Q.S.A. cuenta con un limitado ancho de banda el cual debe ser bien administrado para poder satisfacer las necesidades tanto de usuarios internos locales y remotos, así como de usuarios externos remotos.

2.1.2 CLASIFICACIÓN DE APLICACIONES

Las aplicaciones que se ejecutan sobre la red de datos de la E.E.Q.S.A., son en su mayoría desarrolladas por los profesionales de la División de Tecnología de la Información y Comunicaciones. Básicamente se desarrollan aplicaciones de acuerdo a los requerimientos del área usuaria, donde los datos son almacenados en bases de datos. La E.E.Q.S.A. cuenta con sistemas de Bases de Datos ORACLE, montados sobre arquitecturas de servidores y ejecutándose sobre plataformas IBM AIX.

A estas aplicaciones se las ha clasificado de acuerdo a la forma en cómo los usuarios acceden. Dentro de esta clasificación se puede distinguir tres formas o ambientes básicos de acceso o ejecución, ambiente Cliente – Servidor, Virtual CITRIX y Web.

- *Ambiente Cliente – Servidor.* Este ambiente implica que el conjunto de aplicaciones contiene un instalador para que éste se ejecute en la máquina cliente, teniendo como única generación de tráfico los datos desde la base de datos hacia el cliente y viceversa. Esta modalidad está siendo migrada hacia ambientes virtualizados y web. Los sistemas que siguen funcionando de esta manera son: El Sistemas de Información Geográfica (GIS), Correo Electrónico (Aplicación Lotus Notes), Sistema Financiero, Bienes y Bodegas, Talleres y Transportes, y Sistema de Recursos Humanos.

- *Ambiente Virtual CITRIX.* Luego de la experiencia en la instalación y mantenimiento de cada PC de escritorio y portátiles de cada uno de los usuarios de la E.E.Q.S.A. para que puedan ejecutar las diferentes aplicaciones, se determinó que cada vez esta labor requería mucho tiempo, personal capacitado y gastos en viajes, más aun cuando esta operación requería realizarse en lugares que no fuesen las edificaciones principales de la E.E.Q.S.A.

  Para minimizar todo este gasto administrativo se procedió a investigar en tecnologías que permitan instalar una sola vez las aplicaciones de los diferentes sistemas y que a partir de esta instalación única, los usuarios puedan acceder y usar.

  Servidores y sistemas CITRIX posibilitaron esta gran ayuda, con lo que el proceso se reduce a la instalación de un software cliente en cada PC configurado adecuadamente, para que a través de esta aplicación se pueda acceder a los diferentes sistemas residentes en servidores CITRIX. Esto implica que la información es única ya que los mandos de teclado y *mouse* son enviados por la red.

  Ahora, no solo estos mandos son enviados por la red, la imagen de la aplicación viaja a través de la red y cuando se envían impresiones estos datos también ocupan recursos de red considerable; una ventaja de los sistemas CITRIX es que todos los datos viajan encriptados dando como consecuencia más carga de tráfico sobre la red.

  Si bien es cierto esto ofrece una gran ayuda en cuanto a mantenimiento y soporte de usuarios, reduciendo la incidencias de fallas, en cambio se tienen dos aspectos que se deben tomar en consideración. La primera es, que el consumo de ancho de banda es mayor y la segunda es que si llegaran a fallar los servidores CITRIX toda la empresa queda sin servicio; esto fue tomado con mucha cautela, por lo que se han mejorado las

condiciones del centro de cómputo, tanto en infraestructura de seguridad como en equipos servidores y de comunicaciones.

- *Ambiente WEB.* Dentro de este ambiente se ejecutan aplicaciones como el SDI[27], Correo Electrónico, Sistemas de Gestión de la Calidad, Web EEQ, Informe Técnico, etc. Es una alternativa que se está empezando a explotar con mayor fuerza en este último año, ya que no requiere mayor configuración del cliente final y los costos se reducen significativamente en relación al ambiente CITRIX. En la *figura 2.1* se muestra el portal del Intranet desde el cual se puede acceder a las diferentes aplicaciones de tipo WEB.

En cuanto al tráfico generado, éste no es muy grande por lo que es conveniente para aquellos lugares remotos que cuentan con velocidades mucho menores a 100 Mbps. La implicación que advierte en temas de seguridad esta opción, es que tanto los navegadores Internet Explorer 6 y 7 y Mozilla 2.15 y 3, deben contar con actualizaciones para evitar problemas de compatibilidad y riesgos en la seguridad informática.

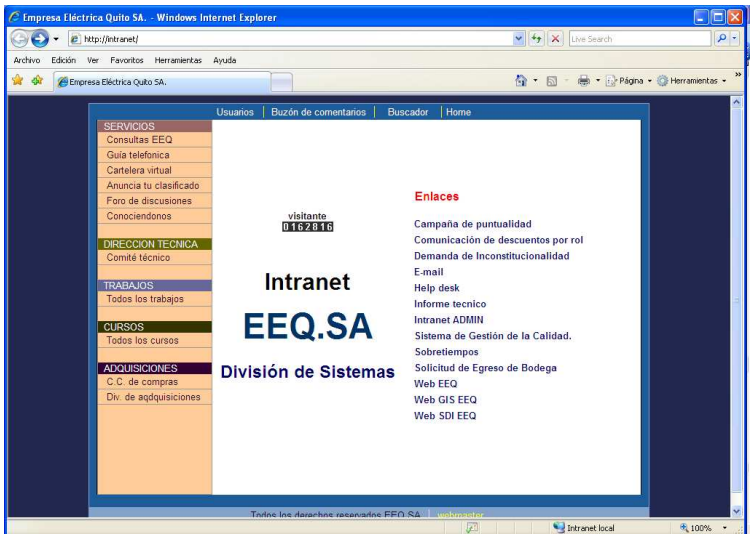


Figura 2.1 Portal de la INTRANET de la E.E.Q.S.A.

[27] SDI (Sistema de Distribución Integrado)

A más de la diversidad de usuarios y de aplicaciones, la razón principal por la que se hace esta clasificación es la de tener una base para saber qué es lo que se va a transportar por la red privada virtual, realizar mediciones y también analizar la realidad actual y así realizar proyecciones futuras en este tipo de enlaces.

2.2 ANÁLISIS DE LOS ENLACES DESDE EL EXTERIOR DE LA E.E.Q.S.A.

Se denominarán enlaces *"desde el exterior de la E.E.Q.S.A."* aquellos que llegan al centro de cómputo del edificio matriz Las Casas, por medio de: enlaces de comunicaciones rentados, a través de redes públicas y también los que son parte de la red inalámbrica *Spread Spectrum* y OFDM.

La E.E.Q.S.A. cuenta con enlaces que permiten la comunicación con sus agencias, subestaciones y centrales de generación, a través de los enlaces mencionados anteriormente. Además se dispone de canales de comunicación para establecer acceso hacia otras empresas, utilizados para distintos fines, como son el monitoreo de vehículos (AVL) y facturación a través de Servipagos. A esta parte de la red se la puede denominar como la extranet.

A continuación se revisarán los enlaces que llegan desde el exterior hacia el edificio matriz, donde se encuentran equipos de comunicación y los servidores de los distintos servicios informáticos, con las que cuenta la E.E.Q.S.A.

2.2.1 RED DE DATOS INALÁMBRICA

La red de datos inalámbrica, consta principalmente de cuatro puntos geográficos, desde donde se distribuye tráfico de datos hacia las diferentes edificaciones que forman parte de la E.E.Q.S.A.

La red nace en el edificio matriz Las Casas, desde ahí se encuentra un enlace hacia Cruz Loma (Pichincha), uno hacia Miravalle (Sector Loma de Puengasí) uno

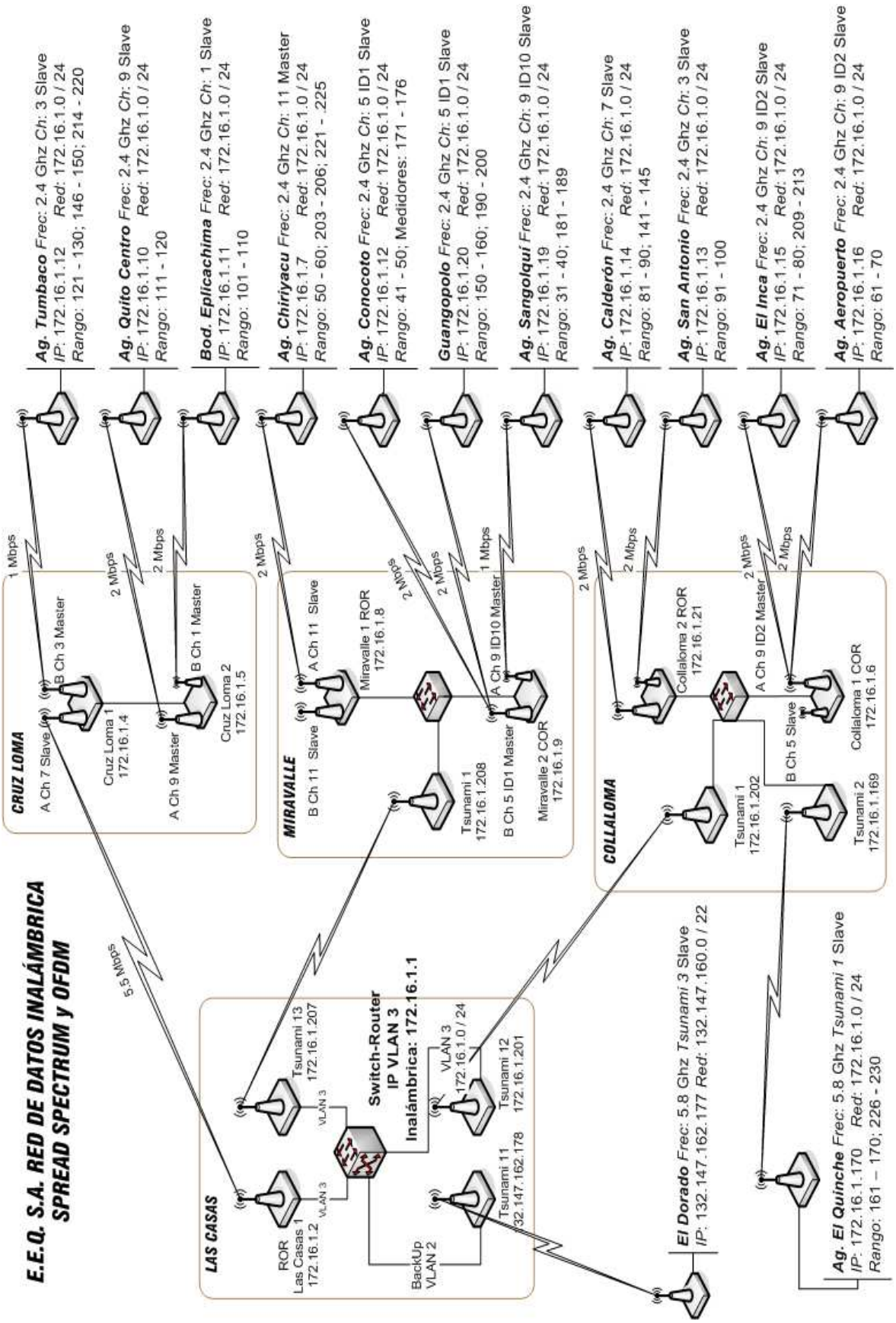


Figura 2.2 Diagrama de los enlaces inalámbricos

hacia Collaloma (Norte de Quito), y el último directamente hacia los altos del edificio polifuncional del centro de operaciones El Dorado.

En la *figura 2.2* se puede apreciar cómo, desde los cuatro puntos geográficos (Las Casas, Cruz Loma, Miravalle y Collaloma) se conforma la red de datos inalámbrica. También, en la *figura 2.2* se muestra la información correspondiente a nombre del lugar, nombre de los radios de repetición, modo de operación de los radios, frecuencias, canales, velocidades de transferencia y rangos de direccionamiento IP.

El *Switch-Router* que se muestra en la *figura 2.2*, es el equipo centralizado de comunicaciones que dispone la E.E.Q.S.A. el cual distribuye la información almacenada en los diferentes servidores del Centro de Cómputo hacia los equipos de usuario tanto internos como externos de la E.E.Q.S.A.; de las configuraciones que se ha realizado a éste equipo, están un conjunto de VLANs, que permiten segmentar redes que a juicio de la E.E.Q.S.A. son diferentes unas de otras, como es el caso de la Red Inalámbrica. En el transcurso de este proyecto se hará mención de este *Switch-Router*, básicamente en los gráficos donde se indica la VLAN a la que corresponde determinado segmento de red o enlace enrutado.

Los enlaces principales se encuentran en el rango de 5.8 Ghz OFDM IEEE[28] 802.11a[29], los cuales corresponden a todos los enlaces que nacen desde el edificio matriz, excepto el que va hacia Cruz Loma que es *Spread Spectrum* IEEE 802.11b[30] a 2.4 Ghz. Además por la distancia que existe entre Collaloma y El Quinche, se ha establecido un enlace de 5.8 Ghz IEEE 802.11a, con antenas de alta potencia (29 dbi).

[28] IEEE (*The Institute of Electrical and Electronics Engineers*, Instituto de Ingenieros Eléctricos y Electrónicos).
[29] IEEE 802.11a Estándar para redes de área local inalámbricos que opera en la banda de 5 GHz y utiliza 52 subportadoras OFDM con una velocidad máxima de 54 Mbps.
[30] IEEE 802.11b Estándar para redes de área local inalámbricos que opera en la banda de 2.4 GHz con velocidades de hasta 5.5 Mbps y 11 Mbps.

2.2.2 ENLACES CON ANDINADATOS Y ANDINATEL (CNT)[31]

Entre la E.E.Q.S.A. y Andinatel se tiene contratado un servicio que permite enviar el desborde de llamadas del *Call Center* de la E.E.Q.S.A., ubicado en el edificio matriz Las Casas, hacia el *Call Center* de Andinatel. Dentro del servicio consta un enlace E1 para datos y que está configurado como se indica en la *figura 2.3*.

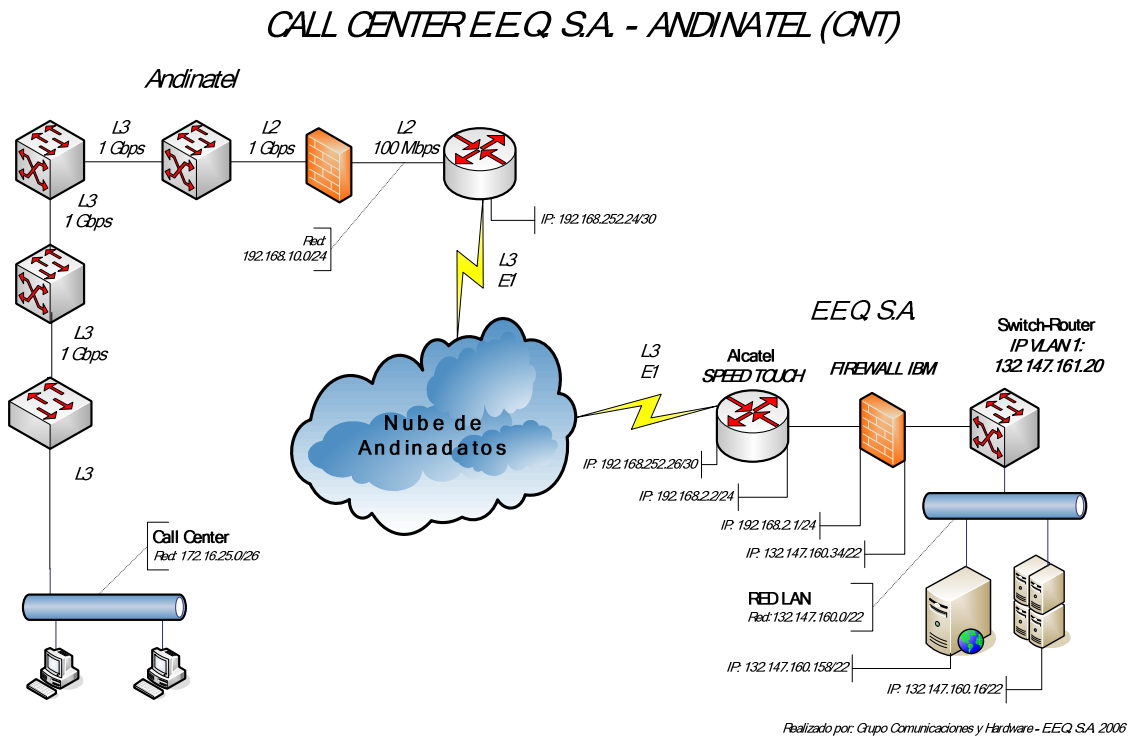


Figura 2.3 Diagrama del enlace con Andinatel

Dentro del sistema de telefonía que maneja Andinatel, se transfieren las llamadas de los clientes que sobrepasan la capacidad de llamadas que puede recibir el *Call Center* de la E.E.Q.S.A.; esta capacidad se refiere a otro enlace E1 ó 30 canales analógicos. En la parte de datos Andinatel tiene acceso al sistema CRM[32], de donde puede acceder a los diferentes servicios de comercialización y atención al público de la E.E.Q.S.A. Además se mantiene una extensión telefónica a través del canal o enlace de datos.

---

[31] Andinatel y Pacifictel actualmente conforman la CNT (Corporación Nacional de Telecomunicaciones), sin embargo en este proyecto se seguirá utilizando el nombre de Andinatel por cuestiones de documentación que mantiene E.E.Q.S.A. en sus diagramas de red.

[32] CRM (*Customer Relationship Management*) Software para la administración de la relación con los clientes.

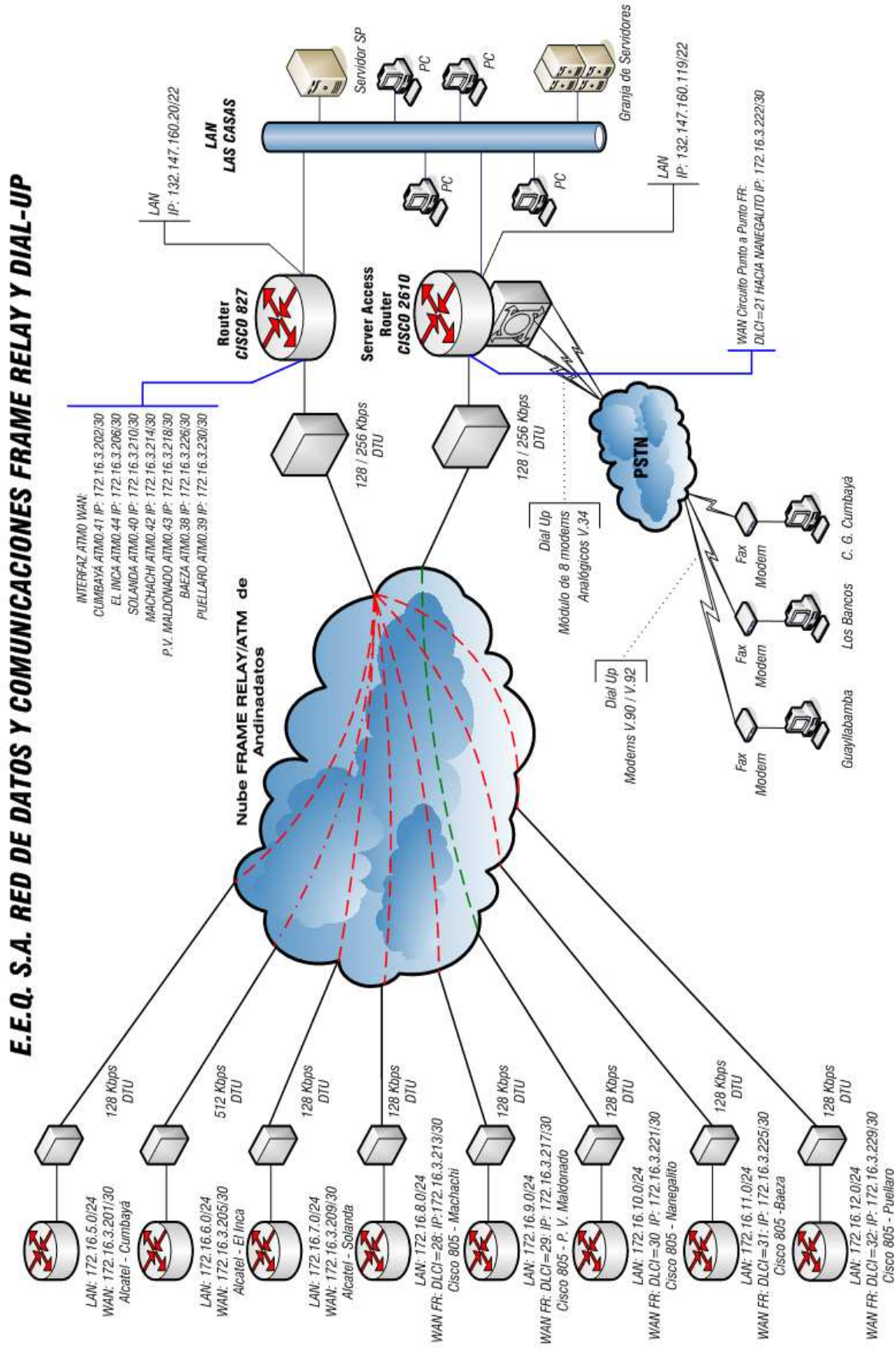


Figura 2.4 Diagrama de enlaces de Agencias Urbanas y Rurales a través de Andinadatos

Con Andinadatos se han establecido contratos de arrendamiento de enlaces con tecnología *Frame Relay*/ATM, para, que agencias como: Solanda, Cumbayá, Machachi, El Inca, Baeza y Puéllaro, puedan tener acceso a la red de datos de la E.E.Q.S.A., a velocidades razonables[33] (entre 64 kbps y 128 kbps) donde se pueda transportar datos de las diferentes aplicaciones comerciales y además telefonía IP.

En el diagrama de la *figura 2.4* se muestra que Andinadatos provee el servicio de transmisión de datos a través de dos enlaces dedicados; el primer enlace lo hace a través de un enlace ATM donde se encuentran configurados varios circuitos virtuales en el *router* CISCO 827 desde el lado de la E.E.Q.S.A. hacia la nube de Andinadatos. Desde el lado de los sitios remotos, la configuración es a través de enlaces con tecnología *Frame Relay*, es así que la información correspondiente al enlace WAN del *router* del sitio remoto contiene una dirección *Frame Relay* DLCI. Los equipos de los sitios Cumbayá, El Inca y Solanda no se presenta la información ya que los *routers* son propiedad de Andinadatos y cuentan con seguridad de acceso, misma que no posee el personal técnico de la E.E.Q.S.A.

En el segundo enlace, a través del *router* CISCO 2610, el sitio Nanegalito se comunica a través de la nube *Frame Relay* de Andinadatos con la red de la E.E.Q.S.A., en los dos sitios los *routers* tienen direcciones *Frame Relay* DLCI.

2.2.3 ENLACE TELCONET – AGENCIAS DE RECAUDACIÓN E.E.Q.S.A., EMPRESAS PARA INTERCAMBIO INTERINSTITUCIONAL Y COMERCIAL

La empresa Servipagos, cuenta con un convenio para recaudar el valor de las facturas, y de esta manera facilitar el pago a los clientes. El tráfico de datos, se lo hacía a través de la red de la empresa Suratel, quien llegaba con sus equipos de comunicaciones al Centro de Cómputo de la E.E.Q.S.A. El diagrama mostrado en la *figura 2.5* permite observar la configuración del enlace entre Servipagos y la E.E.Q.S.A.

[33] Se refiere a que la velocidad de transmisión sea mayor de 33.6 kbps, ya que a velocidades menores las aplicaciones que se ejecutan a través del CITRIX tienen problemas con su tiempo de respuesta.

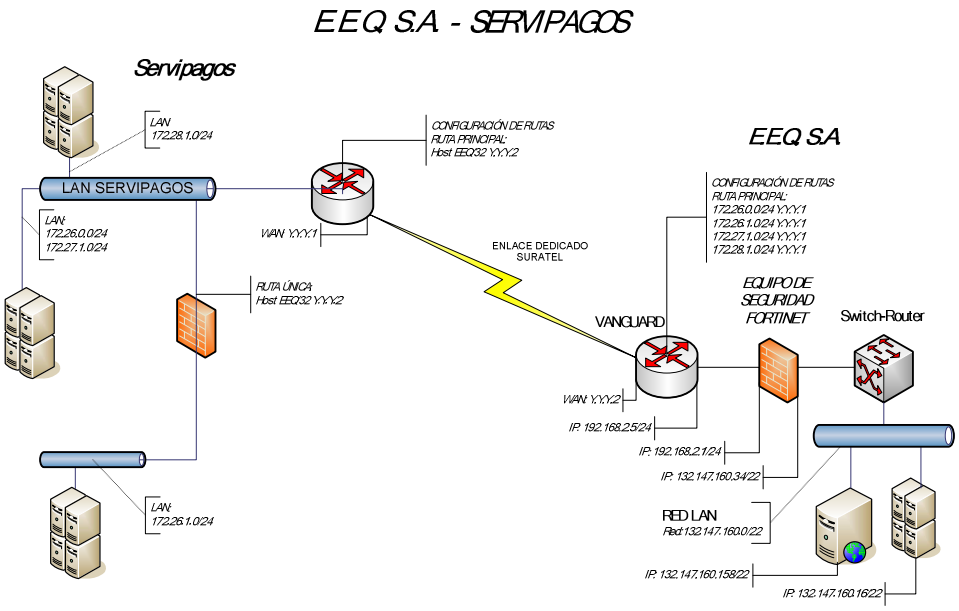


Figura 2.5 Diagrama del enlace con Servipagos

Servipagos ha cambiado su enlace de datos de Suratel por uno de Telconet y varias agencias urbanas y rurales de la E.E.Q.S.A. tienen como enlace principal el provisto por Telconet, que son enlaces nuevos.

Aquellos enlaces de Andinadatos, enlaces inalámbricos OFDM, *Spread Spectrum* y *Dial-Up*, con los que funcionaban algunas agencias han pasado a ser enlaces de respaldo, ya que los nuevos enlaces son de mejores características técnicas (acceso por medio de Fibra Óptica a 1024 kbps).

En la *figura 2.6* se muestra la nueva topología de acceso de las agencias con Telconet y la E.E.Q.S.A.

Además de estos enlaces, se tiene un constante intercambio de información con el CENACE, que necesita conocer datos acerca del manejo de la energía eléctrica que distribuye la E.E.Q.S.A. Esto se lo hace a través de enlaces privados telefónicos (*dial-up*), o por el Internet.

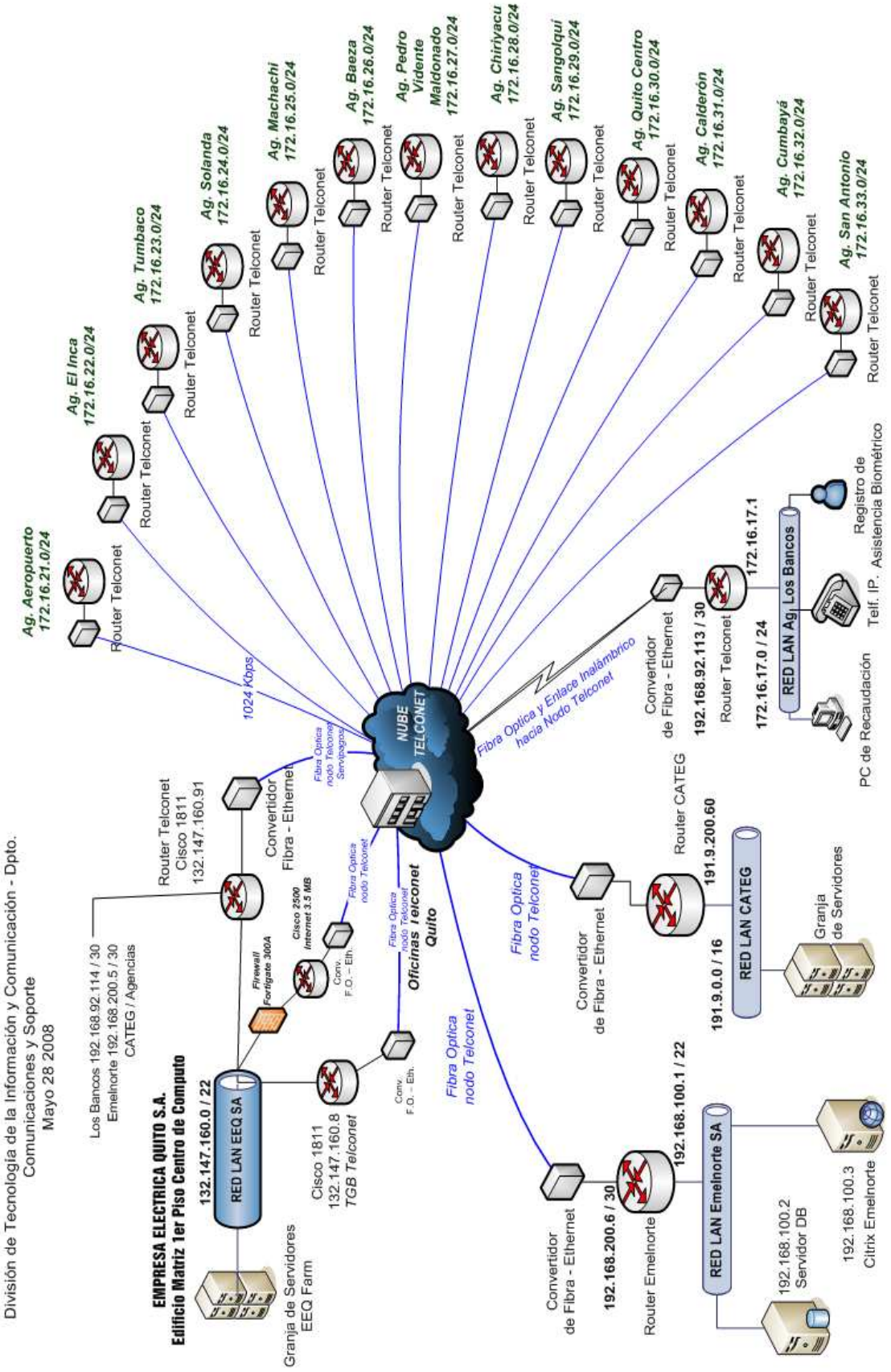


Figura 2.6 Diagrama de enlaces de Agencias Urbanas y Rurales a través de Telconet

En la actualidad el CENACE accederá a los recursos de la red por medio de enlaces privados; si embargo el tener un enlace alternativo como es la VPN[34] se lo consideraría como un sistema de redundancia.

2.2.4 SERVICIO DE INTERNET

El acceso a Internet es un servicio que presta la empresa TELCONET, a través de un enlace, que por el momento cuenta con una capacidad de 3 Mbps en estado activo y 512 Kbps de respaldo en línea, esto garantiza un mejor servicio dentro y fuera de la empresa, a las aplicaciones que se ejecutan por medio del Internet.

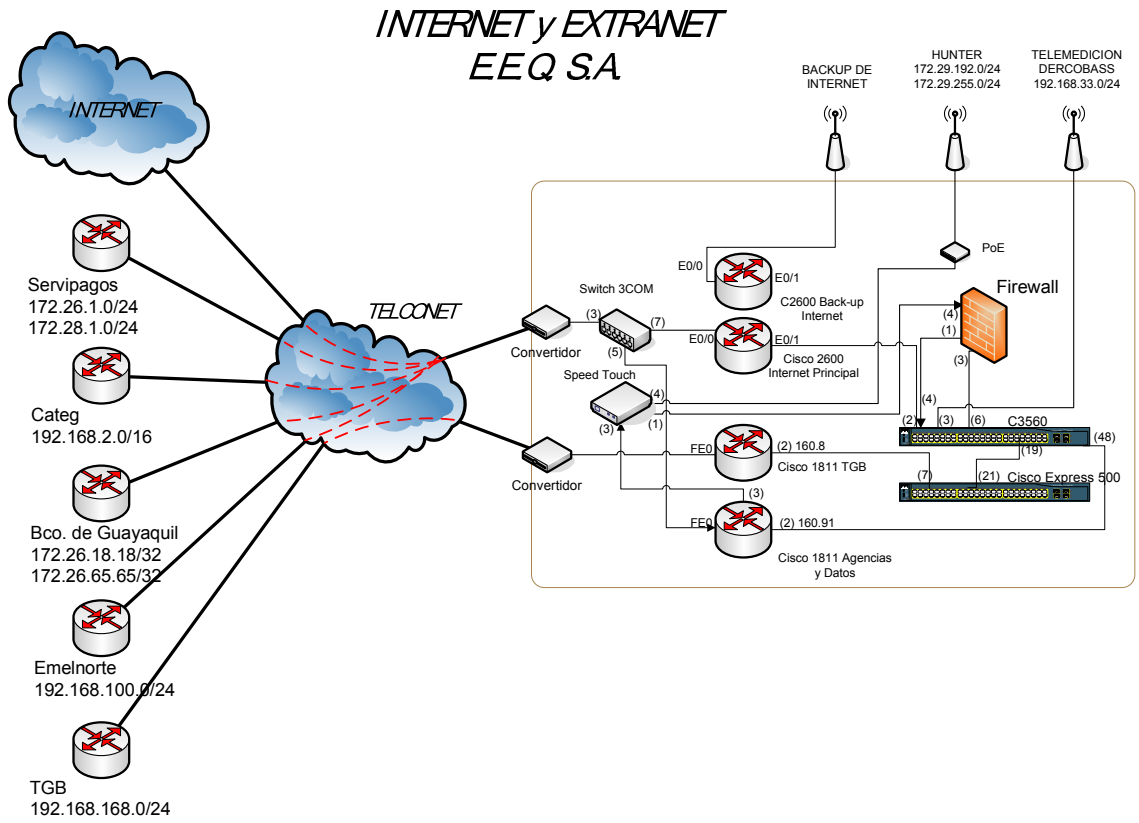


Figura 2.7 Diagrama del enlace corporativo de Internet

En la *figura 2.7* se muestra la topología y configuración del acceso a la nube de Telconet para acceder al Internet. Además se añade la información de los enlaces que ya fueron contratados para acceder a las empresas Servipagos, Categ,

[34] VPN (*Virtual Private Network* – Red Privada Virtual)

Banco de Guayaquil y Telconet (TGB), que utilizan el mismo enlace físico que se tiene para el Internet.

Para el Banco de Guayaquil, lo que le permite este enlace es realizar la recaudación en línea. Tanto los bancos y otras entidades particulares que son conocidos como CARs de la E.E.Q.S.A., tradicionalmente realizan la recaudación fuera de línea. En este proceso fuera de línea, el total recaudado de cada mes por estas entidades, debe ser reportado y entregado a la agencia responsable de dicho CAR. Este proceso será explicado con mayor detalle en el Capítulo 3 de este proyecto.

2.2.5 ENLACES A TRAVÉS DEL SERVIDOR RAS[35]

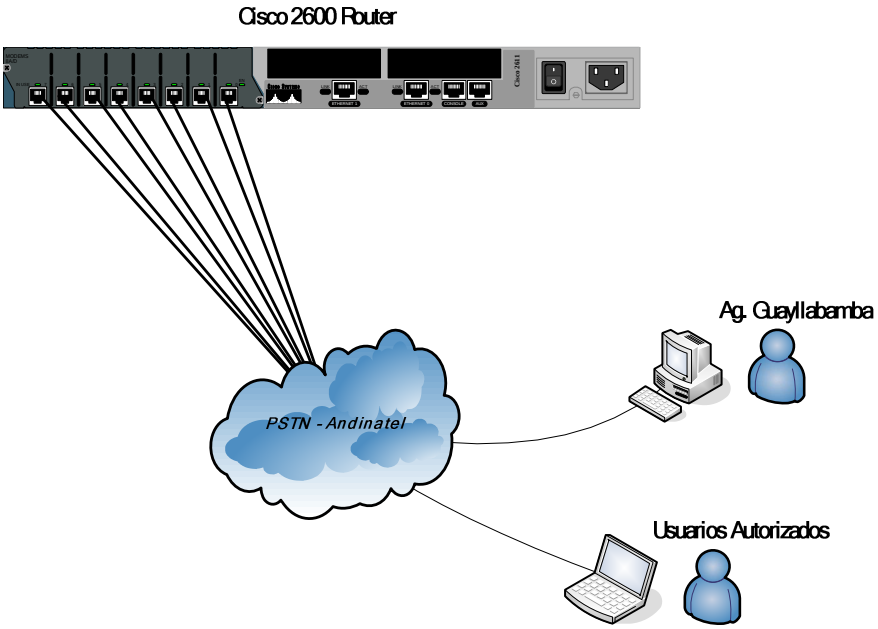


Figura 2.8 Diagrama de acceso a través de Dial-Up

Como una alternativa para acceder a la red corporativa de la E.E.Q.S.A., se tiene implementado un servidor RAS, que consta de un *pool*[36] de 8 modems bajo el

[35] RAS (*Remote Access Server*)
[36] Grupo de interfaces disponibles

estándar V.34[37] conectados a la PSTN (Red de telefonía pública conmutada). Los usuarios de este tipo de acceso, son la agencia de recaudación Guayllabamba y usuarios autorizados en su mayoría de la central de generación térmica Gualberto Hernández en Guangopolo.

Si bien es un medio alternativo de comunicaciones, la seguridad implementada es básica, por lo tanto se necesita mejorar la seguridad de los accesos en este tipo de enlaces.

2.3 ESTUDIO Y ANÁLISIS DE FUNCIONAMIENTO DEL *FIREWALL* ACTIVO

El *firewall* que está operando, está basado en *software*, sobre un equipo IBM, y sobre el sistema AIX 3.2. Mediante este *firewall* se ha podido realizar el control de acceso y salida, desde y hacia las redes exteriores a la E.E.Q.S.A.

Durante el tiempo que ha estado en funcionamiento ha servido como equipo de seguridad perimetral, es decir, actuando como escudo para la red corporativa de la E.E.Q.S.A. en defensa de las posibles amenazas que provengan de las redes externas; sin embargo, los siguientes factores han sido tomados como decisivos para cambiar a un equipo de seguridad moderno:

Firewall-Software. Al ser un equipo de tipo servidor, se debía gestionar tanto el Sistema Operativo como el *software firewall*, esto implica un doble trabajo y por lo tanto un bajo rendimiento, tomando en cuenta el alto crecimiento de equipos de usuario, que requieren el acceso a Internet.

Manejo de Políticas. Para el administrador del *firewall* ha sido confuso establecer políticas de acceso, lo que ocasiona pérdida de tiempo y una alta posibilidad de que se produzcan errores.

[37] Recomendación UIT-T V.34. Módem que funciona a velocidades de señalización de datos de hasta 33 600 bit/s para uso en la red telefónica general conmutada y en circuitos arrendados punto a punto a dos hilos de tipo telefónico.[2]

Protocolos Antiguos. En algunas ocasiones se realizaron pruebas para establecer túneles VPN, sin éxito alguno. Lo que el administrador del *firewall* le atribuía a una desactualización de protocolos VPN, ya que con los equipos que se requería establecer los enlaces, generaban mensajes de error de protocolo.

Recursos de Hardware. La memoria y disco duro ya no son suficientes para la carga de procesamiento, reportes y *logs*, necesarios para la administración y auditoría.

Lentitud en el acceso a páginas WEB. La funcionalidad de PROXY empezaba a ser lento, debido al crecimiento de peticiones; lo que ocasiona que al establecer una sesión con un sitio *web* sea cada vez más lento.

Administración Compleja. Para administrar el *firewall*, se necesita de un alto grado de conocimiento debido a la complejidad que presenta el *software*.

Sistema fuera de servicio. Como el equipo ya empezaba a saturarse, llega momentos en que las funcionalidades se detienen, lo que comúnmente se lo conoce como un “*equipo colgado*”.

En resumen se puede decir que por obsolescencia tecnológica, y la necesidad de nuevos servicios de seguridad, se hace necesario un cambio de equipo, tanto en *hardware* como en *software*.

El prevenir nuevos sistemas o formas de perjuicio informático a través de la red, ha motivado y ha puesto en alerta al personal responsable de la red de datos, para tomar la decisión en la adquisición de un nuevo equipo de seguridad integral, y no sólo un equipo con la funcionalidad de *firewall*.

Mientras tanto se dará un vistazo a las principales configuraciones de esta valiosa herramienta de seguridad, que ha sido administrada por los técnicos y especialistas encargados del servicio de bases de datos y control de usuarios de los sistemas informáticos.

2.3.1 ESPECIFICACIONES TÉCNICAS DEL *FIREWALL*

Se trata de un equipo con arquitectura de servidor en el cual se ejecuta una plataforma AIX. Se detallarán sus características en cuatro secciones:

- Componentes de *hardware*
- Componentes de *software*
- Funcionalidades
- Configuraciones principales de seguridad

2.3.1.1 Componentes de hardware

En el Centro de Cómputo instalado en el *rack* de servidores IBM se encuentra el equipo servidor IBM RS/6000 B50 *series*. Este equipo mostrado en la *figura 2.9* cumple con las funcionalidades de *firewall* para la red de datos de la E.E.Q.S.A.; tiene las siguientes características de hardware:

Figura 2.9 IBM RS/6000 7046 B50

- Procesador: 375 Mhz 604e 1 MB en cache L2
- Memoria SDRAM: 128 MB hasta 1 GB ECC SDRAM en cuatro slots (512 MB actualmente)
- Disco duro: 18.1 GB USCSI[38]
- Tarjeta de Red: 10/100 Mbps IEEE 802.3
- Puertos: Paralelo, serial y ps/2

[38] USCSI (Ultra SCSI). Tecnología de discos duros para servidores.

En la *figura 2.10* se detallan las características de la serie RS/6000 tipo 7046 de IBM.

Ref Model B50 Includes 375 MHz 604e Processor, 512 MB SDRAM DIMM Memory, (2)18.1 GB Ultra SCSI Disk, 1.44 MB Drive, Ethernet Adapter, 32x Speed CD-ROM Drive

RS/6000 7046 Model B50 Highlights:

- Enables high-density packaging for Internet service providers and application service providers
- Space-saving size provides packaging of up to 20 servers, 60 discrete network connections using Ethernet adapters, and over 700 GB of online storage with two 73.4 GB hard drives for each B50 and up to 20 systems in a rack
- Permits installation of up to 1 GB of SDRAM memory in the server
- Comes with Ethernet and Ultra SCSI controllers integrated on the planar

IBM RS/6000 7046 Model B50 Standard features include:

- 375 MHz PowerPC 604e processor
- 1 MB of L2 cache
- 128 MB of ECC SDRAM memory, expandable to 1 GB
- Integrated on the planar:
  - 10/100 Mbps Ethernet controller (IEEE 802.3 compliant)
  - Ultra SCSI controller
  - Two PCI slots
- Two disk drive bays:
  - 18.2 GB Ultra SCSI disk drive
  - One available
- Two media bays:
  - Optical storage device capable of reading a CD-ROM or DVD-RAM disc
  - 1.44 MB 3.5-inch diskette drive
- Ports:
  - AUI and RJ45 Ethernet
  - Parallel
  - Two serial
  - Keyboard
  - Mouse
  - Ultra SCSI
  - Line in/out

Figura 2.10 Características de IBM RS/6000 7046 B50 del fabricante [13]

En la *figura 2.11* se puede observar que este dispositivo se trata de un servidor que está instalado en un *rack* para servidores IBM. En la *figura 2.12* se detalla el modelo y la identificación que tiene en la E.E.Q.S.A.

Figura 2.11 IBM RS/6000 7046 B50 montado en el rack de servidores IBM en el Centro de Computación del Edificio Matriz Las Casas de la E.E.Q.S.A.

Figura 2.12 Identificación de la EEQ S.A. del Firewall IBM RS/6000 7046 B50

2.3.1.2 Componentes de *software*

El Sistema Operativo es un AIX[39, 40] 3.2 que básicamente es un sistema con un kernel de UNIX y que fue modificado según las necesidades por IBM para que fueran instalados y distribuidos en sus equipos de servidores.

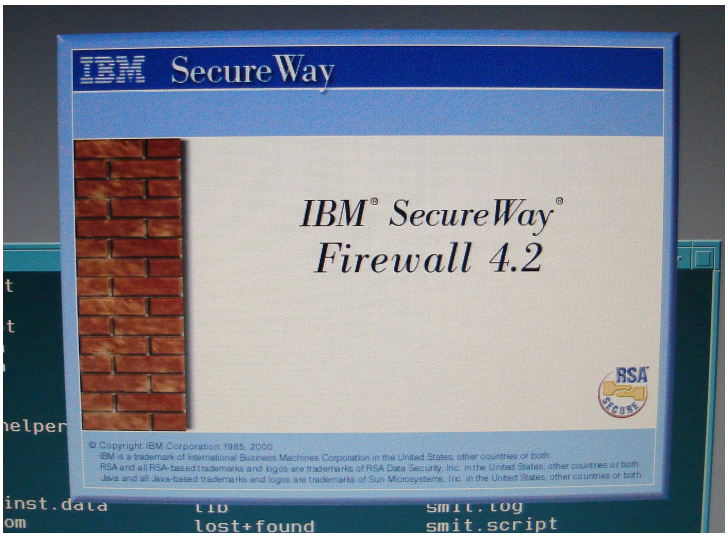


Figura 2.13 Iniciando el IBM SecureWay Firewall

Sobre la plataforma AIX se ejecuta la aplicación que da la funcionalidad de equipo de seguridad perimetral, este software es el IBM *SecureWay Firewall version* 4.2 para AIX.

---

[39] AIX (*Advanced Interactive eXecutive*) es un sistema operativo UNIX *System V* propietario de IBM. Inicialmente significaba "Advanced IBM Unix" pero probablemente el nombre no fue aprobado por el departamento legal y fue cambiado a "Advanced Interactive eXecutive"

[40] Información detallada sobre la plataforma AIX 4.3.3 ver en el documento http://www.redbooks.ibm.com/redbooks/pdfs/sg242014.pdf

Con la ayuda del administrador del *firewall* se ha podido ingresar a la configuración del mismo; en la *figura 2.13* se observa la ventana de presentación del IBM *SecureWay Firewall*.

2.3.1.3 Funcionalidades

Puesto que IBM *Firewall* es básicamente una puerta de enlace IP, divide todo en dos o más redes: una o más redes no protegidas y una o más redes protegidas. La red no protegida es, por ejemplo, Internet. Las redes protegidas pueden ser las redes IP corporativas. Entre las herramientas que IBM *SecureWay Firewall* ofrece se encuentran: [3]

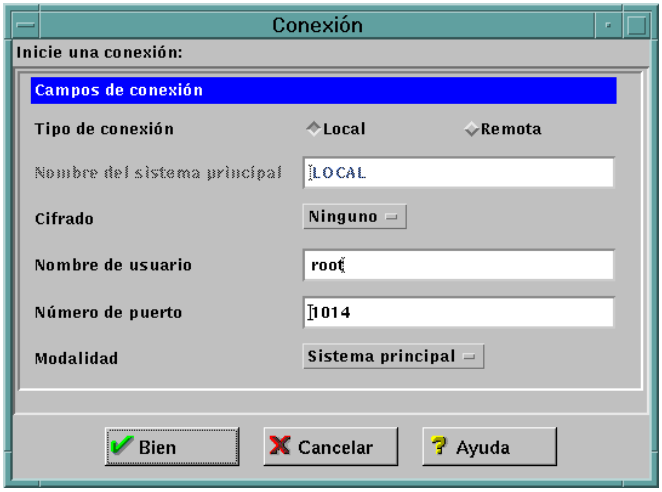


Figura 2.14 Ventana de ingreso al Sistema IBM Firewall [14]

- Filtros expertos
- Servidores *proxy*
- Servidores *socks*[41]
- Autentificación
- Servicios específicos, como el servicio de nombres de dominio (DNS) y el *proxy* de correo protegido
- Conversión de direcciones de red
- Redes privadas virtuales

[41] SOCKS es un protocolo de Internet que permite a las aplicaciones Cliente-servidor usar de manera transparente los servicios de un *firewall* de red. SOCKS es una abreviación de "SOCKetS".

– Comprobación de seguridad de la red

Para poder ver estas funcionalidades primero se debe acceder al sistema, de la manera que se indica en la *figura 2.14*.

Una vez ingresados al sistema se puede navegar por todas las funcionalidades que tiene este *firewall*, tal como se puede observar en la *figura 2.15*.

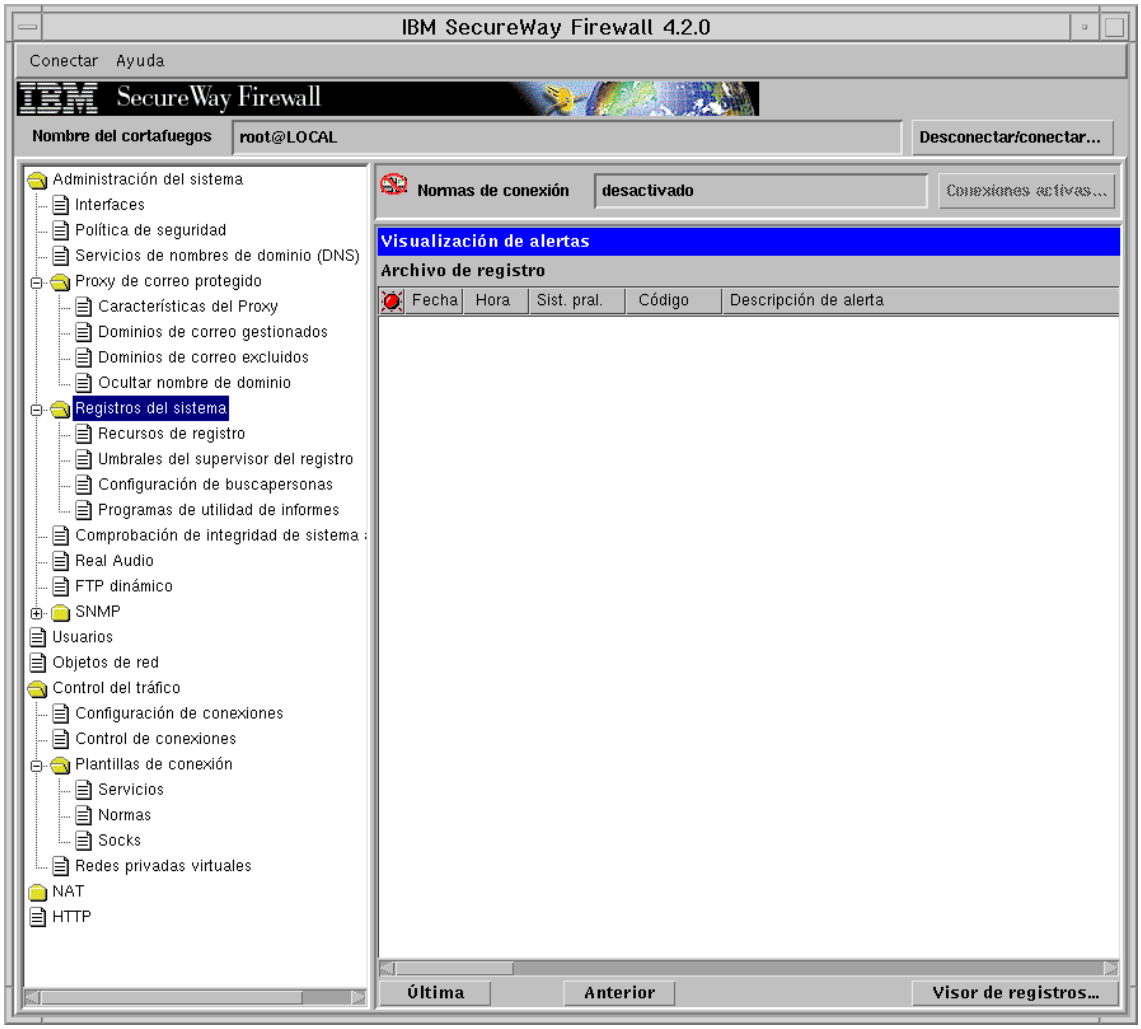


Figura 2.15 Ventana principal del IBM SecureWay Firewall [14]

2.3.1.4 Configuraciones principales de seguridad

De acuerdo a las necesidades de la E.E.Q.S.A. se han realizado las siguientes configuraciones:

Se han creado usuarios de tipo locales para el acceso a Internet. Éstos son administrados dentro de ***opción de usuarios*** del árbol de la ***ventana principal.*** En la *figura 2.16* se observa una parte de los usuarios configurados para acceso al Internet.

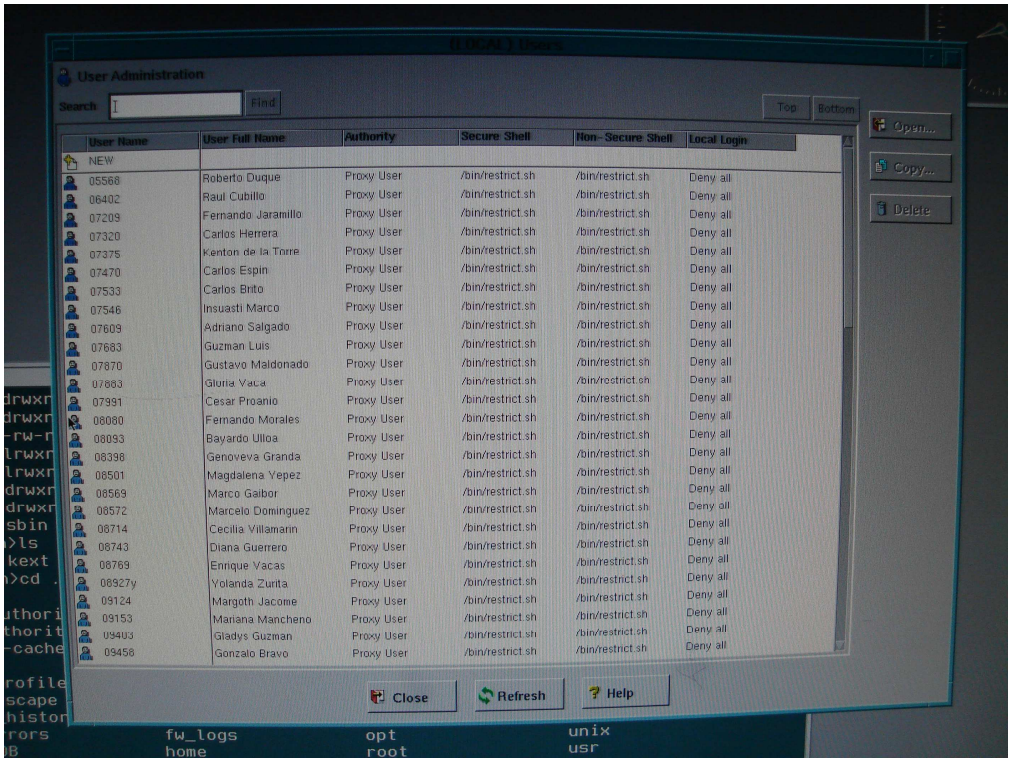


Figura 2.16 Lista de usuarios locales almacenados en el Firewall IBM

En el caso de usuarios, el *firewall* no soporta compatibilidad con Active Directory ni tampoco con RADIUS, esto hace que no sea flexible, ya que la administración de usuarios mejora si es almacenada o migrada a un servidor que exclusivamente permita una operación de gestionador de contraseñas, como así lo demanda el crecimiento de usuarios de la E.E.Q.S.A.

Se tienen configuradas políticas para los distintos objetos del *firewall*, éstos representan equipos, redes, o usuarios. Un extracto de la configuración mencionada es mostrado en la *figura 2.17.*

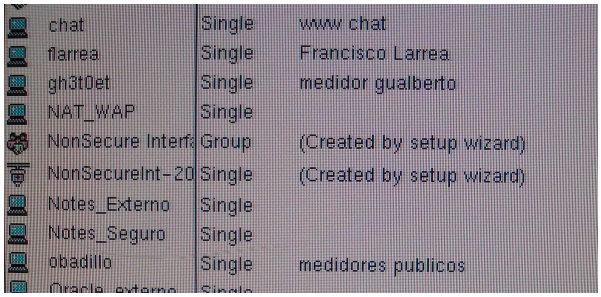


Figura 2.17 Grupo de objetos del Firewall

Algunas de las políticas para estos usuarios se pueden ver en la *figura 2.18*. Estas políticas en lo posterior serán las que deben ser migradas al nuevo equipo de seguridad perimetral.

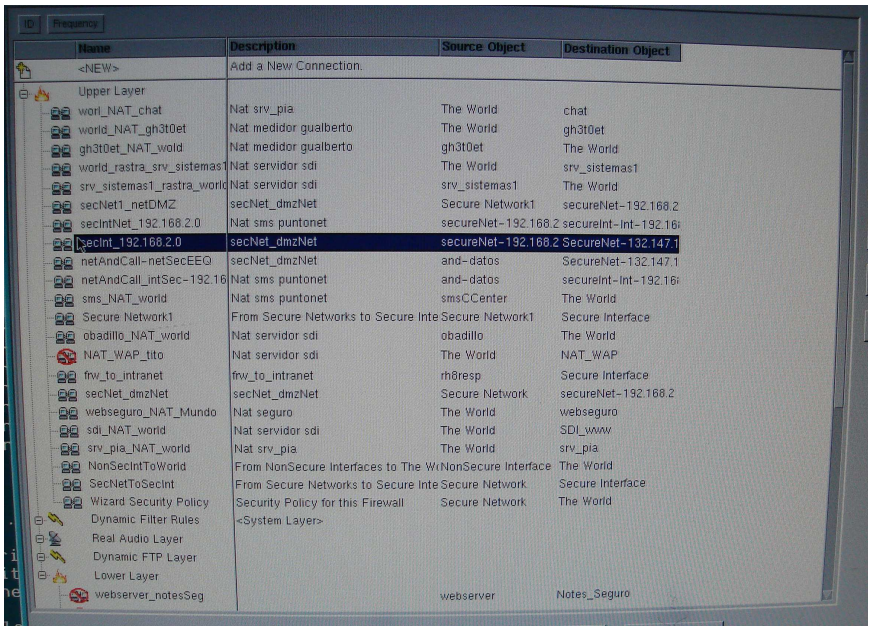


Figura 2.18 Políticas configuradas en el Firewall

El *firewall* puede ser monitoreado y accedido remotamente a través de la red Ethernet, pero eso sólo incluye aspectos relacionados con el sistema operativo, más no con el *software* IBM *SecureWay Firewall 4.2.0*. Para crear, cambiar o modificar parámetros que tengan que ver directamente con el *software* de seguridad, esto se lo debe hacer directamente con el equipo. Como se trata de un equipo que está en el Centro de Cómputo, se crea una incomodidad el tener que registrarse para el ingreso al Centro de Cómputo y además soportar el frío generado por el aire acondicionado.

De acuerdo a lo señalado por el administrador del *firewall*, se hace necesario que la herramienta de seguridad, pueda ser monitoreada y configurada desde un equipo remoto con las seguridades que implica este escenario.

2.4 ANÁLISIS DE LOS MÉTODOS DE ACCESO Y AUTENTICACIÓN DE LOS DIFERENTES USUARIOS A LA RED DE DATOS

Los diferentes usuarios que ingresan a la red de la E.E.Q.S.A., acceden a varias aplicaciones, el acceso va desde el inicio de sesión del sistema operativo hasta los diferentes sistemas que maneja la Empresa, incluido el acceso a Internet.

Existen tres formas en las que los usuarios se autentican con los sistemas informáticos: *Active Directory*, Base de Datos de las Aplicaciones y Base de Datos Locales de los equipos de comunicaciones.

2.4.1 AUTENTICACIÓN POR MEDIO DE *ACTIVE DIRECTORY*

Figura 2.19 Ingreso al correo electrónico de la E.E.Q.S.A.

Las cuentas de usuario son manejadas en un ambiente *Active Directory*, y a partir de ahí se genera una sola clave para cada uno de los sistemas informáticos, los cuales interactúan con las bases de datos y aplicaciones que se encuentran en el Centro de Cómputo.

Las *figuras 2.19* y *2.20* presentan dos de las aplicaciones que ya cuentan con la integración de un solo nombre de usuario y contraseña, el nuevo servicio de correo electrónico y el sistema de Administración de Recursos de Comunicaciones y Redes.

El sistema de contraseñas permite que el usuario desde las opciones del correo electrónico pueda cambiar la contraseña o *password*. Este cambio se ve reflejado cuando se requiere ingresar a un sistema y éste le solicita el nombre de usuario y contraseña. La contraseña sirve y se aplica para cualquier otro sistema integrado con el gestionador de cuentas de *Active Directory*.

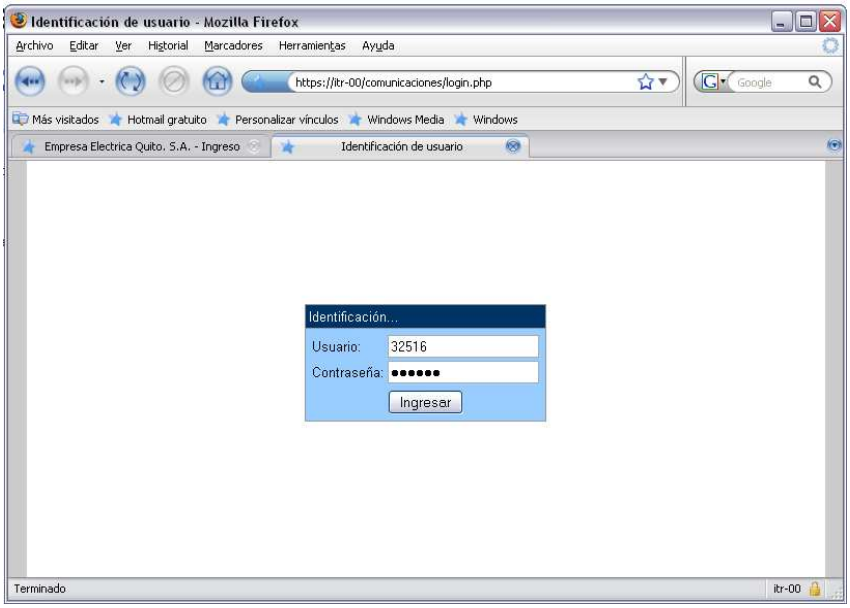


Figura 2.20 Ingreso al sistema de gestión de direcciones IP

Este sistema tiene que reemplazar en su totalidad a los sistemas de contraseñas de cada una de las aplicaciones; sin embargo habrán aplicaciones que por la configuración que posee, tiene dependencia con la cuenta de usuario, como es el

caso del Sistema SDI y SIDECOM los cuales por el momento no se puede cambiar al esquema deseado.

2.4.2 OTROS MEDIOS DE AUTENTICACIÓN PARA EL ACCESO A APLICACIONES

El sistema de autenticación por medio de *Active Directory* no ha sido implementado en su totalidad, es por eso que aplicaciones como el GIS, SDI, Sistema de Recursos Humanos entre otros aun poseen una base de datos de usuarios independientes, residentes en los servidores de aplicación y bases de datos.

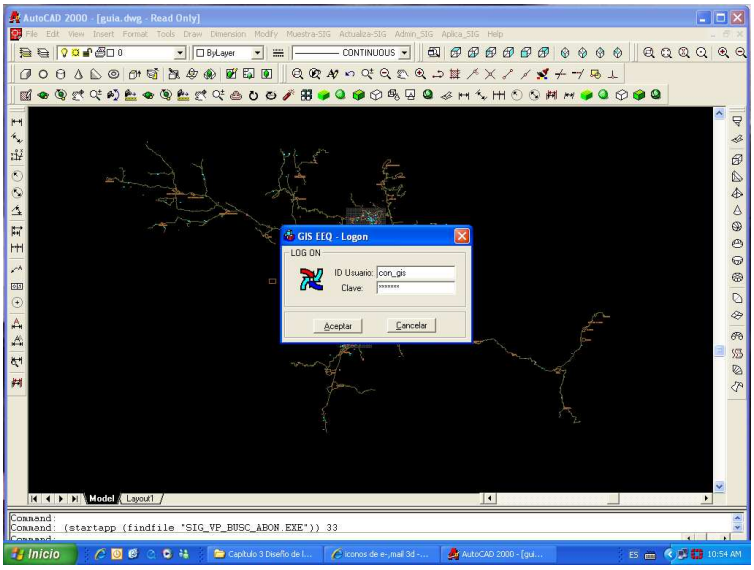


Figura 2.21 Sistema GIS, acceso por medio de la base de datos del mismo sistema GIS

Como se observa en la *figura 2.21*, el nombre de usuario y contraseña de la aplicación GIS tiene una ventana propia del sistema donde se ha desarrollado la aplicación del GIS.

En muchos casos los usuarios tienen que acceder a dos o más aplicaciones de la E.E.Q.S.A., lo que ocasiona un problema cuando tienen que recordar más de un nombre de usuario y contraseña, ocasionando lentitud y poca eficiencia en el trabajo.

Una de las aplicaciones más usadas en el entorno de trabajo diario de los usuarios internos de la E.E.Q.S.A., es el SDI. Este sistema reside en el servidor de aplicación SDI, bajo una plataforma Linux, donde se ha desarrollado dicho sistema. La cuenta de usuario es gestionada por el servidor *WEB* Apache. El modo de acceso se lo puede observar en la *figura 2.22*.

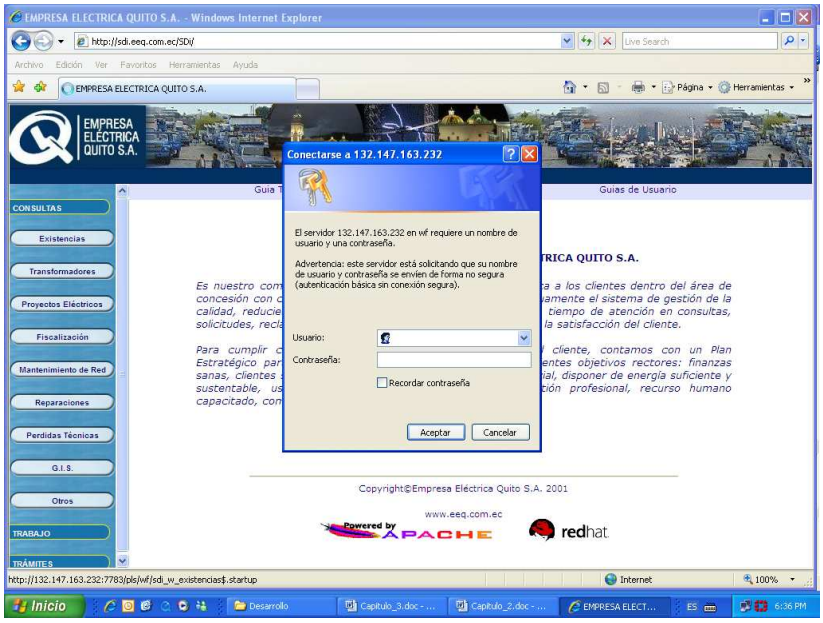


Figura 2.22 Sistema WEB-SDI. Acceso por medio de usuarios localizado en el servidor web de la aplicación

Estos son dos ejemplos de lo que se ha manejado por varios años en la E.E.Q.S.A.; se podría seguir mencionando otras aplicaciones, y se tendría el mismo resultado del análisis que es, nombre de usuario y contraseña diferente.

Si bien es cierto se necesita tener una seguridad aceptable, no es menos cierto que al mantener las contraseñas separadas, pueden ocasionar graves problemas de seguridad, como por ejemplo, copiar las claves en papeles que se pegan en los monitores, mesas, etc., y quedando la seguridad de los sistemas informáticos quebrantada.

2.4.3 ACCESO DE LOS EQUIPOS Y USUARIOS AL DOMINIO DE LA RED CORPORATIVA DE LA E.E.Q.S.A.

La red interna cuenta con un servidor de dominio que se ejecuta en una plataforma *Microsoft Windows Server 2003*. Dentro de este servidor se ejecuta el controlador del dominio para la red local y es el que gestiona las cuentas de usuarios y contraseñas, tanto para acceso a los PCs como para las diferentes aplicaciones. Con ello al ingresar como usuario válido dentro del dominio de la red local, se podrá compartir recursos a través de la red, esto es transparente para el usuario.

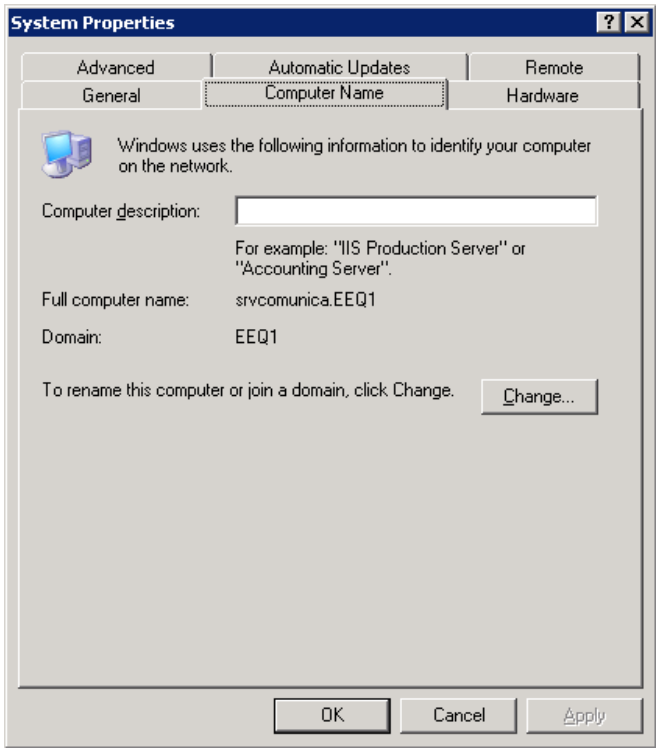


Figura 2.23 Ventana de Propiedades del Sistema de Windows Server 2003 que indica el nombre del equipo en el dominio EEQ1

Para que los equipos y usuarios puedan disponer de los recursos de la red, es necesario que tanto el equipo como el usuario sea parte de un dominio, para el caso de la E.E.Q.S.A., se tiene el dominio EEQ1 y EOL; estos dominios son de tipo *Windows Microsoft NT*. El dominio EOL reside en un servidor que está próximo a dejar de funcionar, lo que obliga a migrar tanto los equipos como a los usuarios al nuevo dominio EEQ1. EEQ1 está operando sobre un equipo moderno

y sistema operativo moderno, ya que EOL funcionaba bajo *Microsoft Windows NT Server 4.0*.

Los requisitos para que un usuario de la E.E.Q.S.A. sea parte del dominio EEQ1 es que el equipo o PC esté instalado *Microsoft Windows 2000 Professional*, *Microsoft Windows XP Professional* o *Microsoft Windows Server 2003*. Estos requisitos son los recomendables en cuanto al equipo, para el caso del usuario es diferente, ya que esto se lo hace a través del Administrador de los Sistemas Informáticos, él es quien crea la cuenta y le configura un perfil de usuario en el servidor que controla el dominio.

Figura 2.24 Lista de dominios cargada en la ventana de ingreso al Sistema Operativo

En el caso de las VPNs, los usuarios estarán en dos bases de datos. La primera y principal estará en funcionamiento bajo un servidor RADIUS y la segunda dentro de un grupo de usuarios de tipo local en el nuevo equipo de seguridad perimetral. Esto con el propósito de diferenciar los usuarios locales de los que acceden vía VPN. Esto se detallará posteriormente en el Capítulo 3.

2.5 ANÁLISIS DE LA CAPACIDAD EN CADA UNO DE LOS ENLACES EXTERIORES

En esta sección se analizarán las capacidades reales de los enlaces que forman parte de la red inalámbrica y la extranet. Para esto se ha utilizado el paquete

PRTG[42] con el que cuenta la E.E.Q.S.A. para monitorear el consumo de ancho de banda de los enlaces que posee y se lo comparará con las capacidades de cada uno de los canales de comunicación.

2.5.1 ENLACE ANDINADATOS – AGENCIAS DE RECAUDACIÓN Y ATENCIÓN AL CLIENTE

Con Andinadatos se ha contratado alrededor de diez enlaces tanto para agencias urbanas y rurales. Cada enlace cuenta con una capacidad de 128 Kbps. Los sitios que cuentan con estos enlaces en la actualidad han sido dotados de nuevos enlaces contratados a la empresa Telconet, con lo que se tiene redundancia de respaldo en dichos sitios. Estos nuevos enlaces tienen un ancho de banda de 1024 kbps.

Andinadatos provee su servicio de datos a la E.E.Q.S.A. instalando un equipo de acceso remoto o DCE y un *router* o DTE en los sitios remotos, generalmente los sitios remotos son Agencias de Recaudación; a excepción de las Agencias de Cumbayá, El Inca y Solanda, los *routers* son propiedad de la E.E.Q.S.A.

El servicio de transmisión de datos proporcionado por Andinadatos es con tecnología *Frame Relay* y/o ATM. En la *figura 2.4* dentro de la nube de Andinadatos se grafica líneas entrecortadas rojas que indica que el enlace tiene configuración de extremo a extremo con tecnología *Frame Relay*, y la línea entrecortada verde significa que el extremo del enlace ubicado en la E.E.Q.S.A. está configurado con parámetros de enlace ATM y en el extremo remoto se ha configurado con parámetros de enlace *Frame Relay*; ésta corresponde a una configuración interna en la red de Andinadatos.

Físicamente la E.E.Q.S.A. tiene dos *routers* para el acceso a la red de Andinadatos. El primer *router* tiene en funcionamiento un enlace con la Agencia Nanegalito, este enlace está contratado con un ancho de banda de 128 kbps y se

[42] PRTG (*Paessler Router Traffic Graphic*). Es una aplicación compatible con sistemas Microsoft y sirve para monitorear básicamente el consumo de ancho de banda de determinada interfaz.

puede revisar en la *figura 2.25*, el tráfico generado en la interfaz Ethernet del *router* Cisco 2600 que está conectado a la red de Andinadatos; este ejemplo permite ver cómo se usa este canal de comunicaciones. En el caso de este *router* como ya lo mencionamos solo cuenta con el enlace hacia la Agencia Nanegalito, por el momento.

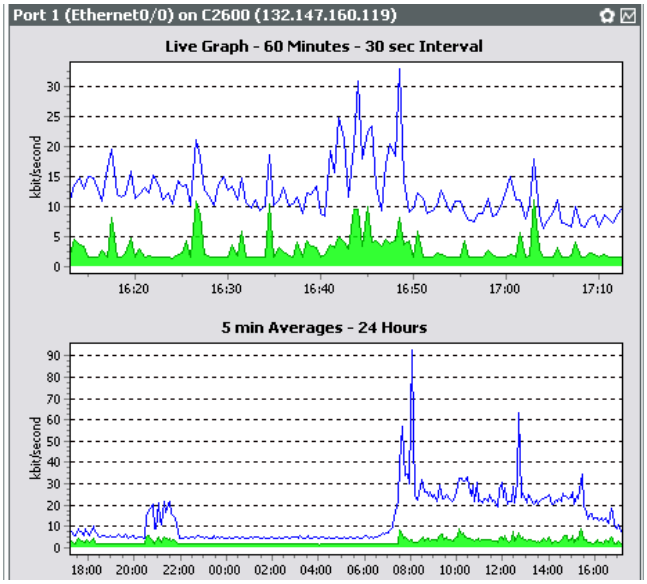


Figura 2.25 Tráfico generado por el enlace Ag. Nanegalito -E.E.Q.S.A. - Andinadatos

El tráfico que se ha generado por este enlace y mostrado en la *figura 2.25*, indica que alcanza un máximo de 35 kbps para un intervalo de monitoreo de 30 segundos y los promedios registrados cada 5 minutos indican un máximo de 90 kbps y variando la actividad entre las 07h30 hasta las 15h30 (horario de trabajo del personal administrativo) de 20 kbps a 30 kbps. Por lo tanto el canal de comunicación se estimaría que tiene un tráfico regular de 30 kbps dentro del horario de trabajo; ahora el canal contratado para esta Agencia es de 128 kbps de subida por lo que el consumo estaría en un 23.44 %. Para el canal de bajada se ha contratado 64 kbps, y como se observa en la *figura 2.25* el área de color verde corresponde al tráfico de subida o salida y tiene un consumo alrededor de 5 kbps en el mismo horario, lo que da un consumo respecto a la capacidad del canal de 7.81 %.

En otro *router*, un Cisco de la serie 800, tiene el resto de enlaces; para ver la actividad de tráfico se revisará la *figura 2.26* donde se podrá ver la actividad en

conjunto de los enlaces y en la *figura 2.27* se observará el caso particular del tráfico de una Agencia.

La interfaz que se va analizar del *router* Cisco 827 es la Ethernet 0, ya que es donde se concentra la actividad de la Agencias Cumbayá, El Inca, Solanda, Machachi, Pedro Vicente Maldonado, Baeza y Puéllaro. Cada uno de estos sitios tiene contratado un enlace de 128 kbps simétrico a excepción de la Agencia El Inca que se tiene contratado 512 kbps simétrico. El consumo dentro de la interfaz Ethernet 0 del Cisco 827 para el canal de bajada tiene un pico o valor máximo de consumo de alrededor de 450 kbps, y para el canal de subida tiene un pico de aproximadamente 200 kbps. La actividad registrada también indica que existen otros picos de hasta 350 kbps en el tráfico de entrada o bajada y que tiene una regularidad de alrededor de 200 kbps, en cambio para el canal de subida se tiene una regularidad de alrededor de 70 kbps. El canal principal tiene una capacidad contratada de 640 kbps tanto de bajada como de subida lo que da una utilización regular del canal de bajada de 31.25 %. Para el tráfico de subida el porcentaje de utilización regular es de 10.94 %. En la *figura 2.26* se muestra la actividad de la interfaz Ethernet 0 y es de donde se han recolectado los valores antes mencionados para las respectivas estimaciones de utilización del enlace.

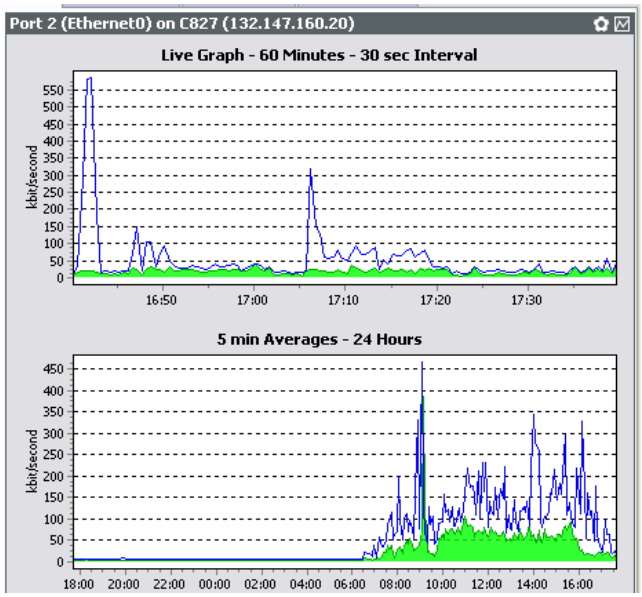


Figura 2.26 Tráfico del enlace E.E.Q.S.A. – Andinadatos a través del Cisco 827 interfaz Ethernet

Para el caso de la *figura 2.27* se ha tomado como referencia la Agencia El Inca, que es una de las Agencias más grandes en cuanto a equipos computacionales y de gran afluencia de clientes del servicio de energía eléctrica, por lo tanto es una de las Agencias con más movimientos en la red. Las otras agencias presentan actividad de tráfico menor.

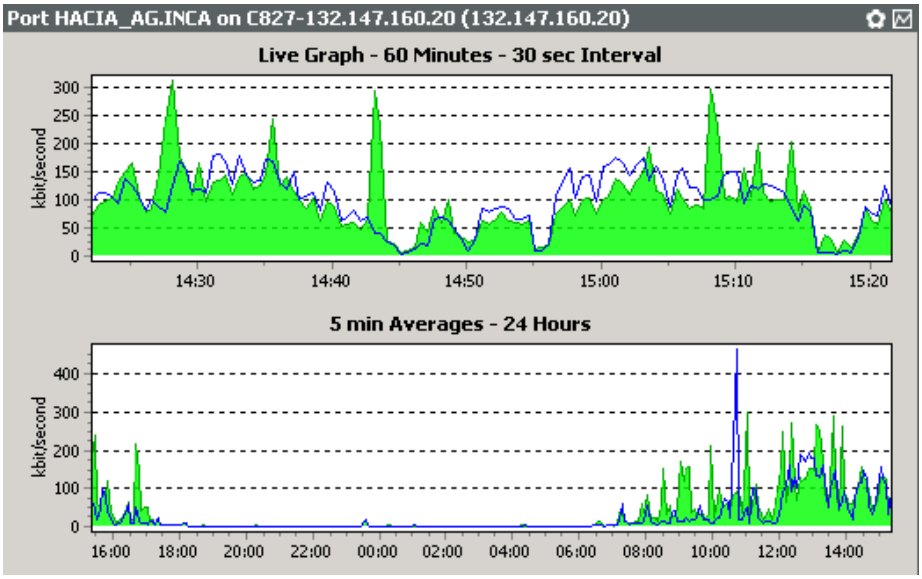


Figura 2.27 Tráfico generado por la Agencia El Inca

En la *figura 2.27* se puede apreciar que la línea azul que corresponde al tráfico de entrada, presenta unos valores máximos entre 150 kbps y 200 kbps, mientras que el área verde presenta valores de consumo de hasta 300 kbps, y también se podrá notar que los valores de tráfico regulares tanto de entrada como de salida son similares y que alcanzan sus máximos en aproximadamente 190 kbps, de lo que se puede apreciar. Para realizar una estimación de la utilización del canal se tomará el valor de 190 kbps, lo que da una utilización respecto a los 512 kbps contratados, de 37.11 % de la capacidad del canal utilizado tanto de subida como de bajada.

2.5.2 ENLACE TELCONET – EMPRESAS DE INTERCAMBIO INTERINSTITUCIONAL Y COMERCIAL

Con Telconet se tiene enlaces con empresas como Emelnorte, CATEG, Servipagos y Banco de Guayaquil. Todas estas empresas generan un tráfico en

conjunto que se detalla en la *figura 2.28*. Estos enlaces ingresan a la empresa a través de un solo enlace de físico, y dentro del *router* que pertenece a Telconet se procesa la información de las redes de las distintas empresas.

Esto ocasiona que no se pueda ver a detalle el tráfico particular de cada uno. Por lo tanto se deberá implementar un mecanismo para poder visualizar cada red y de ser posible, también implementar seguridad en el enlace.

La *figura 2.28* permite observar que este multienlace tiene una alta actividad, comparada con los enlaces de Andinadatos, aquí básicamente fluye tráfico asociado al sistema SIDECOM.

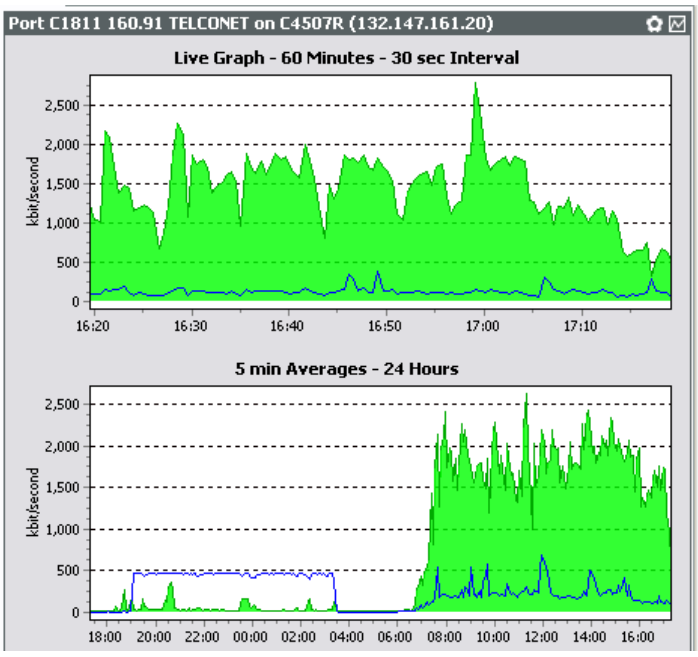


Figura 2.28 Tráfico generado por el enlace de Telconet

La forma en como se provee el servicio de transmisión de datos de Telconet, es a través de fibra óptica desde un nodo cercano al edificio Matriz Las Casas de la E.E.Q.S.A. La fibra óptica llega a un convertidor para que la señal óptica llegue a una interfaz Fast-Ethernet del *router* que es de propiedad de Telconet. Por otra interfaz Fast-Ethernet, el *router* se conecta a la red de la E.E.Q.S.A. Por este enlace las diferentes empresas pueden conectarse con los servicios que necesitan para realizar las operaciones correspondientes, como por ejemplo

Servipagos y Banco de Guayaquil para recaudación, CATEG y EMELNORTE asesoría del sistema informático comercial, y Telconet para asesoría técnica y comercial de enlaces de datos.

En la *figura 2.7* se detalla la red IP correspondiente a cada enlace de la extranet que utiliza el servicio de Telconet; de lo que se observa por el multienlace llegan dos redes IP de Servipagos, una de la CATEG, dos del Banco de Guayaquil y una de Emelnorte. La *figura 2.7* también muestra que sobre un solo enlace físico se provee de servicio a cuatro empresas que requieren el acceso a los servidores de comercialización de la E.E.Q.S.A.

Todos los enlaces y redes IP que cruzan por el multienlace de Telconet - E.E.Q.S.A. están generando un tráfico que tiene un promedio de 2000 kbps de salida y 250 kbps de entrada en el horario de oficina; este tráfico se genera sobre la interfaz Fast-Ethernet del *router* de Telconet. Como el servicio es para empresas externas, la capacidad del canal de las diferentes redes de la extranet, sería la suma de cada uno de los enlaces, ya que es Telconet quien se compromete a garantizar dichos enlaces, y que para realizar este servicio llega a la E.E.Q.S.A. por fibra óptica, que es el enlace de última milla. Sin embargo la capacidad del canal de comunicaciones está dado por la capacidad física entre el convertidor de medio hacia la interfaz del *router* de Telconet que se encuentra en el centro de computo de la E.E.Q.S.A. y que es Fast-Ethernet o 100 Mbps. Como se sabe en Fast-Ethernet los 100 Mbps son para transmisión y otros 100 Mbps para recepción en modo *Full Duplex*, es decir que el porcentaje de utilización para el enlace de bajada es de 2 % y para el de subida es de 0.25 %. Estos valores nos indican que la última milla entre Telconet y la E.E.Q.S.A. tiene alta capacidad de crecimiento futuro si es el caso de que otras empresas o la misma E.E.Q.S.A. necesitan utilizar este enlace para acceder a los sistemas informáticos de la red de datos de la E.E.Q.S.A.

2.5.3 ENLACES INALÁMBRICOS

Los enlaces inalámbricos son una solución que permiten establecer comunicación con aquellas edificaciones pertenecientes a la E.E.Q.S.A., que se encuentran en lugares donde adquirir un enlace dedicado es costoso y no cumple con un ancho de banda adecuado para el aceptable funcionamiento de las aplicaciones o simplemente no existen redes por parte de las empresas que proveen el servicio de datos.

Una infraestructura propia para este tipo de comunicaciones, permitirá que se puedan tener mejores condiciones para la transmisión de datos, posibilitando ejecutar de manera aceptable las aplicaciones necesarias para cumplir con las labores de recaudación, servicio y atención al cliente, gestión de personal, impresiones, etc.

Actualmente la red inalámbrica está en modo de enlace de respaldo para aquellas edificaciones donde se ha añadido enlaces a través de Telconet, que tiene mejores tiempos de respuesta. Sin embargo se ha optado por utilizar este medio para la aplicación de telefonía IP, lo cual implica que estos enlaces deben manejar seguridad y calidad de servicio.

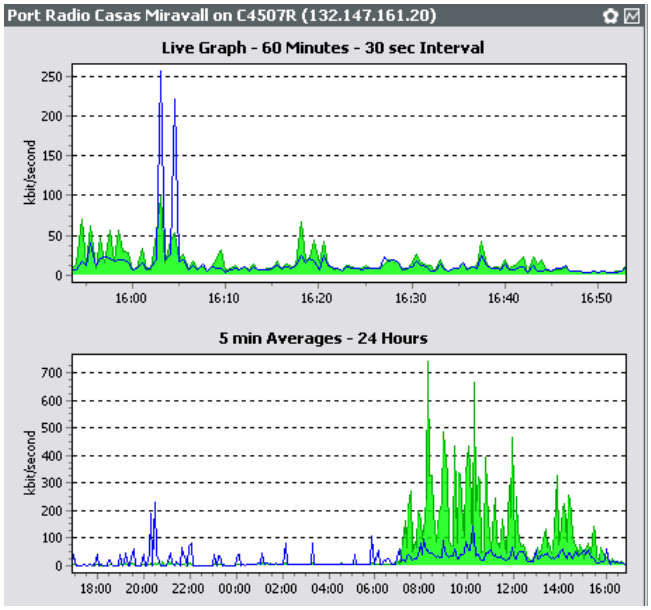


Figura 2.29 Tráfico del enlace principal desde el Edificio Matriz Las Casas hacia el sitio de repetición en Miravalle

En la *figura 2.29* se muestra la actividad del tráfico del enlace principal entre el edificio matriz Las Casas y el sitio de repetición Miravalle, ya que desde este sitio se distribuye el acceso de datos hacia la Central Térmica de Generación Gualberto Hernández y Central Hidroeléctrica de Generación en el sector de Guangopolo, las Agencias de Sangolquí y Conocoto, esto para el sector del Valle de los Chillos; para el sur de Quito Agencia Solanda y para el centro de Quito la Agencia Chiriyacu. Este conjunto de dependencias de la E.E.Q.S.A. generan sobre el enlace Las Casas – Miravalle un tráfico de salida promedio de alrededor de 200 kbps con picos en el tráfico que sobrepasan los 700 kbps, estos datos son tomados de la *figura 2.29* en la parte correspondiente al reporte de tráfico diario. En el caso de los enlaces inalámbricos la capacidad del canal está dado por los radios que cumplen la función de *Bridges* o puentes; cada par de radios que conforman un enlace, tiene una configuración donde se establecen los parámetros de comunicación inalámbrica, como frecuencia, canal, identificación del canal, velocidad de transmisión, nombre del equipo y nombre del sistema de comunicación, estos parámetros se los puede observar en las *figuras 2.30 y 2.31*, que corresponden al enlace principal entre Matriz Las Casas – Miravalle. La velocidad del enlace está configurado en 12 Mbps y este valor es la capacidad del canal, respecto al tráfico de salida se tiene que la utilización es de 1.67 %

Se analizará el enlace inalámbrico de la Agencia Sangolquí; la *figura 2.32* indica los parámetros de configuración del enlace inalámbrico entre el sitio de repetición Miravalle y la Agencia Sangolquí. La *figura 2.33* permite mostrar el comportamiento de la actividad de tráfico y del que se puede ver que el tráfico de salida es de 300 kbps que se estima como promedio. Si se observa la *figura 2.32* el parámetro correspondiente a la velocidad de transmisión está en 2 Mbps lo que da una utilización de 15%.

El comportamiento del resto de enlaces inalámbricos es muy similar a los expuestos en esta sección y lo que cabe indicar es que son enlaces que tienen una utilización baja; por esta razón se puede esperar que un crecimiento futuro en la utilización no afecte el rendimiento del enlace. Lo que si frenaría un posible crecimiento en la utilización, son problemas tales como: interferencias en la

frecuencia de uso, saturación de canales para *Spread Spectrum* en 2.4 Ghz y tormentas eléctricas que pueden afectar físicamente a los equipos de comunicación. Estos inconvenientes hace que se tomen medidas como cambiar la banda de frecuencia a 5.8 Ghz que tiene más canales para utilizar y también mejorar la infraestructura no solo de comunicaciones sino de seguridad eléctrica ante la amenaza de tormentas eléctricas.

2.5.4 ENLACE TELCONET - INTERNET

El Internet es uno de los principales medios para implementar las redes privadas virtuales. Es por eso que es importante conocer el estado del enlace de Internet.

Este enlace provisto por Telconet tiene una capacidad contratada de 3.5 Mbps. Un dato que es de mucha importancia y con el que no se cuenta hasta el momento, es el número de equipos que están ingresando al Internet, así como un detallado informe estadístico del uso de este medio. Solo a través de un analizador de tráfico se puede advertir si el acceso al Internet tiene un comportamiento normal o anormal. Es así que se cuenta con este gráfico y las cuentas de usuario del *firewall* como únicos medios de ayuda para gestionar el acceso hacia el Internet.

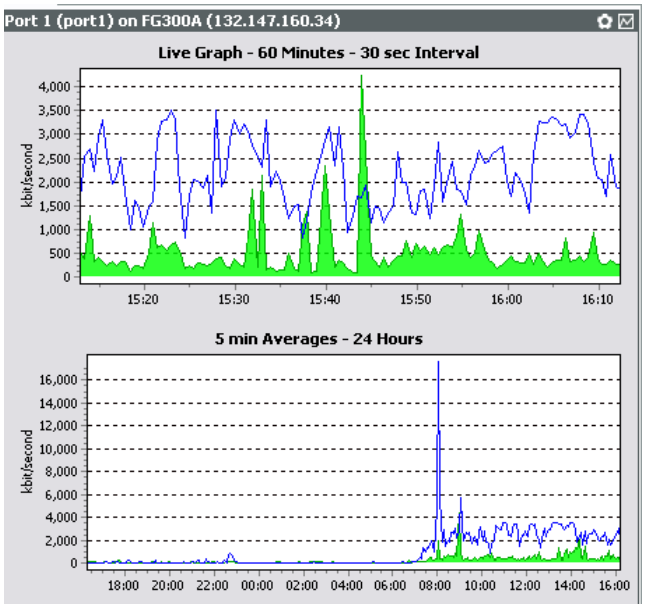


Figura 2.30 Tráfico tomado de la interfaz correspondiente al acceso de Internet en el Switch – Router

Como se puede ver en la *figura 2.34* el tráfico de entrada que se genera tiene un promedio estimado de 3000 kbps lo que da una utilización de 85.71%, valor alto de ocupación si se toma en cuenta que se necesita implementar VPNs. Al no tener un adecuado control en el acceso a Internet, esto complica determinar qué puede causar que se tengan niveles de utilización altos; por ejemplo el tiempo de utilización que los usuarios están conectados al Internet, tomando en cuenta que por razones del puesto de trabajo la mayoría de usuarios deben estar un tiempo mínimo accediendo al Internet, no hay razón para que estén horas conectados al Internet. Antes de aumentar la capacidad del enlace para el acceso al Internet es necesario que se verifique otros factores que pueden afectar el consumo de la capacidad del enlace como *software* que este ejecutándose automáticamente en los PCs para acceder al Internet, entre estas aplicaciones se tiene espías, troyanos, chats, videos en línea, descarga de *software* que no tiene que ver con el trabajo de la empresa, posibles ataques desde el exterior y otras amenazas que posiblemente ocasionen que se genere tráfico no deseado en el enlace. La depuración de los equipos de la red interna y el control del acceso con herramientas adecuadas por parte de los Administradores del acceso a Internet y de la red de la E.E.Q.S.A. permitirá establecer si es necesario o no contratar más capacidad en el enlace para así tener éxito en la implementación de los canales virtuales seguros.

2.6 RESUMEN Y CONSIDERACIONES DEL CAPÍTULO

Este resumen de la actual situación de la red de datos, da la posibilidad de obtener una mejor visión y manejar un buen criterio, para establecer prioridades en los accesos a la red. Es por esto que este proyecto tratará en lo posible dejar información importante para mejorar en el aspecto de seguridad en la red de datos.

2.6.1 USUARIOS Y APLICACIONES DEL SISTEMA INFORMÁTICO DE LA E.E.Q.S.A.

Los usuarios que tiene la E.E.Q.S.A. como se ha señalado en este capítulo son de tres tipos, los que pertenecen a la DTICs (División de Tecnología de la Información y Comunicaciones), los usuarios Locales, y los Remotos. Estos tres grupos de usuarios se diferencian por la localización y la naturaleza de sus necesidades; es así, que quienes sean administradores del sistema informático en lo posible deben estar cerca del Centro de Cómputo y satisfacer las necesidades del cliente tanto interno como externo. Los Usuarios Locales y Usuarios Remotos Internos, son los que a diario necesitan ejecutar las herramientas informáticas que demanda su puesto de trabajo y que operan en las dependencias de la E.E.Q.S.A. que forman parte de la red corporativa. Los Usuarios Remotos Externos que acceden a la sitio *WEB* de la E.E.Q.S.A. y quienes tienen autorización para ingresar a través de redes externas a los recursos informáticos, necesitan que su acceso sea confiable y que por parte de la E.E.Q.S.A. no existan deficiencias que limite el uso del servicio que la empresa presta a través de los medios de comunicación informático.

Las aplicaciones que cuenta la E.E.Q.S.A. como herramienta para gestionar los distintos procesos administrativos, son variadas en cuanto respecta a su origen de desarrollo. Es así que el sistema SIDECOM que permite realizar los procesos Comerciales de la empresa, tiene su origen sobre una plataforma distinta a la de entorno gráfico que hoy se conoce; de hecho el ambiente gráfico es lo nuevo de este sistema si embargo la funcionalidad sigue en la misma plataforma. El sistema SDI básicamente maneja los procesos que corresponden a la distribución del sistema eléctrico, esta aplicación está implementada sobre una plataforma Linux y desarrollado para que los usuarios puedan acceder a través de un navegador Web. El WEB-GIS que también se ejecuta sobre navegadores Web, y está implementado sobre una plataforma *Microsoft Windows NT*. Las aplicaciones de Talleres y Transportes, Recursos Humanos, Financiero, Bodegas, etc., aplicaciones cliente-servidor que luego de la inclusión de los sistemas CITRIX han pasado a ser parte de las aplicaciones virtuales. Todas las aplicaciones

mencionadas están íntimamente relacionadas con el sistema de base de datos de la E.E.Q.S.A. que es gestionado por el motor de base de datos ORACLE 10i.

2.6.2 ENLACES DESDE EL EXTERIOR DE LA E.E.Q.S.A.

Como se ha podido señalar, la red de datos con la que cuenta la E.E.Q.S.A., tiene variedad en los medios de comunicación, debido al tamaño y geografía que comprende el área de concesión y de la necesidad de poder integrar toda esta área al sistema informático central.

Los primeros enlaces en analizar fueron los que correspondían a los de tipo inalámbrico, donde se indicaba que se tienen cuatro puntos geográficos para la distribución de los datos hacia las distintas dependencias de la E.E.Q.S.A. A través de la *figura 2.2* se indica los parámetros de configuración de cada enlace inalámbrico y la tecnología usada para determinado enlace. Como se puede observar en la *figura 2.2* se indica que se utiliza equipos de comunicación inalámbrica que operan con tecnología IEEE 802.11a (OFDM) y IEEE 802.11b (*Spread Spectrum*). Los puntos geográficos de los que se menciona son, Edificio Matriz Las Casas, Cruz Loma, Miravalle, Collaloma, desde estos puntos varias agencias pueden acceder a la red corporativa, cubriendo gran parte de la zona urbana y parte de la zona periférica de Quito, donde se encuentran las dependencias de la E.E.Q.S.A.

Con Andinadatos se mantienen enlaces de datos de tipo WAN, estos enlaces son de 128 kbps simétrico para todas las agencias a excepción de la agencia El Inca que cuenta con un enlace de 512 kbps simétrico. La tecnología WAN utilizada en los siete de los ocho enlaces es *Frame Relay*/ATM, la agencia Nanegalito es la única que tiene una configuración extremo a extremo del tipo *Frame Relay*.

Un nuevo grupo de enlaces provistos por Telconet brinda acceso a varias agencias de la E.E.Q.S.A. y a varias empresas para acceder a la red corporativa. El método de acceso por parte de Telconet es por medio de fibra óptica como enlace de última milla, llega con un convertidor de medio (de fibra óptica a

Ethernet) a un *router* Cisco y éste con una interfaz Ethernet o Fast-Ethernet ingresa a la red local de los sitios que comprenden el enlace. En el lado del Centro de Cómputo de la E.E.Q.S.A. llega con dos *router* Cisco; un *router* Cisco 2600 sirve de acceso al Internet y un Cisco 1811 sirve de puerta de enlace para agencias y la extranet. También se ha mencionado sobre el servidor RAS que presta servicio a usuarios que a través del *dial-up* ingresan a los servicios del sistema informático de la E.E.Q.S.A.

2.6.3 *FIREWALL* ACTIVO Y MÉTODOS DE ACCESO Y AUTENTICACIÓN

El *firewall* activo con el que ha contado la red corporativa de la E.E.Q.S.A. hasta la actualidad, ha ido presentado ciertas limitaciones que cada vez que avanza el tiempo son muy notorias y que comprometen la seguridad del sistema informático de la red corporativa. Las limitaciones más destacables son: Complejidad de la administración del sistema operativo de plataforma y del *software-firewall*, desactualización de protocolos, *hardware* relativamente viejo, lentitud en el acceso a sitios Web del Internet, básica gestión de los usuarios, fallas de funcionamiento, entre otras.

Los sistemas de acceso y autenticación dentro de los diferentes servicios y aplicaciones de la E.E.Q.S.A. son muy variados; principalmente se tienen los sistemas antiguos de autenticación que están basados en que la aplicación de forma independiente tiene una base de datos de nombres de usuarios y contraseñas. El *Active Directory* ha ido implementándose paulatinamente y modificándolo según las necesidades, el objetivo es llegar a cubrir por completo el acceso con un solo sistema de gestión de cuentas de usuario.

2.6.4 CAPACIDAD DE LOS ENLACES EXTERIORES

Los enlaces exteriores tienen una capacidad dada por el contrato con empresas que prestan el servicio de transmisión de datos o también por las condiciones del enlace se realiza una configuración donde se establece una velocidad, esto básicamente sucede en los enlaces inalámbricos.

La utilización de cada enlace puede determinar la condición y el estado de dicho enlace, con un analizador de tráfico es posible estimar la utilización medido en porcentaje. Al haber anomalías en la utilización se investiga sobre las posibles causas que pueden afectar el buen desempeño del canal de comunicaciones. En la *tabla 2.1* se muestra un resumen de los enlaces que han sido analizados su actividad y utilización en este capítulo.

Enlace	**Medio (Última milla)**	**Propiedad**	**Capacidad (kbps)**		**Utilización (kbps) - El promedio diario**		**Utilización (%)**	
			Bajada	**Subida**	**Bajada**	**Subida**	**Bajada**	**Subida**
Agencia Nanegalito - E.E.Q.S.A.	Cobre	Andinadatos	128	64	30	5	23.44%	7.81%
E.E.Q.S.A. - Andinadatos	Cobre	Andinadatos	640	640	200	70	31.25%	10.94%
Agencia El Inca - E.E.Q.S.A.	Cobre	Andinadatos	512	512	190	190	37.11%	37.11%
E.E.Q.S.A. - Telconet	Fibra Óptica	Telconet	100000	100000	250	2000	0.25%	2.00%
Las Casas E.E.Q.S.A. - Miravalle	Inalámbrico (OFDM)	E.E.Q.S.A.	12000	12000	200	50	1.67%	0.42%
Agencia Sangolquí - Miravalle	Inalámbrico (*Spread Spectrum*)	E.E.Q.S.A.	2000	2000	300	100	15.00%	5.00%
Internet (E.E.Q.S.A. - Telconet)	Fibra Óptica	Telconet	3500	3500	3000	500	85.71%	14.29%

Tabla 2.1 Resumen de capacidad y utilización de los enlaces exteriores a la E.E.Q.S.A.

En todos los enlaces los datos de utilización dependen del punto de referencia desde donde se los está midiendo; por ejemplo el enlace Agencia Nanegalito – E.E.Q.S.A. se ha tomado como referencia para la lectura del tráfico la interfaz WAN en el lado del *router* de la E.E.Q.S.A., lo que indica que desde la agencia se ha estado enviando información hacia el *router*, como por ejemplo desde algún PC de escritorio del personal de soporte se haya establecido una sesión de escritorio remoto.

Un ejemplo de la actividad de tráfico que ratifica el comportamiento que espera, es el generado por el enlace de acceso al Internet; se tiene gran cantidad de consumo de bajada, lo que quiere decir que desde el interior de la E.E.Q.S.A. se realizan grandes cantidades sesiones con sitios *Web* que contemplan muchos

objetivos como descarga de archivos, revisar el correo exterior, aplicaciones multimedia, etc.

Se puede concluir que la actividad de tráfico de datos sobre estos enlaces, es baja para lo que a diario se necesita en las diferentes actividades, lo que también indica que es posible explotar de mejor manera estos enlaces, introduciendo si cabe la necesidad mecanismos de seguridad como por ejemplo encripción de los datos que circulan a diario por estos enlaces.

2.6.5 CONSIDERACIONES DEL CAPÍTULO

Se considera que la red es nueva, ya que está en plena modernización, no hace mucho se cambiaron los enlaces seriales asíncronos. Existen todavía sitios que se conectan a la empresa a través de enlaces *dial-up* con modems V.34.

Un dato muy importante y que hasta el momento no se lo ha mencionado, es el relacionado al direccionamiento de la red corporativa. La red corporativa comprende varios segmentos de red, muchos de los cuales utilizan diferentes espacios de direcciones, sin embargo hay que señalar que el espacio de direcciones más importante lo constituyen los equipos que se encuentran en el centro de cómputo en el edificio Matriz, Edificio Alvarez y Edificio Mariana de Jesús. La mayoría de los equipos de estos sitios utilizan la red 132.147.160.0 con 22 bits de máscara de subred (255.255.252.0), lo que da cabida para 1022 direcciones IP válidas para *hosts*. Como la red ha ido creciendo se hace necesario rediseñar el direccionamiento, con el objetivo de minimizar problemas en la red como direcciones IP duplicadas en los *hosts*, administración tediosa, etc. Para otros sitios se está utilizando como red principal la 172.16.0.0 con 16 bits de máscara que ha partir de esta red de tipo B se la ha estado dividiendo en subredes con máscara de 23 y 24 bits según la necesidad. La modalidad de obtener la dirección es estática, pero dependiendo del escenario es muy posible que necesite habilitar un servidor DHCP, como por ejemplo una red WLAN.

El *firewall* activo debido a su complejidad y poca versatilidad para la administración no permitió que se pudieran atrapar imágenes adecuadas que facilite visualizar de mejor manera la configuración y el estado del *firewall*, por lo que se fotografiaron las pantallas con información que se consideraban más importantes.

La red corporativa de la E.E.Q.S.A. no es la única de esta empresa; una red de datos está en pleno despliegue y que tiene como objetivo integrar a las subestaciones de distribución del servicio de energía eléctrica y a varias centrales de generación, a la red corporativa, ya que la lectura de datos de los equipos de medición eléctricos ya no serán de forma manual. Los nuevos equipos que realizan lecturas de las variables eléctricas tienen como interfaz de comunicación un puerto RJ-45 para poder integrarse a una red Ethernet. Esto indica el gran despliegue de la red corporativa de la E.E.Q.S.A. que compromete a mejorar la zona neurálgica de la red corporativa dotándola de mejores mecanismos de seguridad y administración.

Hay que señalar que la red de la E.E.Q.S.A. es muy cambiante, así como los enlaces exteriores, por lo que no debe sorprender si al término de este proyecto se han registrado cambios en la topología y configuración de la red, así como actualizaciones, renovaciones de contratos, etc.

Por último, es importante mencionar que en muchas de la *figuras* de este capítulo se menciona un equipo *Switch-Router*; este *Switch-Router* es un dispositivo de capa 3 Cisco 3560, en el que se han configurado varias VLANs y que debido al gran despliegue se sigue aumentado las VLANs. Es así que se tiene la VLAN 1 o administrativa para la red 132.147.160.0 / 22, VLAN 6 para la red inalámbrica 172.16.1.0 / 24, VLAN 7 para el Internet y así un gran número de VLANs. Es por esto que el mismo equipo es referenciado en varias de las *figuras* de este Capítulo pero la dirección de puerta de enlace es la que cambia; ya que cada VLAN tiene asociada una red IP diferente donde la primera dirección está asociada a la interfaz virtual del Cisco 3560, que tiene como dirección IP para la

VLAN administrativa la dirección 132.147.161.20 que sería la excepción al no ser la primera dirección valida de la red 132.147.160.0.

CAPÍTULO 3

DISEÑO DE LA RED PRIVADA VIRTUAL

3.1 DETERMINACIÓN DE USUARIOS Y APLICACIONES QUE UTILIZARÁN LAS VPNs

La solución de acceso a través de VPN, permite que los usuarios puedan utilizar este medio de comunicación. En lo que respecta al alcance de este proyecto, este se orientará a las necesidades de los recaudadores, administradores de sistemas informáticos, personal autorizado para utilizar VoIP y posibles *teleworkers*[43] o teletrabajadores de la E.E.Q.S.A.

En los centros de recaudación, es necesario que se les permita el acceso al sistema de comercialización (SIDECOM), el cual está disponible en las siguientes formas, a través de la red de datos:

- *Telnet (versión antigua) y,*
- *CITRIX (Aplicación moderna para recaudación en línea)*

Para aquellos administradores de sistemas informáticos, como de sistemas CITRIX, Base de datos, Seguridad y Redes de Comunicaciones, el acceso hacia los recursos de red debe ser de manera segura y confiable. De esta manera es posible realizar gestión sobre los sistemas sin necesidad de estar físicamente en la ubicación de los equipos. Cabe destacar que esta opción es limitada, ya que de existir un problema donde se requiera el soporte de manera personalizada y en el sitio, la VPN no puede hacer mucho para ayudar a solucionarlo.

El uso de la telefonía es un factor muy importante y básico en las comunicaciones, pero al tratarse de VoIP[44], implica disponer de seguridad y sobre todo calidad de servicio (QoS). La facilidad de marcar a una extensión directa a

[43] Un *teleworker* es aquella persona que utiliza la telemática para la realización de su profesión. Esta actividad se realiza fuera del establecimiento empresarial.[1]
[44] Voz sobre IP

través de la red de datos, lo hace más atractivo para quienes buscan agilidad fuera de los predios de los edificios de la empresa.

Posibles *teleworkers*, pueden ser usuarios autorizados a utilizar el acceso a ciertos recursos informáticos, desde cualquier dispositivo que soporte enlaces VPN en cualquiera de sus posibles tecnologías; esto con el objetivo de resolver problemas de tiempo y recursos de espacio y movilidad.

3.1.1 CENTROS AUTORIZADOS DE RECAUDACIÓN - SISTEMA DE COMERCIALIZACIÓN SIDECOM

Los CARs, son locales que realizan de manera particular recaudación de la tarifa de consumo eléctrico, y que cobran una tasa por cada factura recaudada. Al finalizar el periodo de recaudación, el CAR tiene que llevar los talonarios de las facturas recaudadas hacia la agencia encargada de dicho CAR; por lo general la agencia encargada, es la más cercana al CAR.

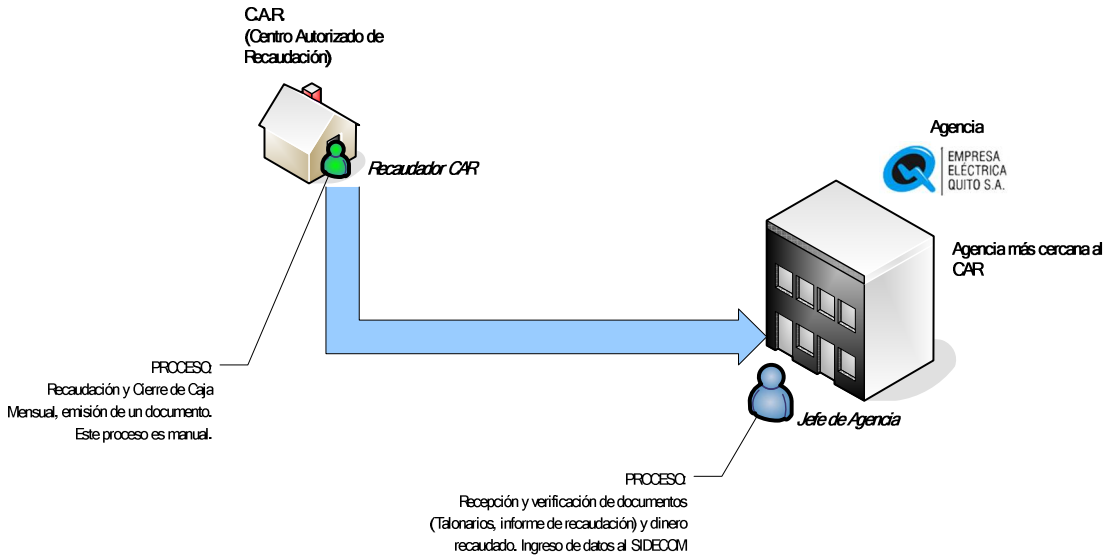


Figura 3.1 Diagrama del proceso de recaudación del CAR en modo manual

El proceso es totalmente manual, es decir, la entrega de los talonarios y el dinero recaudado se lo hace con los registros que son entregados. Como parte del proceso de recaudación y lógicamente por cuestiones de seguridad, los jefes de agencia deben realizar la verificación que el dinero recaudado corresponda a las

facturas registradas. Esto supone dos situaciones: Primero, que el dueño del CAR, realiza un proceso manual para la recaudación, esto es, desde la apertura de la caja hasta su respectivo cierre; y, segundo, que el jefe de la agencia de la E.E.Q.S.A., realiza el mismo trabajo, lo cual implica una pérdida de tiempo para los sujetos implicados (*Ver figura 3.1*).

Por resolución administrativa, los CARs deben realizar la recaudación en línea, ya que se evita este engorroso proceso, y también para mejorar la imagen de la E.E.Q.S.A. agilitando el servicio.

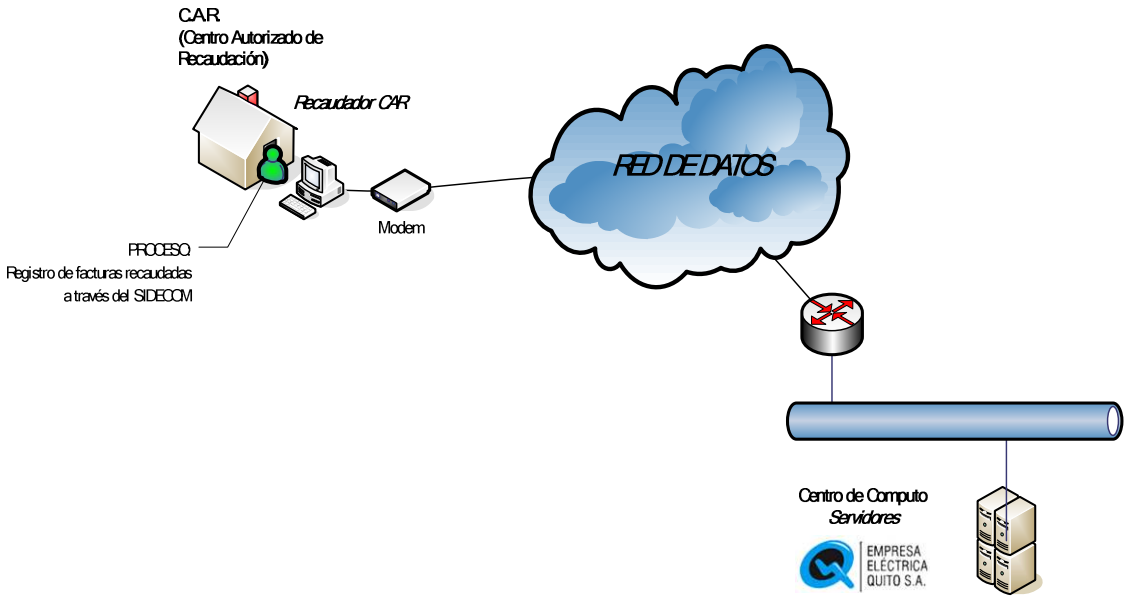


Figura 3.2 Diagrama del proceso de recaudación del CAR en línea

Hay que mencionar que muchos de los bancos locales y otras instituciones, realizan este proceso de recaudación, aunque para la mayoría de clientes el proceso tenga la apariencia de un sistema automatizado; solo el banco de Guayaquil y Servipagos por el momento tienen la posibilidad de realizar recaudación en línea, ya que cuentan con enlaces dedicados con la E.E.Q.S.A. La *figura 3.2* muestra el diagrama de topología de red para el proceso de recaudación en línea.

Se revisaron varias alternativas para realizar la recaudación en línea en los distintos CARs, y se llegó a varias conclusiones. Entre las más importantes que los CARs con mayor afluencia de usuarios (comparable con una agencia de la E.E.Q.S.A.) deberían ingresar al SIDECOM a través de enlaces dedicados y privados.

Los CARs medianos, tendrían que hacer este proceso a través de medios más económicos y asequibles. Para los medianos y algunos pequeños CARs, la solución es a través de una red pública de gran alcance como es la Red de Telefonía Pública Conmutada (PSTN). Sin embargo no es la única solución, ya que las empresas de telefonía celular han crecido de tal manera, que en ciertos sectores pueden dar servicio de datos, lo cual es una alternativa válida.

Cualquiera que sea la solución, el ingreso hacia la red corporativa de la E.E.Q.S.A. debe hacerse a través de un enlace o enlaces seguros, que no comprometan la integridad de la información que maneja la E.E.Q.S.A. (Ver *figura 3.3*).

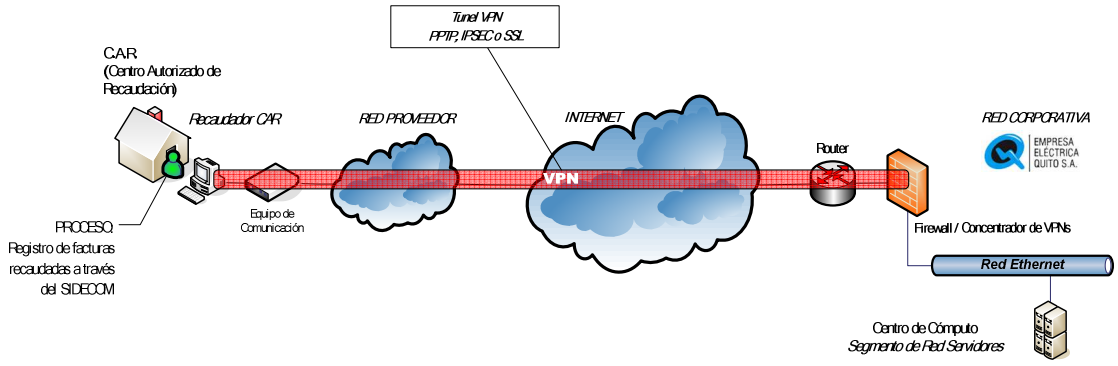


Figura 3.3 VPN formada para el acceso del CAR a la red de la E.E.Q.S.A.

La aplicación del SIDECOM es la herramienta que deberán utilizar los CARs. Las dos formas posibles de acceso a este sistema, tiene costos informáticos diferentes, y que se los analizará a continuación.

3.1.1.1 Análisis de requerimientos de *software* y ancho de banda para el caso de acceso al SIDECOM vía TELNET

Si se utiliza, el acceso a través de Telnet, el equipo final debe contemplar una aplicación que le permita establecer la comunicación a través del puerto 23, lo cual no es muy complicado ya que los actuales sistemas operativos tienen accesorios para acceder a este puerto de comunicaciones. Sin embargo la E.E.Q.S.A. de manera oficial utiliza la aplicación CHAMALEON, que dispone de mejores herramientas para acceso al SIDECOM.

En cada sesión de Telnet se tiene un consumo de recurso de red, el cual no es muy significativo en ambientes LAN, pero para un enlace VPN puede llegar a ser significativo; y cuando sobre éste se realice transacciones, el uso del ancho de banda, disponible será considerable.

Hay que añadir a esto, que al integrar varios CARs, la cantidad de accesos concurrentes por el canal de acceso de Internet de la E.E.Q.S.A., será considerable.

Se ha considerado, según información provista por el personal que administra el SIDECOM y del Departamento de Recaudación, que alrededor de 30 CARs, accederán a esta aplicación. En el peor de los casos se supondrá que los 30 CARs accederán a través de Telnet, lo que implica el establecimiento de al menos 30 sesiones de VPN al mismo tiempo.

De hecho no todas estarán al mismo tiempo realizando recaudación, pero se asumirá que por un lapso de 5 minutos todas realizarán procesos concernientes a transacciones de recaudación.

El tráfico más grande generado a través de Telnet es aproximadamente de 20 kbps; para una conexión *dial-up* de 56 kbps, cumpliría el requerimiento con holgura, pero se debe tomar en cuenta que la capacidad real de establecimiento de la conexión es menor a los 56 kbps; por varios agentes externos propios de este tipo de comunicación, se puede estimar que la capacidad del canal de

comunicaciones estaría en promedio alrededor de los 40 kbps. De todas formas habría un margen de 20 kbps destinados al incremento por causa del encapsulamiento de los datos, y que éstos puedan ser enviados a través de la VPN.

Para iniciar este proyecto de acceso a la red corporativa de la E.E.Q.S.A. se ha decidido comenzar con 5 CARs de afluencia considerable de usuarios.

3.1.1.2 Análisis de requerimientos de software y ancho de banda para el caso de acceso al SIDECOM vía CITRIX

En el caso de utilizar CITRIX para acceder al aplicativo SIDECOM Windows, se debe tomar en cuenta dos aspectos. El primero, es que se necesita de un cliente con licencia de uso del cliente CITRIX, y la segunda, que es recomendable si se lo ejecuta sobre una PC que tenga una calidad de color de al menos de 16 bits.

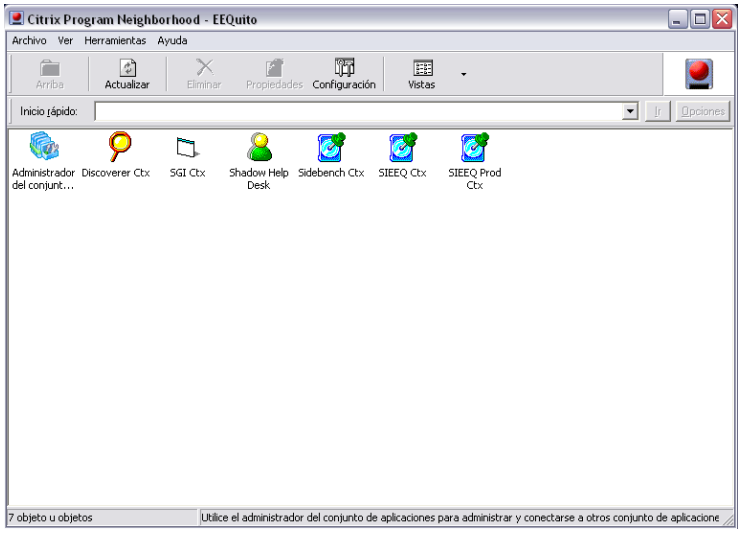


Figura 3.4 Perfil de usuario para acceso a aplicaciones por medio del Sistema CITRIX

Para tener acceso por medio de CITRIX al sistema de comercialización, es necesario que en *Active Directory* se cree una cuenta de usuario; esta cuenta de usuario según el requerimiento del puesto de trabajo, tendrá acceso a una o varias aplicaciones que se ejecutan a través del CITRIX, a esto se le denomina el perfil de usuario CITRIX para la E.E.Q.S.A. En la *figura 3.4* se observa un perfil de usuario que corresponde a un administrador del sistema informático. Visualmente

en la *figura 3.4* se muestra la ventana de perfil de usuario donde en el área de íconos de la venta se tienen accesos a varias aplicaciones entre ellas el SIDECOM, el ícono para acceder a esta aplicación es el que tiene la etiqueta SIEEQ Ctx.

Al ejecutar el SIDECOM la aplicación tiene la apariencia que se puede ver en la *figura 3.5*. Como se observa el nombre de SIDECOM ha sido reemplazado por SIEEQ Comercial, éste es el nombre que se ha adoptado para la versión en modo gráfico, al contrario de la versión anterior que es en modo texto, con la única intención de diferenciarlos.

Figura 3.5 Pantalla de inicio del SIDECOM a través de CITRIX

El cliente que se ejecuta es compatible con distribuciones *Microsoft* (*Windows 98, Windows Me, Windows 2000 y Windows XP*).

El consumo de ancho de banda por cada transacción[45] es de 26 Kbps. Si se supone que el acceso será por medio de *dial-up* no habría inconvenientes, siempre y cuando el establecimiento de la comunicación por *dial-up* alcance una capacidad de al menos 40 kbps.

[45] En un ambiente virtual como CITRIX una transacción significa enviar información a través de un evento generado por un dispositivo de entrada y salida como el teclado, lector de barras, ratón, etc.

3.1.2 ADMINISTRADORES DE SISTEMAS INFORMÁTICOS - VARIOS PROTOCOLOS DE RED Y APLICACIONES DE GESTIÓN INFORMÁTICA

La administración de los recursos informáticos, es vital en cualquier empresa. Por esta razón aquellas personas que realicen gestión deben ingresar de manera segura a los sistemas informáticos correspondientes.

Lo adecuado y procedente sería hacerlo personalmente, pero de hecho existen varias circunstancias por las cuales es muy difícil realizarlo; por esta razón las VPNs ayudan de manera significativa, a este propósito.

Protocolos de red como SNMP, HTTP, SSH, etc, permiten realizar gestión, ingresando a los equipos que necesitan ser administrados. La mejor forma será hacerlo con medios de comunicación seguros y confiables; hacerlo como si se estuviera en la oficina o en el centro de cómputo, es el objetivo cada vez más, de quienes están al frente de estos sistemas.

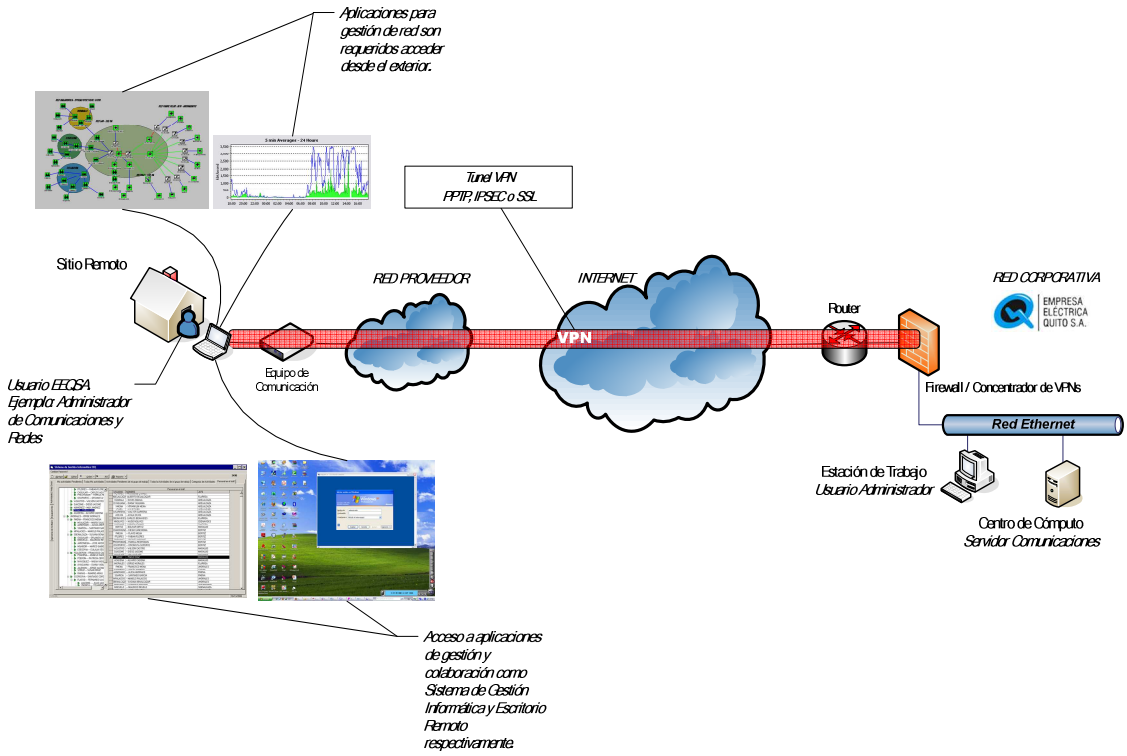


Figura 3.6 Conjunto de aplicaciones que se pueden ejecutar a través de la VPN

En la actualidad a más de existir este tipo de protocolos de administración, sistemas operativos como los distribuidos por Microsoft tienen herramientas que permiten acceder a través de escritorios remotos a los servidores o computadores que tienen información referente a la gestión informática respectiva.

En el caso de los administradores de los sistemas de comunicaciones y redes de información, es importante poder ingresar a la configuración de los equipos de conectividad y a un registro actualizado y en tiempo real del tráfico de datos que se generan por las diferentes interfaces de estos equipos.

Las diferentes aplicaciones que pueda manejar un administrador de red necesitan una velocidad aceptable y de calidad, lo que permitiría una gestión confiable; la *figura 3.6* muestra un conjunto de aplicaciones que debería acceder un técnico que administre la red de la E.E.Q.S.A. y que lo podría hacer a través de un enlace VPN.

De manera general, estar dentro de la red corporativa de la empresa, a través de un host desde el exterior de la empresa, permite ejecutar aplicaciones como si se estuviera dentro de la red LAN, aunque se debe aclarar que por cuestiones de acceso y capacidad de ancho de banda, será siempre limitado ejecutar estas aplicaciones. Es decir, si se ejecuta el escritorio remoto sobre una VPN, entre un host que accede por medio de *dial-up* y uno que está dentro de la red corporativa, los tiempos de respuesta serán muy altos en este último. Aunque se logre ejecutar, será molestoso manejar dicha aplicación con tanta lentitud. A diferencia de aplicaciones que utilizan protocolos como SNMP, HTTP, SSH y TELNET los tiempos de respuesta son mejores y es más ágil su manejo.

3.1.3 REQUERIMIENTOS Y CONSIDERACIONES PARA IMPLEMENTAR VPNs ENTRE LA E.E.Q.S.A. Y EMPRESAS DE INTERCAMBIO INTERINSTITUCIONAL Y COMERCIAL

Como se ha señalado en el Capítulo 2, tanto Andinatel como Servipagos tienen acceso a la red de la E.E.Q.S.A. y específicamente acceso a los servicios del

sistema CRM para realizar atención de llamadas de desborde para el *Call Center* y SIDECOM para poder ejecutar el proceso de Recaudación, respectivamente; el tráfico generado al utilizar estas aplicaciones no representa de un alto consumo comparado con el tráfico que se produce en una agencia de tipo urbana como la Agencia El Inca. Hay que tomar en cuenta que estas empresas tienen enlaces dedicados con capacidad superior al de un *dial-up*, como por ejemplo un E1 o ADSL de banda ancha.

La capacidad del canal de comunicaciones que tienen estas empresas para acceder a la E.E.Q.S.A. se lo puede explotar de mejor manera; si se utiliza una red de acceso público, será necesario establecer un túnel virtual o VPN. En el caso de un enlace físico directo entre la E.E.Q.S.A. y cualquiera de las empresas que conforman la extranet, establecer un túnel virtual se lo considerará como opcional, sin embargo la recomendación sería agregar seguridad a los enlaces con VPNs.

En el caso de telefonía, hay que considerar que no todos los teléfonos IP tienen soporte propio para VPN, más que el de una integración básica a la red de datos y de telefonía IP, por lo que una configuración VPN *LAN - LAN* se convierte en un alternativa adecuada para su implementación; sin embargo hay que considerar que existen teléfonos IP en forma de aplicación para estaciones de trabajo, y éstos a su vez dependen de la configuración de red del sistema operativo de plataforma sobre el cual han sido instalados. De esta manera una alternativa de configuración VPN acertada seria *LAN - Host* o de *Acceso Remoto*, según las necesidades y requerimientos de las empresas que conforman la extranet como Andinadatos y Servipagos.

Del tráfico de datos de los enlaces analizados desde el exterior de la E.E.Q.S.A. en el Capítulo 2, se debe recordar que se necesitaría un mínimo de 16 kbps con G.723 de 5.3 kbps, aunque se puede mejorarlo con el códec G.729A a 8 kbps, porque se requiere una mejor calidad de voz en la conversación. Si alguna de las aplicaciones o equipos de VoIP no soporta G.723 a 5.3 kbps o G.729A a 8 kbps, en lo posible se tratará de que los códecs con los que viene integrado el equipo

no generen consumos de ancho de banda superiores a 20 kbps, ya que se no los consideraría aptos para realizar una adecuada comunicación de voz sobre una conexión *dial-up*, misma que se la tomaría como una condición extremo de comunicación. El códec debe tener una calidad de voz que permita una conversación clara y sin retardos considerables.

Los equipos que servirán como extremo de la conexión VPN de la extranet, deberán ser compatibles o soportar tecnologías VPN como IPSec, PPTP o SSL; ya que por ser tecnologías con amplio avance y estandarizadas, ofrecen un mínimo de compatibilidad entre marcas diferentes de fabricantes; no obstante hay que tomar en cuenta que podrían carecer de garantías en ciertas instancias de la comunicación, algo no deseable pero probable al momento de implementar un enlace no sólo VPN sino en general de comunicaciones.

3.1.4 POSIBLES *TELEWORKERS* Y OTROS USUARIOS CON ACCESO A APLICACIONES RESTRINGIDAS DE LA RED CORPORATIVA DE LA E.E.Q.S.A.

El concepto de *teleworkers* se ha difundido de manera amplia en los países desarrollados y en la actualidad ha llegado a ser muy común, obteniendo buenos resultados en muchas de las empresas que lo han adoptado.

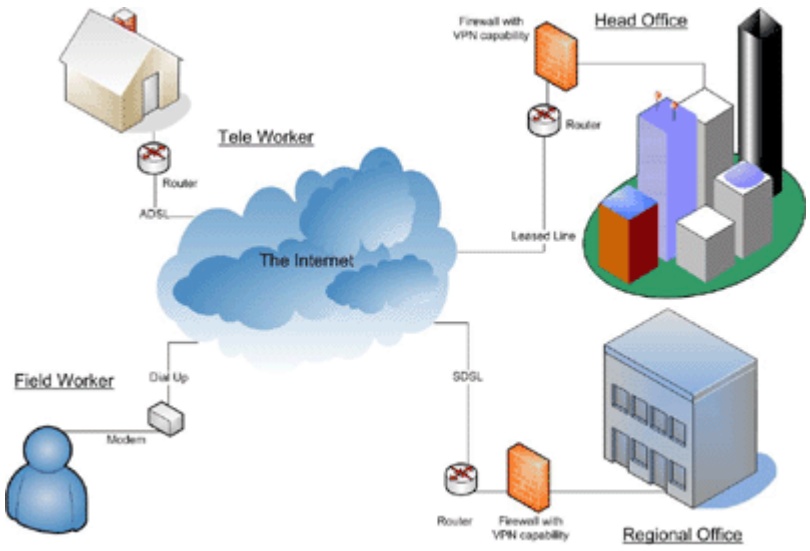


Figura 3.7 Esquema general de los usuarios que se encuentran fuera y están conectados por medio de VPN a las oficinas centrales [15]

Para países como Ecuador, este concepto es relativamente nuevo. Se les denominará *teleworkers* a aquellos usuarios móviles, que requieren acceso a aplicaciones específicas de la red corporativa de la E.E.Q.S.A., como aquellos usuarios que realizan actividades de revisiones, inspecciones, etc., dentro del área de concesión de la E.E.Q.S.A. pero fuera de los predios de la misma. Como se grafica en la *figura 3.7*, un *teleworker* accede a la oficina central desde el hogar por medio de VPN utilizando un servicio ADSL para conectarse al Internet y otro *teleworker* móvil (*Field Worker* en la *figura 3.7*) utiliza un MODEM celular para acceder al Internet y posteriormente establecer un túnel VPN para ingresar al sistema informático de la empresa

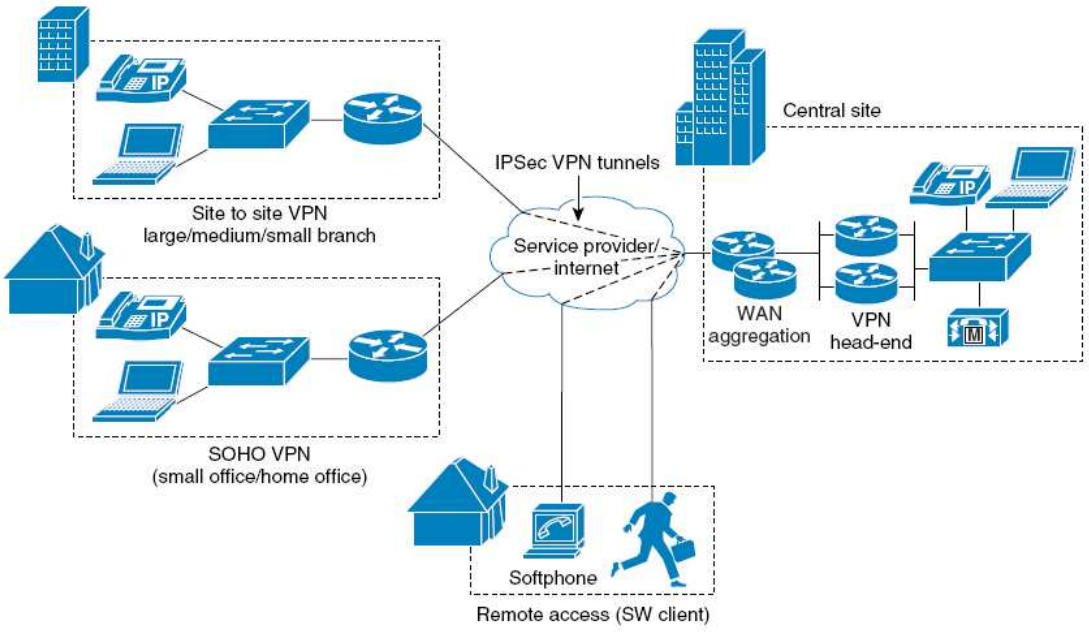


Figura 3.8 Componentes de varias VPN IPSec que incluye elementos para la comunicación de VoIP seguro [16]

Los usuarios que a diario tiene la E.E.Q.S.A. en labores de inspección, monitoreo, y todas aquellas actividades que impliquen movilización, hace que se piense en soluciones para agilizar el trabajo, mejorar las condiciones de labor diaria, reducir el consumo de materiales de oficina, etc.

El otro grupo de usuarios, en los que destacan principalmente ejecutivos y funcionarios de la empresa, tienen requerimientos de acceso a sus equipos

personales, aplicaciones de red, telefonía y posiblemente video conferencia. En la *figura 3.8* se muestra un escenario donde los elementos de VoIP son parte del diseño para formar VPNs. Los equipos de telefonía IP no solo pueden ser equipos destinados para ese propósito sino también teléfonos IP tipo software o *softphones* como lo indica la *figura 3.8* en la parte correspondiente a Acceso Remoto.

Para todos ellos la posibilidad de ingresar a la red corporativa es de suma importancia. Como un plan de visión futura hacia los nuevos requerimientos de usuarios se ha tomado en cuenta a este sector que sería de gran crecimiento para los próximos años.

3.2 ESTUDIO DE REQUERIMIENTOS ADECUADOS PARA IMPLEMENTAR VoIP SOBRE VPN

Para implementar VoIP sobre la VPN, se debe tomar en cuenta los siguientes factores:

- *Ancho de banda necesario y disponible*
- *Equipos donde nace y termina la telefonía convencional e IP*

3.2.1 ANCHO DE BANDA NECESARIO Y DISPONIBLE

El ancho de banda que se va a requerir para establecer una comunicación de voz sobre IP, utilizando el códec G.729 (códec que será tomado como referencia para realizar las posteriores estimaciones de ancho de banda necesario) es de 24 kbps hasta la capa 3 del modelo OSI, tomando en cuenta que el *payload* de G.729 es de 20 bytes; los 20 bytes son encapsulados por los bits de los protocolos RTP, UDP e IP que en conjunto forman el encabezado de los datos de voz (Ver *figura 3.9*).

Para las tecnologías de comunicaciones que se disponen en la actualidad, incluyendo desde los que tienen baja capacidad de transmisión como *dial-up* con

módems V.90 y V.92, los 24 kbps son posibles transmitirlos sin mayor dificultad. Pero como se ha mencionado a lo largo de este documento, se debe sumar los bits que se agrega a la cabecera del PDU correspondiente, es decir al paquete, para poder realizar el encapsulado de VPN.

En la *figura 3.9* se muestra el proceso de encapsulado tomando como tecnología para formar una VPN a IPSec. Los motivos por el cual se realizan los cálculos de ancho de banda con IPSec son:

- Dentro del proceso de encapsulamiento de IPSec los bits de cabecera y cola del paquete IP original, contienen especificaciones que ofrecen seguridad basada en encripción robusta en relación a tecnologías como PPTP o L2TP, que también son muy utilizadas para formar VPNs.

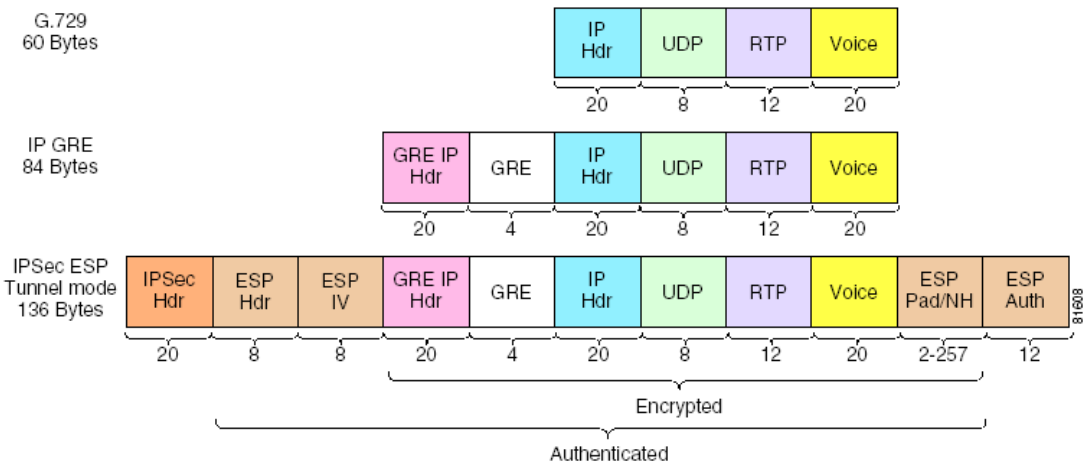


Figura 3.9 Formación del encapsulado IPSec ESP modo Túnel [16]

- Al agregar control de seguridad, entre otros parámetros, implica que el PDU final tiene un tamaño considerable tomando en cuenta el tamaño del paquete IP original, lo que permite referenciar una capacidad del canal para otras tecnologías de VPNs que agregan similar o menor cantidad de *overhead* en los PDUs.

- IPSec es una tecnología que está diseñada exclusivamente para redes TCP/IP, y la red de la E.E.Q.S.A. en conjunto con otras redes externas están ampliamente utilizadas por aplicaciones basadas en TCP/IP.

- Sobre IPSec se han desarrollado varios escenarios de VoIP, los cuales han sido tomados como referencia para desarrollar esta sección.

Como se puede observar en la *figura 3.9*, el paquete IP original que tiene información de tipo voz codificado con G.729, consta de 60 bytes para su ingreso a un túnel VPN IPSec.

Al utilizar IPSec como tecnología para formar las VPNs, se tendrían paquetes de 136 bytes listos para ser encapsulados por una trama. El proceso para deducir estos 136 bytes es: primero determinar el tamaño del *payload* G.729, que por medio del período de muestreo de 10 ms que genera 80 bits, pero como el tamaño del PDU del códec se forma con 2 periodos del muestreo, se tiene un PDU de 160 bits o 20 bytes que son encapsulados por RTP, UDP, IP e IPSec que dan un tamaño de 136 bytes.

El campo ESP Pad/NH está compuesto de 2 bytes y un relleno de 4 bytes, esto debido a que la suma del paquete IP GRE es de 84 bytes y para cifrarlo con DES es necesario tener bloques de 8 bytes tal como se lo define al algoritmo de cifrado DES; el último bloque del paquete en mención tendría 4 bytes, por esa razón y al ser un valor fijo se tomará en cuenta y solo para este caso los 4 bytes de relleno. Los otros campos tienen una longitud definida. El caso mostrado en la *figura 3.9* corresponde a la configuración IPSec ESP modo Túnel.

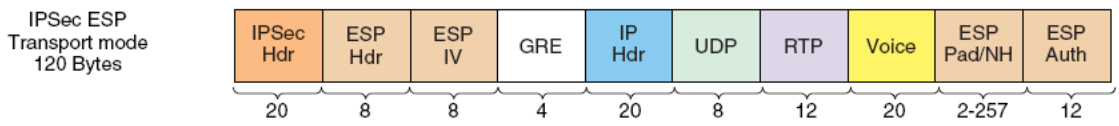


Figura 3.10 Formación del encapsulado IPSec ESP modo Transporte [16]

Al ser el muestreo de 20 ms, 50 PDUs se generan cada segundo para ser encapsulados lo que da un total 136 x 50 = 6800 bytes cada segundo o 54400 bps

(54.4 kbps). En la *figura 3.10* se muestra el encapsulado con IPSec en el modo Transporte, donde se puede apreciar que el campo GRE IP no forma parte de este nuevo PDU que tiene un tamaño de 120 bytes, lo cual ocasiona una reducción en el consumo de la capacidad del canal. También hay que mencionar que cambia el tamaño del campo ESP Pad/NH ya que el tamaño que hay que encriptar es de 64 bytes, lo que permite tener bloques de 8 bytes exactos, de esta manera no se realizan rellenos. Este modo es utilizado principalmente en comunicaciones extremo a extremo entre dos *hosts*.

El análisis del estado actual de los enlaces hacia el exterior de la red de la E.E.Q.S.A. realizado en el Capítulo 2, va a permitir establecer las condiciones iniciales con las que se puede empezar a implementar un túnel VPN.

El propósito es proveer un ahorro del consumo de ancho de banda pero al mismo tiempo, no bajar de manera significativa la calidad de la voz. Es por eso que se ha tomado como referencia el códec G.729, el cual permite estimar un ancho de banda que sería necesario contar para poder implementar enlaces VPNs.

3.2.2 EQUIPOS QUE CONFORMAN LA INFRAESTRUCTURA DE TELEFONÍA CONVENCIONAL E IP

Figura 3.11 Esquema de integración de telefonía IP y analógica [17]

La infraestructura de telefonía de la E.E.Q.S.A. está compuesta básicamente por el sistema analógico convencional o TDM y un sistema IP, y a su vez estos dos sistemas se encuentran integrados en un solo sistema que también tiene salida a la PSTN y operadoras de telefonía celular locales, en un esquema similar al de la *figura 3.11*; de tal manera que un teléfono IP o analógico puede iniciar y mantener una llamada hacia una extensión IP o convencional, atravesando por las redes IP y TDM.

Los equipos disponibles dentro de la empresa son: teléfonos convencionales e IP, *gateways* para telefonía IP, PBX o central analógica, central IP (H.323), *software* emulador de teléfono IP (*softphone*). El sistema de telefonía IP de la E.E.Q.S.A. está basado en una arquitectura H.323 lo que implica elementos para distribuir el servicio de voz a los diferentes terminales que maneja este estándar (Ver *figura 3.12*), sin embargo la E.E.Q.S.A. no cuenta con un completo sistema H.323, más que el necesario para cubrir las necesidades de comunicación interna y externa de voz.

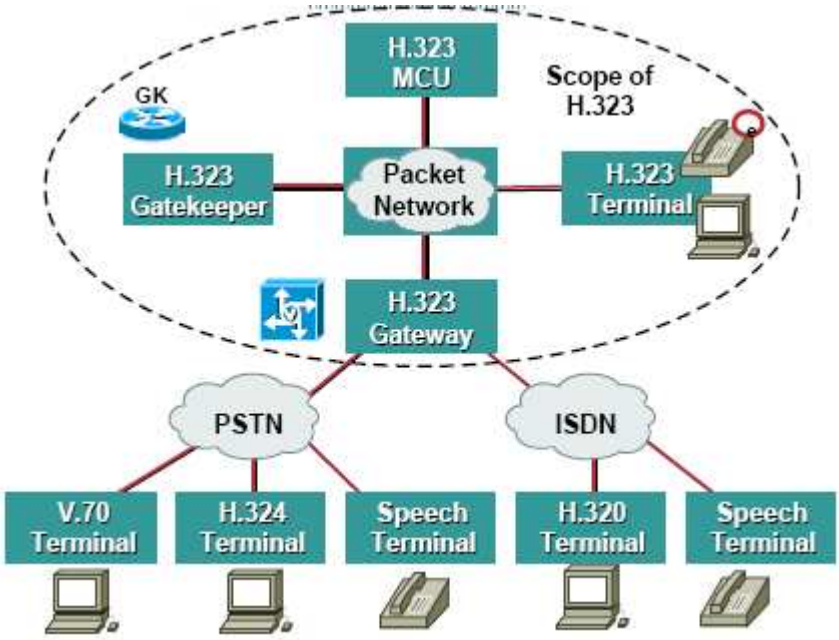


Figura 3.12 Componentes de un sistema de telefonía IP H.323 [18]

Para la implementación de enlaces VPN los equipos terminales de telefonía con los que cuenta la E.E.Q.S.A. no poseen la capacidad de establecer por si solos una conexión VPN, por lo que dependerán de equipos de comunicación capaces de establecer enlaces VPN para levantar o recibir llamadas a través de redes externas como el Internet; a partir de esta consideración la topología VPN adecuada para la aplicación de VoIP sería *Acceso Remoto* o *LAN - LAN*. En las dos topologías uno de los extremos es una *LAN* que para el caso de la E.E.Q.S.A. sería una segmento de su red corporativa y el otro extremo sería una LAN o un solo *host,* que bien podría ser un computador o teléfono IP que soporte tecnologías VPN como IPSec, PPTP, L2TP o SSL. Un esquema similar al comentado anteriormente para comunicación de voz sobre VPN, lo ilustra la *figura 3.12*, donde se tienen dos Accesos Remotos de Banda Ancha, éstos se conectan al Internet y acceden al proveedor de servicio de telefonía. El proveedor de telefonía sería la E.E.Q.S.A. En la *figura 3.13*, se muestra también, que es un sistema con plataforma de telefonía IP SIP. El esquema de la E.E.Q.S.A. es similar con la diferencia que en lugar de un servicio de telefonía IP SIP es con H.323.

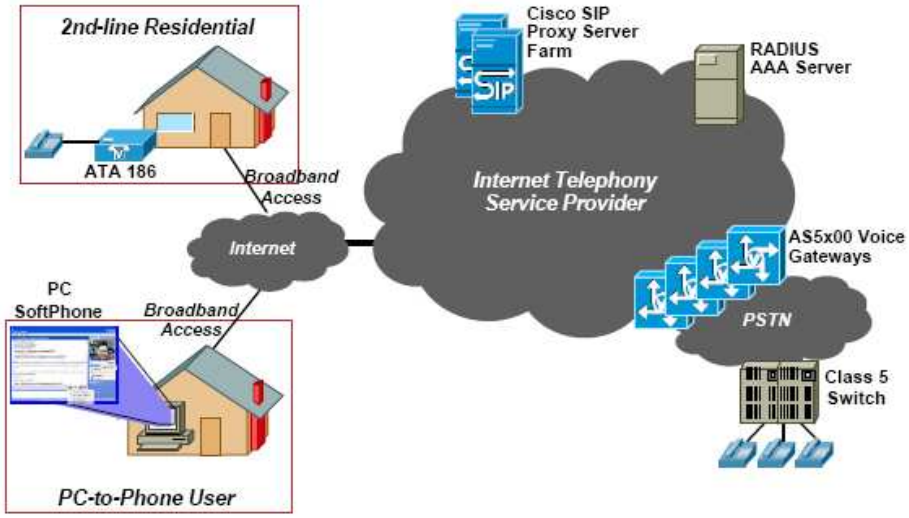


Figura 3.13 Arquitectura del servicio SIP entregado a un escenario con usuarios remotos [19]

Uno de los retos de las empresas es que los empleados puedan estar conectados la mayoría del tiempo con la empresa, incluso si se encuentran fuera de los

edificios y que mejor si es con aplicaciones de voz que permitan interactuar en tiempo real con el personal.

Un sistema de telefonía IP puede ser explotado de tal manera que dispositivos móviles que soporten navegación Internet y enlaces VPN, puedan ser parte de la infraestructura de comunicaciones telefónicas de la E.E.Q.S.A. La *figura 3.14* permite visualizar un esquema de telefonía con dispositivos móviles.

Figura 3.14 Equipos finales que manejan voz y convergen en una infraestructura IP [19]

3.3 ANÁLISIS DE OPCIONES TECNOLÓGICAS MÁS ADECUADAS PARA IMPLEMENTAR VPNs PARA LA E.E.Q.S.A.

Existen tecnologías para VPN que han surgido y desarrollado para ser altamente compatibles con las redes TCP/IP, así como también aquellas que no necesariamente utilizan directamente el conjunto de protocolos de TCP/IP para iniciar túneles VPN, caso concreto tecnologías de capa 2 del modelo OSI.

Para el presente proyecto se ha optado por IPSec, PPTP y SSL como las principales tecnologías para usarse y se aplicará cada una de ellas dependiendo del requerimiento de acceso.

IPSec y PPTP, son tecnologías que han sido ampliamente usadas, y que han madurado de tal manera que existe un amplio soporte para la mayoría de aplicaciones que se requiera implementar sobre VPN; pero además de ser ampliamente usadas se puede mencionar algunos de los factores por lo que implementar VPNs con IPSec o PPTP resulta beneficioso para la E.E.Q.S.A.

3.3.1 ANÁLISIS DE LA OPCIÓN VPN CON IPSEC

IPSec es una tecnología que ofrece un robusto sistema de seguridad para los datos que viajan a través del túnel; esta robustez está asociada a una configuración detallada del cliente VPN que en caso de perderse tal configuración un usuario sin el suficiente conocimiento tendría complicaciones para establecer nuevamente el enlace VPN. A más de esta observación se analizan las bondades y contrapartes de esta tecnología:

- IPSec a más de ofrecer una conectividad virtual, permite que la comunicación viaje de forma segura con un sistema de cifrado robusto como DES, 3DES o AES.

- La integridad de la información se ve protegida con protocolos como MD5 y SHA, así una modificación no detectada del contenido no es posible en el camino.

- Implementar VPNs con topología *LAN - LAN*, necesita que los extremos manejen una tecnología que soporte una gran variedad de fabricantes, para obtener una alta compatibilidad la tecnología debe estar estandarizada, IPSec cumple con estos requerimientos aunque no es la única.

- Sistemas Operativos para estaciones de trabajo como *Windows 2000 Professional*, *Windows XP Professional* y varias distribuciones Linux, soportan clientes para establecer VPN de Acceso Remoto con IPSec.

- En las referencias para desarrollar los temas relacionados con VoIP de este proyecto, se hace mucho énfasis en ejemplos de telefonía IP sobre VPN IPSec, lo cual es una ventaja, ya que se tiene una base sobre la cual sustentar los requerimientos para implementar un escenario de telefonía o VoIP sobre VPN, sobre todo en el hecho de que la tecnología ha sido probada con resultados exitosos, lo que queda es adaptar a la realidad de la red de la E.E.Q.S.A. y determinar si es adecuada o no.

3.3.2 ANÁLISIS DE LA OPCIÓN VPN CON PPTP

Esta tecnología permite conexiones rápidas y de bajo *overhead*, sin embargo esta rapidez está asociada a un bajo nivel de seguridad comparado con otras tecnologías VPN como IPSec. A continuación un resumen de las principales características de esta opción para enlaces VPN:

- PPTP es una tecnología de capa 2 del modelo OSI, y tiene como principal ventaja la simplicidad en el establecimiento de la comunicación, un amplio soporte para estaciones de trabajo principalmente sobre plataformas *Windows como 98SE*, *2000 Professional*, *XP Professional* y *Vista*.

- PPTP no agrega tanto *overhead* a los PDU de capa superiores como lo hace IPSec, lo que lo hace más adecuado para implementarlo sobre enlaces de baja capacidad, como *dial-up* o enlaces de gran capacidad como accesos a Internet de banda ancha pero que se encuentran saturados.

- PPTP ofrece una seguridad de autenticación con PAP, CHAP o MS-CHAP, siendo la autenticación opcional, sin embargo los tres protocolos que manejan la autenticación no son tan robustos como SHA. Por ejemplo PAP proporciona autenticación pero los datos son enviados en texto plano; CHAP y MS-CHAP soportan autenticación con el algoritmo MD4 (*Message*

Diggest 4), sin embargo es un algoritmo que ha presentado debilidades demostradas[46].

3.3.3 ANÁLISIS DE LA OPCIÓN VPN CON SSL

En el caso de SSL también se lo implementará, ya que tiene una ventaja particular, que el cliente por naturaleza es un navegador Web que soporte SSL, como Internet Explore 6.0 o superior y Mozilla Firefox 2.15 o superior. SSL en la actualidad tiene la capacidad de formar túneles al instalar un componente de tipo *Applet* de Java o un *Active X*, esto depende del fabricante del equipo. Esta aplicación es instalada manualmente por el cliente y se agrega una nueva conexión de tipo virtual en el sistema operativo. Esta modalidad de cliente VPN está siendo ampliamente difundida sobre todo para sistemas Microsoft como Windows XP Professional.

Una vez formado el túnel, el acceso es como si el usuario estuviera trabajado con una VPN de tipo PPTP o IPSec; hay que tomar en cuenta que se trata de una conexión VPN no tan difundida, que al momento de implementarse podría presentar algún tipo de problemas en ciertos tipos de protocolos, especialmente con los asociados a tipo multimedia (VoIP y Videoconferencia).

Para la E.E.Q.S.A. le resulta conveniente esta tecnología ya que el usuario no tiene que configurar ningún parámetro de la conexión VPN, lo que facilitaría y agilitaría las labores del usuario.

3.4 DIMENSIONAMIENTO DE LOS ENLACES VPNs PARA DATOS Y VoIP

En el dimensionamiento del canal de comunicaciones para formar los túneles VPN, se debe tomar en cuenta el tipo de aplicación que servirá para el proceso de recaudación. Hasta el momento de desarrollar esta parte del proyecto, no se ha

[46] Ciertas debilidades en MD4 fueron demostradas por Den Boer y Bosselaers en un documento publicado en 1991

definido cuál sería la aplicación más conveniente; sin embargo se ha tomado como referencia el sistema de servidores CITRIX y sus clientes, ya que a través de esta tecnología, se ha migrado en casi la totalidad el sistema de comercialización (SIDECOM).

El ambiente de aplicaciones bajo CITRIX, consiste básicamente, que desde el servidor se ejecutan todas las sesiones abiertas por los diferentes usuarios. Las aplicaciones que se ejecutan en el servidor, son las del sistema comercial, sistema de distribución integrado, GIS; en fin la proyección es que todas las aplicaciones se ejecuten bajo este esquema informático. Los clientes únicamente realizan peticiones de eventos, como los relacionados al teclado, ratón, impresora, *scanner* y otros elementos de entrada y salida de datos.

Para otras aplicaciones y otros usuarios, al establecer la VPN será como si estuviesen dentro de la red local, con los retardos propios de este medio de comunicaciones a través de redes públicas como el Internet.

3.4.1 MODALIDAD DE ACCESO VPN

La modalidad de acceso dependerá del medio de acceso a la red pública (Internet), el tipo de aplicación y del grupo de usuarios que requieran este acceso. Para este caso la modalidad será a través de Acceso Remoto, es así que los usuarios remotos externos serán los CARs y Usuarios Remotos Internos serán empleados y funcionarios de la E.E.Q.S.A., tal como se lo explicó en el Capítulo2.

El primer grupo de usuarios de tipo externo deberán acceder por medio de IPSec; de existir algún motivo por el cual no es posible por IPSec se revisará el acceso con SSL o PPTP, siguiendo ese orden, ya que IPSec soporta un robusto sistema de seguridad, lo que es crítico si los enlaces se los realiza con entidades externas a la E.E.Q.S.A. En el caso de los operadores que son empleados de la E.E.Q.S.A. ingresarán a la red de datos por medio de PPTP o IPSec. Estos operadores tienen equipos móviles que tienen acceso al Internet por medio de MODEM celulares; la velocidad de transmisión está por debajo de 64 kbps en zonas

rurales que es donde más se realizan las actividades que deben cumplir a diario estos operadores, por lo que es adecuado PPTP ya que no sobrecarga un enlace como lo haría IPSec. Sin embargo si el trabajo es en zonas urbanas donde se confirme una tasa de transferencia superior a 64 kbps se debe implementar la VPN con IPSec.

MODALIDAD - VPN DE ACCESO REMOTO

Nro.	Usuario	Tecnología de Acceso a Internet	Lugar de Acceso	Tecnología VPN	Tipo de Usuario	Aplicaciones Requeridas
1	CAR1	*Dial-Up*	Área de Concesión E.E.Q.S.A.	IPSec	Fijo	SIDECOM – Recaudación
2	CAR2	*Dial-Up*	Área de Concesión E.E.Q.S.A.	IPSec	Fijo	SIDECOM – Recaudación
3	CAR3	*Dial-Up*	Área de Concesión E.E.Q.S.A.	IPSec	Fijo	SIDECOM – Recaudación
4	CAR4	*Dial-Up*	Área de Concesión E.E.Q.S.A.	IPSec	Fijo	SIDECOM – Recaudación
5	CAR5	*Dial-Up*	Área de Concesión E.E.Q.S.A.	IPSec	Fijo	SIDECOM – Recaudación
6	Operador 1	EV-DO	Área de Concesión E.E.Q.S.A.	PPTP/IPSec	Móvil	SIDECOM – Múltiples Opciones / SDI / Web Mail / Intranet
7	Operador 2	EV-DO	Área de Concesión E.E.Q.S.A.	PPTP/IPSec	Móvil	SIDECOM – Múltiples Opciones / SDI / Web Mail / Intranet
8	Operador 3	EV-DO	Área de Concesión E.E.Q.S.A.	PPTP/IPSec	Móvil	SIDECOM – Múltiples Opciones / SDI / Web Mail / Intranet
9	Operador 4	EV-DO	Área de Concesión E.E.Q.S.A.	PPTP/IPSec	Móvil	SIDECOM – Múltiples Opciones / SDI / Web Mail / Intranet
10	Operador 5	EV-DO	Área de Concesión E.E.Q.S.A.	PPTP/IPSec	Móvil	SIDECOM – Multiples Opciones / SDI / Web Mail / Intranet
11	Administrador 1	EV-DO / ADSL / CABLE / *Dial-Up*	Cualquier lugar	PPTP/IPSec/SSL	Fijo/Móvil	Sofware de Gestión de equipos y sistemas informáticos
12	Administrador 2	EV-DO / ADSL / CABLE / *Dial-Up*	Cualquier lugar	PPTP/IPSec/SSL	Fijo/Móvil	Sofware de Gestión de equipos y sistemas informáticos
13	Administrador 3	EV-DO / ADSL / CABLE / *Dial-Up*	Cualquier lugar	PPTP/IPSec/SSL	Fijo/Móvil	Sofware de Gestión de equipos y sistemas informáticos
14	Ejecutivo 1	EV-DO / ADSL / CABLE / *Dial-Up*	Cualquier lugar	PPTP/IPSec	Fijo/Móvil	Acceso Archivos / Mail / SIDECOM /SDI/Intranet
15	Ejecutivo 2	EV-DO / ADSL / CABLE / *Dial-Up*	Cualquier lugar	PPTP/IPSec	Fijo/Móvil	Acceso Archivos / Mail / SIDECOM /SDI/Intranet

Tabla 3.1 Usuarios con requerimiento de acceso a la red de la E.E.Q.S.A. por medio de Internet

A los Administradores de los Sistemas Informáticos se les otorga la libertad de escoger una determinada tecnología para VPN, tomando en cuenta que este tipo de usuarios tiene el suficiente criterio para escoger una u otra tecnología VPN, la *tabla 3.1* resume el requerimiento de los diferentes usuarios antes mencionados.

Los datos mostrados en la *tabla 3.1* indican que al implementar la VPN se tendrá en cuenta no solo los CARs como usuarios, sino a otros usuarios que ejecutan otro tipo aplicaciones, aunque el objetivo es realizar y analizar por el momento cinco enlaces VPN simultáneos. Esta primera parte de la implementación se podrá hacer con cinco CARs o cinco de cualquier combinación que están en la *tabla 3.1*, que sería una prueba adecuada para evaluar los enlaces. En base a este requerimiento se tomará como referencia a IPSec para determinar cuánta capacidad del enlace se necesita para la transmisión de datos. En el caso de la aplicación de VoIP se ha determinado el valor del consumo de la capacidad del canal anteriormente en el presente Capítulo, añadiendo el análisis para datos se podrá tener un valor de la capacidad que permita ejecutar los dos tipos de aplicaciones.

3.4.2 DIMENSIONAMIENTO DEL CANAL DE COMUNICACIONES PARA APLICACIONES COMERCIALES Y DE ADMINISTRACIÓN

Para iniciar el dimensionamiento se revisará el comportamiento del tráfico en un computador de uso exclusivo para recaudación. El PC o computador de recaudación es un equipo de marca IBM modelo ThinkPad que tiene un procesador Intel Celeron, memoria RAM de 512 MB, puertos PS2 para teclado, *mouse*, puertos USB para el lector de código de barras, puerto paralelo par la impresora matricial y el puerto de red Ethernet 10/100 Mbps, esto como información básica de *hardware* del equipo.

El monitoreo de tráfico de este equipo de recaudación es realizado en la Agencia de Recaudación del edificio matriz Las Casas, sobre la red LAN que se conecta a los servidores del centro de cómputo del mismo edificio. El equipo está conectado a un *switch* de marca 3COM modelo *Office Connect* de 16 puertos, y este a su

vez está conectado con un *switch* Cisco Catalyst 2950 y que a su vez se encuentra conectado en el *switch* principal Cisco 3560, todos en cascada.

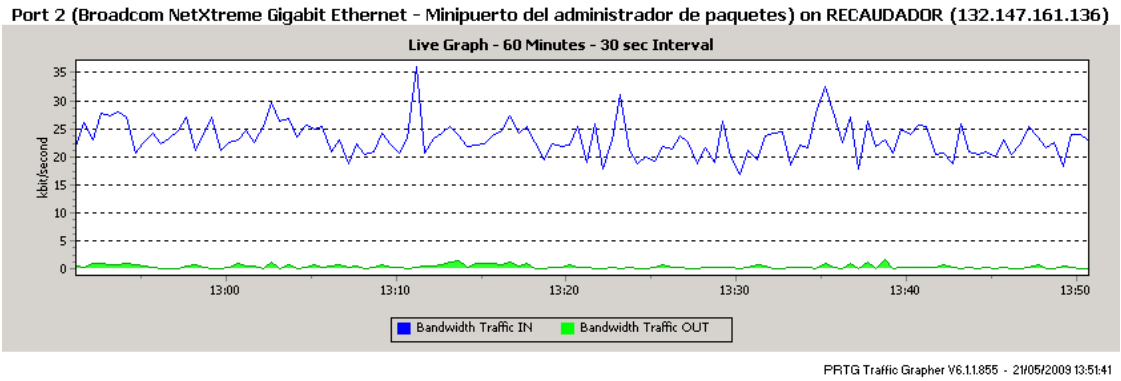


Figura 3.15 Gráfico del tráfico de red generado por el computador de recaudación

El *software* instalado es el siguiente: el sistema operativo base es *Windows XP Professional* con *Service Pack 2*, cliente *Citrix Program Neighborhood* Versión 9.230.50211. El cliente Citrix es configurado de tal manera que pueda tener acceso con un nombre de usuario del dominio EEQ1 a través del cual podrá acceder al sistema comercial SIDECOM (SIEEQ). Una vez que se ingresa al SIDECOM puede empezar a realizar el proceso de recaudación; una actividad normal de este proceso presenta el tráfico de red de las *figuras 3.15 y 3.16*.

Port 2 (Broadcom NetXtreme Gigabit Ethernet - Minipuerto del administrador de paquetes) on RECAUDADOR (132.147.161.136)

Graph: 60 Minutes | Graph: 24 Hours | Graph: 30 Days | Graph: 365 Days | Table: 24 Hours | Table: 30 Days | Table: 365 Days

	Port 2 (Broadcom NetXtreme Gigabit Ethernet - Minipuerto del administrador de paquetes) on RECAUDADOR (132.147.161.136)						
	Bandwidth Traffic IN		Bandwidth Traffic OUT		Sum		Coverage
	kbyte	kbit/second	kbyte	kbit/second	kbyte	kbit/second	%
21/05/2009 13:45 - 13:50	809.699	22.116	8.239	0.225	817.938	22.341	100
21/05/2009 13:40 - 13:45	815.199	22.266	7.257	0.198	822.456	22.465	100
21/05/2009 13:35 - 13:40	891.008	24.338	20.054	0.548	911.062	24.886	100
21/05/2009 13:30 - 13:35	810.482	22.137	8.074	0.221	818.557	22.357	100
21/05/2009 13:25 - 13:30	783.263	21.393	8.112	0.222	791.375	21.615	100
21/05/2009 13:20 - 13:25	818.886	22.366	7.006	0.191	825.892	22.558	100
21/05/2009 13:15 - 13:20	855.675	23.372	20.918	0.571	876.593	23.943	100
21/05/2009 13:10 - 13:15	884.911	24.169	21.643	0.591	906.554	24.760	100

Show Legend Auto Refresh Close

Figura 3.16 Tabulación de los datos de tráfico del computador de recaudación

El intervalo de tiempo analizado es de 60 minutos, tomado entre las 12h50 hasta las 13h50 de un día normal de actividades de la Agencia, tiempo en el cual se encuentra con un flujo de recaudación constante. Se puede observar en la *figura*

3.15 que el tráfico de salida del computador (área de color verde) se aproxima a 0 kbps, esto quiere decir que las peticiones realizadas desde el computador de recaudación hacia el servidor son mínimas frente al tráfico de entrada que prácticamente es el consumo total de la sesión CITRIX para acceder al SIDECOM; hay que tomar en cuenta que dentro de este proceso también se emite impresiones hacia la impresora de recaudación.

Con los datos mostrados se puede indicar que el ancho de banda para la aplicación SIDECOM a través del sistema Citrix, que corresponde a la segunda columna (*kbit/second*) del campo *Sum*[47] de la pestaña *Table 24 Hours* de la *figura 3.16*, es de 23.64 kbps que es el promedio del monitoreo de la última hora y que se lo puede observar en la *tabla 3.2*.

	Bandwidth Traffic IN	***Bandwidth Traffic IN***	***Bandwidth Traffic OUT***	***Bandwidth Traffic OUT***	***Sum***	***Sum***	***Coverage***
	kbyte	***kbit/second***	***kbyte***	***kbit/second***	***kbyte***	***kbit/second***	***%***
13:45 - 13:50	809.699	22.116	8.239	0.225	817.938	22.341	100
13:40 - 13:45	815.199	22.266	7.257	0.198	822.456	22.465	100
13:35 - 13:40	891.008	24.338	20.054	0.548	911.062	24.886	100
13:30 - 13:35	810.482	22.137	8.074	0.221	818.557	22.357	100
13:25 - 13:30	783.263	21.393	8.112	0.222	791.375	21.615	100
13:20 - 13:25	818.886	22.366	7.006	0.191	825.892	22.558	100
13:15 - 13:20	855.675	23.372	20.918	0.571	876.593	23.943	100
13:10 - 13:15	884.911	24.169	21.643	0.591	906.554	24.76	100
13:05 - 13:10	815.167	22.265	13.767	0.376	828.934	22.641	100
13:00 - 13:05	916.282	25.026	16.012	0.437	932.294	25.464	100
12:55 - 13:00	869.021	23.737	8.848	0.242	877.869	23.979	100
12:50 - 12:55	914.84	24.988	24.275	0.663	939.115	25.651	100
12:45 - 12:50	885.546	24.188	18.851	0.515	904.396	24.703	100
				Promedio		23.64330769	

Tabla 3.2 Datos tabulados que sirven para calcular el promedio de la actividad de tráfico

El proceso de recaudación de un computador para un CAR sería el mismo que el realizado por uno de una agencia normal, por lo tanto el ancho de banda necesario para realizar el proceso de recaudación es de 23.64 kbps, lo que en un enlace *dial-up* es posible; sin embargo a este valor de ocupación del canal de comunicaciones, hay que agregarle un porcentaje extra que corresponde al

[47] Suma del consumo de tráfico de entrada (IN) más el de salida (OUT)

encapsulamiento por parte de IPSec que es la tecnología de referencia para formar la VPN. Antes de agregar el porcentaje extra, se hace necesario conocer cuánto en realidad consume el protocolo que utiliza Citrix para establecer la comunicación de extremo a extremo.

En el lapso de la hora de la muestra del monitoreo, solo se ha realizado el proceso de recaudación lo que indica que el tráfico casi en su totalidad corresponde al proceso mencionado; sin embargo hay que notar que dentro de la red LAN de la E.E.Q.S.A. circula información hacia los equipos de la red, y es muy probable que este tipo de información altere de alguna manera la información del tráfico recopilado; por esta razón se procede a analizar la sesión Citrix entre un cliente y un servidor.

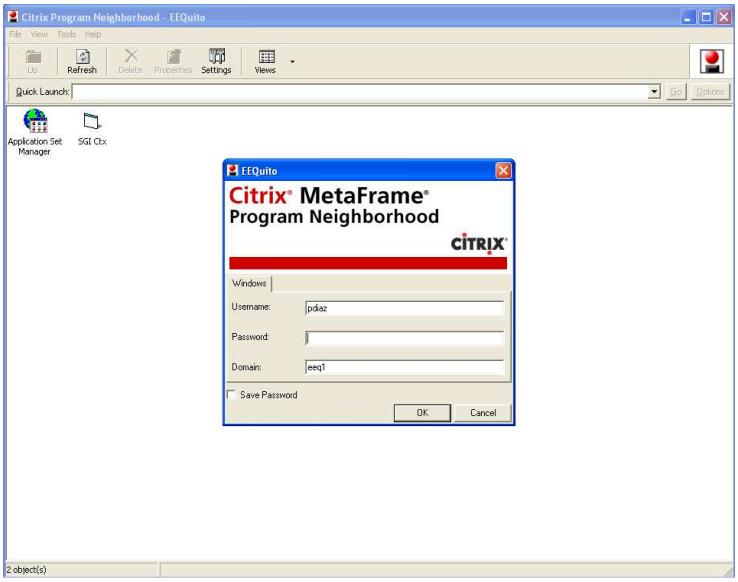


Figura 3.17 Cuadro de diálogo para el ingreso al sistema SGI a través de Citrix

3.4.2.1 Análisis del consumo de la capacidad del canal generado por el protocolo de comunicaciones ICA de Citrix

En los sistemas de virtualización Citrix, se debe indicar que no importa la aplicación que se ejecute sobre estos sistemas, el tráfico generado tiende a ser el mismo, por lo tanto ejecutar SIDECOM, SGI (Sistema de Gestión Informático), GIS, CRM, MS Office, etc., generará el mismo tráfico ya que cada aplicación, se ejecuta en los servidores Citrix y es la imagen de la actividad o mandos

ejecutados por dispositivos de entrada y salida como un ratón, teclado o impresora, que viajan a través de la red.

Para no interferir en las actividades del recaudador se ha visto la alternativa de utilizar otra aplicación que se ejecuta a través del sistema Citrix en otro equipo de usuario como lo hace SIDECOM; la aplicación seleccionada es el SGI. En el análisis del comportamiento de la aplicación SGI sobre Citrix en la red, se va a utilizar el *software Wireshark*[48] con el cual se podrá ver la información de los paquetes de una muestra tomada al ejecutar sobre un equipo que pertenece a la misma red del equipo de recaudación de la E.E.Q.S.A.

Figura 3.18 Ventana que indica que se está intentando conectar a una aplicación de los sistemas Citrix

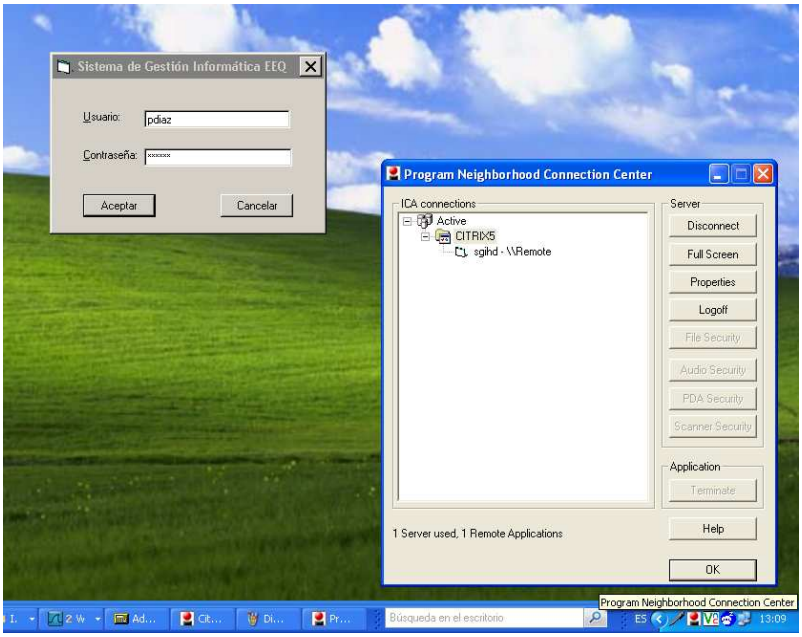


Figura 3.19 Ventana de la aplicación SGI sobre un servidor del sistema Citrix y estado de la conexión Citrix

[48] Antes conocido como *Ethereal*, es un analizador de protocolos utilizado para realizar análisis y solucionar problemas en redes de comunicaciones para desarrollo de *software* y protocolos. Cuenta con todas las características estándar de un analizador de protocolos

El usuario ejecuta el cliente de conexión *Citrix Program Neighborhood* y esto hace que se ejecute una ventana donde el icono de la aplicación del sistema SGI está habilitado para ejecutarlo.

Al ejecutar este vínculo, la granja de servidores mediante un proceso automático de balanceo de carga asigna un servidor Citrix que responde a través del cliente Citrix pidiendo la información de autenticación del usuario, tal como lo muestra la *figura 3.17*; al ingresar correctamente los datos se presiona el botón *OK* el cual permitirá establecer la conexión con la aplicación que se encuentra en un servidor Citrix (Ver *figura 3.18*).

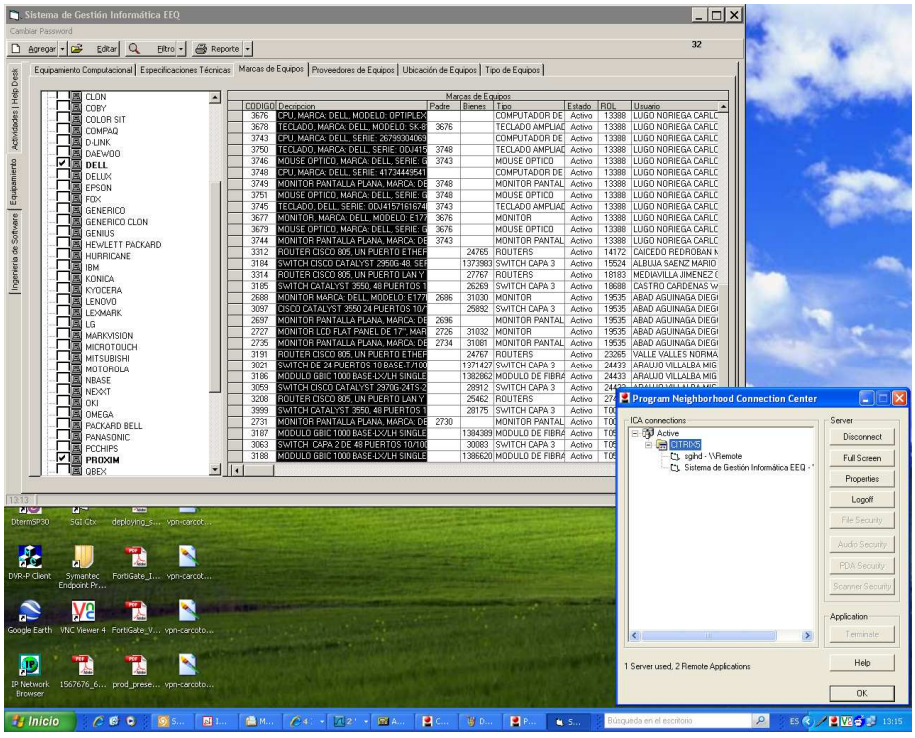


Figura 3.20 Uso de la aplicación según la necesidad del usuario

Al conectarse se inicia la aplicación requerida; en el caso del SGI se inicia con una ventana que solicita el ingreso de usuario y contraseña, a más de esta aplicación en ejecución se puede observar en la *figura 3.19* la conexión al servidor Citrix, la ventana de información indica la aplicación que se ejecuta y el nombre del servidor Citrix al que se ha conectado el cliente.

Una vez ingresado a la aplicación se procede a realizar las operaciones que el usuario necesite, mientras tanto con el analizador de protocolos *wireshark* se procede a prepararlo para atrapar la actividad de tráfico de datos sobre la red, contenida entre el cliente con dirección IP 132.147.163.55 y el servidor CITRIX5 con dirección IP 132.147.160.120 (Ver *figuras 3.19* y *3.20*).

Toda esta actividad se está registrando en el *Wireshark*, el mismo que está configurado para que registre toda la actividad de la interfaz de red Ethernet en modo promiscuo[49], tal como lo muestra la *figura 3.21*.

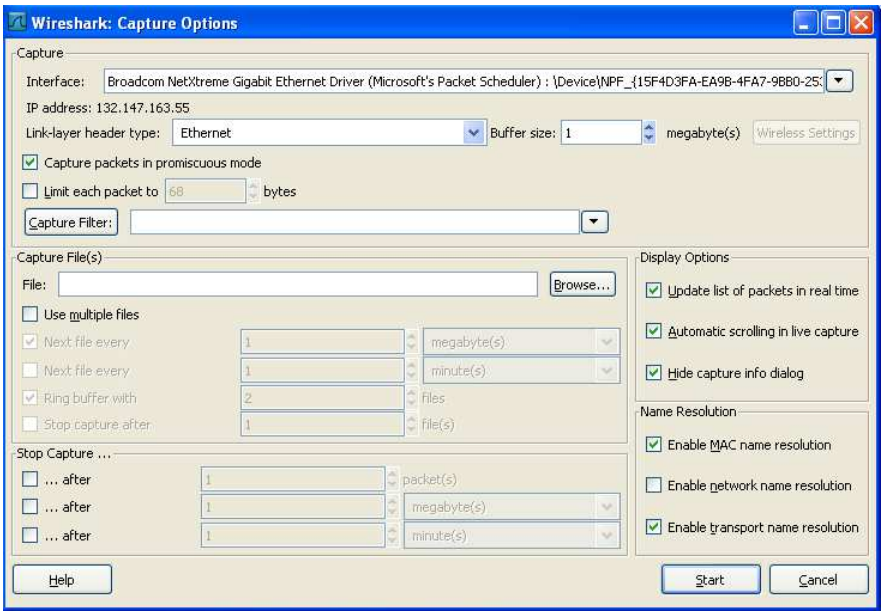


Figura 3.21 Cuadro de diálogo de la configuración de la interfaz que se requiere analizar

Mientras el usuario realiza operaciones en la aplicación SGI se da inicio a la captura de paquetes en la interfaz seleccionada.

La *figura 3.22* muestra que al realizar la captura de los paquetes algunos de estos corresponden al protocolo (ICA puerto 1494 en lado del servidor) que Citrix utiliza para realizar la comunicación. Se realiza una muestra de 335 segundos de duración aproximadamente de lo que resulta una captura de 40842 paquetes (Ver *figura 3.23*). Esta información hay que filtrarla de tal manera que se pueda

[49] **Modo Promiscuo**, es aquel en el que una computadora conectada a una red compartida, tanto la basada en cable de cobre como la basada en tecnología inalámbrica, captura todo el tráfico que circula por ella.

encontrar el par de conexión que utiliza el protocolo ICA y en la que intervienen los equipos antes mencionados.

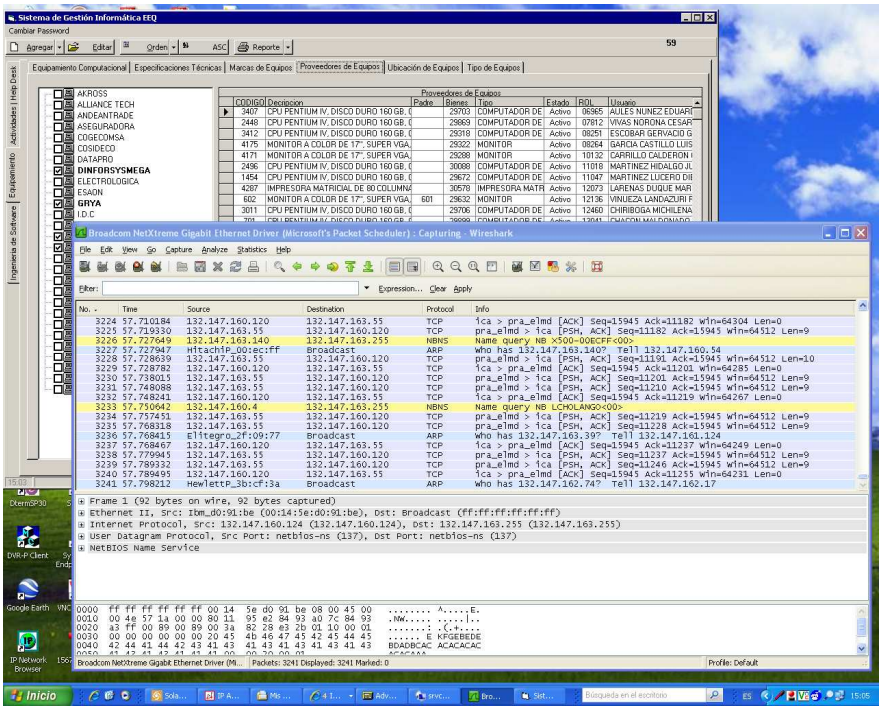


Figura 3.22 Se inicia la captura de tráfico y se ejecuta la aplicación SGI por medio de Citrix

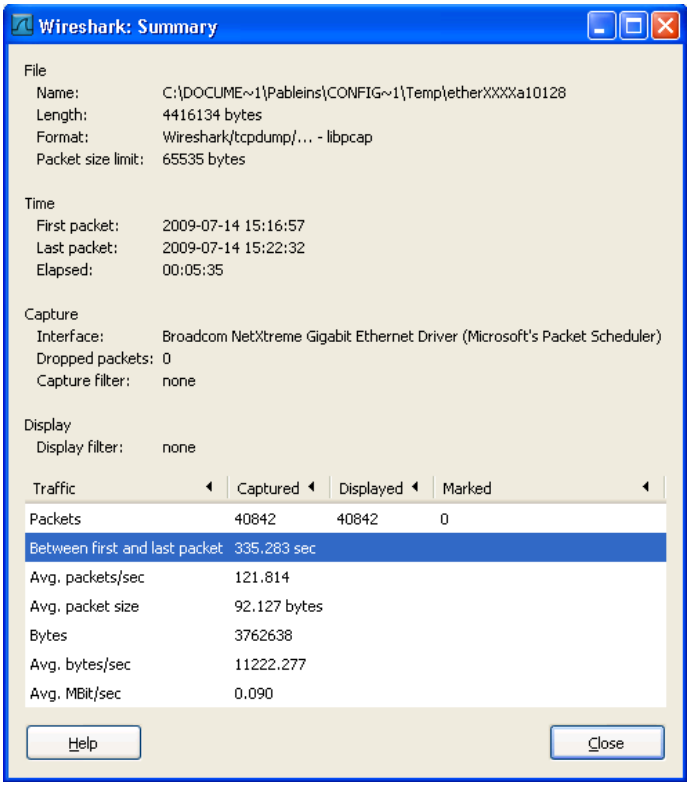


Figura 3.23 Resumen de la captura

Para encontrar el par de comunicación se debe acceder al menú *Statistics* e ingresar en la opción *Conversations (*Ver *figura 3.24)*.

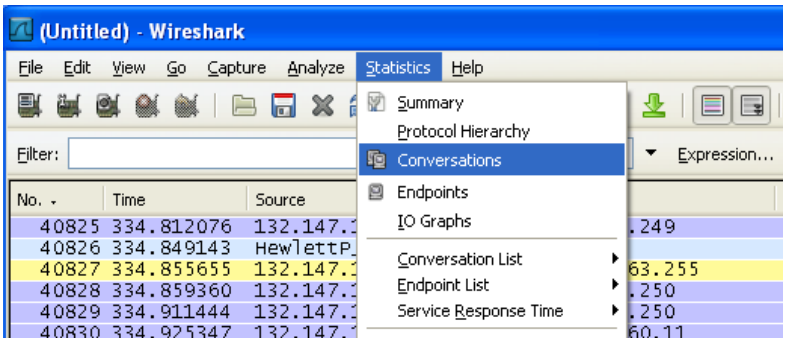


Figura 3.24 Opción Conversations del menú Statistics de Wireshark para analizar el tráfico entre pares de conexiones

Esta opción permite observar varias conversaciones y también permite escoger el nivel de la conversación que se desee analizar, para el caso de la muestra que se ha tomado, se debe escoger el nivel TCP ya que ahí se puede distinguir una conversación del protocolo ICA o que utiliza el puerto 1494 en el lado del servidor Citrix. En la *figura 3.25* se observa que se ha identificado la conversación que se necesita analizar.

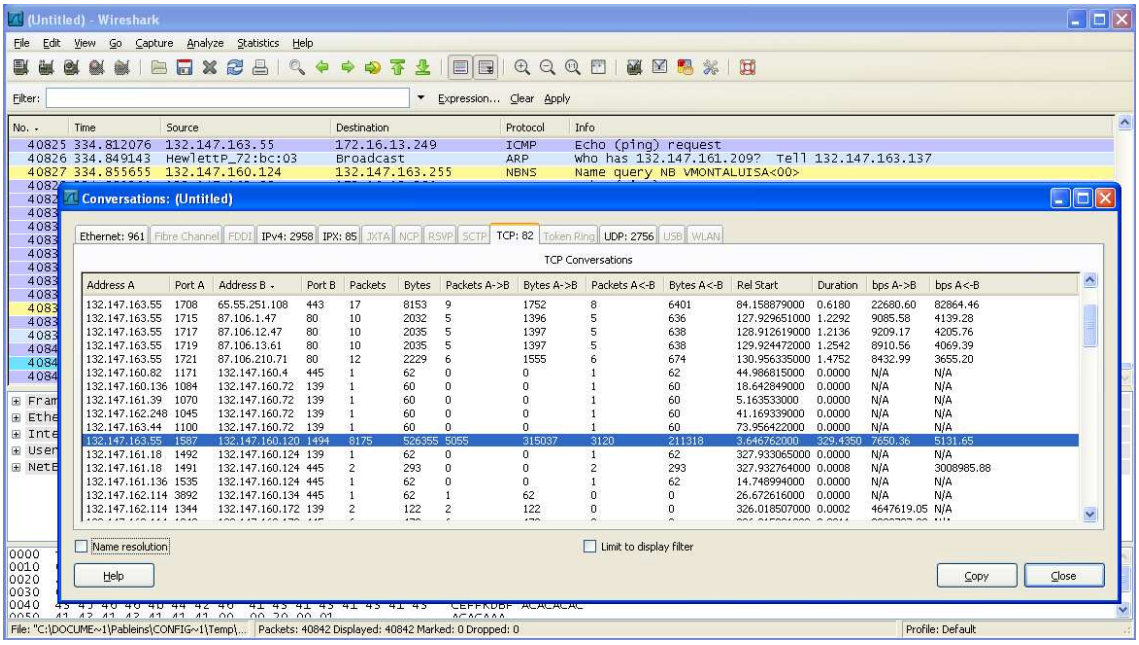


Figura 3.25 Identificación del par de conexión entre el cliente y servidor Citrix

En la *figura 3.26* se muestra que se puede habilitar la opción de resolución de nombres de protocolo, y al activarlo el valor del puerto 1494 cambia a ICA, con lo que se asegura que es la conversación que se está buscando.

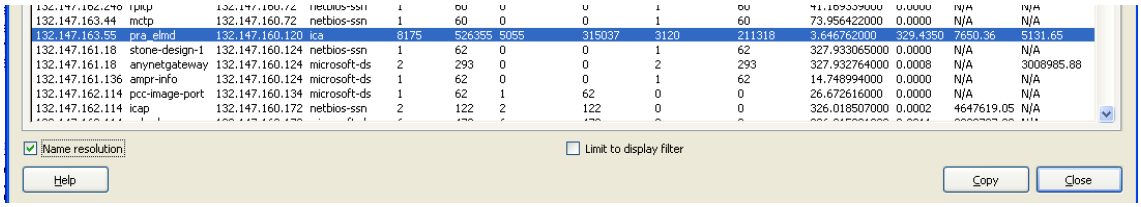


Figura 3.26 Habilitación para la resolución de nombres de puerto y se observa que el puerto 1494 corresponde al protocolo ICA

Los valores mostrados en la conversación seleccionada en la *figura 3.26* son copiados a la *tabla 3.3* en la que se realiza el análisis para determinar cuánto ocupa el protocolo ICA en un canal de comunicación y cuál sería el dimensionamiento si este protocolo se lo utiliza en un enlace VPN IPSec.

Los datos correspondientes a la conversación entre el cliente y servidor Citrix generados en el reporte de la *figura 3.26* son copiados a la *tabla 3.3* para el respectivo análisis y consideraciones del dimensionamiento requerido.

Dirección IP A	**Dirección IP B**
132.147.163.55	132.147.160.120
Puerto TCP A	**Puerto TCP B**
1587	1494
Paquetes	
8175	
Bytes	
526355	
Paquetes A → B	**Bytes A → B**
5055	315037
Paquetes A ← B	**Bytes A ← B**
3120	211310
Duración	
329.435 segundos	
bps A → B	**bps A ← B**
7560.36	5131.65

Tabla 3.3 Resumen de la conversación entre el equipo cliente y el servidor Citrix

Los valores de bits por segundo (bps) entre A y B en los dos sentidos de la comunicación, son el resultado final, es decir que la velocidad indicada en la *tabla 3.3* es la que se obtiene en las tramas Ethernet. IPSec es un protocolo de capa 3 por lo tanto este encapsula antes que Ethernet y después que IP, por lo que se necesita analizar el comportamiento hasta capa 3, en este caso sería hasta el protocolo IP. Para esto se debe conocer cuánta cantidad de bits en realidad agrega Ethernet al paquete IP. El analizador de protocolos permite mostrar a un paquete la cantidad de bits que se le agrega cuando éste llega a Ethernet, para lo cual se analiza un paquete IP que contiene el protocolo ICA y utiliza el puerto 1494 (ver *figura 3.27*).

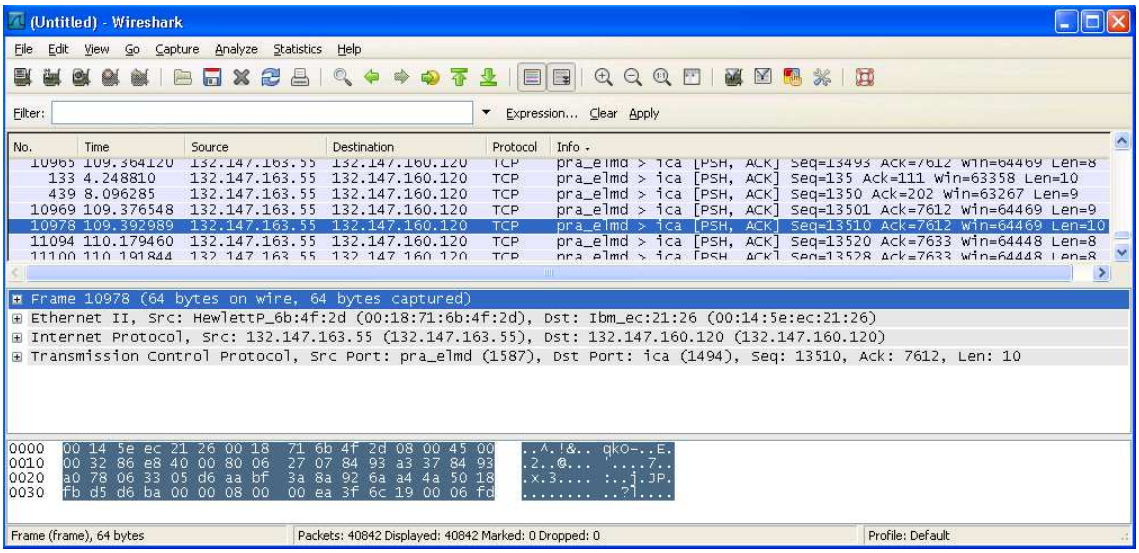


Figura 3.27 Paquetes capturados que corresponden al protocolo ICA para el respectivo análisis de protocolos

Uno de los paquetes es seleccionado para el respectivo análisis (ver *figura 3.28*).

En la *figura 3.28* se observa cómo un mensaje que tiene un tamaño de 10 bytes es tomado como campo de datos del segmento TCP. TCP le agrega 20 bytes que corresponden a la cabecera, para luego pasar el segmento a la capa de red donde se le agrega 20 bytes correspondientes a la cabecera del protocolo IP. Hasta el momento se tiene un paquete IP de 50 bytes de longitud; en la información mostrada en la *figura 3.28* donde se indica la trama capturada, se puede observar que el valor final de la trama es de 64 bytes y utiliza el protocolo

Ethernet como tecnología de capa 2. Esto quiere decir que al protocolo IP Ethernet le ha agregado 14 bytes que corresponden a los bytes de control de la trama Ethernet.

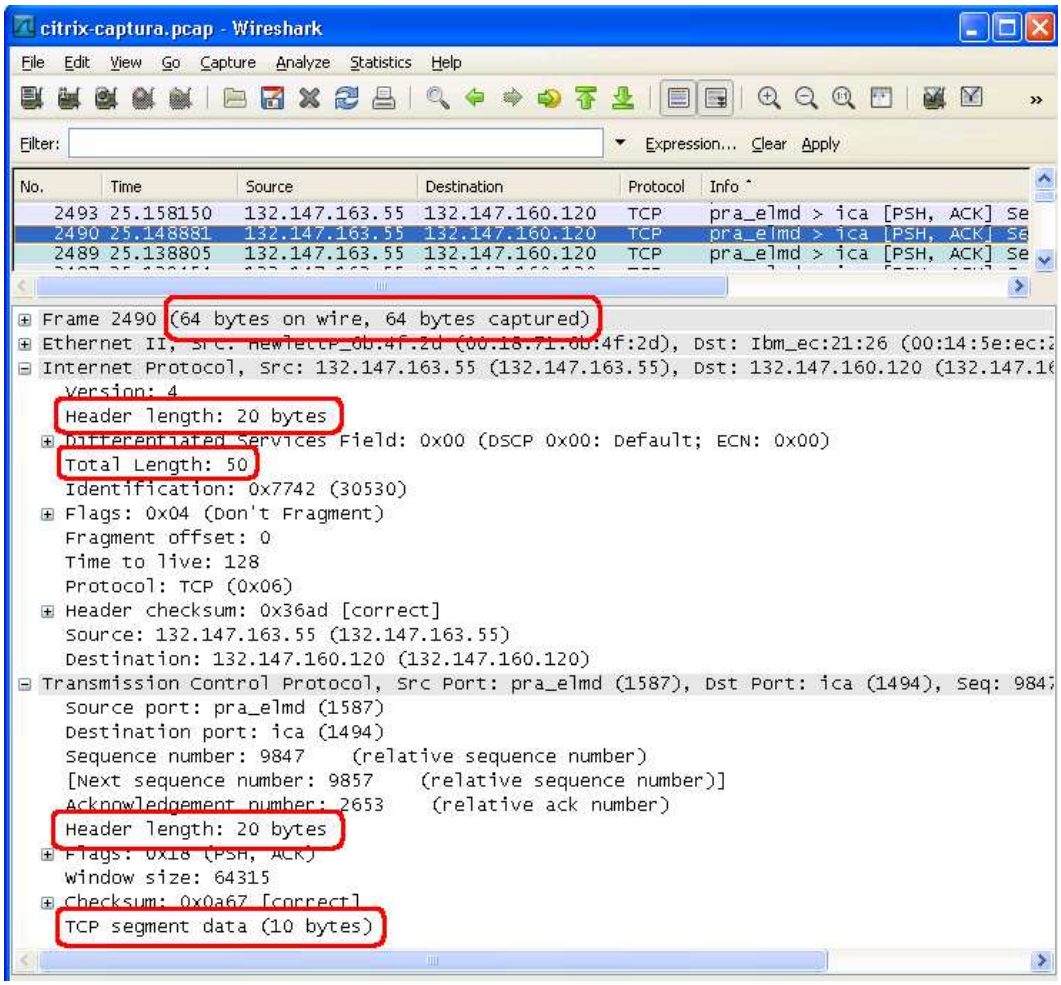


Figura 3.28 Información mostrada de cada protocolo del paquete capturado

Para determinar la tasa de transferencia hasta el protocolo IP la operación que se debe realizar es la siguiente:

- Obtener el número total de paquetes transferidos desde el cliente al servidor y viceversa.

  Paquetes transferidos = 8175

- Obtener el número total de bytes trasferidos en la conversación.

Bytes transferidos = 526355

- Obtener el tiempo total de la conversación.

Tiempo total de conversación = 329.44 segundos

- Multiplicar el valor de bytes de control de Ethernet por el total de paquetes de la conversación.

Total Bytes Ethernet = cabecera Ethernet X Paquetes transferidos
Total Bytes Ethernet = 14 X 8175
Total Bytes Ethernet = 114450

- Restar el número de bytes de Ethernet (multiplicación anterior) del total de bytes transferidos.

Total Bytes IP = Bytes transferidos - Total Bytes de cabecera Ethernet
Total Bytes IP = 526355 – 114450
Total Bytes IP = 411905

- El resultado anterior dividir para el tiempo total que dura la conversación.

Ocupación del Canal = Total Bytes IP ÷ Tiempo de duración
Ocupación del Canal = 411905 bytes ÷ 329.44 segundos
Ocupación del Canal = 1250.32 bytes/segundo

- El valor obtenido de la anterior operación es la tasa de transferencia hasta la capa de red o la que corresponde al protocolo IP. Para obtener el valor en *bps* hay que multiplicar este valor por 8 que es el número de bits que contiene un byte.

Ocupación del Canal = 1250.32 byte/segundo X 8 bits/byte
Ocupación del Canal = 10002.56 bits/s / 1000
Ocupación del Canal = 10.00 kbps

3.4.2.2 Dimensionamiento para un enlace VPN con IPSec modo Túnel utilizando el protocolo ESP

Una vez que se sabe la cantidad de ancho de banda que se necesita para ejecutar una sesión Citrix entre un cliente y servidor hasta la capa 3, se realizará el cálculo necesario para poder transportar la misma sesión por un canal virtual utilizando IPSec.

Para determinar el valor de capacidad que se necesita en IPSec, se realizan los siguientes cálculos:

- Determinar el valor en bytes de la información que agrega IPSec a los paquetes IP.

  IPSec utiliza el modo de operación Transporte y Túnel con los protocolos AH o ESP. El modo Túnel con ESP es lo que se analizará por tres razones importantes:

  1. Es un referente en razón de que genera más *overhead* en relación al modo transporte. Si el canal es dimensionado respecto a este modo se asegura una capacidad en una condición extrema de carga de información de control y seguridad del PDU.

  2. Ofrece mayor seguridad al mensaje dando la mejora de confidencialidad, es decir la información de las cabeceras IP y TCP además de los datos de capas superiores es cifrado.

  3. La implementación sugiere que, en uno de los extremos de la comunicación, no posea un sistema de seguridad VPN IPSec propio y éste depende de un ente como un *router*, *firewall* o *Gateway VPN* que soporte IPSec.

Por lo tanto un paquete de datos generado por Citrix se lo encapsularía como se muestra en la *figura 3.29*.

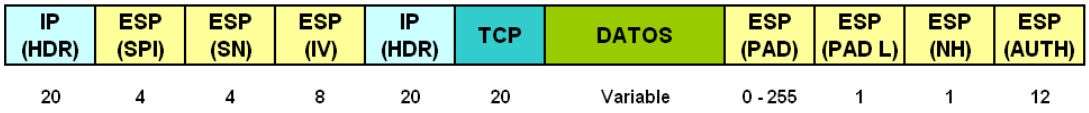


Figura 3.29 Encapsulado de un paquete IP con IPSec en modo túnel con ESP

En general el campo denominado DATOS de la *figura 3.29* puede ser de cualquier aplicación que se ejecute en el enlace VPN. La *figura 3.29* también muestra que el valor de bytes que se utiliza para implementar IPSec con ESP es la suma de todos los campos con excepción de la cabecera IP del interior, la cabecera TCP y los datos de la aplicación. La suma referida da un total de 50 bytes agregados al paquete IP. Esta suma no incluye la consideración que se debe tener al campo PADDING de ESP, ya que debido a lo variable del tamaño de los paquetes generados por el protocolo ICA no es posible determinar un valor fijo de relleno, sin embargo es posible suponer una condición extrema en la que si se cifra con el algoritmo DES o 3DES al paquete IP se le deberá agregar un máximo de 7 bytes de relleno, ya que estos algoritmos cifran en bloques de 8 bytes o 64 bits. Con esta última consideración la cantidad de bytes agregados al paquete IP original sería de 57 bytes.

– Con el valor obtenido de los bytes que se agrega por parte de IPSec al paquete IP, se debe multiplicar por el total de paquetes capturados en el analizador de protocolos, y de esta manera conocer el valor de bytes que se agregarían en la conversación analizada.

Total Bytes IPSec = cabecera IPSec X Paquetes transferidos
Total Bytes IPSec = 57 X 8175
Total Bytes IPSec = 465975

- Para obtener el número total de bytes que serían transferidos con IPSec en modo Túnel utilizando el protocolo ESP, se debe sumar el valor de ***Total Bytes IPSec*** más el ***Total Bytes IP***.

  Total Bytes con IPSec = Total Bytes IPSec + Total Bytes IP
  Total Bytes con IPSec = 465975 + 411905
  Total Bytes con IPSec = 877880

- El resultado de la anterior suma de divide para el tiempo total que dura la conversación.

  Ocupación del Canal = Total Bytes con IPSec ÷ Tiempo de duración
  Ocupación del Canal = 877880 bytes ÷ 329.44 segundos
  Ocupación del Canal = 2664.76 bytes/segundo

- El valor obtenido de la anterior operación es la tasa de transferencia que se tendría con IPSec en el modo que se ha estado señalando. Para obtener el valor en *bps* hay que multiplicar este valor por 8 que es el número de bits que contiene un byte.

  Ocupación del Canal = 2664.76 byte/segundo X 8 bits/byte
  Ocupación del Canal = 21318.08 bits/s / 1000
  Ocupación del Canal = 21.32 kbps

El valor obtenido en ***Ocupación del Canal*** corresponde a la velocidad hasta capa 3 del modelo OSI, tal como se lo ha estado recalcando. El último paso es de obtener el valor de ***Ocupación del Canal*** para un protocolo de capa 2.

La *tabla 3.1* indica los medios de comunicación que se utilizarán por parte de los equipos de usuarios para acceder al Internet. Cada uno coincide en el protocolo de capa 2, que es PPP. Este protocolo es adaptado a *Dial-Up*, ADSL y EV-DO, para su respectivo manejo en subcapas de enlace y posteriormente la preparación de la trama final de datos hacia la capa física, que es la que se encargará de enviar los datos por el medio de transmisión.

En el caso de *Dial-Up*, por lo general se utiliza PPP como protocolo de capa 2, que posteriormente son enviadas a la capa física para su respectiva adecuación al medio.

Para ADSL se tiene una consideración, que esta tecnología utiliza PPPoA o PPPoE, ambos sugieren que PPP es el protocolo que encapsule al paquete IP. Aquí el paquete dentro de la trama sufrirá segmentaciones sobre todo si se utiliza PPPoA, ya que este protocolo utiliza a AAL5 para encapsular a PPP. AAL5 es un protocolo de la capa de adaptación ATM y desde esa capa el mensaje de capas superiores, si sobrepasa la longitud de celda de 53 bytes el mensaje es segmentado.

Con EV-DO la situación es muy similar a ADSL, ya que PPP encapsula al paquete IP (Ver *figura 3.31*). Al ser una tecnología de transmisión inalámbrica de tipo móvil, se realizan mecanismos para adecuar la trama PPP al medio inalámbrico como segmentar el mensaje de capas superiores en este caso la trama PPP, por lo que este aspecto es materia de otro proyecto.

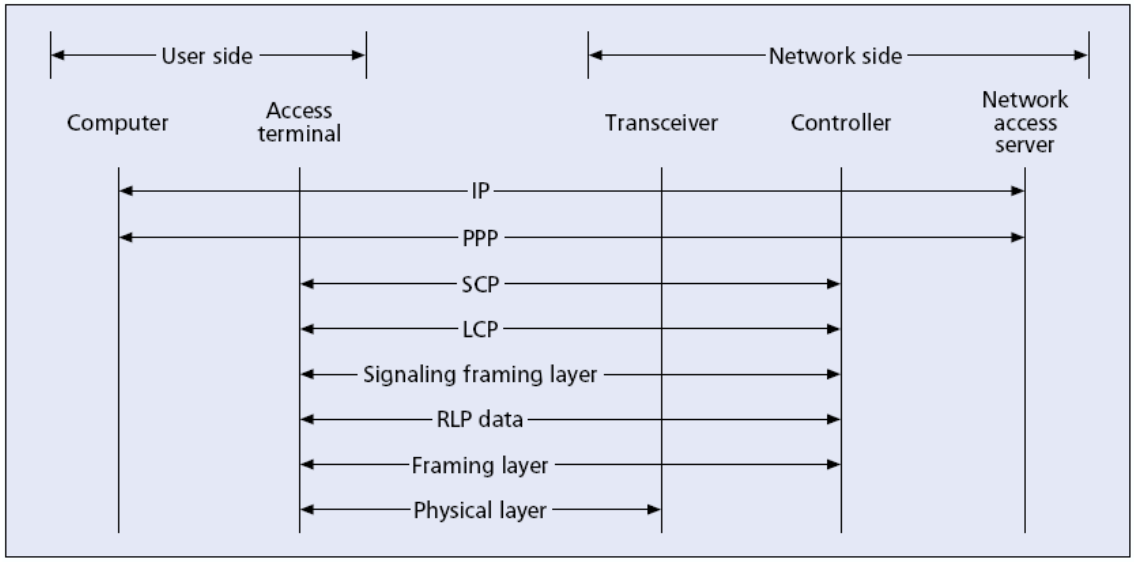


Figura 3.30 Protocolos para la interfaz aire entre equipos finales de CDMA/HDR (1xEV-DO) [20]

Por lo tanto se realizará una consideración general y final de realizar el último cálculo de la tasa de transferencia requerida hasta el encapsulamiento del

paquete IPSec con PPP. El formato de trama PPP mostrado en la *figura 3.31* indica que se puede tener hasta 8 bytes entre cabecera y la cola.

Bandera	Dirección	Control	Protocolo	Datos	FCS	Bandera
1 byte	1 byte	1 byte	2 bytes	Longitud variable. Datos de capa 3.	2 o 4 bytes	1 byte

Figura 3.31 Formato de la trama PPP [21]

Con los 8 bytes que se añade al paquete se tendría el último valor para realizar el respectivo cálculo y culminar con el dimensionamiento requerido.

Se necesita obtener el valor total de bytes que se añadirían al usar PPP.

Total Bytes PPP = cabecera PPP X Paquetes transferidos
Total Bytes PPP = 8 X 8175
Total Bytes PPP = 65400

El valor de bytes de PPP se le suma al total de bytes generados en IPSec. Al número total de bytes que se debe transmitir se lo divide para el tiempo de duración de la conversación y luego realizar la respectiva transformación para obtener el valor de la tasa de transferencia en kbps.

Total Bytes con PPP = Total Bytes PPP + Total Bytes IPSec
Total Bytes con PPP = 65400 + 877880
Total Bytes con PPP = 943280

Ocupación del Canal = Total Bytes con PPP ÷ Tiempo de duración
Ocupación del Canal = 943280 bytes ÷ 329.44 segundos
Ocupación del Canal = 2863.28 bytes/segundo

Ocupación del Canal = 2863.28 byte/segundo X 8 bits/byte
Ocupación del Canal = 22906.24 bits/s / 1000
Ocupación del Canal = 22.91 kbps

Si se analiza un enlace *dial-up* de 56 kbps se obtendría un comportamiento aceptable de la aplicación en el tiempo de respuesta, pero hay que señalar que un enlace de este tipo se conecta en el mejor de los casos entre 40 kbps y 48 kbps; sin embargo no implica que no funcione correctamente, lo que sucedería en algunos casos, es que se tornaría lento si sufre picos altos, lo que no es muy frecuente. Si el enlace *dial-up* es menor a 22.91 kbps se tendría problemas de retardo continuamente y probablemente se puedan presentar desconexiones ocasionando molestias en el proceso de recaudación.

Una combinación y uso simultáneo de aplicaciones de red sobre una VPN IPSec requerirá más ancho de banda. Un escenario ideal de un servicio de comunicaciones incluye el servicio de VoIP; por lo tanto para dimensionar un canal de comunicaciones VPN IPSec con el cliente Citrix y VoIP, se sumará la capacidad obtenida del análisis del tráfico generado por la sesión Citrix y la obtenida con la aplicación de voz con G.729.

Capacidad Canal Datos y VoIP = Ocupación Canal Citrix + Ocupación Canal VoIP G.729
Capacidad Canal Datos y VoIP = 22.91 kbps + 54.4 kbps
Capacidad Canal Datos y VoIP = 77.31 kbps

La *tabla 3.4* resume el proceso de dimensionamiento del canal de comunicaciones VPN-IPSec.

Aplicación	Tasa de transferencia en Capa 3 Protocolo IP (kbps)	Tasa de transferencia en Capa 2 Protocolo PPP (kbps)	Tasa de transferencia con IP+IPSec	Tasa de transferencia con IP+IPSec+PPP (kbps)	Porcentaje incremento de Capa 3 a encapsulamiento IPSec (%)
VoIP (G.729)	24.00	27.20	45.60	**48.80**	90.00
GSM	28.40	31.60	48.80	**52.00**	71.83
Citrix	10.00	11.59	21.32	**22.91**	113.20

Tabla 3.4 Resumen del dimensionamiento para un túnel VPN con IPSec ESP

El canal de comunicaciones VPN IPSec con ESP, debe tener al menos la capacidad indicada en la columna de color verde para cada aplicación analizada. Los datos de cada aplicación indican que se pueden presentar diferentes

porcentajes de incrementos; es así que mientras el PDU original sin IPSec sea más pequeño el porcentaje de incremento es mayor, lo que indica que es menos eficiente la comunicación VPN si los datos son relativamente cortos.

Aplicaciones	Tasa de transferencia en Capa 2 Protocolo PPP (kbps)	Tasa de transferencia con IP+IPSec	Tasa de transferencia con IP+IPSec+PPP (kbps)	Porcentaje incremento de la capacidad de un canal sin IPSec a uno con IPsec (%)
VoIP (G.729)+ Citrix	38.79	66.92	**71.71**	84.87
VoIP (GSM)+ Citrix	43.19	70.12	**74.91**	73.44

Tabla 3.5 Capacidad del canal de comunicaciones para VPN IPSec con aplicaciones simultáneas

En el caso de tener que utilizar más de una aplicación al mismo tiempo, se hace necesario sumar la capacidad calculada de las aplicaciones requeridas, como el que se muestra en la *tabla 3.5*, donde indica el valor de ancho de banda necesario para una combinación de aplicaciones que se estén utilizando simultáneamente. Si se observa el porcentaje de incremento de un canal sin VPN con uno que utiliza VPN IPSec, el incremento es significativo, y es muy importante tomarlo en cuenta al momento de contratar un acceso a Internet o de datos.

Los valores de la columna verde de la *tabla 3.4* y la *tabla 3.5*, serán los que se utilicen como referencia para implementar el canal de comunicaciones de cada usuario que requiera el servicio. Dependiendo del requerimiento se utilizará una sola aplicación o la combinación de 2 o más aplicaciones dando como prioridad a la aplicación Citrix. Otras aplicaciones pueden ser de requerimientos en http, escritorio remoto, archivos y directorios compartidos, impresiones, etc., estas aplicaciones en modo simultáneo de uso requieren conexiones de banda ancha (256 kbps de *downlink* al menos), ya que el análisis de esta sección corresponde a la necesidad del proceso de recaudación de los CARs.

3.5 ANÁLISIS DE UN SISTEMA ALTERNATIVO (REDUNDANTE) PARA LOS ENLACES VPN Y EL PERÍMETRO DE SEGURIDAD

El objetivo de este análisis, es proveer una solución de redundancia, tanto para la seguridad perimetral como para los enlaces VPN.

La solución adecuada sería el disponer un equipo, que cuente con al menos el mismo número de interfaces de red y capacidad de permitir una configuración igual al equipo principal de seguridad. Existen algunas alternativas, pero la más adecuada es adquirir un equipo de la misma marca y al menos que sea del mismo modelo o uno superior; con esto se asegura compatibilidad y que la configuración se pueda copiar sin problemas en la sintaxis, ya que el sistema operativo del equipo debería ser el mismo.

3.5.1 JUSTIFICACIÓN DE UN EQUIPO DE SEGURIDAD PERIMETRAL REDUNDANTE

Una empresa como la E.E.Q.S.A. actualmente tiene aplicaciones que los usuarios, empresas privadas, entidades de regulación, entidades gubernamentales, etc. acceden a diario y la utilizan para diversos motivos. Que la E.E.Q.S.A. quede fuera del Internet por varios minutos representa pérdidas financieras y de imagen corporativa. Para lo cual es altamente necesario contar con un sistema de seguridad redundante, lo que no pasa en el caso de las Agencias, que al no existir en determinado momento comunicaciones para el SIDECOM, el proceso de recaudación momentáneamente pase a operación manual, o si los trabajos de reparación del sistema de distribución de energía eléctrica requieren una orden de trabajo y ésta es emitida por el sistema SDI que se ejecuta a través de la red y al no tener comunicación el trabajo puede ser realizado; sin embargo el registro de operaciones debe ser almacenado de forma manual y temporalmente hasta que el servicio de red de datos se restaure.

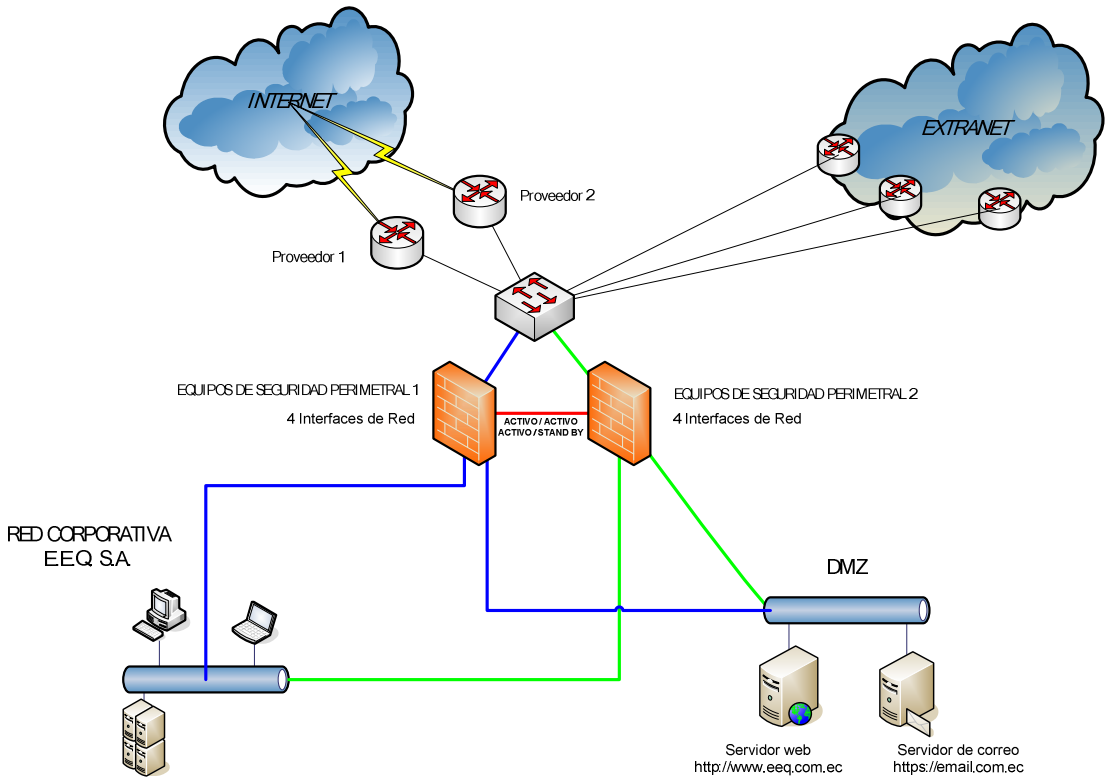


Figura 3.32 Solución de seguridad perimetral con un equipo de respaldo en línea

Todo esto implica molestias para quienes usan los diferentes sistemas informáticos pero no quiere decir que no se vaya a ejecutar o se vaya a paralizar el normal desempeño de estos y otros procesos, donde un sistema de redundancia no es tan indispensable como el que si se necesita para el sistema de seguridad perimetral.

Sin embargo es posible mantener en servicio un equipo con funciones de *Firewall*, como un servidor de propósito general, como la empresa lo ha tenido durante los últimos años, aunque levantarlo y ponerlo en funcionamiento tomaría demasiado tiempo, lo que en la práctica no sería adecuado.

Se necesitaría una configuración estable y confiable y estas exigencias las podría cubrir equipos similares y se podría implementar una topología en el área perimetral como se muestra en la *figura 3.32*.

3.5.2 MODOS DE OPERACIÓN DE LOS EQUIPOS DE SEGURIDAD PERIMETRAL

Las configuraciones adecuadas para el efecto de un sistema redundante, deben cumplir con la función principal en el caso de fallar uno de los dispositivos y de manera transparente, reiniciar el servicio de seguridad y acceso a redes externas en el menor tiempo posible.

En el caso de dos equipos similares, debería existir la capacidad de configurarse en modo de balanceo de carga, es decir, que los dos equipos trabajen por igual, repartiéndose de manera equitativa la carga de tráfico y políticas de seguridad. Otro modo sería una configuración de *stand by*, que significa que el dispositivo secundario permanece en un estado de bloqueo y entra en funcionamiento de manera inmediata cuando el principal por algún motivo no está activo.

Al ser equipos de iguales características, se espera que para las dos configuraciones, el tiempo de recuperación del servicio sea el menor posible.

En el caso de equipos de diferentes fabricantes, por cuestiones de compatibilidad, sería mejor optar por una configuración en *stand by*; sin embargo puede existir la posibilidad de que estos equipos puedan trabajar en modo balanceo de carga. En este caso, es muy probable que el tiempo de recuperación del servicio sea mayor que en el modo de balanceo de carga, sin embargo a nivel de usuario debe aparentar ser lo menos molestoso.

3.6 CONSIDERACIONES PARA LA APLICACIÓN DE SISTEMAS DE SEGURIDAD MODERNOS EN EL TRÁFICO DE DATOS (SISTEMAS ANTI-X[50], IPS[51], *FIREWALL*, ANTI-SPAM)

Las amenazas informáticas que circulan a través de las redes de datos, es un tema que continuamente está evolucionando. Es por esto que desde los sistemas

[50] Sistema Anti-X es un término que agrupa a los ya conocidos como *Anti-Virus*, *Anti-Spam*, *Anti-Spyware*, etc.
[51] Sistema de Prevención de Intrusos (IPS) establece políticas de seguridad para proteger el equipo o la red de un ataque.

de acceso más sencillos como los *users* y *passwords* en texto plano sin cifrado, hasta los más sofisticados sistemas biométricos de acceso y de inspección del contenido del paquete de datos, presentan características cada vez más complejas. Estos sistemas debido a su constante estudio y trabajo tratan de impedir en lo posible que las amenazas, que no son más que consecuencias de vulnerabilidades de todo sistema informático, sean explotadas de manera maliciosa.

Para el caso de la E.E.Q.S.A., es importante saber donde va a estar ubicado el equipo de seguridad perimetral y qué servicios desde el exterior e interior se podrán tener acceso. Para esto se ha considerado establecer tres niveles de seguridad.

3.6.1 PRIMER NIVEL DE SEGURIDAD

Como primer nivel de seguridad, se tendrá la restricción de servicios, es decir, que desde redes externas solo se pueda tener acceso a determinada aplicación o servicio; como por ejemplo desde el Internet se puede tener acceso de manera pública al sitio Web, correo electrónico y al Geographical *Information Satelital* (GIS).

En el caso de las extranets, accederán a servicios específicos como por ejemplo, los sistemas SDI, SIDECOM o telefonía.

Esto es posible realizar configurando, *Network Address Translation* (NAT) y políticas de *firewall*.

3.6.2 SEGUNDO NIVEL DE SEGURIDAD

Un segundo nivel de seguridad sería el de proteger los datos, contra posibles ataque de virus, espías, gusanos, troyanos, *back doors* y *spam*. En esta parte, el equipo o sistema de protección debe ser tan capaz de manejar todo esto sin alterar en gran medida el desempeño y calidad de funcionamiento.

Uno de los problemas más comunes y molestosos que tiene todo usuario, no solo de la E.E.Q.S.A., sino de cualquier red, es el denominado *spam*. Para el efecto de frenar este malestar, se ha optado por mantener, el servidor que controla el *spam* y agregarle a éste una segunda barrera que sería el equipo de seguridad perimetral.

3.6.3 TERCER NIVEL DE SEGURIDAD

Un tercer nivel de seguridad, es el provisto por un sistema de prevención de intrusos (IPS). Este tipo de sistemas son los que están en pleno funcionamiento y estudio así como también en evolución, ya que permiten una seguridad profunda de la información que transita, no solo en determinado nivel de la comunicación, sino que llega hasta completar la inspección de toda la información.

No solo basta con identificar el peligro, sino también el de actuar de manera proactiva. Es así que con los IPS es posible llegar a este nivel de seguridad. Ahora dependiendo de la carga de tráfico que pase por un equipo de éstos, determinará qué tipo de *hardware* sería el adecuado. Para el caso de la E.E.Q.S.A., el número de usuarios que utilizan los recursos de red, principalmente el Internet, es considerable, alrededor de mil equipos entre PCs, impresoras, teléfonos y equipos que permiten la conectividad.

Así que el equipo que posea la funcionalidad de IPS, debe tener gran capacidad de transportar el tráfico, que pase por él. De hecho en el mercado ya se cuenta con equipos que realizan este tipo de funcionalidades, directamente a través de *hardware*, es decir los denominados equipos *appliance*.

A esto se debe añadir el hecho de que la División de Tecnología de la Información y Comunicaciones de la E.E.Q.S.A. a través de su Departamento de Comunicaciones y Soporte, está en pleno proceso de modernización y mejoramiento de los sistemas de comunicación. Esto quiere decir que no solo se mejorará la calidad de las comunicaciones, sino que crecerá la red de datos y por consiguiente el número de usuarios y dispositivos, en un futuro cercano.

3.7 ESQUEMA DE RED PARA EL DISEÑO DE LA RED VPN Y EL EQUIPO DE SEGURIDAD PERIMETRAL

En esta sección en base a los aspectos antes analizados y estudiados, se realizará un resumen, dando a conocer las características técnicas generales que debe cumplir el equipo de equipo de seguridad perimetral así como la ubicación del equipo y los enlaces que estarían dentro de la topología de red de la E.E.Q.S.A.

Cabe mencionar que lo que se requiere es un sistema de seguridad integral, el cual en el mejor de los casos, todas las funcionalidades residan en un solo equipo, sin que esto implique una reducción en el desempeño de la red.

Enlace	Características	Equipo	Propiedad	Observaciones
Internet	Ethernet UPT Cat. 5e	*Router*	Proveedor	Instalado y en funcionamiento
Extranet	Ethernet UPT Cat. 5e Trunk IEEE 802.1q	*Switch*	E.E.Q.S.A.	Por instalar
Red Corporativa	Ethernet UPT Cat. 5e VLAN A	*Switch* Principal	E.E.Q.S.A.	Instalado y en funcionamiento
DMZ (Zona Desmilitarizada)	Ethernet UPT Cat. 5e VLAN B	*Switch* Principal	E.E.Q.S.A.	Instalado y en funcionamiento
Seguridad	4 Puertos Ethernet 10/100	Seguridad Perimetral	E.E.Q.S.A.	Por adquirir

Tabla 3.6 Equipos y enlaces que conforman el diseño para la seguridad perimetral

A parte de esto se debe señalar que se debe mejorar el servicio de Internet, es decir mejorar el ancho de banda, tanto en cantidad como en calidad. Para lo cual la E.E.Q.S.A. tiene contratado el servicio de acceso hacia el Internet con la empresa Telconet y que se ha comprometido a incrementar el ancho de banda si así lo requiere la empresa sin costo adicional, esto es parte de un convenio.

Los requerimientos en equipamiento, para poder cumplir con el estudio realizado, es de al menos dos elementos: Equipo de seguridad perimetral, y mejorar los enlaces exteriores, sobre todo el que corresponde al Internet.

3.7.1 EQUIPAMIENTO Y ENLACES DISPONIBLES

El equipamiento para el acceso a Internet está estipulado en el contrato del proveedor, básicamente se indica que debe instalar el enlace de última milla y un equipo de acceso (MODEM, *router*, etc.), el cual debe tener una interfaz Ethernet disponible para conectar con la red corporativa de la E.E.Q.S.A.

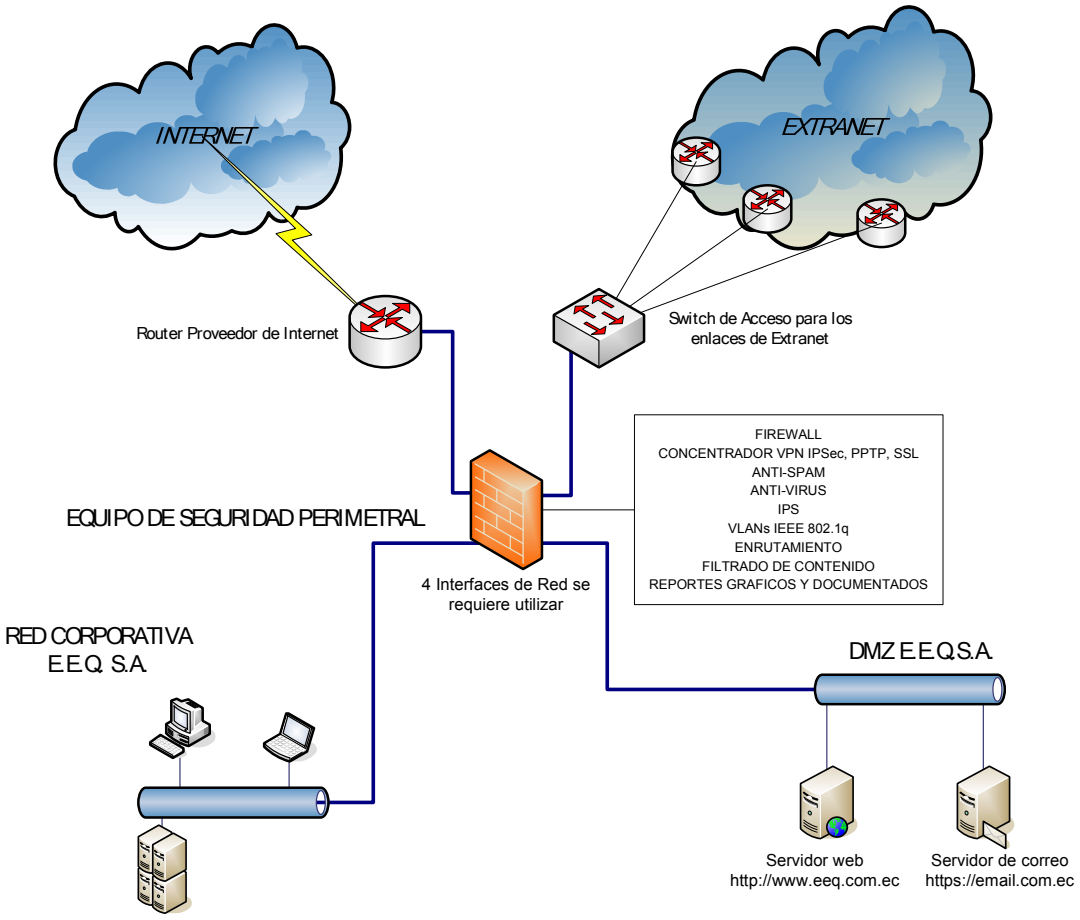


Figura 3.33 Diagrama básico del diseño de la red donde se señalan las interfaces de red necesarias

Los equipos de las empresas que acceden a la red corporativa por medio de enlaces dedicados o través del Internet forman la parte de la extranet de la E.E.Q.S.A. Estas empresas ingresan con su propia infraestructura al centro de cómputo de la E.E.Q.S.A. y esto incluye equipamiento activo como *routers* modems, etc. Estos equipos del proveedor convergen en un *switch* de capa 2 y a su vez este equipo se conecta en una interfaz del *firewall*.

El esquema que se ha estado utilizando es el adecuado, pero al introducir el nuevo equipo de seguridad perimetral es necesario que cada enlace corresponda a una sub-interfaz diferente, es decir se necesita realizar una configuración de VLANs en el *switch* de capa 2 donde convergen dichos enlaces (Ver *figura 3.33)*. Por lo tanto el *switch* debe ser cambiado por uno que pueda soportar IEEE 802.1q y en este caso el equipo de seguridad perimetral también debe soportar IEEE 802.1q para la respectiva configuración del enlace troncalizado, con el objetivo que diferentes redes seccionadas por VLANs pasen a través del enlace de *trunk* entre *switch* de acceso extranet y el equipo de seguridad.

El enlace actual de Internet tiene como esquema de red, un enlace de última milla y un *router*, el cual se conecta a una VLAN del *switch* principal tal como se ha explicado y detallado en el Capítulo 2.

3.7.2 DISEÑO DE VLANs PARA LOS ENLACES DE EXTRANET

Como se ha mencionado en la sección anterior una manera de administrar y controlar los acceso corporativos externos, es teniendo VLANs configuradas en el *switch* de acceso extranet. Estas VLANs no tendrán ninguna relación con el sistema de VLANs ya implementado en la red corporativa de la E.E.Q.S.A., es decir será un sistema totalmente independiente en el cual el único vínculo entre estas redes y la red de la E.E.Q.S.A. será el FG300A que está en el medio. Además al ser independiente no se corre el riesgo de un sobrelapamiento de identificadores de VLANs.

El estándar en común que deberán soportar estos equipos será el IEEE 802.1q, con el cual será posible establecer entre estos dos equipos un enlace troncal o *trunk* para el transporte de varias VLANs por un solo canal físico.

Aunque en el esquema mencionado no se tiene vínculos con las VLANs de la red corporativa de la E.E.Q.S.A., se hace necesario identificarlos con otra numeración, lo que ayudaría en la administración.

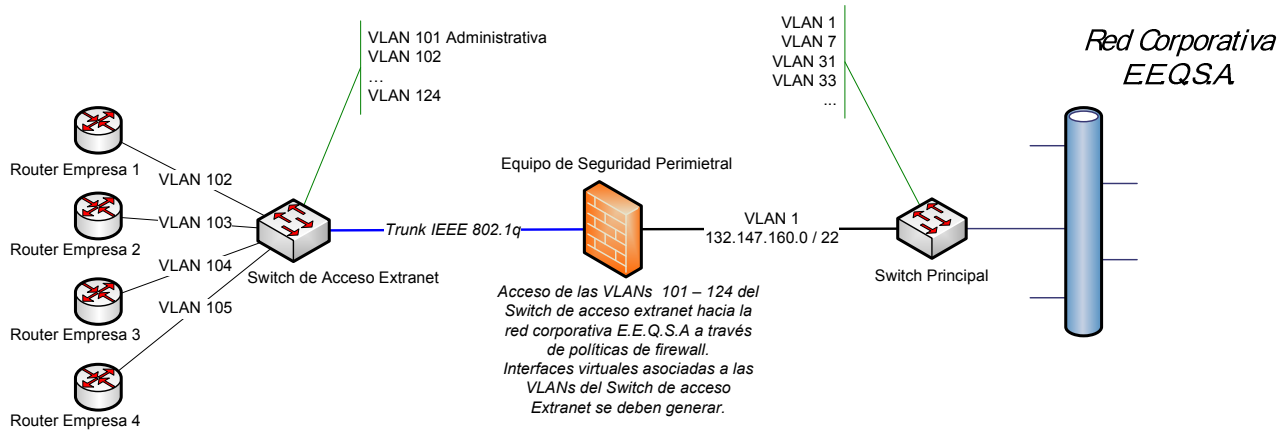


Figura 3.34 Diseño de VLANs para acceso de Extranet

Se ha establecido para este sistema de VLANs sobre el *switch* de acceso extranet un rango numeración para los identificadores que empezará desde la VLAN 101 hasta la VLAN 124 (Ver *figura 3.34*). Un total de 24 VLANs que corresponden al número de interfaces Fast-Ethernet que deberá soportar el *switch* de acceso extranet y que serán suficientes para integrar los actuales enlaces exteriores y un futuro creamiento de estos enlaces, sobre todo los correspondientes a VPN del tipo *LAN - LAN*.

El esquema de nombres de las VLANs obedecerá el siguiente formato:

VLAN_*NOMBRE QUE IDENTIFICA EL ENLACE O RED*

Es así que la VLAN administrativa tendrá el nombre de VLAN_ADMIN, donde todo el nombre estará en mayúsculas.

3.7.3 DIRECCIONAMIENTO IP EN LOS ENLACES VPN

Los clientes VPN adoptarán el direccionamiento IP que estará conformado de la siguiente forma:

- **Direccionamiento de acceso remoto o *Dial – Up*.** Dentro de este acceso se ha asignará la red 172.16.20.0 / 24, la cual tendrá como máximo 254 direcciones disponibles de las cuales las 50 primeras direcciones se

asignarán a los accesos con PPTP, las siguientes 50 a IPSec y las 50 siguientes a VPN-SSL. El resto se utilizará para un incremento futuro. Este direccionamiento se lo realizará automáticamente, es decir que se activará un servidor DHCP en el equipo de seguridad para que le asigne al cliente que solicita una conexión una dirección disponible del *pool* de direcciones.

- **Direccionamiento de *LAN - LAN*.** Para esta modalidad la red remota podrá mantener su direccionamiento si no se sobrepone con alguna red de la E.E.Q.S.A., de ser el caso se optará por usar NAT para evitar la duplicación de la red; de hecho esta opción se la considerará como requisito para activar el enlace VPN. En el NAT se utilizarán las direcciones restantes de la red 172.16.20.0 / 24, es decir a partir de la dirección 172.16.20.151 / 24.

- **Direccionamiento para servidores**. Los equipos que complementarán el servicio de VPN serán servidores de diferentes aplicaciones como: servidor de autenticación RADIUS, servidor de telefonía IP, analizador de reportes y otros que se puedan presentar durante la implementación; para el efecto se ha verificado la disponibilidad de direcciones de la red IP 132.147.160.0 / 22, que son las siguientes: 132.147.163.166, 132.147.163.247 y 132.147.163.55.

- **Direccionamiento para la administración del *Switch* de acceso para los enlaces extranet.** Como el *switch* de acceso debe ser un equipo administrable es necesario que cuente con una dirección IP para la respectiva gestión, configuración y monitoreo. No se espera muchos *hosts* en este segmento de red, por lo que se ha considerado utilizar la red IP 192.168.10.0 / 28, que ofrecerá una capacidad de 14 direcciones IP disponibles, de las cuales las 2 primeras se utilizarán en la interfaz virtual del equipo de seguridad y en la interfaz virtual correspondiente del *switch*.

Todas estas direcciones de red, de ser necesario, estarán enrutadas con las direcciones de red que conforman el direccionamiento IP de la red corporativa de la E.E.Q.S.A., con las debidas restricciones de cada caso.

3.7.4 EQUIPO NECESARIO PARA LA FUNCIONALIDAD DE SEGURIDAD PERIMETRAL

El equipo de seguridad perimetral debe tener entre sus funcionalidades las siguientes: *Firewall*, VPN, *Router*, Filtrado de Contenido *Web*, IPS, Anti-Virus, Anti-Spam. Un interfaz para el acceso a Internet, uno para extranet, uno para la DMZ y un cuarto para la red interna o red corporativa de la E.E.Q.S.A.

En la *tabla 3.6* se indica los enlaces y equipos que van a intervenir en el diseño, de lo que se puede mencionar lo siguiente: la infraestructura depende íntegramente de la adquisición del equipo de seguridad perimetral ya que los enlaces y equipos se encuentran disponibles y la mayoría trabajando con el actual *firewall*. En el caso del acceso a Internet, éste se mantendrá a través de un enlace independiente, con el propósito de manejar sin contratiempos el cambio de equipos y mantener en primera instancia la configuración anterior a la instalación del nuevo equipo de seguridad.

Las características generales requeridas del nuevo equipo se reforzarán con nuevas y modernas características que surgirán de las propuestas de los posibles proveedores del equipo de seguridad perimetral.

Varios de los proveedores han sido notificados del interés de adquirir un equipo de seguridad perimetral por parte de la E.E.Q.S.A. En la siguiente sección se indicará la empresa y el producto que puede ofrecer a la E.E.Q.S.A. dentro del mercado local.

3.8 PRODUCTOS EN EL MERCADO LOCAL

El mercado local ofrece básicamente dos tipos de soluciones que se ajustan a los requerimientos, equipos tipo *appliance* y sistemas de seguridad basados en

software. De estas soluciones se va a analizar lo que el mercado puede ofrecer, por medio de diferentes empresas que ofertan soluciones de seguridad, incluido equipamiento.

Los ejemplos de soluciones de seguridad perimetral toman en cuenta las peticiones a los proveedores de demostraciones o en su lugar información técnica y explicación del producto que pueden ofertar; de ninguna manera se trata de un concurso.

Luego de la demostración por parte de los proveedores, se elaborará una lista de los requerimientos en función de las necesidades con un reforzado en base a las exposiciones previas de los proveedores, para luego de un proceso administrativo interno de la E.E.Q.S.A. lanzar a concurso la compra de un equipo de seguridad perimetral de manera formal.

Equipos Appliance	
-	Cisco Systems equipos de la serie ASA
-	Fortinet con la serie de equipos FGT500A y FGT300A
-	3COM con sus equipos TippingPoint
Equipos Servidores Linux	
-	Astaro Security Gateway

Tabla 3.7 Cuadro de sugerencias de equipos de seguridad de datos de proveedores de la E.E.Q.S.A.

Por parte del Departamento de Comunicaciones y Soporte, debe quedar claro los requerimientos y cuáles son las posibles soluciones, para así poder realizar la lista de especificaciones técnicas que debe reunir el equipo o solución de seguridad perimetral que más se ajuste a las necesidades de la E.E.Q.S.A.

Una vez realizada la invitación a los proveedores, se registraron cuatro soluciones, que se muestran en la *tabla 3.7* y que son brevemente analizadas en las siguientes secciones.

3.8.1 CISCO SYSTEMS EQUIPOS DE LA SERIE ASA

Dentro de esta serie de equipos, se puede anotar lo más destacable en cuanto a rendimiento y características de seguridad requerida. La serie de equipos ASA comprende tres tipos de modelos, Cisco ASA 5510, 5520 y 5540; hasta la fecha de haber terminado este proyecto no se encontró nuevos modelos. En la *figura 3.35* se muestra la parte frontal de un Cisco ASA.

Figura 3.35 Cisco ASA 5500 series [22]

La referencia que se puede hacer respecto a estos equipos se remonta a los ya conocidos *firewalls* Cisco PIX 500, Sistemas de Prevención de Intrusos Cisco IPS 4200 y a los concentradores de VPN Cisco VPN 3000. La funcionalidad para lo que fueron diseñados cada uno de estos sistemas de seguridad son recogidos por los equipos Cisco ASA, donde se tiene funcionalidad de *firewall*, Sistema de Prevención de Intrusos (IPS) y Concentrador de VPN, además de otras funcionalidades inherentes a *switching* y *routing*.

Una vez obtenida la información general sobre esta serie de equipos, se puede analizar cuál de estos modelos se acopla mejor a las necesidades actuales y futuras (hasta 5 años) de la red de datos de la E.E.Q.S.A. En la *tabla 3.8* se señala lo más destacable de estos equipos Cisco en cuanto a desempeño.

En cuanto al modelo ASA 5510, no cumple con el requerimiento o característica de alta disponibilidad, ya que en un futuro a corto plazo se ha pensado en un

equipo de respaldo que funcione en modo activo o bloqueado, también carece de la funcionalidad de VLAN IEEE 802.1q.

El modelo ASA 5520, cumple con los requerimientos de funcionalidad básica, como son: *firewall*, IPS, y concentrador de VPN (IPSec, SSL y PPTP).

Características	**Descripciones**		
	CISCO ASA 5510	**CISCO ASA 5520**	**CISCO ASA 5540**
Firewall Throughput	Hasta 300 Mbps	Hasta 450 Mbps	Hasta 650 Mbps
VPN 3DES/AES *Throughput*	Hasta 170 Mbps	Hasta 225 Mbps	Hasta 325 Mbps
Pares VPN IPSec	50	300	300
Sesiones Concurrentes	32000	130000	280000
Nuevas Sesiones Por Segundo	6000	9000	20000
Interfaces de Red Integrados	3 Fast-Ethernet	4 Gigabit-Ethernet y 1 Fast-Ethernet	4 Gigabit-Ethernet y 1 Fast-Ethernet
Puertos de Administración	1 serial, 1 Fast-Ethernet y 2 USB	1 serial y 2 USB	2 serial y 2 USB
Funcionalidad de Sistemas Anti-X	Si	Si	Si
Funcionalidad de IPS	Si	Si	Si
VLANs	0	25	100
Alta Disponibilidad	No Soporta	Activo/Activo y Activo/*Stand by*	Activo/Activo y Activo/*Stand by*

Tabla 3.8 Características de los modelos de la serie ASA 5500 de Cisco Systems [22]

El ASA 5540 cumple con los requerimientos solicitados y supera las expectativas en cuanto a desempeño en *firewall* y VPN, incluso este modelo estaría sobredimensionado para la red corporativa de la E.E.Q.S.A. Sin embargo es posible por cuestiones de un crecimiento futuro sea el equipo que se ajuste a esta proyección.

3.8.2 FORTINET CON LA SERIE DE EQUIPOS FGT500A Y FGT300A

Fortinet ofrece en sus equipos Fortigate 300A y 500A una serie de servicios basados en procesamiento en tiempo real como son: *Firewall*, Antivirus, VPN IPSec, IPS, realizando estas operaciones basado en la potencialidad de los ASICs que cumplen con todas estas funciones.

Figura 3.36 Fortigate FG300A [23]

La *figura 3.36* muestra la parte frontal de un Fortigate 300A, donde se puede apreciar los 4 interfaces de red a 10/100 Mbps, 2 a 10/100/1000 Mbps, puertos USB, puerto de consola y un *display* de información.

Características	**Descripciones**	
	Fortigate 300A	**Fortigate 500A**
Firewall Throughput	400 Mbps	500 Mbps
VPN 3DES/AES *Throughput*	120 Mbps	150 Mbps
Túneles Dedicados	1500	3000
Sesiones Concurrentes	400000	400000
Nuevas Sesiones Por Segundo	10000	10000
Interfaces de Red Integrados	2 Gigabit-Ethernet y 4 Fast-Ethernet	3 Gigabit-Ethernet y 4 Fast-Ethernet
Puertos de Administración	1 serial y 2 USB	2 serial y 2 USB
Funcionalidad de Sistemas Anti-X	Si	Si
Funcionalidad de IPS	Si	Si
VLANs	VLAN 802.1q	VLAN 802.1q
Alta Disponibilidad	Activo/Activo y Activo/*Stand by*	Activo/Activo y Activo/*Stand by*

Tabla 3.9 Características de los modelos FG300A y FG500A de Fortinet [23]

Los dos modelos presentados por parte del proveedor, cumplen con los requerimientos básicos de seguridad y supera en gran medida características de desempeño comparado con los Cisco ASA.

Una funcionalidad denominada *traffic shaping* que sirve para controlar el ancho de banda para determinado enlace controlado por una política de *firewall*, Fortinet lo implementa en esta serie de equipos.

Para enlaces VPN IPSec la autenticación se puede extender hacia un tercer equipo que sería un servidor RADIUS.

Estas dos funcionalidades serán tomadas en cuenta como innovación tecnológica para elaborar el definitivo documento de especificaciones técnicas.

3.8.3 EQUIPOS TIPPINGPOINT – 3COM

Su seguridad se basa en implementar un IPS de gran rendimiento permitiendo a los usuarios ingresar a sitios con toda confianza.

Figura 3.37 TippingPoint 400 [24]

La *figura 3.37* muestra la parte frontal de un TippingPoint 400. Se trata de un equipo de alto rendimiento en capa 2 comparado con un Cisco ASA o un Fortinet, pero carece de funcionalidades de capa 3.

Características	**Descripciones**
	TippingPoint 400
Firewall Throughput	No tiene esta función
VPN 3DES/AES *Throughput*	No tiene esta función
Túneles Dedicados	No tiene esta función
Sesiones Concurrentes	2000000
Nuevas Sesiones Por Segundo	750000
Interfaces de Red Integrados	2 Gigabit-Ethernet
Puertos de Administración	1 serial y 1 USB
Funcionalidad de Sistemas Anti-X	Si
Funcionalidad de IPS	Si
VLANs	VLAN 802.1q
Alta Disponibilidad	Activo/Activo y Activo/*Stand by*

Tabla 3.10 Características del modelo TP400 de TippingPoint [24]

Este equipo fue presentado e incluso se realizó pruebas dentro del Centro de Cómputo de la E.E.Q.S.A. pero no cubría los requerimientos. La razón es que se

trata de un equipo que tiene la funcionalidad específica de IPS y Sistema Anti-X (ver *tabla 3.10*); sin embargo los distribuidores de esta marca ofrecieron que para el concurso podrían presentar un modelo del TippingPoint que tiene funcionalidades de *Firewall* y concentrador de VPNs a parte de las ya mencionadas y detalladas en el cuadro.

3.8.4 EQUIPO DE SEGURIDAD SOBRE PLATAFORMA LINUX ASTARO *SECURITY GATEWAY*

Esta solución incluye un paquete con licencia para cada una de las opciones de seguridad requerida. Se instala el *software* sobre un equipo de tipo servidor y se empieza a habilitar dichas opciones.

Figura 3.38 Astaro Security Gateway Software Appliance [25]

La *figura 3.38* muestra la presentación del software grabado en un disco compacto. Las diferentes funcionalidades se activan bajo la contratación de licencia.

Las características presentadas son relativas ya que dependerán del equipo sobre el cual se instale el *software*. Hay dos opciones, la primera es que se lo instale y configure en un servidor de la E.E.Q.S.A. y la otra es que la empresa que ofrece este producto incluya en su propuesta el equipo y de esta manera poder mejorar las características de desempeño del equipo. La *tabla 3.11* recoge características mínimas de la opción en *appliance* del fabricante Astaro, ya que no se puede

establecer tales características hasta que se defina el *hardware* sobre el cual se instalaría la aplicación de seguridad.

Características	**Descripciones**
	Astaro Security Gateway Software
Firewall Throughput	100 Mbps
VPN 3DES/AES *Throughput*	30 Mbps
Sesiones Concurrentes	5000
Nuevas Sesiones Por Segundo	1000
Interfaces de Red Integrados	2 Gigabit-Ethernet
Puertos de Administración	1 serial
Funcionalidad de Sistemas Anti-X	Si
Funcionalidad de IPS	Si
VLANs	VLAN 802.1q
Alta Disponibilidad	Activo/Activo y Activo/*Stand by*

Tabla 3.11 Características del Astaro Security Gateway Software [25]

3.8.5 CARACTERÍSTICAS DEFINITIVAS PARA LA ADQUISICIÓN DEL EQUIPO DE SEGURIDAD

Luego de haber revisado las alternativas que algunos proveedores han facilitado, se han optado por recopilar aspectos generales y que satisfagan las necesidades del los requerimientos. También hay que anotar que lo que se busca es una solución basada en equipamiento de reconocida reputación a nivel internacional.

Las especificaciones técnicas deben obedecer a los requerimientos de seguridad perimetral y al estudio realizado para la formación de VPN con IPSec ESP, PPTP y SSL.

En primer lugar se especificará el detalle físico del equipo

- Se necesita 4 interfaces de red Ethernet a 10/100 Mbps, sin embargo por alguna configuración adicional es posible que se necesite una interfaz más. Así que la especificación para puertos de red estará en un número 5

Ethernet a 10/100 Mbps y que tengan la capacidad de auto sensar el extremo que se conecta y también detecte puertos MDI o MDIX.

- Para la administración local y básica se necesita un puerto serial RS-232. El cual permitirá en casos en que el equipo no funcione su interfaz gráfica configurarlo o restablecer el servicio de manera local y a través de un puerto serial.

- La dimensión del largo debe ser de 19” para que sea montable en un *rack* de dicha dimensión entre bastidores, ya que ese tipo de soporte es con el que cuenta la E.E.Q.S.A. en su centro de cómputo.

- Como una característica opcional se plantea que el equipo tenga 2 fuentes de alimentación eléctrica ya que se haría una instalación de dos circuitos diferentes en el centro de cómputo y en cada uno de ellos se conectaría una fuente del equipo de seguridad perimetral, esto con la prevención de tener respaldo de energía.

Características de desempeño del equipo

- El *firewall* que está en funcionamiento no permite registrar el número de sesiones concurrentes ni de nuevas sesiones por segundo, pero se haría un estimado del número de usuarios que están habilitados para acceder a Internet. El número de usuarios que tiene acceso al Internet es de aproximadamente 500. Un acceso a un sitio *web* como la de un banco es de alrededor de 5 sesiones, el usuario normal ingresa a este tipo de sitios, por lo tanto serían 2500 sesiones concurrentes que se podrían generar. Como este valor es un límite se lo duplicará por varias razones entre ellas que la clave de Internet del usuario autorizado se comparte, hasta realizar ese control es mejor prevenir una posible sobrecarga en el número de sesiones concurrentes.

- Para el caso de nuevas sesiones por segundo se estimará que todas las posibles cuentas de Internet ingresen en el mismo instante lo que daría 500 nuevas sesiones, pero nuevamente por cuestiones que salen del control de acceso a Internet se estimará en el doble, es decir 1000 nuevas sesiones por segundo.

- El *throughput* del *firewall* está fijado básicamente en las 4 interfaces de red que se conectará al Internet y otras redes externas y será del valor máximo de la capacidad de cada interfaz que es de 100 Mbps y multiplicado por 4 que es el número de puertos Ethernet que se requiere. Hay que mencionar que el enlace a Internet es de 3.5 Mbps y que entre éstos están los accesos a la extranet, DMZ y red interna que necesiten acceder y entre ellos no superarían ni el 30 % de la capacidad de cada interfaz Ethernet.

- VPN IPSec con cifrado 3DES ofrece una seguridad robusta. El *throughput* que se debería manejar en el equipo con IPSec sería de 30 enlaces a 128 kbps que es el número de enlaces que aproximadamente se trataría formar. Los 128 kbps están justificados por la capacidad que necesitaría un enlace para que ejecute Citrix y VoIP con codec GSM o G.729, pero en la realidad según la *tabla 3.5* se necesitaría 74.91 kbps y se sabe que el acceso a Internet (que no sea *Dial Up)* más bajo en última milla es de 128 kbps de *downlink* y 64 kbps de *uplink*; si se supone un caso extremo con 30 enlaces al mismo tiempo, daría un total de 3840 kbps. Para los usuarios que no son CARs como los administrativos, operadores y ejecutivos, el ancho de banda se lo ampliaría ya que necesitarían ejecutar más aplicaciones; un incremento a 512 kbps por enlace es adecuado. Hasta el momento se tienen 10 usuarios con estas características lo que indica que el equipo deberá procesar en un supuesto caso hasta 5120 kbps. Con estos antecedentes el *throughput* mínimo de procesamiento para VPN IPSec es de 10 Mbps, se considerará que esta necesidad aumentará a corto plazo por lo que el requerimiento se lo considerará de 50 Mbps.

Funcionalidades básicas del equipo

- La funcionalidad de Anti-Virus, Anti-Spam, protege al equipo del ingreso de estas amenazas, lo que mejora la seguridad en el acceso de redes externas como Internet y la extranet.

- Un IPS dentro de las funcionalidades permite controlar amenazas en base a las acciones que se le pueda ordenar y configurar, complementando la seguridad que ofrece un *firewall*. La E.E.Q.S.A. debe proteger la integridad de la información que circula en modo electrónico, la cual debe ser protegida por mecanismos como un inspector de contenido y que éste tome las decisiones correctas para evitar daños en la información que procesa y almacena la E.E.Q.S.A.

- Funcionalidad de *Firewall*. Esta funcionalidad es básica y es una de las razones de ser de este proyecto. NAT, PAT, con el objetivo de optimizar las direcciones IP públicas y puertos disponibles y ocultar la red corporativa de las redes externas.

- La funcionalidad VPN es la principal razón de ser del presente proyecto y en cual se detallan los siguientes requerimientos: Túneles VPN que necesita la empresa no llega a 100, sin embargo para que la base de la especificación sea alta se colocará 300 que es el número que puede manejar un Cisco ASA 5520 que cumple los requerimientos básicos de seguridad. Las tecnologías que deberá soportar serán PPTP, IPSec y SSL. Para la encripción se deberá exigir los algoritmos DES, 3DES y AES, por ser de gran robustez para la confidencialidad de la información. En la autenticación se requerirá que cumpla al menos con el algoritmo MD5. Detección del estado del túnel, calidad de servicio para las aplicaciones multimedia. Que cumpla con una certificación a nivel internacional en la operación de VPN IPSec.

- Filtrado de contenido *web* permite que los usuarios de manera voluntariamente o involuntariamente accedan a sitios que atenten contra las normas básicas del buen uso de los recursos informáticos, entre los que se puede mencionar el ingreso a sitios pornográficos, sitios de ocio, descarga de videos y música en varios formatos, juegos en línea, etc.

- La funcionalidad de respaldo en línea permite una redundancia ante ciertos eventos que puedan provocar el corte del servicio de seguridad; además este respaldo que debe tener la capacidad de balanceo de carga (Activo-Activo) podría aumentar en el doble las capacidades que un solo equipo de seguridad perimetral puede ofrecer.

- Una funcionalidad que permite optimizar el uso de las interfaces físicas es el de VLAN con el etiquetado IEEE 802.1q. Al manejar varios enlaces por un solo puerto físico se está dando un mejor uso a la interfaz y agrega seguridad, ya que no solo ofrece servicio de enrutamiento entre segmentos diferentes de red, sino que entre estos segmentos para que exista el flujo de tráfico se tendrá la opción de agregar políticas de seguridad.

- Soporte para IPv4 y IPv6, asegurando la compatibilidad para el futuro de las redes IP.

Gestión, enrutamiento y funcionalidades adicionales

- Soporte para autenticación por medio de LDAP, *Active Directory*, *Radius* y XAuth para VPN IPSec que es el *Radius* en VPN.

- *Traffic Shaping* para controlar y optimizar el uso de los enlaces contratados como por ejemplo el Internet.

- Administración y gestión, a través de diferentes medios como SSH (Telnet seguro), HTTPS, SNMPv2 y v3.

- Funcionalidad de enrutamiento con los protocolos RIPv1 y v2, OSPF y estático.

- Capacitación a dos técnicos del Departamento de Comunicaciones y Soporte en el manejo del equipo y configuraciones de seguridad.

- Otras funcionalidades que permiten que la adquisición del equipo asegure que sea de alto desempeño.

La *tabla 3.12* recoge en resumen las especificaciones técnicas detalladas anteriormente y que serán publicadas en el sitio *web* de la empresa y las mismas que serán enviadas a los proveedores para que presenten su cotización.

Especificaciones Técnicas para el nuevo Equipo de Seguridad para la Red de Datos de la E.E.Q.S.A.

Item	Descripción de los requerimientos para el Equipo de Seguridad de la Red de Datos
1	Cinco (5) interfaces Ethernet/Fast Ethernet soporte Auto MDI-MDIX y *Autosensing* 10/100 Mbps para soporte de múltiples enlaces WAN/LAN
2	Puerto de consola RS-232 para administración y configuración local.
3	Dimensiones adecuadas para instalación en *Rack* 19"
4	Sistema de energía redundante para alta disponibilidad (opcional).
5	Capacidad mínima de cinco mil (5000) sesiones concurrentes.
6	Capacidad mínima de mil (1000) nuevas sesiones por segundo.
7	*Throughput* mínimo de *firewall* 400 Mbps.
8	*Throughput* mínimo de VPN (168 3DES) 50 Mbps.
9	Funcionalidad de escaneo de HTTP, SMTP, POP3, IMAP, IM, FTP y túneles encriptados VPN para protección contra VIRUS, TROYANOS, GUSANOS y ESPIAS. Estas protecciones deben estar habilitadas para su completo funcionamiento al menos 1 año a partir de la compra, con facilidad de renovación (Casos de licenciamiento). Certificación internacional al menos en Antivirus y Anti-Spyware.
10	ANTISPAM, control sobre cabeceras de e-mails y listas de direcciones IP. Esta protección debe estar habilitada para su completo funcionamiento al menos 1 año a partir de la compra, con facilidad de renovación (Casos de licenciamiento).
11	Soporte para control para aplicaciones de Mensajería Instantánea y CHATS
12	Sistema de prevención y detección de intrusos para flujos de datos desde capa 2 a capa 7 (Modelo OSI). Básicamente protección para aplicaciones y protocolos asociados con Servicios Web, transferencia de archivos, correo electrónico, multimedia, bases de datos, y sistemas operativos. Entre los principales debe incluir protección para bases de datos Oracle y Cisco IOS/ Certificación internacional.
13	Modo de operación firewall NAT, PAT (opcional), routed, transparente. Certificación Internacional en Firewall
14	Soporte para Filtrado de Contenido Web (Verificación de URL/palabras clave/bloques de frases, Listas de URL clasificadas, Bloques de Java Applets, Cookies y Active X.

15	Funcionalidad VPN: Soporte de protocolos PPTP, L2TP y IPSec, 300 túneles concurrentes mínimo, encripción DES, 3DES y AES (mínimo), soporte SSL, autenticación MD5, soporte certificados digitales (X.509 mínimo), soporte de arquitecturas LAN - LAN, Host - LAN y Host - Host, detección de estado de túnel VPN, calidad de servicio (QoS) para aplicaciones multimedia (VoIP, telefonía en los protocolos H.323 y SIP) mínimo. Certificación internacional mínimo VPN IPSec.
16	Soporte de protocolo SNMP V2 y V3, para monitoreo
17	Reportes gráficos y detallados sobre actividad maliciosa, sospechosa, estado del tráfico en cada una de las interfaces físicas y virtuales, estado operativo del equipo tanto hardware y software. Detección y notificación de falla en el dispositivo.
18	Capacidad de notificación a e-mails sobre ataques y virus.
19	Soporte de clustering en configuración Activo/Activo y Activo/Pasivo
20	Soporte VLAN estándar IEEE 802.1q
21	Soporte para IPv4, IPv6
22	Soporte de políticas basadas en enrutamiento
23	Capacidad de configuración vía WebUI(HTTPS) y Línea de comandos
24	Soporte de SSH para configuración y monitoreo.
25	Soporte de múltiples administradores y niveles de usuarios
26	Capacidad para actualizaciones y cambios via TFTP y WebUI
27	Soporte para base de datos LDAP/RADIUS (IEEE 802.1x), para autenticaciones de usuarios.
28	Soporte de Xauth sobre servidor RADIUS para VPN en IPSec, para autenticación de usuarios.
29	Soporte para *Windows Active Directory*
30	Soporte de políticas basadas en *Traffic Shaping*
31	Soporte de manejo de ancho de banda priorizado/garantizado/máximo
32	Soporte para enrutamiento dinámico con los siguientes protocolos RIP V1 y V2, OSPF y Estático
33	Capacitación certificada para operación y mantenimiento del equipo de seguridad para al menos 2 personas.

Tabla 3.12 Cuadro de especificaciones técnicas del nuevo equipo de seguridad

La *tabla 3.12* es básicamente el conjunto de requerimientos que se ha ido analizando y lo que ofrece el mercado local; con esto se puede estar seguro que al menos se tendrá tres ofertas y así poder tener alternativas para escoger la mejor opción.

3.9 COMPARACIÓN DE ALTERNATIVAS Y SELECCIÓN DEL PRODUCTO EN BASE A CRITERIOS TÉCNICO-ECONÓMICOS

Luego de la publicación e invitación al concurso para ofertar una solución de seguridad perimetral, los proveedores entregaron la documentación necesaria para participar en este concurso. Las ofertas que pasaron por el proceso de

adquisición de equipos y pudieron llegar para la revisión técnica en el Departamento de Comunicaciones y Soporte son listadas en la *tabla 3.13*.

Proveedor	**Opción 1**	**Opción 2**	**Opción 3**
EvolutioNet	Fortigate 300A	Fortigate 500A	2 equipos Fortigate 300A
Grupo Microsistemas GMS	Astaro ASG320	Astaro ASG425	
Zas Computers	Tipping Point X505		

Tabla 3.13 Cuadro de proveedores con las ofertas respectivas

Estas ofertas fueron estudiadas por el personal técnico de Comunicaciones y Redes de la E.E.Q.S.A., para determinar en base a un estudio técnico-económico la mejor opción. Solo queda verificar si estas ofertas cumplen con lo detallado en las bases del concurso. Para ello se ha realizado un cuadro comparativo en el que se verifica el cumplimento o no de cada una de las características. En la *tabla 3.14* se puede observar la comparación:

Especificaciones Técnicas del nuevo Equipo de Seguridad para la Red de Datos de la EEQ. S.A.							
Item	**Descripción de los requerimientos para el Equipo de Seguridad de la Red de Datos (Firewall + VPN + IPS).**	**EvolutioNet (op1) Fortigate 300A**	**EvolutioNet (op2) Fortigate 500A**	**EvolutioNet (op3) 2 equipos Fortigate 300A**	**Grupo microsistemas gms Astaro ASG320**	**Grupo microsistemas gms Astaro ASG425**	**Zas Computers Tipping Point X505**
1	Cinco (5) interfaces ethernet/fast-ethernet soporte Auto MDI-MDIX y Autosensing 10/100 Mbps (Número y características requeridas de los interfaces son mínimas).	2 (100/1000) y 4 (10/100)	6 (10/100) +1 SW 4p (10/100)	6 (10/100) +1 SW 4p (10/100)	4(10/100) y 4 (10/100/1000)	8 (10/100/1000)	4 (10/100) y 1 admin (10/100)
	Puerto de consola RS-232 o alternativo para administración y configuración local.	si	si	si	si 2 puertos	si 2 puertos	si
	Dimensiones adecuadas para instalación en Rack 19"	si	si	si	si	si	si
	Sistema de energía redundante para alta disponiblidad (opcional).	si	si	si	si	si	no
	Soporte de clustering en configuración Activo/Activo y Activo/Pasivo. (Opcional)	si	si	si	si	si	no
	Capacidad mínima de cinco mil (5000) sesiones concurrentes.	400000 sesiones	400000 sesiones	400000 sesiones	550000 sesiones	700000 sesiones	128000 sesiones
	Capacidad mínima de mil (1000) nuevas sesiones por segundo.	10000 sps	10000 sps	10000 sps	2000 sps	2000 sps	no especifica
	Throughput mínimo en firewall 400 Mbps.	400mbps	500mbps	500mbps	420mbps	1200mbps	no cumple 100mbps
	Throughput mínimo en VPN (128 DES) 50 Mbps	120mbps	150mbps	150mbps	200mbps	265mbps	50 mbps

	Modo de operación firewall: NAT, PAT (opcional),routed y transparente. Certificación Internacional en Firewall	si	si	si	si	si	si
	Soporte para IPv4, IPv6	si	si	si	si	si	IPv6 no cumple
	Funcionalidad de escaneo de HTTP, SMTP, POP3, IMAP, IM, FTP y túneles encriptados VPN para protección contra VIRUS, TROYANOS, GUSANOS y ESPIAS. Estas protecciones deben estar habilitadas para su completo funcionamiento al menos 1 año a partir de la compra, con facilidad de renovación (Casos de licenciamiento). Certificación internacional al menos en Antivirus.	si	si	si	si	si	si
	ANTISPAM, control sobre cabeceras de e-mails, listas de direcciones IP, análisis de archivos adjuntos, capacidad de configurar los mails detectados como spam en: cuarentena, rechazar, eliminar, alertar. Esta protección debe estar habilitada para su completo funcionamiento al menos 1 año a partir de la compra, con facilidad de renovación (Casos de licenciamiento).	si	si	si	si	si	no
	Soporte para control de aplicaciones de Mensajería Instantánea y CHATS	si	si	si	si	si	si
	Sistema de prevención y detección de intrusos (IPS) para flujos de datos desde capa 2 a capa 7 (Modelo OSI). Básicamente protección para aplicaciones y protocolos asociados con Servicios Web, transferencia de archivos, correo electrónico, multimedia, bases de datos, y sistemas operativos. Entre los principales debe incluir protección para bases de datos Oracle y Cisco IOS. Certificación internacional.	si	si	si	si	si	si
	Soporte para Filtrado de Contenido Web (Verificación de URL/palabras clave/bloques de frases, Listas de URL clasificadas, Bloques de Java Applets, Cookies y Active X). Aplicación de reglas para acceso a sitios web por direcciones IP, por redes, o por grupos de usuarios.	si	si	si	si	si	no especifica bloqueo de java applets, grupo de usuarios

	Funcionalidad VPN: Soporte de protocolos PPTP, L2TP y IPSec, VPN basado en SSL, 300 túneles concurrentes mínimo, encripción DES, 3DES y AES (mínimo), soporte SSL, autenticación MD5, soporte certificados digitales (X.509 mínimo), soporte de arquitecturas LAN - LAN, Host - LAN y Host - Host, detección de estado de tunel VPN, calidad de servicio (QoS) para aplicaciones multimedia (VoIP, telefonía en los protocolos H.323 y SIP) mínimo.	si	si	si	si	si	no soporta SSL, MD5.
	Soporte de autenticación extendida de usuarios sobre servidor RADIUS para VPN en IPSec.	si	si	si	si	si	no especifica RADIUS sobre IPsec
	Reportes gráficos y detallados en tiempo real sobre: servicios que presta el equipo como: Firewall, VPN, antivirus, antispam, tráfico en cada interface física y virtual por protocolos, aplicaciones e IPs, estado operativo del equipo, detección y notificación de falla en el dispositivo, etc. Mínimo debe cubrir estos requerimientos. (Si esto implica un software o hardware-software extra con licencia para el uso, se considera parte del equipo).	si	si	si	si	si	no especifica antispam
	Capacidad de notificación a e-mails sobre ataques y virus.	si	si	si	si	si	si
	Soporte VLAN estándar IEEE 802.1q	si	si	si	si	si	si
	Soporte para enrutamiento dinámico con los siguientes protocolos OSPF, RIP v1 y v2 (Opcional) y Estático.	si	si	si	no especifica	no especifica	si
	Soporte de políticas basadas en enrutamiento	si	si	si	si	si	si
	Soporte para base de datos LDAP/RADIUS (IEEE 802.1x), para autenticacion de usuarios.	si	si	si	si	si	si
	Soporte de perfiles de usuarios basados en IP/MAC	si	si	si	si	si	no especifica manejo de perfiles
	Soporte para Windows Active Directory	si	si	si	si	si	no especifica
	Soporte de políticas basadas en Traffic shaping para manejo de ancho de banda priorizado/garantizado/máximo. (Opcional).	si	si	si	si	si	si

	Capacidad de configuración vía WebUI(HTTPS) y Línea de comandos. Capacidad para actualizaciones y cambios via TFTP y WebUI. En caso de que se necesite un software adicional para el funcionamiento correcto de WebUI, este se debe incluir como parte del equipo.	si	si	si	si	si	si
	Soporte de SSH (se requiere versiones actualizadas a la fecha de entrega de equipo) para configuración y monitoreo. (Opcional)	si	si	si	si	si	no
	Soporte de múltiples administradores y niveles de usuarios	si	si	si	si	si	si
	Instalación, pruebas de configuración hasta completar con los requerimientos de seguridad de la red de datos de la EEQ. S.A., y puesta a punto del equipo de seguridad para su funcionamiento.	si	si	si	si	si	si
	Capacitación certificada mínimo para 2 personas de la Empresa Eléctrica Quito S.A. División de Tecnología de la Información y Comunicaciones para manejo y operación del equipo de seguridad.	2 personas certificación en Fortinet Centro o Sud América	2 personas certificación en Fortinet Centro o Sud América	2 personas certificación en Fortinet Centro o Sud América	3 personas certificación Local 10 horas	3 personas certificación Local 10 horas	2 personas certificación de 3COM
nota		INCLUYE FORTI ANALYZER FL100A	INCLUYE FORTI ANALYZER FL100A	INCLUYE FORTI ANALYZER FL100A	soporte de 300 usuarios sin licencias adicionales	soporte de 750 usuarios sin licencias adicionales	
	GARANTIA	1 AÑO	1 AÑO	1 AÑO	1 AÑO	1 AÑO	NO CUMPLE
	PRECIO (USD)	15733.76	20941.76	26292	16744	22904	12919.2

Tabla 3.14 Cuadro de calificación de las ofertas de cada proveedor

De las alternativas se puede observar que no existe proveedor que ofrezca un equipo Cisco ASA, los equipos ofertados son varias soluciones con Fortinet por parte de la firma Evolutionet, un Tipping Point por parte de la firma ZAS Computers y la solución ASTARO de la firma GSM.

La firma ZAS Computers oferta un equipo que en varios de los ítems que conforma la especificación técnica o no cumple o no la especifica o no es muy clara la información, por lo tanto no califica técnicamente.

La firma GSM oferta equipos ASTARO ASG320 y ASG425 mismos que no se especifican los protocolos de enrutamiento. Una observación al final de la oferta es el número de licencias que permite cada modelo. Este aspecto no es conveniente ya que la E.E.Q.S.A. tiene fácilmente 1000 usuarios que potencialmente usarían el acceso por medio del equipo de seguridad perimetral hacia otras redes y si se escoge a ASTARO se necesitaría más licencias y por ende mayor presupuesto.

Las opciones ofertadas por la firma Evolutionet, cumplen con los requerimientos y expectativas de seguridad de los técnicos de la E.E.Q.S.A. Una de las opciones propone dos equipos para configurarlos en modo de alta disponibilidad y las dos restantes un solo equipo de diferente modelo (FG300A y FG500A). Las tres opciones incluyen un equipo que almacena los *logs* y permite observar los reportes generados por al actividad que se genera en el Fortinet, estas opciones cumplen y califican para su análisis económico.

La firma GSM también califica con sus equipos ASTARO y Evolutionet con sus equipos Fortigate de Fortinet. Las opciones de GSM no permiten un crecimiento futuro sin que se compren licencias para equipos extras clientes. La primera opción FG300A cumple las funcionalidades de seguridad y que están contempladas en el diseño de VPNs y seguridad, la segunda opción FG500A cumple al igual que la primera y la tercera opción es la solución ideal. Por cuestiones de presupuesto es necesario recomendar la compra de la primera opción, quedando como una futura compra un equipo de similares características para implementar la funcionalidad de alta disponibilidad.

Estos resultados fueron llevados según el trámite respectivo, a la comisión que evalúa las ofertas en la E.E.Q.S.A. quien ha determinado que la oferta que califica técnicamente sea la que deba adquirirse.

El proveedor será notificado sobre este asunto para que realice el respectivo trámite y entrega del equipo en los términos del contrato.

Todo este proceso esta documentado y puesto a disposición en los anexos de este proyecto.

CAPÍTULO 4

IMPLEMENTACIÓN DE LA RED PRIVADA VIRTUAL, CONFIGURACIÓN DE EQUIPOS Y PRUEBAS DEL DISEÑO IMPLEMENTADO

4.1 INSTALACIÓN DE LOS EQUIPOS EN EL CENTRO DE CÓMPUTO

Después de la adquisición de los equipos, éstos fueron fiscalizados e instalados. Los equipos instalados son: Un equipo de seguridad perimetral UTM FG300A y un FortiAnalizer 100A, a los que se suma un *switch* Cisco Catalyst Express 500 de 24 puertos y que forman parte del equipamiento propio de la E.E.Q.S.A., dentro de las instalaciones del Centro de Cómputo de la E.E.Q.S.A.

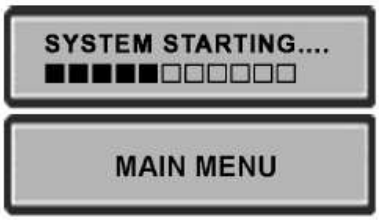


Figura 4.1 Mensajes del display al iniciar el FG300A [26]

Estos equipos han sido instalados en el *rack* 1 de Comunicaciones del Centro de Cómputo de la E.E.Q.S.A. En este mismo *rack* se encuentra el *switch* principal o de *core*.

El proceso de instalación y puesta a punto de los equipos antes mencionados, seguirá el siguiente plan:

- Iniciar el FG300A sin conexiones de red
- Acceso a la consola de configuración del FG300A y modo de operación en la red
- Asignación de funcionalidad para interfaces del FG300A

- Acceso por medio de HTTPS al FG300A
- Creación de respaldo de la configuración inicial

4.1.1 INICIAR EL FG300A SIN CONEXIONES DE RED

Una vez que el FG300A ha sido instalado en el *rack* 1 de comunicaciones, se procede a iniciarlo conectándolo a la red eléctrica y mediante el indicador que dispone en la parte frontal se podrá observar el avance de la inicialización del sistema operativo del equipo y al finalizar se desplegará el mensaje MAIN MENU (ver *figura 4.1*).

El mensaje anterior indica que el equipo está listo para ser configurado por el usuario.

4.1.2 ACCESO A LA CONSOLA DE CONFIGURACIÓN DEL FG300A Y MODO DE OPERACIÓN EN LA RED

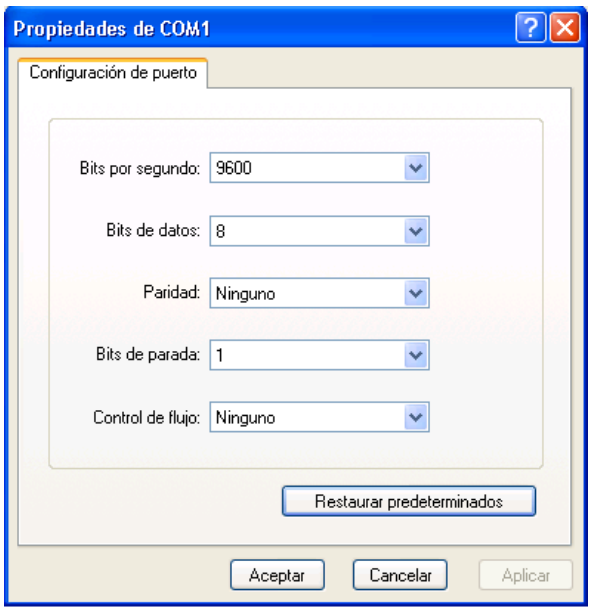


Figura 4.2 Parámetros para el acceso por consola RS-232

La primera configuración de acceso al FG300A se lo realiza a través de la consola por el puerto serial RS-232 con el cable RJ45 a DB9; del otro extremo un computador portátil es preparado para realizar la conexión por consola utilizando

la aplicación *Hyperterminal* de *Windows XP Professional* donde los parámetros de configuración del *Hyperterminal* para la conexión con el FG300A son como lo indica la *figura 4.2*.

Al ingresar al sistema operativo a través de la consola, el FG300A solicita un nombre de usuario y luego la contraseña correspondiente como lo muestra la *figura 4.3*. El nombre de usuario es *admin* y no tiene contraseña.

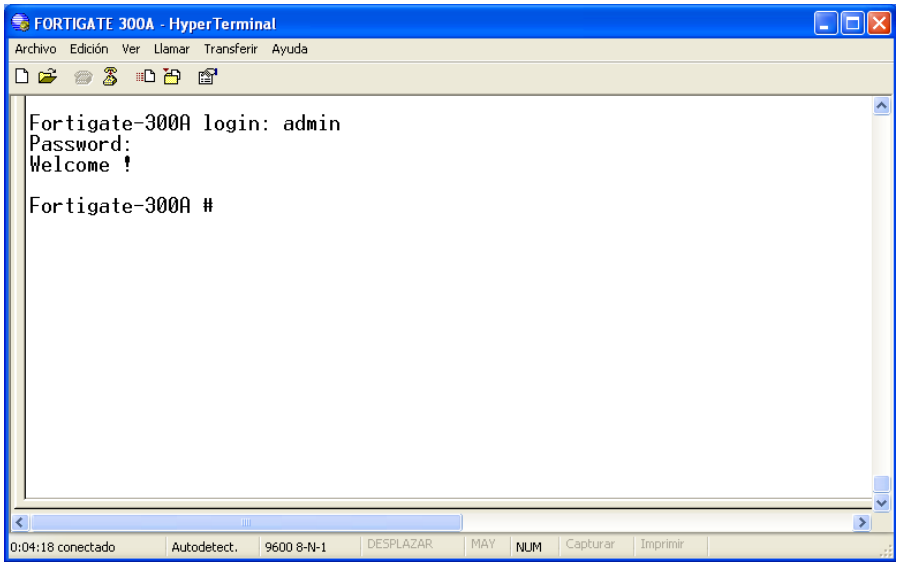


Figura 4.3 Ingreso a la consola de configuración a través de RS-232

El FG300A tiene una configuración inicial de fábrica, esta configuración incluye el modo de operación de la red, que para el modelo FG300A está fijado en NAT/Route, esto implica que cada interfaz es un segmento de red diferente. La *figura 4.4*. muestra un cuadro donde detalla el nombre de usuario y contraseña de la cuenta de administrador, los valores de cada interfaz, un puerto de sugerencia para la red externa y direcciones DNS.

Las configuraciones y funcionalidades que por defecto tiene el FG300A serán cambiadas según el diseño de la *figura 3.33* donde se ha designado la funcionalidad, principalmente de cada una de la interfaces y estos cambios también obedecerán a la configuración de red de la E.E.Q.S.A.

Administrator account	User name: Password:	admin (none)
Port 1	IP: Netmask: Administrative Access:	192.168.1.99 255.255.255.0 HTTPS, Ping
Port 2	IP: Netmask: Administrative Access:	192.168.100.99 255.255.255.0 Ping
Port 3	IP: Netmask: Administrative Access:	0.0.0.0 0.0.0.0 Ping
Port 4	IP: Netmask: Administrative Access:	10.10.10.1 0.0.0.0 HTTPS, Ping
Port 5	IP: Netmask: Administrative Access:	0.0.0.0 0.0.0.0 Ping
Port 6	IP: Netmask: Administrative Access:	0.0.0.0 0.0.0.0 Ping
Network Settings	Default Gateway (for default route)	192.168.100.1
	Interface connected to external network (for default route)	port2
	Default Route A default route consists of a default gateway and the name of the interface connected to the external network (usually the Internet). The default gateway directs all non-local traffic to this interface and to the external network.	
	Primary DNS Server	207.192.200.1
	Secondary DNS Server	207.192.200.129

Figura 4.4 Valores de la configuración por defecto de los puertos en el modo de red NAT/Route del FG300A [26]

Si el modo de operación se lo cambia a transparente los parámetros de red de las interfaces cambian a valores de fábrica pero exclusivos para este modo de operación. La *figura 4.5* muestra los valores de fábrica de las interfaces del FG300A para este modo de operación.

Administrator account	User name: Password:	admin (none)
Management IP	IP: Netmask:	10.10.10.1 255.255.255.0
DNS	Primary DNS Server: Secondary DNS Server:	207.194.200.1 207.194.200.129
Administrative access	Port 1 Port 2 Port 3 Port 4 Port 5 Port 6	HTTPS, Ping Ping Ping HTTPS, Ping Ping Ping

Figura 4.5 Valores de la configuración por defecto de los puertos en el modo de red Transparente del FG300A [26]

Una vez que se ha autenticado correctamente se procede a mostrar en pantalla el estado de operación actual del FG300A con el comando ***get system status***.

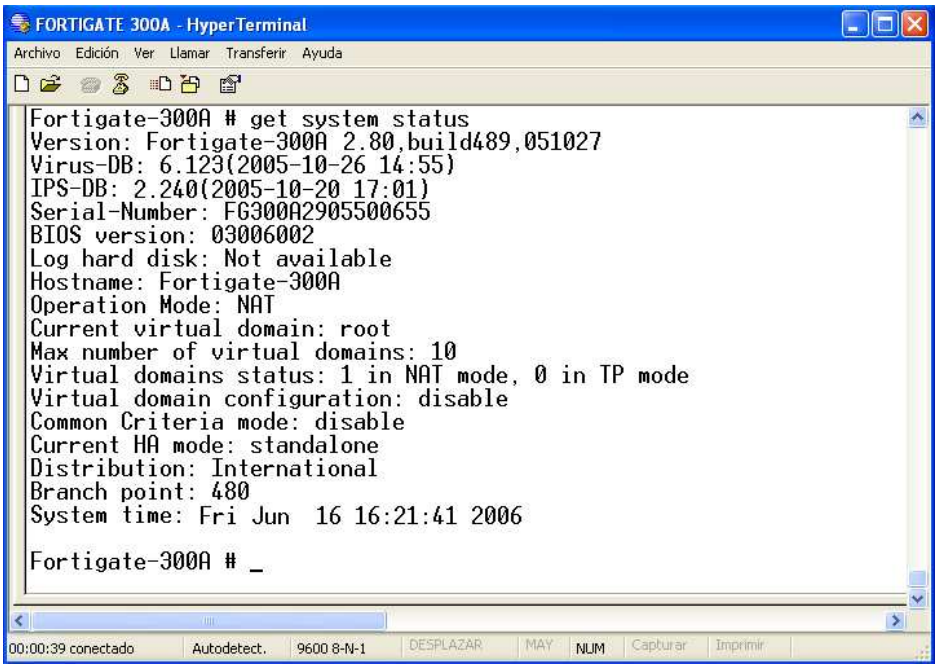


Figura 4.6 Estado actual del sistema del FG300A

La *figura 4.6* permite mostrar información que corresponde a las versiones del sistema operativo, base de datos del antivirus, base de datos del IPS, del BIOS; nombre por defecto del equipo y sobre todo el modo de operación que está fijado en NAT.

4.1.3 ASIGNACIÓN DE FUNCIONALIDAD PARA INTERFACES DEL FG300A

En el modo NAT se podrá dar funcionalidad diferente a cada interfaz, para lo cual se ha establecido las siguientes funcionalidades antes de proceder a la configuración definitiva.

Como antecedente hay que recordar que el *switch* principal tiene configurado varias VLANs. La VLAN con identificador 7 y etiqueta RED_EXTERNA tiene a los 4 primeros puertos *Fast Ethernet* de este *switch* en esta VLAN. El puerto 2 del *switch* principal se conecta al *router* del proveedor.

Las funcionalidades estarán acordes al diseño desarrollado y mostrado en la *figura 3.33*. A continuación se enumeran las funcionalidades de cada interfaz del FG300A:

- ***Puerto 1***. Acceso a Internet por medio del segmento de red correspondiente a la VLAN 7 del *switch* principal. Este puerto se conectará al puerto 4 que es parte de la VLAN 7. El direccionamiento IP que se le asignará es 200.93.231.242 / 28 la puerta de enlace es 200.93.231.241. Al ser este puerto la entrada y salida a una red insegura no se habilitará ningún tipo de acceso para administración del equipo.

- ***Puerto 2***. Corresponde a la DMZ, específicamente está conectado el servidor Web de la E.E.Q.S.A. y al servidor de correo externo de la E.E.Q.S.A. Este segmento tiene como dirección de red la 192.168.21.0 / 24 y se configurará la misma dirección que estuvo en el puerto correspondiente del *firewall IBM Secure Way*, es decir la dirección 192.168.21.10 / 24. Para control de tráfico de red se le habilitará el protocolo SNMP.

- ***Puerto 3***. Este puerto será el acceso para las redes externas hacia la red corporativa de la E.E.Q.S.A. Por lo tanto este puerto estará conectado a un puerto del *switch* principal que esté en la VLAN con identificador 1 y etiqueta *default*; así mismo se le asignará la dirección IP que tenía el *IBM SecureWay Firewall* en la correspondiente interfaz. Dirección 132.147.160.34 / 22 puerta de enlace 132.147.161.20. Este puerto es parte de la red interna y al ser la puerta de enlace hacia las redes externas es necesario acceder a la administración, por lo tanto se permitirá el acceso a través de HTTPS, SSH y para el monitoreo del tráfico en la red se permitirá habilitar el PING y el protocolo de gestión de red SNMP.

- ***Puerto 4***. Este puerto tendrá la funcionalidad de conectar las redes externas corporativas y de servicio a la red corporativa de la E.E.Q.S.A. El

diseño de este proyecto para este acceso indica que se requiere un *switch* capa 2 que soporte IEEE 802.1q para configurar VLANs y un enlace de *trunk* entre el FG300A y el *switch* mencionado. Para no desconectar el acceso a las redes externas se mantendrá provisionalmente el *switch* original y progresivamente en coordinación con las empresas externas se migrará cada enlace al nuevo *switch* que está listo para la nueva configuración. Se le asigna la dirección 192.168.2.1 / 24 que tenía el puerto correspondiente en el *IBM SecureWay Firewall.* Para control de tráfico de red se le habilitará el PING y el protocolo SNMP.

– ***Puerto 5***. Para uso futuro.

– ***Puerto 6***. Para uso futuro.

En la *figura 4.7* se puede observar los segmentos de red conectados al FG300A con las funcionalidades y parámetros antes especificados.

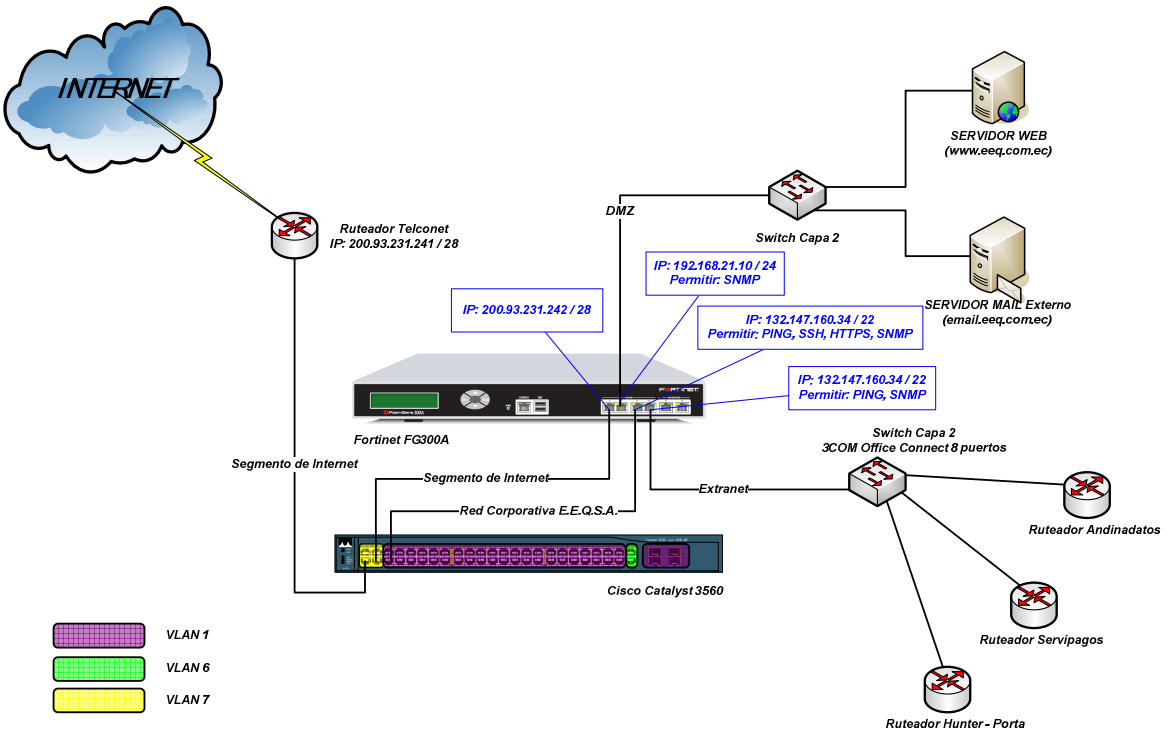


Figura 4.7 Diagrama de red con el equipo de seguridad perimetral

Para realizar la configuración en un determinado puerto se hará la demostración con el puerto 3 asignando cada uno de los parámetros de red que corresponden a este puerto (Ver *figura 4.8*).

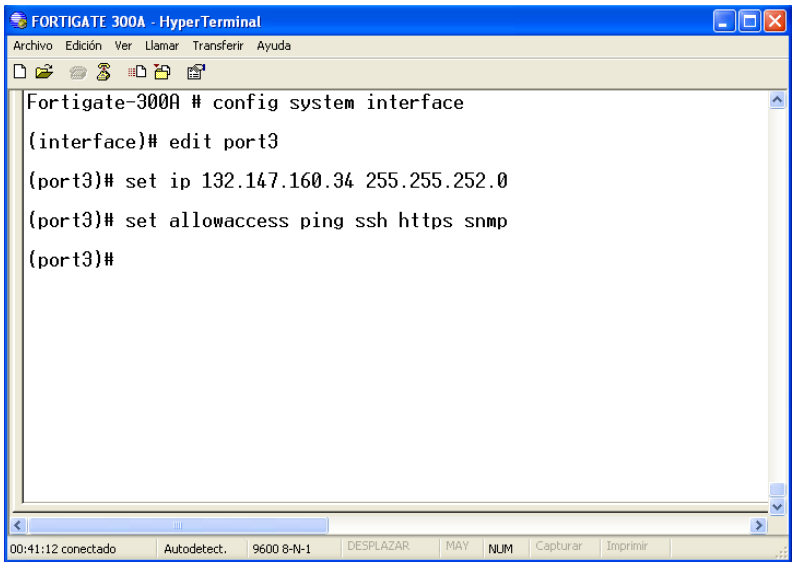


Figura 4.8 Configuración del puerto 3 del FG300A

El procedimiento mostrado en la *figura 4.8* se aplica a todos los puertos con sus respectivos parámetros. En la *figura 4.9* se puede observar el comando que se ejecuta para poder ver la configuración de los puertos del FG300A.

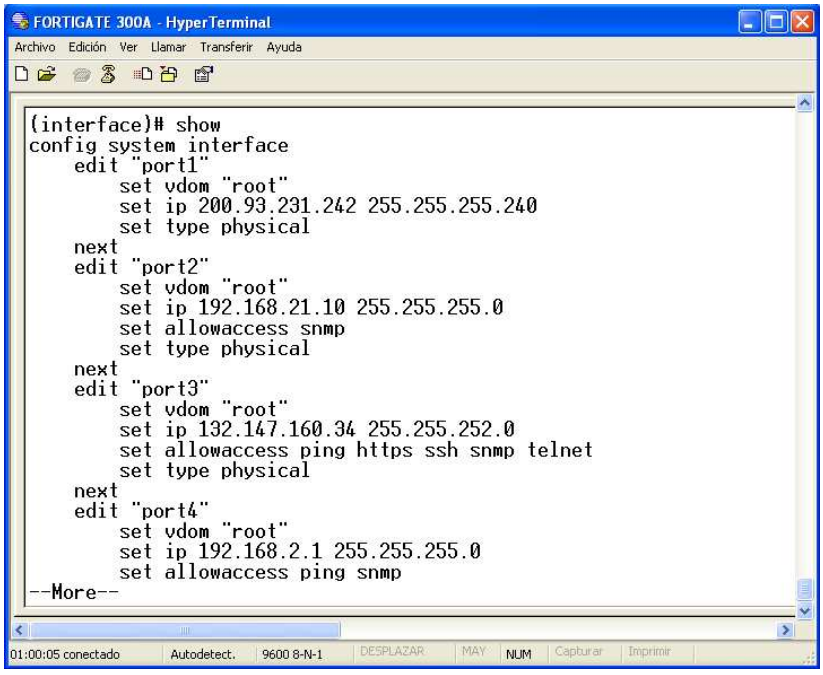


Figura 4.9 Configuración de los puertos del FG300A

4.1.4 ACCESO POR MEDIO DE HTTPS AL FG300A

El protocolo *Hypertext Transfer Protocol Secure* o HTTPS, por ofrecer una conexión segura entre un *host* y el FG300A y la ventaja de ofrecer un ambiente de trabajo amigable para la configuración del FG300A, se ha considerado como el principal método de acceso para tales fines.

Para acceder por medio de este protocolo se necesita ejecutar sobre un navegador de sitios web como Internet Explorer 7 o Mozilla Firefox 2.0.15, en la barra de direcciones escribir la dirección **https://132.147.160.34** y luego presionar el botón ENTER. Al instante el navegador web emite mensajes de error asociados al certificado de seguridad. Al ser un sitio web generado por el FG300A se trata de un sitio de confianza además que los únicos equipos que intervienen en esta sesión HTTPS son el FG300A a través del puerto 3 y un computador de escritorio por medio de su interfaz Ethernet, por lo tanto no existe riesgo de ningún tipo al acceder por medio del hipervínculo *Vaya a este sitio web (no recomendado)* que tiene el ícono de un escudo rojo (Ver *figura 4.10*). De inmediato aparecerá la página para la autenticación de un usuario que desee ingresar a la consola de configuración del FG300A, tal como se lo puede apreciar en la *figura 4.11*.

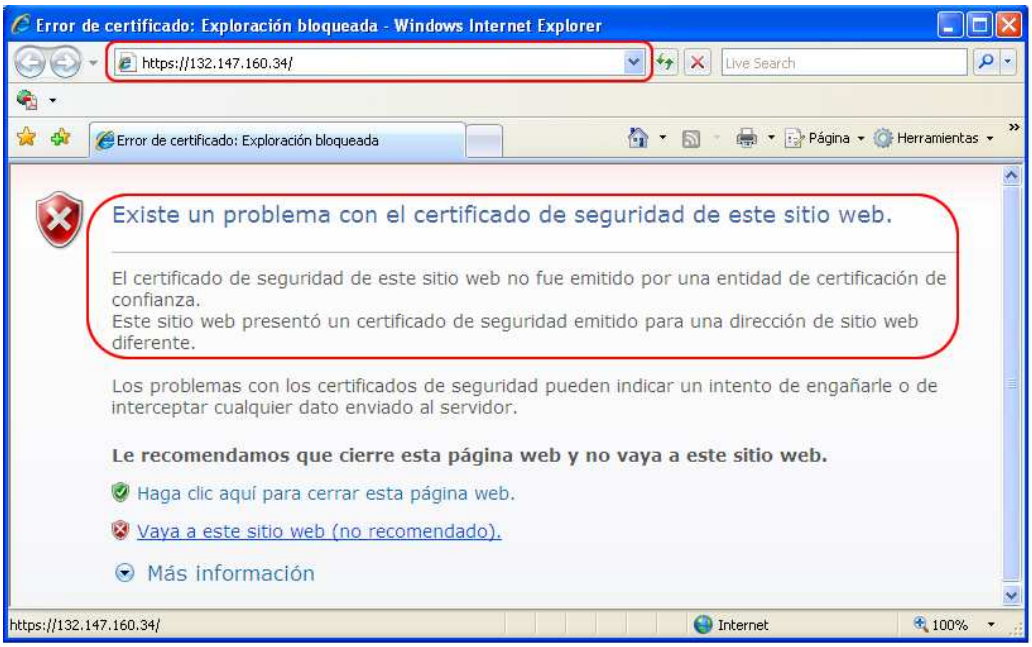


Figura 4.10 Errores de Certificado de Seguridad antes de ingresar a la consola del FG300A

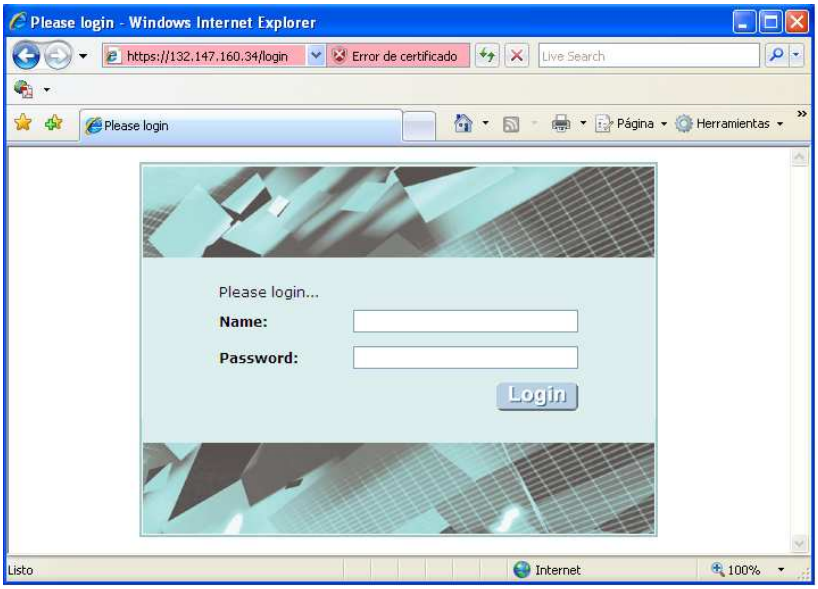


Figura 4.11 Página para la autenticación del usuario

El nombre de usuario a utilizarse durante el proceso configuración de los parámetros de red y seguridad será *admin*; la contraseña no se la configurará hasta terminar con la puesta a punto, la última configuración será la contraseña. Con HTTPS se realizará la mayoría de configuraciones, si este modo no soporta algún tipo de configuración se procederá a realizarlo a través de SSH que utiliza los mismos comandos que en el acceso a la consola por medio de la conexión serial RS-232.

4.1.5 CREACIÓN DE RESPALDO DE LA CONFIGURACIÓN INICIAL

Las configuraciones se almacenan localmente en el FG300A pero si el sistema falla o por accidente de quien manipula el equipo borra la configuración personalizada, es importante que se cree un respaldo cada vez que se realiza un cambio en la configuración.

El FG300A no entrará directamente a operar en modo NAT/Route ya que primero se lo instalará entre el *IBM SecureWay Firewall* y la red corporativa en el modo de operación transparente, con el fin de analizar la actividad de tráfico para determinar el momento propicio para el cambio de equipo.

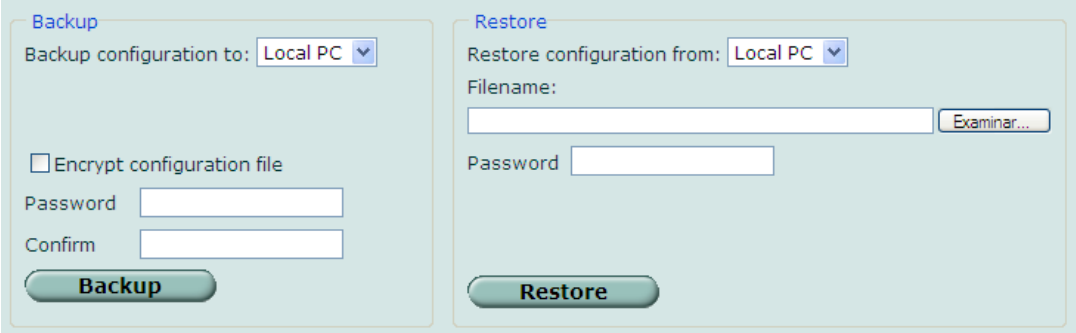


Figura 4.12 Respaldo y restauración de la configuración del FG300A

Para respaldar la configuración se ingresa al equipo por medio de HTTPS y desde el menú principal que se localiza en la parte izquierda de la página se sigue el camino ***System → Maintenance → Backup & Restore*** donde se tienen las opciones de *Backup* en la parte izquierda y *Restore* en la parte derecha de la página (Ver *figura 4.12*). En la opción *Backup* se tiene un botón del mismo nombre que al presionarlo genera una ventana indicando que el usuario desea descargar desde el FG300A un archivo con el nombre ***fg_system.conf***. Este archivo contiene la configuración con el último cambio realizado el cual debe ser almacenado en algún directorio del equipo que solicita guardar tal configuración. El proceso para la restauración es similar al proceso de adjuntar un archivo a un correo electrónico y esto se lo realiza desde la opción ***Restore*** de la misma página (Ver *figura 4.13*).

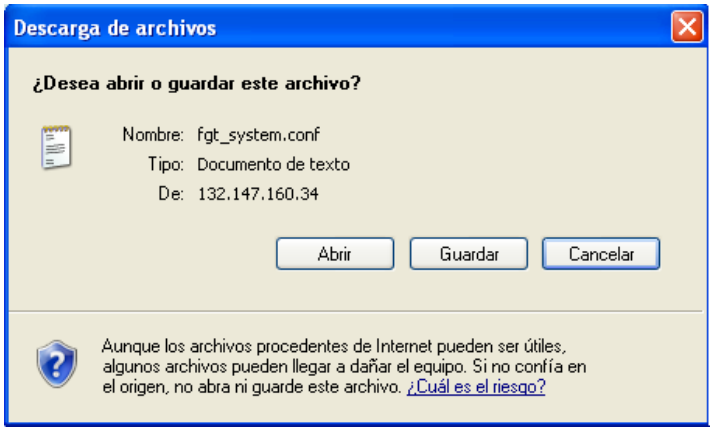


Figura 4.13 Descarga del archivo de configuración desde el FG300A

El método de respaldo y restauración de la configuración que se utilizará en este proyecto será a través de un computador conectado por medio de la red, ya que

existen otras formas de realizar el respaldo, como son por medio de USB y línea de comandos CLI desde un archivo de texto.

4.2 PRUEBAS PREVIAS DE SEGURIDAD PARA EL TRÁFICO DE DATOS, VPNs Y VoIP

Estas pruebas corresponden a la instalación y configuración del equipo de seguridad perimetral en modo transparente para establecer la funcionalidad adecuada del equipo. Aquí lo que se hace es seguir las instrucciones del fabricante, que por medio de la documentación que viene junto al equipo y que indica cómo debe hacerse la inicialización del FG300A antes de entrar a las configuraciones personalizadas para la E.E.Q.S.A.

Al ingresar al equipo FG300A en el modo de configuración *web*, para activar el modo de operación Transparente, se de acceder al menú principal y navegar por las opciones ***System → Config → Operation*;** una vez ingresado a la opción ***Operation*** se tiene disponible dentro de una lista, dos opciones de operación que son: ***NAT*** y ***Transparent***. Se selecciona el modo ***Transparent*** y luego para activar o aplicar esta configuración se presiona el botón ***Apply*** (Ver *figura 4.14*)**.**

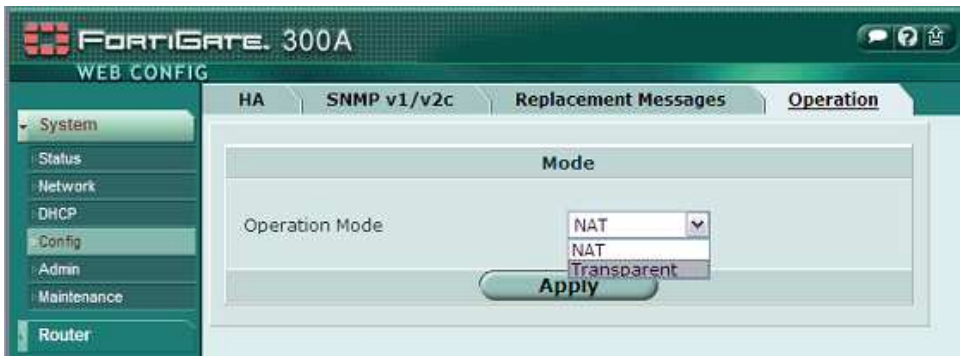


Figura 4.14 Selección del modo de operación

Una vez terminada esta configuración se puede regresar a la opción **Status** del menú ***System***, y verificar que el cambio ha sido aplicado (Ver *figura 4.16*). Cuando se realiza este cambio es necesario configurar una dirección IP diferente para la administración del equipo a través de la red. Como la dirección IP 132.147.160.34 estará en uso se cambia a la dirección IP 132.147.163.249 que

está disponible y pertenece a la misma red para acceder a través de un computador de la E.E.Q.S.A. a la consola. Siguiendo el mismo procedimiento para asignar una dirección IP mostrado en la *figura 4.8* se cambia la dirección.

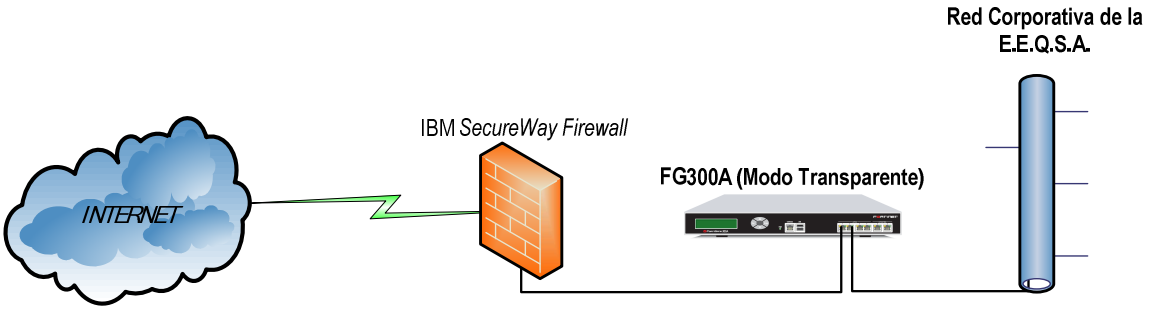


Figura 4.15 Diagrama de la topología para el modo de operación Transparente

La *figura 4.15* permite observar la topología donde el FG300A se ubica en el medio del *firewall* activo y la red corporativa de la E.E.Q.S.A. El modo transparente del FG300A le permite aparentar que está oculto para los segmentos de red que éste conecta; en este caso permanecerá oculto para la red corporativa y el IBM *SecureWay Firewall* ya que se encuentra en medio de los dos elementos de la topología y a la vez registrará entre otros parámetros, el número de sesiones y utilización de la red; estos datos ayudarán a verificar el momento propicio para realizar el cambio de equipo.

Cabe indicar que el momento propicio se refiere a un número bajo de sesiones, que podría ser entre 10 y 50 sesiones concurrentes y que estas sesiones generen un tráfico de red cercano no mayor a 50 kbps, esto indicará que el impacto de la desconexión hacia el Internet será mínima. Sin embargo será necesario informar a través de correo electrónico a todo el personal que tiene permiso para acceder al Internet, que en determinada fecha y hora se suspenderá el servicio y que esta suspensión no será mayor a 1 hora, que es el tiempo estimado para activar y poner en funcionamiento el nuevo equipo de seguridad perimetral FG300A.

Por experiencia por parte del personal del Departamento de Administración de Sistemas y Bases de datos y del Departamento de Comunicaciones y Soporte de la E.E.Q.S.A., indican que los días viernes luego de la jornada de labores es decir

después de las 15h30, el flujo de tráfico en todos los segmentos de red es muy bajo.

Figura 4.16 Verificación del modo de operación

Según la información recopilada, en esos días y luego de la jornada de labores se pueden realizar descargas de archivos que están alrededor de los 100 MB de tamaño en disco en menos de 10 minutos, lo que indica que el acceso y el tráfico de red corporativo es muy bajo; por lo tanto el cambio de equipos se lo realizará un día viernes a partir de la 18h00. La *figura 4.17* muestra la sección ***System Status*** que su parámetro ***System Time*** indica que es un viernes con 18h31, día y hora apropiada para el cambio.

Antes de realizar el cambio es necesario confirmar que la utilización del acceso a Internet sea el apropiado. En las *figuras 4.17* y *4.18* se puede observar el número de sesiones, la utilización de la red y el detalle de las sesiones que en el instante de la visualización por medio del acceso *web* están activos.

Como se observa el número de sesiones llega a 25 y la utilización está en 3 kbps, con lo cual se indica que es el momento propicio para el cambio de equipos.

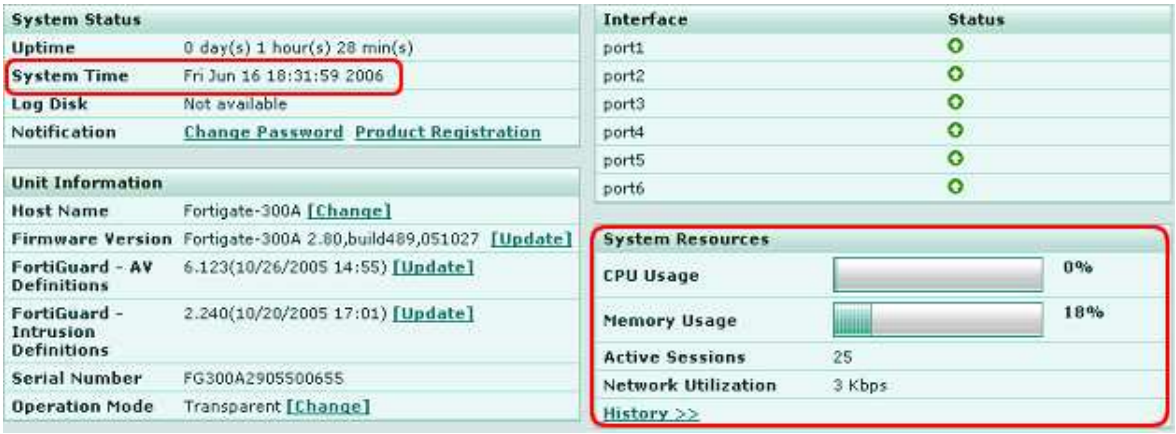


Figura 4.17 Visualización de parámetros que corresponden al estado del equipo

A más de confirmar el bajo número de sesiones y de utilización de la red, se puede observar en la misma *figura 4.17* el uso del CPU y memoria del FG300A, en el que se observa un consumo muy bajo de estos recursos. Este consumo de recursos computaciones irá aumentado a medida que se vaya agregando funcionalidades.

Protocol	From IP	From Port	To IP	To Port	Expire(secs)	Policy ID
udp	132.147.161.147	1029	193.0.14.129	53	82	4
udp	132.147.161.147	1029	202.12.27.33	53	86	4
tcp	132.147.162.23	3901	132.147.163.249	443	97	
tcp	132.147.162.23	3885	132.147.163.249	443	71	
udp	132.147.161.147	1029	198.32.64.12	53	82	4
udp	132.147.160.158	37165	192.58.128.30	53	168	2
udp	132.147.161.147	1029	192.36.148.17	53	86	4
udp	132.147.160.4	1050	192.58.128.30	53	75	4
udp	132.147.160.158	37165	128.63.2.53	53	177	2
udp	132.147.160.4	1050	198.41.0.4	53	82	4
udp	132.147.160.4	1050	192.33.4.12	53	82	4
udp	127.0.0.1	1026	127.0.0.1	53	178	
udp	132.147.160.158	37165	198.41.0.4	53	172	2
udp	132.147.160.158	37165	192.5.5.241	53	171	2
udp	132.147.160.158	37165	192.33.4.12	53	175	2
tcp	172.16.25.57	3046	132.147.160.158	80	45	
tcp	172.16.25.57	3048	132.147.160.158	80	56	
udp	132.147.161.147	1029	192.203.230.10	53	75	4
udp	132.147.160.4	1050	128.9.0.107	53	82	4
tcp	132.147.162.23	3902	132.147.163.249	443	102	

Figura 4.18 Listado de sesiones que están activos

En la *figura 4.18* se indica por medio de recuadros rojos las sesiones que mantiene el equipo con el cual se está realizando la configuración del FG300A, donde se puede también apreciar el puerto TCP 443 que está activo en el FG300A para la administración. La columna ***Policy ID*** muestra el identificador de la política del IBM *SecureWay Firewall* asignada al flujo de tráfico de la fila.

Con esta información y con la configuración inicial del equipo se ha podido observar que el equipo está listo para realizar la configuración y migración del *firewall* antiguo al nuevo. Por lo tanto se regresa al modo de operación *NAT/Route* y se restaura la configuración almacenada el computador del usuario administrador.

En lo que corresponde a la migración, se han revisado las opciones que manejan ambos sistemas, sobre todo en lo que corresponde a compatibilidad de archivos. Al no encontrar formas de trasladar ficheros de configuración del *firewall* antiguo al equipo de seguridad nuevo, cada una de las configuraciones se las realizará de manera manual. En la sección 4.3 se detalla estas y otras configuraciones del equipo de seguridad perimetral.

4.3 CONFIGURACIÓN DEL SISTEMA DE SEGURIDAD INTEGRAL DE DATOS

Esta configuración implica una serie de criterios y un adecuado conocimiento del *software* que permite administrar este equipo de seguridad así como también conocimiento en Redes de Comunicaciones de Datos y una lógica que llevará a cabo toda la configuración de seguridad como: políticas del *firewall* para el acceso, protección y/o denegación hacia recursos de la red corporativa, usuarios y grupos de usuarios, redes privadas virtuales, etc.

Se ha elaborado un plan de configuración el cual se describe a continuación:

- Descripción del ambiente de acceso a la consola por medio de HTTP/HTTPS
- Configuración de redes y enrutamiento

- Configuración de usuarios y grupos de usuarios
- Configuración de seguridad

4.3.1 DESCRIPCIÓN DEL AMBIENTE DE ACCESO A LA CONSOLA POR MEDIO DE HTTP/HTTPS

El acceso a la consola de configuración por medio de HTTPS, permite un ambiente de trabajo amigable e intuitivo para un técnico con conocimientos en Seguridad en Redes, Redes WAN y LAN. Sin embargo no está por demás realizar una breve descripción de este ambiente de configuración del FG300A lo que ayudará a entender de mejor manera las *figuras* que se presentarán en esta sección.

En la *figura 4.19* se muestra el ambiente de configuración; en el caso de la *figura 4.19* la consola muestra el estado de configuración de rutas estáticas para la opción ***Router***. Para llegar a esta y otras opciones se debe indicar que este ambiente tiene 4 áreas principales de navegación y que están debidamente indicadas en la *figura 4.19*.

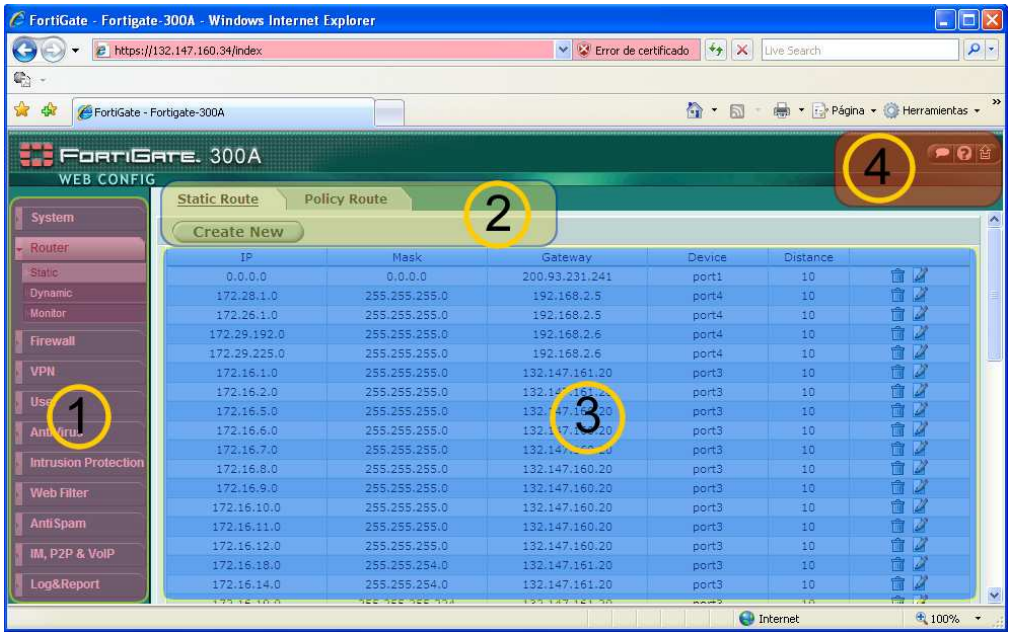


Figura 4.19 Ambiente de administración y configuración en HTTPS del FG300A

El área marcada con el número 1 contiene el menú principal de opciones y cada opción contiene un submenú. El menú principal solo tiene dos niveles. Las opciones que tiene este menú son:

- *System*
- *Router*
- *Firewall*
- *VPN*
- *User*
- *Antivirus*
- *Intrusion Protection*
- *Web Filter*
- *Anti Spam*
- *IM, P2P & VoIP*
- *Log&Report*

El área marcada con el número 2 presentará una o varias pestañas según la opción escogida en el menú principal. A estas pestañas es posible que le acompañe uno o varios botones para agregar o crear determinada función o elemento.

El área marcada con el número 3 desplegará el campo de trabajo e información, es decir que en esta área estarán a disposición y según la opción del menú principal, formularios de configuración, información de configuraciones realizadas, estado del equipo, etc.; para el desarrollo de la configuración del FG300A, esta área será en la que se trabajará la mayor parte del tiempo.

El área marcada con el número 4 tiene 3 opciones que tienen la función de: contactar con un agente de servicio de Fortinet, la segunda para acceder al soporte de ayuda en línea sobre una determinada funcionalidad y la tercera para salir de la consola de configuración.

Para indicar la forma de llegar a determinada configuración en la consola, se utilizará el siguiente convenio tomando como ejemplo la *figura 4.19*: La primera palabra indicará la opción del menú principal; si se encuentra la opción escogida en el siguiente nivel esta palabra estará antecedida de una flecha con dirección a la derecha. Cualquiera que sea el nivel donde se encuentre y la opción escogida se encuentra en una pestaña, la palabra que indique esta opción estará antecedida de una flecha en doble sentido, así para indicar la localización de lo que se observa en el área de trabajo 3 de la *figura 4.19* se le debe indicar de la siguiente manera:

Router → Static ↔ Static Route

Así la palabra ***Router*** indica la opción del menú principal, ***Static*** la opción del submenú de ***Router*** y ***Static Route*** es una pestaña de la opción ***Static***.

4.3.2 CONFIGURACIÓN DE REDES Y ENRUTAMIENTO

La primera configuración corresponde a las redes y enrutamiento, para tal efecto se necesita que todas las interfaces estén bien configuradas y habilitadas para recibir y enviar tráfico entre segmentos de red.

4.3.2.1 Visualización de la configuración y estado de los puertos de red

Los parámetros en los puertos de red, se configuraron inicialmente con la consola a través de la conexión serial RS-232, sin embargo es pertinente indicar la pantalla que permite realizar la misma configuración pero a través de la consola en el modo acceso HTTPS (Ver *figura 4.20*). Para mostrar la configuración actual de todas las interfaces es preciso ir a ***System → Network ↔ Interface***.

Name	IP / Netmask	Access	Status	
port1	200.93.231.242 / 255.255.255.240		Bring Down	
port2	192.168.21.10 / 255.255.255.0	SNMP	Bring Down	
port3	132.147.160.34 / 255.255.252.0	HTTPS,PING,SSH,SNMP	Bring Down	
port4	192.168.2.1 / 255.255.255.0	PING,SNMP	Bring Down	
port5	/	HTTPS,PING,SNMP	Bring Up	
port6	/	HTTPS,PING,SNMP	Bring Up	

Figura 4.20 Configuración y estado de todos los puertos de red

Dentro de la pestaña se puede acceder a la configuración del puerto 3 dando un *click* en el ícono de edición correspondiente**.** Dentro de la edición de la interfaz se incluye información respecto a la dirección física o MAC-*Address* y que se muestra en la *figura 4.20*.

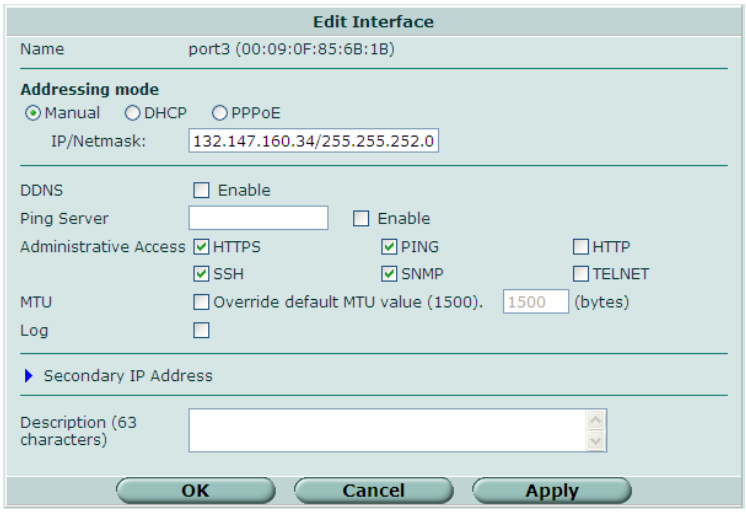


Figura 4.21 Configuración del puerto o interfaz 3 (Red Corporativa)

El estado actual de las interfaces mostrado en la *figura 4.20* indica que las 4 primeras interfaces están activas y en funcionamiento mientras que las interfaces 5 y 6 están en estado *down* o sin conexión.

4.3.2.2 Creación de rutas y visualización de rutas estáticas

En esta instancia se realizará la migración de manera manual de las redes que estaban configuradas en el *IBM SecureWay Firewall*. Las redes para poder interconectarse deben estar declaradas en el FG300A y tener una ruta de acceso. Para el caso particular de la E.E.Q.S.A. el enrutamiento se lo hace de manera estática debido a que cada enlace tiene una puerta de enlace predeterminada.

Para ingresar una nueva ruta estática se debe ingresar a ***Router → Static ↔ Static Route*** y hacer un *click* en el botón ***Create New***, esto hará aparecer una página donde permitirá ingresar una nueva red, la máscara, el puerto de acceso, la puerta de enlace para esa red y el número de saltos o distancia que necesita

esa red para llegar al FG300A (Ver *figura 4.22*). La ruta ingresada y otras pueden ser observadas en la lista de rutas estáticas que se muestra en la *figura 4.23* luego haber ingresado la ruta de la *figura 4.22*.

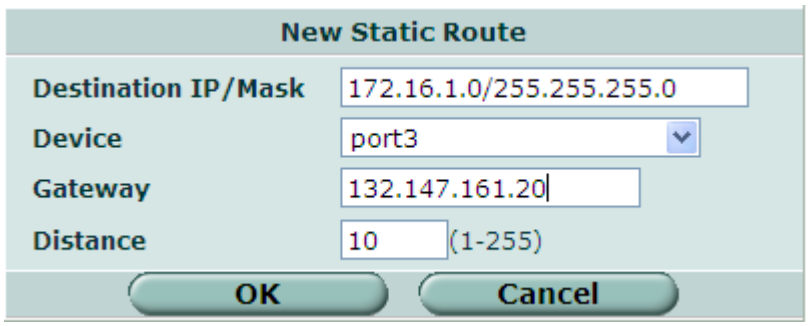
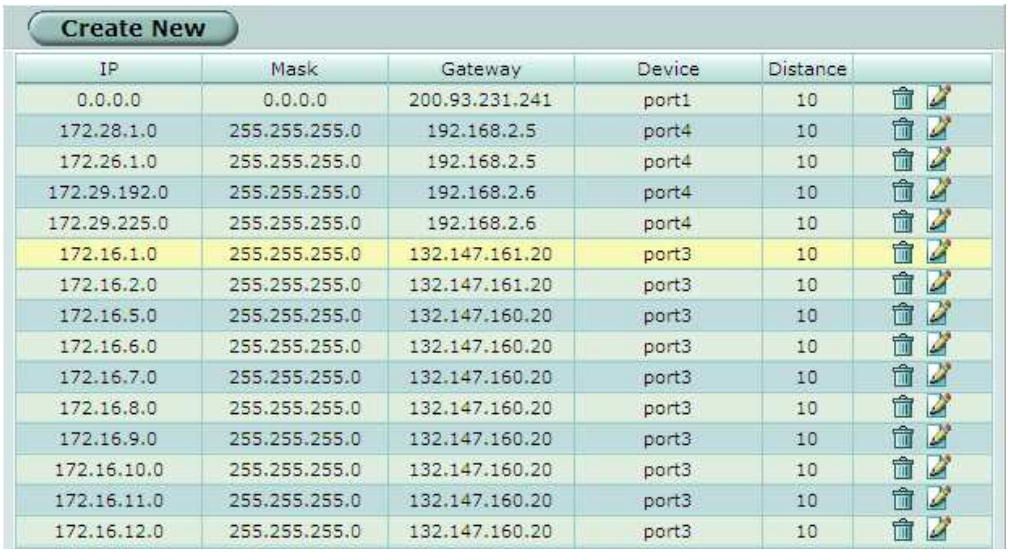


Figura 4.22 Ingreso de una nueva ruta estática

Si una ruta está mal configurada o se han realizado cambios en un determinado enlace, es posible borrar la ruta o modificar los parámetros accediendo por medio de los *links* representados por un ícono con la imagen de un bote de basura para "borrar" o el ícono con la imagen de un papel y lápiz para la "edición".



IP	Mask	Gateway	Device	Distance
0.0.0.0	0.0.0.0	200.93.231.241	port1	10
172.28.1.0	255.255.255.0	192.168.2.5	port4	10
172.26.1.0	255.255.255.0	192.168.2.5	port4	10
172.29.192.0	255.255.255.0	192.168.2.6	port4	10
172.29.225.0	255.255.255.0	192.168.2.6	port4	10
172.16.1.0	255.255.255.0	132.147.161.20	port3	10
172.16.2.0	255.255.255.0	132.147.161.20	port3	10
172.16.5.0	255.255.255.0	132.147.160.20	port3	10
172.16.6.0	255.255.255.0	132.147.160.20	port3	10
172.16.7.0	255.255.255.0	132.147.160.20	port3	10
172.16.8.0	255.255.255.0	132.147.160.20	port3	10
172.16.9.0	255.255.255.0	132.147.160.20	port3	10
172.16.10.0	255.255.255.0	132.147.160.20	port3	10
172.16.11.0	255.255.255.0	132.147.160.20	port3	10
172.16.12.0	255.255.255.0	132.147.160.20	port3	10

Figura 4.23 Listado de rutas estáticas

4.3.3 CONFIGURACIÓN DE USUARIOS Y GRUPOS DE USUARIOS

En esta sección se define los usuarios que van acceder al servicio de Internet, es decir cómo van a ser creados o desde qué base de información se va a recoger

los nombres de usuarios y contraseñas, así como también las técnicas de protección que se empleará para proteger esta información.

Dentro de esta configuración se tienen algunas opciones que las puede ver en la *figura 4.24*.

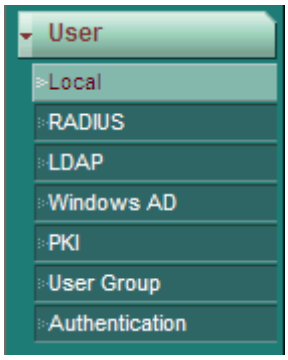


Figura 4.24 Menú de la opción User

Como opciones se tienen varias alternativas; para el propósito de este proyecto se ha considerado por razones de factibilidad y cumplimiento de normas de seguridad las opciones ***Local***, ***RADIUS*** y ***User Group***.

4.3.3.1 Configuración de usuarios Locales

Los usuarios tipo locales son aquellos que residen en la memoria o disco duro del FG300A, que tiene capacidad de almacenar alrededor de 1000 nombres de usuarios y contraseñas. El equipo almacenará todos los usuarios que necesiten acceder a una red externa como el Internet.

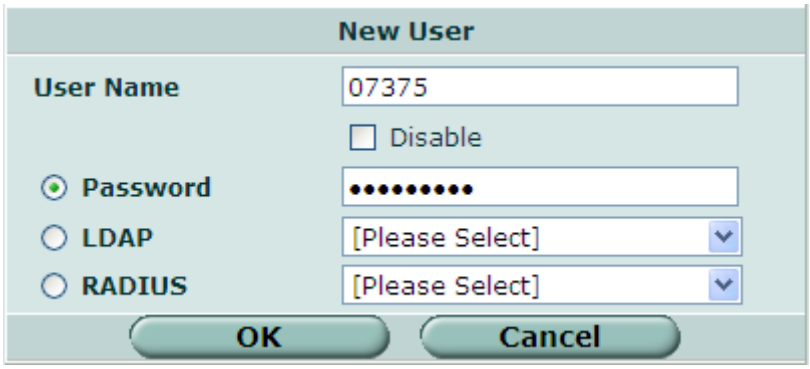


Figura 4.25 Ingreso de nuevo usuario Local

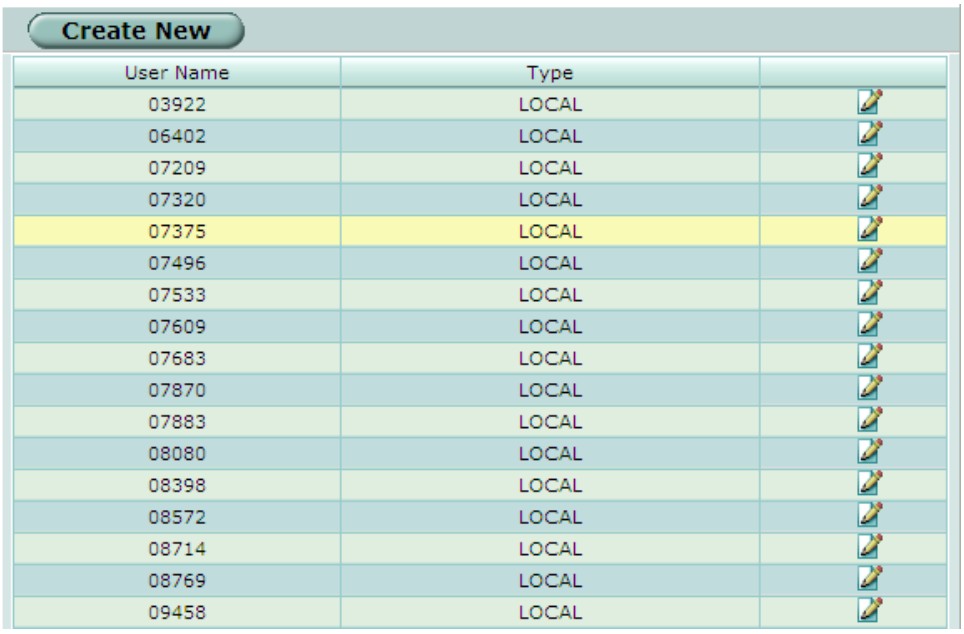


Figura 4.26 Lista de usuarios locales

Para ingresar un nuevo usuario local se debe ingresar a ***User → Local ↔ Local Route*** y en el botón ***Create New*** hacer un *click* y aparecerá una página donde se podrá ingresar el nombre de usuario y la contraseña; para que esta cuenta de usuario sea considerado como local se debe obviar las opciones ***LDAP*** y ***RADIUS*** (Ver *figura 4.25*).

Al hacer un *click* en el botón ***OK*** de la *figura 4.25* el nuevo usuario se añadirá a la base de datos de usuarios locales del FG300A. En la *figura 4.26* se puede observar una parte de lista de usuarios y se resalta el último ingreso.

4.3.3.2 Configuración de usuarios RADIUS

En la *figura 4.25* se aprecia que el usuario de tipo local necesita configurar una contraseña. Si se especifica las opciones LDAP o RADIUS el campo para llenar la contraseña no se utiliza; esto es debido a que este tipo de usuarios son una referencia de una cuenta que está almacenado en un servidor LDAP o RADIUS (Ver *figura 4.27*). El acceso a estos servidores debe ser previamente configurado en el FG300A.

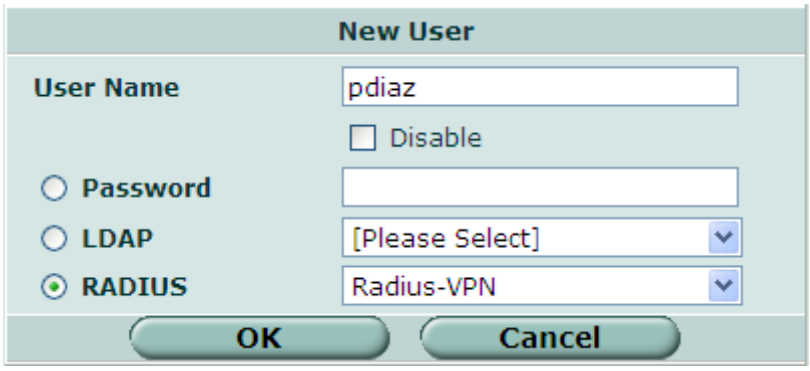


Figura 4.27 Ingreso de un nuevo usuario de tipo RADIUS

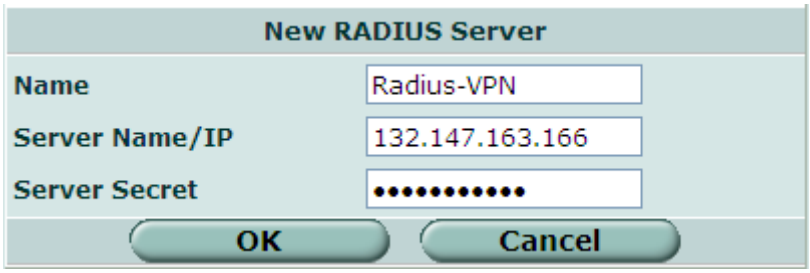


Figura 4.28 Ingreso de un nuevo acceso a un servidor RADIUS

El acceso a un servidor RADIUS se configura accediendo a ***User → RADIUS ↔ RADIUS*** donde desplegará una página en la que se debe hacer un *click* en el botón ***Create New***, lo que hará que se abra una página donde se permite ingresar un identificador del servidor para el FG300A, el nombre o dirección IP del servidor RADIUS en la red y el ***Server Secret*** o palabra secreta de negociación entre el servidor y el FG300A (Ver *figura 4.28*).

Se ingresa el nuevo servidor e inmediatamente se despliega la lista de servidores RADIUS configurados en el FG300A que se muestra en la *figura 4.29*. El detalle correspondiente a la dirección IP 132.147.163.166 del servidor RADIUS se explicará más adelante cuando se realice la configuración de la VPN con IPSec.

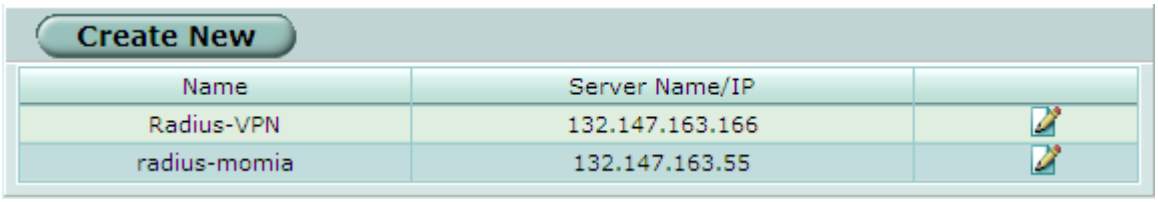


Figura 4.29 Lista de servidores RADIUS

4.3.3.3 Configuración de Grupos de Usuarios

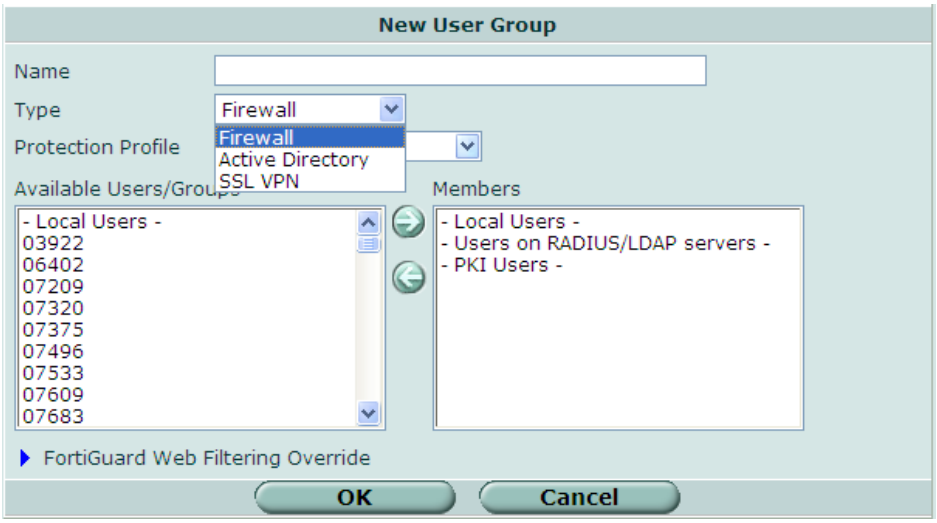


Figura 4.30 Nuevo grupo de usuarios

Configurar grupos de usuarios permite agrupar cuentas de usuarios que tienen la misma finalidad de uso en el acceso a una red externa como por ejemplo el Internet. El administrador puede crear grupos de usuarios los mismos que serán tipo de grupos de usuarios y diferenciados por el perfil. El detalle del perfil será revisado en la configuración de políticas del *firewall*. Para crear un nuevo grupo de usuarios se debe ir a ***User → User Group ↔ User Group***. La *figura 4.30* permite observar el formulario para el ingreso de un nuevo grupo de usuarios, se destaca el campo ***Type*** porque permite escoger diferentes tipos de grupos de usuarios.

Los 3 grupos de usuarios pueden ser utilizados en cualquier política del *firewall*; sin embargo cada uno de este tipo de grupos tiene diferencias relacionado al ámbito de usuarios que cubren. Cuando se tiene al menos un grupo de usuarios de cada tipo, la lista de grupos de usuarios se distribuye según la *figura 4.31*.

Figura 4.31 Lista de grupo de usuarios

Los grupos de usuarios de tipo ***Firewall*** son utilizados cuando la política del *firewall* requiere que éste autentique al usuario. Para el tipo ***Active Directory*** es el servidor de Active Directory (AD) que autenticará a ese grupo de usuarios, para lo cual se debe haber creado el vínculo o conexión con el servidor AD para que éste a su vez exporte los usuarios que contenga su base de datos hacia el FG300A. El tipo de grupo de usuarios ***SSL VPN*** permite darles versatilidad y una configuración única a los clientes que se conecten a través de una VPN de tipo SSL. Cuando se revise la configuración de SSL VPN se detallará este aspecto.

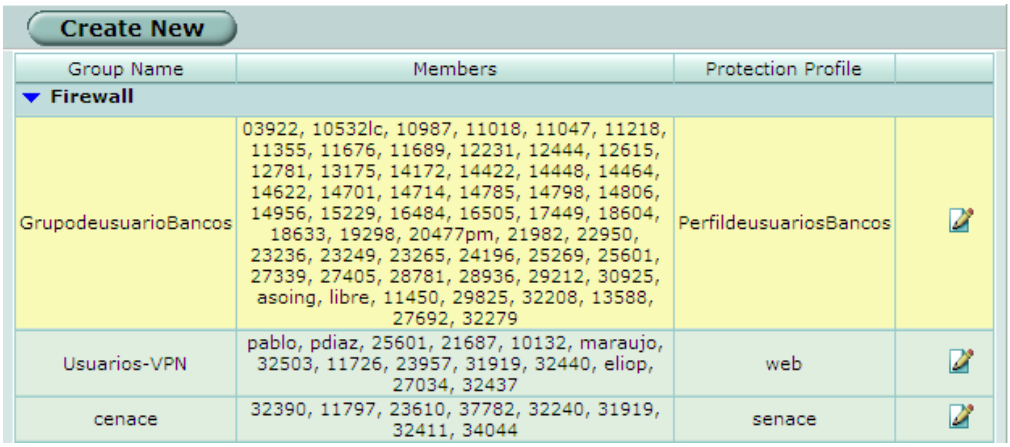


Figura 4.32 Lista de grupos de usuarios de tipo Firewall

La *figura 4.32* muestra una parte de la lista de usuarios de tipo ***Firewall*** configurados y listos para ser utilizados en las políticas del *firewall*.

4.3.4 CONFIGURACIÓN DE SEGURIDAD

Aquí básicamente lo que se busca es proteger el contenido tanto del tráfico de datos que ingresa como también del que sale de la red corporativa de la E.E.Q.S.A. Es así que de esta manera se va a explotar las funcionalidades que ofrece el FG300A dentro de las opciones de ***Firewall***, ***Intrusion Protection*** y ***Web Filter***.

4.3.4.1 Configuración de políticas del *Firewall*

Dentro de esta configuración que se llevará acabo sobre el FG300A, se incluyen las políticas que han sido configuradas y puestas en funcionamiento en el *IBM*

SecureWay Firewall y otras que conforme se vayan requiriendo se las estará implementando.

Para la configuración del *firewall* se necesita tener conocimiento del tipo de tráfico que se quiere bloquear o permitir para el respectivo acceso hacia los segmentos de red que convergen en el FG300A.

Además es importante anotar que en esta sección se podrán realizar las configuraciones que corresponden a IP *Virtual*, NAT, con lo que se podrá publicar servicios de la red interna hacia las redes externas como el Internet.

Las políticas del *firewall* recogen las múltiples configuraciones que se hay realizado o que se vayan a realizar en cada una de las opciones de seguridad, como se lo verá en el caso de filtrado *web*, perfiles de usuarios, usuarios, etc. También se destaca que es aquí donde se realiza la última configuración de los enlaces VPN de cualquier tipo que puedan ser configurados en el FG300A.

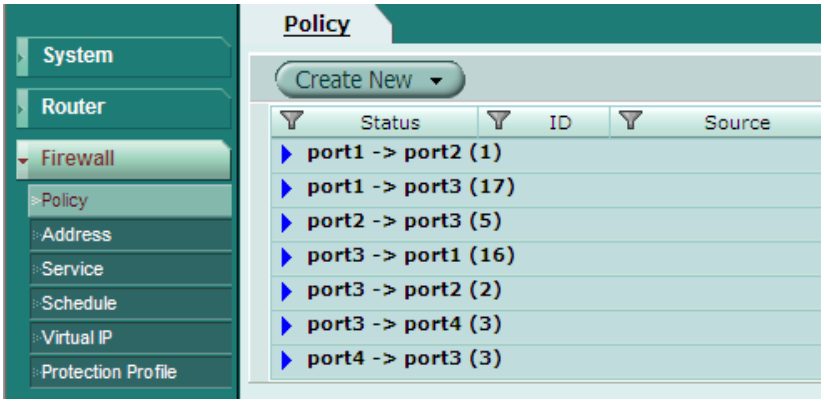


Figura 4.33 Menú de la opción Firewall y grupo de políticas

En la *figura 4.33* se muestra los posibles puertos donde se pueden aplicar políticas de seguridad; como se aprecia estos puertos corresponden al sentido que toma el tráfico. Como por ejemplo las políticas que permiten el ingreso de tráfico desde el Internet (Puerto 1) hacia la red interna o corporativa de la E.E.Q.S.A. (Puerto 3), corresponden al tráfico del Puerto 1 hacia el Puerto 3. Al tener 6 puertos se debe considerar que para cada combinación de puertos se puede tener un grupo de políticas, sin embargo no es la única combinación que se

puede dar en el FG300A ya que este equipo dispone de la capacidad de crear puertos virtuales relacionados con VLANs o VPN de tipo IPSec, así que el número de combinaciones puede crecer ampliamente. La *figura 4.33* también permite observar el menú que dispone la opción ***Firewall***.

Figura 4.34 Creación de una nueva política de firewall

Para crear una nueva política se debe ir a ***Firewall → Policy ↔ Policy***, hacer un *click* sobre el botón ***Create New*** el cual desplegará una página que contiene un formulario para especificar una nueva política tal como se lo puede apreciar en la *figura 4.34*.

En la *figura 4.34* se puede observar que agregar una nueva política requiere de algunos parámetros que necesitan ser explicados.

- ***Source Interface/Zone***. Puerto físico o virtual donde se genera o realiza una petición.

- ***Source Address***. Dirección o grupos de direcciones IP que a través del puerto anterior generan las peticiones de acceso.
- ***Destination Interfaz/Zone***. Puerto físico o virtual que recibe las peticiones originadas a través del ***Source Interfaz/Zone***.
- ***Destination Address***. Dirección o grupos de direcciones IP que reciben las peticiones de las ***Source Address***.
- ***Schedule***. Horario de aplicación de la política.
- ***Service***. Servicio asociado a un puerto o grupo de puertos que permiten acceso a una o varias aplicaciones.
- ***Action***. Acción tomada frente a los parámetros antes mencionados. Se puede aceptar o denegar (***Action***), el servicio (***Service***) en el horario fijado (***Schedule***) desde la dirección origen (***Source Address***) hacia la dirección destino (***Destination Address***).
- ***NAT***. Activación de *Network Address Translation*, cuando una dirección IP interna se oculta a través de una dirección IP virtual es necesario activar esta opción para que tenga efecto el ocultamiento de la dirección privada o interna.
- ***Protection Profile***. Es un perfil previamente configurado para proteger o evitar acceder a sitios no permitidos por la E.E.Q.S.A.
- ***Log Allowed Traffic***. Es un registro del tráfico que ha sido permitido.
- ***Authentication***. Al activar esta opción se puede hacer uso de los grupos de usuarios de tipo ***Firewall*** o ***Active Directory***.
- ***Traffic Shaping***. Permite controlar o establecer un ancho de banda según las necesidades del usuario y de la aplicación.
- ***User Authentication Disclaimer***. Es un mensaje para informar al usuario que se ha autenticado que la entidad que le ha permitido el acceso no se responsabiliza del uso de dicho acceso. No se utilizará este parámetro en las políticas del FG300A para la red de la E.E.Q.S.A.

Los primeros 7 parámetros para agregar una nueva política son obligatorios, los restantes son opcionales u obligatorios dependiendo de la naturaleza de la política, como el caso de una política que requiere aplicar NAT.

Una vez que se ha podido entender la funcionalidad de cada uno de los parámetros de una política de *firewall* del FG300A, se puede ir agregando las políticas antiguas e ir agregando nuevas que complementen o reemplacen a algunas políticas que por el cambio de direcciones, puertos o por algún motivo, han sufrido modificaciones.

4.3.4.2 Configuración de Direcciones IP y Grupo de Direcciones IP

Una opción que permite manejar nombres para direcciones IP, direcciones de redes IP o un grupo de las dos es la opción ***Address*** que es parte del menú de ***Firewall***, aquí se puede personalizar el nombre de la red o subred, como también agrupar un conjunto de direcciones asociadas a equipos o redes.

La finalidad de esta opción es especificar los equipos que estarán dentro de una política; como por ejemplo un grupo de equipos que necesiten tener acceso las 24 horas del día al Internet sin que los usuarios de estos equipos deban introducir nombres de usuario y contraseñas. A este grupo se le puede dar un nombre y así poder identificarlo, para que cuando se realice la política que involucra a este grupo de equipos le afecte única y exclusivamente a este grupo de equipos o *hosts*. Para agregar un nombre a una dirección o subred se debe ingresar a ***Firewall*** → ***Address*** ↔ ***Address***, hacer un *click* sobre el botón ***Create New***, esta acción a su vez desplegará una página con un formulario donde se podrá ingresar el nombre que identificará la dirección o subred, la dirección como tal y el puerto físico al cual esta relacionado tal dirección (ver *figura 4.35*).

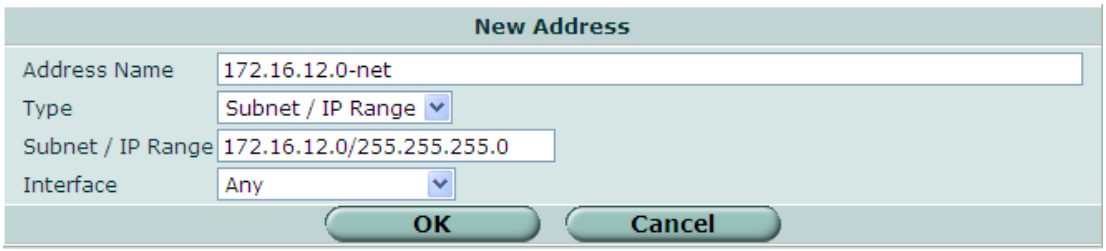


Figura 4.35 Nuevo nombre para una dirección de red IP

De esta manera se puede ir agregando todos los nombres que se requiera para ir personalizando la configuración general del FG300A y así también poder entender

de mejor manera las políticas que se están implementando en el *firewall*. La *figura 4.36* permite mostrar la lista de algunas direcciones y redes que han sido asignadas nombres de identificación.

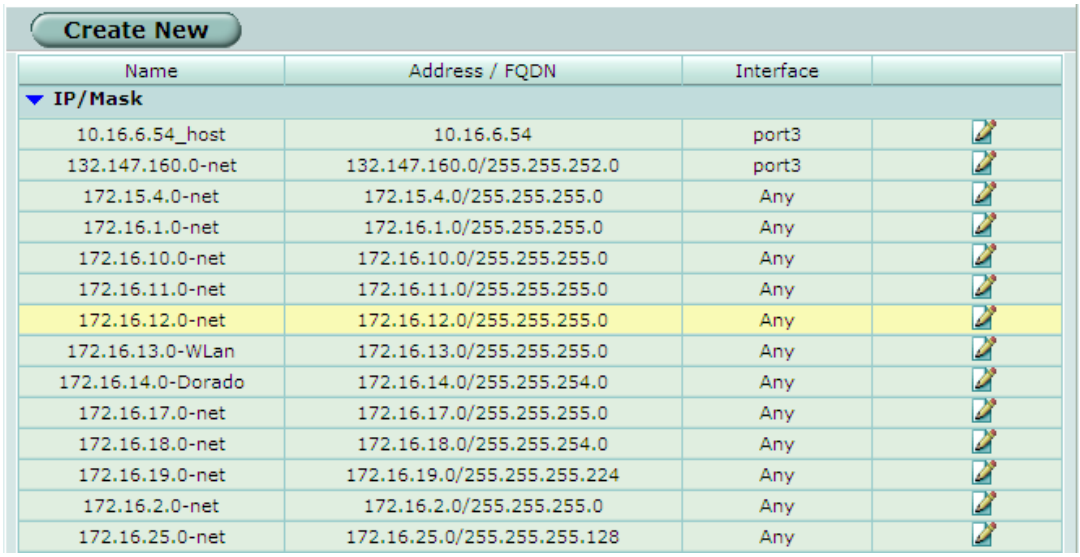


Figura 4.36 Listado de nombres de direcciones de redes

Las *figuras 4.37* y *4.38* permiten observar la creación de un grupo de nombre de direcciones y el listado de grupos de nombres de direcciones respectivamente.

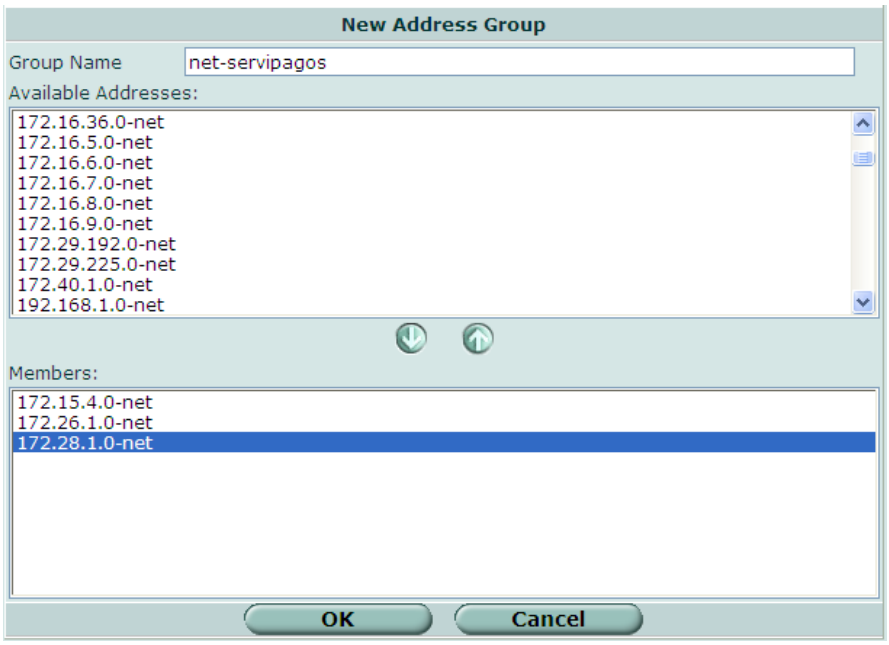
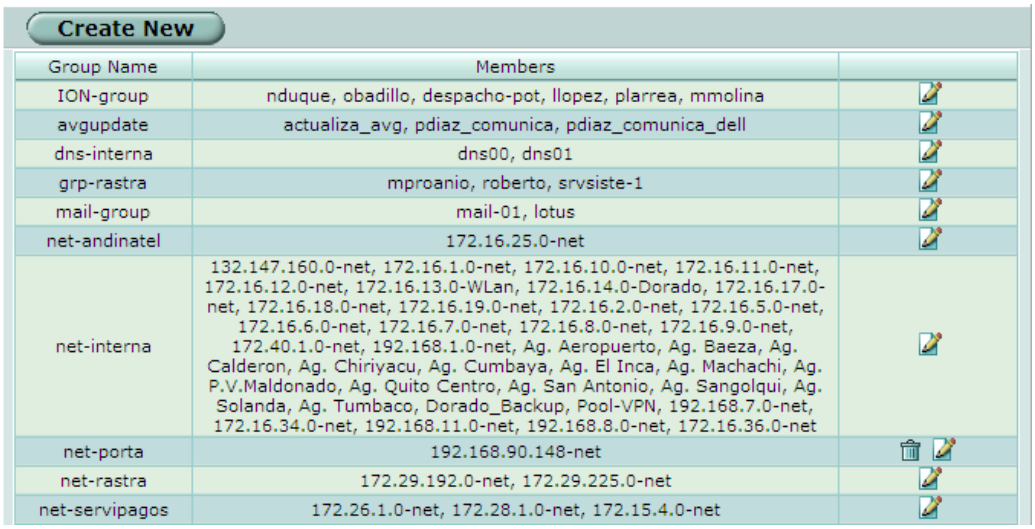


Figura 4.37 Creación de nuevo grupo de nombres de direcciones

Para crear un grupo de nombres de direcciones es preciso que previamente se haya configurado al menos un nombre de dirección. En la *figura 4.38* se muestra el listado de algunos grupos donde también se puede apreciar los nombres de dirección que las conforman.



Group Name	Members
ION-group	nduque, obadillo, despacho-pot, llopez, plarrea, mmolina
avgupdate	actualiza_avg, pdiaz_comunica, pdiaz_comunica_dell
dns-interna	dns00, dns01
grp-rastra	mproanio, roberto, srvsiste-1
mail-group	mail-01, lotus
net-andinatel	172.16.25.0-net
net-interna	132.147.160.0-net, 172.16.1.0-net, 172.16.10.0-net, 172.16.11.0-net, 172.16.12.0-net, 172.16.13.0-WLan, 172.16.14.0-Dorado, 172.16.17.0-net, 172.16.18.0-net, 172.16.19.0-net, 172.16.2.0-net, 172.16.5.0-net, 172.16.6.0-net, 172.16.7.0-net, 172.16.8.0-net, 172.16.9.0-net, 172.40.1.0-net, 192.168.1.0-net, Ag. Aeropuerto, Ag. Baeza, Ag. Calderon, Ag. Chiriyacu, Ag. Cumbaya, Ag. El Inca, Ag. Machachi, Ag. P.V.Maldonado, Ag. Quito Centro, Ag. San Antonio, Ag. Sangolqui, Ag. Solanda, Ag. Tumbaco, Dorado_Backup, Pool-VPN, 192.168.7.0-net, 172.16.34.0-net, 192.168.11.0-net, 192.168.8.0-net, 172.16.36.0-net
net-porta	192.168.90.148-net
net-rastra	172.29.192.0-net, 172.29.225.0-net
net-servipagos	172.26.1.0-net, 172.28.1.0-net, 172.15.4.0-net

Figura 4.38 Listado de grupos de nombres de direcciones

4.3.4.3 Configuración de Servicios y Grupo de Servicios

Otro parámetro importante para la configuración de una política, es la que se refiere al tipo servicio; el termino servicio está asociado al número de puerto TCP o UDP que determinada aplicación utilice dentro de una red IP. Estas configuraciones van desde cualquier servicio (***ANY***) hasta un puerto específico. El FG300A tiene una lista de servicios asociados a números de puertos TCP o UDP comunes que se los puede utilizar; sin embargo si se tiene que especificar un puerto específico que no está dentro del grupo de servicios y puertos comunes, lo que se debe realizar es personalizar el servicio. Un ejemplo de esto es el puerto TCP 1521 que ORACLE utiliza para realizar sus transacciones a través de la red, este puerto no está predefinido en el FG300A así que hay que crearlo para así poder utilizarlo en alguna política asociada a este servicio (Ver *figura 4.40*).

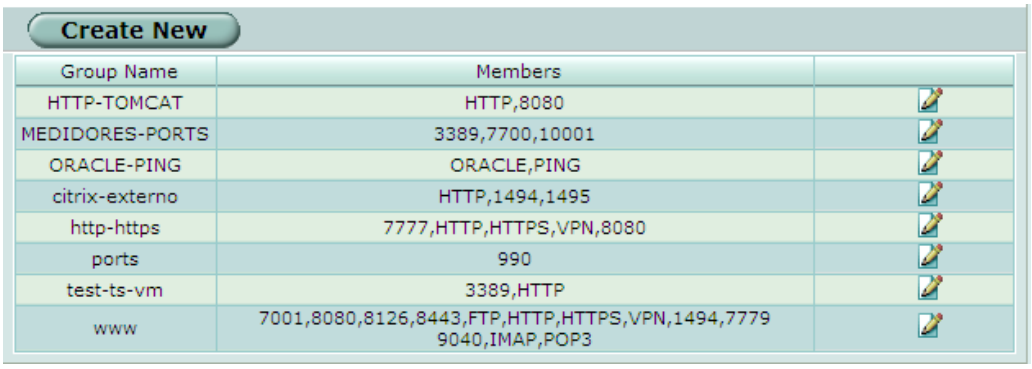


Figura 4.39 Listado de grupos de servicios

La *figura 4.39* muestra el listado de grupos de servicios que han sido configurados basados en las necesidades de acceso de la E.E.Q.S.A. hacia el exterior y del exterior hacia la E.E.Q.S.A. que previamente fueron configurados en *IBM SecureWay Firewall*.

Esto permitirá filtrar el tráfico que debe pasar y también optimizar el uso de direcciones IP públicas disponibles, como también ofrecer un nivel de seguridad al impedir que por algún puerto no permitido se realicen actos mal intencionados en contra de la empresa.

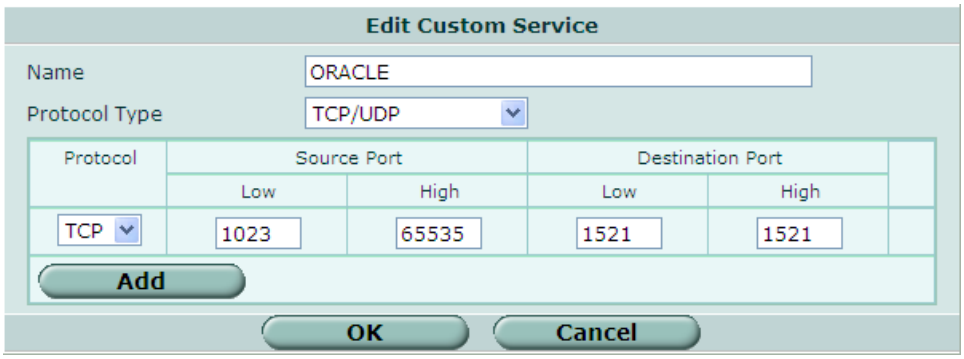


Figura 4.40 Edición del servicio personalizado de ORACLE

4.3.4.4 Configuración de direcciones IP Virtuales

Otra de las configuraciones importantes es la que se tiene que realizar para aquellos servidores o *hosts* de la red corporativa de la E.E.Q.S.A. que necesitan que sus servicios puedan ser accedidos a través de redes externas; mayormente a través del Internet. Para esto la opción ***Virtual IP*** del menú de ***Firewall***, permite ocultar la dirección de la red local de la E.E.Q.S.A. utilizando una de las

direcciones IP públicas que se tiene a disposición o lo que es lo mismo utilizar el concepto de NAT.

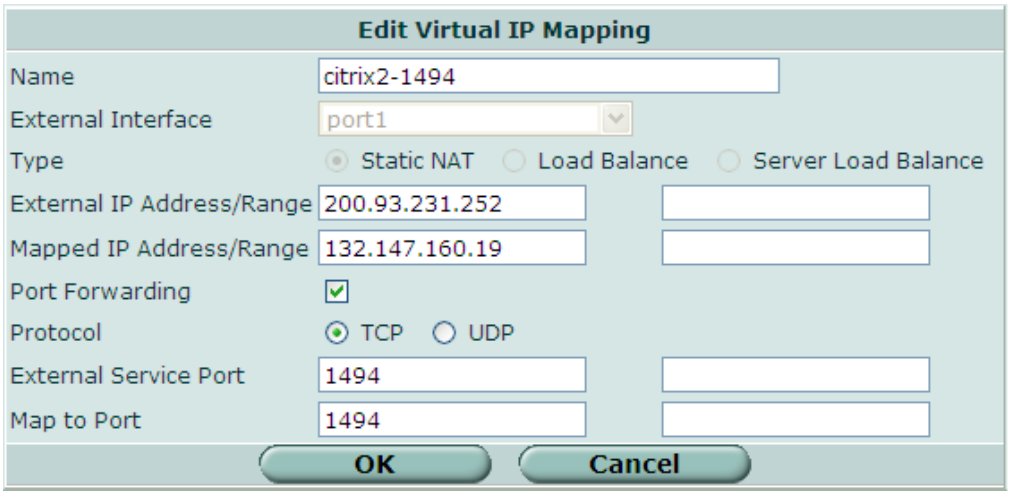
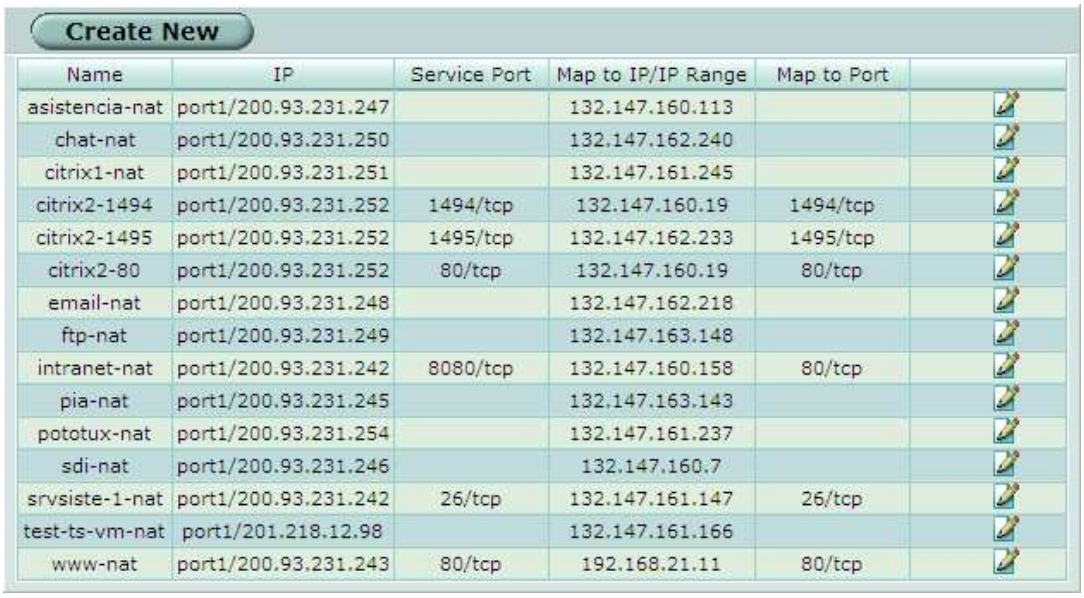


Figura 4.41 Edición de una IP virtual

En la *figura 4.41* se puede apreciar que el servidor de nombre *citrix2* necesita que su servicio sea accedido a través del Internet pero utilizando una dirección IP pública.



Name	IP	Service Port	Map to IP/IP Range	Map to Port	
asistencia-nat	port1/200.93.231.247		132.147.160.113		
chat-nat	port1/200.93.231.250		132.147.162.240		
citrix1-nat	port1/200.93.231.251		132.147.161.245		
citrix2-1494	port1/200.93.231.252	1494/tcp	132.147.160.19	1494/tcp	
citrix2-1495	port1/200.93.231.252	1495/tcp	132.147.162.233	1495/tcp	
citrix2-80	port1/200.93.231.252	80/tcp	132.147.160.19	80/tcp	
email-nat	port1/200.93.231.248		132.147.162.218		
ftp-nat	port1/200.93.231.249		132.147.163.148		
intranet-nat	port1/200.93.231.242	8080/tcp	132.147.160.158	80/tcp	
pia-nat	port1/200.93.231.245		132.147.163.143		
pototux-nat	port1/200.93.231.254		132.147.161.237		
sdi-nat	port1/200.93.231.246		132.147.160.7		
srvsiste-1-nat	port1/200.93.231.242	26/tcp	132.147.161.147	26/tcp	
test-ts-vm-nat	port1/201.218.12.98		132.147.161.166		
www-nat	port1/200.93.231.243	80/tcp	192.168.21.11	80/tcp	

Figura 4.42 Listado de direcciones IP virtuales

Un aspecto importante es el relacionado al puerto TCP, donde se especifica que tanto el número del puerto externo como el número del puerto interno deben

permanecer fijos, seguramente porque la aplicación cliente buscará en una dirección un puerto específico.

La *figura 4.42* muestra el conjunto de direcciones IP virtuales configuradas para diferentes servicios que presta a través del Internet, como ejemplo el sitio *web* de la empresa.

4.3.4.5 Configuración de horario de aplicación de política, perfiles y filtro URL

Se puede aplicar un horario donde una determinada política se ejecute automáticamente; a partir de ese horario la política se ejecuta y fuera del horario la acción contraria es la que se ejecuta. Por ejemplo si se tiene un grupo de usuarios que tienen acceso al Internet, realizando la configuración en la opción **Schedule** se les puede limitar el uso otorgándoles permiso de acceso desde las 06h00 hasta las 16h00; lo contrario será que fuera de este horario no puedan acceder al Internet a través de la red corporativa de la E.E.Q.S.A.

Cuando se crea un horario éste necesita 3 parámetros, el nombre, los días e intervalos de horas que consiste este horario. La *figura 4.43* muestra un listado de horarios disponibles para ser utilizados en cualquier política de *firewall*.

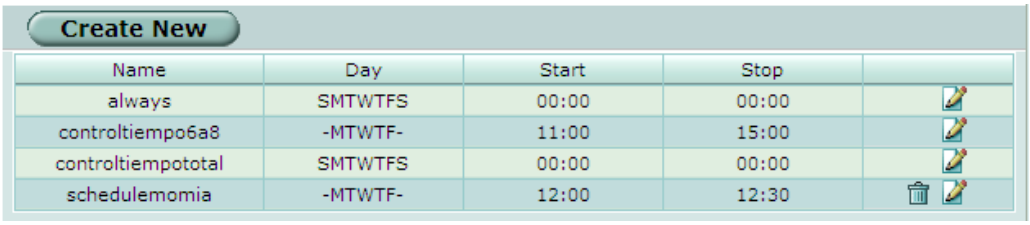


Figura 4.43 Listado de horarios

Un perfil de protección evita que los usuarios accedan ya sea de manera intencional o no a sitios que no formen parte de las actividades o que ayuden a la producción diaria de la empresa. Dentro de estos perfiles se puede escoger una amplia gama de opciones como lo muestra la *figura 4.44*, de los cuales las opciones *Anti-Virus*, *Web Filtering*, *IPS* e *IM/P2P* son las que serán configuradas. Los demás parámetros serán estudiados para posteriormente ser explotados de mejor manera dentro de las políticas del *firewall*.

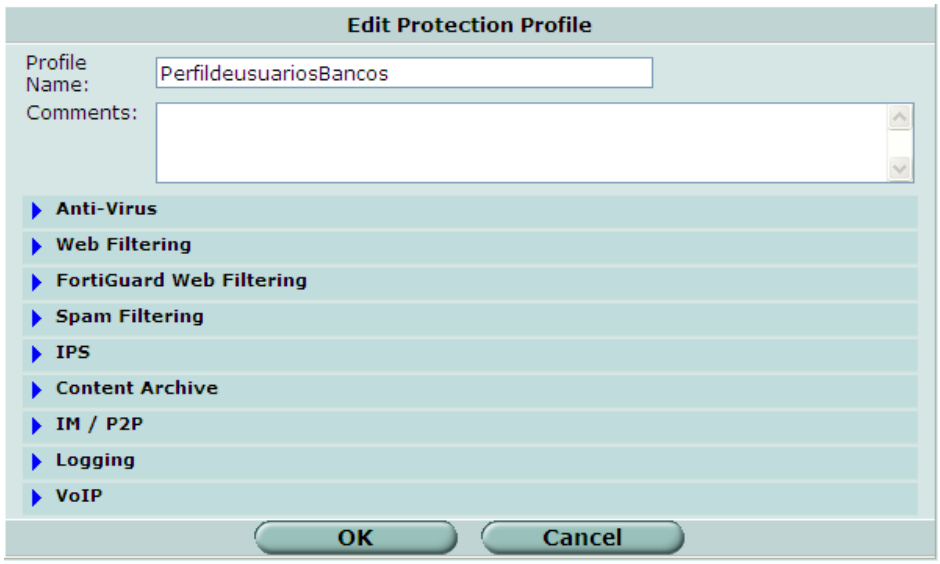


Figura 4.44 Edición de un perfil de usuario

Básicamente lo que se debe hacer, en el caso de *Anti-Virus*, aplicar sobre protocolos comunes en los que se base la política, por ejemplo la navegación por Internet el *Anti-Virus* deberá ejecutarse sobre protocolos como HTTP, HTTPS, TELNET, FTP, etc.

Web Filtering se aplica sobre patrones comunes y nocivos que están por todo el Internet como son: Sitios pornográficos, juegos en red, descarga sin límite de archivos multimedia como audio o video en varios formatos, ocio, etc. En la *figura 4.45* se muestra la lista de filtros *web* de tipo URL listos para ser utilizados en las políticas del *firewall*.

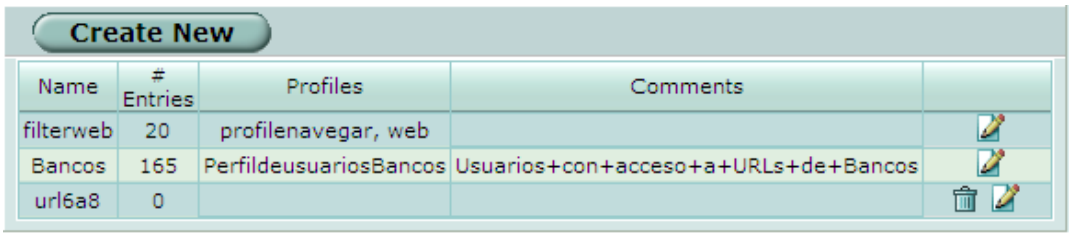
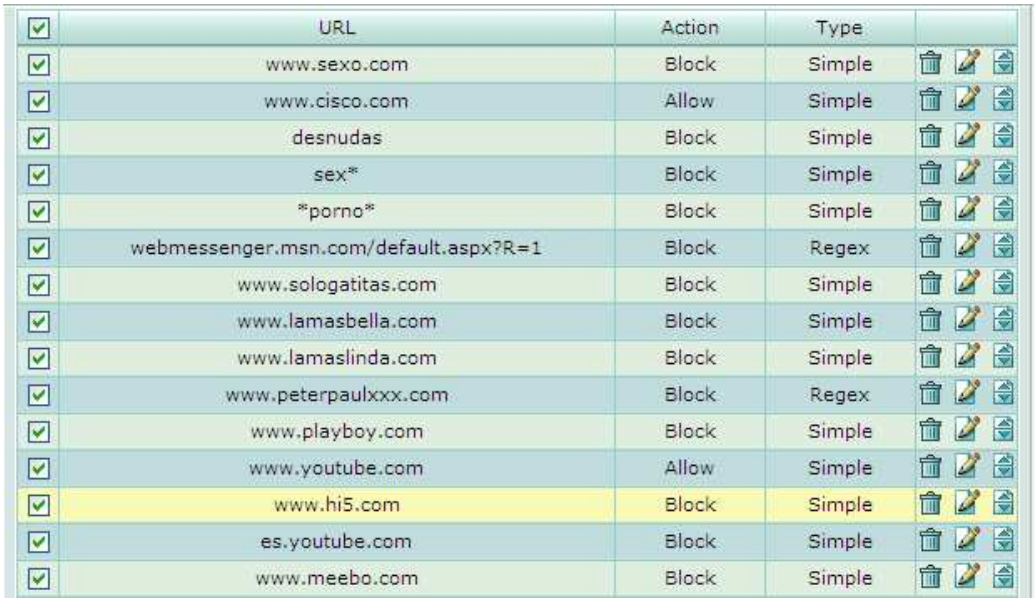


Figura 4.45 Lista de filtros web basados en URL



URL	Action	Type
www.sexo.com	Block	Simple
www.cisco.com	Allow	Simple
desnudas	Block	Simple
sex*	Block	Simple
porno	Block	Simple
webmessenger.msn.com/default.aspx?R=1	Block	Regex
www.sologatitas.com	Block	Simple
www.lamasbella.com	Block	Simple
www.lamaslinda.com	Block	Simple
www.peterpaulxxx.com	Block	Regex
www.playboy.com	Block	Simple
www.youtube.com	Allow	Simple
www.hi5.com	Block	Simple
es.youtube.com	Block	Simple
www.meebo.com	Block	Simple

Figura 4.46 Contenido de un filtro web de tipo basado en URL

Claramente se observa en la *figura 4.46* un listado de URLs las mismas que tendrán un valor de **Action** según si el contenido es nocivo o improductivo para la E.E.Q.S.A., por ejemplo se sabe que el sitio en Internet *www.hi5.com* permite crear y luego personalizar páginas con actividades como subir imágenes, archivos de audio, etc. Primeramente se considera que es altamente perjudicial para el consumo de ancho de banda del acceso a Internet corporativo y luego es una distracción para quienes lo usan, por lo tanto se ha bloqueado el URL de *hi5*.

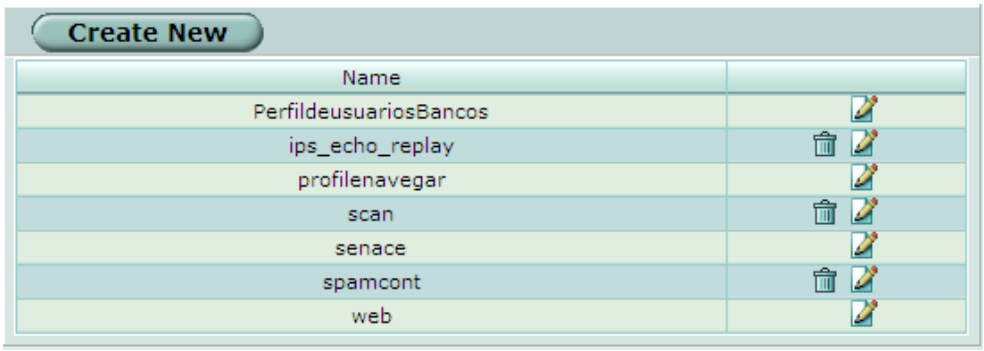


Figura 4.47 Listado de perfiles de protección

IM/P2P son aplicaciones que sirven para interactuar con usuarios del Internet permitiendo el uso y descarga de archivos y demás aplicaciones; si bien es cierto se trata de una potencial herramienta, los usuarios tanto interno como externos a la E.E.Q.S.A. no explotan de manera positiva esta herramienta y que por el

contrario distraen la actividad laboral de los empleados que tienen este acceso, por lo tanto se deben bloquear hasta crear una cultura del buen uso de algunos de estos aplicativos.

La *figura 4.47* muestra el listado de perfiles de protección que serán utilizados en las diferentes políticas de *firewall* del FG300A según el requerimiento.

El *IPS* será analizado a continuación.

4.3.4.6 Sistema de Protección de Intrusos (*IPS*)

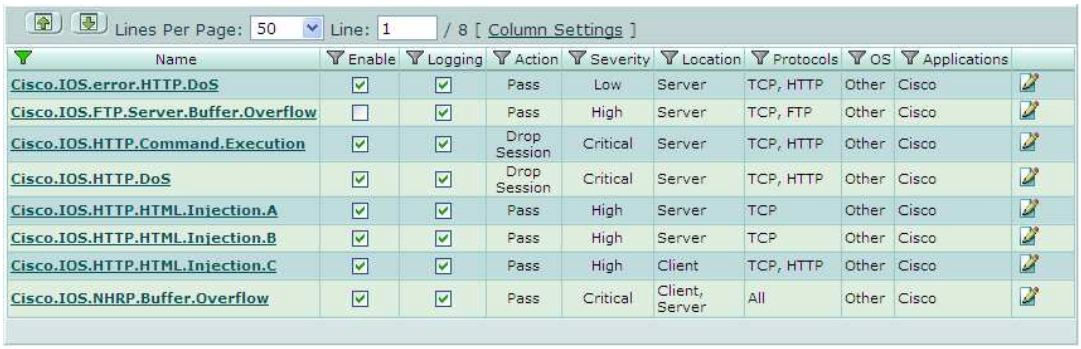


Figura 4.48 Firma o signature asociada a amenazas encontradas para el IOS de equipos Cisco

El IPS funciona de modo que los usuarios no perciben que los datos que ingresan de un segmento a otro del FG300A son inspeccionados; se trata de verificar posibles amenazas que pueden ingresar a la red de datos. El IPS tiene una base de datos de las amenazas que pueden afectar a la red que se protege. Para esto cuenta con un servicio de actualización desde los servidores de Fortinet publicados en el Internet.

Para que esta configuración surta efecto se la debe aplicar al perfil de protección.

La *figura 4.48* permite mostrar el listado de las *signatures* o firmas de errores encontrados en el sistema operativo (IOS) de Cisco. Éste es un grupo de firmas o *signatures* que pueden ser configuradas para determinar la acción y la severidad con la que deba utilizar dicha acción y es ahí donde radica la funcionalidad del IPS ya que permite tomar acciones ante determinada firma (Ver *figura 4.49*). La

firma no necesariamente debe ser bloqueada ya que puede ocasionar que se evite el funcionamiento adecuado de una aplicación, por lo que esta configuración debe hacerse con el mayor cuidado y sin apresuramientos.

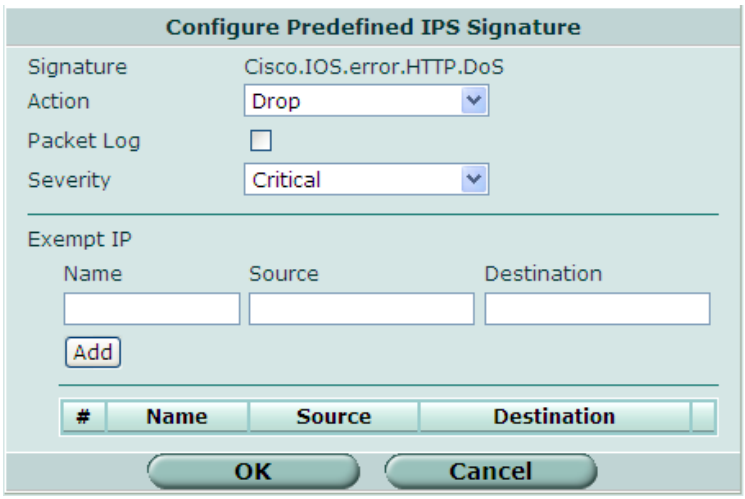


Figura 4.49 Configuración de un signature predefinido

Las anomalías en cambio son acciones que potencialmente pueden convertirse en amenazas y por lo tanto pueden hacer daño a las redes de datos, equipos y servidores ya que estas anomalías están relacionadas a la actividad de protocolos como ICMP, TCP y UDP, por lo tanto en la configuración de la opción **Anomaly** debe tomarse en cuenta los protocolos y aplicaciones utilizadas para el monitoreo de la red de la E.E.Q.S.A. con el propósito de no alterar la administración que se desarrolla sobre la red. La *figura 4.50* permite observar un listado de nombres de anomalías que tienen el campo **Action** con el valor de **Drop** o rechazo.

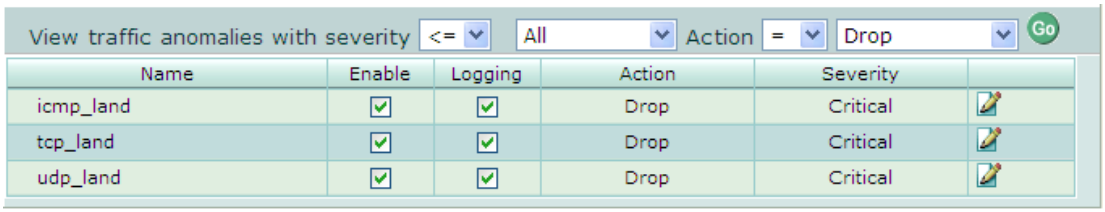


Figura 4.50 Listado de anomalías con el valor del campo Action en Drop o rechazo

Las anomalías pueden ser editadas para poder asignarles la acción apropiada (Ver *figura 4.51*).

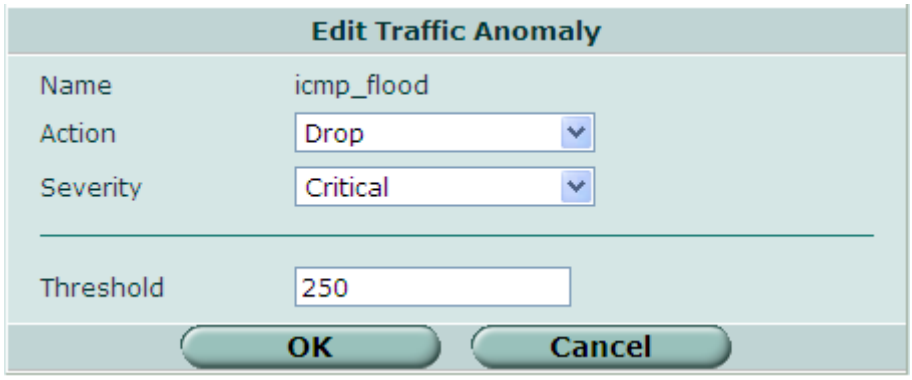


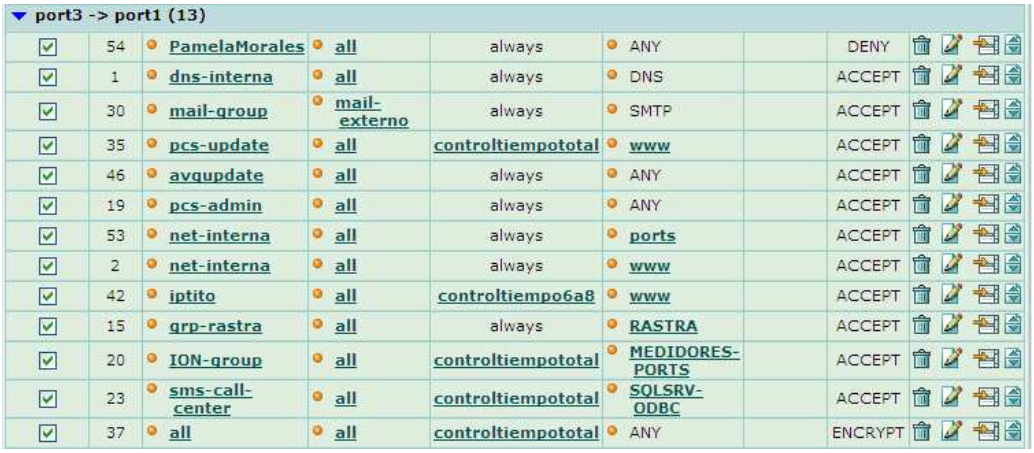
Figura 4.51 Edición de una anomalía

4.3.4.7 Consideraciones en la configuración de las políticas del *firewall*

Se han presentado los parámetros más relevantes y que se están implementando para un desempeño adecuado de la funcionalidad de *firewall* del FG300A. A más de estos parámetros existen otros que ayudan a optimizar las políticas del *firewall* en cuanto al funcionamiento; éstos se analizarán cuando se revise las configuraciones de las VPNs.

En resumen, el grupo de políticas del puerto 3 hacia el puerto 1 es el que se muestra en la *figura 4.52*. Las políticas tienen que ir desde la más específica hasta la más general, esto respecto al número de equipos implicados. Por ejemplo una política entre dos *hosts* debe ir primera y la navegación de todos los *hosts* de la E.E.Q.S.A. hacia el Internet deberá ser la última o una de las últimas.

Las configuraciones de políticas del *firewall* son administradas por el personal del Departamento de Administración de Sistemas y Bases de Datos y son solo ellos quienes pueden crear nuevas políticas; cabe destacar en este punto que la administración de este equipo está compartida y coordinada con el Departamento de Comunicaciones y Soporte, ya que el equipo si bien es cierto es un elemento propiamente de red, tiene dentro de sus capacidades aspectos íntimamente relacionados con la administración de los sistemas informáticos, básicamente en lo que respecta al acceso y manejo cuentas de usuarios.



port3 -> port1 (13)

☑	54	PamelaMorales	all	always	ANY		DENY
☑	1	dns-interna	all	always	DNS		ACCEPT
☑	30	mail-group	mail-externo	always	SMTP		ACCEPT
☑	35	pcs-update	all	controltiempototal	www		ACCEPT
☑	46	avgupdate	all	always	ANY		ACCEPT
☑	19	pcs-admin	all	always	ANY		ACCEPT
☑	53	net-interna	all	always	ports		ACCEPT
☑	2	net-interna	all	always	www		ACCEPT
☑	42	iptito	all	controltiempo6a8	www		ACCEPT
☑	15	grp-rastra	all	always	RASTRA		ACCEPT
☑	20	ION-group	all	controltiempototal	MEDIDORES-PORTS		ACCEPT
☑	23	sms-call-center	all	controltiempototal	SQLSRV-ODBC		ACCEPT
☑	37	all	all	controltiempototal	ANY		ENCRYPT

Figura 4.52 Listado de políticas que corresponden al tráfico en sentido Puerto 3 hacia Puerto 1

4.4 CONFIGURACIÓN DE LAS REDES PRIVADAS VIRTUALES

Una vez puesto en marcha el funcionamiento del equipo de seguridad se puede empezar a realizar las primeras configuraciones de VPN en este equipo.

El equipo de seguridad FG300A soporta como ya se ha explicado en un inicio, VPNs con PPTP, SSL e IPSec. A continuación se detallarán las configuraciones que permitirán a los equipos remotos establecer túneles VPN con el FG300A utilizando las mencionadas tecnologías VPN, para el transporte principalmente de tráfico de tipo Citrix y VoIP (G.729 o GSM).

Figura 4.53 Menú de la opción VPN

La *figura 4.53* ilustra las opciones disponibles en el modo de acceso HTTPS a la consola del FG300A y de las cuales se utilizará para la implementación las tres primeras opciones de navegación.

4.4.1 CONFIGURACIÓN DEL FORTINET FG300A PARA ESTABLECER VPNs CON PPTP

PPTP se configura de una manera muy sencilla, solo se necesita habilitar el protocolo, un rango de direcciones IP y un grupo de usuarios.

4.4.1.1 Configuración del servidor VPN PPTP

La configuración consta de la activación del servicio. Se debe especificar un rango de direcciones; este rango es un *pool* de direcciones disponibles para ser utilizadas por el cliente PPTP mientras mantiene una sesión con el servidor de VPN de tipo PPTP que en este caso es el FG300A a través de su módulo VPN PPTP. Para llegar a esta configuración se debe ir a ***VPN → PPTP ↔ PPTP Range***.

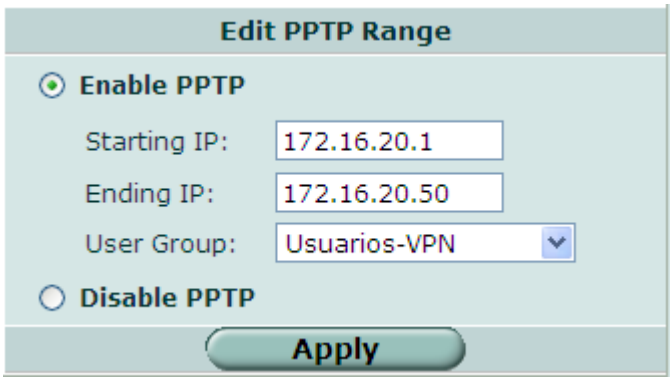


Figura 4.54 Formulario para la configuración del servidor VPN PPTP

La *figura 4.54* muestra los parámetros para la configuración del servidor VPN PPTP; cabe indicar que el direccionamiento IP utilizado es el propuesto en el diseño de la sección correspondiente del Capítulo 3 del presente proyecto.

4.4.1.2 Configuración de usuarios para VPN PPTP

Los usuarios son especificados en el campo ***User Group*** y se puede escoger un grupo de entre los que se encuentran configurados. Para esta configuración el

grupo de usuarios tiene el nombre de **Usuarios-VPN** y puede estar conformado por usuarios de tipos locales y RADIUS del FG300A.

Usuarios-VPN	pablo, pdiaz, 25601, 21687, 10132, maraujo, 32503, 11726, 23957, 31919, 32440, eliop, 27034, 32437	web	

Figura 4.55 Grupo de usuarios para VPN configurados en el FG300A

Como se puede apreciar en la *figura 4.55* la tercera columna se refiere al tipo de Perfil de Protección o ***Protection Profile***, el cual para este grupo de usuarios está personalizado bajo el nombre de **web** el mismo que tiene configuraciones básicas de seguridad, los cuales se irán mejorando según los riesgos y requerimientos que implique este tipo de acceso.

4.4.1.3 Configuración de la política del *firewall* para VPN PPTP

Para finalizar la configuración VPN PPTP se debe agregar y configurar una política en el *firewall* para que el acceso sea permitido y controlado. La *figura 4.56* permite observar la configuración de la política del *firewall* para el acceso VPN PPTP.

En la política del *firewall* mostrada en la *figura 4.56* se puede indicar lo siguiente:

- *Sentido del flujo de tráfico*. La política indica que ésta debe ser desde el Puerto 1 hacia el Puerto 3, ya que los clientes se conectarán desde el Internet (Puerto 1) y requerirán acceder a los servicios que se encuentran en la red interna o corporativa de la E.E.Q.S.A. (Puerto 3).

- *Direcciones*. Como direcciones origen se ha establecido un grupo denominado VPN-PPTP el cual tiene un rango comprendido entre la dirección 172.16.20.1 hasta la 172.16.20.50. Si bien es cierto en la configuración VPN PPTP también se especificó un rango de direcciones, hay que indicar que el rango de direcciones que se establece en al política es la que contiene al de la configuración VPN PPTP, de manera que si no se va a utilizar todo el rango VPN-PPTP se puede establecer una parte de

este rango en la configuración VPN PPTP; para esta implementación el rango será el mismo. En el campo de direcciones de destino se puede observar en la *figura 4.56* que tiene el valor de *Multiple*, y esto siginifica que se trata de la combinación de uno o más nombres de direcciones o grupo de direcciones; para el caso de VPN PPTP se ha escogido el grupo de direcciones **net-interna** y **www** los cuales corresponden a direcciones la red corporativa de la E.E.Q.S.A.

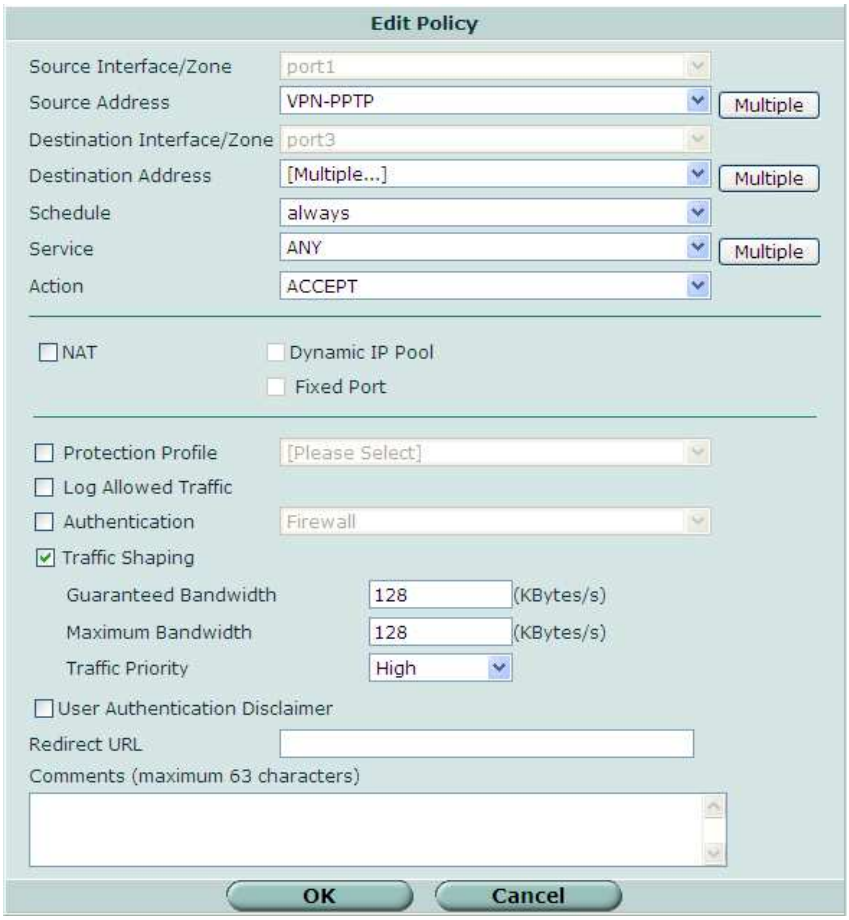


Figura 4.56 Edición de la política para la VPN PPTP

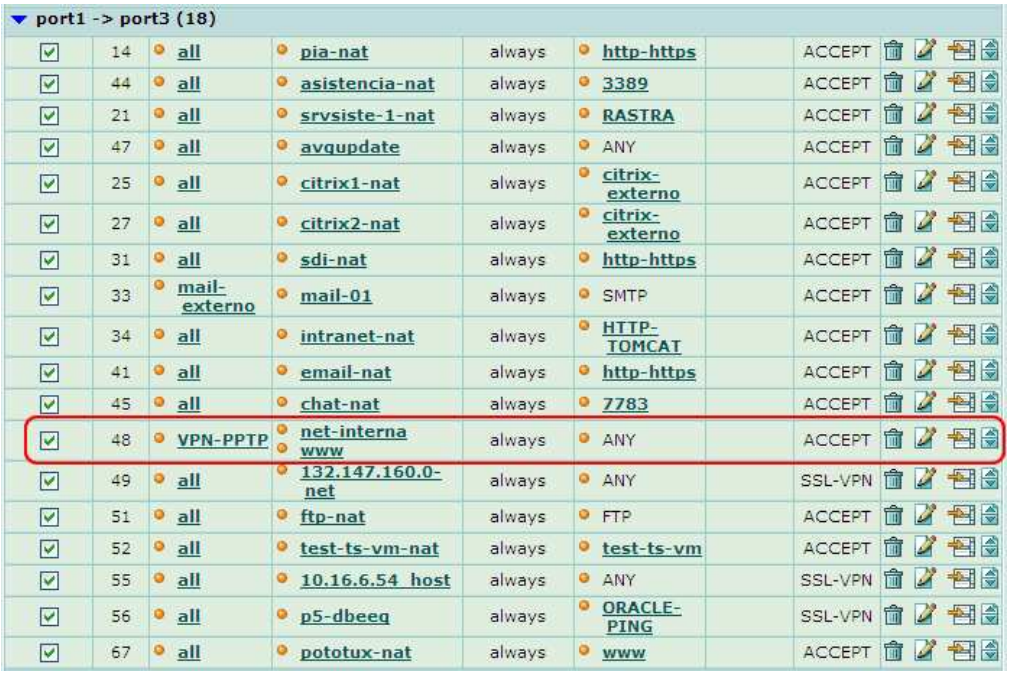
– Para el horario (***schedule***) en que la política se aplicará estará disponible todo el tiempo (***always***) ya que usuarios de tipo administradores necesitarán utilizar este acceso en cualquier momento.

- El tipo de servicio (***service***) para este caso será cualquiera (***ANY***), posteriormente se evaluará si se debe o no restringir el tipo de aplicaciones que circularán por este medio.

- El valor de ***Action*** se ha establecido en ***ACCEPT*** lo que indica que la política tiene la finalidad de permitir un acceso y no denegarlo.

- La opción de ***NAT*** no es aplicable a esta configuración al igual que ***Protection Profile*** y ***Authentication***, ya que estas configuraciones están implícitas en la configuración VPN PPTP.

- ***Traffic Shaping*** tiene fijado y garantizado un ancho de banda de 128 kbps y el valor máximo no debe sobrepasar este valor. Como se había indicado en el diseño este es el valor ideal de capacidad de canal para ejecutar Citrix y VoIP simultáneamente. De requerir más enlaces se incrementará este valor dependiendo también de la capacidad del enlace hacia el Internet.



port1 -> port3 (18)							
☑	14	all	pia-nat	always	http-https		ACCEPT
☑	44	all	asistencia-nat	always	3389		ACCEPT
☑	21	all	srvsiste-1-nat	always	RASTRA		ACCEPT
☑	47	all	avqupdate	always	ANY		ACCEPT
☑	25	all	citrix1-nat	always	citrix-externo		ACCEPT
☑	27	all	citrix2-nat	always	citrix-externo		ACCEPT
☑	31	all	sdi-nat	always	http-https		ACCEPT
☑	33	mail-externo	mail-01	always	SMTP		ACCEPT
☑	34	all	intranet-nat	always	HTTP-TOMCAT		ACCEPT
☑	41	all	email-nat	always	http-https		ACCEPT
☑	45	all	chat-nat	always	7783		ACCEPT
☑	48	VPN-PPTP	net-interna www	always	ANY		ACCEPT
☑	49	all	132.147.160.0-net	always	ANY		SSL-VPN
☑	51	all	ftp-nat	always	FTP		ACCEPT
☑	52	all	test-ts-vm-nat	always	test-ts-vm		ACCEPT
☑	55	all	10.16.6.54_host	always	ANY		SSL-VPN
☑	56	all	p5-dbeeq	always	ORACLE-PING		SSL-VPN
☑	67	all	pototux-nat	always	www		ACCEPT

Figura 4.57 Ubicación de la política VPN PPTP

La *figura 4.57* permite observar la ubicación de la política dentro del grupo que corresponde a las que van desde el Puerto 1 hacia el Puerto 3. Este grupo de políticas tienen un común denominador que son las direcciones de origen y que en general está fijado en el valor de *all* por lo que la ubicación estará determinada por las direcciones destino. Para el caso de la política de VPN PPTP la ubicación es la adecuada ya que, si bien es cierto, la direcciones origen son de un rango muy reducido, detrás de estas direcciones el establecimiento se da por medio de cualquier dirección que está en el Internet, así que se trata de una política con un matiz de tipo general.

4.4.2 CONFIGURACIÓN DEL FORTINET FG300A PARA ESTABLECER VPNs CON SSL

SSL es la tecnología que se pretende explotar por su fácil implementación y menor tiempo de configuración en lado del cliente, además como se ha estado señalando el cliente tradicional es un navegador web; para esta implementación se utilizará a los navegadores Internet Explorer 7 y Mozilla 3. Hay que recordar que SSL contempla 3 tipos de clientes: el mencionado navegador *web*, aplicaciones sobre el navegador *web* y el túnel VPN SSL a través de la instalación de un componente *ActiveX* o un *Applet*. El FG300A contiene un componente *ActiveX* el cual tendrá una configuración similar al cliente VPN PPTP de *Windows XP Professional*.

4.4.2.1 Configuración del servidor VPN SSL

Las *figuras 4.58* a *4.64* detallan cada una de las configuraciones que necesita VPN SSL para ser habilitado.

En la *figura 4.58* se pueden apreciar parámetros que son explicados a continuación:

- ***Login Port***. Es el campo para especificar el puerto utilizado por el servidor VPN SSL, para que los clientes se conecten a través del navegador y

especifiquen el puerto TCP 10443 y se pueda realizar la conexión HTTP segura (HTTPS). No se utiliza el puerto TCP 443 estándar de SSL debido a que es una medida de seguridad y solo personal autorizado de la E.E.Q.S.A. lo conoce; así que cuando el cliente desee conectarse al portal seguro de la E.E.Q.S.A. deberá escribir en el campo de dirección del navegador *web* de la siguiente manera: **https://200.93.231.242:10443**.

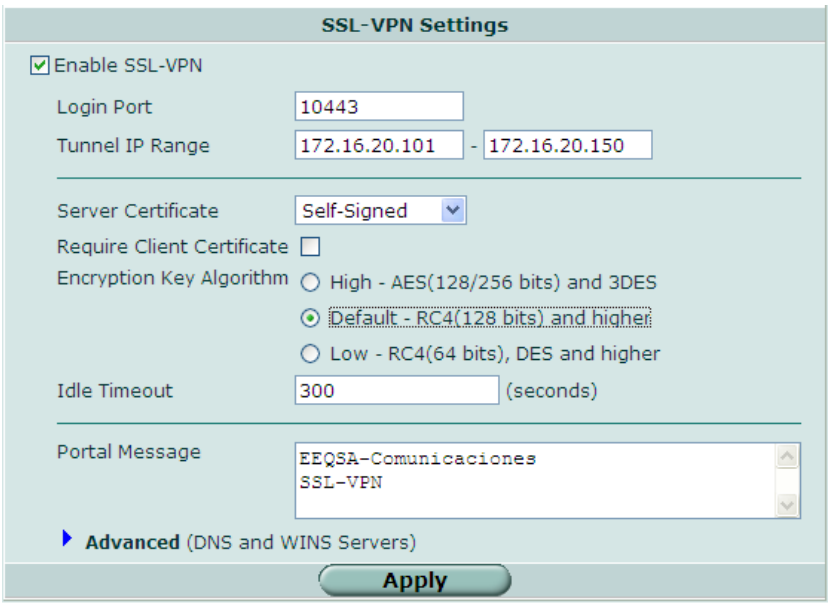


Figura 4.58 Configuración estándar del servidor VPN SSL

- ***Tunnel IP Range***. Se especifica un rango de direcciones que serán utilizados por los clientes que accedan en el modo de cliente liviano (componente *ActiveX*) y establezcan un túnel VPN más avanzado con SSL. Este rango está acorde al diseño propuesto en este proyecto.

- ***Server Certificate***. Al no tener establecido un servidor de certificados se fijará este campo con el valor por defecto ***Self-Signed***. Tampoco se requerirá del certificado del cliente. De ser necesario y por medidas de seguridad se requerirá personalizar estos dos campos que corresponden a la certificación.

- ***Encryption Key Algorithm***. Se escoge de entre las opciones disponibles el algoritmo de encripción RC4 de 128 bits ya que Internet Explorer 7 y

Mozilla 3 lo soportan sobre el sistema operativo *Windows XP Professional*. No está garantizado el pleno funcionamiento de estos navegadores con los algoritmos AES y 3DES. Escoger RC4 de 64 bits como algoritmo de encripción reduce el consumo de ancho de banda y la rapidez de encripción y desencripción, pero el precio de esta reducción lo asume la reducción de seguridad en el enlace.

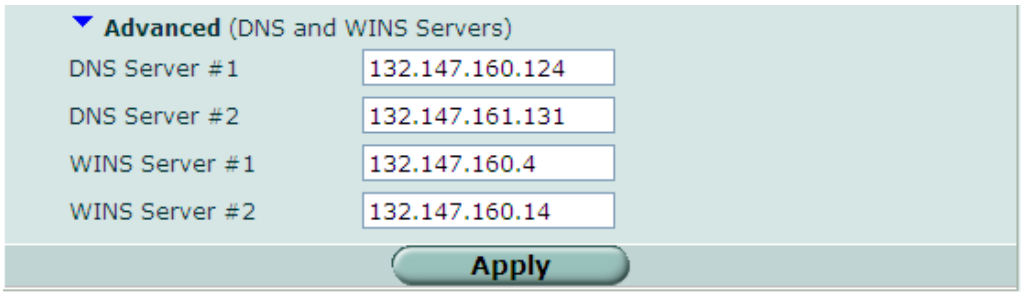


Figura 4.59 Configuración avanzada del servidor SSL VPN

- ***Idle Timeout***. El tiempo que una sesión esté sin actividad se fijará en 300 segundos, es decir 5 minutos, tiempo en que el portal del navegador *web* se reiniciará. Si se ha establecido el túnel a través del cliente liviano, el servidor considerará activa la conexión mientras se mantenga conectado el túnel.

- ***Portal Message***. Es un mensaje que el portal mostrará al usuario que logre autenticarse con éxito.

- ***Advanced***. Permite añadir la información de direcciones de los servidores DNS y WINS que utiliza la E.E.Q.S.A. para resolver los nombres de los *hosts* en la red (Ver *figura 4.59*). Este campo es útil para el cliente liviano.

4.4.2.2 Configuración de usuarios para VPN SSL

Los usuarios que podrán acceder a la red de la E.E.Q.S.A. a través de la VPN SSL, sus cuentas serán de tipo local en el FG300A y estas cuentas serán parte de grupos de usuarios de tipo ***SSL VPN*** como lo muestra la *figura 4.60*.

Los parámetros para este grupo de usuarios cambian respecto a los de tipo ***Firewall***. La *figura 4.60* permite observar que al seleccionar el tipo ***SSL VPN***, el parámetro ***Protection Profile*** desaparece así como el grupo de opciones ***FortiGuard Web Filtering Override*** (Ver *figura 4.30*) es reemplazado por ***SSL-VPN User Group Options*** que a diferencia del anterior grupo de opciones a este grupo se lo va a tomar en cuenta para la respectiva personalización.

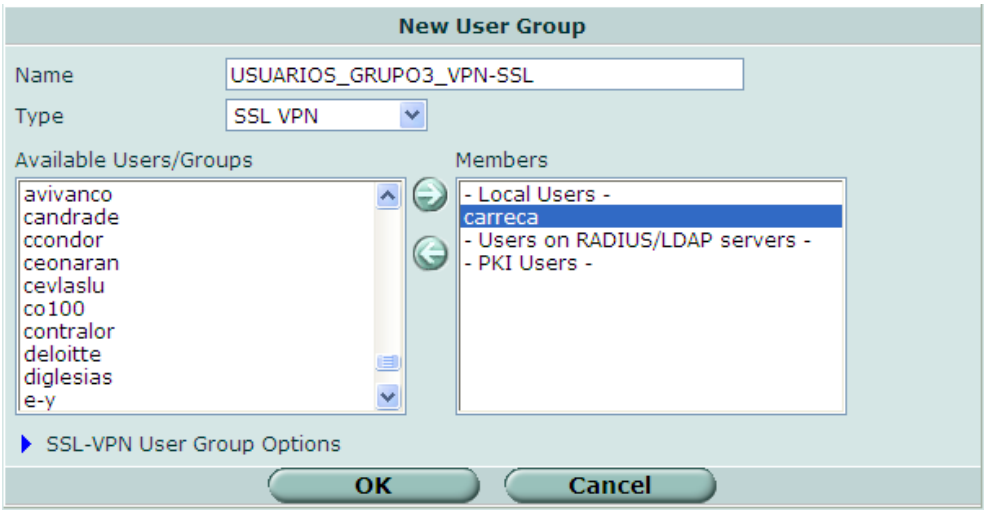


Figura 4.60 Creación de un grupo de usuarios tipo SSL VPN

En las opciones extendidas de este tipo de grupo de usuarios mostrado en la *figura 4.61* se puede ver que se debe especificar las siguientes opciones:

Enable SSL-VPN Tunnel service. Habilitar este servicio permite al usuario descargar el componente *Active-X* para realizar la instalación del cliente liviano de SSL sobre el computador y de esta manera tener una interfaz virtual y poder levantar el túnel VPN de tipo SSL. Este componente contiene la configuración de red personalizada según los parámetros fijados en el servidor VPN SSL y esta configuración. ***Allow Split Tunneling***, permite que el enlace a Internet en lado del cliente se divida para el túnel VPN y para el acceso normal hacia el Internet.

Restrict tunnel IP range for this group. Una de las ventajas de esta configuración es la de asignar a cada grupo de usuarios SSL VPN un rango diferente de direcciones IP, esto ayudará a la administración de las conexiones. En el diseño se ha asignado para las conexiones SSL VPN el rango de

direcciones IP 172.16.20.101 - 172.16.20.150; de este rango se divirán las primeras 30 direcciones para los usuarios de los CARs y Operadores de la E.E.Q.S.A., los 10 siguientes para usuarios de tipo ejecutivo y los 10 restantes para los usuarios administradores de la División de Tecnología.

En la *figura 4.61* también se puede observar opciones de tipo *Applet* de Java, para se pueda ejecutar sobre el navegador *web*.

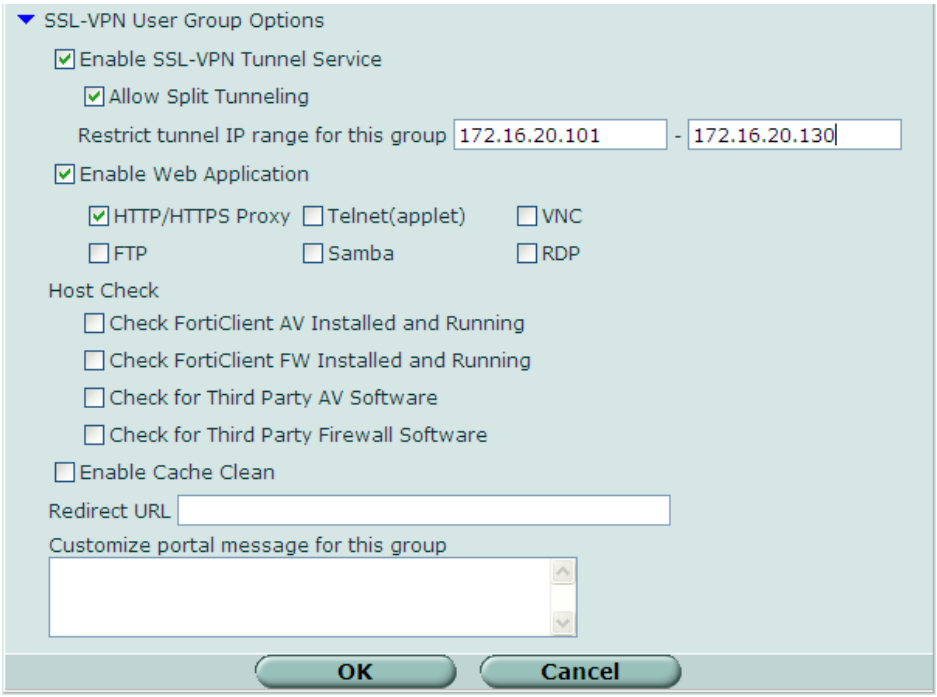


Figura 4.61 Opciones extendidas de usuarios tipo SSL VPN

Enable Web Application. El grupo de usuarios tendrá un portal *web* en el cual se le podrá habilitar aplicaciones que se ejecutan sobre la página HTTPS. En este grupo de aplicaciones a excepción de la opción ***HTTP/HTTPS Proxy*** el resto necesita del componente Java en el sistema operativo *Windows XP Professional* para la ejecución de *applets* de Java. Para los usuarios de CARs y operadores solo se les habilitará ***HTTP/HTTPS Proxy*** y para los usuarios ejecutivos y administradores se habilitará todas las aplicaciones a excepción de ***Samba***.

El resto de opciones no serán configuradas para ningún grupo ya que dependen de la instalación de un *software* cliente en el equipo remoto y éste a su vez

tendría que ejecutar un *Anti-Virus* y *Firewall* personal, lo que ocasionaría que se presenten cargas innecesarias de tráfico y latencia sobre el enlace.

4.4.2.3 Configuración de la política del *firewall* para VPN SSL

El servidor y grupo de usuarios para la VPN SSL han sido configurados, ahora se necesita configurar una política en el *firewall*, para permitir que las conexiones de tipo VPN SSL realizadas por los usuarios remotos, puedan tener el acceso desde el Internet.

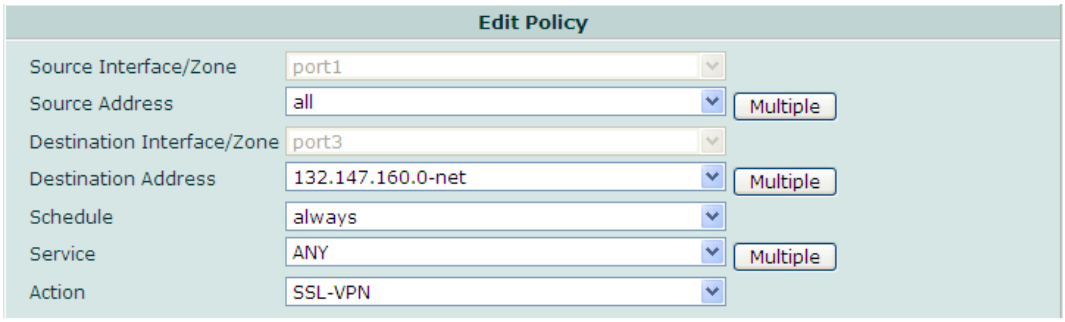


Figura 4.62 Configuración política para el acceso VPN SSL primera parte

La política para su implementación será revisada en tres partes que corresponden a diferentes ámbitos de la conexión y seguridad.

La primera parte corresponde a la *figura 4.62*, donde se muestra que el puerto 1 de conexión al Internet es el puerto de origen y el campo de dirección origen (***Source Address***) está fijado en el valor ***all***, esto indica que desde este acceso y desde cualquier dirección en Internet se podrá acceder al FG300A por medio de VPN SSL. El puerto 3 de la red interna será el destino y dentro de este puerto se especifica a través del campo de dirección destino (***Destination Address***) que el acceso será solo a la red 132.147.160.0 / 22. El valor del nombre de dirección o de red de dicho campo puede cambiar según el requerimiento del grupo de usuario que se asigne mas adelante. También en esta primera parte se requiere que el servicio sea cualquiera y todo el tiempo. La acción (***Action***) para este acceso se fija en ***SSL-VPN***, para habilitar la selección de grupos de usuarios de tipo ***SSL-VPN*** que tendrán la autorización de acceso por este medio virtual.

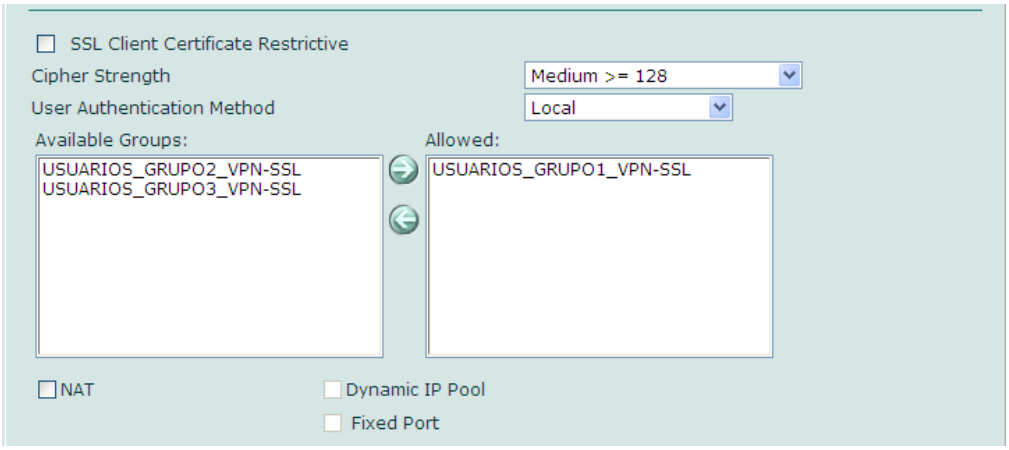


Figura 4.63 Configuración política para el acceso VPN SSL segunda parte

La *figura 4.63* permite observar que para la segunda parte de la configuración de la política se puede seleccionar el nivel de Cifrado SSL de la sesión, en el caso de esta implementación se fijará en el nivel medio (128 bits). Método de autenticación será por medio de cuentas locales del FG300A y los grupos disponibles están en la lista de la parte izquierda; para permitir el acceso se traslada el grupo o grupos que requieran este tipo de acceso.

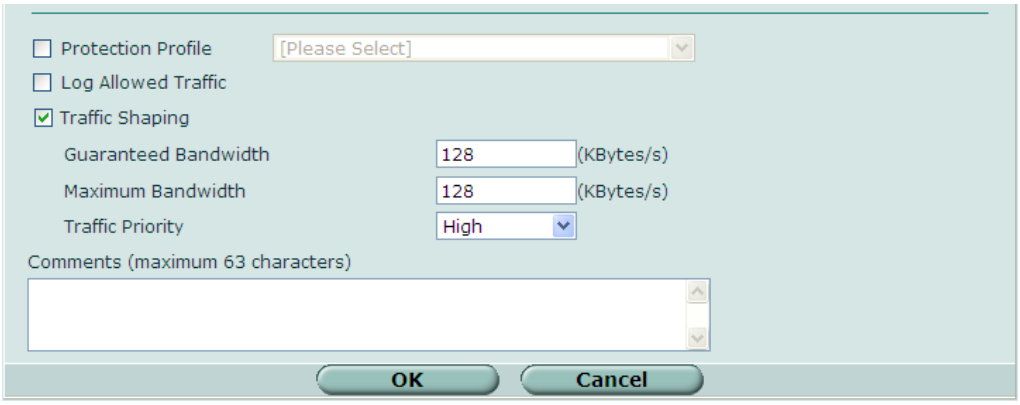
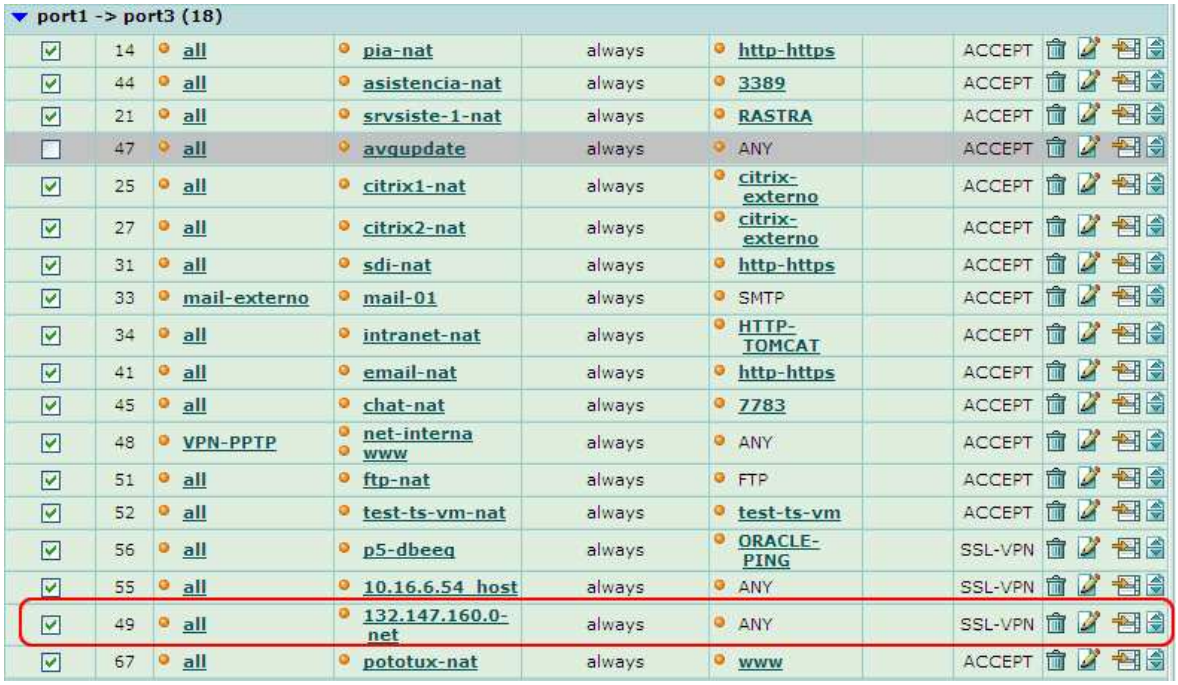


Figura 4.64 Configuración política para el acceso VPN SSL tercera parte

En la tercera parte de esta configuración se especificará el control de tráfico el mismo que se fijará en 128 kbps como capacidad garantizada y máxima, de requerir un incremento de este valor se lo realizará con las mismas consideraciones realizadas para la política de VPN PPTP para el control de tráfico (Ver *figura 4.64*).



port1 -> port3 (18)

☑	14	all	pia-nat	always	http-https		ACCEPT
☑	44	all	asistencia-nat	always	3389		ACCEPT
☑	21	all	srvsiste-1-nat	always	RASTRA		ACCEPT
☐	47	all	avgupdate	always	ANY		ACCEPT
☑	25	all	citrix1-nat	always	citrix-externo		ACCEPT
☑	27	all	citrix2-nat	always	citrix-externo		ACCEPT
☑	31	all	sdi-nat	always	http-https		ACCEPT
☑	33	mail-externo	mail-01	always	SMTP		ACCEPT
☑	34	all	intranet-nat	always	HTTP-TOMCAT		ACCEPT
☑	41	all	email-nat	always	http-https		ACCEPT
☑	45	all	chat-nat	always	7783		ACCEPT
☑	48	VPN-PPTP	net-interna www	always	ANY		ACCEPT
☑	51	all	ftp-nat	always	FTP		ACCEPT
☑	52	all	test-ts-vm-nat	always	test-ts-vm		ACCEPT
☑	56	all	p5-dbeeq	always	ORACLE-PING		SSL-VPN
☑	55	all	10.16.6.54_host	always	ANY		SSL-VPN
☑	49	all	132.147.160.0-net	always	ANY		SSL-VPN
☑	67	all	pototux-nat	always	www		ACCEPT

Figura 4.65 Ubicación de la política de VPN SSL

Una vez terminada la configuración de la política, ésta se agrega en la lista de políticas que le corresponde. Como se muestra en la *figura 4.65* se puede identificar las políticas de tipo SSL por su valor de ***SSL-VPN*** en la columna que corresponde a la acción tomada en dicha política. En la *figura 4.65* también se puede apreciar que la política ingresada se ubica al final de las políticas del mismo tipo, ya que ésta tiene un ámbito más general que las dos anteriores.

4.4.3 CONFIGURACIÓN EN EL FORTINET FG300A PARA ESTABLECER VPNs CON IPSEC

Para la puesta a punto del servidor de VPNs para IPSec se debe tener en cuenta que la autenticación en este caso se la realizará a través de un servidor de contraseñas, específicamente un servidor RADIUS y no de manera local como se lo ha estado realizando con los servidores VPN para PPTP y SSL.

Otro aspecto a tomar en cuenta es el relacionado a la topología de conexión. Los dos primeros servidores (VPN PPTP y VPN SSL) se han configurado para acceso remoto, es decir, desde un equipo de usuario con conexión a Internet, éste realiza mediante un software cliente el requerimiento del establecimiento de la VPN al

FG300A de la E.E.Q.S.A., pero solo lo hace para un equipo. En VPN IPSec se utilizará dos topologías de conexión, la primera será en acceso remoto es decir similar a los dos servidores anteriores, y la segunda será con *LAN – LAN*, lo cual implica ciertas diferencias en los parámetros de configuración y otras consideraciones respecto a la autenticación de usuarios que se revisará más adelante.

Entonces antes de iniciar con la configuración de IPSec, se iniciará con la instalación y puesta en marcha de un servidor de autenticación RADIUS para los usuarios de acceso remoto.

4.4.3.1 Instalación y configuración de un servidor RADIUS

La implementación de este servidor de autenticación va dirigida hacia los usuarios que trabajarán sobre la topología de acceso remoto.

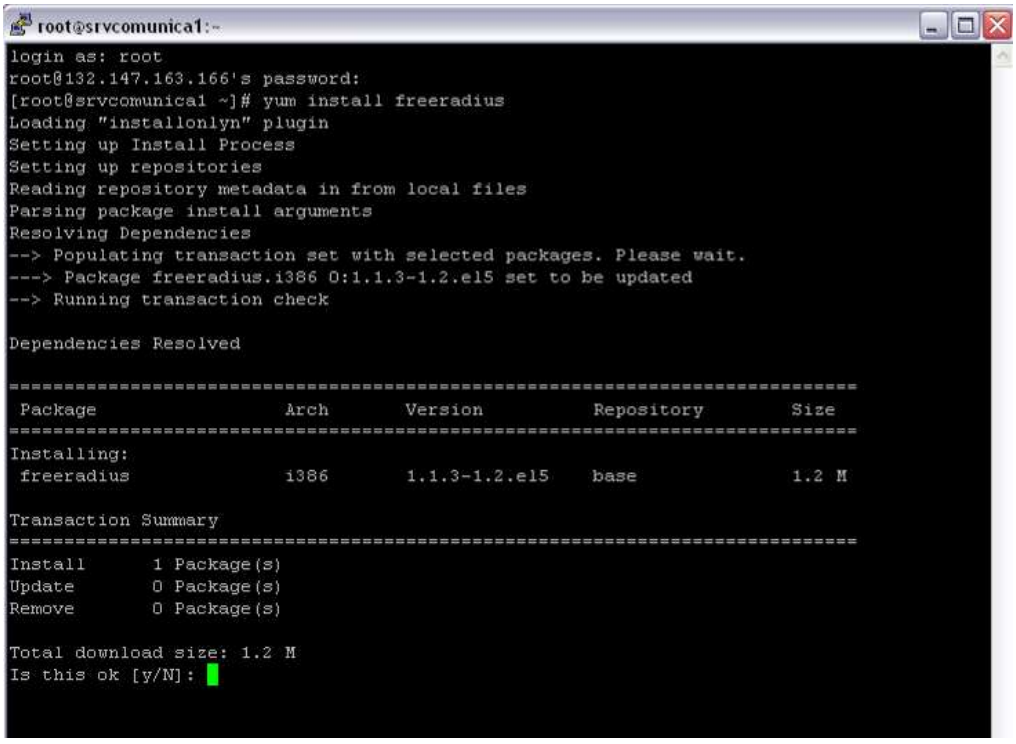


Figura 4.66 Información del paquete de instalación de la aplicación freeRadius

La versión que se utilizará será la prevista para la distribución Linux *Centos* en su versión 5.2. Se justifica el haber escogido esta distribución de Linux por tener un

soporte adecuado en el manejo e implementación de servidores. Hay que anotar que cuenta con una versión de *kernel* similar a la versión de *Linux Red Hat Enterprise 5* que es una plataforma ampliamente reconocida para servidores.

El Linux por lo pronto será instalado y configurado como un equipo virtualizado y residirá en un computador del departamento de Comunicaciones y Soporte que está dentro de la red de la E.E.Q.S.A. A este servidor se le configurará en su interfaz Fast-Ethernet la dirección IP 132.147.163.166 y que está disponible para su utilización.

La configuración del Linux será básica y no tendrá seguridad configurada; este aspecto se lo tratará posteriormente.

Instalado y puesto en funcionamiento el sistema operativo *Linux CentOS 5.2*, se procede a instalar el servicio RADIUS, que no es más que una aplicación gratuita de nombre *freeRadius* en su última versión. Dentro del paquete de aplicaciones del Linux no viene preinstalado este servicio, así que se lo hará a través de la consola ejecutando el comando *yum install freeradius*. Previamente el Linux debe estar conectado al Internet ya que este comando busca las actualizaciones de *freeRadius* en una dirección en el Internet.

Figura 4.67 Información de instalación de la aplicación freeRadius

En la *figura 4.66* se puede observar que desde la consola se ha ejecutado el comando *yum install freeradius* y que al ejecutar pone en contacto al servidor con

los repositorios del Internet que tienen este paquete y luego el usuario acepta la descarga del paquete.

Figura 4.68 Administrador de servicios en Linux CentOS 5.2

El paquete de instalación es descargado y se procede a iniciar la instalación. El paquete *freeRadius.i386* versión *1.1.3-1.2.el5* es instalado (Ver *figura 4.67*) y el servicio ha quedado ha disposición del usuario para que éste configure y ejecute en los modos que dispone la aplicación.

Con el *freeRadius* se trabajará en dos opciones de ejecución para el servicio de autenticación. El primero es a través del administrador de servicios de Linux, donde el servicio asociado al *freeRadius* se agregó y desde el que se puede personalizar la puesta en marcha del servicio (Ver *figura 4.68*).

La segunda opción de ejecución del servicio es en modo *debug* por medio de líneas de comando en la consola. En esta opción es posible visualizar el comportamiento y la actividad del proceso de autenticación de los usuarios de la VPN IPSEC. La *figura 4.69* muestra el estado de espera en el que se encuentra la consola al ejecutar la línea de comandos *radiusd –X*.

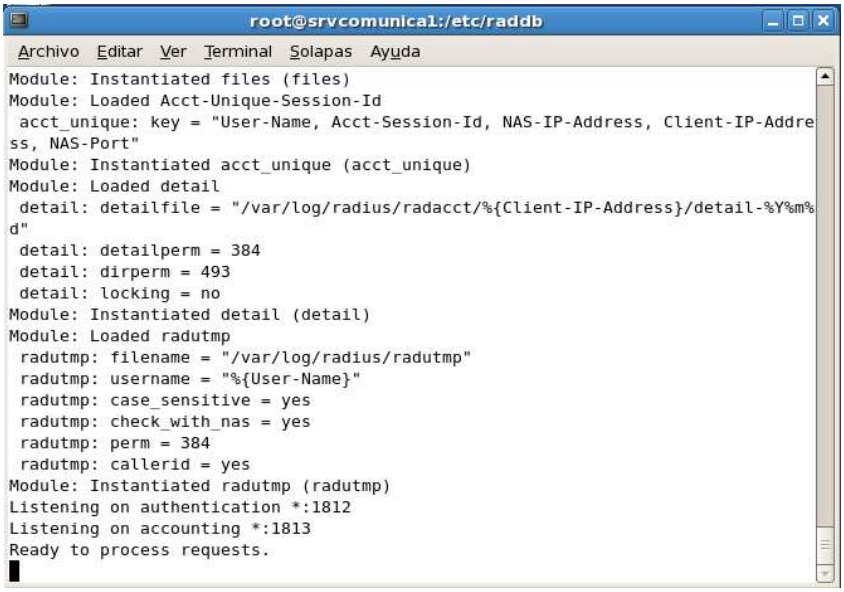


Figura 4.69 Proceso radiusd en espera de requerimientos de autenticación de usuarios VPN IPSEC

Antes de que este servicio se haya puesto en ejecución, se realizaron las respectivas configuraciones en los archivos correspondientes a cuentas de usuario, clientes y configuración general del servicio RADIUS.

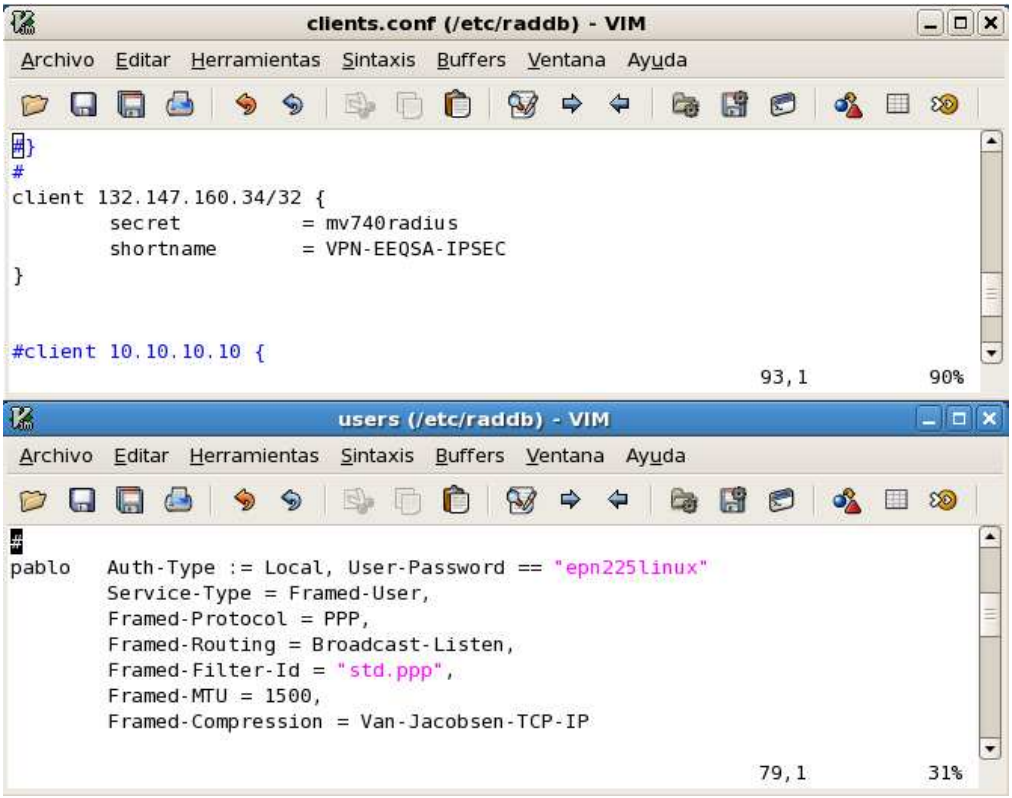


Figura 4.70 Fragmentos de los archivos de configuración para el servicio RADIUS

En la *figura 4.70* se ilustra la configuración de estos archivos para la autenticación de usuarios. En la parte superior se puede observar el archivo ***clients.conf*** donde se definen los clientes del servidor RADIUS; en este caso el cliente es el FG300A desde su interfaz de red interna, por lo que se especifica la dirección IP del puerto 3, también se observa un nombre de identificación de la conexión. En la parte inferior de la *figura 4.70* se observa un fragmento del archivo ***users*** donde se define las cuentas de usuario para su respectiva autenticación. La cuenta de usuario que se observa utiliza una plantilla de parámetros recomendados para este tipo de conexiones. A más de la cuenta de usuario presentada se ha definido las siguientes cuentas de usuario:

- **carreca**. Para usuarios de recaudación de los CARs.
- **operador**. Cuenta de usuarios para los operadores de la E.E.Q.S.A. que trabajan en el campo.
- **ejecutivo**. Cuenta de usuario para empleados y ejecutivos de la E.E.Q.S.A.
- **administrador**. Cuenta de usuario para los administradores de sistemas informáticos, y comunicaciones y redes de la E.E.Q.S.A.

Estas cuentas de usuario utilizan la misma plantilla de parámetros que el primer usuario. El archivo de configuración ***radiusd.conf*** no ha sufrido modificaciones en su configuración inicial, simplemente se lo ha revisado para verificar si éste contiene los vínculos con los archivos ***users*** y ***clients.conf***, así como los módulos correspondientes a la autenticación con los protocolos PAP y CHAP, y de lo que se puede indicar que si cuenta con los módulos respectivos.

4.4.3.2 Configuración de IPSec para Clientes de Acceso Remoto

La configuración de IPSec en el FG300A se puede implementar de manera manual o automática con el protocolo IKE en dos fases. Este trabajo se basará en la implementación de enlaces VPN IPSec con el protocolo de intercambio de llaves automático IKE.

La fase 1 permite determinar la autenticidad de quien requiere realizar el enlace VPN; para lo cual se muestra los campos de configuración en la *figura 4.71*:

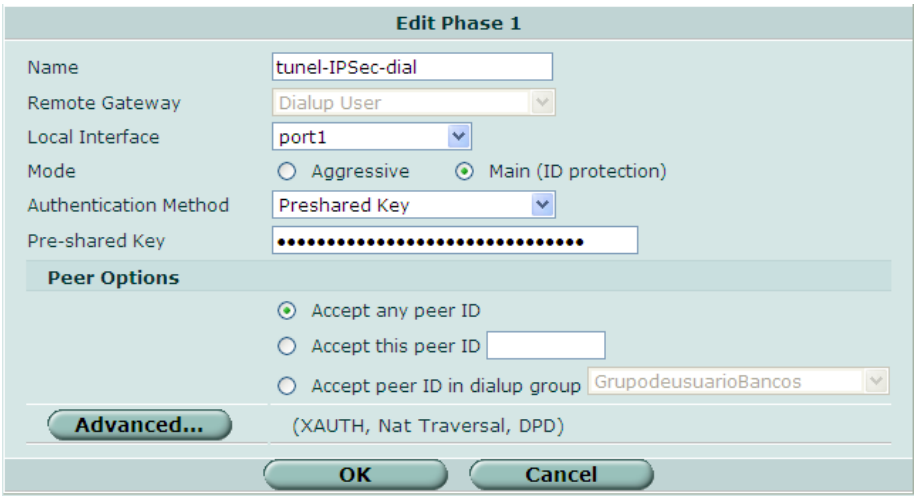


Figura 4.71 Configuración IPSec para Acceso Remoto Fase 1 (Primera Parte)

- ***Name***. Nombre que identifica el túnel en su fase 1 de negociación.
- ***Remote Gateway***. La opción se fija en ***Dialup User***. Es el tipo de equipo remoto para establecer el túnel con el FG300A. En acceso remoto el equipo que solicita la conexión lo hace a través de la aplicación FortiClient.
- ***Preshared Key*** y ***RSA Signature***. Dentro de esta fase el túnel VPN necesita ser identificado, especificar el método de autenticación, que será con clave compartida.
- ***Mode***. Se fija en la opción ***Main*** para que la información de autenticación viaje encriptada.
- ***Autentication Method***. Se puede escoger entre clave compartida (***Preshared Key***) o una firma RSA (***RSA Signature***). Se selecciona ***Preshared Key*** ya que para la opción ***RSA Signature*** se necesita un servidor de certificados digitales el cual por el momento no está implementado.
- ***Preshared Key***. Clave en común entre el FG300A y el equipo remoto para iniciar el proceso de autenticación.
- ***Peer Options***. Por el momento se seleccionará la opción ***Accept any peer ID*** ya que a través de la configuración avanzada de esta fase 1 en el campo ***User Group***, se asociará un grupo de usuarios previamente

configurados y que tienen acceso a la red corporativa por este medio (Ver *figura 4.72*), de ser necesario se escalará a este tipo de registro fijando la opción a una más específica para el identificador del par de conexión de la VPN IPSec para un mejor control.

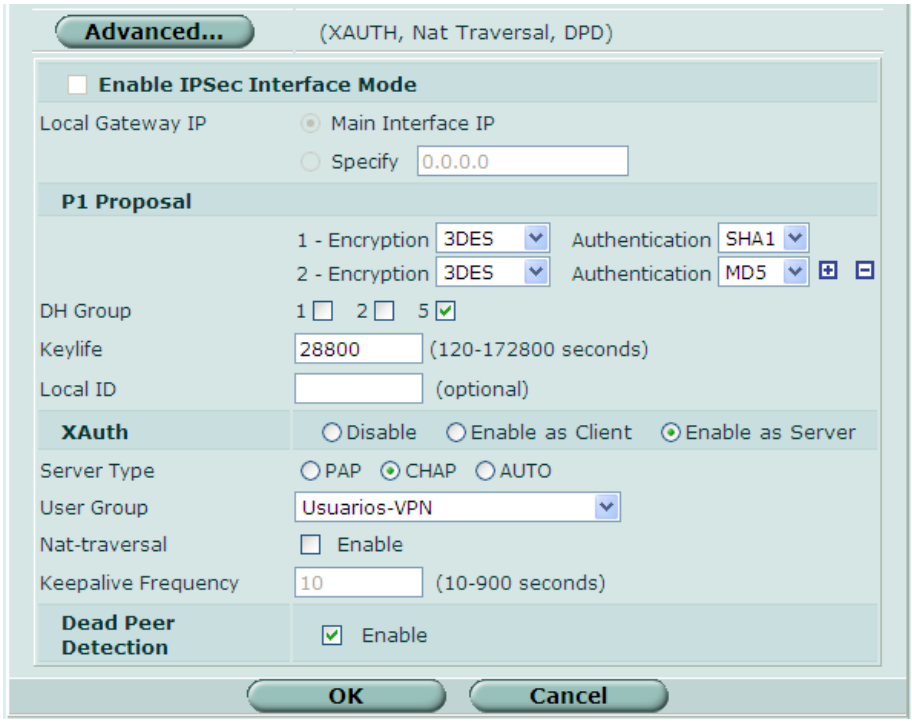


Figura 4.72 Configuración IPSec para Acceso Remoto Fase 1 (Segunda Parte)

En las opciones avanzadas se especifica los algoritmos de cifrado y autenticación para la conexión, así como el grupo *Diffie-Hellman* (***DH Group***) para la generación de las claves y por último el tipo de autenticación extendida a nivel de usuario.

Se han fijado parámetros de seguridad robustos tanto en cifrado (***Encription***) con 3DES y de autenticación (***Authentication***) con SHA1; el grupo DH se fija en 5. Dependiendo de la respuesta del enlace y el cliente se podrá ir modificando estos parámetros para un mejor desempeño en el establecimiento de la comunicación.

En el grupo de opciones de ***XAuth*** se especifica que se activará al FG300A como servidor de autenticación; el FG300A permitirá el establecimiento de conexión cuando el servidor RADIUS con dirección IP 132.147.163.166 lo autorice. Entre el

servidor RADIUS y el FG300A se utilizará el protocolo CHAP para la autenticación de usuarios que corresponden al grupo **Usuarios-VPN** del campo ***User Group***. Si el par IPSec remoto ha dejado de funcionar se activa la opción ***Dead Peer Detection*** con lo que se podrá detectar la no presencia del par remoto y por consiguiente el FG300A terminará la sesión evitando un consumo innecesario de tráfico en la red, procesamiento y consumo de memoria del equipo.

Como se verá más adelante el usuario utilizará el cliente para conexiones VPN FortiClient, el cual soporta los algoritmos de cifrado y autenticación fijados en ***P1 Proposal*** de la configuración IPSec.

En resumen, la fase 1 de la configuración permite establecer un canal seguro para luego; en la fase 2, negociar mecanismos de seguridad y de transporte de los datos que el usuario necesita.

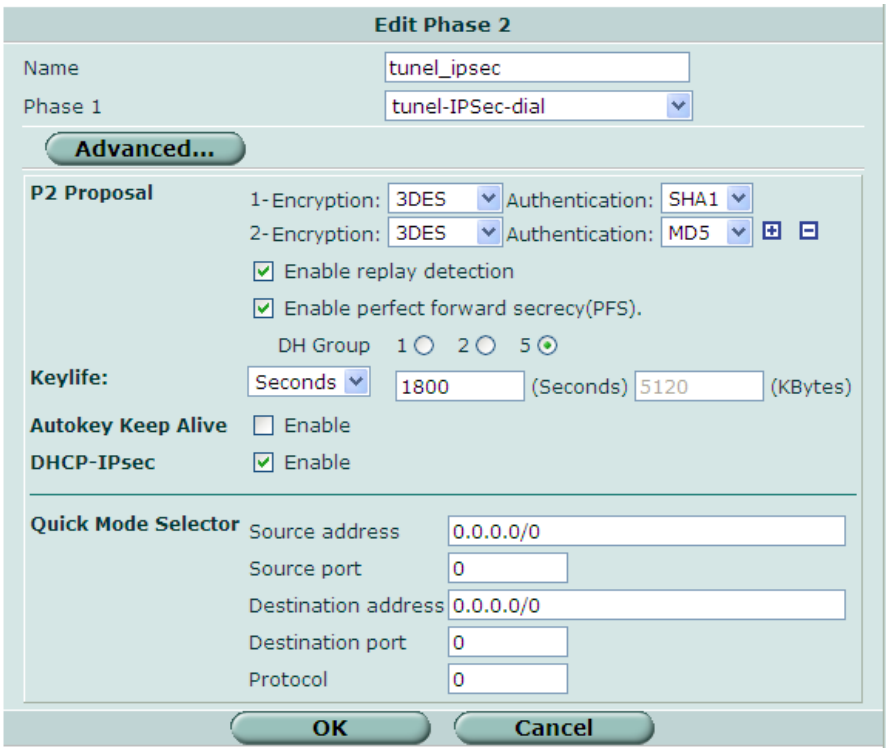


Figura 4.73 Configuración IPSec para Acceso Remoto Fase 2

La fase 2 debe estar referenciada a una configuración de fase 1. De las configuraciones de fase 1 disponibles se debe escoger una para seguir con la

configuración, para este caso se tiene configurada una fase 1 con nombre **tunel-IPSec-dial** (Ver *figura 4.71*) con el cual se inicia la configuración de la fase 2 (Ver *figura 4.73*).

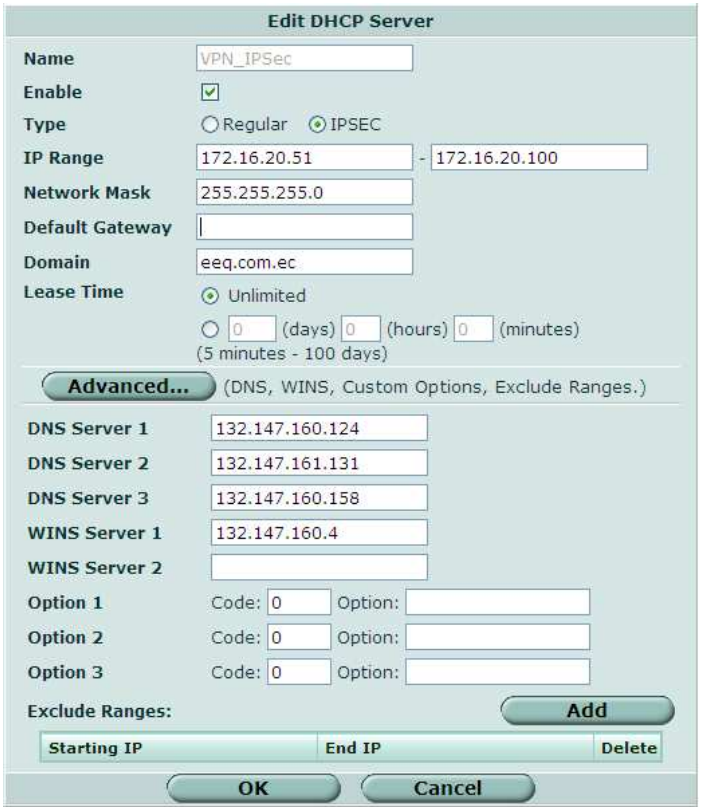


Figura 4.74 Configuración servidor DHCP para conexiones VPN IPSec de Acceso Remoto

A la fase 2 se le asigna el nombre **tunel-ipsec**. En este nivel se ha fijado el algoritmo de cifrado en 3DES y el de autenticación en SHA1, permitiendo una seguridad robusta como se lo ha establecido en la fase 1. Esta configuración que corresponde al ***P2 Proposal*** es igual al ***P1 Proposal*** en la fase 1, sin embargo puede ser diferente ya que la negociación de cada fase es independiente respecto a los algoritmos utilizados en cada fase.

En la *figura 4.73* también se puede observar que se selecciona la opción de ***DHCP-IPSec***. En las configuraciones para los servidores VPN PPTP y SSL se habilitaron rangos de la red 172.16.20.0 / 24, para que los usuarios obtengan una dirección de manera dinámica. En la configuración de IPSec se especifica un servidor DHCP, el cual es configurado desde ***System→DHCP↔Service***, en esta

página se puede seleccionar el puerto donde se necesite configurar un servidor DHCP; para éste caso es el puerto 1 de acceso a Internet. En la página de configuración se añade un servidor y se procede a configurar el direccionamiento según lo diseñado para este tipo de VPN (*Ver figura 4.74*).

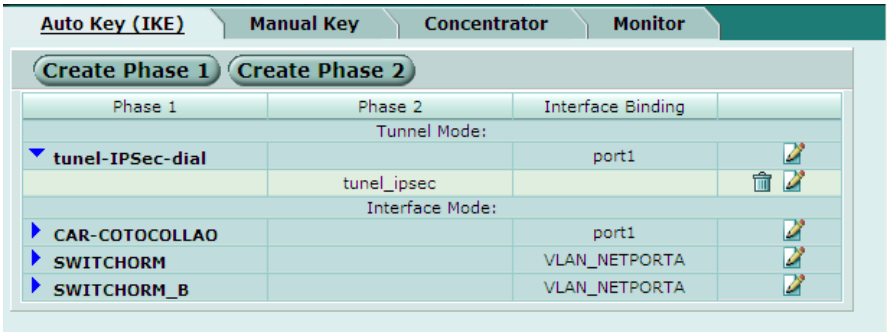


Figura 4.75 Listado de túneles VPN IPSec configurados

Para que este servidor tenga un contexto en VPN IPSec se debe seleccionar la opción ***IPSEC*** en el campo ***Type***.

Una vez finalizada la configuración VPN IPSec para acceso remoto, ésta puede ser observada en la lista de conexiones VPN IPSec disponibles. En *figura 4.75* se observa el listado de conexiones VPN IPSec.

4.4.3.3 Configuración la política de *firewall* para VPN IPSec de Acceso Remoto

Una vez finalizada la configuración de VPN IPSec para Acceso Remoto se procede a configurar una política de *firewall* para esta conexión. Para IPSec el sentido de la conexión es desde un puerto interno (Puerto 3) hacia un puerto de red externa (Puerto 1).

En el campo ***Action*** de la *figura 4.76*, se selecciona la opción IPSEC, lo que genera un grupo de parámetros diferente al de una política normal; uno de estos parámetros es el correspondiente al campo ***VPN Tunnel***, que es una lista de conexiones VPN IPSec disponibles. Si el sentido de los puertos de la política es

correcto, en la lista se podrá escoger el túnel VPN configurado en la sección 4.4.3.2. Todo lo mencionado se puede observar en la *figura 4.76*.

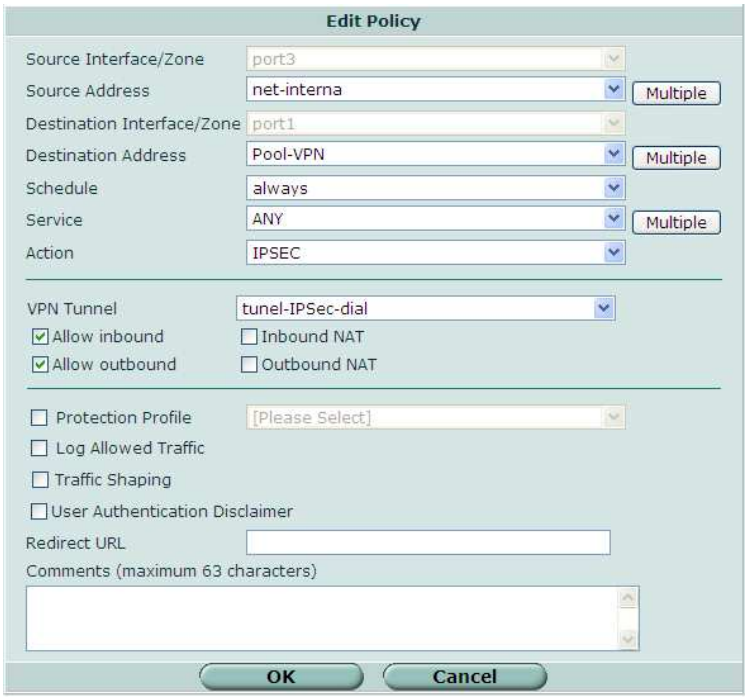


Figura 4.76 Configuración política de firewall para VPN IPSec de Acceso Remoto

Para finalizar se activan las opciones para permitir el tráfico en doble sentido (***Allow inbound*** y ***Allow outbound***).

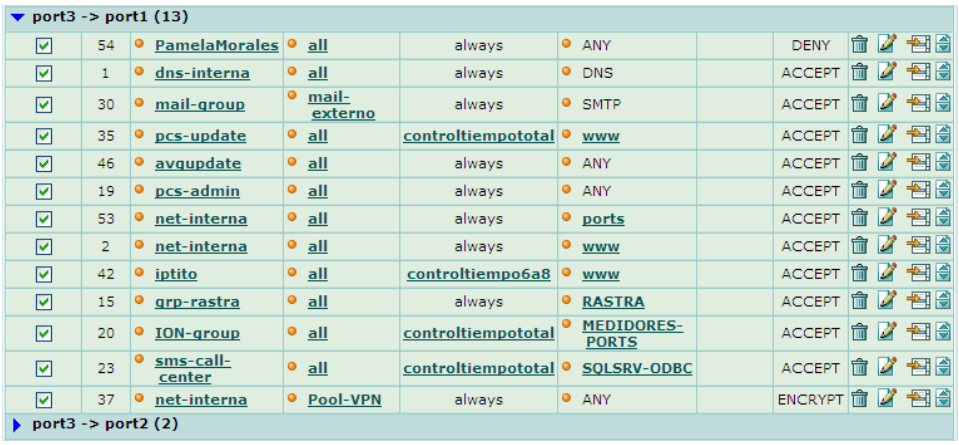


Figura 4.77 Listado de políticas desde el puerto 3 hacia el puerto 1

La dirección origen seleccionada en la política corresponde a toda la red interna o corporativa de la E.E.Q.S.A. (**net-interna**) y la dirección origen corresponde a la

red para enlaces VPN (**Pool-VPN**). Considerando que el grupo de direcciones **net-interna** es muy amplio y el servicio requerido es cualquiera (***ANY***), se lo considera como una política de contexto general, por lo que ocupará el último lugar de la lista de políticas. En el correspondiente a ***Action***, se puede apreciar que está etiquetado con ***ENCRYTP***, lo que indica que se trata de un túnel VPN IPSec (Ver *figura 4.77*).

4.4.3.4 Configuración IPSec para Clientes en modo de conexión *LAN - LAN*

En esta configuración se tomará como referencia el requerimiento de conexión del CAR Cotocollao. El modo de conexión de este CAR es a través de una empresa que presta sus servicios de datos, es decir, que la empresa intermediadora de nombre SWITCHORM con residencia en la ciudad de Guayaquil, solventará todo lo correspondiente a servicio de procesamiento de datos y enlaces de comunicación entre el CAR y la E.E.Q.S.A.; para lo cual SWITCHORM ha contratado el servicio de enlace de Internet con la empresa PORTA, este enlace permite no ocupar el acceso a Internet corporativo de las dos empresas, con lo cual este enlace se convierte en un canal exclusivo para el túnel VPN.

Los enlaces de última milla fueron instalados tanto en el centro de cómputo de la E.E.Q.S.A. como también en SWITCHORM, todos a cargo de esta empresa, estos enlaces de última milla tienen una capacidad de 128 kbps cada uno con tecnología de banda ancha ADSL.

En esta implementación se configurará el *switch* de capa 2 para los enlaces de extranet, que por el momento se conectará en el puerto 5 del FG300A, hasta que se pueda coordinar la migración en su totalidad de los enlaces de extranet. El puerto switch Cisco que se utilizará será el Gi2 (*Gigabit Ethernet 2*).

Para conectar el *switch Cisco Catalyst Express 500* (CE500-EXTRANET) con el FG300A se lo realizará configurando un enlace de *trunk* entre los puertos Gi2 del CE500-EXTRANET y el 5 del FG300A. El CE500-EXTRANET debe ser inicializado y configurado antes de ser instalado en el *rack* 1 de comunicaciones.

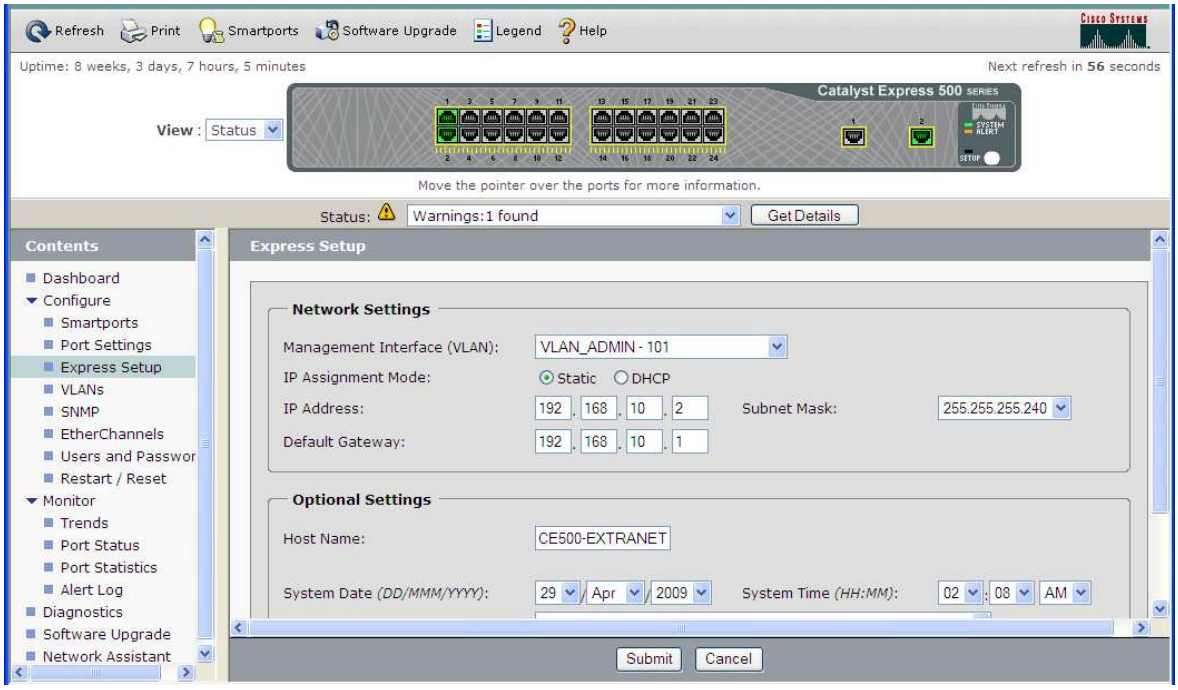


Figura 4.78 Configuración de dirección IP y VLAN en el CE500-EXTRANET

El CE500-EXTRANET se lo inicializa y en la configuración inicial se le ingresa la dirección IP 192.168.10.2 / 28 para la interfaz virtual VLAN 101 de nombre VLAN_ADMIN, tal como se lo ha detallado en la sección 3.7.2 de este proyecto (Ver *figura 4.78*).

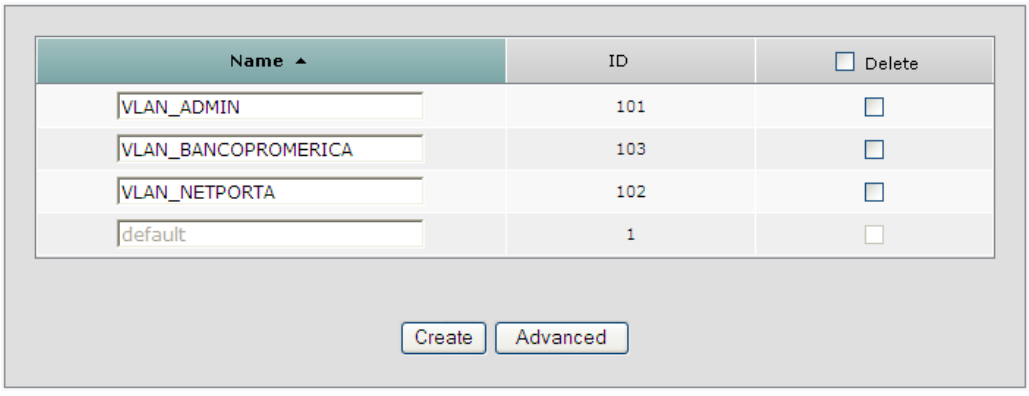


Figura 4.79 Configuración de VLANs en el CE500-EXTRANET

Dentro de esta consola se ha agregado otras VLANs que corresponden a enlaces de los CARs que requieren el acceso hacia la E.E.Q.S.A. La VLAN de nombre VLAN_NETPORTA corresponde al enlace de última milla hacia el Internet que ha

contratado la empresa SWITCHORM; en la *figura 4.79* se muestra esta parte de la configuración.

Para configurar el puerto de *trunk* en el CE500-EXTRANET, es necesario asignarle el rol que tendrá el puerto Gi2, en este caso para que funcione como *trunk* se le asigna el rol de *router*, ya que en escencia es un router el que estará conectado en el mencionado puerto (Ver *figura 4.80*).

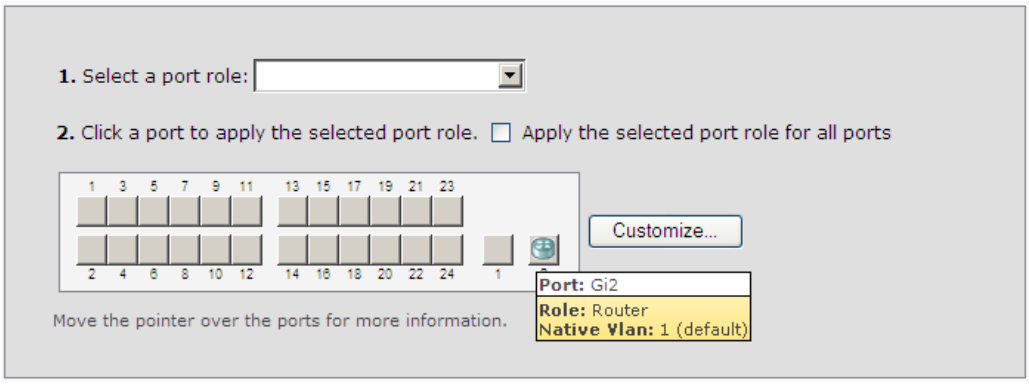


Figura 4.80 Configuración de puerto de trunk en el CE500-EXTRANET

Una vez listo el *switch* de acceso extranet, se procede a configurar las interfaces virtuales en el FG300A las cuales estarán asociadas a las VLANs creadas en el CE500-EXTRANET. Para configurar estos puertos virtuales se debe ir a ***System→Network↔Interface*** y luego de hacer *click* en el botón ***Create New*** se despliega la página de creación para una nueva interfaz. Esta nueva interfaz debe tener un puerto físico de referencia y un identificador (VLAN ID). La *figura 4.81* muestra la configuración de la interfaz virtual asociada a la **VLAN_ADMIN** con identificador 101, la cual está referenciada al puerto físico 5 y que se le asigna la dirección IP 192.168.10.1 / 28, tal como se lo ha especificado en la sección 3.7.3 de este proyecto.

De esta manera se pueden realizar las interfaces virtuales que sean necesarias. La *figura 4.82* permite observar la lista de interfaces virtuales configuradas sobre el puerto 5 del FG300A.

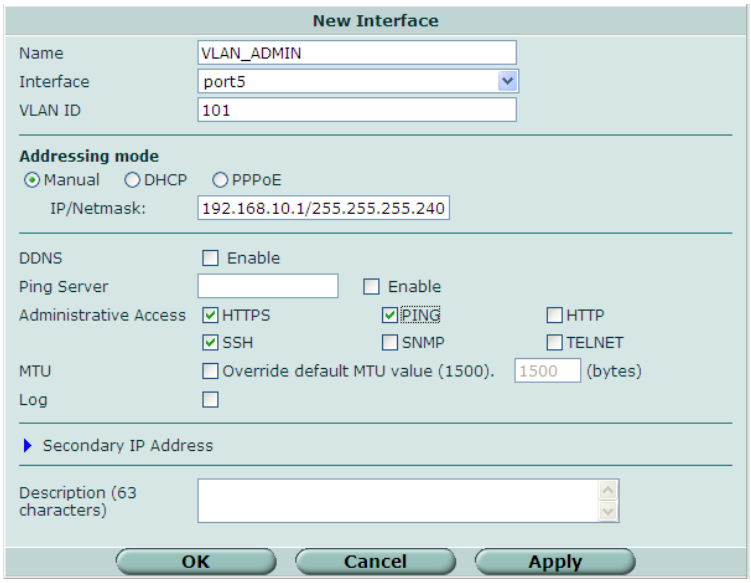


Figura 4.81 Configuración de una interfaz virtual asociada a una VLAN del CE500-EXTRANET

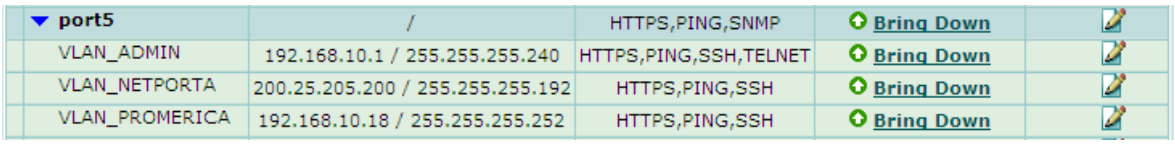


Figura 4.82 Listado de interfaces virtuales asociadas a las VLANs de CE500-EXTRANET

Desde la consola de comandos se puede verificar que las interfaces están activas y responden al comando ***exec ping*** del FG300A (Ver *figura 4.83*).

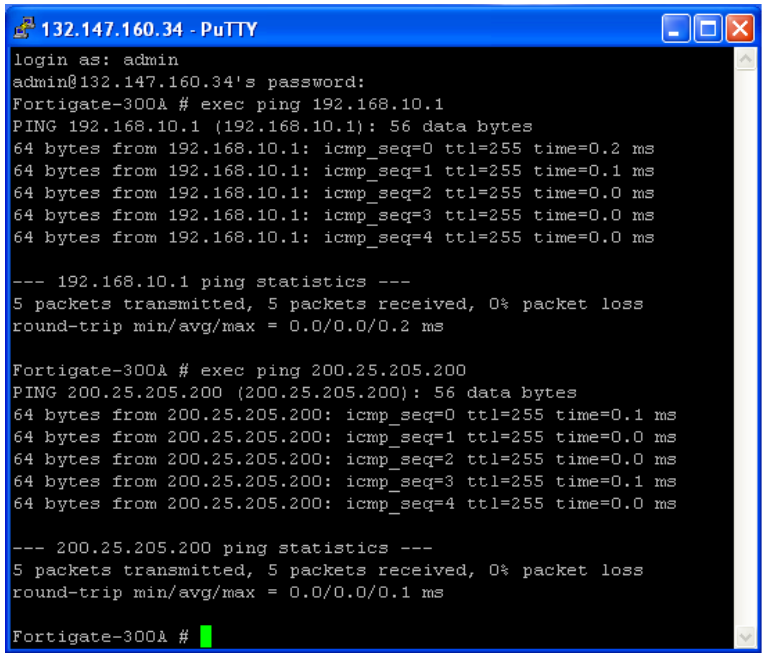


Figura 4.83 Respuesta de CE500-EXTRANET y VLAN_NETPORTA al ping desde CE500-EXTRANET

Con la interfaz virtual configurada y el enlace hacia el Internet con el enlace de última milla de PORTA, el siguiente paso es crear una VPN IPSec, para conectar E.E.Q.S.A. con SWITCHORM.

Al igual que la configuración para acceso remoto se deben establecer 2 fases para la VPN IPSec, ya que el mecanismo de intercambio de llaves será automático utilizando el protocolo IKE.

En la fase 1 (***PHASE 1***) a diferencia de lo configurado en acceso remoto, se debe especificar que el campo ***Remote Gateway*** se debe fijar en ***Static IP Address***, ya que es conocida la dirección IP pública del equipo remoto (dirección IP pública 200.25.202.195) provista por el enlace de PORTA. El método de autenticación se manejará en clave compartida (***Preshared key***) (ver *figura 4.84*).

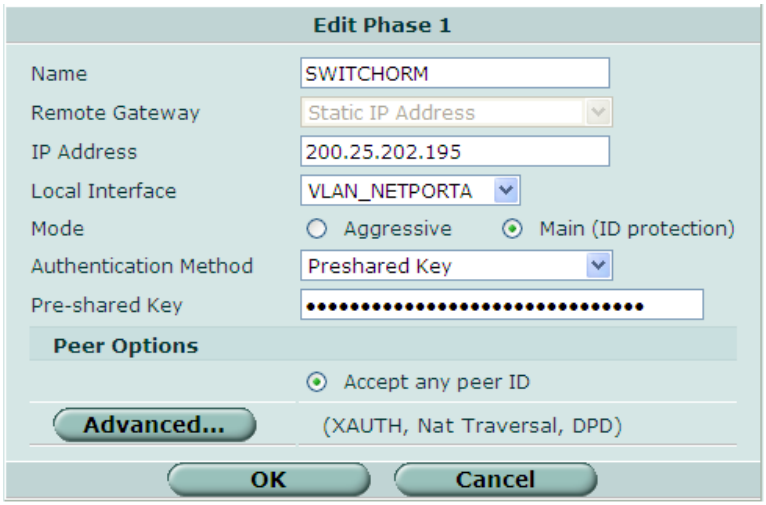


Figura 4.84 Configuración de la fase 1 de IPSec para el enlace con SWITCHORM

En configuración avanzada de la fase 1 (***Advanced***), se habilitará la opción ***Enable IPSec Interface Mode***, de tal manera que la VPN IPSec tendrá una interfaz virtual asociada a la fase 1 de IPSec que es distinta a las interfaces de las VLANs. Con el técnico de contacto en Guayaquil se procedió a establecer los parámetros para esta parte de la configuración. Se quedó de acuerdo en proveerle a la conexión una seguridad robusta utilizando para la encripción el algoritmo 3DES y para autenticación SHA1 (Ver *figura 4.85*).

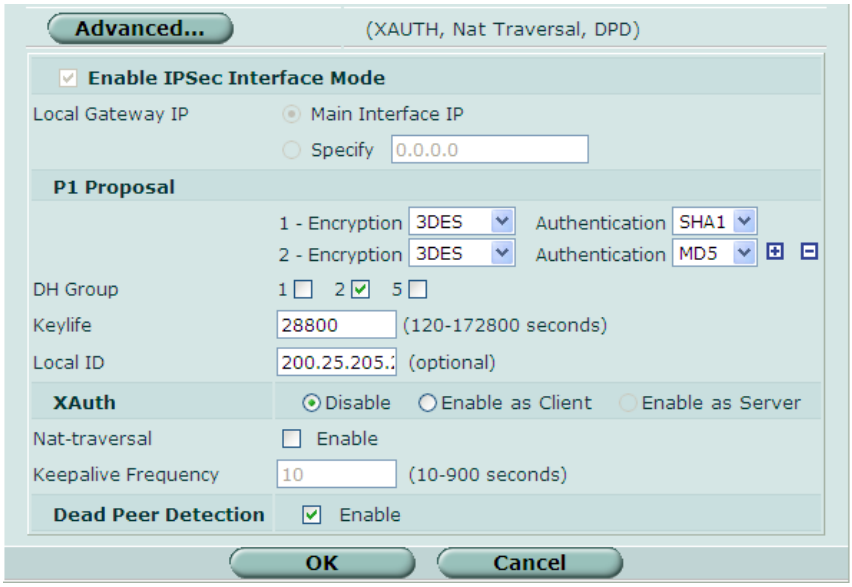


Figura 4.85 Configuración avanzada de la fase 1 para la VPN IPSec de SWITCHORM

En la fase 2 de esta VPN IPSec, se mantiene el esquema de robustez tanto en el cifrado como en la autenticación, y además de esto se especifica la dirección origen (LAN E.E.Q.S.A.) y destino del tráfico (LAN SWITCHORM), todo esto mostrado en la *figura 4.86*.

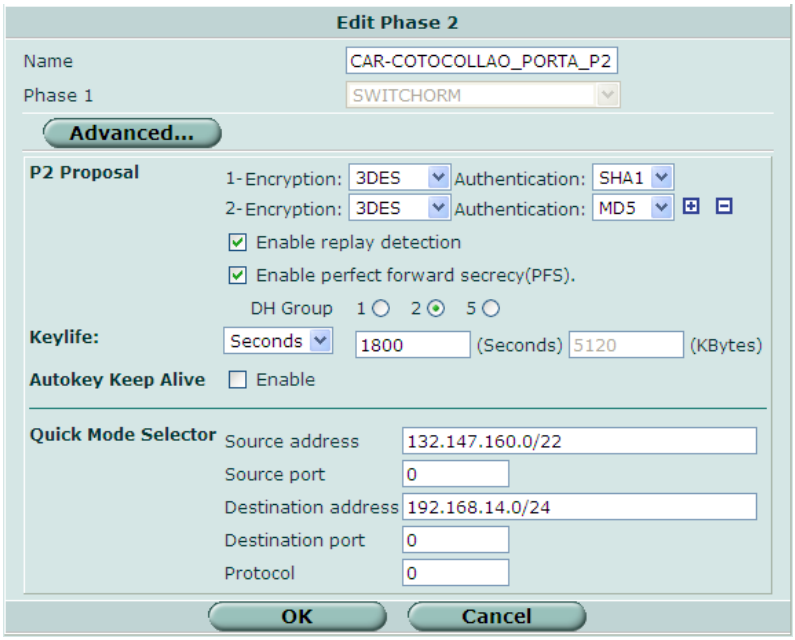


Figura 4.86 Configuración de la fase 2 de IPSec para el enlace con SWITCHORM

4.4.3.5 Configuración la política de *firewall* para VPN IPSec en modo *LAN - LAN*

La política para este tipo de enlaces originará un par de variantes, tanto en la política del *firewall* como en la fase 1 de la VPN IPSec.

Los equipos de conectividad de los CARs, proveedores y otras empresas que conforman la extranet, son de diferentes fabricantes, y si bien la mayoría de los equipos soportan el estándar de protocolos de IPSec, no quiere decir que en el momento de la configuración no se vayan a presentar problemas en el establecimiento de la comunicación.

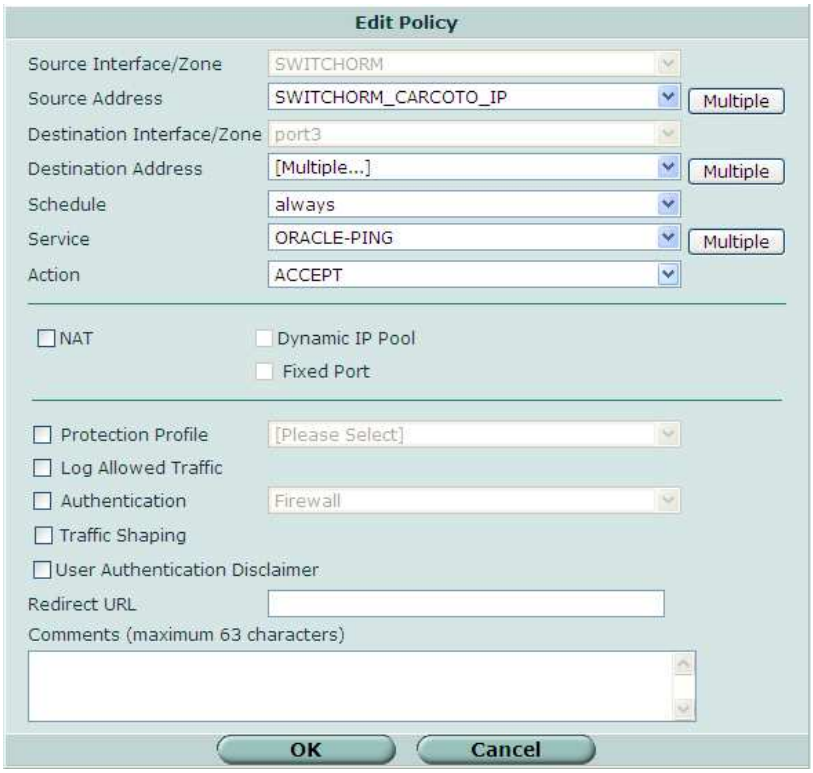


Figura 4.87 Configuración de la política de firewall para el enlace VPN IPSec de tipo LAN to LAN con SWITCHORM

SWITCHORM tiene como equipo final un *firewall* que también es un servidor de VPNs IPSec de marca ZyXEL modelo ZyWALL USG 300. Con este equipo en un inicio el FG300A no se estableció la conexión VPN IPSec en el modo *LAN to LAN*. La configuración inicial señalaba que el campo ***Action*** debe estar fijado en el valor ***IPSEC*** tal como se lo había realizado en el modo de acceso remoto. Una alternativa a esta configuración es que en el campo ***Action*** se fije el valor a

ACCEPT como si fuese una política normal (ver *figura 4.87*). Para que esto funcione es necesario que en la fase 1 en la sección de configuración avanzada se active la opción ***Enable IPSec Interface Mode*** (Ver *figura 4.85*) con lo cual se crea una nueva interfaz virtual de tipo IPSec sobre el puerto 5, es decir sobre este puerto físico explícitamente se declara una interfaz virtual. Con estas dos variantes se estableció la comunicación entre los servidores VPN IPSec.

Además en la configuración de la política se destacan los campos ***Source Address*** que tiene un valor fijado hacia una dirección específica de la red LAN 192.168.14.0 / 24 de SWITCHORM, el campo ***Destination Address*** que tiene fijado múltiples direcciones de hosts de la E.E.Q.S.A. de destino; entre estas direcciones se encuentran las de servidores de base de datos y de un *host* para pruebas de conectividad. Y por último el servicio se ha restringido a los puertos asociados a la conectividad con la base de datos ORACLE y la prueba de conectividad PING (Ver *figura 4.87*).

Figura 4.88 Listado de la política para el enlace VPN IPSec en modo LAN to LAN con SWITCHORM

En una política de tipo ***IPSEC*** solo es necesario que se configure en un sentido de tráfico. Como cambia el tipo de política a ***ACCEPT*** es necesario configurar una política similar pero en el sentido contrario, con esto se podrá tener una comunicación en *full duplex*. La *figura 4.88* muestra que en listado de políticas se ha generado un nuevo grupo de políticas y que corresponde a la interfaz virtual IPSEC **SWITCHORM** hacia el puerto 3.

Figura 4.89 Política en sentido contrario para el enlace VPN IPSec en modo LAN to LAN con SWITCHORM

La *figura 4.89* muestra la política en sentido contrario para poder establecer una comunicación en doble sentido simultáneamente.

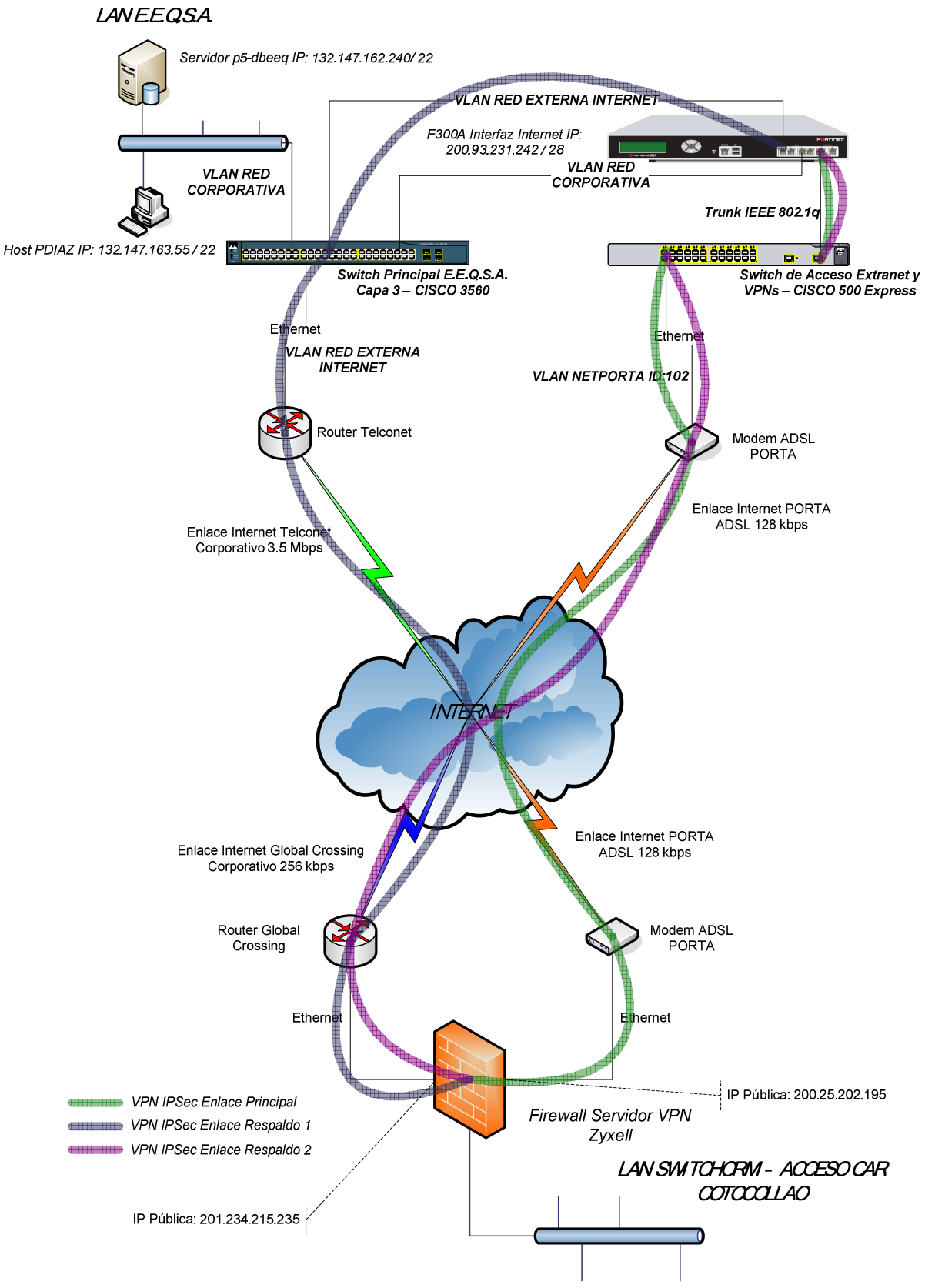


Figura 4.90 Diagrama completo de la topología para VPN IPSec modo LAN - LAN con SWITCHORM

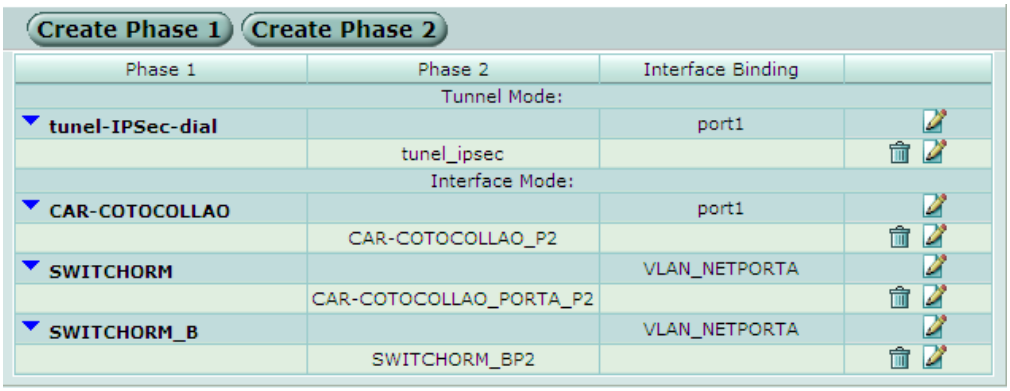


Figura 4.91 Listado de VPN IPSec disponibles

Por cuestiones de redundancia entre la empresa SWITCHORM y la E.E.Q.S.A. los técnicos de estas empresas han quedado de acuerdo en establecer dos respaldos adicionales al principal, los cuales presentan configuraciones similares a la primera VPN, con la diferencia que se utilizan accesos diferentes hacia el Internet en cada VPN. La *figura 4.91* muestra los tres túneles configurados para el acceso con SWITCHORM.

Las *figuras 4.92* y *4.93* muestran los listados de las políticas de todos los enlaces VPN IPSec modo *LAN - LAN*.

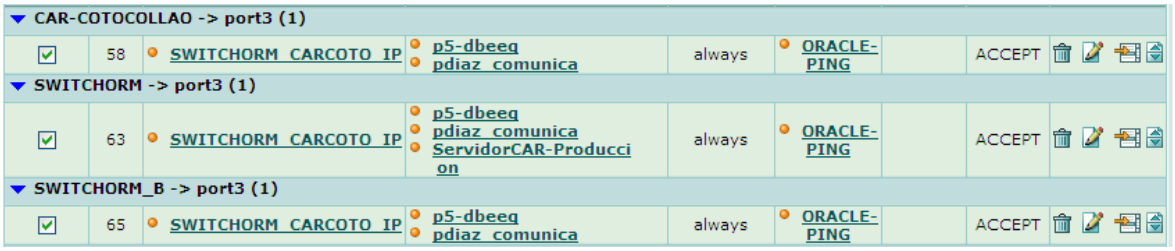


Figura 4.92 Listado de las políticas para VPN IPSec en el primer sentido de tráfico

En la *figura 4.90* se presenta un diagrama con un resumen completo de la topología para el acceso *LAN - LAN* con SWITCHORM que incluye los enlaces de respaldo, última milla, equipamiento y direccionamiento.

port3 -> CAR-COTOCOLLAO (1)							
☑	57	p5-dbeeq pdiaz_comunica	SWITCHORM_CARCOTO_IP	always	ORACLE-PING		ACCEPT
port3 -> SWITCHORM (1)							
☑	64	p5-dbeeq pdiaz_comunica ServidorCAR-Produccion	SWITCHORM_CARCOTO_IP	always	ORACLE-PING		ACCEPT
port3 -> SWITCHORM_B (1)							
☑	66	p5-dbeeq pdiaz_comunica	SWITCHORM_CARCOTO_IP	always	ORACLE-PING		ACCEPT

Figura 4.93 Listado de las políticas para VPN IPSec en el segundo sentido de tráfico

4.5 CONFIGURACIÓN DE VoIP SOBRE REDES PRIVADAS VIRTUALES (*SECURE VoIP*)

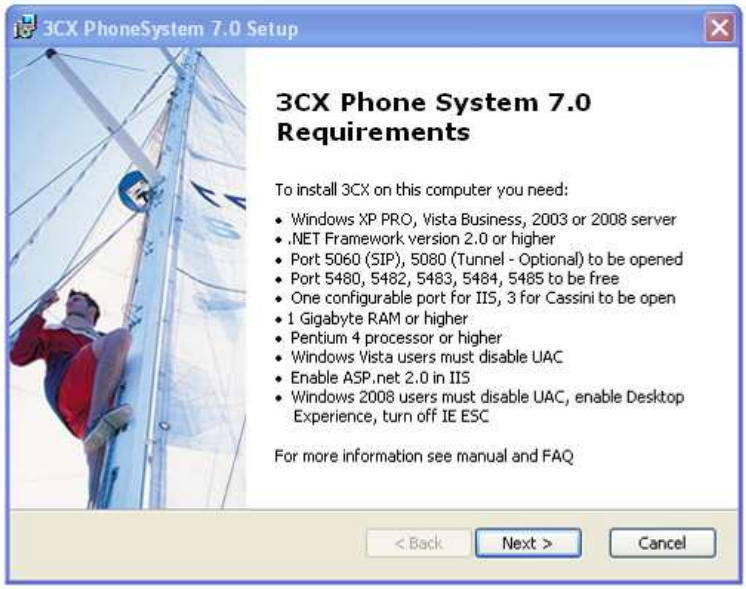


Figura 4.94 Inicialización del asistente de instalación y configuración inicial de la PBX 3CX Phone System 7.0

Para poner en marcha el servicio de telefonía sobre la VPN fue necesario buscar alternativas, ya que el servicio de telefonía IP de la empresa, que fue la idea original, ya no dispone de extensiones actualmente, específicamente por razones de licenciamiento; esto lleva a que se busque aplicativos, uno de éstos fue el de instalar una central de la marca 3CX que se está promocionando a través del Internet, y que para atraer a potenciales usuarios pone a disposición una versión gratuita del servidor de tipo SIP, así como el cliente que es un teléfono en *software* o *softphone*. En la página *web* de 3CX se encuentra disponible este *software*.

En esta configuración se va realizar la implementación de un servidor de telefonía IP sobre un equipo de la red corporativa. El servidor de telefonía 3CX o PBX en software que se tiene disponible utiliza el protocolo estándar SIP para telefonía IP.

El servidor de telefonía es muy útil y en su versión gratuita es limitado, pero para los propósitos de este proyecto es suficiente su funcionalidad.

4.5.1 INSTALACIÓN, CONFIGURACIÓN Y ACTIVACIÓN DE TELEFONÍA IP SIP CON *3CX PHONE SYSTEM 7.0*

El 3CX es una aplicación para sistemas Microsoft Windows, en esta implementación se ha procedido a instalar sobre un computador con las siguientes características:

- Marca: HP Compaq
- Modelo: dc5100
- Procesador: Intel Pentium 4 Hyper *HyperThreading* 3.00 Ghz
- Capacidad Memoria RAM: 1 GB
- Capacidad Disco Duro: 160 GB
- Tarjeta de Red: *Broadcom Gigabit Ethernet*
- Sistema Operativo: *Microsoft Windows XP Professional SP2*
- Aplicación Necesaria 1: *Internet Information Server v5.1*
- Aplicación Necesaria 2: *Microsoft.NET Framework 2.0*

Al iniciar el asistente de instalación y configuración de la aplicación de servidor de telefonía 3CX indica los requerimientos en *hardware* y *software* que necesita del servidor (Ver *figura 4.95*). El equipo cuenta con los requerimientos solicitados; lo siguiente es configurar entre otros aspectos parámetros como: idioma, nueva central o actualización, número de dígitos para las extensiones y el nombre o dirección IP del servidor. Lo que interesa básicamente en esta configuración inicial, es establecer el número de dígitos, que en este caso será de 4, con lo cual se mantiene el esquema de numeración que tiene la E.E.Q.S.A. en su sistema de telefonía corporativo. El nombre o dirección del servidor donde se instalará y al

que los clientes o extensiones deberán referenciar para su respectivo registro, es el equipo *pdiaz.eeq1* que tiene la dirección IP 132.147.163.55 (Ver *figura 4.96*).

Figura 4.95 Configuración del nombre del servidor de telefonía SIP 3CX

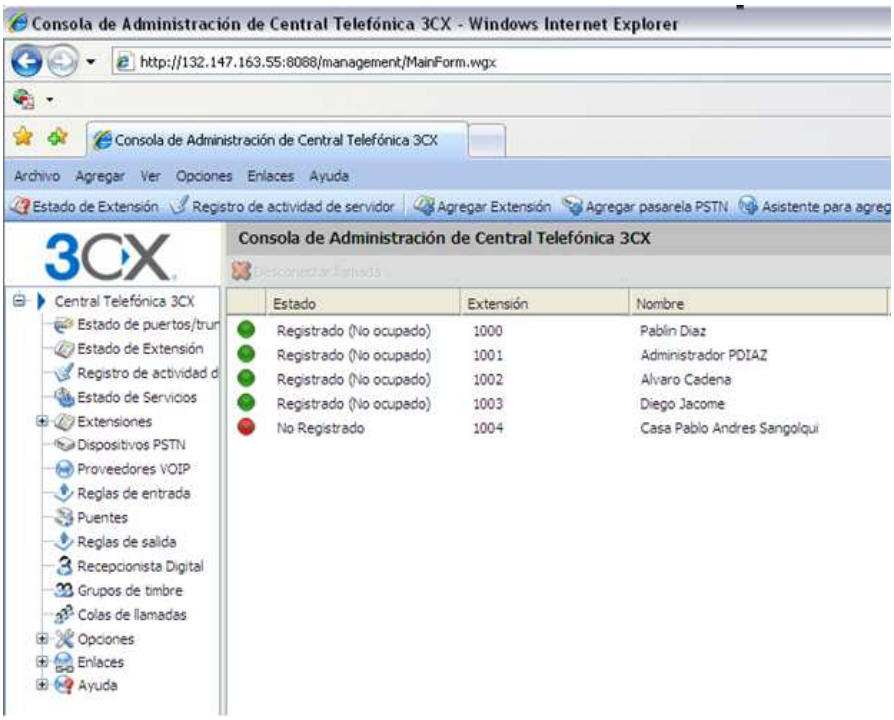


Figura 4.96 Consola de administración y configuración de la PBX SIP 3CX

Se finaliza la instalación agregando nuevas extensiones, que en este caso será de 4 dígitos y por el momento se utilizarán las extensiones 1000 hasta la 1010.

El servicio de PBX cuenta con una administración a través de un servidor *web* que está incorporado en el sistema 3CX, en el cual se ha configurado el puerto TCP 8088 para el respectivo acceso por medio de un navegador *web* como Internet Explorer 7, y es en donde se pueden configurar varios parámetros incluyendo nuevas extensiones. En la *figura 4.97* se puede observar la consola de administración en la que se encuentran listados los números y usuarios de las extensiones telefónicas inicialmente configuradas.

4.5.2 CONFIGURACIÓN DEL CLIENTE DE TELEFONÍA IP SIP *3CX VoIP CLIENT*

Para la instalación y configuración del cliente es necesario que el equipo cuente al menos con un *hardware* que soporte *Windows XP Professional SP2* y conexión de red Ethernet. La instalación y configuración del cliente es sencilla y breve. Hay que anotar que en esta versión gratuita del cliente 3CX se utiliza 3 códecs de voz que son: el G.711 en sus versiones de Ley U y Ley A y G.728 o GSM (Ver *figura 4.81*).

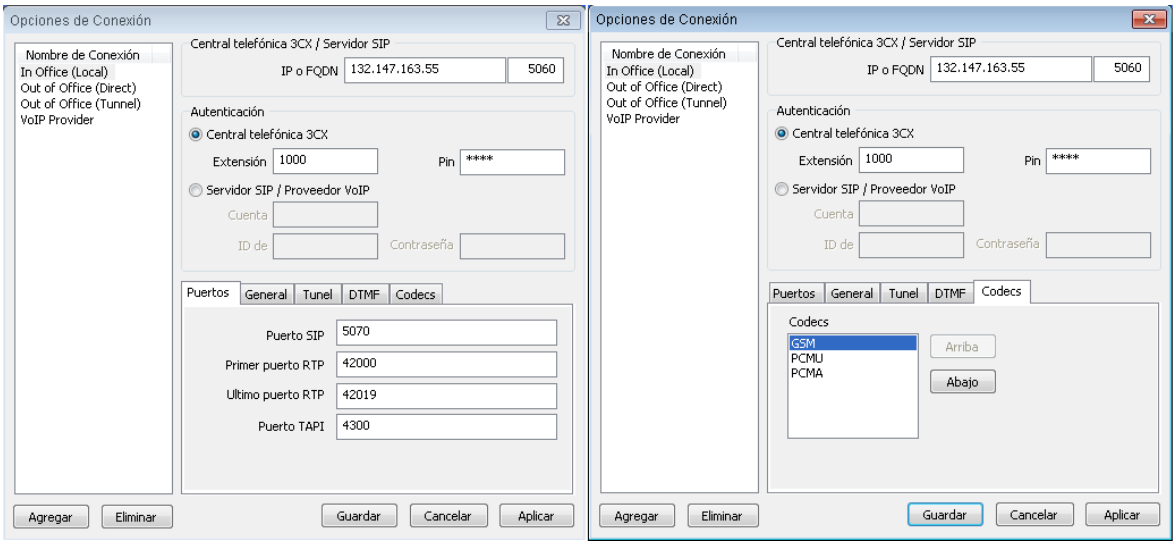


Figura 4.97 Configuración de puertos y códecs del cliente 3CX

El códec G.711 tiene una ocupación de ancho de banda de 64 kbps, lo que para ambientes LAN no es un problema, pero sí para ambientes de red WAN o más aún si la red que se va a utilizar es el Internet. Para esto se utilizará el G.728 o GSM que genera un ancho de banda de entre 12 kbps y 15 kbps que es adecuado para los propósitos de análisis de tráfico de este proyecto.

Como se puede observar en la *figura 4.98* se debe especificar la dirección del servidor y el puerto de inicialización del servicio. Los valores de estos puertos ya están pre-configurados. El cambio que se debe realizar es respecto al códec, el cual ya se analizado y resuelto que deberá ser GSM.

Figura 4.98 Cliente de telefonía IP SIP 3CX listo para el servicio

Como se puede apreciar en la *figura 4.99* el estado del cliente indica el número de extensión que corresponde y además la lista de extensiones disponibles.

Al ejecutar este cliente de telefonía IP, no es necesario especificar otros parámetros, como por ejemplo si está o no dentro de la red local. Al formar la VPN con cualquiera de las tecnologías propuestas, el equipo que ejecuta el cliente sólo tiene que estar conectado al Internet y realizar un enlace VPN para que esta aplicación de telefonía IP se conecte al servidor que se encuentra en la Matriz Las Casas.

4.6 PUESTA A PUNTO DE LOS EQUIPOS REMOTOS QUE UTILIZARÁN ENLACES VPN PARA ACCEDER A LA RED DE DATOS DE LA E.E.Q.S.A.

Los equipos que participarán como extremo remoto de la conexión con la E.E.Q.S.A., serán los siguientes:

- ***Para acceso remoto.*** PCs de escritorio o portátiles con procesadores Pentium 4 de 2.8 Ghz mínimo, 256 MB en memoria RAM mínimo, disco de 40 GB mínimo, tarjeta de red Ethernet a 10/100 Mbps, tarjeta fax MODEM v.90., resolución gráfica a 32 bits para la gama de colores. Para el caso de portátiles, *slots* PCMCIA y USB para conectar modems celulares.

- ***Para acceso LAN - LAN.*** Un equipo que soporte conexiones túneles VPN IPSec con el protocolo ESP.

Para el caso de los CARs y equipos remotos de los usuarios se requiere que sean computadores de escritorio o computadores portátiles, en los cuales se encuentre instalado y funcionando adecuadamente el sistema operativo *Windows XP Professional SP2* actualizado, y que esté disponible conexiones de red virtuales PPTP.

En el caso de las empresas de intercambio comercial, es necesario que tengan acceso al Internet y no tengan restricciones para manejar túneles VPN con IPSec, PPTP o SSL.

4.6.1 CONFIGURACIÓN DE CLIENTE VPN PPTP BAJO *WINDOWS XP PROFESSIONAL*

En esta configuración los equipos que tienen instalado *Windows XP Professional*, tienen la ventaja de disponer un cliente incorporado para conexiones VPN con la tecnología PPTP.

Para crear una nueva conexión en el ambiente de *Windows XP Professional* se debe ingresar a **Panel de Control** → **Conexiones de Red** y en el menú de la parte izquierda hacer *click* en la opción **Crear una conexión nueva.** La *figura 4.100* permite observar el asistente que se ejecuta al ingresar a la opción escogida antes mencionada.

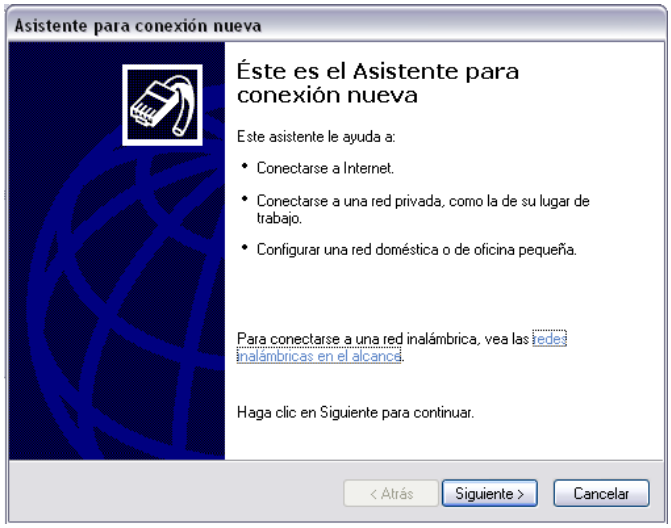


Figura 4.99 Asistente de configuración de conexiones

En las *figuras 4.101* y *4.102* se detalla cada uno de los parámetros que necesita este cliente para conectarse con el servidor de VPN PPTP ubicado en la E.E.Q.S.A. Al hacer *click* en el botón **Siguiente** se abre la ventana mostrada en la *figura 4.101*.

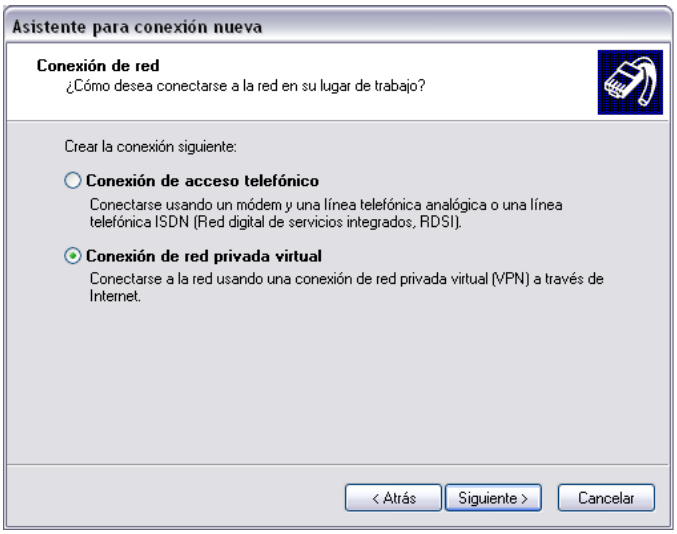


Figura 4.100 Selección de una conexión VPN

La misma *figura 4.101* indica que se puede escoger entre una **Conexión de acceso telefónico** y una **Conexión de red privada virtual**, que es la opción con la que se va a trabajar.

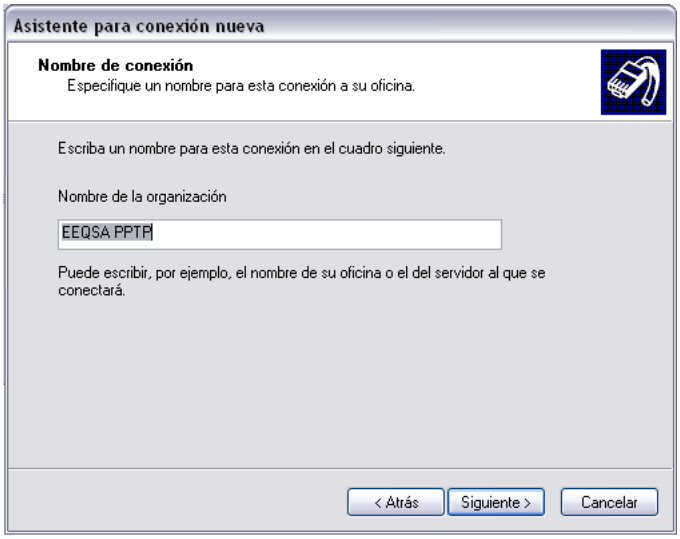


Figura 4.101 Asignación de un nombre a la conexión

De la misma forma como se abren las ventanas del **Asistente para conexión nueva** la siguiente ventana permite asignar un nombre a la conexión, para este caso el nombre seleccionado es EEQSA PPTP (Ver *figura 4.102*).

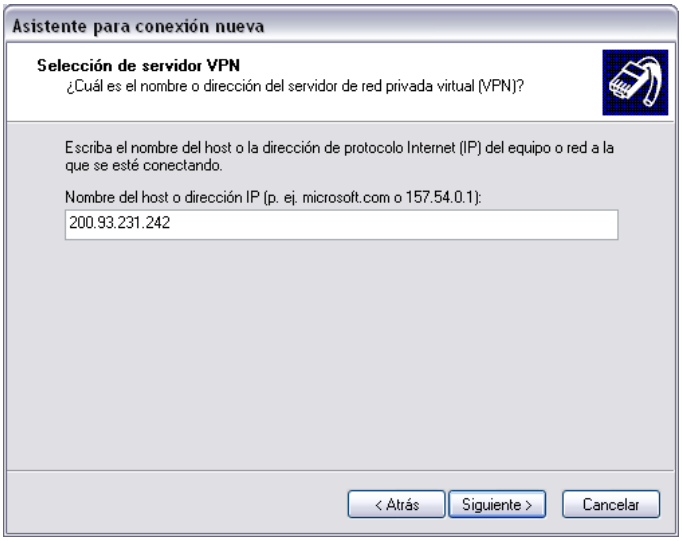


Figura 4.102 Ingreso de la dirección pública de la E.E.Q.S.A. a la que debe conectarse

Una vez listo el nombre de la conexión se hace un *click* sobre el botón siguiente para ingresar en la pantalla que corresponde a fijar la dirección IP pública a la que debe conectarse el cliente VPN PPTP, para el caso particular de la E.E.Q.S.A. la dirección IP es 200.93.231.242 (Ver *figura 4.103*).

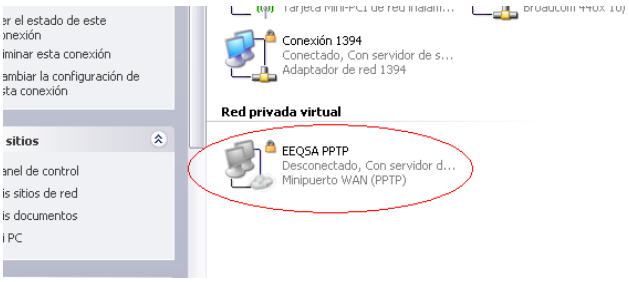


Figura 4.103 Cliente listo para conexión PPTP

El acceso VPN está listo para ser usado en situaciones muy generales, es decir tiene una configuración por defecto y dicha configuración inicial no es apropiada para la red de la E.E.Q.S.A.

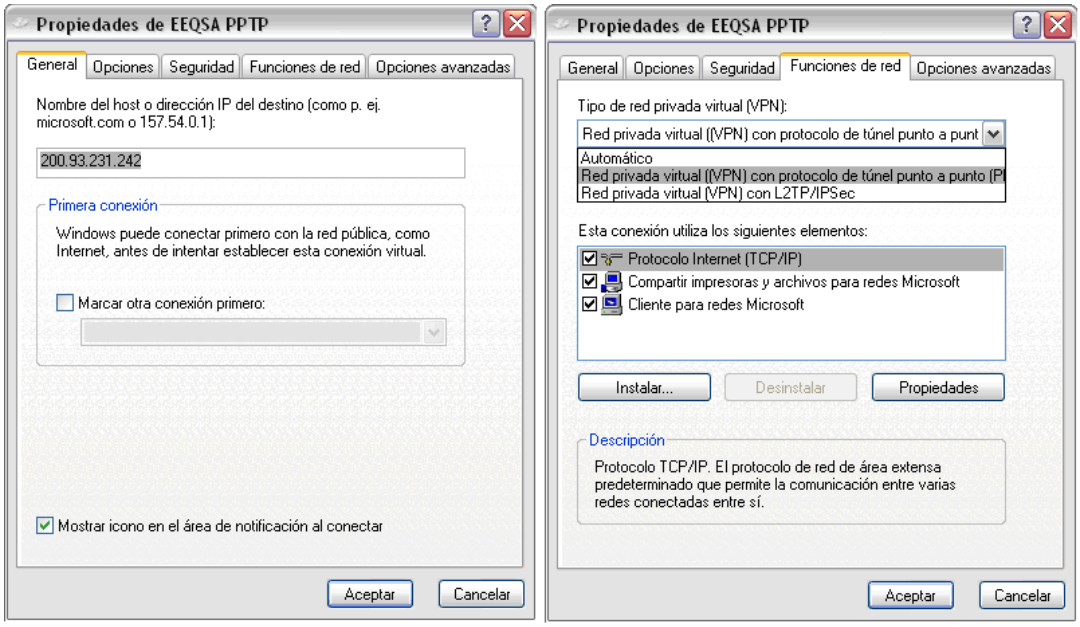


Figura 4.104 Verificación de dirección IP destino (izquierda) y especificación del tipo de VPN (derecha)

Es necesario en primer lugar determinar si se requiere que al iniciar una sesión VPN con PPTP también se permita mantener el acceso al Internet, así como agregar servidores DNS, habilitar NetBios sobre TCP/IP, prefijos de red, etc.

Como todos estos parámetros no están configurados se hace necesario configurarlos. Las *figuras 4.105*, *4.106* y *4.107* presentan esta parte de la configuración.

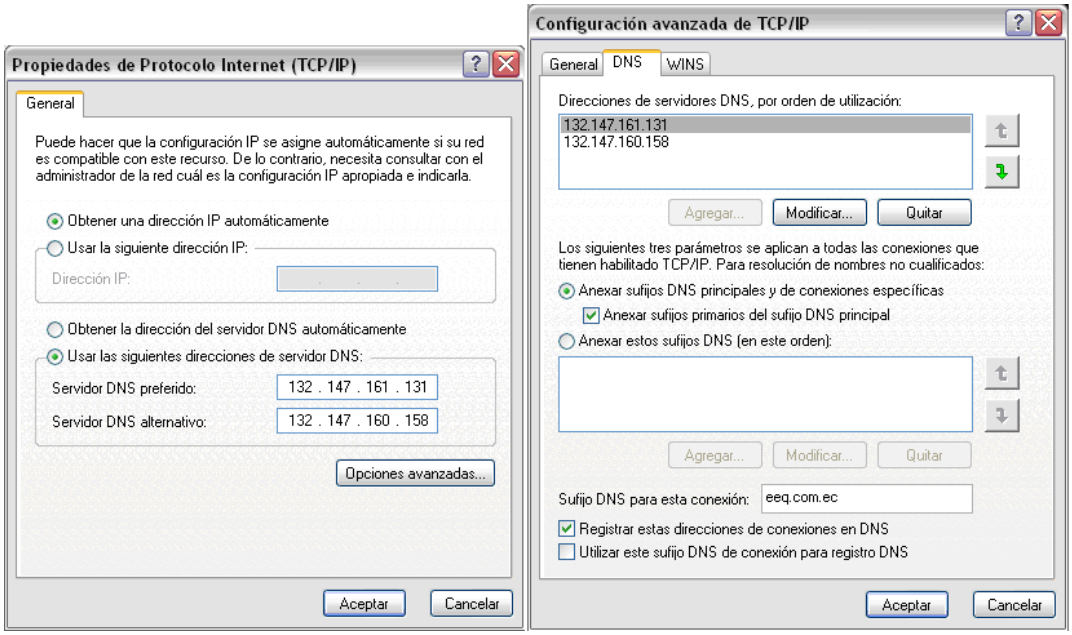


Figura 4.105 Configuración avanzada de TCP/IP - DNS

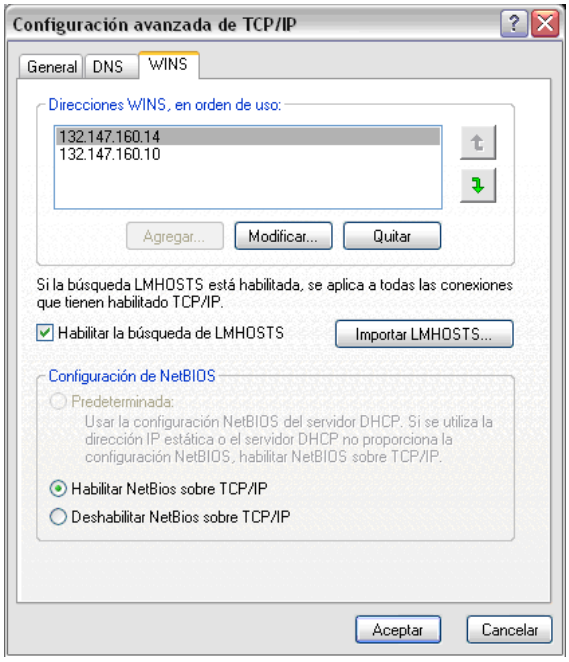


Figura 4.106 Configuración avanzada TCP/IP - WINS

El cliente con las opciones antes configuradas, está apto para realizar la comunicación con el FG300A, en el caso de PPTP, no requiere de mayor configuración y por lo tanto se trata de una configuración de rápido establecimiento de conexión.

4.6.2 CONFIGURACIÓN DEL CLIENTE VPN SSL BAJO *WINDOWS XP PROFESSIONAL*

Este cliente es de tres tipos: cliente *web*, cliente *web* con aplicaciones avanzadas mediante *Applets* de Java y el cliente liviano que permitirá extender las funcionalidades del enlace como si éste fuera de tipo IPSec o PPTP.

Figura 4.107 Dirección del portal de VPN SSL de la E.E.Q.S.A. en el Internet

Para este grupo de clientes es necesario que el equipo que va a solicitar una conexión VPN SSL cuente con el navegador *web* Internet Explorer 7 o Mozilla 3 como versiones recomendadas para la ejecución de VPN SSL.

El modo de acceso a la VPN SSL, constará de dos partes:

Figura 4.108 Ingreso de nombre de usuario para el portal de VPN SSL

La primera a través del portal generado en la configuración VPN SSL en el FG300A en la sección 4.4.2 de este proyecto (Ver *figura 4.107*).

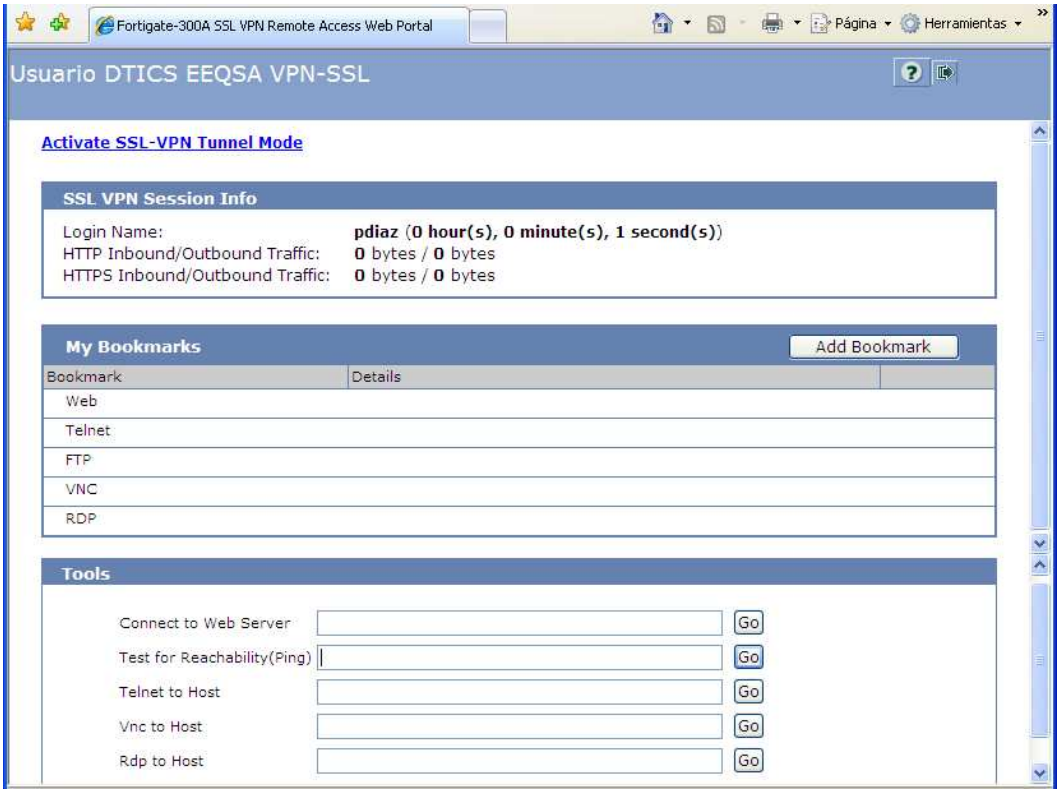


Figura 4.109 Portal de VPN SSL en FG300A para un usuario de la E.E.Q.S.A.

Al ejecutar la dirección URL mostrada en la *figura 4.107* se genera una página para ingresar el nombre de usuario y contraseña autorizado y que corresponde a este tipo de acceso (Ver *figura 4.108*).

Al ingresar al portal se tiene varias opciones con las que se puede ingresar a varios servidores que tienen activados los servicios de *Web Server*, Servicio Telnet, Servicio FTP, Servicio VNC y Servicio RDP (Escritorio Remoto de *Microsoft Windows*) (Ver *figura 4.109*); todos los servicios enumerados se ejecutan sobre el navegador *web* y los servicios TELNET, VNC y RDP requieren de la ejecución de un *Applet* de java para su respectiva funcionalidad adecuada.

El portal permite al usuario personalizar con hipervínculos accesos a varios servidores, esta configuración queda fija hasta cuando el usuario decide

cambiarla o cuando el administrador elimina la cuenta de usuario (ver *figuras 4.110* a *4.111*).

Para agregar un hipervínculo a un servicio en particular se puede especificar el tipo de aplicación que puede ser de los tipos antes mencionados y se escribe el URL, tal como lo ilustra la *figura 4.110*.

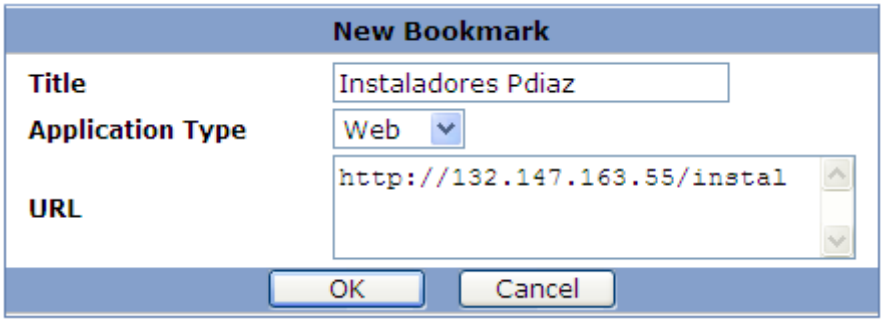


Figura 4.110 Acceso directo a un servidor de la red corporativa de la E.E.Q.S.A.

Una personalización del portal permite que el cliente a través del navegador *web* se convierta en un cliente versátil y de rápido acceso. La *figura 4.111* permite observar la personalización del portal donde se ha configurado varios accesos hacia servidores y equipos de comunicación a los cuales el usuario requiere acceder a través de una conexión remota.

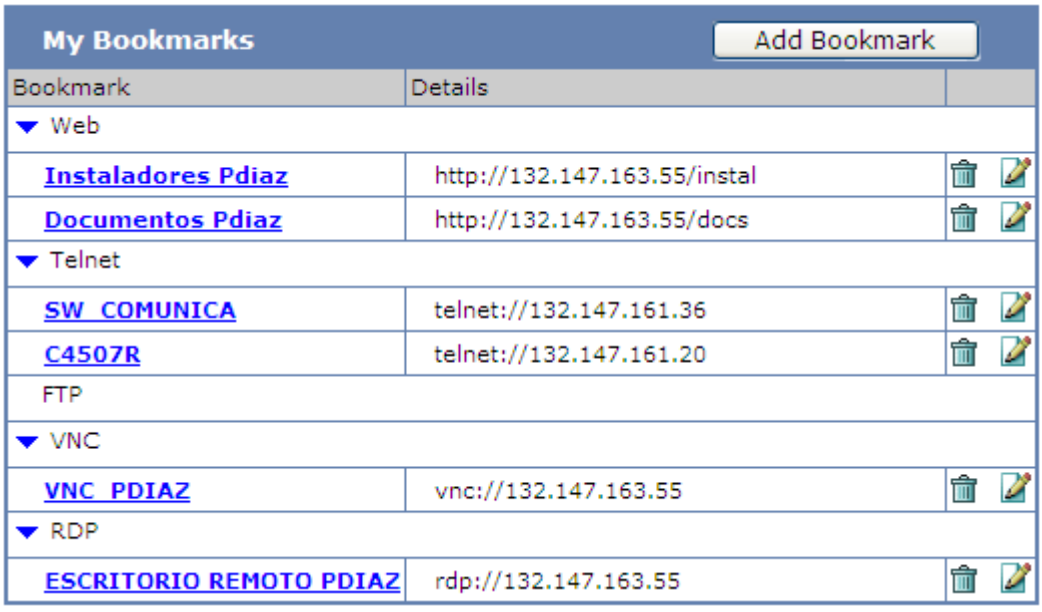


Figura 4.111 Portal personalizado con accesos directos a varios servicios de la E.E.Q.S.A.

La segunda es que una vez que el usuario se ha autenticado en el portal y si los permisos de grupo de usuario lo permiten, éste puede descargar e instalar el componente o control de tipo ActiveX para que en el computador se pueda instalar una interfaz virtual, la cual servirá para establecer un túnel donde se podrá ejecutar los aplicativos requeridos por el usuario (Ver *figuras 4.112* a *4.115*).

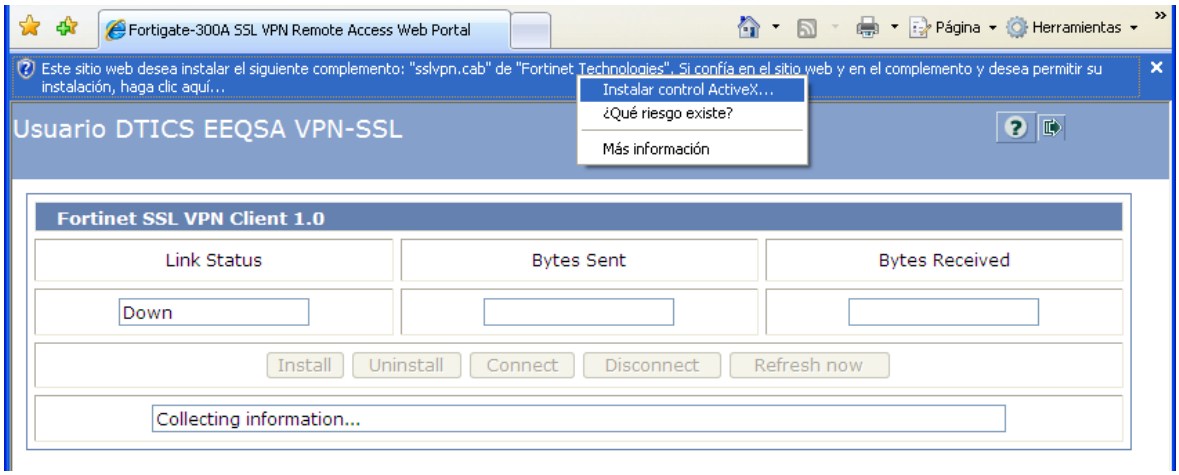


Figura 4.112 Inicio de instalación del cliente liviano VPN SSL

El control ActiveX reside en el FG300A y si las configuraciones de seguridad del navegador *web* lo permiten, éste permitirá descargar e instalar el cliente sobre el sistema operativo del computador del usuario (ver *figura 4.112*).

Es un software que tiene la firma del fabricante Fortinet lo cual permite que la instalación sea confiable (ver *figura 4.113*).

Figura 4.113 Instalador de tipo ActiveX empaquetado en un archivo de tipo .cab

Luego de unos instantes el control ActiveX es instalado y el sistema operativo lo reconoce como una interfaz virtual (ver *figura 4.115*); cabe destacar que el cliente Fortinet SSL VPN es compatible con sistemas *Microsoft Windows 2000 Professional* y *XP Professional*.

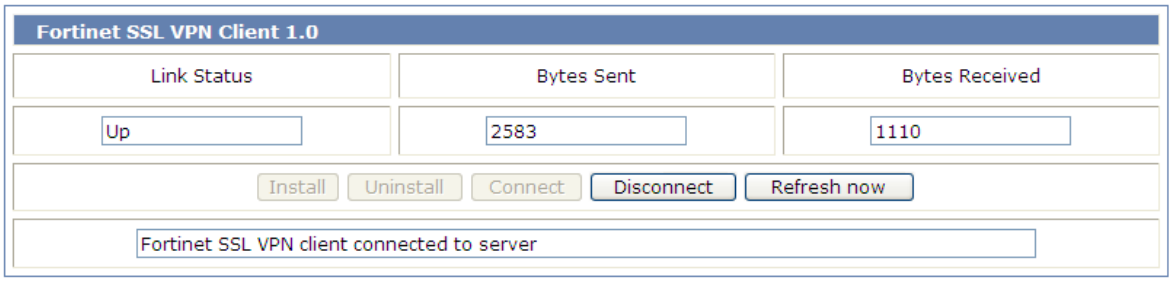


Figura 4.114 Indicador del estado del cliente VPN SSL

Cuando el cliente es reconocido el portal cierra la sección de los hipervínculos personalizados y abre una página donde se registra la actividad del estado de conexión del cliente (ver *figura 4.114*); a más de verificar la actividad es posible gestionar de manera básica la conexión. Sólo en este portal es posible conectar y desconectar el cliente liviano VPN SSL.

Figura 4.115 Agregación de un nuevo interfaz de red de tipo virtual VPN SSL

4.6.3 CONFIGURACIÓN DEL CLIENTE VPN IPSEC BAJO *WINDOWS XP PROFESSIONAL*

En la configuración de los equipos con este protocolo es necesario instalar el cliente de Fortinet, el producto se llama FortiClient, y entre sus funcionalidades permite habilitar servicios de seguridad como Antivirus, Firewall, VPN IPSec, AntiSpam, etc., sin embargo se instalará esta aplicación únicamente con la opción de VPN IPSec. A continuación se detalla la instalación y configuración del cliente VPN en un PC de escritorio con *Windows XP Professional*.

Este cliente puede ser descargado del sitio *web* de Fortinet (*http://www.fortinet.com*), aunque se necesita obtener la licencia de uso del cliente, el cual se lo puede adquirir al distribuidor autorizado. En el caso de la E.E.Q.S.A., se realizó la compra del equipo y 25 licencias de clientes FortiClient.

Este cliente está diseñado para que funcione en el sistema operativo *Windows XP*. Las *figuras 4.116* a *4.122* detallan los pasos para instalar este cliente del fabricante Fortinet.

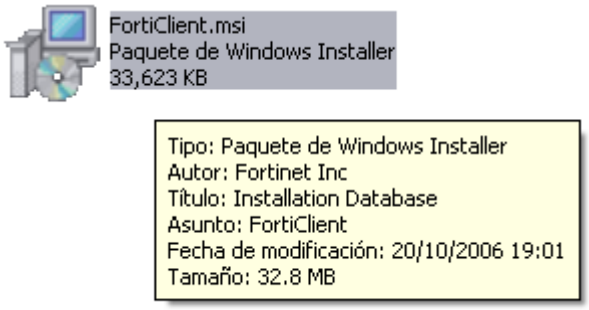


Figura 4.116 Paquete del instalador FortiClient versión 3.0.308

A partir del cliente se lo ejecuta para instalarlo en el equipo que operará como cliente remoto y en el cual se accederán a aplicaciones que se encuentran en los servidores del centro de cómputo de la E.E.Q.S.A. La *figura 4.117* muestra el inicio del asistente de instalación de la aplicación cliente FortiClient.

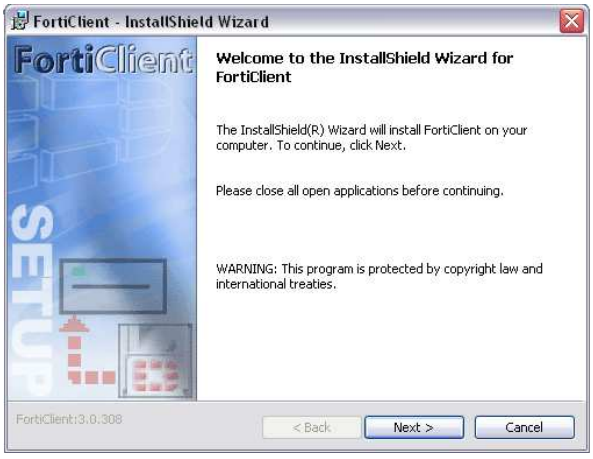


Figura 4.117 Asistente de instalación en el equipo que funcionará como cliente remoto

Se recomienda utilizar la opción de personalización del cliente, ya que en esta opción se puede habilitar IPSec VPN (Ver *figuras 4.118* y *4.119*). El resto de opciones no son tomadas en cuenta ya que solo interesa la aplicación del túnel con IPSec.

Figura 4.118 Se configura con la opción personalizada

En la configuración por defecto del modo *custom* o personalizado de la *figura 4.119*, todas las aplicaciones están activadas para ser instaladas; se desactivan todas las funcionalidades a excepción de IPSec VPN. Esta acción tiene el propósito de utilizar únicamente el cliente para establecer con el FG300A un túnel VPN IPSec.

Figura 4.119 Selección de IPSec-VPN de las opciones disponibles

Una vez especificado el paquete a instalar el proceso de instalación es de corta duración. Dentro del computador queda instalada la aplicación *FortiClient* que permitirá conectar con el servidor de VPNs FG300A y establecer la comunicación a través de VPN IPSec.

Figura 4.120 Pantalla de ingreso de la licencia de FortiClient

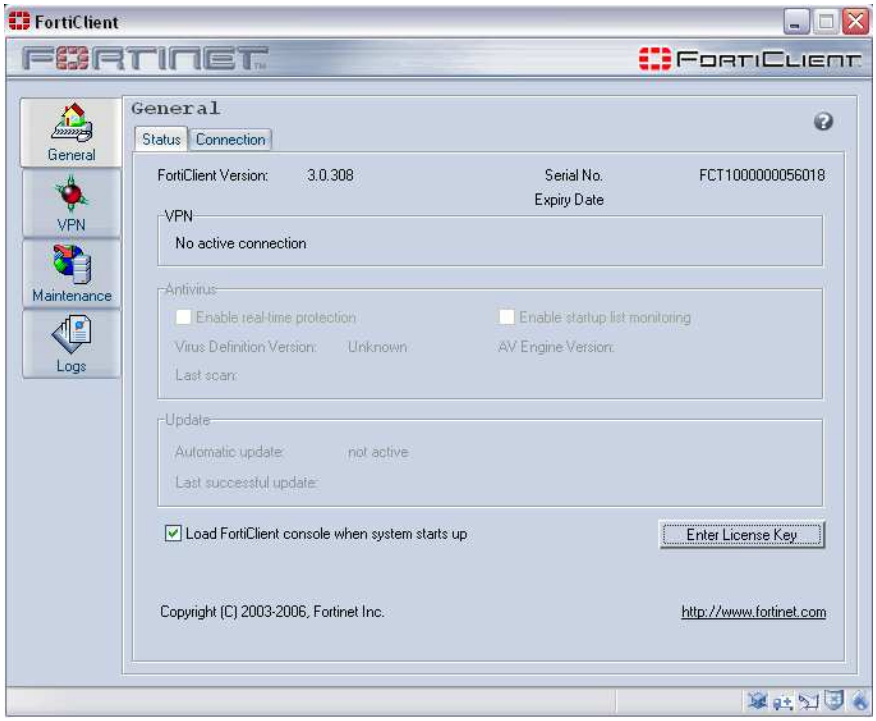


Figura 4.121 Cliente listo para ser configurado

Al finalizar la instalación el asistente del *FortiClient* solicita al usuario reiniciar el computador para que se apliquen los respectivos cambios en el sistema operativo.

Una vez reiniciado el sistema operativo, la aplicación solicita al usuario una configuración adicional posterior a la instalación inicial, que consiste en el ingreso de la licencia de uso de la aplicación *FortiClient* como se muestra en la *figura 4.121*. Con esto se finaliza la instalación del cliente.

A continuación se podrán configurar los parámetros de conectividad y así establecer la comunicación a través de VPN IPSEC. La ventana del cliente listo para la configuración se muestra en la *figura 4.121*.

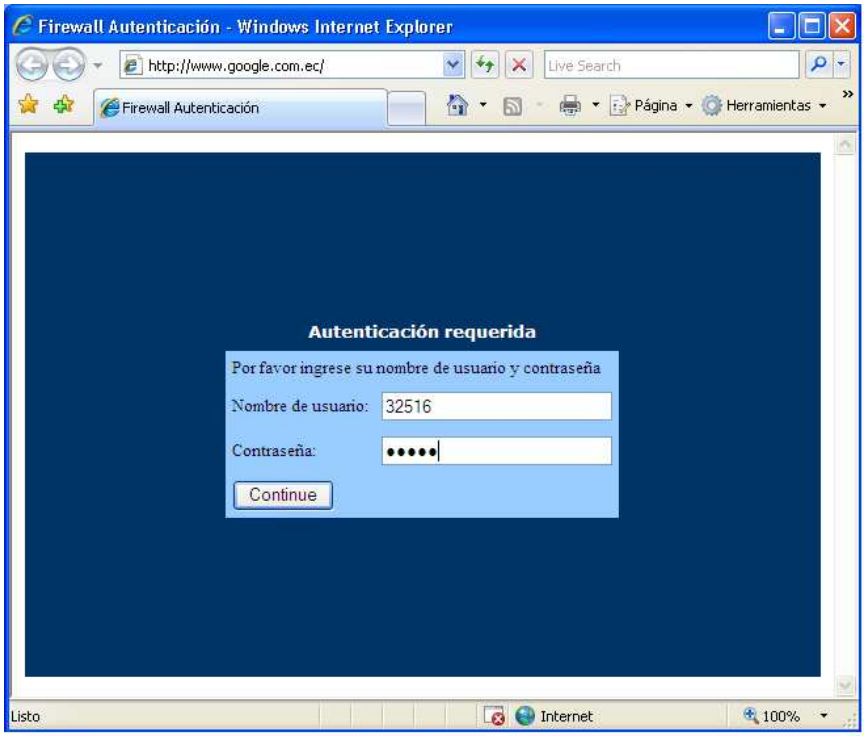


Figura 4.122 Pantalla de nombre de usuario y contraseña para el acceso a Internet

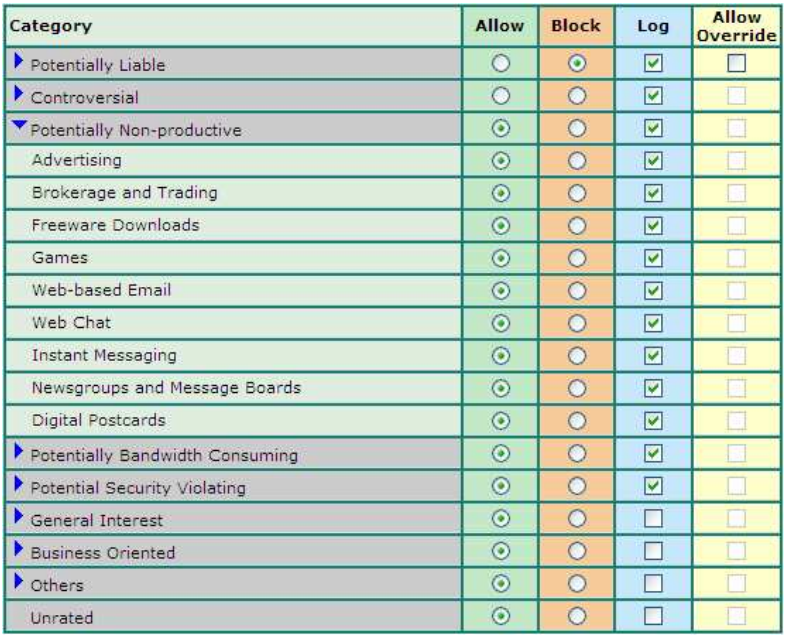
4.7 PRUEBAS DE TRÁFICO DEL DISEÑO PROPUESTO

Una vez configurado varios módulos y parámetros del sistema de seguridad y VPNs sobre el FG300A, se procede a realizar las siguientes pruebas:

- Pruebas de seguridades
- Pruebas de medida de ocupación del canal VPN y seguridad
- Prueba de VoIP sobre VPN

4.7.1 PRUEBA DE SEGURIDADES

Estas pruebas corresponden a la verificación de la seguridad que existe en el control de acceso hacia segmentos de red de la E.E.Q.S.A. y protocolos que se encuentran ejecutándose en la red corporativa. A estas pruebas se las clasificará como Seguridad de acceso desde la E.E.Q.S.A. hacia el Internet y Seguridad de acceso desde el Internet o red externa hacia la E.E.Q.S.A.



Category	Allow	Block	Log	Allow Override
Potentially Liable	○	◉	☑	☐
Controversial	○	○	☑	☐
Potentially Non-productive	◉	○	☑	☐
Advertising	◉	○	☑	☐
Brokerage and Trading	◉	○	☑	☐
Freeware Downloads	◉	○	☑	☐
Games	◉	○	☑	☐
Web-based Email	◉	○	☑	☐
Web Chat	◉	○	☑	☐
Instant Messaging	◉	○	☑	☐
Newsgroups and Message Boards	◉	○	☑	☐
Digital Postcards	◉	○	☑	☐
Potentially Bandwidth Consuming	◉	○	☑	☐
Potential Security Violating	◉	○	☑	☐
General Interest	◉	○	☐	☐
Business Oriented	◉	○	☐	☐
Others	◉	○	☐	☐
Unrated	◉	○	☐	☐

Figura 4.123 Categorías de sitios web desarrollado por Fortinet y aplicado a perfiles de usuario

4.7.1.1 Seguridad de acceso desde la E.E.Q.S.A. hacia el Internet

La mayoría de los usuarios tienen acceso al Internet. Para el acceso dentro del FG300A se ha configurado un control de acceso a través de la política que se encuentra en el grupo de políticas ***port3 -> port1*** y que tiene ***ID = 2***.

Tiene la particularidad que en la configuración de la política se ha habilitado el campo ***Authentication***, y dentro de este campo se ha seleccionado la opción

Firewall, lo que quiere decir que los usuarios pertenecen a un grupo de usuarios de tipo ***Firewall*** y a su vez deberán autenticarse con los nombres de usuario y contraseña de la cuenta local almacenada en el FG300A.

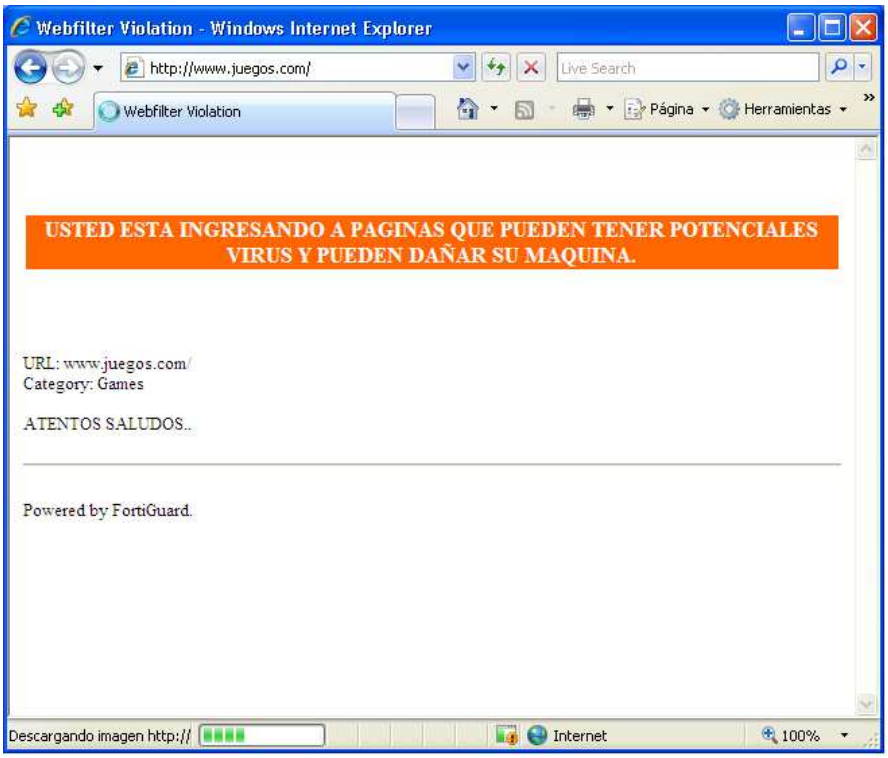


Figura 4.124 Página de información de la prohibición de acceso a sitios de categoría Games

El esquema de nombres de usuarios contraseñas para el acceso al Internet adoptado por la Administración de Sistemas Informáticos de la E.E.Q.S.A., ha determinado que se lo hará con la identificación del empleado (número entero de 5 dígitos o ROL) y una contraseña acordada entre el administrador y el usuario. Cuando el usuario requiera acceder a Internet lo hará desde un navegador *Web* como Internet Explorer 7, escribirá en la barra de dirección un URL del Internet y en pocos instantes aparecerá una página donde tiene que ingresar los datos para la autenticación como lo muestra la *figura 4.122*.

El usuario que ha ingresado correctamente sus datos tiene la posibilidad de poder acceder a una gran variedad de sitios *web* del Internet; sin embargo por cuestiones de seguridad y optimización del recurso informático se ha habilitado el bloqueo a través de listas categorizadas, que continuamente los servidores de

Fortinet inyectan esta información hacia los equipos con licencias activas como es el caso del FG300A de la E.E.Q.S.A.. Dentro de estas categorías se encuentran los mostrados en la *figura 4.123*.

En la *figura 4.123* se puede observar que dentro de la categoría ***Potencially Non-productive*** existe la subcategoría ***Games***; si el usuario intenta ingresar a una página de este tipo automáticamente se despliega una página que informa la prohibición de acceso a este tipo de sitios y no permite que se puede ejecutar la navegación en ese sitio (ver *figura 4.124*).

Existen sitios que no están dentro de una categoría y que la Administración E.E.Q.S.A. requiere bloquear; este es el caso de sitios como *www.hi5.com* que es altamente visitado por usuarios internos y que provoca varios problemas de tipo productivo y de consumo de recursos empresariales. Este sitio ha sido listado localmente en el FG300A y fijado una bandera que especifica que se bloquea el acceso para los usuarios con perfil de ***profilenavegar***; si algún usuario intenta ingresar automáticamente se despliega un mensaje dentro de una página como el mostrado en la *figura 4.125*.

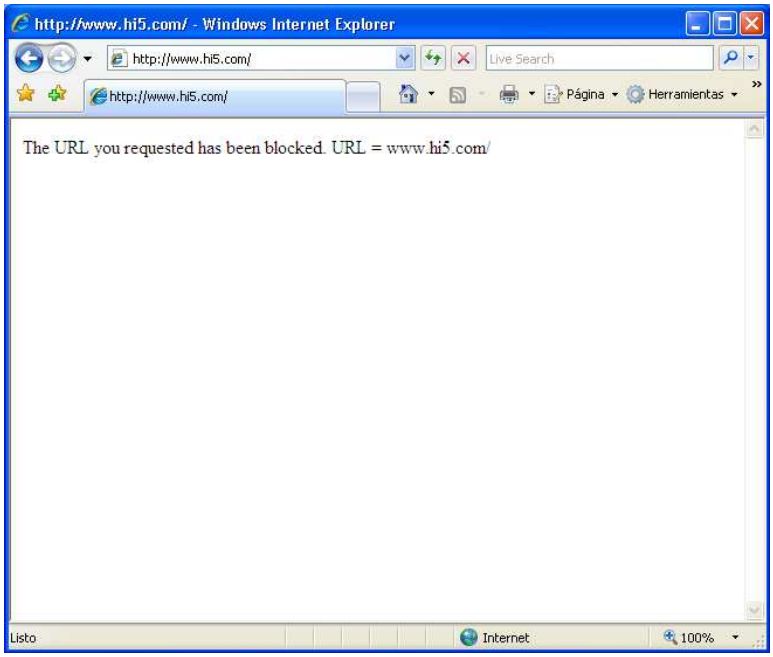


Figura 4.125 Página de información y bloqueo de acceso a un determinado sitio web

4.7.1.2 Seguridad de acceso desde el Internet o redes externas hacia la E.E.Q.S.A.

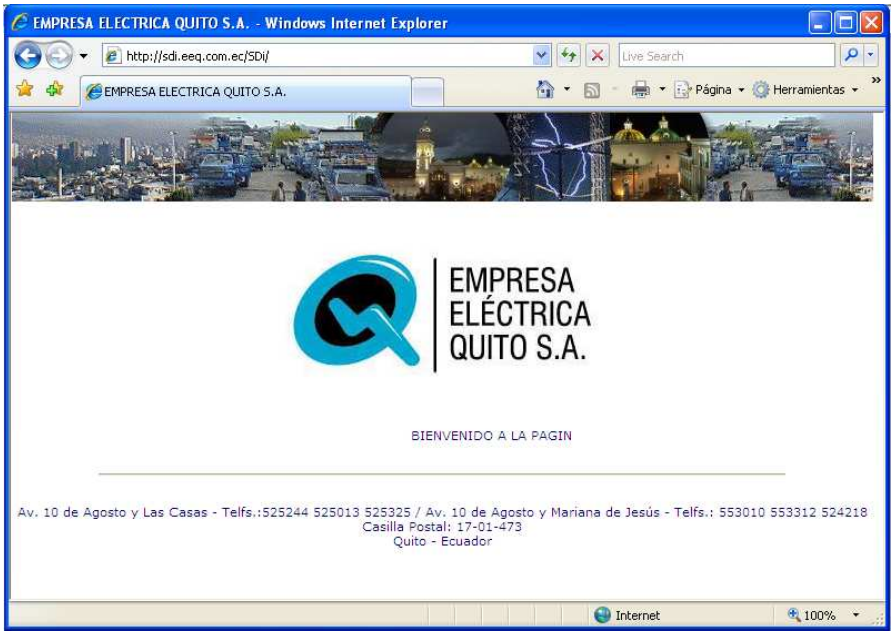


Figura 4.126 Página de ingreso al sistema SDI accedido desde el Internet

El público en general tiene acceso a la E.E.Q.S.A. a través del sitio *web*, así mismo las empresas contratistas que tienen convenio con la E.E.Q.S.A. tienen cuentas de usuario para utilizar el sistema SDI y GIS de la E.E.Q.S.A. Todos estos sitios pueden ser accedidos a través del Internet ya que en el FG300A se ha configurado el acceso a estos servicios por medio de NAT, permitiendo una utilización adecuada de direccionamiento IP público y al mismo tiempo ocultando el direccionamiento interno de los servidores.

Un computador que se encuentra en el Internet y que requiera acceder a *http://sdi.eeq.com.ec/SDi*, podrá realizarlo sin inconvenientes (ver *figura 4.126*).

A parte de este sitio y el sitio *web* de la E.E.Q.S.A. se tienen algunos servicios publicados; la *figura 4.127* nuestra la lista de servidores con configuración NAT en el FG300A.

Create New

Name	IP	Service Port	Map to IP/IP Range	Map to Port	
asistencia-nat	port1/200.93.231.247		132.147.160.113		
chat-nat	port1/200.93.231.250		132.147.162.240		
citrix1-nat	port1/200.93.231.251		132.147.161.245		
citrix2-1494	port1/200.93.231.252	1494/tcp	132.147.160.19	1494/tcp	
citrix2-1495	port1/200.93.231.252	1495/tcp	132.147.162.233	1495/tcp	
citrix2-80	port1/200.93.231.252	80/tcp	132.147.160.19	80/tcp	
email-nat	port1/200.93.231.248		132.147.162.218		
ftp-nat	port1/200.93.231.249		132.147.163.148		
intranet-nat	port1/200.93.231.242	8080/tcp	132.147.160.158	80/tcp	
p5-dbeeq-nat	VLAN_PROMERICA/192.168.10.19		132.147.162.240		
pia-nat	port1/200.93.231.245		132.147.163.143		
pototux-nat	port1/200.93.231.254		132.147.161.237		
sdi-nat	port1/200.93.231.246		132.147.160.7		
srvsiste-1-nat	port1/200.93.231.242	26/tcp	132.147.161.147	26/tcp	
test-ts-vm-nat	port1/201.218.12.98		132.147.161.166		
www-nat	port1/200.93.231.243	80/tcp	192.168.21.11	80/tcp	

Figura 4.127 Listado de servidores con configuración NAT

Existen algunos servidores como el SRVCOMUNICA con dirección IP 132.147.163.120 que no están en la lista de NAT del FG300A. Este equipo está ejecutando diariamente el monitoreo de tráfico de varios puntos de la red corporativa de la E.E.Q.S.A. y que se puede acceder a través de un navegador *web* desde un equipo de la red local (Ver *figura 4.128*); pero desde redes externas como el Internet no tiene una configuración para el libre acceso.

Figura 4.128 Acceso desde la red local al servidor de monitoreo de tráfico de red

Dentro del servidor DNS la dirección 132.147.163.120 está asociada al nombre *comunica.eeq.com.ec*[52]. En la barra de dirección se puede cambiar la dirección IP por el nombre de *host* mencionado y acceder de igual manera (ver *figura 4.129*).

[52] En la configuración de red de área local de las *NICs* de la E.E.Q.S.A. se tiene establecido el sufijo *eeq.com.ec*, por lo que es suficiente escribir *http://comunica:8081* en lugar de *http://comunica.eeq.com.ec:8081* en la barra de dirección del navegador *web*

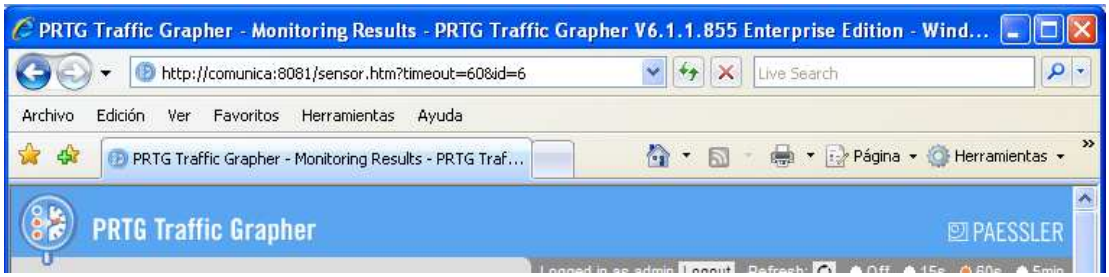


Figura 4.129 Acceso desde la red local al servidor de monitoreo de tráfico de red utilizando el nombre registrado en el servidor DNS

Al intentar ingresar a este servidor por medio del Internet se desplegará la página de error del navegador *web* como se observa en la *figura 4.130*.

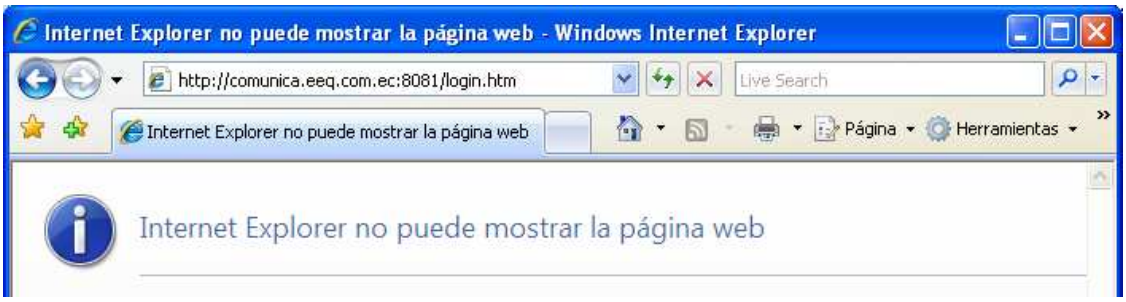


Figura 4.130 Página con el mensaje de problema en la conexión al intentar ingresar al servidor comunica desde el Internet

Para acceder a servidores y servicios que no están en la lista de NAT del FG300A de la red corporativa de la E.E.Q.S.A., los empleados y funcionarios que por varios motivos lo deben realizar desde el Internet deberán realizar accesos de tipo seguro, como por ejemplo a través de VPNs. A continuación se revisarán los aspectos de seguridad y de ocupación del canal de comunicaciones para las VPNs.

4.7.2 PRUEBAS DE MEDIDA DE OCUPACIÓN DEL CANAL VPN Y SEGURIDAD

El FG300A tiene configurado políticas para el acceso VPN, en las cuales se ha especificado que se puede controlar el ancho de banda fijando un valor preestablecido en la configuración de la política. Las VPNs IPSEC de acceso remoto se la analizará detenidamente mientras las VPNs IPSEC *LAN – LAN* se analizará la ocupación de canal en términos generales.

4.7.2.1 Pruebas de negociación IKE, autenticación con RADIUS y análisis del tráfico generado

Para el acceso remoto se va a configurar el ***Traffic Shaping*** de la política en 128 kbps como valor garantizado y máximo de capacidad de tráfico para esa política, el cual se lo va a saturar realizando una descarga de archivos y *ping* desde el equipo remoto, y a través de un analizador de tráfico verificar que la ocupación del canal no exceda los 128 kbps.

El equipo de pruebas será un computador que se encuentra en la red externa del proveedor TELCONET, así mismo este equipo tendrá configurado en la tarjeta de red una dirección IP de tipo pública. Las características del equipo de pruebas son las siguientes:

- Procesador *Intel Core Duo* 1.60 Ghz
- Memoria RAM de 1024 MB
- Disco Duro de 80 GB
- Tarjeta de red *Fast-Ethernet*
- *Windows XP Professional SP2*
- Internet Explorer 7.0
- Mozilla 3.0.8

TELCONET ha facilitado para estas pruebas la dirección IP pública 201.218.12.100 / 28 con dirección de puerta de enlace 200.93.231.241 y direcciones de servidor DNS 200.93.216.2 y 200.93.216.5; la *figura 4.131* permite observar la configuración de red de la tarjeta del equipo de pruebas.

El equipo de pruebas se conectará a la VLAN con ID 7 del *switch* principal de la E.E.Q.S.A. que corresponde al segmento de red externa de TELCONET o acceso a Internet.

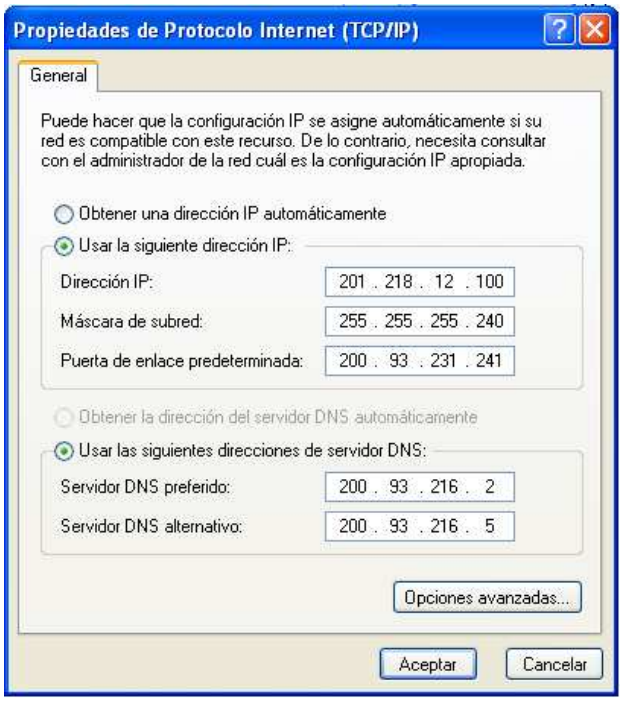


Figura 4.131 Configuración de la tarjeta de red del equipo de pruebas

El Forticlient ha sido instalado en el equipo de pruebas tal como se lo indicado en la sección 4.6.3, lo siguiente será configurar los parámetros de conexión.

La *figura 4.131* indica los parámetros de red para la tarjeta Fast-Ethernet del equipo de pruebas de VPN y seguridades. Desde este equipo se procede a utilizar la aplicación Forticlient para realizar la conexión VPN IPSEC con el FG300A.

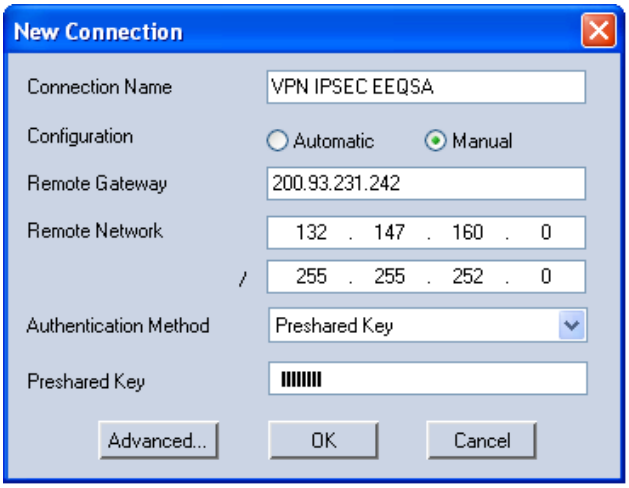


Figura 4.132 Configuración de red del Forticlient y parámetros para la negociación IKE

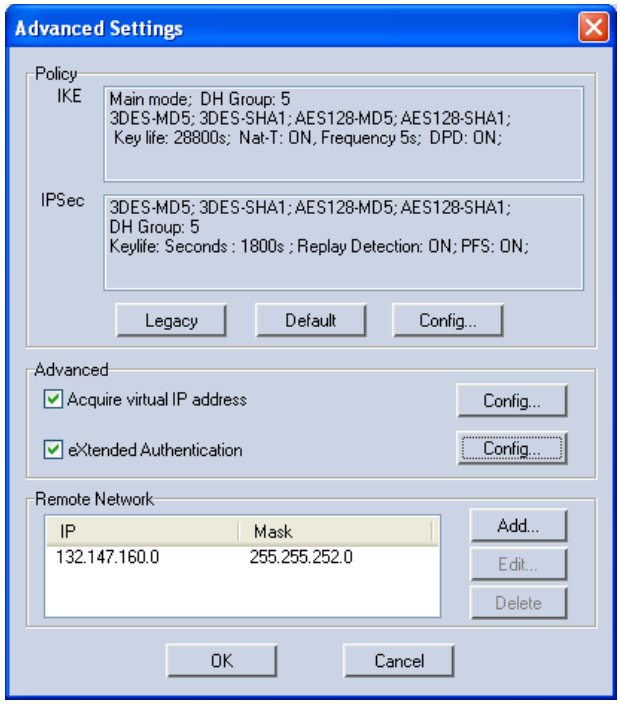


Figura 4.133 Configuración avanzada del Forticlient

En la aplicación Forticlient se debe configurar los parámetros de identificación de la conexión, el equipo remoto de conexión (IP pública del FG300A), red de destino, método de acceso de autenticación y clave compartida (Ver *figura 4.132*). A más de estos parámetros se puede ampliar otras configuraciones, accediendo a la configuración avanzada por medio del botón ***Advanced*** de la *figura 4.132*, donde se podrá especificar si el equipo remoto cliente adquiere o no una dirección IP virtual (desde el servidor DHCP) y también se podrá especificar si se utilizará autenticación extendida (XAuth) (Ver *figura 4.133*).

Los parámetros deben estar acorde a la configuración VPN IPSEC realizada en el FG300A. Del lado de la red de la E.E.Q.S.A. se tiene activado y en espera de requerimientos el servidor RADIUS.

Una vez que el equipo de pruebas se encuentra conectado al Internet, se procede a establecer la conexión VPN a través del Forticlient, cuando se realiza la petición de establecimiento de conexión se genera una ventana en donde se informa al usuario los pasos de negociación que se ejecuta mientras se realiza el establecimiento de la conexión (Ver *figura 4.134*).

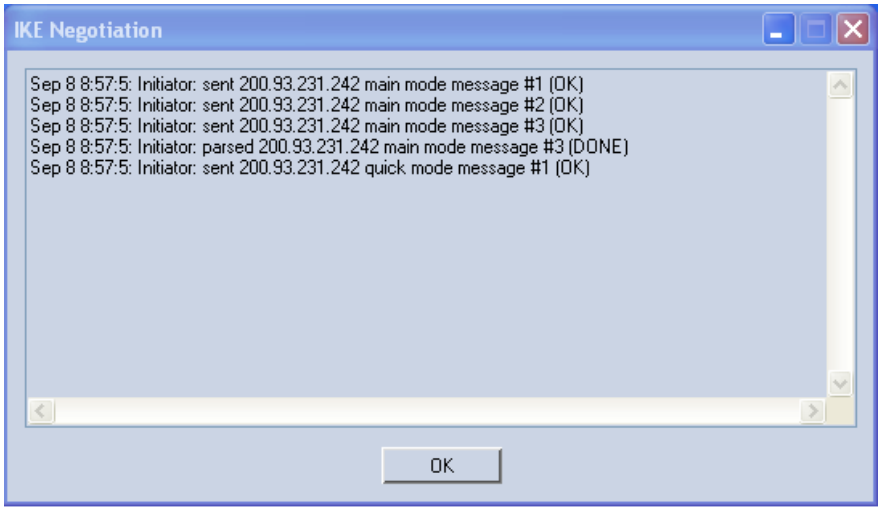


Figura 4.134 Log de negociación de IKE

Figura 4.135 Ventana de ingreso de datos para la autenticación del usuario

Al mismo tiempo se abre también la ventana de ingreso de datos para la autenticación del usuario, tal como se muestra en la *figura 4.135*.

En la *figura 4.135* podemos ver que se despliega la ventana que solicita la contraseña del usuario "*pablo*". Este usuario está registrado en el FG300A como un usuario de tipo RADIUS y en el servidor RADIUS se encuentra registrado la cuenta "*pablo*" con contraseña "*epn225linux*", la cual debe ser ingresada correctamente para que se pueda realizar el establecimiento del túnel VPN.

Si el nombre de usuario o la contraseña no son los correctos, la ventana de *login* y *password* solicita nuevamente el ingreso de los datos correctos.

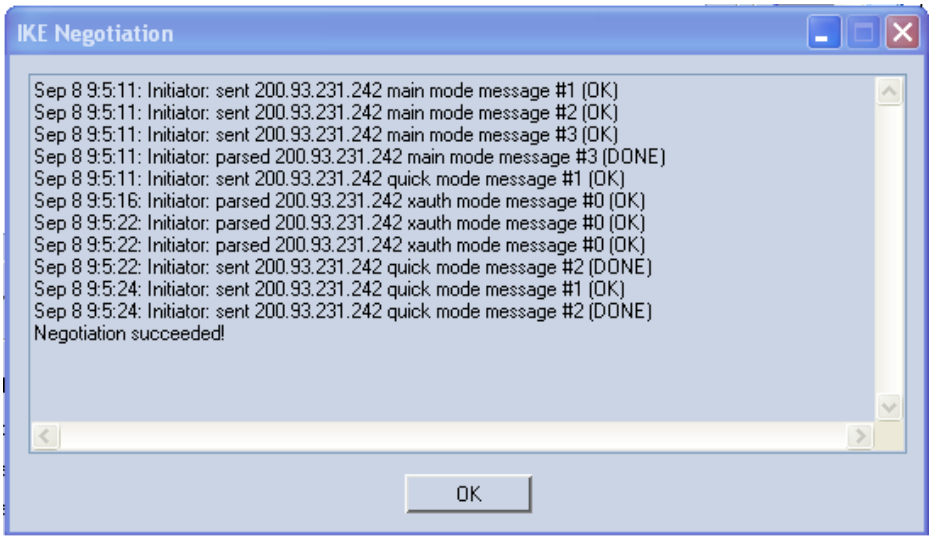


Figura 4.136 Registro de establecimiento de la negociación IKE exitosa

Si los datos son correctos el mensaje en la ventana de *log* de la negociación IKE finalizará como lo muestra la *figura 4.136*.

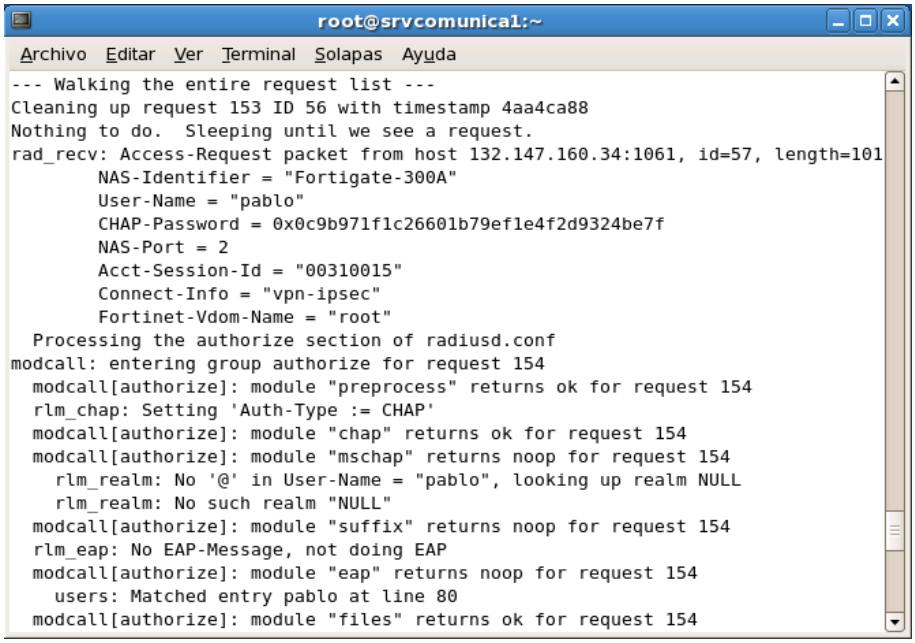


Figura 4.137 Registro de negociación de la autenticación de un usuario en el servidor RADIUS

Mientras esto sucede en el lado del cliente remoto, el servidor de autenticación RADIUS genera un reporte de la actividad del usuario que ha sido otorgado el permiso de acceso a la red de la E.E.Q.S.A. La *figura 4.137* permite observar que al iniciar la autenticación se verifican los parámetros correspondientes a nombre del cliente RADIUS que es el FG300A, el nombre de la cuenta de usuario que es

"*pablo*" y también se puede observar que la clave está cifrada ya que se ha utilizado el protocolo de autenticación CHAP para la negociación de la conexión entre el servidor RADIUS y el FG300A.

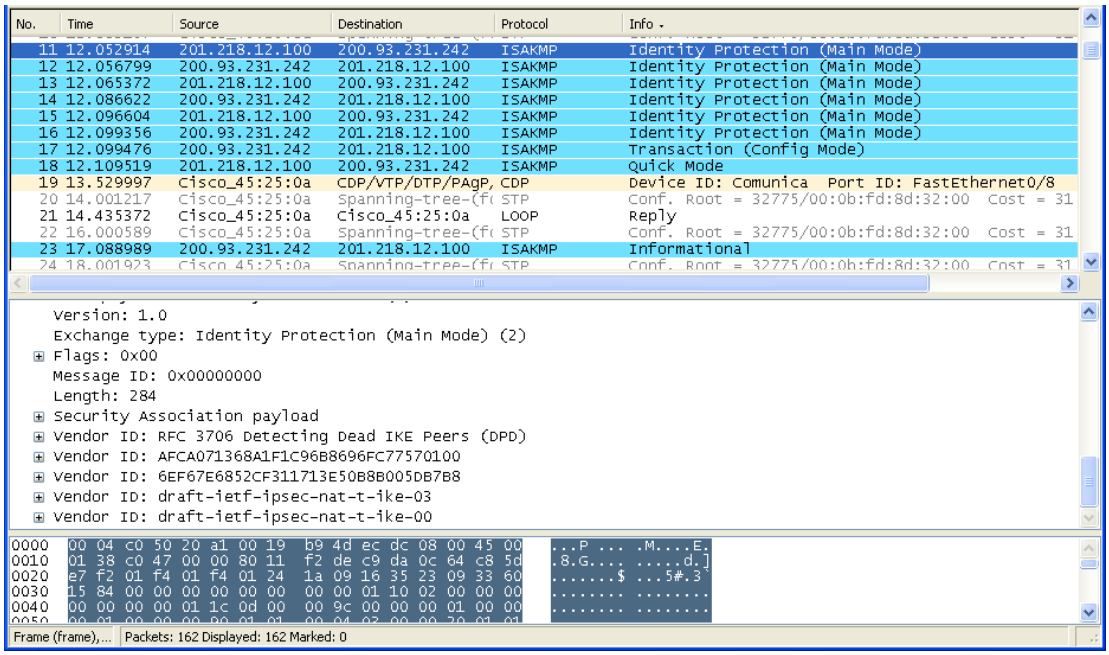


Figura 4.138 Visualización de la negociación IKE a través de un analizador de protocolos Wireshark

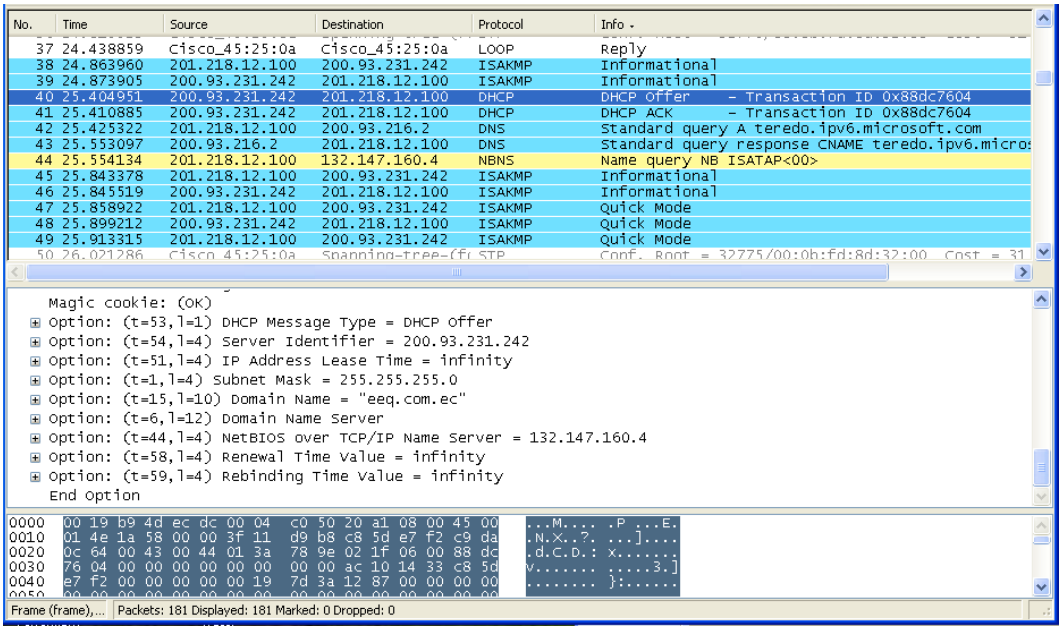


Figura 4.139 Visualización de la asignación de parámetros de red para la interfaz virtual

Los pasos para el establecimiento de negociación han sido un éxito lo que ha permitido establecer el túnel VPN IPSEC. Detrás del establecimiento de la

negociación es oportuno verificar que ha sucedido en el intercambio de paquetes, esto se lo podrá observar mediante la aplicación *Wireshark*.

Al inicio del establecimiento de la conexión VPN IPSEC la trama indica que el equipo con dirección IP 201.218.12.100 requiere conectarse con el equipo de dirección 200.93.231.242 para formar la VPN (Ver *figura 4.138*).

También se puede observar que el protocolo utilizado en el paquete es ISAKMP y que se está utilizando el Modo ***Main*** para la protección de la identidad.

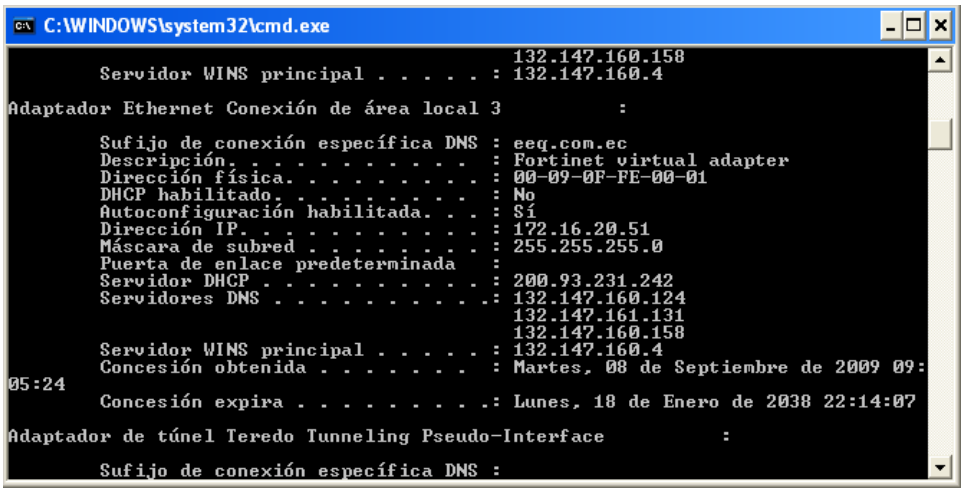


Figura 4.140 Información de los parámetros de red asignados por el servidor DHCP

Una vez establecida la conexión el último paso es adquirir una dirección IP del servidor DHCP y que reside en el FG300A. La *figura 4.139* muestra la información que es transferida al cliente remoto para que éste pueda obtener los parámetros de red necesarios.

La interfaz virtual adquiere una dirección del *pool* de direcciones del DHCP. Esta información es posible observarla a través del comando ***ipconfig*** *de Windows XP Professional* en la consola de comandos (ver *figura 4.140*).

A continuación se realiza una descarga de archivo para verificar la ocupación del canal virtual. El equipo *pdiaz* que es parte de la red local de la E.E.Q.S.A. y pertenecen al segmento de red IP 132.147.160.0 / 22, tiene configurado un

servidor *web* donde se ha publicado un directorio, del cual se va a realizar una descarga. La *figura 4.141* muestra la descarga de un archivo de 308 MB y la realiza con una velocidad de transferencia de 528 Kbytes/s, es decir ocupa la capacidad del canal Fast-Ethernet sin restricción.

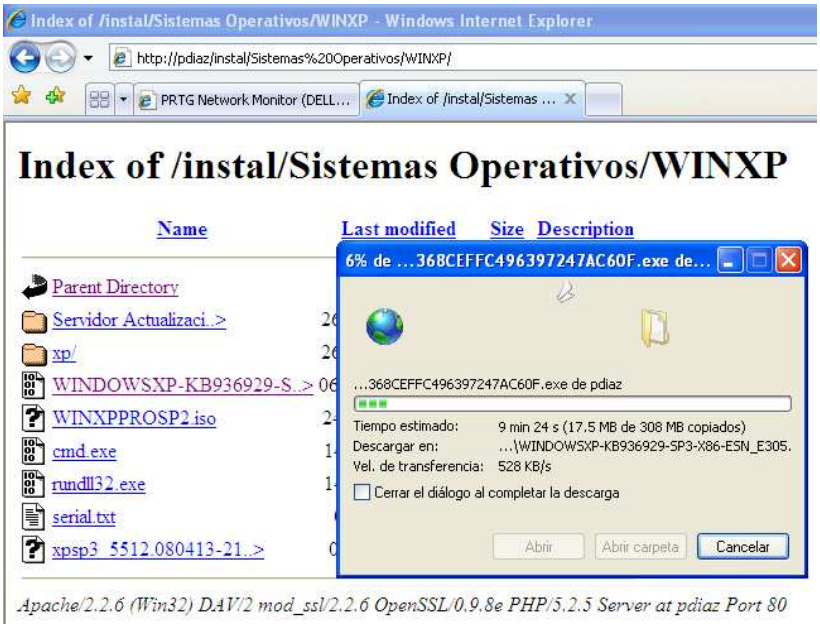


Figura 4.141 Descarga de un archivo sin restricción de la capacidad del canal VPN

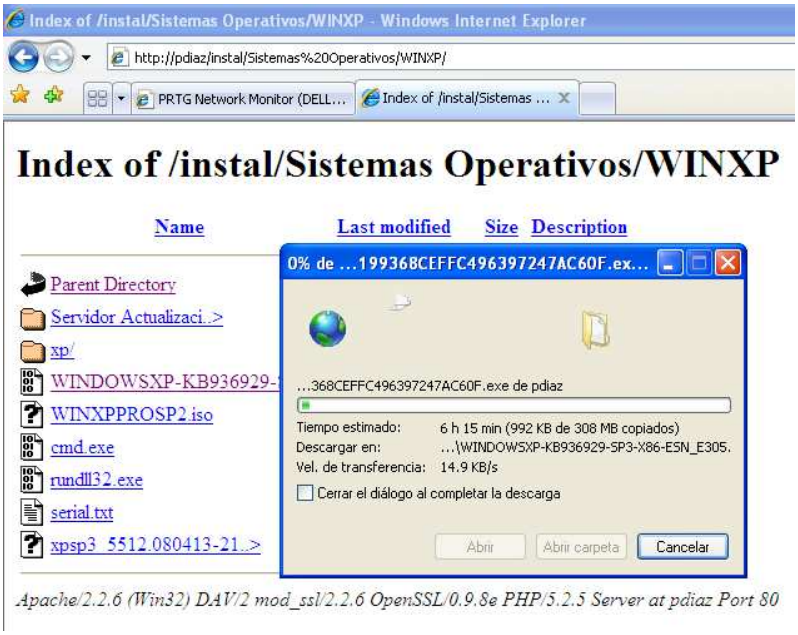


Figura 4.142 Descarga del mismo archivo pero con restricción del ancho de banda del enlace VPN

La política para este acceso en la modalidad de prueba, no se la ha habilitado el valor de ***Traffic Shapping***, y como se puede ver en la *figura 4.141* la tasa de transferencia no está controlado por lo que la descarga es muy rápida. Si esto sucede frecuentemente el acceso a Internet colapsaría, por lo tanto es imprescindible controlar el ancho de banda de esta política.

Para controlar este consumo excesivo se demostrará que al limitar el ancho banda con el ***Traffic Shapping*** fijando el valor a 128 kbps, se puede observar un cambio en la descarga y por lo tanto en la ocupación del canal.

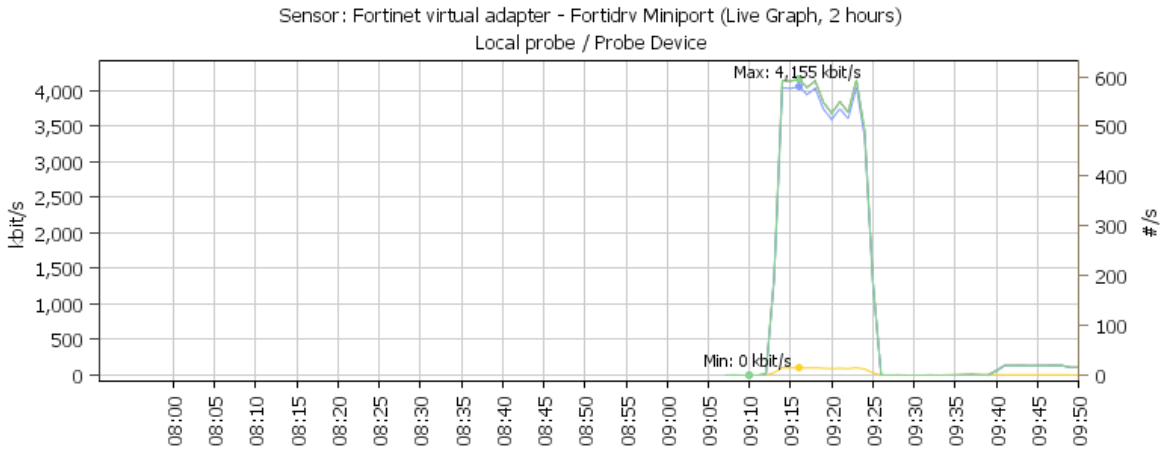


Figura 4.143 Reporte gráfico del tráfico generado en al interfaz virtual VPN

Cuando se realiza el cambio en la política se pierde la conexión y el cliente Forticlient solicita nuevamente el ingreso de los datos de autenticación. Una vez reconectado se procede a realizar nuevamente la misma descarga.

Al realizar este cambio se puede observar que la tasa de transferencia baja al valor especificado, es decir entre 14 Kbytes/s y 16 kbytes/s que corresponde aproximadamente a 128 kbps.

Sum (speed)	Traffic in (volume)	Traffic in (speed)	Traffic out (volume)	Traffic out (speed)
134 kbit/s	953 KByte	130 kbit/s	27 KByte	4 kbit/s
132 kbit/s	942 KByte	129 kbit/s	26 KByte	4 kbit/s
134 kbit/s	951 KByte	130 kbit/s	27 KByte	4 kbit/s
133 kbit/s	952 KByte	130 kbit/s	27 KByte	4 kbit/s
13 kbit/s	72 KByte	10 kbit/s	27 KByte	4 kbit/s
0.27 kbit/s	1 KByte	0.11 kbit/s	1 KByte	0.16 kbit/s
0.03 kbit/s	0 KByte	0 kbit/s	0.20 KByte	0.03 kbit/s
99 kbit/s	700 KByte	96 kbit/s	22 KByte	3 kbit/s
134 kbit/s	953 KByte	130 kbit/s	27 KByte	4 kbit/s
21 kbit/s	136 KByte	18 kbit/s	19 KByte	3 kbit/s
2,348 kbit/s	16,806 KByte	2,290 kbit/s	426 KByte	58 kbit/s
4,703 kbit/s	33,638 KByte	4,587 kbit/s	855 KByte	117 kbit/s
3,712 kbit/s	26,476 KByte	3,620 kbit/s	672 KByte	92 kbit/s
3,826 kbit/s	27,391 KByte	3,731 kbit/s	695 KByte	95 kbit/s
3,511 kbit/s	25,051 KByte	3,424 kbit/s	637 KByte	87 kbit/s
2,781 kbit/s	19,892 KByte	2,712 kbit/s	505 KByte	69 kbit/s

Figura 4.144 Detalle con valores tabulados de la velocidad de transmisión de las descargas realizadas

Un reporte histórico del tráfico generado con la interfaz virtual es mostrado en la *figura 4.143* donde la descarga realizada sin control de ancho de banda presenta valores altos de velocidad de transmisión con un pico de 4.155 kbps.

Luego de realizar la restricción del consumo del canal, la tasa de transferencia baja notablemente que en la gráfica no es posible divisar los valores, para lo cual se tiene el detalle de la *figura 4.144*, donde claramente se puede observar que los primeros 6 valores corresponden al tráfico sin restricción y los últimos 4 corresponden a la restricción de la política.

Como no se trata de un solo equipo que estará conectado se fijará la capacidad del enlace VPN para 5 enlaces lo que dará un total de 80 kbytes/s o 640 kbps.

4.7.2.2 Comportamiento del estado de las VPNs IPSEC *LAN – LAN* y monitoreo de los enlaces VPN IPSEC

Los enlaces de tipo *LAN – LAN* están en funcionamiento, lo que se realizará es un análisis de lo más relevante en el tráfico generado por estos enlaces virtuales.

Para visualizar el comportamiento del tráfico generado por la empresa SWITCHORM, se ha recogido la información almacenada en el analizador de

tráfico de la E.E.Q.S.A. en el que la *figura 4.145* muestra la ocupación del canal virtual, el cual indica que no tiene mucha actividad.

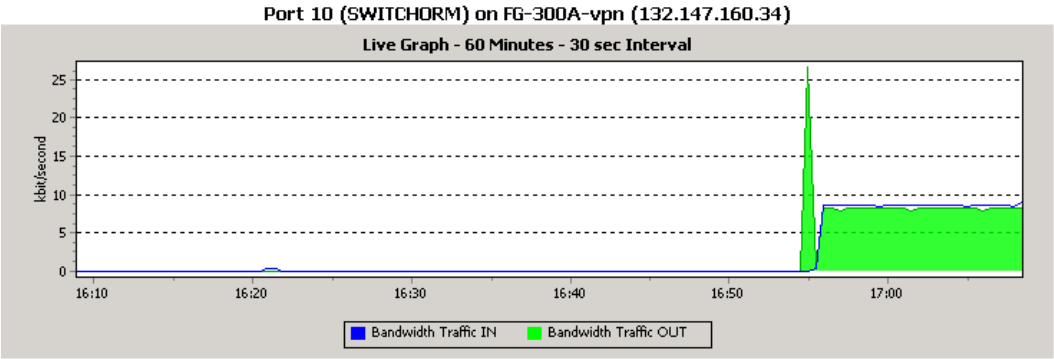


Figura 4.145 Gráfico de tráfico del enlace LAN - LAN con SWITCHORM

La actividad registrada en los últimos 15 minutos corresponde al PING realizado desde el *host* con dirección IP 132.147.163.55 hacia el servidor de SWITHCORM con dirección IP 192.168.14.13. El pico alto que se observa corresponde al establecimiento de la comunicación ya que se encontraba este enlace desconectado. La modalidad del servicio de recaudación provoca que no se obtenga mayores consumos del canal VPN, ya que en un determinado instante el servidor remoto realizará la actualización de la base de datos de la E.E.Q.S.A. y no constantemente.

Debido a un cambio en el modo de recaudación en línea, el cliente CITRIX no será utilizado en esta modalidad de acceso, por varios motivos administrativos; en su lugar los CARs deberán acceder a la base de datos de la E.E.Q.S.A. y actualizarla según el procedimiento de la Administración de Sistemas Informáticos y del Departamento de Desarrollo de *Software*. Este tipo de transacciones no presentan mayor consumo del canal, como se la ha observado en la *figura 4.145*. Es importante anotar que CITRIX fue la referencia para el diseño de la capacidad del canal, sin embargo con la nueva modalidad no produce un mayor consumo en el canal virtual.

Si esta modalidad se impone se puede presagiar que no existirá en corto plazo un incremento elevado en la ocupación del canal, ya que la política indica que los

equipos de las redes remotas solo tienen acceso al puerto TCP 1521 que corresponde al acceso al sistema de base de datos ORACLE. Sin embargo no está por demás asegurar que este canal esté fijado su capacidad en 128 kbps como máximo.

La *figura 4.146* muestra el monitoreo que se puede realizar a las conexiones VPN IPSEC desde la consola de administración del FG300A, también se puede apreciar la diferencia del tipo de VPNs IPSEC configuradas en el FG300A. El tipo ***Dialup*** corresponde al equipo de pruebas y que tiene dirección IP 172.16.20.51 para la interfaz virtual y la misma corresponde al *pool* de direcciones del DHCP configurado en el puerto 1.

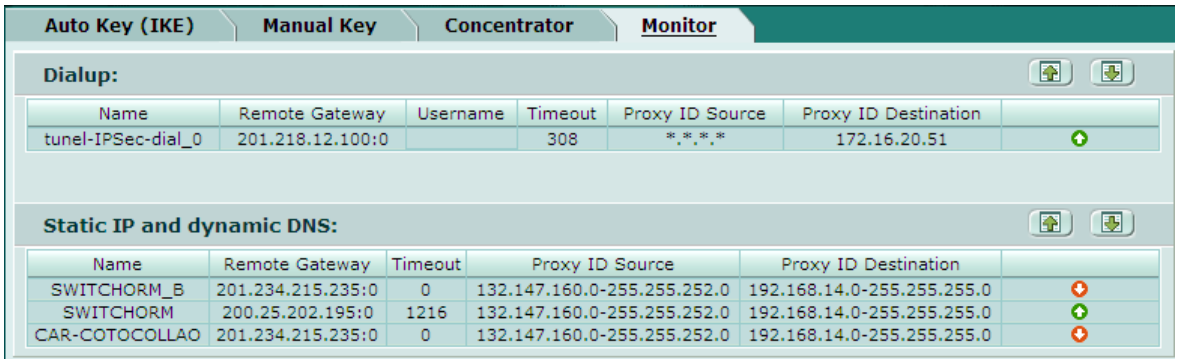


Figura 4.146 Monitoreo del estado de los enlaces VPN IPSEC

La información de la actividad del túnel ***Dialup*** sólo puede ser vista si la conexión está activa, caso contrario permanece el listado vacío. A diferencia del primer grupo de túneles el segundo grupo de nombre ***Static IP and dynamic DNS*** permanece en lista, ya que se ha creado interfaces virtuales dentro del FG300A, mientras estas interfaces permanezcan configuradas, el listado de estos túneles estará vigente aún cuando no exista actividad.

La *figura 4.147* muestra el listado de conexiones que utilizan el puerto UDP 500 para establecer una VPN IPSEC, estas dos sesiones corresponden a los enlaces VPN IPSEC que se encuentran de respaldo, periódicamente el FG300A emite estos mensajes para saber si el extremo remoto está disponible para realizar la respectiva conexión.

Line: 1 / 2 Clear All Filters

#	Protocol	Source Address	Source Port	Destination Address	Destination Port	Policy ID	Expiry (sec)	
1	udp	200.93.231.242	500	201.234.215.235	500		175	
2	udp	200.25.205.200	500	201.234.215.235	500		175	

Figura 4.147 Listado de sesiones que utilizan el puerto UDP 500

4.7.3 PRUEBA DE VoIP SOBRE VPN

Figura 4.148 Cliente con extensión 1000 realiza una llamada hacia la extensión 1001

Los equipos que intervendrán en esta prueba serán: el equipo de pruebas y el *host pdiaz* con dirección IP 132.147.163.55. Estos equipos tienen instalados y configurados los clientes de telefonía tal como se lo ha detallado en la sección 4.5.2 de este proyecto. El equipo de la red local de la E.E.Q.S.A. tiene activo y registrado el *softphone* con la extensión 1001 mientras que el equipo remoto realiza el establecimiento de la conexión VPN IPSEC de acceso remoto e inicia la aplicación *3CX VoIP Client* y se registra con la extensión 1000.

El equipo remoto de pruebas tiene la dirección IP 172.16.20.51 y desde este equipo se inicia una llamada hacia el equipo que se encuentra en la red LAN de la E.E.Q.S.A., es decir se realiza la llamada desde la extensión 1000 hacia la extensión 1001 y se inicia una conversación donde los usuarios que utilizan estos

equipos mantienen una conversación normal de telefonía (Ver *figura 4.148*). El servidor de telefonía IP o PBX registra que las extensiones 1000 y 1001 están conectadas tal como se puede apreciar en la *figura 4.149*.

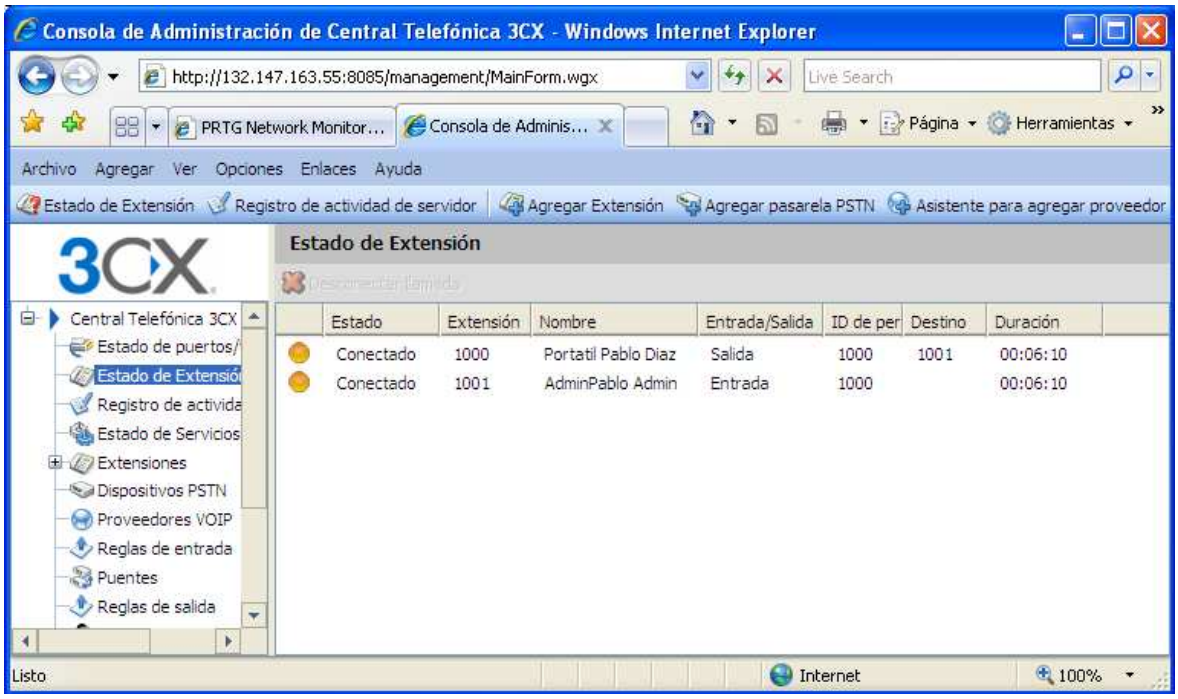
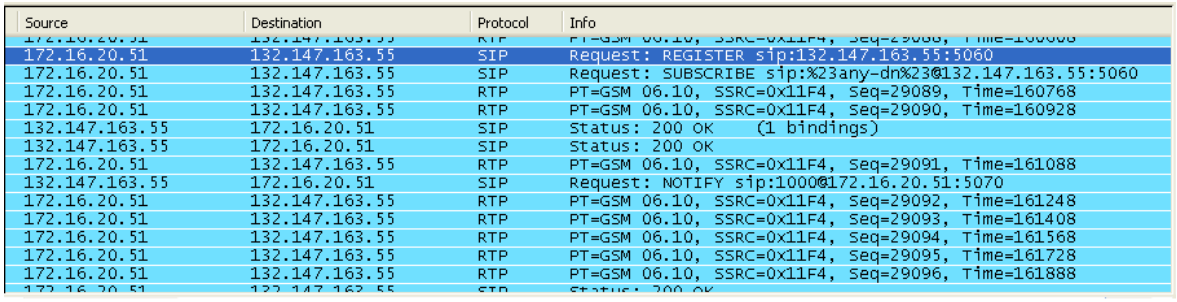


Figura 4.149 Consola de administración de la PBX muestra el estado de las extensiones que mantienen una llamada

Mientras la conversación se inicia, dura y se libera, internamente la interfaz Fast-Ethernet del equipo local y la interfaz del equipo de pruebas intercambian paquetes con los datos de voz. Nuevamente se utiliza la aplicación Wireshark para observar el intercambio de paquetes y tramas. La *figura 4.150* permite mostrar la información de las tramas cuando se inicia la conversación de VoIP.

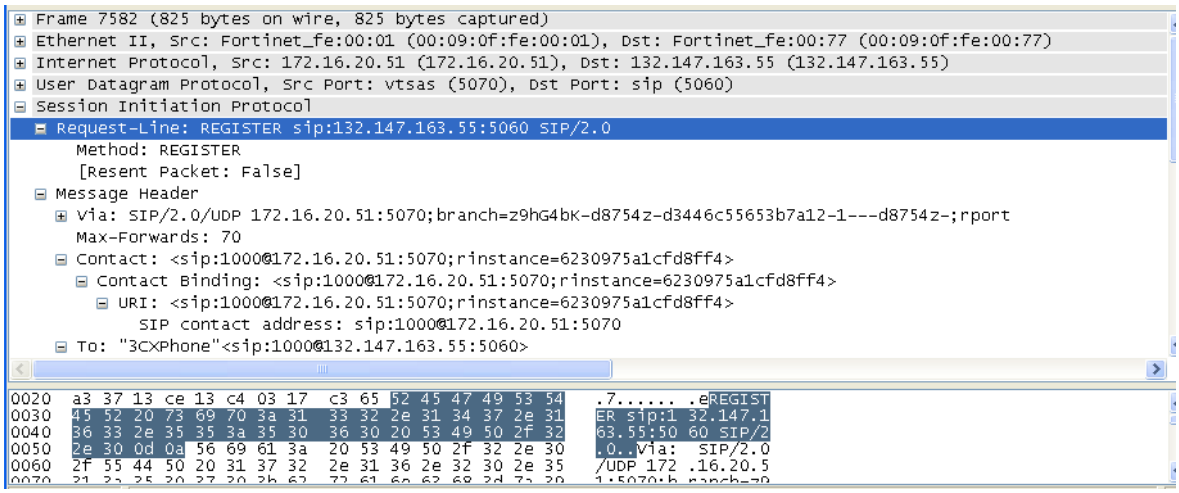
La primera trama en su contenido tiene información que indica que las direcciones MAC ADDRESS de los equipos que intervienen son del fabricante Fortinet lo que es lógico ya que los interfaces que mantienen la conversación a nivel de capa 2 son el FG300A y la interfaz virtual Forticlient. La dirección origen es la remota 172.16.20.51 y la destino la local 132.147.163.55, el puerto que se utiliza es el UDP 5070 para el origen y el UDP 5060 para el destino.



Source	Destination	Protocol	Info
172.16.20.51	132.147.163.55	SIP	Request: REGISTER sip:132.147.163.55:5060
172.16.20.51	132.147.163.55	SIP	Request: SUBSCRIBE sip:%23any-dn%23@132.147.163.55:5060
172.16.20.51	132.147.163.55	RTP	PT=GSM 06.10, SSRC=0x11F4, Seq=29089, Time=160768
172.16.20.51	132.147.163.55	RTP	PT=GSM 06.10, SSRC=0x11F4, Seq=29090, Time=160928
132.147.163.55	172.16.20.51	SIP	Status: 200 OK (1 bindings)
132.147.163.55	172.16.20.51	SIP	Status: 200 OK
172.16.20.51	132.147.163.55	RTP	PT=GSM 06.10, SSRC=0x11F4, Seq=29091, Time=161088
132.147.163.55	172.16.20.51	SIP	Request: NOTIFY sip:1000@172.16.20.51:5070
172.16.20.51	132.147.163.55	RTP	PT=GSM 06.10, SSRC=0x11F4, Seq=29092, Time=161248
172.16.20.51	132.147.163.55	RTP	PT=GSM 06.10, SSRC=0x11F4, Seq=29093, Time=161408
172.16.20.51	132.147.163.55	RTP	PT=GSM 06.10, SSRC=0x11F4, Seq=29094, Time=161568
172.16.20.51	132.147.163.55	RTP	PT=GSM 06.10, SSRC=0x11F4, Seq=29095, Time=161728
172.16.20.51	132.147.163.55	RTP	PT=GSM 06.10, SSRC=0x11F4, Seq=29096, Time=161888

Figura 4.150 Generación de paquetes al iniciar una sesión de tipo SIP

La información del protocolo SIP revela los datos del registro de la extensión y la marca del equipo cliente, entre otros parámetros (Ver *figura 4.151*).



```
⊞ Frame 7582 (825 bytes on wire, 825 bytes captured)
⊞ Ethernet II, Src: Fortinet_fe:00:01 (00:09:0f:fe:00:01), Dst: Fortinet_fe:00:77 (00:09:0f:fe:00:77)
⊞ Internet Protocol, Src: 172.16.20.51 (172.16.20.51), Dst: 132.147.163.55 (132.147.163.55)
⊞ User Datagram Protocol, Src Port: vtsas (5070), Dst Port: sip (5060)
⊟ Session Initiation Protocol
  ⊟ Request-Line: REGISTER sip:132.147.163.55:5060 SIP/2.0
      Method: REGISTER
      [Resent Packet: False]
  ⊟ Message Header
    ⊞ Via: SIP/2.0/UDP 172.16.20.51:5070;branch=z9hG4bK-d8754z-d3446c55653b7a12-1---d8754z-;rport
      Max-Forwards: 70
    ⊟ Contact: <sip:1000@172.16.20.51:5070;rinstance=6230975a1cfd8ff4>
      ⊟ Contact Binding: <sip:1000@172.16.20.51:5070;rinstance=6230975a1cfd8ff4>
        ⊟ URI: <sip:1000@172.16.20.51:5070;rinstance=6230975a1cfd8ff4>
            SIP contact address: sip:1000@172.16.20.51:5070
    ⊟ To: "3CXPhone"<sip:1000@132.147.163.55:5060>
```

```
0020  a3 37 13 ce 13 c4 03 17  c3 65 52 45 47 49 53 54   .7...... .eREGIST
0030  45 52 20 73 69 70 3a 31  33 32 2e 31 34 37 2e 31   ER sip:1 32.147.1
0040  36 33 2e 35 35 3a 35 30  36 30 20 53 49 50 2f 32   63.55:50 60 SIP/2
0050  2e 30 0d 0a 56 69 61 3a  20 53 49 50 2f 32 2e 30   .0..Via:  SIP/2.0
0060  2f 55 44 50 20 31 37 32  2e 31 36 2e 32 30 2e 35   /UDP 172 .16.20.5
0070  31 3a 35 30 37 30 3b 62  72 61 6e 63 68 3d 7a 39   1:5070;b ranch=z9
```

Figura 4.151 Detalle de la trama de inicio de la sesión SIP

En la *figura 4.150* se puede observar que luego del establecimiento de la llamada telefónica se generan paquetes de tipo RTP, donde claramente se puede apreciar que el códec utilizado es GSM.

Todo este proceso de establecimiento y duración de la conversación ha generado una ocupación del canal VPN; esta ocupación mostrada en la *figura 4.152* indica que una conversación telefónica a través de este medio consume un alto porcentaje del canal virtual, el canal tiene 128 kbps de capacidad y el pico de la conversación llega a 93 kbps es decir el 72.65 % del canal es utilizado en la conversación lo que deja un 27.35 % es decir 35 kbps disponibles para otras aplicaciones.

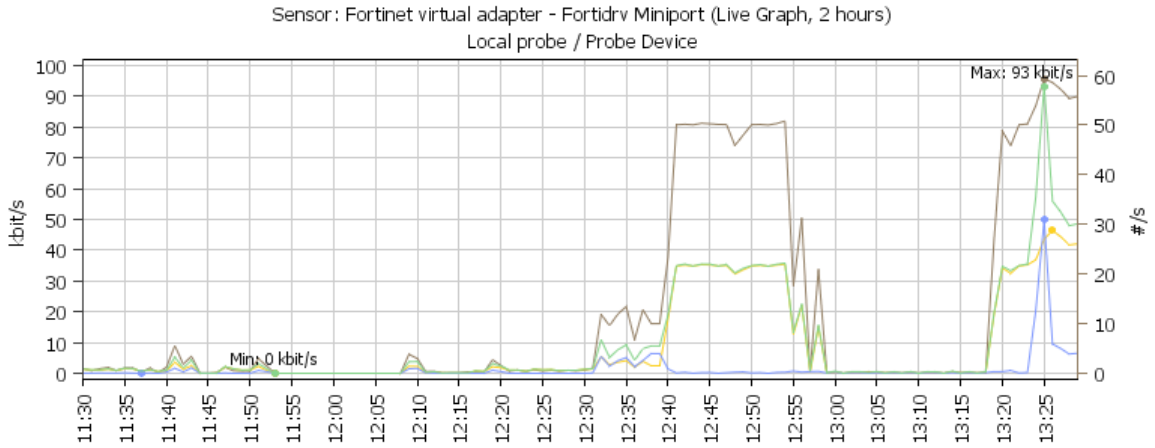


Figura 4.152 Ocupación del canal generado por la llamada de tipo SIP sobre el canal VPN

CAPÍTULO 5

CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- El proceso de modernización de la E.E.Q.S.A. ha permitido que en el área de tecnología informática se estén implementado mecanismos de mejora para brindar a la sociedad un mejor servicio. En el caso de las Redes Privadas Virtuales al ser implementadas, los procesos correspondientes a recaudación obtienen una significante mejora y la empresa aumenta su imagen corporativa.

- El nuevo equipo de seguridad perimetral ha permitido que el administrador mejore su productividad al poder realizar configuraciones en mucho menor tiempo que el utilizado cuando tenía que configurar el *IBM SecureWay Firewall*. Ahora lo puede hacer de forma remota a través de una sesión HTTPS o una conexión SSH, ofreciendo seguridad en la administración y gestión del FG300A.

- Al dimensionar el canal de comunicaciones se pudo establecer la capacidad que se debería obtener para ejecutar el sistema de recaudación así como el de telefonía, más aun, este dimensionamiento ha permitido que desde el equipo de seguridad perimetral FG300A se garantice la capacidad dimensionada a través del ***Traffic Shaping*** configurable en cada política, con lo cual se han obtenido dos beneficios: el primero es que el usuario remoto o red remota sabe el requerimiento de velocidad de transmisión para obtener un sistema adecuado, lo que le obliga a cumplir con el requerimiento; y el segundo, que la E.E.Q.S.A. asegura que quienes de alguna manera excedan sus accesos de última milla a Internet en relación al valor dimensionado, no saturen el acceso de última milla corporativo de la E.E.Q.S.A.. Muestra de ello es lo realizado en las pruebas de tráfico, en las que se verificó que al no tener controlado la capacidad del canal, automáticamente se utilizó toda la capacidad del medio para realizar la

descarga de prueba, lo que indica que fácilmente esta puerta de acceso se puede convertir en una amenaza si no es controlada.

- La red de datos corporativa de la E.E.Q.S.A., es una red ampliamente diversa tanto en lugares o sitios a donde llega la información, como también de los medios de transmisión que se necesita para llegar a estos sitios donde se encuentran las diferentes dependencias de la E.E.Q.S.A.. Esto no ha impedido que funcionen sobre una plataforma completamente IP, lo que hace que se pueda acceder desde el Internet por medio de una VPN sin complicaciones, ya que las velocidades de transmisión que se manejan para llegar al edificio matriz permiten tiempos de respuesta aceptables (igual o superior a 1024 kbps), lo cual implica que al acceder desde el Internet no serán críticos los tiempos de respuesta al tratar de ingresar a un *host* que se encuentra por ejemplo en alguna agencia rural o central de generación y que están a grandes distancias del edificio matriz.

- El aumento de equipos de escritorio y portátiles así como nuevos empleados que tienen asignado un equipo de éstos, implica un incremento de entradas de acceso al correo electrónico y al Internet. Con el anterior equipo la frecuencia de interrupciones por el colapso de nuevas sesiones sería un grave problema; el nuevo equipo ha demostrado que se puede seguir incrementado usuarios ya que la capacidad máxima está todavía lejos de ser alcanzada.

- El mantenimiento del equipo de seguridad perimetral se ha reducido en casi el 100 % ya que no requiere un mantenimiento programado como el que se lo realizaba al *IBM SecureWay Firewall*.

- Se ha podido comprender que el recurso de acceso a Internet puede ser explotado de mejor manera, utilizando de manera productiva para procesos en los cuales se los realizaba manualmente, como ha sido la recaudación realizada por los CARs y las revisiones realizadas por los operadores de turno.

- Los operadores que manejan equipos portátiles y que acceden a Internet a través de los modems celulares, muy frecuentemente realizan trabajos e inspecciones donde se requiere que el ingreso de los datos al sistema SIDECOM se lo realice en línea. Se conoce que el medio inalámbrico presenta serios problemas respecto a la velocidad con la que se puede conectar al Internet. En los equipos de estos usuarios, se les ha configurado el acceso a la E.E.Q.S.A. por medio de VPN PPTP ya que no requiere una configuración avanzada; el establecimiento de la conexión es rápida respecto a IPSEC y no genera tanto *overhead* como lo hace IPSEC

- La introducción de un puerto de *trunk* IEEE 802.1q ha permitido un cambio en la topología de la red de la E.E.Q.S.A. específicamente en la parte de la extranet. Las empresas externas dejarán de ingresar directamente a los segmentos de red de la E.E.Q.S.A. y cada enlace podrá ser manejado bajo políticas entre segmentos de red e interfaces virtuales de tipo VLAN que corresponderían a las empresas externas. Esta configuración con el IBM *SecureWay Firewall* no habría sido posible ya que cada interfaz de este equipo no puede manejar IEEE 802.1q; además al configurar la VPN IPSEC en el modo *LAN – LAN* se pudo realizar el levantamiento del enlace sin mayores complicaciones. Esto confirma que al estar el equipo actualizado con los protocolos de seguridad, permite una interoperabilidad con otros equipos de diferentes fabricantes que también deben estar actualizados; de igual manera esto no habría sido posible con el equipo de seguridad anterior.

- Tanto las aplicaciones de tipo virtual CITRIX, cliente servidor y *web* no tendrán inconveniente en ser ejecutados sobre el canal VPN, ya que se ha demostrado a través de las pruebas que la ejecución de estas aplicaciones estará limitada por la capacidad de acceso a Internet. En ese caso se ha determinado en el diseño de este proyecto, los valores referenciales para una óptima respuesta de los aplicativos más importantes que se ejecutarían sobre una VPN.

- Al tener un límite en la creación de cuentas de usuario locales sobre el FG300A se abre la necesidad de utilizar un tercer elemento como es el servidor RADIUS que sirva exclusivamente para la autenticación de usuarios. El servidor permite un crecimiento de cuentas de usuario necesarias el cual no será un problema y que además podrá ser gestionado y servirá para los procesos de auditoría en su debido momento.

- El acceso a los recursos informáticos a través de un canal seguro proporciona a los administradores de los sistemas informáticos rapidez en la detección y solución de problemas; basta que el técnico tenga un acceso a Internet y éste podrá conectar a la red corporativa de la E.E.Q.S.A. y solucionar los diferentes problemas que se susciten sin tener que realizar grandes traslados que en muchos casos pueden ser innecesarios.

- La VPN SSL con el cliente liviano permite a los usuarios tener la facilidad de poder conectarse a la red la E.E.Q.S.A. sin tener que configurar o que un técnico del Departamento de Comunicaciones y Redes lo esté asesorando continuamente.

- Los CARs con gran capacidad de gestión están empezando a explotar la capacidad que ofrece la conexión VPN IPSEC de tipo *LAN – LAN* de la E.E.Q.S.A. con lo que se ratifica la creación de este proyecto. A su vez este proyecto inyectará una amplia documentación con la cual los técnicos del Departamento de Comunicaciones y Soporte podrán crear y ejecutar redes privadas virtuales tanto para usuarios internos como externos.

- La E.E.Q.S.A. al ofrecer a los CARs accesos de tipo VPN ha permito que éstos mejoren su nivel de servicio hacia la comunidad; la E.E.Q.S.A. por su parte puede realizar en tiempo real consultas de los abonados para realizar los respectivos informes y cierres de caja. Estos procesos propios del sistema de recaudación se agilita brevemente al tener registrado y actualizado el cobro de facturas en el sistema de base de datos. Mientras

los CARs vayan implementado sus accesos hacia la E.E.Q.S.A. por medio de la VPN, los procesos serán más ágiles y la información será más confiable que el generado de forma manual, y a un costo mínimo.

- La implementación de la Telefonía IP ha permitido comprobar que las conversaciones pueden ser realizadas a través del canal VPN con calidad aceptable lo que permite mantener conversaciones fuera de la red corporativa tanto de datos como de voz. Éste es el primer paso para justificar y llevar a cabo un proyecto de telefonía íntegramente IP y motivar a los altos funcionarios de la E.E.Q.S.A. sobre las ventajas que pueden llegar a tener un sistema que permita establecer conversaciones de voz dentro y fuera de la E.E.Q.S.A. con la ayuda del Internet.

- Esta implementación es el primer paso a un amplio campo de aplicación sobre las redes que está instalando a largo del área de concesión; se espera que a corto o mediano plazo sobre la infraestructura de fibra óptica y equipos de conectividad autoridades y técnicos tomen la iniciativa de este proyecto en el aspecto de la importancia de las redes privadas virtuales y sus aplicaciones para implementar una red MPLS y sobre ésta implementar VPNs de altas velocidades de transmisión.

- La VPN en un inicio se focalizó sobre el Internet, sin embargo la VPN se ha extendido sobre enlaces privados lo que permite que el acceso corporativo de Internet no se vea reducido y por otra parte se pueda seguir con la ampliación de VPNs. Se estima que las VPNs tomen un giro más popular entre los empleados a corto plazo, sobre todo en aquellos que por razones de la naturaleza del puesto de trabajo sean usuarios móviles o remotos. En el caso de los accesos *LAN – LAN* se espera que todas las empresas que tienen convenios con la E.E.Q.S.A. ingresen a través de esta modalidad llegando a establecer un procedimiento con el cual los nuevos enlaces deban cumplir con una serie de requerimientos para establecer la VPN IPSEC. Con lo que se llegaría a una modernización, actualización y mejora en la gestión de enlaces que no pueden ser controlados en su totalidad y

para lo cual se requiere de la ayuda de mecanismos de seguridad como el implementado.

- Las VPNs ahora forman parte de la estructura de la red corporativa de la E.E.Q.S.A., lo cual indica que cuando se llegue a agotar la capacidad de establecimiento de túneles VPN se analice la posibilidad de adquirir un equipo de superiores características técnicas que permitan ampliar la capacidad de túneles VPN; paralelamente a esto se espera que la capacidad de la última milla para el acceso a Internet se incremente según las necesidades, ya no solo en la navegación de sitios *web,* sino para incrementar los accesos VPN, es decir que se espera mantener y hacer de las VPNs un medio y herramienta que facilite las labores empresariales en todos los niveles de la E.E.Q.S.A.

5.2 RECOMENDACIONES

- El FG300A requiere de complementos para garantizar la seguridad en la red corporativa de la E.E.Q.S.A. Si bien es cierto este equipo posee la capacidad de protegerse de ataques de virus, *Spyware* y otras amenazas, los huecos de seguridad aparecen en los sitios más débiles, que son los equipos de escritorio y portátiles. Es necesario contar con un adecuado sistema de antivirus y un sistema de actualizaciones de sistemas operativos *Microsoft Windows*.

- Los CARs al no tener bien claro cómo acceder a la red corporativa de la E.E.Q.S.A. han adoptado el acceso por medio de VPN de tipo *LAN – LAN*; esto sugiere que se instale un enlace por cada CAR. Si bien es cierto el FG300A soporta grandes cantidades de sesiones, no es práctico que cada CAR instale un enlace hacia la E.E.Q.S.A., lo recomendable será utilizar proveedores de servicios que lleguen con una infraestructura robusta a la E.E.Q.S.A. como Andinadatos y Telconet.

- Es necesario que se pueda adquirir el equipo de seguridad perimetral de respaldo ya que éste mejorará la disponibilidad del acceso hacia redes externas de la E.E.Q.S.A. como el Internet. Para garantizar que el respaldo sea un éxito se recomienda implementar el estudio realizado en este proyecto.

- El sistema de Telefonía de VoIP implementado en este proyecto no contempla un equipamiento ni un plan de numeración específico a nivel corporativo, sin embargo puede solucionar la demanda de requerimientos puntuales. Lo recomendable es establecer un proyecto de migración de la telefonía híbrida que funciona actualmente hacia un completo y robusto sistema de telefonía IP, el cual sería explotado ampliamente sobre las VPN que están en funcionamiento, lo que permitiría una amplia mejoría en el desempeño de actividades vinculadas a reuniones, conferencias, presentaciones, etc. de empleados que están fuera de los predios de la E.E.Q.S.A. También se puede llegar a obtener movilidad sin desconectarse de la oficina y promover de mejor manera los servicios y actividades que ofrece la E.E.Q.S.A.

- Es importante que el servidor RADIUS que está implementado se lo migre sobre un equipo físico con arquitectura de servidor lo cual permitiría una fiabilidad y una alta disponibilidad para el servicio de autenticación, también dentro de este aspecto sería importante que paulatinamente los sistemas se apoyen sobre este servidor para realizar la autenticación de usuarios. Un ejemplo podría ser el ingreso a los equipos de comunicaciones como *switches*, *routers*, *Gateway*s de telefonía, etc., que al tener registrado los accesos de los usuarios sobre un servidor se mejoraría la seguridad en cuanto al personal autorizado que manipula las configuraciones de los equipos de la infraestructura de red.

- Cuando un usuario requiera acceder o establecer una VPN con PPTP, SSL o IPSEC, es necesario saber qué tipo de conexión hacia Internet se dispone. No todas las empresas permiten que desde el interior de la red se

pueda ejecutar una VPN, ya que cuentan con *proxys* que solo permiten navegación por Internet con los protocolos más comunes como HTTP, HTTPS, SMTP, TELNET, POP3, etc. pero no están habilitados los protocolos IPSEC, PPTP o SSL.

- Al momento de implementar la política que especifica la navegación hacia el Internet de la mayoría de los usuarios de la E.E.Q.S.A., no tiene controlado la capacidad del canal. Es importante realizar una distribución adecuada del capacidad del canal, de tal manera que usuarios críticos como Funcionarios y Ejecutivos, Administradores de los Sistemas Informáticos y varios equipos servidores, tengan garantizado un ancho de banda del enlace de última milla hacia el Internet, con lo cual se priorizaría el recurso informático llegando a una optimización del mismo.

- El FortiAnalyzer es el complemento del FG300A para la gestión de reportes, por lo tanto los administradores deberán colocar en funcionamiento lo más pronto posible este equipo que ayudará a revisar las incidencias que se puedan suscitar dentro de la red. Una breve gestión y un buen conocimiento en el manejo de reportes disminuye los tiempos de respuesta ante problemas que se puedan presentar en el equipo de seguridad perimetral.

- Para mejorar el control de tráfico en los diferentes segmentos principales que se conectan al FG300A, es preciso profundizar en el manejo del módulo IPS, ya que con una configuración con un alto grado de conocimiento, ofrecería una mejora en la utilización de un determinado enlace, que podría ser el acceso a Internet; esto presume que un técnico se especialice en el manejo de políticas y del módulo IPS del FG300A hasta lograr una configuración que se adapte de manera óptima en la red corporativa de la E.E.Q.S.A.

- Para mejorar la seguridad en todos los enlaces y accesos desde redes externas hacia la E.E.Q.S.A. se debe implementar un procedimiento formal

que sea parte de las políticas de acceso y que sea auditado; esto lleva a garantizar la seguridad en los accesos y una mejora en la supervisión por parte de terceros.

- Los enlaces que aun no han ingresado por medio del FG300A se recomienda que deben ingresar por el mismo y exigir que se implemente un túnel VPN IPSEC para garantizar la confidencialidad e integridad sobre los datos que la E.E.Q.S.A. debe compartir.

- El FG300A puede ser manejado y puesto en funcionamiento gracias al sistema operativo FortiOS. Este sistema operativo tiene varias versiones, la versión con la que llegó a la E.E.Q.S.A. fue la 2.80 la cual incluye todas las funcionalidades revisadas en éste proyecto. Durante la realización del proyecto se realizó una actualización del sistema operativo a la versión 3.00 MR4, la cual entre otras funcionalidades, amplía aplicaciones de tipo colaborativos (Escritorios Remotos con RDP y VNC) a VPN SSL. Esto demuestra que es importante revisar las bondades de las nuevas versiones del FortiOS para saber si es o no conveniente actualizar el sistema operativo. Si se toma la decisión de actualizar el FortiOS se recuerda que se debe respaldar el archivo de configuración para evitar la eliminación permanente de la configuración del equipo que si toma tiempo considerable en la puesta a punto.

REFERENCIAS BIBLIOGRÁFICAS

[1] WIKIPEDIA LA ENCICLOPEDIA LIBRE, Red privada virtual, Tipos de VPN http://es.wikipedia.org/wiki/Red_privada_virtual

[2] APUNTES DE CLASE SEGURIDAD EN REDES, Ing. Nelson Ávila.

[3] WORLD METEOROLOGICAL ORGANIZATION, Guide for Virtual Private Networks (VPN) via the Internet between GTS centres, World Meteorological Organization Commission for Basic Systems Opag on Information Systems & Services http://www.wmo.int/pages/prog/www/TEM/ICT-ISS2002/guideVPN.doc.

[4] CISCO SYSTEMS, Controlling Security Threats. http://www.cisco.com/go/tds

[5] FORTINET, FortiGate-3600 Security System, ADVANCED REAL-TIME DATA SECURITY SOLUTIONS. http://www.fortinet.com/doc/

[6] ASTARO INTERNET SECURITY. http://www.astaro.com/our_products/astaro_security_gateway/software_appliance.

[7] ALCATEL, Alcatel Vision for Secured Next Generation Networks. http://www.alcatel-lucent.com/wps/portal/WhitePapers/Detail?LMSG_CABINET=Docs_and_Resource_Ctr&LMSG_CONTENT_FILE=White_Papers/Vision_for_Secured_NGN.pdf

[8] NEWPORT NETWORKS, VoIP Bandwidth Calculation, 2005. ftp://ftp.ui.edu/onnopurbo/library/library-ref-eng/ref-eng-3/physical/voip/52-VoIP-Bandwidth.pdf

[9] CISCO SYSTEMS, SSL VPN Guía de configuración CISCO IOS.

[10] ALCATEL, VPNS BGP/MPLS: TUTORIAL Y CONSIDERACIONES DE ESCALAMIENTO. http://www1.alcatel-lucent.com/doctypes/articlepaperlibrary/pdf /ATR2004Q4/ T0411-MPLS-VPN-ES.pdf

[11] METRO ETHERNET FORUM, Metro Ethernet Services - A Technical Overview
http://metroethernetforum.org/PDF_Documents/metro-ethernet-services.pdf

[12] ALCATEL, TUTORIAL TÉCNICO DEL VPLS.
http://www1.alcatel-lucent.com/doctypes/articlepaperlibrary/pdf/ATR2004Q4/T0411-VPLS-ES.pdf

[13] XS INTERNATIONAL, Welcome to the IBM store.
http://www.xsnet.com/retail/XQ/catalog_name.IBM/category_name.RS+6000/parent_category_name.RS+6000/product_id.IBM-RS6000-SYS-7046-B50-512-2x18/QX/xsi.product.asp

[14] IBM, IBM SecureWay Firewall para AIX, Guía del usuario, Herramientas de IBM Firewall Versión 4 Release 2, Número de documento GC10-3277-03

[15] DANSK IT MANAGEMENT, Teleworker.
http://www.telemanagement.dk/44_teleworker.htm

[16] CISCO SYSTEMS, Voice and Video Enabled IPSec VPN (V3PN) Solution Reference Network Design.
http://www.cisco.com/application/pdf/en/us/guest/netsol/ns241/c649/ccmigration_09186a0080146c8e.pdf

[17] ITS TELECOM, Convergencia Fijo-Móvil - Gateways Celulares.
http://www.ipbusiness.net/uploads/solutions/its.pdf

[18] CISCO SYSTEMS, Understanding Voice over IP Protocols.
http://www.cisco.com/application/pdf/en/us/guest/tech/tk587/c1506/ccmigration_09186a008012dd36.pdf

[19] CISCO SYSTEMS, Cisco Introduces Broad Support for SIP across Packet Voice Products.
http://www.cisco.com/application/pdf/en/us/guest/tech/tk701/c1482/ccmigration_09186a00800b3f21.pdf

[20] IEEE COMMUNICATIONS MAGAZINE - July 2000, CDMA/HDR: A Bandwidth-Efficient High-Speed Wireless Data Service for Nomadic Users.
http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=852034

[21] WIKIPEDIA LA ENCICLOPEDIA LIBRE, Point-to-Point Protocol.
http://es.wikipedia.org/wiki/Point-to-Point_Protocol

[22] CISCO SYSTEMS, Cisco ASA 5500 Series Adaptive Security Appliance Platform And Module Datasheet. http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/product_data_sheet0900aecd802930c5.html

[23] FORTINET, FortiGate 200-800 Series. http://www.fortinet.com/doc/FGT200_800DS.pdf

[24] TIPPINGPOINT, TippingPoint Intrusion Prevention Systems. http://www.tippingpoint.com/products_ips.html

[25] ASTARO INTERNET SECURITY, Astaro Security Gateway Software Appliance. http://www.astaro.com/products/astaro-security-gateway-software-appliance

[26] FORTINET, FortiGate 300A Installation Guide Version 2.80 MR5 2005. http://docs.fortinet.com/fgt/archives/install/01-28005-0092-20041015_FortiGate-300A_Installation_Guide.pdf